Distributed Programming using Role-Parametric Session Types in Go

Statically-Typed Endpoint APIs for Dynamically-Instantiated Communication Structures

DAVID CASTRO, Imperial College London, United Kingdom
RAYMOND HU, Imperial College London, United Kingdom
SUNG-SHIK JONGMANS, Open University of the Netherlands, The Netherlands and Imperial College London, United Kingdom
NICHOLAS NG, Imperial College London, United Kingdom
NOBUKO YOSHIDA, Imperial College London, United Kingdom

This paper presents a framework for the static specification and safe programming of message passing protocols where the number and kinds of participants are *dynamically* instantiated.

We develop the first theory of *distributed* multiparty session types (MPST) to support parameterised protocols with indexed roles—our framework statically infers the different kinds of participants induced by a protocol definition as *role variants*, and produces *decoupled* endpoint projections of the protocol onto each variant. This enables safe MPST-based programming of the parameterised endpoints in distributed settings: each endpoint can be implemented separately by different programmers, using different techniques (or languages). We prove the decidability of role variant inference and well-formedness checking, and the correctness of projection.

We implement our theory as a toolchain for programming such role-parametric MPST protocols in Go. Our approach is to generate API families of lightweight, protocol- and variant-specific type wrappers for I/O. The APIs ensure a well-typed Go endpoint program (by native Go type checking) will perform only compliant I/O actions w.r.t. the source protocol. We leverage the abstractions of MPST to support the specification and implementation of Go applications involving multiple channels, possibly over mixed transports (e.g., Go channels, TCP), and channel passing via a unified programming interface. We evaluate the applicability and run-time performance of our generated APIs using microbenchmarks and real-world applications.

CCS Concepts: • **Computing methodologies → Distributed programming languages**; • **Software and its engineering → Source code generation**; **Concurrent programming languages**;

Additional Key Words and Phrases: multiparty session types, indexed roles, distributed programming, Go

ACM Reference Format:
David Castro, Raymond Hu, Sung-Shik Jongmans, Nicholas Ng, and Nobuko Yoshida. 2019. Distributed Programming using Role-Parametric Session Types in Go: Statically-Typed Endpoint APIs for Dynamically-Instantiated Communication Structures. *Proc. ACM Program. Lang.* 3, POPL, Article 29 (January 2019), 30 pages. https://doi.org/10.1145/3290342

Authors' addresses: David Castro, Department of Computing, Imperial College London, United Kingdom, d.castro-perez@imperial.ac.uk; Raymond Hu, Department of Computing, Imperial College London, United Kingdom, raymond.hu@imperial.ac.uk; Sung-Shik Jongmans, Department of Computer Science, Open University of the Netherlands, The Netherlands, ssj@ou.nl, Department of Computing, Imperial College London, United Kingdom; Nicholas Ng, Department of Computing, Imperial College London, United Kingdom, nickng@imperial.ac.uk; Nobuko Yoshida, Department of Computing, Imperial College London, United Kingdom, n.yoshida@imperial.ac.uk.

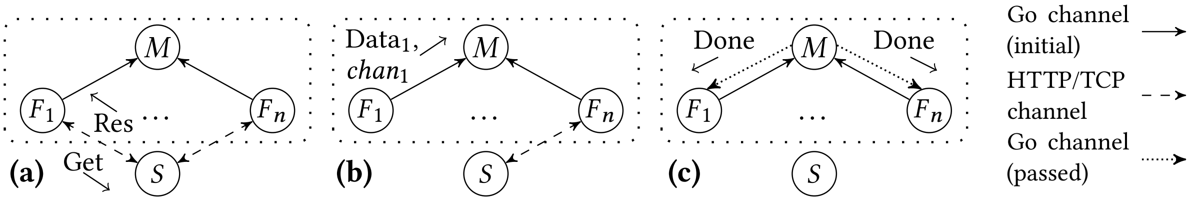


Fig. 1. Distributed and shared memory communications in a role-parametric parallel HTTP downloader.

1 BACKGROUND

1.1 Channel-Based Concurrent and Distributed Programming in Go

Go is a popular industrial systems language.[1] One of its primary design features is first-class language support for lightweight concurrency on multicore machines. Go offers easy spawning of parallel coroutines, called *goroutines*, that are transparently multiplexed over an underlying set of system threads. Goroutines communicate and synchronize via message passing over typed *channels*, designed to alleviate the difficulties of low-level mechanisms such as mutexes, condition variables and memory barriers commonly used in systems programming. As first-class objects, an interesting and *useful* feature is the ability to pass *channels over channels*.

Go is also well-established in distributed systems; e.g., it is the implementation language of frameworks such as Kubernetes, Docker and Jaeger. As the aforementioned concurrency features of Go are specific to shared memory, a significant class of distributed programming in Go is conducted using channel-based networking libraries via TCP, HTTP, etc. as transports. Developers appreciate Go since distributed programming in practice often involves local concurrency: goroutines and channels are effective for dealing locally with the inherent asynchrony of distributed interactions.

We illustrate such an application that integrates shared memory and distributed concurrency as a running example, a parallel downloader (e.g., HTTP) which we refer to as Pget.[2] Fig. 1 depicts the components of the application and the communication structures that arise.

(a) There are three categories of participants, one Master (M), $n > 0$ Fetchers (F), and one Server (S). M creates a *worker pool* of n goroutines to serve as Fs, where the value of n is set at *run-time*, and shares a Go channel with each to retrieve the data. Each F performs its download task (by a Get/Res message exchange) with S concurrently via a separate HTTP channel.

(b) When an F finishes its download, it passes to M the data and a *continuation channel* over the initially shared Go channel (this pattern is as in the implementation of `htcat`[2]).

(c) The passed channel (dotted line) permits M to relay the next message *type* in the protocol after receiving a Data: e.g., to give the F another download task, or to end the goroutine (Done).

Go channels are homogeneously typed: the syntax of channel types is `chan T` for a given type `T`. Channel passing as above (i.e., bundling the continuation channel into the current message) is a way to affect the causality between the communications of *different* message types, as a safer alternative to declaring and allocating all channels upfront: passing the continuation channel as part of using the "current" channel helps prevent using them out of the intended order.

[1] https://golang.org/. Companies using Go: https://github.com/golang/go/wiki/GoUsers. Go success stories: https://github.com/golang/go/wiki/SuccessStories. Survey of 3,595 Go users: https://blog.golang.org/survey2016-results.

[2] Pget is based on `htcat` (https://github.com/htcat/htcat), a tool for parallelising HTTP `GET`s written in Go using channels (and channel passing) and the standard `net` package, with performance gains compared to `curl`.

1.2 Key Programming Challenges

The Pget example demonstrates some of the key challenges faced by distributed programmers in many engineering languages, including recent languages like Go. As a terminology, we shall refer to Go channels as *shared memory channels*, signifying intra-process message passing.

Communication and concurrency errors Go offers convenient primitives for shared memory channels, but does *not* offer any language support against classical errors such as *deadlocks* (goroutines stuck on mutually blocking inputs). In a recent survey,[1] users perceived this to be the main challenge in Go: "*We asked how strongly people agreed [with] various statements about Go. [...] Users* ***least agreed*** *that they are able to* ***effectively debug uses of Go's concurrency features****.*" One factor is that Go's channel *types* are limited. They do not *at heart* constrain the *direction* of communication;[3] nor reflect the *causality* of communications across *separate* channels, which also gives rise to *reception errors* (receiving an incorrect message type). These problems apply similarly to uses of distributed channel libraries, that often are effectively "untyped" in practice.

Disparate communication abstractions Key to understanding an application like Pget *as a whole* is the *choreography* of I/O behaviours by every participant across the multiple channels. At the *specification* level, there is first the question of how to statically specify protocols where the number and kinds of participants are dynamically determined: we refer to such protocols as having *dynamically-instantiated communication structures*. In practice many protocols are only informally specified, itself a cause of errors. This problem is compounded at the *implementation* level, where *disparate* primitives/libraries are used to implement heterogeneous parts of an endpoint (e.g., shared memory and HTTP in *F*)—even with an adequate specification, the programming abstractions do not guide a correct implementation of the *overall* application protocol nor facilitate its verification.

1.3 Multiparty Session Types: Motivations

Towards addressing these challenges, in this paper, we present a new, practical framework for the static specification and safe implementation of distributed Go programs, centred around a pivotal extension of the theory of *multiparty session types* (MPST) [Coppo et al. 2016; Honda et al. 2016]. Our general motivation for using MPST to address the challenges in § 1.2 is as follows.

In common practice, channel-oriented *communications* programming, embodied by standard networking libraries in many languages (including those with static *data* typing), is often effectively "untyped": for example, standard TCP socket APIs simply expose a raw byte stream in each communication direction. Higher-level and more recent facilities, such as service-oriented APIs and frameworks (e.g., SOAP, REST or Apache Thrift) and Go channels, can offer the improvement of *message-type safety*: the messages to be sent and received can be statically checked to be of known types. However, this still falls short of what is ultimately desired for communications-oriented programming in general: *protocol compliance*. The aforementioned facilities mask this limitation to certain extents: service-oriented frameworks essentially hardcode interaction *structures* to call-return patterns, thus reducing protocol compliance (for *individual* invocations) to message-type safety; Go channels are homogeneously typed, and often used with additional restrictions on the communication direction (via ad hoc casting of channel types).

The above limitations of current practices are readily exposed in many applications. For example, non-trivial service-based applications often involve, as a *whole*, the composition of multiple, smaller services: e.g., invoke service A *then* B, which in turn uses *either* C (then the protocol is *repeated* from the start) *or* D, and so on; such scenarios are increasingly promoted by architectures such as microservices that favour fine-grained service decomposition. In the setting of Go channels, such interaction structures require multiple *independent* channels to cater for the range of data types

[3] Go's directed channel types (`<-chan T` or `chan<- T`) are derived by ad hoc casting, and offer no guarantees against deadlock.

and communication directions. In contrast to the safety benefits of data typing enjoyed for “local” computations, programming of such communications suffers from errors arising from *protocol violations* (i.e., *non-protocol-compliant* I/O actions): despite message-type safety, these include the classical *reception errors* (receiving an out-of-order message, e.g., an incorrect invocation of B before A), *deadlocks* (a wait-for cycle of input dependencies) and *orphan messages* (“leftover” messages). The idea of MPST is to detect such errors at compile-time through static typing.

The rest of this paper summarises our contributions (§ 2), demonstrates our work through the running examples (§ 3), and presents our theory (§ 4), implementation (§ 5) and evaluation (§ 6). Our **Supplement**[4] gives additional examples and detailed proofs.

2 OUR CONTRIBUTIONS

2.1 In a Nutshell

(1) We develop the first theory of MPST to support role-parametric protocols in the traditional *distributed* spirit of MPST, including proofs of *decidability* (inferring “role variants”; checking well-formedness) and *correctness* of projection; § 2.2 details this contribution. Our theory is directly motivated by Go applications, but the foundations are *independent* of Go. Our approach thus also applies to other settings where shared-memory and distributed channel-based communication can be mixed (e.g., Rust).

(2) We implement our theory to give the first practical toolchain for MPST-based programming in Go. Our toolchain generates lightweight, *typed APIs* for users to implement the endpoint programs. Our toolchain is also the first to support practical *programming* of *role-parametric* MPST, targeting a language such as Go (cf., dependently typed session π-calculus). It ensures a statically well-typed endpoint program (i.e., by native Go type checking) will *never* perform a non-compliant I/O action w.r.t. to the run-time instantiation of the role-parametric protocol.

(3) Besides safety, we confer programmatic benefits of MPST to Go. Our toolchain enriches channel-over-channel passing in Go to *session delegation* (session-typed channel passing). Session code written using our generated APIs is also transport-*independent*: switching and mixing transports (e.g., Go channels, TCP) is safe and set by a single API argument.

(4) We demonstrate the applicability of our framework and run-time performance of our generated APIs by specifying and implementing a range of use cases from parallel algorithms and Internet applications, including modifying existing Go implementations of real-world applications—e.g., the overheads of our APIs are mostly negligible in programs adapted from [Gouy 2017].

We clarify the conditions for concrete applications of our practical framework:

- We target message passing applications where message delivery is *reliable* and *order-preserving* between each pair of participants in each direction (e.g, TCP, or FIFOs in shared memory). Our core theory is based on the standard *asynchronous* model of MPST, i.e., non-blocking outputs with blocking inputs, but our results also hold for synchronous communications.
- Our framework is top-down from a source protocol specification, which must be well-formed according to our definitions (§ 4). The expressiveness of our framework is attested by practical examples (§ 3), formal examples (§ 4.2), and a range of real-world applications (§ 6.2).

2.2 The Advances of this Paper to MPST

MPST basics. Multiparty session types (MPST) is one of the approaches in the field of behavioural type theory [Ancona et al. 2016; Hüttel et al. 2016] proposed to address the challenges discussed in § 1.2. Fig. 2 (a) depicts the standard top-down methodology of the originating MPST

[4] Technical report 2018/04, Department of Computing, Imperial College London. https://www.doc.ic.ac.uk/research/technicalreports/2018/#4

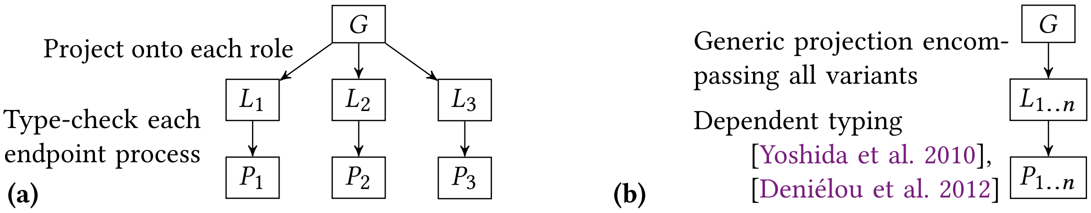

Project onto each role
Type-check each endpoint process
(a)
G
L_1
L_2
L_3
P_1
P_2
P_3
Generic projection encompassing all variants
Dependent typing [Yoshida et al. 2010], [Deniélou et al. 2012]
(b)
G
$L_{1..n}$
$P_{1..n}$

Fig. 2. Contrasting **(a)** the traditional top-down, distributed view of MPST [Coppo et al. 2016; Honda et al. 2016]; and **(b)** the "centralised" view of existing role-parametric MPST systems.

systems in the π-calculus [Coppo et al. 2016; Honda et al. 2016], which we illustrate by a small example: a ring communication structure between three Workers, W_1, W_2, and W_3.

$$G = \mathtt{W}_1 \longrightarrow \mathtt{W}_2 : \mathtt{T} \,.\, \mathtt{W}_2 \longrightarrow \mathtt{W}_3 : \mathtt{T} \,.\, \mathtt{W}_3 \longrightarrow \mathtt{W}_1 : \mathtt{T} \,.\, \mathtt{end}$$

G is a *global type*: a specification of the communication structure (i.e., *protocol*) between the participants (abstracted as *roles*) from a global perspective. G says W_1 first sends a $\mathtt{T}$ message to W_2, who then sends a message to W_3, who finally sends a message to W_1. For each role r, the global type is then *projected* to a *local type*, that describes the localised I/O actions from r's perspective:

$$L_1 = \mathtt{W}_2 \,!\, \mathtt{T} \,.\, \mathtt{W}_3 \,?\, \mathtt{T} \,.\, \mathtt{end} \qquad L_2 = \mathtt{W}_1 \,?\, \mathtt{T} \,.\, \mathtt{W}_3 \,!\, \mathtt{T} \,.\, \mathtt{end} \qquad L_3 = \mathtt{W}_2 \,?\, \mathtt{T} \,.\, \mathtt{W}_1 \,!\, \mathtt{T} \,.\, \mathtt{end}$$

L_1 says W_1 should first send ($\mathtt{!}$) a $\mathtt{T}$ message to W_2, *followed by* receiving ($\mathtt{?}$) a $\mathtt{T}$ message from W_3; the $\mathtt{W}_2 \longrightarrow \mathtt{W}_3$ interaction is transparent to W_1. Local types are used to statically *type check* endpoint programs (formally, session π-calculus processes) implementing these roles: intuitively, the typing checks protocol compliance by matching the structure of the I/O actions in the local type to a correspondingly structured usage of I/O primitives in the program. A well-typed system of processes, one for each role, is guaranteed free from reception errors and deadlocks.

A crucial design point of MPST is that projection promotes *modularity*: it decouples the programming (and verification) of each endpoint. This is especially important for distributed programming, which in addition to inter-process communications, may also be characterised by endpoints being *separately* implemented by different programmers, using different techniques (e.g., multithreaded, event-driven, etc.), technologies (e.g., client vs. server), and languages.

Addressing an open problem. One of the biggest challenges in MPST is *expressiveness*: essentially, to attain the strong static guarantees that MPST aims to provide, global types are syntactically limited and subject to conservative *well-formedness* and *projectibility* constraints (i.e., projection is a partial operator).

A crucial practical limitation of MPST concerns the lack of support for *role-parameterisation*, i.e., global and local types where roles are parameterised by indices. For instance, it should be possible to write a single global type for a ring communication structure of *any* size, instantiated dynamically; other applications include those involving parameterised worker/service instantiations (e.g., Pget), and many parallel algorithms. The original theory of MPST does not support such role-parameterisation, and while attempts have been made to extend the theory, these extensions ultimately had to sacrifice (1) general decidability of type checking and (2) modularity of projection.

This paper presents a new theory that is the first to support role-parametricity in MPST without the previous compromises, maintaining both decidability and modularity. Due to our new theory, we are able to contribute the first practical toolchain for role-parametric, distributed, MPST-based programming in an engineering language such as Go *without* relying on dependent types at the implementation level. Our framework guarantees only I/O actions that are compliant with the run-time instantiation of the role-parametric protocol are performed.

Comparison. To further clarify our contributions, we illustrate the approach of Deniélou et al. [2012]; Yoshida et al. [2010], the initial theoretical works that formulate a dependently typed MPST for protocols with indexed roles by adding a primitive recursion operator **R** to types and processes. The generalisation of the above example to a ring between $k \geq 2$ participants can be written as:

$$G = \Pi\mathtt{k}{:}I.(\mathbf{R}\,G'\,\lambda\mathtt{i}.\lambda\mathbf{x}.G'') \qquad G' = \mathtt{W[k]} \longrightarrow \mathtt{W[0]} : \mathtt{T}\ .\ \mathtt{end} \qquad G'' = \mathtt{W[k\text{-}i\text{-}1]} \longrightarrow \mathtt{W[k\text{-}i]} : \mathtt{T}\ .\ \mathbf{x}$$

where I is the parameter domain ($\geq$2), i is an index variable, and **x** is a recursion variable. The use of **R** in G can essentially be read as: repeat G'' for i from k-1 to 0, then finish by doing G'.

In contrast to standard MPST, however, Fig. 2 (b) shows a corresponding top-down view of the methodology promoted by these works. G is projected to a *single* local type (called the *generic projection*) that encompasses the entire range of different index-value dependent behaviours *as one*.

$$\begin{aligned} L_{1..n} = \mathbf{R}\,&(\mathtt{if}\ p = \mathtt{W[k]}\ (\mathtt{W[0]}\ !\ \mathtt{T}\ .\ \mathtt{end})\ \mathtt{else\ if}\ p = \mathtt{W[0]}\ (\mathtt{W[k]}\ ?\ \mathtt{T}\ .\ \mathtt{end})\ \mathtt{else\ end}) \\ &(\lambda\mathtt{i}.\lambda\mathbf{x}.\mathtt{if}\ p = \mathtt{W[k\text{-}i\text{-}1]}\ (\mathtt{W[k\text{-}i]}\ !\ \mathtt{T}\ .\ \mathbf{x})\ \mathtt{else\ if}\ p = \mathtt{W[k\text{-}i]}\ (\mathtt{W[k\text{-}i\text{-}1]}\ ?\ \mathtt{T}\ .\ \mathbf{x})\ \mathtt{else}\ \mathbf{x}) \end{aligned}$$

As the **R** operator iterates through the index range k..0 for each participant p, the embedded index expression cases will spell out the three *distinct* behaviours present in the ring: those of W[0], W[1..k-1], and W[k]. We note that supplying the (valid) index domain, i.e., k ≥ 2, in their system *fixes* the type family—the intuitive case of a *two*-party ring requires declaring a separate type family (cf., k = 1 is invalid in the above). Fixing the (finite) domain is required for decidability of type checking.

We now give the same example in our framework. The global type is:

$$G_{\text{Ring}} = \mathtt{W}\overset{1}{\Longrightarrow}[\mathtt{1..k}] : \mathtt{T}\ .\ \mathtt{W[k]} \longrightarrow \mathtt{W[1]} : \mathtt{T}\ .\ \mathtt{end}$$

where $\overset{1}{\Longrightarrow}$ denotes a parameterised pipeline structure along the specified interval, i.e., W[1] ⟶ W[2]... W[k-1] ⟶ W[k]; it is syntactic sugar (§ 4.2) for an instance of our *MPST-oriented* foreach construct: $\mathtt{foreach}\ \mathtt{W\{i_1{:}1..k\text{-}1,\ i_2{:}2..k\}}\ \mathtt{do}\ \mathtt{W[i_1]} \longrightarrow \mathtt{W[i_2]} : \mathtt{T}\ .\ \mathtt{cont}$ (cf. the generic **R**). Our toolchain statically determines there are three *variants* of W, with *decoupled* projections:

$$L_{\text{Ring}}^{\mathtt{W[1]}} = \mathtt{W[2]}\ !\ .\ \mathtt{W[k]}\ ? \qquad L_{\text{Ring}}^{\mathtt{W[2..k\text{-}1]}} = \mathtt{W[self\text{-}1]}\ ?\ .\ \mathtt{W[self\text{+}1]}\ ! \qquad L_{\text{Ring}}^{\mathtt{W[k]}} = \mathtt{W[k\text{-}1]}\ ?\ .\ \mathtt{W[1]}\ !$$

(We omit the T *message labels* and end.) self denotes the run-time value of the local process identifier. From this single specification, the toolchain also determines the two valid endpoint *families*: that comprising variants $L_{\text{Ring}}^{\mathtt{W[1]}}$ and $L_{\text{Ring}}^{\mathtt{W[k]}}$ (when k = 2), and when all three are involved (k > 2).

3 METHODOLOGY OVERVIEW

3.1 Go Basics

We first summarise some basic Go features needed to understand our approach and code examples.

Types and variables. The following is a *type declaration* for a *defined type* (left), a *variable declaration* (centre), and a *shortened* declaration (right):

```
type Init struct { Err error; id uint64; Ept *S_1to1 }        var data Data        proto := Pget.New()
```

The left side defines a *struct type* named Init, that is a typed record with fields Err of type error, id of uint64 and Ept of type *S_1to1 (i.e., a *pointer type* with *base type* S_1to1). The declaration in the centre creates a variable data of type Data, automatically initialised to the *zero value* of that type (e.g., nil for interfaces and pointers). The right side is a shortened declaration for variable proto whose type and initial value is given by the expression Pget.New().

Methods and interfaces. A method is a function with a *receiver*, i.e., a value upon which the method is invoked. The following is a method declaration (left) and a method call (right):

```
func (c *Foo) Job(a []Job) *M_3 { /* Method body omitted */ }                   y := x.Job(myJobs)
```

The left side declares a method Job, with *receiver type* *Foo, a parameter a of type []Job (method/type names are unrelated), and result type *M_3. Arguments are always passed by value. An *interface* specifies a set of methods; a type with a superset of methods *implements* the interface *implicitly*.

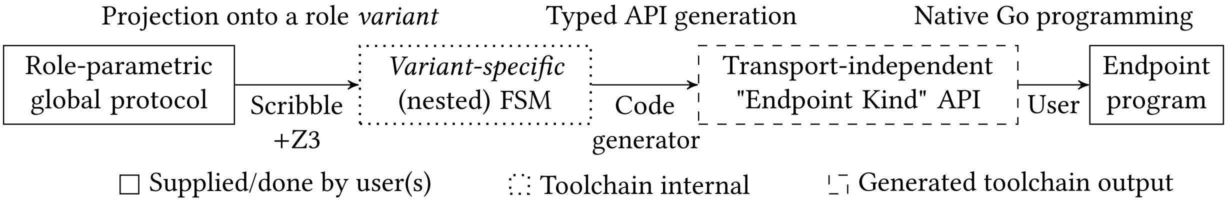

Projection onto a role *variant*
Typed API generation
Native Go programming
Role-parametric global protocol
Scribble +Z3
Variant-specific (nested) FSM
Code generator
Transport-independent "Endpoint Kind" API
User
Endpoint program
□ Supplied/done by user(s)
Toolchain internal
Generated toolchain output

Fig. 3. Main toolchain stages: role-parametric global protocol specification, projection onto a role variant, and distributed Endpoint API generation.

```
type Bar interface { m1(); m2() }                func (b *Baz) m1() { }     func (b *Baz) m2() { }
```

The left side defines an *interface type* `Bar`; the right side implements it for the base type `Baz`.

Package aliases. It is useful to note that Go allows packages (e.g., our generated APIs) to be imported under an alias. This feature allows users of our APIs to locally alias the default generation names, e.g., `import S "github.com/.../pget/Proto1/S_1to1"` aliases `S_1to1` as `S`.

3.2 Distributed, Role-Parametric MPST for Go: Overall Methodology – Pget

We demonstrate our framework by using our toolchain, depicted in Fig. 3, to work through Pget (§ 1.1). For practical protocol specifications, we implement our new theory of role-parametric MPST as an extension to Scribble (http://www.scribble.org/), an existing protocol language based on standard MPST [Coppo et al. 2016]. From the spec, our toolchain generates lightweight APIs that safely prescribe the I/O behaviour of each *role variant* (endpoint *kind*) as a *whole*, i.e., by capturing the causality between I/O actions conducted over otherwise separate underlying channels.

Global protocol. The basic scenario comprises a Master (`M`) coordinating `K` Fetchers (`F`) to download a file from an HTTP Server (`S`). The original project[2] upon which Pget is based implements the former two, to interoperate with standard third party Web servers (e.g., Apache). A *global* protocol, however, specifies the overall application from a neutral perspective: provided the interaction structure can be expressed in terms of (MPST-based) message passing, the details of how any individual endpoint may be implemented remain abstract at this level. This allows for the specification of multiparty applications formed (or partly formed) by a composition of smaller services (e.g., traditional RPCs), similarly to the role of the HTTP server here.

Fig. 4 (top) lists a global protocol `Pget` written in our extended Scribble. We flesh out the description from § 1.1 but keep certain aspects simple for conciseness; subsequent examples will demonstrate further features. We capture the channel mobility in `Pget` using *session-typed* channel passing, called session *delegation* in the literature. The parameterised communication structure in this example is also representative of protocols in other applications (e.g., § 6.2).

The protocol declares the three base *role names* `M`, `F` and `S`. An asynchronous *interaction* is written, e.g., `Job from M to F[1,K];`, where `M` is the *sender*-side, and `F[1,K]` the *receiver*-side; `F[1,K]` stands for the set of `F` in the inclusive, non-empty interval $[1, \mathtt{K}]$, where the value of `K` is to be supplied when the session is initiated at *run-time*. By default, `K` is taken to be in $\mathbb{N}_{\geq 1}$: our well-formedness conditions (§ 4.5) determine that the only *valid* instantiations of `K` are values ≥1 (specifically, well-formedness dictates that every interval must be non-empty); the validity of concrete parameter values is checked at run-time. `Job` is the *message signature*, declared in the Scribble module by, e.g.,

```
sig <go> "messages.Job" from "github.com/.../pget/messages" as Job;
```

where `messages.Job` is a Go data type that implements the Scribble API for data serialization. We omit the similar declarations for the other messages. All together, this interaction specifies a

```
global protocol Pget(role M, role F, role S) {
  Head from F[1]   to S;  Res    from S      to F[1];   // (1) Obtain metadata from Server
  Meta from F[1]   to M;  Job    from M      to F[1,K]; // (2) Allocate Fetcher download tasks
  Get  from F[1,K] to S;  Res    from S      to F[1,K]; // (3) Perform downloads
  Data from F[1,K] to M;  Sync@A from F[1,K] to M;      // (4) Gather data and control channels
} // Sync@A is the local type projection of Sync onto A, i.e., a delegation
global protocol Sync(role A, role B) { choice at A { Done from A to B; } // Choice: terminate B (i.e., F_i) or ...
                                               or { ... } }
```

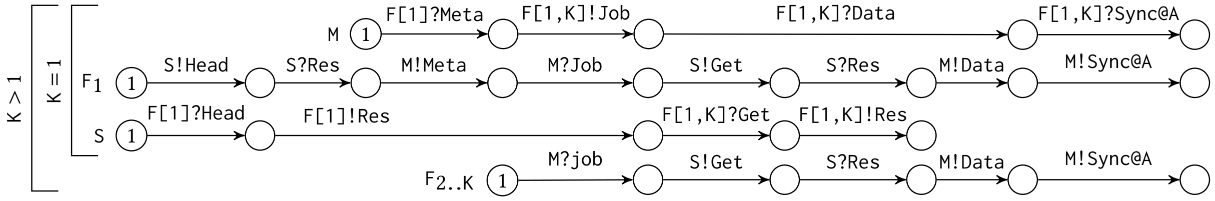


Fig. 4. Pget example from § 1.1 in our extended Scribble: (top) role-parametric global protocol; (bottom) the projections onto each role variant, M, F_1 and $F_{2..k}$, represented as communicating FSMs.

scatter of Job messages (possibly with different values) from the single sender to the K receivers. Similarly, Get from F[1,K] to S; specifies a *gather* of K Get messages from the Fs by the single S. Singleton-indexed scatters/gathers coincide as a basic point-to-point interaction.

The message signature of the *delegation* action is Sync@A (adopting the syntax of Scalas et al. [2017]), which denotes passing a *channel* for the A endpoint in the Sync protocol (obtained through projection; see below). For clarity, we name M as A and F as B in Sync (M and F could be reused); and give only the case for terminating the B/F goroutine by sending a Done on the delegated channel.

Projection. The distinct behaviours associated with each role name, i.e., the *role variants*, are inferred from how the role names are *indexed* and used in the protocol body. A role name that is never indexed is implicitly indexed over a singleton constant interval (whose value is irrelevant), as is the case for M and S. Our toolchain infers from the indices that the definition of Pget induces *four* role variants, i.e., four kinds of endpoints: M, F_1, $F_{2..K}$ and S. Fig. 4 (bottom) depicts the projection of Pget onto each: our implementation uses a representation of our index-parameterised local types (§ 4.2) based on *communicating finite state machines* [Brand and Zafiropulo 1983; Deniélou and Yoshida 2012] that correspond straightforwardly to the syntactic types. In our setting, the FSMs communicate via *scatter/gather* I/O (subsuming basic point-to-point messaging), and may feature *nesting* of FSMs inside states (demonstrated in § 3.3). The toolchain also determines these variants form two valid *families*: one has M, F_1 and S ($K = 1$), and the other has all ($K > 1$).

The initial states are marked 1. For instance, in the FSM for M, the first action F[1]?Meta receives the Meta message from F[1], followed by F[1,K]!Job that scatters Jobs to the K Fs. Then M waits until it has gathered a Data from each F, and likewise the delegated control channel of type Sync@A.

API types generation. The purpose of the API generation is to capture a projection as Go type definitions to guide programming of the target variant, and impart safety assurances through a combination of type checking and the functionality of the underlying generated code. It is possible to generate various kinds of API, suited to different programming styles—a benefit of our distributed framework (cf. previous “monolithic” approaches Ng et al. [2015]; Yoshida et al. [2010]) is that different endpoints could be separately implemented using different APIs: we present the most direct API generation from a projection, that is close to channel-based programming in common practices (e.g., TCP sockets, Go channels) and to the session π-calculi in MPST formalisms.

State type (with nested peer/action types)			**Method name and signature** (parameters, result type)	
State	Peer(s)	I/O action	Message label/values, aux. functions	Successor
`M_1`	`F_1`	`Receive`	`Meta(a *Meta)`	`*M_2`
`M_2`	`F_1toK`	`Scatter`	`Job(a []Job)`	`*M_3`
`M_3`	`F_1toK`	`Gather`	`Data(a []Data)`	`*M_4`
`M_4`	`F_1toK`	`GatherAndSpawn`	`Sync_A(run func(*A_1) End_A)`	`End_M`

```
func mainM(req HttpReq, K int) {
  proto := Pget.New()
  M := proto.M.Kgt1.New(K) // API for K>1
  ss1 := shm.Listen(8888+1); defer ss1.close()
  go mainF1(req, 8888+1)
  M.F_1.Accept(ss1)
  for i := 2; i <= K; i++ {
    ssi := shm.Listen(8888+i); defer ssi.close()
    go mainF_2toK(req, 8888+i)
    M.F_2toK.Accept(i, ssi) // Supported by K>1 API
  M.run(runM) // runM: func(*M_1) End_M
} }
```

```
func runM(m *M_1) End_M {
  var meta Meta; var data Data
  // F[1]?Meta. F[1,K]!Job. F[1,K]?Data. F[1,K]?Sync@A
  return m.F_1   .Receive       .Meta(&meta).
           F_1toK.Scatter       .Job(split(&meta)).
           F_1toK.Reduce        .Data(&data, agg).
           F_1toK.GatherAndSpawn.Sync_A(runA)
}

func runA(a *A_1) End_A {
  return a.B.Send.Done() // Just do Done, for brevity
}
```

Fig. 5. (top) Go API types and I/O method signatures generated for `M` in Pget; (bottom) an `M` endpoint implementation using the generated API.

In short, the API generation takes the FSM for a target role *variant* and (i) reifies each state as a *state-specific* Go type, that (ii) offers a generated I/O method for each of the *transitions* from that state; the result type of each I/O method is set to the *successor* state of that transition. We refer to instances of the state-specific types as *state channels*, and they are created only by the API itself. A state channel API is basically an interlinked set of lightweight, variant- and state-specific type wrappers that abstract from the concrete I/O actions on the underlying channels (Go channels, TCP, etc.) to the various participants of a multiparty communication session.

Fig. 5 (top) summarises the state channel API generated for `M`. On the left, 'State' is the "top-level" type for each protocol (FSM) state. 'Peer' is a type that denotes the valid interaction peers at each state, accessed as a field of State; similarly the valid 'I/O action's are also denoted by types accessed as fields of Peer. On the right, the valid message types for each action are offered as methods on the action types, taking the message values as parameters, and resulting in the successor state type. The various actions (e.g., `Receive`, `Scatter`) and parameters are generated based on the FSM state.

As an example, assuming variables `m` and `meta` of the initial state type `M_1` and message type `meta`, respectively, the first I/O action in an `M` program may be guided by the API as:

`m.F_1.Receive.Meta(&meta)` which can be read as: on channel `m`, do $\mathtt{F}_1$`?Meta`.

Since the result type of I/O methods is used for successor states, input methods like `Receive`/`Gather` are generated to store the deserialized message values into the pointer arguments (e.g., `meta`), following idiomatic usage of standard Go APIs (e.g., `encoding/gob`). The alternative of returning a pair of the successor state and the deserialized values hinders fluent call-chaining. Variable declarations in Go allocate memory initialised to zero values (and are thus safe to read).

We highlight that the I/O method parameters relate only to messages: all index computations and mappings to underlying channels are internalised within the API from the source specification. For simplicity, we use the default type/method naming as illustrated; users may instead use Go package/type aliases (each state has a separate subpackage; cf. § 3.1) in the local program, or supply name annotations in the protocol—i.e., specific naming schemes are not a crucial detail.

Endpoint programming. Fig. 5 gives an example Go implementation of `M` using the API generated as above. We assume Go type definitions (e.g., `Get`, `Res`) for each message signature as described earlier, and a `HttpReq` helper type that holds the various field values of a HTTP request.

Endpoint initiation An endpoint implementation typically starts by establishing a new session for the target protocol, signified by instantiating the generated API frontend type: here, proto of type Pget. This is used to create a new *Endpoint* by using the appropriate constructor from a generated "menu" of nested type functions: e.g., line 3 in Fig. 5 uses the constructor for M under the K_gt1 (K > 1) family. An incompatible K argument for this family is a run-time error: a check on the implicit constraint (derived from the protocol) is built into the generated method (§ 5.3).

An Endpoint is first used to establish communication links to its peers by the generated connection methods Accept (lines 6 and 10) and Dial (illustrated below), similarly to standard Socket APIs (e.g., tcp or unix via the net package), with the additional option to use shared memory Go channels (shm package) as a transport; in Pget, for instance, the Master and the Fetchers communicate via shared memory, as indicated by the usage of the shm package on Lines 4 and 8. The K > 1 API selected for M in this code supports (i.e., allows by static typing) the Accept (and Dial) method for $F_{2..K}$ (line 10); whereas the K = 1 API has connection methods only for F_1.

After initiating the session, we use a generated run method on the Endpoint to conduct the protocol by supplying a func(*M_1) End_M, where M_1 is the *initial* state channel type of this endpoint, and End_M is the *terminal* type. We note the result is set to the End type even for non-terminating endpoints (i.e., persistent *sessions*)—since no generated I/O method will actually return a state channel of this type, this signifies the function should be non-terminating.

Protocol implementation Intuitively from an FSM view, an implementation of the run argument function using the state channel API must observe one simple usage condition: *on the current state channel, call* exactly one *I/O method to obtain the next, up to the terminal state* (if any). Following this, the implementation, e.g., runM (line 14), is thus guided by the static type of each state channel as the programmer works through the protocol. For a given session instance, the only way to obtain a value from the API that statically satisfies the End result type of a (terminating) endpoint is to reach and perform a generated I/O method that corresponds to a terminal transition.

We have used the API in a concise call-chaining style; the user may also use the generated types in more explicitly imperative (e.g., protocol steps as sequenced statements) or "functional" (e.g., via functions with state type parameters and result) styles, interleaved with other application operations as needed. The Reduce method on line 19 is an additionally generated convenience variant of the basic Gather (Fig. 5, top). We omit the simple definitions of functions split and agg.

Transport abstraction and delegation Endpoint programs for each variant are implemented in a similar fashion. Assuming an F1 Endpoint object created using the generated API, we may find in a preamble for F_1:

```
F1.M.Dial(shm.Client, "localhost", portM); F1.S.Dial(tcp.Client, req.Host, req.Port)
```

F1 is used to connect (Dial) to M and S on shared memory and TCP transports, respectively.

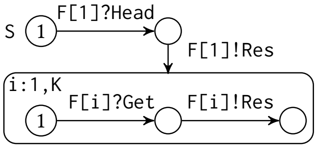
Starting from the initial state channel (below, f), the programmer can rely on the API to guide the way through the multiparty protocol for F_1 (cf. its FSM, Fig. 4) as a whole, correctly dispatching the interleaved I/O operations with M and S on the underlying shm and tcp channels:

```
// Assuming vars req:HttpReq, res:Res, job:Job, etc., F₁ does: S!Head. S?Res. M!Meta. M?Job. ...
f. S.Send.Head(req.Head()). S.Receive.Res(&res). M.Send.Meta(res.Meta()). M.Receive.Job(&job). ...
```

Our API generation takes advantage of cheap goroutine spawning to offer various convenience methods for delegations. In the run method of the delegation sender, i.e., F_1:

```
   // New Sync session   // Spawns B goroutine       // M!Sync@A.end -- i.e., delegate 'a' to M
... proto := Sync.New(); a := proto.Shm.A.New(runB);   return f8.M.Send.Sync_A(a)
```

The second step is a Scribble-Go API facility for establishing shared memory sessions: the New constructs an A endpoint of a new session for the Sync protocol (Fig. 4), while spawning a goroutine



```
1 func runS(s *S_1) End {
2   var head *Head
3   return s.F_1.Receive.Head(head).
4            F_1.Send.Res(Res.New(head)).
5            Foreach(nested) }

7 func nested(i int, s *S3_1) S3_End {
8   var get *Get
9   return s.F_i.Receive.Get(get).
10           F_i.Send.Res(Res.New(get))
11 }
```

Fig. 6. Projection and example user code for S in the revision of Pget using foreach.

for the implementation function supplied for each of the other endpoints (i.e., runB for B); shm channels are implicitly created between each endpoint. Assuming f8 is of the penultimate state type for F$_1$, the Send then *delegates* the state channel a to M, satisfying the local type M!Sync@A. The GatherAndSpawn in M (Fig. 5, line 20) is generated for receiving *channels*: it implicitly spawns the supplied function, typed from the received state to End, as a goroutine for each received channel.

State channel linearity and safety guarantees The use-exactly-once (i.e., *linear* use) condition of state channel APIs means a program should never *re*use a state channel instance: as a default, the API generation inlines minimal run-time checks against repeat channel use into the API, though our examples illustrate how call-chaining may help avoid linearity errors by keeping intermediate channel values implicit. But *regardless* of channel linearity, a generated API guarantees that an endpoint implementation *never* performs a non-compliant I/O action w.r.t. to the run-time instantiation of the parameterised protocol, up to premature termination (e.g., failures). We discuss linearity, options for *static* linearity, and our safety guarantees in § 5.4.

3.3 Pget – Revised using foreach (Role-Parametric Subprotocols as Nested FSMs)

Like the original program, an MPST-based (re-)implementation of the client side of Pget (M, F$_1$ and F$_{2..K}$) is interoperable with a third-party S such as Apache. However, our framework equally allows to implement an S that would be interoperable with the original client (and our Scribble client).

The specification in Fig. 4 has: Get from F[1,K] to S; Res from S to F[1,K];. As depicted there, the projection onto S results in a gather from all Fs (F[1,K]?Get) and a scatter to all Fs (F[1,K]!Res). In practice, the more desirable behaviour is for S to serve the Get-Res exchange with each F *concurrently*. This may be specified via our foreach extension to Scribble, that allows to express a form of *role-parametric subprotocols*: we can replace line 4 in Fig. 4 by

```
foreach F[i:1,K] { Get from F[i] to S; Res from S to F[i]; }
```

Fig. 6 depicts the projection by our toolchain onto S: the *default* behaviour is to repeat the nested FSM for i:1..K in sequence. The same FSMs and APIs are generated for F$_1$ and F$_{2..K}$ as in Fig. 4.

Fig. 6 (right) gives an implementation of S using the default foreach API generation. The basic API generation for a state s with a nested FSM is to generate a Foreach method, that on entering s first executes the subprotocols to completion: it takes the nested behaviour as a first-class function, and performs it sequentially over the parameter range [1,K] (implicit within the generated API). In general, Foreach then returns an intermediary value for performing the transition out of s; in this example, it directly returns End. When parameterised variants within a foreach do *not* interact with each other, however, an additional method is generated that alternatively performs the subprotocols in *parallel*. As desired of S above, this allows by replacing lines 3–5 in Fig. 6:

```
return s. F_1.Receive.Head(head). F_1.Send.Res(Res.New(head)). Parallel(nested)
```

The Parallel method spawns a separate nested goroutine for each parameter value.

Further examples. We demonstrate protocol *branching* and *recursion* in a range of later examples, in formal notation (e.g., Ex. 4.4, Ex. 4.8 in § 4.2) and our Go APIs (e.g., Fig. 13 in § 5.3). An implementation of F$_1$ and other larger examples are in the Supplement[4] (e.g., § I.1.3, § I.2, § IV.1.2).

$$\begin{array}{l}
E \in \mathbb{E} ::= E_1{+}E_2 \mid E_1{-}E_2 \mid a \mid k \qquad D \in \mathbb{D} ::= E_1 \mathinner{..} E_2 \qquad a \in \mathbb{A} \qquad k \in \mathbb{K} \qquad i \in \mathbb{I} \qquad x \in \mathbb{E} \cup \mathbb{I} \\
G \in \mathbb{G} ::= r_1[x_1] \rightarrow r_2[x_2] : \{\ell_j \,.\, G_j\}_{j \in J} \mid \texttt{foreach}\, R\{i_j : D_j\}_{j \in J}\ \texttt{do}\ G_1 \,;\, G_2 \mid \texttt{cont} \mid \texttt{rec}\, X\, G \mid X \mid \texttt{end} \\
L \in \mathbb{L} ::= r[x]\,!\,\{\ell_j \,.\, L_j\}_{j \in J} \mid r[x]\,?\{\ell_j \,.\, L_j\}_{j \in J} \mid \texttt{foreach}\, R\{i_j : D_j\}_{j \in J}\ \texttt{do}\ L_1 \,;\, L_2 \mid \texttt{cont} \mid \texttt{rec}\, X\, L \mid X \mid \texttt{end}
\end{array}$$

Fig. 7. Syntax of rank expressions ($E \in \mathbb{E}$), intervals ($D \in \mathbb{D}$), global types ($G \in \mathbb{G}$), and local types ($L \in \mathbb{L}$)

4 THEORY

Our new theory generalises the original MPST [Coppo et al. 2015; Honda et al. 2016]. It consists of the following contributions: § 4.1 – an abstract algebra of *ranks* to index role names, which subsumes index domains in existing parameterised MPST approaches; § 4.2 – languages of parameterised global types and local types, to specify communication patterns among indexed roles from a global perspective and a local perspective, using a new `foreach` construct; § 4.3 – the first static *inference procedure* for role variants; § 4.4 – a new projection operator that produces local types for role variants, based on a global type; and § 4.5 – theorems that certify role variant inference is decidable, checking well-formedness is decidable, and projection is correct (i.e., the set of local types projected from a well-formed global type is equivalent to the global type; this implies safety).

4.1 Roles and Ranks

Roles. Let $\mathbb{R}$ denote the set of all *role names*, ranged over by r (and R over sets of role names). Every role name identifies a *role* that *individuals* (i.e., endpoint programs, e.g., goroutines) enact in a protocol. For instance, the role names in the Pget protocol are `M` for Master, `F` for Fetchers, and `S` for Server. Our theory allows every *single role* to be enacted by *multiple individuals*.

Ranks. Let $\mathbb{A}$ denote the set of all *ranks*, ranged over by a. Every rank identifies an individual among the possibly many that enact the same role (cf. ranks in MPI; principals in Wysteria [Rastogi et al. 2014]), through *indexed role names*. For instance, `F`[3] identifies the third Fetcher.

Our theory is parametric in $\mathbb{A}$, meaning we do not fix a specific set of ranks. Instead, more abstractly, the only structure we assume of $\mathbb{A}$ is the existence of an operator $+$, a constant 0, and relations $\preceq$ and $<$, such that: $\langle \mathbb{A}, +, 0 \rangle$ is a torsion-free abelian group; $\langle \mathbb{A}, \preceq \rangle$ is a partially ordered set; $\langle \mathbb{A}, < \rangle$ is a strictly totally ordered set; $+$ preserves $\preceq$ and $<$; first-order formulas over $\langle \mathbb{A}, +, 0, \preceq \rangle$ are decidable; and the set of ranks between any ranks a_1 and a_2 under $\preceq$ (i.e., $\{a \mid a_1 \preceq a \preceq a_2\}$) is finite and enumerable. If these conditions are satisfied, we call $\langle \mathbb{A}, +, 0, \preceq, < \rangle$ a *rank structure*. The Supplement,[4] § II.1 motivates the need for these conditions.

Example 4.1 (1d). The set of all integers $\mathbb{Z}$, with the standard integer addition for $+$, and with the standard non-strict and strict integer orders for $\preceq$ and $<$, is a rank structure; $\langle \mathbb{A}, +, 0, \preceq \rangle$ yields linear integer arithmetic, which is decidable.

Example 4.2 (2d). The set of all pairs of integers $\mathbb{Z} \times \mathbb{Z}$, with *coordinate-wise addition* for $+$, with the non-strict *product order* for $\preceq$, and with the strict *lexicographic order* for $<$, is a rank structure; $\langle \mathbb{A}, +, 0, \preceq \rangle$ can be encoded in linear integer arithmetic, which is decidable. $\mathbb{A} = \mathbb{Z} \times \mathbb{Z}$ enables indexing role names with *2d coordinates*, for matrix and mesh protocols; see Ex. 4.6, 4.7.

4.2 Global Types and Local Types

Preliminaries. Global types specify communication patterns among a possibly unknown number of individuals from a global perspective. We start with some preliminaries.

- We assume a set $\mathbb{K} = \{\mathsf{k}_1, \mathsf{k}_2, \ldots\}$ of all *parameters*, ranged over by k.
- We define the set $\mathbb{E}$ of all *rank expressions*, ranged over by E (Fig. 7, first line). If a rank expression contains parameters, it is *open*; otherwise, it is *closed*.

- We define the set $\mathbb{D}$ of all *intervals*, ranged over by D (Fig. 7, first line).
- We assume a set $\mathbb{I} = \{\mathtt{i}_1, \mathtt{i}_2, \ldots\}$ of all *index variables*, ranged over by i. We use index variables to iterate over intervals, denoted as $i{:}D$. Let $\mathbb{E} \cup \mathbb{I}$ denote the set of all *indices*, ranged over by x.

Global types. Fig. 7, second line, shows the syntax of global types. $r_1[x_1] \rightarrow r_2[x_2] : \{\ell_j \,.\, G_j\}_{j \in J}$ denotes an asynchronous *communication* of a message labelled as ℓ_j from *sender* $r_1[x_1]$ to *receiver* $r_2[x_2]$, for $j \in J$ (chosen by the sender), followed by G_j; as the syntax of message labels is irrelevant in our theory, we leave it unspecified. We omit curly brackets if J is a singleton; also, if a role is enacted by only one individual, we omit its index (e.g., we write $\mathtt{M}$ instead of $\mathtt{M[0]}$ for Master). $\mathtt{rec}\ X\ G$ denotes *recursion*; $\mathtt{end}$ denotes termination.

iter.	$\mathtt{i}_1$	$\mathtt{i}_2$	body after substitution
1	1	2	$\mathtt{W[1]} \rightarrow \mathtt{W[2]} : \mathtt{Val}\ .\ \mathtt{cont}$
2	2	3	$\mathtt{W[2]} \rightarrow \mathtt{W[3]} : \mathtt{Val}\ .\ \mathtt{cont}$
…	…	…	…
7	8-1	8	$\mathtt{W[8\text{-}1]} \rightarrow \mathtt{W[8]} : \mathtt{Val}\ .\ \mathtt{cont}$

$$G_{\text{Pipe}} = \mathtt{foreach}\ \mathtt{W}\{\mathtt{i}_1{:}\mathtt{1..k\text{-}1},\ \mathtt{i}_2{:}\mathtt{2..k}\}\ \mathtt{do}\ (\mathtt{W[i_1]} \rightarrow \mathtt{W[i_2]} : \mathtt{Val}\ .\ \mathtt{cont})\ ;\ \mathtt{end}$$

Fig. 8. Table ($\mathtt{k} = 8$) for the iteration domain in the Pipeline global type

$\mathtt{foreach}\ R\{i_i : D_j\}_{j \in J}\ \mathtt{do}\ G_1\ ;\ G_2$, the key novelty of our language, denotes a *loop* of the communications specified in *body* G_1, followed by *continuation* G_2; $\mathtt{cont}$ indicates the loop should continue with the next iteration. The *iteration domain* of $\mathtt{foreach}$ is specified by $R\{i_j{:}D_j\}_{j \in J}$, where R denotes a non-empty set of role names, and where every D_j has the same length; it essentially constitutes a "table", where "columns" correspond to index variables, "rows" to iterations, and the "cell" in column i_j, row u, contains the u-th rank in D_j (sorted by $<$). The intervals are iterated over in lock-step: the idea is that in the u-th iteration of the loop, at run-time, individuals communicate with each other as specified in G_1 after substituting $r[a]$ for $r[i_j]$, for every $r \in R$, and where a is the corresponding rank in the table. For instance, Fig. 8 shows the table for the iteration domain in the Pipeline global type. By definition (i.e., the conditions on rank structures, plus every interval has a lower and upper bound), every interval is finitely enumerable.

The bounded "counting" aspect of our $\mathtt{foreach}$ is inspired by dependent type theories and the primitive recursion operator used in previous work (§ 2.2). However, a unique feature of our *MPST-oriented* $\mathtt{foreach}$ is that it essentially iterates over indexed role names ($\mathtt{W[1]}, \mathtt{W[2]}, \ldots$) instead of over "naked" indices ($\mathtt{1}, \mathtt{2}, \ldots$; cf. primitive recursion). Leveraging this role-based information is key to facilitating the static, decidable inference of role variants (§ 4.3), projection (§ 4.4), and checking condition 3 of well-formedness (§ 4.5).

Remark 1. An iteration domain $\{r_1, \ldots, r_n\}\{i_1{:}D_1, \ldots, i_m{:}D_m\}$ can equivalently, and closer to our extended Scribble notation, be represented as a sequence $r_1[i_1{:}D_1], r_1[i_2{:}D_2], \ldots, r_n[i_m{:}D_m]$, where n and m are unrelated. Our present notation is more convenient to deal with in proofs.

Example 4.3 (Pget). Let $\mathtt{k}$ represent the number of Fetchers in the Pget protocol (§ 3.2). The following global type specifies the first half of the Pget protocol ($\mathbb{A} = \mathbb{Z}$): $G_{\text{Pget}} =$

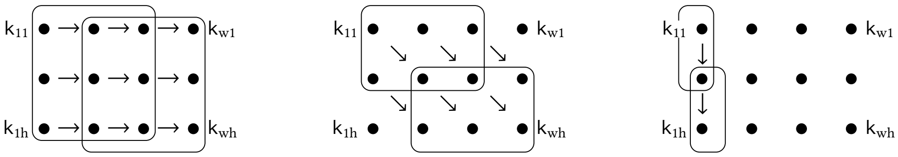
$$\mathtt{F[1]} \longrightarrow \mathtt{S} : \mathtt{Head}\ .\ \mathtt{S} \longrightarrow \mathtt{F[1]} : \mathtt{Res}\ .\ \mathtt{F[1]} \longrightarrow \mathtt{M} : \mathtt{Size}\ .\ \mathtt{foreach}\ \mathtt{F}\{\mathtt{i}{:}\mathtt{1..k}\}\ \mathtt{do}\ (\mathtt{M} \longrightarrow \mathtt{F[i]} : \mathtt{Range}\ .\ \mathtt{cont})\ ;\ \ldots$$

Example 4.4 (Ring). Let $\mathtt{k}$ represent the number of Workers in the Ring protocol (§ 2.2). The following global type specifies the Ring protocol, extended with branching and recursion ($\mathbb{A} = \mathbb{Z}$): $G_{\text{Ring}} = \mathtt{rec}\ \mathtt{X}\ \mathtt{W[1]} \longrightarrow \mathtt{W[2]} :$

$$\left\{\begin{array}{l} \mathtt{Nx}\ .\ \mathtt{foreach}\ \mathtt{W}\{\mathtt{i}_1{:}\mathtt{2..k\text{-}1},\ \mathtt{i}_2{:}\mathtt{3..k}\}\ \mathtt{do}\ (\mathtt{W[i_1]} \longrightarrow \mathtt{W[i_2]} : \mathtt{Nx}\ .\ \mathtt{cont})\ ;\ (\mathtt{W[k]} \longrightarrow \mathtt{W[1]} : \mathtt{Nx}\ .\ \mathtt{X}) \\ \mathtt{Dn}\ .\ \mathtt{foreach}\ \mathtt{W}\{\mathtt{i}_1{:}\mathtt{2..k\text{-}1},\ \mathtt{i}_2{:}\mathtt{3..k}\}\ \mathtt{do}\ (\mathtt{W[i_1]} \longrightarrow \mathtt{W[i_2]} : \mathtt{Dn}\ .\ \mathtt{cont})\ ;\ (\mathtt{W[k]} \longrightarrow \mathtt{W[1]} : \mathtt{Dn}\ .\ \mathtt{end}) \end{array}\right\}$$

Example 4.5 (Fibonacci). The following global type specifies a Fibonacci-$\mathtt{k}$ protocol ($\mathbb{A} = \mathbb{Z}$):

$$\begin{array}{l} G_{\text{Fib}} = \mathtt{foreach}\ \mathtt{Fib}\{\mathtt{i}_{(\text{-}2)}{:}\mathtt{1..k\text{-}2},\ \mathtt{i}_{(\text{-}1)}{:}\mathtt{2..k\text{-}1},\ \mathtt{i}{:}\mathtt{3..k}\}\ \mathtt{do} \\ \qquad (\mathtt{Fib[i_{(\text{-}2)}]} \longrightarrow \mathtt{Fib[i]} : \mathtt{Val}\ .\ \mathtt{Fib[i_{(\text{-}1)}]} \longrightarrow \mathtt{Fib[i]} : \mathtt{Val}\ .\ \mathtt{cont})\ ;\ \mathtt{end} \end{array}$$



(a) Horizontal wave (b) Diagonal wave (c) Column pipeline

Fig. 9. Basic mesh communication patterns (Ex. 4.7)

Example 4.6 (Hadamard). Let $\mathtt{k}_{11}$ and $\mathtt{k}_{\mathrm{wh}}$ represent the top-left and the bottom-right of 2d matrices A, B, and C. The following global types specifies a protocol to compute the Hadamard product (i.e., coordinate-wise product) of A and B as C ($\mathbb{A} = \mathbb{Z} \times \mathbb{Z}$):

$$G_{\mathrm{Had}} = \mathtt{foreach}\ \{\mathtt{A},\mathtt{B},\mathtt{C}\}\{\mathtt{i}:\mathtt{k}_{11}..\mathtt{k}_{\mathrm{wh}}\}\ \mathtt{do}\ (\mathtt{A[i]} \longrightarrow \mathtt{C[i]} : \mathtt{Val}\ .\ \mathtt{B[i]} \longrightarrow \mathtt{C[i]} : \mathtt{Val}\ .\ \mathtt{cont})\ ;\ \mathtt{end}$$

Example 4.7 (Mesh). Let $\mathtt{k}_{11}$, $\mathtt{k}_{1\mathrm{h}}$, $\mathtt{k}_{\mathrm{w}1}$, and $\mathtt{k}_{\mathrm{wh}}$ represent the top-left, the bottom-left, the top-right, and the bottom-right of a 2d mesh. The following global types (message labels omitted), three of which are visualised in Fig. 9 for a 4×3 mesh, specify five basic mesh communication patterns: horizontal wave, diagonal wave, column pipeline, 2d scatter, 2d gather.

$$\begin{aligned}
G_{\mathrm{HWave}} &= \mathtt{foreach}\ \mathtt{W}\{\mathtt{i}_1:\mathtt{k}_{11}..\mathtt{k}_{\mathrm{wh}}\text{-}(1,0), \mathtt{i}_2:\mathtt{k}_{11}\text{+}(1,0)..\mathtt{k}_{\mathrm{wh}}\}\ \mathtt{do}\ (\mathtt{W[i_1]} \longrightarrow \mathtt{W[i_2]}\ .\ \mathtt{cont})\ ;\ \mathtt{end}\\
G_{\mathrm{DWave}} &= \mathtt{foreach}\ \mathtt{W}\{\mathtt{i}_1:\mathtt{k}_{11}..\mathtt{k}_{\mathrm{wh}}\text{-}(1,1), \mathtt{i}_2:\mathtt{k}_{11}\text{+}(1,1)..\mathtt{k}_{\mathrm{wh}}\}\ \mathtt{do}\ (\mathtt{W[i_1]} \longrightarrow \mathtt{W[i_2]}\ .\ \mathtt{cont})\ ;\ \mathtt{end}\\
G_{\mathrm{ColPipe}} &= \mathtt{foreach}\ \mathtt{W}\{\mathtt{i}_1:\mathtt{k}_{11}..\mathtt{k}_{1\mathrm{h}}\text{-}(0,1), \mathtt{i}_2:\mathtt{k}_{11}\text{+}(0,1)..\mathtt{k}_{1\mathrm{h}}\}\ \mathtt{do}\\
&\qquad (\mathtt{W[i_1]} \longrightarrow \mathtt{W[i_2]}\ .\ \mathtt{cont})\ ;\ \mathtt{W[k_{1h}]} \longrightarrow \mathtt{W[k_{11}]}\ .\ \mathtt{end}\\
G_{\mathrm{2dSca}} &= \mathtt{foreach}\ \mathtt{W}\{\mathtt{i}:\mathtt{k}_{11}..\mathtt{k}_{\mathrm{wh}}\}\ \mathtt{do}\ (\mathtt{M} \longrightarrow \mathtt{W[i]}\ .\ \mathtt{cont})\ ;\ \mathtt{end}\\
G_{\mathrm{2dGat}} &= \mathtt{foreach}\ \mathtt{W}\{\mathtt{i}:\mathtt{k}_{11}..\mathtt{k}_{\mathrm{wh}}\}\ \mathtt{do}\ (\mathtt{W[i]} \longrightarrow \mathtt{M}\ .\ \mathtt{cont})\ ;\ \mathtt{end}
\end{aligned}$$

Remark 2. Although our foreach operator for global types unrolls iterations of its body sequentially in terms of its index values, it maintains the concurrency characteristics of MPST. E.g., in standard MPST, the two interactions in $\mathtt{A} \longrightarrow \mathtt{B} : \mathtt{Foo}\ .\ \mathtt{C} \longrightarrow \mathtt{D} : \mathtt{Bar}$ are concurrent since the roles in each are independent; this remains the case if such a fragment occurs inside a foreach, e.g., the A/B action of the final iteration could potentially occur before the C/D of the first iteration.

In addition to such "latent" concurrency, a global foreach may be elided from the *local* type by projection depending on the communication pattern. For instance, none of the Worker local types in the Pipeline protocol (shown in the next paragraph) has foreach, contrasting the global type in Fig. 8. This observation is more pronounced when extended to a Recursive Pipeline protocol, $\mathtt{rec}\ X\ (\mathtt{foreach}\ \mathtt{W}\{\mathtt{i}_1:1..\mathtt{k}\text{-}1, \mathtt{i}_2:2..\mathtt{k}\}\ \mathtt{do}\ (\mathtt{W[i_1]} \longrightarrow \mathtt{W[i_2]} : \mathtt{Val}\ .\ \mathtt{cont})\ ;\ X)$, which allows multiple Worker pairs (participating in different recursive calls) to communicate concurrently.

Our implementation also supports runtime parallelisation of foreach as an optimisation, when parameterised variants do not interact (demonstrated in § 3.3).

Local types. Fig. 7, third line, shows the syntax of local types. $r[x]\,!\{\ell_j\ .\ L_j\}_{j \in J}$ denotes the *send* of a message labelled as ℓ_j to receiver $r[x]$, for $j \in J$ (chosen by the sender), followed by the actions specified in L_j. Symmetrically, $r[x]\,?\{\ell_j\ .\ L_j\}_{j \in J}$ denotes the *receive* of a message labelled as ℓ_j from sender $r[x]$. For instance, the local types for $\mathtt{k} = 3$ Workers in the Pipeline protocol are:

$$L^{\mathtt{W[1]}}_{\mathrm{Pipe}} = \mathtt{W[2]}\ !\ \mathtt{T}\ .\ \mathtt{end} \qquad L^{\mathtt{W[2]}}_{\mathrm{Pipe}} = \mathtt{W[1]}\ ?\ \mathtt{T}\ .\ \mathtt{W[3]}\ !\ \mathtt{T}\ .\ \mathtt{end} \qquad L^{\mathtt{W[3]}}_{\mathrm{Pipe}} = \mathtt{W[2]}\ ?\ \mathtt{T}\ .\ \mathtt{W[4]}\ !\ \mathtt{T}\ .\ \mathtt{end}$$

The Supplement,[4] § II.2 contains more example local types, for the same protocols as above.

Syntactic sugar. Fig. 10 shows syntactic sugar for foreach in global types and local types. $\overset{*}{\longrightarrow}$ expands to an *all-to-all* global type; it demonstrates foreach nesting. $\overset{*}{\Longrightarrow}$ expands to a *pairings* global type. Note that while senders may have multiple labels to choose from (if $|J| > 1$), each of

$$\begin{aligned}
r_1[D_1] \xrightarrow{*} r_2[D_2] : \{\ell_j \,.\, G'\}_{j\in J} &\triangleq \texttt{foreach}\ r_1\{\texttt{i}_1 : D_1\}\ \texttt{do} \\
&\qquad (\texttt{foreach}\ r_2\{\texttt{i}_2 : D_2\}\ \texttt{do}\ (r_1[\texttt{i}_1] \to r_2[\texttt{i}_2] : \{\ell_j \,.\, \texttt{cont}\}_{j\in J})\ ;\ \texttt{cont})\ ;\ G' \\
r_1[D_1] \xRightarrow{*} r_2[D_2] : \{\ell_j \,.\, G'\}_{j\in J} &\triangleq \texttt{foreach}\ \{r_1, r_2\}\{\texttt{i}_1 : D_1, \texttt{i}_2 : D_2\}(r_1[\texttt{i}_1] \to r_2[\texttt{i}_2] : \{\ell_j \,.\, \texttt{cont}\}_{j\in J})\ ;\ G' \\
r_1 \xrightarrow{1} r_2[E_1 \mathinner{..} E_2] : \{\ell_j \,.\, G_j\}_{j\in J} &\triangleq r_1 \to r_2[E_1] : \{\ell_j \,.\, \texttt{foreach}\ r_2\{\texttt{i} : E_1\texttt{+1} \mathinner{..} E_2\}\ \texttt{do}\ (r_1 \to r_2[\texttt{i}] : \ell_j \,.\, \texttt{cont})\ ;\ G_j\}_{j\in J} \\
r \xRightarrow{1} [E_1 \mathinner{..} E_2] : \{\ell_j \,.\, G_j\}_{j\in J} &\triangleq r[E_1] \to r[E_1\texttt{+1}] : \left\{\begin{matrix} \ell_j \,.\, \texttt{foreach}\ r\{\texttt{i}_1 : E_1\texttt{+1} \mathinner{..} E_2\texttt{-1}, \texttt{i}_2 : E_1\texttt{+2} \mathinner{..} E_2\}\ \texttt{do} \\ (r[\texttt{i}_1] \to r[\texttt{i}_2] : \ell_j \,.\, \texttt{cont})\ ;\ G_j \end{matrix}\right\}_{j\in J} \\
r[D]\,\dagger^*\{\ell_j \,.\, L'\}_{j\in J} &\triangleq \texttt{foreach}\ r\{\texttt{i} : D\}\ \texttt{do}\ (r[\texttt{i}]\,\dagger\{\ell_j \,.\, \texttt{cont}\}_{j\in J})\ ;\ L' \quad \text{if } \dagger \in \{!, ?\} \\
r[D]\,!^1\{\ell_j \,.\, L_j\}_{j\in J} &\triangleq r[E_1]\,!\,\{\ell_j \,.\, \texttt{foreach}\ r\{\texttt{i} : E_1\texttt{+1} \mathinner{..} E_2\}\ \texttt{do}\ (r[\texttt{i}]\,!\,\ell_j \,.\, \texttt{cont})\ ;\ G_j\}_{j\in J} \quad \text{if } D = E_1 \mathinner{..} E_2
\end{aligned}$$

Fig. 10. Syntactic sugar for global types ($\xrightarrow{*}$, $\xRightarrow{*}$, $\xrightarrow{1}$, $\xRightarrow{1}$) and local types ($\dagger^*$, $!^1$), under $\mathbb{A} = \mathbb{Z}$

these choices has the same continuation G'. This is to syntactically enforce a fundamental rule of interacting parties in a parameterised setting: if a protocol allows separate parties to make independent (inconsistent) choices without additional synchronisation, the continuation of that protocol cannot depend on any of those choices (because parties are not aware of all choices made).

$\xrightarrow{1}$ expands to a *master-slaves* global type, where the master (r_1) chooses a message label from $\{\ell_j\}_{j\in J}$ and communicates a corresponding message to all its slaves (r_2); the distinguished communication from the master to the first slave ensures the master commits to its initial choice. $\xRightarrow{1}$ expands to a *pipeline* global type, where the front Worker chooses a message label from $\{\ell_j\}_{j\in J}$, then corresponding messages are propagated onward. In these two sugars, only one choice is made (in contrast to $\xrightarrow{*}$ and $\xRightarrow{*}$), known to all parties, allowing choice-dependent continuations.

$\dagger^*$ expands to a *send-to-all* ($\dagger = !$) or *receive-from-all* ($\dagger = ?$) local type that corresponds precisely to the projections of (the expansion of) $\xrightarrow{*}$. Similarly, $!^1$ expands to a send-to-all local type that corresponds precisely to the projections of $\xrightarrow{1}$. The difference between $!^*$ and $!^1$ pertains to *the number of choices* made: with $!^*$, the sender *may* choose a *different* message label for every receiver, while with $!^1$, the sender *must* choose the *same* message label for every receiver. (No special local type sugar is needed for the remaining global type sugar, as its projections have no `foreach`.)

Example 4.8 (Syntactic sugar). The global types in Ex. 4.3, 4.4 can be rewritten:

$G_{\text{Pget}} = \texttt{F[1]} \to \texttt{S} : \texttt{Head} \,.\, \texttt{S} \to \texttt{F[1]} : \texttt{Res} \,.\, \texttt{F[1]} \to \texttt{M} : \texttt{Size} \,.\, \texttt{M} \xrightarrow{*} \texttt{F[1..k]} : \texttt{Range} \,.\, \ldots$

$G_{\text{Ring}} = \texttt{rec X } (\texttt{W} \xRightarrow{1} \texttt{[1..k]} : \{\texttt{Next} \,.\, \texttt{W[k]} \to \texttt{W[1]} : \texttt{Next} \,.\, \texttt{X},\ \texttt{Done} \,.\, \texttt{W[k]} \to \texttt{W[1]} : \texttt{Done} \,.\, \texttt{end}\})$

4.3 Role Variants

Role variants. In our theory, *different* individuals that enact a role with *the same* name may have *different* communication behaviours; theoretically, role names are uninterpreted constants, void of semantics. For instance, the front Worker (who only sends), the middle Workers (who both receive and send), and the back Worker (who only receives) in the Pipeline protocol (Fig. 8) have different communication behaviours, but they all enact the same role `W`.

This phenomenon presents a theoretical challenge: neither can we associate a single local type L with a role r (i.e., L can impossibly cover all behavioural variations exhibited by individuals that enact r), nor can we associate a local type with every individual (i.e., the number of individuals can be unknown until run-time). To solve this problem, we introduce the concept of *role variants*: a group of (ranks of) individuals that *both* enact the same role r *and* have "the same" behaviour, in the sense that the behaviour of each of these individuals can be specified by the same local type. For instance, the single local type that specifies the behaviour of every middle Worker is:

$$L_{\text{Pipe}}^{\texttt{W[2..k-1]}} = \texttt{W[self-1]}\,?\,\texttt{Val} \,.\, \texttt{W[self+1]}\,!\,\texttt{Val} \,.\, \texttt{end}$$

where `self` denotes a distinguished parameter to abstractly represent the rank of a concrete Worker, set at run-time (i.e., $L_{\text{Pipe},\texttt{W[2]}}$ on page 14 is obtained by setting $\texttt{self} = 2$).

Inferring role variants (1). Our language of global types does not feature constructs to explicitly specify role variants. This is because they can be *automatically inferred* from intervals. Before formulating our inference procedure in full generality, we explain its key points with two examples.

Reconsider the Pipeline global type G_{Pipe} in Fig. 8. Suppose we aim to determine the behaviour of Worker a. The iteration domain in G_{Pipe} specifies two intervals: `1..k-1` and `2..k`.

- If a is contained in interval `1..k-1`, but it is not contained in interval `2..k`, then a = `1`. In this case, Worker a participates in exactly one iteration of the loop (i.e., the first one), as a sender.
- If a is not contained in interval `1..k-1`, but it is contained in interval `2..k`, then a = `k`. In this case, Worker a also participates in exactly one iteration of the loop (i.e., the last one), as a receiver.
- If a is contained in both intervals, then `1` $<$ a $<$ `k`. In this case, Worker a participates in *two* iterations of the loop: first as a receiver, and then as a sender.

The crucial insight demonstrated by this example is that the behaviour of any Worker is *completely* determined by the intervals that contain its rank; there are no other sources of behavioural variation. Moreover, since the number of intervals in any global type is bounded, the number of role variants is bounded as well: role `W` occurs with only two intervals in G_{Pipe}, so `W` has at most 2^2 variants.

Inferring role variants (2). Consider global type $G'_{\text{Pipe}} = \texttt{M} \longrightarrow \texttt{W[1]} : \texttt{Init} \,.\, G_{\text{Pipe}}$, which prefixes G_{Pipe} with an initial communication from the Master to the first Worker. In this global type, role name `W` occurs actually with *three* intervals: two explicit ones in the iteration domain in G_{Pipe} (as before), and one implicit one in the initial communication, namely `1..1`. To see where this implicit interval comes from, note that the initial communication can be rewritten with `foreach`:

$$\texttt{foreach W\{i:1..1\} do (M} \longrightarrow \texttt{W[i] : Init . cont)} \;;\; G_{\text{Pipe}}$$

(Such rewriting is not always possible, because it generally does not preserve well-formedness; we do it here only to show what we mean with "implicit intervals".) Since role `W` occurs with three intervals in G'_{Pipe}, `W` has at most 2^3 variants. Four of these "potential variants" of `W` are *invalid.* For instance, there exists no rank a that is *both* in interval `1..1` *and* in interval `2..k`.

Inference procedure. We formulate our inference procedure as follows. Let $\mathsf{ival}(r, G)$ denote the set of intervals consisting of $\{D_j\}_{j \in J}$ for every $\texttt{foreach}\ R \cup \{r\}\{i_j : D_j\}_{j \in J}\ \texttt{do}\ G_1 \,;\, G_2$ in G and $E\,..\,E$ for every $r[E]$ in G. Note that ival does *not* interpret intervals into sets of concrete ranks; every element in $\mathsf{ival}(r, G)$ is syntactic, of the shape $E_1\,..\,E_2$. Every binary partition $\mathcal{D}, \bar{\mathcal{D}}$ of $\mathsf{ival}(r, G)$, of the total $2^{|\mathsf{ival}(r,G)|}$, characterises a potential variant of role r; we denote this variant as $r[\mathcal{D}, \bar{\mathcal{D}}]$. To check its validity, we construct a formula $\Phi(\mathcal{D}, \bar{\mathcal{D}})$. Let $k_1, k_2, \ldots$ denote the parameters in G.

$$\Phi(E_1\,..\,E_2) = E_1 \leq \texttt{self} \leq E_2 \qquad \Phi(\mathcal{D}, \bar{\mathcal{D}}) = \exists \texttt{self}.\big[\big[\textstyle\bigwedge_{D \in \mathcal{D}} \Phi(D)\big] \wedge \big[\textstyle\bigwedge_{\bar{D} \in \bar{\mathcal{D}}} \neg\Phi(\bar{D})\big]\big]$$

If $\exists k_1.\exists k_2.\ldots\Phi(\mathcal{D}, \bar{\mathcal{D}})$ is true, there exists at least one instantiation of parameters $k_1, k_2, \ldots$ such that there exists a individual (i.e., $\exists\texttt{self}$) whose rank is contained in all the intervals in $\mathcal{D}$ (i.e., $\bigwedge_{D \in \mathcal{D}} \Phi(D)$), and not contained in all the intervals in $\bar{\mathcal{D}}$ (i.e., $\bigwedge_{\bar{D} \in \bar{\mathcal{D}}} \neg\Phi(\bar{D})$). In more operational terms, if $\Phi(\mathcal{D}, \bar{\mathcal{D}})$ is true, there exists at least one run-time configuration of parameters in which at least one individual enacts the role variant characterised by $\Phi(\mathcal{D}, \bar{\mathcal{D}})$; thus, $r[\mathcal{D}, \bar{\mathcal{D}}]$ is valid. Conversely, if $\Phi(\mathcal{D}, \bar{\mathcal{D}})$ is false, there exists no such run-time configuration, meaning invalidity.

Thus, our inference procedure for variants of role r works as follows: (1) compute $\mathsf{ival}(r, G)$; (2) for every partition $\mathcal{D}, \bar{\mathcal{D}}$ of $\mathsf{ival}(r, G)$, check $\Phi(\mathcal{D}, \bar{\mathcal{D}})$; (3) $\Phi(\mathcal{D}, \bar{\mathcal{D}})$ is true iff $r[\mathcal{D}, \bar{\mathcal{D}}]$ is valid.

Inferring families. A *family* is a set of role variants that collectively constitute a consistent run-time configuration of an application. For instance, the Pipeline protocol has two families (Fig. 8): one for `k` = `2` (front and last Worker), and one for `k` > `2` (front, middle, and last Worker).

Role variant families can be inferred using a similar approach as for role variants. Let V_{all} denote the set of all inferred role variants. For every partition $V, \bar{V}$ of V_{all}, construct the following formula:

$$\Xi(V, \bar{V}) = \left[\, \textstyle\bigwedge_{r[\mathcal{D},\bar{\mathcal{D}}] \in V} \Phi(\mathcal{D}, \bar{\mathcal{D}}) \right] \wedge \left[\, \textstyle\bigwedge_{r[\mathcal{D},\bar{\mathcal{D}}] \in \bar{V}} \neg\Phi(\mathcal{D}, \bar{\mathcal{D}}) \right]$$

If $\exists k_1.\exists k_2.\ldots\Xi(V, \bar{V})$ is true, there exists at least one instantiation of parameters $k_1, k_2, \ldots$ such that only every variant in V is enacted by at least one individual, so V is a family.

4.4 Projection

Our final ingredient is a *projection* operator, $\upharpoonright$: it consumes as input a global type G and a role variant $r[\mathcal{D}, \bar{\mathcal{D}}]$, and it produces as output *one* local type that specifies the behaviour of *all* individuals that enact $r[\mathcal{D}, \bar{\mathcal{D}}]$. Below is an excerpt of the definition:

$$(r_1[x_1] \rightarrow r_2[x_2] : \{\ell_j\ .\ G_j\}_{j\in J}) \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}] = \begin{cases} r_2[x_2]\ !\ \{\ell_j\ .\ G_j \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}]\}_{j\in J} & \text{if } r_1 = r \neq r_2,\ x_1..x_1 \in \mathcal{D} \\ r_1[x_1]\ ?\{\ell_j\ .\ G_j \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}]\}_{j\in J} & \text{if } r_1 \neq r = r_2,\ x_2..x_2 \in \mathcal{D} \\ \sqcap\{G_j \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}]\}_{j\in J} & \text{if } r_1 \neq r \neq r_2 \end{cases}$$

$$(\texttt{foreach}\ R\{i_j : D_j\}_{j\in J}\ \texttt{do}\ G_1\ ;\ G_2) \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}] = \begin{cases} \ldots\ \textit{(omitted – see Supplement,[4] §II.3)} & \text{if } r \in R \\ \texttt{foreach}\ R\{i_j : D_j\}_{j\in J}\ \texttt{do} & \text{if } r \notin R \\ \quad (G_1 \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}])\ ;\ (G_2 \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}]) & \end{cases}$$

$$\texttt{rec}\ X\ G \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}] = \texttt{rec}\ X\ (G \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}]) \qquad X \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}] = X \qquad G \upharpoonright r[\mathcal{D}, \bar{\mathcal{D}}] = G \quad \textbf{if: } G \in \{\texttt{cont}, \texttt{end}\}$$

$\upharpoonright$ recursively traverses the structure of global type G and checks for every communication whether role variant $r[\mathcal{D}, \bar{\mathcal{D}}]$ (i.e., an individual that enacts $r[\mathcal{D}, \bar{\mathcal{D}}]$) participates as the sender or the receiver. If so, it adds a corresponding I/O action to the local type under construction; otherwise, it continues the traversal and *merges* projections of the continuations using $\sqcap$; the definition of $\sqcap$ is standard (e.g., [Deniélou et al. 2012]), extended in the natural way for `foreach`. As usual (e.g., [Coppo et al. 2016; Honda et al. 2016]), projection is partial: it is undefined for unsafe protocols.

If `foreach` is encountered, our projection operator checks if r is in the iteration domain. If it *is not*, $r[\mathcal{D}, \bar{\mathcal{D}}]$ participates in *all* iterations of the loop (i.e., `foreach` must be preserved in the local type under construction), and in every iteration, it behaves according to the projected body (possibly empty, i.e., `cont`). Otherwise, if r *is* in the iteration domain, $r[\mathcal{D}, \bar{\mathcal{D}}]$ participates in only *some* iterations (i.e., `foreach` must not be preserved), for which special measures need to be taken, represented above as "…"; see the Supplement,[4] § II.3 for the full definition.

Example 4.9. Role `S` *does not* occur in the iteration domain of `foreach` in G_{Pget}, Ex. 4.3, so must be preserved in $G_{\text{Pget}} \upharpoonright \texttt{S}[\{\texttt{0..0}\}, \emptyset]$. This is as expected: Server receives from all Fetchers, so it participates in all iterations. In contrast, role `F` *does* occur in the iteration domain, so `foreach` is lost in $G_{\text{Pget}} \upharpoonright \texttt{F}[\{\texttt{2..k}\}, \{\texttt{1..1}\}]$. This, too, is as expected: every Fetcher sends exactly once to Server.

4.5 Decidability and Correctness

Inference procedures. We first address the decidability of our inference procedures in § 4.3.

Theorem 4.10. *Inference of role variants and families is decidable.*

Proof. Because $\text{ival}(r, G)$ is finite (i.e., the set of intervals that occur syntactically in G), the number of binary partitions $\mathcal{D}, \bar{\mathcal{D}}$ is finite as well. Also, $\Phi(\mathcal{D}, \bar{\mathcal{D}})$ and $\Xi(V, \bar{V})$ are formulas over $\langle \mathbb{A}, +, 0, \leq \rangle$, which is decidable (see § 4.1 and Ex. 4.1, 4.2). □

Well-formedness. We guarantee correctness and safety for *well-formed* global types. Let $\mathbb{K} \rightharpoonup \mathbb{A}$ denote the set of all partial *substitutions* of values for parameters, ranged over by σ, τ; let $G\,\langle\!\langle \sigma \rangle\!\rangle$ denote the *instantiation* of G in accordance with σ. A substitution σ *closes* global type G if $G\,\langle\!\langle \sigma \rangle\!\rangle$ has no parameters; $G\,\langle\!\langle \sigma \rangle\!\rangle$ is *well-closed* if all intervals in $G\,\langle\!\langle \sigma \rangle\!\rangle$ are non-empty.

A global type G is well-formed if for all σ such that $G\,\langle\!\langle \sigma \rangle\!\rangle$ is well-closed: (1) index variables and type variables in G are bound by `foreach` and `rec`; (2) `rec` does not occur under `foreach` in G; (3) an "inner" `foreach` in G cannot range over role names already ranged over by an "outer" `foreach`; (4) all intervals in the same iteration domain in $G\,\langle\!\langle \sigma \rangle\!\rangle$ have the same length. Condition (2) ensures that every iteration of a loop terminates; we support only tail recursion. Condition (3) ensures that the number of iterations an individual participates in can be computed statically. Condition (4) ensures that the "table" for every iteration domain (e.g., Fig. 8) has a well-defined number of "rows".

Theorem 4.11. *Checking well-formedness is decidable.*

Proof. Conditions (1), (2), and (3) are structural and independent of σ; checking them is trivially decidable. In contrast, checking condition (4) requires universal quantification over the set $\{\sigma \mid G \langle\!\langle \sigma \rangle\!\rangle \text{ is well-closed}\}$, which can be infinite. To check (4), we construct a first-order formula over $\langle \mathbb{A}, +, 0, \preceq \rangle$, which is decidable (see § 4.1 and Ex. 4.1, 4.2), as follows. Let $k_1, k_2, \ldots$ denote the parameters that occur in G, and let $\mathcal{I}$ denote the set of all iteration domains that occur in G:

$$\Psi_{\neg\emptyset}(\{i_j : E_{j,1} .. E_{j,2}\}_{j \in J}) = \textstyle\bigwedge_{j \in J} E_{j,1} \preceq E_{j,2} \qquad \Psi(\mathcal{I}) = \forall k_1.\forall k_2 \ldots \big[\textstyle\bigwedge_{I \in \mathcal{I}} \Psi_{\neg\emptyset}(I) \Rightarrow \textstyle\bigwedge_{I \in \mathcal{I}} \Psi_{=}(I) \big]$$

$$\Psi_{=}(\{i_j : E_{j,1} .. E_{j,2}\}_{j \in J}) = \textstyle\bigwedge_{j_1, j_2 \in J} (E_{j_1,2} - E_{j_1,1} = E_{j_2,2} - E_{j_2,1})$$

Now, $\Psi(\mathcal{I})$ is true iff (4) holds. □

Correctness and safety. In words, ***correctness*** of $\restriction$ means that the behaviour specified by an instantiated well-formed global type G equals the joint behaviour specified by the instantiated local types projected from G, namely one for every individual that enacts an inferred role variant.

Let $L \langle\!\langle \tau \rangle\!\rangle$, $\mathcal{D} \langle\!\langle \tau \rangle\!\rangle$, and $\bar{\mathcal{D}} \langle\!\langle \tau \rangle\!\rangle$ denote the instantiation of the parameters in local type L and sets of intervals $\mathcal{D}, \bar{\mathcal{D}}$ according to τ (cf. $G \langle\!\langle \sigma \rangle\!\rangle$, above). Let $\equiv$ denote trace equivalence of the LTSs induced by a global type and a system (parallel composition) of local types [Deniélou and Yoshida 2013]. The following theorem states correctness; see the Supplement,[4] § II.4 for our proof.

Theorem 4.12. *For all well-formed G and σ such that $G \langle\!\langle \sigma \rangle\!\rangle$ is well-closed:*

$$G \langle\!\langle \sigma \rangle\!\rangle \equiv \{ (G \restriction r[\mathcal{D}, \bar{\mathcal{D}}]) \langle\!\langle \tau \rangle\!\rangle \mid \exists a : \mathcal{D} \uplus \bar{\mathcal{D}} = \mathsf{ival}(r, G),\ \tau = \sigma \cup \{\texttt{self} \mapsto a\},\ \models \Phi(\mathcal{D} \langle\!\langle \tau \rangle\!\rangle, \bar{\mathcal{D}} \langle\!\langle \tau \rangle\!\rangle) \}$$

Projection guarantees ***safety*** if the joint behaviour specified by the instantiated local types projected from a well-formed global type is free of deadlocks and reception errors. Safety is a direct consequence of correctness: deadlocks and reception errors cannot be specified in our language of global types, so a correct projection never produces an unsafe system of local types. The formalisation of the following corollary relies on the same LTS semantics of global types and systems of local types as the one that underlies Thm. 4.12; see [Deniélou and Yoshida 2013].

Corollary 4.13. *Projection guarantees safety.*

5 IMPLEMENTATION

5.1 Extension of Scribble based on Distributed, Role-Parametric MPST

We extend the Scribble protocol language for role-parametric protocols based on our core formalism in § 4 and the syntactic sugars outlined in § 4.2. Our presented design results from experimenting with various combinations of primitives and communication patterns for a range of examples (summarised in Fig. 15). Fig. 11 (top) outlines our grammar: we add `foreach`, and cover the special global type arrows from Fig. 10 by extending the global interaction of Scribble (`from`/`to`) with indexed roles p and inline message choices ℓ_1 `or` … `or` ℓ_n, and adding the `pair`/`pipe` primitives; for simplicity, we show a restriction to one-dimensional indices (Ex. 4.1). g is a protocol name, and A stands for basic boolean expressions for constraints on index variables; other notation not explicitly defined here (e.g., r, E) is as in § 4.2. p^1 means the restriction of D to `[`E`,` E`]` or `[`i`]`. In our experience, these particular primitives are beneficial for writing protocols and using the generated APIs (cf. "manual" `foreach` encodings), and also run-time performance.

Fig. 11 (bottom) illustrates the correspondence between our formal notation and Scribble syntax. The Scribble PP choice subsumes the case of unary choices. For paired/pipelined-PP (top right), `pair` corresponds to $\overset{*}{\Rightarrow}$, where the choice is made *independently* by each $r_1[i]$ to its opposing peer in the r_2 interval; `pipe` may be used here as the special case where $r_1 = r_2$ (so the choice is made

$$
\begin{array}{lcl}
P & ::= & \texttt{global protocol}\ g\ \texttt{@}A\,(\texttt{role}\ r_1\texttt{, ..., }\texttt{role}\ r_n)\ \{\ G\ \} \qquad p\ ::=\ r\texttt{[}y\texttt{]} \qquad y\ ::=\ D \mid i \qquad D\ ::=\ E_1\texttt{,}\ E_2 \\
G & ::= & \ell_1\ \texttt{or}\ \ldots\ \texttt{or}\ \ell_n\ \texttt{from}\ p_1\ \texttt{to}\ p_2\texttt{;}\ \mid\ \texttt{choice at}\ p^1\ \{\ G_1\ \}\ \texttt{or}\ \ldots\ \texttt{or}\ \{\ G_n\ \}\ \mid\ \texttt{do}\ g\texttt{(}r_1\texttt{, ..., }r_n\texttt{);}\ \mid\ G_1\ G_2 \\
 & \mid & \ell\ \texttt{pair}\ p_1\ \texttt{to}\ p_2\texttt{;}\ \mid\ \ell\ \texttt{pipe}\ r\texttt{[}D\texttt{];}\ \mid\ \texttt{foreach}\ r_1\texttt{[}i_1\texttt{:}D_1\texttt{], ..., }r_n\texttt{[}i_n\texttt{:}D_n\texttt{]}\ \{\ G\ \}
\end{array}
$$

Role-parametric subprotocols	$\texttt{foreach}\ R\{i_j : D_j\}_{j\in J}\ \texttt{do}\ G_1$	$\texttt{foreach}\ r_1\texttt{[}D_1\texttt{], ..., }r_n\texttt{[}D_n\texttt{]}\{\ G\ \}$
Choice(s)	Scatter/gather/all-to-all: →	Paired/pipelined unicasts: ⇒
Peer-to-peer	$r_1[D_1] \xrightarrow{*} r_2[D_2]\{\ell_1, \ell_2\}\ ;\ G$	$r_1[D_1] \overset{*}{\Rightarrow} r_2[D_2]\{\ell_1, \ell_2\}\ ;\ G$
(PP): $*$	$\ell_1\ \texttt{or}\ \ell_2\ \texttt{from}\ r_1\texttt{[}D_1\texttt{]}\ \texttt{to}\ r_2\texttt{[}D_2\texttt{];}\ G$	$\ell_1\ \texttt{or}\ \ell_2\ \texttt{pair}\ r_1\texttt{[}D_1\texttt{]}\ \texttt{to}\ r_2\texttt{[}D_2\texttt{];}\ G$
Master-slaves	$p^1 \xrightarrow{1} r_2[D_2]\{\ell_1.G_1, \ell_2.G_2\}$	$r \overset{1}{\Rightarrow} E_1\,..\,E_2\{\ell_1.G_1, \ell_2.G_2\}$
(MS): 1	$\texttt{choice at}\ p^1\ \{\ \ell_1\ \texttt{from}\ p^1\ \texttt{to}\ r_2\texttt{[}D\texttt{];}\ G_1\ \}$	$\texttt{choice at}\ r\texttt{[}E_1\texttt{]}\ \{\ \ell_1\ \texttt{pipe}\ r\texttt{[}E_1\texttt{,}E_2\texttt{];}\ G_1\ \}$
	$\texttt{or}\ \{\ \ell_2\ \texttt{from}\ p^1\ \texttt{to}\ r_2\texttt{[}D\texttt{];}\ G_2\ \}$	$\texttt{or}\ \{\ \ell_2\ \texttt{pipe}\ r\texttt{[}E_1\texttt{,}E_2\texttt{];}\ G_2\ \}$

Fig. 11. Practical syntax for role-parametric protocols: (top) extended Scribble grammar; (bottom) illustration of global type and Scribble correspondence (cf., the formal syntactic sugars in Fig. 10).

at each step along the interval). The MS choice is for more than one case (we show only binary choices for brevity). For pipelined-MS (bottom right), the interaction must be a pipe, where the choice is *propagated* along the interval, for the MS choice to be consistent at all receivers. In the Scribble foreach, $(r\texttt{[D]})_{1..n}$ enumerates the ranges used in the formal notation (cf. Rem. 1).

We omit the implementation details of basic syntactic checks (e.g., valid combinations of choice and from/pair/pipe as per Fig. 11) and well-formedness (§ 4.5) that are as expected. Cond. (4) of well-formedness, valid role variants, and variant families are similarly determined following § 4.3. Our toolchain integrates Scribble with Z3 to check the induced constraints; e.g., for Pipeline (Fig. 8), this generated Z3 assertion confirms the middleman is a valid variant:

```
(assert (exists ((self Int) (K Int)) (and (> K 1) // Annotated domain constraint
   (>= self 1) (<= self (- K 1)) (<= 1 (- K 1)) (>= self 2) (<= self K) (<= 2 K) // 𝒟 constraints for W2..K−1
   (not (and (>= self 1) (<= self 1))) (not (and (>= self K) (<= self K)))  )))  // 𝒟̄ constraints for W2..K−1
```

5.2 Communicating FSM Based Representation of Local Types

Our toolchain uses an internal representation of local types (§ 4.2) based on communicating FSMs with *gather/scatter I/O* and *parameterised nesting* of sub-FSMs within states. The correspondence between the syntactic types and our FSMs is straightforward: we outline the correspondence below, and provide a full definition in the Supplement,[4] § III.1.

Based on our local types, we write $r[D] \dagger \ell$, $\dagger \in \{!, ?\}$, for the scatter/gather I/O of our FSMs. Fig. 12 shows the FSMs for MS and PP choices; the latter demonstrates the basic FSM for foreach.

MS The $!^1$ send-to-all local type (§ 4.2), which selects the *same* choice at all peers, corresponds to an FSM scatter: the type $r[y] \ddagger \{\ell_j\ .\ L_j\}_{j\in J}$ is simply represented as a state with each of the J cases as a separate transition. Dually, MS input is implicitly a standard ? from a single peer (i.e., there is no $?^1$), for MS choices to be consistent across all receivers.

PP Non-unary PP choices are represented as nested FSMs, via foreach desugaring of $\xrightarrow{*}$ / $\overset{*}{\Rightarrow}$ (Fig. 10). For the example type $\texttt{foreach}\ r\{i\!:\!D\}\ \texttt{do}\ r[i] \dagger \{\ell_j\ .\ \texttt{cont}\}_{j\in J}; L$, the subprotocol – i.e., a †-choice of J cases – is nested and parameterised within the initial state of the FSM for the continuation L, denoted s_0^L. This FSM is just a representation of the local type behaviour: first repeat the nested FSM for each value of i in D in sequence, then perform one of $\alpha_{1..n}$ (standard state transition). At the local type level, unary PP choices coincide with MS choices: as an optimisation, we represent unary PP choices similarly to MS choices (i.e., without nesting).

We introduce some notation for our FSMs, that we shall use for defining our Go API generation. A *role variant FSM* (henceforth, *FSM*) is a tuple $M = (\mathbb{S}, \mathbb{R}, s_0, \mathbb{T}, \delta, \phi)$. Apart from the last element, all are standard [Deniélou and Yoshida 2012]. $\mathbb{S} = \{s_1, s_2, \ldots\}$ is a set of *state* identifiers; $s_0 \in \mathbb{S}$ is

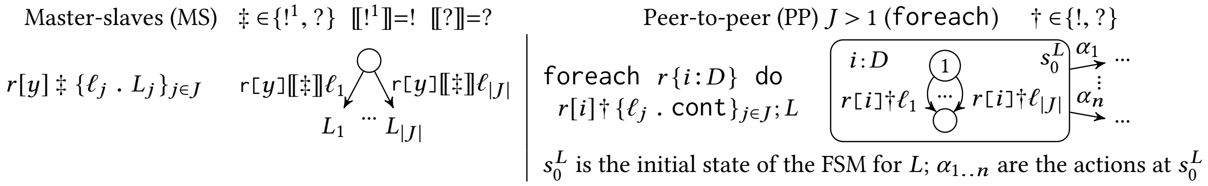

Master-slaves (MS) $\ddagger \in \{!^1, ?\}$ $[\![!^1]\!] = !$ $[\![?]\!] = ?$
$r[y] \ddagger \{\ell_j \,.\, L_j\}_{j \in J}$
$\mathtt{r[}y\mathtt{]}[\![\ddagger]\!]\ell_1$
$\mathtt{r[}y\mathtt{]}[\![\ddagger]\!]\ell_{|J|}$
L_1 ⋯ $L_{|J|}$
Peer-to-peer (PP) $J > 1$ (foreach) $\dagger \in \{!, ?\}$
foreach $r\{i:D\}$ do
$r[i] \dagger \{\ell_j \,.\, \mathtt{cont}\}_{j \in J}; L$
$i:D$
1
$\mathtt{r[}i\mathtt{]}\dagger\ell_1$
$\mathtt{r[}i\mathtt{]}\dagger\ell_{|J|}$
s_0^L
α_1
α_n
s_0^L is the initial state of the FSM for L; $\alpha_{1..n}$ are the actions at s_0^L

Fig. 12. Representation of local types as communicating FSMs (partial illustration).

the *initial state*. $\mathbb{R} = \{r_1, r_2, \ldots\}$ is a set of role names. $\mathbb{T} = \{\ell_1, \ell_2, \ldots\}$ is a set of *message labels*. $\delta : \mathbb{S} \times \{\alpha_1, \alpha_2, \ldots\} \longrightarrow \mathbb{S}$ is the *transition function*, where $\alpha_1, \alpha_2, \ldots$ are *local actions* of the form $r[y] \dagger \ell$ with $\dagger \in \{!, ?\}$. Finally, $\phi : \mathbb{S} \longrightarrow \mathbb{M} \times \mathbb{P}$ is the *nesting function*, where $\mathbb{M}$ is the domain of FSMs and $\mathbb{P}$ is the domain of sets of indexed intervals, ranged over by P.

By the syntax and properties of global types and projection (§ 4), every transition from a state has the same action kind $\dagger$; and every transition of an *input* state has the same *peer* $r[y]$. We also collapse every occurrence of `end` in a local type, if any, to a single terminal state at the top level of its FSM (similarly, for `cont` at the top level of a `foreach`). A "plain" state (i.e., that we depict without a nested FSM) corresponds to a state that nests a sole (terminal) state.

5.3 State Channel API Types Generation for Go

We first explain the key types and methods generation for states, I/O and branching, and nested FSMs. We simplify the presentation in two ways. First, we abstract from the details of specific naming schemes for types and methods: we use the notation $[\![\cdot]\!]$ to stand for any concrete name mapping, e.g., $[\![s]\!]$ is a Go type name for a state s, and $[\![s, \alpha]\!]$ is an I/O method name for action α from s. Second, we assume a "flat" naming scheme for methods, instead of the scheme presented in § 3, e.g., `S_Send_Head(...)` instead of `S.Send.Head(...)`; we illustrate the more cosmetically elaborate types generation for the latter in the Supplement,[4] § I.1.1. As noted earlier, a local program may use Go package/type aliases, or the user could supply custom names as Scribble annotations.

In the following, assume a variant $v = r[\mathcal{D}, \bar{\mathcal{D}}]$ (of some protocol g), and let s be a state in the FSM of v such that $\delta(s) = \{\alpha_j \mapsto s_j\}_{j \in J}$ and $\phi(s) = M, P$. Let $[\![M_0]\!]$ (resp. $[\![M_{\mathsf{End}}]\!]$) be a type name derived from the initial (resp. terminal, if present) state of M; and $[\![v]\!]$ be the type name of the Endpoint for v (e.g., the type of `M` on the left of Fig. 5, line 3).

Nested FSMs. Fig. 13 (top) shows the types generated w.r.t. the nesting of M in s. $[\![s]\!]$ is the "main" (or entry) *state channel* type for s (e.g., the initial state, or result of the previous I/O method). It offers a `Foreach` method, that takes a function from $[\![M_0]\!]$ to $[\![M_{\mathsf{End}}]\!]$, i.e., an implementation of the nested behaviour. The result (after all nested behaviours are completed) is $[\![s]\!]'$, an intermediary type for finally performing a transition out of s. The basic Go code for executing a nested FSM and the subsequent state transition may thus look like:

`s.Foreach(nested).m(...)` `s` is a variable of type $[\![s]\!]$, `nested` is of type `func(`$[\![M_0]\!]$`)` $[\![M_{\mathsf{End}}]\!]$

`Foreach` is generated to repeat `nested` over the intervals P embedded into the API, and `m` is the I/O method generated for the subsequent transition, explained next.

I/O and branching. The generation of I/O methods depends on which kind of state s is.

Output or unary-input For each $\alpha_j = r_1[y] \,!\ell_j$ with $|J| > 1$, or for $\alpha_1 = r_j[y] \,?\ell_1$ when $|J| = 1$:

`func (c *`$[\![s]\!]'$`)` $[\![s, \alpha_j]\!]$ `(m` $\langle\!\langle \ell_j \rangle\!\rangle$`) *`$[\![\delta(s, \ell_j)]\!]$ `{ ... }` $\langle\!\langle \ell_j \rangle\!\rangle$ is, e.g., $*\ell_j$ for `Send/Receive`, `[]`ℓ_j for `Scatter/Gather`

$(c *[\![s]\!]')$ is the method receiver (i.e., the intermediary result type of `Foreach`), $[\![s, \alpha_j]\!]$ is the method name, and $\langle\!\langle \ell_j \rangle\!\rangle$ stands for the parameters according to the I/O action kind (e.g., singleton `Send` `/Receive` are special cases of `Scatter/Gather`). We omit details of further variations, e.g., `Reduce`.

```
type ⟦s⟧ struct { Err error; id uint64; ep *⟦v⟧; ... } // State channel type: first do Foreach
func new_⟦s⟧(...) *⟦s⟧ { ... return &⟦s⟧{...} }          // Private constructor (used internally within API)
type ⟦s⟧′ struct { Err error; id uint64; ep *⟦v⟧; ... } // Intermediary type (after Foreach done)
func (c *⟦s⟧) Foreach(nested func(int, *⟦M₀⟧) ⟦M_End⟧) *⟦s⟧′ { ... } // int is the Foreach index param
```

State type		**Method name, signature**		
State	Peer	I/O	Label, value	Succ.
W_2toK_1	W_self_sub1	Branch()		*W_2toK_1_Cases
W_2toK_2	W_self_plus1	Send	Next(a *Next)	*W_2toK_1
W_2toK_3	W_self_plus1	Send	Done(a *Done)	End
W_2toK_1_Cases is an interface, implemented by the below case types				
$t_{\mathtt{Next}}$	n/a	Receive	Next(a *Next)	*W_2toK_2
$t_{\mathtt{Done}}$	n/a	Receive	Done(a *Done)	*W_2toK_3

```
var n next; var d Done
for {
  switch c := w.W_self_sub1.Branch().(type) {
  case *t_Next:
    w = c.             Receive.Next(&n).
          W_self_plus1.Send.    Next(&n)
  case *t_Done:
    return c.          Receive.Done(&d).
          W_self_plus1.Send.    Done(&d)    } }
```

Fig. 13. State channel API generation: (top) state channel and Foreach type signatures; (bottom) type switch branch API types and I/O methods for the $\mathtt{W}_{2..\mathtt{K}-1}$ variant in Ring (Ex. 4.4), and an example implementation.

Branch-input ($|J| > 1$) We show the branch API generation that targets Go *type switch* statements.

```
type ⟦s⟧_Cases interface { ⟦s⟧_Case() }
func (c *⟦s⟧′) Branch() *⟦s⟧_Cases { ... }
```

```
type ⟦s⟧_ℓⱼ struct { Err error; id uint64; ep *⟦v⟧; ... }
func (*⟦s⟧_ℓⱼ) ⟦s⟧_Case() { } // Implement _Cases i/face
func (c *⟦s⟧_ℓⱼ) ⟦s, αⱼ⟧(m *ℓⱼ) *⟦δ(s, ℓⱼ)⟧ { ... }
```

On the left, $[\![s]\!]$_Cases is an interface representing the valid choice cases: on the right, for each $\alpha_j = r[x]?\ell_j$, we generate an $[\![s]\!]_{\ell_j}$ type that implements this interface (via the token $[\![s]\!]$_Case method) and offers an appropriate $[\![s, \alpha_j]\!]$ input method. The Branch method, with receiver $*[\![s]\!]'$ (like the I/O methods above), is then generated to block until a message is received, and return the corresponding implementation of the $[\![s]\!]$_Cases interface.

As an example, Fig. 13 (bottom) summarises the branch API types generated for the $\mathtt{W}_{2..\mathtt{K}-1}$ "middleman" variant in Ring (Ex. 4.4) and gives a user implementation. A type switch switch c := ....(type) evaluates the expression (assigned to c) and selects the first case that matches the run-time *type* of the result. IDEs can auto-generate exhaustive switch cases for the programmer.

Our implementation simplifies the generated API as expected in certain cases. E.g., when M is a single state (i.e., s is a "plain" state), the API generation skips the intermediary $[\![s]\!]'$ type and Foreach method, and sets the receiver of the I/O methods directly to $[\![s]\!]$. Our examples in this paper assume a $[\![\cdot]\!]$ that maps terminal states to an End type; we also set the result of terminal I/O methods to a *non*-pointer End type for stronger safety, as it prevents, e.g., return nil.

Note that FSMs are explicitly used only at *compile*-time for the presented types generation: the point of the types is to statically guide the FSM structure implicitly in the program. At run-time, the only checks introduced by our APIs are on session initiation parameters and channel linearity, as explained in the next paragraph.

Automated inlining of dynamic checks. The static assurances of the generated Go API types are supported by automated inlining of a few kinds of lightweight run-time checks into the API.

Go preliminaries: a *defer* statement pushes a function call (e.g., a channel closure) onto a list; the list is executed after the surrounding function returns. *Panic* is a built-in function that stops the control flow of the calling goroutine and executes any deferred calls at each level of its call stack; control flow may be regained by (a deferred call to) the built-in *recover* function.

Endpoint initiation The first check is on the parameter values supplied to the Endpoint constructor (e.g., K in Fig. 5, line 3), derived straightforwardly from the $\mathcal{D}, \bar{\mathcal{D}}$ elements of the variant. This is a simpler version of the compile-time Z3 assertion illustrated in § 5.1 that just checks the constraints on concrete values (as a Go expression) rather than existential quantifications.

Secondly, the `Dial`/`Accept` methods are generated to check for, e.g., duplicate connections; similarly, the top-level `run` checks for missing connections. A violation of these checks raises a panic.

State channel API The implicit usage contract of a state channel API is to use every channel *instance* exactly once, i.e., *linearly*. Repeat usage is dynamically checked by assigning a fresh ID value to each channel instance (the `uint64` fields in Fig. 13, top) and recording for each Endpoint the ID of the currently active channel: every I/O method is generated to check the target channel is the indeed the currently active one. Endpoint completion, guided by the `End` return type of the generated top-level `run` method, is an (at most) one-time deferred check within `run`.

Error handling and failures. We integrate the call-chaining nature of the presented APIs with the explicit error handling paradigm of Go. The API is generated to (1) set the state channel `Err` field (Fig. 13, top) in the successor channel instance if the preceding action caused an error (`error` is an in-built interface type), or else `Err` is `nil`; and (2) raise a panic when an I/O method is called on a channel whose `Err` is not `nil`. By our safety guarantees (see below), an error means a failure in the underlying I/O or networking facilities, or perhaps the reception of an incorrect message type when interacting with a potentially unsafe participant—the deserialization operations in our generated API code for inputs serve as implicit compliance checks on received message types.

Idiomatic Go error handling using a state channel API is as below (cf. lines 18–19 in Fig. 5).

```
if m3 := m2.F_1toK.Scatter.Job(split(&meta)); m3.Err != nil { // Explicit handling (e.g., networking failure)
  ... } else { ... m4 := m3.F_1toK.Reduce.Data(&data, agg) ... } // Using m3 with m3.Err != nil would raise a panic
```

Here, we use the standard Go construct `if x := f(); P(x){ g(x) } else { h(x) }`, which first evaluates `f()` and assigns the result to `x`, then evaluates `P(x)` to true or false, and finally executes `g(x)` or `h(x)`; the scope of `x` is constrained to this statement. The above code thus first attempts a scatter to the Fetchers. If no error (e.g., network failure) occurs, `m3` is the expected successor state channel, `m3.Err` is nil, and the then-branch is executed; if an error occurs, `m3.Err` is non-nil and the else-branch is executed. Handling errors in this way is idiomatic Go.

5.4 Practical Safety Guarantees of our Generated APIs

Our results in § 4.5 ensure, for a given family in a well-formed role-parametric protocol, the set of projections onto each variant constitutes a safe, distributed decomposition of the protocol. In other words, a distributed instance of this protocol (i.e., a *session*) is guaranteed free from reception errors, deadlocks and orphan messages, at the level of abstraction of our target model of asynchronous, pairwise-ordered and reliable message passing between the endpoints. The purpose of the API generation step of our framework is then to promote *compliance* of concrete endpoint implementations to their projections via native Go type checking, supported by the dynamic checks built into the API (§ 5.3).

Specifically, a generated state channel API ensures: in a successfully initiated session,

> *a* statically *well-typed endpoint implementation will* never *perform a non-compliant I/O action w.r.t. the run-time instantiation of the role-parametric protocol, up to premature session termination.*

This is because the *only* way to *attempt* a non-compliant I/O action is to violate linear usage of a channel instance, in which case the in-built API check will (by default) raise a panic *without* actually performing the offending action. Such a situation effectively results, at worst, in an incomplete or premature termination of the endpoint, and thus the session, w.r.t. the protocol. Note, however, that premature termination is always a caveat in practice, due to program errors outside the session code, or node/network failures. In this regard, our API generation considers linearity violations and failures (via `Err`) uniformly, appealing to Go's in-built `panic`, `defer` and `recover` facilities.

Once a session is initiated, the only dynamic checks are on linear channel usage, giving an affine form [Tov and Pucella 2011] of the *MPST safety* discussed above. If the simple linearity condition of our APIs is respected, however, Go type checking is sufficient to ensure MPST safety. It would thus be possible to combine our approach with a technique for statically checking linear resource usage, given such a technique (with associated restrictions), to obtain the classical MPST safety outright.

Another highlight of our approach, and a basis for safety, is that the API generation *internalises* the management of parameter values and index expressions related to identifying the session peer(s) of every I/O action in the protocol—the user-supplied arguments of the generated I/O methods relate only to messages. As observed by Samofalov et al. [2005] of process rank indices/expression bugs in the setting of MPI programming, incorrect management of indices and parameters can be a tricky source of communication errors in practice.

On static channel linearity. We note *dynamic linearity checks are* **not** *fundamental to our overall approach.* By our results in § 4.5, our framework is amenable to the use of alternative API generation methods for separate endpoints: our toolchain also supports *callback*-based API generation, illustrated below for the first two states of `M` in Pget (Fig. 4):

```
M.register(M_1.state, func(c Cache, meta *Meta) { c.meta = meta }) // Callback for M_1: F_1?Meta
 .register(M_2.state, func(c Cache) { new M_2.F_1toK.Job(split(c.meta)) }) // M_2: F[1,K]!Job
 .... // Callbacks registered by user for each state on the generated Endpoint M
```

The above style of generated API encapsulates all communication channels under the API and internalises the *FSM* itself: after session initiation, the API calls back the user-supplied, state-specific functions at each state (upon message receipt for input states). Consequently, a Go endpoint program using the callback API enjoys *fully static* MPST safety (for a successfully initiated session with compliant peers); the tradeoff is requiring programming in an *event-driven* style.

The main API style presented in this paper promotes session programming in Go that is close to standard channel/socket based APIs (and the session π-calculi in MPST formalisms). One advantage is it allows us to re-implement existing Go programs more directly, as part of evaluating the applicability of our framework (see § 6). In our experience, debugging *local* linearity violations (as exceptions) is much simpler than the full task of debugging reception errors or deadlocks between distributed, non-compliant endpoint implementations.

The interested reader may find details on the Scribble-Go Runtime in the Supplement,[4] § III.2.

6 EVALUATION

We evaluate our framework in terms of run-time performance (§ 6.1), and applications (§ 6.2), using a machine with an Intel i7-8770 processor (6 physical and 6 virtual cores) and 16GB RAM, running Debian 9.1 and Go version `go1.11.2`. We used the Go benchmarking tools (https://godoc.org/testing).

6.1 Run-time Overheads of Generated APIs

Microbenchmarks. We measure the overheads introduced by our framework during session execution, due to using the generated state channel API, our Runtime, and dynamic linearity checks. We first present microbenchmarks as a worst-case for the above overheads in isolation, by performing no work other than I/O. We use three kinds of microbenchmark programs, for the core patterns: **One-to-Many** (multi-destination send, single-source receive), **Many-to-One** (single-destination send, multi-source receive), and **Many-to-Many** (multi-destination send, multi-source receive). Each benchmark kind is parameterised on a k: in the first two, k is the number of goroutines at the Many side; in the third, k is divided evenly between sender/receiver goroutines.

We implement each benchmark by two methods. **(1) Scribble-Go**: we specify the above patterns as protocols in our extended Scribble and implement the Endpoints using our generated APIs. For each Endpoint, we have two versions of initiation that differ only by the selected Runtime transport, **`shm`** or **`tcp`**. **(2) Go base cases**: each Scribble-Go program has a Go base case that corresponds to

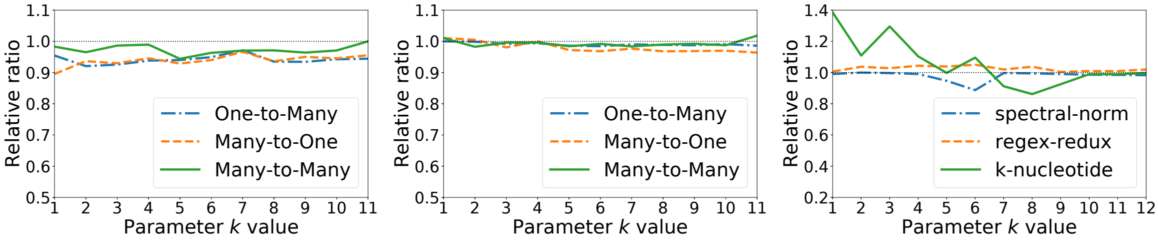


Fig. 14. **Scribble-Go** exec. time vs. **Go base cases**: (left) `shm` micro, (middle) `tcp` micro, and (right) CLBG.

replacing all occurrences and uses of state channels by direct references and uses of the underlying communication facilities, i.e., (unbounded) Go channels, or TCP sockets from the `net` package. We specify messages as having an `int` payload, and let k range over 1..11.

We measure the *execution time* from session start at the first sender (after *all* goroutines and connections established – in Scribble-Go, that is after entering the generated top-level `run`), to the end at the last receiver (before *any* connections closed). Since the execution time of a single instance of the above patterns is very small (on the order of nanoseconds), we repeat the communication actions (i.e., extend the "session length") in a loop of N iterations in each endpoint program and take the mean (N is set by the benchmarking tool, e.g., $> 10^6$, such that a run exceeds one second). The `tcp` endpoints are run as intra-process goroutines by the same setup as for `shm`, communicating through localhost TCP. We repeat each benchmark run 40 times and take the mean.

Fig. 14 (left) shows Go base case `shm` session execution time relative to Scribble-Go: x ranges over the value of k, and y is given by t_{go} / t_{api} ($y = 1$ is the baseline). The relative overheads of Scribble-Go are ∼10% in most cases, over the range of k; for reference, we note that the *absolute* overhead per pattern is ∼20 nanoseconds. Fig. 14 (middle) shows the corresponding results for `tcp`: the overheads are mostly $< 3\%$. We remark that the relative overheads will continue to diminish as latency increases, e.g., for TCP over LAN or the Internet.

Case study: Computer Language Benchmarks Game (CLBG). We next present benchmarks using existing applications from Debian's CLBG [Gouy 2017], a repository of programs used to compare the performance of different languages (e.g., [Brunthaler 2010; Shirako et al. 2009; St-Amour et al. 2012; Wrigstad et al. 2010]). We use three concurrent Go programs: **(a)** `k-nucleotide` counts occurrences of molecule sequences in a DNA string, **(b)** `regex-redux` matches regex patterns against a DNA string, and **(c)** `spectral-norm` computes the greatest eigenvalue of a matrix. All three are based on scatter/gather work parallelisation between goroutines using Go channels. We take the original programs, written by the Go Authors, as the **Go base cases**. For **Scribble-Go**, we specify the (previously implicit) application protocols using our extended Scribble, each parameterised on a number $1 \leq k \leq 12$ of "worker" goroutines; and modify the original programs by replacing all vanilla Go channels, sends and receives with `shm` state channels and calls to the generated APIs.

For these macrobenchmarks, we measure the execution time of the *whole* application (i.e., including channel creations, Scribble-Go Endpoint initiations, etc.). We use the standard inputs defined in the CLBG, and take the mean of 20 repetitions for each application. Fig. 14 (right) shows the execution time of the Go base cases relative to Scribble-Go: x ranges over k, and y is t_{go} / t_{api}.

The results show Scribble-Go performs at least as well as the original programs in most cases; we expect the cost of computations in real applications such as these will often render the overheads negligible, considering the absolute values measured in the microbenchmarks. Scribble-Go is actually faster in some cases for `regex-redux` and `k-nucleotide` (observed for different versions of our Runtime). We believe this is due to including channel creations in the time measurement, and a

		Pt	Sc	Ga	FE
Core I/O patterns	1. One-to-Many (§ 6.1)		●		○
	2. Many-to-One (§ 6.1)			●	○
	3. Many-to-Many (§ 6.1)		●	●	○

Above, ○ are possible alt. implementations

		Pt	Sc	Ga	FE	Pipe	MS	PP	Rec	Del
Parallel Topologies	4. Pipeline (§ 4)	●				●				
	5. Ring (§ 3; 4)	●			●	●		●	●	
	6. Hadamard (§ 4)	●			●					
	7. Mesh (§ 4)	●			●	●				
	8. Fork-Join		●	●						
Applications	9. Pget^2 (□ is the difference between the two versions in § 3.2; § 3.3)	●	●	●	□					●
	10. Vickrey auction (Supplement, § IV.1.2)	●	●	●	●		●		●	
	11. Jacobi solution of discrete Poisson equation. [Bejleri et al. 2009]	●	●	●	●		●		●	
	12. n-body simulation (based on Ring) [Bejleri et al. 2009]	●			●	●		●	●	
	13. Iterative linear equation solver (based on Mesh) [Ng and Yoshida 2015]	●	●		●	●	●		●	
	14. `k-nucleotide` [Gouy 2017] (§ 6.1)		●	●						
	15. `regex-redux` [Gouy 2017] (§ 6.1)		●	●						
	16. `spectral-norm` [Gouy 2017] (§ 6.1)		●	●			●		●	
	17. Fibonacci [Lange et al. 2017]	●			●					
	18. Quote-Request [Austin et al. 2004; Ng and Yoshida 2015]		●	●	●		●		●	
	19. P2P multiplayer game [Scalas et al. 2017]	●			●	●		●	●	●
	20. Web Crawler [Akhmadeev 2016; Neykova and Yoshida 2017]	●	●	●	●					
	21. n-buyers [Coppo et al. 2016; Honda et al. 2016]	●			●		●		●	

Pt: point-to-point; Sc: Scatter; Ga: Gather; FE: Foreach; Pipe: Pipeline; MS: MS choices; PP: PP choices; Rec: Recursion; Del: Delegation

Fig. 15. Role-parametric protocols for communication patterns, topologies and applications in Scribble-Go.

small restructuring of the program to use the generated API: the original programs create their goroutines and channels on the fly, whereas our adapted programs "pre-create" the goroutines and channels up front in a session initiation phase. In profiling, we find the actual computation code, which is the *same* in both versions, takes longer in the originals—one reason may be that the adapted versions run with better thread locality and fewer cache misses without such "interruptions" from goroutine spawning and channel creation.

6.2 Use Cases – Expressiveness and Applicability

We demonstrate the expressiveness and applicability of our framework by using our toolchain to specify and implement protocols for a range of role-parametric communication patterns, topologies and applications, listed in Table 15. The columns indicate the features of our extended Scribble used in the protocol. We cite the background and related works from where we draw the examples—in every case of parameterised session types literature, the parameterised aspect of the example was treated by either an *ad hoc* or *centralised* (non-distributed) method. The topologies in 4–8 are common in parallel algorithms. Due to space constraints, we explain the details of the examples in the Supplement,[4] § IV.1.

7 RELATED WORK

Parameterised MPST and implementations of session types. § 2.2 gave initial discussions of the closest related works on MPST for role-parametric protocols; we continue below.

Deniélou et al. [2012]; Yoshida et al. [2010] developed a role-parametric MPST using a dependent types approach. Unlike our work, the top-down *generic projection* in their theoretical-only work does not *infer* nor *decouple* role variants from the protocol; it simply encapsulates variant behaviours into a consolidated local type. To compensate, they combine with a *bottom-up* mechanism of taking endpoint decouplings from a pre-existing system of processes, and showing equivalence between the generic projection and target types; roughly speaking, however, for types that are "not syntactically close" (e.g., the generic projection of Ring and its role variants) the equivalence is often undecidable. In general, the programmers of individual endpoints in a modular development of some non-trivial multiparty application (e.g., not just binary RPCs) should commence development top-down from some notion of agreed protocol—otherwise the separate programmers cannot locally determine the (inherently stateful) I/O structure that their endpoint should implement.

Charalambides et al. [2016] extend MPST theory with parameterised versions of session type operators that represent repeat applications of the operator for some parameter value (possibly run-time instantiated). Unlike our work, their system does not support *role-parametric* protocols as their approach expressly requires prohibiting separate occurrences of a role with different indices; this rules out, e.g., role-parametric pipeline structures. Also, they did not implement their theory.

Regarding implementations and applications, Ng et al. [2015]; Ng and Yoshida [2015] use parameterised MPST [Deniélou et al. 2012] to generate an MPI backbone in C that encapsulates the *whole* protocol (i.e., every endpoint), and weaves (merges) it with user-supplied computation kernels. Their approach fundamentally produces complete, "centralised" programs, due to lacking notions of identifying and projecting role variants. By contrast, our toolchain generates typed APIs that allow the programmer to implement an individual endpoint more flexibly, i.e., not tied to a specific transport or messaging interface (MPI), nor a specific program structure.

López et al. [2015] develop a verification framework for MPI/C inspired by multiparty session types by translating parameterised protocol specifications to protocols in VCC [Cohen et al. 2009]. Their VCC verification is driven by program annotations, e.g., to match up individual control flow statements (e.g., `if-else`, `while`) to choices and loops in the specification, and pre/post conditions on recursive functions. Their approach is *purely global* (i.e., monolithic) from an MPST perspective: their specific aim is to verify a complete MPI program directly against a global protocol.

None of the remaining works in this paragraph support *parameterised* session types. Our API generation builds on the basic idea of Hu and Yoshida [2016] for Java, which our framework reformulates and extends for parameterised endpoints/families and nested FSMs in Go. Our API design leverages Go features that Java lacks (e.g., type switch, select); and is augmented in a range of ways, e.g., explicit error handling, nested struct types for peers/actions (which improves the IDE ergonomics of our APIs, while bypassing Go's lack of method overloading and reliance on singleton types), and promoting `End`-results to assist linearity. They did not evaluate run-time performance. Dynamic linearity checking is also employed in applications of session types in OCaml (Padovani [2017]) and Scala (Scalas et al. [2017]); our toolchain supports an alternative callback-based API generation that does not require dynamic checks. Gay et al. [2010] and Kouzapas et al. [2016] apply session types to object-oriented languages via *typestates* [Strom and Yemini 1986]. Unlike our API generation that targets programming in native Go, both are implemented as heavier-weight Java extensions with new syntax. (By contrast, the approach we use could possibly be described as *statetypes*.) As in our work and others above, these typestate approaches again rely on some form of cross-cutting linearity analysis.

Verification of message passing programs in Go. Our work aims to promote protocol compliance-by-construction in distributed programs through generation of types, to exploit lightweight error detection while programming and other support from IDEs and compile-time tools (e.g., "dot-driven" content assist and code auto-completion). Alternatively, the following are several recent works on *a posteriori* verification of message passing in existing Go programs. All of them employ *whole*-program techniques, and support only the built-in Go channel *primitives* (i.e., intra-process messaging); none of them, however, support channel-over-channel passing (§ 6.2).

Ng and Yoshida [2016] extract a graph-based protocol specification [Lange et al. 2015] from a Go program that is checked for deadlock-freedom; Stadtmüller et al. [2016] extract a regex-based protocol specification [Sulzmann and Thiemann 2016], checked for deadlock-freedom. Both approaches work only for programs restricted to *synchronous* Go channels; the former also requires all goroutines to be spawned before any communication among them occurs, and the latter has limited support for branching behaviours. Lange et al. [2017, 2018] statically infer channel communication patterns from a Go program as *behavioural types*, that are checked for liveness properties. The earlier work focuses on their analysis, a bounded symbolic method that does not scale well to large input models, and does not describe the inference procedure; it also does not take into account channel aliasing. The later work puts forward a concrete inference algorithm (for a restricted subset of Go) that considers channel aliasing. It checks the extracted types are restricted to finite control (not required in our work), which is required by a subsequent verification of the types by model checking; their model checker (mCRL2) also does not support channel passing, unlike our work (e.g., Pget). Their verification is best-effort only, due to the imprecision of the inference, and the verification times (and timeouts) preclude practical checking on the fly during programming.

The above works are the most related; we mention some further works in the Supplement[4] (§ V).

8 FUTURE WORK

We stated the conditions for concrete applications of our framework in § 2.1. We clarify further limitations relevant to our aims in this paper, and how they may be addressed in future work.

Dynamic participants. Our framework supports protocols where the (parameterised) participants are fixed on session initiation, as standard in MPST. We plan to integrate with explicitly (session-)typed *connection* actions [Hu and Yoshida 2017] for dynamic joining/leaving of parameterised participants during session execution; this would also eliminate some of the run-time connection checks at endpoint initiation (§ 5.3). To do so, we will extend our well-formedness based on the model checking approach of Hu and Yoshida [2017] for verifying MPST safety.

Failure handling. Our API generation is integrated with the explicit error handling paradigm of Go, where errors include node and networking failures. Our API design and safety guarantees currently consider the occurrence of such an error as a premature session termination (similar to linearity violations). We will investigate extending our framework to *fault-tolerant* protocols, e.g., for a session to continue between the remaining participants after one fails. We believe our formalism developed in this paper, that interprets our extensions in terms of a core base theory (§ 4), is well suited for such investigations: we may take one of the recent theoretical MPST works on link failures [Adameit et al. 2017] or crash failures [Viering et al. 2018] as a base theory.

Programming styles. This paper focuses on an API style that is close to channel-based programming using standard libraries and Go channels; our aim is to offer MPST-based programming through a familiar interface to Go users, and to facilitate the reimplementation of existing Go programs for our evaluation. The presented APIs promote a popular call-chaining programming style (cf. fluent APIs) that permits some flexibility between more "imperative" or more "functional" styles within the context of Go. We briefly illustrated our alternative callback-based API generation, that inherently precludes run-time linearity checks, but requires programming in an event-driven style—also a widely used style in practice. We plan to add further API generation styles, such as a "monadic" or CPS-based style that relies less on side effects for input methods (cf. Fig. 5, line 17). We note the *necessary* language features to implement (a basic version of) our approach are relatively modest support for static typing of data and functions/methods. We have leveraged additional Go specific features to produce better user APIs (e.g., type-switch and goroutines), but they are inessential. We believe our approach may be readily ported to other languages, given that we have demonstrated an implementation for Go whose type system is (by design) relatively bare.

Acknowledgements. We thank the anonymous reviewers and Simon Castellan for their feedback. This work is partially supported by EU COST Action IC1402 ARVI, EPSRC projects EP/K034413/1, EP/K011715/1, EP/L00058X/1, EP/N027833/1 and EP/N028201/1.

REFERENCES

Manuel Adameit, Kirstin Peters, and Uwe Nestmann. 2017. Session Types for Link Failures. In *Formal Techniques for Distributed Objects, Components, and Systems - 37th IFIP WG 6.1 International Conference, FORTE 2017, Held as Part of the 12th International Federated Conference on Distributed Computing Techniques, DisCoTec 2017, Neuchâtel, Switzerland, June 19-22, 2017, Proceedings (Lecture Notes in Computer Science)*, Vol. 10321. Springer, 1–16. https://doi.org/10.1007/978-3-319-60225-7_1

Foat Akhmadeev. 2016. Web Crawling With Akka. http://foat.me/articles/crawling-with-akka/.

Davide Ancona, Viviana Bono, Mario Bravetti, Joana Campos, Giuseppe Castagna, Pierre-Malo Deniélou, Simon J. Gay, Nils Gesbert, Elena Giachino, Raymond Hu, Einar Broch Johnsen, Francisco Martins, Viviana Mascardi, Fabrizio Montesi, Rumyana Neykova, Nicholas Ng, Luca Padovani, Vasco T. Vasconcelos, and Nobuko Yoshida. 2016. Behavioral Types in Programming Languages. *Foundations and Trends in Programming Languages* 3, 2-3 (2016), 95–230. https://doi.org/10.1561/2500000031

Daniel Austin, Abbie Barbir, Ed Peters, and Steve Ross-Talbot. 2004. Web Services Choreography Requirements. https://www.w3.org/TR/2004/WD-ws-chor-reqs-20040311/#UC-002.

Andi Bejleri, Raymond Hu, and Nobuko Yoshida. 2009. Session-Based Programming for Parallel Algorithms: Expressiveness and Performance. In *Proceedings Second International Workshop on Programming Language Approaches to Concurrency and Communication-cEntric Software, PLACES 2009, York, UK, 22nd March 2009. (EPTCS)*, Vol. 17. 17–29. https://doi.org/10.4204/EPTCS.17.2

Daniel Brand and Pitro Zafiropulo. 1983. On Communicating Finite-State Machines. *J. ACM* 30, 2 (1983), 323–342. https://doi.org/10.1145/322374.322380

Stefan Brunthaler. 2010. Inline Caching Meets Quickening. In *ECOOP 2010 - Object-Oriented Programming, 24th European Conference, Maribor, Slovenia, June 21-25, 2010. Proceedings (Lecture Notes in Computer Science)*, Theo D'Hondt (Ed.), Vol. 6183. Springer, 429–451. https://doi.org/10.1007/978-3-642-14107-2_21

Minas Charalambides, Peter Dinges, and Gul A. Agha. 2016. Parameterized, concurrent session types for asynchronous multi-actor interactions. *Sci. Comput. Program.* 115-116 (2016), 100–126. https://doi.org/10.1016/j.scico.2015.10.006

Ernie Cohen, Markus Dahlweid, Mark A. Hillebrand, Dirk Leinenbach, Michal Moskal, Thomas Santen, Wolfram Schulte, and Stephan Tobies. 2009. VCC: A Practical System for Verifying Concurrent C. In *Theorem Proving in Higher Order Logics, 22nd International Conference, TPHOLs 2009, Munich, Germany, August 17-20, 2009. Proceedings (Lecture Notes in Computer Science)*, Stefan Berghofer, Tobias Nipkow, Christian Urban, and Makarius Wenzel (Eds.), Vol. 5674. Springer, 23–42. https://doi.org/10.1007/978-3-642-03359-9_2

Mario Coppo, Mariangiola Dezani-Ciancaglini, Luca Padovani, and Nobuko Yoshida. 2015. A Gentle Introduction to Multiparty Asynchronous Session Types. In *15th International School on Formal Methods for the Design of Computer, Communication and Software Systems: Multicore Programming (LNCS)*, Vol. 9104. Springer, 146–178.

Mario Coppo, Mariangiola Dezani-Ciancaglini, Nobuko Yoshida, and Luca Padovani. 2016. Global progress for dynamically interleaved multiparty sessions. *Mathematical Structures in Computer Science* 26, 2 (2016), 238–302. https://doi.org/10.1017/S0960129514000188

Pierre-Malo Deniélou and Nobuko Yoshida. 2012. Multiparty Session Types Meet Communicating Automata. In *Programming Languages and Systems - 21st European Symposium on Programming, ESOP 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings (Lecture Notes in Computer Science)*, Helmut Seidl (Ed.), Vol. 7211. Springer, 194–213. https://doi.org/10.1007/978-3-642-28869-2_10

Pierre-Malo Deniélou and Nobuko Yoshida. 2013. Multiparty Compatibility in Communicating Automata: Characterisation and Synthesis of Global Session Types. In *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part II (Lecture Notes in Computer Science)*, Fedor V. Fomin, Rusins Freivalds, Marta Z. Kwiatkowska, and David Peleg (Eds.), Vol. 7966. Springer, 174–186. https://doi.org/10.1007/978-3-642-39212-2_18

Pierre-Malo Deniélou, Nobuko Yoshida, Andi Bejleri, and Raymond Hu. 2012. Parameterised Multiparty Session Types. *Logical Methods in Computer Science* 8, 4 (2012). https://doi.org/10.2168/LMCS-8(4:6)2012

Simon J. Gay, Vasco T. Vasconcelos, António Ravara, Nils Gesbert, and Alexandre Z. Caldeira. 2010. Modular Session Types for Distributed Object-oriented Programming. In *Proceedings of the 37th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '10)*. ACM, New York, NY, USA, 299–312. https://doi.org/10.1145/1706299.1706335

Issac Gouy. 2017. Computer Language Benchmark Game. http://benchmarksgame.alioth.debian.org.

Kohei Honda, Nobuko Yoshida, and Marco Carbone. 2016. Multiparty Asynchronous Session Types. *J. ACM* 63, 1 (2016), 9:1–9:67. https://doi.org/10.1145/2827695

Raymond Hu and Nobuko Yoshida. 2016. Hybrid Session Verification Through Endpoint API Generation. In *Fundamental Approaches to Software Engineering - 19th International Conference, FASE 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings (Lecture Notes in Computer Science)*, Perdita Stevens and Andrzej Wasowski (Eds.), Vol. 9633. Springer, 401–418. https://doi.org/10.1007/

978-3-662-49665-7_24

Raymond Hu and Nobuko Yoshida. 2017. Explicit Connection Actions in Multiparty Session Types. In *Fundamental Approaches to Software Engineering - 20th International Conference, FASE 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings (Lecture Notes in Computer Science)*, Marieke Huisman and Julia Rubin (Eds.), Vol. 10202. Springer, 116–133. https://doi.org/10.1007/978-3-662-54494-5_7

Hans Hüttel, Ivan Lanese, Vasco T. Vasconcelos, Luís Caires, Marco Carbone, Pierre-Malo Deniélou, Dimitris Mostrous, Luca Padovani, António Ravara, Emilio Tuosto, Hugo Torres Vieira, and Gianluigi Zavattaro. 2016. Foundations of Session Types and Behavioural Contracts. *ACM Comput. Surv.* 49, 1 (2016), 3:1–3:36. https://doi.org/10.1145/2873052

Dimitrios Kouzapas, Ornela Dardha, Roly Perera, and Simon J. Gay. 2016. Typechecking protocols with Mungo and StMungo. In *PPDP*. 146–159. https://doi.org/10.1145/2967973.2968595

Julien Lange, Nicholas Ng, Bernardo Toninho, and Nobuko Yoshida. 2017. Fencing off go: liveness and safety for channel-based programming. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017*, Giuseppe Castagna and Andrew D. Gordon (Eds.). ACM, 748–761. http://dl.acm.org/citation.cfm?id=3009847

Julien Lange, Nicholas Ng, Bernardo Toninho, and Nobuko Yoshida. 2018. A Static Verification Framework for Message Passing in Go using Behavioural Types. In *40th International Conference on Software Engineering*. ACM. To appear.

Julien Lange, Emilio Tuosto, and Nobuko Yoshida. 2015. From Communicating Machines to Graphical Choreographies. In *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2015, Mumbai, India, January 15-17, 2015*, Sriram K. Rajamani and David Walker (Eds.). ACM, 221–232. https://doi.org/10.1145/2676726.2676964

Hugo A. López, Eduardo R. B. Marques, Francisco Martins, Nicholas Ng, César Santos, Vasco Thudichum Vasconcelos, and Nobuko Yoshida. 2015. Protocol-based verification of message-passing parallel programs. In *Proceedings of the 2015 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications, OOPSLA 2015, part of SPLASH 2015, Pittsburgh, PA, USA, October 25-30, 2015*, Jonathan Aldrich and Patrick Eugster (Eds.). ACM, 280–298. https://doi.org/10.1145/2814270.2814302

Rumyana Neykova and Nobuko Yoshida. 2017. Let It Recover: Multiparty Protocol-Induced Recovery. In *26th International Conference on Compiler Construction*. ACM, 98–108.

Nicholas Ng, José Gabriel de Figueiredo Coutinho, and Nobuko Yoshida. 2015. Protocols by Default - Safe MPI Code Generation Based on Session Types. In *Compiler Construction - 24th International Conference, CC 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings (Lecture Notes in Computer Science)*, Björn Franke (Ed.), Vol. 9031. Springer, 212–232. https://doi.org/10.1007/978-3-662-46663-6_11

Nicholas Ng and Nobuko Yoshida. 2015. Pabble: parameterised Scribble. *Service Oriented Computing and Applications* 9, 3-4 (2015), 269–284. https://doi.org/10.1007/s11761-014-0172-8

Nicholas Ng and Nobuko Yoshida. 2016. Static deadlock detection for concurrent go by global session graph synthesis. In *Proceedings of the 25th International Conference on Compiler Construction, CC 2016, Barcelona, Spain, March 12-18, 2016*, Ayal Zaks and Manuel V. Hermenegildo (Eds.). ACM, 174–184. https://doi.org/10.1145/2892208.2892232

Luca Padovani. 2017. A simple library implementation of binary sessions. *J. Funct. Program.* 27 (2017), e4. https://doi.org/10.1017/S0956796816000289

Aseem Rastogi, Matthew A. Hammer, and Michael Hicks. 2014. Wysteria: A Programming Language for Generic, Mixed-Mode Multiparty Computations. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP '14)*. IEEE Computer Society, Washington, DC, USA, 655–670. https://doi.org/10.1109/SP.2014.48

Victor Samofalov, V. Krukov, B. Kuhn, S. Zheltov, Alexander V. Konovalov, and J. DeSouza. 2005. Automated Correctness Analysis of MPI Programs with Intel(r) Message Checker. In *Parallel Computing: Current & Future Issues of High-End Computing, Proceedings of the International Conference ParCo 2005, 13-16 September 2005, Department of Computer Architecture, University of Malaga, Spain (John von Neumann Institute for Computing Series)*, Vol. 33. Central Institute for Applied Mathematics, Jülich, Germany, 901–908.

Alceste Scalas, Ornela Dardha, Raymond Hu, and Nobuko Yoshida. 2017. A Linear Decomposition of Multiparty Sessions for Safe Distributed Programming. In *31st European Conference on Object-Oriented Programming, ECOOP 2017, June 19-23, 2017, Barcelona, Spain (LIPIcs)*, Peter Müller (Ed.), Vol. 74. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 24:1–24:31. https://doi.org/10.4230/LIPIcs.ECOOP.2017.24

Jun Shirako, David M. Peixotto, Vivek Sarkar, and William N. Scherer III. 2009. Phaser accumulators: A new reduction construct for dynamic parallelism. In *23rd IEEE International Symposium on Parallel and Distributed Processing, IPDPS 2009, Rome, Italy, May 23-29, 2009*. IEEE, 1–12. https://doi.org/10.1109/IPDPS.2009.5161071

Vincent St-Amour, Sam Tobin-Hochstadt, and Matthias Felleisen. 2012. Optimization coaching: optimizers learn to communicate with programmers. In *Proceedings of the 27th Annual ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications, OOPSLA 2012, part of SPLASH 2012, Tucson, AZ, USA, October 21-25, 2012*, Gary T. Leavens and Matthew B. Dwyer (Eds.). ACM, 163–178. https://doi.org/10.1145/2384616.2384629

Kai Stadtmüller, Martin Sulzmann, and Peter Thiemann. 2016. Static Trace-Based Deadlock Analysis for Synchronous Mini-Go. In *Programming Languages and Systems - 14th Asian Symposium, APLAS 2016, Hanoi, Vietnam, November 21-23, 2016, Proceedings (Lecture Notes in Computer Science)*, Atsushi Igarashi (Ed.), Vol. 10017. 116–136. https://doi.org/10.1007/978-3-319-47958-3_7

R E Strom and S Yemini. 1986. Typestate: A Programming Language Concept for Enhancing Software Reliability. *IEEE Trans. Softw. Eng.* 12, 1 (Jan. 1986), 157–171. https://doi.org/10.1109/TSE.1986.6312929

Martin Sulzmann and Peter Thiemann. 2016. Forkable Regular Expressions. In *Language and Automata Theory and Applications - 10th International Conference, LATA 2016, Prague, Czech Republic, March 14-18, 2016, Proceedings (Lecture Notes in Computer Science)*, Adrian-Horia Dediu, Jan Janousek, Carlos Martín-Vide, and Bianca Truthe (Eds.), Vol. 9618. Springer, 194–206. https://doi.org/10.1007/978-3-319-30000-9_15

Jesse A. Tov and Riccardo Pucella. 2011. Practical affine types. In *Proceedings of the 38th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2011, Austin, TX, USA, January 26-28, 2011*. ACM, 447–458. https://doi.org/10.1145/1926385.1926436

Malte Viering, Tzu-Chun Chen, Patrick Eugster, Raymond Hu, and Lukasz Ziarek. 2018. A Typing Discipline for Statically Verified Crash Failure Handling in Distributed Systems. In *Programming Languages and Systems - 27th European Symposium on Programming, ESOP 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings (Lecture Notes in Computer Science)*, Vol. 10801. Springer, 799–826. https://doi.org/10.1007/978-3-319-89884-1_28

Tobias Wrigstad, Francesco Zappa Nardelli, Sylvain Lebresne, Johan Östlund, and Jan Vitek. 2010. Integrating typed and untyped code in a scripting language. In *Proceedings of the 37th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2010, Madrid, Spain, January 17-23, 2010*, Manuel V. Hermenegildo and Jens Palsberg (Eds.). ACM, 377–388. https://doi.org/10.1145/1706299.1706343

Nobuko Yoshida, Pierre-Malo Deniélou, Andi Bejleri, and Raymond Hu. 2010. Parameterised Multiparty Session Types. In *Foundations of Software Science and Computational Structures, 13th International Conference, FOSSACS 2010, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2010, Paphos, Cyprus, March 20-28, 2010. Proceedings (Lecture Notes in Computer Science)*, Vol. 6014. Springer, 128–145. https://doi.org/10.1007/978-3-642-12032-9_10

Supplement

This supplement contains **additional discussions and examples**, **omitted definitions** and **full proofs** of the results.

A note on section and figure numbering: references within this supplement are prefixed by the part number, while references without a part number prefix refer to the main paper. E.g., §I.1 refers to the section in this supplement, while §3 refers to the section in the main paper.

Contents

Part I
[§3] Methodology Overview

I.1 [§3.2] Pget – Distributed, Role-Parametric MPST for Go: Overall Methodology

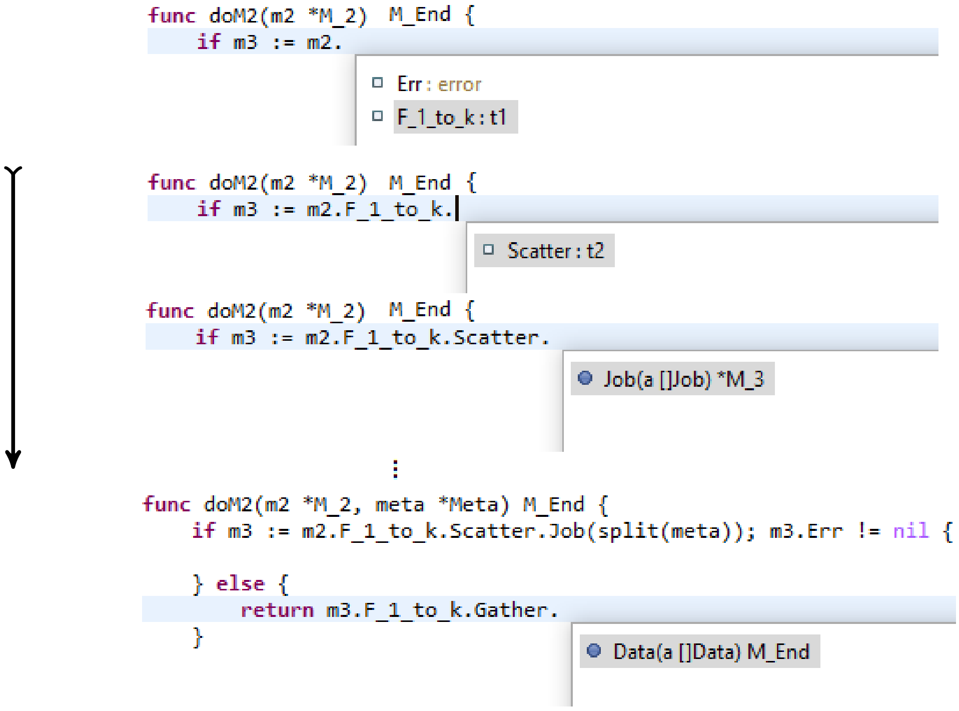
I.1.1 API Types Generation for API Style of §3

Following is an extract from the Go types and I/O method signatures belonging to API generated for `M` in Pget, as used in the example code in §3.2.

```
// Variant- and state-specific type wrappers for channel(s)
type M_2 struct { Err error; id uint64; F_1toK t1; ... }
// t1..4 internal API types (not directly exposed to user)
type t1 struct { Scatter t2; ... }
type t2 struct { ... }
func (s *t2) Job(a []Job) *M_3 { ... /* Scatter a[i] to F */ }
type M_3 struct { Err error; id uint64; F_1toK t3; ... }
type t3 struct { Gather t4; ... }
type t4 struct { ... }
func (s *t4) Data(a []Data) *M_End { ... /* Gather from each Fi into a[i] */ }
```

I.1.2 Ergonomics of our Generated APIs

Below are screen shots of programming `M` in Pget in an IDE (GoClipse Eclipse) using the generated API types and methods listed above. Our toolchain could be directly integrated as an IDE plugin.



```
func doM2(m2 *M_2)  M_End {
    if m3 := m2.
```

```
func doM2(m2 *M_2)  M_End {
    if m3 := m2.F_1_to_k.
```

```
func doM2(m2 *M_2)  M_End {
    if m3 := m2.F_1_to_k.Scatter.
```

⋮

```
func doM2(m2 *M_2, meta *Meta) M_End {
    if m3 := m2.F_1_to_k.Scatter.Job(split(meta)); m3.Err != nil {

    } else {
        return m3.F_1_to_k.Gather.
    }
```

I.1.3 Example Endpoint Program for $\mathtt{F}_1$ in Pget

Following is an example implementation of $\mathtt{F}_1$; we do not explicitly list the generated API types, but this code can be directly compared its the source CFSM.

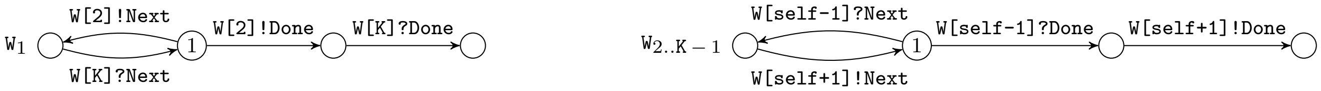
```
 1 // Implementation of B (i.e., F) in Sync
 2 func runB(b *B_1) End_B { ... }
 3
 4 func mainF1(req HttpReq, portM int) {
 5   proto := Pget.New()
 6   F1 := proto.F_1.New() // F_1 API same for K>=1
 7   F1.M.Dial(shm.Client, "localhost", portM)
 8   F1.S.Dial(tcp.Client, req.Host, req.Port)
 9   F1.run(runF1)
10 }
11
12 func runF1(f *F_1_1) End_F_1 {
13   var res Res; var job Job;
14   f_deleg := f.
15       S.Send    .Head(req.Head()).   // S!Head.
16       S.Receive .Res(&res).          // S?Res.
17       M.Send    .Meta(res.Meta()).   // M!Meta.
18       M.Receive .Job(&job).          // M?Job.
19       S.Send    .Get(Get.New(&job)). // S!Get.
20       S.Receive .Res(&res).          // S?Res.
21       M.Send    .Data(res.Data())    // M!Data.
22   proto := Sync.New()
23   a := proto.Shm.A.New(runB) // Spawns B goroutine
24   return f_deleg.M.Send.Sync_A(a) // M!Sync@A.end
25 }
```

The Endpoint `F1` is used to connect (`Dial`) to `M` and `S` on shared memory and TCP transports, respectively. Then in `runF1`, the programmer can rely on the state channel API to guide the way through the multiparty protocol as a whole, correctly dispatching the interleaved I/O operations with `M` and `S` on the corresponding underlying channels. On line 23, we use an API convenience facility for establishing shared memory sessions: the `New` constructs an `A` endpoint of a new session for the `Sync` protocol, while spawning a goroutine for the implementation function supplied for each of the other endpoints (i.e., `B`); `shm` channels are implicitly created between each endpoint. Line 24 *delegates* the state channel `a` to `M`, satisfying the local type action `M!Sync@A` and resulting in the generated `End` type.

I.2 Ring – Extended with Protocol Branching and Recursion

Global protocol Fig. I.2.1 (top) gives a version of Ring (cf. G_{Ring} in §2.2) elaborated with protocol *branching* and *recursion*. The annotation `@K>1` specifies an additional domain constraint on `K`. The `choice` construct specifies a branch point in the protocol where the *choice subject* `W[1]` makes an *internal choice* about which case the protocol should follow (the specification abstracts from the exact decision procedure); the decision result is then communicated as an *external choice* to the other participants via explicit messages. The syntax `Next pipe W[1,K];` describes a *pipeline* communication structure along the specified intervals: `W[1] to W[2]`, `W[2] to W[3]`, etc. The `do`-statement in the `Next` case is a recursive protocol definition: the protocol allows zero or more cycles of `Next` messages around the ring, followed by one cycle of `Done` messages.

```
global protocol Ring(role W) @K>1 {
  choice at W[1] { Next pipe W[1,K]; Next from W[K] to W[1]; do Ring(W); }
              or { Done pipe W[1,K]; Done from W[K] to W[1]; } }
```



State type			Method name, signature	
State	Peer	I/O	Label, value	Successor
W_1_1	W_2	Send	Next(a *Next)	*W_1_2
			Done(a *Done)	*W_1_3
W_1_2	W_K	Receive	Next(a *Next)	*W_1_1
W_1_3	W_K	Receive	Done(a *Done)	End

State type		Method name, signature	
State	Peer	I/O	Successor
W_2toK_1	W_self_sub1	Branch()	(*W_2toK_1_Next, *W_2toK_1_Done, error)
W_2toK_1_Next	n/a	Case(a *Next)	<-chan W_2toK_2
W_2toK_1_Done	n/a	Case(a *Done)	<-chan W_2toK_3

State type			Method name, signature	
State	Peer	I/O	Label, value	Successor
W_2toK_2	W_self_plus1	Send	Next(a *Next)	*W_2toK_1
W_2toK_3	W_self_plus1	Send	Done(a *Done)	End

```
// Pre: K>2, 2<=self<K (self = local endpoint ID)
func mainW_2toKsub1(left ScribTcpListener,
    K, self, right int) {
  defer left.close()
  proto := Ring.New()
  mid := proto.W_2toKsub1.New(K, self)
  mid.W_self_sub1.Accept(left)
  mid.W_self_plus1.Dial(tcp.Client, "host", right)
  mid.run(midman)
}

func midman(w *W_2toKsub1_1) End {
  var n Next; var d Done
  for { // Continuous loop (until return)
    next, done, _ := w.W_self_sub1.Branch()
    select { // Select between input on next/done
    case succ := <-next.Case(&n):
      w = succ.W_self_plus1.Send.Next(&n)
    case succ := <-done.Case(&d):
      return succ.W_self_plus1.Send.Done(&d)
    }
} }
```

Fig. I.2.1. A version of Ring (cf. G_{Ring} in §2.2) extended with branching and recursion: (top) global protocol; (center) projections onto variants $\mathtt{W}_1$ and $\mathtt{W}_{2..\mathtt{K}-1}$ as CFSMs; (bottom-left) their generated API types and I/O methods; (bottom-right) distributed (TCP) implementation of $\mathtt{W}_{2..\mathtt{K}-1}$ "middleman" variant (i.e., $\mathtt{K} > 2$).

Projection As for the earlier, simpler version of Ring, the toolchain infers this protocol definition induces *two* endpoint families: one involving only variants $\mathtt{W}_1$ and $\mathtt{W}_\mathtt{K}$, and the other additionally involving $\mathtt{W}_{2..\mathtt{K}-1}$. Fig. I.2.1 (centre) depicts the projections onto $\mathtt{W}_1$ and $\mathtt{W}_{2..\mathtt{K}-1}$. The keyword self stands for the run-time value of the local endpoint ID (1..K). As in standard MPST: (i) the characteristics of our role-parametric global types ensures that every (non-terminal) state of an endpoint is either output-only or input-only; and (ii) recursion is restricted to tail recursion (FSM cycles).

API types generation State channel API generation for output choices is a straightforward enumeration of each case as an output method (e.g., Send). State channel linearity implies exactly one case must be selected. E.g., the $\mathtt{W}_1$ API includes the W_1_x types in Fig. I.2.1 (bottom left). Recursion manifests as mutual references between the receiver and result types of the I/O methods.

For non-unary input choices, our implementation supports two styles of API generation, targetting different Go features. Fig. I.2.1 (bottom right) illustrates the API generation that targets the Go *select* statement (for the initial state of $\mathtt{W}_{2..\mathtt{K}}$). A select statement first evaluates the operands of channel operations of every case, and then chooses a single case when one or more can proceed.

The generated Branch method returns a set of *case values*, one for each case. Case values offer a single Case method that takes a pointer for the expected message, and returns a Go channel that produces the successor state channel if that case is enacted (e.g., type <-chan W_2toK_2 means a channel for *receiving* W_2toK_2). Like state channels, case values are linear objects, implying each one should be used exactly once in the `select`. §5.3 explains our other Branch API style that targets *type switch* statements.

Endpoint programming Fig. I.2.1 (bottom-right) gives an implementation of $\mathtt{W}_{2..\mathtt{K}-1}$ that connects to its neighbours via TCP. An invalid `self` value (i.e., endpoint identifier) in the endpoint constructor causes a run-time error. In the `midman` function, the `select` discerns the case received from `W[self-1]` and assigns the according type to `succ`.

For the other two variants, the API family would be selected by the programmer: the API will statically constrain whether or not connections to the middleman are allowed, supported by the run-time check that the value of `K` is compatible with the selected API.

Part II
[§4] Theory

II.1 [§4.1] Conditions on Rank Structures

We motivate the need for the conditions on rank structures as follows:

- **$\langle \mathbb{A}, \preceq \rangle$ is a partially ordered set**

  We use $\preceq$ to define the set of ranks that are contained in interval $E_1 \mathinner{..} E_2$, i.e., the formal *interpretation* of $E_1 \mathinner{..} E_2$ is the set $\{a \mid [\![E_1]\!] \preceq a \preceq [\![E_2]\!]\}$, where $[\![E_1]\!]$ and $[\![E_2]\!]$ denote the evaluations of E_1 and E_2. The reason $\preceq$ is partial is that it offers more flexibility; our main motivating example for this is the 2d-integers (Example 4.2).

  If $\preceq$ were total, we would not have been able to instantiate it with the product order on pairs of integers (as in Example 4.2), but only with some linear extension of that product order, such as the lexicographic order. As a result, interval `(1,1)..(2,2)` would consist of not only `(1,1)`, `(1,2)`, `(2,1)`, and `(2,2)` (as intended, e.g., in mesh protocols), but also `(1,3)`, `(1,4)`, `(1,5)` and infinitely many others. By allowing $\preceq$ to be partial (i.e., product order is fine), we overcome this problem.

- **$\langle \mathbb{A}, < \rangle$ is a strictly totally ordered set**

  While we use $\preceq$ to *select* the ranks in an interval $E_1 \mathinner{..} E_2$, we use $<$ to *sort* the ranks in the selection, so they can be iterated over. This order must be total to ensure the semantics of our parameterised global and local types is deterministic (just as global and local types in the original MPST). It may be possible to incorporate nondeterminism in our approach as well (by interpreting parameterised global and local types as *sets of* original global and local types, instead of as individual ones), but we have not explored this yet. We also note that $<$ does not have to be a linear extension of $\preceq$: after selection has occurred using $\preceq$, any total order on the resulting selection is fine.

- **$\langle \mathbb{A}, +, 0 \rangle$ is a torsion-free abelian group** and **+ preserves $\preceq$ and $<$**

  To explain the significance of these two requirements, we first need to introduce two auxiliary concepts: the *gradient* of an interval and the *distance* between two intervals.

  The gradient of an interval $E_1 \mathinner{..} E_2$ is defined as the rank $\nabla = E_1 - E_2$. For instance, with the integers, $\nabla + 1$ coincides exactly with the number of elements in the interval ("+1" because our intervals are inclusive at both ends), i.e., the *length* of the interval. We use gradients to reason about well-formedness (§4.5), and specifically, to check non-emptiness of closed intervals, and to check that "all intervals in the same iteration domain [...] have the same length". For the former check, we require that + preserves $\preceq$, and we require the existence of an identity element 0 in $\mathbb{A}$ such that a closed interval is empty iff its gradient equals 0. To define the gradient using $-$ (as we showed above), moreover, we need inverse elements of +.

  The distance between intervals D_1 and D_2 is defined as the rank Δ such that adding Δ to every rank in D_1 yields D_2; if such a Δ does not exist, the distance is undefined. We use distances to reason about "offsets" in the projection operator. For instance, in the Pipeline protocol, the projection operator needs to do some calculations with the intervals in the global type (Fig. 8) to determine that in the local type for the middle Worker, such a Worker first receives from `self-1` and then sends to `self+1` (i.e., the distance between intervals `1..k-1` and `2..k` is `-1` in one direction, and `1` in the other). Moreover, the projection operator is undefined if the distance between two intervals (in the same iteration domain) is the identity rank 0, because this could lead to self-communications (which are traditionally forbidden in MPST). To prove that these calculations performed by our projection operator are correct, we use associativity of +, commutativity of +, and torsion-freeness, but we speculate that some (or all) of these requirements may in principle be superfluous: we assume them because they made an already complicated proof somewhat easier, and because they are reasonable and unrestrictive (i.e., practically useful domains satisfy these requirements, including the $n{\geq}1$-dimensional integers).

- **first-order formulas over $\langle \mathbb{A}, +, 0, \preceq \rangle$ are decidable**

  This condition is necessary to ensure that inference of role variants and checking of well-formedness are decidable. Specifically, note that the formulas that are constructed in the proofs of Thms. 4.10 and 4.11 are first-order formulas over $\langle \mathbb{A}, +, 0, \preceq \rangle$.

- **the set of ranks between a_1 and a_2 under $\preceq$ is finite and enumerable**

  This conditions ensures that the body of every **`foreach`** is repeated only a finite number of times, and that the intervals (i.e., iterations) can actually be computed.

II.2 [§4.2] Examples of Local Types

Example II.2.1 (Pget)**.** The Pget protocol, as specified in Example 4.3 (main paper), consists of three roles: `M`, `F`, and `S`. As `M` is enacted by only one individual, `M` has only one variant; this variant is specified by one local type. The same holds for `S`. In contrast, `F` has two variants; accordingly, each of these variants is specified by a different local type.

$L^{\texttt{M}}_{\text{Pget}} = \texttt{F[1]}\,\texttt{?}\,\texttt{Size}\,.\,\textbf{foreach}\ \texttt{F\{i:1..k\}}\ \textbf{do}\ (\texttt{F[i]}\,\texttt{!}\,\texttt{Range}\,.\,\textbf{cont})\,\textbf{;}\ \ldots$

$L^{\texttt{F[1]}}_{\text{Pget}} = \texttt{S}\,\texttt{!}\,\texttt{Head}\,.\,\texttt{S}\,\texttt{?}\,\texttt{Res}\,.\,\texttt{M}\,\texttt{!}\,\texttt{Size}\,.\,\texttt{M}\,\texttt{?}\,\texttt{Range}\,.\,\ldots$

$L^{\texttt{F[2..k]}}_{\text{Pget}} = \texttt{M}\,\texttt{?}\,\texttt{Range}\,.\,\ldots$

$L^{\texttt{S}}_{\text{Pget}} = \texttt{F[1]}\,\texttt{?}\,\texttt{Head}\,.\,\texttt{F[1]}\,\texttt{!}\,\texttt{Res}\,.\,\ldots$

Example II.2.2 (Ring)**.** The Ring protocol, as specified in Example 4.4 (main paper), consists of one role, `W`, which has three variants: one for the front Worker, one for the middle Workers, and one for the back Worker.

$L^{\texttt{W[1]}}_{\text{Ring}} = \textbf{rec}\ \texttt{X}\ (\texttt{W[2]}\,\texttt{!}\{\texttt{Next}\,.\,\texttt{W[k]}\,\texttt{?}\,\texttt{Next}\,.\,\texttt{X},\ \texttt{Done}\,.\,\texttt{W[k]}\,\texttt{?}\,\texttt{Done}\,.\,\textbf{end}\})$

$L^{\texttt{W[2..k-1]}}_{\text{Ring}} = \textbf{rec}\ \texttt{X}\ (\texttt{W[}\textbf{self}\texttt{-1]}\,\texttt{?}\{\texttt{Next}\,.\,\texttt{W[}\textbf{self}\texttt{+1]}\,\texttt{!}\,\texttt{Next}\,.\,\texttt{X},\ \texttt{Done}\,.\,\texttt{W[}\textbf{self}\texttt{+1]}\,\texttt{!}\,\texttt{Done}\,.\,\textbf{end}\})$

$L^{\texttt{W[k]}}_{\text{Ring}} = \textbf{rec}\ \texttt{X}\ (\texttt{W[k-1]}\,\texttt{?}\{\texttt{Next}\,.\,\texttt{W[1]}\,\texttt{!}\,\texttt{Next}\,.\,\texttt{X},\ \texttt{Done}\,.\,\texttt{W[1]}\,\texttt{!}\,\texttt{Done}\,.\,\textbf{end}\})$

Example II.2.3 (Fibonacci)**.** The Fibonacci protocol, as specified in Example 4.5 (main paper), has one role, `Fib`, which has five variants: one for the first Fibonacci number, one for the second, one for the penultimate, one for the last, and one for all the others.

$L^{\texttt{Fib[1]}}_{\text{Fib}} = \texttt{Fib[3]}\,\texttt{!}\,\texttt{Val}\,.\,\textbf{end}$

$L^{\texttt{Fib[2]}}_{\text{Fib}} = \texttt{Fib[3]}\,\texttt{!}\,\texttt{Val}\,.\,\texttt{Fib[4]}\,\texttt{!}\,\texttt{Val}\,.\,\textbf{end}$

$L^{\texttt{Fib[3..k-2]}}_{\text{Fib}} = \texttt{Fib[}\textbf{self}\texttt{-2]}\,\texttt{?}\,\texttt{Val}\,.\,\texttt{Fib[}\textbf{self}\texttt{-1]}\,\texttt{?}\,\texttt{Val}\,.\,\texttt{Fib[}\textbf{self}\texttt{+1]}\,\texttt{!}\,\texttt{Val}\,.\,\texttt{Fib[}\textbf{self}\texttt{+2]}\,\texttt{!}\,\texttt{Val}\,.\,\textbf{end}$

$L^{\texttt{Fib[k-1]}}_{\text{Fib}} = \texttt{Fib[k-3]}\,\texttt{?}\,\texttt{Val}\,.\,\texttt{Fib[k-2]}\,\texttt{?}\,\texttt{Val}\,.\,\texttt{Fib[k]}\,\texttt{!}\,\texttt{Val}\,.\,\textbf{end}$

$L^{\texttt{Fib[k]}}_{\text{Fib}} = \texttt{Fib[k-2]}\,\texttt{?}\,\texttt{Val}\,.\,\texttt{Fib[k-1]}\,\texttt{?}\,\texttt{Val}\,.\,\textbf{end}$

Example II.2.4 (Hadamard)**.** The Hadamard protocol, as specified in Example 4.6 (main paper), has three roles, `A`, `B`, and `C`, each of which has one variant.

$$\begin{aligned}
L^{\texttt{A}}_{\text{Had}} &= \texttt{C}[\textbf{self}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\textbf{end}\\
L^{\texttt{B}}_{\text{Had}} &= \texttt{C}[\textbf{self}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\textbf{end}\\
L^{\texttt{C}}_{\text{Had}} &= \texttt{A}[\textbf{self}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\,\texttt{B}[\textbf{self}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\,\textbf{end}
\end{aligned}$$

Example II.2.5 (Mesh)**.** The wraparound mesh protocol, as specified in Example 4.7 (main paper), has one role, `W`, which has five variants.

$$\begin{aligned}
L^{\texttt{W}[\texttt{k}_{11}]}_{\text{Mesh}} &= \texttt{W}[\texttt{k}_{11}\texttt{+(1,0)}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\texttt{W}[\texttt{k}_{\text{w1}}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\\
&\ \texttt{W}[\texttt{k}_{11}\texttt{+(0,1)}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\texttt{W}[\texttt{k}_{\text{1h}}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\,\textbf{end}\\
L^{\texttt{W}[\texttt{k}_{11}\texttt{+(0,1)..}\texttt{k}_{\text{1h}}\texttt{-(0,1)}]}_{\text{Mesh}} &= \texttt{W}[\textbf{self}\texttt{+(1,0)}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\texttt{W}[\textbf{self}\texttt{+}\texttt{k}_{\text{w1}}\texttt{-}\texttt{k}_{11}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\\
&\ \texttt{W}[\textbf{self}\texttt{-(0,1)}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\,\texttt{W}[\textbf{self}\texttt{+(0,1)}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\textbf{end}\\
L^{\texttt{W}[\texttt{k}_{\text{1h}}]}_{\text{Mesh}} &= \texttt{W}[\texttt{k}_{\text{1h}}\texttt{+(1,0)}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\texttt{W}[\texttt{k}_{\text{wh}}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\\
&\ \texttt{W}[\texttt{k}_{\text{1h}}\texttt{-(0,1)}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\,\texttt{W}[\texttt{k}_{11}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\textbf{end}\\
L^{\texttt{W}[\texttt{k}_{11}\texttt{+(1,0)..}\texttt{k}_{\text{wh}}\texttt{-(1,0)}]}_{\text{Mesh}} &= \texttt{W}[\textbf{self}\texttt{-(1,0)}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\,\texttt{W}[\textbf{self}\texttt{+(1,0)}]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\textbf{end}\\
L^{\texttt{W}[\texttt{k}_{\text{w1}}\texttt{..}\texttt{k}_{\text{wh}}]}_{\text{Mesh}} &= \texttt{W}[\textbf{self}\texttt{-(1,0)}]\,\textbf{?}\,\texttt{Val}\,\textbf{.}\,\texttt{W}[\textbf{self}\texttt{-}(\texttt{k}_{\text{w1}}\texttt{-}\texttt{k}_{11})]\,\textbf{!}\,\texttt{Val}\,\textbf{.}\,\textbf{end}
\end{aligned}$$

II.3 [§4.4] Projection

The full definition of projection appears in Part VII, Section VII.8.2, Figure VII.8.2 (page 46), as part of the collection of all definitions, lemmas, and theorems in our theory.

II.4 [§4.5] Proof of Thm. 4.12

We recall the following from the main paper. Projection is correct if it satisfies the following equation, for all well-formed G and σ such that $G\,\langle\!\langle\sigma\rangle\!\rangle$ is well-closed:

$$G\,\langle\!\langle\sigma\rangle\!\rangle \equiv \{(G \restriction r[\mathcal{D},\bar{\mathcal{D}}])\,\langle\!\langle\tau\rangle\!\rangle \mid \mathcal{D} \uplus \bar{\mathcal{D}} = \mathsf{ivals}(r, G),\ \tau = \sigma \cup \{\textbf{self} \mapsto a\},\ \models \varphi(\mathcal{D}\,\langle\!\langle\tau\rangle\!\rangle, \bar{\mathcal{D}}\,\langle\!\langle\tau\rangle\!\rangle)\}$$

To prove correctness, our general strategy is as follows. We first prove correctness for well-formed global types *without* parameters. In this restricted case, the correctness equation becomes:

$$G \equiv \{(G \restriction r[\mathcal{D},\bar{\mathcal{D}}])\,\langle\!\langle\tau\rangle\!\rangle \mid \mathcal{D} \uplus \bar{\mathcal{D}} = \mathsf{ivals}(r, G),\ \tau = \{\textbf{self} \mapsto a\},\ \models \varphi(\mathcal{D}\,\langle\!\langle\tau\rangle\!\rangle, \bar{\mathcal{D}}\,\langle\!\langle\tau\rangle\!\rangle)\}$$

First, we define the semantics of global types and sets of local types, by interpreting every global/local type T in our theory as a global/local type $[\![T]\!]$ in the original theory of MPST (i.e., without **foreach**), for which reduction semantics have been defined [DY13]. Essentially, $[\![\cdot]\!]$ unrolls all loops, which is possible because the restricted case has no parameters (i.e., all intervals can be evaluated to concrete values), and because iteration domains are finite. Next, we prove that if $\mathcal{D} \uplus \bar{\mathcal{D}} = \mathsf{ivals}(r, G)$, $\tau = \{\textbf{self} \mapsto a\}$, and $\models \varphi(\mathcal{D}\,\langle\!\langle\tau\rangle\!\rangle, \bar{\mathcal{D}}\,\langle\!\langle\tau\rangle\!\rangle)$, **projection and interpretation commute**: $[\![(G \restriction r[\mathcal{D},\bar{\mathcal{D}}])\,\langle\!\langle\{\textbf{self} \mapsto a\}\rangle\!\rangle]\!] = [\![G]\!] \restriction_{\text{orig}} r[a]$, where $\restriction_{\text{orig}}$ denotes the projection operator in the original theory. Finally, we leverage a result in the original theory of MPST, stating that $\restriction_{\text{orig}}$ is

$$\begin{tikzcd}
\mathbb{G} \arrow[r, "\langle\!\langle\cdot\rangle\!\rangle"] \arrow[d, "\restriction"'] \arrow[dr, phantom, "\circlearrowright"] & \mathbb{G}_{\mathrm{restr}} \arrow[r, "{[\![\cdot]\!]}"] \arrow[d, "\restriction"'] \arrow[dr, phantom, "\circlearrowright"] & \mathbb{G}_{\mathrm{orig}} \arrow[d, "\restriction_{\mathrm{orig}}"] \\
\mathbb{L} \arrow[r, "\langle\!\langle\cdot\rangle\!\rangle"] & \mathbb{L}_{\mathrm{restr}} \arrow[r, "{[\![\cdot]\!]}"] & \mathbb{L}_{\mathrm{orig}}
\end{tikzcd}$$

Fig. II.4.1. Proof strategy

correct,[1] under trace equivalence. Trace equivalence is sufficient, as global types and sets of local types represent closed systems. Thus:

$$
\begin{aligned}
&[\![G]\!] \equiv_{\mathrm{orig}} \{[\![G]\!] \restriction_{\mathrm{orig}} r[a] \mid r[a] \in [\![G]\!]\} \Longrightarrow Tr[\![G]\!] = Tr\{[\![G]\!] \restriction_{\mathrm{orig}} r[a] \mid r[a] \in [\![G]\!]\} \\
\Longrightarrow\ & Tr[\![G]\!] = Tr\{[\![(G \restriction r[\mathcal{D}, \bar{\mathcal{D}}])\, \langle\!\langle \tau \rangle\!\rangle]\!] \mid \mathcal{D} \uplus \bar{\mathcal{D}} = \mathsf{ivals}(r, G),\ \tau = \{\texttt{\textbf{self}} \mapsto a\},\ \models \varphi(\mathcal{D}\, \langle\!\langle \tau \rangle\!\rangle, \bar{\mathcal{D}}\, \langle\!\langle \tau \rangle\!\rangle)\} \\
\Longrightarrow\ & G \equiv \{(G \restriction r[\mathcal{D}, \bar{\mathcal{D}}])\, \langle\!\langle \tau \rangle\!\rangle \mid \mathcal{D} \uplus \bar{\mathcal{D}} = \mathsf{ivals}(r, G),\ \tau = \{\texttt{\textbf{self}} \mapsto a\},\ \models \varphi(\mathcal{D}\, \langle\!\langle \tau \rangle\!\rangle, \bar{\mathcal{D}}\, \langle\!\langle \tau \rangle\!\rangle)\}
\end{aligned}
$$

To extend our proof to the general case, it is enough to show that **projection and instantiation commute**: $(G \restriction r[\mathcal{D}, \bar{\mathcal{D}}])\, \langle\!\langle \sigma \rangle\!\rangle = (G\, \langle\!\langle \sigma \rangle\!\rangle \restriction r[\mathcal{D}\, \langle\!\langle \sigma \rangle\!\rangle, \bar{\mathcal{D}}\, \langle\!\langle \sigma \rangle\!\rangle])$.

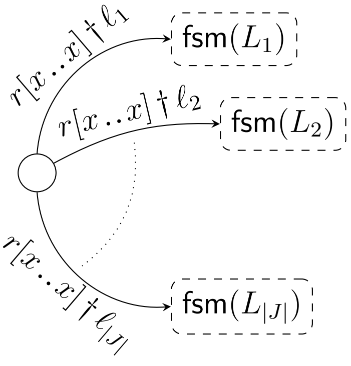
The crucial, non-trivial steps of our proof rely on the bold-emphasised properties above: commutativity of projection and interpretation, and commutativity projection and instantiation; this proof strategy is visualised in Figure II.4.1 (a more detailed version of this figure appears in Section VII.8.2). The full definitions, auxiliary lemmas, and theorems appear separately in Part VII; detailed proofs of these results appear separately in Part VIII.

Part III
[§5] Implementation

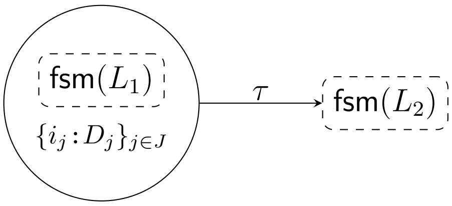
III.1 [§5.2] Communicating FSM Based Representation of Local Types

From local types to communicating FSMs. Let fsm denote a function from local types to FSMs. The following equations inductively define fsm for core local types in terms of a graphical notation for FSMs. Circles represent states; arrows represent transitions (labelled with scatter/gather I/O actions, or silent action τ); dashed rectangles represent FSMs and serve either as *continuation FSMs* or as *nested FSMs* inside states; labels below states indicate state identifiers (identifiers of states without labels do not matter and are freshly generated by need). Let $\dagger \in \{!, ?\}$.

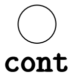
$\mathsf{fsm}(r[x] \dagger \{\ell_j \,\mathbf{.}\, L_j\}_{j\in J})$ =


$r[x\,..\,x] \dagger \ell_1$
$\mathsf{fsm}(L_1)$
$r[x\,..\,x] \dagger \ell_2$
$\mathsf{fsm}(L_2)$
$r[x\,..\,x] \dagger \ell_{|J|}$
$\mathsf{fsm}(L_{|J|})$

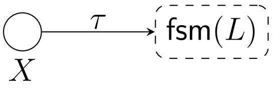
$\mathsf{fsm}(\mathbf{foreach}\ R\{i_j : D_j\}_{j\in J}\ \mathbf{do}\ L_1\ \mathbf{;}\ L_2)$ =



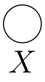
$\mathsf{fsm}(\mathbf{cont})$ =



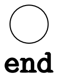
$\mathsf{fsm}(\mathbf{rec}\ X\ L)$ =



$\mathsf{fsm}(X)$ =

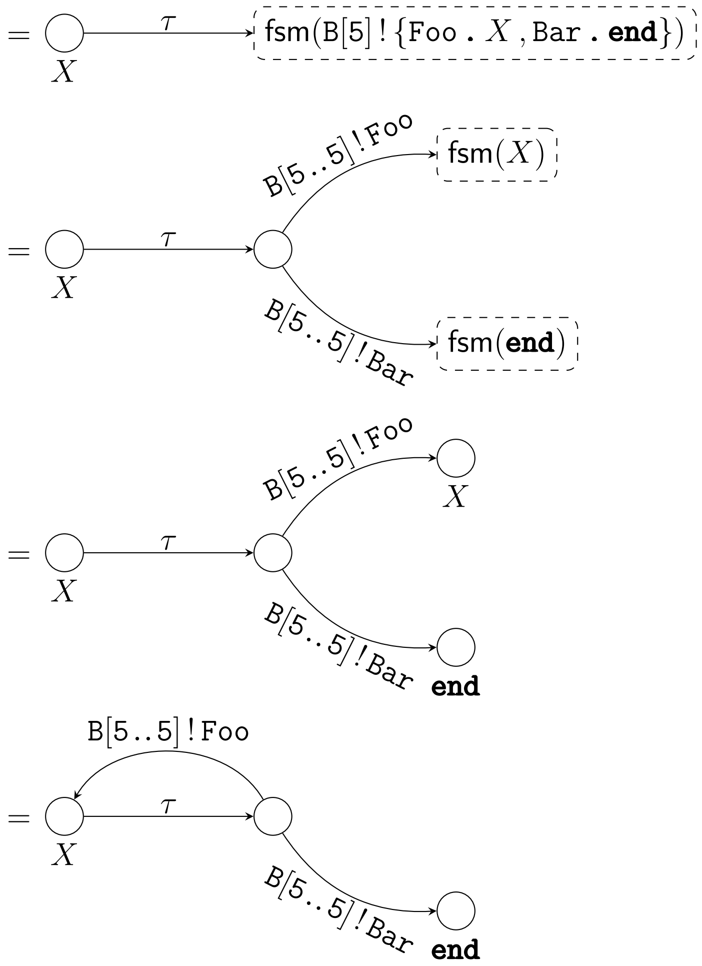


$\mathsf{fsm}(\mathbf{end})$ =



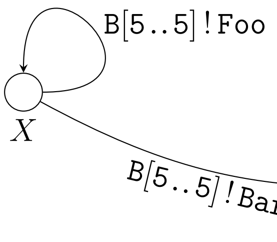
For instance:

$\mathsf{fsm}(\mathbf{rec}\ X\ \mathtt{B}[5]\,!\,\{\mathtt{Foo}\,\textbf{.}\,X\,,\mathtt{Bar}\,\textbf{.}\,\mathbf{end}\})$



The last step explicitly shows that states with the same identifier are intended to be unified.

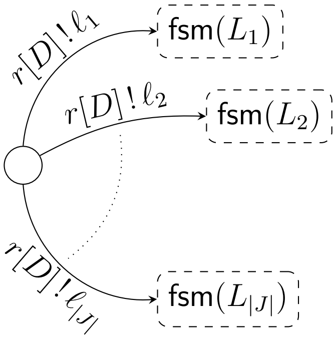
We also note that if a state s' does not have a nested FSM, τ transitions from a state s to s' can safely be abstracted away (up to weak bisimilarity, i.e., fsm never yields an FSM with τ-branching): every outgoing transition of s' is transformed into an outgoing transition of s, and the τ transition between s and s' is removed. This essentially means that instead of *explicitly* making an internal transition from s to s' before being able to make the next external transition, any one of those external transitions can be made immediately. Thus, the FSM in the previous example can be simplified to:



Finally, the following equations additionally define fsm for our local type syntactic sugar:

$$\mathsf{fsm}(r[D] \dagger^* \{\ell_j \,.\, L_j\}_{j \in J}) = \begin{cases} \bigcirc \xrightarrow{r[D] \dagger \ell_1} \boxed{\mathsf{fsm}(L_1)} & \textbf{if: } |J| = 1 \\ \mathsf{fsm}(\text{desugarred version of } r[D] \dagger^* \{\ell_j \,.\, L_j\}_{j \in J}) & \textbf{otherwise} \end{cases}$$

$\mathsf{fsm}(r[D]\,!^1\,\{\ell_j \,.\, L_j\}_{j \in J}) \;=$



III.2 Endpoint API Code Generation and the Scribble-Go Runtime

Transport abstraction. For the most part, the code generation for the I/O operations underlying the API type signatures outlined above is as expected: our goal is to provide lightweight type wrappers around standard channel communication facilities. Due to [DY13], our correctness results are directly applicable to any concrete transport with the standard semantics of asynchronous session types: an unbounded FIFO in each direction between each pair of endpoints (i.e., non-blocking output, reliable, order-preserving). The API code generation targets our Runtime session I/O library, which declares an abstract interface for binary, bi-directional channels with the above semantics: concrete transports are added to the Runtime by implementing this interface. API users select the transport as part of using the generated `Dial`/`Accept` methods (as in, e.g., §3.2).

Our current implementation supports bindings for the distributed transports of the standard `net` package (`https://golang.org/pkg/net/`), e.g., TCP and Unix domain sockets (we used such standard APIs as a basis for our generation). Our shared memory bindings are implemented by determining from the source protocol the set of message types that may be communicated between the relevant endpoint pair, and establishing a pair of Go channels (for each direction) for each type—we find this to be significantly faster than casting types through a raw `chan interface{}`. By default, messages are passed as pointers; the user may also specify to pass messages by value. We note that the core safety properties that we build on in §4.5 also hold for bounded asynchronous and synchronous channels [DY10]—it is thus safe for our APIs to wrap any such Go channels.

Optimisations. The main (potential) sources of run-time overhead introduced by our APIs during the execution of a running session are the creation and garbage collection of state channel structs, indirection of I/O operations through the Scribble-Go interfaces, and dynamic linearity checks. In early experiments, we found the former to be the dominating factor. In our current implementation, we have eliminated these costs by pre-creating a *single* instance of each channel struct in the API on Endpoint initiation. I/O methods are generated to simply return a pointer to the existing struct for the successor state (with the `id` linearity field set to a fresh value).

We find checking channel linearity by our method to be faster than the alternative of checking a `bool` usage guard pointed to from each channel struct in shared memory microbenchmarks; note, unlike our mechanism, directly embedding the `bool` as a struct field is unsafe due to potential copying of structs by the user. The cost of either method, however, tends to be insignificant in applications with non-trivial computations, and when using any other (more costly) transport than shared memory such as TCP (see §6 for our performance evaluations).

§3.3 demonstrated the API generation of the `Parallel` method (alongside `Foreach`) for nested FSMs where the indexed roles do not interact with each other. `Parallel` takes the same `func` type argument for the nested behaviour as `Foreach`, but spawns a separate goroutine to execute the `func` for each iteration; it returns after all the goroutines have terminated.

State channel delegation Our Runtime currently supports delegation in `shm` settings only, i.e., the state channel being delegated encapsulates only `shm` channels, and is being delegated over an `shm` channel—delegation is supported "for free" over Go channels: the underlying Go type is, e.g., `chan *A_1` (cf., `Pget`); note our linearity checking method allows passing the state channel by pointer (the channel is set as "used" at the sender-side via the *Endpoint*-tracked ID). Mechanisms for distributed delegation (e.g, [HYH08, SDHY17]) are orthogonal to this paper.

		Pt	Sc	Ga	FE	Pipe	MS	PP	Rec	Del
Core I/O patterns	1. One-to-Many (§6.1)		●		○					
	2. Many-to-One (§6.1)			●	○					
	3. Many-to-Many (§6.1)		●	●	○					
Parallel Topologies	4. Pipeline (§4.2)	●				●				
	5. Ring (§4.2; I.2)	●			●	●		●	●	
	6. Hadamard (§4.2)	●			●					
	7. Mesh (§4.2)	●			●	●				
	8. Fork-Join		●	●						
Applications	9. Pget^2 (□ is the difference between the two versions in §3.2; §3.3	●	●	●	□					●
	10. Vickrey auction (§ IV.1.2)	●	●	●	●		●		●	
	11. Jacobi solution of discrete Poisson equation. [BHY09]	●	●	●	●		●		●	
	12. n-body simulation (based on Ring) [BHY09]	●			●	●		●	●	
	13. Iterative linear equation solver (based on Mesh) [NY15]	●	●		●	●	●		●	
	14. `k-nucleotide` [Gou17] (§6.1)		●	●						
	15. `regex-redux` [Gou17] (§6.1)		●	●						
	16. `spectral-norm` [Gou17] (§6.1)		●	●			●		●	
	17. Fibonacci [LNTY17]	●			●					
	18. Quote-Request [ABPRT04, NY15]		●	●	●		●		●	
	19. P2P multiplayer game [SDHY17]	●			●	●		●	●	●
	20. Web Crawler [Akh16, NY17]	●	●	●	●					
	21. n-buyers [HYC16, CDYP16]	●			●		●		●	

Above, ○ are possible alt. implementations

Pt: point-to-point; Sc: Scatter; Ga: Gather; FE: Foreach; Pipe: Pipeline; MS: MS choices; PP: PP choices; Rec: Recursion; Del: Delegation

Fig. IV.1.1. Role-parametric protocols for communication patterns, topologies and applications in Scribble-Go.

Part IV
[§6] Evaluation

IV.1 [§6.2] Use Cases

IV.1.1 Description of Use Cases

We demonstrate the expressiveness and applicability of our framework through Table IV.1.1. The table lists protocols from this paper or in the literature that can be represented in our framework which we can generate APIs for. All the protocols listed in the table are either parameterised, or can be naturally adapted to be parameterised.

Each column represents a feature (or primitive) used by a given protocol, a ● indicates that a feature is present in the protocol; a ○ or □ indicate features present in alternative representation of protocol. The columns Pt, Sc, Ga mean direct peer-to-peer, one-to-many (scatter), and many-to-one (gather) communication; FE means role-parametric subprotocols using the `foreach` primitive. Peer-to-peer, scatter, and gather can all be represented with foreach (cf. Fig. 10), hence FE may be present if either of the base primitives is. Pipe is the pipeline communication (the `pipe` primitive). MS is branching (`choice`) and Rec is recursion with the `do`-statement. Finally, Del is delegation. The protocols are divided into the following categories:

Basic communication patterns Protocols 1–3 are the three base communication primitives *scatter*, *gather*, and *all-to-all* from the microbenchmarks in §6.1.

Common parallel topologies These protocols are commonly used in implementing parallel algorithms. Protocol 4 (Pipeline) is the basic parameterised pipeline structure. Protocol 5–7 are examples from §4.2: *Ring* (Example 4.4), *Hadamard* (Example 4.6), and *Mesh* (Example 4.7), MapReduce is the distribution and collection protocol for large-scale data processing; a parameterised session protocol was given by [NY15].

Protocols derived from applications Protocols in this category are extracted from real world applications or described in the literature. Protocol 9 (Pget) and its optimised version from §3.3 are the running examples of this paper. The optimised version uses foreach instead of scatter-gather communication. Protocols 14–16 are the three CLBG case studies in §6.1. Protocol 17 calculates the Fibonacci sequence and its definition is given in Example 4.5. Protocol 18 is a Quote-Request protocol specification (C-UC-002) [ABPRT04] published by the W3C Web Services Choreography Working Group [W3C02]. The protocol describes the interaction between a buyer who interacts with multiple suppliers who act as proxies to manufacturers to get a quote for goods or services. A parameterised protocol was specified in session types by [NY15]. Protocol 19 is a peer-to-peer multiplayer Game protocol introduced by [SDHY17]. The protocol describes three clients, initially unknown to each other, connects to a "matchmaking" server which sets up a game session where they can interact directly through delegation. We extended the protocol to be parameterised over the number of clients. Protocol 20 is a protocol from an open source web crawler [Akh16], which coordinates multiple processes to download then parse a specified webpage. A parameterised session protocol was given by [NY17]. Protocol 21 is a parameterised n-buyer protocol, where n buyers cooperate to buy a book from a seller. The protocol is adapted from the original three buyer protocol by [BCD$^+$08]. Protocol 10 is a Vickrey auction protocol, which describes an auction between multiple bidders and a coordinator. The bidding process involves repeated rounds of bidding where the bidders either post a higher bid to outbid their opponents or surrender until there is only one bidder left. The protocol uses gather to collect the bids and decisions from the bidders. Details of the protocol are given in § IV.1.2.

Comparison with existing parameterised MPST Previous theories and implementations of parameterised protocols are monolithic, and require index-dependency support in the execution runtime (e.g. generating code for MPI [NdFCY15]). Our framework supports most existing parameterised MPST protocols [DYBH12, NY15], but our approach brings the expressiveness of parameterised MPST protocols to *independent, distributed* endpoints that do not have dependent types.

IV.1.2 Example: Vickrey Auction

A *Vickrey auction* is an auction where k *bidders* aim to outbid each other through an *auctioneer*; the bidder with the second highest bid wins (e.g., Google and Yahoo! use generalised variants of the Vickrey auction to sell online advertisements [EOS07]). The auction proceeds in rounds.

In round $n = 1$, each of the k bidders communicates an `int` (initial bid) to the auctioneer. The auctioneer subsequently communicates an `int` (highest initial bid) to the bidders.

In round $n > 1$, each of the k bidders has a choice: communicate either an `int` (higher bid) or a `bool` (skip round) to the auctioneer. If the auctioneer receives only `bool`s, the auction is over, and the auctioneer communicates a `string` (winner announcement) to the bidders. Otherwise, the auctioneer communicates an `int` (new highest bid) to the bidders.

The Auction protocol with k bidders is specified by the following global type:

Example IV.1.1 (Auction).

$$\begin{aligned}
G_{\text{Auction}} = {} & \mathtt{B[1..k]} \xrightarrow{*} \mathtt{A} : \mathtt{InitialBid} \,.\, \mathtt{A} \xrightarrow{*} \mathtt{B[1..k]} : \mathtt{HighestBid} \,. \\
& \quad \mathbf{rec}\ \mathtt{X}\ \mathbf{foreach}\ \mathtt{B\{i:1..k\}}\ \mathbf{do}\ \left(\mathtt{B[i]} \rightarrow \mathtt{A} : \begin{Bmatrix} \mathtt{Bid} \,.\, \mathbf{cont} \\ \mathtt{Skip} \,.\, \mathbf{cont} \end{Bmatrix}\right)\ ; \\
& \qquad \mathtt{A} \xrightarrow{1} \mathtt{B[1..k]} : \begin{Bmatrix} \mathtt{HighestBid} \,.\, \mathtt{X} \\ \mathtt{Winner} \,.\, \mathbf{cont} \end{Bmatrix}\ ;\ \mathbf{end}
\end{aligned}$$

Example IV.1.2 (Auction)**.** The auction protocol as specified in Example IV.1.1, has two roles, Bidder B and Auctioneer A.

$$
\begin{aligned}
L^{\mathtt{B[1..k]}}_{\text{Auction}} &= \mathtt{A}\,\mathbf{!}\,\mathtt{InitialBid}\,\mathbf{.}\,\mathtt{A}\,\mathbf{?}\,\mathtt{HighestBid}\,\mathbf{.}\\
&\qquad \mathbf{rec}\ \mathtt{X}\ \mathtt{A}\,\mathbf{!}\left\{\begin{array}{l}\ \mathtt{Bid}\,\mathbf{.}\,\mathtt{A}\,\mathbf{?}\,\{\mathtt{HighestBid}\,\mathbf{.}\,\mathtt{X},\ \mathtt{Winner}\,\mathbf{.}\,\mathbf{end}\}\\ \mathtt{Skip}\,\mathbf{.}\,\mathtt{A}\,\mathbf{?}\,\{\mathtt{HighestBid}\,\mathbf{.}\,\mathtt{X},\ \mathtt{Winner}\,\mathbf{.}\,\mathbf{end}\}\end{array}\right\}\\
L^{\mathtt{A}}_{\text{Auction}} &= \mathtt{B[1..k]}\,\mathbf{?}^{*}\,\mathtt{InitialBid}\,\mathbf{.}\,\mathtt{B[1..k]}\,\mathbf{!}^{*}\,\mathtt{HighestBid}\,\mathbf{.}\\
&\qquad \mathbf{rec}\ \mathtt{X}\ \mathbf{foreach}\ \mathtt{B}\{\mathtt{i{:}1..k}\}\ \mathbf{do}\ (\mathtt{B[i]}\,\mathbf{?}\,\{\mathtt{Bid}\,\mathbf{.}\,\mathbf{cont},\ \mathtt{Skip}\,\mathbf{.}\,\mathbf{cont}\})\,\mathbf{;}\\
&\qquad\qquad \mathtt{B[1..k]}\,\mathbf{!}^{1}\,\{\mathtt{HighestBid}\,\mathbf{.}\,\mathtt{X},\ \mathtt{Winner}\,\mathbf{.}\,\mathbf{end}\}
\end{aligned}
$$

An example implementation of the Auction protocol using the generated APIs is given below:

```go
// Main body of one of the 1..k Bidders
func Bidder(b1 *B_1) End_B {
  var (
    highest int
    winnerName string
  )
  b2 := b1.A.Send. InitialBid(myBid).
            A.Receive.HighestBid(&highest)
  for {
    if highest < myMaxBid {
      b3 = b2.A.Send.Bid(myBid+1)
    } else {
      b3 = b2.A.Send.Skip(false)
    }
    highestBid, winner, _ := b3.A.Branch()
    select {
    case succ := <-highestBid.Case(&highest):
      b2 = succ
    case succ := <-winner.Case(&winnerName):
      print(winnerName)
      return succ
    }
  }
}

// Main body of the Auctioneer
func Auctioneer(a1 *A_1) End_A {
  var highest int
  a2 := a1.B_1toK.Gather.InitialBid(&bids)
  highest := max(bids)
  a3 := a2.B_1toK.Scatter.HighestBid(split(highest))
  var bidorskip []BidSkip
  for {
    a3 := a2.B_1toK.Gather.BidOrSkip(&bidorskip)
    newHighest, winnerId := findWinner(bidorskip)
        // sets winnerId if all skip
    if newHighest > highest {
      highest = newHighest
      a2 = a3.B_1toK.Scatter.HighestBid(split(highest))
    } else {
      return a3.B_1toK.Scatter.Winner(winnerId)
    }
  }
}
```

Part V
[§7] Related Work

V.1 Additional Related Work

Parallel programming abstractions and code generation for safe communication. Another approach of guaranteeing safety-by-construction is to hide communications behind an additional layer of programming abstractions for parallel computations. Examples include high-level constructs in languages with implicit/data parallelism [CGS$^+$05, CCZ07, Jr.05, CLJ$^+$07, Ble96, Cha01, Rei07], algorithmic skeleton APIs [Col88, GL10, LP10, CK10, ADK$^+$11], and domain-specific languages/ APIs that compile to parallel code [BSL$^+$11, CSB$^+$11, SLB$^+$11, DJP$^+$11, RBA$^+$13]. Besides safety, such languages/APIs are often highly optimised. However, the constructs of these languages/APIs embody a fixed, predetermined range of communication patterns, typically by design with respect to their target application domains. By contrast, our work targets open-ended specification and implementation of custom communication patterns and protocols, for any application or domain suited to our supported communication semantics; domain-specific abstractions may be built on top (e.g., via syntactic sugars or encodings; §4.2).

[ACRS16] present a calculus for parallel computations, that can encode abstractions for parallelism such as fork-join. The calculus is expressive, but is untyped; it offers no support against errors such as deadlock.

Part VI
Supplement References

[ABPRT04] Daniel Austin, Abbie Barbir, Ed Peters, and Steve Ross-Talbot. Web services choreography requirements. https://www.w3.org/TR/2004/WD-ws-chor-reqs-20040311/#UC-002, 2004.

[ACRS16] Umut A. Acar, Arthur Charguéraud, Mike Rainey, and Filip Sieczkowski. Dag-calculus: A calculus for parallel computation. In *Proceedings of the 21st ACM SIGPLAN International Conference on Functional Programming*, ICFP 2016, pages 18–32, New York, NY, USA, 2016. ACM.

[ADK$^+$11] Marco Aldinucci, Marco Danelutto, Peter Kilpatrick, Massimiliano Meneghin, and Massimo Torquati. Accelerating code on multi-cores with fastflow. In Emmanuel Jeannot, Raymond Namyst, and Jean Roman, editors, *Euro-Par 2011 Parallel Processing - 17th International Conference, Euro-Par 2011, Bordeaux, France, August 29 - September 2, 2011, Proceedings, Part II*, volume 6853 of *Lecture Notes in Computer Science*, pages 170–181. Springer, 2011.

[Akh16] Foat Akhmadeev. Web crawling with akka. http://foat.me/articles/crawling-with-akka/, 2016.

[BCD$^+$08] Lorenzo Bettini, Mario Coppo, Loris D'Antoni, Marco De Luca, Mariangiola Dezani-Ciancaglini, and Nobuko Yoshida. Global Progress in Dynamically Interleaved Multiparty Sessions. In *19th International Conference on Concurrency Theory*, volume 5201 of *LNCS*, pages 418–433. Springer, 2008.

[BHY09] Andi Bejleri, Raymond Hu, and Nobuko Yoshida. Session-based programming for parallel algorithms: Expressiveness and performance. In *Proceedings Second International Workshop on Programming Language Approaches to Concurrency and Communication-cEntric Software, PLACES 2009, York, UK, 22nd March 2009.*, volume 17 of *EPTCS*, pages 17–29, 2009.

[Ble96] Guy E. Blelloch. Programming parallel algorithms. *Commun. ACM*, 39(3):85–97, 1996.

[BSL$^+$11] Kevin J. Brown, Arvind K. Sujeeth, HyoukJoong Lee, Tiark Rompf, Hassan Chafi, Martin Odersky, and Kunle Olukotun. A heterogeneous parallel framework for domain-specific languages. In Lawrence Rauchwerger and Vivek Sarkar, editors, *2011 International Conference on Parallel Architectures and Compilation Techniques, PACT 2011, Galveston, TX, USA, October 10-14, 2011*, pages 89–100. IEEE Computer Society, 2011.

[CCZ07] Bradford L. Chamberlain, David Callahan, and Hans P. Zima. Parallel programmability and the chapel language. *IJHPCA*, 21(3):291–312, 2007.

[CDYP16] Mario Coppo, Mariangiola Dezani-Ciancaglini, Nobuko Yoshida, and Luca Padovani. Global progress for dynamically interleaved multiparty sessions. *Mathematical Structures in Computer Science*, 26(2):238–302, 2016.

[CGS$^+$05] Philippe Charles, Christian Grothoff, Vijay A. Saraswat, Christopher Donawa, Allan Kielstra, Kemal Ebcioglu, Christoph von Praun, and Vivek Sarkar. X10: an object-oriented approach to non-uniform cluster computing. In Ralph E. Johnson and Richard P. Gabriel, editors, *Proceedings of the 20th Annual ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications, OOPSLA 2005, October 16-20, 2005, San Diego, CA, USA*, pages 519–538. ACM, 2005.

[Cha01] Rohit Chandra. *Parallel programming in openMP*. Morgan Kaufmann, 2001.

[CK10] Philipp Ciechanowicz and Herbert Kuchen. Enhancing muesli's data parallel skeletons for multi-core computer architectures. In *12th IEEE International Conference on High Performance Computing and Communications, HPCC 2010, 1-3 September 2010, Melbourne, Australia*, pages 108–113. IEEE, 2010.

[CLJ$^+$07] Manuel M. T. Chakravarty, Roman Leshchinskiy, Simon L. Peyton Jones, Gabriele Keller, and Simon Marlow. Data parallel haskell: a status report. In Neal Glew and Guy E. Blelloch, editors, *Proceedings of the POPL 2007 Workshop on Declarative Aspects of Multicore Programming, DAMP 2007, Nice, France, January 16, 2007*, pages 10–18. ACM, 2007.

[Col88] Murray Cole. *Algorithmic skeletons : a structured approach to the management of parallel computation*. PhD thesis, University of Edinburgh, UK, 1988.

[CSB$^+$11] Hassan Chafi, Arvind K. Sujeeth, Kevin J. Brown, HyoukJoong Lee, Anand R. Atreya, and Kunle Olukotun. A domain-specific approach to heterogeneous parallelism. In Calin Cascaval and Pen-Chung Yew, editors, *Proceedings of the 16th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming, PPOPP 2011, San Antonio, TX, USA, February 12-16, 2011*, pages 35–46. ACM, 2011.

[DJP$^+$11] Zach DeVito, Niels Joubert, Francisco Palacios, Stephen Oakley, Montserrat Medina, Mike Barrientos, Erich Elsen, Frank Ham, Alex Aiken, Karthik Duraisamy, Eric Darve, Juan Alonso, and Pat Hanrahan. Liszt: a domain specific language for building portable mesh-based PDE solvers. In Scott Lathrop, Jim Costa, and William Kramer, editors, *Conference on High Performance Computing Networking, Storage and Analysis, SC 2011, Seattle, WA, USA, November 12-18, 2011*, pages 9:1–9:12. ACM, 2011.

[DY10] Pierre-Malo Deniélou and Nobuko Yoshida. Buffered communication analysis in distributed multiparty sessions. In *CONCUR 2010 - Concurrency Theory, 21th International Conference, CONCUR 2010, Paris, France, August 31-September 3, 2010. Proceedings*, volume 6269 of *Lecture Notes in Computer Science*, pages 343–357. Springer, 2010.

[DY13] Pierre-Malo Deniélou and Nobuko Yoshida. Multiparty compatibility in communicating automata: Characterisation and synthesis of global session types. In Fedor V. Fomin, Rusins Freivalds, Marta Z. Kwiatkowska, and David Peleg, editors, *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part II*, volume 7966 of *Lecture Notes in Computer Science*, pages 174–186. Springer, 2013.

[DYBH12] Pierre-Malo Deniélou, Nobuko Yoshida, Andi Bejleri, and Raymond Hu. Parameterised multiparty session types. *Logical Methods in Computer Science*, 8(4), 2012.

[EOS07] Benjamin Edelman, Michael Ostrovsky, and Michael Schwarz. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. *American Economic Review*, 97(1):424–259, 2007.

[GL10] Horacio González-Vélez and Mario Leyton. A survey of algorithmic skeleton frameworks: high-level structured parallel programming enablers. *Softw., Pract. Exper.*, 40(12):1135–1160, 2010.

[Gou17] Issac Gouy. Computer language benchmark game. `http://benchmarksgame.alioth.debian.org`, 2017.

[HYC16] Kohei Honda, Nobuko Yoshida, and Marco Carbone. Multiparty asynchronous session types. *J. ACM*, 63(1):9:1–9:67, 2016.

[HYH08] Raymond Hu, Nobuko Yoshida, and Kohei Honda. Session-based distributed programming in java. In *ECOOP 2008 - Object-Oriented Programming, 22nd European Conference, Paphos, Cyprus, July 7-11, 2008, Proceedings*, volume 5142 of *Lecture Notes in Computer Science*, pages 516–541. Springer, 2008.

[Jr.05] Guy L. Steele Jr. Parallel programming and parallel abstractions in fortress. In *14th International Conference on Parallel Architecture and Compilation Techniques (PACT 2005), 17-21 September 2005, St. Louis, MO, USA*, page 157. IEEE Computer Society, 2005.

[LNTY17] Julien Lange, Nicholas Ng, Bernardo Toninho, and Nobuko Yoshida. Fencing off go: liveness and safety for channel-based programming. In Giuseppe Castagna and Andrew D. Gordon, editors, *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017*, pages 748–761. ACM, 2017.

[LP10] Mario Leyton and José M. Piquer. Skandium: Multi-core programming with algorithmic skeletons. In Marco Danelutto, Julien Bourgeois, and Tom Gross, editors, *Proceedings of the 18th Euromicro Conference on Parallel, Distributed and Network-based Processing, PDP 2010, Pisa, Italy, February 17-19, 2010*, pages 289–296. IEEE Computer Society, 2010.

[NdFCY15] Nicholas Ng, José Gabriel de Figueiredo Coutinho, and Nobuko Yoshida. Protocols by default - safe MPI code generation based on session types. In Björn Franke, editor, *Compiler Construction - 24th International Conference, CC 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings*, volume 9031 of *Lecture Notes in Computer Science*, pages 212–232. Springer, 2015.

[NY15] Nicholas Ng and Nobuko Yoshida. Pabble: parameterised scribble. *Service Oriented Computing and Applications*, 9(3-4):269–284, 2015.

[NY17] Rumyana Neykova and Nobuko Yoshida. Let It Recover: Multiparty Protocol-Induced Recovery. In *26th International Conference on Compiler Construction*, pages 98–108. ACM, 2017.

[RBA$^+$13] Jonathan Ragan-Kelley, Connelly Barnes, Andrew Adams, Sylvain Paris, Frédo Durand, and Saman P. Amarasinghe. Halide: a language and compiler for optimizing parallelism, locality, and recomputation in image processing pipelines. In Hans-Juergen Boehm and Cormac Flanagan, editors, *ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI '13, Seattle, WA, USA, June 16-19, 2013*, pages 519–530. ACM, 2013.

[Rei07] James Reinders. *Intel threading building blocks - outfitting C++ for multi-core processor parallelism.* O'Reilly, 2007.

[SDHY17] Alceste Scalas, Ornela Dardha, Raymond Hu, and Nobuko Yoshida. A linear decomposition of multiparty sessions for safe distributed programming. In Peter Müller, editor, *31st European Conference on Object-Oriented Programming, ECOOP 2017, June 19-23, 2017, Barcelona, Spain*, volume 74 of *LIPIcs*, pages 24:1–24:31. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[SLB$^+$11] Arvind K. Sujeeth, HyoukJoong Lee, Kevin J. Brown, Tiark Rompf, Hassan Chafi, Michael Wu, Anand R. Atreya, Martin Odersky, and Kunle Olukotun. Optiml: An implicitly parallel domain-specific language for machine learning. In Lise Getoor and Tobias Scheffer, editors, *Proceedings of the 28th International Conference on Machine Learning, ICML 2011, Bellevue, Washington, USA, June 28 - July 2, 2011*, pages 609–616. Omnipress, 2011.

[W3C02] W3C. Web services choreography working group. `https://www.w3.org/2002/ws/chor/`, 2002.

1. $\langle \mathbb{A}, +, 0, - \rangle$ is a torsion-free abelian group

2. $\langle \mathbb{A}, \preceq \rangle$ is a partially ordered set

3. $\langle \mathbb{A}, < \rangle$ is a strictly totally ordered set

4. $\Big[a_1 \preceq a_2 \ \textsf{\textbf{and}}\ \ a_3 = a_4\Big] \ \textsf{\textbf{impl.}}\ \ a_1 + a_3 \preceq a_2 + a_4$

5. $\Big[a_1 < a_2 \ \textsf{\textbf{and}}\ \ a_3 = a_4\Big] \ \textsf{\textbf{impl.}}\ \ a_1 + a_3 < a_2 + a_4$

6. $\delta(a_1^{\mathsf{lo}}, a_1^{\mathsf{hi}}) = \delta(a_2^{\mathsf{lo}}, a_2^{\mathsf{hi}}) \ \textsf{\textbf{impl.}}\ \ \{\tilde{a}_1 + \delta(a_1^{\mathsf{lo}}, a_2^{\mathsf{lo}}) \mid a_1^{\mathsf{lo}} \preceq \tilde{a}_1 \preceq a_1^{\mathsf{hi}}\} = \{\tilde{a}_2 \mid a_2^{\mathsf{lo}} \preceq \tilde{a}_2 \preceq a_2^{\mathsf{hi}}\}$

Fig. VII.2.1. Addition, identity, inverse, selection, arrangement (ranks)

Part VII
Full Definitions

(The notation in this part and the next differs slightly from the notation above and in the main paper.)

VII.1 Preliminaries

Definition VII.1.1. Let $\mathfrak{Nat} = \{\mathfrak{0}, \mathfrak{1}, \ldots\}$ denote the set of all *natural numbers*, ranged over by $\mathfrak{n}$.

Remark VII.1.1. By convention, $\tilde{\cdot}$ indicates symbols bound by explicit quantifiers in mathematical statement (e.g., $\Big[\Big[\tilde{\mathfrak{n}} \neq \mathfrak{0} \ \textsf{\textbf{impl.}}\ \ \tilde{\mathfrak{n}} > \mathfrak{0}\Big] \ \textsf{\textbf{for-all}}\ \ \tilde{\mathfrak{n}}\Big]$) or by implicit quantifiers in set-builder notation (e.g., $\{\tilde{\mathfrak{n}} + \mathfrak{1} \mid \tilde{\mathfrak{n}} \in \mathfrak{Nat}\}$).

Remark VII.1.2. All lemmas are stated without proof; they follow directly from preceding definitions and figures. In contrast, all theorems are stated with proof.

VII.2 Ranks

VII.2.1 Elements

Definition VII.2.1. Let $\mathbb{A}$ denote the set of all *ranks*, ranged over by a.

Definition VII.2.2. Let $a_1 + a_2$ denote the *addition* of a_1 and a_2. Let 0 denote the *identity.* Let $-a$ denote the *negation* of a. Let $a_1 \preceq a_2$ denote the *selection* of a_1 before a_2. Let $a_1 < a_2$ denote the *arrangement* of a_1 before a_2. Let $\delta(a_1, a_2) = a_2 + (-a_1)$ denote the *distance* between a_1 and a_2. Fig. VII.2.1 axiomatises $+$, 0, $-$, $\preceq$, and $<$.

Lemma VII.2.1.

1. $A \neq \emptyset \ \textsf{\textbf{impl.}}\ \ \min \langle \{\tilde{a} + a \mid \tilde{a} \in A\}, < \rangle = \min \langle A, < \rangle + a$

2. $\delta(a_1^{\mathsf{lo}}, a_1^{\mathsf{hi}}) = \delta(a_2^{\mathsf{lo}}, a_2^{\mathsf{hi}}) \preceq^{-1} 0 \ \textsf{\textbf{impl.}}\ \ \{\tilde{a}_1 + \delta(a_1^{\mathsf{lo}}, a_2^{\mathsf{lo}}) \mid a_1^{\mathsf{lo}} \preceq \tilde{a}_1 \preceq a_1^{\mathsf{hi}}\} = \{\tilde{a}_2 \mid a_2^{\mathsf{lo}} \preceq \tilde{a}_2 \preceq a_2^{\mathsf{hi}}\} \neq \emptyset$

$$\mathsf{head}\, A = \min \langle A, < \rangle$$

$$\mathsf{tail}\, A = A \setminus \{\min \langle A, < \rangle\}$$

$$\delta(A_1, A_2) = a \quad \textsf{\textbf{if:}}\ \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2 \neq \emptyset$$

Fig. VII.2.2. Head, tail, distance (sets of ranks)

$$\frac{\mathsf{head}\, A_1 < \mathsf{head}\, A_2 \qquad \mathsf{tail}\, A_1 < \mathsf{tail}\, A_2}{A_1 < A_2} \qquad \frac{}{\emptyset < \emptyset}$$

Fig. VII.2.3. Arrangement (sets of ranks)

VII.2.2 Sets

Definition VII.2.3. Let $2^{\mathbb{A}}$ denote the set of all *sets of ranks* (ordered by $<$), ranged over by A.

Definition VII.2.4. Let $\mathsf{head}\, A$ denote the *head* of A. Let $\mathsf{tail}\, A$ denote the *tail* of A. Let $\delta(A_1, A_2)$ denote the *distance* between A_1 and A_2. Fig. VII.2.2 defines head, tail, and δ.

Lemma VII.2.2. $\mathsf{head} : 2^{\mathbb{A}} \rightharpoonup \mathbb{A}$

Lemma VII.2.3. $\mathsf{tail} : 2^{\mathbb{A}} \rightharpoonup 2^{\mathbb{A}}$

Lemma VII.2.4.

1. $\delta : 2^{\mathbb{A}} \times 2^{\mathbb{A}} \rightharpoonup \mathbb{A}$
2. $\delta(A_1, A_2) \neq 0$ **impl.** $A_1 \neq A_2$
3. $\delta(\{a_1\}, \{a_2\}) = \delta(a_1, a_2)$

Theorem VII.2.1. $\langle A_1, A_2 \rangle \in \operatorname{dom} \delta$ **impl.** $\delta(A_1, A_2) = \delta(\mathsf{head}\, A_1, \mathsf{head}\, A_2)$

Proof. See Section VIII.1. □

Definition VII.2.5. Let $A_1 < A_2$ denote the *arrangement* of A_1 before A_2. Fig. VII.2.3 defines $<$.

Theorem VII.2.2. $\Big[0 < a$ **and** $\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2\Big]$ **impl.** $A_1 < A_2$

Proof. See Section VIII.2. □

VII.2.3 Families

Definition VII.2.6. Let $\mathbb{Z}$ denote the set of all *rank variables*, ranged over by z. Let $\operatorname{fam} \langle \mathbb{Z}, \mathbb{A} \rangle = \mathbb{Z} \rightharpoonup \mathbb{A}$ denote the set of all *families of ranks*, ranged over by ϕ. Let $\operatorname{fam} \langle \mathbb{Z}, 2^{\mathbb{A}} \rangle = \mathbb{Z} \rightharpoonup 2^{\mathbb{A}}$ denote the set of all *families of sets of ranks*, ranged over by Φ.

Definition VII.2.7. Let ϕ / z denote the *normalisation* of ϕ to z. Fig. VII.2.4 defines $/$.

Lemma VII.2.5.

$$\phi/z = \{\tilde{z} \mapsto \phi(z) + \delta(\phi(z), \phi(\tilde{z})) \mid \tilde{z} \in \mathbb{Z}\}$$

Fig. VII.2.4. Normalisation (families of ranks)

$$\begin{aligned} \mathsf{head}\,\Phi &= \{\tilde{z} \mapsto \mathsf{head}\,\Phi(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} \\ \mathsf{tail}\,\Phi &= \{\tilde{z} \mapsto \mathsf{tail}\,\Phi(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} \\ \delta\Phi &= \{\langle \tilde{z}_1, \tilde{z}_2\rangle \mapsto \delta(\Phi(\tilde{z}_1), \Phi(\tilde{z}_2)) \mid \tilde{z}_1, \tilde{z}_2 \in \mathbb{Z}\} \\ \mathsf{len}\,\Phi &= \mathfrak{n} \quad \textsf{\textbf{if:}}\ \mathfrak{n} = |\Phi(\tilde{z})|\ \textsf{\textbf{for-all}}\ \tilde{z} \in \operatorname{dom}\Phi \end{aligned}$$

Fig. VII.2.5. Head, tail, distance matrix, length (families of sets of ranks)

1. $/ : \operatorname{fam}\langle \mathbb{Z}, \mathbb{A}\rangle \times \mathbb{Z} \to \operatorname{fam}\langle \mathbb{Z}, \mathbb{A}\rangle$
2. $\langle \phi, z\rangle \in \operatorname{dom}/$ **impl.** $\phi/z = \phi$

Definition VII.2.8. Let $\mathsf{head}\,\Phi$ denote the *head* of Φ. Let $\mathsf{tail}\,\Phi$ denote the *tail* of Φ. Let $\delta\Phi$ denote the *distance matrix* of Φ. Let $\mathsf{len}\,\Phi$ denote the *lengths* of Φ. Fig. VII.2.5 defines head, tail, δ, and len.

Lemma VII.2.6.

1. $\mathsf{head} : \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle \to \operatorname{fam}\langle \mathbb{Z}, \mathbb{A}\rangle$
2. $\Big[\big[\Phi(\tilde{z}) \neq \emptyset$ **for-all** $\tilde{z} \in \operatorname{dom}\Phi\big]$ **impl.** $\operatorname{dom}\Phi \subseteq \operatorname{dom}(\mathsf{head}\,\Phi)\Big]$ **and** $\operatorname{dom}(\mathsf{head}\,\Phi) \subseteq \operatorname{dom}\Phi$
3. $\big[\Phi(z) \in \operatorname{dom}\mathsf{head}$ **or** $z \in \operatorname{dom}(\mathsf{head}\,\Phi)\big]$ **impl.** $\mathsf{head}\,\Phi(z) = (\mathsf{head}\,\Phi)(z)$
4. $\Phi_1 \cup \Phi_2 \in \operatorname{dom}\mathsf{head}$ **impl.** $\mathsf{head}\,(\Phi_1 \cup \Phi_2) = (\mathsf{head}\,\Phi_1) \cup (\mathsf{head}\,\Phi_2)$
5. $\Phi_1 \setminus \Phi_2 \in \operatorname{dom}\mathsf{head}$ **impl.** $\mathsf{head}\,(\Phi_1 \setminus \Phi_2) = (\mathsf{head}\,\Phi_1) \setminus (\mathsf{head}\,\Phi_2)$

Lemma VII.2.7.

1. $\mathsf{tail} : \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle \to \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle$
2. $\Big[\big[\Phi(\tilde{z}) \neq \emptyset$ **for-all** $\tilde{z} \in \operatorname{dom}\Phi\big]$ **impl.** $\operatorname{dom}\Phi \subseteq \operatorname{dom}(\mathsf{tail}\,\Phi)\Big]$ **and** $\operatorname{dom}(\mathsf{tail}\,\Phi) \subseteq \operatorname{dom}\Phi$
3. $\big[\Phi(z) \in \operatorname{dom}\mathsf{tail}$ **or** $z \in \operatorname{dom}(\mathsf{tail}\,\Phi)\big]$ **impl.** $\mathsf{tail}\,\Phi(z) = (\mathsf{tail}\,\Phi)(z)$
4. $\Phi_1 \cup \Phi_2 \in \operatorname{dom}\mathsf{tail}$ **impl.** $\mathsf{tail}\,(\Phi_1 \cup \Phi_2) = (\mathsf{tail}\,\Phi_1) \cup (\mathsf{tail}\,\Phi_2)$
5. $\Phi_1 \setminus \Phi_2 \in \operatorname{dom}\mathsf{tail}$ **impl.** $\mathsf{tail}\,(\Phi_1 \setminus \Phi_2) = (\mathsf{tail}\,\Phi_1) \setminus (\mathsf{tail}\,\Phi_2)$

Lemma VII.2.8.

1. $\delta : \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle \to (\mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{A})$
2. $\operatorname{dom}\delta\Phi \subseteq (\operatorname{dom}\Phi) \times (\operatorname{dom}\Phi)$

$$\phi{\cdot}\Phi = \{\tilde{z} \mapsto \{\phi(\tilde{z})\} \cup \Phi(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\}$$

$$\Phi \mathbin{\mathsf{to}} z[a] = \begin{cases} \{\tilde{z} \mapsto \emptyset \mid \tilde{z} \in \operatorname{dom}\Phi\} & \textbf{if: } \Phi \in \operatorname{dom}\mathsf{len} \textbf{ and } a \in \Phi(z) \textbf{ and } a = (\mathsf{head}\,\Phi)(z) \\ (\mathsf{head}\,\Phi){\cdot}((\mathsf{tail}\,\Phi) \mathbin{\mathsf{to}} z[a]) & \textbf{if: } \Phi \in \operatorname{dom}\mathsf{len} \textbf{ and } a \in \Phi(z) \textbf{ and } a \neq (\mathsf{head}\,\Phi)(z) \end{cases}$$

$$\Phi \mathbin{\mathsf{from}} z[a] = \begin{cases} \Phi & \textbf{if: } \Phi \in \operatorname{dom}\mathsf{len} \textbf{ and } a \in \Phi(z) \textbf{ and } a = (\mathsf{head}\,\Phi)(z) \\ (\mathsf{tail}\,\Phi) \mathbin{\mathsf{from}} z[a] & \textbf{if: } \Phi \in \operatorname{dom}\mathsf{len} \textbf{ and } a \in \Phi(z) \textbf{ and } a \neq (\mathsf{head}\,\Phi)(z) \end{cases}$$

Fig. VII.2.6. Extension, largest prefix, smallest suffix (families of sets of ranks)

3. $\Big[\langle \Phi(z_1), \Phi(z_2)\rangle \in \operatorname{dom}\delta$ **or** $\langle z_1, z_2\rangle \in \operatorname{dom}\delta\Phi\Big]$ **impl.** $\delta(\Phi(z_1), \Phi(z_2)) = \delta\Phi(z_1, z_2)$

4. $\Big[\langle z_1, z_2\rangle \in \operatorname{dom}\delta\Phi$ **and** $\Phi(z_1) = \Phi(z_2)\Big]$ **impl.** $\delta\Phi(z_1, z_2) = 0$

5. $\Big[\langle z_1, z_2\rangle \in \operatorname{dom}\delta\Phi$ **and** $\Phi(z_1) \neq \Phi(z_2)\Big]$ **impl.** $\delta\Phi(z_1, z_2) \neq 0$

Lemma VII.2.9.

1. $\mathsf{len} : \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle \rightharpoonup \mathfrak{Nat}$

2. $\Big[\Phi \in \operatorname{dom}\mathsf{len}$ **and** $\Phi(z) \neq \emptyset\Big]$ **impl.** $\mathsf{len}\,\Phi > \mathsf{0}$

3. $\Big[\Phi \in \operatorname{dom}\mathsf{len}$ **and** $\Phi(z) \neq \emptyset$ **and** $z' \in \operatorname{dom}\Phi\Big]$ **impl.** $\Phi(z') \neq \emptyset$

Theorem VII.2.3.

1. $\Big[A = \min\langle \operatorname{img}\Phi, <\rangle$ **and** $A \neq \emptyset\Big]$ **impl.** $\mathsf{tail}\,A = \min\langle \operatorname{img}(\mathsf{tail}\,\Phi), <\rangle$

2. $\Big[A = \max\langle \operatorname{img}\Phi, <\rangle$ **and** $A \neq \emptyset\Big]$ **impl.** $\mathsf{tail}\,A = \max\langle \operatorname{img}(\mathsf{tail}\,\Phi), <\rangle$

Proof. See Section VIII.3. □

Theorem VII.2.4. $\langle z_1, z_2\rangle \in \operatorname{dom}\delta\Phi$ **impl.** $\delta\Phi(z_1, z_2) = \delta((\mathsf{head}\,\Phi)(z_1), (\mathsf{head}\,\Phi)(z_2))$

Proof. See Section VIII.4. □

Theorem VII.2.5. $\mathsf{len}\,\Phi > \mathsf{0}$ **impl.** $\mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi$

Proof. See Section VIII.5. □

Definition VII.2.9. Let $\phi{\cdot}\Phi$ denote the *extension* of Φ with ϕ. Let $\Phi \mathbin{\mathsf{to}} z[a]$ denote the *largest prefix* of Φ that excludes $z[a]$. Let $\Phi \mathbin{\mathsf{from}} z[a]$ denote the *smallest suffix* of Φ that includes $z[a]$. Fig. VII.2.6 defines $\cdot$, to, and from.

Lemma VII.2.10.

1. $\cdot : \operatorname{fam}\langle \mathbb{Z}, \mathbb{A}\rangle \times \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle \to \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle$

2. $\operatorname{dom}\phi{\cdot}\Phi = (\operatorname{dom}\phi) \cap (\operatorname{dom}\Phi)$

3. $\Big[\big[z \in \operatorname{dom}\phi$ **and** $z \in \operatorname{dom}\Phi\big]$ **or** $z \in \operatorname{dom}\phi{\cdot}\Phi\Big]$ **impl.** $\{\phi(z)\} \cup \Phi(z) = (\phi{\cdot}\Phi)(z)$

Lemma VII.2.11.

1. $\mathsf{to} : \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle \times (\mathbb{Z} \times \mathbb{A}) \rightharpoonup \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle$

2. $\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{to}$ **impl.** $\operatorname{dom}\Phi = \operatorname{dom}(\Phi\,\mathsf{to}\,z[a])$

3. $\big[\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{to}$ **and** $z' \in \operatorname{dom}\Phi\big]$ **impl.** $(\Phi\,\mathsf{to}\,z[a])(z') \subseteq \Phi(z')$

Lemma VII.2.12.

1. $\mathsf{from} : \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle \times (\mathbb{Z} \times \mathbb{A}) \rightharpoonup \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle$

2. $\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{from}$ **impl.** $\operatorname{dom}\Phi = \operatorname{dom}(\Phi\,\mathsf{from}\,z[a])$

3. $\big[\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{from}$ **and** $z' \in \operatorname{dom}\Phi\big]$ **impl.** $(\Phi\,\mathsf{from}\,z[a])(z') \subseteq \Phi(z')$

Theorem VII.2.6.

1. $\big[\Phi \in \operatorname{dom}\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\,\Phi)(z)\big]$ **impl.** $\mathsf{head}\,\Phi = \mathsf{head}\,(\Phi\,\mathsf{to}\,z[a])$

2. $\big[\langle\mathsf{tail}\,\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{to}$ **and** $\Phi \in \operatorname{dom}\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\,\Phi)(z)\big]$
impl. $(\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a] = \mathsf{tail}\,(\Phi\,\mathsf{to}\,z[a])$

3. $\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{to}$ **impl.** $\Phi\,\mathsf{to}\,z[a] \in \operatorname{dom}\mathsf{len}$

Proof. See Section VIII.6. □

Theorem VII.2.7.

1. $\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{from}$ **impl.** $a = (\mathsf{head}\,(\Phi\,\mathsf{from}\,z[a]))(z)$

2. $\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{from}$ **impl.** $\mathsf{len}\,(\Phi\,\mathsf{from}\,z[a]) > \mathfrak{o}$

3. $\big[\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{from}$ **and** $z' \in \operatorname{dom}\Phi\big]$ **impl.** $(\Phi\,\mathsf{from}\,z[a])(z') \neq \emptyset$

4. $\big[\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{from}$ **and** $\Phi(z_1) < \Phi(z_2)\big]$ **impl.** $(\Phi\,\mathsf{from}\,z[a])(z_1) < (\Phi\,\mathsf{from}\,z[a])(z_2)$

5. $\big[\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{from}$ **and** $\Phi(z') < \Phi(z)$ **and** $a \in \Phi(z')\big]$ **impl.** $a \in (\Phi\,\mathsf{from}\,z[a])(z')$

6. $\big[\langle\Phi, z_1[a]\rangle, \langle\Phi, z_2[a]\rangle \in \operatorname{dom}\mathsf{from}$ **and** $\Phi(z_2) < \Phi(z_1)\big]$
impl. $\Phi\,\mathsf{from}\,z_2[a] = (\Phi\,\mathsf{from}\,z_1[a])\,\mathsf{from}\,z_2[a]$

Proof. See Section VIII.7. □

Theorem VII.2.8.

1. $\big[\langle\Phi(z_1), \Phi(z_2)\rangle \in \operatorname{dom}\delta$ **and** $\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{to}$ **and** $a \neq (\mathsf{head}\,\Phi)(z)\big]$
impl. $\delta(\Phi(z_1), \Phi(z_2)) = \delta((\Phi\,\mathsf{to}\,z[a])(z_1), (\Phi\,\mathsf{to}\,z[a])(z_2))$

$$\begin{array}{lcl}
\check{E} \in \check{\mathbb{E}} & ::= & \check{E}_1 \texttt{+} \check{E}_2 \;\;|\;\; \check{E}_1 \texttt{-} \check{E}_2 \;\;|\;\; a \;\;|\;\; k \\
\hat{E} \in \hat{\mathbb{E}} & ::= & \hat{E}_1 \texttt{+} \hat{E}_2 \;\;|\;\; \hat{E}_1 \texttt{-} \hat{E}_2 \;\;|\;\; a \\
\\
\check{D} \in \check{\mathbb{D}} & ::= & \check{E}^{\mathsf{lo}} \,..\, \check{E}^{\mathsf{hi}} \\
\hat{D} \in \hat{\mathbb{D}} & ::= & \hat{E}^{\mathsf{lo}} \,..\, \hat{E}^{\mathsf{hi}} \\
\\
\check{C} \in \check{\mathbb{C}} & ::= & \{z_i : \check{D}_i\}_{i \in I} \;\; \textbf{if: } \Big[i_1 \neq i_2 \;\textbf{impl.}\; z_{i_1} \neq z_{i_2} \Big] \;\textbf{for-all}\; i_1, i_2 \in I \\
\hat{C} \in \hat{\mathbb{C}} & ::= & \{z_i : \hat{D}_i\}_{i \in I} \;\; \textbf{if: } \Big[i_1 \neq i_2 \;\textbf{impl.}\; z_{i_1} \neq z_{i_2} \Big] \;\textbf{for-all}\; i_1, i_2 \in I
\end{array}$$

Fig. VII.3.1. Open/closed rank expressions, open/closed intervals, open/closed iterators

2. $\Big[\langle \Phi(z_1), \Phi(z_2)\rangle \in \operatorname{dom} \delta \;\textbf{ and }\; \langle \Phi, z[a]\rangle \in \operatorname{dom} \mathsf{from}\Big]$
$\textbf{impl. } \delta(\Phi(z_1), \Phi(z_2)) = \delta((\Phi \,\mathsf{from}\, z[a])(z_1), (\Phi \,\mathsf{from}\, z[a])(z_2))$

Proof. See Section VIII.8. □

Theorem VII.2.9.

1. $\Big[\langle \Phi \cup \Phi_{\mathsf{co}}, z[a]\rangle \in \operatorname{dom} \mathsf{to} \;\textbf{ and }\; \Phi(z) = \max \langle \operatorname{img} \Phi, <\rangle \;\textbf{ and }\; \Big[a \notin \Phi_{\mathsf{co}}(\tilde{z}) \;\textbf{ for-all }\; \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}}\Big]\Big]$
$\textbf{impl. } a \notin \bigcup \operatorname{img}((\Phi \cup \Phi_{\mathsf{co}}) \,\mathsf{to}\, z[a])$

2. $\left[\begin{array}{l} \langle \Phi \cup \Phi_{\mathsf{co}}, z[a]\rangle \in \operatorname{dom} \mathsf{from} \;\textbf{ and } \\ \Phi(z) = \min \langle \operatorname{img} \Phi, <\rangle \;\textbf{ and }\; \Big[a \notin \Phi_{\mathsf{co}}(\tilde{z}) \;\textbf{ for-all }\; \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}}\Big] \end{array}\right]$
$\textbf{impl. } a \notin \bigcup \operatorname{img}(\mathsf{tail}((\Phi \cup \Phi_{\mathsf{co}}) \,\mathsf{from}\, z[a]))$

3. $\left[\begin{array}{l} \langle (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}) \,\mathsf{from}\, z_1[a], z_2[a]\rangle \in \operatorname{dom} \mathsf{to} \;\textbf{ and } \\ \Phi(z_1) = \max \langle \operatorname{img} \Phi, <\rangle \;\textbf{ and }\; \Phi(z_2) = \max \langle \operatorname{img}(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}), <\rangle \;\textbf{ and } \\ \Big[\Phi(\tilde{z}) < \Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}}) \;\textbf{ for-all }\; \tilde{z} \in \operatorname{dom} \Phi, \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} \Phi_{\mathsf{gr}}\Big] \;\textbf{ and }\; \Big[a \notin \Phi_{\mathsf{co}}(\tilde{z}) \;\textbf{ for-all }\; \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}}\Big] \end{array}\right]$
$\textbf{impl. } a \notin \bigcup \operatorname{img}(\mathsf{tail}((\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}) \,\mathsf{from}\, z_1[a] \,\mathsf{to}\, z_2[a]))$

Proof. See Section VIII.9. □

VII.3 Rank Expressions, Intervals, and Iterators

VII.3.1 Syntax

Definition VII.3.1. Let $\mathbb{K}$ denote the set of all *parameters*, ranged over by k. Let $\texttt{self} \in \mathbb{K}$ denote a distinguished parameter.

Definition VII.3.2. Let $\check{\mathbb{E}}$ and $\hat{\mathbb{E}}$ denote the sets of all *open and closed rank expressions*, ranged over by $\check{E}$ and $\hat{E}$. Let $\check{\mathbb{D}}$ and $\hat{\mathbb{D}}$ denote the sets of all *open and closed intervals*, ranged over by $\check{D}$ and $\hat{D}$. Let $2^{\check{\mathbb{D}}}$ and $2^{\hat{\mathbb{D}}}$ denote the set of all *sets of open and closed rank intervals*, ranged over by $\check{\mathcal{D}}$ and $\hat{\mathcal{D}}$. Let $\check{\mathbb{C}}$ and $\hat{\mathbb{C}}$ denote the sets of all *open and closed iterators*, ranged over by $\check{C}$ and $\hat{C}$. Fig. VII.3.1 defines $\check{\mathbb{E}}$, $\hat{\mathbb{E}}$, $\check{\mathbb{D}}$, $\hat{\mathbb{D}}$, $\check{\mathbb{C}}$, and $\hat{\mathbb{C}}$.

$$\begin{aligned}
\mathsf{vars}(\{z_i\!:\!\check{D}_i\}_{i\in I}) &= \{z_i \mid i \in I\}\\
\mathsf{ivals}(\{z_i\!:\!\check{D}_i\}_{i\in I}) &= \{D_i \mid i \in I\}
\end{aligned}$$

Fig. VII.3.2. Rank variables, intervals (open iterators)

$$\begin{aligned}
\check{E}_1\texttt{+}\check{E}_2 \langle\!\langle\psi\rangle\!\rangle &= (\check{E}_1 \langle\!\langle\psi\rangle\!\rangle)\texttt{+}(\check{E}_2 \langle\!\langle\psi\rangle\!\rangle)\\
\check{E}_1\texttt{-}\check{E}_2 \langle\!\langle\psi\rangle\!\rangle &= (\check{E}_1 \langle\!\langle\psi\rangle\!\rangle)\texttt{-}(\check{E}_2 \langle\!\langle\psi\rangle\!\rangle)\\
a \langle\!\langle\psi\rangle\!\rangle &= a\\
k \langle\!\langle\psi\rangle\!\rangle &= \begin{cases}\psi(k) & \textsf{\textbf{if:}}\ k \in \operatorname{dom}\psi\\ k & \textsf{\textbf{if:}}\ k \notin \operatorname{dom}\psi\end{cases}\\
\check{E}^{\mathsf{lo}}\,..\,\check{E}^{\mathsf{hi}} \langle\!\langle\psi\rangle\!\rangle &= (\check{E}^{\mathsf{lo}} \langle\!\langle\psi\rangle\!\rangle)\,..\,(\check{E}^{\mathsf{hi}} \langle\!\langle\psi\rangle\!\rangle)\\
\{z_i\!:\!\check{D}_i\}_{i\in I} \langle\!\langle\psi\rangle\!\rangle &= \{z_i\!:\!\check{D}_i \langle\!\langle\psi\rangle\!\rangle\}_{i\in I}\\
z \langle\!\langle\psi\rangle\!\rangle &= z
\end{aligned}$$

Fig. VII.3.3. Parameter instantiation (open rank expressions, open intervals, open iterators)

Definition VII.3.3. Let $\check{\mathbb{E}} \cup \mathbb{Z}$ and $\hat{\mathbb{E}} \cup \mathbb{Z}$ denote the set of all *open and closed indices*, ranged over by $\check{x}$ and $\hat{x}$. We shall often write x instead of $\check{x}$ and $\hat{x}$.

Lemma VII.3.1. $\hat{\mathbb{E}} \subseteq \check{\mathbb{E}}$

Lemma VII.3.2. $\hat{\mathbb{D}} \subseteq \check{\mathbb{D}}$

Lemma VII.3.3. $\hat{\mathbb{C}} \subseteq \check{\mathbb{C}}$

Definition VII.3.4. Let $\mathsf{vars}(\check{C})$ denote the *rank variables* that occur in $\check{C}$. Let $\mathsf{ivals}(\check{C})$ denote the set of all *rank intervals* that occur in $\check{C}$. Fig. VII.3.2 defines vars and ivals.

Lemma VII.3.4.

1. $\mathsf{vars} : \check{\mathbb{C}} \cup \hat{\mathbb{C}} \to 2^{\mathbb{Z}}$

2. $z\!:\!\check{D} \in \check{C}$ **impl.** $z \in \mathsf{vars}(\check{C})$

Lemma VII.3.5.

1. $\mathsf{ivals} : \check{\mathbb{C}} \cup \hat{\mathbb{C}} \to 2^{\check{\mathbb{D}}} \cup 2^{\hat{\mathbb{D}}}$

2. $z\!:\!\check{D} \in \check{C}$ **impl.** $\check{D} \in \mathsf{ivals}(\check{C})$

VII.3.2 Parameter Instantiation

Definition VII.3.5. Let $\mathbf{\Psi} = \mathbb{K} \rightharpoonup \mathbb{A}$ denote the set of all *parameter substitutions*, ranged over by ψ. Let $2^{\mathbf{\Psi}}$ denote the set of all *sets of parameter substitutions*, ranged over by Ψ.

Definition VII.3.6. Let $\check{E} \langle\!\langle\psi\rangle\!\rangle$, $\check{D} \langle\!\langle\psi\rangle\!\rangle$, $\check{C} \langle\!\langle\psi\rangle\!\rangle$, and $z \langle\!\langle\psi\rangle\!\rangle$ denote the *parameter instantiation* of $\check{E}$, $\check{D}$, $\check{C}$, and z with ψ. Fig. VII.3.3 defines $\cdot \langle\!\langle\cdot\rangle\!\rangle$.

$$
\begin{aligned}
[\![\hat{E}_1\mathsf{+}\hat{E}_2]\!] &= [\![\hat{E}_1]\!] + [\![\hat{E}_2]\!] \\
[\![\hat{E}_1\mathsf{-}\hat{E}_2]\!] &= [\![\hat{E}_1]\!] + (-[\![\hat{E}_2]\!]) \\
[\![a]\!] &= a \\
[\![\hat{E}^{\mathsf{lo}}\,..\,\hat{E}^{\mathsf{hi}}]\!] &= \{\tilde{a} \mid [\![\hat{E}^{\mathsf{lo}}]\!] \preceq \tilde{a} \preceq [\![\hat{E}^{\mathsf{hi}}]\!]\} \\
[\![\{z_i : \hat{D}_i\}_{i\in I}]\!] &= \{z_i \mapsto [\![\hat{D}_i]\!] \mid i \in I\} \\
[\![z]\!] &= z
\end{aligned}
$$

Fig. VII.3.4. Denotation (closed rank expressions, closed intervals, closed iterators, rank variables)

Lemma VII.3.6.

1. $\cdot\,\langle\!\langle\cdot\rangle\!\rangle : (\check{\mathbb{E}} \cup \check{\mathbb{D}} \cup \check{\mathbb{C}} \cup \mathbb{Z}) \times \boldsymbol{\Psi} \to \check{\mathbb{E}} \cup \check{\mathbb{D}} \cup \check{\mathbb{C}} \cup \mathbb{Z}$
2. $\hat{E}\,\langle\!\langle\psi\rangle\!\rangle = \hat{E}$
3. $\check{E}\,\langle\!\langle\psi_1\rangle\!\rangle\,\langle\!\langle\psi_2\rangle\!\rangle = \check{E}\,\langle\!\langle\psi_1 \cup (\psi_2 \setminus \{k \mapsto \psi_2(k) \mid k \in (\operatorname{dom}\psi_1) \cap (\operatorname{dom}\psi_2)\})\rangle\!\rangle$
4. $\hat{C}\,\langle\!\langle\psi\rangle\!\rangle = \hat{C}$
5. $\check{C}\,\langle\!\langle\psi_1\rangle\!\rangle\,\langle\!\langle\psi_2\rangle\!\rangle = \check{C}\,\langle\!\langle\psi_1 \cup (\psi_2 \setminus \{k \mapsto \psi_2(k) \mid k \in (\operatorname{dom}\psi_1) \cap (\operatorname{dom}\psi_2)\})\rangle\!\rangle$
6. $\check{C} = \emptyset$ **impl.** $\check{C}\,\langle\!\langle\psi\rangle\!\rangle = \emptyset$
7. $\check{C} \neq \emptyset$ **impl.** $\check{C}\,\langle\!\langle\psi\rangle\!\rangle \neq \emptyset$
8. $(\check{C}_1 \cup \check{C}_2)\,\langle\!\langle\psi\rangle\!\rangle = (\check{C}_1\,\langle\!\langle\psi\rangle\!\rangle) \cup (\check{C}_2\,\langle\!\langle\psi\rangle\!\rangle)$
9. $(\check{C}_1 \setminus \check{C}_2)\,\langle\!\langle\psi\rangle\!\rangle = (\check{C}_1\,\langle\!\langle\psi\rangle\!\rangle) \setminus (\check{C}_2\,\langle\!\langle\psi\rangle\!\rangle)$
10. $\{\tilde{z} : \tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}\,\langle\!\langle\psi\rangle\!\rangle = \{\tilde{z} : \tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \in \check{C}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \in \{\tilde{\tilde{\check{D}}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\tilde{\check{D}}} \in \check{\mathcal{D}}\}\}$
11. $\hat{x}\,\langle\!\langle\psi\rangle\!\rangle = \hat{x}$
12. $\check{x}\,\langle\!\langle\psi_1\rangle\!\rangle\,\langle\!\langle\psi_2\rangle\!\rangle = \check{x}\,\langle\!\langle\psi_1 \cup (\psi_2 \setminus \{k \mapsto \psi_2(k) \mid k \in (\operatorname{dom}\psi_1) \cap (\operatorname{dom}\psi_2)\})\rangle\!\rangle$

VII.3.3 Semantics

Definition VII.3.7. Let $[\![\hat{E}]\!]$, $[\![\hat{D}]\!]$, $[\![\hat{C}]\!]$, and $[\![z]\!]$ denote the *denotation* of $\hat{E}$ (as a rank), $\hat{D}$ (as a set of ranks, ordered by $<$), $\hat{C}$ (as a family of sets of ranks, ordered by $<$), and z (as a rank variable). Fig. VII.3.4 defines $[\![\cdot]\!]$.

Lemma VII.3.7.

1. $[\![\cdot]\!] : \hat{\mathbb{E}} \cup \hat{\mathbb{D}} \cup \hat{\mathbb{C}} \cup \mathbb{Z} \to \mathbb{A} \cup 2^{\mathbb{A}} \cup \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle \cup \mathbb{Z}$
2. $\Big[z : \hat{D} \in \hat{C}$ **impl.** $z \in \operatorname{dom}[\![\hat{C}]\!]\Big]$ **and** $\Big[\Big[z \in \operatorname{dom}[\![\hat{C}]\!]$ **impl.** $z : \hat{D} \in \hat{C}\Big]$ **for-some** $\hat{D}\Big]$
3. $\Big[z : \hat{D} \in \hat{C}$ **impl.** $[\![\hat{C}]\!](z) = [\![\hat{D}]\!]\Big]$ **and** $\Big[[\![\hat{C}]\!](z) = [\![\hat{D}]\!]$ **impl.** $z : \hat{D} \in \hat{C}\Big]$
4. $\hat{C}_1 \cup \hat{C}_2 \in \operatorname{dom}[\![\cdot]\!]$ **impl.** $[\![\hat{C}_1 \cup \hat{C}_2]\!] = [\![\hat{C}_1]\!] \cup [\![\hat{C}_2]\!]$

$$\begin{aligned}
\Delta(\check{E}_1, \check{E}_2) &= \check{E}_2 \text{-} \check{E}_1 \\
\Delta(\check{E}_1^{\mathsf{lo}} \mathinner{..} \check{E}_1^{\mathsf{hi}}, \check{E}_2^{\mathsf{lo}} \mathinner{..} \check{E}_2^{\mathsf{hi}}) &= \Delta(\check{E}_1^{\mathsf{lo}}, \check{E}_2^{\mathsf{lo}}) \\
\Delta(\{z_i : \check{D}_i\}_{i \in I}) &= \{\langle z_{i_1}, z_{i_2}\rangle \mapsto \Delta(\check{D}_{i_1}, \check{D}_{i_2}) \mid i_1, i_2 \in I\} \\[1ex]
\nabla(\check{E}^{\mathsf{lo}} \mathinner{..} \check{E}^{\mathsf{hi}}) &= \Delta(\check{E}^{\mathsf{lo}}, \check{E}^{\mathsf{hi}})
\end{aligned}$$

Fig. VII.3.5. Distance (open rank expressions, open intervals, open iterators), gradient (open intervals)

$$\begin{tikzcd}
\check{\mathbb{E}} \times \check{\mathbb{E}} \arrow[r, "\cdot\, \langle\!\langle \psi \rangle\!\rangle"] \arrow[d, "\Delta"] \arrow[dr, phantom, "\circlearrowright"] & \hat{\mathbb{E}} \times \hat{\mathbb{E}} \arrow[r, "{[\![\cdot]\!]}"] \arrow[d, "\Delta"] \arrow[dr, phantom, "\circlearrowright"] & \mathbb{A} \times \mathbb{A} \arrow[d, "\delta"] \\
\check{\mathbb{E}} \arrow[r, "\cdot\, \langle\!\langle \psi \rangle\!\rangle"] & \hat{\mathbb{E}} \arrow[r, "{[\![\cdot]\!]}"] & \mathbb{A}
\end{tikzcd}$$

Fig. VII.3.6. Theorem VII.3.2

5. $\left[\hat{C}_1 \cup \hat{C}_2 \in \operatorname{dom} [\![\cdot]\!] \ \textsf{and}\ z \in \operatorname{dom} [\![\hat{C}_1]\!]\right]$ **impl.** $[\![\hat{C}_1 \cup \hat{C}_2]\!](z) = [\![\hat{C}_1]\!](z)$

6. $[\![\hat{C} \setminus \{z : \hat{D}\}]\!] = [\![\hat{C}]\!] \setminus \{z \mapsto [\![\hat{D}]\!]\}$

Theorem VII.3.1. $\operatorname{dom} [\![\hat{C}]\!] = \mathsf{vars}(\hat{C})$

Proof. See Section VIII.10. □

VII.3.4 Distances

Definition VII.3.8. Let $\Delta(\check{E}_1, \check{E}_2)$, $\Delta(\check{D}_1, \check{D}_2)$, and $\Delta(\check{C})$ denote the *distance* from $\check{E}_1$ to $\check{E}_2$, the *distance* from $\check{D}_1$ to $\check{D}_2$, and the *distance matrix* of $\check{C}$. Let $\nabla(D)$ denote the *gradient* of D. Fig. VII.3.5 defines Δ and ∇.

Lemma VII.3.8. $\Delta : (\check{\mathbb{E}} \times \check{\mathbb{E}}) \times (\check{\mathbb{D}} \times \check{\mathbb{D}}) \times (\check{\mathbb{C}} \times \check{\mathbb{C}}) \to \check{\mathbb{E}} \cup \check{\mathbb{E}} \cup (\mathbb{Z} \times \mathbb{Z} \rightharpoonup \check{\mathbb{E}})$

Lemma VII.3.9. $\nabla : \check{\mathbb{D}} \to \check{\mathbb{E}}$

Theorem VII.3.2. *The diagram in Fig. VII.3.6 commutes:*

1. $\Delta(\check{E}_1, \check{E}_2) \,\langle\!\langle \psi \rangle\!\rangle = \Delta(\check{E}_1 \,\langle\!\langle \psi \rangle\!\rangle, \check{E}_2 \,\langle\!\langle \psi \rangle\!\rangle)$

2. $[\![\Delta(\hat{E}_1, \hat{E}_2)]\!] = \delta([\![\hat{E}_1]\!], [\![\hat{E}_2]\!])$

Proof. See Section VIII.11. □

Theorem VII.3.3. *The diagram in Fig. VII.3.7 commutes.*

1. $\Delta(\check{D}_1, \check{D}_2) \,\langle\!\langle \psi \rangle\!\rangle = \Delta(\check{D}_1 \,\langle\!\langle \psi \rangle\!\rangle, \check{D}_2 \,\langle\!\langle \psi \rangle\!\rangle)$

2. $[\![\nabla(\hat{D}_1)]\!] = [\![\nabla(\hat{D}_2)]\!] \preceq^{\text{-}1} 0$ **impl.** $[\![\Delta(\hat{D}_1, \hat{D}_2)]\!] = \delta([\![\hat{D}_1]\!], [\![\hat{D}_2]\!])$

Proof. See Section VIII.12. □

Theorem VII.3.4. $\langle z_1, z_2 \rangle \in \operatorname{dom} \Delta(\check{C})$ **impl.** $\Delta(\check{C})(z_1, z_2) \,\langle\!\langle \psi \rangle\!\rangle = \Delta(\check{C} \,\langle\!\langle \psi \rangle\!\rangle)(z_1, z_2)$

Proof. See Section VIII.13. □

$$\begin{tikzcd}
\check{\mathbb{D}} \times \check{\mathbb{D}} \arrow[r, "\cdot \langle\!\langle\psi\rangle\!\rangle"] \arrow[d, "\Delta"] \arrow[dr, phantom, "\circlearrowright"] & \hat{\mathbb{D}} \times \hat{\mathbb{D}} \arrow[r, "\llbracket\cdot\rrbracket"] \arrow[d, "\Delta"] \arrow[dr, phantom, "\circlearrowright"] & 2^{\mathbb{A}} \times 2^{\mathbb{A}} \arrow[d, "\delta"] \\
\check{\mathbb{D}} \arrow[r, "\cdot \langle\!\langle\psi\rangle\!\rangle"] & \hat{\mathbb{D}} \arrow[r, "\llbracket\cdot\rrbracket"] & \mathbb{A}
\end{tikzcd}$$

Fig. VII.3.7. Theorem VII.3.3

$$\frac{\left[\check{E}_1^{\mathsf{lo}} \langle\!\langle\psi\rangle\!\rangle, \check{E}_1^{\mathsf{lo}} \langle\!\langle\psi\rangle\!\rangle \in \hat{\mathbb{E}} \ \textsf{\textbf{impl.}}\ \llbracket\check{E}_1^{\mathsf{lo}} \langle\!\langle\psi\rangle\!\rangle\rrbracket < \llbracket\check{E}_2^{\mathsf{lo}} \langle\!\langle\psi\rangle\!\rangle\rrbracket\right] \ \textsf{\textbf{for-all}}\ \psi}{z_1 : \check{E}_1^{\mathsf{lo}} \mathinner{\ldotp\ldotp} E_1^{\mathsf{hi}} \ll z_2 : E_2^{\mathsf{lo}} \mathinner{\ldotp\ldotp} \check{E}_2^{\mathsf{hi}}}$$

Fig. VII.3.8. Arrangement (open iterators)

$$\frac{\begin{array}{c} \llbracket\nabla(\hat{D}_{i_1})\rrbracket = \llbracket\nabla(\hat{D}_{i_2})\rrbracket \preceq^{\text{-1}} 0 \ \textsf{\textbf{for-all}}\ i_1, i_2 \in I \\ \left[z_{i_1} \neq z_{i_2} \ \textsf{\textbf{impl.}}\ \llbracket\Delta(\hat{D}_{i_1}, \hat{D}_{i_2})\rrbracket \neq 0\right] \ \textsf{\textbf{for-all}}\ i_1, i_2 \in I \\ \langle\{z_i : \hat{D}_i\}_{i \in I}, \ll\rangle \text{ is a strictly totally ordered set} \end{array}}{\{z_i : \hat{D}_i\}_{i \in I} \in \checkmark}$$

Fig. VII.3.9. Tick (closed iterators)

VII.3.5 Arrangement

Definition VII.3.9. Let $z_1 : \check{D}_1 \ll z_2 : \check{D}_2$ denote the *arrangement* of $z_1 : \check{D}_1$ before $z_2 : \check{D}_2$. Fig. VII.3.8 defines $\ll$.

Theorem VII.3.5. $z : \check{D} = \max \langle \check{C}, \ll \rangle$ **impl.** $z : \check{D} \langle\!\langle\psi\rangle\!\rangle = \max \langle \check{C} \langle\!\langle\psi\rangle\!\rangle, \ll \rangle$

Proof. See Section VIII.14. □

VII.3.6 Tick

Definition VII.3.10. Let $\checkmark$ denote the set of all *ticked* iterators. Fig. VII.3.9 defines $\checkmark$.

Lemma VII.3.10.

1. $\checkmark \subseteq \hat{\mathbb{C}}$
2. $\left[\hat{C} \in \checkmark\right.$ **and** $\left.z_1 : \hat{D}_1, z_2 : \hat{D}_2 \in \hat{C}\right]$ **impl.** $\llbracket\nabla(\hat{D}_1)\rrbracket = \llbracket\nabla(\hat{D}_2)\rrbracket \preceq^{\text{-1}} 0$
3. $\left[\hat{C} \in \checkmark\right.$ **and** $z_1 : \hat{D}_1, z_2 : \hat{D}_2 \in \hat{C}$ **and** $\left.z_1 \neq z_2\right]$ **impl.** $\llbracket\Delta(\hat{D}_1, \hat{D}_2)\rrbracket \neq 0$
4. $\hat{C}_1 \cup \hat{C}_2 \in \checkmark$ **impl.** $\hat{C}_1 \in \checkmark$
5. $\hat{C}_1 \in \checkmark$ **impl.** $\hat{C}_1 \setminus \hat{C}_2 \in \checkmark$

Theorem VII.3.6. $\hat{C} \in \checkmark$ **impl.** $\mathsf{len}\, \llbracket\hat{C}\rrbracket > \mathsf{0}$

Proof. See Section VIII.15. □

Theorem VII.3.7.

1. $\hat{C} \in \checkmark$ **impl.** $\operatorname{dom} \delta[\![\hat{C}]\!] = \operatorname{dom} \Delta(\hat{C})$

2. $\hat{C} \in \checkmark$ **impl.** $\operatorname{dom} \delta[\![\hat{C}]\!] = \mathsf{vars}(\hat{C}) \times \mathsf{vars}(\hat{C})$

3. $\Big[\langle z_1, z_2\rangle \in \operatorname{dom} \delta[\![\hat{C}]\!]$ **and** $\hat{C} \in \checkmark\Big]$ **impl.** $\delta[\![\hat{C}]\!](z_1, z_2) = [\![\Delta(\hat{C})(z_1, z_2)]\!]$

4. $\Big[\langle z_1, z_2\rangle \in \operatorname{dom} \delta[\![\hat{C}]\!]$ **and** $z_1 = z_2$ **and** $\hat{C} \in \checkmark\Big]$ **impl.** $\delta[\![\hat{C}]\!](z_1, z_2) = 0$

5. $\Big[\langle z_1, z_2\rangle \in \operatorname{dom} \delta[\![\hat{C}]\!]$ **and** $z_1 \neq z_2$ **and** $\hat{C} \in \checkmark\Big]$ **impl.** $\delta[\![\hat{C}]\!](z_1, z_2) \neq 0$

Proof. See Section VIII.16. □

Theorem VII.3.8.

1. $\Big[\hat{C} \in \checkmark$ **and** $z_1 : \hat{D}_1, z_2 : \hat{D}_2 \in \hat{C}$ **and** $z_1 : \hat{D}_1 \ll z_2 : \hat{D}_2\Big]$ **impl.** $[\![\hat{C}]\!](z_1) < [\![\hat{C}]\!](z_2)$

2. $\Big[\hat{C} \in \checkmark$ **and** $z : \hat{D} = \min \langle \hat{C}, \ll\rangle\Big]$ **impl.** $[\![\hat{C}]\!](z) = \min \langle \operatorname{img} [\![\hat{C}]\!], <\rangle$

3. $\Big[\hat{C} \in \checkmark$ **and** $z : \hat{D} = \max \langle \hat{C}, \ll\rangle\Big]$ **impl.** $[\![\hat{C}]\!](z) = \max \langle \operatorname{img} [\![\hat{C}]\!], <\rangle$

Proof. See Section VIII.17. □

VII.4 Non-Parametrised Theory (Syntax; Well-Formedness; Unfolding)

VII.4.1 Syntax

Definition VII.4.1. Let $\mathbb{R}$ denote the set of all *role names*, ranged over by r. Let $2^{\mathbb{R}}$ denote the set of all *sets of role names*, ranged over by R. Let $\boldsymbol{\mathcal{L}}$ denote the set of all *labels*, ranged over by ℓ. Let $\mathbb{X}$ denote the set of all *type constants*, ranged over by X, Y. Let $\mathtt{end}, \mathtt{cont} \in \mathbb{X}$ denote distinguished type constants.

Definition VII.4.2. Let $\mathbb{G}$ denote the set of all *basic global types*, ranged over by G. Let $\mathbb{L}$ denote the set of all *basic local types*, ranged over by L. Let $\mathbb{Q}$ denote the set of all *queues*, ranged over by Q. Fig. VII.4.1 defines $\mathbb{G}$, $\mathbb{L}$, and $\mathbb{Q}$.

Definition VII.4.3. Let $\mathbb{G}_{\mathtt{rec}} = \{\mathtt{rec}\ \tilde{X}\ \tilde{G} \mid \tilde{X} \in \mathbb{X}$ **and** $\tilde{G} \in \mathbb{G}\}$ denote the set of all *recursive basic global types*. Let $\mathbb{G} \cup \mathbb{L}$ denote the set of all *basic types*, ranged over by T. Let $\dot{\mathbb{R}} = \mathbb{R} \times \mathbb{A}$ denote the set of all *ranked role names*, ranged over by $\dot{r}_1, \dot{r}_2, \dot{r}$; we shall write $r[a]$ instead of $\langle r, a\rangle$. Let $\ddot{\mathbb{R}} = \mathbb{R} \times \mathbb{Z}$ denote the set of all *iterated role names*, ranged over by $\ddot{r}_1, \ddot{r}_2, \ddot{r}$; we shall write $r[z]$ instead of $\langle r, z\rangle$. Let $\mathbb{A}\mathrm{ct} = (\mathbb{R} \times \mathbb{A}) \times (\mathbb{R} \times \mathbb{A}) \times \{\,\mathbf{!}\,,\,\mathbf{?}\} \times \boldsymbol{\mathcal{L}}$ denote the set of all *actions*, ranged over by α; we shall write $\dot{r}_1\dot{r}_2\,\mathbf{!}\,\ell$ and $\dot{r}_1\dot{r}_2\,\mathbf{?}\ell$ instead of $\langle \dot{r}_1, \dot{r}_2,\ \mathbf{!}\,, \ell\rangle$ and $\langle \dot{r}_1, \dot{r}_2,\ \mathbf{?}, \ell\rangle$.

VII.4.2 Well-formedness

Definition VII.4.4. Let $\mathsf{Wf}_{f,\mathcal{X}}(T)$ denote the *well-formedness* of T. Fig. VII.4.2 defines Wf.

Lemma VII.4.1.

1. $\mathsf{Wf}_{f \cup g,\mathcal{X}}(T)$ **impl.** $\mathsf{Wf}_{f,\mathcal{X}}(T)$

2. $\mathsf{Wf}_{f,\mathcal{X}}(T)$ **impl.** $\mathsf{Wf}_{f,\mathcal{X} \cup \mathcal{Y}}(T)$

$$\begin{array}{rcll}
G \in \mathbb{G} & ::= & r_1[x_1] \rightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I} & \\
& \mid & \mathtt{\textbf{rec}}\ X\ G \quad \textsf{\textbf{if:}}\ X \notin \{\mathtt{\textbf{end}}, \mathtt{\textbf{cont}}\} & \\
& \mid & X & \\
\\
L \in \mathbb{L} & ::= & r_2[x_2]\, !\{\ell_i \,.\, L_i\}_{i \in I} & \\
& \mid & r_1[x_1]\, ?\{\ell_i \,.\, L_i\}_{i \in I} & \\
& \mid & \mathtt{\textbf{rec}}\ X\ L \quad \textsf{\textbf{if:}}\ X \notin \{\mathtt{\textbf{end}}, \mathtt{\textbf{cont}}\} & \\
& \mid & X & \\
\\
Q \in \mathbb{Q} & ::= & \ell.Q & \\
& \mid & \varepsilon &
\end{array}$$

Fig. VII.4.1. Basic global types, basic local types, queues

$$\frac{r_1 \in \operatorname{dom} f\ \textsf{\textbf{impl.}}\ x_1 \in f(r_1) \qquad r_2 \in \operatorname{dom} f\ \textsf{\textbf{impl.}}\ x_2 \in f(r_2) \qquad \mathsf{Wf}_{f,\mathcal{X}}(G_i)\ \textsf{\textbf{for-all}}\ i \in I}{\mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \rightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I})}$$

$$\frac{r_2 \in \operatorname{dom} f\ \textsf{\textbf{impl.}}\ x_2 \in f(r_2) \qquad \mathsf{Wf}_{f,\mathcal{X}}(L_i)\ \textsf{\textbf{for-all}}\ i \in I}{\mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\, !\{\ell_i \,.\, L_i\}_{i \in I})}$$

$$\frac{r_1 \in \operatorname{dom} f\ \textsf{\textbf{impl.}}\ x_1 \in f(r_1) \qquad \mathsf{Wf}_{f,\mathcal{X}}(L_i)\ \textsf{\textbf{for-all}}\ i \in I}{\mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\, ?\{\ell_i \,.\, L_i\}_{i \in I})}$$

$$\frac{\mathsf{Wf}_{f,\mathcal{X} \cup \{X\}}(T)}{\mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\textbf{rec}}\ X\ T)} \qquad \frac{X \in \mathcal{X}}{\mathsf{Wf}_{f,\mathcal{X}}(X)}$$

Fig. VII.4.2. Well-formedness (basic global types, basic local types)

VII.4.3 Unfolding

Definition VII.4.5. Let $T\,\{T_Y/Y\}$ denote the *unfolding* of every Y to T_Y in T. Fig. VII.4.3 defines $\cdot\,\{\cdot/\cdot\}$.

Lemma VII.4.2.

1. $\cdot\,\{\cdot/\cdot\} : (\mathbb{G} \cup \mathbb{L}) \times (\mathbb{G} \cup \mathbb{L}) \times \mathbb{X} \to \mathbb{G} \cup \mathbb{L}$
2. $T\,\{Y/Y\} = T$
3. $Y_1 = Y_2$ **impl.** $T\,\{T_1/Y_1\}\,\{T_2/Y_2\} = T\,\{T_1\,\{T_2/Y_2\}/Y_1\}$
4. $Y_1 \neq Y_2$ **impl.** $T\,\{T_1/Y_1\}\,\{T_2/Y_2\} = T\,\{T_2/Y_2\}\,\{T_1\,\{T_2/Y_2\}/Y_1\}$

Theorem VII.4.1.

1. $\Big[\mathsf{Wf}_{f,\mathcal{X}}(T)\ \textsf{\textbf{and}}\ \mathsf{Wf}_{f,\mathcal{X}}(T_Y)\Big]\ \textsf{\textbf{impl.}}\ \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_Y/Y\})$
2. $\Big[\mathsf{Wf}_{f,\mathcal{X} \cup \{\mathtt{\textbf{cont}}\}}(T)\ \textsf{\textbf{and}}\ \mathsf{Wf}_{f,\mathcal{X}}(T_{\mathtt{\textbf{cont}}})\Big]\ \textsf{\textbf{impl.}}\ \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_{\mathtt{\textbf{cont}}}/\mathtt{\textbf{cont}}\})$

$$
\begin{aligned}
r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I}\,\{T_Y/Y\} &= r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\,\{T_Y/Y\}\}_{i \in I}\\
r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\!\{\ell \,.\, G\}\!\}\,\{T_Y/Y\} &= r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\!\{\ell \,.\, G\,\{T_Y/Y\}\}\!\}\\
r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\}_{i \in I}\,\{T_Y/Y\} &= r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\,\{T_Y/Y\}\}_{i \in I}\\
r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i \in I}\,\{T_Y/Y\} &= r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\,\{T_Y/Y\}\}_{i \in I}\\
\mathtt{rec}\ X\ T\,\{T_Y/Y\} &= \begin{cases} \mathtt{rec}\ X\ T & \textsf{if: } X = Y\\ \mathtt{rec}\ X\ (T\,\{T_Y/Y\}) & \textsf{if: } X \neq Y \end{cases}\\
X\,\{T_Y/Y\} &= \begin{cases} T_Y & \textsf{if: } X = Y\\ X & \textsf{if: } X \neq Y \end{cases}
\end{aligned}
$$

Fig. VII.4.3. Unfolding (basic global types, basic local types)

$$
L_1 \sqcap L_2 = \begin{cases}
r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i \in I} & \textsf{if: } L_1 = r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_{i,1}\}_{i \in I} \ \textsf{and}\\
 & \phantom{\textsf{if: }} L_2 = r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_{i,2}\}_{i \in I}\\
r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\}_{i \in I_1 \setminus I_2} \cup & \textsf{if: } L_1 = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\}_{i \in I_1} \ \textsf{and}\\
\qquad \{\ell_i \,.\, L_{i,2}\}_{i \in I_2 \setminus I_1} \cup & \phantom{\textsf{if: }} L_2 = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,2}\}_{i \in I_2} \ \textsf{and}\\
\qquad \{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i \in I_1 \cap I_2} & \phantom{\textsf{if: }} \left[\ell_{i_1} \neq \ell_{i_2} \ \textsf{for-all}\ i_1 \in I_1 \setminus I_2, i_2 \in I_2 \setminus I_1\right]\\
\mathtt{rec}\ X\ (L_{X,1} \sqcap L_{X,2}) & \textsf{if: } L_1 = \mathtt{rec}\ X\ L_{X,1} \ \textsf{and}\ L_2 = \mathtt{rec}\ X\ L_{X,2}\\
X & \textsf{if: } L_1 = L_2 = X
\end{cases}
$$

Fig. VII.5.1. Merge (basic local types)

Proof. See Section VIII.18. □

Theorem VII.4.2. $\mathsf{Wf}_{f,\mathcal{X}\setminus\{Y\}}(T)$ **impl.** $T\,\{T_Y/Y\} = T$

Proof. See Section VIII.19. □

VII.5 Non-Parametrised Theory (Merge; Projection)

VII.5.1 Merge

Definition VII.5.1. Let $L_1 \sqcap L_2$ denote the *merge* of L_1 and L_2. Fig. VII.5.1 defines $\sqcap$.

Lemma VII.5.1.

1. $\sqcap : \mathbb{L} \times \mathbb{L} \rightharpoonup \mathbb{L}$

2. $L \sqcap L = L$

Theorem VII.5.1.

1. $\langle L_1, L_2 \rangle \in \operatorname{dom} \sqcap$ **impl.** $(L_1 \sqcap L_2)\,\{L/Y\} = L_1\,\{L/Y\} \sqcap L_2\,\{L/Y\}$

2. $\langle L_1, L_2 \rangle \in \operatorname{dom} \sqcap$ **impl.** $L\,\{L_1 \sqcap L_2/Y\} = L\,\{L_1/Y\} \sqcap L\,\{L_2/Y\}$

3. $(L_1 \sqcap L_2)\,\{L_3 \sqcap L_4/Y\} \neq L_1\,\{L_3/Y\} \sqcap L_2\,\{L_4/Y\}$ **for-some** L_1, L_2, L_3, L_4, Y

Proof. See Section VIII.20. □

$$
\begin{aligned}
r_1[x_1] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, G_i\}_{i \in I} \upharpoonright r[a] &= \begin{cases} r_2[x_2] \,\mathbf{!}\, \{\ell_i \,.\, G_i \upharpoonright r[a]\}_{i \in I} & \textsf{\textbf{if:}}\ r_1[x_1] = r[a] \neq r_2[x_2] \\ r_1[x_1] \,\mathbf{?}\{\ell_i \,.\, G_i \upharpoonright r[a]\}_{i \in I} & \textsf{\textbf{if:}}\ r_1[x_1] \neq r[a] = r_2[x_2] \\ \bigsqcap \{G_i \upharpoonright r[a]\}_{i \in I} & \textsf{\textbf{if:}}\ r_1[x_1] \neq r[a] \neq r_2[x_2] \end{cases} \\
\texttt{rec}\ X\ G \upharpoonright r[a] &= \texttt{rec}\ X\ (G \upharpoonright r[a]) \\
X \upharpoonright r[a] &= X
\end{aligned}
$$

Fig. VII.5.2. Projection (basic global types)

$$
\begin{aligned}
r[x] \, (\!(R[\phi])\!) &= \begin{cases} r[\phi(x)] & \textsf{\textbf{if:}}\ r \in R\ \textsf{\textbf{and}}\ x \in \operatorname{dom} \phi \\ r[x] & \textsf{\textbf{if:}}\ r \notin R\ \textsf{\textbf{or}}\ x \notin \operatorname{dom} \phi \end{cases} \\
r_1[x_1] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, G_i\}_{i \in I} \, (\!(R[\phi])\!) &= r_1[x_1] \, (\!(R[\phi])\!) \rightarrowtriangle r_2[x_2] \, (\!(R[\phi])\!) \,\mathbf{:}\, \{\ell_i \,.\, G_i \, (\!(R[\phi])\!)\}_{i \in I} \\
r_2[x_2] \,\mathbf{!}\, \{\ell_i \,.\, L_i\}_{i \in I} \, (\!(R[\phi])\!) &= r_2[x_2] \, (\!(R[\phi])\!) \,\mathbf{!}\, \{\ell_i \,.\, L_i \, (\!(R[\phi])\!)\}_{i \in I} \\
r_1[x_1] \,\mathbf{?}\{\ell_i \,.\, L_i\}_{i \in I} \, (\!(R[\phi])\!) &= r_1[x_1] \, (\!(R[\phi])\!) \,\mathbf{?}\{\ell_i \,.\, L_i \, (\!(R[\phi])\!)\}_{i \in I} \\
\texttt{rec}\ X\ T \, (\!(R[\phi])\!) &= \texttt{rec}\ X\ (T \, (\!(R[\phi])\!)) \\
X \, (\!(R[\phi])\!) &= X
\end{aligned}
$$

Fig. VII.6.1. Variable instantiation (basic global types, basic local types)

VII.5.2 Projection

Definition VII.5.2. Let $G \upharpoonright r[a]$ denote the *projection* of G onto $r[a]$. Fig. VII.5.2 defines $\upharpoonright$.

Lemma VII.5.2. $\upharpoonright : \mathbb{G} \times \dot{\mathbb{R}} \rightharpoonup \mathbb{L}$

Theorem VII.5.2. $\big[\langle G, r[a] \rangle \in \operatorname{dom} \upharpoonright\ \textsf{\textbf{and}}\ \langle G_Y, r[a] \rangle \in \operatorname{dom} \upharpoonright\big]$
$\textsf{\textbf{impl.}}\ (G \upharpoonright r[a]) \, \{G_Y \upharpoonright r[a] / Y\} = G \, \{G_Y / Y\} \upharpoonright r[a]$

Proof. See Section VIII.21. □

VII.6 Non-Parametrised Theory (Variable Instantiation; Iteration)

VII.6.1 Variable Instantiation

Definition VII.6.1. Let $r[x] \, (\!(R[\phi])\!)$ and $T \, (\!(R[\phi])\!)$ denote the *variable instantiation* of $r[x]$ and T under $R[\phi]$. Fig. VII.6.1 defines $\cdot \, (\!(\cdot)\!)$.

Lemma VII.6.1. $\cdot \, (\!(\cdot)\!) : ((\mathbb{R} \times (\check{\mathbb{E}} \cup \mathbb{Z})) \cup \mathbb{G} \cup \mathbb{L}) \times (2^{\mathbb{R}} \times \operatorname{fam} \langle \mathbb{Z}, \mathbb{A} \rangle) \to (\mathbb{R} \times (\check{\mathbb{E}} \cup \mathbb{Z})) \cup \mathbb{G} \cup \mathbb{L}$

Theorem VII.6.1. $\textsf{Wf}_{f,\mathcal{X}}(T)\ \textsf{\textbf{impl.}}\ \textsf{Wf}_{f,\mathcal{X}}(T \, (\!(R[\phi])\!))$

Proof. See Section VIII.22. □

Theorem VII.6.2. $T \, (\!(R[\phi])\!) \, \{T_Y \, (\!(R[\phi])\!) / Y\} = T \, \{T_Y / Y\} \, (\!(R[\phi])\!)$

Proof. See Section VIII.23. □

Theorem VII.6.3. $\langle L_1, L_2 \rangle \in \operatorname{dom} \sqcap\ \textsf{\textbf{impl.}}\ (L_1 \sqcap L_2) \, (\!(R[\phi])\!) = L_1 \, (\!(R[\phi])\!) \sqcap L_2 \, (\!(R[\phi])\!)$

$$\mathsf{iter}(T_1, T_2, R, \Phi) = \begin{cases} T_1 \left(\!\left(R[\mathsf{head}\,\Phi]\right)\!\right) \{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)/\mathbf{cont}\} & \textbf{if: } \mathsf{len}\,\Phi > 0 \\ T_2 & \textbf{if: } \mathsf{len}\,\Phi = 0 \end{cases}$$

Fig. VII.6.2. Iteration (basic global types, basic local types)

Proof. See Section VIII.24. □

Theorem VII.6.4. $\left[\langle G, r[a]\rangle \in \mathrm{dom} \restriction \ \textbf{and} \ r \notin R\right]$ **impl.** $(G \restriction r[a]) \left(\!\left(R[\phi]\right)\!\right) = G \left(\!\left(R[\phi]\right)\!\right) \restriction r[a]$

Proof. See Section VIII.25. □

Theorem VII.6.5.

1. $R \cap R' = \emptyset$ **impl.** $x \left(\!\left(R[\phi]\right)\!\right) \left(\!\left(R'[\phi']\right)\!\right) = x \left(\!\left(R'[\phi']\right)\!\right) \left(\!\left(R[\phi]\right)\!\right)$

2. $R \cap R' = \emptyset$ **impl.** $T \left(\!\left(R[\phi]\right)\!\right) \left(\!\left(R'[\phi']\right)\!\right) = T \left(\!\left(R'[\phi']\right)\!\right) \left(\!\left(R[\phi]\right)\!\right)$

Proof. See Section VIII.26. □

Theorem VII.6.6. $\left[\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathrm{dom}\,\phi \mid \tilde{r} \in R\}, \mathcal{X}}(G) \ \textbf{and} \ (\mathrm{expr}\, G) \cap \mathbb{G}_{\mathbf{rec}} = \emptyset \ \textbf{and} \ r \in R \ \textbf{and} \ a \notin \mathrm{img}\,\phi\right]$
impl. $\left[\mathbf{cont} = G \restriction r[a] \ \textbf{and} \ \mathbf{cont} = G \left(\!\left(R[\phi]\right)\!\right) \restriction r[a]\right]$

Proof. See Section VIII.27. □

VII.6.2 Iteration

Definition VII.6.2. Let $\mathsf{iter}(T_1, T_2, R, \Phi)$ denote the *iteration* over Φ of T_1, followed by T_2. Fig. VII.6.2 defines iter.

Lemma VII.6.2.

1. $\mathsf{iter} : (\mathbb{G} \cup \mathbb{L}) \times (\mathbb{G} \cup \mathbb{L}) \times 2^{\mathbb{R}} \times \mathrm{fam}\,\langle \mathbb{Z}, 2^{\mathbb{A}}\rangle \to \mathbb{G} \cup \mathbb{L}$

2. $\Phi \in \mathrm{dom}\,\mathsf{len}$ **impl.** $\mathsf{iter}(T_1, \mathbf{cont}, R, \Phi) \{T_2/\mathbf{cont}\} = \mathsf{iter}(T_1, T_2, R, \Phi)$

Theorem VII.6.7.

$\left[\langle \Phi, z[a]\rangle \in \mathrm{dom}\ \mathsf{to} \ \textbf{and} \ \langle \Phi, z[a]\rangle \in \mathrm{dom}\ \mathsf{from}\right]$
impl. $\mathsf{iter}(T, \mathbf{cont}, R, \Phi\ \mathsf{to}\ z[a]) \{\mathsf{iter}(T, \mathbf{cont}, R, \Phi\ \mathsf{from}\ z[a])/\mathbf{cont}\} = \mathsf{iter}(T, \mathbf{cont}, R, \Phi)$

Proof. See Section VIII.28. □

Theorem VII.6.8.

1. $\left[\Phi \in \mathrm{dom}\,\mathsf{len} \ \textbf{and} \ \mathsf{Wf}_{f,\mathcal{X}}(T_1) \ \textbf{and} \ \mathsf{Wf}_{f,\mathcal{X}}(T_2)\right]$ **impl.** $\mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(T_1, T_2, R, \Phi))$

2. $\left[\Phi \in \mathrm{dom}\,\mathsf{len} \ \textbf{and} \ \mathsf{Wf}_{f,\{\mathbf{cont}\}}(T_1) \ \textbf{and} \ \mathsf{Wf}_{f,\mathcal{X}}(T_2)\right]$ **impl.** $\mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(T_1, T_2, R, \Phi))$

Proof. See Section VIII.29. □

Theorem VII.6.9. $\left[\Phi \in \mathrm{dom}\,\mathsf{len} \ \textbf{and} \ \mathsf{Wf}_{f,\{\mathbf{cont}\}}(T_1)\right]$
impl. $\mathsf{iter}(T_1, T_2, R, \Phi) \{T_Y/Y\} = \mathsf{iter}(T_1, T_2 \{T_Y/Y\}, R, \Phi)$

Proof. See Section VIII.30. □

Theorem VII.6.10.

1. $\mathsf{iter}(L_1 \sqcap L_2, L, R, \Phi) \neq \mathsf{iter}(L_1, L, R, \Phi) \sqcap \mathsf{iter}(L_2, L, R, \Phi)$ **for-some** L, L_1, L_2, R, Φ

2. $\Big[\langle L_1, L_2 \rangle \in \operatorname{dom} \sqcap$ **and** $\Phi \in \operatorname{dom} \mathsf{len}\Big]$
   impl. $\mathsf{iter}(L, L_1 \sqcap L_2, R, \Phi) = \mathsf{iter}(L, L_1, R, \Phi) \sqcap \mathsf{iter}(L, L_2, R, \Phi)$

Proof. See Section VIII.31. □

Theorem VII.6.11. $\Big[\langle G_1, r[a] \rangle \in \operatorname{dom} \upharpoonright$ **and** $\langle G_2, r[a] \rangle \in \operatorname{dom} \upharpoonright$ **and** $\Phi \in \operatorname{dom} \mathsf{len}$ **and** $r \notin R\Big]$
impl. $\mathsf{iter}(G_1 \upharpoonright r[a], G_2 \upharpoonright r[a], R, \Phi) = \mathsf{iter}(G_1, G_2, R, \Phi) \upharpoonright r[a]$

Proof. See Section VIII.32. □

Theorem VII.6.12. $\Big[\Phi \in \operatorname{dom} \mathsf{len}$ **and** $R \cap R' = \emptyset\Big]$
impl. $\mathsf{iter}(T_1 \,(\!(R'[\phi'])\!), T_2 \,(\!(R'[\phi'])\!), R, \Phi) = \mathsf{iter}(T_1, T_2, R, \Phi) \,(\!(R'[\phi'])\!)$

Proof. See Section VIII.33. □

Theorem VII.6.13. $\Big[\Phi \in \operatorname{dom} \mathsf{len}$ **and** $\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \operatorname{dom} \Phi \mid \tilde{r} \in R\}, \{\mathbf{cont}\}}(G)$ **and** $\operatorname{expr} G \cap \mathbb{G}_{\mathbf{rec}} = \emptyset$ **and** $r \in R$ **and** $a \notin \bigcup \operatorname{img} \Phi\Big]$
impl. $\mathbf{cont} = \mathsf{iter}(G, \mathbf{cont}, R, \Phi) \upharpoonright r[a]$

Proof. See Section VIII.34. □

VII.7 Parametrised Theory (Syntax; Parameter Instantiation; Well-Formedness; Unfolding; Denotation)

VII.7.1 Syntax

Definition VII.7.1. Let $\check{\mathbb{G}}$ and $\hat{\mathbb{G}}$ denote the sets of all *open and closed global types*, ranged over by $\check{G}$ and $\hat{G}$. Let $\check{\mathbb{L}}$ and $\hat{\mathbb{L}}$ denote the sets of all *open and closed local types*, ranged over by $\check{L}$ and $\hat{L}$. Let $\mathring{\cdot}$ range over $\{\check{\cdot}, \hat{\cdot}\}$. Fig. VII.7.1 defines $\check{\mathbb{G}}$, $\hat{\mathbb{G}}$, $\check{\mathbb{L}}$, and $\hat{\mathbb{L}}$.

Definition VII.7.2. Let $\check{\mathbb{G}} \cup \check{\mathbb{L}}$ denote the set of all *open types*, ranged over by $\check{T}$. Let $\hat{\mathbb{G}} \cup \hat{\mathbb{L}}$ denote the set of all *closed types*, ranged over by $\hat{T}$.

Lemma VII.7.1. $\hat{\mathbb{G}} \subseteq \check{\mathbb{G}}$

Lemma VII.7.2. $\hat{\mathbb{L}} \subseteq \check{\mathbb{L}}$

Definition VII.7.3. Let $\mathsf{ivals}(r, \check{T})$ denote the set of all *intervals* that occur in $\check{T}$ with r. Fig. VII.7.2 defines ivals.

Lemma VII.7.3. $\mathsf{ivals} : \mathbb{R} \times (\check{\mathbb{G}} \cup \check{\mathbb{L}}) \to 2^{\mathbb{D}}$

$$\begin{array}{lcll}
\mathring{G} \in \mathring{\mathbb{G}} & ::= & r_1[\mathring{x}_1] \rightarrow r_2[\mathring{x}_2] \,\mathbf{:}\, \{\ell_i \,\mathbf{.}\, \mathring{G}_i\}_{i \in I} & \textbf{if: } \texttt{self} \notin \operatorname{expr} \mathring{x}_1 \textbf{ and } \texttt{self} \notin \operatorname{expr} \mathring{x}_2 \\
 & \mid & \texttt{foreach}\ R[\mathring{C}]\ \texttt{do}\ \mathring{G}_1\ \texttt{;}\ \mathring{G}_2 & \\
 & \mid & \texttt{rec}\ X\ \mathring{G} \quad \textbf{if: } X \notin \{\texttt{end}, \texttt{cont}\} & \\
 & \mid & X & \\
 & & & \\
\mathring{L} \in \mathring{\mathbb{L}} & ::= & r_2[\mathring{x}_2]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, \mathring{L}_i\}_{i \in I} & \\
 & \mid & r_1[\mathring{x}_1]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, \mathring{L}_i\}_{i \in I} & \\
 & \mid & \texttt{foreach}\ R[\mathring{C}]\ \texttt{do}\ \mathring{L}_1\ \texttt{;}\ \mathring{L}_2 & \\
 & \mid & \texttt{rec}\ X\ \mathring{L} \quad \textbf{if: } X \notin \{\texttt{end}, \texttt{cont}\} & \\
 & \mid & X &
\end{array}$$

Fig. VII.7.1. Open/closed global types, open/closed local types

$$\begin{array}{ll}
\mathsf{ivals}(r, r_1[x_1] \rightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,\mathbf{.}\, \check{G}_i\}_{i \in I}) & = \{\check{E} \mathinner{..} \check{E} \mid r[\check{E}] \in \{r_1[x_1], r_2[x_2]\}\} \cup \bigcup \{\mathsf{ivals}(r, \check{G}_i) \mid i \in I\} \\
\mathsf{ivals}(r, r_2[x_2]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, \check{L}_i\}_{i \in I}) & = \{\check{E} \mathinner{..} \check{E} \mid r[\check{E}] \in \{r_2[x_2]\}\} \cup \bigcup \{\mathsf{ivals}(\hat{L}_i) \mid i \in I\} \\
\mathsf{ivals}(r, r_1[x_1]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, \check{L}_i\}_{i \in I}) & = \{\check{E} \mathinner{..} \check{E} \mid r[\check{E}] \in \{r_1[x_1]\}\} \cup \bigcup \{\mathsf{ivals}(\hat{L}_i) \mid i \in I\} \\
\mathsf{ivals}(r, \texttt{foreach}\ R[\check{C}]\ \texttt{do}\ \check{T}_1\ \texttt{;}\ \check{T}_2) & = \begin{cases} \mathsf{ivals}(\check{C}) \cup \mathsf{ivals}(r, \check{T}_1) \cup \mathsf{ivals}(r, \check{T}_2) & \textbf{if: } r \in R \\ \mathsf{ivals}(r, \check{T}_1) \cup \mathsf{ivals}(r, \check{T}_2) & \textbf{if: } r \notin R \end{cases} \\
\mathsf{ivals}(r, \texttt{rec}\ X\ \check{T}) & = \mathsf{ivals}(r, \check{T}) \\
\mathsf{ivals}(r, X) & = \emptyset
\end{array}$$

Fig. VII.7.2. Intervals (open global types, open local types)

VII.7.2 Parameter Instantiation

Definition VII.7.4. Let $\check{T} \langle\!\langle \psi \rangle\!\rangle$ denote the *parameter instantiation* of $\check{T}$ under ψ. Fig. VII.7.3 defines $\cdot \langle\!\langle \cdot \rangle\!\rangle$.

Lemma VII.7.4.

1. $\cdot \langle\!\langle \cdot \rangle\!\rangle : (\check{\mathbb{G}} \cup \check{\mathbb{L}}) \times (\mathbb{K} \rightharpoonup \mathbb{A}) \to \check{\mathbb{G}} \cup \check{\mathbb{L}}$
2. $\hat{T} \langle\!\langle \psi \rangle\!\rangle = \hat{T}$

VII.7.3 Well-formedness

Definition VII.7.5. Let $\mathsf{Wf}_{\Psi}(\check{T})$ and $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T})$ denote the *well-formedness* of $\check{T}$ and $\hat{T}$. Fig. VII.7.4 defines Wf.

Lemma VII.7.5.

1. $\mathsf{Wf}_{f,\mathcal{X}}(\check{T})$ **impl.** $\mathsf{Wf}_{f \backslash g,\mathcal{X}}(\check{T})$
2. $\mathsf{Wf}_{f,\mathcal{X}}(\check{T})$ **impl.** $\mathsf{Wf}_{f,\mathcal{X} \cup \mathcal{Y}}(\check{T})$

$$\begin{aligned}
r_1[x_1] \rightarrow r_2[x_2] \,\texttt{:}\, \{\ell_i \,\texttt{.}\, \check{G}_i\}_{i\in I} \langle\!\langle\psi\rangle\!\rangle &= r_1[x_1 \langle\!\langle\psi\rangle\!\rangle] \rightarrow r_2[x_2 \langle\!\langle\psi\rangle\!\rangle] \,\texttt{:}\, \{\ell_i \,\texttt{.}\, \check{G}_i \langle\!\langle\psi\rangle\!\rangle\}_{i\in I}\\
r_2[x_2] \,\texttt{!}\, \{\ell_i \,\texttt{.}\, \check{L}_i\}_{i\in I} \langle\!\langle\psi\rangle\!\rangle &= r_2[x_2 \langle\!\langle\psi\rangle\!\rangle] \,\texttt{!}\, \{\ell_i \,\texttt{.}\, \check{L}_i \langle\!\langle\psi\rangle\!\rangle\}_{i\in I}\\
r_1[x_1] \,\texttt{?}\, \{\ell_i \,\texttt{.}\, \check{L}_i\}_{i\in I} \langle\!\langle\psi\rangle\!\rangle &= r_1[x_1 \langle\!\langle\psi\rangle\!\rangle] \,\texttt{?}\, \{\ell_i \,\texttt{.}\, \check{L}_i \langle\!\langle\psi\rangle\!\rangle\}_{i\in I}\\
\texttt{foreach}\ R[\check{C}]\ \texttt{do}\ \check{T}_1 \,\texttt{;}\, \check{T}_2 \langle\!\langle\psi\rangle\!\rangle &= \texttt{foreach}\ R[\check{C} \langle\!\langle\psi\rangle\!\rangle]\ \texttt{do}\ (\check{T}_1 \langle\!\langle\psi\rangle\!\rangle) \,\texttt{;}\, (\check{T}_2 \langle\!\langle\psi\rangle\!\rangle)\\
\texttt{rec}\ X\ \check{T} \langle\!\langle\psi\rangle\!\rangle &= \texttt{rec}\ X\ (\check{T} \langle\!\langle\psi\rangle\!\rangle)\\
X \langle\!\langle\psi\rangle\!\rangle &= X
\end{aligned}$$

Fig. VII.7.3. Parameter instantiation (open global types, open local types)

VII.7.4 Unfolding

Definition VII.7.6. Let $\check{T}\,\{\check{T}_Y/Y\}$ denote the *unfolding* of every Y to $\check{T}_Y$ in $\check{T}$. Fig. VII.7.5 defines $\cdot\,\{\cdot/\cdot\}$.

Lemma VII.7.6.

1. $\cdot\,\{\cdot/\cdot\} : (\check{\mathbb{G}} \cup \check{\mathbb{L}}) \times (\check{\mathbb{G}} \cup \check{\mathbb{L}}) \times \mathbb{X} \to \check{\mathbb{G}} \cup \check{\mathbb{L}}$
2. $\check{T}\,\{Y/Y\} = \check{T}$

Theorem VII.7.1. $\check{T} \langle\!\langle\psi\rangle\!\rangle \{\check{T}_Y \langle\!\langle\psi\rangle\!\rangle/Y\} = \check{T}\,\{\check{T}_Y/Y\} \langle\!\langle\psi\rangle\!\rangle$

Proof. See Section VIII.35. □

Theorem VII.7.2. $\left[\mathsf{Wf}_{f,\mathcal{X}}(\hat{T})\ \textsf{\textbf{and}}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y)\right]\ \textsf{\textbf{impl.}}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\})$

Proof. See Section VIII.36. □

VII.7.5 Denotation

Definition VII.7.7. Let $[\![\hat{T}]\!]$ denote the *denotation* of $\hat{T}$, as a basic global or local type. Fig. VII.7.6 defines $[\![\cdot]\!]$.

Lemma VII.7.7.

1. $[\![\cdot]\!] : \hat{\mathbb{G}} \cup \hat{\mathbb{L}} \to \mathbb{G} \cup \mathbb{L}$
2. $\operatorname{expr} \hat{G} \cap \mathbb{G}_{\texttt{rec}} = \emptyset\ \textsf{\textbf{impl.}}\ \operatorname{expr} [\![\hat{G}]\!] \cap \mathbb{G}_{\texttt{rec}} = \emptyset$

Theorem VII.7.3. $\left[\mathsf{Wf}_{f,\mathcal{X}}(\hat{T})\ \textsf{\textbf{and}}\ \operatorname{img} f \subseteq 2^{\mathbb{Z}}\right]\ \textsf{\textbf{impl.}}\ \mathsf{Wf}_{f,\mathcal{X}}([\![\hat{T}]\!])$

Proof. See Section VIII.37. □

Theorem VII.7.4. $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T})\ \textsf{\textbf{impl.}}\ [\![\hat{T}\,\{\hat{T}_Y/Y\}]\!] = [\![\hat{T}]\!]\,\{[\![\hat{T}_Y]\!]/Y\}$

Proof. See Section VIII.38. □

$$\frac{\Big[\check{T}\,\langle\!\langle\tilde{\psi}\rangle\!\rangle \in \hat{\mathbb{G}} \cup \hat{\mathbb{L}} \;\;\textsf{\textbf{impl.}}\;\; \mathsf{Wf}_{\emptyset,\{\mathtt{\mathbf{end}}\}}(\check{T}\,\langle\!\langle\tilde{\psi}\rangle\!\rangle)\Big] \;\;\textsf{\textbf{for-all}}\;\; \tilde{\psi} \in \Psi}{\mathsf{Wf}_{\Psi}(\check{T})}$$

(a) Open global types, open local types

$$\frac{r_1 \in \operatorname{dom} f \;\;\textsf{\textbf{impl.}}\;\; x_1 \in f(r_1) \qquad r_2 \in \operatorname{dom} f \;\;\textsf{\textbf{impl.}}\;\; x_2 \in f(r_2) \qquad \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i) \;\;\textsf{\textbf{for-all}}\;\; i \in I}{\mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i\in I})}$$

$$\frac{r_2 \in \operatorname{dom} f \;\;\textsf{\textbf{impl.}}\;\; x_2 \in f(r_2) \qquad \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i) \;\;\textsf{\textbf{for-all}}\;\; i \in I}{\mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, \hat{L}_i\}_{i\in I})}$$

$$\frac{r_1 \in \operatorname{dom} f \;\;\textsf{\textbf{impl.}}\;\; x_1 \in f(r_1) \qquad \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i) \;\;\textsf{\textbf{for-all}}\;\; i \in I}{\mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, \hat{L}_i\}_{i\in I})}$$

$$\frac{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} \qquad \hat{C} \in \checkmark \qquad \begin{matrix}\operatorname{expr} \hat{T}_1 \cap \mathbb{G}_{\mathtt{\mathbf{rec}}} = \emptyset \\ \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\mathtt{\mathbf{cont}}\}}(\hat{T}_1)\end{matrix} \qquad \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_2)}{\mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\mathbf{foreach}}\; R[\hat{C}]\; \mathtt{\mathbf{do}}\; \hat{T}_1 \,\mathbf{;}\, \hat{T}_2)}$$

$$\frac{\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T})}{\mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\mathbf{rec}}\; X\; \hat{T})} \qquad \frac{X \in \mathcal{X}}{\mathsf{Wf}_{f,\mathcal{X}}(X)}$$

(b) Closed global types, closed local types

Fig. VII.7.4. Well-formedness (open/closed global types, open/closed local types)

VII.8 Parametrised Theory (Merge; Projection)

VII.8.1 Merge

Definition VII.8.1. Let $\check{L}_1 \sqcap \check{L}_2$ denote the *merge* of $\check{L}_1$ and $\check{L}_2$. Fig. VII.8.1 defines $\sqcap$.

Lemma VII.8.1.

1. $\sqcap : \check{\mathbb{L}} \times \check{\mathbb{L}} \rightharpoonup \check{\mathbb{L}}$
2. $\check{L} \sqcap \check{L} = \check{L}$

Theorem VII.8.1. $\langle \check{L}_1, \check{L}_2\rangle \in \operatorname{dom} \sqcap$ **impl.** $(\check{L}_1 \sqcap \check{L}_2)\,\langle\!\langle\psi\rangle\!\rangle = \check{L}_1\,\langle\!\langle\psi\rangle\!\rangle \sqcap \check{L}_2\,\langle\!\langle\psi\rangle\!\rangle$

Proof. See Section VIII.39. □

Theorem VII.8.2. $\langle \hat{L}_1, \hat{L}_2\rangle \in \operatorname{dom} \sqcap$ **impl.** $[\![\hat{L}_1 \sqcap \hat{L}_2]\!] = [\![\hat{L}_1]\!] \sqcap [\![\hat{L}_2]\!]$

Proof. See Section VIII.40. □

Theorem VII.8.3. $\Big[\langle \hat{L}_1, \hat{L}_2\rangle \in \operatorname{dom} \sqcap$ **and** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1)$ **and** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_2)\Big]$ **impl.** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1 \sqcap \hat{L}_2)$

Proof. See Section VIII.41. □

$$\begin{aligned}
r_1[x_1] \rightarrowtriangle r_2[x_2] \mathbin{\texttt{:}} \{\ell_i \mathbin{\texttt{.}} \check{G}_i\}_{i \in I} \,\{\check{T}_Y / Y\} &= r_1[x_1] \rightarrowtriangle r_2[x_2] \mathbin{\texttt{:}} \{\ell_i \mathbin{\texttt{.}} \check{G}_i \,\{\check{T}_Y / Y\}\}_{i \in I} \\
r_2[x_2] \,\texttt{!}\, \{\ell_i \mathbin{\texttt{.}} \check{L}_i\}_{i \in I} \,\{\check{T}_Y / Y\} &= r_2[x_2] \,\texttt{!}\, \{\ell_i \mathbin{\texttt{.}} \check{L}_i \,\{\check{T}_Y / Y\}\}_{i \in I} \\
r_1[x_1] \,\texttt{?}\{\ell_i \mathbin{\texttt{.}} \check{L}_i\}_{i \in I} \,\{\check{T}_Y / Y\} &= r_1[x_1] \,\texttt{?}\{\ell_i \mathbin{\texttt{.}} \check{L}_i \,\{\check{T}_Y / Y\}\}_{i \in I} \\
\texttt{foreach}\ R[\check{C}]\ \texttt{do}\ \check{T}_1 \mathbin{\texttt{;}} \check{T}_2 \,\{\check{T}_Y / Y\} &= \texttt{foreach}\ R[\check{C}]\ \texttt{do}\ \check{T}_1 \mathbin{\texttt{;}} (\check{T}_2 \,\{\check{T}_Y / Y\}) \\
\texttt{rec}\ X\ \check{T} \,\{\check{T}_Y / Y\} &= \begin{cases} \texttt{rec}\ X\ \check{T} & \textsf{if:}\ X = Y \\ \texttt{rec}\ X\ (\check{T} \,\{\check{T}_Y / Y\}) & \textsf{if:}\ X \neq Y \end{cases} \\
X \,\{\check{T}_Y / Y\} &= \begin{cases} \check{T}_Y & \textsf{if:}\ X = Y \\ X & \textsf{if:}\ X \neq Y \end{cases}
\end{aligned}$$

Fig. VII.7.5. Unfolding (open global types, open local types)

$$\begin{aligned}
[\![r_1[x_1] \rightarrowtriangle r_2[x_2] \mathbin{\texttt{:}} \{\ell_i \mathbin{\texttt{.}} \hat{G}_i\}_{i \in I}]\!] &= r_1[[\![x_1]\!]] \rightarrowtriangle r_2[[\![x_2]\!]] \mathbin{\texttt{:}} \{\ell_i \mathbin{\texttt{.}} [\![\hat{G}_i]\!]\}_{i \in I} \\
[\![r_2[x_2] \,\texttt{!}\, \{\ell_i \mathbin{\texttt{.}} \hat{L}_i\}_{i \in I}]\!] &= r_2[[\![x_2]\!]] \,\texttt{!}\, \{\ell_i \mathbin{\texttt{.}} [\![\hat{L}_i]\!]\}_{i \in I} \\
[\![r_1[x_1] \,\texttt{?}\{\ell_i \mathbin{\texttt{.}} \hat{L}_i\}_{i \in I}]\!] &= r_1[[\![x_1]\!]] \,\texttt{?}\{\ell_i \mathbin{\texttt{.}} [\![\hat{L}_i]\!]\}_{i \in I} \\
[\![\texttt{foreach}\ R[\hat{C}]\ \texttt{do}\ \hat{T}_1 \mathbin{\texttt{;}} \hat{T}_2]\!] &= \mathsf{iter}([\![\hat{T}_1]\!], [\![\hat{T}_2]\!], R, [\![\hat{C}]\!]) \\
[\![\texttt{rec}\ X\ \hat{T}]\!] &= \texttt{rec}\ X\ [\![\hat{T}]\!] \\
[\![X]\!] &= X
\end{aligned}$$

Fig. VII.7.6. Denotation (closed global types, closed local types)

VII.8.2 Projection

Definition VII.8.2. Let $\check{G} \upharpoonright r\check{\mathcal{D}}$ denote the *projection* of $\check{G}$ onto $r\check{\mathcal{D}}$ (level 1). Let $\check{G} \upharpoonright_{\check{C}} r[\check{C}]$ denote the *projection* of $\check{G}$ onto $r[\check{C}]$ (level 2). Let $\check{G} \upharpoonright_{\check{C}} r[z]$ denote the *projection* of $\check{G}$ onto $r[z]$ under $\check{C}$ (level 3). Fig. VII.8.2 defines $\upharpoonright$.

Lemma VII.8.2. $\upharpoonright : \check{\mathbb{G}} \times ((\mathbb{R} \times 2^{\check{\mathbb{D}}}) \cup (\mathbb{C} \times (\mathbb{R} \times 2^{\check{\mathbb{D}}})) \cup (\mathbb{C} \times (\mathbb{R} \times \mathbb{Z}))) \rightharpoonup \check{\mathbb{L}}$

The following theorems pertain to projection (level 3).

Theorem VII.8.4. $\Big[\langle \check{G}, R[\check{C}], r[z] \rangle \in \operatorname{dom} {\upharpoonright}\ \textsf{and}\ \texttt{self} \notin \operatorname{dom} \psi\Big]$

$\textsf{impl.}\ (\check{G} \upharpoonright_{R[\check{C}]} r[z]) \,\langle\!\langle \psi \rangle\!\rangle = \check{G} \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \,\langle\!\langle \psi \rangle\!\rangle]} r[z]$

Proof. See Section VIII.42. □

Theorem VII.8.5.

$$\begin{aligned}
&\Big[\langle \hat{G}, R[\hat{C}], r[z] \rangle \in \operatorname{dom} {\upharpoonright}\ \textsf{and}\ \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G})\ \textsf{and}\ f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}}\Big] \\
&\textsf{impl.}\ \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle)
\end{aligned}$$

Proof. See Section VIII.43. □

Theorem VII.8.6.

$$\begin{aligned}
&\Big[\langle \hat{G}, R[\hat{C}], r[z] \rangle \in \operatorname{dom} {\upharpoonright}\ \textsf{and}\ \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G})\ \textsf{and}\ \hat{C} \in \checkmark\ \textsf{and}\ r \in R\ \textsf{and}\ z \in \mathsf{vars}(\hat{C})\Big] \\
&\textsf{impl.}\ [\![(\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle]\!] = [\![\hat{G}]\!] \,(\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a]
\end{aligned}$$

$$\check{L}_1 \sqcap \check{L}_2 = \begin{cases} r_2[x_2]\,\textbf{!}\{\ell_i \,\textbf{.}\, \check{L}_{i,1} \sqcap \check{L}_{i,2}\}_{i \in I} & \textsf{\textbf{if:}}\ \check{L}_1 = r_2[x_2]\,\textbf{!}\{\ell_i \,\textbf{.}\, \check{L}_{i,1}\}_{i \in I}\ \textsf{\textbf{and}} \\ & \phantom{\textsf{\textbf{if:}}}\ \check{L}_2 = r_2[x_2]\,\textbf{!}\{\ell_i \,\textbf{.}\, \check{L}_{i,2}\}_{i \in I} \\ r_1[x_1]\,\textbf{?}\{\ell_i \,\textbf{.}\, \check{L}_{i,1}\}_{i \in I_1 \setminus I_2} \cup & \textsf{\textbf{if:}}\ \check{L}_1 = r_1[x_1]\,\textbf{?}\{\ell_i \,\textbf{.}\, \check{L}_{i,1}\}_{i \in I_1}\ \textsf{\textbf{and}} \\ \qquad\quad \{\ell_i \,\textbf{.}\, \check{L}_{i,2}\}_{i \in I_2 \setminus I_1} \cup & \phantom{\textsf{\textbf{if:}}}\ \check{L}_2 = r_1[x_1]\,\textbf{?}\{\ell_i \,\textbf{.}\, \check{L}_{i,2}\}_{i \in I_2}\ \textsf{\textbf{and}} \\ \qquad\quad \{\ell_i \,\textbf{.}\, \check{L}_{i,1} \sqcap \check{L}_{i,2}\}_{i \in I_1 \cap I_2} & \phantom{\textsf{\textbf{if:}}}\ \Big[\ell_{i_1} \neq \ell_{i_2}\ \textsf{\textbf{for-all}}\ i_1 \in I_1 \setminus I_2, i_2 \in I_2 \setminus I_1\Big] \\ \texttt{\textbf{foreach}}\ R[\check{C}]\ \texttt{\textbf{do}}\ \check{L}\ \textbf{;}\ \check{L}_{\textbf{;},1} \sqcap \check{L}_{\textbf{;},2} & \textsf{\textbf{if:}}\ \check{L}_1 = \texttt{\textbf{foreach}}\ R[\check{C}]\ \texttt{\textbf{do}}\ \check{L}\ \textbf{;}\ \check{L}_{\textbf{;},1}\ \textsf{\textbf{and}} \\ & \phantom{\textsf{\textbf{if:}}}\ \check{L}_2 = \texttt{\textbf{foreach}}\ R[\check{C}]\ \texttt{\textbf{do}}\ \check{L}\ \textbf{;}\ \check{L}_{\textbf{;},2} \\ \texttt{\textbf{rec}}\ X\ (L_{X,1} \sqcap \check{L}_{X,2}) & \textsf{\textbf{if:}}\ \check{L}_1 = \texttt{\textbf{rec}}\ X\ \check{L}_{X,1}\ \textsf{\textbf{and}}\ \check{L}_2 = \texttt{\textbf{rec}}\ X\ \check{L}_{X,2} \\ X & \textsf{\textbf{if:}}\ \check{L}_1 = \check{L}_2 = X \end{cases}$$

Fig. VII.8.1. Merge (open local types)

Proof. See Section VIII.44. □

The following theorems pertain to projection (level 2).

Theorem VII.8.7. $\Big[\langle \texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \texttt{\textbf{do}}\ \check{G}\ \textbf{;}\ \texttt{\textbf{cont}}, r[\check{C}]\rangle \in \operatorname{dom} {\restriction}\ \textsf{\textbf{and}}\ \texttt{\textbf{self}} \notin \operatorname{dom} \psi\Big]$

$$\textsf{\textbf{impl.}}\ \left[\begin{array}{c} (\texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \texttt{\textbf{do}}\ \check{G}\ \textbf{;}\ \texttt{\textbf{cont}} \restriction r[\check{C}])\ \langle\!\langle \psi \rangle\!\rangle = \\ = \texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \texttt{\textbf{do}}\ \check{G}\ \textbf{;}\ \texttt{\textbf{cont}}\ \langle\!\langle \psi \rangle\!\rangle \restriction r[\check{C}\ \langle\!\langle \psi \rangle\!\rangle] \end{array}\right]$$

Proof. See Section VIII.45. □

Theorem VII.8.8.

$$\left[\begin{array}{l} \langle \texttt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{\textbf{do}}\ \hat{G}\ \textbf{;}\ \texttt{\textbf{cont}}, r[\hat{C}]\rangle \in \operatorname{dom} {\restriction}\ \textsf{\textbf{and}} \\ \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \{\texttt{\textbf{cont}}\}}(\hat{G})\ \textsf{\textbf{and}}\ f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} \end{array}\right]$$

$$\textsf{\textbf{impl.}}\ \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \{\texttt{\textbf{cont}}\}}((\texttt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{\textbf{do}}\ \hat{G}\ \textbf{;}\ \texttt{\textbf{cont}} \restriction r[\hat{C}])\ \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle)$$

Proof. See Section VIII.46. □

Theorem VII.8.9.

1.

$$\left[\begin{array}{l} \langle \texttt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \texttt{\textbf{do}}\ \hat{G}\ \textbf{;}\ \texttt{\textbf{cont}}, r[\hat{C}]\rangle \in \operatorname{dom} {\restriction}\ \textsf{\textbf{and}} \\ \mathsf{Wf}_{f,\mathcal{X}}(\texttt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \texttt{\textbf{do}}\ \hat{G}\ \textbf{;}\ \texttt{\textbf{cont}})\ \textsf{\textbf{and}} \\ \Big[a \in [\![\hat{C}]\!](\tilde{z})\ \textsf{\textbf{for-all}}\ \tilde{z} \in \operatorname{dom} [\![\hat{C}]\!]\Big]\ \textsf{\textbf{and}} \\ \Big[a \notin [\![\hat{C}_{\mathsf{co}}]\!](\tilde{z})\ \textsf{\textbf{for-all}}\ \tilde{z} \in \operatorname{dom} [\![\hat{C}_{\mathsf{co}}]\!]\Big]\ \textsf{\textbf{and}}\ r \in R\ \textsf{\textbf{and}} \\ z_1 : \hat{D}_1 = \max \langle \hat{C}, \lll \rangle\ \textsf{\textbf{and}}\ \Big[|\hat{C}| > \mathtt{1}\ \textsf{\textbf{impl.}}\ z_2 : \hat{D}_2 = \max \langle \hat{C} \setminus \{z_1 : \hat{D}_1\}, \lll \rangle\Big]\ \textsf{\textbf{and}} \\ \Big[[\![\hat{C}]\!](\tilde{z}) < [\![\hat{C}_{\mathsf{gr}}]\!](\tilde{z}_{\mathsf{gr}})\ \textsf{\textbf{for-all}}\ \tilde{z} \in \operatorname{dom} [\![\hat{C}]\!], \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} [\![\hat{C}_{\mathsf{gr}}]\!]\Big] \end{array}\right]$$

$$\textsf{\textbf{impl.}}\ \left[\begin{array}{c} [\![(\texttt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \texttt{\textbf{do}}\ \hat{G}\ \textbf{;}\ \texttt{\textbf{cont}} \restriction r[\hat{C}])\ \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle]\!] \\ = \mathsf{iter}([\![\hat{G}]\!], \texttt{\textbf{cont}}, R, [\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!]\ \mathsf{from}\ z[a]) \restriction r[a] \end{array}\right]$$

$$
r_1[x_1] \mathrel{-\!\!\triangleright} r_2[x_2] \mathbin{\textbf{:}} \{\ell_i \mathbin{\textbf{.}} \check{G}_i\}_{i\in I} \upharpoonright r\check{\mathcal{D}} =
\begin{cases}
r_2[x_2] \,\textbf{!}\,\{\ell_i \mathbin{\textbf{.}} \check{G}_i \upharpoonright r\check{\mathcal{D}}\}_{i\in I} & \textsf{\textbf{if:}}\ r_1 = r \neq r_2 \ \textsf{\textbf{and}}\ x_1 .. x_1 \in \check{\mathcal{D}} \\
r_1[x_1] \,\textbf{?}\{\ell_i \mathbin{\textbf{.}} \check{G}_i \upharpoonright r\check{\mathcal{D}}\}_{i\in I} & \textsf{\textbf{if:}}\ r_1 \neq r = r_2 \ \textsf{\textbf{and}}\ x_2 .. x_2 \in \check{\mathcal{D}} \\
\bigsqcap\{\check{G}_i \upharpoonright r\check{\mathcal{D}}\}_{i\in I} & \textsf{\textbf{if:}}\ r_1 \neq r \neq r_2
\end{cases}
$$

$$
\texttt{\textbf{foreach}}\ R[\check{C}]\ \texttt{\textbf{do}}\ \check{G}_1 \mathbin{\textbf{;}} \check{G}_2 \upharpoonright r\check{\mathcal{D}} =
\begin{cases}
(\texttt{\textbf{foreach}}\ R[\check{C}]\ \texttt{\textbf{do}}\ \check{G}_1 \mathbin{\textbf{;}} \texttt{\textbf{cont}} \upharpoonright r[\check{C}_{\check{\mathcal{D}}}])\,\{\check{G}_2 \upharpoonright r\check{\mathcal{D}}/\texttt{\textbf{cont}}\} \\
\quad \textsf{\textbf{if:}}\ r \in R \ \textsf{\textbf{and}}\ \check{C}_{\check{\mathcal{D}}} = \{\tilde{z} : \tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} \\
\texttt{\textbf{foreach}}\ R[\check{C}]\ \texttt{\textbf{do}}\ (\check{G}_1 \upharpoonright r\check{\mathcal{D}}) \mathbin{\textbf{;}} (\check{G}_2 \upharpoonright r\check{\mathcal{D}}) \\
\quad \textsf{\textbf{if:}}\ r \notin R
\end{cases}
$$

$$
\begin{aligned}
\texttt{\textbf{rec}}\ X\ \check{G} \upharpoonright r\check{\mathcal{D}} &= \texttt{\textbf{rec}}\ X\ (\check{G} \upharpoonright r\check{\mathcal{D}}) \\
X \upharpoonright r\check{\mathcal{D}} &= X
\end{aligned}
$$

(a) Level 1

$$
\texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\textsf{co}}]\ \texttt{\textbf{do}}\ \check{G} \mathbin{\textbf{;}} \texttt{\textbf{cont}} \upharpoonright r[\check{C}] =
$$
$$
\begin{cases}
\texttt{\textbf{cont}} \\
\quad \textsf{\textbf{if:}}\ \check{C} = \emptyset \\
(\check{G} \upharpoonright_{R[\check{C} \cup \check{C}_{\textsf{co}}]} r[z])\,\{\texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\textsf{co}}]\ \texttt{\textbf{do}}\ \check{G} \mathbin{\textbf{;}} \texttt{\textbf{cont}} \upharpoonright r[\check{C} \setminus \{z : \check{D}\}]/\texttt{\textbf{cont}}\} \\
\quad \textsf{\textbf{if:}}\ \check{C} \neq \emptyset \ \textsf{\textbf{and}}\ z : \check{D} = \max \langle \check{C}, \ll \rangle
\end{cases}
$$

(b) Level 2

$$
r_1[x_1] \mathrel{-\!\!\triangleright} r_2[x_2] \mathbin{\textbf{:}} \{\ell_i \mathbin{\textbf{.}} \check{G}_i\}_{i\in I} \upharpoonright_{R[\check{C}]} r[z] =
\begin{cases}
r_2[\texttt{\textbf{self}}\texttt{+}\Delta(\check{C})(x_1, x_2)] \,\textbf{!}\,\{\ell_i \mathbin{\textbf{.}} \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i\in I} \\
\quad \textsf{\textbf{if:}}\ r_1[x_1] = r[z] \neq r_2[x_2] \ \textsf{\textbf{and}} \\
\qquad r_2 \in R \ \textsf{\textbf{and}}\ \{x_1, x_2\} \subseteq \textsf{vars}(\check{C}) \\
r_2[x_2] \,\textbf{!}\,\{\ell_i \mathbin{\textbf{.}} \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i\in I} \\
\quad \textsf{\textbf{if:}}\ r_1[x_1] = r[z] \neq r_2[x_2] \ \textsf{\textbf{and}} \\
\qquad \big[r_2 \notin R \ \textsf{\textbf{or}}\ \{x_1, x_2\} \not\subseteq \textsf{vars}(\check{C})\big] \\
r_1[\texttt{\textbf{self}}\texttt{+}\Delta(\check{C})(x_2, x_1)] \,\textbf{?}\{\ell_i \mathbin{\textbf{.}} \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i\in I} \\
\quad \textsf{\textbf{if:}}\ r_1[x_1] \neq r[z] = r_2[x_2] \ \textsf{\textbf{and}} \\
\qquad r_1 \in R \ \textsf{\textbf{and}}\ \{x_2, x_1\} \subseteq \textsf{vars}(\check{C}) \\
r_1[x_1] \,\textbf{?}\{\ell_i \mathbin{\textbf{.}} \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i\in I} \\
\quad \textsf{\textbf{if:}}\ r_1[x_1] \neq r[z] = r_2[x_2] \ \textsf{\textbf{and}} \\
\qquad \big[r_1 \notin R \ \textsf{\textbf{or}}\ \{x_2, x_1\} \not\subseteq \textsf{vars}(\check{C})\big] \\
\bigsqcap\{\check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i\in I} \quad \textsf{\textbf{if:}}\ r_1[x_1] \neq r[z] \neq r_2[x_2]
\end{cases}
$$

$$
\begin{aligned}
\texttt{\textbf{foreach}}\ R'[\check{C}']\ \texttt{\textbf{do}}\ \check{G}_1 \mathbin{\textbf{;}} \check{G}_2 \upharpoonright_{R[\check{C}]} r[z] &= \texttt{\textbf{foreach}}\ R'[\check{C}']\ \texttt{\textbf{do}}\ (\check{G}_1 \upharpoonright_{R[\check{C}]} r[z]) \mathbin{\textbf{;}} (\check{G}_2 \upharpoonright_{R[\check{C}]} r[z]) \\
\texttt{\textbf{rec}}\ X\ \check{G} \upharpoonright_{R[\check{C}]} r[z] &= \texttt{\textbf{rec}}\ X\ (\check{G} \upharpoonright_{R[\check{C}]} r[z]) \\
X \upharpoonright_{R[\check{C}]} r[z] &= X
\end{aligned}
$$

(c) Level 3

Fig. VII.8.2. Projection (open global types)

$$\begin{tikzcd}
\check{\mathbb{G}} \arrow[r, "\cdot\,\langle\!\langle\psi\rangle\!\rangle"] \arrow[d, "\cdot \restriction r\check{\mathcal{D}}"'] \arrow[dr, phantom, "\circlearrowright"] & \hat{\mathbb{G}} \arrow[rr, "\llbracket\cdot\rrbracket"] \arrow[d, "\cdot \restriction r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}"] \arrow[drr, phantom, "\circlearrowright"] & & \mathbb{G} \arrow[d, "\cdot \restriction r[a]"] \\
\check{\mathbb{L}} \arrow[r, "\cdot\,\langle\!\langle\psi\rangle\!\rangle"] & \check{\mathbb{L}} \arrow[r, "\cdot\,\langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle"] & \hat{\mathbb{L}} \arrow[r, "\llbracket\cdot\rrbracket"] & \mathbb{L}
\end{tikzcd}$$

Fig. VII.8.3. Theorem VII.8.10

2. $$\left[\begin{array}{l} \langle \texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{; cont}, r[\hat{C}]\rangle \in \operatorname{dom}\restriction\ \textsf{and} \\ \mathsf{Wf}_{f,\mathcal{X}}(\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{; cont})\ \textsf{and} \\ \left[a \in \llbracket\hat{C}\rrbracket(\tilde{z})\ \textsf{for-all}\ \tilde{z} \in \operatorname{dom}\llbracket\hat{C}\rrbracket\right]\ \textsf{and}\ \left[a \notin \llbracket\hat{C}_{\mathsf{co}}\rrbracket(\tilde{z})\ \textsf{for-all}\ \tilde{z} \in \operatorname{dom}\llbracket\hat{C}_{\mathsf{co}}\rrbracket\right]\ \textsf{and}\ r \in R \end{array}\right]$$
$$\textsf{impl.}\ \left[\begin{array}{l} \quad \llbracket(\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{; cont} \restriction r[\hat{C}])\,\langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle\rrbracket \\ = \llbracket\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{; cont}\rrbracket \restriction r[a] \end{array}\right]$$

Proof. See Section VIII.47. □

The following theorems pertains to projection (level 1).

Theorem VII.8.10. *The diagram in Fig. VII.8.3 commutes:*

1. $\left[\langle\check{G}, r\check{\mathcal{D}}\rangle \in \operatorname{dom}\restriction\ \textsf{and}\ \texttt{self} \notin \operatorname{dom}\psi\right]\ \textsf{impl.}\ (\check{G} \restriction r\check{\mathcal{D}})\,\langle\!\langle\psi\rangle\!\rangle = \check{G}\,\langle\!\langle\psi\rangle\!\rangle \restriction r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}$

2. $$\left[\begin{array}{l} \langle\hat{G}, r\hat{\mathcal{D}}\rangle \in \operatorname{dom}\restriction\ \textsf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{G})\ \textsf{and} \\ \left[a \in \llbracket\hat{D}\rrbracket\ \textsf{for-all}\ \hat{D} \in \hat{\mathcal{D}}\right]\ \textsf{and}\ \left[a \notin \llbracket\hat{D}\rrbracket\ \textsf{for-all}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}) \setminus \hat{\mathcal{D}}\right] \end{array}\right]$$
$$\textsf{impl.}\ \llbracket(\hat{G} \restriction r\hat{\mathcal{D}})\,\langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle\rrbracket = \llbracket\hat{G}\rrbracket \restriction r[a]$$

Proof. See Section VIII.48. □

Corollary VII.8.1.

$$\left[\begin{array}{l} \langle\check{G}, r\check{\mathcal{D}}\rangle \in \operatorname{dom}\restriction\ \textsf{and}\ \texttt{self} \notin \operatorname{dom}\psi\ \textsf{and}\ \mathsf{Wf}_{\Psi\cup\{\psi\}}(\check{G})\ \textsf{and} \\ \left[a \in \llbracket\check{D}\,\langle\!\langle\psi\rangle\!\rangle\rrbracket\ \textsf{for-all}\ \check{D} \in \check{\mathcal{D}}\right]\ \textsf{and}\ \left[a \notin \llbracket\check{D}\,\langle\!\langle\psi\rangle\!\rangle\rrbracket\ \textsf{for-all}\ \check{D} \in \mathsf{ivals}(r, \check{G}) \setminus \check{\mathcal{D}}\right] \end{array}\right]$$
$$\textsf{impl.}\ \llbracket(\check{G} \restriction r\check{\mathcal{D}})\,\langle\!\langle\psi\rangle\!\rangle\,\langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle\rrbracket = \llbracket\check{G}\,\langle\!\langle\psi\rangle\!\rangle\rrbracket \restriction r[a]$$

Part VIII
Detailed Proofs

VIII.1 Proof of Theorem VII.2.1

- **A1.** $\langle A_1, A_2 \rangle \in \operatorname{dom} \delta$
- **B1.** Conclude:

$\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} \neq \emptyset$ $(\exists a)$

impl. $A_1 \neq \emptyset$ (–)

impl. $\min \langle A_1, < \rangle + a = \min \langle \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\}, < \rangle$ (Lem. VII.2.1:1)

- **B1.** Conclude:

$\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2 \neq \emptyset$ $(\exists a)$

impl. $\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2$ **and** $\min \langle A_1, < \rangle + a = \min \langle \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\}, < \rangle$ (B1)

impl. $\min \langle A_1, < \rangle + a = \min \langle A_2, < \rangle$ (=)

impl. $\min \langle A_1, < \rangle + a + (-\min \langle A_1, < \rangle) = \min \langle A_2, < \rangle + (-\min \langle A_1, < \rangle)$ (–)

impl. $a = \min \langle A_2, < \rangle + (-\min \langle A_1, < \rangle)$ (Fig. VII.2.1:1)

impl. $a = \delta(\min \langle A_1, < \rangle, \min \langle A_2, < \rangle)$ (p25)

impl. $a = \delta(\mathsf{head}\, A_1, \mathsf{head}\, A_2)$ (Fig. VII.2.2)

Conclude:

$\langle A_1, A_2 \rangle \in \operatorname{dom} \delta$ (A1)

impl. $\delta(A_1, A_2) = a$ **and** $\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2 \neq \emptyset$ (Fig. VII.2.2, $\exists a$)

impl. $\delta(A_1, A_2) = \delta(\mathsf{head}\, A_1, \mathsf{head}\, A_2)$ (B1)

QED.

VIII.2 Proof of Theorem VII.2.2

- **A1.** $0 < a$
- **A2.** $\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2$

By induction on $|A_1|$.

- **Base.** $|A_1| = \mathrm{o}$
  - **B1.** Conclude:

$|A_1| = \mathrm{o}$ (Base)

impl. $A_1 = \emptyset$ (–)

- **B2.** Conclude:

$$\begin{array}{lll} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2 & \text{(A2)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in \emptyset\} = A_2 & \text{(B1)} \\ \textbf{impl.} & \emptyset = A_2 & \text{(–)} \end{array}$$

Conclude:

$$\begin{array}{lll} & \emptyset < \emptyset & \text{(Fig. VII.2.3)} \\ \textbf{impl.} & A_1 < A_2 & \text{(B1, B2)} \end{array}$$

- **Step.** $|A_1| > \mathsf{o}$
  - **C1.** Conclude:

$$\begin{array}{lll} & |A_1| > \mathsf{o} & \text{(Step)} \\ \textbf{impl.} & A_1 \neq \emptyset & \text{(–)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} \neq \emptyset & \text{(–)} \end{array}$$

  - **C2.** Conclude:

$$\begin{array}{lll} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} \neq \emptyset & \text{(C1)} \\ \textbf{impl.} & \min \langle \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\}, < \rangle = \min \langle A_1, < \rangle + a & \text{(Lem. VII.2.1:1)} \end{array}$$

  - **C3.** Conclude:

$$\begin{array}{lll} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2 \neq \emptyset & \text{(A2, C1)} \\ \textbf{impl.} & \min \langle \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\}, < \rangle = \min \langle A_2, < \rangle & \text{(Fig. VII.2.1:1)} \\ \textbf{impl.} & \min \langle A_1, < \rangle + a = \min \langle A_2, < \rangle & \text{(C2)} \\ \textbf{impl.} & \mathsf{o} < a \ \textbf{and} \ \min \langle A_1, < \rangle + a = \min \langle A_2, < \rangle & \text{(A1)} \\ \textbf{impl.} & \mathsf{o} + \min \langle A_1, < \rangle + a < a + \min \langle A_2, < \rangle & \text{(Fig. VII.2.1:5)} \\ \textbf{impl.} & \mathsf{o} + \min \langle A_1, < \rangle + a + (-a) < a + \min \langle A_2, < \rangle + (-a) & \text{(Fig. VII.2.1:5)} \\ \textbf{impl.} & \min \langle A_1, < \rangle < \min \langle A_2, < \rangle & \text{(Fig. VII.2.1:1)} \\ \textbf{impl.} & \textsf{head}\, A_1 < \textsf{head}\, A_2 & \text{(Fig. VII.2.2)} \end{array}$$

  - **C4.** Conclude:

$$\begin{array}{lll} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} = A_2 \neq \emptyset & \text{(A2, C1)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} \setminus \{\min \langle \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\}, < \rangle\} = A_2 \setminus \{\min \langle A_2, < \rangle\} & \text{(–)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} \setminus \{\min \langle A_1, < \rangle + a\} = A_2 \setminus \{\min \langle A_2, < \rangle\} & \text{(C2)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1 \ \textbf{and} \ \tilde{a}_1 \neq \min \langle A_1, < \rangle\} = A_2 \setminus \{\min \langle A_2, < \rangle\} & \text{(–)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1 \setminus \{\min \langle A_1, < \rangle\}\} = A_2 \setminus \{\min \langle A_2, < \rangle\} & \text{(–)} \end{array}$$

  - **C5.** Conclude:

$$\begin{array}{lll} & |\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\}| = |A_1| & \text{(–)} \\ \textbf{impl.} & |\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\}| = |A_1| \ \textbf{and} \ \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} \neq \emptyset & \text{(C1)} \\ \textbf{impl.} & |\{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} \setminus \{\min \langle \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\}, < \rangle\}| < |A_1| & \text{(–)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1\} \setminus \{\min \langle A_1, < \rangle + a\} < |A_1| & \text{(C2)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1 \ \textbf{and} \ \tilde{a}_1 \neq \min \langle A_1, < \rangle\} < |A_1| & \text{(–)} \\ \textbf{impl.} & \{\tilde{a}_1 + a \mid \tilde{a}_1 \in A_1 \setminus \{\min \langle A_1, < \rangle\}\} < |A_1| & \text{(–)} \end{array}$$

- **C6.** Conclude:

$$\begin{aligned} & A_1 \setminus \{\min\langle A_1, <\rangle\} < A_2 \setminus \{\min\langle A_2, <\rangle\} && \text{(A1, C4, C5} \Rightarrow \text{Induction)} \\ \textbf{impl.}\ & \mathsf{tail}\, A_1 < \mathsf{tail}\, A_2 && \text{(Fig. VII.2.2)} \end{aligned}$$

Conclude:

$$A_1 < A_2 \qquad \text{(C3, C6} \Rightarrow \text{Fig. VII.2.3)}$$

QED.

VIII.3 Proof of Theorem VII.2.3

Proof of (1)

- **A1.** $A = \min\langle \operatorname{img}\Phi, <\rangle$
- **A2.** $A \neq \emptyset$

Conclude:

$$\begin{aligned} & A = \min\langle \operatorname{img}\Phi, <\rangle && \text{(A1)} \\ \textbf{impl.}\ & A = \min\langle \{\Phi(\tilde{z}) \mid \tilde{z} \in \operatorname{dom}\Phi\}, <\rangle && \text{(–)} \\ \textbf{impl.}\ & \Big[A \neq \Phi(\tilde{z})\ \textbf{impl.}\ A < \Phi(\tilde{z})\Big]\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\Phi && \text{(–)} \\ \textbf{impl.}\ & \Big[A \neq \Phi(\tilde{z})\ \textbf{impl.}\ \Big[\mathsf{tail}\, A < \mathsf{tail}\, \Phi(\tilde{z})\ \textbf{or}\ A = \emptyset\Big]\Big]\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\Phi && \text{(Fig. VII.2.3)} \\ \textbf{impl.}\ & \Big[A \neq \Phi(\tilde{z})\ \textbf{impl.}\ \mathsf{tail}\, A < \mathsf{tail}\, \Phi(\tilde{z})\Big]\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\Phi && \text{(A2)} \\ \textbf{impl.}\ & \Big[A \setminus \{\min\langle A, <\rangle\} \neq \Phi(\tilde{z}) \setminus \{\min\langle \Phi(\tilde{z}), <\rangle\}\ \textbf{impl.}\ \mathsf{tail}\, A < \mathsf{tail}\, \Phi(\tilde{z})\Big]\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\Phi && \text{(–)} \\ \textbf{impl.}\ & \Big[\mathsf{tail}\, A \neq \mathsf{tail}\, \Phi(\tilde{z})\ \textbf{impl.}\ \mathsf{tail}\, A < \mathsf{tail}\, \Phi(\tilde{z})\Big]\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\Phi && \text{(Fig. VII.2.2)} \\ \textbf{impl.}\ & \Big[\mathsf{tail}\, A \neq (\mathsf{tail}\, \Phi)(\tilde{z})\ \textbf{impl.}\ \mathsf{tail}\, A < (\mathsf{tail}\, \Phi)(\tilde{z})\Big]\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\Phi && \text{(Lem. VII.2.7:3)} \\ \textbf{impl.}\ & \Big[\mathsf{tail}\, A \neq (\mathsf{tail}\, \Phi)(\tilde{z})\ \textbf{impl.}\ \mathsf{tail}\, A < (\mathsf{tail}\, \Phi)(\tilde{z})\Big]\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}(\mathsf{tail}\, \Phi) && \text{(Lem. VII.2.7:2)} \\ \textbf{impl.}\ & \mathsf{tail}\, A = \min\langle \{(\mathsf{tail}\, \Phi)(\tilde{z}) \mid \tilde{z} \in \operatorname{dom}(\mathsf{tail}\, \Phi)\}, <\rangle && \text{(–)} \\ \textbf{impl.}\ & \mathsf{tail}\, A = \min\langle \operatorname{img}(\mathsf{tail}\, \Phi), <\rangle && \text{(Fig. VII.2.5)} \end{aligned}$$

QED.

Proof of (2)

- **A1.** $A = \max\langle \operatorname{img}\Phi, <\rangle$
- **A2.** $A \neq \emptyset$

Conclude:

$$\begin{array}{lll}
& A = \max \langle \operatorname{img} \Phi, < \rangle & \text{(A1)} \\
\textbf{\textsf{impl.}} & A = \max \langle \{ \Phi(\tilde{z}) \mid \tilde{z} \in \operatorname{dom} \Phi \}, < \rangle & \text{(–)} \\
\textbf{\textsf{impl.}} & \left[A \neq \Phi(\tilde{z}) \ \textbf{\textsf{impl.}} \ \Phi(\tilde{z}) < A \right] \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(–)} \\
\textbf{\textsf{impl.}} & \left[A \neq \Phi(\tilde{z}) \ \textbf{\textsf{impl.}} \ \left[\textsf{tail}\, \Phi(\tilde{z}) < \textsf{tail}\, A \ \textbf{\textsf{or}} \ A = \emptyset \right] \right] \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.3)} \\
\textbf{\textsf{impl.}} & \left[A \neq \Phi(\tilde{z}) \ \textbf{\textsf{impl.}} \ \textsf{tail}\, \Phi(\tilde{z}) < \textsf{tail}\, A \right] \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(A2)} \\
\textbf{\textsf{impl.}} & \left[A \setminus \{ \min \langle A, < \rangle \} \neq \Phi(\tilde{z}) \setminus \{ \min \langle \Phi(\tilde{z}), < \rangle \} \ \textbf{\textsf{impl.}} \ \textsf{tail}\, \Phi(\tilde{z}) < \textsf{tail}\, A \right] \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(–)} \\
\textbf{\textsf{impl.}} & \left[\textsf{tail}\, A \neq \textsf{tail}\, \Phi(\tilde{z}) \ \textbf{\textsf{impl.}} \ \textsf{tail}\, \Phi(\tilde{z}) < \textsf{tail}\, A \right] \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.2)} \\
\textbf{\textsf{impl.}} & \left[\textsf{tail}\, A \neq (\textsf{tail}\, \Phi)(\tilde{z}) \ \textbf{\textsf{impl.}} \ (\textsf{tail}\, \Phi)(\tilde{z}) < \textsf{tail}\, A \right] \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(Lem. VII.2.7:3)} \\
\textbf{\textsf{impl.}} & \left[\textsf{tail}\, A \neq (\textsf{tail}\, \Phi)(\tilde{z}) \ \textbf{\textsf{impl.}} \ (\textsf{tail}\, \Phi)(\tilde{z}) < \textsf{tail}\, A \right] \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} (\textsf{tail}\, \Phi) & \text{(Lem. VII.2.7:2)} \\
\textbf{\textsf{impl.}} & \textsf{tail}\, A = \max \langle \{ (\textsf{tail}\, \Phi)(\tilde{z}) \mid \tilde{z} \in \operatorname{dom} (\textsf{tail}\, \Phi) \}, < \rangle & \text{(–)} \\
\textbf{\textsf{impl.}} & \textsf{tail}\, A = \max \langle \operatorname{img} (\textsf{tail}\, \Phi), < \rangle & \text{(Fig. VII.2.5)}
\end{array}$$

QED.

VIII.4 Proof of Theorem VII.2.4

- **A1.** $\langle z_1, z_2 \rangle \in \operatorname{dom} \delta\Phi$

Conclude:

$$\begin{array}{lll}
& \delta\Phi(z_1, z_2) & \\
= & \delta(\Phi(z_1), \Phi(z_2)) & \text{(A1} \Rightarrow \text{Lem. VII.2.8:3)} \\
= & \delta(\textsf{head}\, \Phi(z_1), \textsf{head}\, \Phi(z_2)) & \text{(Thm. VII.2.1)} \\
= & \delta((\textsf{head}\, \Phi)(z_1), (\textsf{head}\, \Phi)(z_2)) & \text{(Lem. VII.2.6:3)}
\end{array}$$

QED.

VIII.5 Proof of Theorem VII.2.5

- **A1.** $\textsf{len}\, \Phi > 0$
- **B1.** Conclude:

$$\begin{array}{lll}
& \textsf{len}\, \Phi > 0 & \text{(A1)} \\
\textbf{\textsf{impl.}} & |\Phi(\tilde{z})| > 0 \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.5)} \\
\textbf{\textsf{impl.}} & \Phi(\tilde{z}) \neq \emptyset \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(–)} \\
\textbf{\textsf{impl.}} & |\Phi(\tilde{z}) \setminus \{ \min \langle \Phi(\tilde{z}), < \rangle \}| = |\Phi(\tilde{z})| - 1 \ \textbf{\textsf{for-all}} \ \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.1:3)}
\end{array}$$

- **B2.** Conclude:

$$\begin{aligned}
& \mathsf{len}\,\Phi > 0 && \text{(A1)}\\
\textbf{impl. } & \mathsf{len}\,\Phi = |\Phi(\tilde{z})| \;\textbf{ for-all }\; \tilde{z} \in \mathrm{dom}\,\Phi && \text{(Fig. VII.2.5, } \exists\mathfrak{n}\text{)}\\
\textbf{impl. } & \mathsf{len}\,\Phi - 1 = |\Phi(\tilde{z})| - 1 \;\textbf{ for-all }\; \tilde{z} \in \mathrm{dom}\,\Phi && (-)\\
\textbf{impl. } & \mathsf{len}\,\Phi - 1 = |\Phi(\tilde{z}) \setminus \{\min\langle \Phi(\tilde{z}), <\rangle\}| \;\textbf{ for-all }\; \tilde{z} \in \mathrm{dom}\,\Phi && \text{(B1)}\\
\textbf{impl. } & \mathsf{len}\,\Phi - 1 = |\mathsf{tail}\,\Phi(\tilde{z})| \;\textbf{ for-all }\; \tilde{z} \in \mathrm{dom}\,\Phi && \text{(Fig. VII.2.2)}\\
\textbf{impl. } & \mathsf{len}\,\Phi - 1 = |(\mathsf{tail}\,\Phi)(\tilde{z})| \;\textbf{ for-all }\; \tilde{z} \in \mathrm{dom}\,\Phi && \text{(Lem. VII.2.7:3)}\\
\textbf{impl. } & \mathsf{len}\,\Phi - 1 = |(\mathsf{tail}\,\Phi)(\tilde{z})| \;\textbf{ for-all }\; \tilde{z} \in \mathrm{dom}\,(\mathsf{tail}\,\Phi) && \text{(Lem. VII.2.7:2)}\\
\textbf{impl. } & \mathsf{len}\,(\mathsf{tail}\,\Phi) = \mathsf{len}\,\Phi - 1 && \text{(Fig. VII.2.5)}
\end{aligned}$$

Conclude:

$$\begin{aligned}
& \mathsf{len}\,\Phi - 1 < \mathsf{len}\,\Phi && (-)\\
\textbf{impl. } & \mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi && \text{(B2)}
\end{aligned}$$

QED.

VIII.6 Proof of Theorem VII.2.6

Proof of (1)

- **A1.** $\Phi \in \mathrm{dom}\,\mathsf{len}$
- **A2.** $a \in \Phi(z)$
- **A3.** $a \neq (\mathsf{head}\,\Phi)(z)$

Conclude:

$$\begin{aligned}
& \mathsf{head}\,\Phi\\
= \;& \{\tilde{z} \mapsto \mathsf{head}\,\Phi(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} && \text{(Fig. VII.2.5)}\\
= \;& \{\tilde{z} \mapsto \min\langle \Phi(\tilde{z}), <\rangle \mid \tilde{z} \in \mathbb{Z}\} && \text{(Fig. VII.2.2)}\\
= \;& \{\tilde{z} \mapsto \min(\{\min\langle \Phi(\tilde{z}), <\rangle\} \cup (\Phi(\tilde{z}) \setminus \{\min\langle \Phi(\tilde{z}), <\rangle\})) \mid \tilde{z} \in \mathbb{Z}\} && (-)\\
= \;& \{\tilde{z} \mapsto \min(\{\mathsf{head}\,\Phi(\tilde{z})\} \cup (\mathsf{tail}\,\Phi(\tilde{z}))) \mid \tilde{z} \in \mathbb{Z}\} && \text{(Fig. VII.2.2, Fig. VII.2.2)}\\
= \;& \{\tilde{z} \mapsto \min(\{(\mathsf{head}\,\Phi)(\tilde{z})\} \cup (\mathsf{tail}\,\Phi)(\tilde{z})) \mid \tilde{z} \in \mathbb{Z}\} && \text{(Lem. VII.2.6:3, Lem. VII.2.7:3)}\\
= \;& \{\tilde{z} \mapsto \min((\mathsf{head}\,\Phi)\cdot(\mathsf{tail}\,\Phi))(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} && \text{(Lem. VII.2.10:3)}\\
= \;& \{\tilde{z} \mapsto \min(\Phi\;\mathsf{to}\;z[a])(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} && \text{(A1, A2, A3} \Rightarrow \text{Fig. VII.2.6)}\\
= \;& \{\tilde{z} \mapsto \mathsf{head}\,(\Phi\;\mathsf{to}\;z[a])(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} && \text{(Fig. VII.2.2)}\\
= \;& \mathsf{head}\,(\Phi\;\mathsf{to}\;z[a]) && \text{(Fig. VII.2.5)}
\end{aligned}$$

QED.

Proof of (2)

- **A1.** $\langle \mathsf{tail}\,\Phi, z[a]\rangle \in \mathrm{dom}\,\mathsf{to}$
- **A2.** $\Phi \in \mathrm{dom}\,\mathsf{len}$
- **A3.** $a \in \Phi(z)$
- **A4.** $a \neq (\mathsf{head}\,\Phi)(z)$
- **B1.** Conclude:

$$\begin{array}{lll}
 & \langle \mathsf{tail}\,\Phi, z[a]\rangle \in \mathrm{dom}\,\mathsf{to} & \text{(A1)}\\
\textbf{impl.} & \langle \mathsf{tail}\,\Phi, z[a]\rangle \in \mathrm{dom}\,\mathsf{to}\ \ \textbf{and} & \text{(Lem. VII.2.11:3)}\\
 & \Big[((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(\tilde{z}) \subseteq (\mathsf{tail}\,\Phi)(\tilde{z})\ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,\Phi\Big] & \\
\textbf{impl.} & ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(\tilde{z}) \subseteq (\mathsf{tail}\,\Phi)(\tilde{z})\ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]) & \text{(Lem. VII.2.11:2)}
\end{array}$$

- **B2.** Conclude:

$$\begin{array}{lll}
 & \min\langle \Phi(z'), <\rangle \in ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z')\ \ \textbf{and}\ \ z' \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]) & (\exists z')\\
\textbf{impl.} & \min\langle \Phi(z'), <\rangle \in (\mathsf{tail}\,\Phi)(z') & \text{(B1)}\\
\textbf{impl.} & \min\langle \Phi(z'), <\rangle \in \mathsf{tail}\,\Phi(z') & \text{(Lem. VII.2.7:3)}\\
\textbf{impl.} & \min\langle \Phi(z'), <\rangle \in \Phi(z') \setminus \{\min\langle \Phi(z'), <\rangle\} & \text{(Fig. VII.2.2)}\\
\textbf{impl.} & \textbf{false} & (-)
\end{array}$$

- **B3.** Conclude:

$$\begin{array}{lll}
 & z' \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]) & (\exists z')\\
\textbf{impl.} & z' \in \mathrm{dom}\,(\mathsf{tail}\,\Phi) & \text{(Lem. VII.2.11:2)}\\
\textbf{impl.} & z' \in \mathrm{dom}\,\Phi & \text{(Lem. VII.2.7:2)}\\
\textbf{impl.} & \Phi \in \mathrm{dom}\,\mathsf{len}\ \ \textbf{and}\ \ a \in \Phi(z)\ \ \textbf{and}\ \ z' \in \mathrm{dom}\,\Phi & \text{(A2, A3)}\\
\textbf{impl.} & \Phi(z') \neq \emptyset & \text{(Lem. VII.2.9:3)}
\end{array}$$

- **B4.** Conclude:

$$\begin{array}{lll}
 & z' \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]) & (\exists z')\\
\textbf{impl.} & \Phi(z') \neq \emptyset & \text{(B3)}\\
\textbf{impl.} & \{\min\langle \Phi(z'), <\rangle\} \setminus \{\min\langle \Phi(z'), <\rangle\} = \emptyset & \text{(Fig. VII.2.1:3)}
\end{array}$$

- **B5.** Conclude:

$$\begin{array}{lll}
 & z' \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]) & (\exists z')\\
\textbf{impl.} & \Phi(z') \neq \emptyset & \text{(B3)}\\
\textbf{impl.} & \min\langle \Phi(z'), <\rangle < \tilde{a}\ \ \textbf{for-all}\ \ \tilde{a} \in \Phi(z') \setminus \{\min\langle \Phi(z'), <\rangle\} & (-)\\
\textbf{impl.} & \min\langle \Phi(z'), <\rangle < \tilde{a}\ \ \textbf{for-all}\ \ \tilde{a} \in \mathsf{tail}\,\Phi(z') & \text{(Fig. VII.2.2)}\\
\textbf{impl.} & \min\langle \Phi(z'), <\rangle < \tilde{a}\ \ \textbf{for-all}\ \ \tilde{a} \in (\mathsf{tail}\,\Phi)(z') & \text{(Lem. VII.2.7:3)}
\end{array}$$

- **B6.** Conclude:

$$z' \in \operatorname{dom}((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a]) \tag{$\exists z'$}$$

$$\textbf{impl.}\ z' \in \operatorname{dom}((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])\ \textbf{and}\ \Big[\min\langle\Phi(z'), <\rangle < \tilde{a}\ \textbf{for-all}\ \tilde{a} \in (\mathsf{tail}\,\Phi)(z')\Big] \tag{B5}$$

$$\textbf{impl.}\ \min\langle\Phi(z'), <\rangle < \tilde{a}\ \textbf{for-all}\ \tilde{a} \in ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(z') \tag{B1}$$

$$\textbf{impl.}\ \Big[\min\langle\Phi(z'), <\rangle \neq \tilde{a}\ \textbf{impl.}\ \min\langle\Phi(z'), <\rangle < \tilde{a}\Big] \tag{–}$$

$$\qquad \textbf{for-all}\ \tilde{a} \in \{\min\langle\Phi(z'), <\rangle\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(z')$$

$$\textbf{impl.}\ \min\langle\Phi(z'), <\rangle = \min\langle\{\min\langle\Phi(z'), <\rangle\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(z'), <\rangle \tag{–}$$

Conclude:

$$(\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a]$$

$$= \{\tilde{z} \mapsto ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} \tag{A1}$$

$$= \{\tilde{z} \mapsto ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z}) \setminus \{\min\langle\Phi(\tilde{z}), <\rangle\} \mid \tilde{z} \in \mathbb{Z}\} \tag{B2}$$

$$= \left\{\tilde{z} \mapsto \begin{array}{c}(\{\min\langle\Phi(\tilde{z}), <\rangle\} \setminus \{\min\langle\Phi(\tilde{z}), <\rangle\}) \cup \\ (((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z}) \setminus \{\min\langle\Phi(\tilde{z}), <\rangle\})\end{array} \middle|\ \tilde{z} \in \mathbb{Z}\right\} \tag{B4}$$

$$= \{\tilde{z} \mapsto (\{\min\langle\Phi(\tilde{z}), <\rangle\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z})) \setminus \{\min\langle\Phi(\tilde{z}), <\rangle\} \mid \tilde{z} \in \mathbb{Z}\} \tag{–}$$

$$= \left\{\tilde{z} \mapsto \begin{array}{c}(\{\min\langle\Phi(\tilde{z}), <\rangle\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z})) \setminus \\ \{\min\langle\{\min\langle\Phi(\tilde{z}), <\rangle\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z}), <\rangle\}\end{array} \middle|\ \tilde{z} \in \mathbb{Z}\right\} \tag{B6}$$

$$= \{\tilde{z} \mapsto \mathsf{tail}\,(\{\min\langle\Phi(\tilde{z}), <\rangle\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z})) \mid \tilde{z} \in \mathbb{Z}\} \tag{Fig. VII.2.2}$$

$$= \{\tilde{z} \mapsto \mathsf{tail}\,(\{\mathsf{head}\,\Phi(\tilde{z})\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z})) \mid \tilde{z} \in \mathbb{Z}\} \tag{Fig. VII.2.2}$$

$$= \{\tilde{z} \mapsto \mathsf{tail}\,(\{(\mathsf{head}\,\Phi)(\tilde{z})\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z})) \mid \tilde{z} \in \mathbb{Z}\} \tag{Lem. VII.2.6:3}$$

$$= \{\tilde{z} \mapsto \mathsf{tail}\,((\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a]))(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} \tag{Lem. VII.2.10:3}$$

$$= \{\tilde{z} \mapsto \mathsf{tail}\,(\Phi\,\mathsf{to}\,z[a])(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\} \tag{A2, A3, A4 $\Rightarrow$ Fig. VII.2.6}$$

$$= \mathsf{tail}\,(\Phi\,\mathsf{to}\,z[a]) \tag{Fig. VII.2.5}$$

QED.

Proof of (3)

- **A1.** $\langle\Phi, z[a]\rangle \in \operatorname{dom}\mathsf{to}$

By induction on A1 (Fig. VII.2.6):

- **Base.** $\Phi\,\mathsf{to}\,z[a] = \{\tilde{z} \mapsto \emptyset \mid \tilde{z} \in \operatorname{dom}\Phi\}$ **and**
  $\Phi \in \operatorname{dom}\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a = (\mathsf{head}\,\Phi)(z)$

  Conclude:

$$|\emptyset| = \mathfrak{o}\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\Phi \tag{–}$$

$$\textbf{impl.}\ |\{\tilde{\tilde{z}} \mapsto \emptyset \mid \tilde{\tilde{z}} \in \operatorname{dom}\Phi\}(\tilde{z})| = \mathfrak{o}\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\Phi \tag{–}$$

$$\textbf{impl.}\ \mathsf{len}\,\{\tilde{\tilde{z}} \mapsto \emptyset \mid \tilde{\tilde{z}} \in \operatorname{dom}\Phi\} = \mathfrak{o} \tag{Fig. VII.2.5}$$

$$\textbf{impl.}\ \mathsf{len}\,(\Phi\,\mathsf{to}\,z[a]) = \mathfrak{o} \tag{Base}$$

- **Step.** $\Phi\ \mathsf{to}\ z[a] = (\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$ **and**
  $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\,\Phi)(z)$

  Conclude:

$(\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a] \in \mathrm{dom}\,\mathsf{len}$ (Step ⇒ Induction)

impl. $\mathfrak{n} = |((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(\tilde{z})|$ **for-all** $\tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$ (Fig. VII.2.5, $\exists\mathfrak{n}$)

impl. $\mathfrak{n} = |\mathsf{tail}\,(\Phi\ \mathsf{to}\ z[a])(\tilde{z})|$ **for-all** $\tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$ (Step ⇒ Thm. VII.2.6:2)

impl. $\mathfrak{n} = |(\Phi\ \mathsf{to}\ z[a])(\tilde{z}) \setminus \{\min\langle(\Phi\ \mathsf{to}\ z[a])(\tilde{z}), <\rangle\}|$ (Fig. VII.2.2)
for-all $\tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$

impl. $\mathfrak{n} + \mathfrak{1} = |\{\min\langle(\Phi\ \mathsf{to}\ z[a])(\tilde{z}), <\rangle\} \cup (\Phi\ \mathsf{to}\ z[a])(\tilde{z}) \setminus \{\min\langle(\Phi\ \mathsf{to}\ z[a])(\tilde{z}), <\rangle\}|$ (–)
for-all $\tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$

impl. $\mathfrak{n} + \mathfrak{1} = |\{\mathsf{head}\,(\Phi\ \mathsf{to}\ z[a])(\tilde{z})\} \cup \mathsf{tail}\,(\Phi\ \mathsf{to}\ z[a])(\tilde{z})|$ (Fig. VII.2.2, Fig. VII.2.2)
for-all $\tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$

impl. $\mathfrak{n} + \mathfrak{1} = |\{(\mathsf{head}\,(\Phi\ \mathsf{to}\ z[a]))(\tilde{z})\} \cup \mathsf{tail}\,(\Phi\ \mathsf{to}\ z[a])(\tilde{z})|$ (Lem. VII.2.6:3)
for-all $\tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$

impl. $\mathfrak{n} + \mathfrak{1} = |\{(\mathsf{head}\,\Phi)(\tilde{z})\} \cup \mathsf{tail}\,(\Phi\ \mathsf{to}\ z[a])(\tilde{z})|$ (Step ⇒ Thm. VII.2.6:1)
for-all $\tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$

impl. $\mathfrak{n} + \mathfrak{1} = |\{(\mathsf{head}\,\Phi)(\tilde{z})\} \cup ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(\tilde{z})|$ (Step ⇒ Thm. VII.2.6:2)
for-all $\tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])$

impl. $\mathfrak{n} + \mathfrak{1} = |\{(\mathsf{head}\,\Phi)(\tilde{z})\} \cup ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(\tilde{z})|$ (–)
for-all $\tilde{z} \in (\mathrm{dom}\,(\mathsf{head}\,\Phi)) \cap (\mathrm{dom}\,((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]))$

impl. $\mathfrak{n} + \mathfrak{1} = |((\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]))(\tilde{z})|$ (Lem. VII.2.10:3, Lem. VII.2.10:2)
for-all $\tilde{z} \in \mathrm{dom}\,((\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]))$

impl. $\mathfrak{n} + \mathfrak{1} = |(\Phi\ \mathsf{to}\ z[a])(\tilde{z})|$ **for-all** $\tilde{z} \in \mathrm{dom}\,(\Phi\ \mathsf{to}\ z[a])$ (Step)

impl. $\mathsf{len}\,(\Phi\ \mathsf{to}\ z[a]) = \mathfrak{n} + \mathfrak{1}$ (Fig. VII.2.5)

QED.

VIII.7 Proof of Theorem VII.2.7

Proof of (1)

- **A1.** $\langle\Phi, z[a]\rangle \in \mathrm{dom}\,\mathsf{from}$

By induction on A1 (Fig. VII.2.6):

- **Base.** $\Phi\ \mathsf{from}\ z[a] = \Phi$ **and** $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a = (\mathsf{head}\,\Phi)(z)$

  Conclude:

$a = (\mathsf{head}\,\Phi)(z)$ (Base)

impl. $a = (\mathsf{head}\,(\Phi\ \mathsf{from}\ z[a]))(z)$ (Base)

- **Step.** $\Phi\ \mathsf{from}\ z[a] = (\mathsf{tail}\,\Phi)\ \mathsf{from}\ z[a]$ **and** $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\,\Phi)(z)$

Conclude:

$$\begin{array}{ll} & a = (\mathsf{head}\,((\mathsf{tail}\,\Phi)\,\mathsf{from}\,z[a]))(z) \qquad \text{(Step} \Rightarrow \text{Induction)} \\ \textbf{impl.} & a = (\mathsf{head}\,(\Phi\,\mathsf{from}\,z[a]))(z) \qquad \text{(Step)} \end{array}$$

QED.

Proof of (2)

- **A1.** $\langle \Phi, z[a] \rangle \in \mathrm{dom}\,\mathsf{from}$

By induction on A1 (Fig. VII.2.6):

- **Base.** $\Phi\,\mathsf{from}\,z[a] = \Phi$ **and** $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a = (\mathsf{head}\,\Phi)(z)$
  Conclude:

$$\begin{array}{ll} & \mathsf{len}\,\Phi > \mathsf{0} \qquad \text{(Base} \Rightarrow \text{Lem. VII.2.9:2)} \\ \textbf{impl.} & \mathsf{len}\,(\Phi\,\mathsf{from}\,z[a]) > \mathsf{0} \qquad \text{(Base)} \end{array}$$

- **Step.** $\Phi\,\mathsf{from}\,z[a] = (\mathsf{tail}\,\Phi)\,\mathsf{from}\,z[a]$ **and** $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\,\Phi)(z)$
  Conclude:

$$\begin{array}{ll} & \mathsf{len}\,((\mathsf{tail}\,\Phi)\,\mathsf{from}\,z[a]) > \mathsf{0} \qquad \text{(Step} \Rightarrow \text{Induction)} \\ \textbf{impl.} & \mathsf{len}\,(\Phi\,\mathsf{from}\,z[a]) > \mathsf{0} \qquad \text{(Step)} \end{array}$$

QED.

Proof of (3)

- **A1.** $\langle \Phi, z[a] \rangle \in \mathrm{dom}\,\mathsf{from}$
- **A2.** $z' \in \mathrm{dom}\,\Phi$

By induction on A1 (Fig. VII.2.6):

- **Base.** $\Phi\,\mathsf{from}\,z[a] = \Phi$ **and** $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a = (\mathsf{head}\,\Phi)(z)$
  Conclude:

$$\begin{array}{ll} & \Phi(z') \neq \emptyset \qquad \text{(Base, A2} \Rightarrow \text{Lem. VII.2.9:3)} \\ \textbf{impl.} & (\Phi\,\mathsf{from}\,z[a])(z') \neq \emptyset \qquad \text{(Base)} \end{array}$$

- **Step.** $\Phi\,\mathsf{from}\,z[a] = (\mathsf{tail}\,\Phi)\,\mathsf{from}\,z[a]$ **and** $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\,\Phi)(z)$
  Conclude:

$$\begin{array}{ll} & ((\mathsf{tail}\,\Phi)\,\mathsf{from}\,z[a])(z') \neq \emptyset \qquad \text{(Step, A2} \Rightarrow \text{Induction)} \\ \textbf{impl.} & (\Phi\,\mathsf{from}\,z[a])(z') \neq \emptyset \qquad \text{(Step)} \end{array}$$

QED.

Proof of (4)

- **A1.** $\langle \Phi, z[a] \rangle \in \mathrm{dom}\, \mathsf{from}$
- **A2.** $\Phi(z_1) < \Phi(z_2)$

By induction on A1 (Fig. VII.2.6):

- **Base.** $\Phi\, \mathsf{from}\, z[a] = \Phi$ **and** $\Phi \in \mathrm{dom}\, \mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a = (\mathsf{head}\, \Phi)(z)$

  Conclude:

$$\begin{array}{lll} & \Phi(z_1) < \Phi(z_2) & \text{(A2)} \\ \textbf{impl.} & (\Phi\, \mathsf{from}\, z[a])(z_1) < (\Phi\, \mathsf{from}\, z[a])(z_2) & \text{(Base)} \end{array}$$

- **Step.** $\Phi\, \mathsf{from}\, z[a] = (\mathsf{tail}\, \Phi)\, \mathsf{from}\, z[a]$ **and** $\Phi \in \mathrm{dom}\, \mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\, \Phi)(z)$

  - **B1.** Conclude:

$$\begin{array}{lll} & \Phi(z_1) < \Phi(z_2) & \text{(A2)} \\ \textbf{impl.} & \mathsf{tail}\, \Phi(z_1) < \mathsf{tail}\, \Phi(z_2) \ \textbf{or} \ \Phi(z_1) = \emptyset & \text{(Fig. VII.2.3)} \\ \textbf{impl.} & \mathsf{tail}\, \Phi(z_1) < \mathsf{tail}\, \Phi(z_2) & \text{(Step} \Rightarrow \text{Lem. VII.2.9:3)} \\ \textbf{impl.} & (\mathsf{tail}\, \Phi)(z_1) < (\mathsf{tail}\, \Phi)(z_2) & \text{(Lem. VII.2.7:3)} \end{array}$$

  Conclude:

$$\begin{array}{lll} & ((\mathsf{tail}\, \Phi)\, \mathsf{from}\, z[a])(z_1) < ((\mathsf{tail}\, \Phi)\, \mathsf{from}\, z[a])(z_2) & \text{(Step, B1} \Rightarrow \text{Induction)} \\ \textbf{impl.} & (\Phi\, \mathsf{from}\, z[a])(z_1) < (\Phi\, \mathsf{from}\, z[a])(z_2) & \text{(Step)} \end{array}$$

QED.

Proof of (5)

- **A1.** $\langle \Phi, z[a] \rangle \in \mathrm{dom}\, \mathsf{from}$
- **A2.** $\Phi(z') < \Phi(z)$
- **A3.** $a \in \Phi(z')$

By induction on A1 (Fig. VII.2.6):

- **Base.** $\Phi\, \mathsf{from}\, z[a] = \Phi$ **and** $\Phi \in \mathrm{dom}\, \mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a = (\mathsf{head}\, \Phi)(z)$

  Conclude:

$$\begin{array}{lll} & a \in \Phi(z') & \text{(A3)} \\ \textbf{impl.} & a \in (\Phi\, \mathsf{from}\, z[a])(z') & \text{(Base)} \end{array}$$

- **Step.** $\Phi\, \mathsf{from}\, z[a] = (\mathsf{tail}\, \Phi)\, \mathsf{from}\, z[a]$ **and** $\Phi \in \mathrm{dom}\, \mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\, \Phi)(z)$

- **B1.** Conclude:

$$\begin{array}{lll}
 & \Phi(z') < \Phi(z) & \text{(A2)} \\
\textbf{impl.} & \mathsf{tail}\,\Phi(z') < \mathsf{tail}\,\Phi(z) \;\; \textbf{or} \;\; \Phi(z') = \emptyset & \text{(Fig. VII.2.3)} \\
\textbf{impl.} & \mathsf{tail}\,\Phi(z') < \mathsf{tail}\,\Phi(z) & \text{(Step} \Rightarrow \text{Lem. VII.2.9:3)} \\
\textbf{impl.} & (\mathsf{tail}\,\Phi)(z') < (\mathsf{tail}\,\Phi)(z) & \text{(Lem. VII.2.7:3)}
\end{array}$$

- **B2.** Conclude:

$$\begin{array}{lll}
 & \Phi(z') < \Phi(z) & \text{(A2)} \\
\textbf{impl.} & \mathsf{head}\,\Phi(z') < \mathsf{head}\,\Phi(z) \;\; \textbf{or} \;\; \Phi(z') = \emptyset & \text{(Fig. VII.2.3)} \\
\textbf{impl.} & \mathsf{head}\,\Phi(z') < \mathsf{head}\,\Phi(z) & \text{(A3)} \\
\textbf{impl.} & \min\langle\Phi(z'), <\rangle\rangle < \min\langle\Phi(z), <\rangle & \text{(Fig. VII.2.2)}
\end{array}$$

- **B3.** Conclude:

$$\begin{array}{lll}
 & a = \min\langle\Phi(z'), <\rangle & \\
\textbf{impl.} & a < \min\langle\Phi(z), <\rangle & \text{(B2)} \\
\textbf{impl.} & a \notin \Phi(z) & \text{(–)} \\
\textbf{impl.} & \textbf{false} & \text{(Step)}
\end{array}$$

- **B4.** Conclude:

$$\begin{array}{lll}
 & a \in \Phi(z') & \text{(A3)} \\
\textbf{impl.} & a = \min\langle\Phi(z'), <\rangle \;\; \textbf{or} \;\; a \in \Phi(z') \setminus \{\min\langle\Phi(z'), <\rangle\} & \text{(Fig. VII.2.1:3)} \\
\textbf{impl.} & a \in \Phi(z') \setminus \{\min\langle\Phi(z'), <\rangle\} & \text{(B3)} \\
\textbf{impl.} & a \in \mathsf{tail}\,\Phi(z') & \text{(Fig. VII.2.2)} \\
\textbf{impl.} & a \in (\mathsf{tail}\,\Phi)(z') & \text{(Lem. VII.2.7)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
 & a \in ((\mathsf{tail}\,\Phi)\;\mathsf{from}\;z[a])(z') & \text{(Step, B1, B4} \Rightarrow \text{Induction)} \\
\textbf{impl.} & a \in (\Phi\;\mathsf{from}\;z[a])(z') & \text{(Step)}
\end{array}$$

QED.

Proof of (6)

- **A1.** $\langle\Phi, z_1[a]\rangle, \langle\Phi, z_2[a]\rangle \in \mathrm{dom}\,\mathsf{from}$
- **A2.** $\Phi(z_2) < \Phi(z_1)$

By induction on A1 (Fig. VII.2.6):

- **Base.** $\Phi\;\mathsf{from}\;z_1[a] = \Phi$ **and** $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z_1)$ **and** $a = (\mathsf{head}\,\Phi)(z_1)$

  Conclude:

$$\begin{array}{lll}
 & \Phi\;\mathsf{from}\;z_2[a] & \\
= & (\Phi\;\mathsf{from}\;z_1[a])\;\mathsf{from}\;z_2[a] & \text{(A2, Base)}
\end{array}$$

- **Step.** $\Phi\ \mathsf{from}\ z_1[a] = (\mathsf{tail}\,\Phi)\ \mathsf{from}\ z_1[a]$ **and**
  $\Phi \in \operatorname{dom} \mathsf{len}$ **and** $a \in \Phi(z_1)$ **and** $a \neq (\mathsf{head}\,\Phi)(z_1)$

  - **B1.** Conclude:

    $\langle \Phi, z_2[a] \rangle \in \operatorname{dom} \mathsf{from}$ (A2)
    impl. $a \in \Phi(z_2)$ (Fig. VII.2.6)

  - **B2.** Conclude:

    $\Phi(z_2) < \Phi(z_1)$ (A2)
    impl. $\mathsf{head}\,\Phi(z_2) < \mathsf{head}\,\Phi(z_1)$ **or** $\Phi(z_2) = \emptyset$ (Fig. VII.2.3)
    impl. $\mathsf{head}\,\Phi(z_2) < \mathsf{head}\,\Phi(z_1)$ (B1)
    impl. $\min \langle \Phi(z_2), < \rangle\rangle < \min \langle \Phi(z_1), < \rangle$ (Fig. VII.2.2)

  - **B3.** Conclude:

    $a = \min \langle \Phi(z_2), < \rangle$
    impl. $a < \min \langle \Phi(z_1), < \rangle$ (B2)
    impl. $a \notin \Phi(z_1)$ (–)
    impl. **false** (Step)

  - **B4.** Conclude:

    $a \in \Phi(z_2)$ (B1)
    impl. $a = \min \langle \Phi(z_2), < \rangle$ **or** $a \in \Phi(z_2) \setminus \{\min \langle \Phi(z_2), < \rangle\}$ (Fig. VII.2.1:3)
    impl. $a \in \Phi(z_2) \setminus \{\min \langle \Phi(z_2), < \rangle\}$ (B3)
    impl. $a \neq \min \langle \Phi(z_2), < \rangle$ (–)
    impl. $a \neq \mathsf{head}\,\Phi(z_2)$ (Fig. VII.2.2)
    impl. $a \neq (\mathsf{head}\,\Phi)(z_2)$ (Lem. VII.2.6)

  - **B5.** Conclude:

    $\Phi\ \mathsf{from}\ z_2[a] = (\mathsf{tail}\,\Phi)\ \mathsf{from}\ z_2[a]$ (Step, B1, B4 ⇒ Fig. VII.2.6)

  - **B6.** Conclude:

    $\Phi(z_2) < \Phi(z_1)$ (A2)
    impl. $\mathsf{tail}\,\Phi(z_2) < \mathsf{tail}\,\Phi(z_1)$ **or** $\Phi(z_2) = \emptyset$ (Fig. VII.2.3)
    impl. $\mathsf{tail}\,\Phi(z_2) < \mathsf{tail}\,\Phi(z_1)$ (Step ⇒ Lem. VII.2.9:3)
    impl. $(\mathsf{tail}\,\Phi)(z_2) < (\mathsf{tail}\,\Phi)(z_1)$ (Lem. VII.2.7:3)

  Conclude:

  $\Phi\ \mathsf{from}\ z_2[a]$
  $= (\mathsf{tail}\,\Phi)\ \mathsf{from}\ z_2[a]$ (B5)
  $= ((\mathsf{tail}\,\Phi)\ \mathsf{from}\ z_1[a])\ \mathsf{from}\ z_2[a]$ (Step, B6 ⇒ Induction)
  $= (\Phi\ \mathsf{from}\ z_1[a])\ \mathsf{from}\ z_2[a]$ (Step)

QED.

VIII.8 Proof of Theorem VII.2.8

Proof of (1)

- **A1.** $\langle \Phi(z_1), \Phi(z_2) \rangle \in \operatorname{dom} \delta$
- **A2.** $\langle \Phi, z[a] \rangle \in \operatorname{dom} \mathsf{to}$
- **A3.** $a \neq (\mathsf{head}\,\Phi)(z)$

By induction on A2 (Fig. VII.2.6):

- **Base.** $\Phi\,\mathsf{to}\,z[a] = \{\tilde{z} \mapsto \emptyset \mid \tilde{z} \in \operatorname{dom} \Phi\}$ **and**
  $\Phi \in \operatorname{dom} \mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a = (\mathsf{head}\,\Phi)(z)$

  Conclude:

  $$\textbf{false} \qquad \text{(A3, Base)}$$

- **Step.** $\Phi\,\mathsf{to}\,z[a] = (\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])$ **and**
  $\Phi \in \operatorname{dom} \mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\,\Phi)(z)$

  - **B1.** Conclude:

  $$\begin{array}{rll} & a \in \Phi(z) & \text{(Step)} \\ \textbf{impl.} & a = \min \langle \Phi(z), < \rangle \ \textbf{or} \ a \in \Phi(z) \setminus \{\min \langle \Phi(z), < \rangle\} & \text{(Fig. VII.2.1:3)} \\ \textbf{impl.} & a = \mathsf{head}\,\Phi(z) \ \textbf{or} \ a \in \mathsf{tail}\,\Phi(z) & \text{(Fig. VII.2.2, Fig. VII.2.2)} \\ \textbf{impl.} & a = (\mathsf{head}\,\Phi)(z) \ \textbf{or} \ a \in (\mathsf{tail}\,\Phi)(z) & \text{(Lem. VII.2.6:3, Lem. VII.2.7:3)} \\ \textbf{impl.} & a \in (\mathsf{tail}\,\Phi)(z) & \text{(Step)} \end{array}$$

  By case distinction:

  - **Case.** $a = (\mathsf{head}\,\mathsf{tail}\,\Phi)(z)$
    - **C1.** Conclude:

    $$\begin{array}{rll} & \langle \Phi(z_1), \Phi(z_2) \rangle \in \operatorname{dom} \delta & \text{(A1)} \\ \textbf{impl.} & z_1, z_2 \in \operatorname{dom} \Phi & \text{(–)} \end{array}$$

    - **C2.** Conclude:

    $$\begin{array}{rll} & a \in (\mathsf{tail}\,\Phi)(z) \ \textbf{and} \ a = (\mathsf{head}\,\mathsf{tail}\,\Phi)(z) & \text{(B1, Case)} \\ \textbf{impl.} & (\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a] = \{\tilde{z} \mapsto \emptyset \mid \tilde{z} \in \operatorname{dom} \Phi\} & \text{(Fig. VII.2.6)} \end{array}$$

Conclude:

$$\begin{aligned}
&\delta(\Phi(z_1),\Phi(z_2)) \\
=\ &\delta(\mathsf{head}\,\Phi(z_1),\mathsf{head}\,\Phi(z_2)) && \text{(A1 $\Rightarrow$ Thm. VII.2.1)}\\
=\ &\delta((\mathsf{head}\,\Phi)(z_1),(\mathsf{head}\,\Phi)(z_2)) && \text{(Lem. VII.2.6:3)}\\
=\ &\delta(\{(\mathsf{head}\,\Phi)(z_1)\},\{(\mathsf{head}\,\Phi)(z_2)\}) && \text{(Lem. VII.2.4:3)}\\
=\ &\delta(\{(\mathsf{head}\,\Phi)(z_1)\}\cup\emptyset,\{(\mathsf{head}\,\Phi)(z_2)\}\cup\emptyset) && \text{(–)}\\
=\ &\delta(\{(\mathsf{head}\,\Phi)(z_1)\}\cup\{\tilde{z}\mapsto\emptyset \mid \tilde{z}\in\operatorname{dom}\Phi\}(z_1), && \text{(C1)}\\
&\quad\{(\mathsf{head}\,\Phi)(z_2)\}\cup\{\tilde{z}\mapsto\emptyset \mid \tilde{z}\in\operatorname{dom}\Phi\}(z_2))\\
=\ &\delta(\{(\mathsf{head}\,\Phi)(z_1)\}\cup((\mathsf{tail}\,\Phi)\mathbin{\mathsf{to}}z[a])(z_1),\{(\mathsf{head}\,\Phi)(z_2)\}\cup((\mathsf{tail}\,\Phi)\mathbin{\mathsf{to}}z[a])(z_2)) && \text{(C2)}\\
=\ &\delta(((\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\mathbin{\mathsf{to}}z[a]))(z_1),((\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\mathbin{\mathsf{to}}z[a]))(z_2)) && \text{(Lem. VII.2.10:3)}\\
=\ &\delta((\Phi\mathbin{\mathsf{to}}z[a])(z_1),(\Phi\mathbin{\mathsf{to}}z[a])(z_2)) && \text{(Step)}
\end{aligned}$$

- **Case.** $a \neq (\mathsf{head}\,\mathsf{tail}\,\Phi)(z)$
  - **D1.** Conclude:

$$\begin{aligned}
&\Phi\in\operatorname{dom}\mathsf{len} && \text{(Step)}\\
\textbf{impl. }\ &\mathfrak{n}=|\Phi(\tilde{z})|\ \textbf{ for-all }\ \tilde{z}\in\operatorname{dom}\Phi && \text{(Fig. VII.2.5, $\exists\mathfrak{n}$)}\\
\textbf{impl. }\ &\Big[\mathfrak{n}=|\Phi(\tilde{z})|\ \textbf{ and }\ \Phi(\tilde{z})\neq\emptyset\Big]\ \textbf{ for-all }\ \tilde{z}\in\operatorname{dom}\Phi && \text{(Step $\Rightarrow$ Lem. VII.2.9:3)}\\
\textbf{impl. }\ &\mathfrak{n}-\mathfrak{1}=|\Phi(\tilde{z})\setminus\{\min\langle\Phi(\tilde{z}),<\rangle\}|\ \textbf{ for-all }\ \tilde{z}\in\operatorname{dom}\Phi && \text{(Fig. VII.2.1:3)}\\
\textbf{impl. }\ &\mathfrak{n}-\mathfrak{1}=|\mathsf{tail}\,\Phi(\tilde{z})|\ \textbf{ for-all }\ \tilde{z}\in\operatorname{dom}\Phi && \text{(Fig. VII.2.2)}\\
\textbf{impl. }\ &\mathsf{tail}\,\Phi\in\operatorname{dom}\mathsf{len} && \text{(Fig. VII.2.5)}
\end{aligned}$$

  - **D2.** Conclude:

$$\begin{aligned}
&\langle\Phi(z_1),\Phi(z_2)\rangle\in\operatorname{dom}\delta && \text{(A1)}\\
\textbf{impl. }\ &\{\tilde{a}_1+a' \mid \tilde{a}_1\in\Phi(z_1)\}=\Phi(z_2)\neq\emptyset && \text{(Fig. VII.2.2, $\exists a'$)}\\
\textbf{impl. }\ &\{\tilde{a}_1+a' \mid \tilde{a}_1\in\Phi(z_1)\}\neq\emptyset\ \textbf{ and } && \text{(Fig. VII.2.1:3)}\\
&\{\tilde{a}_1+a' \mid \tilde{a}_1\in\Phi(z_1)\}\setminus\{\min\langle\{\tilde{a}_1+a' \mid \tilde{a}_1\in\Phi(z_1)\},<\rangle\}=\\
&\Phi(z_2)\setminus\{\min\langle\Phi(z_2),<\rangle\}\\
\textbf{impl. }\ &\{\tilde{a}_1+a' \mid \tilde{a}_1\in\Phi(z_1)\}\setminus\{\min\langle\Phi(z_1),<\rangle+a'\}= && \text{(Lem. VII.2.1:1)}\\
&\Phi(z_2)\setminus\{\min\langle\Phi(z_2),<\rangle\}\\
\textbf{impl. }\ &\{\tilde{a}_1+a' \mid \tilde{a}_1\in\Phi(z_1)\ \textbf{ and }\ \tilde{a}_1\neq\min\langle\Phi(z_1),<\rangle\}=\Phi(z_2)\setminus\{\min\langle\Phi(z_2),<\rangle\}\\
& && \text{(–)}\\
\textbf{impl. }\ &\{\tilde{a}_1+a' \mid \tilde{a}_1\in\Phi(z_1)\setminus\{\min\langle\Phi(z_1),<\rangle\}\}=\Phi(z_2)\setminus\{\min\langle\Phi(z_2),<\rangle\} && \text{(–)}\\
\textbf{impl. }\ &\{\tilde{a}_1+a' \mid \tilde{a}_1\in\mathsf{tail}\,\Phi(z_1)\}=\mathsf{tail}\,\Phi(z_2) && \text{(Fig. VII.2.2)}\\
\textbf{impl. }\ &\{\tilde{a}_1+a' \mid \tilde{a}_1\in(\mathsf{tail}\,\Phi)(z_1)\}=(\mathsf{tail}\,\Phi)(z_2) && \text{(Lem. VII.2.7:3)}\\
\textbf{impl. }\ &\{\tilde{a}_1+a' \mid \tilde{a}_1\in(\mathsf{tail}\,\Phi)(z_1)\}=(\mathsf{tail}\,\Phi)(z_2)\neq\emptyset && \text{(D1, B1 $\Rightarrow$ Lem. VII.2.9:3)}\\
\textbf{impl. }\ &\langle(\mathsf{tail}\,\Phi)(z_1),(\mathsf{tail}\,\Phi)(z_2)\rangle\in\operatorname{dom}\delta && \text{(Fig. VII.2.2)}
\end{aligned}$$

- **D3.** Conclude:

$$\begin{array}{lll}
 & \langle\Phi(z_1),\Phi(z_2)\rangle \in \operatorname{dom}\delta & \text{(A1)}\\
\textbf{impl.} & \delta(\Phi(z_1),\Phi(z_2)) = \delta(\mathsf{head}\,\Phi(z_1),\mathsf{head}\,\Phi(z_2)) & \text{(Thm. VII.2.1)}\\
\textbf{impl.} & \delta(\Phi(z_1),\Phi(z_2)) = \delta((\mathsf{head}\,\Phi)(z_1),(\mathsf{head}\,\Phi)(z_2)) & \text{(Lem. VII.2.6:3)}\\
\textbf{impl.} & \delta(\Phi(z_1),\Phi(z_2)) = (\mathsf{head}\,\Phi)(z_2) + (-(\mathsf{head}\,\Phi)(z_1)) & \text{(p25)}\\
\textbf{impl.} & (\mathsf{head}\,\Phi)(z_1) + \delta(\Phi(z_1),\Phi(z_2)) = & \text{(–)}\\
 & (\mathsf{head}\,\Phi)(z_1) + (\mathsf{head}\,\Phi)(z_2) + (-(\mathsf{head}\,\Phi)(z_1)) & \\
\textbf{impl.} & (\mathsf{head}\,\Phi)(z_1) + \delta(\Phi(z_1),\Phi(z_2)) = (\mathsf{head}\,\Phi)(z_2) & \text{(Fig. VII.2.1:1)}
\end{array}$$

- **D4.** Conclude:

$$\begin{array}{lll}
 & \delta(\Phi(z_1),\Phi(z_2)) = a' & (\exists a')\\
\textbf{impl.} & \delta(\Phi(z_1),\Phi(z_2)) = a' \ \textbf{and}\ (\mathsf{head}\,\Phi)(z_1) + \delta(\Phi(z_1),\Phi(z_2)) = (\mathsf{head}\,\Phi)(z_2) & \text{(D3)}\\
\textbf{impl.} & (\mathsf{head}\,\Phi)(z_1) + a' = (\mathsf{head}\,\Phi)(z_2) & (=)
\end{array}$$

- **D5.** Conclude:

$$\begin{array}{lll}
 & \delta(\Phi(z_1),\Phi(z_2)) = a' \ \textbf{and} & (\exists a')\\
 & \{\tilde a_1 + a' \mid \tilde a_1 \in ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_1)\} = ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_2) \neq \emptyset & \\
\textbf{impl.} & (\mathsf{head}\,\Phi)(z_1) + a' = (\mathsf{head}\,\Phi)(z_2) \ \textbf{and} & \text{(D4)}\\
 & \{\tilde a_1 + a' \mid \tilde a_1 \in ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_1)\} = ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_2) \neq \emptyset & \\
\textbf{impl.} & \{(\mathsf{head}\,\Phi)(z_1) + a'\} \cup \{\tilde a_1 + a' \mid \tilde a_1 \in ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_1)\} = & \text{(–)}\\
 & \{(\mathsf{head}\,\Phi)(z_2)\} \cup ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_2) \neq \emptyset & \\
\textbf{impl.} & \{\tilde a_1 + a' \mid \tilde a_1 = (\mathsf{head}\,\Phi)(z_1) \ \textbf{or}\ \tilde a_1 \in ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_1)\} = & \text{(–)}\\
 & \{(\mathsf{head}\,\Phi)(z_2)\} \cup ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_2) \neq \emptyset & \\
\textbf{impl.} & \{\tilde a_1 + a' \mid \tilde a_1 \in \{(\mathsf{head}\,\Phi)(z_1)\} \cup ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_1)\} = & \text{(–)}\\
 & \{(\mathsf{head}\,\Phi)(z_2)\} \cup ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_2) \neq \emptyset & \\
\textbf{impl.} & \{\tilde a_1 + a' \mid \tilde a_1 \in ((\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]))(z_1)\} = & \text{(Lem. VII.2.10:3)}\\
 & ((\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a]))(z_2) \neq \emptyset & \\
\textbf{impl.} & \{\tilde a_1 + a' \mid \tilde a_1 \in (\Phi\ \mathsf{to}\ z[a])(z_1)\} = (\Phi\ \mathsf{to}\ z[a])(z_2) \neq \emptyset & \text{(Step)}\\
\textbf{impl.} & \delta((\Phi\ \mathsf{to}\ z[a])(z_1),(\Phi\ \mathsf{to}\ z[a])(z_2)) = a' & \text{(Fig. VII.2.2)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
 & \delta(\Phi(z_1),\Phi(z_2)) = & \text{(D2, Step, Case} \Rightarrow \text{Induction)}\\
 & \delta(((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_1),((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_2)) & \\
\textbf{impl.} & \delta(\Phi(z_1),\Phi(z_2)) = a' \ \textbf{and} & (\text{Fig. VII.2.2}, \exists a')\\
 & \{\tilde a_1 + a' \mid \tilde a_1 \in ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_1)\} = ((\mathsf{tail}\,\Phi)\ \mathsf{to}\ z[a])(z_2) \neq \emptyset & \\
\textbf{impl.} & \delta(\Phi(z_1),\Phi(z_2)) = \delta((\Phi\ \mathsf{to}\ z[a])(z_1),(\Phi\ \mathsf{to}\ z[a])(z_2)) & \text{(D5)}
\end{array}$$

QED.

Proof of (2)

- **A1.** $\langle \Phi(z_1), \Phi(z_2) \rangle \in \operatorname{dom} \delta$
- **A2.** $\langle \Phi, z[a] \rangle \in \operatorname{dom} \mathsf{from}$

By induction on A2 (Fig. VII.2.6):

- **Base.** $\Phi \mathbin{\mathsf{from}} z[a] = \Phi \;\; \textsf{\textbf{and}} \;\; \Phi \in \operatorname{dom} \mathsf{len} \;\; \textsf{\textbf{and}} \;\; a \in \Phi(z) \;\; \textsf{\textbf{and}} \;\; a = (\mathsf{head}\, \Phi)(z)$

  Conclude:

$$\begin{array}{rll}
& \delta(\Phi(z_1), \Phi(z_2)) & \\
= & \delta((\Phi \mathbin{\mathsf{from}} z[a])(z_1), (\Phi \mathbin{\mathsf{from}} z[a])(z_2)) & \text{(A2, Base)}
\end{array}$$

- **Step.** $\Phi \mathbin{\mathsf{from}} z[a] = (\mathsf{tail}\, \Phi) \mathbin{\mathsf{from}} z[a] \;\; \textsf{\textbf{and}} \;\; \Phi \in \operatorname{dom} \mathsf{len} \;\; \textsf{\textbf{and}} \;\; a \in \Phi(z) \;\; \textsf{\textbf{and}} \;\; a \neq (\mathsf{head}\, \Phi)(z)$

  - **B1.** Conclude:

$$\begin{array}{rll}
& \Phi \in \operatorname{dom} \mathsf{len} & \text{(Step)} \\
\textsf{\textbf{impl.}} & \mathfrak{n} = |\Phi(\tilde{z})| \;\; \textsf{\textbf{for-all}} \;\; \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.5, } \exists \mathfrak{n}\text{)} \\
\textsf{\textbf{impl.}} & \Big[\mathfrak{n} = |\Phi(\tilde{z})| \;\; \textsf{\textbf{and}} \;\; \Phi(\tilde{z}) \neq \emptyset\Big] \;\; \textsf{\textbf{for-all}} \;\; \tilde{z} \in \operatorname{dom} \Phi & \text{(Step} \Rightarrow \text{Lem. VII.2.9:3)} \\
\textsf{\textbf{impl.}} & \mathfrak{n} - \mathfrak{1} = |\Phi(\tilde{z}) \setminus \{\min \langle \Phi(\tilde{z}), < \rangle\}| \;\; \textsf{\textbf{for-all}} \;\; \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.1:3)} \\
\textsf{\textbf{impl.}} & \mathfrak{n} - \mathfrak{1} = |\mathsf{tail}\, \Phi(\tilde{z})| \;\; \textsf{\textbf{for-all}} \;\; \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.2)} \\
\textsf{\textbf{impl.}} & \mathsf{tail}\, \Phi \in \operatorname{dom} \mathsf{len} & \text{(Fig. VII.2.5)}
\end{array}$$

  - **B2.** Conclude:

$$\begin{array}{rll}
& a \in \Phi(z) & \text{(Step)} \\
\textsf{\textbf{impl.}} & a = \min \langle \Phi(z), < \rangle \;\; \textsf{\textbf{or}} \;\; a \in \Phi(z) \setminus \{\min \langle \Phi(z), < \rangle\} & \text{(Fig. VII.2.1:3)} \\
\textsf{\textbf{impl.}} & a = \mathsf{head}\, \Phi(z) \;\; \textsf{\textbf{or}} \;\; a \in \mathsf{tail}\, \Phi(z) & \text{(Fig. VII.2.2, Fig. VII.2.2)} \\
\textsf{\textbf{impl.}} & a = (\mathsf{head}\, \Phi)(z) \;\; \textsf{\textbf{or}} \;\; a \in (\mathsf{tail}\, \Phi)(z) & \text{(Lem. VII.2.6:3, Lem. VII.2.7:3)} \\
\textsf{\textbf{impl.}} & a \in (\mathsf{tail}\, \Phi)(z) & \text{(Step)}
\end{array}$$

  - **B3.** Conclude:

$$\begin{array}{rll}
& \langle \Phi(z_1), \Phi(z_2) \rangle \in \operatorname{dom} \delta & \text{(A1)} \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in \Phi(z_1)\} = \Phi(z_2) \neq \emptyset & \text{(Fig. VII.2.2, } \exists a'\text{)} \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in \Phi(z_1)\} \neq \emptyset \;\; \textsf{\textbf{and}} & \text{(Fig. VII.2.1:3)} \\
& \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in \Phi(z_1)\} \setminus \{\min \langle \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in \Phi(z_1)\}, < \rangle\} = \Phi(z_2) \setminus \{\min \langle \Phi(z_2), < \rangle\} & \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in \Phi(z_1)\} \setminus \{\min \langle \Phi(z_1), < \rangle + a'\} = & \text{(Lem. VII.2.1:1)} \\
& \Phi(z_2) \setminus \{\min \langle \Phi(z_2), < \rangle\} & \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in \Phi(z_1) \;\; \textsf{\textbf{and}} \;\; \tilde{a}_1 \neq \min \langle \Phi(z_1), < \rangle\} = \Phi(z_2) \setminus \{\min \langle \Phi(z_2), < \rangle\} & (-) \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in \Phi(z_1) \setminus \{\min \langle \Phi(z_1), < \rangle\}\} = \Phi(z_2) \setminus \{\min \langle \Phi(z_2), < \rangle\} & (-) \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in \mathsf{tail}\, \Phi(z_1)\} = \mathsf{tail}\, \Phi(z_2) & \text{(Fig. VII.2.2)} \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in (\mathsf{tail}\, \Phi)(z_1)\} = (\mathsf{tail}\, \Phi)(z_2) & \text{(Lem. VII.2.7:3)} \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + a' \mid \tilde{a}_1 \in (\mathsf{tail}\, \Phi)(z_1)\} = (\mathsf{tail}\, \Phi)(z_2) \neq \emptyset & \text{(B1, B2} \Rightarrow \text{Lem. VII.2.9:3)} \\
\textsf{\textbf{impl.}} & \langle (\mathsf{tail}\, \Phi)(z_1), (\mathsf{tail}\, \Phi)(z_2) \rangle \in \operatorname{dom} \delta & \text{(Fig. VII.2.2)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
 & \delta(\Phi(z_1),\Phi(z_2)) = & \text{(B3, Step} \Rightarrow \text{Induction)}\\
 & \delta(((\mathsf{tail}\,\Phi)\ \mathsf{from}\ z[a])(z_1),((\mathsf{tail}\,\Phi)\ \mathsf{from}\ z[a])(z_2)) & \\
\textbf{impl.} & \delta(\Phi(z_1),\Phi(z_2)) = \delta((\Phi\ \mathsf{from}\ z[a])(z_1),(\Phi\ \mathsf{from}\ z[a])(z_2)) & \text{(Step)}
\end{array}$$

QED.

VIII.9 Proof of Theorem VII.2.9

Proof of (1)

- **A1.** $\langle \Phi \cup \Phi_{\mathsf{co}}, z[a]\rangle \in \operatorname{dom} \mathsf{to}$
- **A2.** $\Phi(z) = \max \langle \operatorname{img} \Phi, <\rangle$
- **A3.** $a \notin \Phi_{\mathsf{co}}(\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}}$

By induction on A1 (Fig. VII.2.6):

- **Base.** $(\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a] = \{\tilde{z} \mapsto \emptyset \mid \tilde{z} \in \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}})\}$ **and** $\Phi \cup \Phi_{\mathsf{co}} \in \operatorname{dom} \mathsf{len}$ **and** $a \in (\Phi \cup \Phi_{\mathsf{co}})(z)$ **and** $a = (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))(z)$

  Conclude:

$$\begin{array}{lll}
 & a \notin \emptyset\ \textbf{for-all}\ \tilde{z} \in \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}}) & (-)\\
\textbf{impl.} & a \notin \bigcup \{\emptyset \mid \tilde{z} \in \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}})\} & (-)\\
\textbf{impl.} & a \notin \bigcup \operatorname{img} \{\tilde{z} \mapsto \emptyset \mid \tilde{z} \in \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}})\} & (-)\\
\textbf{impl.} & a \notin \bigcup \operatorname{img}((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a]) & \text{(Base)}
\end{array}$$

- **Step.** $(\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a] = (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))\cdot((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a])$ **and** $\Phi \cup \Phi_{\mathsf{co}} \in \operatorname{dom} \mathsf{len}$ **and** $a \in (\Phi \cup \Phi_{\mathsf{co}})(z)$ **and** $a \neq (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))(z)$

  - **B1.** Conclude:

$$\begin{array}{lll}
 & \Phi(z) = \max \langle \operatorname{img} \Phi, <\rangle & \text{(A2)}\\
\textbf{impl.} & z \in \operatorname{dom} \Phi & (-)
\end{array}$$

  - **B2.** Conclude:

$$\begin{array}{lll}
 & a \in (\Phi \cup \Phi_{\mathsf{co}})(z)\ \textbf{and}\ z \in \operatorname{dom} \Phi & \text{(Step, B1)}\\
\textbf{impl.} & a \in \Phi(z) & (-)\\
\textbf{impl.} & \Phi(z) \neq \emptyset & (-)
\end{array}$$

  - **B3.** Conclude:

$$\begin{array}{lll}
 & \Phi(z) \neq \emptyset & \text{(B2)}\\
\textbf{impl.} & \min \langle \Phi(z), <\rangle < \tilde{a}\ \textbf{for-all}\ \tilde{a} \in \Phi(z) \setminus \{\min \langle \Phi(z), <\rangle\} & \text{(Fig. VII.2.1:3)}
\end{array}$$

- **B4.** Conclude:

$$\begin{array}{lll}
 & a \neq (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))(z) & \text{(Step)}\\
\textbf{impl.} & a \neq \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}})(z) & \text{(Lem. VII.2.6:3)}\\
\textbf{impl.} & a \neq \min \langle (\Phi \cup \Phi_{\mathsf{co}})(z), < \rangle & \text{(Fig. VII.2.2)}\\
\textbf{impl.} & a \neq \min \langle (\Phi \cup \Phi_{\mathsf{co}})(z), < \rangle \ \textbf{and}\ a \in (\Phi \cup \Phi_{\mathsf{co}})(z) & \text{(Step)}\\
\textbf{impl.} & a \in (\Phi \cup \Phi_{\mathsf{co}})(z) \setminus \{\min \langle (\Phi \cup \Phi_{\mathsf{co}})(z), < \rangle\} & \text{(–)}\\
\textbf{impl.} & \min \langle (\Phi \cup \Phi_{\mathsf{co}})(z), < \rangle < a & \text{(B3)}\\
\textbf{impl.} & \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}})(z) < a & \text{(Fig. VII.2.2)}\\
\textbf{impl.} & \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}})(z) < a \ \textbf{and}\ z \in \operatorname{dom} \Phi & \text{(B1)}\\
\textbf{impl.} & \mathsf{head}\,\Phi(z) < a & \text{(–)}
\end{array}$$

- **B5.** Conclude:

$$\begin{array}{lll}
 & \mathsf{head}\,\Phi(z) < a & \text{(B4)}\\
\textbf{impl.} & \mathsf{head}\,\Phi(z) \neq a & \text{(Fig. VII.2.1:3)}\\
\textbf{impl.} & \Big[\Phi(z) = \Phi(\tilde{z}) \ \textbf{impl.}\ \mathsf{head}\,\Phi(\tilde{z}) \neq a\Big] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi & \text{(–)}
\end{array}$$

- **B6.** Conclude:

$$\begin{array}{lll}
 & \Phi(z) = \max \langle \operatorname{img} \Phi, < \rangle & \text{(A2)}\\
\textbf{impl.} & \Phi(z) = \max \langle \{\Phi(\tilde{z}) \mid \tilde{z} \in \operatorname{dom} \Phi\}, < \rangle & \text{(–)}\\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \ \textbf{impl.}\ \Phi(\tilde{z}) < \Phi(z)\Big] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi & \text{(–)}\\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \ \textbf{impl.}\ \Big[\mathsf{head}\,\Phi(\tilde{z}) < \mathsf{head}\,\Phi(z) \ \textbf{or}\ \Phi(z) = \emptyset\Big]\Big] & \text{(Fig. VII.2.3)}\\
 & \quad \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi & \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \ \textbf{impl.}\ \mathsf{head}\,\Phi(\tilde{z}) < \mathsf{head}\,\Phi(z)\Big] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi & \text{(B2)}\\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \ \textbf{impl.}\ \mathsf{head}\,\Phi(\tilde{z}) < \mathsf{head}\,\Phi(z) < a\Big] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi & \text{(B4)}\\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \ \textbf{impl.}\ \mathsf{head}\,\Phi(\tilde{z}) < a\Big] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.1:3)}\\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \ \textbf{impl.}\ \mathsf{head}\,\Phi(\tilde{z}) \neq a\Big] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi & \text{(Fig. VII.2.1:3)}
\end{array}$$

- **B7.** Conclude:

$$\begin{array}{lll}
 & \Big[\Big[\Phi(z) = \Phi(\tilde{z}) \ \textbf{impl.}\ \mathsf{head}\,\Phi(\tilde{z}) \neq a\Big] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi\Big] \ \textbf{and} & \text{(B5, B6)}\\
 & \Big[\Big[\Phi(z) \neq \Phi(\tilde{z}) \ \textbf{impl.}\ \mathsf{head}\,\Phi(\tilde{z}) \neq a\Big] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi\Big] & \\
\textbf{impl.} & \mathsf{head}\,\Phi(\tilde{z}) \neq a \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi & \text{(–)}
\end{array}$$

- **B8.** Conclude:

$$\begin{array}{lll}
 & (\Phi \cup \Phi_{\mathsf{co}})(\tilde{z}) \neq \emptyset \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} (\Phi \cup \Phi_{\mathsf{co}}) & \text{(Step} \Rightarrow \text{Lem. VII.2.9:3)}\\
\textbf{impl.} & \Phi_{\mathsf{co}}(\tilde{z}) \neq \emptyset \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}} & \text{(–)}
\end{array}$$

- **B9.** Conclude:

$$\begin{array}{lll}
 & (\Phi \cup \Phi_{\mathsf{co}})(\tilde{z}) \neq \emptyset \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}}) & (\text{Step} \Rightarrow \text{Lem. VII.2.9:3}) \\
\textbf{impl.} & \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}}) \subseteq \operatorname{dom}(\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}})) \ \ \textbf{and} & (\text{Lem. VII.2.7:2}) \\
 & \operatorname{dom}(\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}})) \subseteq \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}}) & \\
\textbf{impl.} & \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}}) = \operatorname{dom}(\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}})) & (-)
\end{array}$$

- **B10.** Conclude:

$$\begin{array}{lll}
 & \Big[a \notin \Phi_{\mathsf{co}}(\tilde{z}) \ \ \textbf{and} \ \ \Phi_{\mathsf{co}}(\tilde{z}) \neq \emptyset\Big] \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & (\text{A3, B8}) \\
\textbf{impl.} & l \neq \min\langle \Phi_{\mathsf{co}}(\tilde{z}), < \rangle \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & (\text{Fig. VII.2.1:3}) \\
\textbf{impl.} & l \neq \mathsf{head}\,\Phi_{\mathsf{co}}(\tilde{z}) \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & (\text{Fig. VII.2.2})
\end{array}$$

- **B11.** Conclude:

$$\begin{array}{lll}
 & \langle \Phi \cup \Phi_{\mathsf{co}}, z[a] \rangle \in \operatorname{dom}\mathsf{to} & (\text{A1}) \\
\textbf{impl.} & \Phi \cup \Phi_{\mathsf{co}} \in \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}} \rangle & (\text{Lem. VII.2.11:1})
\end{array}$$

- **B12.** Conclude:

$$\begin{array}{lll}
 & \Big[a \neq \mathsf{head}\,\Phi(\tilde{z}) \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi\Big] \ \ \textbf{and} & (\text{B7, B10, B11}) \\
 & \Big[a \neq \mathsf{head}\,\Phi_{\mathsf{co}}(\tilde{z}) \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}}\Big] \ \ \textbf{and} \ \ \Phi \cup \Phi_{\mathsf{co}} \in \operatorname{fam}\langle \mathbb{Z}, 2^{\mathbb{A}} \rangle & \\
\textbf{impl.} & a \neq \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}})(\tilde{z}) \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}}) & (-) \\
\textbf{impl.} & a \neq (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))(\tilde{z}) \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}(\Phi \cup \Phi_{\mathsf{co}}) & (\text{Lem. VII.2.6:3})
\end{array}$$

- **B13.** Conclude:

$$\begin{array}{lll}
 & \mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}) & \\
= & (\mathsf{tail}\,\Phi) \cup (\mathsf{tail}\,\Phi_{\mathsf{co}}) & (\text{Step} \Rightarrow \text{Lem. VII.2.7:4})
\end{array}$$

- **B14.** Conclude:

$$\begin{array}{lll}
 & \langle \mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}), z[a] \rangle \in \operatorname{dom}\mathsf{to} & (\text{Step}) \\
\textbf{impl.} & \langle (\mathsf{tail}\,\Phi) \cup (\mathsf{tail}\,\Phi_{\mathsf{co}}), z[a] \rangle \in \operatorname{dom}\mathsf{to} & (\text{Lem. VII.2.7:4})
\end{array}$$

- **B15.** Conclude:

$$\begin{array}{lll}
 & \Phi(z) = \max\langle \operatorname{img}\Phi, < \rangle \ \ \textbf{and} \ \ \Phi(z) \neq \emptyset & (\text{A2, B2}) \\
\textbf{impl.} & \mathsf{tail}\,\Phi(z) = \max\langle \operatorname{img}(\mathsf{tail}\,\Phi), < \rangle & (\text{Thm. VII.2.3:2}) \\
\textbf{impl.} & (\mathsf{tail}\,\Phi)(z) = \max\langle \operatorname{img}(\mathsf{tail}\,\Phi), < \rangle & (\text{Lem. VII.2.7:3})
\end{array}$$

- **B16.** Conclude:

$$\begin{array}{lll}
 & \Big[a \notin \Phi_{\mathsf{co}}(\tilde{z}) \ \ \textbf{and} \ \ \Phi_{\mathsf{co}}(\tilde{z}) \neq \emptyset\Big] \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & (\text{A3, B8}) \\
\textbf{impl.} & a \notin \Phi_{\mathsf{co}}(\tilde{z}) \setminus \{\min\langle \Phi_{\mathsf{co}}(\tilde{z}), < \rangle\} \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & (\text{Fig. VII.2.1:3}) \\
\textbf{impl.} & a \notin \mathsf{tail}\,\Phi_{\mathsf{co}}(\tilde{z}) \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & (\text{Fig. VII.2.2}) \\
\textbf{impl.} & a \notin (\mathsf{tail}\,\Phi_{\mathsf{co}})(\tilde{z}) \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & (\text{Lem. VII.2.7:3}) \\
\textbf{impl.} & a \notin (\mathsf{tail}\,\Phi_{\mathsf{co}})(\tilde{z}) \ \ \textbf{for-all} \ \ \tilde{z} \in \operatorname{dom}(\mathsf{tail}\,\Phi_{\mathsf{co}}) & (\text{Lem. VII.2.7:2})
\end{array}$$

- **B17.** Conclude:

$$\begin{aligned}
& a \notin \bigcup \mathrm{img}\,((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a]) && \text{(B14, B15, B16} \Rightarrow \text{Induction+B13)}\\
\textbf{impl. } & a \notin \bigcup \{((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a])(\tilde{z}) \mid \tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a])\} && (-)\\
\textbf{impl. } & a \notin ((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a])(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a]) && (-)\\
\textbf{impl. } & a \notin ((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a])(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}})) && \text{(Lem. VII.2.11:2)}\\
\textbf{impl. } & a \notin ((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a])(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{co}}) && \text{(B9)}
\end{aligned}$$

Conclude:

$$\begin{aligned}
& \Big[a \neq (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{co}})\Big] \ \ \textbf{and} && \text{(B12, B17)}\\
& \Big[a \notin ((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a])(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{co}})\Big] && \\
\textbf{impl. } & a \notin \{(\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))(\tilde{z})\} \cup ((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a])(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{co}}) && (-)\\
\textbf{impl. } & a \notin (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}){\cdot}((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{to}\ z[a]))(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{co}}) && \\
& && \text{(Lem. VII.2.10:2)}\\
\textbf{impl. } & a \notin ((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a])(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{co}}) && \text{(Step)}\\
\textbf{impl. } & a \notin ((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a])(\tilde{z}) \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a]) && \text{(Lem. VII.2.11:2)}\\
\textbf{impl. } & a \notin \bigcup \{((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a])(\tilde{z}) \mid \tilde{z} \in \mathrm{dom}\,((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a])\} && (-)\\
\textbf{impl. } & a \notin \bigcup \mathrm{img}\,((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{to}\ z[a]) && (-)
\end{aligned}$$

QED.

Proof of (2)

- **A1.** $\langle \Phi \cup \Phi_{\mathsf{co}}, z[a]\rangle \in \mathrm{dom}\,\mathsf{from}$
- **A2.** $\Phi(z) = \min\,\langle \mathrm{img}\,\Phi, <\rangle$
- **A3.** $a \notin \Phi_{\mathsf{co}}(\tilde{z})$ **for-all** $\tilde{z} \in \mathrm{dom}\,\Phi_{\mathsf{co}}$
- **B1.** Conclude:

$$\begin{aligned}
& \Phi(z) = \min\,\langle \mathrm{img}\,\Phi, <\rangle && \text{(A2)}\\
\textbf{impl. } & z \in \mathrm{dom}\,\Phi && (-)
\end{aligned}$$

- **B2.** Conclude:

$$\begin{aligned}
& (\Phi \cup \Phi_{\mathsf{co}})(\tilde{z}) \neq \emptyset \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{co}}) && \text{(Step} \Rightarrow \text{Lem. VII.2.9:3)}\\
\textbf{impl. } & \Phi_{\mathsf{co}}(\tilde{z}) \neq \emptyset \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,\Phi_{\mathsf{co}} && (-)
\end{aligned}$$

By induction on A1 (Fig. VII.2.6):

- **Base.** $(\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z[a] = \Phi \cup \Phi_{\mathsf{co}}$ **and**
  $\Phi \cup \Phi_{\mathsf{co}} \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in (\Phi \cup \Phi_{\mathsf{co}})(z)$ **and** $a = (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))(z)$

- **C1.** Conclude:

$$\begin{array}{lll}
 & a = (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}}))(z) & \text{(Base)} \\
\textbf{impl.} & a = \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}})(z) & \text{(Lem. VII.2.6:3)} \\
\textbf{impl.} & a = \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{co}})(z) \;\; \textbf{and} \;\; z \in \operatorname{dom}\Phi & \text{(B1)} \\
\textbf{impl.} & a = \mathsf{head}\,\Phi(z) & \text{(–)}
\end{array}$$

- **C2.** Conclude:

$$\begin{array}{lll}
 & a = \mathsf{head}\,\Phi(z) & \text{(C1)} \\
\textbf{impl.} & a = \min\langle \Phi(z), < \rangle & \text{(Fig. VII.2.2)} \\
\textbf{impl.} & a \notin \Phi(z) \setminus \{\min\langle \Phi(z), < \rangle\} & \text{(–)} \\
\textbf{impl.} & a \notin \mathsf{tail}\,\Phi(z) & \text{(Fig. VII.2.2)} \\
\textbf{impl.} & \Big[\Phi(z) = \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; a \notin \mathsf{tail}\,\Phi(\tilde{z})\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \text{(–)}
\end{array}$$

- **C3.** Conclude:

$$\begin{array}{lll}
 & \Phi(z) = \min\langle \operatorname{img}\Phi, < \rangle & \text{(A2)} \\
\textbf{impl.} & \Phi(z) = \min\langle \{\Phi(\tilde{z}) \mid \tilde{z} \in \operatorname{dom}\Phi\}, < \rangle & \text{(–)} \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; \Phi(z) < \Phi(\tilde{z})\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \text{(–)} \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; \Big[\mathsf{head}\,\Phi(z) < \mathsf{head}\,\Phi(\tilde{z}) \;\; \textbf{or} \;\; \Phi(z) = \emptyset\Big]\Big] & \text{(Fig. VII.2.3)} \\
 & \quad \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; \mathsf{head}\,\Phi(z) < \mathsf{head}\,\Phi(\tilde{z})\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \text{(B1)} \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; \mathsf{head}\,\Phi(z) < \min\langle \Phi(\tilde{z}), < \rangle\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \text{(Fig. VII.2.2)} \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; \Big[\mathsf{head}\,\Phi(z) \notin \Phi(\tilde{z}) \;\; \textbf{and} \;\; \Phi(\tilde{z}) \neq \emptyset\Big]\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \text{(–)} \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; \mathsf{head}\,\Phi(z) \notin \Phi(\tilde{z}) \setminus \{\min\langle \Phi(\tilde{z}), < \rangle\}\Big] & \text{(Fig. VII.2.1:3)} \\
 & \quad \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; \mathsf{head}\,\Phi(z) \notin \mathsf{tail}\,\Phi(\tilde{z})\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \text{(Fig. VII.2.2)} \\
\textbf{impl.} & \Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; a \notin \mathsf{tail}\,\Phi(\tilde{z})\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \text{(C1)}
\end{array}$$

- **C4.** Conclude:

$$\begin{array}{lll}
 & \Big[\Big[\Phi(z) = \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; a \notin \mathsf{tail}\,\Phi(\tilde{z})\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi\Big] \;\; \textbf{and} & \text{(C2, C3)} \\
 & \Big[\Big[\Phi(z) \neq \Phi(\tilde{z}) \;\; \textbf{impl.} \;\; a \notin \mathsf{tail}\,\Phi(\tilde{z})\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi\Big] & \\
\textbf{impl.} & a \notin \mathsf{tail}\,\Phi(\tilde{z}) \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi & \text{(–)}
\end{array}$$

- **C5.** Conclude:

$$\begin{array}{lll}
 & \Big[a \notin \Phi_{\mathsf{co}}(\tilde{z}) \;\; \textbf{and} \;\; \Phi_{\mathsf{co}}(\tilde{z}) \neq \emptyset\Big] \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & \text{(A3, B2)} \\
\textbf{impl.} & a \notin \Phi_{\mathsf{co}}(\tilde{z}) \setminus \{\min\langle \Phi_{\mathsf{co}}(\tilde{z}), < \rangle\} \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & \text{(Fig. VII.2.1:3)} \\
\textbf{impl.} & a \notin \mathsf{tail}\,\Phi_{\mathsf{co}}(\tilde{z}) \;\; \textbf{for-all} \;\; \tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}} & \text{(Fig. VII.2.2)}
\end{array}$$

- **C6.** Conclude:

$$\begin{array}{lll}
 & \langle \Phi \cup \Phi_{\mathsf{co}}, z[a] \rangle \in \operatorname{dom} \mathsf{to} & \text{(A1)} \\
\textbf{impl.} & \Phi \cup \Phi_{\mathsf{co}} \in \operatorname{fam} \langle \mathbb{Z}, 2^{\mathbb{A}} \rangle & \text{(Lem. VII.2.11:1)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
 & \Big[a \notin \mathsf{tail}\, \Phi(\tilde{z}) \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi \Big] \ \textbf{and} & \text{(C4, C5, C6)} \\
 & \Big[a \notin \mathsf{tail}\, \Phi_{\mathsf{co}}(\tilde{z}) \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}} \Big] \ \textbf{and}\ \Phi \cup \Phi_{\mathsf{co}} \in \operatorname{fam} \langle \mathbb{Z}, 2^{\mathbb{A}} \rangle & \\
\textbf{impl.} & a \notin \mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}})(\tilde{z}) \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} (\Phi \cup \Phi_{\mathsf{co}}) & (-) \\
\textbf{impl.} & a \notin (\mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}}))(\tilde{z}) \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} (\Phi \cup \Phi_{\mathsf{co}}) & \text{(Lem. VII.2.7:3)} \\
\textbf{impl.} & a \notin (\mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}}))(\tilde{z}) \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} (\mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}})) & \text{(Lem. VII.2.7:2)} \\
\textbf{impl.} & a \notin \bigcup \operatorname{img} (\mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}})) & (-) \\
\textbf{impl.} & a \notin \bigcup \operatorname{img} (\mathsf{tail}\, ((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z[a])) & \text{(Base)}
\end{array}$$

- **Step.** $(\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z[a] = (\mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{from}\ z[a]$ **and** $\Phi \cup \Phi_{\mathsf{co}} \in \operatorname{dom} \mathsf{len}$ **and** $a \in (\Phi \cup \Phi_{\mathsf{co}})(z)$ **and** $a \neq (\mathsf{head}\, (\Phi \cup \Phi_{\mathsf{co}}))(z)$

  - **D1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}}) & \\
= & (\mathsf{tail}\, \Phi) \cup (\mathsf{tail}\, \Phi_{\mathsf{co}}) & \text{(Step} \Rightarrow \text{Lem. VII.2.7:4)}
\end{array}$$

  - **D2.** Conclude:

$$\begin{array}{lll}
 & a \in (\Phi \cup \Phi_{\mathsf{co}})(z) & \text{(Step)} \\
\textbf{impl.} & a = \min \langle (\Phi \cup \Phi_{\mathsf{co}})(z), < \rangle \ \textbf{or} & \text{(Fig. VII.2.1:3)} \\
 & a \in (\Phi \cup \Phi_{\mathsf{co}})(z) \setminus \{ \min \langle (\Phi \cup \Phi_{\mathsf{co}})(z), < \rangle \} & \\
\textbf{impl.} & a = \mathsf{head}\, (\Phi \cup \Phi_{\mathsf{co}})(z) \ \textbf{or}\ a \in \mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}})(z) & \text{(Fig. VII.2.2, Fig. VII.2.2)} \\
\textbf{impl.} & a = (\mathsf{head}\, (\Phi \cup \Phi_{\mathsf{co}}))(z) \ \textbf{or}\ a \in (\mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}}))(z) & \\
 & & \text{(Lem. VII.2.6:3, Lem. VII.2.7:3)} \\
\textbf{impl.} & a \in (\mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}}))(z) & \text{(Step)} \\
\textbf{impl.} & \langle \mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}}), z[a] \rangle \in \operatorname{dom} \mathsf{from} & \text{(Fig. VII.2.6)} \\
\textbf{impl.} & \langle (\mathsf{tail}\, \Phi) \cup (\mathsf{tail}\, \Phi_{\mathsf{co}}), z[a] \rangle \in \operatorname{dom} \mathsf{from} & \text{(Lem. VII.2.7:4)}
\end{array}$$

  - **D3.** Conclude:

$$\begin{array}{lll}
 & \langle \Phi \cup \Phi_{\mathsf{co}}, z[a] \rangle \in \operatorname{dom} \mathsf{from} & \text{(A1)} \\
\textbf{impl.} & a \in (\Phi \cup \Phi_{\mathsf{co}})(z) & \text{(Fig. VII.2.6)} \\
\textbf{impl.} & a \in (\Phi \cup \Phi_{\mathsf{co}})(z) \ \textbf{and}\ z \in \operatorname{dom} \Phi & \text{(B1)} \\
\textbf{impl.} & a \in \Phi(z) & (-) \\
\textbf{impl.} & \Phi(z) \neq \emptyset & (-) \\
\textbf{impl.} & \Phi(z) = \min \langle \operatorname{img} \Phi, < \rangle \ \textbf{and}\ \Phi(z) \neq \emptyset & \text{(A2)} \\
\textbf{impl.} & \mathsf{tail}\, \Phi(z) = \min \langle \operatorname{img} (\mathsf{tail}\, \Phi), < \rangle & \text{(Thm. VII.2.3:1)} \\
\textbf{impl.} & (\mathsf{tail}\, \Phi)(z) = \min \langle \operatorname{img} (\mathsf{tail}\, \Phi), < \rangle & \text{(Lem. VII.2.7:3)}
\end{array}$$

- **D4.** Conclude:

$$\begin{array}{lll} & \Big[a \notin \Phi_{\mathsf{co}}(\tilde{z}) \ \textbf{and} \ \Phi_{\mathsf{co}}(\tilde{z}) \neq \emptyset\Big] \ \textbf{for-all} \ \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}} & \text{(A3, B2)} \\ \textbf{impl.} & a \notin \Phi_{\mathsf{co}}(\tilde{z}) \setminus \{\min \langle \Phi_{\mathsf{co}}(\tilde{z}), < \rangle\} \ \textbf{for-all} \ \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}} & \text{(Fig. VII.2.1:3)} \\ \textbf{impl.} & a \notin \mathsf{tail}\, \Phi_{\mathsf{co}}(\tilde{z}) \ \textbf{for-all} \ \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}} & \text{(Fig. VII.2.2)} \\ \textbf{impl.} & a \notin (\mathsf{tail}\, \Phi_{\mathsf{co}})(\tilde{z}) \ \textbf{for-all} \ \tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}} & \text{(Lem. VII.2.7:3)} \\ \textbf{impl.} & a \notin (\mathsf{tail}\, \Phi_{\mathsf{co}})(\tilde{z}) \ \textbf{for-all} \ \tilde{z} \in \operatorname{dom} (\mathsf{tail}\, \Phi_{\mathsf{co}}) & \text{(Lem. VII.2.7:2)} \end{array}$$

Conclude:

$$\begin{array}{lll} & a \notin \bigcup \operatorname{img} (\mathsf{tail}\, ((\mathsf{tail}\, (\Phi \cup \Phi_{\mathsf{co}}))\ \mathsf{from}\ z[a])) & \text{(D2, D3, D4} \Rightarrow \text{Induction+D1)} \\ \textbf{impl.} & a \notin \bigcup \operatorname{img} (\mathsf{tail}\, ((\Phi \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z[a])) & \text{(Step)} \end{array}$$

QED.

Proof of (3)

- **A1.** $\langle (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z_1[a], z_2[a] \rangle \in \operatorname{dom} \mathsf{to}$
- **A2.** $\Phi(z_1) = \max \langle \operatorname{img} \Phi, < \rangle$
- **A3.** $\Phi(z_2) = \max \langle \operatorname{img} (\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}), < \rangle$
- **A4.** $\Phi(\tilde{z}) < \Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}})$ **for-all** $\tilde{z} \in \operatorname{dom} \Phi, \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} \Phi_{\mathsf{gr}}$
- **A5.** $a \notin \Phi_{\mathsf{co}}(\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom} \Phi_{\mathsf{co}}$
- **B1.** Conclude:

$$\begin{array}{lll} & \langle (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z_1[a], z_2[a] \rangle \in \operatorname{dom} \mathsf{to} & \text{(A1)} \\ \textbf{impl.} & \langle \Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}, z_1[a] \rangle \in \operatorname{dom} \mathsf{from} & (-) \end{array}$$

- **B2.** Conclude:

$$\begin{array}{lll} & \Phi(z_1) = \max \langle \operatorname{img} \Phi, < \rangle \ \textbf{and} \ \Phi(z_2) = \max \langle \operatorname{img} (\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}), < \rangle & \text{(A2, A3)} \\ \textbf{impl.} & z_1, z_2 \in \operatorname{dom} \Phi & (-) \end{array}$$

- **B3.** Conclude:

$$\begin{array}{lll} & \langle \Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}, z_1[a] \rangle \in \operatorname{dom} \mathsf{from} \ \textbf{and} & \text{(B1, A1)} \\ & \langle (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z_1[a], z_2[a] \rangle \in \operatorname{dom} \mathsf{to} & \\ \textbf{impl.} & a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_1) \ \textbf{and} \ a \in ((\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z_1[a])(z_2) & \text{(Fig. VII.2.6)} \\ \textbf{impl.} & a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_1) \ \textbf{and} \ a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2) & \text{(Base)} \\ \textbf{impl.} & a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_1) \ \textbf{and} \ a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2) \ \textbf{and} \ z_1, z_2 \in \operatorname{dom} \Phi & \text{(B2)} \\ \textbf{impl.} & a \in \Phi(z_1) \ \textbf{and} \ a \in \Phi(z_2) & (-) \end{array}$$

- **B4.** Conclude:

$$\begin{array}{lll} & a \in \Phi(z_1) \ \textbf{and} \ a \in \Phi(z_2) & \text{(B3)} \\ \textbf{impl.} & \Phi(z_1) \neq \emptyset \ \textbf{and} \ \Phi(z_2) \neq \emptyset & (-) \end{array}$$

- **B5.** Conclude:

$$\begin{aligned}
& (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(\tilde{z}) \neq \emptyset \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}) && \text{(Step} \Rightarrow \text{Lem. VII.2.9:3)}\\
\textbf{impl.}\ \ & \Phi_{\mathsf{co}}(\tilde{z}) \neq \emptyset \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,\Phi_{\mathsf{co}} && (-)
\end{aligned}$$

By induction on B1 (Fig. VII.2.6):

- **Base.** $(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z_1[a] = \Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}$ **and**
  $\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}} \in \mathrm{dom}\,\mathsf{len}$ **and**
  $a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_1)$ **and** $a = (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(z_1)$

  - **C1.** Conclude:

$$\begin{aligned}
& a = (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(z_1) && \text{(Base)}\\
\textbf{impl.}\ \ & a = \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_1) && \text{(Lem. VII.2.6:3)}\\
\textbf{impl.}\ \ & a = \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_1) \ \ \textbf{and}\ \ z_1 \in \mathrm{dom}\,\Phi && \text{(B2)}\\
\textbf{impl.}\ \ & a = \mathsf{head}\,\Phi(z_1) && (-)
\end{aligned}$$

  - **C2.** Conclude:

$$\begin{aligned}
& \Phi(z_2) = \max\,\langle \mathrm{img}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}), < \rangle && \text{(A3)}\\
\textbf{impl.}\ \ & \Phi(z_2) \in \mathrm{img}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}) && (-)\\
\textbf{impl.}\ \ & \Phi(z_2) \notin \mathrm{img}\,\{z_1 \mapsto \Phi(z_1)\} && (-)\\
\textbf{impl.}\ \ & \Phi(z_2) \neq \Phi(z_1) && (-)\\
\textbf{impl.}\ \ & \Phi(z_2) \neq \Phi(z_1) \ \ \textbf{and}\ \ z_2 \neq z_1 && (-)
\end{aligned}$$

  - **C3.** Conclude:

$$\begin{aligned}
& \Phi(z_1) = \max\,\langle \mathrm{img}\,\Phi, < \rangle && \text{(A2)}\\
\textbf{impl.}\ \ & \Phi(z_1) = \max\,\langle \{\Phi(\tilde{z}) \mid \tilde{z} \in \mathrm{dom}\,\Phi\}, < \rangle && (-)\\
\textbf{impl.}\ \ & \Big[\Phi(z_1) \neq \Phi(\tilde{z}) \ \ \textbf{impl.}\ \ \Phi(\tilde{z}) < \Phi(z_1)\Big] \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,\Phi && (-)\\
\textbf{impl.}\ \ & \Big[\Phi(z_1) \neq \Phi(\tilde{z}) \ \ \textbf{impl.}\ \ \Big[\mathsf{head}\,\Phi(\tilde{z}) < \mathsf{head}\,\Phi(z) \ \ \textbf{or}\ \ \Phi(z_1) = \emptyset\Big]\Big] && \text{(Fig. VII.2.3)}\\
& \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,\Phi\\
\textbf{impl.}\ \ & \Big[\Phi(z_1) \neq \Phi(\tilde{z}) \ \ \textbf{impl.}\ \ \mathsf{head}\,\Phi(\tilde{z}) < \mathsf{head}\,\Phi(z_1)\Big] \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,\Phi && \text{(B4)}\\
\textbf{impl.}\ \ & \Big[\Phi(z_1) \neq \Phi(\tilde{z}) \ \ \textbf{impl.}\ \ \mathsf{head}\,\Phi(\tilde{z}) < a\Big] \ \ \textbf{for-all}\ \ \tilde{z} \in \mathrm{dom}\,\Phi && \text{(C1)}\\
\textbf{impl.}\ \ & \Phi(z_1) \neq \Phi(z_2) \ \ \textbf{impl.}\ \ \mathsf{head}\,\Phi(z_2) < a && \text{(B2)}\\
\textbf{impl.}\ \ & \mathsf{head}\,\Phi(z_2) < a && \text{(C2)}\\
\textbf{impl.}\ \ & \mathsf{head}\,\Phi(z_2) \neq a && \text{(Fig. VII.2.1:3)}
\end{aligned}$$

  - **C4.** Conclude:

$$\begin{aligned}
& a = (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(z_2)\\
\textbf{impl.}\ \ & a = \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2) && \text{(Lem. VII.2.6:3)}\\
\textbf{impl.}\ \ & a = \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2) \ \ \textbf{and}\ \ z_2 \in \mathrm{dom}\,\Phi && \text{(B2)}\\
\textbf{impl.}\ \ & a = \mathsf{head}\,\Phi(z_2) && (-)\\
\textbf{impl.}\ \ & \textbf{false} && \text{(C3)}
\end{aligned}$$

- **C5.** Conclude:

$\langle(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})\,\mathsf{from}\,z_1[a], z_2[a]\rangle \in \mathrm{dom}\,\mathsf{to}$ (A1)

impl. $\langle \Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}, z_2[a]\rangle \in \mathrm{dom}\,\mathsf{to}$ (Base)

impl. $a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2)$ (Fig. VII.2.6)

impl. $a = \min\langle(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2), <\rangle$ **or** (Fig. VII.2.1:3)
$a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2) \setminus \{\min\langle(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2), <\rangle\}$

impl. $a = \mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2)$ **or** $a \in \mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2)$
(Fig. VII.2.2, Fig. VII.2.2)

impl. $a = (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(z_2)$ **or** (Lem. VII.2.6:3, Lem. VII.2.7:3)
$a \in (\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(z_2)$

impl. $a \in (\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(z_2)$ (C4)

impl. $\langle \mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}), z_2[a]\rangle \in \mathrm{dom}\,\mathsf{to}$ (Fig. VII.2.6)

impl. $\langle \mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}), z_2[a]\rangle \in \mathrm{dom}\,\mathsf{to}$ **and** $z_1 \in \mathrm{dom}\,\Phi$ (B2)

impl. $\langle \mathsf{tail}\,((\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}) \cup \{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}), z_2[a]\rangle \in \mathrm{dom}\,\mathsf{to}$ (–)

impl. $\langle (\mathsf{tail}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})) \cup (\mathsf{tail}\,(\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})), z_2[a]\rangle \in \mathrm{dom}\,\mathsf{to}$
(Lem. VII.2.7:4)

- **C6.** Conclude:

$\Phi(z_2) \neq \emptyset$ **and** $z_2 \neq z_1$ (B4, C2)

impl. $(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})(z_2) \neq \emptyset$ (–)

- **C7.** Conclude:

$\Phi(z_2) = \max\langle \mathrm{img}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}), <\rangle$ **and** $z_2 \neq z_1$ (A3, C2)

impl. $(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})(z_2) = \max\langle \mathrm{img}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}), <\rangle$ (–)

impl. $(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})(z_2) = \max\langle \mathrm{img}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}), <\rangle$ **and** (C6)
$(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})(z_2) \neq \emptyset$

impl. $\mathsf{tail}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})(z_2) = \max\langle \mathrm{img}\,(\mathsf{tail}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})), <\rangle$
(Thm. VII.2.3:2)

impl. $(\mathsf{tail}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}))(z_2) = \max\langle \mathrm{img}\,(\mathsf{tail}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})), <\rangle$
(Lem. VII.2.7:3)

- **C8.** Conclude:

$a = \mathsf{head}\,\Phi(z_1)$ (C1)

impl. $a = \min\langle \Phi(z_1), <\rangle$ (Fig. VII.2.2)

impl. $a \notin \Phi(z_1) \setminus \{\min\langle \Phi(z_1), <\rangle\}$ (–)

impl. $a \notin \mathsf{tail}\,\Phi(z_1)$ (Fig. VII.2.2)

impl. $a \notin \mathsf{tail}\,\{z_1 \mapsto \Phi(z_1)\}(z_1)$ (–)

impl. $a \notin \mathsf{tail}\,\{z_1 \mapsto \Phi(z_1)\}(\tilde{z})$ **for-all** $\tilde{z} \in \mathrm{dom}\,\{z_1 \mapsto \Phi(z_1)\}$ (–)

- **C9.** Conclude:

$\Phi(\tilde{z}) < \Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}})$ **for-all** $\tilde{z} \in \operatorname{dom}\Phi, \tilde{z}_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}$ (A4)
impl. $\Phi(z_1) < \Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}})$ **for-all** $\tilde{z}_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}$ (B2)
impl. $\Big[\mathsf{head}\,\Phi(z_1) < \mathsf{head}\,\Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}})$ **or** $\Phi(z_1) = \emptyset\Big]$ **for-all** $\tilde{z}_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}$ (Fig. VII.2.3)
impl. $\mathsf{head}\,\Phi(z_1) < \mathsf{head}\,\Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}})$ **for-all** $\tilde{z}_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}$ (B4)
impl. $a < \mathsf{head}\,\Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}})$ **for-all** $\tilde{z}_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}$ (C1)
impl. $a < \min\langle\Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}}), <\rangle$ **for-all** $\tilde{z}_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}$ (Fig. VII.2.2)
impl. $a \notin \Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}}) \setminus \{\min\langle\Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}}), <\rangle\}$ **for-all** $\tilde{z}_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}$ (–)
impl. $a \notin \mathsf{tail}\,\Phi_{\mathsf{gr}}(\tilde{z}_{\mathsf{gr}})$ **for-all** $\tilde{z}_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}$ (Fig. VII.2.2)

- **C10.** Conclude:

$\Big[a \notin \Phi_{\mathsf{co}}(\tilde{z})$ **and** $\Phi_{\mathsf{co}}(\tilde{z}) \neq \emptyset\Big]$ **for-all** $\tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}}$ (A5, B5)
impl. $a \notin \Phi_{\mathsf{co}}(\tilde{z}) \setminus \{\min\langle\Phi_{\mathsf{co}}(\tilde{z}), <\rangle\}$ **for-all** $\tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}}$ (Fig. VII.2.1:3)
impl. $a \notin \mathsf{tail}\,\Phi_{\mathsf{co}}(\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}}$ (Fig. VII.2.2)

- **C11.** Conclude:

$\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}} \in \operatorname{dom}\mathsf{len}$ (Step)
impl. $\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}} \in \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle$ (Lem. VII.2.9)
impl. $\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}} \in \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle$ **and** $z_1 \in \operatorname{dom}\Phi$ (B2)
impl. $(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}) \cup \{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}} \in \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle$ (–)
impl. $\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}} \in \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle$ (–)

- **C12.** Conclude:

$\left[\begin{array}{l} a \notin \mathsf{tail}\,\{z_1 \mapsto \Phi(z_1)\}(\tilde{z}) \\ \quad \textbf{for-all}\ \tilde{z} \in \operatorname{dom}\{z_1 \mapsto \Phi(z_1)\}\end{array}\right]$ **and** (C8, C9, C10, C11)
$\Big[a \notin \mathsf{tail}\,\Phi_{\mathsf{gr}}(\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom}\Phi_{\mathsf{gr}}\Big]$ **and**
$\Big[a \notin \mathsf{tail}\,\Phi_{\mathsf{co}}(\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom}\Phi_{\mathsf{co}}\Big]$ **and** $\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}} \in \operatorname{fam}\langle\mathbb{Z}, 2^{\mathbb{A}}\rangle$
impl. $a \notin \mathsf{tail}\,(\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(\tilde{z})$ (–)
for-all $\tilde{z} \in \operatorname{dom}(\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})$
impl. $a \notin (\mathsf{tail}\,(\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(\tilde{z})$ (Lem. VII.2.7:3)
for-all $\tilde{z} \in \operatorname{dom}(\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})$
impl. $a \notin (\mathsf{tail}\,(\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(\tilde{z})$ (Lem. VII.2.7:2)
for-all $\tilde{z} \in \operatorname{dom}(\mathsf{tail}\,(\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))$

- **C13.** Conclude:

$a \notin (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2)$
impl. $a \notin (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_2)$ **and** $z_2 \in \operatorname{dom}\Phi$ (B2)
impl. $a \notin \Phi(z_2)$ (–)
impl. **false** (B3)

Conclude:

$a \notin \bigcup \mathrm{img}\,(((\mathsf{tail}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})) \cup (\mathsf{tail}\,(\{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))) \mathbin{\mathsf{to}} z_2[a])$ (C5, C7, C12 $\Rightarrow$ Thm. VII.2.9:1)

impl. $a \notin \bigcup \mathrm{img}\,((\mathsf{tail}\,((\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}) \cup \{z_1 \mapsto \Phi(z_1)\} \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})) \mathbin{\mathsf{to}} z_2[a])$ (Lem. VII.2.7:4)

impl. $a \notin \bigcup \mathrm{img}\,((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})) \mathbin{\mathsf{to}} z_2[a])$ (–)

impl. $a \notin \bigcup \mathrm{img}\,(\mathsf{tail}\,((\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}) \mathbin{\mathsf{to}} z_2[a]))$ (Step, C13, C4 $\Rightarrow$ Thm. VII.2.6:2)

impl. $a \notin \bigcup \mathrm{img}\,(\mathsf{tail}\,((\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}) \mathbin{\mathsf{from}} z_1[a] \mathbin{\mathsf{to}} z_2[a]))$ (Base)

- **Step.** $(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}) \mathbin{\mathsf{from}} z_1[a] = (\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})) \mathbin{\mathsf{from}} z_1[a]$ **and**
  $\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}} \in \mathrm{dom}\,\mathsf{len}$ **and**
  $a \in (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(z_1)$ **and** $a \neq (\mathsf{head}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))(z_1)$

  - **D1.** Conclude:

    $\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})$

    $= (\mathsf{tail}\,\Phi) \cup (\mathsf{tail}\,\Phi_{\mathsf{gr}}) \cup (\mathsf{tail}\,\Phi_{\mathsf{co}})$ (Step $\Rightarrow$ Lem. VII.2.7:4)

  - **D2.** Conclude:

    $\langle (\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}) \mathbin{\mathsf{from}} z_1[a], z_2[a] \rangle \in \mathrm{dom}\,\mathsf{to}$ (A1)

    impl. $\langle (\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})) \mathbin{\mathsf{from}} z_1[a], z_2[a] \rangle \in \mathrm{dom}\,\mathsf{to}$ (Step)

    impl. $\langle (\mathsf{tail}\,\Phi) \cup (\mathsf{tail}\,\Phi_{\mathsf{gr}}) \cup (\mathsf{tail}\,\Phi_{\mathsf{co}}) \mathbin{\mathsf{from}} z_1[a], z_2[a] \rangle \in \mathrm{dom}\,\mathsf{to}$ (Lem. VII.2.7:4)

  - **D3.** Conclude:

    $\Phi(z_1) = \max \langle \mathrm{img}\,\Phi, < \rangle$ **and** $\Phi(z_1) \neq \emptyset$ (A2, B4)

    impl. $\mathsf{tail}\,\Phi(z_1) = \max \langle \mathrm{img}\,(\mathsf{tail}\,\Phi), < \rangle$ (Thm. VII.2.3:2)

    impl. $(\mathsf{tail}\,\Phi)(z_1) = \max \langle \mathrm{img}\,(\mathsf{tail}\,\Phi), < \rangle$ (Lem. VII.2.7:3)

  - **D4.** Conclude:

    $\Phi(z_2) = \max \langle \mathrm{img}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\}), < \rangle$ **and** $\Phi(z_2) \neq \emptyset$ (A3, B4)

    impl. $\mathsf{tail}\,\Phi(z_2) = \max \langle \mathrm{img}\,(\mathsf{tail}\,(\Phi \setminus \{z_1 \mapsto \Phi(z_1)\})), < \rangle$ (Thm. VII.2.3:2)

    impl. $\mathsf{tail}\,\Phi(z_2) = \max \langle \mathrm{img}\,((\mathsf{tail}\,\Phi) \setminus (\mathsf{tail}\,\{z_1 \mapsto \Phi(z_1)\})), < \rangle$ (Lem. VII.2.7:5)

    impl. $\mathsf{tail}\,\Phi(z_2) = \max \langle \mathrm{img}\,((\mathsf{tail}\,\Phi) \setminus \{z_1 \mapsto \mathsf{tail}\,\Phi(z_1)\}), < \rangle$ (Fig. VII.2.5)

    impl. $(\mathsf{tail}\,\Phi)(z_2) = \max \langle \mathrm{img}\,((\mathsf{tail}\,\Phi) \setminus \{z_1 \mapsto (\mathsf{tail}\,\Phi)(z_1)\}), < \rangle$ (Lem. VII.2.7:3)

  - **D5.** Conclude:

    $(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})(\tilde{z}) \neq \emptyset$ **for-all** $\tilde{z} \in \mathrm{dom}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})$ (Step $\Rightarrow$ Lem. VII.2.9:3)

    impl. $\Phi(\tilde{z}) \neq \emptyset$ **for-all** $\tilde{z} \in \mathrm{dom}\,\Phi$ (–)

- **D6.** Conclude:

$$
\begin{aligned}
& \Big[\Phi(\tilde z) < \Phi_{\mathsf{gr}}(\tilde z_{\mathsf{gr}}) \ \textbf{for-all}\ \tilde z \in \operatorname{dom}\Phi, \tilde z_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}}\Big] && \text{(A4)}\\
\textbf{impl.}\ & \Big[\mathsf{tail}\,\Phi(\tilde z) < \mathsf{tail}\,\Phi_{\mathsf{gr}}(\tilde z_{\mathsf{gr}}) \ \textbf{or}\ \Phi(\tilde z) = \emptyset\Big] \ \textbf{for-all}\ \tilde z \in \operatorname{dom}\Phi, \tilde z_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}} && \text{(Fig. VII.2.3)}\\
\textbf{impl.}\ & \mathsf{tail}\,\Phi(\tilde z) < \mathsf{tail}\,\Phi_{\mathsf{gr}}(\tilde z_{\mathsf{gr}}) \ \textbf{for-all}\ \tilde z \in \operatorname{dom}\Phi, \tilde z_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}} && \text{(D5)}\\
\textbf{impl.}\ & (\mathsf{tail}\,\Phi)(\tilde z) < (\mathsf{tail}\,\Phi_{\mathsf{gr}})(\tilde z_{\mathsf{gr}}) \ \textbf{for-all}\ \tilde z \in \operatorname{dom}\Phi, \tilde z_{\mathsf{gr}} \in \operatorname{dom}\Phi_{\mathsf{gr}} && \text{(Lem. VII.2.7:3)}\\
\textbf{impl.}\ & (\mathsf{tail}\,\Phi)(\tilde z) < (\mathsf{tail}\,\Phi_{\mathsf{gr}})(\tilde z_{\mathsf{gr}}) \ \textbf{for-all}\ \tilde z \in \operatorname{dom}(\mathsf{tail}\,\Phi), \tilde z_{\mathsf{gr}} \in \operatorname{dom}(\mathsf{tail}\,\Phi_{\mathsf{gr}}) && \text{(Lem. VII.2.7:2)}
\end{aligned}
$$

- **D7.** Conclude:

$$
\begin{aligned}
& \Big[a \notin \Phi_{\mathsf{co}}(\tilde z) \ \textbf{and}\ \Phi_{\mathsf{co}}(\tilde z) \neq \emptyset\Big] \ \textbf{for-all}\ \tilde z \in \operatorname{dom}\Phi_{\mathsf{co}} && \text{(A5, B5)}\\
\textbf{impl.}\ & a \notin \Phi_{\mathsf{co}}(\tilde z) \setminus \{\min\langle \Phi_{\mathsf{co}}(\tilde z), <\rangle\} \ \textbf{for-all}\ \tilde z \in \operatorname{dom}\Phi_{\mathsf{co}} && \text{(Fig. VII.2.1:3)}\\
\textbf{impl.}\ & a \notin \mathsf{tail}\,\Phi_{\mathsf{co}}(\tilde z) \ \textbf{for-all}\ \tilde z \in \operatorname{dom}\Phi_{\mathsf{co}} && \text{(Fig. VII.2.2)}\\
\textbf{impl.}\ & a \notin (\mathsf{tail}\,\Phi_{\mathsf{co}})(\tilde z) \ \textbf{for-all}\ \tilde z \in \operatorname{dom}\Phi_{\mathsf{co}} && \text{(Lem. VII.2.7:3)}\\
\textbf{impl.}\ & a \notin (\mathsf{tail}\,\Phi_{\mathsf{co}})(\tilde z) \ \textbf{for-all}\ \tilde z \in \operatorname{dom}(\mathsf{tail}\,\Phi_{\mathsf{co}}) && \text{(Lem. VII.2.7:2)}
\end{aligned}
$$

Conclude:

$$
\begin{aligned}
& a \notin \bigcup \operatorname{img}(\mathsf{tail}\,(((\mathsf{tail}\,\Phi) \cup (\mathsf{tail}\,\Phi_{\mathsf{gr}}) \cup (\mathsf{tail}\,\Phi_{\mathsf{co}}))\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])) \\
& && \text{(D2, D3, D4, D6, D7} \Rightarrow \text{Induction+D1)}\\
\textbf{impl.}\ & a \notin \bigcup \operatorname{img}(\mathsf{tail}\,((\mathsf{tail}\,(\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}}))\ \mathsf{from}\ z[a]\ \mathsf{to}\ z_2[a])) && \text{(Lem. VII.2.7:4)}\\
\textbf{impl.}\ & a \notin \bigcup \operatorname{img}(\mathsf{tail}\,((\Phi \cup \Phi_{\mathsf{gr}} \cup \Phi_{\mathsf{co}})\ \mathsf{from}\ z[a]\ \mathsf{to}\ z_2[a])) && \text{(Step)}
\end{aligned}
$$

QED.

VIII.10 Proof of Theorem VII.3.1

By case distinction (Fig. VII.3.1):

- **Case.** $\hat C = \{z_i : \hat D_i\}_{i \in I}$

  Conclude:

$$
\begin{aligned}
& \operatorname{dom}[\![\hat C]\!] \\
=\ & \operatorname{dom}[\![\{z_i : \hat D_i\}_{i\in I}]\!] && \text{(Case)}\\
=\ & \operatorname{dom}\{z_i \mapsto [\![\hat D_i]\!] \mid i \in I\} && \text{(Fig. VII.3.4)}\\
=\ & \{z_i \mid i \in I\} && \text{(–)}\\
=\ & \mathsf{vars}(\{z_i : \hat D_i\}_{i\in I}) && \text{(Fig. VII.3.2)}\\
=\ & \mathsf{vars}(\hat C) && \text{(Case)}
\end{aligned}
$$

QED.

VIII.11 Proof of Theorem VII.3.2

Proof of (1)

Conclude:

$$\begin{aligned}
& \Delta(\check{E}_1, \check{E}_2)\, \langle\!\langle \psi \rangle\!\rangle \\
= \;& \check{E}_2 \text{-} \check{E}_1\, \langle\!\langle \psi \rangle\!\rangle && \text{(Fig. VII.3.5)} \\
= \;& (\check{E}_2\, \langle\!\langle \psi \rangle\!\rangle) \text{-} (\check{E}_1\, \langle\!\langle \psi \rangle\!\rangle) && \text{(Fig. VII.3.3)} \\
= \;& \Delta(\check{E}_1\, \langle\!\langle \psi \rangle\!\rangle, \check{E}_2\, \langle\!\langle \psi \rangle\!\rangle) && \text{(Fig. VII.3.5)}
\end{aligned}$$

QED.

Proof of (2)

Conclude:

$$\begin{aligned}
& [\![\Delta(\hat{E}_1, \hat{E}_2)]\!] \\
= \;& [\![\hat{E}_2 \text{-} \hat{E}_1]\!] && \text{(Fig. VII.3.5)} \\
= \;& [\![\hat{E}_2]\!] + (-[\![\hat{E}_1]\!]) && \text{(Fig. VII.3.4)} \\
= \;& \delta([\![\hat{E}_1]\!], [\![\hat{E}_2]\!]) && \text{(p25)}
\end{aligned}$$

QED.

VIII.12 Proof of Theorem VII.3.3

Proof of (1)

By case distinction (Fig. VII.3.1):

- **Case.** $\check{D}_1 = \check{E}_1^{\mathsf{lo}} \,..\, \check{E}_1^{\mathsf{hi}}$ **and** $\check{D}_2 = \check{E}_2^{\mathsf{lo}} \,..\, \check{E}_2^{\mathsf{hi}}$

  Conclude:

$$\begin{aligned}
& \Delta(\check{D}_1, \check{D}_2)\, \langle\!\langle \psi \rangle\!\rangle \\
= \;& \Delta(\check{E}_1^{\mathsf{lo}} \,..\, \check{E}_1^{\mathsf{hi}}, \check{E}_2^{\mathsf{lo}} \,..\, \check{E}_2^{\mathsf{hi}})\, \langle\!\langle \psi \rangle\!\rangle && \text{(Case)} \\
= \;& \Delta(\check{E}_1^{\mathsf{lo}}, \check{E}_2^{\mathsf{lo}})\, \langle\!\langle \psi \rangle\!\rangle && \text{(Fig. VII.3.5)} \\
= \;& \Delta(\check{E}_1^{\mathsf{lo}}\, \langle\!\langle \psi \rangle\!\rangle, \check{E}_2^{\mathsf{lo}}\, \langle\!\langle \psi \rangle\!\rangle) && \text{(Thm. VII.3.2:1)} \\
= \;& \Delta((\check{E}_1^{\mathsf{lo}}\, \langle\!\langle \psi \rangle\!\rangle) \,..\, (\check{E}_1^{\mathsf{hi}}\, \langle\!\langle \psi \rangle\!\rangle), (\check{E}_2^{\mathsf{lo}}\, \langle\!\langle \psi \rangle\!\rangle) \,..\, (\check{E}_2^{\mathsf{hi}}\, \langle\!\langle \psi \rangle\!\rangle)) && \text{(Fig. VII.3.5)} \\
= \;& \Delta(\check{E}_1^{\mathsf{lo}} \,..\, \check{E}_1^{\mathsf{hi}}\, \langle\!\langle \psi \rangle\!\rangle, \check{E}_2^{\mathsf{lo}} \,..\, \check{E}_2^{\mathsf{hi}}\, \langle\!\langle \psi \rangle\!\rangle) && \text{(Fig. VII.3.3)} \\
= \;& \Delta(\check{D}_1\, \langle\!\langle \psi \rangle\!\rangle, \check{D}_2\, \langle\!\langle \psi \rangle\!\rangle) && \text{(Case)}
\end{aligned}$$

QED.

Proof of (2)

- **A1.** $[\![\nabla(\hat{D}_1)]\!] = [\![\nabla(\hat{D}_2)]\!] \preceq^{\text{-}1} 0$

By case distinction (Fig. VII.3.1):

- **Case.** $\hat{D}_1 = \hat{E}_1^{\mathsf{lo}} \mathinner{..} \hat{E}_1^{\mathsf{hi}}$ **and** $\hat{D}_2 = \hat{E}_2^{\mathsf{lo}} \mathinner{..} \hat{E}_2^{\mathsf{hi}}$

  - **B1.** Conclude:

$$\begin{aligned}
& [\![\nabla(\hat{D}_1)]\!] = [\![\nabla(\hat{D}_2)]\!] \preceq^{\text{-}1} 0 && \text{(A1)}\\
\textbf{impl. } & [\![\nabla(\hat{E}_1^{\mathsf{lo}} \mathinner{..} \hat{E}_1^{\mathsf{hi}})]\!] = [\![\nabla(\hat{E}_2^{\mathsf{lo}} \mathinner{..} \hat{E}_2^{\mathsf{hi}})]\!] \preceq^{\text{-}1} 0 && \text{(Case)}\\
\textbf{impl. } & [\![\Delta(\hat{E}_1^{\mathsf{lo}}, \hat{E}_1^{\mathsf{hi}})]\!] = [\![\Delta(\hat{E}_2^{\mathsf{lo}}, \hat{E}_2^{\mathsf{hi}})]\!] \preceq^{\text{-}1} 0 && \text{(Fig. VII.3.5)}\\
\textbf{impl. } & \delta([\![\hat{E}_1^{\mathsf{lo}}]\!], [\![\hat{E}_1^{\mathsf{hi}}]\!]) = \delta([\![\hat{E}_2^{\mathsf{lo}}]\!], [\![\hat{E}_2^{\mathsf{hi}}]\!]) \preceq^{\text{-}1} 0 && \text{(Thm. VII.3.2:2)}\\
\textbf{impl. } & \{\tilde{a}_1 + \delta([\![\hat{E}_1^{\mathsf{lo}}]\!], [\![\hat{E}_2^{\mathsf{lo}}]\!]) \mid [\![\hat{E}_1^{\mathsf{lo}}]\!] \preceq \tilde{a}_1 \preceq [\![\hat{E}_1^{\mathsf{hi}}]\!]\} = && \text{(Lem. VII.2.1:2)}\\
& \{\tilde{a}_2 \mid [\![\hat{E}_2^{\mathsf{lo}}]\!] \preceq \tilde{a}_2 \preceq [\![\hat{E}_2^{\mathsf{hi}}]\!]\} \neq \emptyset &&
\end{aligned}$$

  Conclude:

$$\begin{aligned}
& [\![\Delta(\hat{D}_1, \hat{D}_2)]\!] && \\
= \; & [\![\Delta(\hat{E}_1^{\mathsf{lo}} \mathinner{..} \hat{E}_1^{\mathsf{hi}}, \hat{E}_2^{\mathsf{lo}} \mathinner{..} \hat{E}_2^{\mathsf{hi}})]\!] && \text{(Case)}\\
= \; & [\![\Delta(\hat{E}_1^{\mathsf{lo}}, \hat{E}_2^{\mathsf{lo}})]\!] && \text{(Fig. VII.3.5)}\\
= \; & \delta([\![\hat{E}_1^{\mathsf{lo}}]\!], [\![\hat{E}_2^{\mathsf{lo}}]\!]) && \text{(Thm. VII.3.2:2)}\\
= \; & \delta(\{\tilde{a}_1 \mid [\![\hat{E}_1^{\mathsf{lo}}]\!] \preceq \tilde{a}_1 \preceq [\![\hat{E}_1^{\mathsf{hi}}]\!]\}, \{\tilde{a}_2 \mid [\![\hat{E}_2^{\mathsf{lo}}]\!] \preceq \tilde{a}_2 \preceq [\![\hat{E}_2^{\mathsf{hi}}]\!]\}) && \text{(B1} \Rightarrow \text{Fig. VII.2.2)}\\
= \; & \delta([\![\hat{E}_1^{\mathsf{lo}} \mathinner{..} \hat{E}_1^{\mathsf{hi}}]\!], [\![\hat{E}_2^{\mathsf{lo}} \mathinner{..} \hat{E}_2^{\mathsf{hi}}]\!]) && \text{(Fig. VII.3.4)}\\
= \; & \delta([\![D_1]\!], [\![D_2]\!]) && \text{(Case)}
\end{aligned}$$

QED.

VIII.13 Proof of Theorem VII.3.4

- **A1.** $\langle z_1, z_2 \rangle \in \operatorname{dom} \Delta(\check{C})$

By case distinction (Fig. VII.3.1):

- **Case.** $\check{C} = \{z_i : \check{E}_i^{\mathsf{lo}} \mathinner{..} \check{E}_i^{\mathsf{hi}}\}_{i \in I}$

  Conclude:

$$\begin{aligned}
& \Delta(\check{C})(z_1, z_2) \langle\!\langle \psi \rangle\!\rangle && \\
= \; & \Delta(\{z_i : \check{E}_i^{\mathsf{lo}} \mathinner{..} \check{E}_i^{\mathsf{hi}}\}_{i \in I})(z_1, z_2) \langle\!\langle \psi \rangle\!\rangle && \text{(A1, Case)}\\
= \; & \{\langle z_{i_1}, z_{i_2} \rangle \mapsto \Delta(\check{E}_{i_1}^{\mathsf{lo}} \mathinner{..} \check{E}_{i_1}^{\mathsf{hi}}, \check{E}_{i_2}^{\mathsf{lo}} \mathinner{..} \check{E}_{i_2}^{\mathsf{hi}}) \mid i_1, i_2 \in I\}(z_1, z_2) \langle\!\langle \psi \rangle\!\rangle && \text{(Fig. VII.3.5)}\\
= \; & \Delta(\check{E}_1^{\mathsf{lo}} \mathinner{..} \check{E}_1^{\mathsf{hi}}, \check{E}_2^{\mathsf{lo}} \mathinner{..} \check{E}_2^{\mathsf{hi}}) \langle\!\langle \psi \rangle\!\rangle \textbf{ and } 1, 2 \in I && \text{(–)}\\
= \; & \Delta(\check{E}_1^{\mathsf{lo}} \mathinner{..} \check{E}_1^{\mathsf{hi}} \langle\!\langle \psi \rangle\!\rangle, \check{E}_2^{\mathsf{lo}} \mathinner{..} \check{E}_2^{\mathsf{hi}} \langle\!\langle \psi \rangle\!\rangle) \textbf{ and } 1, 2 \in I && \text{(Thm. VII.3.3:1)}\\
= \; & \{\langle z_{i_1}, z_{i_2} \rangle \mapsto \Delta(\check{E}_{i_1}^{\mathsf{lo}} \mathinner{..} \check{E}_{i_1}^{\mathsf{hi}} \langle\!\langle \psi \rangle\!\rangle, \check{E}_{i_2}^{\mathsf{lo}} \mathinner{..} \check{E}_{i_2}^{\mathsf{hi}} \langle\!\langle \psi \rangle\!\rangle) \mid i_1, i_2 \in I\}(z_1, z_2) && \text{(–)}\\
= \; & \Delta(\{z_i : \check{E}_i^{\mathsf{lo}} \mathinner{..} \check{E}_i^{\mathsf{hi}} \langle\!\langle \psi \rangle\!\rangle\}_{i \in I})(z_1, z_2) && \text{(Fig. VII.3.5)}\\
= \; & \Delta(\{z_i : \check{E}_i^{\mathsf{lo}} \mathinner{..} \check{E}_i^{\mathsf{hi}}\}_{i \in I} \langle\!\langle \psi \rangle\!\rangle)(z_1, z_2) && \text{(Fig. VII.3.3)}\\
= \; & \Delta(\check{C} \langle\!\langle \psi \rangle\!\rangle)(z_1, z_2) && \text{(Case)}
\end{aligned}$$

QED.

VIII.14 Proof of Theorem VII.3.5

- **A1.** $z\,{:}\,\check{D} = \max\langle \check{C}, \ll\rangle$

By case distinction (Fig. VII.3.1):

- **Case.** $\check{C} = \{z_i\,{:}\,\check{E}^{\mathsf{lo}}_i \mathinner{..} \check{E}^{\mathsf{hi}}_i\}_{i\in I}$

  - **B1.** Conclude:

$$
\begin{array}{lll}
 & z\,{:}\,\check{D} = z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} & (\exists\tilde{\imath}) \\
\textsf{impl.} & z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} = \max\langle \check{C}, \ll\rangle & \text{(A1)} \\
\textsf{impl.} & z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} = \max\langle \{z_i\,{:}\,\check{E}^{\mathsf{lo}}_i \mathinner{..} \check{E}^{\mathsf{hi}}_i\}_{i\in I}, \ll\rangle & \text{(Case)} \\
\textsf{impl.} & z_i\,{:}\,\check{E}^{\mathsf{lo}}_i \mathinner{..} \check{E}^{\mathsf{hi}}_i \ll z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} \textsf{ for-all } i \in I\setminus\{\tilde{\imath}\} & \\
\textsf{impl.} & \left[\check{E}^{\mathsf{lo}}_i \langle\!\langle\tilde{\psi}\rangle\!\rangle, \check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\tilde{\psi}\rangle\!\rangle \in \hat{\mathbb{E}} \textsf{ impl. } [\![\check{E}^{\mathsf{lo}}_i \langle\!\langle\tilde{\psi}\rangle\!\rangle]\!] < [\![\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\tilde{\psi}\rangle\!\rangle]\!]\right] & \text{(Fig. VII.3.8)} \\
 & \textsf{for-all } \tilde{\psi} \in \boldsymbol{\Psi}, i \in I\setminus\{\tilde{\imath}\} & \\
\textsf{impl.} & \left[\begin{array}{l}\left[\check{E}^{\mathsf{lo}}_i \langle\!\langle\tilde{\psi}\rangle\!\rangle, \check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\tilde{\psi}\rangle\!\rangle \in \hat{\mathbb{E}} \textsf{ impl. } [\![\check{E}^{\mathsf{lo}}_i \langle\!\langle\tilde{\psi}\rangle\!\rangle]\!] < [\![\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\tilde{\psi}\rangle\!\rangle]\!]\right] \\ \textsf{for-all } \tilde{\psi} \in \boldsymbol{\Psi}, i \in I\setminus\{\tilde{\imath}\}\end{array}\right] \textsf{ and} & \text{(Lem. VII.3.6:3)} \\
 & \left[\begin{array}{l}\left[\begin{array}{c}\check{E}^{\mathsf{lo}}_i \langle\!\langle\psi\rangle\!\rangle \langle\!\langle\tilde{\psi}\rangle\!\rangle, \check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle \langle\!\langle\tilde{\psi}\rangle\!\rangle \in \hat{\mathbb{E}} \textsf{ impl.} \\ \check{E}^{\mathsf{lo}}_i \langle\!\langle\psi \cup (\tilde{\psi} \setminus \{k \mapsto \tilde{\psi}(k) \mid k \in (\operatorname{dom}\psi) \cap (\operatorname{dom}\tilde{\psi})\})\rangle\!\rangle, \\ \check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\psi \cup (\tilde{\psi} \setminus \{k \mapsto \tilde{\psi}(k) \mid k \in (\operatorname{dom}\psi) \cap (\operatorname{dom}\tilde{\psi})\})\rangle\!\rangle \in \hat{\mathbb{E}}\end{array}\right] \\ \textsf{for-all } \tilde{\psi} \in \boldsymbol{\Psi}, i \in I\setminus\{\tilde{\imath}\}\end{array}\right] & \\
\textsf{impl.} & \left[\begin{array}{c}\check{E}^{\mathsf{lo}}_i \langle\!\langle\psi\rangle\!\rangle \langle\!\langle\tilde{\psi}\rangle\!\rangle, \check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle \langle\!\langle\tilde{\psi}\rangle\!\rangle \in \hat{\mathbb{E}} \textsf{ impl.} \\ [\![\check{E}^{\mathsf{lo}}_i \langle\!\langle\psi \cup (\tilde{\psi} \setminus \{k \mapsto \tilde{\psi}(k) \mid k \in (\operatorname{dom}\psi) \cap (\operatorname{dom}\tilde{\psi})\})\rangle\!\rangle]\!] < \\ [\![\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\psi \cup (\tilde{\psi} \setminus \{k \mapsto \tilde{\psi}(k) \mid k \in (\operatorname{dom}\psi) \cap (\operatorname{dom}\tilde{\psi})\})\rangle\!\rangle]\!]\end{array}\right] & (-) \\
 & \textsf{for-all } \tilde{\psi} \in \boldsymbol{\Psi}, i \in I\setminus\{\tilde{\imath}\} & \\
\textsf{impl.} & \left[\check{E}^{\mathsf{lo}}_i \langle\!\langle\psi\rangle\!\rangle \langle\!\langle\tilde{\psi}\rangle\!\rangle, \check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle \langle\!\langle\tilde{\psi}\rangle\!\rangle \in \hat{\mathbb{E}} \textsf{ impl. } [\![\check{E}^{\mathsf{lo}}_i \langle\!\langle\psi\rangle\!\rangle \langle\!\langle\tilde{\psi}\rangle\!\rangle]\!] < [\![\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle \langle\!\langle\tilde{\psi}\rangle\!\rangle]\!]\right] & (-) \\
 & \textsf{for-all } \tilde{\psi} \in \boldsymbol{\Psi}, i \in I\setminus\{\tilde{\imath}\} & \\
\textsf{impl.} & z_i\,{:}\,(\check{E}^{\mathsf{lo}}_i \langle\!\langle\psi\rangle\!\rangle) \mathinner{..} (\check{E}^{\mathsf{hi}}_i \langle\!\langle\psi\rangle\!\rangle) \ll z_{\tilde{\imath}}\,{:}\,(\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle) \mathinner{..} (\check{E}^{\mathsf{hi}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle) & \text{(Fig. VII.3.8)} \\
\textsf{impl.} & z_i\,{:}\,\check{E}^{\mathsf{lo}}_i \mathinner{..} \check{E}^{\mathsf{hi}}_i \langle\!\langle\psi\rangle\!\rangle \ll z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle \textsf{ for-all } i \in I\setminus\{\tilde{\imath}\} & \text{(Fig. VII.3.3)}
\end{array}
$$

  - **B2.** Conclude:

$$
\begin{array}{lll}
 & z\,{:}\,\check{D} = z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} \textsf{ and } \tilde{\imath} \in I & (\exists\tilde{\imath}) \\
\textsf{impl.} & z_i\,{:}\,\check{E}^{\mathsf{lo}}_i \mathinner{..} \check{E}^{\mathsf{hi}}_i \langle\!\langle\psi\rangle\!\rangle \ll z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle \textsf{ for-all } i \in I\setminus\{\tilde{\imath}\} \textsf{ and } \tilde{\imath} \in I & \text{(B1)} \\
\textsf{impl.} & z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle = \max\langle \{z_i\,{:}\,\check{E}^{\mathsf{lo}}_i \mathinner{..} \check{E}^{\mathsf{hi}}_i \langle\!\langle\psi\rangle\!\rangle\}_{i\in I}, \ll\rangle & (-) \\
\textsf{impl.} & z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle = \max\langle \{z_i\,{:}\,\check{E}^{\mathsf{lo}}_i \mathinner{..} \check{E}^{\mathsf{hi}}_i\}_{i\in I} \langle\!\langle\psi\rangle\!\rangle, \ll\rangle & \text{(Fig. VII.3.3)} \\
\textsf{impl.} & z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} \langle\!\langle\psi\rangle\!\rangle = \max\langle \check{C} \langle\!\langle\psi\rangle\!\rangle, \ll\rangle & \text{(Case)}
\end{array}
$$

Conclude:

$$z\,{:}\,\check{D} = \max\,\langle \check{C}, \ll \rangle \tag{A1}$$

$$\textbf{impl. } z\,{:}\,\check{D} = \max\,\langle \{z_i\,{:}\,\check{E}^{\mathsf{lo}}_i \mathinner{..} \check{E}^{\mathsf{hi}}_i\}_{i\in I}, \ll \rangle \tag{Case}$$

$$\textbf{impl. } z\,{:}\,\check{D} = z_{\tilde{\imath}}\,{:}\,\check{E}^{\mathsf{lo}}_{\tilde{\imath}} \mathinner{..} \check{E}^{\mathsf{hi}}_{\tilde{\imath}} \textbf{ and } \tilde{\imath} \in I \tag{$\exists\tilde{\imath}$}$$

$$\textbf{impl. } z\,{:}\,\check{D}\,\langle\!\langle\psi\rangle\!\rangle = \max\,\langle \check{C}\,\langle\!\langle\psi\rangle\!\rangle, \ll \rangle \tag{B2}$$

QED.

VIII.15 Proof of Theorem VII.3.6

- **A1.** $\hat{C} \in \checkmark$

By case distinction (Fig. VII.3.1):

- **Case.** $\hat{C} = \{z_i\,{:}\,\hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i\in I}$

Conclude:

$$\hat{C} \in \checkmark \tag{A1}$$

$$\textbf{impl. } \{z_i\,{:}\,\hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i\in I} \in \checkmark \tag{Case}$$

$$\textbf{impl. } \llbracket \nabla(\hat{E}^{\mathsf{lo}}_{i_1} \mathinner{..} \hat{E}^{\mathsf{hi}}_{i_1}) \rrbracket = \llbracket \nabla(\hat{E}^{\mathsf{lo}}_{i_2} \mathinner{..} \hat{E}^{\mathsf{hi}}_{i_2}) \rrbracket \preceq^{\text{-}1} 0 \textbf{ for-all } i_1, i_2 \in I \tag{Fig. VII.3.9}$$

$$\textbf{impl. } \llbracket \Delta(\hat{E}^{\mathsf{lo}}_{i_1}, \hat{E}^{\mathsf{hi}}_{i_1}) \rrbracket = \llbracket \Delta(\hat{E}^{\mathsf{lo}}_{i_2}, \hat{E}^{\mathsf{hi}}_{i_2}) \rrbracket \preceq^{\text{-}1} 0 \textbf{ for-all } i_1, i_2 \in I \tag{Fig. VII.3.5}$$

$$\textbf{impl. } \delta(\llbracket \hat{E}^{\mathsf{lo}}_{i_1} \rrbracket, \llbracket \hat{E}^{\mathsf{hi}}_{i_1} \rrbracket) = \delta(\llbracket \hat{E}^{\mathsf{lo}}_{i_2} \rrbracket, \llbracket \hat{E}^{\mathsf{hi}}_{i_2} \rrbracket) \preceq^{\text{-}1} 0 \textbf{ for-all } i_1, i_2 \in I \tag{Thm. VII.3.2:2}$$

$$\textbf{impl. } \{\tilde{a}_1 + \delta(\llbracket \hat{E}^{\mathsf{lo}}_{i_1} \rrbracket, \llbracket \hat{E}^{\mathsf{lo}}_{i_2} \rrbracket) \mid \llbracket \hat{E}^{\mathsf{lo}}_{i_1} \rrbracket \preceq \tilde{a}_1 \preceq \llbracket \hat{E}^{\mathsf{hi}}_{i_1} \rrbracket\} = \{\tilde{a}_2 \mid \llbracket \hat{E}^{\mathsf{lo}}_{i_2} \rrbracket \preceq \tilde{a}_2 \preceq \llbracket \hat{E}^{\mathsf{hi}}_{i_2} \rrbracket\} \neq \emptyset \tag{Lem. VII.2.1:2}$$
$$\textbf{for-all } i_1, i_2 \in I$$

$$\textbf{impl. } |\{\tilde{a}_1 + \delta(\llbracket \hat{E}^{\mathsf{lo}}_{i_1} \rrbracket, \llbracket \hat{E}^{\mathsf{lo}}_{i_2} \rrbracket) \mid \llbracket \hat{E}^{\mathsf{lo}}_{i_1} \rrbracket \preceq \tilde{a}_1 \preceq \llbracket \hat{E}^{\mathsf{hi}}_{i_1} \rrbracket\}| = |\{\tilde{a}_2 \mid \llbracket \hat{E}^{\mathsf{lo}}_{i_2} \rrbracket \preceq \tilde{a}_2 \preceq \llbracket \hat{E}^{\mathsf{hi}}_{i_2} \rrbracket\}| > \mathfrak{0} \tag{$-$}$$
$$\textbf{for-all } i_1, i_2 \in I$$

$$\textbf{impl. } |\{\tilde{a}_1 \mid \llbracket \hat{E}^{\mathsf{lo}}_{i_1} \rrbracket \preceq \tilde{a}_1 \preceq \llbracket \hat{E}^{\mathsf{hi}}_{i_1} \rrbracket\}| = |\{\tilde{a}_2 \mid \llbracket \hat{E}^{\mathsf{lo}}_{i_2} \rrbracket \preceq \tilde{a}_2 \preceq \llbracket \hat{E}^{\mathsf{hi}}_{i_2} \rrbracket\}| > \mathfrak{0} \textbf{ for-all } i_1, i_2 \in I \tag{Fig. VII.2.1:1}$$

$$\textbf{impl. } |\llbracket \hat{E}^{\mathsf{lo}}_{i_1} \mathinner{..} \hat{E}^{\mathsf{hi}}_{i_1} \rrbracket| = |\llbracket \hat{E}^{\mathsf{lo}}_{i_2} \mathinner{..} \hat{E}^{\mathsf{lo}}_{i_2} \rrbracket| > \mathfrak{0} \textbf{ for-all } i_1, i_2 \in I \tag{Fig. VII.3.4:1}$$

$$\textbf{impl. } |\{z_i \mapsto \llbracket \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i \rrbracket \mid i \in I\}(\tilde{z}_1)| = |\{z_i \mapsto \llbracket \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i \rrbracket \mid i \in I\}(\tilde{z}_2)| > \mathfrak{0} \tag{$-$}$$
$$\textbf{for-all } \tilde{z}_1, \tilde{z}_2 \in \{\tilde{z}_i \mid i \in I\}$$

$$\textbf{impl. } |\llbracket \{z_i\,{:}\,\hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i\in I} \rrbracket(\tilde{z}_1)| = |\llbracket \{z_i\,{:}\,\hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i\in I} \rrbracket(\tilde{z}_2)| > \mathfrak{0} \tag{Fig. VII.3.4:1}$$
$$\textbf{for-all } \tilde{z}_1, \tilde{z}_2 \in \{\tilde{z}_i \mid i \in I\}$$

$$\textbf{impl. } |\llbracket \{z_i\,{:}\,\hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i\in I} \rrbracket(\tilde{z}_1)| = |\llbracket \{z_i\,{:}\,\hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i\in I} \rrbracket(\tilde{z}_2)| > \mathfrak{0} \tag{$-$}$$
$$\textbf{for-all } \tilde{z}_1, \tilde{z}_2 \in \{\tilde{z} \mid \tilde{z}\,{:}\,\tilde{\hat{D}} \in \{z_i\,{:}\,\hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i\in I}\}$$

$$\textbf{impl. } |\llbracket \hat{C} \rrbracket(\tilde{z}_1)| = |\llbracket \hat{C} \rrbracket(\tilde{z}_2)| > \mathfrak{0} \textbf{ for-all } \tilde{z}_1, \tilde{z}_2 \in \{\tilde{z} \mid \tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C}\} \tag{Case}$$

$$\textbf{impl. } |\llbracket \hat{C} \rrbracket(\tilde{z}_1)| = |\llbracket \hat{C} \rrbracket(\tilde{z}_2)| > \mathfrak{0} \textbf{ for-all } \tilde{z}_1, \tilde{z}_2 \in \{\tilde{z} \mid \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket\} \tag{Lem. VII.3.7:2}$$

$$\textbf{impl. } |\llbracket \hat{C} \rrbracket(\tilde{z}_1)| = |\llbracket \hat{C} \rrbracket(\tilde{z}_2)| > \mathfrak{0} \textbf{ for-all } \tilde{z}_1, \tilde{z}_2 \in \operatorname{dom} \llbracket \hat{C} \rrbracket \tag{$-$}$$

$$\textbf{impl. } \mathfrak{n} = |\llbracket \hat{C} \rrbracket(\tilde{z})| > \mathfrak{0} \textbf{ for-all } \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket \tag{$\exists\mathfrak{n}$}$$

$$\textbf{impl. } \mathsf{len}\,\llbracket \hat{C} \rrbracket > \mathfrak{0} \tag{Fig. VII.2.5}$$

QED.

VIII.16 Proof of Theorem VII.3.7

Proof of (1)

- **A1.** $\hat{C} \in \checkmark$

By case distinction (Fig. VII.3.1):

- **Case.** $\hat{C} = \{z_i : \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i \in I}$

  - **B1.** Conclude:

$\langle z_1, z_2 \rangle \in \{\langle \tilde{z}_1, \tilde{z}_2 \rangle \mid \langle \llbracket \hat{C} \rrbracket(\tilde{z}_1), \llbracket \hat{C} \rrbracket(\tilde{z}_2) \rangle \in \operatorname{dom} \delta\}$ ($\exists z_1$, $\exists z_2$)
impl. $\langle \llbracket \hat{C} \rrbracket(z_1), \llbracket \hat{C} \rrbracket(z_2) \rangle \in \operatorname{dom} \delta$ (–)
impl. $z_1, z_2 \in \operatorname{dom} \llbracket \hat{C} \rrbracket$ (–)
impl. $z_1, z_2 \in \operatorname{dom} \llbracket \{z_i : \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i \in I} \rrbracket$ (Case)
impl. $z_1, z_2 \in \operatorname{dom} \{z_i \mapsto \llbracket \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i \rrbracket \mid i \in I\}$ (Fig. VII.3.4)
impl. $z_1, z_2 \in \{z_i \mid i \in I\}$ (–)
impl. $\langle z_1, z_2 \rangle \in \{\langle z_{i_1}, z_{i_2} \rangle \mid i_1, i_2 \in I\}$ (–)

  - **B2.** Conclude:

$\hat{C} \in \checkmark$ (A1)
impl. $\{z_i : \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i \in I} \in \checkmark$ (Case)
impl. $\llbracket \nabla(\hat{E}^{\mathsf{lo}}_{i_1} \mathinner{..} \hat{E}^{\mathsf{hi}}_{i_1}) \rrbracket = \llbracket \nabla(\hat{E}^{\mathsf{lo}}_{i_2} \mathinner{..} \hat{E}^{\mathsf{hi}}_{i_2}) \rrbracket \preceq^{\text{-}1} 0$ **for-all** $i_1, i_2 \in I$ (Fig. VII.3.9)

  - **B3.** Conclude:

$1, 2 \in I$ (–)
impl. $\llbracket \Delta(\hat{E}^{\mathsf{lo}}_1, \hat{E}^{\mathsf{hi}}_1) \rrbracket = \llbracket \Delta(\hat{E}^{\mathsf{lo}}_2, \hat{E}^{\mathsf{hi}}_2) \rrbracket \preceq^{\text{-}1} 0$ (B2)
impl. $\delta(\llbracket \hat{E}^{\mathsf{lo}}_1 \rrbracket, \llbracket \hat{E}^{\mathsf{hi}}_1 \rrbracket) = \delta(\llbracket \hat{E}^{\mathsf{lo}}_2 \rrbracket, \llbracket \hat{E}^{\mathsf{hi}}_2 \rrbracket) \preceq^{\text{-}1} 0$ (Thm. VII.3.2:2)
impl. $\{\tilde{a}_1 + \delta(\llbracket \hat{E}^{\mathsf{lo}}_1 \rrbracket, \llbracket \hat{E}^{\mathsf{lo}}_2 \rrbracket) \mid \llbracket \hat{E}^{\mathsf{lo}}_1 \rrbracket \preceq \tilde{a}_1 \preceq \llbracket \hat{E}^{\mathsf{hi}}_1 \rrbracket\} =$ (Lem. VII.2.1:2)
$\{\tilde{a}_2 \mid \llbracket \hat{E}^{\mathsf{lo}}_2 \rrbracket \preceq \tilde{a}_2 \preceq \llbracket \hat{E}^{\mathsf{hi}}_2 \rrbracket\} \neq \emptyset$
impl. $\{\tilde{a}_1 + \delta(\llbracket \hat{E}^{\mathsf{lo}}_1 \rrbracket, \llbracket \hat{E}^{\mathsf{lo}}_2 \rrbracket) \mid \tilde{a}_1 \in \{\tilde{a} \mid \llbracket \hat{E}^{\mathsf{lo}}_1 \rrbracket \preceq \tilde{a} \preceq \llbracket \hat{E}^{\mathsf{hi}}_1 \rrbracket\}\} =$ (–)
$\{\tilde{a}_2 \mid \tilde{a}_2 \in \{\tilde{a} \mid \llbracket \hat{E}^{\mathsf{lo}}_2 \rrbracket \preceq \tilde{a} \preceq \llbracket \hat{E}^{\mathsf{hi}}_2 \rrbracket\}\} \neq \emptyset$
impl. $\{\tilde{a}_1 + \delta(\llbracket \hat{E}^{\mathsf{lo}}_1 \rrbracket, \llbracket \hat{E}^{\mathsf{lo}}_2 \rrbracket) \mid \tilde{a}_1 \in \llbracket \hat{E}^{\mathsf{lo}}_1 \mathinner{..} \hat{E}^{\mathsf{hi}}_1 \rrbracket\} = \{\tilde{a}_2 \mid \tilde{a}_2 \in \llbracket \hat{E}^{\mathsf{lo}}_2 \mathinner{..} \hat{E}^{\mathsf{hi}}_2 \rrbracket\} \neq \emptyset$
(Fig. VII.3.4)
impl. $\langle \llbracket \hat{E}^{\mathsf{lo}}_1 \mathinner{..} \hat{E}^{\mathsf{hi}}_1 \rrbracket, \llbracket \hat{E}^{\mathsf{lo}}_2 \mathinner{..} \hat{E}^{\mathsf{hi}}_2 \rrbracket \rangle \in \operatorname{dom} \delta$ (Fig. VII.2.2)

  - **B4.** Conclude:

$\langle z_1, z_2 \rangle \in \{\langle z_{i_1}, z_{i_2} \rangle \mid i_1, i_2 \in I\}$ ($\exists z_1$, $\exists z_2$)
impl. $1, 2 \in I$ (–)
impl. $1, 2 \in I$ **and** $\langle \llbracket \hat{E}^{\mathsf{lo}}_1 \mathinner{..} \hat{E}^{\mathsf{hi}}_1 \rrbracket, \llbracket \hat{E}^{\mathsf{lo}}_2 \mathinner{..} \hat{E}^{\mathsf{hi}}_2 \rrbracket \rangle \in \operatorname{dom} \delta$ (B3)
impl. $\langle \{z_i \mapsto \llbracket \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i \rrbracket \mid i \in I\}(z_1), \{z_i \mapsto \llbracket \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i \rrbracket \mid i \in I\}(z_2) \rangle \in \operatorname{dom} \delta$ (–)
impl. $\langle \llbracket \{z_i : \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i \in I} \rrbracket(z_1), \llbracket \{z_i : \hat{E}^{\mathsf{lo}}_i \mathinner{..} \hat{E}^{\mathsf{hi}}_i\}_{i \in I} \rrbracket(z_2) \rangle \in \operatorname{dom} \delta$ (Fig. VII.3.4)
impl. $\langle \llbracket \hat{C} \rrbracket(z_1), \llbracket \hat{C} \rrbracket(z_2) \rangle \in \operatorname{dom} \delta$ (Case)
impl. $\langle z_1, z_2 \rangle \in \{\langle \tilde{z}_1, \tilde{z}_2 \rangle \mid \langle \llbracket \hat{C} \rrbracket(\tilde{z}_1), \llbracket \hat{C} \rrbracket(\tilde{z}_2) \rangle \in \operatorname{dom} \delta\}$ (–)

Conclude:

$$\begin{aligned}
& \operatorname{dom}\delta[\![\hat{C}]\!] \\
={}& \operatorname{dom}\{\langle\tilde{z}_1,\tilde{z}_2\rangle \mapsto \delta([\![\hat{C}]\!](\tilde{z}_1),[\![\hat{C}]\!](\tilde{z}_2)) \mid \tilde{z}_1,\tilde{z}_2 \in \mathbb{Z}\} && \text{(Fig. VII.2.5)} \\
={}& \{\langle\tilde{z}_1,\tilde{z}_2\rangle \mid \langle[\![\hat{C}]\!](\tilde{z}_1),[\![\hat{C}]\!](\tilde{z}_2)\rangle \in \operatorname{dom}\delta\} && \text{(–)} \\
={}& \{\langle z_{i_1},z_{i_2}\rangle \mid i_1,i_2 \in I\} && \text{(B1, B4)} \\
={}& \operatorname{dom}\{\langle z_{i_1},z_{i_2}\rangle \mapsto \Delta(\hat{E}^{\mathsf{lo}}_{i_1}\,..\,\hat{E}^{\mathsf{hi}}_{i_1},\hat{E}^{\mathsf{lo}}_{i_2}\,..\,\hat{E}^{\mathsf{hi}}_{i_2}) \mid i_1,i_2 \in I\} && \text{(–)} \\
={}& \operatorname{dom}\Delta(\{z_i : \hat{E}^{\mathsf{lo}}_{i}\,..\,\hat{E}^{\mathsf{hi}}_{i}\}_{i\in I}) && \text{(Fig. VII.3.5)} \\
={}& \operatorname{dom}\Delta(\hat{C}) && \text{(Case)}
\end{aligned}$$

QED.

Proof of (2)

- **A1.** $\check{C} \in \checkmark$

By case distinction (Fig. VII.3.1):

- **Case.** $\hat{C} = \{z_i : \hat{D}_i\}_{i\in I}$

  Conclude:

$$\begin{aligned}
& \operatorname{dom}\delta[\![\hat{C}]\!] \\
={}& \operatorname{dom}\Delta(\hat{C}) && \text{(A1} \Rightarrow \text{Thm. VII.3.7:1)} \\
={}& \operatorname{dom}\Delta(\{z_i : \hat{D}_i\}_{i\in I}) && \text{(Case)} \\
={}& \operatorname{dom}\{\langle z_{i_1},z_{i_2}\rangle \mapsto \Delta(\hat{D}_{i_1},\hat{D}_{i_2}) \mid i_1,i_2 \in I\} && \text{(Fig. VII.3.5)} \\
={}& \{\langle z_{i_1},z_{i_2}\rangle \mid i_1,i_2 \in I\} && \text{(–)} \\
={}& \{z_i \mid i \in I\} \times \{z_i \mid i \in I\} && \text{(–)} \\
={}& \mathsf{vars}(\{z_i : \hat{D}_i\}_{i\in I}) \times \mathsf{vars}(\{z_i : \hat{D}_i\}_{i\in I}) && \text{(Fig. VII.3.2)} \\
={}& \mathsf{vars}(\hat{C}) \times \mathsf{vars}(\hat{C}) && \text{(Case)}
\end{aligned}$$

QED.

Proof of (3)

- **A1.** $\langle z_1,z_2\rangle \in \operatorname{dom}\delta[\![\hat{C}]\!]$
- **A2.** $\hat{C} \in \checkmark$

By case distinction (Fig. VII.3.1):

- **Case.** $\hat{C} = \{z_i : D_i\}_{i\in I}$
  - **B1.** Conclude:

$$\begin{aligned}
& \langle z_1,z_2\rangle \in \operatorname{dom}\Delta(\hat{C}) && \text{(A1)} \\
\textbf{impl. }& \langle z_1,z_2\rangle \in \operatorname{dom}\Delta(\{z_i : D_i\}_{i\in I}) && \text{(Case)} \\
\textbf{impl. }& \langle z_1,z_2\rangle \in \operatorname{dom}\{\langle z_{i_1},z_{i_2}\rangle \mapsto \Delta(\hat{D}_{i_1},\hat{D}_{i_2}) \mid i_1,i_2 \in I\} && \text{(Fig. VII.3.5)} \\
\textbf{impl. }& \langle z_1,z_2\rangle \in \{\langle z_{i_1},z_{i_2}\rangle \mid i_1,i_2 \in I\} && \text{(–)} \\
\textbf{impl. }& 1,2 \in I && \text{(–)}
\end{aligned}$$

- **B2.** Conclude:

$$\begin{array}{lll}
 & \hat{C} \in \checkmark & \text{(A1)} \\
\textbf{impl.} & \llbracket \nabla(\hat{D}_{i_1}) \rrbracket = \llbracket \nabla(\hat{D}_{i_2}) \rrbracket \preceq^{\text{-1}} 0 \;\; \textbf{for-all} \;\; i_1, i_2 \in I & \text{(Fig. VII.3.9)} \\
\textbf{impl.} & \llbracket \nabla(\hat{D}_1) \rrbracket = \llbracket \nabla(\hat{D}_2) \rrbracket \preceq^{\text{-1}} 0 & \text{(B1)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
 & \delta\llbracket \hat{C} \rrbracket(z_1, z_2) & \\
= & \{\langle \tilde{z}_1, \tilde{z}_2 \rangle \mapsto \delta(\llbracket \hat{C} \rrbracket(\tilde{z}_1), \llbracket \hat{C} \rrbracket(\tilde{z}_2)) \mid \tilde{z}_1, \tilde{z}_2 \in \mathbb{Z}\}(z_1, z_2) & \text{(A1, Fig. VII.2.5)} \\
= & \delta(\llbracket \hat{C} \rrbracket(z_1), \llbracket \hat{C} \rrbracket(z_2)) & (-) \\
= & \delta(\llbracket \{z_i : D_i\}_{i \in I} \rrbracket(z_1), \llbracket \{z_i : D_i\}_{i \in I} \rrbracket(z_2)) & \text{(Case)} \\
= & \delta(\{z_i \mapsto \llbracket \hat{D}_i \rrbracket \mid i \in I\}(z_1), \{z_i \mapsto \llbracket \hat{D}_i \rrbracket \mid i \in I\}(z_2)) & \text{(Fig. VII.3.4)} \\
= & \delta(\llbracket \hat{D}_1 \rrbracket, \llbracket \hat{D}_2 \rrbracket) & (-) \\
= & \llbracket \Delta(\hat{D}_1, \hat{D}_2) \rrbracket & \text{(B2} \Rightarrow \text{Thm. VII.3.3:2)} \\
= & \llbracket \{\langle z_{i_1}, z_{i_2} \rangle \mapsto \Delta(\hat{D}_{i_1}, \hat{D}_{i_2}) \mid i_1, i_2 \in I\}(z_1, z_2) \rrbracket & \text{(B1)} \\
= & \llbracket \Delta(\{z_i : D_i\}_{i \in I})(z_1, z_2) \rrbracket & \text{(Fig. VII.3.5)} \\
= & \llbracket \Delta(\hat{C})(z_1, z_2) \rrbracket & \text{(Case)}
\end{array}$$

QED.

Proof of (4)

- **A1.** $\langle z_1, z_2 \rangle \in \operatorname{dom} \delta\llbracket \hat{C} \rrbracket$
- **A2.** $z_1 = z_2$
- **A3.** $\hat{C} \in \checkmark$

Conclude:

$$\begin{array}{lll}
 & \langle z_1, z_2 \rangle \in \operatorname{dom} \delta\llbracket \hat{C} \rrbracket & \\
\textbf{impl.} & \langle z_1, z_2 \rangle \in \operatorname{dom} \{\langle \tilde{z}_1, \tilde{z}_2 \rangle \mapsto \delta(\llbracket \hat{C} \rrbracket(\tilde{z}_1), \llbracket \hat{C} \rrbracket(\tilde{z}_2)) \mid \tilde{z}_1, \tilde{z}_2 \in \mathbb{Z}\} & \text{(Fig. VII.2.5)} \\
\textbf{impl.} & \langle z_1, z_2 \rangle \in \{\langle \tilde{z}_1, \tilde{z}_2 \rangle \mid \langle \llbracket \hat{C} \rrbracket(\tilde{z}_1), \llbracket \hat{C} \rrbracket(\tilde{z}_2) \rangle \in \operatorname{dom} \delta\} & (-) \\
\textbf{impl.} & \langle \llbracket \hat{C} \rrbracket(z_1), \llbracket \hat{C} \rrbracket(z_2) \rangle \in \operatorname{dom} \delta & (-) \\
\textbf{impl.} & z_1, z_2 \in \operatorname{dom} \llbracket \hat{C} \rrbracket & (-) \\
\textbf{impl.} & \llbracket \hat{C} \rrbracket(z_1) = \llbracket \hat{C} \rrbracket(z_2) & \text{(A2)} \\
\textbf{impl.} & \langle z_1, z_2 \rangle \in \operatorname{dom} \delta\llbracket \hat{C} \rrbracket \;\; \textbf{and} \;\; \llbracket \hat{C} \rrbracket(z_1) = \llbracket \hat{C} \rrbracket(z_2) & \text{(A1)} \\
\textbf{impl.} & \delta\llbracket \hat{C} \rrbracket(z_1, z_2) = 0 & \text{(Lem. VII.2.8:4)}
\end{array}$$

QED.

Proof of (5)

- **A1.** $\langle z_1, z_2 \rangle \in \operatorname{dom} \delta\llbracket \hat{C} \rrbracket$
- **A2.** $z_1 \neq z_2$

- **A3.** $\hat{C} \in \checkmark$

By case distinction (Fig. VII.3.1):

- **Case.** $\hat{C} = \{z_i : D_i\}_{i \in I}$

  - **B1.** Conclude:

    $\hat{C} \in \checkmark$

    impl. $\{z_i : D_i\}_{i \in I} \in \checkmark$ (Case)

    impl. $\Big[\llbracket \nabla(\hat{D}_{i_1}) \rrbracket = \llbracket \nabla(\hat{D}_{i_2}) \rrbracket \preceq^{\text{-}1} 0$ **for-all** $i_1, i_2 \in I\Big]$ **and** (Fig. VII.3.9)
    $\Big[z_{i_1} \neq z_{i_2}$ **impl.** $\llbracket \Delta(\hat{D}_{i_1}, \hat{D}_{i_2}) \rrbracket \neq 0\Big]$ **for-all** $i_1, i_2 \in I$

  - **B2.** Conclude:

    $1, 2 \in I$ (–)

    impl. $\llbracket \nabla(\hat{D}_1) \rrbracket = \llbracket \nabla(\hat{D}_2) \rrbracket \preceq^{\text{-}1} 0$ **and** $\Big[z_1 \neq z_2$ **impl.** $\llbracket \Delta(\hat{D}_{i_1}, \hat{D}_{i_2}) \rrbracket \neq 0\Big]$ (B1)

    impl. $\llbracket \nabla(\hat{D}_1) \rrbracket = \llbracket \nabla(\hat{D}_2) \rrbracket \preceq^{\text{-}1} 0$ **and** $\llbracket \Delta(\hat{D}_{i_1}, \hat{D}_{i_2}) \rrbracket \neq 0$ (A2)

    impl. $\delta(\llbracket \hat{D}_{i_1} \rrbracket, \llbracket \hat{D}_{i_2} \rrbracket) \neq 0$ (Thm. VII.3.3:2)

    impl. $\llbracket \hat{D}_{i_1} \rrbracket \neq \llbracket \hat{D}_{i_2} \rrbracket$ (Lem. VII.2.4:2)

  Conclude:

  $\langle z_1, z_2 \rangle \in \operatorname{dom} \delta \llbracket \hat{C} \rrbracket$

  impl. $\langle z_1, z_2 \rangle \in \operatorname{dom} \{\langle \tilde{z}_1, \tilde{z}_2 \rangle \mapsto \delta(\llbracket \hat{C} \rrbracket(\tilde{z}_1), \llbracket \hat{C} \rrbracket(\tilde{z}_2)) \mid \tilde{z}_1, \tilde{z}_2 \in \mathbb{Z}\}$ (Fig. VII.2.5)

  impl. $\langle z_1, z_2 \rangle \in \{\langle \tilde{z}_1, \tilde{z}_2 \rangle \mid \langle \llbracket \hat{C} \rrbracket(\tilde{z}_1), \llbracket \hat{C} \rrbracket(\tilde{z}_2) \rangle \in \operatorname{dom} \delta\}$ (–)

  impl. $\langle \llbracket \hat{C} \rrbracket(z_1), \llbracket \hat{C} \rrbracket(z_2) \rangle \in \operatorname{dom} \delta$ (–)

  impl. $z_1, z_2 \in \operatorname{dom} \llbracket \hat{C} \rrbracket$ (–)

  impl. $z_1, z_2 \in \operatorname{dom} \llbracket \{z_i : \hat{D}_i\}_{i \in I} \rrbracket$ (Case)

  impl. $z_1, z_2 \in \operatorname{dom} \{z_i \mapsto \llbracket \hat{D}_i \rrbracket \mid i \in I\}$ (Fig. VII.3.4)

  impl. $z_1, z_2 \in \{z_i \mid i \in I\}$ (–)

  impl. $1, 2 \in I$ (–)

  impl. $1, 2 \in I$ **and** $\llbracket \hat{D}_{i_1} \rrbracket \neq \llbracket \hat{D}_{i_2} \rrbracket$ (B2)

  impl. $\{z_i \mapsto \llbracket \hat{D}_i \rrbracket \mid i \in I\}(z_1) \neq \{z_i \mapsto \llbracket \hat{D}_i \rrbracket \mid i \in I\}(z_2)$ (–)

  impl. $\llbracket \{z_i : D_i\}_{i \in I} \rrbracket(z_1) \neq \llbracket \{z_i : D_i\}_{i \in I} \rrbracket(z_2)$ (Fig. VII.3.4)

  impl. $\llbracket \hat{C} \rrbracket(z_1) \neq \llbracket \hat{C} \rrbracket(z_2)$ (Case)

  impl. $\langle z_1, z_2 \rangle \in \operatorname{dom} \delta \llbracket \hat{C} \rrbracket$ **and** $\llbracket \hat{C} \rrbracket(z_1) = \llbracket \hat{C} \rrbracket(z_2)$ (A1)

  impl. $\delta \llbracket \hat{C} \rrbracket(z_1, z_2) \neq 0$ (Lem. VII.2.8:5)

QED.

VIII.17 Proof of Theorem VII.3.8

Proof of (1)

- **A1.** $\hat{C} \in \checkmark$
- **A2.** $z_1 : \hat{D}_1, z_2 : \hat{D}_2 \in \hat{C}$
- **A3.** $z_1 : \hat{D}_1 \ll z_2 : \hat{D}_2$

By case distinction (Fig. VII.3.1):

- **Case.** $\hat{D}_1 = \hat{E}_1^{\mathsf{lo}} \mathinner{..} \hat{E}_1^{\mathsf{hi}}$ **and** $\hat{D}_2 = \hat{E}_2^{\mathsf{lo}} \mathinner{..} \hat{E}_2^{\mathsf{hi}}$
  - **B1.** Conclude:

$$\begin{array}{rll}
 & z_1 : \hat{D}_1 \ll z_2 : \hat{D}_2 & \text{(A3)} \\
\textsf{\textbf{impl.}} & z_1 : \hat{E}_1^{\mathsf{lo}} \mathinner{..} \hat{E}_1^{\mathsf{hi}} \ll z_2 : \hat{E}_2^{\mathsf{lo}} \mathinner{..} \hat{E}_2^{\mathsf{hi}} & \text{(Case)} \\
\textsf{\textbf{impl.}} & \Big[\hat{E}_1^{\mathsf{lo}} \langle\!\langle \psi \rangle\!\rangle, \hat{E}_1^{\mathsf{lo}} \langle\!\langle \psi \rangle\!\rangle \in \hat{\mathbb{E}} \ \textsf{\textbf{impl.}} \ \llbracket \hat{E}_1^{\mathsf{lo}} \langle\!\langle \psi \rangle\!\rangle \rrbracket < \llbracket \hat{E}_2^{\mathsf{lo}} \langle\!\langle \psi \rangle\!\rangle \rrbracket\Big] \ \textsf{\textbf{for-all}} \ \psi & \text{(Fig. VII.3.8)} \\
\textsf{\textbf{impl.}} & \Big[\hat{E}_1^{\mathsf{lo}}, \hat{E}_1^{\mathsf{lo}} \in \hat{\mathbb{E}} \ \textsf{\textbf{impl.}} \ \llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket < \llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket\Big] \ \textsf{\textbf{for-all}} \ \psi & \text{(Lem. VII.3.6:2)} \\
\textsf{\textbf{impl.}} & \llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket < \llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket & \text{(–)} \\
\textsf{\textbf{impl.}} & \llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket + (-\llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket) < \llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket + (-\llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket) & \text{(Fig. VII.2.1:5)} \\
\textsf{\textbf{impl.}} & 0 < \llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket + (-\llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket) & \text{(Fig. VII.2.1:1)} \\
\textsf{\textbf{impl.}} & 0 < \delta(\llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket, \llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket) & \text{(p25)}
\end{array}$$

  - **B2.** Conclude:

$$\begin{array}{rll}
 & \llbracket \nabla(\hat{D}_1) \rrbracket = \llbracket \nabla(\hat{D}_2) \rrbracket \preceq^{\text{-}1} 0 & \text{(A1, A2} \Rightarrow \text{Lem. VII.3.10:2)} \\
\textsf{\textbf{impl.}} & \llbracket \nabla(\hat{E}_1^{\mathsf{lo}} \mathinner{..} \hat{E}_1^{\mathsf{hi}}) \rrbracket = \llbracket \nabla(\hat{E}_2^{\mathsf{lo}} \mathinner{..} \hat{E}_2^{\mathsf{hi}}) \rrbracket \preceq^{\text{-}1} 0 & \text{(Case)} \\
\textsf{\textbf{impl.}} & \llbracket \Delta(\hat{E}_1^{\mathsf{lo}}, \hat{E}_1^{\mathsf{hi}}) \rrbracket = \llbracket \Delta(\hat{E}_2^{\mathsf{lo}}, \hat{E}_2^{\mathsf{hi}}) \rrbracket \preceq^{\text{-}1} 0 & \text{(Fig. VII.3.5)} \\
\textsf{\textbf{impl.}} & \delta(\llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket, \llbracket \hat{E}_1^{\mathsf{hi}} \rrbracket) = \delta(\llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket, \llbracket \hat{E}_2^{\mathsf{hi}} \rrbracket) \preceq^{\text{-}1} 0 & \text{(Thm. VII.3.2:2)} \\
\textsf{\textbf{impl.}} & \{\tilde{a}_1 + \delta(\llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket, \llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket) \mid \llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket \preceq \tilde{a}_1 \preceq \llbracket \hat{E}_1^{\mathsf{hi}} \rrbracket\} = \{\tilde{a}_2 \mid \llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket \preceq \tilde{a}_2 \preceq \llbracket \hat{E}_2^{\mathsf{hi}} \rrbracket\} & \\
 & & \text{(Lem. VII.2.1:2)}
\end{array}$$

  Conclude:

$$\begin{array}{rll}
 & \{\tilde{a}_1 \mid \llbracket \hat{E}_1^{\mathsf{lo}} \rrbracket \preceq \tilde{a}_1 \preceq \llbracket \hat{E}_1^{\mathsf{hi}} \rrbracket\} < \{\tilde{a}_2 \mid \llbracket \hat{E}_2^{\mathsf{lo}} \rrbracket \preceq \tilde{a}_2 \preceq \llbracket \hat{E}_2^{\mathsf{hi}} \rrbracket\} & \text{(B1, B2} \Rightarrow \text{Thm. VII.2.2)} \\
\textsf{\textbf{impl.}} & \llbracket \hat{E}_1^{\mathsf{lo}} \mathinner{..} \hat{E}_1^{\mathsf{hi}} \rrbracket < \llbracket \hat{E}_2^{\mathsf{lo}} \mathinner{..} \hat{E}_2^{\mathsf{hi}} \rrbracket & \text{(Fig. VII.3.4)} \\
\textsf{\textbf{impl.}} & \llbracket \hat{D}_1 \rrbracket < \llbracket \hat{D}_2 \rrbracket & \text{(Case)} \\
\textsf{\textbf{impl.}} & \llbracket \hat{C} \rrbracket(z_1) < \llbracket \hat{C} \rrbracket(z_2) & \text{(A2} \Rightarrow \text{Lem. VII.3.7:3)}
\end{array}$$

QED.

Proof of (2)

- **A1.** $\hat{C} \in \checkmark$
- **A2.** $z\!:\!\hat{D} = \min \langle \hat{C}, \ll \rangle$
- **B1.** Conclude:

$$z\!:\!\hat{D} = \min \langle \hat{C}, \ll \rangle \qquad \text{(A2)}$$

$$\textbf{impl. } z\!:\!\hat{D} \in \hat{C} \qquad \text{(–)}$$

Conclude:

$$z\!:\!\hat{D} = \min \langle \hat{C}, \ll \rangle \qquad \text{(A1)}$$

$$\textbf{impl. } \Big[z\!:\!\hat{D} \neq \tilde{z}\!:\!\tilde{\hat{D}} \textbf{ impl. } z\!:\!\hat{D} \ll \tilde{z}\!:\!\tilde{\hat{D}} \Big] \textbf{ for-all } \tilde{z}\!:\!\tilde{\hat{D}} \in \hat{C} \qquad \text{(–)}$$

$$\textbf{impl. } \Big[\Big[z\!:\!\hat{D} \neq \tilde{z}\!:\!\tilde{\hat{D}} \textbf{ impl. } z\!:\!\hat{D} \ll \tilde{z}\!:\!\tilde{\hat{D}} \Big] \textbf{ for-all } \tilde{z}\!:\!\tilde{\hat{D}} \in \hat{C} \Big] \textbf{ and } z\!:\!\hat{D} \in \hat{C} \textbf{ and } \hat{C} \in \checkmark \qquad \text{(B1, A1)}$$

$$\textbf{impl. } \Big[z\!:\!\hat{D} \neq \tilde{z}\!:\!\tilde{\hat{D}} \textbf{ impl. } \llbracket \hat{C} \rrbracket(z) < \llbracket \hat{C} \rrbracket(\tilde{z}) \Big] \textbf{ for-all } \tilde{z}\!:\!\tilde{\hat{D}} \in \hat{C} \qquad \text{(Thm. VII.3.8:1)}$$

$$\textbf{impl. } \Big[z \neq \tilde{z} \textbf{ impl. } \llbracket \hat{C} \rrbracket(z) < \llbracket \hat{C} \rrbracket(\tilde{z}) \Big] \textbf{ for-all } \tilde{z}\!:\!\tilde{\hat{D}} \in \hat{C} \qquad \text{(–)}$$

$$\textbf{impl. } \Big[z \neq \tilde{z} \textbf{ impl. } \llbracket \hat{C} \rrbracket(z) < \llbracket \hat{C} \rrbracket(\tilde{z}) \Big] \textbf{ for-all } \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket \qquad \text{(Lem. VII.3.7:2)}$$

$$\textbf{impl. } \Big[\llbracket \hat{C} \rrbracket(z) \neq \llbracket \hat{C} \rrbracket(\tilde{z}) \textbf{ impl. } \llbracket \hat{C} \rrbracket(z) < \llbracket \hat{C} \rrbracket(\tilde{z}) \Big] \textbf{ for-all } \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket \qquad \text{(–)}$$

$$\textbf{impl. } \llbracket \hat{C} \rrbracket(z) = \min \langle \{ \llbracket \hat{C} \rrbracket(\tilde{z}) \mid \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket \}, < \rangle \qquad \text{(–)}$$

$$\textbf{impl. } \llbracket \hat{C} \rrbracket(z) = \min \langle \operatorname{img} \llbracket \hat{C} \rrbracket, < \rangle \qquad \text{(–)}$$

QED.

Proof of (3)

- **A1.** $\hat{C} \in \checkmark$
- **A2.** $z\!:\!\hat{D} = \max \langle \hat{C}, \ll \rangle$
- **B1.** Conclude:

$$z\!:\!\hat{D} = \max \langle \hat{C}, \ll \rangle \qquad \text{(A2)}$$

$$\textbf{impl. } z\!:\!\hat{D} \in \hat{C} \qquad \text{(–)}$$

Conclude:

$$\begin{array}{lll}
 & z\!:\!\hat{D} = \max \langle \hat{C}, \ll \rangle & \text{(A1)} \\
\textbf{impl.} & \left[z\!:\!\hat{D} \neq \tilde{z}\!:\!\tilde{\hat{D}} \ \textbf{impl.}\ \tilde{z}\!:\!\tilde{\hat{D}} \ll z\!:\!\hat{D} \right] \ \textbf{for-all}\ \tilde{z}\!:\!\tilde{\hat{D}} \in \hat{C} & (\text{–}) \\
\textbf{impl.} & \left[\left[z\!:\!\hat{D} \neq \tilde{z}\!:\!\tilde{\hat{D}} \ \textbf{impl.}\ \tilde{z}\!:\!\tilde{\hat{D}} \ll z\!:\!\hat{D} \right] \ \textbf{for-all}\ \tilde{z}\!:\!\tilde{\hat{D}} \in \hat{C} \right] \ \textbf{and}\ z\!:\!\hat{D} \in \hat{C} \ \textbf{and}\ \hat{C} \in \checkmark & \text{(B1, A1)} \\
\textbf{impl.} & \left[z\!:\!\hat{D} \neq \tilde{z}\!:\!\tilde{\hat{D}} \ \textbf{impl.}\ [\![\hat{C}]\!](\tilde{z}) < [\![\hat{C}]\!](z) \right] \ \textbf{for-all}\ \tilde{z}\!:\!\tilde{\hat{D}} \in \hat{C} & \text{(Thm. VII.3.8:1)} \\
\textbf{impl.} & \left[z \neq \tilde{z} \ \textbf{impl.}\ [\![\hat{C}]\!](\tilde{z}) < [\![\hat{C}]\!](z) \right] \ \textbf{for-all}\ \tilde{z}\!:\!\tilde{\hat{D}} \in \hat{C} & (\text{–}) \\
\textbf{impl.} & \left[z \neq \tilde{z} \ \textbf{impl.}\ [\![\hat{C}]\!](\tilde{z}) < [\![\hat{C}]\!](z) \right] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} [\![\hat{C}]\!] & \text{(Lem. VII.3.7:2)} \\
\textbf{impl.} & \left[[\![\hat{C}]\!](z) \neq [\![\hat{C}]\!](\tilde{z}) \ \textbf{impl.}\ [\![\hat{C}]\!](\tilde{z}) < [\![\hat{C}]\!](z) \right] \ \textbf{for-all}\ \tilde{z} \in \operatorname{dom} [\![\hat{C}]\!] & (\text{–}) \\
\textbf{impl.} & [\![\hat{C}]\!](z) = \max \langle \{ [\![\hat{C}]\!](\tilde{z}) \mid \tilde{z} \in \operatorname{dom} [\![\hat{C}]\!] \}, < \rangle & (\text{–}) \\
\textbf{impl.} & [\![\hat{C}]\!](z) = \max \langle \operatorname{img} [\![\hat{C}]\!], < \rangle & (\text{–})
\end{array}$$

QED.

VIII.18 Proof of Theorem VII.4.1

Proof of (1)

- **A1.** $\mathsf{Wf}_{f,\mathcal{X}}(T)$
- **A2.** $\mathsf{Wf}_{f,\mathcal{X}}(T_Y)$

By induction on A1 (Fig. VII.4.2):

- **Base.** $T = X$ **and** $X \in \mathcal{X}$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

    $$\begin{array}{lll}
     & \mathsf{Wf}_{f,\mathcal{X}}(T_Y) & \text{(A2)} \\
    \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X\,\{T_Y/Y\}) & (\text{Case} \Rightarrow \text{Fig. VII.4.3}) \\
    \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_Y/Y\}) & \text{(Base)}
    \end{array}$$

  - **Case.** $X \neq Y$

    Conclude:

    $$\begin{array}{lll}
     & \mathsf{Wf}_{f,\mathcal{X}}(T) & \text{(A1)} \\
    \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X) & \text{(Base)} \\
    \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X\,\{T_Y/Y\}) & (\text{Case} \Rightarrow \text{Fig. VII.4.3}) \\
    \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_Y/Y\}) & \text{(Base)}
    \end{array}$$

- **Step.** $T = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I}$ **and**
  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and**
  $\Big[\mathsf{Wf}_{f,\mathcal{X}}(G_i)$ **for-all** $i \in I\Big]$

  Conclude:

  $$\begin{aligned}
  & \Big[\mathsf{Wf}_{f,\mathcal{X}}(G_i) \textbf{ for-all } i \in I\Big] \textbf{ and } \mathsf{Wf}_{f,\mathcal{X}}(T_Y) && \text{(Step, A2)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(G_i\,\{T_Y/Y\}) \textbf{ for-all } i \in I && \text{(Induction)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\,\{T_Y/Y\}\}_{i \in I}) && \text{(Step} \Rightarrow \text{Fig. VII.4.2)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I}\,\{T_Y/Y\}) && \text{(Fig. VII.4.3)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_Y/Y\}) && \text{(Step)}
  \end{aligned}$$

- **Step.** $T = r_2[x_2]\,!\,\{\ell_i \,.\, L_i\}_{i \in I}$ **and**
  $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(L_i)$ **for-all** $i \in I\Big]$

  Conclude:

  $$\begin{aligned}
  & \Big[\mathsf{Wf}_{f,\mathcal{X}}(L_i) \textbf{ for-all } i \in I\Big] \textbf{ and } \mathsf{Wf}_{f,\mathcal{X}}(T_Y) && \text{(Step, A2)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(L_i\,\{T_Y/Y\}) \textbf{ for-all } i \in I && \text{(Induction)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,!\,\{\ell_i \,.\, L_i\,\{T_Y/Y\}\}_{i \in I}) && \text{(Step} \Rightarrow \text{Fig. VII.4.2)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,!\,\{\ell_i \,.\, L_i\}_{i \in I}\,\{T_Y/Y\}) && \text{(Fig. VII.4.3)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_Y/Y\}) && \text{(Step)}
  \end{aligned}$$

- **Step.** $T = r_1[x_1]\,?\{\ell_i \,.\, L_i\}_{i \in I}$ **and**
  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(L_i)$ **for-all** $i \in I\Big]$

  Conclude:

  $$\begin{aligned}
  & \Big[\mathsf{Wf}_{f,\mathcal{X}}(L_i) \textbf{ for-all } i \in I\Big] \textbf{ and } \mathsf{Wf}_{f,\mathcal{X}}(T_Y) && \text{(Step, A2)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(L_i\,\{T_Y/Y\}) \textbf{ for-all } i \in I && \text{(Induction)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,?\{\ell_i \,.\, L_i\,\{T_Y/Y\}\}_{i \in I}) && \text{(Step} \Rightarrow \text{Fig. VII.4.2)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,?\{\ell_i \,.\, L_i\}_{i \in I}\,\{T_Y/Y\}) && \text{(Fig. VII.4.3)}\\
  \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_Y/Y\}) && \text{(Step)}
  \end{aligned}$$

- **Step.** $T = \texttt{rec}\ X\ T_X$ **and** $\mathsf{Wf}_{f,\mathcal{X} \cup \{X\}}(T_X)$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

    $$\begin{aligned}
    & \mathsf{Wf}_{f,\mathcal{X}}(T) && \text{(A1)}\\
    \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ T_X) && \text{(Step)}\\
    \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ T_X\,\{T_Y/Y\}) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
    \textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_Y/Y\}) && \text{(Step)}
    \end{aligned}$$

- **Case.** $X \neq Y$
  Conclude:

$$\begin{array}{lll} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y) & \text{(A2)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_Y) & \text{(Lem. VII.4.1:2)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_X) \textbf{ and } \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_Y) & \text{(Step)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(T_X\,\{T_Y/Y\}) & \text{(Induction)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ (T_X\,\{T_Y/Y\})) & \text{(Fig. VII.4.2)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ T_X\,\{T_Y/Y\}) & \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_Y/Y\}) & \text{(Step)} \end{array}$$

QED.

Proof of (2)

- **A1.** $\mathsf{Wf}_{f,\mathcal{X}\cup\{\texttt{cont}\}}(T)$
- **A2.** $\mathsf{Wf}_{f,\mathcal{X}}(T_{\texttt{cont}})$

By induction on A1 (Fig. VII.4.2):

- **Base.** $T = X$ **and** $X \in \mathcal{X} \cup \{\texttt{cont}\}$
  By case distinction:

  - **Case.** $X = \texttt{cont}$
    Conclude:

$$\begin{array}{lll} & \mathsf{Wf}_{f,\mathcal{X}}(T_{\texttt{cont}}) & \text{(A2)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X\,\{T_{\texttt{cont}}/\texttt{cont}\}) & \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_{\texttt{cont}}/\texttt{cont}\}) & \text{(Base)} \end{array}$$

  - **Case.** $X \neq \texttt{cont}$
    Conclude:

$$\begin{array}{lll} & X \in \mathcal{X} \cup \{\texttt{cont}\} \textbf{ and } X \neq \texttt{cont} & \text{(Step, Case)} \\ \textbf{impl.} & X \in \mathcal{X} & \text{(–)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X) & \text{(Fig. VII.4.2)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X\,\{T_{\texttt{cont}}/\texttt{cont}\}) & \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_{\texttt{cont}}/\texttt{cont}\}) & \text{(Base)} \end{array}$$

- **Step.** $T = r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i\,.\,G_i\}_{i \in I}$ **and**
  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and**
  $\Big[\mathsf{Wf}_{f,\mathcal{X}\cup\{\texttt{cont}\}}(G_i)$ **for-all** $i \in I\Big]$

Conclude:

$$\begin{array}{llr}
 & \left[\mathsf{Wf}_{f,\mathcal{X}\cup\{\mathtt{cont}\}}(G_i)\ \ \textsf{\textbf{for-all}}\ \ i\in I\right]\ \ \textsf{\textbf{and}}\ \ \mathsf{Wf}_{f,\mathcal{X}}(T_{\mathtt{cont}}) & \text{(Step, A2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(G_i\,\{T_{\mathtt{cont}}/\mathtt{cont}\})\ \ \textsf{\textbf{for-all}}\ \ i\in I & \text{(Induction)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\rightarrowtriangle r_2[x_2]:\{\ell_i\,.\,G_i\,\{T_{\mathtt{cont}}/\mathtt{cont}\}\}_{i\in I}) & \text{(Fig. VII.4.2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\rightarrowtriangle r_2[x_2]:\{\ell_i\,.\,G_i\}_{i\in I}\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Fig. VII.4.3)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Step)}
\end{array}$$

- **Step.** $T = r_2[x_2]\,!\{\ell_i\,.\,L_i\}_{i\in I}$ **and**
  $\left[r_2\in\operatorname{dom} f\ \ \textsf{\textbf{impl.}}\ \ x_2\in f(r_2)\right]$ **and** $\left[\mathsf{Wf}_{f,\mathcal{X}\cup\{\mathtt{cont}\}}(L_i)\ \ \textsf{\textbf{for-all}}\ \ i\in I\right]$

  Conclude:

$$\begin{array}{llr}
 & \left[\mathsf{Wf}_{f,\mathcal{X}\cup\{\mathtt{cont}\}}(L_i)\ \ \textsf{\textbf{for-all}}\ \ i\in I\right]\ \ \textsf{\textbf{and}}\ \ \mathsf{Wf}_{f,\mathcal{X}}(T_{\mathtt{cont}}) & \text{(Step, A2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(L_i\,\{T_{\mathtt{cont}}/\mathtt{cont}\})\ \ \textsf{\textbf{for-all}}\ \ i\in I & \text{(Induction)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,!\{\ell_i\,.\,L_i\,\{T_{\mathtt{cont}}/\mathtt{cont}\}\}_{i\in I}) & \text{(Fig. VII.4.2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,!\{\ell_i\,.\,L_i\}_{i\in I}\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Fig. VII.4.3)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Step)}
\end{array}$$

- **Step.** $T = r_1[x_1]\,?\{\ell_i\,.\,L_i\}_{i\in I}$ **and**
  $\left[r_1\in\operatorname{dom} f\ \ \textsf{\textbf{impl.}}\ \ x_1\in f(r_1)\right]$ **and** $\left[\mathsf{Wf}_{f,\mathcal{X}\cup\{\mathtt{cont}\}}(L_i)\ \ \textsf{\textbf{for-all}}\ \ i\in I\right]$

  Conclude:

$$\begin{array}{llr}
 & \left[\mathsf{Wf}_{f,\mathcal{X}\cup\{\mathtt{cont}\}}(L_i)\ \ \textsf{\textbf{for-all}}\ \ i\in I\right]\ \ \textsf{\textbf{and}}\ \ \mathsf{Wf}_{f,\mathcal{X}}(T_{\mathtt{cont}}) & \text{(Step, A2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(L_i\,\{T_{\mathtt{cont}}/\mathtt{cont}\})\ \ \textsf{\textbf{for-all}}\ \ i\in I & \text{(Induction)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,?\{\ell_i\,.\,L_i\,\{T_{\mathtt{cont}}/\mathtt{cont}\}\}_{i\in I}) & \text{(Fig. VII.4.2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,?\{\ell_i\,.\,L_i\}_{i\in I}\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Fig. VII.4.3)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Step)}
\end{array}$$

- **Step.** $T = \mathtt{rec}\ X\ T_X$ **and** $\mathsf{Wf}_{f,\mathcal{X}\cup\{\mathtt{cont}\}\cup\{X\}}(T_X)$

  By case distinction:

  - **Case.** $X = \mathtt{cont}$

    Conclude:

$$\begin{array}{llr}
 & T = \mathtt{rec}\ X\ T_X\ \ \textsf{\textbf{and}}\ \ X = \mathtt{cont} & \text{(Step, Case)}\\
\textsf{\textbf{impl.}} & \textsf{\textbf{false}} & \text{(Fig. VII.4.1)}
\end{array}$$

  - **Case.** $X \neq \mathtt{cont}$

    Conclude:

$$\begin{array}{llr}
 & \mathsf{Wf}_{f,\mathcal{X}\cup\{\mathtt{cont}\}\cup\{X\}}(T_X)\ \ \textsf{\textbf{and}}\ \ \mathsf{Wf}_{f,\mathcal{X}}(T_{\mathtt{cont}}) & \text{(Step, A2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}\cup\{\mathtt{cont}\}\cup\{X\}}(T_X)\ \ \textsf{\textbf{and}}\ \ \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(T_{\mathtt{cont}}) & \text{(Lem. VII.4.1:2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(T_X\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Induction)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{rec}\ X\ (T_X\,\{T_{\mathtt{cont}}/\mathtt{cont}\})) & \text{(Fig. VII.4.2)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{rec}\ X\ T_X\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
\textsf{\textbf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(T\,\{T_{\mathtt{cont}}/\mathtt{cont}\}) & \text{(Step)}
\end{array}$$

QED.

VIII.19 Proof of Theorem VII.4.2

- **A1.** $\mathsf{Wf}_{f,\mathcal{X}\setminus\{Y\}}(T)$

By induction on A1 (Fig. VII.4.2):

- **Base.** $T = X$ **and** $X \in \mathcal{X} \setminus \{Y\}$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

    $$\begin{aligned} & X \in \mathcal{X} \setminus \{Y\} && \text{(Base)} \\ \textbf{impl. } & Y \in \mathcal{X} \setminus \{Y\} && \text{(Base)} \\ \textbf{impl. } & \textbf{false} && \text{(–)} \end{aligned}$$

  - **Case.** $X \neq Y$

    Conclude:

    $$\begin{aligned} & T \\ = \; & X && \text{(Base)} \\ = \; & X\,\{T_Y/Y\} && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ = \; & T\,\{T_Y/Y\} && \text{(Base)} \end{aligned}$$

- **Step.** $T = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i\in I}$ **and**

  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and**

  $\Big[\mathsf{Wf}_{f,\mathcal{X}}(G_i)$ **for-all** $i \in I\Big]$

  Conclude:

  $$\begin{aligned} & T \\ = \; & r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i\in I} && \text{(Step)} \\ = \; & r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\,\{T_Y/Y\}\}_{i\in I} && \text{(Step} \Rightarrow \text{Induction)} \\ = \; & r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i\in I}\,\{T_Y/Y\} && \text{(Fig. VII.4.3)} \\ = \; & T\,\{T_Y/Y\} && \text{(Step)} \end{aligned}$$

- **Step.** $T = r_2[x_2]\,!\,\{\ell_i \,.\, L_i\}_{i\in I}$ **and**

  $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}\setminus\{Y\}}(L_i)$ **for-all** $i \in I\Big]$

  Conclude:

  $$\begin{aligned} & T \\ = \; & r_2[x_2]\,!\,\{\ell_i \,.\, L_i\}_{i\in I} && \text{(Step)} \\ = \; & r_2[x_2]\,!\,\{\ell_i \,.\, L_i\,\{T_Y/Y\}\}_{i\in I} && \text{(Step} \Rightarrow \text{Induction)} \\ = \; & r_2[x_2]\,!\,\{\ell_i \,.\, L_i\}_{i\in I}\,\{T_Y/Y\} && \text{(Fig. VII.4.3)} \\ = \; & T\,\{T_Y/Y\} && \text{(Step)} \end{aligned}$$

- **Step.** $T = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I}$ **and**

  $\Big[r_1 \in \mathrm{dom}\, f \ \textbf{impl.}\ x_1 \in f(r_1)\Big] \ \textbf{and}\ \Big[\mathsf{Wf}_{f,\mathcal{X}\setminus\{Y\}}(L_i)\ \textbf{for-all}\ i \in I\Big]$

  Conclude:

$$\begin{array}{rll} & T & \\ = & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I} & \text{(Step)} \\ = & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\,\{T_Y/Y\}\}_{i\in I} & \text{(Step} \Rightarrow \text{Induction)} \\ = & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I}\,\{T_Y/Y\} & \text{(Fig. VII.4.3)} \\ = & T\,\{T_Y/Y\} & \text{(Step)} \end{array}$$

- **Step.** $T = \texttt{\textbf{rec}}\ X\ T_X$ **and** $\mathsf{Wf}_{f,(\mathcal{X}\setminus\{Y\})\cup\{X\}}(T_X)$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$\begin{array}{rll} & T & \\ = & \texttt{\textbf{rec}}\ X\ T_X & \text{(Step)} \\ = & \texttt{\textbf{rec}}\ X\ T_X\,\{T_Y/Y\} & \text{(Fig. VII.4.3)} \\ = & T\,\{T_Y/Y\} & \text{(Step)} \end{array}$$

  - **Case.** $X \neq Y$

    - **B1.** Conclude:

$$\begin{array}{rll} & \mathsf{Wf}_{f,(\mathcal{X}\setminus\{Y\})\cup\{X\}}(T_X)\ \textbf{and}\ X \neq Y & \text{(Step, Case)} \\ \textbf{impl.} & \mathsf{Wf}_{f,(\mathcal{X}\setminus\{Y\})\cup(\{X\}\setminus\{Y\})}(T_X) & (-) \\ \textbf{impl.} & \mathsf{Wf}_{f,(\mathcal{X}\cup\{X\})\setminus\{Y\}}(T_X) & (-) \end{array}$$

    Conclude:

$$\begin{array}{rll} & T & \\ = & \texttt{\textbf{rec}}\ X\ T_X & \text{(Step)} \\ = & \texttt{\textbf{rec}}\ X\ (T_X\,\{T_Y/Y\}) & \text{(B1} \Rightarrow \text{Induction)} \\ = & \texttt{\textbf{rec}}\ X\ T_X\,\{T_Y/Y\} & \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ = & T\,\{T_Y/Y\} & \text{(Step)} \end{array}$$

QED.

VIII.20 Proof of Theorem VII.5.1

Proof of (1)

- **A1.** $\langle L_1, L_2\rangle \in \mathrm{dom} \sqcap$

By induction on A1 (Fig. VII.5.1):

- **Base.** $L_1 = L_2 = X$ **and** $L_1 \sqcap L_2 = X$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$\begin{aligned}
& (L_1 \sqcap L_2)\,\{L/Y\} & \\
={} & X\,\{L/Y\} & \text{(Base)}\\
={} & L & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={} & L \sqcap L & \text{(Lem. VII.5.1:2)}\\
={} & X\,\{L/Y\} \sqcap X\,\{L/Y\} & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={} & L_1\,\{L/Y\} \sqcap L_2\,\{L/Y\} & \text{(Base)}
\end{aligned}$$

  - **Case.** $X \neq Y$

    Conclude:

$$\begin{aligned}
& (L_1 \sqcap L_2)\,\{L/Y\} & \\
={} & X\,\{L/Y\} & \text{(Base)}\\
={} & X & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={} & X \sqcap X & \text{(Lem. VII.5.1:2)}\\
={} & X\,\{L/Y\} \sqcap X\,\{L/Y\} & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={} & L_1\,\{L/Y\} \sqcap L_2\,\{L/Y\} & \text{(Base)}
\end{aligned}$$

- **Step.** $L_1 = r_2[x_2]\,!\{\ell_i \,.\, L_{i,1}\}_{i\in I}$ **and** $L_2 = r_2[x_2]\,!\{\ell_i \,.\, L_{i,2}\}_{i\in I}$ **and**
  $L_1 \sqcap L_2 = r_2[x_2]\,!\{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i\in I}$

  Conclude:

$$\begin{aligned}
& (L_1 \sqcap L_2)\,\{L/Y\} & \\
={} & r_2[x_2]\,!\{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i\in I}\,\{L/Y\} & \text{(Step)}\\
={} & r_2[x_2]\,!\{\ell_i \,.\, (L_{i,1} \sqcap L_{i,2})\,\{L/Y\}\}_{i\in I} & \text{(Fig. VII.4.3)}\\
={} & r_2[x_2]\,!\{\ell_i \,.\, L_{i,1}\,\{L/Y\} \sqcap L_{i,2}\,\{L/Y\}\}_{i\in I} & \text{(Induction)}\\
={} & r_2[x_2]\,!\{\ell_i \,.\, L_{i,1}\,\{L/Y\}\}_{i\in I} \sqcap r_2[x_2]\,!\{\ell_i \,.\, L_{i,2}\,\{L/Y\}\}_{i\in I} & \text{(Fig. VII.5.1)}\\
={} & r_2[x_2]\,!\{\ell_i \,.\, L_{i,1}\}_{i\in I}\,\{L/Y\} \sqcap r_2[x_2]\,!\{\ell_i \,.\, L_{i,2}\}_{i\in I}\,\{L/Y\} & \text{(Fig. VII.4.3)}\\
={} & L_1\,\{L/Y\} \sqcap L_2\,\{L/Y\} & \text{(Step)}
\end{aligned}$$

- **Step.** $L_1 = r_1[x_1]\,?\{\ell_i \,.\, L_{i,1}\}_{i\in I_1}$ **and** $L_2 = r_1[x_1]\,?\{\ell_i \,.\, L_{i,2}\}_{i\in I_2}$ **and**
  $L_1 \sqcap L_2 = r_1[x_1]\,?\{\ell_i \,.\, L_{i,1}\}_{i\in I_1\setminus I_2} \cup \{\ell_i \,.\, L_{i,2}\}_{i\in I_2\setminus I_1} \cup \{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i\in I_1\cap I_2}$ **and**
  $\Big[\ell_{i_1} \neq \ell_{i_2}$ **for-all** $i_1 \in I_1 \setminus I_2, i_2 \in I_2 \setminus I_1\Big]$

Conclude:

$$\begin{aligned}
&(L_1 \sqcap L_2)\,\{L/Y\} \\
= \;& r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\}_{i\in I_1\setminus I_2} \cup \{\ell_i \,.\, L_{i,2}\}_{i\in I_2\setminus I_1} \cup \{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i\in I_1\cap I_2}\,\{L/Y\} && \text{(Step)}\\
= \;& r_1[x_1]\,\mathbf{?} && \text{(Fig. VII.4.3)}\\
&\quad \{\ell_i \,.\, L_{i,1}\,\{L/Y\}\}_{i\in I_1\setminus I_2} \cup \{\ell_i \,.\, L_{i,2}\,\{L/Y\}\}_{i\in I_2\setminus I_1} \cup \{\ell_i \,.\, (L_{i,1} \sqcap L_{i,2})\,\{L/Y\}\}_{i\in I_1\cap I_2}\\
= \;& r_1[x_1]\,\mathbf{?} && \text{(Induction)}\\
&\quad \{\ell_i \,.\, L_{i,1}\,\{L/Y\}\}_{i\in I_1\setminus I_2} \cup \{\ell_i \,.\, L_{i,2}\,\{L/Y\}\}_{i\in I_2\setminus I_1} \cup\\
&\quad \{\ell_i \,.\, L_{i,1}\,\{L/Y\} \sqcap L_{i,2}\,\{L/Y\}\}_{i\in I_1\cap I_2}\\
= \;& r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\,\{L/Y\}\}_{i\in I_1} \sqcap r_1[x_1]\,\{L/Y\}\,\mathbf{?}\{\ell_i \,.\, L_{i,2}\,\{L/Y\}\}_{i\in I_2} && \text{(Step} \Rightarrow \text{Fig. VII.5.1)}\\
= \;& r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\}_{i\in I_1}\,\{L/Y\} \sqcap r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,2}\}_{i\in I_2}\,\{L/Y\} && \text{(Fig. VII.4.3)}\\
= \;& L_1\,\{L/Y\} \sqcap L_2\,\{L/Y\} && \text{(Step)}
\end{aligned}$$

- **Step.** $L_1 = \texttt{rec}\ X\ L_{X,1}$ **and** $L_2 = \texttt{rec}\ X\ L_{X,2}$ **and** $L_1 \sqcap L_2 = \texttt{rec}\ X\ (L_{X,1} \sqcap L_{X,2})$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$\begin{aligned}
&(L_1 \sqcap L_2)\,\{L/Y\} \\
= \;& \texttt{rec}\ X\ (L_{X,1} \sqcap L_{X,2})\,\{L/Y\} && \text{(Step)}\\
= \;& \texttt{rec}\ X\ (L_{X,1} \sqcap L_{X,2}) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
= \;& \texttt{rec}\ X\ L_{X,1} \sqcap \texttt{rec}\ X\ L_{X,2} && \text{(Fig. VII.5.1)}\\
= \;& \texttt{rec}\ X\ L_{X,1}\,\{L/Y\} \sqcap \texttt{rec}\ X\ L_{X,2}\,\{L/Y\} && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
= \;& L_1\,\{L/Y\} \sqcap L_2\,\{L/Y\} && \text{(Step)}
\end{aligned}$$

  - **Case.** $X \neq Y$

    Conclude:

$$\begin{aligned}
&(L_1 \sqcap L_2)\,\{L/Y\} \\
= \;& \texttt{rec}\ X\ (L_{X,1} \sqcap L_{X,2})\,\{L/Y\} && \text{(Step)}\\
= \;& \texttt{rec}\ X\ ((L_{X,1} \sqcap L_{X,2})\,\{L/Y\}) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
= \;& \texttt{rec}\ X\ (L_{X,1}\,\{L/Y\} \sqcap L_{X,2}\,\{L/Y\}) && \text{(Induction)}\\
= \;& \texttt{rec}\ X\ (L_{X,1}\,\{L/Y\}) \sqcap \texttt{rec}\ X\ (L_{X,2}\,\{L/Y\}) && \text{(Fig. VII.5.1)}\\
= \;& \texttt{rec}\ X\ L_{X,1}\,\{L/Y\} \sqcap \texttt{rec}\ X\ L_{X,2}\,\{L/Y\} && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
= \;& L_1\,\{L/Y\} \sqcap L_2\,\{L/Y\} && \text{(Step)}
\end{aligned}$$

QED.

Proof of (2)

- **A1.** $\langle L_1, L_2\rangle \in \operatorname{dom} \sqcap$

By induction on L (Fig. VII.4.1):

- **Base.** $L = X$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$\begin{aligned} & L\,\{L_1 \sqcap L_2/Y\} && \\ =\ & X\,\{L_1 \sqcap L_2/Y\} && \text{(A1, Base)} \\ =\ & L_1 \sqcap L_2 && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ =\ & X\,\{L_1/Y\} \sqcap X\,\{L_2/Y\} && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ =\ & L\,\{L_1/Y\} \sqcap L\,\{L_2/Y\} && \text{(Base)} \end{aligned}$$

  - **Case.** $X \neq Y$

    Conclude:

$$\begin{aligned} & L\,\{L_1 \sqcap L_2/Y\} && \\ =\ & X\,\{L_1 \sqcap L_2/Y\} && \text{(A1, Base)} \\ =\ & X && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ =\ & X \sqcap X && \text{(Lem. VII.5.1:2)} \\ =\ & X\,\{L_1/Y\} \sqcap X\,\{L_2/Y\} && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\ =\ & L\,\{L_1/Y\} \sqcap L\,\{L_2/Y\} && \text{(Base)} \end{aligned}$$

- **Step.** $L = r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\}_{i \in I}$

  Conclude:

$$\begin{aligned} & L\,\{L_1 \sqcap L_2/Y\} && \\ =\ & r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\}_{i \in I}\,\{L_1 \sqcap L_2/Y\} && \text{(A1, Step)} \\ =\ & r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\,\{L_1 \sqcap L_2/Y\}\}_{i \in I} && \text{(Fig. VII.4.3)} \\ =\ & r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\,\{L_1/Y\} \sqcap L_i\,\{L_2/Y\}\}_{i \in I} && \text{(Induction)} \\ =\ & r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\,\{L_1/Y\}\}_{i \in I} \sqcap r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\,\{L_2/Y\}\}_{i \in I} && \text{(Fig. VII.5.1)} \\ =\ & r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\}_{i \in I}\,\{L_1/Y\} \sqcap r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\}_{i \in I}\,\{L_2/Y\} && \text{(Fig. VII.4.3)} \\ =\ & L\,\{L_1/Y\} \sqcap L\,\{L_2/Y\} && \text{(Step)} \end{aligned}$$

- **Step.** $L = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i \in I}$

Conclude:

$$
\begin{aligned}
& L\,\{L_1 \sqcap L_2/Y\} \\
={} & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I}\,\{L_1 \sqcap L_2/Y\} && \text{(A1, Step)} \\
={} & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\,\{L_1 \sqcap L_2/Y\}\}_{i\in I} && \text{(Fig. VII.4.3)} \\
={} & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\,\{L_1/Y\} \sqcap L_i\,\{L_2/Y\}\}_{i\in I} && \text{(Induction)} \\
={} & r_1[x_1]\,\mathbf{?} && \text{(–)} \\
& \quad \{\ell_i \,.\, L_i\,\{L_1/Y\}\}_{i\in\emptyset} \cup \{\ell_i \,.\, L_i\,\{L_2/Y\}\}_{i\in\emptyset} \cup \{\ell_i \,.\, L_i\,\{L_1/Y\} \sqcap L_i\,\{L_2/Y\}\}_{i\in I} \\
={} & r_1[x_1]\,\mathbf{?} && \text{(–)} \\
& \quad \{\ell_i \,.\, L_i\,\{L_1/Y\}\}_{i\in I\setminus I} \cup \{\ell_i \,.\, L_i\,\{L_2/Y\}\}_{i\in I\setminus I} \cup \{\ell_i \,.\, L_i\,\{L_1/Y\} \sqcap L_i\,\{L_2/Y\}\}_{i\in I\cap I} \\
={} & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\,\{L_1/Y\}\}_{i\in I} \sqcap r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\,\{L_2/Y\}\}_{i\in I} && \text{(Fig. VII.5.1)} \\
={} & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I}\,\{L_1/Y\} \sqcap r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I}\,\{L_2/Y\} && \text{(Fig. VII.4.3)} \\
={} & L\,\{L_1/Y\} \sqcap L\,\{L_2/Y\} && \text{(Step)}
\end{aligned}
$$

- **Step.** $L = \texttt{rec}\ X\ L_X$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$
\begin{aligned}
& L\,\{L_1 \sqcap L_2/Y\} \\
={} & \texttt{rec}\ X\ L_X\,\{L_1 \sqcap L_2/Y\} && \text{(A1, Step)} \\
={} & \texttt{rec}\ X\ L_X && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\
={} & \texttt{rec}\ X\ L_X \sqcap \texttt{rec}\ X\ L_X && \text{(Lem. VII.5.1:2)} \\
={} & \texttt{rec}\ X\ L_X\,\{L_1/Y\} \sqcap \texttt{rec}\ X\ L_X\,\{L_2/Y\} && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\
={} & L\,\{L_1/Y\} \sqcap L\,\{L_2/Y\} && \text{(Step)}
\end{aligned}
$$

  - **Case.** $X \neq Y$

    Conclude:

$$
\begin{aligned}
& L\,\{L_1 \sqcap L_2/Y\} \\
={} & \texttt{rec}\ X\ L_X\,\{L_1 \sqcap L_2/Y\} && \text{(A1, Step)} \\
={} & \texttt{rec}\ X\ (L_X\,\{L_1 \sqcap L_2/Y\}) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\
={} & \texttt{rec}\ X\ (L_X\,\{L_1/Y\} \sqcap L_X\,\{L_2/Y\}) && \text{(Induction)} \\
={} & \texttt{rec}\ X\ (L_X\,\{L_1/Y\}) \sqcap \texttt{rec}\ X\ (L_X\,\{L_2/Y\}) && \text{(Fig. VII.5.1)} \\
={} & \texttt{rec}\ X\ L_X\,\{L_1/Y\} \sqcap \texttt{rec}\ X\ L_X\,\{L_2/Y\} && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\
={} & L\,\{L_1/Y\} \sqcap L\,\{L_2/Y\} && \text{(Step)}
\end{aligned}
$$

QED.

Proof of (3), v1

Conclude:

$$
\begin{aligned}
&(\texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\textbf{cont} \sqcap \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\textbf{cont})\\
&\quad\{\texttt{M}[6]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\textbf{cont} \sqcap \texttt{M}[6]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\textbf{cont}/\textbf{cont}\}\\
={}& \texttt{M}[5]\,\textbf{?}\{\texttt{foo(int)}\,\textbf{.}\,\textbf{cont}\,,\texttt{bar()}\,\textbf{.}\,\textbf{cont}\} && \text{(Fig. VII.5.1)}\\
&\quad\{\texttt{M}[6]\,\textbf{?}\{\texttt{foo(int)}\,\textbf{.}\,\textbf{cont}\,,\texttt{bar()}\,\textbf{.}\,\textbf{cont}\}/\textbf{cont}\}\\
={}& \texttt{M}[5]\,\textbf{?}\left\{\begin{array}{l}\texttt{foo(int)}\,\textbf{.}\,\texttt{M}[6]\,\textbf{?}\{\texttt{foo(int)}\,\textbf{.}\,\textbf{cont}\,,\texttt{bar()}\,\textbf{.}\,\textbf{cont}\}\,,\\ \quad\texttt{bar()}\,\textbf{.}\,\texttt{M}[6]\,\textbf{?}\{\texttt{foo(int)}\,\textbf{.}\,\textbf{cont}\,,\texttt{bar()}\,\textbf{.}\,\textbf{cont}\}\end{array}\right\} && \text{(Fig. VII.4.3)}\\
\neq{}& \texttt{M}[5]\,\textbf{?}\left\{\begin{array}{l}\texttt{foo(int)}\,\textbf{.}\,\texttt{M}[6]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\textbf{cont}\,,\\ \quad\texttt{bar()}\,\textbf{.}\,\texttt{M}[6]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\textbf{cont}\end{array}\right\} && \text{(–)}\\
={}& \texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\texttt{M}[6]\,\textbf{?}\,\texttt{foo(int)} \sqcap \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\texttt{M}[6]\,\textbf{?}\,\texttt{bar()} && \text{(Fig. VII.5.1)}\\
={}& \texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\textbf{cont}\,\{\texttt{M}[6]\,\textbf{?}\,\texttt{foo(int)}/\textbf{cont}\} \sqcap \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\textbf{cont}\,\{\texttt{M}[6]\,\textbf{?}\,\texttt{bar()}/\textbf{cont}\}\\
& && \text{(Fig. VII.4.3)}
\end{aligned}
$$

QED.

Proof of (3), v2

Conclude:

$$
\begin{aligned}
&(\texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\texttt{X} \sqcap \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\texttt{X})\\
&\quad\{\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\texttt{X} \sqcap \textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\texttt{X}/\texttt{X}\}\\
={}& \texttt{M}[5]\,\textbf{?}\{\texttt{foo(int)}\,\textbf{.}\,\texttt{X}\,,\texttt{bar()}\,\textbf{.}\,\texttt{X}\}\,\{\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\{\texttt{foo(int)}\,\textbf{.}\,\texttt{X}\,,\texttt{bar()}\,\textbf{.}\,\texttt{X}\}/\texttt{X}\} && \text{(Fig. VII.5.1)}\\
={}& \texttt{M}[5]\,\textbf{?}\left\{\begin{array}{l}\texttt{foo(int)}\,\textbf{.}\,\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\{\texttt{foo(int)}\,\textbf{.}\,\texttt{X}\,,\texttt{bar()}\,\textbf{.}\,\texttt{X}\}\,,\\ \quad\texttt{bar()}\,\textbf{.}\,\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\{\texttt{foo(int)}\,\textbf{.}\,\texttt{X}\,,\texttt{bar()}\,\textbf{.}\,\texttt{X}\}\end{array}\right\} && \text{(Fig. VII.4.3)}\\
\neq{}& \texttt{M}[5]\,\textbf{?}\left\{\begin{array}{l}\texttt{foo(int)}\,\textbf{.}\,\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\texttt{X}\,,\\ \quad\texttt{bar()}\,\textbf{.}\,\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\texttt{X}\end{array}\right\} && \text{(–)}\\
={}& \texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)} \sqcap \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\,\texttt{bar()} && \text{(Fig. VII.5.1)}\\
={}& \texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}\,\textbf{.}\,\texttt{X}\,\{\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\,\texttt{foo(int)}/\texttt{X}\} \sqcap && \text{(Fig. VII.4.3)}\\
& \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}\,\textbf{.}\,\texttt{X}\,\{\textbf{rec}\ \texttt{X}\ \texttt{M}[5]\,\textbf{?}\,\texttt{bar()}/\texttt{X}\}
\end{aligned}
$$

QED.

VIII.21 Proof of Theorem VII.5.2

- **A1.** $\langle G, r[a]\rangle \in \mathrm{dom} \upharpoonright$
- **A2.** $\langle G_Y, r[a]\rangle \in \mathrm{dom} \upharpoonright$

By induction on A1 (Fig. VII.5.2):

- **Base.** $G = X$ **and** $G \upharpoonright r[a] = X$

  By case distinction:

- **Case.** $X = Y$

  Conclude:

$$\begin{aligned}
& (G \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \\
={} & X\,\{G_Y \upharpoonright r[a]/Y\} && \text{(A2, Base)}\\
={} & G_Y \upharpoonright r[a] && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={} & X\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={} & G\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Base)}
\end{aligned}$$

- **Case.** $X \neq Y$

  Conclude:

$$\begin{aligned}
& (G \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \\
={} & X\,\{G_Y \upharpoonright r[a]/Y\} && \text{(A2, Base)}\\
={} & X && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={} & X \upharpoonright r[a] && \text{(Fig. VII.5.2)}\\
={} & X\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={} & G\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Base)}
\end{aligned}$$

- **Step.** $G = r_1[x_1] \twoheadrightarrow r_2[x_2]\,\mathbf{:}\,\{\ell_i \,.\, G_i\}_{i\in I}$ **and**
  $G \upharpoonright r[a] = r_2[x_2]\,\mathbf{!}\,\{\ell_i \,.\, G_i \upharpoonright r[a]\}_{i\in I}$ **and** $r_1[x_1] = r[a] \neq r_2[x_2]$

  Conclude:

$$\begin{aligned}
& (G \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \\
={} & r_2[x_2]\,\mathbf{!}\,\{\ell_i \,.\, G_i \upharpoonright r[a]\}_{i\in I}\,\{G_Y \upharpoonright r[a]/Y\} && \text{(A2, Step)}\\
={} & r_2[x_2]\,\mathbf{!}\,\{\ell_i \,.\, (G_i \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\}\}_{i\in I} && \text{(Fig. VII.4.3)}\\
={} & r_2[x_2]\,\mathbf{!}\,\{\ell_i \,.\, G_i\,\{G_Y/Y\} \upharpoonright r[a]\}_{i\in I} && \text{(Induction)}\\
={} & r_1[x_1] \twoheadrightarrow r_2[x_2]\,\mathbf{:}\,\{\ell_i \,.\, G_i\,\{G_Y/Y\}\}_{i\in I} \upharpoonright r[a] && \text{(Step} \Rightarrow \text{Fig. VII.5.2)}\\
={} & r_1[x_1] \twoheadrightarrow r_2[x_2]\,\mathbf{:}\,\{\ell_i \,.\, G_i\}_{i\in I}\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Fig. VII.4.3)}\\
={} & G\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

- **Step.** $G = r_1[x_1] \twoheadrightarrow r_2[x_2]\,\mathbf{:}\,\{\ell_i \,.\, G_i\}_{i\in I}$ **and**
  $G \upharpoonright r[a] = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, G_i \upharpoonright r[a]\}_{i\in I}$ **and** $r_1[x_1] \neq r[a] = r_2[x_2]$

  Conclude:

$$\begin{aligned}
& (G \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \\
={} & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, G_i \upharpoonright r[a]\}_{i\in I}\,\{G_Y \upharpoonright r[a]/Y\} && \text{(A2, Step)}\\
={} & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, (G_i \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\}\}_{i\in I} && \text{(Fig. VII.4.3)}\\
={} & r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, G_i\,\{G_Y/Y\} \upharpoonright r[a]\}_{i\in I} && \text{(Induction)}\\
={} & r_1[x_1] \twoheadrightarrow r_2[x_2]\,\mathbf{:}\,\{\ell_i \,.\, G_i\,\{G_Y/Y\}\}_{i\in I} \upharpoonright r[a] && \text{(Step} \Rightarrow \text{Fig. VII.5.2)}\\
={} & r_1[x_1] \twoheadrightarrow r_2[x_2]\,\mathbf{:}\,\{\ell_i \,.\, G_i\}_{i\in I}\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Fig. VII.4.3)}\\
={} & G\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

- **Step.** $G = r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I}$ **and**
  $G \upharpoonright r[a] = \bigsqcap\{G_i \upharpoonright r[a]\}_{i \in I}$ **and** $r_1[x_1] \neq r[a] \neq r_2[x_2]$

  Conclude:

$$\begin{aligned}
& (G \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \\
={}& (\bigsqcap\{G_i \upharpoonright r[a]\}_{i \in I})\,\{G_Y \upharpoonright r[a]/Y\} && \text{(A2, Step)}\\
={}& \bigsqcap\{(G_i \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\}\}_{i \in I} && \text{(Thm. VII.5.1:1)}\\
={}& \bigsqcap\{G_i\,\{G_Y/Y\} \upharpoonright r[a]\}_{i \in I} && \text{(Induction)}\\
={}& r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, G_i\,\{G_Y/Y\}\}_{i \in I} \upharpoonright r[a] && \text{(Step} \Rightarrow \text{Fig. VII.5.2)}\\
={}& r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I}\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Fig. VII.4.3)}\\
={}& G\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

- **Step.** $G = \mathtt{rec}\ X\ G_X$ **and** $G \upharpoonright r[a] = \mathtt{rec}\ X\ (G_X \upharpoonright r[a])$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$\begin{aligned}
& (G \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \\
={}& \mathtt{rec}\ X\ (G_X \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \text{(A2, Step)}\\
={}& \mathtt{rec}\ X\ (G_X \upharpoonright r[a]) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={}& \mathtt{rec}\ X\ G_X \upharpoonright r[a] && \text{(Step} \Rightarrow \text{Fig. VII.5.2)}\\
={}& \mathtt{rec}\ X\ G_X\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={}& G\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

  - **Case.** $X \neq Y$

    Conclude:

$$\begin{aligned}
& (G \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \\
={}& \mathtt{rec}\ X\ (G_X \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\} && \text{(A2, Step)}\\
={}& \mathtt{rec}\ X\ ((G_X \upharpoonright r[a])\,\{G_Y \upharpoonright r[a]/Y\}) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={}& \mathtt{rec}\ X\ (G_X\,\{G_Y/Y\} \upharpoonright r[a]) && \text{(Induction)}\\
={}& \mathtt{rec}\ X\ (G_X\,\{G_Y/Y\}) \upharpoonright r[a] && \text{(Fig. VII.5.2)}\\
={}& \mathtt{rec}\ X\ G_X\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
={}& G\,\{G_Y/Y\} \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

QED.

VIII.22 Proof of Theorem VII.6.1

- **A1.** $\mathsf{Wf}_{f,\mathcal{X}}(T)$

By induction on A1 (Fig. VII.4.2):

- **Base.** $T = X$ **and** $X \in \mathcal{X}$

  Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(T) & \text{(A1)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X) & \text{(Base)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X\,(\!(R[\phi])\!)) & \text{(Fig. VII.6.1)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,(\!(R[\phi])\!)) & \text{(Base)}
\end{array}$$

- **Step.** $T = r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i\in I}$ **and**

  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and**

  $\Big[\mathsf{Wf}_{f,\mathcal{X}}(G_i)$ **for-all** $i \in I\Big]$

  Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(G_i)\ \textbf{for-all}\ i \in I & \text{(Step)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(G_i\,(\!(R[\phi])\!))\ \textbf{for-all}\ i \in I & \text{(Induction)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,(\!(R[\phi])\!) \twoheadrightarrow r_2[x_2]\,(\!(R[\phi])\!) : \{\ell_i \,.\, G_i\,(\!(R[\phi])\!)\}_{i\in I}) & \text{(Fig. VII.4.2)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i\in I}\,(\!(R[\phi])\!)) & \text{(Fig. VII.6.1)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,(\!(R[\phi])\!)) & \text{(Step)}
\end{array}$$

- **Step.** $T = r_2[x_2]\,!\,\{\ell_i \,.\, L_i\}_{i\in I}$ **and**

  $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(L_i)$ **for-all** $i \in I\Big]$

  Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(L_i)\ \textbf{for-all}\ i \in I & \text{(Step)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(L_i\,(\!(R[\phi])\!))\ \textbf{for-all}\ i \in I & \text{(Induction)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,(\!(R[\phi])\!)\,!\,\{\ell_i \,.\, L_i\,(\!(R[\phi])\!)\}_{i\in I}) & \text{(Fig. VII.4.2)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,!\,\{\ell_i \,.\, L_i\}_{i\in I}\,(\!(R[\phi])\!)) & \text{(Fig. VII.6.1)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,(\!(R[\phi])\!)) & \text{(Step)}
\end{array}$$

- **Step.** $T = r_1[x_1]\,?\{\ell_i \,.\, L_i\}_{i\in I}$ **and**

  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(L_i)$ **for-all** $i \in I\Big]$

  Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(L_i)\ \textbf{for-all}\ i \in I & \text{(Step)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(L_i\,(\!(R[\phi])\!))\ \textbf{for-all}\ i \in I & \text{(Induction)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,(\!(R[\phi])\!)\,?\{\ell_i \,.\, L_i\,(\!(R[\phi])\!)\}_{i\in I}) & \text{(Fig. VII.4.2)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,?\{\ell_i \,.\, G_i\}_{i\in I}\,(\!(R[\phi])\!)) & \text{(Fig. VII.6.1)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T\,(\!(R[\phi])\!)) & \text{(Step)}
\end{array}$$

- **Step.** $T = \texttt{rec}\ X\ T_X$ **and** $\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(T_X)$

Conclude:

$$\begin{array}{rlr}
 & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(T_X) & \text{(Step)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(T_X \llparenthesis R[\phi]\rrparenthesis) & \text{(Induction)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{\textbf{rec}}\ X\ (T_X \llparenthesis R[\phi]\rrparenthesis)) & \text{(Fig. VII.4.2)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{\textbf{rec}}\ X\ T_X \llparenthesis R[\phi]\rrparenthesis) & \text{(Fig. VII.6.1)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(T \llparenthesis R[\phi]\rrparenthesis) & \text{(Step)}
\end{array}$$

QED.

VIII.23 Proof of Theorem VII.6.2

By induction on T (Fig. VII.4.1):

- **Base.** $T = X$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

    $$\begin{array}{rlr}
     & T \llparenthesis R[\phi]\rrparenthesis \{T_Y \llparenthesis R[\phi]\rrparenthesis/Y\} & \\
    = & X \llparenthesis R[\phi]\rrparenthesis \{T_Y \llparenthesis R[\phi]\rrparenthesis/Y\} & \text{(Base)}\\
    = & X \{T_Y \llparenthesis R[\phi]\rrparenthesis/Y\} & \text{(Fig. VII.6.1)}\\
    = & T_Y \llparenthesis R[\phi]\rrparenthesis & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
    = & X \{T_Y/Y\} \llparenthesis R[\phi]\rrparenthesis & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
    = & T \{T_Y/Y\} \llparenthesis R[\phi]\rrparenthesis & \text{(Base)}
    \end{array}$$

  - **Case.** $X \neq Y$

    Conclude:

    $$\begin{array}{rlr}
     & T \llparenthesis R[\phi]\rrparenthesis \{T_Y \llparenthesis R[\phi]\rrparenthesis/Y\} & \\
    = & X \llparenthesis R[\phi]\rrparenthesis \{T_Y \llparenthesis R[\phi]\rrparenthesis/Y\} & \text{(Base)}\\
    = & X \{T_Y \llparenthesis R[\phi]\rrparenthesis/Y\} & \text{(Fig. VII.6.1)}\\
    = & X & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
    = & X \llparenthesis R[\phi]\rrparenthesis & \text{(Fig. VII.6.1)}\\
    = & X \{T_Y/Y\} \llparenthesis R[\phi]\rrparenthesis & \text{(Case} \Rightarrow \text{Fig. VII.4.3)}\\
    = & T \{T_Y/Y\} \llparenthesis R[\phi]\rrparenthesis & \text{(Base)}
    \end{array}$$

- **Step.** $T = r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I}$

Conclude:

$$\begin{aligned}
& T\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \\
={}& r_1[x_1] \rightarrow r_2[x_2]\,\mathbf{:}\{\ell_i \,.\, G_i\}_{i\in I}\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Step)}\\
={}& r_1[x_1]\,(\!(R[\phi])\!) \rightarrow r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{:}\{\ell_i \,.\, G_i\,(\!(R[\phi])\!)\}_{i\in I}\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Fig. VII.6.1)}\\
={}& r_1[x_1]\,(\!(R[\phi])\!) \rightarrow r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{:}\{\ell_i \,.\, G_i\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\}\}_{i\in I} && \text{(Fig. VII.4.3)}\\
={}& r_1[x_1]\,(\!(R[\phi])\!) \rightarrow r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{:}\{\ell_i \,.\, G_i\,\{T_Y/Y\}\,(\!(R[\phi])\!)\}_{i\in I} && \text{(Induction)}\\
={}& r_1[x_1] \rightarrow r_2[x_2]\,\mathbf{:}\{\ell_i \,.\, G_i\,\{T_Y/Y\}\}_{i\in I}\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)}\\
={}& r_1[x_1] \rightarrow r_2[x_2]\,\mathbf{:}\{\ell_i \,.\, G_i\}_{i\in I}\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Fig. VII.4.3)}\\
={}& T\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}$$

- **Step.** $T = r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\}_{i\in I}$

  Conclude:

$$\begin{aligned}
& T\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \\
={}& r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\}_{i\in I}\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Step)}\\
={}& r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\{\ell_i \,.\, L_i\,(\!(R[\phi])\!)\}_{i\in I}\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Fig. VII.6.1)}\\
={}& r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\{\ell_i \,.\, L_i\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\}\}_{i\in I} && \text{(Fig. VII.4.3)}\\
={}& r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\{\ell_i \,.\, L_i\,\{T_Y/Y\}\,(\!(R[\phi])\!)\}_{i\in I} && \text{(Induction)}\\
={}& r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\,\{T_Y/Y\}\}_{i\in I}\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)}\\
={}& r_2[x_2]\,\mathbf{!}\{\ell_i \,.\, L_i\}_{i\in I}\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Fig. VII.4.3)}\\
={}& T\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}$$

- **Step.** $T = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I}$

  Conclude:

$$\begin{aligned}
& T\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \\
={}& r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I}\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Step)}\\
={}& r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?}\{\ell_i \,.\, L_i\,(\!(R[\phi])\!)\}_{i\in I}\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Fig. VII.6.1)}\\
={}& r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?}\{\ell_i \,.\, L_i\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\}\}_{i\in I} && \text{(Fig. VII.4.3)}\\
={}& r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?}\{\ell_i \,.\, L_i\,\{T_Y/Y\}\,(\!(R[\phi])\!)\}_{i\in I} && \text{(Induction)}\\
={}& r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\,\{T_Y/Y\}\}_{i\in I}\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)}\\
={}& r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_i\}_{i\in I}\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Fig. VII.4.3)}\\
={}& T\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}$$

- **Step.** $T = \mathtt{rec}\ X\ T_X$

  By case distinction:

  - **Case.** $X = Y$

Conclude:

$$\begin{aligned}
& T\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} \\
=\ & \mathbf{rec}\ X\ T_X\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Step)} \\
=\ & \mathbf{rec}\ X\ (T_X\,(\!(R[\phi])\!))\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Fig. VII.6.1)} \\
=\ & \mathbf{rec}\ X\ (T_X\,(\!(R[\phi])\!)) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\
=\ & \mathbf{rec}\ X\ T_X\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
=\ & \mathbf{rec}\ X\ T_X\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\
=\ & T\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}$$

- **Case.** $X \neq Y$

  Conclude:

$$\begin{aligned}
& T\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} \\
=\ & \mathbf{rec}\ X\ T_X\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Step)} \\
=\ & \mathbf{rec}\ X\ (T_X\,(\!(R[\phi])\!))\,\{T_Y\,(\!(R[\phi])\!)/Y\} && \text{(Fig. VII.6.1)} \\
=\ & \mathbf{rec}\ X\ (T_X\,(\!(R[\phi])\!)\,\{T_Y\,(\!(R[\phi])\!)/Y\}) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\
=\ & \mathbf{rec}\ X\ (T_X\,\{T_Y/Y\}\,(\!(R[\phi])\!)) && \text{(Induction)} \\
=\ & \mathbf{rec}\ X\ (T_X\,\{T_Y/Y\})\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
=\ & \mathbf{rec}\ X\ T_X\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Case} \Rightarrow \text{Fig. VII.4.3)} \\
=\ & T\,\{T_Y/Y\}\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}$$

QED.

VIII.24 Proof of Theorem VII.6.3

- **A1.** $\langle L_1, L_2 \rangle \in \operatorname{dom} \sqcap$

By induction on A1 (Fig. VII.5.1):

- **Base.** $L_1 = L_2 = X$ **and** $L_1 \sqcap L_2 = X$

  Conclude:

$$\begin{aligned}
& (L_1 \sqcap L_2)\,(\!(R[\phi])\!) \\
=\ & X\,(\!(R[\phi])\!) && \text{(Base)} \\
=\ & X && \text{(Fig. VII.6.1)} \\
=\ & X \sqcap X && \text{(Lem. VII.5.1:2)} \\
=\ & X\,(\!(R[\phi])\!) \sqcap X\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
=\ & L_1\,(\!(R[\phi])\!) \sqcap L_2\,(\!(R[\phi])\!) && \text{(Base)}
\end{aligned}$$

- **Step.** $L_1 = r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,L_{i,1}\}_{i \in I}$ **and** $L_2 = r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,L_{i,2}\}_{i \in I}$ **and** $L_1 \sqcap L_2 = r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,L_{i,1} \sqcap L_{i,2}\}_{i \in I}$

Conclude:

$$
\begin{aligned}
& (L_1 \sqcap L_2)\,(\!(R[\phi])\!) \\
= \;& r_2[x_2]\,\mathbf{!}\,\{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i \in I}\,(\!(R[\phi])\!) && \text{(Step)} \\
= \;& r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\,\{\ell_i \,.\, (L_{i,1} \sqcap L_{i,2})\,(\!(R[\phi])\!)\}_{i \in I} && \text{(Fig. VII.6.1)} \\
= \;& r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\,\{\ell_i \,.\, L_{i,1}\,(\!(R[\phi])\!) \sqcap L_{i,2}\,(\!(R[\phi])\!)\}_{i \in I} && \text{(Induction)} \\
= \;& r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\,\{\ell_i \,.\, L_{i,1}\,(\!(R[\phi])\!)\}_{i \in I} \sqcap r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\,\{\ell_i \,.\, L_{i,2}\,(\!(R[\phi])\!)\}_{i \in I} && \text{(Fig. VII.5.1)} \\
= \;& r_2[x_2]\,\mathbf{!}\,\{\ell_i \,.\, L_{i,1}\}_{i \in I}\,(\!(R[\phi])\!) \sqcap r_2[x_2]\,\mathbf{!}\,\{\ell_i \,.\, L_{i,2}\}_{i \in I}\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
= \;& L_1\,(\!(R[\phi])\!) \sqcap L_2\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}
$$

- **Step.** $L_1 = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\}_{i \in I_1}$ **and** $L_2 = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,2}\}_{i \in I_2}$ **and** $L_1 \sqcap L_2 = r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\}_{i \in I_1 \setminus I_2} \cup \{\ell_i \,.\, L_{i,2}\}_{i \in I_2 \setminus I_1} \cup \{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i \in I_1 \cap I_2}$ **and** $\Big[\ell_{i_1} \neq \ell_{i_2}$ **for-all** $i_1 \in I_1 \setminus I_2, i_2 \in I_2 \setminus I_1\Big]$

Conclude:

$$
\begin{aligned}
& (L_1 \sqcap L_2)\,(\!(R[\phi])\!) \\
= \;& r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\}_{i \in I_1 \setminus I_2} \cup \{\ell_i \,.\, L_{i,2}\}_{i \in I_2 \setminus I_1} \cup \{\ell_i \,.\, L_{i,1} \sqcap L_{i,2}\}_{i \in I_1 \cap I_2}\,(\!(R[\phi])\!) && \text{(Step)} \\
= \;& r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?} && \text{(Fig. VII.6.1)} \\
& \quad \{\ell_i \,.\, L_{i,1}\,(\!(R[\phi])\!)\}_{i \in I_1 \setminus I_2} \cup \{\ell_i \,.\, L_{i,2}\,(\!(R[\phi])\!)\}_{i \in I_2 \setminus I_1} \cup \{\ell_i \,.\, (L_{i,1} \sqcap L_{i,2})\,(\!(R[\phi])\!)\}_{i \in I_1 \cap I_2} \\
= \;& r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?} && \text{(Induction)} \\
& \quad \{\ell_i \,.\, L_{i,1}\,(\!(R[\phi])\!)\}_{i \in I_1 \setminus I_2} \cup \{\ell_i \,.\, L_{i,2}\,(\!(R[\phi])\!)\}_{i \in I_2 \setminus I_1} \cup \{\ell_i \,.\, L_{i,1}\,(\!(R[\phi])\!) \sqcap L_{i,2}\,(\!(R[\phi])\!)\}_{i \in I_1 \cap I_2} \\
= \;& r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\,(\!(R[\phi])\!)\}_{i \in I_1} \sqcap r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?}\{\ell_i \,.\, L_{i,2}\,(\!(R[\phi])\!)\}_{i \in I_2} \\
& && \text{(Step} \Rightarrow \text{Fig. VII.5.1)} \\
= \;& r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,1}\}_{i \in I_1}\,(\!(R[\phi])\!) \sqcap r_1[x_1]\,\mathbf{?}\{\ell_i \,.\, L_{i,2}\}_{i \in I_2}\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
= \;& L_1\,(\!(R[\phi])\!) \sqcap L_2\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}
$$

- **Step.** $L_1 = \texttt{rec}\ X\ L_{X,1}$ **and** $L_2 = \texttt{rec}\ X\ L_{X,2}$ **and** $L_1 \sqcap L_2 = \texttt{rec}\ X\ (L_{X,1} \sqcap L_{X,2})$

Conclude:

$$
\begin{aligned}
& (L_1 \sqcap L_2)\,(\!(R[\phi])\!) \\
= \;& \texttt{rec}\ X\ (L_{X,1} \sqcap L_{X,2})\,(\!(R[\phi])\!) && \text{(Step)} \\
= \;& \texttt{rec}\ X\ ((L_{X,1} \sqcap L_{X,2})\,(\!(R[\phi])\!)) && \text{(Fig. VII.6.1)} \\
= \;& \texttt{rec}\ X\ (L_{X,1}\,(\!(R[\phi])\!) \sqcap L_{X,2}\,(\!(R[\phi])\!)) && \text{(Induction)} \\
= \;& \texttt{rec}\ X\ (L_{X,1}\,(\!(R[\phi])\!)) \sqcap \texttt{rec}\ X\ (L_{X,2}\,(\!(R[\phi])\!)) && \text{(Fig. VII.5.1)} \\
= \;& \texttt{rec}\ X\ L_{X,1}\,(\!(R[\phi])\!) \sqcap \texttt{rec}\ X\ L_{X,2}\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
= \;& L_1\,(\!(R[\phi])\!) \sqcap L_2\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}
$$

QED.

VIII.25 Proof of Theorem VII.6.4

- **A1.** $\langle G, r[a] \rangle \in \operatorname{dom} \restriction$

- **A2.** $r \notin R$

By induction on A1 (Fig. VII.5.2):

- **Base.** $G = X$ **and** $G \upharpoonright r[a] = X$

  Conclude:

$$\begin{aligned}
& (G \upharpoonright r[a])\,(\!(R[\phi])\!) && \\
=\;& X\,(\!(R[\phi])\!) && \text{(Base)}\\
=\;& X && \text{(Fig. VII.6.1)}\\
=\;& X \upharpoonright r[a] && \text{(Fig. VII.5.2)}\\
=\;& X\,(\!(R[\phi])\!) \upharpoonright r[a] && \text{(Fig. VII.6.1)}\\
=\;& G\,(\!(R[\phi])\!) \upharpoonright r[a] && \text{(Base)}
\end{aligned}$$

- **Step.** $G = r_1[x_1] \rightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, G_i\}_{i \in I}$ **and**
  $G \upharpoonright r[a] = r_2[x_2] \,\mathbf{!}\, \{\ell_i \,.\, G_i \upharpoonright r[a]\}_{i \in I}$ **and** $r_1[x_1] = r[a] \neq r_2[x_2]$

  - **B1.** Conclude:

$$\begin{aligned}
& r_1[x_1] = r[a] && \text{(Step)}\\
\textbf{impl. }\; & r_1 = r && \text{(–)}\\
\textbf{impl. }\; & r_1 = r \;\textbf{ and }\; r \notin R && \text{(A2)}\\
\textbf{impl. }\; & r_1 \notin R && \text{(=)}\\
\textbf{impl. }\; & r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1] && \text{(Fig. VII.6.1)}\\
\textbf{impl. }\; & r_1[x_1]\,(\!(R[\phi])\!) = r[a] && \text{(Step)}
\end{aligned}$$

  - **B2.** Conclude:

$$\begin{aligned}
& r_2 = r && \text{(Step)}\\
\textbf{impl. }\; & r_2 = r \;\textbf{ and }\; r \notin R && \text{(A2)}\\
\textbf{impl. }\; & r_2 \notin R && \text{(=)}\\
\textbf{impl. }\; & r_2[x_2]\,(\!(R[\phi])\!) = r_2[x_2] && \text{(Fig. VII.6.1)}\\
\textbf{impl. }\; & r_2[x_2]\,(\!(R[\phi])\!) = r_2[x_2] \;\textbf{ and }\; r[a] \neq r_2[x_2] && \text{(Step)}\\
\textbf{impl. }\; & r_2[x_2]\,(\!(R[\phi])\!) \neq r[a] && \text{(=)}
\end{aligned}$$

  - **B3.** Conclude:

$$\begin{aligned}
& r_2 \neq r \;\textbf{ and }\; r_2[x_2]\,(\!(R[\phi])\!) = r_2[\phi(x_2)] && \\
\textbf{impl. }\; & r_2[\phi(x_2)] \neq r[a] \;\textbf{ and }\; r_2[x_2]\,(\!(R[\phi])\!) = r_2[\phi(x_2)] && \text{(–)}\\
\textbf{impl. }\; & r_2[x_2]\,(\!(R[\phi])\!) \neq r[a] && \text{(=)}
\end{aligned}$$

  - **B4.** Conclude:

$$\begin{aligned}
& r_2 \neq r \;\textbf{ and }\; r_2[x_2]\,(\!(R[\phi])\!) = r_2[x_2] && \\
\textbf{impl. }\; & r_2[x_2] \neq r[a] \;\textbf{ and }\; r_2[x_2]\,(\!(R[\phi])\!) = r_2[x_2] && \text{(–)}\\
\textbf{impl. }\; & r_2[x_2]\,(\!(R[\phi])\!) \neq r[a] && \text{(=)}
\end{aligned}$$

- **B5.** Conclude:

$$\begin{array}{lll}
 & r_2 \neq r & \text{(Step)}\\
\textsf{impl.} & r_2 \neq r\ \ \textsf{and}\ \ \Big[r_2[x_2]\,(\!(R[\phi])\!) = r_2[\phi(x_2)]\ \ \textsf{or}\ \ r_2[x_2]\,(\!(R[\phi])\!) = r_2[x_2]\Big] & \text{(Fig. VII.6.1)}\\
\textsf{impl.} & \Big[r_2 \neq r\ \ \textsf{and}\ \ r_2[x_2]\,(\!(R[\phi])\!) = r_2[\phi(x_2)]\Big]\ \ \textsf{or}\ \ \Big[r_2 \neq r\ \ \textsf{and}\ \ r_2[x_2]\,(\!(R[\phi])\!) = r_2[x_2]\Big] & \\
 & & (-)\\
\textsf{impl.} & r_2[x_2]\,(\!(R[\phi])\!) \neq r[a] & \text{(B3, B4)}
\end{array}$$

- **B6.** Conclude:

$$\begin{array}{lll}
 & r = r_2\ \ \textsf{or}\ \ r \neq r_2 & (-)\\
\textsf{impl.} & r_2[x_2]\,(\!(R[\phi])\!) \neq r[a] & \text{(B2, B5)}
\end{array}$$

Conclude:

$$\begin{array}{rll}
 & (G \upharpoonright r[a])\,(\!(R[\phi])\!) & \\
= & r_2[x_2]\,\mathbf{!}\,\{\ell_i\,.\,G_i \upharpoonright r[a]\}_{i\in I}\,(\!(R[\phi])\!) & \text{(Step)}\\
= & r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\,\{\ell_i\,.\,(G_i \upharpoonright r[a])\,(\!(R[\phi])\!)\}_{i\in I} & \text{(Fig. VII.6.1)}\\
= & r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{!}\,\{\ell_i\,.\,G_i\,(\!(R[\phi])\!) \upharpoonright r[a]\}_{i\in I} & \text{(A2} \Rightarrow \text{Induction)}\\
= & r_1[x_1]\,(\!(R[\phi])\!) \rightarrowtriangle r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{:}\,\{\ell_i\,.\,G_i\,(\!(R[\phi])\!)\}_{i\in I} \upharpoonright r[a] & \text{(B1, B6} \Rightarrow \text{Fig. VII.5.2)}\\
= & r_1[x_1] \rightarrowtriangle r_2[x_2]\,\mathbf{:}\,\{\ell_i\,.\,G_i\}_{i\in I}\,(\!(R[\phi])\!) \upharpoonright r[a] & \text{(Fig. VII.6.1)}\\
= & G\,(\!(R[\phi])\!) \upharpoonright r[a] & \text{(Step)}
\end{array}$$

- **Step.** $G = r_1[x_1] \rightarrowtriangle r_2[x_2]\,\mathbf{:}\,\{\ell_i\,.\,G_i\}_{i\in I}$ **and**
  $G \upharpoonright r[a] = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,G_i \upharpoonright r[a]\}_{i\in I}$ **and** $r_1[x_1] \neq r[a] = r_2[x_2]$

  - **C1.** Conclude:

$$\begin{array}{lll}
 & r_1 = r & \text{(Step)}\\
\textsf{impl.} & r_1 = r\ \ \textsf{and}\ \ r \notin R & \text{(A2)}\\
\textsf{impl.} & r_1 \notin R & (=)\\
\textsf{impl.} & r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1] & \text{(Fig. VII.6.1)}\\
\textsf{impl.} & r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1]\ \ \textsf{and}\ \ r[a] \neq r_1[x_1] & \text{(Step)}\\
\textsf{impl.} & r_1[x_1]\,(\!(R[\phi])\!) \neq r[a] & (=)
\end{array}$$

  - **C2.** Conclude:

$$\begin{array}{lll}
 & r_1 \neq r\ \ \textsf{and}\ \ r_1[x_1]\,(\!(R[\phi])\!) = r_1[\phi(x_1)] & \\
\textsf{impl.} & r_1[\phi(x_1)] \neq r[a]\ \ \textsf{and}\ \ r_1[x_1]\,(\!(R[\phi])\!) = r_1[\phi(x_1)] & (-)\\
\textsf{impl.} & r_1[x_1]\,(\!(R[\phi])\!) \neq r[a] & (=)
\end{array}$$

  - **C3.** Conclude:

$$\begin{array}{lll}
 & r_1 \neq r\ \ \textsf{and}\ \ r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1] & \\
\textsf{impl.} & r_1[x_1] \neq r[a]\ \ \textsf{and}\ \ r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1] & (-)\\
\textsf{impl.} & r_1[x_1]\,(\!(R[\phi])\!) \neq r[a] & (=)
\end{array}$$

- **C4.** Conclude:

$$
\begin{array}{ll}
 & r_1 \neq r \qquad \text{(Step)} \\
\textsf{\textbf{impl.}} & r_1 \neq r \;\textsf{\textbf{and}}\; \Big[r_1[x_1]\,(\!(R[\phi])\!) = r_1[\phi(x_1)] \;\textsf{\textbf{or}}\; r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1]\Big] \qquad \text{(Fig. VII.6.1)} \\
\textsf{\textbf{impl.}} & \Big[r_1 \neq r \;\textsf{\textbf{and}}\; r_1[x_1]\,(\!(R[\phi])\!) = r_1[\phi(x_1)]\Big] \;\textsf{\textbf{or}}\; \Big[r_1 \neq r \;\textsf{\textbf{and}}\; r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1]\Big] \qquad \text{(–)} \\
\textsf{\textbf{impl.}} & r_1[x_1]\,(\!(R[\phi])\!) \neq r[a] \qquad \text{(C2, C3)}
\end{array}
$$

- **C5.** Conclude:

$$
\begin{array}{ll}
 & r = r_1 \;\textsf{\textbf{or}}\; r \neq r_1 \qquad \text{(–)} \\
\textsf{\textbf{impl.}} & r_1[x_2]\,(\!(R[\phi])\!) \neq r[a] \qquad \text{(C1, C4)}
\end{array}
$$

- **C6.** Conclude:

$$
\begin{array}{ll}
 & r_2[x_2] = r[a] \qquad \text{(Step)} \\
\textsf{\textbf{impl.}} & r_2 = r \qquad \text{(–)} \\
\textsf{\textbf{impl.}} & r_2 = r \;\textsf{\textbf{and}}\; r \notin R \qquad \text{(A2)} \\
\textsf{\textbf{impl.}} & r_2 \notin R \qquad \text{(=)} \\
\textsf{\textbf{impl.}} & r_2[x_2]\,(\!(R[\phi])\!) = r_2[x_2] \qquad \text{(Fig. VII.6.1)} \\
\textsf{\textbf{impl.}} & r_2[x_2]\,(\!(R[\phi])\!) = r[a] \qquad \text{(Step)}
\end{array}
$$

Conclude:

$$
\begin{array}{rll}
 & (G \upharpoonright r[a])\,(\!(R[\phi])\!) & \\
= & r_1[x_1]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, G_i \upharpoonright r[a]\}_{i\in I}\,(\!(R[\phi])\!) & \text{(Step)} \\
= & r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?}\{\ell_i \,\mathbf{.}\, (G_i \upharpoonright r[a])\,(\!(R[\phi])\!)\}_{i\in I} & \text{(Fig. VII.6.1)} \\
= & r_1[x_1]\,(\!(R[\phi])\!)\,\mathbf{?}\{\ell_i \,\mathbf{.}\, G_i\,(\!(R[\phi])\!) \upharpoonright r[a]\}_{i\in I} & \text{(A2} \Rightarrow \text{Induction)} \\
= & r_1[x_1]\,(\!(R[\phi])\!) \rightarrowtriangle r_2[x_2]\,(\!(R[\phi])\!)\,\mathbf{:}\{\ell_i \,\mathbf{.}\, G_i\,(\!(R[\phi])\!)\}_{i\in I} \upharpoonright r[a] & \text{(C5, C6} \Rightarrow \text{Fig. VII.5.2)} \\
= & r_1[x_1] \rightarrowtriangle r_2[x_2]\,\mathbf{:}\{\ell_i \,\mathbf{.}\, G_i\}_{i\in I}\,(\!(R[\phi])\!) \upharpoonright r[a] & \text{(Fig. VII.6.1)} \\
= & G\,(\!(R[\phi])\!) \upharpoonright r[a] & \text{(Step)}
\end{array}
$$

- **Step.** $G = r_1[x_1] \rightarrowtriangle r_2[x_2]\,\mathbf{:}\{\ell_i \,\mathbf{.}\, G_i\}_{i\in I}$ **and**
  $G \upharpoonright r[a] = \bigsqcap\{G_i \upharpoonright r[a]\}_{i\in I}$ **and** $r_1[x_1] \neq r[a] \neq r_2[x_2]$

  - **D1.** Conclude:

$$
\begin{array}{ll}
 & r_1 = r \qquad \text{(Step)} \\
\textsf{\textbf{impl.}} & r_1 = r \;\textsf{\textbf{and}}\; r \notin R \qquad \text{(A2)} \\
\textsf{\textbf{impl.}} & r_1 \notin R \qquad \text{(=)} \\
\textsf{\textbf{impl.}} & r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1] \qquad \text{(Fig. VII.6.1)} \\
\textsf{\textbf{impl.}} & r_1[x_1]\,(\!(R[\phi])\!) = r_1[x_1] \;\textsf{\textbf{and}}\; r[a] \neq r_1[x_1] \qquad \text{(Step)} \\
\textsf{\textbf{impl.}} & r_1[x_1]\,(\!(R[\phi])\!) \neq r[a] \qquad \text{(=)}
\end{array}
$$

- **D2.** Conclude:

$$\begin{array}{lll}
 & r_1 \neq r \ \textbf{ and } \ r_1[x_1]\,((R[\phi])) = r_1[\phi(x_1)] & \\
\textbf{impl.} & r_1[\phi(x_1)] \neq r[a] \ \textbf{ and } \ r_1[x_1]\,((R[\phi])) = r_1[\phi(x_1)] & (-) \\
\textbf{impl.} & r_1[x_1]\,((R[\phi])) \neq r[a] & (=)
\end{array}$$

- **D3.** Conclude:

$$\begin{array}{lll}
 & r_1 \neq r \ \textbf{ and } \ r_1[x_1]\,((R[\phi])) = r_1[x_1] & \\
\textbf{impl.} & r_1[x_1] \neq r[a] \ \textbf{ and } \ r_1[x_1]\,((R[\phi])) = r_1[x_1] & (-) \\
\textbf{impl.} & r_1[x_1]\,((R[\phi])) \neq r[a] & (=)
\end{array}$$

- **D4.** Conclude:

$$\begin{array}{lll}
 & r_1 \neq r & (\text{Step}) \\
\textbf{impl.} & r_1 \neq r \ \textbf{ and } \ \Big[r_1[x_1]\,((R[\phi])) = r_1[\phi(x_1)] \ \textbf{ or } \ r_1[x_1]\,((R[\phi])) = r_1[x_1]\Big] & (\text{Fig. VII.6.1}) \\
\textbf{impl.} & \Big[r_1 \neq r \ \textbf{ and } \ r_1[x_1]\,((R[\phi])) = r_1[\phi(x_1)]\Big] \ \textbf{ or } \ \Big[r_1 \neq r \ \textbf{ and } \ r_1[x_1]\,((R[\phi])) = r_1[x_1]\Big] & \\
 & & (-) \\
\textbf{impl.} & r_1[x_1]\,((R[\phi])) \neq r[a] & (\text{D2, D3})
\end{array}$$

- **D5.** Conclude:

$$\begin{array}{lll}
 & r = r_1 \ \textbf{ or } \ r \neq r_1 & (-) \\
\textbf{impl.} & r_1[x_2]\,((R[\phi])) \neq r[a] & (\text{D1, D4})
\end{array}$$

- **D6.** Conclude:

$$\begin{array}{lll}
 & r_2 = r & (\text{Step}) \\
\textbf{impl.} & r_2 = r \ \textbf{ and } \ r \notin R & (\text{A2}) \\
\textbf{impl.} & r_2 \notin R & (=) \\
\textbf{impl.} & r_2[x_2]\,((R[\phi])) = r_2[x_2] & (\text{Fig. VII.6.1}) \\
\textbf{impl.} & r_2[x_2]\,((R[\phi])) = r_2[x_2] \ \textbf{ and } \ r[a] \neq r_2[x_2] & (\text{Step}) \\
\textbf{impl.} & r_2[x_2]\,((R[\phi])) \neq r[a] & (=)
\end{array}$$

- **D7.** Conclude:

$$\begin{array}{lll}
 & r_2 \neq r \ \textbf{ and } \ r_2[x_2]\,((R[\phi])) = r_2[\phi(x_2)] & \\
\textbf{impl.} & r_2[\phi(x_2)] \neq r[a] \ \textbf{ and } \ r_2[x_2]\,((R[\phi])) = r_2[\phi(x_2)] & (-) \\
\textbf{impl.} & r_2[x_2]\,((R[\phi])) \neq r[a] & (=)
\end{array}$$

- **D8.** Conclude:

$$\begin{array}{lll}
 & r_2 \neq r \ \textbf{ and } \ r_2[x_2]\,((R[\phi])) = r_2[x_2] & \\
\textbf{impl.} & r_2[x_2] \neq r[a] \ \textbf{ and } \ r_2[x_2]\,((R[\phi])) = r_2[x_2] & (-) \\
\textbf{impl.} & r_2[x_2]\,((R[\phi])) \neq r[a] & (=)
\end{array}$$

- **D9.** Conclude:

$$
\begin{aligned}
& r_2 \neq r && \text{(Step)}\\
\textbf{impl. } & r_2 \neq r \ \textbf{and}\ \Big[r_2[x_2] \llparenthesis R[\phi] \rrparenthesis = r_2[\phi(x_2)] \ \textbf{or}\ r_2[x_2] \llparenthesis R[\phi] \rrparenthesis = r_2[x_2] \Big] && \text{(Fig. VII.6.1)}\\
\textbf{impl. } & \Big[r_2 \neq r \ \textbf{and}\ r_2[x_2] \llparenthesis R[\phi] \rrparenthesis = r_2[\phi(x_2)] \Big] \ \textbf{or}\ \Big[r_2 \neq r \ \textbf{and}\ r_2[x_2] \llparenthesis R[\phi] \rrparenthesis = r_2[x_2] \Big] && \text{(–)}\\
\textbf{impl. } & r_2[x_2] \llparenthesis R[\phi] \rrparenthesis \neq r[a] && \text{(D7, D8)}
\end{aligned}
$$

- **D10.** Conclude:

$$
\begin{aligned}
& r = r_2 \ \textbf{or}\ r \neq r_2 && \text{(–)}\\
\textbf{impl. } & r_2[x_2] \llparenthesis R[\phi] \rrparenthesis \neq r[a] && \text{(D6, D9)}
\end{aligned}
$$

Conclude:

$$
\begin{aligned}
& (G \upharpoonright r[a]) \llparenthesis R[\phi] \rrparenthesis \\
=\ & (\textstyle\bigsqcap \{ G_i \upharpoonright r[a] \}_{i \in I}) \llparenthesis R[\phi] \rrparenthesis && \text{(Step)}\\
=\ & \textstyle\bigsqcap \{ (G_i \upharpoonright r[a]) \llparenthesis R[\phi] \rrparenthesis \}_{i \in I} && \text{(Thm. VII.6.3)}\\
=\ & \textstyle\bigsqcap \{ G_i \llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] \}_{i \in I} && \text{(A2 $\Rightarrow$ Induction)}\\
=\ & r_1[x_1] \llparenthesis R[\phi] \rrparenthesis \rightarrowtriangle r_2[x_2] \llparenthesis R[\phi] \rrparenthesis : \{ \ell_i \,.\, G_i \llparenthesis R[\phi] \rrparenthesis \}_{i \in I} \upharpoonright r[a] && \text{(D5, D10 $\Rightarrow$ Fig. VII.5.2)}\\
=\ & r_1[x_1] \rightarrowtriangle r_2[x_2] : \{ \ell_i \,.\, G_i \}_{i \in I} \llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] && \text{(Fig. VII.6.1)}\\
=\ & G \llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] && \text{(Step)}
\end{aligned}
$$

- **Step.** $G = \texttt{rec}\ X\ G_X$ **and** $G \upharpoonright r[a] = \texttt{rec}\ X\ (G_X \upharpoonright r[a])$

  Conclude:

$$
\begin{aligned}
& (G \upharpoonright r[a]) \llparenthesis R[\phi] \rrparenthesis \\
=\ & \texttt{rec}\ X\ (G_X \upharpoonright r[a]) \llparenthesis R[\phi] \rrparenthesis && \text{(Base)}\\
=\ & \texttt{rec}\ X\ ((G_X \upharpoonright r[a]) \llparenthesis R[\phi] \rrparenthesis) && \text{(Fig. VII.6.1)}\\
=\ & \texttt{rec}\ X\ (G_X \llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a]) && \text{(Induction)}\\
=\ & \texttt{rec}\ X\ (G_X \llparenthesis R[\phi] \rrparenthesis) \upharpoonright r[a] && \text{(Fig. VII.5.2)}\\
=\ & \texttt{rec}\ X\ G_X \llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] && \text{(Fig. VII.6.1)}\\
=\ & G \llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] && \text{(Base)}
\end{aligned}
$$

QED.

VIII.26 Proof of Theorem VII.6.5

Proof of (1)

- **A1.** $R \cap R' = \emptyset$

By case distinction (Fig. VII.6.1):

- **Case.** $r[x]\,\llparenthesis R[\phi]\rrparenthesis = r[\phi(x)]$ **and** $r \in R$ **and** $x \in \operatorname{dom}\phi$ **and**
  $r[x]\,\llparenthesis R'[\phi']\rrparenthesis = r[\phi'(x)]$ **and** $r \in R'$ **and** $x \in \operatorname{dom}\phi'$

  Conclude:

$$\begin{array}{llr} & r \in R \textbf{ and } r \in R' & \text{(Case)} \\ \textbf{impl.} & r \in R \cap R' & \text{(–)} \\ \textbf{impl.} & \textbf{false} & \text{(A1)} \end{array}$$

- **Case.** $r[x]\,\llparenthesis R[\phi]\rrparenthesis = r[\phi(x)]$ **and** $r \in R$ **and** $x \in \operatorname{dom}\phi$ **and**
  $r[x]\,\llparenthesis R'[\phi']\rrparenthesis = r[x]$ **and** $\Big[r \notin R'$ **or** $x \notin \operatorname{dom}\phi'\Big]$

  - **B1.** Conclude:

$$\begin{array}{llr} & r \in R & \text{(Case)} \\ \textbf{impl.} & r \notin R' & \text{(A1)} \end{array}$$

  Conclude:

$$\begin{array}{llr} & r[x]\,\llparenthesis R[\phi]\rrparenthesis\,\llparenthesis R'[\phi']\rrparenthesis & \\ = & r[\phi(x)]\,\llparenthesis R'[\phi']\rrparenthesis & \text{(Case)} \\ = & r[\phi(x)] & \text{(B1} \Rightarrow \text{Fig. VII.6.1)} \\ = & r[x]\,\llparenthesis R[\phi]\rrparenthesis & \text{(Case)} \\ = & r[x]\,\llparenthesis R'[\phi']\rrparenthesis\,\llparenthesis R[\phi]\rrparenthesis & \text{(Case)} \end{array}$$

- **Case.** $r[x]\,\llparenthesis R[\phi]\rrparenthesis = r[x]$ **and** $\Big[r \notin R$ **or** $x \notin \operatorname{dom}\phi\Big]$ **and**
  $r[x]\,\llparenthesis R'[\phi']\rrparenthesis = r[\phi'(x)]$ **and** $r \in R'$ **and** $x \in \operatorname{dom}\phi'$

  - **C1.** Conclude:

$$\begin{array}{llr} & r \in R' & \text{(Case)} \\ \textbf{impl.} & r \notin R & \text{(A1)} \end{array}$$

  Conclude:

$$\begin{array}{llr} & r[x]\,\llparenthesis R[\phi]\rrparenthesis\,\llparenthesis R'[\phi']\rrparenthesis & \\ = & r[x]\,\llparenthesis R'[\phi']\rrparenthesis & \text{(Case)} \\ = & r[\phi'(x)] & \text{(Case)} \\ = & r[\phi'(x)]\,\llparenthesis R[\phi]\rrparenthesis & \text{(C1} \Rightarrow \text{Fig. VII.6.1)} \\ = & r[x]\,\llparenthesis R'[\phi']\rrparenthesis\,\llparenthesis R[\phi]\rrparenthesis & \text{(Case)} \end{array}$$

- **Case.** $r[x]\,\llparenthesis R[\phi]\rrparenthesis = r[x]$ **and** $\Big[r \notin R$ **or** $x \notin \operatorname{dom}\phi\Big]$ **and**
  $r[x]\,\llparenthesis R'[\phi']\rrparenthesis = r[x]$ **and** $\Big[r \notin R'$ **or** $x \notin \operatorname{dom}\phi'\Big]$

Conclude:

$$\begin{aligned}
& r[x]\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!) \\
= {}& r[x]\,(\!(R'[\phi'])\!) && \text{(Case)} \\
= {}& r[x] && \text{(Case)} \\
= {}& r[x]\,(\!(R[\phi])\!) && \text{(Case)} \\
= {}& r[x]\,(\!(R'[\phi'])\!)\,(\!(R[\phi])\!) && \text{(Case)}
\end{aligned}$$

QED.

Proof of (2)

- **A1.** $R \cap R' = \emptyset$

By induction on T (Fig. VII.4.1):

- **Base.** $T = X$

  Conclude:

$$\begin{aligned}
& T\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!) \\
= {}& X\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!) && \text{(Base)} \\
= {}& X\,(\!(R'[\phi'])\!) && \text{(Fig. VII.6.1)} \\
= {}& X && \text{(Fig. VII.6.1)} \\
= {}& X\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
= {}& T\,(\!(R'[\phi'])\!)\,(\!(R[\phi])\!) && \text{(Base)}
\end{aligned}$$

- **Step.** $T = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i\in I}$

  Conclude:

$$\begin{aligned}
& T\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!) \\
= {}& r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i\in I}\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!) && \text{(Step)} \\
= {}& r_1[x_1\,(\!(R[\phi])\!)] \rightarrowtriangle r_2[x_2\,(\!(R[\phi])\!)] : \{\ell_i \,.\, G_i\,(\!(R[\phi])\!)\}_{i\in I}\,(\!(R'[\phi'])\!) && \text{(Fig. VII.6.1)} \\
= {}& r_1[x_1\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!)] \rightarrowtriangle r_2[x_2\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!)] : \{\ell_i \,.\, G_i\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!)\}_{i\in I} \\
& && \text{(Fig. VII.6.1)} \\
= {}& r_1[x_1\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!)] \rightarrowtriangle r_2[x_2\,(\!(R[\phi])\!)\,(\!(R'[\phi'])\!)] : && \text{(A1} \Rightarrow \text{Induction)} \\
& \quad \{\ell_i \,.\, G_i\,(\!(R'[\phi'])\!)\,(\!(R[\phi])\!)\}_{i\in I} \\
= {}& r_1[x_1\,(\!(R'[\phi'])\!)\,(\!(R[\phi])\!)] \rightarrowtriangle r_2[x_2\,(\!(R'[\phi'])\!)\,(\!(R[\phi])\!)] : && \text{(A1} \Rightarrow \text{Thm. VII.6.5:1)} \\
& \quad \{\ell_i \,.\, G_i\,(\!(R'[\phi'])\!)\,(\!(R[\phi])\!)\}_{i\in I} \\
= {}& r_1[x_1\,(\!(R'[\phi'])\!)] \rightarrowtriangle r_2[x_2\,(\!(R'[\phi'])\!)] : \{\ell_i \,.\, G_i\,(\!(R'[\phi'])\!)\}_{i\in I}\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
= {}& r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, G_i\}_{i\in I}\,(\!(R'[\phi'])\!)\,(\!(R[\phi])\!) && \text{(Fig. VII.6.1)} \\
= {}& T\,(\!(R'[\phi'])\!)\,(\!(R[\phi])\!) && \text{(Step)}
\end{aligned}$$

- **Step.** $T = r_2[x_2]\,!\,\{\ell_i \,.\, L_i\}_{i\in I}$

Conclude:

$$\begin{aligned}
& T \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis \\
={}& r_2[x_2]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, L_i\}_{i\in I} \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis && \text{(Step)}\\
={}& r_2[x_2 \llparenthesis R[\phi] \rrparenthesis]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R[\phi] \rrparenthesis\}_{i\in I} \llparenthesis R'[\phi'] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& r_2[x_2 \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis\}_{i\in I} && \text{(Fig. VII.6.1)}\\
={}& r_2[x_2 \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis\}_{i\in I} && \text{(A1} \Rightarrow \text{Induction)}\\
={}& r_2[x_2 \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis\}_{i\in I} && \text{(A1} \Rightarrow \text{Thm. VII.6.5:1)}\\
={}& r_2[x_2 \llparenthesis R'[\phi'] \rrparenthesis]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R'[\phi'] \rrparenthesis\}_{i\in I} \llparenthesis R[\phi] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& r_2[x_2]\,\mathbf{!}\{\ell_i \,\mathbf{.}\, L_i\}_{i\in I} \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& T \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis && \text{(Step)}
\end{aligned}$$

- **Step.** $T = r_1[x_1]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, L_i\}_{i\in I}$

  Conclude:

$$\begin{aligned}
& T \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis \\
={}& r_1[x_1]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, L_i\}_{i\in I} \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis && \text{(Step)}\\
={}& r_1[x_1 \llparenthesis R[\phi] \rrparenthesis]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R[\phi] \rrparenthesis\}_{i\in I} \llparenthesis R'[\phi'] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& r_1[x_1 \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis\}_{i\in I} && \text{(Fig. VII.6.1)}\\
={}& r_1[x_1 \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis\}_{i\in I} && \text{(A1} \Rightarrow \text{Induction)}\\
={}& r_1[x_1 \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis\}_{i\in I} && \text{(A1} \Rightarrow \text{Thm. VII.6.5:1)}\\
={}& r_1[x_1 \llparenthesis R'[\phi'] \rrparenthesis]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, L_i \llparenthesis R'[\phi'] \rrparenthesis\}_{i\in I} \llparenthesis R[\phi] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& r_1[x_1]\,\mathbf{?}\{\ell_i \,\mathbf{.}\, L_i\}_{i\in I} \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& T \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis && \text{(Step)}
\end{aligned}$$

- **Step.** $T = \texttt{rec}\ X\ T_X$

  Conclude:

$$\begin{aligned}
& T \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis \\
={}& \texttt{rec}\ X\ T_X \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis && \text{(Step)}\\
={}& \texttt{rec}\ X\ (T_X \llparenthesis R[\phi] \rrparenthesis) \llparenthesis R'[\phi'] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& \texttt{rec}\ X\ (T_X \llparenthesis R[\phi] \rrparenthesis \llparenthesis R'[\phi'] \rrparenthesis) && \text{(Fig. VII.6.1)}\\
={}& \texttt{rec}\ X\ (T_X \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis) && \text{(A1} \Rightarrow \text{Induction)}\\
={}& \texttt{rec}\ X\ (T_X \llparenthesis R'[\phi'] \rrparenthesis) \llparenthesis R[\phi] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& \texttt{rec}\ X\ T_X \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis && \text{(Fig. VII.6.1)}\\
={}& T \llparenthesis R'[\phi'] \rrparenthesis \llparenthesis R[\phi] \rrparenthesis && \text{(Step)}
\end{aligned}$$

QED.

VIII.27 Proof of Theorem VII.6.6

- **A1.** $\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto \operatorname{dom}\phi \mid \tilde{r}\in R\},\{\texttt{cont}\}}(G)$

- **A2.** $(\operatorname{expr} G) \cap \mathbb{G}_{\texttt{rec}} = \emptyset$
- **A3.** $r \in R$
- **A4.** $a \notin \operatorname{img} \phi$

By induction on A1 (Fig. VII.4.2):

- **Base.** $G = X$ **and** $X \in \{\texttt{cont}\}$
  - **B1.** Conclude:

$$\begin{array}{llr} & X \in \{\texttt{cont}\} & \text{(Base)} \\ \textbf{impl.} & X = \texttt{cont} & (-) \end{array}$$

  - **B2.** Conclude:

$$\begin{array}{llr} & \texttt{cont} & \\ = & \texttt{cont} \restriction r[a] & \text{(Fig. VII.5.2)} \\ = & X \restriction r[a] & \text{(B1)} \\ = & G \restriction r[a] & \text{(Base)} \end{array}$$

  - **B3.** Conclude:

$$\begin{array}{llr} & \texttt{cont} & \\ = & \texttt{cont} \restriction r[a] & \text{(Fig. VII.5.2)} \\ = & \texttt{cont}\,(\!(R[\phi])\!) \restriction r[a] & \text{(Fig. VII.6.1)} \\ = & X\,(\!(R[\phi])\!) \restriction r[a] & \text{(B1)} \\ = & G\,(\!(R[\phi])\!) \restriction r[a] & \text{(Base)} \end{array}$$

  Conclude:

$$\texttt{cont} = G \restriction r[a] \;\textbf{and}\; \texttt{cont} = G\,(\!(R[\phi])\!) \restriction r[a] \qquad \text{(B2, B3)}$$

- **Step.** $G = r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I}$ **and**
  $\Big[r_1 \in \operatorname{dom}(f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})$ **impl.** $x_1 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r_1)\Big]$ **and**
  $\Big[r_2 \in \operatorname{dom}(f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})$ **impl.** $x_2 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r_2)\Big]$ **and**
  $\Big[\mathsf{Wf}_{f,\{\texttt{cont}\}}(G_i)$ **for-all** $i \in I\Big]$
  - **C1.** Conclude:

$$\begin{array}{llr} & (\operatorname{expr} G) \cap \mathbb{G}_{\texttt{rec}} = \emptyset & \text{(A2)} \\ \textbf{impl.} & (\operatorname{expr} r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, G_i\}_{i \in I}) \cap \mathbb{G}_{\texttt{rec}} = \emptyset & \text{(Step)} \\ \textbf{impl.} & (\operatorname{expr} G_i) \cap \mathbb{G}_{\texttt{rec}} = \emptyset \;\textbf{for-all}\; i \in I & (-) \end{array}$$

- **C2.** Conclude:

$r = r_1$

impl. $r = r_1$ **and** (Step)

$\Big[r_1 \in \operatorname{dom}(f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})$ **impl.** $x_1 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)\Big]$

impl. $r \in \operatorname{dom}(f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})$ **impl.** (=)

$x_1 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$

impl. $r \in \operatorname{dom}\{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\}$ **impl.** $x_1 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$ (–)

impl. $r \in \{\tilde{r} \mid \tilde{r} \in R\}$ **impl.** $x_1 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$ (–)

impl. $r \in R$ **impl.** $x_1 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$ (–)

impl. $x_1 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$ (A3)

impl. $x_1 \in \operatorname{dom}\phi$ (A3)

impl. $x_1 \in \mathbb{Z}$ (–)

- **C3.** Conclude:

$r[a] = r_1[x_1]$

impl. $r = r_1$ **and** $a = x_1$ (–)

impl. $x_1 \in \mathbb{Z}$ **and** $a = x_1$ (C2)

impl. $a \in \mathbb{Z}$ (=)

impl. **false** ($\mathbb{A} \cap \mathbb{Z} = \emptyset$)

- **C4.** Conclude:

$r = r_2$

impl. $r = r_2$ **and** (Step)

$\Big[r_2 \in \operatorname{dom}(f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})$ **impl.** $x_2 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)\Big]$

impl. $r \in \operatorname{dom}(f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})$ **impl.** (=)

$x_2 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$

impl. $r \in \operatorname{dom}\{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\}$ **impl.** $x_2 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$ (–)

impl. $r \in \{\tilde{r} \mid \tilde{r} \in R\}$ **impl.** $x_2 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$ (–)

impl. $r \in R$ **impl.** $x_2 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$ (–)

impl. $x_2 \in (f \cup \{\tilde{r} \mapsto \operatorname{dom}\phi \mid \tilde{r} \in R\})(r)$ (A3)

impl. $x_2 \in \operatorname{dom}\phi$ (A3)

impl. $x_2 \in \mathbb{Z}$ (–)

- **C5.** Conclude:

$r[a] = r_2[x_2]$

impl. $r = r_2$ **and** $a = x_2$ (–)

impl. $x_2 \in \mathbb{Z}$ **and** $a = x_2$ (C4)

impl. $a \in \mathbb{Z}$ (=)

impl. **false** ($\mathbb{A} \cap \mathbb{Z} = \emptyset$)

- **C6.** Conclude:

$$\begin{array}{lll}
 & \mathtt{cont} & \\
= & \bigsqcap\{\mathtt{cont} \mid i \in I\} & \text{(Lem. VII.5.1:2)} \\
= & \bigsqcap\{G_i \upharpoonright r[a] \mid i \in I\} & \text{(Step, C1, A3, A4} \Rightarrow \text{Induction)} \\
= & r_1[x_1] \rightarrowtriangle r_2[x_2] \,\boldsymbol{:}\, \{\ell_i \,\boldsymbol{.}\, G_i\}_{i \in I} \upharpoonright r[a] & \text{(C3, C5} \Rightarrow \text{Fig. VII.5.2)} \\
= & G \upharpoonright r[a] & \text{(Step)}
\end{array}$$

- **C7.** Conclude:

$$\begin{array}{lll}
 & a = \phi(x) & (\exists x) \\
\textsf{impl.} & a \in \operatorname{img} \phi & (-) \\
\textsf{impl.} & \textsf{false} & \text{(A4)}
\end{array}$$

- **C8.** Conclude:

$$\begin{array}{lll}
 & r[a] = r_1[x_1] \,\llparenthesis R[\phi] \rrparenthesis & \\
\textsf{impl.} & a = \phi(x_1) \;\textsf{ or }\; r[a] = r_1[x_1] & \text{(Fig. VII.6.1)} \\
\textsf{impl.} & \textsf{false} & \text{(C7, C3)}
\end{array}$$

- **C9.** Conclude:

$$\begin{array}{lll}
 & r[a] = r_2[x_2] \,\llparenthesis R[\phi] \rrparenthesis & \\
\textsf{impl.} & a = \phi(x_2) \;\textsf{ or }\; r[a] = r_2[x_2] & \text{(Fig. VII.6.1)} \\
\textsf{impl.} & \textsf{false} & \text{(C7, C5)}
\end{array}$$

- **C10.** Conclude:

$$\begin{array}{lll}
 & \mathtt{cont} & \\
= & \bigsqcap\{\mathtt{cont} \mid i \in I\} & \text{(Lem. VII.5.1:2)} \\
= & \bigsqcap\{G_i \,\llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] \mid i \in I\} & \text{(Step, C1, A3, A4} \Rightarrow \text{Induction)} \\
= & r_1[x_1] \,\llparenthesis R[\phi] \rrparenthesis \rightarrowtriangle r_2[x_2] \,\llparenthesis R[\phi] \rrparenthesis \,\boldsymbol{:}\, \{\ell_i \,\boldsymbol{.}\, G_i \,\llparenthesis R[\phi] \rrparenthesis\}_{i \in I} \upharpoonright r[a] & \text{(C8, C9} \Rightarrow \text{Fig. VII.5.2)} \\
= & r_1[x_1] \rightarrowtriangle r_2[x_2] \,\boldsymbol{:}\, \{\ell_i \,\boldsymbol{.}\, G_i\}_{i \in I} \,\llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] & \text{(Fig. VII.6.1)} \\
= & G \,\llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] & \text{(Step)}
\end{array}$$

Conclude:

$$\mathtt{cont} = G \upharpoonright r[a] \;\textsf{ and }\; \mathtt{cont} = G \,\llparenthesis R[\phi] \rrparenthesis \upharpoonright r[a] \qquad \text{(C6, C10)}$$

- **Step.** $G = \mathtt{rec}\ X\ G_X$ **and** $\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \operatorname{dom} \phi \mid \tilde{r} \in R\}, \{\mathtt{cont}\} \cup \{X\}}(G_X)$

  Conclude:

$$\begin{array}{lll}
 & (\operatorname{expr} G) \cap \mathbb{G}_{\mathtt{rec}} = \emptyset & \text{(A2)} \\
\textsf{impl.} & (\operatorname{expr} \mathtt{rec}\ X\ G_X) \cap \mathbb{G}_{\mathtt{rec}} = \emptyset & \text{(Step)} \\
\textsf{impl.} & (\{\mathtt{rec}\ X\ G_X\} \cup (\operatorname{expr} G_X)) \cap \mathbb{G}_{\mathtt{rec}} = \emptyset & (-) \\
\textsf{impl.} & \{\mathtt{rec}\ X\ G_X\} \cap \mathbb{G}_{\mathtt{rec}} = \emptyset & (-) \\
\textsf{impl.} & \mathtt{rec}\ X\ G_X \notin \mathbb{G}_{\mathtt{rec}} & (-) \\
\textsf{impl.} & \mathtt{rec}\ X\ G_X \notin \{\mathtt{rec}\ \tilde{X}\ \tilde{G} \mid \tilde{X} \in \mathbb{X} \;\textsf{ and }\; \tilde{G} \in \mathbb{G}\} & (\mathbb{G}_{\mathtt{rec}}) \\
\textsf{impl.} & \textsf{false} & (-)
\end{array}$$

QED.

VIII.28 Proof of Theorem VII.6.7

- **A1.** $\langle \Phi, z[a] \rangle \in \mathrm{dom}\,\mathsf{to}$
- **A2.** $\langle \Phi, z[a] \rangle \in \mathrm{dom}\,\mathsf{from}$

By induction on A1 (Fig. VII.2.6):

- **Base.** $\Phi\,\mathsf{to}\,z[a] = \{\tilde{z} \mapsto \emptyset \mid \tilde{z} \in \mathrm{dom}\,\Phi\}$ **and**
  $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a = (\mathsf{head}\,\Phi)(z)$

  - **B1.** Conclude:

$$\begin{array}{lll} & |\emptyset| = \mathsf{0} \ \textbf{for-all}\ \tilde{z} \in \mathrm{dom}\,\Phi & (-) \\ \textbf{impl.} & |\{\tilde{\tilde{z}} \mapsto \emptyset \mid \tilde{\tilde{z}} \in \mathrm{dom}\,\Phi\}(\tilde{z})| = \mathsf{0} \ \textbf{for-all}\ \tilde{z} \in \mathrm{dom}\,\Phi & (-) \\ \textbf{impl.} & \mathsf{len}\,\{\tilde{\tilde{z}} \mapsto \emptyset \mid \tilde{\tilde{z}} \in \mathrm{dom}\,\Phi\} = \mathsf{0} & \text{(Fig. VII.2.5)} \\ \textbf{impl.} & \mathsf{len}\,(\Phi\,\mathsf{to}\,z[a]) = \mathsf{0} & \text{(Base)} \end{array}$$

  Conclude:

$$\begin{array}{lll} & \mathsf{iter}(T, \texttt{cont}, R, \Phi\,\mathsf{to}\,z[a])\,\{\mathsf{iter}(T, \texttt{cont}, R, \Phi\,\mathsf{from}\,z[a])/\texttt{cont}\} & \\ = & \texttt{cont}\,\{\mathsf{iter}(T, \texttt{cont}, R, \Phi\,\mathsf{from}\,z[a])/\texttt{cont}\} & \text{(B1} \Rightarrow \text{A2, Fig. VII.6.2)} \\ = & \mathsf{iter}(T, \texttt{cont}, R, \Phi\,\mathsf{from}\,z[a]) & \text{(Fig. VII.4.3)} \\ = & \mathsf{iter}(T, \texttt{cont}, R, \Phi) & \text{(Base)} \end{array}$$

- **Step.** $\Phi\,\mathsf{to}\,z[a] = (\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])$ **and**
  $\Phi \in \mathrm{dom}\,\mathsf{len}$ **and** $a \in \Phi(z)$ **and** $a \neq (\mathsf{head}\,\Phi)(z)$

  - **C1.** Conclude:

$$\begin{array}{lll} & \mathsf{len}\,(\Phi\,\mathsf{to}\,z[a]) = \mathsf{0} & \\ \textbf{impl.} & |(\Phi\,\mathsf{to}\,z[a])(\tilde{z})| = \mathsf{0} \ \textbf{for-all}\ \tilde{z} \in \mathrm{dom}\,(\Phi\,\mathsf{to}\,z[a]) & \text{(Fig. VII.2.5)} \\ \textbf{impl.} & (\Phi\,\mathsf{to}\,z[a])(\tilde{z}) = \emptyset \ \textbf{for-all}\ \tilde{z} \in \mathrm{dom}\,(\Phi\,\mathsf{to}\,z[a]) & (-) \\ \textbf{impl.} & ((\mathsf{head}\,\Phi)\cdot((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a]))(\tilde{z}) = \emptyset \ \textbf{for-all}\ \tilde{z} \in \mathrm{dom}\,(\Phi\,\mathsf{to}\,z[a]) & \text{(Step)} \\ \textbf{impl.} & \{(\mathsf{head}\,\Phi)(\tilde{z})\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z}) = \emptyset \ \textbf{for-all}\ \tilde{z} \in \mathrm{dom}\,(\Phi\,\mathsf{to}\,z[a]) & \\ & & \text{(Lem. VII.2.10:3)} \\ \textbf{impl.} & \{(\mathsf{head}\,\Phi)(\tilde{z})\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(\tilde{z}) = \emptyset \ \textbf{for-all}\ \tilde{z} \in \mathrm{dom}\,(\Phi\,\mathsf{to}\,z[a]) & \\ & & \text{(Lem. VII.2.11:2)} \\ \textbf{impl.} & \{(\mathsf{head}\,\Phi)(z)\} \cup ((\mathsf{tail}\,\Phi)\,\mathsf{to}\,z[a])(z) = \emptyset & \text{(Step)} \\ \textbf{impl.} & \{(\mathsf{head}\,\Phi)(z)\} = \emptyset & \text{(Step)} \\ \textbf{impl.} & \textbf{false} & (-) \end{array}$$

  - **C2.** Conclude:

$$\begin{array}{lll} & \Phi\,\mathsf{to}\,z[a] \in \mathrm{dom}\,\mathsf{len} & \text{(A1} \Rightarrow \text{Thm. VII.2.6:3)} \\ \textbf{impl.} & \mathsf{len}\,(\Phi\,\mathsf{to}\,z[a]) = \mathsf{0} \ \textbf{or}\ \mathsf{len}\,(\Phi\,\mathsf{to}\,z[a]) > \mathsf{0} & \text{(Lem. VII.2.9:1)} \\ \textbf{impl.} & \mathsf{len}\,(\Phi\,\mathsf{to}\,z[a]) > \mathsf{0} & \text{(C1)} \end{array}$$

- **C3.** Conclude:

  $$\mathsf{len}\,\Phi > \mathsf{o} \qquad \text{(Step} \Rightarrow \text{Lem. VII.2.9:2)}$$

Conclude:

$$\begin{aligned}
& \mathsf{iter}(T, \mathbf{cont}, R, \Phi\ \mathsf{to}\ z[a])\ \{\mathsf{iter}(T, \mathbf{cont}, R, \Phi\ \mathsf{from}\ z[a])/\mathbf{cont}\} \\
= {} & T\ \llparenthesis R[\mathsf{head}\ (\Phi\ \mathsf{to}\ z[a])]\rrparenthesis\ \{\mathsf{iter}(T, \mathbf{cont}, R, \mathsf{tail}\ (\Phi\ \mathsf{to}\ z[a]))/\mathbf{cont}\} && \text{(C2} \Rightarrow \text{A2, Fig. VII.6.2)} \\
& \quad \{\mathsf{iter}(T, \mathbf{cont}, R, \Phi\ \mathsf{from}\ z[a])/\mathbf{cont}\} \\
= {} & T\ \llparenthesis R[\mathsf{head}\ (\Phi\ \mathsf{to}\ z[a])]\rrparenthesis\ \{\mathsf{iter}(T, \mathbf{cont}, R, (\mathsf{tail}\ \Phi)\ \mathsf{to}\ z[a])/\mathbf{cont}\} \\
& && \text{(A1, Step} \Rightarrow \text{Thm. VII.2.6:2)} \\
& \quad \{\mathsf{iter}(T, \mathbf{cont}, R, \Phi\ \mathsf{from}\ z[a])/\mathbf{cont}\} \\
= {} & T\ \llparenthesis R[\mathsf{head}\ (\Phi\ \mathsf{to}\ z[a])]\rrparenthesis\ \{\mathsf{iter}(T, \mathbf{cont}, R, (\mathsf{tail}\ \Phi)\ \mathsf{to}\ z[a])/\mathbf{cont}\} && \text{(Step} \Rightarrow \text{Fig. VII.2.6)} \\
& \quad \{\mathsf{iter}(T, \mathbf{cont}, R, (\mathsf{tail}\ \Phi)\ \mathsf{from}\ z[a])/\mathbf{cont}\} \\
= {} & T\ \llparenthesis R[\mathsf{head}\ (\Phi\ \mathsf{to}\ z[a])]\rrparenthesis && \text{(Lem. VII.4.2:3)} \\
& \quad \{\mathsf{iter}(T, \mathbf{cont}, R, (\mathsf{tail}\ \Phi)\ \mathsf{to}\ z[a])\ \{\mathsf{iter}(T, \mathbf{cont}, R, (\mathsf{tail}\ \Phi)\ \mathsf{from}\ z[a])/\mathbf{cont}\}/\mathbf{cont}\} \\
= {} & T\ \llparenthesis R[\mathsf{head}\ (\Phi\ \mathsf{to}\ z[a])]\rrparenthesis\ \{\mathsf{iter}(T, \mathbf{cont}, R, \mathsf{tail}\ \Phi)/\mathbf{cont}\} && \text{(Induction)} \\
= {} & T\ \llparenthesis R[\mathsf{head}\ \Phi]\rrparenthesis\ \{\mathsf{iter}(T, \mathbf{cont}, R, \mathsf{tail}\ \Phi)/\mathbf{cont}\} && \text{(Step} \Rightarrow \text{Thm. VII.2.6:1)} \\
= {} & \mathsf{iter}(T, \mathbf{cont}, R, \Phi) && \text{(C3} \Rightarrow \text{Fig. VII.6.2)}
\end{aligned}$$

QED.

VIII.29 Proof of Theorem VII.6.8

Proof of (1)

- **A1.** $\Phi \in \mathrm{dom}\,\mathsf{len}$
- **A2.** $\mathsf{Wf}_{f,\mathcal{X}}(T_1)$
- **A3.** $\mathsf{Wf}_{f,\mathcal{X}}(T_2)$

By induction on A1 (Fig. VII.2.5):

- **Base.** $\mathsf{len}\,\Phi = \mathsf{o}$

  Conclude:

  $$\begin{aligned}
  & \mathsf{Wf}_{f,\mathcal{X}}(T_2) && \text{(A3)} \\
  \textbf{impl.}\ & \mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(T_1, T_2, R, \Phi)) && \text{(Base} \Rightarrow \text{Fig. VII.6.2)}
  \end{aligned}$$

- **Step.** $\mathsf{len}\,\Phi > \mathsf{o}$

  - **B1.** Conclude:

    $$\begin{aligned}
    & \mathsf{Wf}_{f,\mathcal{X}}(T_1) && \text{(A2)} \\
    \textbf{impl.}\ & \mathsf{Wf}_{f,\mathcal{X}}(T_1\ \llparenthesis R[\mathsf{head}\ \Phi]\rrparenthesis) && \text{(Thm. VII.6.1)}
    \end{aligned}$$

- **B2.** Conclude:

  $$\mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi \qquad \text{(Step} \Rightarrow \text{Thm. VII.2.5)}$$

- **B3.** Conclude:

  $$\mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)) \qquad \text{(A2, A3, B2} \Rightarrow \text{Induction)}$$

Conclude:

$$\begin{aligned} & \mathsf{Wf}_{f,\mathcal{X}}(T_1\ \llparenthesis R[\mathsf{head}\,\Phi]\rrparenthesis\ \{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)/\texttt{\textbf{cont}}\}) && \text{(B1, B3} \Rightarrow \text{Thm. VII.4.1:1)} \\ \textbf{impl.}\ & \mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(T_1, T_2, R, \Phi)) && \text{(Step} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

QED.

Proof of (2)

- **A1.** $\Phi \in \mathrm{dom}\,\mathsf{len}$
- **A2.** $\mathsf{Wf}_{f,\{\texttt{\textbf{cont}}\}}(T_1)$
- **A3.** $\mathsf{Wf}_{f,\mathcal{X}}(T_2)$

By induction on A1 (Fig. VII.2.5):

- **Base.** $\mathsf{len}\,\Phi = \mathsf{0}$

  Conclude:

  $$\begin{aligned} & \mathsf{Wf}_{f,\mathcal{X}}(T_2) && \text{(A3)} \\ \textbf{impl.}\ & \mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(T_1, T_2, R, \Phi)) && \text{(Base} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

- **Step.** $\mathsf{len}\,\Phi > \mathsf{0}$

  - **B1.** Conclude:

    $$\begin{aligned} & \mathsf{Wf}_{f,\{\texttt{\textbf{cont}}\}}(T_1\ \llparenthesis R[\mathsf{head}\,\Phi]\rrparenthesis) && \text{(A2} \Rightarrow \text{Thm. VII.6.1)} \\ \textbf{impl.}\ & \mathsf{Wf}_{f,\mathcal{X}\cup\{\texttt{\textbf{cont}}\}}(T_1\ \llparenthesis R[\mathsf{head}\,\Phi]\rrparenthesis) && \text{(Lem. VII.4.1:2)} \end{aligned}$$

  - **B2.** Conclude:

    $$\mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi \qquad \text{(Step} \Rightarrow \text{Thm. VII.2.5)}$$

  - **B3.** Conclude:

    $$\mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)) \qquad \text{(A2, A3, B2} \Rightarrow \text{Induction)}$$

  Conclude:

  $$\begin{aligned} & \mathsf{Wf}_{f,\mathcal{X}}(T_1\ \llparenthesis R[\mathsf{head}\,\Phi]\rrparenthesis\ \{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)/\texttt{\textbf{cont}}\}) && \text{(B2, B3} \Rightarrow \text{Thm. VII.4.1:2)} \\ \textbf{impl.}\ & \mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(T_1, T_2, R, \Phi)) && \text{(Step} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

QED.

VIII.30 Proof of Theorem VII.6.9

Assume:

- **A1.** $\Phi \in \operatorname{dom} \mathsf{len}$
- **A2.** $\mathsf{Wf}_{f,\{\mathbf{cont}\}}(T_1)$

By induction on A1 (Fig. VII.2.5).

- **Base.** $\mathsf{len}\,\Phi = 0$

  Conclude:

$$\begin{aligned} & \mathsf{iter}(T_1, T_2, R, \Phi)\,\{T_Y/Y\} & \\ = \;& T_2\,\{T_Y/Y\} & \text{(Base} \Rightarrow \text{Fig. VII.6.2)} \\ = \;& \mathsf{iter}(T_1, T_2\,\{T_Y/Y\}, R, \Phi) & \text{(Base} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

- **Step.** $\mathsf{len}\,\Phi > 0$

  By case distinction:

  - **Case.** $Y = \mathbf{cont}$
    - **B1.** Conclude:

$$\begin{aligned} & \mathsf{len}\,\Phi > 0 & \text{(Step)} \\ \textbf{impl.}\;& \mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi & \text{(Thm. VII.2.5)} \end{aligned}$$

    Conclude:

$$\begin{aligned} & \mathsf{iter}(T_1, T_2, R, \Phi)\,\{T_Y/Y\} & \\ = \;& T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)/\mathbf{cont}\}\,\{T_Y/Y\} & \text{(Step} \Rightarrow \text{Fig. VII.6.2)} \\ = \;& T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)\,\{T_Y/Y\}/\mathbf{cont}\} & \text{(Case} \Rightarrow \text{Lem. VII.4.2:3)} \\ = \;& T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(T_1, T_2\,\{T_Y/Y\}, R, \mathsf{tail}\,\Phi)/\mathbf{cont}\} & \text{(B1, A2} \Rightarrow \text{Induction)} \\ = \;& \mathsf{iter}(T_1, T_2\,\{T_Y/Y\}, R, \Phi) & \text{(Step} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

  - **Case.** $Y \neq \mathbf{cont}$
    - **C1.** Conclude:

$$\begin{aligned} & \mathsf{len}\,\Phi > 0 & \text{(Step)} \\ \textbf{impl.}\;& \Phi \in \operatorname{dom} \mathsf{head} \;\textbf{ and }\; \mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi & \text{(Thm. VII.2.5)} \end{aligned}$$

    - **C2.** Conclude:

$$\begin{aligned} & \mathsf{Wf}_{f,\{\mathbf{cont}\}}(T_1) & \text{(A2)} \\ \textbf{impl.}\;& \mathsf{Wf}_{f,\{\mathbf{cont}\}\setminus\{Y\}}(T_1) & \text{(Case)} \\ \textbf{impl.}\;& \mathsf{Wf}_{f,\{\mathbf{cont}\}\setminus\{Y\}}(T_1\,(\!(R[\mathsf{head}\,\Phi])\!)) & \text{(C1, Thm. VII.6.1)} \end{aligned}$$

Conclude:

$$
\begin{aligned}
&\mathsf{iter}(T_1, T_2, R, \Phi)\,\{T_Y/Y\} \\
={}& T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)/\texttt{\textbf{cont}}\}\,\{T_Y/Y\} && \text{(Step} \Rightarrow \text{Fig. VII.6.2)} \\
={}& T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{T_Y/Y\}\,\{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)\,\{T_Y/Y\}/\texttt{\textbf{cont}}\} \\
& && \text{(Case} \Rightarrow \text{Lem. VII.4.2:4)} \\
={}& T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{T_Y/Y\} && \text{(C1, A2} \Rightarrow \text{Induction)} \\
&\quad \{\mathsf{iter}(T_1, T_2\,\{T_Y/Y\}, R, \mathsf{tail}\,\Phi)/\texttt{\textbf{cont}}\} \\
={}& T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(T_1, T_2\,\{T_Y/Y\}, R, \mathsf{tail}\,\Phi)/\texttt{\textbf{cont}}\} && \text{(C2} \Rightarrow \text{Thm. VII.4.2)} \\
={}& \mathsf{iter}(T_1, T_2\,\{T_Y/Y\}, R, \Phi) && \text{(Step} \Rightarrow \text{Fig. VII.6.2)}
\end{aligned}
$$

QED.

VIII.31 Proof of Theorem VII.6.10

Proof of (1)

- **B1.** Conclude:

$$
\begin{aligned}
&\mathsf{iter}(\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}}, \mathbf{end}, \{\texttt{M}\}, \{\texttt{i} \mapsto \{\mathsf{5}, \mathsf{6}\}\}) \\
={}& (\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}})\,(\!(\{\texttt{M}\}[\mathsf{head}\,\{\texttt{i} \mapsto \{\mathsf{5}, \mathsf{6}\}\}])\!) && \text{(Fig. VII.6.2)} \\
&\quad \{\mathsf{iter}(\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}}, \mathbf{end}, \{\texttt{M}\}, \mathsf{tail}\,\{\texttt{i} \mapsto \{\mathsf{5}, \mathsf{6}\}\})/\texttt{\textbf{cont}}\} \\
={}& (\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}})\,(\!(\{\texttt{M}\}[\{\texttt{i} \mapsto \mathsf{head}\,\{\mathsf{5}, \mathsf{6}\}\}])\!) && \text{(Fig. VII.2.5)} \\
&\quad \{\mathsf{iter}(\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}}, \mathbf{end}, \{\texttt{M}\}, \{\texttt{i} \mapsto \mathsf{tail}\,\{\mathsf{5}, \mathsf{6}\}\})/\texttt{\textbf{cont}}\} \\
={}& (\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}})\,(\!(\{\texttt{M}\}[\{\texttt{i} \mapsto \mathsf{5}\}])\!) && \text{(Fig. VII.2.2)} \\
&\quad \{\mathsf{iter}(\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}}, \mathbf{end}, \{\texttt{M}\}, \{\texttt{i} \mapsto \{\mathsf{6}\}\})/\texttt{\textbf{cont}}\} \\
={}& (\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}}\,(\!(\{\texttt{M}\}[\{\texttt{i} \mapsto \mathsf{5}\}])\!) \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}}\,(\!(\{\texttt{M}\}[\{\texttt{i} \mapsto \mathsf{5}\}])\!)) \\
& && \text{(Thm. VII.6.3)} \\
&\quad \{\mathsf{iter}(\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}}, \mathbf{end}, \{\texttt{M}\}, \{\texttt{i} \mapsto \{\mathsf{6}\}\})/\texttt{\textbf{cont}}\} \\
={}& (\texttt{M}[\mathsf{5}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\mathsf{5}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}}) && \text{(Fig. VII.6.1)} \\
&\quad \{\mathsf{iter}(\texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{foo(int)}\,\mathbf{.}\,\texttt{\textbf{cont}} \sqcap \texttt{M}[\texttt{i}]\,\mathbf{?}\,\texttt{bar()}\,\mathbf{.}\,\texttt{\textbf{cont}}, \mathbf{end}, \{\texttt{M}\}, \{\texttt{i} \mapsto \{\mathsf{6}\}\})/\texttt{\textbf{cont}}\}
\end{aligned}
$$

- **B2.** Conclude:

$$\begin{aligned}
&\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{\mathtt{6}\}\}) \\
= \;& (\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont})\,(\!(\{\mathtt{M}\}[\mathsf{head}\,\{\mathtt{i} \mapsto \{\mathtt{6}\}\}])\!) && \text{(Fig. VII.6.2)} \\
& \quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \mathsf{tail}\,\{\mathtt{i} \mapsto \{\mathtt{6}\}\})/\mathbf{cont}\} \\
= \;& (\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont})\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathsf{head}\,\{\mathtt{6}\}\}])\!) && \text{(Fig. VII.2.5)} \\
& \quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \mathsf{tail}\,\{\mathtt{6}\}\})/\mathbf{cont}\} \\
= \;& (\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont})\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathtt{6}\}])\!) && \text{(Fig. VII.2.2)} \\
& \quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \emptyset\})/\mathbf{cont}\} \\
= \;& (\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathtt{6}\}])\!) \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathtt{6}\}])\!)) \\
& && \text{(Thm. VII.6.3)} \\
& \quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \emptyset\})/\mathbf{cont}\} \\
= \;& (\mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}) && \text{(Fig. VII.6.1)} \\
& \quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \emptyset\})/\mathbf{cont}\} \\
= \;& (\mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont})\,\{\mathbf{cont}/\mathbf{cont}\} && \text{(Fig. VII.6.2)} \\
= \;& \mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,\{\mathbf{cont}/\mathbf{cont}\} \sqcap \mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}\,\{\mathbf{cont}/\mathbf{cont}\} && \text{(Thm. VII.5.1:1)} \\
= \;& \mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont} && \text{(Fig. VII.4.3)}
\end{aligned}$$

- **B3.** Conclude:

$$\begin{aligned}
&\mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \\
= \;& \mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,\{\mathbf{cont}/\mathbf{cont}\} && \text{(Fig. VII.4.3)} \\
= \;& \mathtt{M}[\mathtt{6}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,\{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \emptyset\})/\mathbf{cont}\} \\
& && \text{(Fig. VII.6.2)} \\
= \;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathtt{6}\}])\!) && \text{(Fig. VII.6.1)} \\
& \quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \emptyset\})/\mathbf{cont}\} \\
= \;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathsf{head}\,\{\mathtt{6}\}\}])\!) && \text{(Fig. VII.2.2)} \\
& \quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \mathsf{tail}\,\{\mathtt{6}\}\})/\mathbf{cont}\} \\
= \;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,(\!(\{\mathtt{M}\}[\mathsf{head}\,\{\mathtt{i} \mapsto \{\mathtt{6}\}\}])\!) && \text{(Fig. VII.2.5)} \\
& \quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \mathsf{tail}\,\{\mathtt{i} \mapsto \{\mathtt{6}\}\})/\mathbf{cont}\} \\
= \;& \mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{\mathtt{6}\}\}) && \text{(Fig. VII.6.2)}
\end{aligned}$$

- **B4.** Conclude:

$$\begin{aligned}
&\mathtt{M}[6]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont} \\
=\;& \mathtt{M}[6]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,\{\mathbf{cont}/\mathbf{cont}\} && \text{(Fig. VII.4.3)} \\
=\;& \mathtt{M}[6]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,\{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \emptyset\})/\mathbf{cont}\} && \text{(Fig. VII.6.2)} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto 6\}])\!) && \text{(Fig. VII.6.1)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \emptyset\})/\mathbf{cont}\} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathsf{head}\,\{6\}\}])\!) && \text{(Fig. VII.2.2)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \mathsf{tail}\,\{6\}\})/\mathbf{cont}\} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\mathsf{head}\,\{\mathtt{i} \mapsto \{6\}\}])\!) && \text{(Fig. VII.2.5)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \mathsf{tail}\,\{\mathtt{i} \mapsto \{6\}\})/\mathbf{cont}\} \\
=\;& \mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{6\}\}) && \text{(Fig. VII.6.2)}
\end{aligned}$$

- **B5.** Conclude:

$$\begin{aligned}
&\mathtt{M}[5]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}\,\{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{6\}\})/\mathbf{cont}\} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto 5\}])\!) && \text{(Fig. VII.6.1)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{6\}\})/\mathbf{cont}\} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathsf{head}\,\{5, 6\}\}])\!) && \text{(Fig. VII.2.2)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \mathsf{tail}\,\{5, 6\}\})/\mathbf{cont}\} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\mathsf{head}\,\{\mathtt{i} \mapsto \{5, 6\}\}])\!) && \text{(Fig. VII.2.5)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \mathsf{tail}\,\{\mathtt{i} \mapsto \{5, 6\}\})/\mathbf{cont}\} \\
=\;& \mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{foo(int)}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{5, 6\}\}) && \text{(Fig. VII.6.2)}
\end{aligned}$$

- **B6.** Conclude:

$$\begin{aligned}
&\mathtt{M}[5]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,\{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{6\}\})/\mathbf{cont}\} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto 5\}])\!) && \text{(Fig. VII.6.1)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{6\}\})/\mathbf{cont}\} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\{\mathtt{i} \mapsto \mathsf{head}\,\{5, 6\}\}])\!) && \text{(Fig. VII.2.2)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \mathsf{tail}\,\{5, 6\}\})/\mathbf{cont}\} \\
=\;& \mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}\,(\!(\{\mathtt{M}\}[\mathsf{head}\,\{\mathtt{i} \mapsto \{5, 6\}\}])\!) && \text{(Fig. VII.2.5)} \\
&\quad \{\mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \mathsf{tail}\,\{\mathtt{i} \mapsto \{5, 6\}\})/\mathbf{cont}\} \\
=\;& \mathsf{iter}(\mathtt{M}[\mathtt{i}]\,\mathbf{?}\,\mathtt{bar()}\,\mathbf{.}\,\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{5, 6\}\}) && \text{(Fig. VII.6.2)}
\end{aligned}$$

Conclude:

$$
\begin{aligned}
& \mathsf{iter}(\mathtt{M[i]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M[i]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{\mathtt{5},\mathtt{6}\}\}) \\
={} & (\mathtt{M[5]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M[5]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}) && \text{(B1)} \\
& \quad \{\mathsf{iter}(\mathtt{M[i]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M[i]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{\mathtt{6}\}\}) / \mathbf{cont}\} \\
={} & (\mathtt{M[5]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M[5]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}) && \text{(B2)} \\
& \quad \{\mathtt{M[6]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} \sqcap \mathtt{M[6]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont} / \mathbf{cont}\} \\
\neq{} & \mathtt{M[5]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,\{\mathtt{M[6]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont} / \mathbf{cont}\} \sqcap && \text{(Proof of Thm. VII.5.1:3)} \\
& \mathtt{M[5]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}\,\{\mathtt{M[6]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont} / \mathbf{cont}\} \\
={} & \mathtt{M[5]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}\,\{\mathsf{iter}(\mathtt{M[i]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{\mathtt{6}\}\}) / \mathbf{cont}\} \sqcap && \text{(B3, B4)} \\
& \mathtt{M[5]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}\,\{\mathsf{iter}(\mathtt{M[i]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{\mathtt{6}\}\}) / \mathbf{cont}\} \\
={} & \mathsf{iter}(\mathtt{M[i]}\,\mathbf{?}\,\mathtt{foo(int)}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{\mathtt{5},\mathtt{6}\}\}) \sqcap && \text{(B5, B6)} \\
& \mathsf{iter}(\mathtt{M[i]}\,\mathbf{?}\,\mathtt{bar()}\;\mathbf{.}\;\mathbf{cont}, \mathbf{end}, \{\mathtt{M}\}, \{\mathtt{i} \mapsto \{\mathtt{5},\mathtt{6}\}\})
\end{aligned}
$$

QED.

Proof of (2)

- **A1.** $\langle L_1, L_2 \rangle \in \mathrm{dom}\,\sqcap$
- **A2.** $\Phi \in \mathrm{dom}\,\mathsf{len}$

By induction on A2 (Fig. VII.2.5):

- **Base.** $\mathsf{len}\,\Phi = 0$

  Conclude:

$$
\begin{aligned}
& \mathsf{iter}(L, L_1 \sqcap L_2, R, \Phi) \\
={} & L_1 \sqcap L_2 && \text{(Base} \Rightarrow \text{A1, Fig. VII.6.2)} \\
={} & \mathsf{iter}(L, L_1, R, \Phi) \sqcap \mathsf{iter}(L, L_2, R, \Phi) && \text{(Base} \Rightarrow \text{Fig. VII.6.2)}
\end{aligned}
$$

- **Step.** $\mathsf{len}\,\Phi > 0$

  - **B1.** Conclude:

$$
\begin{aligned}
& \mathsf{len}\,\Phi > 0 && \text{(Step)} \\
\textbf{impl.}\ & \mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi && \text{(Thm. VII.2.5)}
\end{aligned}
$$

  Conclude:

$$
\begin{aligned}
& \mathsf{iter}(L, L_1 \sqcap L_2, R, \Phi) \\
={} & L\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(L, L_1 \sqcap L_2, R, \mathsf{tail}\,\Phi) / \mathbf{cont}\} && \text{(Step} \Rightarrow \text{A1, Fig. VII.6.2)} \\
={} & L\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(L, L_1, R, \mathsf{tail}\,\Phi) \sqcap \mathsf{iter}(L, L_2, R, \mathsf{tail}\,\Phi) / \mathbf{cont}\} && \text{(B1} \Rightarrow \text{Induction)} \\
={} & L\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(L, L_1, R, \mathsf{tail}\,\Phi) / \mathbf{cont}\} \sqcap && \text{(Thm. VII.5.1:2)} \\
& L\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(L, L_2, R, \mathsf{tail}\,\Phi) / \mathbf{cont}\} \\
={} & \mathsf{iter}(L, L_1, R, \Phi) \sqcap \mathsf{iter}(L, L_2, R, \Phi) && \text{(Step} \Rightarrow \text{Fig. VII.6.2)}
\end{aligned}
$$

QED.

VIII.32 Proof of Theorem VII.6.11

- **A1.** $\langle G_1, r[a]\rangle \in \mathrm{dom} \restriction$
- **A2.** $\langle G_2, r[a]\rangle \in \mathrm{dom} \restriction$
- **A3.** $\Phi \in \mathrm{dom}\,\mathsf{len}$
- **A4.** $r \notin R$

By induction on A3 (Fig. VII.2.5):

- **Base.** $\mathsf{len}\,\Phi = \mathsf{0}$

  Conclude:

$$\begin{aligned} & \mathsf{iter}(G_1 \restriction r[a], G_2 \restriction r[a], R, \Phi) \\ = \;& G_2 \restriction r[a] && \text{(Base} \Rightarrow \text{A1, A2, Fig. VII.6.2)} \\ = \;& \mathsf{iter}(G_1, G_2, R, \Phi) \restriction r[a] && \text{(Base} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

- **Step.** $\mathsf{len}\,\Phi > \mathsf{0}$
  - **B1.** Conclude:

$$\begin{aligned} & \mathsf{len}\,\Phi > \mathsf{0} && \text{(Step)} \\ \textbf{impl.}\;& \mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi && \text{(Thm. VII.2.5)} \end{aligned}$$

  Conclude:

$$\begin{aligned} & \mathsf{iter}(G_1 \restriction r[a], G_2 \restriction r[a], R, \Phi) \\ = \;& (G_1 \restriction r[a])\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(G_1 \restriction r[a], G_2 \restriction r[a], R, \mathsf{tail}\,\Phi)/\mathbf{\mathtt{cont}}\} \\ & && \text{(Step} \Rightarrow \text{A1, A2, Fig. VII.6.2)} \\ = \;& (G_1\,(\!(R[\mathsf{head}\,\Phi])\!) \restriction r[a])\,\{\mathsf{iter}(G_1 \restriction r[a], G_2 \restriction r[a], R, \mathsf{tail}\,\Phi)/\mathbf{\mathtt{cont}}\} && \text{(A4} \Rightarrow \text{Thm. VII.6.4)} \\ = \;& (G_1\,(\!(R[\mathsf{head}\,\Phi])\!) \restriction r[a])\,\{\mathsf{iter}(G_1, G_2, R, \mathsf{tail}\,\Phi) \restriction r[a]/\mathbf{\mathtt{cont}}\} && \text{(B1, A4} \Rightarrow \text{Induction)} \\ = \;& G_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(G_1, G_2, R, \mathsf{tail}\,\Phi)/\mathbf{\mathtt{cont}}\} \restriction r[a] && \text{(Thm. VII.5.2)} \\ = \;& \mathsf{iter}(G_1, G_2, R, \Phi) \restriction r[a] && \text{(Step} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

QED.

VIII.33 Proof of Theorem VII.6.12

- **A1.** $\Phi \in \mathrm{dom}\,\mathsf{len}$
- **A2.** $R \cap R' = \emptyset$

By induction on A1 (Fig. VII.2.5):

- **Base.** $\mathsf{len}\,\Phi = \mathsf{0}$

  Conclude:

$$\begin{aligned} & \mathsf{iter}(T_1\,(\!(R'[\phi'])\!), T_2\,(\!(R'[\phi'])\!), R, \Phi) && \\ = {} & T_2\,(\!(R'[\phi'])\!) && \text{(Base} \Rightarrow \text{Fig. VII.6.2)} \\ = {} & \mathsf{iter}(T_1, T_2, R, \Phi)\,(\!(R'[\phi'])\!) && \text{(Base} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

- **Step.** $\mathsf{len}\,\Phi > \mathsf{0}$

  - **B1.** Conclude:

$$\begin{aligned} & \mathsf{len}\,\Phi > \mathsf{0} && \text{(Step)} \\ \textbf{impl.}\ & \mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi && \text{(Thm. VII.2.5)} \end{aligned}$$

  Conclude:

$$\begin{aligned} & \mathsf{iter}(T_1\,(\!(R'[\phi'])\!), T_2\,(\!(R'[\phi'])\!), R, \Phi) && \\ = {} & T_1\,(\!(R'[\phi'])\!)\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(T_1\,(\!(R'[\phi'])\!), T_2\,(\!(R'[\phi'])\!), R, \mathsf{tail}\,\Phi)/\mathtt{cont}\} && \\ & && \text{(Step} \Rightarrow \text{Fig. VII.6.2)} \\ = {} & T_1\,(\!(R'[\phi'])\!)\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)\,(\!(R'[\phi'])\!)/\mathtt{cont}\} && \text{(B1, A2} \Rightarrow \text{Induction)} \\ = {} & T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,(\!(R'[\phi'])\!)\,\{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)\,(\!(R'[\phi'])\!)/\mathtt{cont}\} && \text{(A2} \Rightarrow \text{Thm. VII.6.5:2)} \\ = {} & T_1\,(\!(R[\mathsf{head}\,\Phi])\!)\,\{\mathsf{iter}(T_1, T_2, R, \mathsf{tail}\,\Phi)/\mathtt{cont}\}\,(\!(R'[\phi'])\!) && \text{(Thm. VII.6.2)} \\ = {} & \mathsf{iter}(T_1, T_2, R, \Phi)\,(\!(R'[\phi'])\!) && \text{(Step} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

QED.

VIII.34 Proof of Theorem VII.6.13

- **A1.** $\Phi \in \mathrm{dom}\,\mathsf{len}$
- **A2.** $\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathrm{dom}\,\Phi \mid \tilde{r} \in R\}, \{\mathtt{cont}\}}(G)$
- **A3.** $\mathrm{expr}\,G \cap \mathbb{G}_{\mathtt{rec}} = \emptyset$
- **A4.** $r \in R$
- **A5.** $a \notin \bigcup \mathrm{img}\,\Phi$

By induction on A1 (Fig. VII.2.5):

- **Base.** $\mathsf{len}\,\Phi = \mathsf{0}$

  Conclude:

$$\begin{aligned} & \mathtt{cont} && \\ = {} & \mathtt{cont} \restriction r[a] && \text{(Fig. VII.5.2)} \\ = {} & \mathsf{iter}(G, \mathtt{cont}, R, \Phi) \restriction r[a] && \text{(Base} \Rightarrow \text{Fig. VII.6.2)} \end{aligned}$$

- **Step.** $\mathsf{len}\,\Phi > 0$
  - **B1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{len}\,\Phi > 0 & \text{(Step)} \\
\textbf{impl.} & |\Phi(\tilde{z})| > 0 \ \textbf{for-all} \ \tilde{z} \in \mathrm{dom}\,\Phi & \text{(Fig. VII.2.5)} \\
\textbf{impl.} & \Phi(\tilde{z}) \neq \emptyset \ \textbf{for-all} \ \tilde{z} \in \mathrm{dom}\,\Phi & (-)
\end{array}$$

  - **B2.** Conclude:

$$\begin{array}{lll}
 & a \notin \bigcup \mathrm{img}\,\Phi & \text{(A5)} \\
\textbf{impl.} & a \notin \Phi(\tilde{z}) \ \textbf{for-all} \ \tilde{z} \in \mathrm{dom}\,\Phi & (-) \\
\textbf{impl.} & \Big[a \notin \Phi(\tilde{z}) \ \textbf{for-all} \ \tilde{z} \in \mathrm{dom}\,\Phi\Big] \ \textbf{and} \ \Big[\Phi(\tilde{z}) \neq \emptyset \ \textbf{for-all} \ \tilde{z} \in \mathrm{dom}\,\Phi\Big] & \text{(B1)} \\
\textbf{impl.} & a \neq \min \Phi(\tilde{z}) \ \textbf{for-all} \ \tilde{z} \in \mathrm{dom}\,\Phi & (-) \\
\textbf{impl.} & a \neq \mathsf{head}\,\Phi(\tilde{z}) \ \textbf{for-all} \ \tilde{z} \in \mathrm{dom}\,\Phi & \text{(Fig. VII.2.2)} \\
\textbf{impl.} & a \notin \{\mathsf{head}\,\Phi(\tilde{z}) \mid \tilde{z} \in \mathrm{dom}\,\Phi\} & (-) \\
\textbf{impl.} & a \notin \mathrm{img}\,\{\tilde{z} \mapsto \mathsf{head}\,\Phi(\tilde{z}) \mid \tilde{z} \in \mathrm{dom}\,\Phi\} & (-) \\
\textbf{impl.} & a \notin \mathsf{head}\,\Phi & \text{(Fig. VII.2.5)}
\end{array}$$

  - **B3.** Conclude:

$$\begin{array}{lll}
 & \mathrm{dom}\,\Phi \subseteq \mathrm{dom}\,(\mathsf{head}\,\Phi) \ \textbf{and} \ \mathrm{dom}\,(\mathsf{head}\,\Phi) \subseteq \mathrm{dom}\,\Phi & \text{(B2} \Rightarrow \text{Lem. VII.2.6:2)} \\
\textbf{impl.} & \mathrm{dom}\,\Phi = \mathrm{dom}\,(\mathsf{head}\,\Phi) & (-) \\
\textbf{impl.} & \mathrm{dom}\,\Phi = \mathrm{dom}\,(\mathsf{head}\,\Phi) \ \textbf{and} \ \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathrm{dom}\,\Phi \mid \tilde{r} \in R\}, \{\mathtt{cont}\}}(G) & \text{(A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathrm{dom}\,(\mathsf{head}\,\Phi) \mid \tilde{r} \in R\}, \{\mathtt{cont}\}}(G) & (=)
\end{array}$$

  - **B4.** Conclude:

$$\begin{array}{lll}
 & \mathsf{len}\,\Phi > 0 & \text{(Step)} \\
\textbf{impl.} & \mathsf{len}\,(\mathsf{tail}\,\Phi) < \mathsf{len}\,\Phi & \text{(Thm. VII.2.5)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
 & \mathtt{cont} & \\
= & \mathtt{cont}\,\{\mathtt{cont}/\mathtt{cont}\} & \text{(Fig. VII.4.3)} \\
= & (G\,((R[\mathsf{head}\,\Phi])) \upharpoonright r[a])\,\{\mathtt{cont}/\mathtt{cont}\} & \text{(B3, A3, A4, B2} \Rightarrow \text{Thm. VII.6.6)} \\
= & (G\,((R[\mathsf{head}\,\Phi])) \upharpoonright r[a]) & \text{(B4, A2, A3, A4, A5} \Rightarrow \text{Induction)} \\
 & \quad \{\mathsf{iter}(G, \mathtt{cont}, R, \mathsf{tail}\,\Phi) \upharpoonright r[a]/\mathtt{cont}\} & \\
= & (G\,((R[\mathsf{head}\,\Phi]))\,\{\mathsf{iter}(G, \mathtt{cont}, R, \mathsf{tail}\,\Phi)/\mathtt{cont}\}) \upharpoonright r[a] & \text{(Thm. VII.5.2)} \\
= & \mathsf{iter}(G, \mathtt{cont}, R, \Phi) \upharpoonright r[a] & \text{(Step} \Rightarrow \text{Fig. VII.6.2)}
\end{array}$$

QED.

VIII.35 Proof of Theorem VII.7.1

By induction on $\check{T}$ (Fig. VII.7.1):

- **Base.** $\check{T} = X$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

    $$\begin{aligned}
    &\check{T}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \\
    =\;& X\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Base)}\\
    =\;& X\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Fig. VII.7.3)}\\
    =\;& \check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle && \text{(Case} \Rightarrow \text{Fig. VII.7.5)}\\
    =\;& X\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Case} \Rightarrow \text{Fig. VII.7.5)}\\
    =\;& \check{T}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Base)}
    \end{aligned}$$

  - **Case.** $X \neq Y$

    Conclude:

    $$\begin{aligned}
    &\check{T}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \\
    =\;& X\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Base)}\\
    =\;& X\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Fig. VII.7.3)}\\
    =\;& X && \text{(Case} \Rightarrow \text{Fig. VII.7.5)}\\
    =\;& X\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.3)}\\
    =\;& X\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Case} \Rightarrow \text{Fig. VII.7.5)}\\
    =\;& \check{T}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Base)}
    \end{aligned}$$

- **Step.** $\check{T} = r_1[x_1] \rightarrow r_2[x_2] \mathbin{\boldsymbol{:}} \{\ell_i \,.\, \check{G}_i\}_{i\in I}$

  Conclude:

  $$\begin{aligned}
  &\check{T}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \\
  =\;& r_1[x_1] \rightarrow r_2[x_2] \mathbin{\boldsymbol{:}} \{\ell_i \,.\, \check{G}_i\}_{i\in I}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Step)}\\
  =\;& r_1[x_1\,\langle\!\langle\psi\rangle\!\rangle] \rightarrow r_2[x_2\,\langle\!\langle\psi\rangle\!\rangle] \mathbin{\boldsymbol{:}} \{\ell_i \,.\, \check{G}_i\,\langle\!\langle\psi\rangle\!\rangle\}_{i\in I}\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Fig. VII.7.3)}\\
  =\;& r_1[x_1\,\langle\!\langle\psi\rangle\!\rangle] \rightarrow r_2[x_2\,\langle\!\langle\psi\rangle\!\rangle] \mathbin{\boldsymbol{:}} \{\ell_i \,.\, \check{G}_i\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\}\}_{i\in I} && \text{(Fig. VII.7.5)}\\
  =\;& r_1[x_1\,\langle\!\langle\psi\rangle\!\rangle] \rightarrow r_2[x_2\,\langle\!\langle\psi\rangle\!\rangle] \mathbin{\boldsymbol{:}} \{\ell_i \,.\, \check{G}_i\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle\}_{i\in I} && \text{(Induction)}\\
  =\;& r_1[x_1] \rightarrow r_2[x_2] \mathbin{\boldsymbol{:}} \{\ell_i \,.\, \check{G}_i\,\{\check{T}_Y/Y\}\}_{i\in I}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.3)}\\
  =\;& r_1[x_1] \rightarrow r_2[x_2] \mathbin{\boldsymbol{:}} \{\ell_i \,.\, \check{G}_i\}_{i\in I}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.5)}\\
  =\;& \check{T}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Step)}
  \end{aligned}$$

- **Step.** $\check{T} = r_2[x_2] \,\boldsymbol{!}\, \{\ell_i \,.\, \check{L}_i\}_{i\in I}$

Conclude:

$$\begin{aligned}
&\check{T}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} \\
={}& r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,\check{L}_i\}_{i\in I}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Step)} \\
={}& r_2[x_2\,\langle\!\langle\psi\rangle\!\rangle]\,\mathbf{!}\{\ell_i\,.\,\check{L}_i\,\langle\!\langle\psi\rangle\!\rangle\}_{i\in I}\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Fig. VII.7.3)} \\
={}& r_2[x_2\,\langle\!\langle\psi\rangle\!\rangle]\,\mathbf{!}\{\ell_i\,.\,\check{L}_i\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\}\}_{i\in I} && \text{(Fig. VII.7.5)} \\
={}& r_2[x_2\,\langle\!\langle\psi\rangle\!\rangle]\,\mathbf{!}\{\ell_i\,.\,\check{L}_i\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle\}_{i\in I} && \text{(Induction)} \\
={}& r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,\check{L}_i\,\{\check{T}_Y/Y\}\}_{i\in I}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,\check{L}_i\}_{i\in I}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.5)} \\
={}& \check{T}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{T} = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\check{L}_i\}_{i\in I}$

  Conclude:

$$\begin{aligned}
&\check{T}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} \\
={}& r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\check{L}_i\}_{i\in I}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Step)} \\
={}& r_1[x_1\,\langle\!\langle\psi\rangle\!\rangle]\,\mathbf{?}\{\ell_i\,.\,\check{L}_i\,\langle\!\langle\psi\rangle\!\rangle\}_{i\in I}\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Fig. VII.7.3)} \\
={}& r_1[x_1\,\langle\!\langle\psi\rangle\!\rangle]\,\mathbf{?}\{\ell_i\,.\,\check{L}_i\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\}\}_{i\in I} && \text{(Fig. VII.7.5)} \\
={}& r_1[x_1\,\langle\!\langle\psi\rangle\!\rangle]\,\mathbf{?}\{\ell_i\,.\,\check{L}_i\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle\}_{i\in I} && \text{(Induction)} \\
={}& r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\check{L}_i\,\{\check{T}_Y/Y\}\}_{i\in I}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\check{L}_i\}_{i\in I}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.5)} \\
={}& \check{T}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{T} = \texttt{\textbf{foreach}}\ R[\check{C}]\ \textsf{\textbf{do}}\ \check{T}_1\,\mathbf{;}\,\check{T}_2$

  Conclude:

$$\begin{aligned}
&\check{T}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} \\
={}& \texttt{\textbf{foreach}}\ R[\check{C}]\ \textsf{\textbf{do}}\ \check{T}_1\,\mathbf{;}\,\check{T}_2\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Step)} \\
={}& \texttt{\textbf{foreach}}\ R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]\ \textsf{\textbf{do}}\ (\check{T}_1\,\langle\!\langle\psi\rangle\!\rangle)\,\mathbf{;}\,(\check{T}_2\,\langle\!\langle\psi\rangle\!\rangle)\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Fig. VII.7.3)} \\
={}& \texttt{\textbf{foreach}}\ R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]\ \textsf{\textbf{do}}\ (\check{T}_1\,\langle\!\langle\psi\rangle\!\rangle)\,\mathbf{;}\,(\check{T}_2\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\}) && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \texttt{\textbf{foreach}}\ R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]\ \textsf{\textbf{do}}\ (\check{T}_1\,\langle\!\langle\psi\rangle\!\rangle)\,\mathbf{;}\,(\check{T}_2\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle) && \text{(Induction)} \\
={}& \texttt{\textbf{foreach}}\ R[\check{C}]\ \textsf{\textbf{do}}\ \check{T}_1\,\mathbf{;}\,(\check{T}_2\,\{\check{T}_Y/Y\})\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& \texttt{\textbf{foreach}}\ R[\check{C}]\ \textsf{\textbf{do}}\ \check{T}_1\,\mathbf{;}\,\check{T}_2\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \check{T}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{T} = \texttt{\textbf{rec}}\ X\ \check{T}_X$

  By case distinction:

  - **Case.** $X = Y$

Conclude:

$$\begin{aligned}
& \check{T}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \\
={}& \textbf{\texttt{rec}}\ X\ \check{T}_X\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Step)} \\
={}& \textbf{\texttt{rec}}\ X\ (\check{T}_X\,\langle\!\langle\psi\rangle\!\rangle)\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Fig. VII.7.3)} \\
={}& \textbf{\texttt{rec}}\ X\ (\check{T}_X\,\langle\!\langle\psi\rangle\!\rangle) && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \textbf{\texttt{rec}}\ X\ \check{T}_X\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& \textbf{\texttt{rec}}\ X\ \check{T}_X\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \check{T}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Step)}
\end{aligned}$$

- **Case.** $X \neq Y$

  Conclude:

$$\begin{aligned}
& \check{T}\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \\
={}& \textbf{\texttt{rec}}\ X\ \check{T}_X\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Step)} \\
={}& \textbf{\texttt{rec}}\ X\ (\check{T}_X\,\langle\!\langle\psi\rangle\!\rangle)\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\} && \text{(Fig. VII.7.3)} \\
={}& \textbf{\texttt{rec}}\ X\ (\check{T}_X\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{T}_Y\,\langle\!\langle\psi\rangle\!\rangle/Y\}) && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \textbf{\texttt{rec}}\ X\ (\check{T}_X\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle) && \text{(Induction)} \\
={}& \textbf{\texttt{rec}}\ X\ (\check{T}_X\,\{\check{T}_Y/Y\})\,\langle\!\langle\psi\rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& \textbf{\texttt{rec}}\ X\ \check{T}_X\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \check{T}\,\{\check{T}_Y/Y\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Step)}
\end{aligned}$$

QED.

VIII.36 Proof of Theorem VII.7.2

Assume:

- **A1.** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T})$
- **A2.** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y)$

By induction on A1 (Fig. VII.7.4):

- **Base.** $\hat{T} = X$ **and** $X \in \mathcal{X}$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y) && \text{(A2)} \\
\textbf{impl. }& \mathsf{Wf}_{f,\mathcal{X}}(X\,\{\hat{T}_Y/Y\}) && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
\textbf{impl. }& \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\}) && \text{(Base)}
\end{aligned}$$

- **Case.** $X \neq Y$
  Conclude:

$$\begin{array}{rlr}
 & \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}) & \text{(A1)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X) & \text{(Base)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(X\,\{\hat{T}_Y/Y\}) & \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\}) & \text{(Base)}
\end{array}$$

- **Step.** $\hat{T} = r_1[x_1] \mathrel{-\!\!\blacktriangleright} r_2[x_2] \mathbin{\boldsymbol{:}} \{\ell_i \mathbin{\boldsymbol{.}} \hat{G}_i\}_{i\in I}$ **and**
  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and**
  $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i)$ **for-all** $i \in I\Big]$
  Conclude:

$$\begin{array}{rlr}
 & \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i) \textbf{ for-all } i \in I\Big] \textbf{ and } \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y) & \text{(Step, A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i\,\{\hat{T}_Y/Y\}) \textbf{ for-all } i \in I & \text{(Induction)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \mathrel{-\!\!\blacktriangleright} r_2[x_2] \mathbin{\boldsymbol{:}} \{\ell_i \mathbin{\boldsymbol{.}} \hat{G}_i\,\{\hat{T}_Y/Y\}\}_{i\in I}) & \text{(Step} \Rightarrow \text{Fig. VII.7.4)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \mathrel{-\!\!\blacktriangleright} r_2[x_2] \mathbin{\boldsymbol{:}} \{\ell_i \mathbin{\boldsymbol{.}} \hat{G}_i\}_{i\in I}\,\{\hat{T}_Y/Y\}) & \text{(Fig. VII.7.5)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\}) & \text{(Step)}
\end{array}$$

- **Step.** $\hat{T} = r_2[x_2]\,\boldsymbol{!}\,\{\ell_i \mathbin{\boldsymbol{.}} \hat{L}_i\}_{i\in I}$ **and**
  $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i)$ **for-all** $i \in I\Big]$
  Conclude:

$$\begin{array}{rlr}
 & \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i) \textbf{ for-all } i \in I\Big] \textbf{ and } \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y) & \text{(Step, A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i\,\{\hat{T}_Y/Y\}) \textbf{ for-all } i \in I & \text{(Induction)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,\boldsymbol{!}\,\{\ell_i \mathbin{\boldsymbol{.}} \hat{L}_i\,\{\hat{T}_Y/Y\}\}_{i\in I}) & \text{(Step} \Rightarrow \text{Fig. VII.7.4)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,\boldsymbol{!}\,\{\ell_i \mathbin{\boldsymbol{.}} \hat{L}_i\}_{i\in I}\,\{\hat{T}_Y/Y\}) & \text{(Fig. VII.7.5)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\}) & \text{(Step)}
\end{array}$$

- **Step.** $\hat{T} = r_1[x_1]\,\boldsymbol{?}\{\ell_i \mathbin{\boldsymbol{.}} \hat{L}_i\}_{i\in I}$ **and**
  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i)$ **for-all** $i \in I\Big]$
  Conclude:

$$\begin{array}{rlr}
 & \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i) \textbf{ for-all } i \in I\Big] \textbf{ and } \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y) & \text{(Step, A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i\,\{\hat{T}_Y/Y\}) \textbf{ for-all } i \in I & \text{(Induction)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,\boldsymbol{?}\{\ell_i \mathbin{\boldsymbol{.}} \hat{L}_i\,\{\hat{T}_Y/Y\}\}_{i\in I}) & \text{(Step} \Rightarrow \text{Fig. VII.7.4)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,\boldsymbol{?}\{\ell_i \mathbin{\boldsymbol{.}} \hat{L}_i\}_{i\in I}\,\{\hat{T}_Y/Y\}) & \text{(Fig. VII.7.5)} \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\}) & \text{(Step)}
\end{array}$$

- **Step.** $\hat{T} = \texttt{foreach}\ R[\hat{C}]\ \textbf{do}\ \hat{T}_1 \mathbin{\boldsymbol{;}} \hat{T}_2$ **and**
  $f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}}$ **and** $\hat{C} \in \checkmark$ **and** $\operatorname{expr} \hat{T}_1 \cap \mathbb{G}_{\texttt{rec}} = \emptyset$ **and**
  $\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \{\texttt{cont}\}}(\hat{T}_1)$ **and** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_2)$

Conclude:

$\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_2)$ **and** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y)$ (Step, A2)
impl. $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_2\,\{\hat{T}_Y/Y\})$ (Induction)
impl. $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{foreach}\ R[\hat{C}]\ \texttt{do}\ \hat{T}_1\ \texttt{;}\ (\hat{T}_2\,\{\hat{T}_Y/Y\}))$ (Step ⇒ Fig. VII.7.4)
impl. $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{foreach}\ R[\hat{C}]\ \texttt{do}\ \hat{T}_1\ \texttt{;}\ \hat{T}_2\,\{\hat{T}_Y/Y\})$ (Fig. VII.7.5)
impl. $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\})$ (Step)

- **Step.** $\hat{T} = \texttt{rec}\ X\ \hat{T}_X$ **and** $\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_X)$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

    $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T})$ (A1)
    impl. $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ \hat{T}_X)$ (Step)
    impl. $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ \hat{T}_X\,\{\hat{T}_Y/Y\})$ (Case ⇒ Fig. VII.7.5)
    impl. $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\})$ (Step)

  - **Case.** $X \neq Y$

    Conclude:

    $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_Y)$ (A2)
    impl. $\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_Y)$ (Lem. VII.7.5:2)
    impl. $\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_X)$ **and** $\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_Y)$ (Step)
    impl. $\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_X\,\{\hat{T}_Y/Y\})$ (Induction)
    impl. $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ (\hat{T}_X\,\{\hat{T}_Y/Y\}))$ (Fig. VII.7.4)
    impl. $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ \hat{T}_X\,\{\hat{T}_Y/Y\})$ (Case ⇒ Fig. VII.7.5)
    impl. $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}\,\{\hat{T}_Y/Y\})$ (Step)

QED.

VIII.37 Proof of Theorem VII.7.3

- **A1.** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T})$
- **A2.** $\operatorname{img} f \subseteq 2^{\mathbb{Z}}$
- **B1.** Conclude:

  $x \in f(r)$ ($\exists x$, $\exists r$)
  impl. $x \in f(r) \in 2^{\mathbb{Z}}$ (A2)
  impl. $x \in \mathbb{Z}$ (–)
  impl. $[\![x]\!] = x$ (Fig. VII.3.4)

By induction on A1 (Fig. VII.7.4):

- **Base.** $\hat{T} = X$ **and** $X \in \mathcal{X}$

  Conclude:

$$
\begin{aligned}
& X \in \mathcal{X} && \text{(Base)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(X) && \text{(Fig. VII.4.2)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}([\![X]\!]) && \text{(Fig. VII.7.6)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}([\![\hat{T}]\!]) && \text{(Base)}
\end{aligned}
$$

- **Step.** $\hat{T} = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}$ **and**
  $\Big[r_1 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ x_1 \in f(r_1)\Big]$ **and** $\Big[r_2 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ x_2 \in f(r_2)\Big]$ **and**
  $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i) \ \textsf{\textbf{for-all}}\ i \in I\Big]$

  - **C1.** Conclude:

$$
\begin{aligned}
& \Big[r_1 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ x_1 \in f(r_1)\Big] \ \textsf{\textbf{and}}\ \Big[r_2 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ x_2 \in f(r_2)\Big] && \text{(Step)}\\
\textsf{\textbf{impl.}}\ & \Big[r_1 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ [\![x_1]\!] \in f(r_1)\Big] \ \textsf{\textbf{and}}\ \Big[r_2 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ [\![x_2]\!] \in f(r_2)\Big] && \text{(B1)}
\end{aligned}
$$

  Conclude:

$$
\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i) \ \textsf{\textbf{for-all}}\ i \in I && \text{(Step)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}([\![\hat{G}_i]\!]) \ \textsf{\textbf{for-all}}\ i \in I && \text{(A2} \Rightarrow \text{Induction)}\\
\textsf{\textbf{impl.}}\ & \Big[r_1 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ [\![x_1]\!] \in f(r_1)\Big] \ \textsf{\textbf{and}}\ \Big[r_2 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ [\![x_2]\!] \in f(r_2)\Big] \ \textsf{\textbf{and}} && \text{(C1)}\\
& \Big[\mathsf{Wf}_{f,\mathcal{X}}([\![\hat{G}_i]\!]) \ \textsf{\textbf{for-all}}\ i \in I\Big] &&\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(r_1[[\![x_1]\!]] \rightarrowtriangle r_2[[\![x_2]\!]] : \{\ell_i \,.\, [\![\hat{G}_i]\!]\}_{i \in I}) && \text{(Fig. VII.4.2)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}([\![r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}]\!]) && \text{(Fig. VII.7.6)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}([\![\hat{T}]\!]) && \text{(Step)}
\end{aligned}
$$

- **Step.** $\hat{T} = r_2[x_2] \,!\, \{\ell_i \,.\, \hat{L}_i\}_{i \in I}$ **and**
  $\Big[r_2 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ x_2 \in f(r_2)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i) \ \textsf{\textbf{for-all}}\ i \in I\Big]$

  - **D1.** Conclude:

$$
\begin{aligned}
& r_2 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ x_2 \in f(r_2) && \text{(Step)}\\
\textsf{\textbf{impl.}}\ & r_2 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ [\![x_2]\!] \in f(r_2) && \text{(B1)}
\end{aligned}
$$

  Conclude:

$$
\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i) \ \textsf{\textbf{for-all}}\ i \in I && \text{(Step)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}([\![\hat{L}_i]\!]) \ \textsf{\textbf{for-all}}\ i \in I && \text{(A2} \Rightarrow \text{Induction)}\\
\textsf{\textbf{impl.}}\ & \Big[r_2 \in \operatorname{dom} f \ \textsf{\textbf{impl.}}\ [\![x_2]\!] \in f(r_2)\Big] \ \textsf{\textbf{and}}\ \Big[\mathsf{Wf}_{f,\mathcal{X}}([\![\hat{L}_i]\!]) \ \textsf{\textbf{for-all}}\ i \in I\Big] && \text{(C1)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(r_2[[\![x_2]\!]] \,!\, \{\ell_i \,.\, [\![\hat{L}_i]\!]\}_{i \in I}) && \text{(Fig. VII.4.2)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}([\![r_2[x_2] \,!\, \{\ell_i \,.\, \hat{L}_i\}_{i \in I}]\!]) && \text{(Fig. VII.7.6)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}([\![\hat{T}]\!]) && \text{(Step)}
\end{aligned}
$$

- **Step.** $\hat{T} = r_1[x_1]\,\textbf{?}\{\ell_i\,\textbf{.}\,\hat{L}_i\}_{i\in I}$ **and**

  $\Big[r_1 \in \operatorname{dom} f \;\; \textbf{\textsf{impl.}} \;\; x_1 \in f(r_1)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i) \;\; \textbf{\textsf{for-all}} \;\; i \in I\Big]$

  - **E1.** Conclude:

$$\begin{array}{rll} & r_1 \in \operatorname{dom} f \;\; \textbf{\textsf{impl.}} \;\; x_1 \in f(r_1) & \text{(Step)} \\ \textbf{\textsf{impl.}} & r_1 \in \operatorname{dom} f \;\; \textbf{\textsf{impl.}} \;\; \llbracket x_1 \rrbracket \in f(r_1) & \text{(B1)} \end{array}$$

  Conclude:

$$\begin{array}{rll} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i) \;\; \textbf{\textsf{for-all}} \;\; i \in I & \text{(Step)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\llbracket \hat{L}_i \rrbracket) \;\; \textbf{\textsf{for-all}} \;\; i \in I & \text{(A2} \Rightarrow \text{Induction)} \\ \textbf{\textsf{impl.}} & \Big[r_1 \in \operatorname{dom} f \;\; \textbf{\textsf{impl.}} \;\; \llbracket x_1 \rrbracket \in f(r_1)\Big] \;\; \textbf{\textsf{and}} \;\; \Big[\mathsf{Wf}_{f,\mathcal{X}}(\llbracket \hat{L}_i \rrbracket) \;\; \textbf{\textsf{for-all}} \;\; i \in I\Big] & \text{(E1)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[\llbracket x_1 \rrbracket]\,\textbf{?}\{\ell_i\,\textbf{.}\,\llbracket \hat{L}_i \rrbracket\}_{i\in I}) & \text{(Fig. VII.4.2)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\llbracket r_1[x_1]\,\textbf{?}\{\ell_i\,\textbf{.}\,\hat{L}_i\}_{i\in I} \rrbracket) & \text{(Fig. VII.7.6)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\llbracket \hat{T} \rrbracket) & \text{(Step)} \end{array}$$

- **Step.** $\hat{T} = \texttt{foreach}\ R[\hat{C}]\ \texttt{do}\ \hat{T}_1\ \textbf{;}\ \hat{T}_2$ **and**

  $f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}}$ **and** $\hat{C} \in \checkmark$ **and** $\operatorname{expr} \hat{T}_1 \cap \mathbb{G}_{\texttt{rec}} = \emptyset$ **and**

  $\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\texttt{cont}\}}(\hat{T}_1)$ **and** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_2)$

  - **F1.** Conclude:

$$\begin{array}{ll} \mathsf{len}\, \llbracket \hat{C} \rrbracket > \mathsf{0} & \text{(Step} \Rightarrow \text{Thm. VII.3.6)} \end{array}$$

  Conclude:

$$\begin{array}{rll} & \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\texttt{cont}\}}(\hat{T}_1) \;\; \textbf{\textsf{and}} \;\; \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_2) & \text{(Step)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\{\texttt{cont}\}}(\hat{T}_1) \;\; \textbf{\textsf{and}} \;\; \mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_2) & \text{(Lem. VII.7.5:1)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\{\texttt{cont}\}}(\llbracket \hat{T}_1 \rrbracket) \;\; \textbf{\textsf{and}} \;\; \mathsf{Wf}_{f,\mathcal{X}}(\llbracket \hat{T}_2 \rrbracket) & \text{(A2} \Rightarrow \text{Induction)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\mathsf{iter}(\llbracket \hat{T}_1 \rrbracket, \llbracket \hat{T}_2 \rrbracket, R, \llbracket \hat{C} \rrbracket)) & \text{(F1} \Rightarrow \text{Thm. VII.6.8:2)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\llbracket \texttt{foreach}\ R[\hat{C}]\ \texttt{do}\ \hat{T}_1\ \textbf{;}\ \hat{T}_2 \rrbracket) & \text{(Fig. VII.7.6)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\llbracket \hat{T} \rrbracket) & \text{(Step)} \end{array}$$

- **Step.** $\hat{T} = \texttt{rec}\ X\ \hat{T}_X$ **and** $\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_X)$

  Conclude:

$$\begin{array}{rll} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_X) & \text{(Step)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\llbracket \hat{T}_X \rrbracket) & \text{(A2} \Rightarrow \text{Induction)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ \llbracket \hat{T}_X \rrbracket) & \text{(Fig. VII.4.2)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\llbracket \texttt{rec}\ X\ \hat{T}_X \rrbracket) & \text{(Fig. VII.7.6)} \\ \textbf{\textsf{impl.}} & \mathsf{Wf}_{f,\mathcal{X}}(\llbracket \hat{T} \rrbracket) & \text{(Step)} \end{array}$$

QED.

VIII.38 Proof of Theorem VII.7.4

Assume:

- **A1.** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T})$

By induction on A1 (Fig. VII.7.4):

- **Base.** $\hat{T} = X$ **and** $X \in \mathcal{X}$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$\begin{aligned}
&\llbracket \hat{T}\,\{\hat{T}_Y/Y\} \rrbracket \\
={}& \llbracket X\,\{\hat{T}_Y/Y\} \rrbracket && \text{(Base)} \\
={}& \llbracket \hat{T}_Y \rrbracket && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
={}& X\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Base} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \llbracket X \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{T} \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Base)}
\end{aligned}$$

  - **Case.** $X \neq Y$

    Conclude:

$$\begin{aligned}
&\llbracket \hat{T}\,\{\hat{T}_Y/Y\} \rrbracket \\
={}& \llbracket X\,\{\hat{T}_Y/Y\} \rrbracket && \text{(Base)} \\
={}& \llbracket X \rrbracket && \text{(Case} \Rightarrow \text{Fig. VII.7.5)} \\
={}& X && \text{(Fig. VII.7.6)} \\
={}& X\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Base} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \llbracket X \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{T} \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Base)}
\end{aligned}$$

- **Step.** $\hat{T} = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i\,.\,\hat{G}_i\}_{i \in I}$ **and**
  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and**
  $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i)$ **for-all** $i \in I\Big]$

  Conclude:

$$\begin{aligned}
&\llbracket \hat{T}\,\{\hat{T}_Y/Y\} \rrbracket \\
={}& \llbracket r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i\,.\,\hat{G}_i\}_{i \in I}\,\{\hat{T}_Y/Y\} \rrbracket && \text{(Step)} \\
={}& \llbracket r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i\,.\,\hat{G}_i\,\{\hat{T}_Y/Y\}\}_{i \in I} \rrbracket && \text{(Fig. VII.7.5)} \\
={}& r_1[\llbracket x_1 \rrbracket] \rightarrowtriangle r_2[\llbracket x_2 \rrbracket] : \{\ell_i\,.\,\llbracket \hat{G}_i\,\{\hat{T}_Y/Y\} \rrbracket\}_{i \in I} && \text{(Fig. VII.7.6)} \\
={}& r_1[\llbracket x_1 \rrbracket] \rightarrowtriangle r_2[\llbracket x_2 \rrbracket] : \{\ell_i\,.\,\llbracket \hat{G}_i \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\}\}_{i \in I} && \text{(Step} \Rightarrow \text{Induction)} \\
={}& r_1[\llbracket x_1 \rrbracket] \rightarrowtriangle r_2[\llbracket x_2 \rrbracket] : \{\ell_i\,.\,\llbracket \hat{G}_i \rrbracket\}_{i \in I}\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Fig. VII.7.5)} \\
={}& \llbracket r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i\,.\,\hat{G}_i\}_{i \in I} \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{T} \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{T} = r_2[x_2]\,\mathbf{!}\,\{\ell_i\,.\,\hat{L}_i\}_{i\in I}$ **and**
  $\Big[r_2 \in \operatorname{dom} f$ **impl.** $x_2 \in f(r_2)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i)$ **for-all** $i \in I\Big]$

  Conclude:

$$\begin{aligned}
&\llbracket \hat{T}\,\{\hat{T}_Y/Y\}\rrbracket \\
=\;& \llbracket r_2[x_2]\,\mathbf{!}\,\{\ell_i\,.\,\hat{L}_i\}_{i\in I}\,\{\hat{T}_Y/Y\}\rrbracket && \text{(Step)}\\
=\;& \llbracket r_2[x_2]\,\mathbf{!}\,\{\ell_i\,.\,\hat{L}_i\,\{\hat{T}_Y/Y\}\}_{i\in I}\rrbracket && \text{(Fig. VII.7.5)}\\
=\;& r_2[\llbracket x_2\rrbracket]\,\mathbf{!}\,\{\ell_i\,.\,\llbracket \hat{L}_i\,\{\hat{T}_Y/Y\}\rrbracket\}_{i\in I} && \text{(Fig. VII.7.6)}\\
=\;& r_2[\llbracket x_2\rrbracket]\,\mathbf{!}\,\{\ell_i\,.\,\llbracket \hat{L}_i\rrbracket\,\{\llbracket\hat{T}_Y\rrbracket/Y\}\}_{i\in I} && \text{(Step} \Rightarrow \text{Induction)}\\
=\;& r_2[\llbracket x_2\rrbracket]\,\mathbf{!}\,\{\ell_i\,.\,\llbracket \hat{L}_i\rrbracket\}_{i\in I}\,\{\llbracket\hat{T}_Y\rrbracket/Y\} && \text{(Fig. VII.7.5)}\\
=\;& \llbracket r_2[x_2]\,\mathbf{!}\,\{\ell_i\,.\,\hat{L}_i\}_{i\in I}\rrbracket\,\{\llbracket\hat{T}_Y\rrbracket/Y\} && \text{(Fig. VII.7.6)}\\
=\;& \llbracket \hat{T}\rrbracket\,\{\llbracket\hat{T}_Y\rrbracket/Y\} && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{T} = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_i\}_{i\in I}$ **and**
  $\Big[r_1 \in \operatorname{dom} f$ **impl.** $x_1 \in f(r_1)\Big]$ **and** $\Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_i)$ **for-all** $i \in I\Big]$

  Conclude:

$$\begin{aligned}
&\llbracket \hat{T}\,\{\hat{T}_Y/Y\}\rrbracket \\
=\;& \llbracket r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_i\}_{i\in I}\,\{\hat{T}_Y/Y\}\rrbracket && \text{(Step)}\\
=\;& \llbracket r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_i\,\{\hat{T}_Y/Y\}\}_{i\in I}\rrbracket && \text{(Fig. VII.7.5)}\\
=\;& r_1[\llbracket x_1\rrbracket]\,\mathbf{?}\{\ell_i\,.\,\llbracket \hat{L}_i\,\{\hat{T}_Y/Y\}\rrbracket\}_{i\in I} && \text{(Fig. VII.7.6)}\\
=\;& r_1[\llbracket x_1\rrbracket]\,\mathbf{?}\{\ell_i\,.\,\llbracket \hat{L}_i\rrbracket\,\{\llbracket\hat{T}_Y\rrbracket/Y\}\}_{i\in I} && \text{(Step} \Rightarrow \text{Induction)}\\
=\;& r_1[\llbracket x_1\rrbracket]\,\mathbf{?}\{\ell_i\,.\,\llbracket \hat{L}_i\rrbracket\}_{i\in I}\,\{\llbracket\hat{T}_Y\rrbracket/Y\} && \text{(Fig. VII.7.5)}\\
=\;& \llbracket r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_i\}_{i\in I}\rrbracket\,\{\llbracket\hat{T}_Y\rrbracket/Y\} && \text{(Fig. VII.7.6)}\\
=\;& \llbracket \hat{T}\rrbracket\,\{\llbracket\hat{T}_Y\rrbracket/Y\} && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{T} = \texttt{foreach}\ R[\hat{C}]\ \mathbf{do}\ \hat{T}_1\ \mathbf{;}\ \hat{T}_2$ **and**
  $f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}}$ **and** $\hat{C} \in \checkmark$ **and** $\operatorname{expr} \hat{T}_1 \cap \mathbb{G}_{\texttt{rec}} = \emptyset$ **and**
  $\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\texttt{cont}\}}(\hat{T}_1)$ **and** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{T}_2)$

  - **B1.** Conclude:

$$\mathsf{len}\,\llbracket\hat{C}\rrbracket > 0 \qquad \text{(Step} \Rightarrow \text{Thm. VII.3.6)}$$

  - **B2.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\texttt{cont}\}}(\hat{T}_1)\ \textbf{and}\ f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} && \text{(Step)}\\
\textbf{impl.}\ & \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\texttt{cont}\}}(\hat{T}_1)\ \textbf{and}\ \operatorname{img}(f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}) \subseteq 2^{\mathbb{Z}} && \text{(–)}\\
\textbf{impl.}\ & \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\texttt{cont}\}}(\llbracket\hat{T}_1\rrbracket) && \text{(Thm. VII.7.3)}
\end{aligned}$$

Conclude:

$$
\begin{aligned}
& \llbracket \hat{T}\,\{\hat{T}_Y/Y\} \rrbracket \\
={}& \llbracket \mathtt{\mathbf{foreach}}\ R[\hat{C}]\ \mathtt{\mathbf{do}}\ \hat{T}_1\ \mathtt{\mathbf{;}}\ \hat{T}_2\,\{\hat{T}_Y/Y\} \rrbracket && \text{(Step)} \\
={}& \llbracket \mathtt{\mathbf{foreach}}\ R[\hat{C}]\ \mathtt{\mathbf{do}}\ \hat{T}_1\ \mathtt{\mathbf{;}}\ (\hat{T}_2\,\{\hat{T}_Y/Y\}) \rrbracket && \text{(Fig. VII.7.5)} \\
={}& \mathsf{iter}(\llbracket \hat{T}_1 \rrbracket, \llbracket \hat{T}_2\,\{\hat{T}_Y/Y\} \rrbracket, R, \llbracket \hat{C} \rrbracket) && \text{(Fig. VII.7.6)} \\
={}& \mathsf{iter}(\llbracket \hat{T}_1 \rrbracket, \llbracket \hat{T}_2 \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\}, R, \llbracket \hat{C} \rrbracket) && \text{(Step} \Rightarrow \text{Induction)} \\
={}& \mathsf{iter}(\llbracket \hat{T}_1 \rrbracket, \llbracket \hat{T}_2 \rrbracket, R, \llbracket \hat{C} \rrbracket)\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(B1, B2} \Rightarrow \text{Thm. VII.6.9)} \\
={}& \llbracket \mathtt{\mathbf{foreach}}\ R[\hat{C}]\ \mathtt{\mathbf{do}}\ \hat{T}_1\ \mathtt{\mathbf{;}}\ \hat{T}_2 \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{T} \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Step)}
\end{aligned}
$$

- **Step.** $\hat{T} = \mathtt{\mathbf{rec}}\ X\ \hat{T}_X$ **and** $\mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{T}_X)$

  By case distinction:

  - **Case.** $X = Y$

    Conclude:

$$
\begin{aligned}
& \llbracket \hat{T}\,\{\hat{T}_Y/Y\} \rrbracket \\
={}& \llbracket \mathtt{\mathbf{rec}}\ X\ \hat{T}_X\,\{\hat{T}_Y/Y\} \rrbracket && \text{(Step)} \\
={}& \llbracket \mathtt{\mathbf{rec}}\ X\ T_X \rrbracket && \text{(Fig. VII.7.5)} \\
={}& \mathtt{\mathbf{rec}}\ X\ \llbracket T_X \rrbracket && \text{(Fig. VII.7.6)} \\
={}& \mathtt{\mathbf{rec}}\ X\ \llbracket T_X \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Step} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \llbracket \mathtt{\mathbf{rec}}\ X\ T_X \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{T} \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Step)}
\end{aligned}
$$

  - **Case.** $X \neq Y$

    Conclude:

$$
\begin{aligned}
& \llbracket \hat{T}\,\{\hat{T}_Y/Y\} \rrbracket \\
={}& \llbracket \mathtt{\mathbf{rec}}\ X\ \hat{T}_X\,\{\hat{T}_Y/Y\} \rrbracket && \text{(Step)} \\
={}& \llbracket \mathtt{\mathbf{rec}}\ X\ (T_X\,\{T_Y/Y\}) \rrbracket && \text{(Fig. VII.7.5)} \\
={}& \mathtt{\mathbf{rec}}\ X\ \llbracket T_X\,\{T_Y/Y\} \rrbracket && \text{(Fig. VII.7.6)} \\
={}& \mathtt{\mathbf{rec}}\ X\ (\llbracket T_X \rrbracket\,\{\llbracket T_Y \rrbracket/Y\}) && \text{(Step} \Rightarrow \text{Induction)} \\
={}& \mathtt{\mathbf{rec}}\ X\ \llbracket T_X \rrbracket\,\{\llbracket T_Y \rrbracket/Y\} && \text{(Step} \Rightarrow \text{Fig. VII.7.5)} \\
={}& \llbracket \mathtt{\mathbf{rec}}\ X\ T_X \rrbracket\,\{\llbracket T_Y \rrbracket/Y\} && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{T} \rrbracket\,\{\llbracket \hat{T}_Y \rrbracket/Y\} && \text{(Step)}
\end{aligned}
$$

QED.

VIII.39 Proof of Theorem VII.8.1

- **A1.** $\langle \check{L}_1, \check{L}_2 \rangle \in \mathrm{dom} \sqcap$

By induction on A1 (Fig. VII.8.1):

- **Base.** $\check{L}_1 = \check{L}_2 = X$ **and** $\check{L}_1 \sqcap \check{L}_2 = X$

  Conclude:

$$\begin{aligned}
&(\check{L}_1 \sqcap \check{L}_2)\, \langle\!\langle \psi \rangle\!\rangle \\
={}& X\, \langle\!\langle \psi \rangle\!\rangle && \text{(Base)} \\
={}& X && \text{(Fig. VII.7.3)} \\
={}& X \sqcap X && \text{(Lem. VII.8.1:2)} \\
={}& X\, \langle\!\langle \psi \rangle\!\rangle \sqcap X\, \langle\!\langle \psi \rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& \check{L}_1\, \langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_2\, \langle\!\langle \psi \rangle\!\rangle && \text{(Base)}
\end{aligned}$$

- **Step.** $\check{L}_1 = r_2[x_2]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,1}\}_{i \in I}$ **and** $\check{L}_2 = r_2[x_2]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,2}\}_{i \in I}$ **and**
  $\check{L}_1 \sqcap \check{L}_2 = r_2[x_2]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,1} \sqcap \check{L}_{i,2}\}_{i \in I}$

  Conclude:

$$\begin{aligned}
&(\check{L}_1 \sqcap \check{L}_2)\, \langle\!\langle \psi \rangle\!\rangle \\
={}& r_2[x_2]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,1} \sqcap \check{L}_{i,2}\}_{i \in I}\, \langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
={}& r_2[x_2\, \langle\!\langle \psi \rangle\!\rangle]\, \mathbf{!}\, \{\ell_i \,.\, (\check{L}_{i,1} \sqcap \check{L}_{i,2})\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} && \text{(Fig. VII.7.3)} \\
={}& r_2[x_2\, \langle\!\langle \psi \rangle\!\rangle]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,1}\, \langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_{i,2}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} && \text{(Induction)} \\
={}& r_2[x_2\, \langle\!\langle \psi \rangle\!\rangle]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,1}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \sqcap r_2[x_2\, \langle\!\langle \psi \rangle\!\rangle]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,2}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} && \text{(Fig. VII.8.1)} \\
={}& r_2[x_2]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,1}\}_{i \in I}\, \langle\!\langle \psi \rangle\!\rangle \sqcap r_2[x_2]\, \mathbf{!}\, \{\ell_i \,.\, \check{L}_{i,2}\}_{i \in I}\, \langle\!\langle \psi \rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& \check{L}_1\, \langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_2\, \langle\!\langle \psi \rangle\!\rangle && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{L}_1 = r_1[x_1]\, \mathbf{?} \{\ell_i \,.\, \check{L}_{i,1}\}_{i \in I_1}$ **and** $\check{L}_2 = r_1[x_1]\, \mathbf{?} \{\ell_i \,.\, \check{L}_{i,2}\}_{i \in I_2}$ **and**
  $\check{L}_1 \sqcap \check{L}_2 = r_1[x_1]\, \mathbf{?} \{\ell_i \,.\, \check{L}_{i,1}\}_{i \in I_1 \setminus I_2} \cup \{\ell_i \,.\, \check{L}_{i,2}\}_{i \in I_2 \setminus I_1} \cup \{\ell_i \,.\, \check{L}_{i,1} \sqcap \check{L}_{i,2}\}_{i \in I_1 \cap I_2}$ **and**
  $\Big[\ell_{i_1} \neq \ell_{i_2}$ **for-all** $i_1 \in I_1 \setminus I_2, i_2 \in I_2 \setminus I_1\Big]$

  Conclude:

$$\begin{aligned}
&(\check{L}_1 \sqcap \check{L}_2)\, \langle\!\langle \psi \rangle\!\rangle \\
={}& r_1[x_1]\, \mathbf{?} \{\ell_i \,.\, \check{L}_{i,1}\}_{i \in I_1 \setminus I_2} \cup \{\ell_i \,.\, \check{L}_{i,2}\}_{i \in I_2 \setminus I_1} \cup \{\ell_i \,.\, \check{L}_{i,1} \sqcap \check{L}_{i,2}\}_{i \in I_1 \cap I_2}\, \langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
={}& r_1[x_1\, \langle\!\langle \psi \rangle\!\rangle]\, \mathbf{?} && \text{(Fig. VII.7.3)} \\
& \quad \{\ell_i \,.\, \check{L}_{i,1}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I_1 \setminus I_2} \cup \{\ell_i \,.\, \check{L}_{i,2}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I_2 \setminus I_1} \cup \{\ell_i \,.\, (\check{L}_{i,1} \sqcap \check{L}_{i,2})\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I_1 \cap I_2} \\
={}& r_1[x_1\, \langle\!\langle \psi \rangle\!\rangle]\, \mathbf{?} && \text{(Induction)} \\
& \quad \{\ell_i \,.\, \check{L}_{i,1}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I_1 \setminus I_2} \cup \{\ell_i \,.\, \check{L}_{i,2}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I_2 \setminus I_1} \cup \{\ell_i \,.\, \check{L}_{i,1}\, \langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_{i,2}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I_1 \cap I_2} \\
={}& r_1[x_1\, \langle\!\langle \psi \rangle\!\rangle]\, \mathbf{?} \{\ell_i \,.\, \check{L}_{i,1}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I_1} \sqcap r_1[x_1\, \langle\!\langle \psi \rangle\!\rangle]\, \mathbf{?} \{\ell_i \,.\, \check{L}_{i,2}\, \langle\!\langle \psi \rangle\!\rangle\}_{i \in I_2} && \text{(Step} \Rightarrow \text{Fig. VII.8.1)} \\
={}& r_1[x_1]\, \mathbf{?} \{\ell_i \,.\, \check{L}_{i,1}\}_{i \in I_1}\, \langle\!\langle \psi \rangle\!\rangle \sqcap r_1[x_1]\, \mathbf{?} \{\ell_i \,.\, \check{L}_{i,2}\}_{i \in I_2}\, \langle\!\langle \psi \rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& \check{L}_1\, \langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_2\, \langle\!\langle \psi \rangle\!\rangle && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{L}_1 = \texttt{foreach}\ R[\check{C}]\ \textbf{do}\ \check{L}\ \mathbf{;}\ \check{L}_{;,1}$ **and** $\check{L}_2 = \texttt{foreach}\ R[\check{C}]\ \textbf{do}\ \check{L}\ \mathbf{;}\ \check{L}_{;,2}$ **and**
  $\check{L}_1 \sqcap \check{L}_2 = \texttt{foreach}\ R[\check{C}]\ \textbf{do}\ \check{L}\ \mathbf{;}\ \check{L}_{;,1} \sqcap \check{L}_{;,2}$

Conclude:

$$\begin{aligned}
& (\check{L}_1 \sqcap \check{L}_2)\,\langle\!\langle \psi \rangle\!\rangle \\
={}& \mathtt{foreach}\ R[\check{C}]\ \mathtt{do}\ \check{L}\ \mathtt{;}\ \check{L}_{\mathtt{;},1} \sqcap \check{L}_{\mathtt{;},2}\,\langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
={}& \mathtt{foreach}\ R[\check{C}\,\langle\!\langle \psi \rangle\!\rangle]\ \mathtt{do}\ (\check{L}\,\langle\!\langle \psi \rangle\!\rangle)\ \mathtt{;}\ ((\check{L}_{\mathtt{;},1} \sqcap \check{L}_{\mathtt{;},2})\,\langle\!\langle \psi \rangle\!\rangle) && \text{(Fig. VII.7.3)} \\
={}& \mathtt{foreach}\ R[\check{C}\,\langle\!\langle \psi \rangle\!\rangle]\ \mathtt{do}\ (\check{L}\,\langle\!\langle \psi \rangle\!\rangle)\ \mathtt{;}\ (\check{L}_{\mathtt{;},1}\,\langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_{\mathtt{;},2}\,\langle\!\langle \psi \rangle\!\rangle) && \text{(Induction)} \\
={}& \mathtt{foreach}\ R[\check{C}\,\langle\!\langle \psi \rangle\!\rangle]\ \mathtt{do}\ (\check{L}\,\langle\!\langle \psi \rangle\!\rangle)\ \mathtt{;}\ (\check{L}_{\mathtt{;},1}\,\langle\!\langle \psi \rangle\!\rangle) \sqcap && \text{(Fig. VII.8.1)} \\
& \mathtt{foreach}\ R[\check{C}\,\langle\!\langle \psi \rangle\!\rangle]\ \mathtt{do}\ (\check{L}\,\langle\!\langle \psi \rangle\!\rangle)\ \mathtt{;}\ (\check{L}_{\mathtt{;},2}\,\langle\!\langle \psi \rangle\!\rangle) \\
={}& \mathtt{foreach}\ R[\check{C}]\ \mathtt{do}\ \check{L}\ \mathtt{;}\ \check{L}_{\mathtt{;},1}\,\langle\!\langle \psi \rangle\!\rangle \sqcap \mathtt{foreach}\ R[\check{C}]\ \mathtt{do}\ \check{L}\ \mathtt{;}\ \check{L}_{\mathtt{;},2}\,\langle\!\langle \psi \rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& \check{L}_1\,\langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_2\,\langle\!\langle \psi \rangle\!\rangle && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{L}_1 = \mathtt{rec}\ X\ \check{L}_{X,1}$ **and** $\check{L}_2 = \mathtt{rec}\ X\ \check{L}_{X,2}$ **and** $\check{L}_1 \sqcap \check{L}_2 = \mathtt{rec}\ X\ (\check{L}_{X,1} \sqcap \check{L}_{X,2})$

  Conclude:

$$\begin{aligned}
& (\check{L}_1 \sqcap \check{L}_2)\,\langle\!\langle \psi \rangle\!\rangle \\
={}& \mathtt{rec}\ X\ (\check{L}_{X,1} \sqcap \check{L}_{X,2})\,\langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
={}& \mathtt{rec}\ X\ ((\check{L}_{X,1} \sqcap \check{L}_{X,2})\,\langle\!\langle \psi \rangle\!\rangle) && \text{(Fig. VII.7.3)} \\
={}& \mathtt{rec}\ X\ (\check{L}_{X,1}\,\langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_{X,2}\,\langle\!\langle \psi \rangle\!\rangle) && \text{(Induction)} \\
={}& \mathtt{rec}\ X\ (\check{L}_{X,1}\,\langle\!\langle \psi \rangle\!\rangle) \sqcap \mathtt{rec}\ X\ (\check{L}_{X,2}\,\langle\!\langle \psi \rangle\!\rangle) && \text{(Fig. VII.8.1)} \\
={}& \mathtt{rec}\ X\ \check{L}_{X,1}\,\langle\!\langle \psi \rangle\!\rangle \sqcap \mathtt{rec}\ X\ \check{L}_{X,2}\,\langle\!\langle \psi \rangle\!\rangle && \text{(Fig. VII.7.3)} \\
={}& \check{L}_1\,\langle\!\langle \psi \rangle\!\rangle \sqcap \check{L}_2\,\langle\!\langle \psi \rangle\!\rangle && \text{(Step)}
\end{aligned}$$

QED.

VIII.40 Proof of Theorem VII.8.2

- **A1.** $\langle \hat{L}_1, \hat{L}_2 \rangle \in \operatorname{dom} \sqcap$

By induction on A1 (Fig. VII.8.1):

- **Base.** $\hat{L}_1 = \hat{L}_2 = X$ **and** $\hat{L}_1 \sqcap \hat{L}_2 = X$

  Conclude:

$$\begin{aligned}
& \llbracket \hat{L}_1 \sqcap \hat{L}_2 \rrbracket \\
={}& \llbracket X \rrbracket && \text{(Base)} \\
={}& X && \text{(Fig. VII.7.6)} \\
={}& X \sqcap X && \text{(Lem. VII.8.1:2)} \\
={}& \llbracket X \rrbracket \sqcap \llbracket X \rrbracket && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{L}_1 \rrbracket \sqcap \llbracket \hat{L}_2 \rrbracket && \text{(Base)}
\end{aligned}$$

- **Step.** $\hat{L}_1 = r_2[x_2]\,\mathtt{!}\{\ell_i\,\mathtt{.}\,\hat{L}_{i,1}\}_{i\in I}$ **and** $\hat{L}_2 = r_2[x_2]\,\mathtt{!}\{\ell_i\,\mathtt{.}\,\hat{L}_{i,2}\}_{i\in I}$ **and** $\hat{L}_1 \sqcap \hat{L}_2 = r_2[x_2]\,\mathtt{!}\{\ell_i\,\mathtt{.}\,\hat{L}_{i,1} \sqcap \hat{L}_{i,2}\}_{i\in I}$

Conclude:

$$
\begin{aligned}
& [\![\hat{L}_1 \sqcap \hat{L}_2]\!] \\
= \;& [\![r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,\hat{L}_{i,1} \sqcap \hat{L}_{i,2}\}_{i\in I}]\!] && \text{(Step)} \\
= \;& r_2[[\![x_2]\!]]\,\mathbf{!}\{\ell_i\,.\,[\![\hat{L}_{i,1} \sqcap \hat{L}_{i,2}]\!]\}_{i\in I} && \text{(Fig. VII.7.6)} \\
= \;& r_2[[\![x_2]\!]]\,\mathbf{!}\{\ell_i\,.\,[\![\hat{L}_{i,1}]\!] \sqcap [\![\hat{L}_{i,2}]\!]\}_{i\in I} && \text{(Induction)} \\
= \;& r_2[[\![x_2]\!]]\,\mathbf{!}\{\ell_i\,.\,[\![\hat{L}_{i,1}]\!]\}_{i\in I} \sqcap r_2[[\![x_2]\!]]\,\mathbf{!}\{\ell_i\,.\,[\![\hat{L}_{i,2}]\!]\}_{i\in I} && \text{(Fig. VII.8.1)} \\
= \;& [\![r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I}]\!] \sqcap [\![r_2[x_2]\,\mathbf{!}\{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I}]\!] && \text{(Fig. VII.7.6)} \\
= \;& [\![\hat{L}_1]\!] \sqcap [\![\hat{L}_2]\!] && \text{(Step)}
\end{aligned}
$$

- **Step.** $\hat{L}_1 = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I_1}$ **and** $\hat{L}_2 = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I_2}$ **and** $\hat{L}_1 \sqcap \hat{L}_2 = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I_1\setminus I_2} \cup \{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I_2\setminus I_1} \cup \{\ell_i\,.\,\hat{L}_{i,1} \sqcap \hat{L}_{i,2}\}_{i\in I_1\cap I_2}$ **and** $\Big[\ell_{i_1} \neq \ell_{i_2}$ **for-all** $i_1 \in I_1 \setminus I_2, i_2 \in I_2 \setminus I_1\Big]$

Conclude:

$$
\begin{aligned}
& [\![\hat{L}_1 \sqcap \hat{L}_2]\!] \\
= \;& [\![r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I_1\setminus I_2} \cup \{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I_2\setminus I_1} \cup \{\ell_i\,.\,\hat{L}_{i,1} \sqcap \hat{L}_{i,2}\}_{i\in I_1\cap I_2}]\!] && \text{(Step)} \\
= \;& r_1[[\![x_1]\!]]\,\mathbf{?}\{\ell_i\,.\,[\![\hat{L}_{i,1}]\!]\}_{i\in I_1\setminus I_2} \cup \{\ell_i\,.\,[\![\hat{L}_{i,2}]\!]\}_{i\in I_2\setminus I_1} \cup \{\ell_i\,.\,[\![\hat{L}_{i,1} \sqcap \hat{L}_{i,2}]\!]\}_{i\in I_1\cap I_2} && \text{(Fig. VII.7.6)} \\
= \;& r_1[[\![x_1]\!]]\,\mathbf{?}\{\ell_i\,.\,[\![\hat{L}_{i,1}]\!]\}_{i\in I_1\setminus I_2} \cup \{\ell_i\,.\,[\![\hat{L}_{i,2}]\!]\}_{i\in I_2\setminus I_1} \cup \{\ell_i\,.\,[\![\hat{L}_{i,1}]\!] \sqcap [\![\hat{L}_{i,2}]\!]\}_{i\in I_1\cap I_2} && \text{(Induction)} \\
= \;& r_1[[\![x_1]\!]]\,\mathbf{?}\{\ell_i\,.\,[\![\hat{L}_{i,1}]\!]\}_{i\in I_1} \sqcap r_1[[\![x_1]\!]]\,\mathbf{?}\{\ell_i\,.\,[\![\hat{L}_{i,2}]\!]\}_{i\in I_2} && \text{(Step} \Rightarrow \text{Fig. VII.8.1)} \\
= \;& [\![r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I_1}]\!] \sqcap [\![r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I_2}]\!] && \text{(Fig. VII.7.6)} \\
= \;& [\![\hat{L}_1]\!] \sqcap [\![\hat{L}_2]\!] && \text{(Step)}
\end{aligned}
$$

- **Step.** $\hat{L}_1 = \texttt{foreach}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \textbf{;}\ \hat{L}_{\mathbf{;},1}$ **and** $\hat{L}_2 = \texttt{foreach}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \textbf{;}\ \hat{L}_{\mathbf{;},2}$ **and** $\hat{L}_1 \sqcap \hat{L}_2 = \texttt{foreach}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \textbf{;}\ \hat{L}_{\mathbf{;},1} \sqcap \hat{L}_{\mathbf{;},2}$

  - **B1.** Conclude:

$$
\begin{aligned}
& \langle [\![\hat{L}]\!], [\![\hat{L}_{\mathbf{;},1}]\!], R, [\![\hat{C}]\!] \rangle \in \operatorname{dom} \mathsf{iter} \\
\textbf{impl.}\;\; & [\![\hat{C}]\!] \in \operatorname{dom} \mathsf{len} && \text{(Fig. VII.6.2)}
\end{aligned}
$$

Conclude:

$$
\begin{aligned}
& [\![\hat{L}_1 \sqcap \hat{L}_2]\!] \\
= \;& [\![\texttt{foreach}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \textbf{;}\ \hat{L}_{\mathbf{;},1} \sqcap \hat{L}_{\mathbf{;},2}]\!] && \text{(Step)} \\
= \;& \mathsf{iter}([\![\hat{L}]\!], [\![\hat{L}_{\mathbf{;},1} \sqcap \hat{L}_{\mathbf{;},2}]\!], R, [\![\hat{C}]\!]) && \text{(Fig. VII.7.6)} \\
= \;& \mathsf{iter}([\![\hat{L}]\!], [\![\hat{L}_{\mathbf{;},1}]\!] \sqcap [\![\hat{L}_{\mathbf{;},2}]\!], R, [\![\hat{C}]\!]) && \text{(Step)} \\
= \;& \mathsf{iter}([\![\hat{L}]\!], [\![\hat{L}_{\mathbf{;},1}]\!], R, [\![\hat{C}]\!]) \sqcap \mathsf{iter}([\![\hat{L}]\!], [\![\hat{L}_{\mathbf{;},2}]\!], R, [\![\hat{C}]\!]) && \text{(B1} \Rightarrow \text{Thm. VII.6.10:2)} \\
= \;& [\![\texttt{foreach}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \textbf{;}\ \hat{L}_{\mathbf{;},1}]\!] \sqcap [\![\texttt{foreach}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \textbf{;}\ \hat{L}_{\mathbf{;},2}]\!] && \text{(Fig. VII.7.6)} \\
= \;& [\![\hat{L}_1]\!] \sqcap [\![\hat{L}_2]\!] && \text{(Step)}
\end{aligned}
$$

- **Step.** $\hat{L}_1 = \texttt{rec}\ X\ \hat{L}_{X,1}$ **and** $\hat{L}_2 = \texttt{rec}\ X\ \hat{L}_{X,2}$ **and** $\hat{L}_1 \sqcap \hat{L}_2 = \texttt{rec}\ X\ (\hat{L}_{X,1} \sqcap \hat{L}_{X,2})$

Conclude:

$$\begin{aligned}
& \llbracket \hat{L}_1 \sqcap \hat{L}_2 \rrbracket && \\
={} & \llbracket \mathtt{\textbf{rec}}\ X\ (\hat{L}_{X,1} \sqcap \hat{L}_{X,2}) \rrbracket && \text{(Step)} \\
={} & \mathtt{\textbf{rec}}\ X\ \llbracket \hat{L}_{X,1} \sqcap \hat{L}_{X,2} \rrbracket && \text{(Fig. VII.7.6)} \\
={} & \mathtt{\textbf{rec}}\ X\ (\llbracket \hat{L}_{X,1} \rrbracket \sqcap \llbracket \hat{L}_{X,2} \rrbracket) && \text{(Induction)} \\
={} & \mathtt{\textbf{rec}}\ X\ \llbracket \hat{L}_{X,1} \rrbracket \sqcap \mathtt{\textbf{rec}}\ X\ \llbracket \hat{L}_{X,2} \rrbracket && \text{(Fig. VII.8.1)} \\
={} & \llbracket \mathtt{\textbf{rec}}\ X\ \hat{L}_{X,1} \rrbracket \sqcap \llbracket \mathtt{\textbf{rec}}\ X\ \hat{L}_{X,2} \rrbracket && \text{(Fig. VII.7.6)} \\
={} & \llbracket \hat{L}_1 \rrbracket \sqcap \llbracket \hat{L}_2 \rrbracket && \text{(Step)}
\end{aligned}$$

QED.

VIII.41 Proof of Theorem VII.8.3

- **A1.** $\langle \hat{L}_1, \hat{L}_2 \rangle \in \operatorname{dom} \sqcap$
- **A2.** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1)$
- **A3.** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_2)$

By induction on A1 (Fig. VII.8.1):

- **Base.** $\hat{L}_1 = \hat{L}_2 = X$ **and** $\hat{L}_1 \sqcap \hat{L}_2 = X$

  Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1) && \text{(A2)} \\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(X) && \text{(Base)} \\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1 \sqcap \hat{L}_2) && \text{(Base)}
\end{aligned}$$

- **Step.** $\hat{L}_1 = r_2[x_2]\,\mathbf{!}\,\{\ell_i\ .\ \hat{L}_{i,1}\}_{i \in I}$ **and** $\hat{L}_2 = r_2[x_2]\,\mathbf{!}\,\{\ell_i\ .\ \hat{L}_{i,2}\}_{i \in I}$ **and** $\hat{L}_1 \sqcap \hat{L}_2 = r_2[x_2]\,\mathbf{!}\,\{\ell_i\ .\ \hat{L}_{i,1} \sqcap \hat{L}_{i,2}\}_{i \in I}$

  - **B1.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1)\ \textsf{\textbf{and}}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_2) && \text{(A2, A3)} \\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,\mathbf{!}\,\{\ell_i\ .\ \hat{L}_{i,1}\}_{i \in I})\ \textsf{\textbf{and}}\ \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,\mathbf{!}\,\{\ell_i\ .\ \hat{L}_{i,2}\}_{i \in I}) && \text{(Step)} \\
\textsf{\textbf{impl.}}\ & \Big[r_2 \in \operatorname{dom} f\ \textsf{\textbf{impl.}}\ x_2 \in f(r_2)\Big]\ \textsf{\textbf{and}} && \text{(Fig. VII.7.4)} \\
& \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1})\ \textsf{\textbf{for-all}}\ i \in I\Big]\ \textsf{\textbf{and}}\ \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1})\ \textsf{\textbf{for-all}}\ i \in I\Big] &&
\end{aligned}$$

  Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1} \sqcap \hat{L}_{i,2})\ \textsf{\textbf{for-all}}\ i \in I && \text{(Step, B1} \Rightarrow \text{Induction)} \\
\textsf{\textbf{impl.}}\ & \Big[r_2 \in \operatorname{dom} f\ \textsf{\textbf{impl.}}\ x_2 \in f(r_2)\Big]\ \textsf{\textbf{and}}\ \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1} \sqcap \hat{L}_{i,2})\ \textsf{\textbf{for-all}}\ i \in I\Big] && \text{(B1)} \\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(r_2[x_2]\,\mathbf{!}\,\{\ell_i\ .\ \hat{L}_{i,1} \sqcap \hat{L}_{i,2}\}_{i \in I}) && \text{(Fig. VII.7.4)} \\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1 \sqcap \hat{L}_2) && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{L}_1 = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I_1}$ **and** $\hat{L}_2 = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I_2}$ **and** $\hat{L}_1 \sqcap \hat{L}_2 = r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I_1\setminus I_2} \cup \{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I_2\setminus I_1} \cup \{\ell_i\,.\,\hat{L}_{i,1}\sqcap\hat{L}_{i,2}\}_{i\in I_1\cap I_2}$ **and** $\Big[\ell_{i_1}\neq\ell_{i_2}\ \textbf{for-all}\ i_1\in I_1\setminus I_2, i_2\in I_2\setminus I_1\Big]$

  - **C1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1)\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_2) & \text{(A2, A3)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I})\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I}) & \text{(Step)}\\
\textbf{impl.} & \Big[r_1\in\operatorname{dom} f\ \textbf{impl.}\ x_1\in f(r_1)\Big]\ \textbf{and} & \text{(Fig. VII.7.4)}\\
 & \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1})\ \textbf{for-all}\ i\in I_1\Big]\ \textbf{and}\ \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1})\ \textbf{for-all}\ i\in I_2\Big] &
\end{array}$$

  Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1}\sqcap\hat{L}_{i,2})\ \textbf{for-all}\ i\in I_1\cap I_2 & \text{(Step, C1}\Rightarrow\text{Induction)}\\
\textbf{impl.} & \Big[r_1\in\operatorname{dom} f\ \textbf{impl.}\ x_1\in f(r_1)\Big]\ \textbf{and} & \text{(C1)}\\
 & \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1})\ \textbf{for-all}\ i\in I_1\setminus I_2\Big]\ \textbf{and}\ \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1})\ \textbf{for-all}\ i\in I_2\setminus I_1\Big]\ \textbf{and} & \\
 & \Big[\mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{i,1}\sqcap\hat{L}_{i,2})\ \textbf{for-all}\ i\in I_1\cap I_2\Big] & \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1]\,\mathbf{?}\{\ell_i\,.\,\hat{L}_{i,1}\}_{i\in I_1\setminus I_2}\cup\{\ell_i\,.\,\hat{L}_{i,2}\}_{i\in I_2\setminus I_1}\cup\{\ell_i\,.\,\hat{L}_{i,1}\sqcap\hat{L}_{i,2}\}_{i\in I_1\cap I_2}) & \text{(Fig. VII.7.4)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1\sqcap\hat{L}_2) & \text{(Step)}
\end{array}$$

- **Step.** $\hat{L}_1 = \mathtt{\textbf{foreach}}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \mathbf{;}\ \hat{L}_{\mathbf{;},1}$ **and** $\hat{L}_2 = \mathtt{\textbf{foreach}}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \mathbf{;}\ \hat{L}_{\mathbf{;},2}$ **and** $\hat{L}_1\sqcap\hat{L}_2 = \mathtt{\textbf{foreach}}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \mathbf{;}\ \hat{L}_{\mathbf{;},1}\sqcap\hat{L}_{\mathbf{;},2}$

  - **D1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1)\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_2) & \text{(A2, A3)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\textbf{foreach}}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \mathbf{;}\ \hat{L}_{\mathbf{;},1})\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\textbf{foreach}}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \mathbf{;}\ \hat{L}_{\mathbf{;},2}) & \text{(Step)}\\
\textbf{impl.} & f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\}:\mathbb{R}\rightharpoonup 2^{\mathbb{Z}}\ \textbf{and}\ \hat{C}\in\checkmark\ \textbf{and} & \text{(Fig. VII.7.4)}\\
 & \operatorname{expr}\hat{L}\cap\mathbb{G}_{\mathtt{rec}}=\emptyset\ \textbf{and}\ \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\mathtt{cont}\}}(\hat{L}) & \\
 & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{\mathbf{;},1})\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{\mathbf{;},2}) &
\end{array}$$

  Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{\mathbf{;},1}\sqcap\hat{L}_{\mathbf{;},2}) & \text{(Step, D1}\Rightarrow\text{Induction)}\\
\textbf{impl.} & f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\}:\mathbb{R}\rightharpoonup 2^{\mathbb{Z}}\ \textbf{and}\ \hat{C}\in\checkmark\ \textbf{and} & \text{(D1)}\\
 & \operatorname{expr}\hat{L}\cap\mathbb{G}_{\mathtt{rec}}=\emptyset\ \textbf{and}\ \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\{\mathtt{cont}\}}(\hat{L})\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_{\mathbf{;},1}\sqcap\hat{L}_{\mathbf{;},2}) & \\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\textbf{foreach}}\ R[\hat{C}]\ \textbf{do}\ \hat{L}\ \mathbf{;}\ \hat{L}_{\mathbf{;},1}\sqcap\hat{L}_{\mathbf{;},2}) & \text{(Fig. VII.7.4)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1\sqcap\hat{L}_2) & \text{(Step)}
\end{array}$$

- **Step.** $\hat{L}_1 = \mathtt{\textbf{rec}}\ X\ \hat{L}_{X,1}$ **and** $\hat{L}_2 = \mathtt{\textbf{rec}}\ X\ \hat{L}_{X,2}$ **and** $\hat{L}_1\sqcap\hat{L}_2 = \mathtt{\textbf{rec}}\ X\ (\hat{L}_{X,1}\sqcap\hat{L}_{X,2})$

  - **E1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1)\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_2) & \text{(A2, A3)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\textbf{rec}}\ X\ \hat{L}_{X,1})\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\textbf{rec}}\ X\ \hat{L}_{X,2}) & \text{(Step)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{L}_{X,1})\ \textbf{and}\ \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{L}_{X,2}) & \text{(Fig. VII.7.4)}
\end{array}$$

Conclude:

$$\begin{array}{rll} & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{L}_{X,1} \sqcap \hat{L}_{X,2}) & \text{(Step, E1} \Rightarrow \text{Induction)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{rec}\ X\ (\hat{L}_{X,1} \sqcap \hat{L}_{X,2})) & \text{(Fig. VII.7.4)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{L}_1 \sqcap \hat{L}_2) & \text{(Step)} \end{array}$$

QED.

VIII.42 Proof of Theorem VII.8.4

- **A1.** $\langle \check{G}, R[\check{C}], r[z] \rangle \in \mathrm{dom} \upharpoonright$
- **A2.** $\texttt{self} \notin \mathrm{dom}\, \psi$

By induction on A1 (Fig. VII.8.2c):

- **Base.** $\check{G} = X$ **and** $\check{G} \upharpoonright_{R[\check{C}]} r[z] = X$

  Conclude:

  $$\begin{array}{rll} & (\check{G} \upharpoonright_{R[\check{C}]} r[z])\, \langle\!\langle \psi \rangle\!\rangle & \\ = & X\, \langle\!\langle \psi \rangle\!\rangle & \text{(Step)} \\ = & X & \text{(Fig. VII.7.3)} \\ = & X \upharpoonright_{R[\check{C}\, \langle\!\langle \psi \rangle\!\rangle]} r[z] & \text{(Fig. VII.8.2c)} \\ = & X\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C}\, \langle\!\langle \psi \rangle\!\rangle]} r[z] & \text{(Fig. VII.7.3)} \\ = & \check{G}\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C}\, \langle\!\langle \psi \rangle\!\rangle]} r[z] & \text{(Step)} \end{array}$$

- **Step.** $\check{G} = r_1[x_1] \rightarrow r_2[x_2]\, \mathbf{:} \{\ell_i\, .\, \check{G}_i\}_{i \in I}$ **and**
  $\check{G} \upharpoonright_{R[\check{C}]} r[z] = r_2[\texttt{self}\texttt{+}\Delta(\check{C})(x_1, x_2)]\, \mathbf{!} \{\ell_i\, .\, \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] = r[z] \neq r_2[x_2]$ **and** $r_2 \in R$ **and** $\{x_1, x_2\} \subseteq \mathsf{vars}(\check{C})$

  - **B1.** Conclude:

    $$\begin{array}{rll} & r_1[x_1] = r[z] & \text{(Step)} \\ \textbf{impl.} & r_1 = r\ \textbf{and}\ x_1 = z & \text{(–)} \end{array}$$

  - **B2.** Conclude:

    $$\begin{array}{rll} & z\, \langle\!\langle \psi \rangle\!\rangle = z & \text{(Fig. VII.3.3)} \\ \textbf{impl.} & x_1\, \langle\!\langle \psi \rangle\!\rangle = x_1 & \text{(B1)} \end{array}$$

  - **B3.** Conclude:

    $$\begin{array}{rll} & \{x_1, x_2\} \subseteq \mathsf{vars}(\check{C}) & \text{(Step)} \\ \textbf{impl.} & x_2 \in \mathsf{vars}(\check{C}) & \text{(–)} \\ \textbf{impl.} & x_2 \in \mathbb{Z} & \text{(Lem. VII.3.4)} \\ \textbf{impl.} & x_2\, \langle\!\langle \psi \rangle\!\rangle = x_2 & \text{(Fig. VII.3.3)} \end{array}$$

Conclude:

$$\begin{aligned}
&(\check{G} \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle \psi \rangle\!\rangle \\
=\ & r_2[\texttt{\textbf{self}}\texttt{+}\Delta(\check{C})(x_1,x_2)] \,\mathbf{!}\{\ell_i \,\mathbf{.}\, \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i\in I} \langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
=\ & r_2[\texttt{\textbf{self}}\texttt{+}\Delta(\check{C})(x_1,x_2) \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{!}\{\ell_i \,\mathbf{.}\, (\check{G}_i \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle \psi \rangle\!\rangle\}_{i\in I} && \text{(Fig. VII.7.3)} \\
=\ & r_2[\texttt{\textbf{self}}\texttt{+}\Delta(\check{C})(x_1,x_2) \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{!}\{\ell_i \,\mathbf{.}\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i\in I} && \text{(A2} \Rightarrow \text{Induction)} \\
=\ & r_2[(\texttt{\textbf{self}} \langle\!\langle \psi \rangle\!\rangle)\texttt{+}(\Delta(\check{C})(x_1,x_2) \langle\!\langle \psi \rangle\!\rangle)] \,\mathbf{!}\{\ell_i \,\mathbf{.}\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i\in I} && \text{(Fig. VII.3.3)} \\
=\ & r_2[\texttt{\textbf{self}}\texttt{+}(\Delta(\check{C})(x_1,x_2) \langle\!\langle \psi \rangle\!\rangle)] \,\mathbf{!}\{\ell_i \,\mathbf{.}\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i\in I} && \text{(A2} \Rightarrow \text{Fig. VII.3.3)} \\
=\ & r_2[\texttt{\textbf{self}}\texttt{+}(\Delta(\check{C} \langle\!\langle \psi \rangle\!\rangle)(x_1,x_2))] \,\mathbf{!}\{\ell_i \,\mathbf{.}\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i\in I} && \text{(Thm. VII.3.4)} \\
=\ & r_1[x_1] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\{\ell_i \,\mathbf{.}\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle\}_{i\in I} \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Step} \Rightarrow \text{Fig. VII.8.2c)} \\
=\ & r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] \rightarrowtriangle r_2[x_2 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{:}\{\ell_i \,\mathbf{.}\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle\}_{i\in I} \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(B2, B3)} \\
=\ & r_1[x_1] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\{\ell_i \,\mathbf{.}\, \check{G}_i\}_{i\in I} \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Fig. VII.7.3)} \\
=\ & \check{G} \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{G} = r_1[x_1] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\{\ell_i \,\mathbf{.}\, \check{G}_i\}_{i\in I}$ **and**
  $\check{G} \upharpoonright_{R[\check{C}]} r[z] = r_2[x_2] \,\mathbf{!}\{\ell_i \,\mathbf{.}\, \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i\in I}$ **and**
  $r_1[x_1] = r[z] \neq r_2[x_2]$ **and** $\Big[r_2 \notin R$ **or** $\{x_1, x_2\} \not\subseteq \mathsf{vars}(\check{C})\Big]$

  - **C1.** Conclude:

    $$\begin{aligned}
    & r[z] = r_2[x_2 \langle\!\langle \psi \rangle\!\rangle] \\
    \textbf{impl.}\ & r = r_2 \ \textbf{and}\ z = x_2 \langle\!\langle \psi \rangle\!\rangle && (-) \\
    \textbf{impl.}\ & r = r_2 \ \textbf{and}\ z = x_2 && \text{(Fig. VII.3.3)} \\
    \textbf{impl.}\ & r[z] = r_2[x_2] && (-) \\
    \textbf{impl.}\ & \textbf{false} && \text{(Step)}
    \end{aligned}$$

  - **C2.** Conclude:

    $$\begin{aligned}
    & \Big[r_2 \notin R \ \textbf{or}\ \{x_1, x_2\} \not\subseteq \mathsf{vars}(\check{C})\Big] && \text{(Step)} \\
    \textbf{impl.}\ & \Big[r_2 \notin R \ \textbf{or}\ \{x_1, x_2 \langle\!\langle \psi \rangle\!\rangle\} \not\subseteq \mathsf{vars}(\check{C})\Big] && \text{(Fig. VII.3.3)}
    \end{aligned}$$

  - **C3.** Conclude:

    $$\begin{aligned}
    & r_1[x_1] = r[z] && \text{(Step)} \\
    \textbf{impl.}\ & r_1 = r \ \textbf{and}\ x_1 = z && (-)
    \end{aligned}$$

  - **C4.** Conclude:

    $$\begin{aligned}
    & z \langle\!\langle \psi \rangle\!\rangle = z && \text{(Fig. VII.3.3)} \\
    \textbf{impl.}\ & x_1 \langle\!\langle \psi \rangle\!\rangle = x_1 && \text{(C3)}
    \end{aligned}$$

Conclude:

$$\begin{aligned}
&(\check{G} \restriction_{R[\check{C}]} r[z]) \langle\!\langle \psi \rangle\!\rangle \\
={}& r_2[x_2] \,\mathbf{!}\, \{\ell_i \,.\, \check{G}_i \restriction_{R[\check{C}]} r[z]\}_{i \in I} \langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
={}& r_2[x_2 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{!}\, \{\ell_i \,.\, (\check{G}_i \restriction_{R[\check{C}]} r[z]) \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} && \text{(Fig. VII.7.3)} \\
={}& r_2[x_2 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{!}\, \{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i \in I} && \text{(A2} \Rightarrow \text{Induction)} \\
={}& r_1[x_1] \rightarrow r_2[x_2 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Step, C1, C2} \Rightarrow \text{Fig. VII.8.2c)} \\
={}& r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] \rightarrow r_2[x_2 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(C4)} \\
={}& r_1[x_1] \rightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I} \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Fig. VII.7.3)} \\
={}& \check{G} \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{G} = r_1[x_1] \rightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I}$ **and**
  $\check{G} \restriction_{R[\check{C}]} r[z] = r_1[\mathtt{self}+\Delta(\check{C})(x_2, x_1)] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \restriction_{R[\check{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] \neq r[z] = r_2[x_2]$ **and** $r_1 \in R$ **and** $\{x_2, x_1\} \subseteq \mathsf{vars}(\check{C})$

  - **D1.** Conclude:

    $$\begin{aligned}
    & r[z] = r_2[x_2] && \text{(Step)} \\
    \textbf{impl. }& r = r_2 \textbf{ and } z = x_2 && (-)
    \end{aligned}$$

  - **D2.** Conclude:

    $$\begin{aligned}
    & z \langle\!\langle \psi \rangle\!\rangle = z && \text{(Fig. VII.3.3)} \\
    \textbf{impl. }& x_2 \langle\!\langle \psi \rangle\!\rangle = x_2 && \text{(D1)}
    \end{aligned}$$

  - **D3.** Conclude:

    $$\begin{aligned}
    & \{x_1, x_2\} \subseteq \mathsf{vars}(\check{C}) && \text{(Step)} \\
    \textbf{impl. }& x_1 \in \mathsf{vars}(\check{C}) && (-) \\
    \textbf{impl. }& x_1 \in \mathbb{Z} && \text{(Lem. VII.3.4)} \\
    \textbf{impl. }& x_1 \langle\!\langle \psi \rangle\!\rangle = x_1 && \text{(Fig. VII.3.3)}
    \end{aligned}$$

Conclude:

$$\begin{aligned}
&(\check{G} \restriction_{R[\check{C}]} r[z]) \langle\!\langle \psi \rangle\!\rangle \\
={}& r_1[\mathtt{self}+\Delta(\check{C})(x_2, x_1)] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \restriction_{R[\check{C}]} r[z]\}_{i \in I} \langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
={}& r_1[\mathtt{self}+\Delta(\check{C})(x_2, x_1) \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{?}\{\ell_i \,.\, (\check{G}_i \restriction_{R[\check{C}]} r[z]) \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} && \text{(Fig. VII.7.3)} \\
={}& r_1[\mathtt{self}+\Delta(\check{C})(x_2, x_1) \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i \in I} && \text{(A2} \Rightarrow \text{Induction)} \\
={}& r_1[(\mathtt{self} \langle\!\langle \psi \rangle\!\rangle)+(\Delta(\check{C})(x_2, x_1) \langle\!\langle \psi \rangle\!\rangle)] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i \in I} && \text{(Fig. VII.3.3)} \\
={}& r_1[\mathtt{self}+(\Delta(\check{C})(x_2, x_1) \langle\!\langle \psi \rangle\!\rangle)] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i \in I} && \text{(A2} \Rightarrow \text{Fig. VII.3.3)} \\
={}& r_1[\mathtt{self}+(\Delta(\check{C} \langle\!\langle \psi \rangle\!\rangle)(x_2, x_1))] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i \in I} && \text{(Thm. VII.3.4)} \\
={}& r_1[x_1] \rightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Step} \Rightarrow \text{Fig. VII.8.2c)} \\
={}& r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] \rightarrow r_2[x_2 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(D2, D3)} \\
={}& r_1[x_1] \rightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I} \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Fig. VII.7.3)} \\
={}& \check{G} \langle\!\langle \psi \rangle\!\rangle \restriction_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{G} = r_1[x_1] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I}$ **and**
  $\check{G} \upharpoonright_{R[\check{C}]} r[z] = r_1[x_1] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] \neq r[z] = r_2[x_2]$ **and** $\Big[r_1 \notin R$ **or** $\{x_2, x_1\} \not\subseteq \mathsf{vars}(\check{C})\Big]$

  - **E1.** Conclude:

    $$\begin{array}{lll} & r[z] = r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] & \\ \textbf{impl.} & r = r_1 \textbf{ and } z = x_1 \langle\!\langle \psi \rangle\!\rangle & (-) \\ \textbf{impl.} & r = r_1 \textbf{ and } z = x_1 & (\text{Fig. VII.3.3}) \\ \textbf{impl.} & r[z] = r_1[x_1] & (-) \\ \textbf{impl.} & \textbf{false} & (\text{Step}) \end{array}$$

  - **E2.** Conclude:

    $$\begin{array}{lll} & \Big[r_1 \notin R \textbf{ or } \{x_1, x_2\} \not\subseteq \mathsf{vars}(\check{C})\Big] & (\text{Step}) \\ \textbf{impl.} & \Big[r_1 \notin R \textbf{ or } \{x_1 \langle\!\langle \psi \rangle\!\rangle, x_2\} \not\subseteq \mathsf{vars}(\check{C})\Big] & (\text{Fig. VII.3.3}) \end{array}$$

  - **E3.** Conclude:

    $$\begin{array}{lll} & r[z] = r_2[x_2] & (\text{Step}) \\ \textbf{impl.} & r = r_2 \textbf{ and } z = x_2 & (-) \end{array}$$

  - **E4.** Conclude:

    $$\begin{array}{lll} & z \langle\!\langle \psi \rangle\!\rangle = z & (\text{Fig. VII.3.3}) \\ \textbf{impl.} & x_2 \langle\!\langle \psi \rangle\!\rangle = x_2 & (\text{E3}) \end{array}$$

  Conclude:

  $$\begin{array}{lll} & (\check{G} \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle \psi \rangle\!\rangle & \\ = & r_1[x_1] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i \in I} \langle\!\langle \psi \rangle\!\rangle & (\text{Step}) \\ = & r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{?}\{\ell_i \,.\, (\check{G}_i \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} & (\text{Fig. VII.7.3}) \\ = & r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z]\}_{i \in I} & (\text{A2} \Rightarrow \text{Induction}) \\ = & r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] & (\text{Step, E1, E2} \Rightarrow \text{Fig. VII.8.2c}) \\ = & r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] \rightarrowtriangle r_2[x_2 \langle\!\langle \psi \rangle\!\rangle] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] & (\text{E4}) \\ = & r_1[x_1] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I} \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] & (\text{Fig. VII.7.3}) \\ = & \check{G} \langle\!\langle \psi \rangle\!\rangle \upharpoonright_{R[\check{C} \langle\!\langle \psi \rangle\!\rangle]} r[z] & (\text{Step}) \end{array}$$

- **Step.** $\check{G} = r_1[x_1] \rightarrowtriangle r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I}$ **and**
  $\check{G} \upharpoonright_{R[\check{C}]} r[z] = \bigsqcap\{\check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i \in I}$ **and** $r_1[x_1] \neq r[z] \neq r_2[x_2]$

  - **F1.** Conclude:

    $$\begin{array}{lll} & r[z] = r_1[x_1 \langle\!\langle \psi \rangle\!\rangle] & \\ \textbf{impl.} & r = r_1 \textbf{ and } z = x_1 \langle\!\langle \psi \rangle\!\rangle & (-) \\ \textbf{impl.} & r = r_1 \textbf{ and } z = x_1 & (\text{Fig. VII.3.3}) \\ \textbf{impl.} & r[z] = r_1[x_1] & (-) \\ \textbf{impl.} & \textbf{false} & (\text{Step}) \end{array}$$

- **F2.** Conclude:

  $r[z] = r_2[x_2 \langle\!\langle\psi\rangle\!\rangle]$

  impl. $r = r_2$ **and** $z = x_2 \langle\!\langle\psi\rangle\!\rangle$ (–)

  impl. $r = r_2$ **and** $z = x_2$ (Fig. VII.3.3)

  impl. $r[z] = r_2[x_2]$ (–)

  impl. **false** (Step)

Conclude:

$(\check{G} \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle$

$= \bigsqcap\{\check{G}_i \upharpoonright_{R[\check{C}]} r[z]\}_{i\in I} \langle\!\langle\psi\rangle\!\rangle$ (Step)

$= \bigsqcap\{(\check{G}_i \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle\}_{i\in I}$ (Thm. VII.8.1)

$= \bigsqcap\{\check{G}_i \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]\}_{i\in I}$ (A2 ⇒ Induction)

$= r_1[x_1 \langle\!\langle\psi\rangle\!\rangle] \rightarrowtriangle r_2[x_2 \langle\!\langle\psi\rangle\!\rangle] \mathbin{\boldsymbol{:}} \{\ell_i \mathbin{\boldsymbol{.}} \check{G}_i \langle\!\langle\psi\rangle\!\rangle\}_{i\in I} \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (F1, F2 ⇒ Fig. VII.8.2c)

$= r_1[x_1] \rightarrowtriangle r_2[x_2] \mathbin{\boldsymbol{:}} \{\ell_i \mathbin{\boldsymbol{.}} \check{G}_i\}_{i\in I} \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (Fig. VII.7.3)

$= \check{G} \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (Step)

- **Step.** $\check{G} = \texttt{foreach}\ R'[\check{C}']\ \textbf{do}\ \check{G}_1 \mathbin{\boldsymbol{;}} \check{G}_2$ **and**
  $\check{G} \upharpoonright_{R[\check{C}]} r[z] = \texttt{foreach}\ R'[\check{C}']\ \textbf{do}\ (\check{G}_1 \upharpoonright_{R[\check{C}]} r[z]) \mathbin{\boldsymbol{;}} (\check{G}_2 \upharpoonright_{R[\check{C}]} r[z])$

Conclude:

$(\check{G} \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle$

$= \texttt{foreach}\ R'[\check{C}']\ \textbf{do}\ (\check{G}_1 \upharpoonright_{R[\check{C}]} r[z]) \mathbin{\boldsymbol{;}} (\check{G}_2 \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle$ (Step)

$= \texttt{foreach}\ R'[\check{C}' \langle\!\langle\psi\rangle\!\rangle]\ \textbf{do}\ ((\check{G}_1 \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle) \mathbin{\boldsymbol{;}} ((\check{G}_2 \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle)$ (Fig. VII.7.3)

$= \texttt{foreach}\ R'[\check{C}' \langle\!\langle\psi\rangle\!\rangle]\ \textbf{do}$ (A2 ⇒ Induction)
$\quad (\check{G}_1 \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]) \mathbin{\boldsymbol{;}} (\check{G}_2 \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z])$

$= \texttt{foreach}\ R'[\check{C}' \langle\!\langle\psi\rangle\!\rangle]\ \textbf{do}\ (\check{G}_1 \langle\!\langle\psi\rangle\!\rangle) \mathbin{\boldsymbol{;}} (\check{G}_2 \langle\!\langle\psi\rangle\!\rangle) \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (Fig. VII.8.2c)

$= \texttt{foreach}\ R'[\check{C}']\ \textbf{do}\ \check{G}_1 \mathbin{\boldsymbol{;}} \check{G}_2 \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (Fig. VII.7.3)

$= \check{G} \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (Step)

- **Step.** $\check{G} = \texttt{rec}\ X\ \check{G}_X$ **and** $\check{G} \upharpoonright_{R[\check{C}]} r[z] = \texttt{rec}\ X\ (\check{G}_X \upharpoonright_{R[\check{C}]} r[z])$

Conclude:

$(\check{G} \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle$

$= \texttt{rec}\ X\ (\check{G}_X \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle$ (Step)

$= \texttt{rec}\ X\ ((\check{G}_X \upharpoonright_{R[\check{C}]} r[z]) \langle\!\langle\psi\rangle\!\rangle)$ (Fig. VII.7.3)

$= \texttt{rec}\ X\ (\check{G}_X \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z])$ (A2 ⇒ Induction)

$= \texttt{rec}\ X\ (\check{G}_X \langle\!\langle\psi\rangle\!\rangle) \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (Fig. VII.8.2c)

$= \texttt{rec}\ X\ \check{G}_X \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (Fig. VII.7.3)

$= \check{G} \langle\!\langle\psi\rangle\!\rangle \upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]$ (Step)

QED.

VIII.43 Proof of Theorem VII.8.5

- **A1.** $\langle \hat{G}, R[\hat{C}], r[z] \rangle \in \mathrm{dom} \restriction$
- **A2.** $\mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G})$
- **A3.** $f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}}$
- **B1.** Conclude:

$$\begin{array}{lll} & f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} & \text{(A3)} \\ \textsf{impl.} & (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(\tilde{r}) \in 2^{\mathbb{Z}} \textsf{ for-all } \tilde{r} \in \mathrm{dom}\,(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) & \text{(–)} \end{array}$$

By induction on A1 (Fig. VII.8.2c):

- **Base.** $\hat{G} = X$ **and** $\hat{G} \restriction_{R[\hat{C}]} r[z] = X$

  Conclude:

$$\begin{array}{lll} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) & \text{(A2)} \\ \textsf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(X) & \text{(Base)} \\ \textsf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(X \,\langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) & \text{(Fig. VII.7.3)} \\ \textsf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}((\hat{G} \restriction_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) & \text{(Base)} \end{array}$$

- **Step.** $\hat{G} = r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}$ **and**
  $\hat{G} \restriction_{R[\hat{C}]} r[z] = r_2[\texttt{self}{+}\Delta(\hat{C})(x_1, x_2)] \,!\, \{\ell_i \,.\, \hat{G}_i \restriction_{R[\hat{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] = r[z] \neq r_2[x_2]$ **and** $r_2 \in R$ **and** $\{x_1, x_2\} \subseteq \mathsf{vars}(\hat{C})$

  - **C1.** Conclude:

$$\begin{array}{lll} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) & \text{(A2)} \\ \textsf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(r_1[x_1] \twoheadrightarrow r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}) & \text{(Step)} \\ \textsf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \textsf{ for-all } i \in I & \text{(Fig. VII.7.4)} \end{array}$$

  - **C2.** Conclude:

$$\begin{array}{lll} & r_2 \in \mathrm{dom}\,(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) & \\ \textsf{impl.} & r_2 \in (\mathrm{dom}\, f) \setminus (\mathrm{dom}\, \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) & \text{(–)} \\ \textsf{impl.} & r_2 \notin \mathrm{dom}\, \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\} & \text{(–)} \\ \textsf{impl.} & r_2 \notin \{\tilde{r} \mid \tilde{r} \in R \textsf{ and } \tilde{r} \in \mathrm{dom}\, f\} & \text{(–)} \\ \textsf{impl.} & r_2 \notin R & \text{(–)} \\ \textsf{impl.} & \textsf{false} & \text{(Step)} \\ \textsf{impl.} & \texttt{self}{+}\Delta(\hat{C})(x_1, x_2) \,\langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_2) & \text{(–)} \end{array}$$

Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle)\ \textsf{for-all}\ i\in I && \text{(Step, C1} \Rightarrow \text{Induction)}\\
\textsf{impl.}\ & \begin{bmatrix} r_2\in\operatorname{dom}(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})\ \textsf{impl.}\\ \texttt{self}\texttt{+}\Delta(\hat{C})(x_1,x_2)\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle\in(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})(r_2)\end{bmatrix}\ \textsf{and} && \text{(C2)}\\
& \left[\mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle)\ \textsf{for-all}\ i\in I\right]\\
\textsf{impl.}\ & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(&& \text{(Fig. VII.7.4)}\\
& \quad r_2[\texttt{self}\texttt{+}\Delta(\hat{C})(x_1,x_2)\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle]\,\textbf{!}\,\{\ell_i\,\textbf{.}\,(\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle\}_{i\in I})\\
\textsf{impl.}\ & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(r_2[\texttt{self}\texttt{+}\Delta(\hat{C})(x_1,x_2)]\,\textbf{!}\,\{\ell_i\,\textbf{.}\,\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i\in I}\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle)\\
& && \text{(Fig. VII.7.3)}\\
\textsf{impl.}\ & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z])\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle) && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{G}=r_1[x_1]\rightarrowtriangle r_2[x_2]\,\textbf{:}\,\{\ell_i\,\textbf{.}\,\hat{G}_i\}_{i\in I}$ **and**
  $\hat{G}\upharpoonright_{R[\hat{C}]} r[z]=r_2[x_2]\,\textbf{!}\,\{\ell_i\,\textbf{.}\,\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i\in I}$ **and**
  $r_1[x_1]=r[z]\neq r_2[x_2]$ **and** $\left[r_2\notin R\ \textsf{or}\ \{x_1,x_2\}\not\subseteq\mathsf{vars}(\hat{C})\right]$

  - **D1.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}) && \text{(A2)}\\
\textsf{impl.}\ & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(r_1[x_1]\rightarrowtriangle r_2[x_2]\,\textbf{:}\,\{\ell_i\,\textbf{.}\,\hat{G}_i\}_{i\in I}) && \text{(Step)}\\
\textsf{impl.}\ & \begin{bmatrix} r_2\in\operatorname{dom}(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})\\ \textsf{impl.}\ x_2\in(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})(r_2)\end{bmatrix}\ \textsf{and} && \text{(Fig. VII.7.4)}\\
& \left[\mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}_i)\ \textsf{for-all}\ i\in I\right]
\end{aligned}$$

  - **D2.** Conclude:

$$\begin{aligned}
& r_2\in\operatorname{dom}(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})\\
\textsf{impl.}\ & x_2\in(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})(r_2) && \text{(D1)}\\
\textsf{impl.}\ & x_2\in(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})(r_2)\in 2^{\mathbb{Z}} && \text{(B1)}\\
\textsf{impl.}\ & x_2\in(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})(r_2)\ \textsf{and}\ x_2\in\mathbb{Z} && \text{(–)}\\
\textsf{impl.}\ & x_2\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle\in(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})(r_2) && \text{(Fig. VII.3.3)}
\end{aligned}$$

Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle)\ \textsf{for-all}\ i\in I && \text{(Step, D1} \Rightarrow \text{Induction)}\\
\textsf{impl.}\ & \begin{bmatrix} r_2\in\operatorname{dom}(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})\ \textsf{impl.}\\ x_2\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle\in(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})(r_2)\end{bmatrix}\ \textsf{and} && \text{(D2)}\\
& \left[\mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle)\ \textsf{for-all}\ i\in I\right]\\
\textsf{impl.}\ & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(r_2[x_2\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle]\,\textbf{!}\,\{\ell_i\,\textbf{.}\,(\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle\}_{i\in I})\\
& && \text{(Fig. VII.7.4)}\\
\textsf{impl.}\ & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(r_2[x_2]\,\textbf{!}\,\{\ell_i\,\textbf{.}\,\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i\in I}\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle) && \text{(Fig. VII.7.3)}\\
\textsf{impl.}\ & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z])\,\langle\!\langle\{\texttt{self}\mapsto a\}\rangle\!\rangle) && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{G} = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}$ **and**
  $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = r_1[\texttt{\textbf{self}}\texttt{+}\Delta(\hat{C})(x_2, x_1)]\,\textbf{?}\{\ell_i \,.\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] \neq r[z] = r_2[x_2]$ **and** $r_1 \in R$ **and** $\{x_2, x_1\} \subseteq \mathsf{vars}(\hat{C})$

  - **E1.** Conclude:

$$\begin{array}{ll@{\qquad}r}
 & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) & \text{(A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}) & \text{(Step)} \\
\textbf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \ \textbf{for-all}\ i \in I & \text{(Fig. VII.7.4)}
\end{array}$$

  - **E2.** Conclude:

$$\begin{array}{ll@{\qquad}r}
 & r_1 \in \mathrm{dom}\,(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) & \\
\textbf{impl.} & r_1 \in (\mathrm{dom}\, f) \setminus (\mathrm{dom}\,\{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) & (-) \\
\textbf{impl.} & r_1 \notin \mathrm{dom}\,\{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\} & (-) \\
\textbf{impl.} & r_1 \notin \{\tilde{r} \mid \tilde{r} \in R \ \textbf{and}\ \tilde{r} \in \mathrm{dom}\, f\} & (-) \\
\textbf{impl.} & r_1 \notin R & (-) \\
\textbf{impl.} & \textbf{false} & \text{(Step)} \\
\textbf{impl.} & \texttt{\textbf{self}}\texttt{+}\Delta(\hat{C})(x_2, x_1)\, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_1) & (-)
\end{array}$$

  Conclude:

$$\begin{array}{ll@{\quad}r}
 & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle) \ \textbf{for-all}\ i \in I & \text{(Step, E1} \Rightarrow \text{Induction)} \\
\textbf{impl.} & \begin{bmatrix} r_1 \in \mathrm{dom}\,(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) \ \textbf{impl.} \\ \texttt{\textbf{self}}\texttt{+}\Delta(\hat{C})(x_2, x_1)\, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_1) \end{bmatrix} \ \textbf{and} & \text{(E2)} \\
 & \Big[\mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle) \ \textbf{for-all}\ i \in I\Big] & \\
\textbf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(& \text{(Fig. VII.7.4)} \\
 & \quad r_1[\texttt{\textbf{self}}\texttt{+}\Delta(\hat{C})(x_2, x_1)\, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle]\,\textbf{?}\{\ell_i \,.\, (\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z])\, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle\}_{i \in I}) & \\
\textbf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(r_1[\texttt{\textbf{self}}\texttt{+}\Delta(\hat{C})(x_2, x_1)]\,\textbf{?}\{\ell_i \,.\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I}\, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \\
 & & \text{(Fig. VII.7.3)} \\
\textbf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z])\, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \text{(Step)}
\end{array}$$

- **Step.** $\hat{G} = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}$ **and**
  $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = r_1[x_1]\,\textbf{?}\{\ell_i \,.\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] \neq r[z] = r_2[x_2]$ **and** $\Big[r_1 \notin R$ **or** $\{x_2, x_1\} \not\subseteq \mathsf{vars}(\hat{C})\Big]$

  - **F1.** Conclude:

$$\begin{array}{ll@{\qquad}r}
 & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) & \text{(A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}) & \text{(Step)} \\
\textbf{impl.} & \begin{bmatrix} r_1 \in \mathrm{dom}\,(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) \\ \textbf{impl.}\ x_1 \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_1) \end{bmatrix} \ \textbf{and} & \text{(Fig. VII.7.4)} \\
 & \Big[\mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \ \textbf{for-all}\ i \in I\Big] &
\end{array}$$

- **F2.** Conclude:

$$\begin{array}{lll}
 & r_1 \in \mathrm{dom}\,(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) & \\
\textsf{impl.} & x_1 \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_1) & \text{(F1)} \\
\textsf{impl.} & x_1 \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_1) \in 2^{\mathbb{Z}} & \text{(B1)} \\
\textsf{impl.} & x_1 \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_1) \ \textsf{and}\ x_2 \in \mathbb{Z} & \text{(–)} \\
\textsf{impl.} & x_1 \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_1) & \text{(Fig. VII.3.3)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) \ \textsf{for-all}\ i \in I & \text{(Step, F1} \Rightarrow \text{Induction)} \\
\textsf{impl.} & \left[\begin{array}{c} r_1 \in \mathrm{dom}\,(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) \ \textsf{impl.} \\ x_1 \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \in (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\})(r_1) \end{array}\right] \ \textsf{and} & \text{(F2)} \\
 & \left[\mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) \ \textsf{for-all}\ i \in I\right] & \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(r_1[x_1 \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle] \,\mathbf{?}\{\ell_i \,.\, (\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle\}_{i\in I}) & \\
 & & \text{(Fig. VII.7.4)} \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(r_1[x_1] \,\mathbf{?}\{\ell_i \,.\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i\in I} \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) & \text{(Fig. VII.7.3)} \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) & \text{(Step)}
\end{array}$$

- **Step.** $\hat{G} = r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \hat{G}_i\}_{i\in I}$ **and**
  $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = \bigsqcap\{\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i\in I}$ **and** $r_1[x_1] \neq r[z] \neq r_2[x_2]$

  - **G1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}) & \text{(A2)} \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \hat{G}_i\}_{i\in I}) & \text{(Step)} \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}_i) \ \textsf{for-all}\ i \in I & \text{(Fig. VII.7.4)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) \ \textsf{for-all}\ i \in I & \text{(Step, G1} \Rightarrow \text{Induction)} \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(\bigsqcap\{(\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle\}_{i\in I}) & \text{(Thm. VII.8.3)} \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\bigsqcap\{\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i\in I}) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) & \text{(Thm. VII.8.1)} \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle) & \text{(Step)}
\end{array}$$

- **Step.** $\hat{G} = \texttt{foreach}\ R'[\hat{C}']\ \textsf{do}\ \hat{G}_1 \,\mathbf{;}\, \hat{G}_2$ **and**
  $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = \texttt{foreach}\ R'[\hat{C}']\ \textsf{do}\ (\hat{G}_1 \upharpoonright_{R[\hat{C}]} r[z]) \,\mathbf{;}\, (\hat{G}_2 \upharpoonright_{R[\hat{C}]} r[z])$

  - **H1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}) & \text{(A2)} \\
\textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\mathcal{X}}(\texttt{foreach}\ R'[\hat{C}']\ \textsf{do}\ \hat{G}_1 \,\mathbf{;}\, \hat{G}_2) & \text{(Step)} \\
\textsf{impl.} & (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}') \mid \tilde{r} \in R'\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} \ \textsf{and} & \text{(Fig. VII.7.4)} \\
 & \hat{C}' \in \checkmark \ \textsf{and}\ \mathrm{expr}\,\hat{T}_1 \cap \mathbb{G}_{\texttt{rec}} = \emptyset \ \textsf{and} & \\
 & \mathsf{Wf}_{(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\})\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C}')\mid\tilde{r}\in R'\},\{\texttt{cont}\}}(\hat{T}_1) \ \textsf{and}\ \mathsf{Wf}_{(f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\}),\mathcal{X}}(\hat{T}_2) &
\end{array}$$

  - **H2.** Conclude:

$$\begin{array}{rlr} & \hat{C}' \in \checkmark & \text{(H1)} \\ \textsf{\textbf{impl.}} & \hat{C}' \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle \in \checkmark & \text{(Lem. VII.3.6:4)} \end{array}$$

Conclude:

$$\begin{array}{rlr} & \mathsf{Wf}_{(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}') \mid \tilde{r} \in R'\}, \{\mathtt{\textbf{cont}}\}}((\hat{G}_1 \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) \textsf{ \textbf{and}} & \\ & \mathsf{Wf}_{(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}), \mathcal{X}}((\hat{G}_2 \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \text{(Step, H1} \Rightarrow \text{Induction)} \\ \textsf{\textbf{impl.}} & (f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}') \mid \tilde{r} \in R'\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} \textsf{ \textbf{and}} & \text{(H1, H2)} \\ & \hat{C}' \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle \in \checkmark \textsf{ \textbf{and} } \operatorname{expr} \hat{T}_1 \cap \mathbb{G}_{\mathtt{\textbf{rec}}} = \emptyset \textsf{ \textbf{and}} & \\ & \mathsf{Wf}_{(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}) \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}') \mid \tilde{r} \in R'\}, \{\mathtt{\textbf{cont}}\}}((\hat{G}_1 \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) \textsf{ \textbf{and}} & \\ & \mathsf{Wf}_{(f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}), \mathcal{X}}((\hat{G}_2 \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \\ \textsf{\textbf{impl.}} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(& \text{(Fig. VII.7.4)} \\ & \quad \mathtt{\textbf{foreach}}\ R'[\hat{C}' \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle] \textsf{ \textbf{do}} & \\ & \qquad ((\hat{G}_1 \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) \,\mathtt{\textbf{;}}\, ((\hat{G}_2 \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle)) & \\ \textsf{\textbf{impl.}} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(& \text{(Fig. VII.7.3)} \\ & \quad \mathtt{\textbf{foreach}}\ R'[\hat{C}'] \textsf{ \textbf{do}} \ (\hat{G}_1 \upharpoonright_{R[\hat{C}]} r[z]) \,\mathtt{\textbf{;}}\, (\hat{G}_2 \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \\ \textsf{\textbf{impl.}} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \text{(Step)} \end{array}$$

- **Step.** $\hat{G} = \mathtt{\textbf{rec}}\ X\ \hat{G}_X$ **and** $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = \mathtt{\textbf{rec}}\ X\ (\hat{G}_X \upharpoonright_{R[\hat{C}]} r[z])$

  - **I1.** Conclude:

$$\begin{array}{rlr} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) & \text{(A2)} \\ \textsf{\textbf{impl.}} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\mathtt{\textbf{rec}}\ X\ \hat{G}_X) & \text{(Step)} \\ \textsf{\textbf{impl.}} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X} \cup \{X\}}(\hat{G}_X) & \text{(Fig. VII.7.4)} \end{array}$$

Conclude:

$$\begin{array}{rlr} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X} \cup \{X\}}((\hat{G}_X \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \text{(Step, I1} \Rightarrow \text{Induction)} \\ \textsf{\textbf{impl.}} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\mathtt{\textbf{rec}}\ X\ ((\hat{G}_X \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle)) & \text{(Fig. VII.7.4)} \\ \textsf{\textbf{impl.}} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}(\mathtt{\textbf{rec}}\ X\ (\hat{G}_X \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \text{(Fig. VII.7.3)} \\ \textsf{\textbf{impl.}} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \mathcal{X}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle) & \text{(Step)} \end{array}$$

QED.

VIII.44 Proof of Theorem VII.8.6

- **A1.** $\langle \hat{G}, R[\hat{C}], r[z] \rangle \in \operatorname{dom} \upharpoonright$
- **A2.** $\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G})$
- **A3.** $\hat{C} \in \checkmark$

- **A4.** $r \in R$
- **A5.** $z \in \mathsf{vars}(\hat{C})$
- **B1.** Conclude:

$$\begin{array}{rlr} & \hat{C} \in \checkmark & \text{(A3)} \\ \textsf{\textbf{impl.}} & \operatorname{dom} \delta\llbracket\hat{C}\rrbracket = \operatorname{dom} \Delta(\hat{C}) & \text{(Thm. VII.3.7:1)} \end{array}$$

- **B2.** Conclude:

$$\begin{array}{rlr} & a + \delta\llbracket\hat{C}\rrbracket(x_1, x_2) & (\exists x_1,\ \exists x_2) \\ = & \{\tilde{x} \mapsto a + \delta\llbracket\hat{C}\rrbracket(x_1, \tilde{x}) \mid \langle x_1, \tilde{x}\rangle \in \operatorname{dom} \delta\llbracket\hat{C}\rrbracket\}(x_2) & (-) \\ = & \{\tilde{x} \mapsto a + \delta\llbracket\hat{C}\rrbracket(x_1, \tilde{x}) \mid \langle x_1, \tilde{x}\rangle \in \mathsf{vars}(\hat{C}) \times \mathsf{vars}(\hat{C})\}(x_2) & \text{(Thm. VII.3.1)} \\ = & \{\tilde{x} \mapsto a + \delta\llbracket\hat{C}\rrbracket(x_1, \tilde{x}) \mid x_1, \tilde{x} \in \mathsf{vars}(\hat{C})\}(x_2) & (-) \\ = & \{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(x_1, \tilde{z}) \mid x_1, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_2) & \text{(Lem. VII.3.4:1)} \end{array}$$

- **B3.** Conclude:

$$\begin{array}{rlr} & \llbracket \mathbf{\mathtt{self}}\texttt{+}\Delta(\hat{C})(x_1, x_2)\, \langle\!\langle \{\mathbf{\mathtt{self}} \mapsto a\}\rangle\!\rangle \rrbracket & (\exists x_1,\ \exists x_2) \\ = & \llbracket (\mathbf{\mathtt{self}}\, \langle\!\langle \{\mathbf{\mathtt{self}} \mapsto a\}\rangle\!\rangle)\texttt{+}(\Delta(\hat{C})(x_1, x_2)\, \langle\!\langle \{\mathbf{\mathtt{self}} \mapsto a\}\rangle\!\rangle) \rrbracket & \text{(Fig. VII.3.3)} \\ = & \llbracket a\texttt{+}(\Delta(\hat{C})(x_1, x_2)\, \langle\!\langle \{\mathbf{\mathtt{self}} \mapsto a\}\rangle\!\rangle) \rrbracket & \text{(Fig. VII.3.3)} \\ = & \llbracket a\texttt{+}\Delta(\hat{C})(x_1, x_2) \rrbracket & \text{(Lem. VII.3.8} \Rightarrow \text{Lem. VII.3.6:2)} \\ = & \llbracket a \rrbracket + \llbracket \Delta(\hat{C})(x_1, x_2) \rrbracket & \text{(Fig. VII.3.4)} \\ = & a + \llbracket \Delta(\hat{C})(x_1, x_2) \rrbracket & \text{(Fig. VII.3.4)} \\ = & a + \delta\llbracket\hat{C}\rrbracket(x_1, x_2) & \text{(B1, A3} \Rightarrow \text{Thm. VII.3.7:3)} \\ = & \{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(x_1, \tilde{z}) \mid x_1, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_2) & \text{(B2)} \end{array}$$

- **B4.** Conclude:

$$\begin{array}{rlr} & z \in \mathsf{vars}(\hat{C}) & \text{(A5)} \\ \textsf{\textbf{impl.}} & \langle z, z\rangle \in \mathsf{vars}(\hat{C}) \times \mathsf{vars}(\hat{C}) & (-) \\ \textsf{\textbf{impl.}} & \langle z, z\rangle \in \operatorname{dom} \delta\llbracket\hat{C}\rrbracket & \text{(A3} \Rightarrow \text{Thm. VII.3.7:2)} \end{array}$$

- **B5.** Conclude:

$$\begin{array}{rlr} & r' \in \operatorname{dom}(f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\})\ \textsf{\textbf{impl.}} & (\exists r',\ \exists x) \\ & x \in (f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\})(r') & \\ \textsf{\textbf{impl.}} & r' \in \operatorname{dom} \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}\ \textsf{\textbf{impl.}}\ x \in \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}(r') & (-) \\ \textsf{\textbf{impl.}} & r' \in \operatorname{dom} \{\tilde{r} \mid \tilde{r} \in R\}\ \textsf{\textbf{impl.}}\ x \in \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}(r') & (-) \\ \textsf{\textbf{impl.}} & r' \in R\ \textsf{\textbf{impl.}}\ x \in \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}(r') & (-) \\ \textsf{\textbf{impl.}} & r' \in R\ \textsf{\textbf{impl.}}\ x \in \mathsf{vars}(\hat{C}) & (-) \end{array}$$

By induction on A1 (Fig. VII.8.2c):

- **Base.** $\hat{G} = X$ **and** $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = X$

  Conclude:

$$\begin{array}{lll}
 & \llbracket (\hat{G} \upharpoonright_{R[\hat{C}]} r[z])\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \\
\textbf{impl.} & \llbracket X\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \text{(Base)} \\
\textbf{impl.} & \llbracket X \rrbracket & \text{(Fig. VII.7.3)} \\
\textbf{impl.} & X & \text{(Fig. VII.7.6)} \\
\textbf{impl.} & X \upharpoonright r[a] & \text{(Fig. VII.5.2)} \\
\textbf{impl.} & X\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] & \text{(Fig. VII.6.1)} \\
\textbf{impl.} & \llbracket X \rrbracket\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] & \text{(Fig. VII.7.6)} \\
\textbf{impl.} & \llbracket \hat{G} \rrbracket\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] & \text{(Base)}
\end{array}$$

- **Step.** $\hat{G} = r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \hat{G}_i\}_{i \in I}$ **and**
  $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = r_2[\mathbf{self}{+}\Delta(\hat{C})(x_1,x_2)]\,\mathbf{!}\,\{\ell_i \,.\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] = r[z] \neq r_2[x_2]$ **and** $r_2 \in R$ **and** $\{x_1, x_2\} \subseteq \mathsf{vars}(\hat{C})$

  - **C1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) & \text{(A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \hat{G}_i\}_{i \in I}) & \text{(Step)} \\
\textbf{impl.} & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \ \textbf{for-all}\ i \in I & \text{(Fig. VII.7.4)}
\end{array}$$

  - **C2.** Conclude:

$$\begin{array}{lll}
 & r[z] = r_1[x_1] & \text{(Step)} \\
\textbf{impl.} & r = r_1 \ \textbf{and}\ z = x_1 & \text{(–)} \\
\textbf{impl.} & r = r_1 \ \textbf{and}\ z = x_1 \ \textbf{and}\ r_1 \in R & \text{(A4)}
\end{array}$$

  - **C3.** Conclude:

$$\begin{array}{lll}
 & r_2[\llbracket \mathbf{self}{+}\Delta(\hat{C})(x_1,x_2)\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket] & \\
= & r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(x_1,\tilde{z}) \mid x_1, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_2)] & \text{(B3)} \\
= & r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_2)] & \text{(C2)} \\
= & r_2[x_2]\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(Step} \Rightarrow \text{Fig. VII.6.1)} \\
= & r_2[\llbracket x_2 \rrbracket]\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(Fig. VII.3.4, A5)}
\end{array}$$

  - **C4.** Conclude:

$$\begin{array}{lll}
 & r = r_1 & \text{(C2)} \\
\textbf{impl.} & r[a] = r_1[a] & \text{(–)} \\
\textbf{impl.} & r[a] = r_1[a + 0] & \text{(Fig. VII.2.1:1)} \\
\textbf{impl.} & r[a] = r_1[a + \delta\llbracket\hat{C}\rrbracket(z,z)] & \text{(B4, A3} \Rightarrow \text{Thm. VII.3.7:4)} \\
\textbf{impl.} & r[a] = r_1[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(z)] & \text{(B2)} \\
\textbf{impl.} & r[a] = r_1[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_1)] & \text{(C2)} \\
\textbf{impl.} & r[a] = r_1[x_1]\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(C2} \Rightarrow \text{Fig. VII.6.1)} \\
\textbf{impl.} & r[a] = r_1[\llbracket x_1 \rrbracket]\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(Fig. VII.3.4, A5)}
\end{array}$$

- **C5.** Conclude:

$$\begin{array}{rlr}
 & \{x_1, x_2\} \subseteq \mathsf{vars}(\hat{C}) & \text{(Step)} \\
\textbf{impl.} & x_1, x_2 \in \mathsf{vars}(\hat{C}) & \text{(–)} \\
\textbf{impl.} & \langle x_1, x_2\rangle \in \mathsf{vars}(\hat{C}) \times \mathsf{vars}(\hat{C}) & \text{(–)} \\
\textbf{impl.} & \langle x_1, x_2\rangle \in \operatorname{dom} \delta\llbracket\hat{C}\rrbracket & \text{(A3} \Rightarrow \text{Thm. VII.3.7:2)}
\end{array}$$

- **C6.** Conclude:

$$\begin{array}{rlr}
 & r \neq r_2 & \\
\textbf{impl.} & r \neq r_2 \ \textbf{and}\ \langle x_1, x_2\rangle \in \operatorname{dom} \delta\llbracket\hat{C}\rrbracket & \text{(C5)} \\
\textbf{impl.} & r[a] \neq r_2[a + \delta\llbracket\hat{C}\rrbracket(x_1, x_2)] & \text{(–)}
\end{array}$$

- **C7.** Conclude:

$$\begin{array}{rlr}
 & \{x_1, x_2\} \subseteq \mathsf{vars}(\hat{C}) & \text{(Step)} \\
\textbf{impl.} & x_1, x_2 \in \mathsf{vars}(\hat{C}) & \text{(–)} \\
\textbf{impl.} & x_1, x_2 \in \operatorname{dom} \llbracket\hat{C}\rrbracket & \text{(Thm. VII.3.1)}
\end{array}$$

- **C8.** Conclude:

$$\begin{array}{rlr}
 & z \neq x_2 & \\
\textbf{impl.} & x_1 \neq x_2 & \text{(C2)} \\
\textbf{impl.} & \langle x_1, x_2\rangle \in \operatorname{dom} \delta\llbracket\hat{C}\rrbracket \ \textbf{and}\ x_1 \neq x_2 \ \textbf{and}\ \hat{C} \in \checkmark & \text{(C7, A3)} \\
\textbf{impl.} & 0 \neq \delta\llbracket\hat{C}\rrbracket(x_1, x_2) & \text{(Thm. VII.3.7:5)} \\
\textbf{impl.} & a \neq a + \delta\llbracket\hat{C}\rrbracket(x_1, x_2) & \text{(Fig. VII.2.1:1)} \\
\textbf{impl.} & r[a] \neq r_2[a + \delta\llbracket\hat{C}\rrbracket(x_1, x_2)] & \text{(–)}
\end{array}$$

- **C9.** Conclude:

$$\begin{array}{rlr}
 & r[z] \neq r_2[x_2] & \text{(Step)} \\
\textbf{impl.} & r \neq r_2 \ \textbf{or}\ z \neq x_2 & \text{(–)} \\
\textbf{impl.} & r[a] \neq r_2[a + \delta\llbracket\hat{C}\rrbracket(x_1, x_2)] & \text{(C6, C8)} \\
\textbf{impl.} & r[a] \neq r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(x_1, \tilde{z}) \mid x_1, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_2)] & \text{(B2)} \\
\textbf{impl.} & r[a] \neq r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_2)] & \text{(C2)} \\
\textbf{impl.} & r[a] \neq r_2[x_2] \,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis & \text{(Step} \Rightarrow \text{Fig. VII.6.1)} \\
\textbf{impl.} & r[a] \neq r_2[\llbracket x_2\rrbracket] \,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis & \text{(Fig. VII.3.4, A5)}
\end{array}$$

Conclude:

$$\begin{aligned}
& \llbracket (\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket \\
= \; & \llbracket r_2[\texttt{\textbf{self}}{+}\Delta(\hat{C})(x_1, x_2)] \, \mathbf{!} \, \{\ell_i \, \mathbf{.} \, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I} \, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket && \text{(Step)} \\
= \; & \llbracket r_2[\texttt{\textbf{self}}{+}\Delta(\hat{C})(x_1, x_2) \, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle] \, \mathbf{!} \, \{\ell_i \, \mathbf{.} \, (\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle\}_{i \in I} \rrbracket \\
& && \text{(Fig. VII.7.3)} \\
= \; & r_2[\llbracket \texttt{\textbf{self}}{+}\Delta(\hat{C})(x_1, x_2) \, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket] \, \mathbf{!} \, \{\ell_i \, \mathbf{.} \, \llbracket (\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket\}_{i \in I} \\
& && \text{(Fig. VII.7.6)} \\
= \; & r_2[\llbracket \texttt{\textbf{self}}{+}\Delta(\hat{C})(x_1, x_2) \, \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket] \, \mathbf{!} && \text{(C1, A3, A4, A5} \Rightarrow \text{Induction)} \\
& \quad \{\ell_i \, \mathbf{.} \, \llbracket \hat{G}_i \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a]\}_{i \in I} \\
= \; & r_2[\llbracket x_2 \rrbracket] \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \, \mathbf{!} && \text{(C3)} \\
& \quad \{\ell_i \, \mathbf{.} \, \llbracket \hat{G}_i \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a]\}_{i \in I} \\
= \; & r_1[\llbracket x_1 \rrbracket] \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \twoheadrightarrow && \text{(C4, C9} \Rightarrow \text{Fig. VII.5.2)} \\
& \quad r_2[\llbracket x_2 \rrbracket] \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \, \mathbf{:} \\
& \quad\quad \{\ell_i \, \mathbf{.} \, \llbracket \hat{G}_i \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!)\}_{i \in I} \upharpoonright r[a] \\
= \; & r_1[\llbracket x_1 \rrbracket] \twoheadrightarrow r_2[\llbracket x_2 \rrbracket] \, \mathbf{:} \, \{\ell_i \, \mathbf{.} \, \llbracket \hat{G}_i \rrbracket\}_{i \in I} \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] \\
& && \text{(Fig. VII.6.1)} \\
= \; & \llbracket r_1[x_1] \twoheadrightarrow r_2[x_2] \, \mathbf{:} \, \{\ell_i \, \mathbf{.} \, G_i\}_{i \in I} \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
= \; & \llbracket \hat{G} \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{G} = r_1[x_1] \twoheadrightarrow r_2[x_2] \, \mathbf{:} \, \{\ell_i \, \mathbf{.} \, \hat{G}_i\}_{i \in I}$ **and**
  $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = r_2[x_2] \, \mathbf{!} \, \{\ell_i \, \mathbf{.} \, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] = r[z] \neq r_2[x_2]$ **and** $\Big[r_2 \notin R$ **or** $\{x_1, x_2\} \not\subseteq \mathsf{vars}(\hat{C})\Big]$

  - **D1.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) && \text{(A2)} \\
\textbf{impl.} \; & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(r_1[x_1] \twoheadrightarrow r_2[x_2] \, \mathbf{:} \, \{\ell_i \, \mathbf{.} \, \hat{G}_i\}_{i \in I}) && \text{(Step)} \\
\textbf{impl.} \; & \left[\begin{array}{r} r_1 \in \mathrm{dom}\,(f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}) \\ \textbf{impl.} \;\; x_1 \in (f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\})(r_1) \end{array}\right] \textbf{ and} && \text{(Fig. VII.7.4)} \\
& \left[\begin{array}{r} r_2 \in \mathrm{dom}\,(f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}) \\ \textbf{impl.} \;\; x_2 \in (f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\})(r_2) \end{array}\right] \textbf{ and} \\
& \Big[\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \;\textbf{ for-all }\; i \in I\Big] \\
\textbf{impl.} \; & \Big[r_1 \in R \;\textbf{ impl. }\; x_1 \in \mathsf{vars}(\hat{C})\Big] \textbf{ and } \Big[r_2 \in R \;\textbf{ impl. }\; x_2 \in \mathsf{vars}(\hat{C})\Big] \textbf{ and} && \text{(B5)} \\
& \Big[\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \;\textbf{ for-all }\; i \in I\Big]
\end{aligned}$$

  - **D2.** Conclude:

$$\begin{aligned}
& r[z] = r_1[x_1] && \text{(Step)} \\
\textbf{impl.} \; & r = r_1 \textbf{ and } z = x_1 && \text{(–)} \\
\textbf{impl.} \; & r = r_1 \textbf{ and } z = x_1 \textbf{ and } r_1 \in R && \text{(A4)}
\end{aligned}$$

- **D3.** Conclude:

$$\begin{array}{lll}
 & r_2 \in R & \\
\textbf{impl.} & r_1, r_2 \in R & \text{(D2)} \\
\textbf{impl.} & r_2 \in R \ \textbf{and}\ x_1, x_2 \in \mathsf{vars}(\hat{C}) & \text{(D1)} \\
\textbf{impl.} & \textbf{false} & \text{(Step)}
\end{array}$$

- **D4.** Conclude:

$$\begin{array}{lll}
 & r_2[\llbracket x_2 \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \rrbracket] & \\
= & r_2[\llbracket x_2 \rrbracket] & \text{(Lem. VII.3.6:5)} \\
= & r_2[\llbracket x_2 \rrbracket]\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(D3} \Rightarrow \text{Fig. VII.6.1)}
\end{array}$$

- **D5.** Conclude:

$$\begin{array}{lll}
 & r = r_1 & \text{(D2)} \\
\textbf{impl.} & r[a] = r_1[a] & (-) \\
\textbf{impl.} & r[a] = r_1[a+0] & \text{(Fig. VII.2.1:1)} \\
\textbf{impl.} & r[a] = r_1[a + \delta\llbracket\hat{C}\rrbracket(z,z)] & \text{(B4, A3} \Rightarrow \text{Thm. VII.3.7:4)} \\
\textbf{impl.} & r[a] = r_1[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(z)] & \text{(B2)} \\
\textbf{impl.} & r[a] = r_1[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_1)] & \text{(D2)} \\
\textbf{impl.} & r[a] = r_1[x_1]\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(D2} \Rightarrow \text{Fig. VII.6.1)} \\
\textbf{impl.} & r[a] = r_1[\llbracket x_1 \rrbracket]\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(Fig. VII.3.4, A5)}
\end{array}$$

- **D6.** Conclude:

$$\begin{array}{lll}
 & r \in R \ \textbf{and}\ r_2 \notin R & \text{(B2, D3)} \\
\textbf{impl.} & r \neq r_2 & (-) \\
\textbf{impl.} & r[a] \neq r_2[\llbracket x_2 \rrbracket] & (-) \\
\textbf{impl.} & r[a] \neq r_2[\llbracket x_2 \rrbracket]\, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(D3} \Rightarrow \text{Fig. VII.6.1)}
\end{array}$$

Conclude:

$$\begin{aligned}
& \llbracket (\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket && \\
={}& \llbracket r_2[x_2] \,\mathbf{!}\, \{\ell_i \,\mathbf{.}\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I} \,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket && \text{(Step)} \\
={}& \llbracket r_2[x_2 \,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle] \,\mathbf{!}\, \{\ell_i \,\mathbf{.}\, (\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle\}_{i \in I} \rrbracket && \text{(Fig. VII.7.3)} \\
={}& r_2[\llbracket x_2 \,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket] \,\mathbf{!}\, \{\ell_i \,\mathbf{.}\, \llbracket (\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket\}_{i \in I} && \text{(Fig. VII.7.6)} \\
={}& r_2[\llbracket x_2 \,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket] \,\mathbf{!} && \text{(D1, A3, A4, A5} \Rightarrow \text{Induction)} \\
& \quad \{\ell_i \,\mathbf{.}\, \llbracket \hat{G}_i \rrbracket \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a]\}_{i \in I} && \\
={}& r_2[\llbracket x_2 \rrbracket] \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \,\mathbf{!} && \text{(D4)} \\
& \quad \{\ell_i \,\mathbf{.}\, \llbracket \hat{G}_i \rrbracket \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a]\}_{i \in I} && \\
={}& r_1[\llbracket x_1 \rrbracket] \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \twoheadrightarrow && \text{(D5, D6} \Rightarrow \text{Fig. VII.5.2)} \\
& \quad r_2[\llbracket x_2 \rrbracket] \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \,\mathbf{:} && \\
& \qquad \{\ell_i \,\mathbf{.}\, \llbracket \hat{G}_i \rrbracket \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!)\}_{i \in I} \upharpoonright r[a] && \\
={}& r_1[\llbracket x_1 \rrbracket] \twoheadrightarrow r_2[\llbracket x_2 \rrbracket] \,\mathbf{:}\, \{\ell_i \,\mathbf{.}\, \llbracket \hat{G}_i \rrbracket\}_{i \in I} \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] && \\
& && \text{(Fig. VII.6.1)} \\
={}& \llbracket r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,\mathbf{.}\, \hat{G}_i\}_{i \in I} \rrbracket \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{G} \rrbracket \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{G} = r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,\mathbf{.}\, \hat{G}_i\}_{i \in I}$ **and**
  $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = r_1[\texttt{\textbf{self}}\text{+}\Delta(\hat{C})(x_2, x_1)] \,\mathbf{?}\{\ell_i \,\mathbf{.}\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] \neq r[z] = r_2[x_2]$ **and** $r_1 \in R$ **and** $\{x_2, x_1\} \subseteq \mathsf{vars}(\hat{C})$

  - **E1.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) && \text{(A2)} \\
\textbf{impl. } & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,\mathbf{.}\, \hat{G}_i\}_{i \in I}) && \text{(Step)} \\
\textbf{impl. } & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \ \textbf{for-all} \ i \in I && \text{(Fig. VII.7.4)}
\end{aligned}$$

  - **E2.** Conclude:

$$\begin{aligned}
& r[z] = r_2[x_2] && \text{(Step)} \\
\textbf{impl. } & r = r_2 \ \textbf{and} \ z = x_2 && \text{(–)} \\
\textbf{impl. } & r = r_2 \ \textbf{and} \ z = x_2 \ \textbf{and} \ r_2 \in R && \text{(A4)}
\end{aligned}$$

  - **E3.** Conclude:

$$\begin{aligned}
& r_1[\llbracket \texttt{\textbf{self}}\text{+}\Delta(\hat{C})(x_2, x_1) \,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket] && \\
={}& r_1[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(x_2, \tilde{z}) \mid x_2, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_1)] && \text{(B3)} \\
={}& r_1[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_1)] && \text{(E2)} \\
={}& r_1[x_1] \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) && \text{(Step} \Rightarrow \text{Fig. VII.6.1)} \\
={}& r_1[\llbracket x_1 \rrbracket] \,(\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) && \text{(Fig. VII.3.4, A5)}
\end{aligned}$$

- **E4.** Conclude:

$r = r_2$ (E2)

impl. $r[a] = r_2[a]$ (–)

impl. $r[a] = r_2[a + 0]$ (Fig. VII.2.1:1)

impl. $r[a] = r_2[a + \delta\llbracket\hat{C}\rrbracket(z, z)]$ (B4, A3 ⇒ Thm. VII.3.7:4)

impl. $r[a] = r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(z)]$ (B2)

impl. $r[a] = r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_2)]$ (E2)

impl. $r[a] = r_2[x_2]\ \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis$ (E2 ⇒ Fig. VII.6.1)

impl. $r[a] = r_2[\llbracket x_2\rrbracket]\ \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis$ (Fig. VII.3.4, A5)

- **E5.** Conclude:

$\{x_2, x_1\} \subseteq \mathsf{vars}(\hat{C})$ (Step)

impl. $x_2, x_1 \in \mathsf{vars}(\hat{C})$ (–)

impl. $\langle x_2, x_1\rangle \in \mathsf{vars}(\hat{C}) \times \mathsf{vars}(\hat{C})$ (–)

impl. $\langle x_2, x_1\rangle \in \operatorname{dom}\delta\llbracket\hat{C}\rrbracket$ (A3 ⇒ Thm. VII.3.7:2)

- **E6.** Conclude:

$r \neq r_1$

impl. $r \neq r_1$ **and** $\langle x_2, x_1\rangle \in \operatorname{dom}\delta\llbracket\hat{C}\rrbracket$ (E5)

impl. $r[a] \neq r_1[a + \delta\llbracket\hat{C}\rrbracket(x_2, x_1)]$ (–)

- **E7.** Conclude:

$\{x_2, x_1\} \subseteq \mathsf{vars}(\hat{C})$ (Step)

impl. $x_2, x_1 \in \mathsf{vars}(\hat{C})$ (–)

impl. $x_2, x_1 \in \operatorname{dom}\llbracket\hat{C}\rrbracket$ (Thm. VII.3.1)

- **E8.** Conclude:

$z \neq x_1$

impl. $x_2 \neq x_1$ (E2)

impl. $\langle x_2, x_1\rangle \in \operatorname{dom}\delta\llbracket\hat{C}\rrbracket$ **and** $x_2 \neq x_1$ **and** $\hat{C} \in \checkmark$ (E7, A3)

impl. $0 \neq \delta\llbracket\hat{C}\rrbracket(x_2, x_1)$ (Thm. VII.3.7:5)

impl. $a \neq a + \delta\llbracket\hat{C}\rrbracket(x_2, x_1)$ (Fig. VII.2.1:1)

impl. $r[a] \neq r_1[a + \delta\llbracket\hat{C}\rrbracket(x_2, x_1)]$ (–)

- **E9.** Conclude:

$r[z] \neq r_1[x_1]$ (Step)

impl. $r \neq r_1$ **or** $z \neq x_1$ (–)

impl. $r[a] \neq r_1[a + \delta\llbracket\hat{C}\rrbracket(x_2, x_1)]$ (E6, E8)

impl. $r[a] \neq r_1[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(x_2, \tilde{z}) \mid x_2, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_1)]$ (B2)

impl. $r[a] \neq r_1[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_1)]$ (E2)

impl. $r[a] \neq r_1[x_1]\ \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis$ (Step ⇒ Fig. VII.6.1)

impl. $r[a] \neq r_1[\llbracket x_1\rrbracket]\ \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis$ (Fig. VII.3.4, A5)

Conclude:

$$\begin{aligned}
& \llbracket (\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \rrbracket \\
= {} & \llbracket r_1[\texttt{self}{+}\Delta(\hat{C})(x_2, x_1)]\, \textbf{?} \{\ell_i \,.\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I} \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \rrbracket && \text{(Step)} \\
= {} & \llbracket r_1[\texttt{self}{+}\Delta(\hat{C})(x_2, x_1) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle]\, \textbf{?} \{\ell_i \,.\, (\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle\}_{i \in I} \rrbracket && \text{(Fig. VII.7.3)} \\
= {} & r_1[\llbracket \texttt{self}{+}\Delta(\hat{C})(x_2, x_1) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \rrbracket]\, \textbf{?} \{\ell_i \,.\, \llbracket (\hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \rrbracket\}_{i \in I} && \text{(Fig. VII.7.6)} \\
= {} & r_1[\llbracket \texttt{self}{+}\Delta(\hat{C})(x_2, x_1) \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \rrbracket]\, \textbf{?} && \text{(E1, A3, A4, A5} \Rightarrow \text{Induction)} \\
& \quad \{\ell_i \,.\, \llbracket \hat{G}_i \rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis \upharpoonright r[a]\}_{i \in I} \\
= {} & r_1[\llbracket x_1 \rrbracket] \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis\, \textbf{?} && \text{(E3)} \\
& \quad \{\ell_i \,.\, \llbracket \hat{G}_i \rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis \upharpoonright r[a]\}_{i \in I} \\
= {} & r_1[\llbracket x_1 \rrbracket] \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis \rightarrowtriangle && \text{(E4, E9} \Rightarrow \text{Fig. VII.5.2)} \\
& \quad r_2[\llbracket x_2 \rrbracket] \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis : \\
& \qquad \{\ell_i \,.\, \llbracket \hat{G}_i \rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis\}_{i \in I} \upharpoonright r[a] \\
= {} & r_1[\llbracket x_1 \rrbracket] \rightarrowtriangle r_2[\llbracket x_2 \rrbracket] : \{\ell_i \,.\, \llbracket \hat{G}_i \rrbracket\}_{i \in I} \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis \upharpoonright r[a] && \text{(Fig. VII.6.1)} \\
= {} & \llbracket r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I} \rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis \upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
= {} & \llbracket \hat{G} \rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}] \rrparenthesis \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{G} = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}$ **and**
  $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = r_1[x_1]\, \textbf{?} \{\ell_i \,.\, \hat{G}_i \upharpoonright_{R[\hat{C}]} r[z]\}_{i \in I}$ **and**
  $r_1[x_1] \neq r[z] = r_2[x_2]$ **and** $\left[r_1 \notin R \textbf{ or } \{x_2, x_1\} \not\subseteq \mathsf{vars}(\hat{C})\right]$

  - **F1.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}) && \text{(A2)} \\
\textbf{impl. } & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}) && \text{(Step)} \\
\textbf{impl. } & \left[\begin{array}{c} r_1 \in \mathrm{dom}\,(f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}) \\ \textbf{impl. } x_1 \in (f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\})(r_1) \end{array}\right] \textbf{ and} && \text{(Fig. VII.7.4)} \\
& \left[\begin{array}{c} r_2 \in \mathrm{dom}\,(f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}) \\ \textbf{impl. } x_2 \in (f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\})(r_2) \end{array}\right] \textbf{ and} \\
& \left[\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \textbf{ for-all } i \in I\right] \\
\textbf{impl. } & \left[r_1 \in R \textbf{ impl. } x_1 \in \mathsf{vars}(\hat{C})\right] \textbf{ and } \left[r_2 \in R \textbf{ impl. } x_2 \in \mathsf{vars}(\hat{C})\right] \textbf{ and} && \text{(B5)} \\
& \left[\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \mathcal{X}}(\hat{G}_i) \textbf{ for-all } i \in I\right]
\end{aligned}$$

  - **F2.** Conclude:

$$\begin{aligned}
& r[z] = r_2[x_2] && \text{(Step)} \\
\textbf{impl. } & r = r_2 \textbf{ and } z = x_2 && \text{(–)} \\
\textbf{impl. } & r = r_2 \textbf{ and } z = x_2 \textbf{ and } r_2 \in R && \text{(A4)}
\end{aligned}$$

- **F3.** Conclude:

$$\begin{array}{lll}
 & r_1 \in R & \\
\textbf{impl.} & r_1, r_2 \in R & \text{(F2)} \\
\textbf{impl.} & r_1 \in R \ \textbf{and} \ x_1, x_2 \in \mathsf{vars}(\hat{C}) & \text{(F1)} \\
\textbf{impl.} & \textbf{false} & \text{(Step)}
\end{array}$$

- **F4.** Conclude:

$$\begin{array}{lll}
 & r_2[\llbracket x_2 \, \langle\!\langle \{\texttt{self} \mapsto a\} \rangle\!\rangle \rrbracket] & \\
= & r_2[\llbracket x_2 \rrbracket] & \text{(Lem. VII.3.6:5)} \\
= & r_2[\llbracket x_2 \rrbracket] \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(F3} \Rightarrow \text{Fig. VII.6.1)}
\end{array}$$

- **F5.** Conclude:

$$\begin{array}{lll}
 & r = r_2 & \text{(F2)} \\
\textbf{impl.} & r[a] = r_2[a] & (-) \\
\textbf{impl.} & r[a] = r_2[a + 0] & \text{(Fig. VII.2.1:1)} \\
\textbf{impl.} & r[a] = r_2[a + \delta\llbracket\hat{C}\rrbracket(z, z)] & \text{(B4, A3} \Rightarrow \text{Thm. VII.3.7:4)} \\
\textbf{impl.} & r[a] = r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(z)] & \text{(B2)} \\
\textbf{impl.} & r[a] = r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}(x_2)] & \text{(F2)} \\
\textbf{impl.} & r[a] = r_2[x_2] \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid z, \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(F2} \Rightarrow \text{Fig. VII.6.1)} \\
\textbf{impl.} & r[a] = r_2[\llbracket x_2 \rrbracket] \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(Fig. VII.3.4, A5)}
\end{array}$$

- **F6.** Conclude:

$$\begin{array}{lll}
 & r \in R \ \textbf{and} \ r_1 \notin R & \text{(B2, F3)} \\
\textbf{impl.} & r \neq r_1 & (-) \\
\textbf{impl.} & r[a] \neq r_1[\llbracket x_1 \rrbracket] & (-) \\
\textbf{impl.} & r[a] \neq r_1[\llbracket x_1 \rrbracket] \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) & \text{(F3} \Rightarrow \text{Fig. VII.6.1)}
\end{array}$$

Conclude:

$$\begin{array}{lll}
& [\![(\hat{G} \restriction_{R[\hat{C}]} r[z])\ \langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle]\!] & \\
= & [\![r_1[x_1]\,\mathbf{?}\{\ell_i\,\mathbf{.}\,\hat{G}_i \restriction_{R[\hat{C}]} r[z]\}_{i\in I}\ \langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle]\!] & \text{(Step)} \\
= & [\![r_1[x_1\ \langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle]\,\mathbf{?}\{\ell_i\,\mathbf{.}\,(\hat{G}_i \restriction_{R[\hat{C}]} r[z])\ \langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle\}_{i\in I}]\!] & \text{(Fig. VII.7.3)} \\
= & r_1[[\![x_1\ \langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle]\!]]\,\mathbf{?}\{\ell_i\,\mathbf{.}\,[\![(\hat{G}_i \restriction_{R[\hat{C}]} r[z])\ \langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle]\!]\}_{i\in I} & \text{(Fig. VII.7.6)} \\
= & r_1[[\![x_1\ \langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle]\!]]\,\mathbf{?} & \text{(F1, A3, A4, A5} \Rightarrow \text{Induction)} \\
& \quad \{\ell_i\,\mathbf{.}\,[\![\hat{G}_i]\!]\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \restriction r[a]\}_{i\in I} & \\
= & r_1[[\![x_1]\!]]\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!)\,\mathbf{?} & \text{(F4)} \\
& \quad \{\ell_i\,\mathbf{.}\,[\![\hat{G}_i]\!]\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \restriction r[a]\}_{i\in I} & \\
= & r_1[[\![x_1]\!]]\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \rightarrowtriangle & \text{(F5, F6} \Rightarrow \text{Fig. VII.5.2)} \\
& \quad r_2[[\![x_2]\!]]\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!)\,\mathbf{:} & \\
& \qquad \{\ell_i\,\mathbf{.}\,[\![\hat{G}_i]\!]\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!)\}_{i\in I} \restriction r[a] & \\
= & r_1[[\![x_1]\!]] \rightarrowtriangle r_2[[\![x_2]\!]]\,\mathbf{:}\{\ell_i\,\mathbf{.}\,[\![\hat{G}_i]\!]\}_{i\in I}\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \restriction r[a] & \\
& & \text{(Fig. VII.6.1)} \\
= & [\![r_1[x_1] \rightarrowtriangle r_2[x_2]\,\mathbf{:}\{\ell_i\,\mathbf{.}\,\hat{G}_i\}_{i\in I}]\!]\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \restriction r[a] & \text{(Fig. VII.7.6)} \\
= & [\![\hat{G}]\!]\ (\!(R[\{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \restriction r[a] & \text{(Step)}
\end{array}$$

- **Step.** $\hat{G} = r_1[x_1] \rightarrowtriangle r_2[x_2]\,\mathbf{:}\{\ell_i\,\mathbf{.}\,\hat{G}_i\}_{i\in I}$ **and** $\hat{G} \restriction_{R[\hat{C}]} r[z] = \bigsqcap\{\hat{G}_i \restriction_{R[\hat{C}]} r[z]\}_{i\in I}$ **and** $r_1[x_1] \neq r[z] \neq r_2[x_2]$

  - **G1.** Conclude:

$$\begin{array}{lll}
& \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}) & \text{(A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\mathcal{X}}(r_1[x_1] \rightarrowtriangle r_2[x_2]\,\mathbf{:}\{\ell_i\,\mathbf{.}\,\hat{G}_i\}_{i\in I}) & \text{(Step)} \\
\textbf{impl.} & \left[\begin{array}{l} \quad r_1 \in \mathrm{dom}\,(f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}) \\ \textbf{impl.}\ \ x_1 \in (f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\})(r_1) \end{array}\right] \textbf{ and} & \text{(Fig. VII.7.4)} \\
& \left[\begin{array}{l} \quad r_2 \in \mathrm{dom}\,(f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}) \\ \textbf{impl.}\ \ x_2 \in (f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\})(r_2) \end{array}\right] \textbf{ and} & \\
& \left[\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}_i)\ \textbf{ for-all }\ i \in I\right] & \\
\textbf{impl.} & \left[r_1 \in R\ \textbf{ impl. }\ x_1 \in \mathsf{vars}(\hat{C})\right] \textbf{ and } \left[r_2 \in R\ \textbf{ impl. }\ x_2 \in \mathsf{vars}(\hat{C})\right] \textbf{ and} & \text{(B5)} \\
& \left[\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}_i)\ \textbf{ for-all }\ i \in I\right] &
\end{array}$$

  - **G2.** Conclude:

$$\begin{array}{lll}
& a = \{\tilde{z} \mapsto a + \delta[\![\hat{C}]\!](z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}([\![x]\!]) & (\exists x) \\
\textbf{impl.} & a = a + \delta[\![\hat{C}]\!](z,[\![x]\!]) & (-) \\
\textbf{impl.} & \delta[\![\hat{C}]\!](z,[\![x]\!]) = 0 & \text{(Fig. VII.2.1:1)} \\
\textbf{impl.} & \delta[\![\hat{C}]\!](z,[\![x]\!]) = 0\ \textbf{ and }\ \hat{C} \in \checkmark & \text{(A3)} \\
\textbf{impl.} & z = [\![x]\!] & \text{(Thm. VII.3.7:5)} \\
\textbf{impl.} & z = x & \text{(Fig. VII.3.4)}
\end{array}$$

- **G3.** Conclude:

$r[a] = r_1[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}(\llbracket x_1\rrbracket)]$

impl. $r = r_1$ **and** $a = \{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}(\llbracket x_1\rrbracket)$ (–)

impl. $r = r_1$ **and** $z = x_1$ (G2)

impl. $r[z] = r_1[x_1]$ (–)

impl. **false** (Step)

- **G4.** Conclude:

$r[a] = r_1[\llbracket x\rrbracket]$ **and** $r_1 \notin R$ ($\exists x$)

impl. $r = r_1$ **and** $r_1 \notin R$ (–)

impl. $r \notin R$ (=)

impl. **false** (A4)

- **G5.** Conclude:

$z' \in \mathsf{vars}(\hat{C})$ ($\exists z$)

impl. $z, z' \in \mathsf{vars}(\hat{C})$ (A5)

impl. $\langle z, z'\rangle \in \mathsf{vars}(\hat{C}) \times \mathsf{vars}(\hat{C})$ (–)

impl. $\langle z, z'\rangle \in \operatorname{dom} \delta\llbracket\hat{C}\rrbracket$ (A3 ⇒ Thm. VII.3.7:2)

- **G6.** Conclude:

$r_1 \in R$

impl. $x_1 \in \mathsf{vars}(\hat{C})$ (G1)

impl. $x_1 \in \{\tilde{z} \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}$ (–)

impl. $x_1 \in \operatorname{dom} \{\tilde{z} \mapsto \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}$ (G5)

impl. $\llbracket x_1\rrbracket \in \operatorname{dom} \{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}$ (Fig. VII.3.4)

- **G7.** Conclude:

$r[a] = r_1[\llbracket x_1\rrbracket]\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis$

impl. $r[a] = r_1[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}(\llbracket x_1\rrbracket)]$ **or** (Fig. VII.6.1)

$\Big[r[a] = r_1[\llbracket x_1\rrbracket]$ **and** $r_1 \notin R\Big]$ **or**

$\Big[r_1 \in R$ **and** $\llbracket x_1\rrbracket \notin \operatorname{dom} \{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}\Big]$

impl. **false** (G3, G4, G6)

- **G8.** Conclude:

$r[a] = r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}(\llbracket x_2\rrbracket)]$

impl. $r = r_2$ **and** $a = \{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}(\llbracket x_2\rrbracket)$ (–)

impl. $r = r_2$ **and** $z = x_2$ (G2)

impl. $r[z] = r_2[x_2]$ (–)

impl. **false** (Step)

- **G9.** Conclude:

$$
\begin{array}{lll}
 & r_2 \in R & \\
\textbf{impl.} & x_2 \in \mathsf{vars}(\hat{C}) & \text{(G1)} \\
\textbf{impl.} & x_2 \in \{\tilde{z} \mid \tilde{z} \in \mathsf{vars}(\hat{C})\} & (-) \\
\textbf{impl.} & x_2 \in \operatorname{dom}\{\tilde{z} \mapsto \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\} & \text{(G5)} \\
\textbf{impl.} & \llbracket x_2\rrbracket \in \operatorname{dom}\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\} & \text{(Fig. VII.3.4)}
\end{array}
$$

- **G10.** Conclude:

$$
\begin{array}{lll}
 & r[a] = r_2[\llbracket x_2\rrbracket]\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis & \\
\textbf{impl.} & r[a] = r_2[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}(\llbracket x_2\rrbracket)] \;\; \textbf{or} & \text{(Fig. VII.6.1)} \\
 & \Big[r[a] = r_2[\llbracket x_2\rrbracket] \;\; \textbf{and} \;\; r_2 \notin R\Big] \;\; \textbf{or} & \\
 & \Big[r_2 \in R \;\; \textbf{and} \;\; \llbracket x_2\rrbracket \notin \operatorname{dom}\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}\Big] & \\
\textbf{impl.} & \textbf{false} & \text{(G8, G4, G9)}
\end{array}
$$

Conclude:

$$
\begin{array}{lll}
 & \llbracket(\hat{G} \restriction_{R[\hat{C}]} r[z])\,\langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle\rrbracket & \\
= & \llbracket\bigsqcap\{\hat{G}_i \restriction_{R[\hat{C}]} r[z]\}_{i\in I}\,\langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle\rrbracket & \text{(Step)} \\
= & \llbracket\bigsqcap\{(\hat{G}_i \restriction_{R[\hat{C}]} r[z])\,\langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle\}_{i\in I}\rrbracket & \text{(Thm. VII.8.1)} \\
= & \bigsqcap\{\llbracket(\hat{G}_i \restriction_{R[\hat{C}]} r[z])\,\langle\!\langle\{\mathtt{self} \mapsto a\}\rangle\!\rangle\rrbracket\}_{i\in I} & \text{(Thm. VII.8.2)} \\
= & \bigsqcap\{\llbracket\hat{G}_i\rrbracket\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \restriction r[a]\}_{i\in I} & \text{(G1, A3, A4, A5} \Rightarrow \text{Induction)} \\
= & r_1[\llbracket x_1\rrbracket]\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \mathrel{-\!\!\blacktriangleright} & \text{(G7, G10} \Rightarrow \text{Fig. VII.5.2)} \\
 & \quad r_2[\llbracket x_2\rrbracket]\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis : & \\
 & \qquad \{\ell_i \,.\, \llbracket\hat{G}_i\rrbracket\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis\}_{i\in I} \restriction r[a] & \\
= & r_1[\llbracket x_1\rrbracket] \mathrel{-\!\!\blacktriangleright} r_2[\llbracket x_2\rrbracket] : \{\ell_i \,.\, \llbracket\hat{G}_i\rrbracket\}_{i\in I}\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \restriction r[a] & \\
 & & \text{(Fig. VII.6.1)} \\
= & \llbracket r_1[x_1] \mathrel{-\!\!\blacktriangleright} r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i\in I}\rrbracket\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \restriction r[a] & \text{(Fig. VII.7.6)} \\
= & \llbracket\hat{G}\rrbracket\,\llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z,\tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \restriction r[a] & \text{(Step)}
\end{array}
$$

- **Step.** $\hat{G} = \mathtt{foreach}\ R'[\hat{C}']\ \textbf{do}\ \hat{G}_1\ \textbf{;}\ \hat{G}_2$ **and**
  $\hat{G} \restriction_{R[\hat{C}]} r[z] = \mathtt{foreach}\ R'[\hat{C}']\ \textbf{do}\ (\hat{G}_1 \restriction_{R[\hat{C}]} r[z])\ \textbf{;}\ (\hat{G}_2 \restriction_{R[\hat{C}]} r[z])$

  - **H1.** Conclude:

$$
\begin{array}{lll}
 & \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}) & \text{(A2)} \\
\textbf{impl.} & \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\mathcal{X}}(\mathtt{foreach}\ R'[\hat{C}']\ \textbf{do}\ \hat{G}_1\ \textbf{;}\ \hat{G}_2) & \text{(Step)} \\
\textbf{impl.} & f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}') \mid \tilde{r} \in R'\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} \;\; \textbf{and} & \\
 & & \text{(Fig. VII.7.4)} \\
 & \hat{C}' \in \checkmark \;\; \textbf{and} \;\; \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\}\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C}')\mid\tilde{r}\in R'\},\mathcal{X}}(\hat{G}_1) \;\; \textbf{and} \;\; \mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C})\mid\tilde{r}\in R\},\mathcal{X}}(\hat{G}_2) &
\end{array}
$$

  - **H2.** Conclude:

$$
\begin{array}{ll}
\mathsf{len}\,\llbracket\hat{C}'\rrbracket > 0 & \text{(H1} \Rightarrow \text{Thm. VII.3.6)}
\end{array}
$$

- **H3.** Conclude:

$$\begin{array}{lll} & f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}') \mid \tilde{r} \in R'\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} & \text{(H1)} \\ \textbf{impl.} & (\mathrm{dom}\,\{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}) \cap (\mathrm{dom}\,\{\tilde{r} \mapsto \mathsf{vars}(\hat{C}') \mid \tilde{r} \in R'\}) = \emptyset & (\text{–}) \\ \textbf{impl.} & \{\tilde{r} \mid \tilde{r} \in R\} \cap \{\tilde{r} \mid \tilde{r} \in R'\} = \emptyset & (\text{–}) \\ \textbf{impl.} & R \cap R' = \emptyset & (\text{–}) \end{array}$$

- **H4.** Conclude:

$$\begin{array}{lll} & R \cap R' = \emptyset & \text{(H3)} \\ \textbf{impl.} & r \notin R' & \text{(A4)} \end{array}$$

Conclude:

$$\begin{array}{lll} & \llbracket (\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \\ = & \llbracket \mathbf{foreach}\ R'[\hat{C}']\ \mathbf{do}\ (\hat{G}_1 \upharpoonright_{R[\hat{C}]} r[z]) \,\mathbf{;}\, (\hat{G}_2 \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \text{(Step)} \\ = & \llbracket \mathbf{foreach}\ R'[\hat{C}' \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle]\ \mathbf{do} & \text{(Fig. VII.7.3)} \\ & \quad ((\hat{G}_1 \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle) \,\mathbf{;}\, ((\hat{G}_2 \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle) \rrbracket & \\ = & \mathsf{iter}(& \text{(Fig. VII.7.6)} \\ & \quad \llbracket (\hat{G}_1 \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket, \llbracket (\hat{G}_2 \upharpoonright_{R[\hat{C}]} r[z]) \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket, R', \llbracket \hat{C}' \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket) & \\ = & \mathsf{iter}(& \text{(H1, A3, A4, A5} \Rightarrow \text{Induction)} \\ & \quad \llbracket \hat{G}_1 \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a], & \\ & \quad \llbracket \hat{G}_2 \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a], R', \llbracket \hat{C}' \, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket) & \\ = & \mathsf{iter}(& \text{(Lem. VII.3.6:4)} \\ & \quad \llbracket \hat{G}_1 \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a], & \\ & \quad \llbracket \hat{G}_2 \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a], R', \llbracket \hat{C}' \rrbracket) & \\ = & \mathsf{iter}(& \text{(H2, H4} \Rightarrow \text{Thm. VII.6.11)} \\ & \quad \llbracket \hat{G}_1 \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!), & \\ & \quad \llbracket \hat{G}_2 \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!), R', \llbracket \hat{C}' \rrbracket) \upharpoonright r[a] & \\ = & \mathsf{iter}(\llbracket \hat{G}_1 \rrbracket, \llbracket \hat{G}_2 \rrbracket, R', \llbracket \hat{C}' \rrbracket) & \text{(H2, H3} \Rightarrow \text{Thm. VII.6.12)} \\ & \quad (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] & \\ = & \llbracket \mathbf{foreach}\ R'[\hat{C}']\ \mathbf{do}\ \hat{G}_1 \,\mathbf{;}\, \hat{G}_2 \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] & \text{(Fig. VII.7.6)} \\ = & \llbracket \hat{G} \rrbracket \, (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}])\!) \upharpoonright r[a] & \text{(Step)} \end{array}$$

- **Step.** $\hat{G} = \mathbf{rec}\ X\ \hat{G}_X$ **and** $\hat{G} \upharpoonright_{R[\hat{C}]} r[z] = \mathbf{rec}\ X\ (\hat{G}_X \upharpoonright_{R[\hat{C}]} r[z])$

  - **I1.** Conclude:

$$\begin{array}{lll} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}) & \text{(A2)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\mathbf{rec}\ X\ \hat{G}_X) & \text{(Step)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X} \cup \{X\}}(\hat{G}_X) & \text{(Fig. VII.7.4)} \end{array}$$

Conclude:

$$\begin{array}{rlr}
 & \llbracket(\hat{G} \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle\rrbracket & \\
= & \llbracket\texttt{\textbf{rec}}\ X\ (\hat{G}_X \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle\rrbracket & \text{(Step)} \\
= & \llbracket\texttt{\textbf{rec}}\ X\ ((\hat{G}_X \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle)\rrbracket & \text{(Fig. VII.7.3)} \\
= & \texttt{\textbf{rec}}\ X\ \llbracket((\hat{G}_X \upharpoonright_{R[\hat{C}]} r[z]) \langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle)\rrbracket & \text{(Fig. VII.7.6)} \\
= & \texttt{\textbf{rec}}\ X\ (\llbracket\hat{G}_X\rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \upharpoonright r[a]) & \\
 & & \text{(I1, A3, A4, A5} \Rightarrow \text{Induction)} \\
= & \texttt{\textbf{rec}}\ X\ (\llbracket\hat{G}_X\rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis) \upharpoonright r[a] & \text{(Fig. VII.5.2)} \\
= & \texttt{\textbf{rec}}\ X\ \llbracket\hat{G}_X\rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \upharpoonright r[a] & \text{(Fig. VII.6.1)} \\
= & \llbracket\texttt{\textbf{rec}}\ X\ \hat{G}_X\rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \upharpoonright r[a] & \text{(Fig. VII.7.6)} \\
= & \llbracket\hat{G}\rrbracket \llparenthesis R[\{\tilde{z} \mapsto a + \delta\llbracket\hat{C}\rrbracket(z, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C})\}]\rrparenthesis \upharpoonright r[a] & \text{(Step)}
\end{array}$$

QED.

VIII.45 Proof of Theorem VII.8.7

- **A1.** $\langle \texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \textbf{do}\ \check{G}\ \textbf{;}\ \textbf{cont}, r[\check{C}] \rangle \in \operatorname{dom} \upharpoonright$
- **A2.** $\texttt{\textbf{self}} \notin \operatorname{dom} \psi$

By induction on A1 (Fig. VII.8.2b)

- **Base.** $\texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \textbf{do}\ \check{G}\ \textbf{;}\ \textbf{cont} \upharpoonright r[\check{C}] = \textbf{cont}$ **and** $\check{C} = \emptyset$

  Conclude:

$$\begin{array}{rlr}
 & (\texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \textbf{do}\ \check{G}\ \textbf{;}\ \textbf{cont} \upharpoonright r[\check{C}]) \langle\!\langle \psi \rangle\!\rangle & \\
= & \textbf{cont}\ \langle\!\langle \psi \rangle\!\rangle & \text{(Step)} \\
= & \textbf{cont} & \text{(Fig. VII.7.3)} \\
= & \texttt{\textbf{foreach}}\ R[\check{C} \cup (\check{C}_{\mathsf{co}} \langle\!\langle \psi \rangle\!\rangle)]\ \textbf{do}\ (\check{G} \langle\!\langle \psi \rangle\!\rangle)\ \textbf{;}\ \textbf{cont} \upharpoonright r[\check{C}] & \text{(Base} \Rightarrow \text{Fig. VII.8.2c)} \\
= & \texttt{\textbf{foreach}}\ R[(\check{C} \langle\!\langle \psi \rangle\!\rangle) \cup (\check{C}_{\mathsf{co}} \langle\!\langle \psi \rangle\!\rangle)]\ \textbf{do}\ (\check{G} \langle\!\langle \psi \rangle\!\rangle)\ \textbf{;}\ \textbf{cont} \upharpoonright r[\check{C} \langle\!\langle \psi \rangle\!\rangle] & \text{(Base} \Rightarrow \text{Lem. VII.3.6:6)} \\
= & \texttt{\textbf{foreach}}\ R[(\check{C} \cup \check{C}_{\mathsf{co}}) \langle\!\langle \psi \rangle\!\rangle]\ \textbf{do}\ (\check{G} \langle\!\langle \psi \rangle\!\rangle)\ \textbf{;}\ \textbf{cont} \upharpoonright r[\check{C} \langle\!\langle \psi \rangle\!\rangle] & \text{(Base} \Rightarrow \text{Lem. VII.3.6:8)} \\
= & \texttt{\textbf{foreach}}\ R[(\check{C} \cup \check{C}_{\mathsf{co}}) \langle\!\langle \psi \rangle\!\rangle]\ \textbf{do}\ (\check{G} \langle\!\langle \psi \rangle\!\rangle)\ \textbf{;}\ (\textbf{cont} \langle\!\langle \psi \rangle\!\rangle) \upharpoonright r[\check{C} \langle\!\langle \psi \rangle\!\rangle] & \text{(Fig. VII.7.3)} \\
= & \texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \textbf{do}\ \check{G}\ \textbf{;}\ \textbf{cont} \langle\!\langle \psi \rangle\!\rangle \upharpoonright r[\check{C} \langle\!\langle \psi \rangle\!\rangle] & \text{(Fig. VII.7.3)}
\end{array}$$

- **Step.** $\texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \textbf{do}\ \check{G}\ \textbf{;}\ \textbf{cont} \upharpoonright r[\check{C}] =$
  $(\check{G} \upharpoonright_{R[\check{C}]} r[z])\ \{\texttt{\textbf{foreach}}\ R[\check{C} \cup \check{C}_{\mathsf{co}}]\ \textbf{do}\ \check{G}\ \textbf{;}\ \textbf{cont} \upharpoonright r[\check{C} \setminus \{z\!:\!\check{D}\}]/\textbf{cont}\}$ **and**
  $\check{C} \neq \emptyset$ **and** $z\!:\!\check{D} = \max \langle \check{C}, \ll \rangle$

  - **B1.** Conclude:

$$\begin{array}{rlr}
 & z\!:\!\check{D} = \max \langle \check{C}, \ll \rangle & \text{(Step)} \\
\textbf{impl.} & z\!:\!\check{D} \in \check{C} & (-) \\
\textbf{impl.} & \check{C} = (\check{C} \setminus \{z\!:\!\check{D}\}) \cup \{z\!:\!\check{D}\} & (-) \\
\textbf{impl.} & \check{C} \cup \check{C}_{\mathsf{co}} = (\check{C} \setminus \{z\!:\!\check{D}\}) \cup (\{z\!:\!\check{D}\} \cup \check{C}_{\mathsf{co}}) & (-)
\end{array}$$

- **B2.** Conclude:

$$\check{C}\,\langle\!\langle\psi\rangle\!\rangle \neq \emptyset \qquad (\text{Step} \Rightarrow \text{Lem. VII.3.6:7})$$

- **B3.** Conclude:

$$z\!:\!\check{D}\,\langle\!\langle\psi\rangle\!\rangle = \max\langle \check{C}\,\langle\!\langle\psi\rangle\!\rangle, \ll\rangle \qquad (\text{Step} \Rightarrow \text{Thm. VII.3.5})$$

Conclude:

$$\begin{aligned}
&(\mathtt{foreach}\ R[\check{C}\cup\check{C}_{\mathsf{co}}]\ \mathtt{do}\ \check{G}\ \mathtt{;}\ \mathtt{cont}\upharpoonright r[\check{C}])\,\langle\!\langle\psi\rangle\!\rangle \\
={}&(\check{G}\upharpoonright_{R[\check{C}]} r[z])\,\{\mathtt{foreach}\ R[\check{C}\cup\check{C}_{\mathsf{co}}]\ \mathtt{do}\ \check{G}\ \mathtt{;}\ \mathtt{cont}\upharpoonright r[\check{C}\setminus\{z\!:\!\check{D}\}]/\mathtt{cont}\}\,\langle\!\langle\psi\rangle\!\rangle && (\text{Step}) \\
={}&(\check{G}\upharpoonright_{R[\check{C}]} r[z])\,\langle\!\langle\psi\rangle\!\rangle\,\{(\mathtt{foreach}\ R[\check{C}\cup\check{C}_{\mathsf{co}}]\ \mathtt{do}\ \check{G}\ \mathtt{;}\ \mathtt{cont}\upharpoonright r[\check{C}\setminus\{z\!:\!\check{D}\}])\,\langle\!\langle\psi\rangle\!\rangle/\mathtt{cont}\} \\
& && (\text{Thm. VII.7.1}) \\
={}&(\check{G}\upharpoonright_{R[\check{C}]} r[z])\,\langle\!\langle\psi\rangle\!\rangle && (\text{A2} \Rightarrow \text{Induction+B1}) \\
&\quad\{\mathtt{foreach}\ R[\check{C}\cup\check{C}_{\mathsf{co}}]\ \mathtt{do}\ \check{G}\ \mathtt{;}\ \mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle\upharpoonright r[(\check{C}\setminus\{z\!:\!\check{D}\})\,\langle\!\langle\psi\rangle\!\rangle]/\mathtt{cont}\} \\
={}&(\check{G}\upharpoonright_{R[\check{C}]} r[z])\,\langle\!\langle\psi\rangle\!\rangle && (\text{Lem. VII.3.6:9}) \\
&\quad\{\mathtt{foreach}\ R[\check{C}\cup\check{C}_{\mathsf{co}}]\ \mathtt{do}\ \check{G}\ \mathtt{;}\ \mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle\upharpoonright r[(\check{C}\,\langle\!\langle\psi\rangle\!\rangle)\setminus(\{z\!:\!\check{D}\}\,\langle\!\langle\psi\rangle\!\rangle)]/\mathtt{cont}\} \\
={}&(\check{G}\upharpoonright_{R[\check{C}]} r[z])\,\langle\!\langle\psi\rangle\!\rangle && (\text{Fig. VII.3.3}) \\
&\quad\{\mathtt{foreach}\ R[\check{C}\cup\check{C}_{\mathsf{co}}]\ \mathtt{do}\ \check{G}\ \mathtt{;}\ \mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle\upharpoonright r[(\check{C}\,\langle\!\langle\psi\rangle\!\rangle)\setminus(\{z\!:\!\check{D}\,\langle\!\langle\psi\rangle\!\rangle\})]/\mathtt{cont}\} \\
={}&(\check{G}\,\langle\!\langle\psi\rangle\!\rangle\upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]) && (\text{A2} \Rightarrow \text{Thm. VII.8.4}) \\
&\quad\{\mathtt{foreach}\ R[\check{C}\cup\check{C}_{\mathsf{co}}]\ \mathtt{do}\ \check{G}\ \mathtt{;}\ \mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle\upharpoonright r[(\check{C}\,\langle\!\langle\psi\rangle\!\rangle)\setminus(\{z\!:\!\check{D}\,\langle\!\langle\psi\rangle\!\rangle\})]/\mathtt{cont}\} \\
={}&(\check{G}\,\langle\!\langle\psi\rangle\!\rangle\upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]) && (\text{Fig. VII.7.3}) \\
&\quad\{\mathtt{foreach}\ R[(\check{C}\cup\check{C}_{\mathsf{co}})\,\langle\!\langle\psi\rangle\!\rangle]\ \mathtt{do}\ (\check{G}\,\langle\!\langle\psi\rangle\!\rangle)\ \mathtt{;}\ (\mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle)\upharpoonright r[(\check{C}\,\langle\!\langle\psi\rangle\!\rangle)\setminus(\{z\!:\!\check{D}\,\langle\!\langle\psi\rangle\!\rangle\})]/\mathtt{cont}\} \\
={}&(\check{G}\,\langle\!\langle\psi\rangle\!\rangle\upharpoonright_{R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]} r[z]) && (\text{Lem. VII.3.6:8}) \\
&\quad\{\mathtt{foreach}\ R[(\check{C}\,\langle\!\langle\psi\rangle\!\rangle)\cup(\check{C}_{\mathsf{co}}\,\langle\!\langle\psi\rangle\!\rangle)]\ \mathtt{do}\ (\check{G}\,\langle\!\langle\psi\rangle\!\rangle)\ \mathtt{;}\ (\mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle)\upharpoonright r[(\check{C}\,\langle\!\langle\psi\rangle\!\rangle)\setminus(\{z\!:\!\check{D}\,\langle\!\langle\psi\rangle\!\rangle\})]/\mathtt{cont}\} \\
={}&\mathtt{foreach}\ R[(\check{C}\,\langle\!\langle\psi\rangle\!\rangle)\cup(\check{C}_{\mathsf{co}}\,\langle\!\langle\psi\rangle\!\rangle)]\ \mathtt{do} && (\text{B2, B3} \Rightarrow \text{Fig. VII.8.2b}) \\
&\quad(\check{G}\,\langle\!\langle\psi\rangle\!\rangle)\ \mathtt{;}\ (\mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle)\upharpoonright r[\check{C}\,\langle\!\langle\psi\rangle\!\rangle] \\
={}&\mathtt{foreach}\ R[(\check{C}\cup\check{C}_{\mathsf{co}})\,\langle\!\langle\psi\rangle\!\rangle]\ \mathtt{do}\ (\check{G}\,\langle\!\langle\psi\rangle\!\rangle)\ \mathtt{;}\ (\mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle)\upharpoonright r[\check{C}\,\langle\!\langle\psi\rangle\!\rangle] && (\text{Lem. VII.3.6:8}) \\
={}&\mathtt{foreach}\ R[\check{C}\cup\check{C}_{\mathsf{co}}]\ \mathtt{do}\ \check{G}\ \mathtt{;}\ \mathtt{cont}\,\langle\!\langle\psi\rangle\!\rangle\upharpoonright r[\check{C}\,\langle\!\langle\psi\rangle\!\rangle] && (\text{Fig. VII.7.3})
\end{aligned}$$

QED.

VIII.46 Proof of Theorem VII.8.8

- **A1.** $\langle\mathtt{foreach}\ R[\hat{C}\cup\hat{C}_{\mathsf{co}}]\ \mathtt{do}\ \hat{G}\ \mathtt{;}\ \mathtt{cont}, r[\hat{C}]\rangle \in \operatorname{dom}\upharpoonright$
- **A2.** $\mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\},\{\mathtt{cont}\}}(\hat{G})$
- **A3.** $f\setminus\{\tilde{r}\mapsto f(\tilde{r})\mid\tilde{r}\in R\} : \mathbb{R}\rightharpoonup 2^{\mathbb{Z}}$

By induction on A1 (Fig. VII.8.2b)

- **Base.** $\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont} \upharpoonright r[\hat{C}] = \texttt{cont}$ **and** $\hat{C} = \emptyset$

  Conclude:

$$\begin{array}{lll} & \texttt{cont} \in \{\texttt{cont}\} & (-) \\ \textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})|\tilde{r}\in R\},\{\texttt{cont}\}}(\texttt{cont}) & \text{(Fig. VII.7.4)} \\ \textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})|\tilde{r}\in R\},\{\texttt{cont}\}}(\texttt{cont}\ \langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle) & \text{(Fig. VII.7.3)} \\ \textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})|\tilde{r}\in R\},\{\texttt{cont}\}}((\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont} \upharpoonright r[\hat{C}])\ \langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle) & \text{(Base)} \end{array}$$

- **Step.** $\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont} \upharpoonright r[\hat{C}] =$
  $(\hat{G} \upharpoonright_{R[\hat{C}]} r[z])\ \{\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont} \upharpoonright r[\hat{C} \setminus \{z\!:\!\hat{D}\}]/\texttt{cont}\}$ **and**
  $\hat{C} \neq \emptyset$ **and** $z\!:\!\hat{D} = \max\langle \hat{C}, \lll \rangle$

  - **B1.** Conclude:

$$\mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})|\tilde{r}\in R\},\{\texttt{cont}\}}((\hat{G} \upharpoonright_{R[\hat{C}]} r[z])\ \langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle) \qquad \text{(Step, A2, A3} \Rightarrow \text{Thm. VII.8.5)}$$

  - **B2.** Conclude:

$$\begin{array}{ll} \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})|\tilde{r}\in R\},\{\texttt{cont}\}}(& \text{(Step, A2, A3} \Rightarrow \text{Induction)} \\ \quad (\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont} \upharpoonright r[\hat{C} \setminus \{z\!:\!\hat{D}\}])\ \langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle) & \end{array}$$

  Conclude:

$$\begin{array}{lll} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})|\tilde{r}\in R\},\{\texttt{cont}\}}(& \text{(B1, B2} \Rightarrow \text{Thm. VII.7.2)} \\ & \quad (\hat{G} \upharpoonright_{R[\hat{C}]} r[z])\ \langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle & \\ & \qquad \{(\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont} \upharpoonright r[\hat{C} \setminus \{z\!:\!\hat{D}\}])\ \langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle/\texttt{cont}\}) & \\ \textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})|\tilde{r}\in R\},\{\texttt{cont}\}}(& \text{(Thm. VII.7.1)} \\ & \quad (\hat{G} \upharpoonright_{R[\hat{C}]} r[z])\ \{(\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont} \upharpoonright r[\hat{C} \setminus \{z\!:\!\hat{D}\}])/\texttt{cont}\}\ \langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle) & \\ \textsf{impl.} & \mathsf{Wf}_{f\setminus\{\tilde{r}\mapsto f(\tilde{r})|\tilde{r}\in R\},\{\texttt{cont}\}}((\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont} \upharpoonright r[\hat{C}])\ \langle\!\langle\{\texttt{self} \mapsto a\}\rangle\!\rangle) & \text{(Step)} \end{array}$$

QED.

VIII.47 Proof of Theorem VII.8.9

Proof of (1)

- **A1.** $\langle \texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont}, r[\hat{C}] \rangle \in \operatorname{dom} \upharpoonright$
- **A2.** $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont})$
- **A3.** $a \in [\![\hat{C}]\!](\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom} [\![\hat{C}]\!]$
- **A4.** $a \notin [\![\hat{C}_{\mathsf{co}}]\!](\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom} [\![\hat{C}_{\mathsf{co}}]\!]$
- **A5.** $r \in R$
- **A6.** $z_1\!:\!\hat{D}_1 = \max\langle \hat{C}, \lll \rangle$

- **A7.** $|\hat{C}| > 1$ **impl.** $z_2 : \hat{D}_2 = \max \langle \hat{C} \setminus \{z_1 : \hat{D}_1\}, \ll \rangle$
- **A8.** $[\![\hat{C}]\!](\tilde{z}) < [\![\hat{C}_{\mathsf{gr}}]\!](\tilde{z}_{\mathsf{gr}})$ **for-all** $\tilde{z} \in \operatorname{dom} [\![\hat{C}]\!], \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} [\![\hat{C}_{\mathsf{gr}}]\!]$
- **B1.** Conclude:

$$\begin{aligned} & z_1 : \hat{D}_1 = \max \langle \hat{C}, \ll \rangle && \text{(A6)} \\ \textbf{impl. } & z_1 : \hat{D}_1 \in \hat{C} && \text{(–)} \end{aligned}$$

By induction on A1 (Fig. VII.8.2b)

- **Base.** $\mathtt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;}\ \mathbf{cont} \upharpoonright r[\hat{C}] = \mathbf{cont}$ **and** $\hat{C} = \emptyset$

  Conclude:

$$\begin{aligned} & \textbf{false} && \text{(Base, B1)} \end{aligned}$$

- **Step.** $\mathtt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;}\ \mathbf{cont} \upharpoonright r[\hat{C}] =$
  $(\hat{G} \upharpoonright_{R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]} r[z])\, \{\mathtt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;}\ \mathbf{cont} \upharpoonright r[\hat{C} \setminus \{z : \hat{D}\}] / \mathbf{cont}\}$
  and $\hat{C} \neq \emptyset$ **and** $z : \hat{D} = \max \langle \hat{C}, \ll \rangle$

  - **C1.** Conclude:

$$\begin{aligned} & z_1 : \hat{D}_1 = \max \langle \hat{C}, \ll \rangle && \text{(A6)} \\ \textbf{impl. } & z_1 : \hat{D}_1 = z : \hat{D} && \text{(Step)} \end{aligned}$$

  - **C2.** Conclude:

$$\begin{aligned} & \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;}\ \mathbf{cont}) && \text{(A2)} \\ \textbf{impl. } & f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} \textbf{ and} && \text{(Fig. VII.7.4)} \\ & \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \in \checkmark \textbf{ and } \operatorname{expr} \hat{G} \cap \mathbb{G}_{\mathbf{rec}} = \emptyset \textbf{ and} && \\ & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) \mid \tilde{r} \in R\}, \{\mathbf{cont}\}}(\hat{G}) && \end{aligned}$$

  - **C3.** Conclude:

$$\begin{aligned} & z_1 : \hat{D}_1 \in \hat{C} && \text{(B1)} \\ \textbf{impl. } & z_1 \in \mathsf{vars}(\hat{C}) && \text{(Lem. VII.3.4:2)} \\ \textbf{impl. } & z_1 \in \operatorname{dom} [\![\hat{C}]\!] && \text{(Thm. VII.3.1)} \end{aligned}$$

  - **C4.** Conclude:

$$\begin{aligned} & \mathsf{len}\, [\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] > 0 && \text{(C2} \Rightarrow \text{Thm. VII.3.6)} \end{aligned}$$

  - **C5.** Conclude:

$$\begin{aligned} & \langle \mathtt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;}\ \mathbf{cont}, r[\hat{C}] \rangle \in \operatorname{dom} \upharpoonright && \text{(A1)} \\ \textbf{impl. } & \mathtt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;}\ \mathbf{cont} \in \hat{\mathbb{G}} && \text{(Lem. VII.8.2)} \\ \textbf{impl. } & \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \in \hat{\mathbb{C}} && \text{(–)} \\ \textbf{impl. } & \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \in \operatorname{dom} [\![\cdot]\!] && \text{(Lem. VII.3.7:1)} \end{aligned}$$

- **C6.** Conclude:

$$\begin{array}{rll} & z_1 \in \mathrm{dom}\,\llbracket \hat{C} \rrbracket & \text{(C3)} \\ \textbf{impl.} & a \in \llbracket \hat{C} \rrbracket(z_1) & \text{(A3)} \\ \textbf{impl.} & a \in \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_1) & \text{(C5} \Rightarrow \text{Lem. VII.3.7:5)} \end{array}$$

- **C7.** Conclude:

$$\langle \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket, z_1[a] \rangle \in \mathrm{dom}\,\mathsf{from} \qquad \text{(C4, C6} \Rightarrow \text{Fig. VII.2.6)}$$

- **C8.** Conclude:

$$\begin{array}{rll} & a + \delta\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_1, z') & (\langle z_1, z' \rangle \in \mathrm{dom}\,\delta\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket,\ \exists z') \\ = & a + \delta(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_1), \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z')) & \text{(Lem. VII.2.8:3)} \\ = & a + \delta((\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])(z_1), (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])(z')) & \\ & & \text{(C7} \Rightarrow \text{Thm. VII.2.8:2)} \\ = & a + & \text{(Thm. VII.2.1)} \\ & \delta(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])(z_1), \mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])(z')) & \\ = & a + & \text{(Lem. VII.2.6:3)} \\ & \delta((\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z_1), (\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z')) & \\ = & (\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z_1) + & \text{(C7} \Rightarrow \text{Thm. VII.2.7:1)} \\ & \delta((\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z_1), (\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z')) & \end{array}$$

- **C9.** Conclude:

$$\begin{array}{rll} & \mathrm{dom}\,\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket = \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) & \text{(Thm. VII.3.1)} \\ \textbf{impl.} & \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]) = \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) & \text{(C7} \Rightarrow \text{Lem. VII.2.12:2)} \\ \textbf{impl.} & \mathrm{dom}\,(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])) \subseteq \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) & \text{(Lem. VII.2.6:2)} \\ \textbf{impl.} & \mathrm{dom}\,(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])) \subseteq \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) \subseteq \mathbb{Z} & \\ & & \text{(Lem. VII.3.4:1)} \end{array}$$

- **C10.** Conclude:

$$\begin{array}{rll} & \llbracket (\hat{G} \restriction_{R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]} r[z_1])\ \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket & (\langle \hat{G}, R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}], r[z_1] \rangle \in \restriction) \\ = & \llbracket \hat{G} \rrbracket\ (\!(R[\{\tilde{z} \mapsto a + \delta\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_1, \tilde{z}) \mid \tilde{z} \in \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}})\}])\!) \restriction r[a] & \\ & & \text{(C2, A5, C3} \Rightarrow \text{Thm. VII.8.6)} \\ = & \llbracket \hat{G} \rrbracket\ (\!(R[\left\{ \begin{array}{c} \tilde{z} \mapsto \\ (\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z_1) + \\ \delta((\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z_1), \\ (\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(\tilde{z})) \end{array} \middle| \ \tilde{z} \in \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) \right\}])\!) \restriction r[a] & \\ & & \text{(C8)} \\ = & \llbracket \hat{G} \rrbracket\ (\!(R[\left\{ \begin{array}{c} \tilde{z} \mapsto \\ (\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z_1) + \\ \delta((\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(z_1), \\ (\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))(\tilde{z})) \end{array} \middle| \ \tilde{z} \in \mathbb{Z} \right\}])\!) \restriction r[a] & \text{(C9)} \\ = & \llbracket \hat{G} \rrbracket\ (\!(R[(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))/z_1])\!) \restriction r[a] & \text{(Fig. VII.2.4)} \\ = & \llbracket \hat{G} \rrbracket\ (\!(R[\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])])\!) \restriction r[a] & \text{(Lem. VII.2.5:2)} \end{array}$$

- **C11.** Conclude:

$$\operatorname{expr}[\![\hat{G}]\!] \cap \mathbb{G}_{\mathtt{rec}} = \emptyset \qquad \text{(C2} \Rightarrow \text{Lem. VII.7.7:2)}$$

- **C12.** Conclude:

$$\begin{aligned} & \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \in \checkmark && \text{(C2)} \\ \textbf{impl. } & \hat{C} \in \checkmark && \text{(Lem. VII.3.10:4)} \end{aligned}$$

By case distinction:

- **Case.** $|\hat{C}| = 0$
  Conclude:

$$\begin{aligned} & |\hat{C}| = 0 && \text{(Case)} \\ \textbf{impl. } & \hat{C} = \emptyset && (-) \\ \textbf{impl. } & \textbf{false} && \text{(B1)} \end{aligned}$$

- **Case.** $|\hat{C}| = 1$
  - **D1.** Conclude:

$$\begin{aligned} & z\!:\!\hat{D} = \max\langle \hat{C}, \ll \rangle && \text{(Step)} \\ \textbf{impl. } & z\!:\!\hat{D} \in \hat{C} && (-) \\ \textbf{impl. } & z\!:\!\hat{D} \in \hat{C} \;\textbf{ and }\; |\hat{C}| = 1 && \text{(Case)} \\ \textbf{impl. } & \hat{C} \setminus \{z\!:\!\hat{D}\} = \emptyset && (-) \end{aligned}$$

  - **D2.** Conclude:

$$\begin{aligned} & ([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a])(\tilde{z}) \neq \emptyset && \text{(C7} \Rightarrow \text{Thm. VII.2.7:3)} \\ & \quad \textbf{for-all } \tilde{z} \in \operatorname{dom}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a]) \\ \textbf{impl. } & \operatorname{dom}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a]) \subseteq \operatorname{dom}(\mathsf{tail}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a])) \;\textbf{ and} \\ & \operatorname{dom}(\mathsf{tail}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a])) \subseteq \operatorname{dom}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a]) \\ & && \text{(Lem. VII.2.7:2)} \\ \textbf{impl. } & \operatorname{dom}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a]) = \operatorname{dom}(\mathsf{tail}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a])) && (-) \end{aligned}$$

  - **D3.** Conclude:

$$\begin{aligned} & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) \mid \tilde{r} \in R\}, \{\mathtt{cont}\}}([\![\hat{G}]\!]) && \text{(C2} \Rightarrow \text{Thm. VII.7.3)} \\ \textbf{impl. } & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \operatorname{dom}[\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \mid \tilde{r} \in R\}, \{\mathtt{cont}\}}([\![\hat{G}]\!]) && \text{(Thm. VII.3.1)} \\ \textbf{impl. } & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \operatorname{dom}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a]) \mid \tilde{r} \in R\}, \{\mathtt{cont}\}}([\![\hat{G}]\!]) && \text{(C7} \Rightarrow \text{Lem. VII.2.12:2)} \\ \textbf{impl. } & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \operatorname{dom}(\mathsf{tail}([\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!] \;\mathsf{from}\; z_1[a])) \mid \tilde{r} \in R\}, \{\mathtt{cont}\}}([\![\hat{G}]\!]) && \text{(D2)} \end{aligned}$$

  - **D4.** Conclude:

$$\begin{aligned} & \langle [\![\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\!], z_1[a] \rangle \in \operatorname{dom}\mathsf{from} && \text{(C7)} \\ \textbf{impl. } & \langle [\![\hat{C} \cup \hat{C}_{\mathsf{gr}}]\!] \cup [\![\hat{C}_{\mathsf{co}}]\!], z_1[a] \rangle \in \operatorname{dom}\mathsf{from} && \text{(Lem. VII.3.7:4)} \end{aligned}$$

- **D5.** Conclude:

$$
\begin{array}{lr}
|\hat{C}| = \mathtt{1} \ \ \textsf{\textbf{and}} \ \ z_1 : \hat{D}_1 = \max \langle \hat{C}, \ll \rangle & \text{(Case, A6)} \\
\textsf{\textbf{impl.}} \ z_1 : \hat{D}_1 = \min \langle \hat{C}, \ll \rangle & (-)
\end{array}
$$

- **D6.** Conclude:

$$
\begin{array}{lr}
\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \in \operatorname{dom} \llbracket \cdot \rrbracket & \text{(C5)} \\
\textsf{\textbf{impl.}} \ \hat{C} \cup \hat{C}_{\mathsf{gr}} \in \operatorname{dom} \llbracket \cdot \rrbracket & \text{(Fig. VII.3.4)}
\end{array}
$$

- **D7.** Conclude:

$$
\begin{array}{lr}
\llbracket \hat{C} \rrbracket(z_1) = \min \langle \operatorname{img} \llbracket \hat{C} \rrbracket, < \rangle & \text{(C12, D5} \Rightarrow \text{Thm. VII.3.8:2)} \\
\textsf{\textbf{impl.}} \ \llbracket \hat{C} \rrbracket(z_1) = \min \langle \{ \llbracket \hat{C} \rrbracket(\tilde{z}) \mid \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket \}, < \rangle & (-) \\
\textsf{\textbf{impl.}} \ \Big[\llbracket \hat{C} \rrbracket(z_1) \neq \llbracket \hat{C} \rrbracket(\tilde{z}) \ \textsf{\textbf{impl.}} \ \llbracket \hat{C} \rrbracket(z_1) < \llbracket \hat{C} \rrbracket(\tilde{z}) \Big] \ \textsf{\textbf{for-all}} \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket & (-) \\
\textsf{\textbf{impl.}} \ \begin{bmatrix} \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) \neq \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \ \textsf{\textbf{impl.}} \\ \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) < \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \end{bmatrix} \ \textsf{\textbf{for-all}} \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket & \\
 & \text{(D6} \Rightarrow \text{Lem. VII.3.7:5)}
\end{array}
$$

- **D8.** Conclude:

$$
\begin{array}{lr}
z_1 \in \operatorname{dom} \llbracket \hat{C} \rrbracket & \text{(C3)} \\
\textsf{\textbf{impl.}} \ \llbracket \hat{C} \rrbracket(z_1) < \llbracket \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \ \textsf{\textbf{for-all}} \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket & \text{(A8)} \\
\textsf{\textbf{impl.}} \ \Big[\llbracket \hat{C} \rrbracket(z_1) \neq \llbracket \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \ \textsf{\textbf{impl.}} \ \llbracket \hat{C} \rrbracket(z_1) < \llbracket \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \Big] \ \textsf{\textbf{for-all}} \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket & (-) \\
\textsf{\textbf{impl.}} \ \begin{bmatrix} \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) \neq \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \ \textsf{\textbf{impl.}} \\ \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) < \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \end{bmatrix} \ \textsf{\textbf{for-all}} \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket & \\
 & \text{(D6} \Rightarrow \text{Lem. VII.3.7:5)}
\end{array}
$$

- **D9.** Conclude:

$$
\begin{array}{lr}
\Big[\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) \neq \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \ \textsf{\textbf{impl.}} \ \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) < \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \Big] & \\
 & \text{(D7, D8)} \\
\quad \textsf{\textbf{for-all}} \ \tilde{z} \in (\operatorname{dom} \llbracket \hat{C} \rrbracket) \cup (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) & \\
\textsf{\textbf{impl.}} \ \Big[\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) \neq \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \ \textsf{\textbf{impl.}} \ \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) < \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \Big] & (-) \\
\quad \textsf{\textbf{for-all}} \ \tilde{z} \in \operatorname{dom} (\llbracket \hat{C} \rrbracket \cup \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) & \\
\textsf{\textbf{impl.}} \ \begin{bmatrix} \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) \neq \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \ \textsf{\textbf{impl.}} \\ \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) < \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}) \end{bmatrix} \ \textsf{\textbf{for-all}} \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket & \\
 & \text{(D6} \Rightarrow \text{Lem. VII.3.7:4)} \\
\textsf{\textbf{impl.}} \ \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1) = \min \langle \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket, < \rangle & (-)
\end{array}
$$

- **D10.** Conclude:

$$
\begin{array}{lr}
a \notin \bigcup \operatorname{img} (\mathsf{tail} \, ((\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \rrbracket \cup \llbracket \hat{C}_{\mathsf{co}} \rrbracket) \ \mathsf{from} \ z_1[a])) & \\
 & \text{(D4, D9, A4} \Rightarrow \text{Thm. VII.2.9:2)} \\
\textsf{\textbf{impl.}} \ a \notin \bigcup \operatorname{img} (\mathsf{tail} \, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \ \mathsf{from} \ z_1[a])) & \text{(C5} \Rightarrow \text{Lem. VII.3.7:4)}
\end{array}
$$

- **D11.** Conclude:

$$\begin{array}{rlr} & \langle \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket, z_1[a] \rangle \in \mathsf{from} & \text{(D10)} \\ \textbf{impl.} & \mathsf{len}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a]) > 0 & \text{(Thm. VII.2.7:2)} \\ \textbf{impl.} & \mathsf{len}\,(\mathsf{tail}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a])) < \mathsf{len}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a]) & \\ & & \text{(Thm. VII.2.5)} \end{array}$$

Conclude:

$$\begin{array}{rlr} & \llbracket (\mathbf{foreach}\; R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\; \mathbf{do}\; \hat{G}\, \mathbf{;}\, \mathbf{cont} \upharpoonright r[\hat{C}])\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \\ = & \llbracket (\hat{G} \upharpoonright_{R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]} r[z]) & \text{(Step)} \\ & \quad \{\mathbf{foreach}\; R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\; \mathbf{do}\; \hat{G}\, \mathbf{;}\, \mathbf{cont} \upharpoonright r[\hat{C} \setminus \{z : \hat{D}\}]/\mathbf{cont}\}\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \\ = & \llbracket (\hat{G} \upharpoonright_{R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]} r[z]\, \{\mathbf{cont}/\mathbf{cont}\})\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \text{(D1} \Rightarrow \text{Fig. VII.8.2b)} \\ = & \llbracket (\hat{G} \upharpoonright_{R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]} r[z])\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \text{(Lem. VII.7.6:2)} \\ = & \llbracket (\hat{G} \upharpoonright_{R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]} r[z_1])\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle \rrbracket & \text{(C1)} \\ = & \llbracket \hat{G} \rrbracket\, (\!(R[\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a])])\!) \upharpoonright r[a] & \text{(C10)} \\ = & (\llbracket \hat{G} \rrbracket\, (\!(R[\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a])])\!) \upharpoonright r[a])\, \{\mathbf{cont}/\mathbf{cont}\} & \text{(Lem. VII.4.2:2)} \\ = & (\llbracket \hat{G} \rrbracket\, (\!(R[\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a])])\!) \upharpoonright r[a]) & \\ & \quad \{\mathsf{iter}(\llbracket \hat{G} \rrbracket, \mathbf{cont}, R, \mathsf{tail}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a])) \upharpoonright r[a]/\mathbf{cont}\} & \\ & & \text{(D11, D3, C11, A5, D10} \Rightarrow \text{Thm. VII.6.13)} \\ = & \llbracket \hat{G} \rrbracket\, (\!(R[\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a])])\!) & \text{(Thm. VII.5.2)} \\ & \quad \{\mathsf{iter}(\llbracket \hat{G} \rrbracket, \mathbf{cont}, R, \mathsf{tail}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a]))/\mathbf{cont}\} \upharpoonright r[a] & \\ = & \mathsf{iter}(\llbracket \hat{G} \rrbracket, \mathbf{cont}, R, \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \;\mathsf{from}\; z_1[a]) \upharpoonright r[a] & \text{(Thm. VII.2.7:2} \Rightarrow \text{Fig. VII.6.2)} \end{array}$$

- **Case.** $|\hat{C}| > 1$
  - **E1.** Conclude:

$$\begin{array}{rlr} & \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) \mid \tilde{r} \in R\}, \{\mathbf{cont}\}}(\hat{G}) & \text{(C2)} \\ \textbf{impl.} & \mathsf{Wf}_{f, \{\mathbf{cont}\}}(\hat{G}) & \text{(Lem. VII.7.5:1)} \\ \textbf{impl.} & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \{\mathbf{cont}\}}(\hat{G}) & \text{(Lem. VII.7.5:1)} \end{array}$$

  - **E2.** Conclude:

$$\begin{array}{rlr} & f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} & \text{(C2)} \\ \textbf{impl.} & f : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} & \text{(–)} \\ \textbf{impl.} & f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} & \text{(–)} \end{array}$$

  - **E3.** Conclude:

$$\begin{array}{lr} \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \{\mathbf{cont}\}}(& \text{(Step, E1, E2} \Rightarrow \text{Thm. VII.8.5)} \\ \quad (\hat{G} \upharpoonright_{R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]} r[z])\, \langle\!\langle \{\mathbf{self} \mapsto a\} \rangle\!\rangle) & \end{array}$$

  - **E4.** Conclude:

$$\begin{array}{rlr} & z_1 : \hat{D}_1 \in \hat{C} & \text{(B1)} \\ \textbf{impl.} & \hat{C} = (\hat{C} \setminus \{z_1 : \hat{D}_1\}) \cup \{z_1 : \hat{D}_1\} & \text{(–)} \\ \textbf{impl.} & \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} = (\hat{C} \setminus \{z_1 : \hat{D}_1\}) \cup (\{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}}) \cup \hat{C}_{\mathsf{co}} & \text{(–)} \end{array}$$

- **E5.** Conclude:

  $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont})$ (A2)

  impl. $\mathsf{Wf}_{f,\mathcal{X}}(\texttt{foreach}\ R[(\hat{C} \setminus \{z_1 : \hat{D}_1\}) \cup (\{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}}) \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{;}\ \texttt{cont})$ (E4)

- **E6.** Conclude:

  $z_1 : \hat{D}_1 = \max \langle \hat{C}, \ll \rangle$ (A6)

  impl. $z_1 : \hat{D}_1 = z : \hat{D}$ (Step)

- **E7.** Conclude:

  $|\hat{C}| > 1$ (Case)

  impl. $z_2 : \hat{D}_2 = \max \langle \hat{C} \setminus \{z_1 : \hat{D}_1\}, \ll \rangle$ (A7)

- **E8.** Conclude:

  $\llbracket \hat{C} \rrbracket(z_1) = \max \langle \mathrm{img}\, \llbracket \hat{C} \rrbracket, < \rangle$ (C12, A6 ⇒ Thm. VII.3.8:3)

- **E9.** Conclude:

  $\llbracket \hat{C} \rrbracket(z_1) = \max \langle \mathrm{img}\, \llbracket \hat{C} \rrbracket, < \rangle$ (E8)

  impl. $\llbracket \hat{C} \rrbracket(z_1) = \max \langle \{\llbracket \hat{C} \rrbracket(\tilde{z}) \mid \tilde{z} \in \mathrm{dom}\, \llbracket \hat{C} \rrbracket\}, < \rangle$ (–)

  impl. $\Big[\llbracket \hat{C} \rrbracket(z_1) \neq \llbracket \hat{C} \rrbracket(\tilde{z})$ **impl.** $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \hat{C} \rrbracket(z_1)\Big]$ **for-all** $\tilde{z} \in \mathrm{dom}\, \llbracket \hat{C} \rrbracket$ (–)

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \hat{C} \rrbracket(z_1)$ **for-all** $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}$ (–)

- **E10.** Conclude:

  $\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \in \mathrm{dom}\, \llbracket \cdot \rrbracket$ (C5)

  impl. $(\hat{C} \setminus \{z_1 : \hat{D}_1\}) \cup (\{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}}) \cup \hat{C}_{\mathsf{co}} \in \mathrm{dom}\, \llbracket \cdot \rrbracket$ (E4)

  impl. $\{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \in \mathrm{dom}\, \llbracket \cdot \rrbracket$ (Fig. VII.3.4)

- **E11.** Conclude:

  $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \hat{C} \rrbracket(z_1)$ **for-all** $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}$ (D9)

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \hat{D}_1 \rrbracket$ **for-all** $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}$ (B1 ⇒ Lem. VII.3.7:3)

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \{z_1 \mapsto \llbracket \hat{D}_1 \rrbracket\}(z_1)$ **for-all** $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}$ (–)

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \rrbracket(z_1)$ **for-all** $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}$ (Fig. VII.3.4)

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_1)$ **for-all** $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}$
  (E10 ⇒ Lem. VII.3.7:5)

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_{\mathsf{gr}})$ **for-all** $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}, \tilde{z}_{\mathsf{gr}} \in \{z_1\}$ (–)

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_{\mathsf{gr}})$ (–)
  for-all $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}, \tilde{z}_{\mathsf{gr}} \in \mathrm{dom}\, \{z_1 \mapsto \llbracket \hat{D}_1 \rrbracket\}$

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_{\mathsf{gr}})$ (Fig. VII.3.4)
  for-all $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}, \tilde{z}_{\mathsf{gr}} \in \mathrm{dom}\, \llbracket \{z_1 \mapsto \hat{D}_1\} \rrbracket$

  impl. $\llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(z_{\mathsf{gr}})$ (B1 ⇒ Lem. VII.3.7:3)
  for-all $\tilde{z} \in (\mathrm{dom}\, \llbracket \hat{C} \rrbracket) \setminus \{z_1\}, \tilde{z}_{\mathsf{gr}} \in \mathrm{dom}\, \llbracket \{z_1 : \hat{D}_1\} \rrbracket$

- **E12.** Conclude:

$$\begin{array}{rlr}
& \llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}})\ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket, \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket & \text{(A8)} \\
\textbf{impl.} & \llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}})\ \ \textbf{for-all}\ \ \tilde{z} \in (\operatorname{dom} \llbracket \hat{C} \rrbracket) \setminus \{z_1\}, \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket & \text{(–)}
\end{array}$$

- **E13.** Conclude:

$$\begin{array}{rlr}
& \left[\begin{array}{l} \llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}}) \\ \ \textbf{for-all}\ \ \tilde{z} \in (\operatorname{dom} \llbracket \hat{C} \rrbracket) \setminus \{z_1\}, \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} \llbracket \{z_1 : \hat{D}_1\} \rrbracket \end{array}\right] \textbf{ and} & \text{(E11, E12)} \\
& \left[\begin{array}{l} \llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}}) \\ \ \textbf{for-all}\ \ \tilde{z} \in (\operatorname{dom} \llbracket \hat{C} \rrbracket) \setminus \{z_1\}, \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket \end{array}\right] & \\
\textbf{impl.} & \llbracket \hat{C} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}}) & \text{(–)} \\
& \ \ \textbf{for-all}\ \ \tilde{z} \in (\operatorname{dom} \llbracket \hat{C} \rrbracket) \setminus \{z_1\}, \tilde{z}_{\mathsf{gr}} \in (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) \cup (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) & \\
\textbf{impl.} & (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \llbracket \hat{C} \rrbracket(z_1)\})(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}}) & \text{(C3)} \\
& \ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \llbracket \hat{C} \rrbracket(z_1)\}), \tilde{z}_{\mathsf{gr}} \in (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) \cup (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) & \\
\textbf{impl.} & (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \hat{D}_1\})(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}}) & \text{(B1} \Rightarrow \text{Lem. VII.3.7:3)} \\
& \ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \hat{D}_1\}), \tilde{z}_{\mathsf{gr}} \in (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) \cup (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) & \\
\textbf{impl.} & \llbracket \hat{C} \setminus \{z_1 : \hat{D}_1\} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}}) & \text{(Lem. VII.3.7:6)} \\
& \ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \setminus \{z_1 : \hat{D}_1\} \rrbracket, \tilde{z}_{\mathsf{gr}} \in (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) \cup (\operatorname{dom} \llbracket \hat{C}_{\mathsf{gr}} \rrbracket) & \\
\textbf{impl.} & \llbracket \hat{C} \setminus \{z_1 : \hat{D}_1\} \rrbracket(\tilde{z}) < \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket(\tilde{z}_{\mathsf{gr}}) & \text{(E10} \Rightarrow \text{Lem. VII.3.7:4)} \\
& \ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \setminus \{z_1 : \hat{D}_1\} \rrbracket, \tilde{z}_{\mathsf{gr}} \in \operatorname{dom} \llbracket \{z_1 : \hat{D}_1\} \cup \hat{C}_{\mathsf{gr}} \rrbracket &
\end{array}$$

- **E14.** Conclude:

$$\begin{array}{rlr}
& a \in \llbracket \hat{C} \rrbracket(\tilde{z})\ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket & \text{(A3)} \\
\textbf{impl.} & a \in \llbracket \hat{C} \rrbracket(\tilde{z})\ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \rrbracket \setminus \{z_1\} & \text{(–)} \\
\textbf{impl.} & a \in (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \llbracket \hat{C} \rrbracket(z_1)\})(\tilde{z})\ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \llbracket \hat{C} \rrbracket(z_1)\}) & \text{(C3)} \\
\textbf{impl.} & a \in (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \hat{D}_1\})(\tilde{z}) & \text{(B1} \Rightarrow \text{Lem. VII.3.7:3)} \\
& \ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \hat{D}_1\}) & \\
\textbf{impl.} & a \in \llbracket \hat{C} \setminus \{z_1 : \hat{D}_1\} \rrbracket(\tilde{z})\ \ \textbf{for-all}\ \ \tilde{z} \in \operatorname{dom} \llbracket \hat{C} \setminus \{z_1 : \hat{D}_1\} \rrbracket & \text{(Lem. VII.3.7:6)}
\end{array}$$

- **E15.** Conclude:

$$\begin{array}{rlr}
& \mathsf{len}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]) > \mathsf{o} & \text{(C7} \Rightarrow \text{Thm. VII.2.7:2)}
\end{array}$$

- **E16.** Conclude:

$$\begin{array}{rlr}
& z_2 : \hat{D}_2 = \max \langle \hat{C} \setminus \{z_1 : \hat{D}_1\}, \ll \rangle & \text{(E7)} \\
\textbf{impl.} & z_2 : \hat{D}_2 \in \hat{C} \setminus \{z_1 : \hat{D}_1\} & \text{(–)} \\
\textbf{impl.} & z_2 \in \operatorname{dom} \llbracket \hat{C} \setminus \{z_1 : \hat{D}_1\} \rrbracket & \text{(Lem. VII.3.7:2)} \\
\textbf{impl.} & z_2 \in \operatorname{dom} (\llbracket \hat{C} \rrbracket \setminus \{z_1 \mapsto \llbracket \hat{D}_1 \rrbracket\}) & \text{(Lem. VII.3.7:6)} \\
\textbf{impl.} & z_2 \in (\operatorname{dom} \llbracket \hat{C} \rrbracket) \setminus \operatorname{dom} \{z_1 \mapsto \llbracket \hat{D}_1 \rrbracket\} & \text{(–)} \\
\textbf{impl.} & z_2 \in (\operatorname{dom} \llbracket \hat{C} \rrbracket) \setminus \{z_1\} & \text{(–)} \\
\textbf{impl.} & \llbracket \hat{C} \rrbracket(z_2) < \llbracket \hat{C} \rrbracket(z_1) & \text{(E9)}
\end{array}$$

- **E17.** Conclude:

$z_2 : \hat{D}_2 = \max \langle \hat{C} \setminus \{z_1 : \hat{D}_1\}, \ll \rangle$ (E7)

impl. $z_2 : \hat{D}_2 \in \hat{C} \setminus \{z_1 : \hat{D}_1\}$ (–)

- **E18.** Conclude:

$z_2 : \hat{D}_2 \in \hat{C} \setminus \{z_1 : \hat{D}_1\}$ (E17)

impl. $z_2 : \hat{D}_2 \in \hat{C}$ (–)

- **E19.** Conclude:

$z_2 : \hat{D}_2 \in \hat{C}$ (E18)

impl. $z_2 \in \mathsf{vars}(\hat{C})$ (Lem. VII.3.4:2)

impl. $z_2 \in \mathrm{dom}\, \llbracket \hat{C} \rrbracket$ (Thm. VII.3.1)

impl. $a \in \llbracket \hat{C} \rrbracket(z_2)$ (A3)

impl. $a \in \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_2)$ (C5 ⇒ Lem. VII.3.7:5)

- **E20.** Conclude:

$a \in (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a])(z_2)$ (C7, E16, E19 ⇒ Thm. VII.2.7:5)

- **E21.** Conclude:

$z_1 : \hat{D}_1 = \max \langle \hat{C}, \ll \rangle$ (A6)

impl. $\tilde{z} : \tilde{\hat{D}} \ll z_1 : \hat{D}_1$ **for-all** $\tilde{z} : \tilde{\hat{D}} \in \hat{C} \setminus \{z_1 : \hat{D}_1\}$ (–)

impl. $z_2 : \hat{D}_2 \ll z_1 : \hat{D}_1$ (E17)

impl. $\hat{C} \in \checkmark$ **and** $z_2 : \hat{D}_2, z_1 : \hat{D}_1 \in \hat{C}$ **and** $z_2 : \hat{D}_2 \ll z_1 : \hat{D}$ (C12, E18, B1)

impl. $\llbracket \hat{C} \rrbracket(z_2) < \llbracket \hat{C} \rrbracket(z_1)$ (Thm. VII.3.8:1)

- **E22.** Conclude:

$\llbracket \hat{C} \rrbracket(z_2) < \llbracket \hat{C} \rrbracket(z_1)$ (E21)

impl. $\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_2) < \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_1)$ (C5 ⇒ Lem. VII.3.7:5)

impl. $\langle \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket, z_1[a] \rangle \in \mathrm{dom}\, \mathsf{from}$ **and** (C7)
$\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_2) < \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket(z_1)$

impl. $(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a])(z_2) < (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a])(z_1)$
(Thm. VII.2.7:4)

impl. $\mathsf{head}\, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a])(z_2) < \mathsf{head}\, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a])(z_1)$ **or**
$(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a])(z_1) = \emptyset$ (Fig. VII.2.2)

impl. $\mathsf{head}\, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a])(z_2) < \mathsf{head}\, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a])(z_1)$
(C6 ⇒ Thm. VII.2.7:3)

impl. $(\mathsf{head}\, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a]))(z_2) < (\mathsf{head}\, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a]))(z_1)$
(Lem. VII.2.6:3)

impl. $(\mathsf{head}\, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a]))(z_2) < a$ (Thm. VII.2.7:1)

impl. $(\mathsf{head}\, (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket \; \mathsf{from} \; z_1[a]))(z_2) \neq a$ (Fig. VII.2.1:3)

- **E23.** Conclude:

$\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]) =$ (E15, E20, E22 $\Rightarrow$ Thm. VII.2.6:1)
$\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])$

impl. $\langle \llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a], z_2[a] \rangle \in \mathrm{dom}\, \mathsf{to}$ (–)

impl. $\mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]) =$ (Lem. VII.2.11:2)
$\mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])$

- **E24.** Conclude:

$(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])(\tilde{z}) \neq \emptyset$ (C7 $\Rightarrow$ Thm. VII.2.7:3)
for-all $\tilde{z} \in \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])$

impl. $\mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]) \subseteq \mathrm{dom}\,(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))$ **and**
$\mathrm{dom}\,(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])) \subseteq \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])$
(Lem. VII.2.6:2)

impl. $\mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]) = \mathrm{dom}\,(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))$
(–)

- **E25.** Conclude:

$(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])(z') = \emptyset$ ($\exists z'$)

impl. $\langle (\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])(z'), < \rangle \notin \mathrm{dom}\, \mathrm{min}$ (–)

impl. $(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])(z') \notin \mathrm{dom}\, \mathsf{head}$ (Fig. VII.2.2)

impl. $z' \notin \mathrm{dom}\,\{\tilde{z} \mapsto \mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])(\tilde{z}) \mid \tilde{z} \in \mathbb{Z}\}$ (–)

impl. $z' \notin \mathrm{dom}\,(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]))$ (Fig. VII.2.5)

impl. $z' \notin \mathrm{dom}\,(\mathsf{head}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]))$
(E15, E20, E22 $\Rightarrow$ Thm. VII.2.6:1)

impl. $z' \notin \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])$ (E24)

- **E26.** Conclude:

$(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])(z') = \emptyset$ **and** ($\exists z'$)
$z' \in \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])$

impl. $(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])(z') = \emptyset$ **and** (Lem. VII.2.11:2)
$z' \in \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a])$

impl. **false** (E25)

- **E27.** Conclude:

$(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])(\tilde{z}) \neq \emptyset$ (E26)
for-all $\tilde{z} \in \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])$

impl. $\begin{bmatrix} \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]) \subseteq \\ \mathrm{dom}\,(\mathsf{tail}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])) \end{bmatrix}$ **and** (Lem. VII.2.7:2)
$\begin{bmatrix} \mathrm{dom}\,(\mathsf{tail}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])) \subseteq \\ \mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]) \end{bmatrix}$

impl. $\mathrm{dom}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]) =$ (–)
$\mathrm{dom}\,(\mathsf{tail}\,(\llbracket \hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}} \rrbracket\ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]))$

- **E28.** Conclude:

$\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathsf{vars}(\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}})\mid\tilde{r}\in R\},\{\mathbf{cont}\}}(\llbracket\hat{G}\rrbracket)$ (C2 ⇒ Thm. VII.7.3)

impl. $\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathrm{dom}\,\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\mid\tilde{r}\in R\},\{\mathbf{cont}\}}(\llbracket\hat{G}\rrbracket)$ (Thm. VII.3.1)

impl. $\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathrm{dom}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a])\mid\tilde{r}\in R\},\{\mathbf{cont}\}}(\llbracket\hat{G}\rrbracket)$ (C7 ⇒ Lem. VII.2.12:2)

impl. $\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathrm{dom}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])\mid\tilde{r}\in R\},\{\mathbf{cont}\}}(\llbracket\hat{G}\rrbracket)$ (E23)

impl. $\mathsf{Wf}_{f\cup\{\tilde{r}\mapsto\mathrm{dom}\,(\mathsf{tail}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a]))\mid\tilde{r}\in R\},\{\mathbf{cont}\}}(\llbracket\hat{G}\rrbracket)$ (E27)

- **E29.** Conclude:

$\llbracket\hat{C}\setminus\{z_1:\hat{D}_1\}\rrbracket(z_2)=\max\langle\mathrm{img}\,\llbracket\hat{C}\setminus\{z_1:\hat{D}_1\}\rrbracket,<\rangle$
(C12, E7 ⇒ Thm. VII.3.8:3)

impl. $(\llbracket\hat{C}\rrbracket\setminus\{z_1\mapsto\llbracket\hat{D}_1\rrbracket\})(z_2)=\max\langle\mathrm{img}\,(\llbracket\hat{C}\rrbracket\setminus\{z_1\mapsto\llbracket\hat{D}_1\rrbracket\}),<\rangle$
(Lem. VII.3.7:6)

impl. $(\llbracket\hat{C}\rrbracket\setminus\{z_1\mapsto\llbracket\hat{C}\rrbracket(z_1)\})(z_2)=$ (B1 ⇒ Lem. VII.3.7:3)
$\max\langle\mathrm{img}\,(\llbracket\hat{C}\rrbracket\setminus\{z_1\mapsto\llbracket\hat{C}\rrbracket(z_1)\}),<\rangle$

impl. $\llbracket\hat{C}\rrbracket(z_2)=\max\langle\mathrm{img}\,(\llbracket\hat{C}\rrbracket\setminus\{z_1\mapsto\llbracket\hat{C}\rrbracket(z_1)\}),<\rangle$ (–)

- **E30.** Conclude:

$a\notin\bigcup\mathrm{img}\,(\mathsf{tail}\,((\llbracket\hat{C}\rrbracket\cup\llbracket\hat{C}_{\mathsf{gr}}\rrbracket\cup\llbracket\hat{C}_{\mathsf{co}}\rrbracket)\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a]))$
(E23, E8, E29, A8, A4 ⇒ Thm. VII.2.9:3)

impl. $a\notin\bigcup\mathrm{img}\,(\mathsf{tail}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a]))$ (C5 ⇒ Lem. VII.3.7:4)

- **E31.** Conclude:

$\mathsf{len}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])=\mathsf{0}$

impl. $|(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])(\tilde{z})|=\mathsf{0}$ (Fig. VII.2.5)
for-all $\tilde{z}\in\mathrm{dom}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])$

impl. $(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])(\tilde{z})=\emptyset$ (Fig. VII.2.5)
for-all $\tilde{z}\in\mathrm{dom}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])$

impl. **false** (E26)

- **E32.** Conclude:

$\langle\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a],z_2[a]\rangle\in\mathrm{dom}\,\mathsf{to}$ (E30)

impl. $\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a]\in\mathrm{dom}\,\mathsf{len}$ (Thm. VII.2.6:3)

impl. $\mathsf{len}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])=\mathsf{0}$ **or** (Lem. VII.2.9:1)
$\mathsf{len}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])>\mathsf{0}$

impl. $\mathsf{len}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])>\mathsf{0}$ (E31)

- **E33.** Conclude:

$\mathsf{len}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])>\mathsf{0}$ (E32)

impl. $\mathsf{len}\,(\mathsf{tail}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a]))<$ (Thm. VII.2.5)
$\mathsf{len}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket\;\mathsf{from}\;z_1[a]\;\mathsf{to}\;z_2[a])$

- **E34.** Conclude:

$$\begin{aligned}
&\llbracket(\hat{G} \upharpoonright_{R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]} r[z])\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket && (\langle\hat{G}, R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}], r[z]\rangle \in \upharpoonright)\\
=\ &\llbracket(\hat{G} \upharpoonright_{R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]} r[z_1])\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket && (\text{E6})\\
=\ &\llbracket\hat{G}\rrbracket\ (\!(R[\mathsf{head}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a])])\!) \upharpoonright r[a] && (\text{C10})\\
=\ &\llbracket\hat{G}\rrbracket\ (\!(R[\mathsf{head}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])])\!) \upharpoonright r[a]\\
& && (\text{E15, E20, E22} \Rightarrow \text{Thm. VII.2.6:1})\\
=\ &(\llbracket\hat{G}\rrbracket\ (\!(R[\mathsf{head}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])])\!) \upharpoonright r[a])\ \{\mathbf{cont}/\mathbf{cont}\}\\
& && (\text{Lem. VII.4.2:2})\\
=\ &(\llbracket\hat{G}\rrbracket\ (\!(R[\mathsf{head}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])])\!) \upharpoonright r[a])\\
&\quad\{\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \mathsf{tail}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])) \upharpoonright r[a]/\mathbf{cont}\}\\
& && (\text{E33, E28, C11, A5, E30} \Rightarrow \text{Thm. VII.6.13})\\
=\ &\llbracket\hat{G}\rrbracket\ (\!(R[\mathsf{head}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a])])\!) && (\text{Thm. VII.5.2})\\
&\quad\{\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \mathsf{tail}\,(\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]))/\mathbf{cont}\} \upharpoonright r[a]\\
=\ &\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]) \upharpoonright r[a] && (\text{E32} \Rightarrow \text{Fig. VII.6.2})
\end{aligned}$$

Conclude:

$$\begin{aligned}
&\llbracket(\mathtt{\mathbf{foreach}}\ R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;\ cont} \upharpoonright r[\hat{C}])\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket\\
=\ &\llbracket(\hat{G} \upharpoonright_{R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]} r[z]) && (\text{Step})\\
&\quad\{\mathtt{\mathbf{foreach}}\ R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;\ cont} \upharpoonright r[\hat{C}\setminus\{z\!:\!\hat{D}\}]/\mathbf{cont}\}\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket\\
=\ &\llbracket(\hat{G} \upharpoonright_{R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]} r[z])\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle && (\text{Thm. VII.7.1})\\
&\quad\{(\mathtt{\mathbf{foreach}}\ R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;\ cont} \upharpoonright r[\hat{C}\setminus\{z\!:\!\hat{D}\}])\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle/\mathbf{cont}\}\rrbracket\\
=\ &\llbracket(\hat{G} \upharpoonright_{R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]} r[z])\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket && (\text{E3} \Rightarrow \text{Thm. VII.7.4})\\
&\quad\{\llbracket(\mathtt{\mathbf{foreach}}\ R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;\ cont} \upharpoonright r[\hat{C}\setminus\{z\!:\!\hat{D}\}])\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket/\mathbf{cont}\}\\
=\ &\llbracket(\hat{G} \upharpoonright_{R[\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}]} r[z])\ \langle\!\langle\{\mathtt{\mathbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket && (\text{E5, A5, E7, E13, E14, A4} \Rightarrow \text{Induction+E4})\\
&\quad\{\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_2[a]) \upharpoonright r[a]/\mathbf{cont}\}\\
=\ &\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]) \upharpoonright r[a] && (\text{E34})\\
&\quad\{\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_2[a]) \upharpoonright r[a]/\mathbf{cont}\}\\
=\ &\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]) && (\text{Thm. VII.5.2})\\
&\quad\{\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_2[a])/\mathbf{cont}\} \upharpoonright r[a]\\
=\ &\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]\ \mathsf{to}\ z_2[a]) && (\text{C7, E21} \Rightarrow \text{Thm. VII.2.7:6})\\
&\quad\{\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, (\llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a])\ \mathsf{from}\ z_2[a])/\mathbf{cont}\} \upharpoonright r[a]\\
=\ &\mathsf{iter}(\llbracket\hat{G}\rrbracket, \mathbf{cont}, R, \llbracket\hat{C}\cup\hat{C}_{\mathsf{gr}}\cup\hat{C}_{\mathsf{co}}\rrbracket \ \mathsf{from}\ z_1[a]) \upharpoonright r[a] && (\text{Thm. VII.6.7})
\end{aligned}$$

QED.

Proof of (2)

- **A1.** $\langle\mathtt{\mathbf{foreach}}\ R[\hat{C}\cup\hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;\ cont}, r[\hat{C}]\rangle \in \operatorname{dom} \upharpoonright$
- **A2.** $\mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\mathbf{foreach}}\ R[\hat{C}\cup\hat{C}_{\mathsf{co}}]\ \mathbf{do}\ \hat{G}\ \mathbf{;\ cont})$
- **A3.** $a \in \llbracket\hat{C}\rrbracket(\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom}\llbracket\hat{C}\rrbracket$

- **A4.** $a \notin \llbracket \hat{C}_{\mathsf{co}} \rrbracket(\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{co}} \rrbracket$
- **A5.** $r \in R$
- **B1.** Conclude:

  $\mathsf{Wf}_{f,\mathcal{X}}(\mathtt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \mathtt{\textbf{do}}\ \hat{G}\ \mathtt{\textbf{;}}\ \mathtt{\textbf{cont}})$ (A2)
  impl. $f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{co}}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}}$ **and** (Fig. VII.7.4)
  $\hat{C} \cup \hat{C}_{\mathsf{co}} \in \checkmark$ **and** $\operatorname{expr} \hat{G} \cap \mathbb{G}_{\mathtt{\textbf{rec}}} = \emptyset$ **and** $\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{co}}) \mid \tilde{r} \in R\}, \{\mathtt{\textbf{cont}}\}}(\hat{G})$

- **B2.** Conclude:

  $\mathsf{len}\, \llbracket \hat{C} \cup \hat{C}_{\mathsf{co}} \rrbracket > 0$ (B1 ⇒ Thm. VII.3.6)

- **B3.** Conclude:

  $\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C} \cup \hat{C}_{\mathsf{co}}) \mid \tilde{r} \in R\}, \{\mathtt{\textbf{cont}}\}}(\llbracket \hat{G} \rrbracket)$ (B1 ⇒ Thm. VII.7.3)
  impl. $\mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \operatorname{dom} \llbracket \hat{C} \cup \hat{C}_{\mathsf{co}} \rrbracket \mid \tilde{r} \in R\}, \{\mathtt{\textbf{cont}}\}}(\llbracket \hat{G} \rrbracket)$ (Thm. VII.3.1)

By case distinction on A1 (Fig. VII.8.2b)

- **Case.** $\mathtt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \mathtt{\textbf{do}}\ \hat{G}\ \mathtt{\textbf{;}}\ \mathtt{\textbf{cont}} \restriction r[\hat{C}] = \mathtt{\textbf{cont}}$ **and** $\hat{C} = \emptyset$

  - **C1.** Conclude:

    $a \notin \llbracket \hat{C}_{\mathsf{co}} \rrbracket(\tilde{z})$ **for-all** $\tilde{z} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{co}} \rrbracket$ (A4)
    impl. $a \notin \bigcup \{\llbracket \hat{C}_{\mathsf{co}} \rrbracket(\tilde{z}) \mid \tilde{z} \in \operatorname{dom} \llbracket \hat{C}_{\mathsf{co}} \rrbracket\}$ (–)
    impl. $a \notin \bigcup \operatorname{img} \llbracket \hat{C}_{\mathsf{co}} \rrbracket$ (–)
    impl. $a \notin \bigcup \operatorname{img} \llbracket \emptyset \cup \hat{C}_{\mathsf{co}} \rrbracket$ (–)
    impl. $a \notin \bigcup \operatorname{img} \llbracket \hat{C} \cup \hat{C}_{\mathsf{co}} \rrbracket$ (Case)

  Conclude:

  $\llbracket (\mathtt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{gr}} \cup \hat{C}_{\mathsf{co}}]\ \mathtt{\textbf{do}}\ \hat{G}\ \mathtt{\textbf{;}}\ \mathtt{\textbf{cont}} \restriction r[\hat{C}])\ \langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket$
  $= \llbracket \mathtt{\textbf{cont}}\ \langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle \rrbracket$ (Case)
  $= \llbracket \mathtt{\textbf{cont}} \rrbracket$ (Fig. VII.7.3)
  $= \mathsf{\textbf{cont}}$ (Fig. VII.7.6)
  $= \mathsf{iter}(\llbracket G \rrbracket, \mathsf{\textbf{cont}}, R, \llbracket \hat{C} \cup \hat{C}_{\mathsf{co}} \rrbracket) \restriction r[a]$ (B2, B3, B1, A5, C1 ⇒ Thm. VII.6.13)
  $= \mathsf{iter}(\llbracket G \rrbracket, \llbracket \mathtt{\textbf{cont}} \rrbracket, R, \llbracket \hat{C} \cup \hat{C}_{\mathsf{co}} \rrbracket) \restriction r[a]$ (Fig. VII.7.6)
  $= \llbracket \mathtt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \mathtt{\textbf{do}}\ G\ \mathtt{\textbf{;}}\ \mathtt{\textbf{cont}} \rrbracket \restriction r[a]$ (Fig. VII.7.6)

- **Case.** $\mathtt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \mathtt{\textbf{do}}\ \hat{G}\ \mathtt{\textbf{;}}\ \mathtt{\textbf{cont}} \restriction r[\hat{C}] =$
  $(\hat{G} \restriction_{R[\hat{C} \cup \hat{C}_{\mathsf{co}}]} r[z])\ \{\mathtt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \mathtt{\textbf{do}}\ \hat{G}\ \mathtt{\textbf{;}}\ \mathtt{\textbf{cont}} \restriction r[\hat{C} \setminus \{z\!:\!\hat{D}\}]/\mathtt{\textbf{cont}}\}$ **and**
  $\hat{C} \neq \emptyset$ **and** $z\!:\!\hat{D} = \max \langle \hat{C}, \ll \rangle$

  - **D1.** Conclude:

    $\hat{C} \cup \hat{C}_{\mathsf{co}} \in \checkmark$ (B1)
    impl. $\hat{C} \in \checkmark$ (Lem. VII.3.10:4)

- **D2.** Conclude:

$\hat{C} \in \checkmark$ (D1)

impl. $\hat{C} \setminus \{z\,{:}\,\hat{D}\} \in \checkmark$ (Lem. VII.3.10:5)

impl. $\langle \hat{C} \setminus \{z\,{:}\,\hat{D}\}, \ll \rangle$ is a strictly totally ordered set (Fig. VII.3.9)

- **D3.** Conclude:

$|\hat{C}| > 1$

impl. $|\hat{C} \setminus \{z\,{:}\,\hat{D}\}| \geq 1$ (–)

impl. $\hat{C} \setminus \{z\,{:}\,\hat{D}\} \neq \emptyset$ (–)

impl. $\langle \hat{C} \setminus \{z\,{:}\,\hat{D}\}, \ll \rangle \in \mathrm{dom}\,\max$ (D2)

impl. $z'\,{:}\,D' = \max \langle \hat{C} \setminus \{z\,{:}\,\hat{D}\}, \ll \rangle$ ($\exists z'$, $\exists D'$)

- **D4.** Conclude:

$z' \in \mathrm{dom}\,[\![\hat{C}]\!]$ **and** $z'_{\mathsf{gr}} \in \mathrm{dom}\,\emptyset$ ($\exists z'$, $\exists z'_{\mathsf{gr}}$)

impl. **false** (–)

impl. $[\![\hat{C}]\!](z') < [\![\emptyset]\!](z'_{\mathsf{gr}})$ (–)

- **D5.** Conclude:

$\mathsf{len}\,[\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!] > 0$ (B1 $\Rightarrow$ Thm. VII.3.6)

impl. $\mathsf{len}\,([\![\hat{C}]\!] \cup [\![\hat{C}_{\mathsf{co}}]\!]) > 0$ (Lem. VII.3.7:4)

- **D6.** Conclude:

$\langle \texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{; cont}, r[\hat{C}] \rangle \in \mathrm{dom} \upharpoonright$ (A1)

impl. $\texttt{foreach}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \texttt{do}\ \hat{G}\ \texttt{; cont} \in \hat{\mathbb{G}}$ (Lem. VII.8.2)

impl. $\hat{C} \cup \hat{C}_{\mathsf{co}} \in \hat{\mathbb{C}}$ (–)

impl. $\hat{C} \cup \hat{C}_{\mathsf{co}} \in \mathrm{dom}\,[\![\cdot]\!]$ (Lem. VII.3.7:1)

- **D7.** Conclude:

$z\,{:}\,\hat{D} = \max \langle \hat{C}, \ll \rangle$ (Case)

impl. $z\,{:}\,\hat{D} \in \hat{C}$ (–)

impl. $z \in \mathsf{vars}(\hat{C})$ (Lem. VII.3.4:2)

impl. $z \in \mathrm{dom}\,[\![\hat{C}]\!]$ (Thm. VII.3.1)

impl. $a \in [\![\hat{C}]\!](z)$ (A3)

impl. $a \in [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!](z)$ (D6 $\Rightarrow$ Lem. VII.3.7:5)

impl. $a \in ([\![\hat{C}]\!] \cup [\![\hat{C}_{\mathsf{co}}]\!])(z)$ (Lem. VII.3.7:4)

- **D8.** Conclude:

$\langle [\![\hat{C}]\!] \cup [\![\hat{C}_{\mathsf{co}}]\!], z[a] \rangle \in \mathrm{dom}\,\mathsf{to}$ (D5, D7 $\Rightarrow$ Fig. VII.2.6)

- **D9.** Conclude:

$$[\![\hat{C}]\!](z) = \max \langle \operatorname{img} [\![\hat{C}]\!], < \rangle \qquad \text{(D1, Case} \Rightarrow \text{Thm. VII.3.8:3)}$$

- **D10.** Conclude:

$$\begin{aligned} & a \notin \textstyle\bigcup \operatorname{img}\,(([\![\hat{C}]\!] \cup [\![\hat{C}_{\mathsf{co}}]\!])\;\mathsf{to}\;z[a]) && \text{(D8, D9, A4} \Rightarrow \text{Thm. VII.2.9:1)} \\ \textbf{impl.}\ & a \notin \textstyle\bigcup \operatorname{img}\,(([\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!])\;\mathsf{to}\;z[a]) && \text{(D6} \Rightarrow \text{Lem. VII.3.7:4)} \end{aligned}$$

Conclude:

$$\begin{aligned} & [\![(\mathtt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \mathtt{\textbf{do}}\ \hat{G}\ \mathtt{\textbf{;}}\ \mathtt{\textbf{cont}} \restriction r[\hat{C}])\ \langle\!\langle \{\mathtt{\textbf{self}} \mapsto a\} \rangle\!\rangle]\!] \\ = {} & \mathsf{iter}([\![\hat{\hat{G}}]\!], \mathtt{\textbf{cont}}, R, [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!]\ \mathsf{from}\ z[a]) \restriction r[a] \\ & \qquad \text{(A1, A2, A3, A4, A5, Case, D3, D4} \Rightarrow \text{Thm. VII.8.9:1)} \\ = {} & \mathtt{\textbf{cont}}\ \{\mathsf{iter}([\![\hat{\hat{G}}]\!], \mathtt{\textbf{cont}}, R, [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!]\ \mathsf{from}\ z[a]) \restriction r[a] / \mathtt{\textbf{cont}}\} && \text{(Fig. VII.4.3)} \\ = {} & (\mathsf{iter}([\![\hat{\hat{G}}]\!], \mathtt{\textbf{cont}}, R, [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!]\ \mathsf{to}\ z[a]) \restriction r[a]) && \text{(B2, B3, B1, A5, D10} \Rightarrow \text{Thm. VII.6.13)} \\ & \quad \{\mathsf{iter}([\![\hat{\hat{G}}]\!], \mathtt{\textbf{cont}}, R, [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!]\ \mathsf{from}\ z[a]) \restriction r[a] / \mathtt{\textbf{cont}}\} \\ = {} & \mathsf{iter}([\![\hat{\hat{G}}]\!], \mathtt{\textbf{cont}}, R, [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!]\ \mathsf{to}\ z[a]) && \text{(Thm. VII.5.2)} \\ & \quad \{\mathsf{iter}([\![\hat{\hat{G}}]\!], \mathtt{\textbf{cont}}, R, [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!]\ \mathsf{from}\ z[a]) / \mathtt{\textbf{cont}}\} \restriction r[a] \\ = {} & \mathsf{iter}([\![\hat{\hat{G}}]\!], \mathtt{\textbf{cont}}, R, [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!]) \restriction r[a] && \text{(Thm. VII.6.7)} \\ = {} & \mathsf{iter}([\![G]\!], [\![\mathtt{\textbf{cont}}]\!], R, [\![\hat{C} \cup \hat{C}_{\mathsf{co}}]\!]) \restriction r[a] && \text{(Fig. VII.7.6)} \\ = {} & [\![\mathtt{\textbf{foreach}}\ R[\hat{C} \cup \hat{C}_{\mathsf{co}}]\ \mathtt{\textbf{do}}\ G\ \mathtt{\textbf{;}}\ \mathtt{\textbf{cont}}]\!] \restriction r[a] && \text{(Fig. VII.7.6)} \end{aligned}$$

QED.

VIII.48 Proof of Theorem VII.8.10

Proof of (1)

- **A1.** $\langle \check{G}, r\check{\mathcal{D}} \rangle \in \operatorname{dom} \restriction$
- **A2.** $\mathtt{\textbf{self}} \notin \operatorname{dom} \psi$

By induction on A1 (Fig. VII.8.2a):

- **Base.** $\check{G} = X$ **and** $\check{G} \restriction r\check{\mathcal{D}} = X$

  Conclude:

$$\begin{aligned} & (\check{G} \restriction r\check{\mathcal{D}})\ \langle\!\langle \psi \rangle\!\rangle \\ = {} & X\ \langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\ = {} & X && \text{(Fig. VII.7.3)} \\ = {} & X \restriction r\{\tilde{\check{D}}\ \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.8.2a)} \\ = {} & X\ \langle\!\langle \psi \rangle\!\rangle \restriction r\{\tilde{\check{D}}\ \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.7.3)} \\ = {} & \check{G}\ \langle\!\langle \psi \rangle\!\rangle \restriction r\{\tilde{\check{D}}\ \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step)} \end{aligned}$$

- **Step.** $\check{G} = r_1[x_1] \rightarrowtriangle r_2[x_2]\ \mathbf{:}\ \{\ell_i\ .\ \check{G}_i\}_{i \in I}$ **and**
  $\check{G} \restriction r\check{\mathcal{D}} = r_2[x_2]\ \mathbf{!}\ \{\ell_i\ .\ \check{G}_i \restriction r\check{\mathcal{D}}\}_{i \in I}$ **and** $r_1 = r \neq r_2$ **and** $x_1 .. x_1 \in \check{\mathcal{D}}$

- **B1.** Conclude:

$$\begin{aligned}
& x_1 \mathbin{..} x_1 \in \check{\mathcal{D}} && \text{(Step)}\\
\textbf{impl. } & x_1 \mathbin{..} x_1 \,\langle\!\langle \psi \rangle\!\rangle \in \{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(–)}\\
\textbf{impl. } & (x_1 \,\langle\!\langle \psi \rangle\!\rangle) \mathbin{..} (x_1 \,\langle\!\langle \psi \rangle\!\rangle) \in \{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.3.3)}
\end{aligned}$$

Conclude:

$$\begin{aligned}
& (\check{G} \upharpoonright r\check{\mathcal{D}}) \,\langle\!\langle \psi \rangle\!\rangle \\
= \;& r_2[x_2] \,\mathbf{!}\, \{\ell_i \,.\, \check{G}_i \upharpoonright r\check{\mathcal{D}}\}_{i \in I} \,\langle\!\langle \psi \rangle\!\rangle && \text{(Step)}\\
= \;& r_2[x_2 \,\langle\!\langle \psi \rangle\!\rangle] \,\mathbf{!}\, \{\ell_i \,.\, (\check{G}_i \upharpoonright r\check{\mathcal{D}}) \,\langle\!\langle \psi \rangle\!\rangle\}_{i \in I} && \text{(Fig. VII.7.3)}\\
= \;& r_2[x_2 \,\langle\!\langle \psi \rangle\!\rangle] \,\mathbf{!}\, \{\ell_i \,.\, \check{G}_i \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}\}_{i \in I} && \text{(A2} \Rightarrow \text{Induction)}\\
= \;& r_1[x_1 \,\langle\!\langle \psi \rangle\!\rangle] \twoheadrightarrow r_2[x_2 \,\langle\!\langle \psi \rangle\!\rangle] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \,\langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} \\
& && \text{(Step, B1} \Rightarrow \text{Fig. VII.8.2a)}\\
= \;& r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I} \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.7.3)}\\
= \;& \check{G} \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{G} = r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I}$ **and** $\check{G} \upharpoonright r\check{\mathcal{D}} = r_1[x_1] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \upharpoonright r\check{\mathcal{D}}\}_{i \in I}$ **and** $r_1 \neq r = r_2$ **and** $x_2 \mathbin{..} x_2 \in \check{\mathcal{D}}$

- **C1.** Conclude:

$$\begin{aligned}
& x_2 \mathbin{..} x_2 \in \check{\mathcal{D}} && \text{(Step)}\\
\textbf{impl. } & x_2 \mathbin{..} x_2 \,\langle\!\langle \psi \rangle\!\rangle \in \{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(–)}\\
\textbf{impl. } & (x_2 \,\langle\!\langle \psi \rangle\!\rangle) \mathbin{..} (x_2 \,\langle\!\langle \psi \rangle\!\rangle) \in \{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.3.3)}
\end{aligned}$$

Conclude:

$$\begin{aligned}
& (\check{G} \upharpoonright r\check{\mathcal{D}}) \,\langle\!\langle \psi \rangle\!\rangle \\
= \;& r_1[x_1] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \upharpoonright r\check{\mathcal{D}}\}_{i \in I} \,\langle\!\langle \psi \rangle\!\rangle && \text{(Step)}\\
= \;& r_1[x_1 \,\langle\!\langle \psi \rangle\!\rangle] \,\mathbf{?}\{\ell_i \,.\, (\check{G}_i \upharpoonright r\check{\mathcal{D}}) \,\langle\!\langle \psi \rangle\!\rangle\}_{i \in I} && \text{(Fig. VII.7.3)}\\
= \;& r_1[x_1 \,\langle\!\langle \psi \rangle\!\rangle] \,\mathbf{?}\{\ell_i \,.\, \check{G}_i \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}\}_{i \in I} && \text{(A2} \Rightarrow \text{Induction)}\\
= \;& r_1[x_1 \,\langle\!\langle \psi \rangle\!\rangle] \twoheadrightarrow r_2[x_2 \,\langle\!\langle \psi \rangle\!\rangle] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \,\langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} \\
& && \text{(Step, C1} \Rightarrow \text{Fig. VII.8.2a)}\\
= \;& r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I} \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.7.3)}\\
= \;& \check{G} \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{G} = r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I}$ **and** $\check{G} \upharpoonright r\check{\mathcal{D}} = \bigsqcap\{\check{G}_i \upharpoonright r\check{\mathcal{D}}\}_{i \in I}$ **and** $r_1 \neq r \neq r_2$

Conclude:

$$\begin{aligned}
& (\check{G} \upharpoonright r\check{\mathcal{D}}) \,\langle\!\langle \psi \rangle\!\rangle \\
= \;& \bigsqcap\{\check{G}_i \upharpoonright r\check{\mathcal{D}}\}_{i \in I} \,\langle\!\langle \psi \rangle\!\rangle && \text{(Step)}\\
= \;& \bigsqcap\{(\check{G}_i \upharpoonright r\check{\mathcal{D}}) \,\langle\!\langle \psi \rangle\!\rangle\}_{i \in I} && \text{(Thm. VII.8.1)}\\
= \;& \bigsqcap\{\check{G}_i \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}\}_{i \in I} && \text{(A2} \Rightarrow \text{Induction)}\\
= \;& r_1[x_1 \,\langle\!\langle \psi \rangle\!\rangle] \twoheadrightarrow r_2[x_2 \,\langle\!\langle \psi \rangle\!\rangle] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i \,\langle\!\langle \psi \rangle\!\rangle\}_{i \in I} \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step} \Rightarrow \text{Fig. VII.8.2a)}\\
= \;& r_1[x_1] \twoheadrightarrow r_2[x_2] \,\mathbf{:}\, \{\ell_i \,.\, \check{G}_i\}_{i \in I} \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.7.3)}\\
= \;& \check{G} \,\langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}} \,\langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{G} = \textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \check{G}_2$ **and**
  $\check{G} \upharpoonright r\check{\mathcal{D}} = (\textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \textbf{\texttt{cont}} \upharpoonright r[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}])\,\{\check{G}_2 \upharpoonright r\check{\mathcal{D}}/\textbf{\texttt{cont}}\}$ **and**
  $r \in R$

  - **D1.** Conclude:

$$
\begin{aligned}
& \{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} \subseteq \check{C} && (-)\\
\textbf{impl.}\ & \check{C} = \{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} \cup (\check{C} \setminus \{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}) && (-)
\end{aligned}
$$

Conclude:

$$
\begin{aligned}
& (\check{G} \upharpoonright r\check{\mathcal{D}})\,\langle\!\langle\psi\rangle\!\rangle\\
={}& (\textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \textbf{\texttt{cont}} \upharpoonright r[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}])\,\{\check{G}_2 \upharpoonright r\check{\mathcal{D}}/\textbf{\texttt{cont}}\}\,\langle\!\langle\psi\rangle\!\rangle && \text{(Step)}\\
={}& (\textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \textbf{\texttt{cont}} \upharpoonright r[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}])\,\langle\!\langle\psi\rangle\!\rangle && \text{(Thm. VII.7.1)}\\
& \quad \{(\check{G}_2 \upharpoonright r\check{\mathcal{D}})\,\langle\!\langle\psi\rangle\!\rangle/\textbf{\texttt{cont}}\}\\
={}& (\textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \textbf{\texttt{cont}} \upharpoonright r[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}])\,\langle\!\langle\psi\rangle\!\rangle && \text{(A2} \Rightarrow \text{Induction)}\\
& \quad \{\check{G}_2\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}/\textbf{\texttt{cont}}\}\\
={}& (\textbf{\texttt{foreach}}\ R[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} \cup (\check{C} \setminus \{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\})]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \textbf{\texttt{cont}} \upharpoonright && \text{(D1)}\\
& \quad r[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}])\,\langle\!\langle\psi\rangle\!\rangle\,\{\check{G}_2\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}/\textbf{\texttt{cont}}\}\\
={}& \textbf{\texttt{foreach}}\ R[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} \cup (\check{C} \setminus \{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\})]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \textbf{\texttt{cont}}\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright\\
& \quad r[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}\,\langle\!\langle\psi\rangle\!\rangle]\,\{\check{G}_2\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}/\textbf{\texttt{cont}}\} && \text{(A2} \Rightarrow \text{Thm. VII.8.7)}\\
={}& \textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \textbf{\texttt{cont}}\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r[\{\tilde{z}\,{:}\,\tilde{\check{D}} \in \check{C} \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}\,\langle\!\langle\psi\rangle\!\rangle] && \text{(D1)}\\
& \quad \{\check{G}_2\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}/\textbf{\texttt{cont}}\}\\
={}& \textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \textbf{\texttt{cont}}\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r[\{\tilde{z}\,{:}\,\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \in \check{C}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \in \{\tilde{\tilde{\check{D}}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\tilde{\check{D}}} \in \check{\mathcal{D}}\}\}]\\
& \quad \{\check{G}_2\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}/\textbf{\texttt{cont}}\} && \text{(Lem. VII.3.6:10)}\\
={}& \textbf{\texttt{foreach}}\ R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]\ \textbf{\texttt{do}}\ (\check{G}_1\,\langle\!\langle\psi\rangle\!\rangle)\ \textbf{;}\ (\textbf{\texttt{cont}}\,\langle\!\langle\psi\rangle\!\rangle) \upharpoonright && \text{(Fig. VII.7.3)}\\
& \quad r[\{\tilde{z}\,{:}\,\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \in \check{C}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \in \{\tilde{\tilde{\check{D}}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\tilde{\check{D}}} \in \check{\mathcal{D}}\}\}]\,\{\check{G}_2\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}/\textbf{\texttt{cont}}\}\\
={}& \textbf{\texttt{foreach}}\ R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]\ \textbf{\texttt{do}}\ (\check{G}_1\,\langle\!\langle\psi\rangle\!\rangle)\ \textbf{;}\ \textbf{\texttt{cont}} \upharpoonright && \text{(Fig. VII.7.3)}\\
& \quad r[\{\tilde{z}\,{:}\,\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \in \check{C}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \in \{\tilde{\tilde{\check{D}}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\tilde{\check{D}}} \in \check{\mathcal{D}}\}\}]\,\{\check{G}_2\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}/\textbf{\texttt{cont}}\}\\
={}& \textbf{\texttt{foreach}}\ R[\check{C}\,\langle\!\langle\psi\rangle\!\rangle]\ \textbf{\texttt{do}}\ (\check{G}_1\,\langle\!\langle\psi\rangle\!\rangle)\ \textbf{;}\ (\check{G}_2\,\langle\!\langle\psi\rangle\!\rangle) \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step} \Rightarrow \text{Fig. VII.8.2a)}\\
={}& \textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \check{G}_2\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.7.3)}\\
={}& \check{G}\,\langle\!\langle\psi\rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\,\langle\!\langle\psi\rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step)}
\end{aligned}
$$

- **Step.** $\check{G} = \textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{;}\ \check{G}_2$ **and**
  $\check{G} \upharpoonright r\check{\mathcal{D}} = \textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ (\check{G}_1 \upharpoonright r\check{\mathcal{D}})\ \textbf{;}\ (\check{G}_2 \upharpoonright r\check{\mathcal{D}})$ **and** $r \notin R$

Conclude:

$$\begin{aligned}
& (\check{G} \upharpoonright r\check{\mathcal{D}})\, \langle\!\langle \psi \rangle\!\rangle \\
={}& \textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ (\check{G}_1 \upharpoonright r\check{\mathcal{D}})\ \textbf{\texttt{;}}\ (\check{G}_2 \upharpoonright r\check{\mathcal{D}})\, \langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
={}& \textbf{\texttt{foreach}}\ R[\check{C}\, \langle\!\langle \psi \rangle\!\rangle]\ \textbf{\texttt{do}}\ ((\check{G}_1 \upharpoonright r\check{\mathcal{D}})\, \langle\!\langle \psi \rangle\!\rangle)\ \textbf{\texttt{;}}\ ((\check{G}_2 \upharpoonright r\check{\mathcal{D}})\, \langle\!\langle \psi \rangle\!\rangle) && \text{(Fig. VII.7.3)} \\
={}& \textbf{\texttt{foreach}}\ R[\check{C}\, \langle\!\langle \psi \rangle\!\rangle]\ \textbf{\texttt{do}} && \text{(A2} \Rightarrow \text{Induction)} \\
& \quad (\check{G}_1\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\})\ \textbf{\texttt{;}}\ (\check{G}_2\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}) \\
={}& \textbf{\texttt{foreach}}\ R[\check{C}\, \langle\!\langle \psi \rangle\!\rangle]\ \textbf{\texttt{do}}\ (\check{G}_1\, \langle\!\langle \psi \rangle\!\rangle)\ \textbf{\texttt{;}}\ (\check{G}_2\, \langle\!\langle \psi \rangle\!\rangle) \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step} \Rightarrow \text{Fig. VII.8.2a)} \\
={}& \textbf{\texttt{foreach}}\ R[\check{C}]\ \textbf{\texttt{do}}\ \check{G}_1\ \textbf{\texttt{;}}\ \check{G}_2\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.7.3)} \\
={}& \check{G}\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step)}
\end{aligned}$$

- **Step.** $\check{G} = \textbf{\texttt{rec}}\ X\ \check{G}_X$ **and** $\check{G} \upharpoonright r\check{\mathcal{D}} = \textbf{\texttt{rec}}\ X\ (\check{G}_X \upharpoonright r\check{\mathcal{D}})$

  Conclude:

$$\begin{aligned}
& (\check{G} \upharpoonright r\check{\mathcal{D}})\, \langle\!\langle \psi \rangle\!\rangle \\
={}& \textbf{\texttt{rec}}\ X\ (\check{G}_X \upharpoonright r\check{\mathcal{D}})\, \langle\!\langle \psi \rangle\!\rangle && \text{(Step)} \\
={}& \textbf{\texttt{rec}}\ X\ ((\check{G}_X \upharpoonright r\check{\mathcal{D}})\, \langle\!\langle \psi \rangle\!\rangle) && \text{(Fig. VII.7.3)} \\
={}& \textbf{\texttt{rec}}\ X\ (\check{G}_X\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\}) && \text{(A2} \Rightarrow \text{Induction)} \\
={}& \textbf{\texttt{rec}}\ X\ (\check{G}_X\, \langle\!\langle \psi \rangle\!\rangle) \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.8.2a)} \\
={}& \textbf{\texttt{rec}}\ X\ \check{G}_X\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Fig. VII.7.3)} \\
={}& \check{G}\, \langle\!\langle \psi \rangle\!\rangle \upharpoonright r\{\tilde{\check{D}}\, \langle\!\langle \psi \rangle\!\rangle \mid \tilde{\check{D}} \in \check{\mathcal{D}}\} && \text{(Step)}
\end{aligned}$$

QED.

Proof of (2)

- **A1.** $\langle \hat{G}, r\hat{\mathcal{D}} \rangle \in \operatorname{dom} \upharpoonright$
- **A2.** $\mathsf{Wf}_{f,\mathcal{X}}(\hat{G})$
- **A3.** $a \in \llbracket \hat{D} \rrbracket$ **for-all** $\hat{D} \in \hat{\mathcal{D}}$
- **A4.** $a \notin \llbracket \hat{D} \rrbracket$ **for-all** $\hat{D} \in \mathsf{ivals}(r, \hat{G}) \setminus \hat{\mathcal{D}}$

By induction on A1 (Fig. VII.8.2a):

- **Base.** $\hat{G} = X$ **and** $\hat{G} \upharpoonright r\hat{\mathcal{D}} = X$

  Conclude:

$$\begin{aligned}
& \llbracket (\hat{G} \upharpoonright r\hat{\mathcal{D}})\, \langle\!\langle \{\textbf{\texttt{self}} \mapsto a\} \rangle\!\rangle \rrbracket \\
={}& \llbracket X\, \langle\!\langle \{\textbf{\texttt{self}} \mapsto a\} \rangle\!\rangle \rrbracket && \text{(Base)} \\
={}& \llbracket X \rrbracket && \text{(Fig. VII.7.3)} \\
={}& X && \text{(Fig. VII.7.6)} \\
={}& X \upharpoonright r[a] && \text{(Fig. VII.5.2)} \\
={}& \llbracket X \rrbracket \upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
={}& \llbracket \hat{G} \rrbracket \upharpoonright r[a] && \text{(Base)}
\end{aligned}$$

- **Step.** $\hat{G} = r_1[x_1] \rightarrow r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i\in I}$ **and**
  $\hat{G} \upharpoonright r\hat{\mathcal{D}} = r_2[x_2]\,!\,\{\ell_i \,.\, \hat{G}_i \upharpoonright r\hat{\mathcal{D}}\}_{i\in I}$ **and** $r_1 = r \neq r_2$ **and** $x_1 \mathinner{..} x_1 \in \hat{\mathcal{D}}$
  - **B1.** Conclude:

$$\begin{array}{lll}
 & \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}) & \text{(A1)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \rightarrow r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i\in I}) & \text{(Step)}\\
\textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i) \ \textbf{for-all}\ i \in I & \text{(Fig. VII.7.4)}
\end{array}$$

  - **B2.** Conclude:

$$\begin{array}{lll}
 & a \notin \llbracket \hat{D} \rrbracket \ \textbf{for-all}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}) \setminus \hat{\mathcal{D}} & \text{(A4)}\\
\textbf{impl.} & a \notin \llbracket \hat{D} \rrbracket \ \textbf{for-all}\ \hat{D} \in \mathsf{ivals}(r_1[x_1] \rightarrow r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i\in I}) \setminus \hat{\mathcal{D}} & \text{(Step)}\\
\textbf{impl.} & a \notin \llbracket \hat{D} \rrbracket & \text{(Fig. VII.7.2)}\\
 & \quad \textbf{for-all}\ \hat{D} \in (\{\check{E} \mathinner{..} \check{E} \mid r[\check{E}] \in \{r_1[x_1], r_2[x_2]\}\} \cup \bigcup \{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}} & \\
\textbf{impl.} & a \notin \llbracket \hat{D} \rrbracket & \text{(–)}\\
 & \quad \textbf{for-all}\ \hat{D} \in (\{\check{E} \mathinner{..} \check{E} \mid r[\check{E}] \in \{r_1[x_1], r_2[x_2]\}\} \setminus \hat{\mathcal{D}}) \cup ((\bigcup \{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}}) & \\
\textbf{impl.} & a \notin \llbracket \hat{D} \rrbracket \ \textbf{for-all}\ \hat{D} \in (\bigcup \{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}} & \text{(–)}\\
\textbf{impl.} & a \notin \llbracket \hat{D} \rrbracket \ \textbf{for-all}\ \hat{D} \in \bigcup (\{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\} \setminus \hat{\mathcal{D}}) & \text{(–)}\\
\textbf{impl.} & a \notin \llbracket \hat{D} \rrbracket \ \textbf{for-all}\ \hat{D} \in \bigcup \{\mathsf{ivals}(r, \hat{G}_i) \setminus \hat{\mathcal{D}} \mid i \in I\} & \text{(–)}\\
\textbf{impl.} & \Big[a \notin \llbracket \hat{D} \rrbracket \ \textbf{for-all}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}_i) \setminus \hat{\mathcal{D}}\Big] \ \textbf{for-all}\ i \in I & \text{(–)}
\end{array}$$

  - **B3.** Conclude:

$$\begin{array}{lll}
 & a \in \llbracket \hat{D} \rrbracket \ \textbf{for-all}\ \hat{D} \in \hat{\mathcal{D}} & \text{(A3)}\\
\textbf{impl.} & a \in \llbracket x_1 \mathinner{..} x_1 \rrbracket & \text{(Step)}\\
\textbf{impl.} & a \in \{\tilde{a} \mid \llbracket x_1 \rrbracket \preceq \tilde{a} \preceq \llbracket x_1 \rrbracket\} & \text{(Fig. VII.3.4)}\\
\textbf{impl.} & a \in \{\llbracket x_1 \rrbracket\} & \text{(Fig. VII.2.1:2)}\\
\textbf{impl.} & a = \llbracket x_1 \rrbracket & \text{(–)}\\
\textbf{impl.} & r[a] = r_1[\llbracket x_1 \rrbracket] & \text{(Step)}
\end{array}$$

  - **B4.** Conclude:

$$\begin{array}{lll}
 & r \neq r_2 & \text{(Step)}\\
\textbf{impl.} & r[a] \neq r_2[\llbracket x_2 \rrbracket] & \text{(–)}
\end{array}$$

  Conclude:

$$\begin{array}{lll}
 & \llbracket (\hat{G} \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket & \\
= & \llbracket r_2[x_2]\,!\,\{\ell_i \,.\, \hat{G}_i \upharpoonright r\hat{\mathcal{D}}\}_{i\in I} \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket & \text{(Step)}\\
= & \llbracket r_2[x_2 \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle]\,!\,\{\ell_i \,.\, (\hat{G}_i \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle\}_{i\in I} \rrbracket & \text{(Fig. VII.7.3)}\\
= & r_2[\llbracket x_2 \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket]\,!\,\{\ell_i \,.\, \llbracket (\hat{G}_i \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket\}_{i\in I} & \text{(Fig. VII.7.6)}\\
= & r_2[\llbracket x_2 \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket]\,!\,\{\ell_i \,.\, \llbracket \hat{G}_i \rrbracket \upharpoonright r[a]\}_{i\in I} & \text{(B1, A3, B2} \Rightarrow \text{Induction)}\\
= & r_2[\llbracket x_2 \rrbracket]\,!\,\{\ell_i \,.\, \llbracket \hat{G}_i \rrbracket \upharpoonright r[a]\}_{i\in I} & \text{(Lem. VII.3.6:11)}\\
= & r_1[\llbracket x_1 \rrbracket] \rightarrow r_2[\llbracket x_2 \rrbracket] : \{\ell_i \,.\, \llbracket \hat{G}_i \rrbracket\}_{i\in I} \upharpoonright r[a] & \text{(B3, B4} \Rightarrow \text{Fig. VII.5.2)}\\
= & \llbracket r_1[x_1] \rightarrow r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i\in I} \rrbracket \upharpoonright r[a] & \text{(Fig. VII.7.6)}\\
= & \llbracket \hat{G} \rrbracket \upharpoonright r[a] & \text{(Step)}
\end{array}$$

- **Step.** $\hat{G} = r_1[x_1] \rightarrowtriangle r_2[x_2] \mathbf{:} \{\ell_i \mathbf{.}\ \hat{G}_i\}_{i \in I}$ **and**
  $\hat{G} \upharpoonright r\hat{\mathcal{D}} = r_1[x_1]\,\mathbf{?}\{\ell_i \mathbf{.}\ \hat{G}_i \upharpoonright r\hat{\mathcal{D}}\}_{i \in I}$ **and** $r_1 \neq r = r_2$ **and** $x_2 \mathinner{..} x_2 \in \hat{\mathcal{D}}$

  - **C1.** Conclude:

    $\mathsf{Wf}_{f,\mathcal{X}}(\hat{G})$ (A1)

    impl. $\mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \rightarrowtriangle r_2[x_2] \mathbf{:} \{\ell_i \mathbf{.}\ \hat{G}_i\}_{i \in I})$ (Step)

    impl. $\mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i)$ **for-all** $i \in I$ (Fig. VII.7.4)

  - **C2.** Conclude:

    $a \notin \llbracket \hat{D} \rrbracket$ **for-all** $\hat{D} \in \mathsf{ivals}(r, \hat{G}) \setminus \hat{\mathcal{D}}$ (A4)

    impl. $a \notin \llbracket \hat{D} \rrbracket$ **for-all** $\hat{D} \in \mathsf{ivals}(r_1[x_1] \rightarrowtriangle r_2[x_2] \mathbf{:} \{\ell_i \mathbf{.}\ \hat{G}_i\}_{i \in I}) \setminus \hat{\mathcal{D}}$ (Step)

    impl. $a \notin \llbracket \hat{D} \rrbracket$ (Fig. VII.7.2)
    for-all $\hat{D} \in (\{\check{E} \mathinner{..} \check{E} \mid r[\check{E}] \in \{r_1[x_1], r_2[x_2]\}\} \cup \bigcup \{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}}$

    impl. $a \notin \llbracket \hat{D} \rrbracket$ (–)
    for-all $\hat{D} \in (\{\check{E} \mathinner{..} \check{E} \mid r[\check{E}] \in \{r_1[x_1], r_2[x_2]\}\} \setminus \hat{\mathcal{D}}) \cup ((\bigcup \{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}})$

    impl. $a \notin \llbracket \hat{D} \rrbracket$ **for-all** $\hat{D} \in (\bigcup \{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}}$ (–)

    impl. $a \notin \llbracket \hat{D} \rrbracket$ **for-all** $\hat{D} \in \bigcup(\{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\} \setminus \hat{\mathcal{D}})$ (–)

    impl. $a \notin \llbracket \hat{D} \rrbracket$ **for-all** $\hat{D} \in \bigcup \{\mathsf{ivals}(r, \hat{G}_i) \setminus \hat{\mathcal{D}} \mid i \in I\}$ (–)

    impl. $\left[a \notin \llbracket \hat{D} \rrbracket \textbf{ for-all } \hat{D} \in \mathsf{ivals}(r, \hat{G}_i) \setminus \hat{\mathcal{D}}\right]$ **for-all** $i \in I$ (–)

  - **C3.** Conclude:

    $a \in \llbracket \hat{D} \rrbracket$ **for-all** $\hat{D} \in \hat{\mathcal{D}}$ (A3)

    impl. $a \in \llbracket x_2 \mathinner{..} x_2 \rrbracket$ (Step)

    impl. $a \in \{\tilde{a} \mid \llbracket x_2 \rrbracket \preceq \tilde{a} \preceq \llbracket x_2 \rrbracket\}$ (Fig. VII.3.4)

    impl. $a \in \{\llbracket x_2 \rrbracket\}$ (Fig. VII.2.1:2)

    impl. $a = \llbracket x_2 \rrbracket$ (–)

    impl. $r[a] = r_2[\llbracket x_2 \rrbracket]$ (Step)

  - **C4.** Conclude:

    $r \neq r_1$ (Step)

    impl. $r[a] \neq r_1[\llbracket x_1 \rrbracket]$ (–)

  Conclude:

  $\llbracket (\hat{G} \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket$

  $= \llbracket r_1[x_1]\,\mathbf{?}\{\ell_i \mathbf{.}\ \hat{G}_i \upharpoonright r\hat{\mathcal{D}}\}_{i \in I} \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket$ (Step)

  $= \llbracket r_1[x_1 \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle]\,\mathbf{?}\{\ell_i \mathbf{.}\ (\hat{G}_i \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle\}_{i \in I} \rrbracket$ (Fig. VII.7.3)

  $= r_1[\llbracket x_1 \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket]\,\mathbf{?}\{\ell_i \mathbf{.}\ \llbracket (\hat{G}_i \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket\}_{i \in I}$ (Fig. VII.7.6)

  $= r_1[\llbracket x_1 \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle \rrbracket]\,\mathbf{?}\{\ell_i \mathbf{.}\ \llbracket \hat{G}_i \rrbracket \upharpoonright r[a]\}_{i \in I}$ (C1, A3, C2 ⇒ Induction)

  $= r_1[\llbracket x_1 \rrbracket]\,\mathbf{?}\{\ell_i \mathbf{.}\ \llbracket \hat{G}_i \rrbracket \upharpoonright r[a]\}_{i \in I}$ (Lem. VII.3.6:11)

  $= r_1[\llbracket x_1 \rrbracket] \rightarrowtriangle r_2[\llbracket x_2 \rrbracket] \mathbf{:} \{\ell_i \mathbf{.}\ \llbracket \hat{G}_i \rrbracket\}_{i \in I} \upharpoonright r[a]$ (C3, C4 ⇒ Fig. VII.5.2)

  $= \llbracket r_1[x_1] \rightarrowtriangle r_2[x_2] \mathbf{:} \{\ell_i \mathbf{.}\ \hat{G}_i\}_{i \in I} \rrbracket \upharpoonright r[a]$ (Fig. VII.7.6)

  $= \llbracket \hat{G} \rrbracket \upharpoonright r[a]$ (Step)

- **Step.** $\hat{G} = r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}$ **and** $\hat{G} \upharpoonright r\hat{\mathcal{D}} = \bigsqcap\{\hat{G}_i \upharpoonright r\hat{\mathcal{D}}\}_{i \in I}$ **and** $r_1 \neq r \neq r_2$

  - **D1.** Conclude:

$$\begin{array}{lll} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}) & \text{(A1)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}) & \text{(Step)} \\ \textbf{impl.} & \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_i) \ \textbf{for-all}\ i \in I & \text{(Fig. VII.7.4)} \end{array}$$

  - **D2.** Conclude:

$$\begin{array}{lll} & a \notin [\![\hat{D}]\!] \ \textbf{for-all}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}) \setminus \hat{\mathcal{D}} & \text{(A4)} \\ \textbf{impl.} & a \notin [\![\hat{D}]\!] \ \textbf{for-all}\ \hat{D} \in \mathsf{ivals}(r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}) \setminus \hat{\mathcal{D}} & \text{(Step)} \\ \textbf{impl.} & a \notin [\![\hat{D}]\!] & \text{(Fig. VII.7.2)} \\ & \quad \textbf{for-all}\ \hat{D} \in (\{\check{E}\,..\,\check{E} \mid r[\check{E}] \in \{r_1[x_1], r_2[x_2]\}\} \cup \bigcup\{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}} & \\ \textbf{impl.} & a \notin [\![\hat{D}]\!] & \text{(–)} \\ & \quad \textbf{for-all}\ \hat{D} \in (\{\check{E}\,..\,\check{E} \mid r[\check{E}] \in \{r_1[x_1], r_2[x_2]\}\} \setminus \hat{\mathcal{D}}) \cup ((\bigcup\{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}}) & \\ \textbf{impl.} & a \notin [\![\hat{D}]\!] \ \textbf{for-all}\ \hat{D} \in (\bigcup\{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\}) \setminus \hat{\mathcal{D}} & \text{(–)} \\ \textbf{impl.} & a \notin [\![\hat{D}]\!] \ \textbf{for-all}\ \hat{D} \in \bigcup(\{\mathsf{ivals}(r, \hat{G}_i) \mid i \in I\} \setminus \hat{\mathcal{D}}) & \text{(–)} \\ \textbf{impl.} & a \notin [\![\hat{D}]\!] \ \textbf{for-all}\ \hat{D} \in \bigcup\{\mathsf{ivals}(r, \hat{G}_i) \setminus \hat{\mathcal{D}} \mid i \in I\} & \text{(–)} \\ \textbf{impl.} & \Big[a \notin [\![\hat{D}]\!] \ \textbf{for-all}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}_i) \setminus \hat{\mathcal{D}}\Big] \ \textbf{for-all}\ i \in I & \text{(–)} \end{array}$$

  - **D3.** Conclude:

$$\begin{array}{lll} & r_1 \neq r \neq r_2 & \text{(Step)} \\ \textbf{impl.} & r_1[[\![x_1]\!]] \neq r[a] \neq r_2[[\![x_2]\!]] & \text{(–)} \end{array}$$

  Conclude:

$$\begin{array}{lll} & [\![(\hat{G} \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle]\!] & \\ = & [\![(\bigsqcap\{\hat{G}_i \upharpoonright r\hat{\mathcal{D}}\}_{i \in I}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle]\!] & \text{(Step)} \\ = & [\![\bigsqcap\{(\hat{G}_i \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle\}_{i \in I}]\!] & \text{(Thm. VII.8.1)} \\ = & \bigsqcap\{[\![(\hat{G}_i \upharpoonright r\hat{\mathcal{D}}) \langle\!\langle \{\mathtt{self} \mapsto a\} \rangle\!\rangle]\!]\}_{i \in I} & \text{(Thm. VII.8.2)} \\ = & \bigsqcap\{[\![\hat{G}_i]\!] \upharpoonright r[a]\}_{i \in I} & \text{(D1, A3, D2} \Rightarrow \text{Induction)} \\ = & r_1[[\![x_1]\!]] \rightarrowtriangle r_2[[\![x_2]\!]] : \{\ell_i \,.\, [\![\hat{G}_i]\!]\}_{i \in I} \upharpoonright r[a] & \text{(D3} \Rightarrow \text{Fig. VII.5.2)} \\ = & [\![r_1[x_1] \rightarrowtriangle r_2[x_2] : \{\ell_i \,.\, \hat{G}_i\}_{i \in I}]\!] \upharpoonright r[a] & \text{(Fig. VII.7.6)} \\ = & [\![\hat{G}]\!] \upharpoonright r[a] & \text{(Step)} \end{array}$$

- **Step.** $\hat{G} = \mathtt{foreach}\ R[\hat{C}]\ \mathtt{do}\ \hat{G}_1\ ;\ \hat{G}_2$ **and** $\hat{G} \upharpoonright r\hat{\mathcal{D}} = (\mathtt{foreach}\ R[\hat{C}]\ \mathtt{do}\ \hat{G}_1\ ;\ \mathtt{cont} \upharpoonright r[\{\tilde{z} : \tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}])\,\{\hat{G}_2 \upharpoonright r\hat{\mathcal{D}} / \mathtt{cont}\}$ **and** $r \in R$

  - **E1.** Conclude:

$$\begin{array}{lll} & \{\tilde{z} : \tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} \subseteq \hat{C} & \text{(–)} \\ \textbf{impl.} & \hat{C} = \{\tilde{z} : \tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} \cup (\hat{C} \setminus \{\tilde{z} : \tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}) & \text{(–)} \end{array}$$

- **E2.** Conclude:

$$\begin{aligned}
& \langle \texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}}, r[\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}]\rangle \in \mathrm{dom}\restriction && \text{(Step)}\\
\textsf{\textbf{impl.}}\ & \langle \texttt{\textbf{foreach}}\ R[\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} \cup (\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\})]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}}, && \text{(E1)}\\
& \quad r[\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}]\rangle \in \mathrm{dom}\restriction
\end{aligned}$$

- **E3.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}) && \text{(A1)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \hat{G}_2) && \text{(Step)}\\
\textsf{\textbf{impl.}}\ & f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}}\ \textsf{\textbf{ and }}\ \hat{C} \in \checkmark\ \textsf{\textbf{ and}} && \text{(Fig. VII.7.4)}\\
& \operatorname{expr} \hat{G}_1 \cap \mathbb{G}_{\texttt{\textbf{rec}}} = \emptyset\ \textsf{\textbf{ and }}\ \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \{\texttt{\textbf{cont}}\}}(\hat{G}_1)\ \textsf{\textbf{ and }}\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_2)
\end{aligned}$$

- **E4.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \{\texttt{\textbf{cont}}\}}(\hat{G}) && \text{(E3)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f, \{\texttt{\textbf{cont}}\}}(\hat{G}) && \text{(Lem. VII.7.5:1)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \{\texttt{\textbf{cont}}\}}(\hat{G}) && \text{(Lem. VII.7.5:1)}
\end{aligned}$$

- **E5.** Conclude:

$$\begin{aligned}
& f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} && \text{(E3)}\\
\textsf{\textbf{impl.}}\ & f : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} && \text{(–)}\\
\textsf{\textbf{impl.}}\ & f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\} : \mathbb{R} \rightharpoonup 2^{\mathbb{Z}} && \text{(–)}
\end{aligned}$$

- **E6.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f \setminus \{\tilde{r} \mapsto f(\tilde{r}) \mid \tilde{r} \in R\}, \{\texttt{\textbf{cont}}\}}(&& \text{(E2, E4, E5} \Rightarrow \text{Thm. VII.8.8)}\\
& \quad (\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}} \restriction r[\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}])\,\langle\!\langle \{\texttt{\textbf{self}} \mapsto a\} \rangle\!\rangle)
\end{aligned}$$

- **E7.** Conclude:

$$\begin{aligned}
& a \notin [\![\hat{D}]\!]\ \textsf{\textbf{ for-all }}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}) \setminus \hat{\mathcal{D}} && \text{(A4)}\\
\textsf{\textbf{impl.}}\ & a \notin [\![\hat{D}]\!]\ \textsf{\textbf{ for-all }}\ \hat{D} \in \mathsf{ivals}(r, \texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \hat{G}_2) \setminus \hat{\mathcal{D}} && \text{(Step)}\\
\textsf{\textbf{impl.}}\ & a \notin [\![\hat{D}]\!] && \text{(Step} \Rightarrow \text{Fig. VII.7.2)}\\
& \quad \textsf{\textbf{for-all }}\ \hat{D} \in (\mathsf{ivals}(r, \hat{C}) \cup \mathsf{ivals}(r, \hat{G}_1) \cup \mathsf{ivals}(r, \hat{G}_2)) \setminus \hat{\mathcal{D}}\\
\textsf{\textbf{impl.}}\ & a \notin [\![\hat{D}]\!] && \text{(–)}\\
& \quad \textsf{\textbf{for-all }}\ \hat{D} \in (\mathsf{ivals}(r, \hat{C}) \setminus \hat{\mathcal{D}}) \cup (\mathsf{ivals}(r, \hat{G}_1) \setminus \hat{\mathcal{D}}) \cup (\mathsf{ivals}(r, \hat{G}_2) \setminus \hat{\mathcal{D}})\\
\textsf{\textbf{impl.}}\ & \Big[a \notin [\![\hat{D}]\!]\ \textsf{\textbf{ for-all }}\ \hat{D} \in \mathsf{ivals}(r, \hat{C}) \setminus \hat{\mathcal{D}}\Big]\ \textsf{\textbf{ and}} && \text{(–)}\\
& \Big[a \notin [\![\hat{D}]\!]\ \textsf{\textbf{ for-all }}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}_1) \setminus \hat{\mathcal{D}}\Big]\ \textsf{\textbf{ and }}\ \Big[a \notin [\![\hat{D}]\!]\ \textsf{\textbf{ for-all }}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}_2) \setminus \hat{\mathcal{D}}\Big]
\end{aligned}$$

- **E8.** Conclude:

$$\begin{aligned}
& \texttt{\textbf{cont}} \in \{\texttt{\textbf{cont}}\} && \text{(–)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f, \{\texttt{\textbf{cont}}\}}(\texttt{\textbf{cont}}) && \text{(Fig. VII.7.4)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f, \{\texttt{\textbf{cont}}\}}(\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}}) && \text{(E3} \Rightarrow \text{Fig. VII.7.4)}\\
\textsf{\textbf{impl.}}\ & \mathsf{Wf}_{f, \{\texttt{\textbf{cont}}\}}(&& \text{(E1)}\\
& \quad \texttt{\textbf{foreach}}\ R[\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} \cup (\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\})]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}})
\end{aligned}$$

- **E9.** Conclude:

$$\begin{array}{lll}
 & z \in \mathrm{dom}\,\llbracket\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}\rrbracket & (\exists z) \\
\textbf{impl.} & z\,{:}\,\hat{D} \in \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} & (\text{Lem. VII.3.7:2, } \exists \hat{D}) \\
\textbf{impl.} & z\,{:}\,\hat{D} \in \hat{C} \ \textbf{ and } \ \hat{D} \in \hat{\mathcal{D}} & (-) \\
\textbf{impl.} & z\,{:}\,\hat{D} \in \hat{C} \ \textbf{ and } \ a \in \llbracket\hat{D}\rrbracket & (\text{A3}) \\
\textbf{impl.} & \llbracket\hat{C}\rrbracket(z) = \llbracket\hat{D}\rrbracket \ \textbf{ and } \ a \in \llbracket\hat{D}\rrbracket & (\text{Lem. VII.3.7:3}) \\
\textbf{impl.} & a \in \llbracket\hat{C}\rrbracket(z) & (=) \\
\textbf{impl.} & a \in \llbracket\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} \cup (\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\})\rrbracket(z) & (\text{E1})
\end{array}$$

- **E10.** Conclude:

$$\begin{array}{lll}
 & z \in \mathrm{dom}\,\llbracket\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}\rrbracket & (\exists z) \\
\textbf{impl.} & z \in \mathrm{dom}\,\llbracket\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}\rrbracket \ \textbf{ and } & (\text{E9}) \\
 & a \in \llbracket\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} \cup (\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\})\rrbracket(z) & \\
\textbf{impl.} & a \in \llbracket\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}\rrbracket(z) & (\text{Lem. VII.3.7:5})
\end{array}$$

- **E11.** Conclude:

$$\begin{array}{lll}
 & z\,{:}\,\hat{D} \in \hat{C} \ \textbf{ and } \ z\,{:}\,\hat{D} \notin \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} & (\exists z,\, \exists \hat{D}) \\
\textbf{impl.} & z\,{:}\,\hat{D} \in \hat{C} \ \textbf{ and } \ \Big[z\,{:}\,\hat{D} \notin \hat{C} \ \textbf{ or } \ \hat{D} \notin \hat{\mathcal{D}}\Big] & (-) \\
\textbf{impl.} & z\,{:}\,\hat{D} \in \hat{C} \ \textbf{ and } \ \hat{D} \notin \hat{\mathcal{D}} & (-) \\
\textbf{impl.} & \hat{D} \in \mathsf{ivals}(\hat{C}) \ \textbf{ and } \ \hat{D} \notin \hat{\mathcal{D}} & (\text{Lem. VII.3.5:2}) \\
\textbf{impl.} & \hat{D} \in \mathsf{ivals}(\hat{C}) \setminus \hat{\mathcal{D}} & (-) \\
\textbf{impl.} & \hat{D} \in (\mathsf{ivals}(\hat{C}) \cup \mathsf{ivals}(r, G_1) \cup \mathsf{ivals}(r, G_2) \setminus \hat{\mathcal{D}} & (-) \\
\textbf{impl.} & \hat{D} \in \mathsf{ivals}(r, \texttt{foreach}\ R[\hat{C}]\ \textbf{do}\ \hat{G}_1\ \textbf{;}\ \hat{G}_2) \setminus \hat{\mathcal{D}} & (\text{Step} \Rightarrow \text{Fig. VII.7.2}) \\
\textbf{impl.} & \hat{D} \in \mathsf{ivals}(r, G) \setminus \hat{\mathcal{D}} & (\text{Step}) \\
\textbf{impl.} & a \notin \llbracket\hat{D}\rrbracket & (\text{A4})
\end{array}$$

- **E12.** Conclude:

$$\begin{array}{lll}
 & z \in \mathrm{dom}\,\llbracket\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}\rrbracket & (\exists z) \\
\textbf{impl.} & z\,{:}\,\hat{D} \in \hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} & (\text{Lem. VII.3.7:2, } \exists \hat{D}) \\
\textbf{impl.} & z\,{:}\,\hat{D} \in \hat{C} \ \textbf{ and } \ z\,{:}\,\hat{D} \notin \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} & (-) \\
\textbf{impl.} & z\,{:}\,\hat{D} \in \hat{C} \ \textbf{ and } \ a \notin \llbracket\hat{D}\rrbracket & (\text{E11}) \\
\textbf{impl.} & \llbracket\hat{C}\rrbracket(z) = \llbracket\hat{D}\rrbracket \ \textbf{ and } \ a \notin \llbracket\hat{D}\rrbracket & (\text{Lem. VII.3.7:3}) \\
\textbf{impl.} & a \notin \llbracket\hat{C}\rrbracket(z) & (=) \\
\textbf{impl.} & a \notin \llbracket\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} \cup (\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\})\rrbracket(z) & (\text{E1})
\end{array}$$

- **E13.** Conclude:

$$\begin{array}{lll}
 & z \in \mathrm{dom}\,\llbracket\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}\rrbracket & (\exists z) \\
\textbf{impl.} & z \in \mathrm{dom}\,\llbracket\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}\rrbracket \ \textbf{ and } & (\text{E12}) \\
 & a \notin \llbracket\{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\} \cup (\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\})\rrbracket(z) & \\
\textbf{impl.} & a \notin \llbracket\hat{C} \setminus \{\tilde{z}\,{:}\,\tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}\rrbracket(z) & (\text{Lem. VII.3.7:5})
\end{array}$$

- **E14.** Conclude:

$$\mathsf{len}\,\llbracket\hat{C}\rrbracket > 0 \qquad \text{(E3 $\Rightarrow$ Thm. VII.3.6)}$$

Conclude:

$$\begin{aligned}
& \llbracket(\hat{G} \upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\texttt{\textbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket \\
= {} & \llbracket((\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}} \upharpoonright r[\{\tilde{z} : \tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}])\,\{\hat{G}_2 \upharpoonright r\hat{\mathcal{D}}/\texttt{\textbf{cont}}\}) && \text{(Step)} \\
& \quad \langle\!\langle\{\texttt{\textbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket \\
= {} & \llbracket(\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}} \upharpoonright r[\{\tilde{z} : \tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}])\,\langle\!\langle\{\texttt{\textbf{self}} \mapsto a\}\rangle\!\rangle && \text{(Thm. VII.7.1)} \\
& \quad \{(\hat{G}_2 \upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\texttt{\textbf{self}} \mapsto a\}\rangle\!\rangle/\texttt{\textbf{cont}}\}\rrbracket \\
= {} & \llbracket(\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}} \upharpoonright r[\{\tilde{z} : \tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}])\,\langle\!\langle\{\texttt{\textbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket \\
& && \text{(E6 $\Rightarrow$ Thm. VII.7.4)} \\
& \quad \{\llbracket(\hat{G}_2 \upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\texttt{\textbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket/\texttt{\textbf{cont}}\} \\
= {} & \llbracket(\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}} \upharpoonright r[\{\tilde{z} : \tilde{\hat{D}} \in \hat{C} \mid \tilde{\hat{D}} \in \hat{\mathcal{D}}\}])\,\langle\!\langle\{\texttt{\textbf{self}} \mapsto a\}\rangle\!\rangle\rrbracket \\
& \quad \{\llbracket\hat{G}_2\rrbracket \upharpoonright r[a]/\texttt{\textbf{cont}}\} && \text{(E3, A3, E7 $\Rightarrow$ Induction)} \\
= {} & (\llbracket\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}}\rrbracket \upharpoonright r[a]) && \text{(E2, E8, E10, E13, Step $\Rightarrow$ Thm. VII.8.9:2)} \\
& \quad \{\llbracket\hat{G}_2\rrbracket \upharpoonright r[a]/\texttt{\textbf{cont}}\} \\
= {} & \llbracket\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \texttt{\textbf{cont}}\rrbracket\,\{\llbracket\hat{G}_2\rrbracket/\texttt{\textbf{cont}}\} \upharpoonright r[a] && \text{(Thm. VII.5.2)} \\
= {} & \mathsf{iter}(\llbracket\hat{G}_1\rrbracket, \llbracket\texttt{\textbf{cont}}\rrbracket, R, \llbracket\hat{C}\rrbracket)\,\{\llbracket\hat{G}_2\rrbracket/\texttt{\textbf{cont}}\} \upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
= {} & \mathsf{iter}(\llbracket\hat{G}_1\rrbracket, \texttt{\textbf{cont}}, R, \llbracket\hat{C}\rrbracket)\,\{\llbracket\hat{G}_2\rrbracket/\texttt{\textbf{cont}}\} \upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
= {} & \mathsf{iter}(\llbracket\hat{G}_1\rrbracket, \llbracket\hat{G}_2\rrbracket, R, \llbracket\hat{C}\rrbracket) \upharpoonright r[a] && \text{(E14 $\Rightarrow$ Lem. VII.6.2:2)} \\
= {} & \llbracket\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \hat{G}_2\rrbracket \upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
= {} & \llbracket\hat{G}\rrbracket \upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{G} = \texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \hat{G}_2$ **and**
  $\hat{G} \upharpoonright r\hat{\mathcal{D}} = \texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ (\hat{G}_1 \upharpoonright r\hat{\mathcal{D}})\ \texttt{\textbf{;}}\ (\hat{G}_2 \upharpoonright r\hat{\mathcal{D}})$ **and** $r \notin R$

  - **F1.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}) && \text{(A1)} \\
\textbf{impl. } & \mathsf{Wf}_{f,\mathcal{X}}(\texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \hat{G}_2) && \text{(Step)} \\
\textbf{impl. } & \hat{C} \in \checkmark\ \textbf{ and }\ \mathsf{Wf}_{f \cup \{\tilde{r} \mapsto \mathsf{vars}(\hat{C}) \mid \tilde{r} \in R\}, \{\texttt{\textbf{cont}}\}}(\hat{G}_1)\ \textbf{ and }\ \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}_2) && \text{(Fig. VII.7.4)}
\end{aligned}$$

  - **F2.** Conclude:

$$\begin{aligned}
& a \notin \llbracket\hat{D}\rrbracket\ \textbf{ for-all }\ \hat{D} \in \mathsf{ivals}(r, \hat{G}) \setminus \hat{\mathcal{D}} && \text{(A4)} \\
\textbf{impl. } & a \notin \llbracket\hat{D}\rrbracket\ \textbf{ for-all }\ \hat{D} \in \mathsf{ivals}(r, \texttt{\textbf{foreach}}\ R[\hat{C}]\ \texttt{\textbf{do}}\ \hat{G}_1\ \texttt{\textbf{;}}\ \hat{G}_2) \setminus \hat{\mathcal{D}} && \text{(Step)} \\
\textbf{impl. } & a \notin \llbracket\hat{D}\rrbracket\ \textbf{ for-all }\ \hat{D} \in (\mathsf{ivals}(r, \hat{G}_1) \cup \mathsf{ivals}(r, \hat{G}_2)) \setminus \hat{\mathcal{D}} && \text{(Step $\Rightarrow$ Fig. VII.7.2)} \\
\textbf{impl. } & a \notin \llbracket\hat{D}\rrbracket\ \textbf{ for-all }\ \hat{D} \in (\mathsf{ivals}(r, \hat{G}_1) \setminus \hat{\mathcal{D}}) \cup (\mathsf{ivals}(r, \hat{G}_2) \setminus \hat{\mathcal{D}}) && \text{(–)} \\
\textbf{impl. } & \Big[a \notin \llbracket\hat{D}\rrbracket\ \textbf{ for-all }\ \hat{D} \in \mathsf{ivals}(r, \hat{G}_1) \setminus \hat{\mathcal{D}}\Big]\ \textbf{ and } && \text{(–)} \\
& \Big[a \notin \llbracket\hat{D}\rrbracket\ \textbf{ for-all }\ \hat{D} \in \mathsf{ivals}(r, \hat{G}_2) \setminus \hat{\mathcal{D}}\Big]
\end{aligned}$$

- **F3.** Conclude:

$$\mathsf{len}\,\llbracket\hat{C}\rrbracket > \mathsf{0} \qquad \text{(F1} \Rightarrow \text{Thm. VII.3.6)}$$

Conclude:

$$\begin{aligned}
& \llbracket(\hat{G}\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket \\
={}& \llbracket\mathtt{foreach}\ R[\hat{C}]\ \mathtt{do}\ (\hat{G}_1\upharpoonright r\hat{\mathcal{D}})\ \mathtt{;}\ (\hat{G}_2\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket && \text{(Step)} \\
={}& \llbracket\mathtt{foreach}\ R[\hat{C}\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle]\ \mathtt{do} && \text{(Fig. VII.7.3)} \\
& \quad((\hat{G}_1\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle)\ \mathtt{;}\ ((\hat{G}_2\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle)\rrbracket \\
={}& \mathsf{iter}(&& \text{(Fig. VII.7.6)} \\
& \quad\llbracket(\hat{G}_1\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket, \llbracket(\hat{G}_2\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket, R, \llbracket\hat{C}\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket) \\
={}& \mathsf{iter}(\llbracket\hat{G}_1\rrbracket\upharpoonright r[a], \llbracket\hat{G}_2\rrbracket\upharpoonright r[a], R, \llbracket\hat{C}\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket) && \text{(F1, A3, F2} \Rightarrow \text{Induction)} \\
={}& \mathsf{iter}(\llbracket\hat{G}_1\rrbracket\upharpoonright r[a], \llbracket\hat{G}_2\rrbracket\upharpoonright r[a], R, \llbracket\hat{C}\rrbracket) && \text{(Lem. VII.3.6:4)} \\
={}& \mathsf{iter}(\llbracket\hat{G}_1\rrbracket, \llbracket\hat{G}_2\rrbracket, R, \llbracket\hat{C}\rrbracket)\upharpoonright r[a] && \text{(F3, Step} \Rightarrow \text{Thm. VII.6.11)} \\
={}& \llbracket\mathtt{foreach}\ R[\hat{C}]\ \mathtt{do}\ \hat{G}_1\ \mathtt{;}\ \hat{G}_2\rrbracket\upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
={}& \llbracket\hat{G}\rrbracket\upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

- **Step.** $\hat{G} = \mathtt{rec}\ X\ \hat{G}_X$ **and** $\hat{G}\upharpoonright r\hat{\mathcal{D}} = \mathtt{rec}\ X\ (\hat{G}_X\upharpoonright r\hat{\mathcal{D}})$

  - **G1.** Conclude:

$$\begin{aligned}
& \mathsf{Wf}_{f,\mathcal{X}}(\hat{G}) && \text{(A1)} \\
\textsf{impl.}\ & \mathsf{Wf}_{f,\mathcal{X}}(\mathtt{rec}\ X\ \hat{G}_X) && \text{(Step)} \\
\textsf{impl.}\ & \mathsf{Wf}_{f,\mathcal{X}\cup\{X\}}(\hat{G}_X) && \text{(Fig. VII.7.4)}
\end{aligned}$$

  - **G2.** Conclude:

$$\begin{aligned}
& a \notin \llbracket\hat{D}\rrbracket\ \textsf{for-all}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}) \setminus \hat{\mathcal{D}} && \text{(A4)} \\
\textsf{impl.}\ & a \notin \llbracket\hat{D}\rrbracket\ \textsf{for-all}\ \hat{D} \in \mathsf{ivals}(r, \mathtt{rec}\ X\ \hat{G}_X) \setminus \hat{\mathcal{D}} && \text{(Step)} \\
\textsf{impl.}\ & a \notin \llbracket\hat{D}\rrbracket\ \textsf{for-all}\ \hat{D} \in \mathsf{ivals}(r, \hat{G}_X) \setminus \hat{\mathcal{D}} && \text{(Fig. VII.7.2)}
\end{aligned}$$

Conclude:

$$\begin{aligned}
& \llbracket(\hat{G}\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket \\
={}& \llbracket\mathtt{rec}\ X\ (\hat{G}_X\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket && \text{(Step)} \\
={}& \llbracket\mathtt{rec}\ X\ ((\hat{G}_X\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle)\rrbracket && \text{(Fig. VII.7.3)} \\
={}& \mathtt{rec}\ X\ \llbracket(\hat{G}_X\upharpoonright r\hat{\mathcal{D}})\,\langle\!\langle\{\mathtt{self}\mapsto a\}\rangle\!\rangle\rrbracket && \text{(Fig. VII.7.6)} \\
={}& \mathtt{rec}\ X\ (\llbracket\hat{G}_X\rrbracket\upharpoonright r[a]) && \text{(G1, A3, G2} \Rightarrow \text{Induction)} \\
={}& \mathtt{rec}\ X\ \llbracket\hat{G}_X\rrbracket\upharpoonright r[a] && \text{(Fig. VII.5.2)} \\
={}& \llbracket\mathtt{rec}\ X\ \hat{G}_X\rrbracket\upharpoonright r[a] && \text{(Fig. VII.7.6)} \\
={}& \llbracket\hat{G}\rrbracket\upharpoonright r[a] && \text{(Step)}
\end{aligned}$$

QED.