Exception Handling and Classical Logic

Steffen van Bakel
Department of Computing, Imperial College London, 180 Queen’s Gate, London SW7 2BZ, UK
s.vanbakel@imperial.ac.uk

Abstract

We present \(\lambda^\text{try}\), an extension of the \(\lambda\)-calculus with named exception handling, via \(\text{try}\), \(\text{throw} \, n(N)\) and \(\text{catch} \, n(x) = M\), and present a basic notion of type assignment expressing recoverable exception handling and show that it is sound. We define an interpretation for \(\lambda^\text{try}\) to Parigot’s \(\lambda\mu\)-calculus, and show that reduction (both lazy and call by value) is preserved by the interpretation. We will show that also types assignable in the basic system are preserved by the interpretation.

We will then add a notion of total failure through \(\text{halt}\) that escapes applicative contexts without being caught by a handler, and show that we can interpret this in \(\lambda\mu\) when adding \(\text{top}\) as destination. We will argue that introducing handlers for \(\text{halt}\) will break the relation with \(\lambda\mu\).

We will conclude the paper by showing that it is possible to add handlers for program failure by introducing \(\text{panic}\) and dedicated handlers to \(\lambda^\text{try}\), also via extending the language with a conditional construct that is typed in a non-traditional way, that cannot be expressed in \(\lambda\mu\) or logic. This will allow both recoverable exceptions and total failure, dealt with by handlers; we will show a non-standard soundness result for this system.

keywords: exception handling, abort, classical logic, lambda calculus

Introduction

In this paper we will investigate the relation between exception handling and Classical Logic [9, 21], but will tread a path different to that usually taken over the last 20 years or so. Where the normal approach is to start from Classical Logic and to seek computational content in proofs, here we will do the reverse: we will define a \(\lambda\)-calculus enriched with a primitive form of named (recoverable) exception handling, and investigate if its natural notions of type assignment can be represented in Parigot’s \(\lambda\mu\) [19, 20], a calculus that represents minimal classical logic [1]. We also add non-recoverable exceptions, for which the constant \(\bot\) is added to the type language. Then the corresponding calculus is \(\lambda\mu\text{-top}\) [1], but only if we do not ‘catch’ these exceptions. When trying to add handlers for failing exceptions, the correspondence with \(\lambda\mu\) or \(\lambda\mu\text{-top}\) breaks down, highlighting that type theories based on classical logic do not fully cover exception handling. To stress that point even further, we will enrich \(\lambda^\text{try}\) with a non-conventionally typed conditional structure, and the type constant \(\text{fail}\) that is reserved for failing computations; for this system, we will show that computations either run preserving the type, or run to a term that has type \(\text{fail}\), so fail, as can be expected from the character of exceptions. This thereby is a language for which the standard subject-reduction result does not hold, and which therefore cannot be represented in calculi based on classical logic.\(^1\)

\(^1\) All such calculi are designed to satisfy preservation of provable statements under the operation of cut-elimination, which translates to subject reduction on the level of the calculi.
For a long time it has been thought that only intuitionistic logic had a computational meaning, given its strong relation with types in programming; this is known as the Curry-Howard isomorphism, and is most manifest in the simply typed lambda calculus. However, since it is not possible to comfortably express notions like control or context manipulation in the pure $\lambda$-calculus, it is clear that the $\lambda$-calculus by itself, although Turing complete, is perhaps not expressive enough. Most of these control features, such as direct returns, coroutines, or exception handling, usually exhibit a form of non-local exit, which, albeit specifiable (and therefore realisable) in the pure calculus, are not easily represented, and certainly not using meaningful types. As such, these additions required different formalisms for behaviour specification - e.g. translation to continuation passing style (CPS) or abstract machines.

That situation changed when Griffin [11] observed that the $C$-operator of Felleisen’s $\lambda C$-calculus can be typed with $\neg \neg A \rightarrow A$ (or $((A \rightarrow \bot) \rightarrow \bot) \rightarrow A$), thus highlighting the first link between classical logic and sequential control in computer science. This led to work by Parigot, who introduced a candidate for describing continuations in the form of the $\lambda \mu$-calculus.

The study of the relation between exception handling and classical logic goes back a few decades. Fundamental work has been done by Nakano [16, 17], followed by Crolard [5], in building intuitive systems for analysing throw/catch structures in a functional context. Crolard’s intuition with respect to the representation of throw and catch as certain terms in $\lambda \mu$ is an essential development, and is also used in Bierman’s [3] interpretation into $\lambda \mu$ of de Groote’s [13] calculus $\lambda_{\text{exn}}$, and in a certain sense also by [18], albeit for call-by-value languages. However, in both approaches the argument of the throw-term is the actual exception handler, which is different from the usual perception of what the information encapsulated in a thrown exception should be.

Here we will present the $\lambda \text{try}$-calculus, a $\lambda$-calculus extended with a try/throw/catch syntax which is more similar to the constructions found in common programming languages. In our view, shared by many in the literature, exceptions should exclusively only be thrown when reached during the execution of a program; we therefore accept the (almost) generic approach (an exception is that of [16]) and define reduction strategies that do not permit reduction inside an abstraction; unlike in other papers, here we will we consider both call-by-name (lazy) and call-by-value. Rather than selecting the exception handler through its type, as is the common practice in languages like Java [10], here the handlers are called by name, giving exception handling a more functional ‘feel’. We will show that this calculus can be implemented in $\lambda \mu$ in that we will present an interpretation that preserves both lazy and call-by-value reduction in $\lambda \text{try}$; as was the case in [18, 5, 4], the ‘context erasing’ capability of $\mu$-reduction is used to model the functionality of throw.

To investigate if all natural notions of type assignment for this calculus can correspond to the one for $\lambda \mu$, we will present three variants of $\lambda \text{try}$, with different notions of type assignment. The first comprises a ‘basic’ theory, based on the approach of recoverable exceptions currently used [7] for example in Java; it assumes that all exception handlers return the same type as that of the main term in a try-construct, effectively hiding the occurrence of the exception and allowing for execution to continue normally even after an exception has been thrown. We will show that assignable types are preserved under $\text{cbn}$ and $\text{cbv}$-reduction and under the interpretation into $\lambda \mu$.

The second notion of type assignment we will present represents ‘failure’; we add the construct $\text{halt}$, which cannot be caught so has no possibility of recovery. This induces a notion of type assignment, for which we will show soundness for both $\text{cbn}$ and $\text{cbv}$. We will modify the interpretation into on mapping onto $\lambda \mu$-top, a variant of $\lambda \mu$ that represents full classical logic, and show that assignable types are preserved.

Since both these notions are presented for a small extension of the $\lambda$-calculus, the notions are sound but not really expressive: for example, both throw and halt can have all types.
Although the type ⊥ is used when mapping the calculus into λµ-top, it is not used for the calculus itself, so we cannot tell by the assignable types if a program will fail, an arguably desirable property.

It is fair to state that type assignment for exception handling that marks failing computations is only really relevant in the presence of the conditional construct, where, depending on the evaluation of the boolean expression, the program continues normally or raises an exception. We will therefore extend λµ further, add a conditional construct together with term constants and their types, and add a handling mechanism to deal with occurrences of halt, so achieve a notion of both recoverable and fatal exceptions. Also for this extension we will show a soundness result, which states that a computation either runs preserving the type, or fails. The key difference for this system is that we allow the conditional construct to be typed in a non-conventional way.

These result put into evidence that exception handling can be either recoverable or failing, and that named exception handling is perfectly feasible in the context of functional programming. Moreover, type assignment systems for exception handling need not all be based on classical logic.

**Note:** Because of the restricted length, proofs for the main result appear in the appendix.

1 Related systems

In this section we will revise some formal languages and their type assignment systems that are of interest to this paper. We revisit Curry’s λ-calculus [6, 2], Parigot’s λµ [19], Nakano’s calculus [16] and Crolard’s interpretation into λµ [5], and de Groote’s calculus [13] and Bierman’s interpretation of that [4].

1.1 The λ-calculus

We quickly revise some basic notions for the λ-calculus, to better set the context of this paper.

**Definition 1.1 (Lambda terms, call-by-name and call-by-value reduction [2])**

i) λ-terms are defined by the grammar:

\[ M, N ::= V | MN \]
\[ V ::= x | \lambda x.M \quad \text{(values)} \]

ii) (One-step) β-reduction is defined through the β-rule:

\[ (\beta) : (\lambda x.M) N \rightarrow M\{N/x\} \]

Evaluation contexts are defined as terms with a single hole by:

\[ C ::= [] | CM | MC | \lambda x.C \]

We write \( C[M] \) for the term obtained from the context \( C \) by replacing its hole \( [] \) with \( M \). One-step β reduction is defined as the compatible closure of the β-rule through:

\[ (\beta) : C[(\lambda x.M) N] \rightarrow C[M\{N/x\}] \]

for any evaluation context.

We write \( \rightarrow^* \) for the transitive closure of \( \rightarrow_\beta \), and use that notation for all the notions of reduction we consider in this paper.

iii) Call-by-name evaluation contexts are defined through:
\[(Ax) : \frac{\Gamma,x:A \vdash x:A}{\Gamma} \]
\[(\rightarrow I) : \frac{\Gamma,x:A \vdash M : B}{\Gamma \vdash \lambda x.M : A \rightarrow B} \quad (x \notin \Gamma) \]
\[(\rightarrow E) : \frac{\Gamma \vdash M : A \rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B} \]

Figure 1: Curry type assignment system for the \(\lambda\)-calculus.

\[
C_N ::= \emptyset | C_N M
\]

Call-by-name (cbn) reduction \(\beta^N_{\mu} \) (also known as lazy reduction) is defined through:
\[
(\beta) : C_N[(\lambda x.M)N] \rightarrow C_N[M\{N/x\}]
\]

iv) Call-by-value evaluation contexts are defined through:
\[
(\beta^V) : C_V ::= \emptyset | C_V M | VC_V
\]

Call-by-value (cbv) reduction \(\beta^V_{\mu} \) is defined through:
\[
C_V[(\lambda x.M)V] \rightarrow C_V[M\{V/x\}]
\]

Curry (or simple) type assignment for the \(\lambda\)-calculus is defined as follows:

Definition 1.2 (Curry type assignment for the \(\lambda\)-calculus)

i) Let \(\varphi\) range over a countable (infinite) set of type-variables. The set of Curry types is defined by the grammar:
\[
A, B ::= \varphi | A \rightarrow B
\]

ii) A context of variables \(\Gamma\) is a partial mapping from term variables to types, denoted as a finite set of statements \(x:A\), such that the subjects of the statements \((x)\) are distinct. We write \(\Gamma_1, \Gamma_2\) for the compatible union of \(\Gamma_1\) and \(\Gamma_2\) (if \(x:A_1 \in \Gamma_1\) and \(x:A_2 \in \Gamma_2\), then \(A_1 = A_2\)), and write \(\Gamma,x:A\) for \(\Gamma,\{x:A\}\), and \(x \notin \Gamma\) if there exists no \(A\) such that \(x:A \in \Gamma\).

iii) Curry type assignment is defined by the inference system in Fig. 1.

1.2 On adding exception handling to the \(\lambda\)-calculus

The main topic of this paper is to define an extension of the \(\lambda\)-calculus with exception handling, modelled through try, catch and throw, and investigate notions of type assignment for it and their relation to classical logic. Before coming to that, perhaps we should point out some of the inevitable limitations of extending the \(\lambda\)-calculus with exception handling.

- From the point of view of programming, throwing of exceptions from inside an abstraction, as modelled by the reduction rule
\[
\lambda x.\text{throw } \alpha N \rightarrow \text{throw } \alpha N
\]
should not be allowed.\(^2\) One reason is that subject reduction will then fail (the variable \(x\) might appear in \(N\); see Ex. 4.5), but, perhaps more importantly, it would correspond to letting a program raise an exception just because it occurs in a function definition, regardless of whether or not evaluation of the program has led to the exception.

- In call-by-value or call-by-name functional programming languages, reductions never take place underneath an abstraction, so exceptions defined inside a function are only ever thrown when the function has been called (a redex involving the abstraction has been contracted). This restriction seems to have been applied to almost all proposals for \(\lambda\)-calculi with control in the past (an exception is [16]).

\(^2\) This rule is implied in systems where throw is allowed to escape from any context, as in [16].
A common approach to typeing the `throw` action is to base its rule on the rule for \( \bot \)-elimination from Classical Logic \[9\], which allows any type to be assigned the expression.

\[
\frac{\Gamma \vdash M : A \mid \Delta}{\Gamma \vdash \text{throw } a \ M : B \mid a : A, \Delta}
\]

This, however, is only ever useful in languages that have a conditional construct, when one of the two alternatives throws a recoverable exception whereas the other executes normally (see also Sect. 6). We do not know, a priori, if a boolean will evaluate to `true` or `false`, so if the exception handler is only thrown in the else-part, the type assignment system should be able to express both that the computation will continue normally (in case the boolean evaluates to `true`), or fails (in case the boolean evaluates to `false`).

In order to successfully type this with the normal type assignment rule for the conditional

\[
\frac{\Gamma \vdash M : \text{bool} \mid \Delta \quad \Gamma \vdash P : B \mid \Delta \quad \Gamma \vdash Q : B \mid \Delta}{\Gamma \vdash \text{if } M \text{ then } P \text{ else } Q : B \mid \Delta}
\]

we need to be able to ‘warp’ the type of the `throw` to \( B \), for any \( B \). Type assignment thereby then ‘hides’ the fact that an exception was thrown. This last point will be relevant in Sect. 6 where we present a notion of type assignment that allows for failing exceptions, for which this hiding feature is no longer present, and the type assignment can (in certain cases) predict failure of a program. When adding the conditional construct, as we will do in the final part of the paper, and allowing for both recoverable and failing exceptions, this apparent shortcoming disappears, and part of a program can fail without that affecting the type for the whole.

Normal programming hygiene would demand that exceptions can only be thrown towards an existing and corresponding `catch` (in our case, the one with the right name). Our approach here, where we use a `try`-construct

\[
\text{try } M; \text{catch } n_1(x) = N_1; \ldots; \text{catch } n_n(x) = N_n
\]

that contains a number of `catch` expressions that deal with the exceptions that might be thrown inside \( M \), demands that the result of a normal execution, which would exit from the `try`-construct, cannot contain a `throw` towards one of the exception handlers inside the `try`-construct, but can only refer to exception handlers that are defined outside the `try`-construct. In fact, the names for the exception handlers are bound in the construct, and we do not want reduction ‘to free’ bound names or variables.

If this seems restrictive, dropping this restriction for names is easily dealt with using dynamic scoping, and involves checking if a handler for that name is also defined ‘one level up’, or assuming that all locally defined exception handlers are otherwise redefined on the outermost level where they generate an `undefined` message, with reduction rules like

\[
(\text{try } V; \text{catch } n_i(x) = M_i)P \rightarrow \text{try } VP; \text{catch } m(x) = \text{Error("Message not understood") (} m_i = fn(V))
\]

etc.

Because dynamic scoping cannot be directly represented in \( \lambda \mu \), we choose here to syntactically restrict the terms; this leads to more elegant and tractable solutions to the various theoretical results we achieve, where we can focus on the essential properties without overly complicating the system.

### 1.3 The calculus \( \lambda \mu \)

Parigot’s \( \lambda \mu \)-calculus is a proof-term syntax for classical logic, expressed in Natural Deduction, defined as an extension of the Curry type assignment system for the \( \lambda \)-calculus. With \( \lambda \mu \) Parigot created a multi-conclusion typing system which corresponds to classical logic; the derivable statements have the shape \( \Gamma \vdash_{\lambda \mu} M : A \mid \Delta \), where \( A \) is the main conclusion of the
statement, expressed as the active conclusion, and \( \Delta \) contains the alternative conclusions, consisting of pairs of Greek characters (the names) and types; the left-hand context \( \Gamma \), as usual, contains pairs of Roman characters and types, and represents the types of the free term variables of \( M \). As with Implicative Intuitionistic Logic, the reduction rules for the terms that represent the proofs correspond to proof contractions; the difference is that the reduction rules for the \( \lambda \)-calculus are the logical reductions, i.e. deal with the elimination of a type construct that has been introduced directly above. In addition to these, Parigot expresses also the structural rules that change the focus of a proof, where elimination takes place for a type constructor that appears in one of the alternative conclusions (the Greek variable is the name given to a subterm): he therefore needs to express that the focus of the derivation (proof) changes, and this is achieved by extending the syntax with two new constructs \([x]M\) and \(\mu a.M\) that act as witness to deactivation and activation, which together move the focus of the derivation, and are called a context switch.

We now present the variant of \(\lambda \mu\) we consider in this paper, as defined by Parigot in [20]:

**Definition 1.3 (Syntax of \(\lambda \mu\))** The \(\lambda \mu\)-terms we consider are defined by the grammar:

\[
M, N ::= V \mid MN \mid \mu a. [\beta]M \\
V ::= x \mid \lambda x. M \quad \text{(values)}
\]

Recognising both \(\lambda\) and \(\mu\) as binders, the notion of free and bound names and variables is defined as usual, and we accept Barendregt’s convention to keep free and bound names and variables distinct, using (silent) \(a\)-conversion whenever necessary. We write \(x \in M (a \in M)\) if \(x (a)\) occurs in \(M\), either free of bound. As in Haskell [14], we will use ‘\(\_\)’ as a special name: when we write \(\mu a. [\beta]M\), the name ‘\(\_\)’ does not occur (free) in \([a]M\). We will call the pseudo-terms of the shape \([a]M\) commands, written \(C\), and treat them as terms for reasons of brevity, whenever convenient.

In \(\lambda \mu\), reduction of terms is expressed via implicit substitution; as usual, \(M\{N/x\}\) stands for the substitution of all occurrences of \(x\) in \(M\) by \(N\), \(M\{N\cdot \gamma/a\}\) stands for the term obtained from \(M\) in which every command of the form \([a]P\) is replaced by \([\gamma]PN\) (\(\gamma\) is a fresh name), and \([N\cdot \gamma/a]M\) stands for the term obtained from \(M\) in which every \([a]P\) is replaced by \([\gamma]NP\).

**Definition 1.4 (Structural substitution)**

i) Right-structural substitution, \(M\{N\cdot \gamma/a\}\), is defined inductively over pseudo terms by:

\[
\begin{align*}
N \cdot \gamma/a & \triangleq x \\
(\lambda x. M) \cdot N\cdot \gamma/a & \triangleq \lambda x. (M\{N\cdot \gamma/a\}) \\
(M_1 M_2) \cdot N\cdot \gamma/a & \triangleq M_1 \{N\cdot \gamma/a\} M_2 \{N\cdot \gamma/a\} \\
[a]M \cdot N\cdot \gamma/a & \triangleq [\gamma](M\{N\cdot \gamma/a\}N) \\
[\beta]M \cdot N\cdot \gamma/a & \triangleq [\beta](M\{N\cdot \gamma/a\}) \quad (\beta \neq a) \\
(\mu \delta. C) \cdot N\cdot \gamma/a & \triangleq \mu \delta. (C\{N\cdot \gamma/a\})
\end{align*}
\]

ii) Left-structural substitution, \(\{N\cdot \gamma/a\}M\), is defined inductively over pseudo terms by:

\[
\begin{align*}
{N\cdot \gamma/a} x & \triangleq x \\
{N\cdot \gamma/a} (\lambda x. M) & \triangleq \lambda x. ({N\cdot \gamma/a} M) \\
{N\cdot \gamma/a} (M_1 M_2) & \triangleq {N\cdot \gamma/a} M_1 \{N\cdot \gamma/a\} M_2 \\
{N\cdot \gamma/a} [a]M & \triangleq [\gamma](N\{N\cdot \gamma/a\}M) \\
{N\cdot \gamma/a} [\beta]M & \triangleq [\beta]{N\cdot \gamma/a} M \quad (\beta \neq a) \\
{N\cdot \gamma/a} \mu \delta. C & \triangleq \mu \delta. (N\cdot \gamma/a) C
\end{align*}
\]

[19] only defines the first variant of these notions of structural substitutions (so does not use
the prefix ‘right’); the two notions are defined together, but rather informally, using a notion for contexts in [18].

We have the following notions of reduction on λμ. For the third, call by value, different variants exists in the literature; we adopt the one from [18].

**Definition 1.5 (λμ REDUCTION)** i) The reduction rules of λμ are:

- **logical (β):** \((\lambda x.M)N \rightarrow M\{N/x\}\)
- **structural (μ):** \((\mu a.\cdot)c)N \rightarrow \mu \gamma .\cdot c\{N-\gamma / a\}\) (γ fresh)
- **erasing (E):** \(\mu a.[a]M \rightarrow M\)
- **renaming (R):** \([\beta]\mu \gamma .\cdot c \rightarrow \cdot c[\beta/\gamma]\)

Reduction \(\rightarrow_{\beta\mu}\) on λμ-terms is defined as the compatible closure of these rules.

ii) **Call-by-name evaluation contexts** are defined as:

\[C_N := [] \mid C_N M \mid \mu a.[\beta]C_N\]

Call-by-name reduction \(\rightarrow_{\beta\mu}^n\) is defined through: \(C_N[M] \rightarrow_{\beta\mu}^n C_N[N]\) if \(M \rightarrow N\) using either the β, μ, E, or R-reduction rule.

iii) **Call-by-value evaluation contexts** are defined through:

\[C_V := [] \mid C_V M \mid V C_V \mid \mu a.[\beta]C_V\]

Call-by-value reduction \(\rightarrow_{\beta\mu}^n\) is defined through: \(C_V[M] \rightarrow_{\beta\mu}^n C_V[N]\) if \(M \rightarrow N\) using either μ, E, R, or:

\[(\beta_V): \ (\lambda x.M)V \rightarrow_{\beta\mu}^n M\{V/x\}\]
\[(\mu_V): \ V(\mu a.\cdot)c \rightarrow_{\beta\mu}^n \mu \gamma .\cdot c\{V-\gamma / a\}\) (γ fresh)

iv) Call-by-name **applicative contexts** are defined as:

\[C_N^\wedge := [] \mid C_N^\wedge M\]

whereas call-by-value **applicative contexts** are defined as:

\[C_V^\wedge := [] \mid C_V^\wedge M \mid V C_V^\wedge\]

Remark that, for rule \((\mu_V), \mu a.[\beta]N\) is not a value. Also, unlike for the λ-calculus, call-by-value reduction is not a sub-reduction system of \(\rightarrow_{\beta\mu}\): the rule \((\mu_V)\) (and left-structural substitution) are not part of \(\rightarrow_{\beta\mu}\).

The intuition behind the structural rule is given by de Groote [12]: “in a λμ-term \(\mu a.\cdot M\) of type \(A \rightarrow B\), only the subterms named by \(a\) are really of type \(A \rightarrow B\) (…) hence, when such a \(\mu\)-abstraction is applied to an argument, this argument must be passed over to the sub-terms named by \(a\).” It is possible to define more reduction rules, but Parigot refrained from that since he aimed at defining a confluent reduction system. In this paper, we will only deal with the logical, structural and renaming rule; this is also the restriction made by de Groote in [12].

Type assignment for λμ is defined below; there is a main, or active, conclusion, labelled by a term, and the alternative conclusions are labelled by names α, β, etc.

**Definition 1.6 (Typing rules for λμ)** i) Types and contexts of variables Γ are those of Def. 1.2.

\[
\begin{align*}
(Ax) & : \frac{\Gamma, x:A \vdash x:A}{\Delta} \\
(\rightarrow) & : \frac{\Gamma, x:A \vdash M : B}{\Delta} \\
(\lambda) & : \frac{\Gamma \vdash M : B \mid a:A, \beta:B, \Delta}{\Gamma \vdash \lambda x.M : A \mid a:A, \beta:B, \Delta} \\
(\mu) & : \frac{\Gamma, \mu a.[\beta]:M : A \mid a: A, \beta:B, \Delta}{\Delta} \\
(-E) & : \frac{\Gamma \vdash M : A \mid a:A, \Delta}{\Gamma \vdash \mu a.[a]M : A \mid a: A, \Delta}
\end{align*}
\]

Figure 2: Type assignment rules for λμ
ii) A context of names $\Delta$ is a partial mapping from names to types, denoted as a finite set of statements $\alpha : A$, such that the subjects of the statements ($\alpha$) are distinct. Notions $\Delta_1, \Delta_2$, as well as $\Delta, \alpha : A$ and $\alpha \not\in \Delta$ are defined as for $\Gamma$.

iii) The type assignment rules for $\lambda \mu$ are presented in Fig. 2; we will write $\Gamma \vdash_{\lambda \mu} M : A \mid \Delta$ for statements derivable in this system.

We can think of $[\alpha]M$ as storing the type of $M$ amongst the alternative conclusions by giving it the name $\alpha$.

**Example 1.7** Take the term $\mu \alpha. [\alpha] \mu \beta. [\gamma]M$, such that $M$ does not contain $\alpha$ or $\beta$, and $\alpha \neq \gamma$. Then by renaming,

$$\mu \alpha. [\alpha] \mu \beta. [\gamma]M \to_{\mu \beta} \mu \alpha. [\gamma]M\{\alpha / \beta\} = \mu \alpha. [\gamma]M$$

but also, by erasure, $\mu \alpha. [\alpha] \mu \beta. [\gamma]M \to_{\mu \beta} \mu \beta. [\gamma]M$. Notice that $\mu \alpha. [\gamma]M =_{\alpha} \mu \alpha. [\gamma]M =_{\mu \beta} [\gamma]M$.

We will now show that type assignment is closed under reduction for both call-by-name and call-by-value reduction. This result might itself be as expected, and is presented here mostly for completeness. First we show results for the three notions of substitution.

**Lemma 1.8 (Substitution Lemma)**

i) If $\Gamma, x : B \vdash_{\lambda \mu} M : A \mid \Delta$ and $\Gamma \vdash_{\lambda \mu} L : B \mid \Delta$, then $\Gamma \vdash_{\lambda \mu} M\{L/x\} : A \mid \Delta$.

ii) If $\Gamma \vdash_{\lambda \mu} M : A \mid \Delta$ and $\Gamma \vdash_{\lambda \mu} L : B \mid \Delta$, then $\Gamma \vdash_{\lambda \mu} M\{L \cdot \gamma / \alpha\} : A \mid \gamma : C, \Delta$.

iii) If $\Gamma \vdash_{\lambda \mu} L : B \rightarrow C \mid \Delta$ and $\Gamma \vdash_{\lambda \mu} M : A \mid \alpha : B, \Delta$, then $\Gamma \vdash_{\lambda \mu} \{L \cdot \gamma / \alpha\} M : A \mid \gamma : C, \Delta$.

**Proof:**

i) By induction on the definition of term substitution.

$(x\{L/x\} = L)$: If $\Gamma, x : B \vdash_{\lambda \mu} x : A \mid \Delta$, then $B = A$, so $\Gamma \vdash_{\lambda \mu} L : A \mid \Delta$, so also $\Gamma \vdash_{\lambda \mu} x\{L/x\} : A \mid \Delta$.

$(y\{L/x\} \equiv y (y \neq x))$: Then $y : A \in \Gamma$ and by rule $(Ax)$ we have $\Gamma \vdash_{\lambda \mu} y : A \mid \Delta$.

$(\lambda y. (N\{L/x\}) \equiv (\lambda y. N)\{L/x\})$: Then $\Delta = C \rightarrow D$. If $\Gamma, x : B \vdash_{\lambda \mu} \lambda y. N : C \rightarrow D \mid \Delta$, then by rule $(\rightarrow \ell)$, $\Gamma, x : B, y : C \vdash_{\lambda \mu} N \mid \Delta$. Then by induction, $\Gamma, y : C \vdash_{\lambda \mu} N\{L/x\} : D \mid \Delta$, so by $(\rightarrow II)$, $\Gamma \vdash_{\lambda \mu} \lambda y. N\{L/x\} : C \rightarrow D \mid \Delta$.

$((PQ)\{L/x\} \equiv P\{L/x\} Q\{L/x\})$: If $\Gamma, x : B \vdash_{\lambda \mu} PQ : A \mid \Delta$, then, by rule $(\rightarrow E)$ there exist $C$ such that both $\Gamma, x : B \vdash_{\lambda \mu} P : C \rightarrow A \mid \Delta$ and $\Gamma, x : B' \vdash_{\lambda \mu} Q : C \mid \Delta$. Then, by induction, $\Gamma \vdash_{\lambda \mu} P\{L/x\} : C \rightarrow A \mid \Delta$ and $\Gamma \vdash_{\lambda \mu} Q\{L/x\} : C \mid \Delta$, the result follows by rule $(\rightarrow E)$.

$((\mu \alpha. [\beta] N)\{L/x\} \equiv \mu \alpha. [\beta] N\{L/x\})$: If $\Gamma, x : B \vdash_{\lambda \mu} \mu \alpha. [\beta] N : A \mid \Delta$, then, by rule $(\mu)$ there exist $C$ such that $\Gamma, x : B \vdash_{\lambda \mu} \lambda \alpha. [\beta] N : C \mid \alpha : A, \beta : C', \Delta'$ with $\Delta = \beta : C, \Delta'$. Then, by induction, $\Gamma \vdash_{\lambda \mu} N\{L/x\} : C \mid \alpha : A, \beta : C, \Delta'$, and by rule $(\mu)$ we have $\Gamma \vdash_{\lambda \mu} N\{L/x\} : C \mid \alpha : A, \beta : C, \Delta'$.

ii) By induction on the definition of right-structural substitution.

$(x\{L \cdot \gamma / \alpha\} \triangleq x)$: Then $x : A \in \Gamma$, and by rule $(Ax)$ we have $\Gamma \vdash_{\lambda \mu} x : A \mid \gamma : C, \Delta$.

$((\lambda x. N)\{L \cdot \gamma / \alpha\} \triangleq \lambda x. (N\{L \cdot \gamma / \alpha\}))$: Then $\Delta = D \rightarrow E$ and, by rule $(\rightarrow II)$, $\Gamma, x : D \vdash_{\lambda \mu} \lambda x. N : E \mid \alpha : B, \gamma : C, \Delta$. Thus by induction we have $\Gamma, x : D \vdash_{\lambda \mu} N\{L \cdot \gamma / \alpha\} : E \mid \gamma : C, \Delta$, so by rule $(\rightarrow II)$ we have $\Gamma \vdash_{\lambda \mu} \lambda x. N\{L \cdot \gamma / \alpha\} : D \rightarrow E \mid \gamma : C, \Delta$.

$((PQ)\{L \cdot \gamma / \alpha\} \triangleq P\{L \cdot \gamma / \alpha\} Q\{L \cdot \gamma / \alpha\})$: Then by rule $(\rightarrow E)$ there exists $D$ such that $\Gamma \vdash_{\lambda \mu} P : D \rightarrow A \mid \alpha : B, \gamma : C, \Delta$ and $\Gamma \vdash_{\lambda \mu} Q : D \mid \alpha : B, \gamma : C, \Delta$. Then by induction both $\Gamma \vdash_{\lambda \mu} P\{L \cdot \gamma / \alpha\} : D \rightarrow A \mid \gamma : C, \Delta$ and $\Gamma \vdash_{\lambda \mu} Q\{L \cdot \gamma / \alpha\} : D \mid \gamma : C, \Delta$; the result follows by rule $(\rightarrow E)$.

$(\mu \alpha. [\delta] N\{L \cdot \gamma / \alpha\}) \triangleq \mu \delta. [\gamma] (N\{L \cdot \gamma / \alpha\} L L)$: Then by rule $(\mu)$ $\Gamma \vdash_{\lambda \mu} N : B \rightarrow C \mid \delta : A, \alpha : B, \gamma : C, \Delta$, and by induction $\Gamma \vdash_{\lambda \mu} N\{L \cdot \gamma / \alpha\} : B \rightarrow C \mid \delta : A, \gamma : C, \Delta$. From $\Gamma \vdash_{\lambda \mu} L : B \mid \Delta$, since $\alpha, \delta$ and $\gamma$ all do not occur (free) in $N$, by weakening we also get $\Gamma \vdash_{\lambda \mu} L : B \mid \delta : A, \gamma : C, \Delta$, and we can construct.
Proof: If $M \rightarrow^\beta_{\mu} N$, and $\Gamma \vdash_{\lambda\mu} M : A \mid \Delta$, then $\Gamma \vdash_{\lambda\mu} N : A \mid \Delta$.

**Proof:** By induction on the definition of $\rightarrow^\beta_{\mu}$.

$((\lambda x.M) N \rightarrow^\beta_{\mu} M\{N/x\})$: The derivation for $\Gamma \vdash_{\lambda\mu} (\lambda x.M) N : A \mid \Delta$ is shaped like

$$\Gamma, x : B \vdash_{\lambda\mu} M : A \mid \Delta \quad \Gamma \vdash_{\lambda\mu} \lambda x. M : B \rightarrow A \mid \Delta \quad \Gamma \vdash_{\lambda\mu} N : B \mid \Delta \quad \Gamma \vdash_{\lambda\mu} \mu\delta. [\lambda x. \delta] (L \cdot \gamma/a) : (\Delta)$$

Then, by Lem. 1.8, we have $\Gamma \vdash_{\lambda\mu} M\{N/x\} : A \mid \Delta$.

$((\mu a.[a] M) N \rightarrow^\beta_{\mu} \mu\gamma.[\gamma] M\{N \cdot \gamma/a\} N)$: The derivation for $((\mu a.[a] M) N) \rightarrow^\beta_{\mu} \mu\gamma.[\gamma] M\{N \cdot \gamma/a\} N$ is shaped like

$$\Gamma \vdash_{\lambda\mu} M : B \rightarrow A \mid \Delta \quad \Gamma \vdash_{\lambda\mu} \mu a.[a] M : B \rightarrow A \mid \Delta \quad \Gamma \vdash_{\lambda\mu} N : B \mid \Delta \quad \Gamma \vdash_{\lambda\mu} \mu\delta. [\mu a.[a] \delta] (L \cdot \gamma/a) : L \cdot \gamma/a : : \rightarrow A \mid \Delta$$

Then by Lem. 1.8, we have $\Gamma \vdash_{\lambda\mu} M\{N \cdot \gamma/a\} : B \rightarrow A \mid \gamma : A, \Delta$. Since $\gamma$ is fresh, by weakening also $\Gamma \vdash_{\lambda\mu} N : B \mid \gamma : A, \Delta$, we can construct

We will now show that type assignment respects lazy and call-by-value reduction:

**Theorem 1.9** If $M \rightarrow^\beta_{\mu} N$, and $\Gamma \vdash_{\lambda\mu} M : A \mid \Delta$, then $\Gamma \vdash_{\lambda\mu} N : A \mid \Delta$.
Proof: Theorem 1.10

\((\mu a).[\delta]M N \to_{\rho_\mu}^n \mu \gamma.[\delta]M\{N \cdot \gamma/a\}\) with \(\alpha \neq \delta\): The derivation for \((\mu a).[\delta]M\) \(N\) is shaped like

\[
\frac{\Gamma \vdash_{\lambda_\mu} M\{N \cdot \gamma/a\} : B \rightarrow A | \gamma; A, \Delta}{\Gamma \vdash_{\lambda_\mu} N : \gamma; A, \Delta} \quad (\rightarrow E)
\]

\[
\frac{\Gamma \vdash_{\lambda_\mu} M\{N \cdot \gamma/a\} N : A | \gamma; A, \Delta}{\Gamma \vdash_{\lambda_\mu} \mu \gamma.[\gamma]M\{N \cdot \gamma/a\} N : A | \Delta} \quad (\mu)
\]

with \(\Delta = \delta; C, \Delta'\). Then by Lem. 1.8, we have \(\Gamma \vdash_{\lambda_\mu} M\{N \cdot \gamma/a\} : C | \gamma; A, \delta; C, \Delta',\) and we can construct

\[
\frac{\Gamma \vdash_{\lambda_\mu} M\{N \cdot \gamma/a\} : C | \gamma; A, \delta; C, \Delta'}{\Gamma \vdash_{\lambda_\mu} \mu \gamma.[\delta]M\{N \cdot \gamma/a\} N : A | \delta; C, \Delta'} \quad (\mu)
\]

\((\mu a.[a]M \to_{\rho_\mu}^n M)\): The derivation for \(\mu a.[a]M\) is shaped like

\[
\frac{\Gamma \vdash_{\lambda_\mu} M : A | \alpha; A, \Delta}{\Gamma \vdash_{\lambda_\mu} \mu a.[a]M : A | \Delta} \quad (\mu)
\]

Since \(\alpha\) does not occur in \(M\), we can thin \(\alpha; A, \Delta\) and obtain \(\Gamma \vdash_{\lambda_\mu} M : A | \Delta\).

\((\mu a.[\beta]M \gamma.[\delta]M \to_{\rho_\mu}^n \mu a.[\delta]M\{\beta / \gamma\})\): The derivation for \((\mu a.[\delta]M\) \(N\) is shaped like

\[
\frac{\Gamma \vdash_{\lambda_\mu} M : D | \alpha; A, \beta; B, \gamma; B, \delta; D, \Delta'}{\Gamma \vdash_{\lambda_\mu} \mu \gamma.[\delta]M : B | \alpha; A, \beta; B, \gamma; B, \delta; D, \Delta'} \quad (\mu)
\]

\[
\frac{\Gamma \vdash_{\lambda_\mu} \mu a.[\beta]M \gamma.[\delta]M : A | \beta; B, \delta; D, \Delta'}{\Gamma \vdash_{\lambda_\mu} \mu a.[\beta]M : A | \beta; B, \delta; D, \Delta'} \quad (\mu)
\]

So in particular, replacing all occurrences of \(\gamma\) by \(\beta\), we obtain a derivation for \(\Gamma \vdash_{\lambda_\mu} M\{\beta / \gamma\} : D | \alpha; A, \beta; B, \delta; D, \Delta'.\) Now either:

\((\delta \neq \gamma)\): Then we can construct:

\[
\frac{\Gamma \vdash_{\lambda_\mu} M\{\beta / \gamma\} : D | \alpha; A, \beta; B, \delta; D, \Delta'}{\Gamma \vdash_{\lambda_\mu} \mu a.[\beta]M\{\beta / \gamma\} : A | \beta; B, \delta; D, \Delta'} \quad (\mu)
\]

\((\delta = \gamma)\): Then \(D = B\) as well, and we can construct:

\[
\frac{\Gamma \vdash_{\lambda_\mu} M\{\beta / \gamma\} : B | \alpha; A, \beta; B, \Delta'}{\Gamma \vdash_{\lambda_\mu} \mu a.[\beta]M\{\beta / \gamma\} : A | \beta; B, \Delta'} \quad (\mu)
\]

\((M \to_{\rho_\mu}^n N \Rightarrow MP \to_{\rho_\mu}^n NP, \mu a.[\beta]M \to_{\rho_\mu}^n \mu a.[\beta]N)\): By induction. □

Theorem 1.10 If \(M \to_{\rho_\mu}^n N\), and \(\Gamma \vdash_{\lambda_\mu} M : A | \Delta\), then \(\Gamma \vdash_{\lambda_\mu} N : A | \Delta\).

Proof: By induction on the definition of \(\to_{\rho_\mu}^n\); we only show the cases that deal with left structural substitution; the others are very similar if not identical to the previous theorem.

\((V(\mu a.[a]M) \to_{\rho_\mu}^n \mu \gamma.[\gamma]V\{\gamma \cdot \gamma/a\}M)\): The derivation for \(V(\mu a.[a]M)\) is shaped like
\[ \Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta \]

\[
\Gamma \vdash_{\lambda \mu} M : B \mid a : B, \Delta \\
\Gamma \vdash_{\lambda \mu} \mu a. [a] M : B \mid \Delta \\
\Gamma \vdash_{\lambda \mu} V (\mu a. [a] M) : A \mid \Delta 
\]

\[(\mu) \]

\[
\begin{array}{c}
\Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta \\
\end{array} \quad \frac{\Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta}{\Gamma \vdash_{\lambda \mu} \mu V : \gamma : A, \Delta, \gamma \rightarrow A, \Delta} 
\]

\[(\rightarrow E)\]

Then by Lem. 1.8, we have \(\Gamma \vdash_{\lambda \mu} \{ V \cdot \gamma / a \} M : B \mid \gamma : A, \Delta\), and we can construct

\[
\begin{array}{c}
\Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta \\
\end{array} \quad \frac{\Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta}{\Gamma \vdash_{\lambda \mu} \{ V \cdot \gamma / a \} M : B \mid \gamma : A, \Delta} 
\]

\[(\rightarrow E)\]

\[
\begin{array}{c}
\Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta \\
\end{array} \quad \frac{\Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta}{\Gamma \vdash_{\lambda \mu} \{ V \cdot \gamma / a \} M : B \mid \gamma : A, \Delta} 
\]

\[(\rightarrow E)\]

\[(\mu)\]

\[
\begin{array}{c}
\Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta \\
\end{array} \quad \frac{\Gamma \vdash_{\lambda \mu} V : B \rightarrow A \mid \Delta}{\Gamma \vdash_{\lambda \mu} \{ V \cdot \gamma / a \} M : B \mid \gamma : A, \Delta} 
\]

\[(\rightarrow E)\]

\[(\mu)\]

\[\text{Lemma 1.12 } \]

\[i) \text{ The reduction rule } C^N_\mu \mu a. [\beta] N \rightarrow \mu a. [\beta] N \text{ is admissible in } \rightarrow^\mu.\]

\[ii) \text{ The reduction rule } C^N_\mu \mu a. [\beta] N \rightarrow \mu a. [\beta] N \text{ is admissible in } \rightarrow^\mu.\]

\[\text{Proof: } i) \text{ By induction on the structure of contexts:}\]

\[
\begin{array}{c}
(C^N_\mu = []) : \text{ Immediate.} \\
(C^N_\mu = C^N_\mu M) : \text{ Notice that } \_ \neq \beta \text{ and that there is no sub-term called } \_ \text{ in } N; \text{ then}
\end{array} 
\]

\[\]
\[ C^\nu_N[\mu_-. \beta]N \rightarrow (IH) \ (\mu_.[\beta]N)M \]
\[ \rightarrow_{\beta\mu}^\gamma \mu_\gamma.[\beta]N\{M.\gamma/\_\} \]
\[ = \mu_\gamma.[\beta]N \quad =_a \mu_.[\beta]N \]

Notice that \( \gamma \) is fresh; since there is no sub-term called \( \_ \) in \( M \), the structural substitution \( \{M.\gamma/\_\} \) has no effect, so, in particular, \( \gamma \) does not appear in \( [\beta]M \).

ii) By induction on the structure of contexts. The first two cases are similar to above; the third one is:
\[ (C^\nu = VC^\nu V) : \ V C^\nu V[\mu_-. \beta]M \rightarrow (IH) \ V (\mu_.[\beta]M) \]
\[ \rightarrow_{\beta\mu}^\gamma \mu_\gamma.[\beta]\{V.\gamma/\_\}M \]
\[ = \mu_\gamma.[\beta]M \quad =_a \mu_.[\beta]M \]

Notice that this result also holds for \( \beta = \text{top} \).

1.4 On modelling the catch/throw mechanism in \( \lambda\mu \)

Throwing an exception involves an interruption of normal execution, and a jump out of the current context; those jumps can be modelled by rules that eradicate the context, like for example \( C[A(M)] \rightarrow M \) as used in \( \lambda C \) [8] (using the \textit{abort} constructor \( A \)), or similarly as in [16, 11].

The kind of contexts that can be aborted differ from paper to paper. The most common approach, as used in [8, 4] and here, is to allow aborting applicative contexts only, but, for example, [16] allows aborting executions inside abstractions as well. Allowing the latter kind of comes with obstacles, in that type assignment and in particular soundness (preservation of assignable types under reduction) becomes more difficult to achieve, since in general we cannot preserve types when aborting from an abstraction (see Ex. 4.5 and 6.7), which leaves that (in the context of the \( \lambda \)-calculus with types) we can only safely abort from applicative contexts.

In terms of provable properties it is preferable to model eradication of applicative contexts ‘one syntactic construction at the time’, rather than the \( \lambda C \)-approach, which aborts entire contexts via \( C[A(M)] \rightarrow M \), where the context is assumed to be as large as possible. This is exactly what can be modelled in \( \lambda\mu \) (using the result of Lem. 1.12), where the functionality of throwing an exception \( M \) to name \( n \) can be represented by \( \mu_-.[n]M \) (where \( n \) does not occur in \( M \)), i.e. a context switch that erases (only) an applicative context:
\[ (\mu_.[n]M)PQ \rightarrow (\mu_.[n]M)QR \rightarrow (\mu_.[n]M)R \rightarrow \mu_.[n]M \]

Notice that this will always leave the prefix \( \mu_.[n] \), which therefore has to be removed through the encoding of the catch functionality. We can achieve this using \( \lambda\mu \)'s renaming and erasing reduction steps: we model catching on name \( n \) through \( \mu n.[\alpha]M \), essentially allowing for:
\[ \mu n.[\alpha](\mu_.[n]M)PQ \rightarrow_{\beta\mu}^\gamma (1.12) \ \mu n.[\alpha]\mu_.[n]M \rightarrow_{\beta\mu} (R) \ \mu n.[n]M \rightarrow_{\beta\mu} (E) \ M \]

However, this is not enough; we also want the catch-mechanism to disappear when computation terminates normally, as in
\[ \text{try } V; \ \text{catch } n(x) = M_i \rightarrow V \]
which is then modelled through, as a last step \( \mu n.[\alpha]V \rightarrow_{\beta\mu} V \) but this is only possible when \( \alpha = n \).

In conclusion, throwing to the name \( n \) has to be modelled through \( \mu_.[n] \), whereas catching on the name \( n \) has to be modelled through \( \mu n.[n] \). This is the approach of all interpretations into \( \lambda\mu \) we discuss here, even the historic ones, as, for example, the one presented in [18].
\[
\begin{align*}
(Ax) & : \Gamma, x : A \vdash x : A | \Delta \\
(\to I) & : \Gamma, x : A \vdash M : B | \Delta \\
& \quad \Gamma \vdash \lambda x. M : A \to B | \Delta \\
(\to E) & : \Gamma_1 \vdash M : A \to B | \Delta_1 \\
& \quad \Gamma_2 \vdash N : A | \Delta_2 \\
& \quad \Gamma_1, \Gamma_2 \vdash MN : B | \Delta_1, \Delta_2 \\
(\text{catch}) & : \Gamma \vdash \text{catch } \alpha : A | \Delta \\
& \quad \Gamma \vdash M : A | \Delta \\
(\text{throw}) & : \Gamma \vdash \text{throw } \alpha : M : B | \alpha : (A, \text{Dom}(\Gamma)), \Delta \\
\end{align*}
\]

Figure 3: Type assignment for Nakano’s system

1.5 Nakano’s system and Crolard’s interpretation

In [16], Nakano presented an unnamed programming language with catch and throw, together with a notion of type assignment. It is presented as an extension of a \(\lambda\)-calculus with pairing and disjunctive choice, and by adding tag variables that are used to mark destinations for the throw instructions. Crolard [5] later established a relation between Nakano’s calculus and Parigot’s \(\lambda\mu\) (see below).

We briefly summarise Nakano’s system as appeared in [16]; to facilitate the comparison with \(\lambda^\text{ty}\), we will not consider pairing, disjoint union, nor constants, and use Crolard’s syntax; we will call it \(\lambda^N\) here.

**Definition 1.13 (\(\lambda^N\))**

i) The terms of \(\lambda^N\) are defined through the grammar:

\[ M, N ::= x | \lambda x.M | MN | \text{catch } \alpha M | \text{throw } \alpha M \]

ii) Reduction on terms in \(\lambda^N\) is defined through the rules:

\[ M\{\text{throw } \alpha N / x\} \to \text{throw } \alpha N \] (\(x \in M, M \neq x, M \notin \text{C[catch } \alpha Q[x]]\))^3

\[ \text{catch } \alpha M \to M \] (\(\alpha \notin M\))

\[ \text{catch } \alpha (\text{throw } \alpha M) \to M \] (\(\alpha \notin M\))

\[ (\lambda x.M) N \to M\{N / x\} \]

iii) The notion of types and context of variables \(\Gamma\) is the same as that of Def. 1.6; as usual, we will write \(\text{Dom}(\Gamma)\) for \(\{ x \mid \exists A \ [ x : A \in \Gamma]\}\). The notion of name context maps names to pairs of types and sets of term variables, \(\alpha : (A, V)\). The definition of compatible union of contexts of names \(\Delta_1, \Delta_2\) then requires the type for a name to be the same in both \(\Delta_1\) and \(\Delta_2\), and takes the union of the associated sets.

iv) Type assignment for \(\lambda^N\) is defined through the inference rules in Fig. 3 (modified here to our syntax and limitations of the language).

The extra feature of adding a set of type variables to names in the right-hand context is used in two positions: in rule (\(\to I\)), to avoid binding of a free variable that occurs in a term that gets thrown, and in rule (\(\text{throw}\)) where the set of variables in the context of inputs used to type the term to be thrown gets stored in the context of names. Notice that rule (\(\text{throw}\)) adds \(\alpha : (A, V)\) to the context of names; it is not clear if Nakano intends this to be a true addition, i.e if \(\alpha\) is supposed to not already occur in \(\Delta\); since the third reduction rule demands that the name towards which the expression \(M\) is thrown does not appear in \(M\), this seems to be the case.

Nakano proves that the system satisfies subject reduction; it avoids the problem highlighted in Ex. 4.5 through not allowing abstraction over variables that occur in thrown terms. However, this restriction is quite strong. For example, the term

\[ \lambda x. (\lambda a b) (\text{throw } \alpha x) x \]

3 The third restriction is missing in [16], but this seems to be in error.
would be considered untypeable in Nakano’s system, since we have the \( \lambda^N \)-reduction

\[
\lambda x. (\lambda ab. b) (\text{throw } a \ x) x \rightarrow \text{throw } a \ x
\]
even though its type would be \( A \rightarrow A \), and it safely runs to \( \lambda x. x \) under lazy reduction. In our approach (as detailed below), we will type the term, but not allow an exception to be thrown from inside an abstraction.

Notice that the first reduction rule states that any context can be eradicated by a \text{throw} that occurs inside it; thereby, this yields a highly non-confluent calculus; this was already observed by Nakano, who gives the following example: take

\[
M = \text{catch } a \ ((\lambda xy. I) (\text{throw } a \ K) (\text{throw } a \ Z))
\]

(where \( I = \lambda x. x \), \( K = \lambda ab. a \), and \( Z = \lambda ab. b \)), then we have the following three reduction results:

\[
\begin{align*}
M & \rightarrow \text{catch } a \ ((\lambda y. I) (\text{throw } a \ Z)) \rightarrow \text{catch } a \ I \rightarrow I \\
M & \rightarrow \text{catch } a \ (\text{throw } a \ K) \rightarrow K \\
M & \rightarrow \text{catch } a \ (\text{throw } a \ Z) \rightarrow Z
\end{align*}
\]

So reduction is non-confluent.

In part to address this, Crolard [5] defines an interpretation of the terms in \( \lambda^N \) into \( \lambda\mu \).

Observe that, since reduction in \( \lambda\mu \) is confluent, this interpretation cannot preserve (all) \( \lambda^N \)-reductions.

**Definition 1.14** Crolard’s interpretation \( \mathcal{I}_c : \lambda^N \rightarrow \lambda\mu \) is (adapted to our notation) defined by:

\[
\begin{align*}
\mathcal{I}_c x &= x \\
\mathcal{I}_c \lambda x. N &= \lambda x. \mathcal{I}_c N \\
\mathcal{I}_c MN &= \mathcal{I}_c M \mathcal{I}_c N \\
\mathcal{I}_c \text{catch } a M &= \mu a. [\alpha] \mathcal{I}_c M \\
\mathcal{I}_c \text{throw } a N &= \mu_{-} [\alpha] \mathcal{I}_c N
\end{align*}
\]

Notice that this interpretation follows the observations made in Sect. 1.4. Then, for example, we get:

\[
\begin{align*}
\mathcal{I}_c \text{catch } a \ (\text{throw } a \ M) & \triangleq \mu a. [\alpha] (\mu_{-} [\alpha] \mathcal{I}_c M) \\
& \rightarrow \mu a. [\alpha] \mathcal{I}_c M \rightarrow \mathcal{I}_c M
\end{align*}
\]

The last step is only possible if \( a \) does not occur in \( \mathcal{I}_c M \), so respects the restriction imposed by the \( \lambda^N \)-reduction rule.

Nakano’s example term translates as:

\[
\begin{align*}
\mathcal{I}_c \text{catch } a \ ((\lambda xy. I) (\text{throw } a \ K) (\text{throw } a \ Z)) & \triangleq \mu a. [\alpha] ((\lambda y. I) (\mu_{-} [\alpha] K) (\mu_{-} [\alpha] Z)) \\
\end{align*}
\]

which in \( \lambda\mu \) only reduces as follows:

\[
\begin{align*}
\mu a. [\alpha] ((\lambda y. I) (\mu_{-} [\alpha] K) (\mu_{-} [\alpha] Z)) & \rightarrow \mu a. [\alpha] ((\lambda y. I) (\mu_{-} [\alpha] Z)) \\
\mu a. [\alpha] I & \rightarrow I
\end{align*}
\]

Moreover,

\[
\begin{align*}
\mathcal{I}_c \lambda x. (\lambda ab. b) (\text{throw } a \ x) & \triangleq \lambda x. (\lambda ab. b) (\mu_{-} [\alpha] x) \\
\lambda x. (\lambda ab. b) (\mu_{-} [\alpha] x) & \rightarrow^* \lambda x. x
\end{align*}
\]

\[4\] Nakano uses numbers rather than \( I, K, \) and \( Z \) to get a typeable term.
Nakano’s system is not preserved under Crolard’s interpretation. Moreover, de Groote uses the restrictions present in Def. 2.1 for names, which he calls ‘exception variables’, and keeps for names, which he calls ‘exception variables’, and keeps for them typeability in Nakano’s system is not preserved under Crolard’s interpretation.

1.6 De Groote and Bierman’s approach

In [4], Bierman studies the interpretation of de Groote’s simply-typed calculus $\lambda^{\alpha}_{exn}$ as presented in [13] into an abstract machine that evaluates $\lambda\mu$-terms using a call-by-value strategy. De Groote’s calculus is based on ML’s [15] handling of exceptions. We will follow Bierman’s notation here, updated to ours.

Definition 1.15 $\lambda^{\alpha}_{exn}$-terms are defined through the grammar:

\[
M, N ::= V \mid MN \mid \text{raise} (n, M) \mid \text{let} n \in M \text{ handle} n x \Rightarrow N \text{ end}
\]

\[
V ::= c \mid x \mid \lambda x.M
\]

It uses the set of types defined as $A, B ::= a \mid \bot \mid A \rightarrow B$ (where $a$ ranges over a set of ground types and $\bot$ is a distinguished ground type) and the type assignment rules in Fig. 5 where $\neg A = A \rightarrow exn$, with $exn$ ML’s type of exceptions, represented as $\bot$. $\sigma$ assigns the appropriate ground type to each constant.

This system is, like Nakano’s, developed out of classical logic, and de Groote argues that it is complete, i.e. fully represents classical proofs.

Definition 1.16 The reduction relation on $\lambda^{\alpha}_{exn}$ is defined through the rules:

\[
\begin{align*}
\Gamma, x : A &\vdash x : A \mid \Delta \\
\Gamma, x : A &\vdash M : B \mid \Delta \\
\Gamma &\vdash \lambda x. M : A \rightarrow B \mid \Delta \\
\Gamma &\vdash M : A \rightarrow B \mid \Delta \\
\Gamma &\vdash \alpha \mid \Delta \\
\Gamma &\vdash \text{let} n \in M \text{ handle} n x \Rightarrow N \text{ end} : B \mid \Delta
\end{align*}
\]
\((\lambda x. M) V\) \quad \rightarrow M\{V/x\}

\(V'(\text{raise } (n, V))\) \quad \rightarrow \text{raise } (n, V)

\((\text{raise } (n, V)) M\) \quad \rightarrow \text{raise } (n, V)

\text{raise } (m, \text{raise } (n, V)) \quad \rightarrow \text{raise } (n, V)

\text{let } n \text{ in } V \text{ handle } n \ x \Rightarrow N \text{ end} \quad \rightarrow V \quad (n \ \notin fn(V))

\text{let } n \text{ in } \text{raise } (n, V) \text{ handle } n \ x \Rightarrow N\{V/x\} \quad (n \ \notin fn(V, N))

\text{let } n \text{ in } \text{raise } (m, V) \text{ handle } n \ x \Rightarrow N \text{ end} \quad \rightarrow \text{raise } (m, V) \quad (m \neq n, n \ \notin fn(V))

Notice that there are no rules permitting raising an exception from within an abstraction, thereby avoiding the subject reduction problem mentioned in Ex. 4.5. However, de Groote does not put the side-condition on the last three rules, opening the system to another kind of subject reduction problem; Bierman adds the restrictions in his presentation. Operationally, the \(\lambda\varepsilon\beta\) \-term ‘let \(n\) in \(M\) handle \(n\) \(x\) \Rightarrow \(N\) \text{ end}’ corresponds to the \(\lambda\beta\varepsilon\) \-term ‘try \(M\); catch \(n(x) = N\)’ (see Def. 2.1).

**Definition 1.17 (Interpretation of \(\lambda\varepsilon\beta\) \-into \(\lambda\mu\)**) Bierman defines the interpretation of terms into \(\lambda\mu\)-terms as follows:

\[
\begin{align*}
\text{let } n \text{ in } M \text{ handle } n \ x &= \ N \text{ end}_{\text{j}}{\text{M}}_{\text{\beta}}{\text{N}}{\text{\beta}}_{\text{j}} \\
\mu\beta_n.\beta_n(\lambda x. M) (\mu n. \beta_n) \text{raise } (n, M)_{\beta} &= \mu\beta_n.\beta_n(\lambda x. M) (\mu n. \beta_n) (\mu n. \beta_n) \quad (n \ \notin fn(V), N))
\end{align*}
\]

and states “It is quite easy to verify that this translation preserves the expected operational behaviour.”, intended through his interpretation into the abstract machine which essentially runs call-by-value reduction, but not shown.

**Example 1.18** As illustration of Bierman’s claim, take ‘let \(n\) in \(\text{raise } (n, M)\) handle \(n\) \(x\) \Rightarrow \(M\) \text{ end}’. Then:

\[
\begin{align*}
\text{let } n \text{ in } \text{raise } (n, M) \text{ handle } (n z) &= \text{M end}_{\text{\beta}}{\text{M}}_{\text{\beta}}{\text{N}}{\text{\beta}}_{\text{j}} \\
\mu\beta_n.\beta_n(\lambda x. M) (\mu n. \beta_n) \text{raise } (n, M)_{\beta} &= \mu\beta_n.\beta_n(\lambda x. M) (\mu n. \beta_n) (\mu n. \beta_n) \\
\mu\beta_n.\beta_n(\lambda n. M)_{\beta} (\mu n. \beta_n) \text{N}_{\beta} &= (n \neq \beta_n) \\
\text{let } n \text{ in } V \text{ handle } n \ x &= \ N \text{ end}_{\text{\beta}}{\text{M}}_{\text{\beta}}{\text{N}}_{\beta} \\
\mu\beta_n.\beta_n(\lambda n. M)_{\beta} (\mu n. \beta_n) \text{V}_{\beta} &= (n \neq \beta_n) \\
\mu\beta_n.\beta_n(\lambda n. M)_{\beta} (\mu n. \beta_n) \text{V}_{\beta} &= (n \neq \beta_n)
\end{align*}
\]

Also, for ‘let \(n\) in \(V\) handle \(n\) \(x\) \Rightarrow \(N\) \text{ end}’ with \(n \ \notin fn(V)\) we get:

\[
\begin{align*}
\text{let } n \text{ in } V \text{ handle } n \ x &= \ N \text{ end}_{\text{\beta}}{\text{M}}_{\text{\beta}}{\text{N}}_{\text{\beta}}{\text{V}}_{\beta} \\
\mu\beta_n.\beta_n(\lambda n. M)_{\beta} (\mu n. \beta_n) \text{V}_{\beta} &= (n \neq \beta_n) \\
\mu\beta_n.\beta_n(\lambda n. M)_{\beta} (\mu n. \beta_n) \text{V}_{\beta} &= (n \neq \beta_n) \\
\mu\beta_n.\beta_n(\lambda n. M)_{\beta} (\mu n. \beta_n) \text{V}_{\beta} &= (n \neq \beta_n)
\end{align*}
\]

[3] essentially uses \((\lambda x. \mu\beta_a. [a] M)_{\beta}\), but the use of \(a\) rather than \(n\) seems to be in error.
2 The calculus \( \lambda^{\text{try}} \)

The calculus \( \lambda^{\text{try}} \) we will present in this section will use the C++/Java-like syntax of `try`, `throw`, and `catch`, but will discern the exception handlers by name rather than by type. We will see the term `catch n(x) = M` as an exception handler named \( n \) that can receive a parameter on \( x \) after which it runs \( M \) with the parameter taking the position of \( x \) in \( M \), and `throw n(N)` a call to the exception handler with name \( n \), passing it the argument \( N \). By the very nature of exception handling, this implies that then \( N \) itself is a term that does not call on itself (so exception handling is non-recursive), but can call on other exception handlers, defined outside the scope of the present try-term.

Terms of \( \lambda^{\text{try}} \) are defined as follows:

**Definition 2.1 (Syntax of \( \lambda^{\text{try}} \))**

i) The set of pre-terms of \( \lambda^{\text{try}} \) is defined by the grammar:

\[
\text{Catch Block} ::= e | \text{Catch Block}; \text{catch n(x) = M}
\]

\[
M, N ::= V | MN | \text{try M; Catch Block} | \text{throw n(M)}
\]

\[
V ::= x | \lambda x.M \quad (\text{Values})
\]

ii) We will call \( n \) in `catch n(x) = M` a declared name and will write \( \text{catch n}_i(x) = M_i \) for the catch-block

\[
\text{catch n}_1(x) = M_1; \ldots; \text{catch n}_n(x) = M_n.
\]

The order in which the exception handlers appear in the catch-block is not important.

iii) The set of terms are pre-terms that satisfy the following restrictions:

a) In a try-term the catch-block is never empty (\( e \)), and in a catch-block `catch n_i(x) = M_i` the names \( n_i \) do not occur in the exception handler \( M_j \), for any \( i, j \in n \) (where \( i \in n \) stands for \( i \in \{1, \ldots, n\} \)), and all declared names \( n_1, \ldots, n_n \) are distinct;

b) for each `throw n_i(N)` that occurs inside \( M \) in the term `try M; catch n_i(x) = N_i`, none of the names \( n_i \) occur in \( N \).

iv) We define the notion of bound variables and of bound names of \( M \) (respectively \( \text{bv}(M) \) and \( \text{bn}(M) \)) as usual, considering \( x \) and \( \overline{n} \) bound in `try M; catch n_i(x) = N_i`.

\[
\begin{align*}
\text{bv}(x) &= \emptyset & \text{bn}(x) &= \emptyset \\
\text{bv}(\lambda x.M) &= \text{bv}(M) \cup \{ x \} & \text{bn}(\lambda x.M) &= \text{bn}(M) \\
\text{bv}(MN) &= \text{bv}(M) \cup \text{bv}(N) & \text{bn}(MN) &= \text{bn}(M) \cup \text{bn}(N) \\
\text{bv(try M; catch n_i(x) = N_i)} &= \text{bv}(M) \cup \text{bn}(N) & \text{bn(try M; catch n_i(x) = N_i)} &= \{ n_1, \ldots, n_n \} \cup \\
\text{bv}(N_1) \cup \cdots \cup \text{bv}(N_n) \cup \{ x \} & \text{bn}(M) \cup \text{bn}(N_1) \cup \cdots \cup \text{bn}(N_n) & \\
\text{bv(throw n(M))} &= \text{bv}(M) & \text{bn(throw n(M))} &= \text{bn}(M)
\end{align*}
\]

A variable or name is free in \( M \) if it occurs in \( M \) and is not bound; we write \( \text{fv}(M) \) for the set of free variables in \( M \), and \( \text{fn}(M) \) for the set of its free names.

We accept Barendregt's convention, so all free and bound variables and names are distinct, using renaming of bound variables or names (\( \alpha \)-conversion) when necessary.

To control the throwing of exceptions, we define a notion of call by name (lazy) and call by value reduction; these define an evaluation strategy, where only ever one sub-expression can execute and an exception is only ever thrown when needed to continue reduction.

**Definition 2.2 (\( \lambda^{\text{try}} \)-Reduction)**

i) The notion of call-by-name reduction \( \rightarrow^\text{\text{try}}_n \) on \( \lambda^{\text{try}} \) is defined as an extension of lazy reduction on \( \lambda \)-terms. The main reduction rules are:
\[
(\beta) : (\lambda x. M) N \to M\{N/x\}
\]
\[
(\text{throw}) : \text{throw } n(N) M \to \text{throw } n(N)
\]
\[
(\text{try-throw}) : \text{try throw } n_i(N); \text{Catch}_\text{Block}; \text{catch } n_i(x) = M_i \to M_i\{N/x\}
\]
\[
(\text{try-normal}) : \text{try } N; \text{catch } n_i(x) = M_i \to N (n_i \notin N)
\]

Call-by-name applicative contexts are defined as:
\[
C_N^\lambda := [] | C_N^\lambda M | \text{try } C_N^\lambda; \text{Catch}_\text{Block}
\]

ii) The notion of call-by-value reduction \(\lambda^\text{by}\) on \(\lambda^\mu\) is defined as an extension of call-by-value reduction on \(\lambda\)-terms using the main reduction rules from call-by-name, with the exception of \((\beta)\) which gets replaced by:
\[
(\beta_N) : (\lambda x. M) V \to M\{V/x\}
\]
It adds the rule:
\[
(\text{throw}_N) : V (\text{throw } n(N)) \to \text{throw } n(N)
\]
Call-by-value applicative contexts are defined as:
\[
C_N^\nu := [] | C_N^\nu M | V C_N^\nu | \text{try } C_N^\nu; \text{Catch}_\text{Block}
\]

Notice that, as in all (call by name, or call by value) functional languages, reduction does not allow for the evaluation of the body of an abstraction; this implies that throws inside the body are not ‘triggered’ until at least the surrounding abstraction has disappeared as the result of the contraction of a redex. If execution inside a try-block leads to a term \(N\) that does not contain throws to the declared names, then the result of the try-block is just that \(N\); it is not necessarily the case that reduction of \(N\) has terminated.

3 Interpreting \(\lambda^\text{by}\) in \(\lambda^\mu\)

In this section we will define an interpretation of \(\lambda^\text{by}\)-terms into \(\lambda^\mu\), using the approach we discussed above. Notice that, by the very nature of \(\lambda^\mu\), when encoding throw using a context switch, the body of the throw is not the information that something has gone wrong that gets passed to the exception handler, but in fact the entire exception handler. This implies that, when dealing with the term ‘try \(M\); catch \(n_i(x) = N_i\)’, we need to bring the exception handlers catch \(n(x) = N\) inside the interpretation of \(M\); this is done using substitution,\(^8\) introducing variables \(c_n\) that are placed in front of the argument that is passed to the exception handler in throw \(n_i(M)\).

**Definition 3.1 (Interpretation of \(\lambda^\text{by}\) into \(\lambda^\mu\))** We extend the set of names in \(\lambda^\mu\) with \(n, m, \ldots\), and define the interpretation of terms in \(\lambda^\text{by}\) into \(\lambda^\mu\)-terms as follows:

\[
\begin{align*}
\text{I}_x &\triangleq x \\
\text{I}_x M &\triangleq \lambda x. \text{I}_M \\
\text{I}_M N &\triangleq \mu x. [n] c_n \text{I}_M \\
\text{I}_{\text{throw } n(M)} &\triangleq \mu x. [n] c_n \text{I}_M \\
\text{I}_{\text{try } M; c \text{ of } N} &\triangleq \mu x. [n] c_n \text{I}_M \\
\text{I}_{\text{try } M; \text{Catch}_\text{Block}; \text{catch } n(x) = L} &\triangleq (\mu x. [n] c_n \text{I}_M) \{\lambda x. \text{I}_L / c_n\}
\end{align*}
\]

\(^8\) A perhaps more elegant approach is to encode a try-block using a redex, rather than term substitution, but that implies that we can no longer model lazy (cbv) reduction in \(\lambda^\text{by}\) by lazy (cbv) reduction in \(\lambda^\mu\), in particular when modelling the step \(M \to N \Rightarrow \text{try } M; \text{Catch}_\text{Block} \to \text{try } N; \text{Catch}_\text{Block}\).
Remark 3.2 Although many names can be used in a λβν-term, when interpreting into λμ all collapse onto the outermost one. To illustrate this, take the term

\[ \text{try } M(\text{throw } m(N)) (\text{throw } n(L)); \text{ catch } n = P; \text{ catch } m(x) = Q \]

The interpretation of this term is

\[
\begin{align*}
(μm.[m] (μn.[n] \langle M_M(μ_\mu [m] c_n N_M^L) (μ_\mu [n] c_n N_M^L) \rangle (λx. I_{M_M} / c_n)) (λx. I_{Q_M} / c_m) = & \\
μm.[m] μn.[n] I_{M_M[i]} (μ_\mu [m] (λx. μQ_M[i] μN_M[i]) (μ_\mu [n] (λx. μP_M[i] μL_M[i])) \rightarrow_βμ (R) & \\
μm.[m] I_{M_M[i]} (μ_\mu [m] (λx. μQ_M[i] μN_M[i]) (μ_\mu [n] (λx. μP_M[i] μL_M[i])) \rightarrow_βμ (R) & .
\end{align*}
\]

We will show that both reduction and assignable types (under the basic system, see Sect. 4) are preserved under this interpretation. First we show that term-substitution is preserved under the interpretation.

Lemma 3.3 (I_{M[i]} preserves term substitution)  I_{M[i]} \{N_M[i] / x\} = I_{M[i]} \{N / x\}

Proof: (x):  I_{y[i]} \{N_M[i] / x\} = x  I_{N_M[i] / x} = I_{N_M[i] / x} = I_{x} = I_{N / x}  I_{y[i]}
(y ≠ x):  I_{y[i]} \{N_M[i] / x\} = y  I_{N_M[i] / x} = y = I_{y}  I_{N / x}  I_{y[i]}
(λy.M):  I_{y[i]}  M[i] \{N_M[i] / x\} = (λy. M[i]) \{N_M[i] / x\} = λy. M[i] \{N_M[i] / x\} = (IH) λy. M[i] \{N / x\}  I_{y[i]} = I_{λy. M[i]} \{N / x\}  I_{y[i]} = (IH) I_{M[i]} \{N / x\}  I_{y[i]} = I_{M[i]} \{N / x\}  I_{y[i]}
(PQ):  I_{PQ[i]} \{N_M[i] / x\} = I_{P[i]}  I_{Q[i]} \{N_M[i] / x\} = I_{P[i]}  I_{Q[i]} \{N / x\}  I_{y[i]} = I_{P[i]} \{N / x\}  I_{Q[i]} \{N / x\}  I_{y[i]}

We can now show that cbn-reduction on λβν-terms is preserved as well under the interpretation:

Theorem 3.4 (Soundness of I_{M[i]} with respect to \rightarrow^*_βν) If P \rightarrow^*_βν Q, then I_{P[i]} \rightarrow^*_βμ I_{Q[i]}.

Proof: By induction on the definition of \rightarrow^*_βν. We show the non-trivial cases (and drop the subscript on I_{M[i]}).

(throw): Then P = (throw n(M)) M \rightarrow n(M) = Q, and

\[ I_{\text{throw } n(M)} M_M \triangleq (μ_\mu [n] c_n I_{M_M} \rightarrow_β^μ (1.12) μ_\mu [n] c_n I_{M_M} \triangleq I_{\text{throw } n(M)} I_M \]

(try-throw): Then P = try throw n(N); catch n(x) = M_l \rightarrow M_l \{N / x\} = Q, with l ∈ \{1, \ldots, n\}, and

19
In this section we will define a notion of basic type assignment for terms in $\lambda \mu$.

Similarly, we can verify that the interpretation respects call by value reduction for the $\lambda \mu$-calculus used in these two encoding results are renaming, erasing and $\mu$ (or $\nu$) towards a non-occurring name.

4 Basic type assignment

In this section we will define a notion of basic type assignment for terms in $\lambda \mu$ in the traditional way; in particular, in rule (try), we will demand that the type of the main term is
exactly that returned by all exception handlers; this is, in principle, also the approach chosen for java [7], and all the notions of type assignment presented above in Sect. 1.

**Definition 4.1 (Basic type assignment for $\lambda^{by}$)**  
i) Types and contexts of variables $\Gamma$ are those of Def. 1.2.

ii) A context of names $\Delta$ is a partial mapping from names to types, denoted as a finite set of statements $n:A$, such that the subjects of the statements (n) are distinct. Notions $\Delta_1,\Delta_2$, as well as $\Delta,n:A$ and $n \notin \Delta$ are defined as before.

iii) Basic type assignment for terms in $\lambda^{by}$ is defined through the inference system in Fig. 6.

We write $\Gamma \vdash_b M : A \mid \Delta$ for statements derivable using these rules.

Notice that our (throw) rule is almost identical to Nakano’s in that it allows to derive any type for the term throw n(N), but provided there is an exception handler with name n capable of accepting arguments of the type of N, as represented by the context of names.

As an explanation to rule (try), notice that, if we have derivations for

\[
\Gamma \vdash M : C \mid n_1:A_1 \rightarrow B_1,\Delta
\]

and

\[
\Gamma, x:A_i \vdash N_i : B_i \mid \Delta \quad (\forall i \in n)
\]

then we cannot predict, a priori, if running $M$ to normal form $M'$ will throw an exception or not. If it does not, then running the term $\text{try } M; \text{catch } n_1(x) = N_1$ will result in $M'$ (assuming $M'$ is free of throws) and to achieve subject reduction, $M'$ should be of type C. If it does, running $M$ will produce $\text{throw } n(L)$ and (assuming $n = n_1 \in n_1$), try $M; \text{catch } n_1(x) = N_1$ will run to $N_1\{L/x\}$, which has type $B_i$. So in order to achieve a subject reduction result also for this case, there is no choice but to demand that $C = B_1 = \cdots = B_n$.

**Lemma 4.2 (Weakening and thinning for $\vdash_b$)** The following rules are admissible for $\vdash_b$:

\[
(Wk) : \quad \frac{\Gamma \vdash_b M : A \mid \Delta}{\Gamma' \vdash_b M : A \mid \Delta'} \quad (\Gamma \subseteq \Gamma', \Delta \subseteq \Delta')
\]

\[
(Th) : \quad \frac{\Gamma \vdash_b M : A \mid \Delta}{\Gamma' \vdash_b M : A \mid \Delta'} \quad (\Gamma' = \{x : B \in \Gamma \mid x \in \text{fv}(M)\}, \Delta' = \{n : B \in \Delta \mid n \in \text{fv}(M)\})
\]

**Proof:** Standard. \(\square\)

We can show:

**Lemma 4.3 (Substitution lemma for $\vdash_b$)** If $\Gamma, x:C \vdash_b M : A \mid \Delta$ and $\Gamma \vdash_b N : C \mid \Delta$, then $\Gamma, x{N/x} : \{N/x\} : A \mid \Delta$.

**Proof:** By induction on the definition of term substitution.

1. \((M \equiv x)\): Then $x : A \in \Gamma, x:C$, so $A = C$. Also, $x\{N/x\} = N$, so $\Gamma \vdash_b x\{N/x\} : A \mid \Delta$.
2. \((M \equiv y \neq x)\): Then $y : A \in \Gamma$, so $\Gamma \vdash_b y : A \mid \Delta$.
3. \((M \equiv \lambda y . M')\): Then $A = A' \rightarrow B'$ and $\Gamma, x:C, y:A' \vdash_b M' : B' \mid \Delta$. By induction, $\Gamma, y:A' \vdash_b M' \{N/x\}$:
But then \( \Gamma \vdash_n \lambda y. M' \{ N / x \} : A \mid \Delta \) by \((\rightarrow I)\), so \( \Gamma \vdash_n \lambda y. (M' \{ N / x \}) : A \mid \Delta \). Notice that \( \lambda y. (M' \{ N / x \}) = (\lambda y. M') \{ N / x \} \).

\((M \equiv PQ)\): Then there exists \( B \) such that \( \Gamma, x : C \vdash_n P : B \rightarrow A \mid \Delta \) and \( \Gamma, x : C \vdash_n Q : B \mid \Delta \). By induction both \( \Gamma \vdash_n P \{ N / x \} : B \rightarrow A \mid \Delta \) and \( \Gamma \vdash_n Q \{ N / x \} : B \mid \Delta \); then, by \((\rightarrow E)\), we have \( \Gamma \vdash_n P \{ N / x \} Q \{ N / x \} : A \mid \Delta \). Notice that \( P \{ N / x \} Q \{ N / x \} = (PQ) \{ N / x \} \).

\((M \equiv \text{try } P; \text{catch } n(y) = Q_i)\): Then there exists \( B_i (i \in \mathbb{N}) \) such that \( \Gamma, x : C \vdash_n P : A \mid \Gamma, n_i ; B_i \rightarrow C, \Delta \) and \( \Gamma, x : C ; y : B_i \vdash_n Q_i : A \mid \Delta \), for all \( i \in \mathbb{N} \). By induction, \( \Gamma \vdash_n P \{ N / x \} : A \mid \Gamma, n_i ; B_i \rightarrow C, \Delta \) and \( \Gamma, y : B_i \vdash_n Q_i \{ N / x \} : A \mid \Delta \), for all \( i \in \mathbb{N} \). Then we get \( \Gamma \vdash_n \text{try } P \{ N / x \}; \text{catch } n_i(y) = Q_i \{ N / x \} : A \mid \Delta \) by rule \((\text{try})\). Notice that

\[
\text{try } P \{ N / x \}; \text{catch } n_i(y) = Q_i \{ N / x \} = (\text{try } P; \text{catch } n_i(y) = Q_i) \{ N / x \}
\]

\((M \equiv \text{throw } n(P))\): Then there exists \( B, C \) such that \( n : B \rightarrow C \in \Delta \), and \( \Gamma, x : C \vdash_n P : B \mid \Delta \). By induction \( \Gamma \vdash_n P \{ N / x \} : B \mid \Delta \). Since \( n : B \rightarrow C \in \Delta \), by rule \((\text{throw})\) we get \( \Gamma \vdash_n \text{throw } n(P \{ N / x \}) : A \mid \Delta \); notice that \( \text{throw } n(P \{ N / x \}) = (\text{throw } n(P)) \{ N / x \} \).

\(\square\)

It is relatively straightforward to show that this notion of type assignment is closed under CBN and cbv-reduction:

**Theorem 4.4 (Subject Reduction for \( \vdash_n \))** i) If \( \Gamma \vdash_n P : A \mid \Delta \) and \( P \rightarrow_n^S Q \), then \( \Gamma \vdash_n Q : A \mid \Delta \).

ii) If \( \Gamma \vdash_n P : B \mid \Delta \) and \( P \rightarrow_n^\text{TRY} Q \), then \( \Gamma \vdash_n Q : B \mid \Delta \).

**Proof:** i) By induction on the definition of \( \rightarrow_n^S \).

\((\beta)\): Then \( P = (\lambda x. M) N \rightarrow M \{ N / x \} = Q \), and the derivation for \( P \) is constructed as follows:

\[
\begin{array}{c}
\Gamma, x : D \vdash M : B \mid \Delta \\
\Gamma \vdash \lambda x. M : D \rightarrow B \mid \Delta \\
\Gamma \vdash (\lambda x. M) N : B \mid \Delta
\end{array}
\]

In particular, then \( \Gamma, x : D \vdash M : B \mid \Delta \) and \( \Gamma \vdash_n N : D \mid \Delta \), and the result follows Lemma 4.3.

\((\text{throw})\): Then \( \Delta = n : A \rightarrow C, \Delta' \), \( P = (\text{throw } n(N)) M \rightarrow \text{throw } n(N) = Q \), and the derivation for \( P \) is constructed as:

\[
\begin{array}{c}
\Gamma \vdash n(N) : D \rightarrow B \mid n : A \rightarrow C, \Delta' \\
\Gamma \vdash M : D \mid n : A \rightarrow C, \Delta' \\
\Gamma \vdash (\text{throw } n(N)) M : B \mid n : A \rightarrow C, \Delta'
\end{array}
\]

We can construct the derivation for \( Q \):  

\[
\begin{array}{c}
\Gamma \vdash n(N) : B \mid n : A \rightarrow C, \Delta' \\
\Gamma \vdash (\text{throw } n(N)) : B \mid n : A \rightarrow C, \Delta'
\end{array}
\]

\((\text{try-throw})\): Then \( P = \text{try-throw } n_i(M) ; \text{catch } n_i(x) = N_i \rightarrow N_i \{ M / x \} = Q \) and the derivation for \( P \) is constructed as:

\[
\begin{array}{c}
\Gamma \vdash M : A_i \mid n_i ; A_i \rightarrow B, \Delta \\
\Gamma \vdash n_i(M) : B \mid n_i ; A_i \rightarrow B, \Delta \\
\Gamma \vdash \text{try-throw } n_i(M) ; \text{catch } n(x) : N : B \mid \Delta
\end{array}
\]

\(\uparrow\) Notice that \( \text{throw } n(N) \) changes type; this corresponds to a feature of reduction in \( \lambda \mu \), where in some presentations the structural rule is written as (using the notation of Definition 1.5) \( \mu a. ([\beta] M) \rightarrow \mu a. ((\beta) M \{ N a / a \}) \); before the reduction, \( \alpha \) has type \( A \rightarrow B \), say, and after it has type \( B \).
In particular, we have derivations for both $\Gamma \vdash_{\mathbb{B}} M : A_1 \mid n_i : A_i \rightarrow \overline{C}, \Delta$ and $\Gamma, x : A_1 \vdash_{\mathbb{B}} N_1 : B \mid \Delta$. By the definition of $\lambda^\mu$-terms, we know that $n_i \notin \text{fn}(M)$, for all $i \in \mathbb{I}$, so by thinning (Lem. 4.2) we can remove $n_i : A_i \rightarrow \overline{B}$ from the co-context for the first to obtain $\Gamma \vdash_{\mathbb{B}} M : A_1 \mid \Delta$. Then, by the substitution lemma Lem. 4.3, we obtain $\Gamma \vdash_{\mathbb{B}} N_1 \{M/x\} : B \mid \Delta$.

(try-normal): Then $P = \text{try } Q$; catch $n_i(x) = N_i \rightarrow Q$, and $n_i \notin Q$. Then the derivation for $P$ is constructed as follows:

$$
\begin{align*}
\Gamma \vdash_{\mathbb{B}} Q : B \mid n_i : A_i \rightarrow \overline{B}, \Delta, \\
\Gamma, x : A_1 \vdash_{\mathbb{B}} N_1 : B \mid \Delta \quad (\forall i \in \mathbb{I})
\end{align*}
$$

$$
\Gamma \vdash_{\mathbb{B}} \text{try } Q; \text{catch } n_i(x) = N_i : B \mid \Delta
$$

In particular, we have a derivation for $\Gamma \vdash_{\mathbb{B}} Q : B \mid n_i : A_i \rightarrow \overline{B}, \Delta$; as above we can remove $n_i : A_i \rightarrow \overline{B}$ from the co-context to obtain $\Gamma \vdash_{\mathbb{B}} Q : B \mid \Delta$.

ii) The proof is much like that for the previous part, but with the addition of:

(throw$_\mathbb{B}$): Then $\Delta = n : A \rightarrow C, \Delta'$, $P = V(\text{throw } n(N)) \rightarrow \text{throw } n(N) = Q$, and the derivation for $P$ is constructed as:

$$
\begin{align*}
\Gamma \vdash_{\mathbb{B}} V : E \rightarrow F \mid n : A \rightarrow C, \Delta', \\
\Gamma \vdash_{\mathbb{B}} \text{throw } n(N) : F \mid n : A \rightarrow C, \Delta'
\end{align*}
$$

$$
\Gamma \vdash_{\mathbb{B}} \text{V(throw } n(N)) : F \mid n : A \rightarrow C, \Delta'
$$

We can construct the derivation for $Q$:

$$
\begin{align*}
\Gamma \vdash_{\mathbb{B}} \text{throw } n(N) : F \mid n : A \rightarrow C, \Delta'
\end{align*}
$$

$(M \rightarrow N \Rightarrow VM \rightarrow VN)$: By induction.

Although restricting throwing an exception to applicative contexts might seem too limiting, it is in fact not possible to extend it to full reduction whilst preserving soundness, as we will argue now.

Example 4.5 Assume we would have tried to model throwing exceptions from inside an abstraction as well, by adding the rule:

$$(\text{throw-abstr}) : \lambda x . \text{throw } n(N) \rightarrow \text{throw } n(N)$$

Apart from that this is undesirable within programming languages (it would correspond to throwing an exception simply because it occurs in a function definition), or the fact that we cannot model this reduction in pure $\lambda\mu$, also subject reduction would fail instantly. Suppose we can derive

$$
\begin{align*}
\Gamma, x : A \vdash_{\mathbb{B}} N : D \mid n : D \rightarrow C, \Delta, \\
\Gamma, x : A \vdash_{\mathbb{B}} \text{throw } n(N) : B \mid n : D \rightarrow C, \Delta
\end{align*}
$$

$$
\Gamma \vdash_{\mathbb{B}} \lambda x . \text{throw } n(N) : A \rightarrow B \mid n : D \rightarrow C, \Delta
$$

We can construct

$$
\begin{align*}
\Gamma, x : A \vdash_{\mathbb{B}} \text{throw } n(N) : A \rightarrow B \mid n : D \rightarrow C, \Delta
\end{align*}
$$

but cannot, in general, derive $\Gamma \vdash_{\mathbb{B}} \text{throw } n(N) : A \rightarrow B \mid n : D \rightarrow C, \Delta$: notice that $x$ might be free in $N$, so then would need a type in any derivation for $N$. This problem was observed by Nakano [16, 17], who solved it by not allowing an abstraction to be typeable if the bound...
variable occurs in a thrown term, and avoided by many others who do not allow throwing an exception from within an abstraction, as we do here.

We will now show that our encoding into $\lambda \mu$ preserves types assignable in the basic system:

**Theorem 4.6 (Preservation of Assignable Types)** If $Γ \vdash B : \overline{A_i} \rightarrow \overline{C_i}$, then $Γ, c_{\overline{n}} : A_i \rightarrow \overline{C_i} \vdash_{\lambda \mu} FM_{\lambda \mu} : B \mid n_i : \overline{C_i}$.

**Proof:** By induction on the definition of $\vdash_B$.

(throw): Then the derivation looks like

$$
\Gamma \vdash M : A_i \mid n_i : A_i \rightarrow C_i
$$

(throw)

By induction we have $Γ, c_{\overline{n}} : A_i \rightarrow \overline{C_i} \vdash FM_{\lambda \mu} : A_i \mid n_i : \overline{C_i}, \Delta$, and we can construct:

$$
\Gamma, c_{\overline{n}} : A_i \rightarrow C_i \vdash c_{\overline{n}} : A \rightarrow C_i \mid n_i : C_i
$$

(Ax)

$$
\Gamma, c_{\overline{n}} : A_i \rightarrow C_i \vdash c_{\overline{n}} \cdot FM_{\lambda \mu} : C_i \mid n_i : C_i
$$

($\rightarrow E$)

$$
\Gamma, c_{\overline{n}} : A_i \rightarrow C_i \vdash c_{\overline{n}} \cdot FM_{\lambda \mu} : C_i \mid \theta, n_i : C_i
$$

(Wk)

$$
\Gamma, c_{\overline{n}} : A_i \rightarrow C_i \vdash m_{\overline{n}} \cdot c_{\overline{n}} \cdot FM_{\lambda \mu} : B \mid n_i : \overline{C_i}
$$

($\mu$)

and $\textbf{throw } n_i (M)_{\lambda \mu} = \mu_{\overline{n}} (n_i) \cdot c_{\overline{n}} \cdot FM_{\lambda \mu}$.

(try): Then the derivation ends like

$$
\Gamma \vdash \text{try } M; \text{ catch } m_{\overline{n}}(x) = N_i : B \mid n_i : A_i \rightarrow C_i
$$

(try)

We can now construct derivations for the two alternatives of the interpretation of a try-expression; we only present the second, the first is trivial. So the case we deal with here is

$\text{try } M; \text{ Catch } B \cdot C ; \text{ catch } m(x) = N_i \theta_{\lambda \mu} \triangleq (\mu_{\overline{n}} \cdot [m] \text{ try } M; \text{ Catch } B \cdot C ; [\lambda x. FN_{\lambda \mu} / c_{\overline{m}} ]_{\lambda \mu}$

Let $M' = \text{try } M; \text{ Catch } B \cdot C ;$ then $Γ, c_{\overline{n}} : A_i \rightarrow \overline{C_i}, c_m : D \rightarrow B \vdash FM_{\lambda \mu} : B \mid m, D, n_i : C_i$ and $Γ, c_{\overline{n}} : A_i \rightarrow \overline{C_i}, x : D \vdash FN_{\lambda \mu} : B \mid n_i : \overline{C_i}$ follow by induction. We can construct:

$$
\Gamma, c_{\overline{n}} : A_i \rightarrow \overline{C_i}, x : D \vdash FN_{\lambda \mu} : B \mid \overline{n_i}, \overline{C_i}
$$

(I)

$$
\Gamma, c_{\overline{n}} : A_i \rightarrow \overline{C_i} \vdash x \cdot FN_{\lambda \mu} : D \vdash \overline{n_i}, \overline{C_i}
$$

(Wk)

Then by Lem. 1.8, we have $Γ, c_{\overline{n}} : A_i \rightarrow \overline{C_i} \vdash FM'_{\lambda \mu} \{ \lambda x. FN_{\lambda \mu} / c_{\overline{m}} \} : B \mid m, B, n_i : \overline{C_i}$, and we can construct:

$$
Γ, c_{\overline{n}} : A_i \rightarrow \overline{C_i} \vdash FM'_{\lambda \mu} \{ \lambda x. FN_{\lambda \mu} / c_{\overline{m}} \} : B \mid m, B, n_i : \overline{C_i}
$$

($\mu$)

and $\mu_{\overline{n}} \cdot [m] FM'_{\lambda \mu} \{ \lambda x. FN_{\lambda \mu} / c_{\overline{m}} \} = (\mu_{\overline{n}} \cdot [m] FM'_{\lambda \mu} \{ \lambda x. FN_{\lambda \mu} / c_{\overline{m}} \}$

$\square$

So $\lambda^\text{try}$ with basic type assignment is fully representable in $\lambda \mu$.

Given our interpretation $\#_{\lambda \mu}$ of $\lambda^\text{try}$-terms into $\lambda \mu$ and Thm. 4.6, the rule (throw) is perfectly natural, since we can derive:
Notice that the second weakening step is correct, in that the names \( n \) and \( _\_ \) do not occur in \( N \), so (perhaps using thinning) can be assumed to not occur in \( \Delta \).

### 5 Adding \( \text{halt} \) to \( \lambda^\text{try} \)

We will now define a notion of type assignment that extends the system we defined above, by allowing for both recoverable and unrecoverable failure; to distinguish raising the latter kind of exception from the former, throw, we considered above, we use the keyword \( \text{halt} \). The idea is that \( \text{halt} \) gets propagated through the system and becomes the end result. Therefore, we need to add reduction rules that consume applicative contexts, as for throw, and make sure to not ‘catch’ the \( \text{halt} \), as that would localise the event and limit its range (see also Rem. 5.11). We will argue below that raising a \( \text{halt} \) is different from throw: when aiming for a representation in \( \lambda\mu \), we cannot use handlers and parameter passing for \( \text{halt} \). In Rem. 5.11 we will discuss an alternative approach, and indicate why that does not satisfy the purpose.

As mentioned above, following the suggestion of [1], we will aim to map our calculus onto \( \lambda\mu\text{-top} \), where \( \text{top} \) is a special name that cannot occur bound and denotes the top-level. We would therefore want to define a notion of type assignment that, for example, deals with \( \text{halt} \) by assigning it the type \( \bot \), but that would not be possible, as argued in Ex. 5.10.

We extend the calculus \( \lambda^\text{try} \) from Def. 2.1, by extending the set of pre-terms by adding the construct \( \text{halt} \); the notion of reduction is defined as in Def. 2.2, by adding the rule that expresses that also \( \text{halt} \) consumes an applicative context.

**Definition 5.1 (Syntax of \( \lambda^\text{try} \))**  
\( i \) The set of pre-terms of \( \lambda^\text{try} \) is defined by the grammar:

- \( \text{Catch\_Block} ::= c | \text{Catch\_Block};\text{catch } n(x) = M \)
- \( M, N ::= V \mid MN \mid \text{try } M;\text{Catch\_Block} \mid \text{throw } n(M) \mid \text{halt} \)
- \( V ::= x \mid \lambda x.M \)

\( ii \) The \( \text{cbn} \)-reduction system for \( \lambda^\text{try} \) is like that for \( \lambda^\text{py} \) from Def. 2.2, defined by the rules:

- \( (\beta) \): \( (\lambda x.M) N \rightarrow M\{N/x\} \)
- \( (\text{throw}) \): \( (\text{throw } n(N)) M \rightarrow \text{throw } n(M) \)
- \( (\text{halt}) \): \( \text{halt } M \rightarrow \text{halt} \)
- \( (\text{try-throw}) \): \( \text{try } \text{throw } n_i(N);\text{catch } n_i(x) = M_i \rightarrow M_i\{N/x\} \) \( \text{if } n_i \in \pi_j \)
- \( (\text{try-normal}) \): \( \text{try } N;\text{catch } n_i(x) = M_i \rightarrow N \) \( \text{if } n_i \notin \pi_j \)

\( \text{cbn applicative contexts} \) are defined as in Def. 2.2.

\( iii \) The \( \text{cbv} \)-reduction system for \( \lambda^\text{try} \) is that of \( \text{cbn} \), replacing rule \( (\beta) \) by the first reduction rule, and adding the second and third:

- \( (\beta_{\text{v}}) \): \( (\lambda x.M) V \rightarrow M\{V/x\} \)
- \( (\text{throw}_{\text{v}}) \): \( V(\text{throw } n(N)) \rightarrow \text{throw } n(N) \)
- \( (\text{halt}_{\text{v}}) \): \( V\text{halt} \rightarrow \text{halt} \)

\( \text{cbv applicative contexts} \) are defined as in Def. 2.2.

Notice that the system only handles throws; \( \text{halt} \) is just propagated through the reduction system until it is the remaining term, as in
catch n

Our aim is that the type \( \perp \) indicates the occurrence of a \texttt{halt} during execution, and that throws are in that sense invisible since they return a normal type. Therefore, arguably, we should have opted for the type assignment rule

\[
\text{(try)} : \quad \frac{\Gamma \vdash M : C | n: A \rightarrow C, \Delta \quad \Gamma, x : A \vdash N_i : C | \Delta \ (\forall i \in n)}{\Gamma \vdash \text{try} M; \text{catch} \ n_i(x) = N_i : C | \Delta}
\]

and to tweak the type assignment system such that only the rules \text{(halt)}, \text{(→E)}, and \text{(try)} would derive the type \( \perp \). However, that would not give an expressive enough notion of type assignment.

\textbf{Example 5.3} To illustrate that we have to allow \( C = \perp \) in rule \text{(try)}, take the term

\[\text{try} \ (\lambda xy.x) \ \text{halt} \ (\text{throw} \ n(L)); \ \text{catch} \ n(x) = P\]

which will panic. However, when not allowing the type for the main term in rule \text{(try)} to be \( \perp \), this term would not be typeable. Although we can allow the \text{throw} and \text{halt} to return different types inside \( (\lambda xy.x) \ \text{halt} \ (\text{throw} \ n(L)) \), as in Fig. 5.3, when we place this term inside the context of dealing with the \text{catch} on \( n \), this no longer is the case:

\[
\frac{\Gamma \vdash (\lambda xy.x) \ \text{halt} \ (\text{throw} \ n(L)) : \perp | \Delta_2 \quad \Gamma, x : C \vdash P : A | \Delta}{\Gamma \vdash \text{try} \ (\lambda xy.x) \ \text{halt} \ (\text{throw} \ n(L)); \ \text{catch} \ n(x) = P : \perp | \Delta \ (\text{try})}
\]

Remark that rule \text{(try)} demands that the return type of the handlers and the type of the main term are the same, so \( A = \perp \). So therefore we are forced to accept the rule \text{(try)} as in Fig. 7 which allows for \( C = \perp \), and we cannot conclude from the fact that a term has type \( \perp \) that it will raise a \text{halt}.

We will address this point again in Sect. 6, where we will present a system that does have that characteristic.
We can show the following:

**Lemma 5.4 (Substitution Lemma for \( \vdash_h \))** If \( \Gamma, x : C \vdash_h M : A | \Delta \) and \( \Gamma \vdash_h N : C | \Delta \), then
\[
\Gamma \vdash_h M \{ N / x \} : A | \Delta.
\]

**Proof:** By induction on the definition of term substitution.

\((M \equiv x)\):
If \( \Gamma, x : C \vdash_h x : A | \Delta \) and \( \Gamma \vdash_h N : C | \Delta \), then by rule \((Ax)\) we have \( x : A \in \Gamma, x : C \), so \( A = C \). Also, \( x\{N / x\} = N, \) so \( \Gamma \vdash_h x\{N / x\} : A | \Delta \).

\((M \equiv y \neq x)\):
If \( \Gamma, x : C \vdash_h y : A | \Delta \), then by \( y : A \in \Gamma \) and by rule \((Ax)\) also \( \Gamma \vdash_h y : A | \Delta \).

\((M \equiv \lambda y. M')\):
Then by rule \((\rightarrow I)\) we have \( A = A' \rightarrow B' \) and \( \Gamma, x : C \vdash_h M' : B' | \Delta \). By induction, \( \Gamma, y : A' \vdash_h M'\{N / x\} : B' | \Delta \). But then \( \Gamma \vdash_h \lambda y. M'\{N / x\} : A | \Delta \) by \((\rightarrow I)\), so \( \Gamma \vdash_h \lambda y. (M'\{N / x\}) = (\lambda y. M')\{N / x\} \).

\((M \equiv PQ)\):
Then either the derivation ends with rule \((\rightarrow E)\); then there exists \( B \) such that \( \Gamma, x : C \vdash_h P : B \rightarrow A | \Delta \) and \( \Gamma, x : C \vdash_h Q : B \rightarrow \Delta \). By induction both \( \Gamma \vdash_h P\{N / x\} : B \rightarrow A | \Delta \) and \( \Gamma \vdash_h Q\{N / x\} : B \rightarrow \Delta \). Then, by \((\rightarrow E)\), we have \( \Gamma \vdash_h P\{N / x\} \; Q\{N / x\} : A \rightarrow \Delta \). Notice that \( P\{N / x\} \; Q\{N / x\} = PQ\{N / x\} \).

\((M \equiv \text{try } P ; \text{catch } n_i(y = Q_i))\):
Then by rule \((\text{try})\) there exists \( B_i \) such that \( \Gamma, x : C \vdash_h P : A | \Delta \) and \( \Gamma, x : C \vdash_h B_i : Q_i : \bot \rightarrow \Delta \), for all \( i \in \{1, \ldots, n\} \). By induction, \( \Gamma \vdash_h P\{N / x\} : A \rightarrow \Delta \) and \( \Gamma, y : B_i \vdash_h Q_i\{N / x\} : \bot \rightarrow \Delta \), \( (1 \leq i \leq n) \). Then, by rule \((\text{try})\), we get \( \Gamma \vdash_h \text{try } P\{N / x\} ; \text{catch } n_i(y = Q_i)\{N / x\} : A | \Delta \)

and \( \text{try } P\{N / x\} ; \text{catch } n_i(y = Q_i)\{N / x\} = (\text{try } P ; \text{catch } n_i(y = Q_i))\{N / x\} \).

\((M \equiv \text{halt})\):
Immediate.

We can now show the following soundness result.

**Theorem 5.5 (Subject Reduction for \( \vdash_h \) with respect to \( \rightarrow^s_{\text{try}} \))** If \( \Gamma \vdash_h P : C \; \rightarrow^s_{\text{try}} Q \), then \( \Gamma \vdash_h Q : C \; \Delta \).

**Proof:** By induction on the definition \( \rightarrow^s_{\text{try}} \). The proof is very similar to that of Thm. 4.4; we only show here the interesting cases.

\((\text{halt})\):
Then \( P = \text{halt } M \rightarrow \text{halt } Q \), and the derivation for \( P \) is shaped like:

\[
\begin{array}{c}
\Gamma \vdash \text{halt } A : C \; \Delta \\
\hline
\Gamma \vdash \text{halt } M : C \; \Delta \\
\end{array}
\]

We have \( \Gamma \vdash_h \text{halt } C \; \Delta \) by rule \((\text{halt})\).

We can also show a similar result for cbv:

**Theorem 5.6 (Subject Reduction for \( \vdash_h \) with respect to \( \rightarrow^s_{\text{try}} \))** If \( \Gamma \vdash_h P : C \; \rightarrow^s_{\text{try}} Q \), then \( \Gamma \vdash_h Q : C \; \Delta \).

**Proof:** Similar to that of Thm. 5.5 and Thm. 4.4, but with the added cases:

\((\text{throw}_v)\):
Then \( \Delta = n : A \rightarrow C, \Delta' \), \( P = V(\text{throw } n(N)) \rightarrow \text{throw } n(N) = Q \), and the derivation for \( P \) is constructed as:

\[
\begin{array}{c}
\Gamma \vdash V : E \rightarrow F \; n : A \rightarrow C, \Delta' \\
\hline
\Gamma \vdash \text{throw } n(N) : F \; n : A \rightarrow C, \Delta' \\
\end{array}
\]

We can construct the derivation for \( Q \):
\[\Gamma \vdash n : A \mid n : A \rightarrow C, \Delta' \quad \text{(throw)}\]

(halt\_v): Then \(P = V \text{halt} \rightarrow \text{halt} = Q\), and the derivation for \(P\) is constructed as:

\[\Gamma \vdash V : A \rightarrow C \quad \Gamma \vdash \text{halt} : A \mid \Delta \quad \text{(halt)}\]

\[\Gamma \vdash V \text{halt} : C \mid \Delta \quad \text{\((-E)\)}\]

Notice that we have \(\Gamma \vdash \text{halt} : C \mid \Delta\) by rule (halt).

So, in terms of type assignment for a \(\lambda\)-calculus with exceptions, the failure system satisfies the basic requirement with respect to call-by-name and call-by-value reduction.

We can interpret \(\lambda^\text{TRV}_h\) in \(\lambda\mu\text{-top}\) as follows:

**Definition 5.7** (Interpretation of \(\lambda^\text{TRV}_h\) into \(\lambda\mu\text{-top}\))

i) We add the term constant \(\text{halt}^{10}\) to \(\lambda\mu\text{-top}\) that can only be assigned \(\bot\):

\[(\text{halt}) : \Gamma \vdash \text{halt} : \bot \mid \Delta\]

ii) The interpretation of \(\lambda^\text{TRV}_h\) in \(\lambda\mu\text{-top}\) is defined as follows:

\[
\begin{align*}
&\Gamma^x_j \quad \Delta \\
&\Gamma^\lambda x . M_j \quad \Delta = \lambda x. \Gamma^M_j \\
&\Gamma^MN_j \quad \Delta = \Gamma^M_j \Gamma^N_j \\
&\Gamma^\text{throw} n(M)_j \quad \Delta = \mu_w [n] c_n \Gamma^M_j \\
&\Gamma^\text{try} M ; \text{Catch} _\text{Block} ; \text{catch} n(x) = L_j \quad \Delta = (\mu_\_ \_ [n] \Gamma^\text{try} M ; \text{Catch} _\text{Block} _j) \{\lambda x. \Gamma^L_j / c_n\} \\
&\Gamma^\text{halt} _j \quad \Delta = \mu_\_ [\text{top}] \text{halt}
\end{align*}
\]

Notice that, in order to achieve that \(\Gamma^\text{halt} _j\) consumes applicative contexts, we need to use the prefix ‘\(\mu_\_\)’, as we have done also for \(\Gamma^\text{throw} n(M)_j\).

We can now show:

**Theorem 5.8** (Soundness of the Interpretation for \(\lambda^\text{TRV}_h\))

i) If \(P \rightarrow^*_h Q\), then \(\Gamma P_j \rightarrow^*_{\beta_\mu} \Gamma Q_j\).

ii) If \(P \rightarrow^* Q\), then \(\Gamma P_j \rightarrow^*_{\beta_\mu} \Gamma Q_j\).

**Proof:** i) As in the proof of Thm. 3.4, with the added case (again, we drop the subscript on \(\Gamma_j\)):

\[(\text{halt}): \text{Then } P = \text{halt} M \rightarrow^*_h \text{halt} = Q, \text{ and } \Gamma^\text{halt} M_j \triangleq (\mu_\_ [\text{top}] \text{halt}) \Gamma M_j \rightarrow^*_{\beta_\mu} (1.12) \mu_\_ [\text{top}] \text{halt} \triangleq \Gamma^\text{halt} _j\]

ii) As the proof for the previous case, except for the rules:

\[(\beta_\nu) : \text{As in case } (\beta) \text{ in the previous part.}\]

\[(\text{halt}_v) : \text{Then } P = V \text{halt } \rightarrow \text{halt} = Q, \Gamma^V \text{halt} _j \triangleq \Gamma^V _j (\mu_\_ [\text{top}] \text{halt}) \rightarrow^*_{\beta_\mu} (1.12) \mu_\_ [\text{top}] \text{halt} \triangleq \Gamma^\text{halt} _j\]

We can also show that assignable types are preserved.

**Theorem 5.9** (Preservation of Assignable Types) If \(\Gamma \vdash M : B \mid n_i : A_i \rightarrow C_i\), then \(\Gamma, c_n_i : A_i \rightarrow C_i \vdash^*_l \Gamma M_j : B \mid n_i : C_i\).

---

^{10} \text{We use } \text{halt} \text{ just as a place holder, it is not active in the reduction relation.}
Proof: By induction on the definition of $\vdash_h$, very similar to that of Thm. 4.6, but with an added case.

(halt): Then $M = \text{halt}$. We can construct

$$
\frac{\Gamma \vdash \text{halt} : \bot | a, C, \Delta}{\Gamma \vdash \mu_\bot [\text{top}] \text{halt} : C | \Delta} \quad \text{(halt)}
$$

and $\mu_\bot [\text{top}] \text{halt} = \mu_\bot [\text{top}] \text{halt}$. \hfill \Box

Remark 5.10 In this paper we are mainly looking at the relation between notions of exception handling and classical logic; in that setting, it would be reasonable to add the type constant $\bot$ to the type language, and use it to type $\text{halt}$, as also suggested in the proof of the previous theorem.

This is, on its own, perfectly feasible, and works well on the level of $\lambda^\mu$-terms, but we would not be able to establish a relation with $\lambda \mu$. For example, we can add the rules

$$(\text{halt}) : \frac{\Gamma \vdash \text{halt} : \bot | \Delta}{\frac{\Gamma \vdash M : \bot | \Delta \quad \Gamma \vdash N : A | \Delta}{\Gamma \vdash M N : \bot | \Delta}}$$

for a notion of type assignment geared towards CBV, and add the rule

$$(\to E) : \frac{\Gamma \vdash M : A | \Delta \quad \Gamma \vdash N : \bot | \Delta}{\Gamma \vdash M N : \bot | \Delta}$$

for CBV.\footnote{Notice that these two variants of $(\to E)$ need to be added to achieve subject reduction.}

The problem appears in the proof of Thm. 5.9, where we would have the case

$$(\to E_N) : \text{Then } M = P Q, \text{ the derivation looks like}$$

$$
\frac{\Gamma \vdash P : \bot | n_i : A_i \rightarrow C_i}{\text{(E)}}
$$

and by induction we have $\Gamma, c_{n_i} : A_i \rightarrow C_i \vdash I P_j : \bot | n_i : C_i$ and $\Gamma, c_{n_i} : A_i \rightarrow C_i \vdash I Q_j : D | n_i : C_i$.

In order for us to be able to combine these two derivations in $\vdash_{\top}$, we need to create the arrow type $D \rightarrow \bot$ from $\bot$. The only way to do that, in $\vdash_{\top}$, is to apply rule $(\text{top})$:

$$
\frac{\Gamma, c_{n_i} : A_i \rightarrow C_i \vdash_{\lambda \mu} \mu_{\bot [\text{top}]}, I P_j : \bot | n_i : C_i}{\text{(Wk)}}
$$

but $\mu_{\bot [\text{top}]}, I P_j \neq I P Q_j$. In fact, these terms are computationally incompatible.

So we cannot give the type $\bot$ the role it should have.

In the next section, we will introduce a notion of type assignment that uses the type constant $\bot$ (which can be seen as $\bot$) for calls to $\text{panic}$; as suggested here, we will not be able to establish a relation with $\lambda \mu$ or $\lambda \mu$-$\text{top}$ for that notion.

Remark 5.11 It might seem natural to define failing through $\text{halt}$ in much the same way as $\text{throw}$ (and that is basically what is suggested in [1]). This would lead to, contrary to what we have done above, adding $\text{panic} n(N)$ as a construct, together with dedicated exception handlers $\text{abort} n(x) = L$, so using, for example, the grammar:
and the (additional) reduction rules

\[
\begin{align*}
(\text{panic}) : & \quad (\text{panic } n(N)) M \rightarrow \text{panic } n(N) \\
(\text{try-panic}) : & \quad \text{try panic } n_i(N); \text{abort } n_i(x) = M_i \rightarrow M_i\{N/x\} \quad (n_i \in \bar{\eta}) \\
(\text{try-normal}) : & \quad \text{try } N; \text{abort } n_i(x) = M_i \rightarrow N \quad (n_i \notin \bar{N})
\end{align*}
\]

for cbn, and the inference rules

\[
\begin{align*}
(\text{panic}) & : \quad \Gamma \vdash M : A \mid n: A \rightarrow \bot, \Delta \\
(\rightarrow E_h) & : \quad \Gamma \vdash M : \bot \mid A \quad \Gamma \vdash N : A \mid \Delta \\
(\text{try}_h) & : \quad \Gamma \vdash M : \bot \mid n_i:A \rightarrow \bot, \Delta \quad \Gamma, x:A_i \vdash N_i : \bot \mid \Delta \quad (\forall i \in \eta)
\end{align*}
\]

and extending the interpretation \( \llbracket \cdot \rrbracket_h \) with the cases:

\[
\begin{align*}
\llbracket \text{panic } n(M) \rrbracket_h & \triangleq \mu_{\_} \llbracket \text{top} \rrbracket c_n \llbracket M \rrbracket_h \\
\llbracket \text{try } M; \text{Abort\_Block}; \text{abort } n(x) \rrbracket_h & \triangleq (\mu.n.\llbracket \text{try } M; \text{Abort\_Block}_h \rrbracket) \{\lambda x. \llbracket L_{\_}f \rrbracket / c_n\}
\end{align*}
\]

This would behave well on the level of \( \lambda^\eta \) (see also the next section), but not when we aim to show that

\[
\text{if } P \rightarrow^h Q, \text{ then } \llbracket P \rrbracket_h \rightarrow_{\beta^*_h} \llbracket Q \rrbracket_h,
\]

for either cbn or cbv-reduction. Although that property follows straightforwardly from the proof of Thm. 3.4, and for the additional case panic, the reduction rule try-panic throws a spanner in the works. Then the interpretation of

\[
\text{try panic } n(N); \text{ abort } n(x) = M
\]

does not reduce to that of \( M\{N/x\} \):

\[
\begin{align*}
\llbracket \text{try panic } n(N); \text{ abort } n(x) = M \rrbracket_h & \triangleq (\mu.n.\llbracket \text{panic } n(N) \rrbracket_h) \{\lambda z. \llbracket M \rrbracket / c_n\} \quad \triangleq \\
(\mu.n.\llbracket \text{panic } n(N) \rrbracket_h)_h \{\lambda z. \llbracket M \rrbracket / c_n\} & \triangleq \mu_{\_} \llbracket \text{top} \rrbracket \llbracket M \rrbracket_h \rightarrow_{\beta^*_h} (E) \\
\mu_{\_} \llbracket \text{top} \rrbracket (\lambda x. \llbracket M \rrbracket_h) \rightarrow_{\beta^*_h} \mu_{\_} \llbracket \text{top} \rrbracket \llbracket M \rrbracket_h \{\lambda N \rrbracket / x\} & = (3.3) \quad \mu_{\_} \llbracket \text{top} \rrbracket \llbracket M \rrbracket_h \{\lambda N \rrbracket / x\} \rightarrow_{\beta^*_h}
\end{align*}
\]

So here we have \( \llbracket P \rrbracket_h \rightarrow_{\beta^*_h} \mu_{\_} \llbracket \text{top} \rrbracket \llbracket Q \rrbracket_h \), not \( \llbracket P \rrbracket_h \rightarrow_{\beta^*_h} \mu_{\_} \llbracket \text{top} \rrbracket \llbracket Q \rrbracket_h \), as desired, and the terms \( \mu_{\_} \llbracket \text{top} \rrbracket \llbracket Q \rrbracket_h \) and \( \llbracket Q \rrbracket_h \) are also computationally incompatible.

In a certain sense, the encoding expects \( \llbracket M \rrbracket_h \{N/x\} \) to be ‘thrown again’, which suggests the reduction rule

\[
(\text{try-panic}) : \quad \text{try panic } n_i(N); \overline{\text{abort } n_i(x) = M_i} \rightarrow \text{panic } n_i(M_i\{N/x\}) \quad (n_i \in \bar{\eta})
\]

where handlers for panics should be redefined consistently, violating Barendregt’s convention. Alternatively, we could invoke a handler for all aborts, as in

\[
(\text{try-panic}) : \quad \text{try panic } n_i(N); \overline{\text{abort } n_i(x) = M_i} \rightarrow \text{panic-top}(M_i\{N/x\}) \quad (n_i \in \bar{\eta})
\]

which gets dealt with at the ‘outermost level’.

Otherwise, we can assume that there is no handler named \( n_i \), and that the panic escapes
the try-block without being processed. But that would constitute the solution we presented above, by just using the keyword `halt`.

So, in order to define a notion of aborting exceptions for our language $\lambda^{\text{try}}$ that is strongly related to classical logic, we cannot opt to ‘handle’ these events, or explicitly use the type $\bot$ to type them, but are forced to add simply a constant `halt` to the language that consumes all applicative contexts.

6 Handling failing computation

In this section, we will generalise the approach of the previous section, and add the construct `panic` that is dealt with by handlers. As explained in Rem. 5.10 and 5.11, this is not straightforward, and we will have to forgo on establishing a direct relation with $\lambda\mu$ or $\lambda\mu$-top.

Our approach will be to construct a system that adds a type constant `fail` to the type language, and is set up in such a way that, essentially, only calls to `panic` can be typed with `fail`. Our aim is to define a calculus that is close to ‘normal’ programming: programs can raise exceptions and panic from within the same `try`-statement. As we argued above, for reasons of subject reduction, we have to demand that the return type of the handlers is equal to that of the main term, which would mean that we cannot return `fail` for a failing program without having to demand that all handlers return `fail`. That clearly goes against intuition, since 1) we cannot expect the type checker to decide if a program will fail; 2) failure can depend on input, which need not be part of the code; 3) the programmer should have the liberty to cater for the event of a successful computation and a total failure in a different way.

We therefore introduce a new feature: handlers for exceptions, called `catch`, all return the type of the main term, whereas handlers for panic call, called `abort`, all return `fail`.

The system we will present thereby is unconventional in that the standard subject reduction result does not hold as such. Our aim is to show that, as usual, types are preserved under normal reduction (is sound), but that the type `fail` is only used when a panic is raised; as a result of this duplicity we will not be able to show the normal subject reduction result. Since in standard notions of type assignment for the $\lambda$-calculi this property holds, for both the reduction strategies cbn and cbv we need to explicitly insert the duplicity of keeping the type under reduction or running to a term with type `fail`. Note that this will not be decidable, since modelling the concept that predicts how a program will run, i.e. if a panic will be triggered, through assignable types, is impossible.

To introduce the duplicity, we enrich the language with a conditional construct; then depending on the result of running the boolean expression, either the then or else part will be deployed. Assuming the boolean expression tests if the execution is running normally (like a test for division by zero), we can call `panic` in one part, and continue normal execution in the other. Our aim is that in the first case a term is returned of type `fail`, whereas the second one will return a normal type, `int` in our case. We will type the whole term then with `int`, which then is the type for the result produced by normal reduction.

Remark 6.1 Since the conditional is encodable in the pure $\lambda$-calculus through $\lambda\text{btf} \cdot \text{btf}$, with the boolean constant `true` through $\lambda a. a$, and `false` through $\lambda a. b$, for reasons of expressivity there is no need to add the conditional construct explicitly. The type `bool` then necessarily is a type suitable for both $\lambda a. a$ and $\lambda a. b$, so has to correspond to $A \rightarrow A \rightarrow A$, for any $A$ (or $\forall \varphi. \varphi \rightarrow \varphi \rightarrow \varphi$). This is found also in the standard way of typeing the conditional construct, which demands that the then and else part have the same type as the expression itself, as normally expressed through the rule:
\[
\begin{align*}
(Ax) & : \Gamma, x : A \vdash x : A \mid \Delta \\
(c) & : \Gamma \vdash c : \sigma(c) \mid \Delta \\
(\neg I) & : \Gamma, x : A \vdash M : A \mid \Delta \\
(\lambda x. M) & : \Gamma \vdash \lambda x. M : A \rightarrow B \mid \Delta
\end{align*}
\]

\[
(\neg E) : \quad \Gamma \vdash M : A \rightarrow B \mid \Delta \quad \Gamma \vdash N : A \mid \Delta
\]

\[
\Gamma \vdash MN : B \mid \Delta
\]

\[
(\neg) : \quad \Gamma \vdash M : \text{fail} \mid \Delta \quad \Gamma \vdash N : A \mid \Delta
\]

\[
\Gamma \vdash MN : \text{fail} \mid \Delta
\]

\[
\begin{align*}
\text{(throw)} : & \quad \Gamma \vdash_{\text{try}} M : A \mid n : A \rightarrow B, \Delta \\
\text{(panic)} : & \quad \Gamma \vdash_{\text{try}} \text{panic} n(M) : A \mid n : A \rightarrow \text{fail}, \Delta
\end{align*}
\]

\[
\begin{align*}
\text{(try)} : & \quad \Gamma \vdash_{\text{try}} \text{try} M : C \mid n : A \rightarrow B, \Delta \\
\text{(tryfail)} : & \quad \Gamma \vdash_{\text{try}} \text{try} M : \text{fail} \mid \bar{n}_i : A_i \rightarrow B_i, \Delta \\
& \quad \Gamma, x : A_i \vdash_{\text{try}} N_i : B_i \mid \Delta \quad (\forall i \in \bar{n}) \quad (\forall i \mid B_i = C \vee B_i = \text{fail})
\end{align*}
\]

\[
\begin{align*}
\text{(cond)} : & \quad \Gamma \vdash_{\text{try}} M : \text{bool} \mid \Delta \\
& \quad \Gamma \vdash_{\text{try}} P : A \mid \Delta \\
& \quad \Gamma \vdash_{\text{try}} Q : B \mid \Delta \\
\text{(condfail)} : & \quad \Gamma \vdash_{\text{try}} \text{if} M \text{ then } P \text{ else } Q : \text{fail} \mid \Delta
\end{align*}
\]

Figure 8: The system $\vdash_{\text{fail}}$.

But this standard approach would not allow us the characterisation of failing computations through assignable types we aim for. So, rather, we deviate from that standard approach and, essentially, let bool correspond to

\[
A \rightarrow A \rightarrow A \vee A \rightarrow \text{fail} \rightarrow A \vee \text{fail} \rightarrow A \rightarrow A.
\]

If we would allow that to be a type for both $\lambda ab.a$ and $\lambda ab.b$, we would be forced to set $A = \text{fail}$ and we would be forced to allow for fail to be treated as any type, rather than just the type for panic.

So to be able to express the characteristic we aim for, we are forced to add the conditional construct explicitly, which allows us to use non-standard type assignment rule(s) for the conditional that allow the two branches to have different types, provided that one of them is typed with fail. This is achieved by adding the rules:

\[
\Gamma \vdash M : \text{fail} \mid \Delta \\
\Gamma \vdash P : A \mid \Delta \\
\Gamma \vdash Q : A \mid \Delta
\]

\[
\Gamma \vdash \text{if} M \text{ then } P \text{ else } Q : \text{fail} \mid \Delta
\]

(if running the boolean expression fails, the whole computation will fail)

\[
\Gamma \vdash M : \text{bool} \mid \Delta \\
\Gamma \vdash P : A \mid \Delta \\
\Gamma \vdash Q : \text{fail} \mid \Delta
\]

\[
\Gamma \vdash \text{if} M \text{ then } P \text{ else } Q : A \mid \Delta
\]

(if $M$ runs to false, the computation will fail, otherwise it runs to a term of type $A$)

\[
\Gamma \vdash M : \text{bool} \mid \Delta \\
\Gamma \vdash P : \text{fail} \mid \Delta \\
\Gamma \vdash Q : A \mid \Delta
\]

\[
\Gamma \vdash \text{if} M \text{ then } P \text{ else } Q : A \mid \Delta
\]

(if $M$ runs to true, the computation will fail, otherwise it runs to a term of type $A$).

We define $\lambda_{\text{fail}}^{A}$ by extending the calculus $A^{B}$ from Def. 2.1, by adding panic and abort, a conditional construct and term constants (ranged over by $c$, and including $\text{err}$, $\text{true}$, $\text{false}$, numbers, (prefix) addition and multiplication, boolean operators, etc, etc.) to the set of pre-terms.
Let $\Delta' = m; B \rightarrow \text{fail}, n: C \rightarrow A, \Delta$.

\[ \frac{}{\Gamma, x: \text{fail}, y: A \vdash x: \text{fail} \mid \Delta' \quad (\text{Ax})} \]
\[ \frac{}{\Gamma, x: \text{fail} \vdash \lambda y: x: A \rightarrow \text{fail} \mid \Delta' \quad (\rightarrow I)} \]
\[ \frac{}{\Gamma \vdash \lambda x.y: x: A \rightarrow \text{fail} \mid \Delta' \quad (\rightarrow I)} \]
\[ \frac{}{\Gamma \vdash \text{panic } m(N): A \rightarrow \text{fail} \mid \Delta' \quad (\rightarrow E)} \]
\[ \frac{}{\Gamma \vdash \lambda x.y: \text{panic } m(N): A \rightarrow \text{fail} \mid \Delta' \quad (\rightarrow E)} \]
\[ \frac{}{\Gamma \vdash \lambda x.y: (\text{panic } m(N))(\text{throw } n(L)): A \rightarrow \text{fail} \mid \Delta'} \]

Figure 9: A derivation for $(\lambda x.y: (\text{panic } m(N))(\text{throw } n(L)))$

**Definition 6.2 (TRV)**  
1) The set of pre-terms of $\lambda_{\text{TRV}}$ is defined through the grammar:

- handlers := e | handlers; catch n(x) := M | handlers; abort n(x) := M
- $M, N := V | MN | \text{try } M; \text{handlers } | \text{throw } n(M) | \text{panic } n(M) | \text{if } M \text{ then } P \text{ else } Q
- $V := x | c | \lambda x. M$

The order in which the handlers are listed is not important; we will reorganise them whenever convenient.

2) Call-by-name reduction is defined as in Def. 2.2 by the rules

- $(\beta) : (\lambda x. M) N \rightarrow M\{N/x\}$
- $(\text{throw}) : (\text{throw } n(N)) M \rightarrow \text{throw } n(N)$
- $(\text{try-throw}) : \text{try } \text{throw } n_1(N); \text{handle } n_1(x) = M_i; \text{catch } n_1(x) = M_i \rightarrow M_i\{N/x\}$
- $(\text{try-normal}) : \text{try } N_i; \text{handle } n_i(x) = M_i \rightarrow N \{n_i \not\in N\}$
- $(\text{panic}) : (\text{panic } n(N)) M \rightarrow \text{panic } n(N)$
- $(\text{try-panic}) : \text{try } \text{panic } n_2(N); \text{handle } n_2(x) = M_i; \text{abort } n_2(x) = M_i \rightarrow M_i\{N/x\}$
- $(\text{cond-true}) : \text{if } \text{true then } P \text{ else } Q \rightarrow P$
- $(\text{cond-false}) : \text{if } \text{false then } P \text{ else } Q \rightarrow Q$
- $(\text{cond-throw}) : \text{if } \text{throw } n(N) \text{ then } P \text{ else } Q \rightarrow \text{throw } n(N)$
- $(\text{cond-panic}) : \text{if } \text{panic } n(N) \text{ then } P \text{ else } Q \rightarrow \text{panic } n(N)$

**CBN applicative contexts** are defined as:

\[ C_N^\Delta ::= [] | C_N^\Delta \cdot \text{try } C_N^\Delta; \text{Catch } \text{Block } | \text{if } C_N^\Delta \text{ then } P \text{ else } Q \]

3) Call-by-value reduction is defined as in the previous part by also changing/adding the rule

- $(\beta_v) : (\lambda x. M) V \rightarrow M\{V/x\}$
- $(\text{panic}_v) : V(\text{panic } n(N)) \rightarrow \text{panic } n(N)$

**CBV applicative contexts** are defined as:

\[ C_V^\Delta ::= [] | C_V^\Delta \cdot V \cdot C_V^\Delta; \text{try } C_V^\Delta; \text{Catch } \text{Block } | \text{if } C_V^\Delta \text{ then } P \text{ else } Q \]

We will now define a notion of type assignment that characterises *unrecoverable failure*. The idea is that the exception handlers that deal with panic return terms that are typed fail and have to return a panic call, so panic gets propagated through the system and fail becomes the type of the whole program.\(^{12}\) In order to deal with this properly, we need to extend our notion of type assignment.

**Definition 6.3 (Type assignment with throw and panic)**  
1) We extend the set of types by adding the type constant $\text{fail}$ and normal type constants, ranging over by $c$:

\[ c ::= \text{bool } | \text{int } | \ldots ; A, B ::= \varphi | \text{fail } | c | A \rightarrow B. \]

\(^{12}\) We could even add the term $\text{halt}$ with type $\bot$ for this purpose, similar to the previous section.
iii) Type assignment (with failure) \( \vdash_{\text{fail}} \) for terms in \( \Lambda^\text{TRY} \) is defined through the inference system presented in Fig. 8, where all types are not equal to fail unless explicitly mentioned, and \( \sigma \) assigns the appropriate ground type to each constant.

The notion \( \vdash_{\text{fail}} \) is defined using the rules of Fig. 8, extended with the rule

\[
\frac{\Gamma \vdash M : A \mid \Delta \quad \Gamma \vdash N : \text{fail} \mid \Delta}{\Gamma \vdash MN : \text{fail} \mid \Delta}
\]

Note that we no longer require that the handlers return the same type as the main term in a try-expression, but allow them to either return that type, or fail; moreover, each panic \( n(M) \) is typed with fail (fails), and rules \((\rightarrow E_v)\) and \((\rightarrow E_f)\) propagate the type fail in an applicative contexts. Also, an abstraction can never fail; the only rule that is allowed for abstractions is \((\rightarrow I)\), so the type for an abstraction is of the shape \( A \rightarrow B \), and both \( A \neq \text{fail} \) and \( B \neq \text{fail} \).

**Remark 6.4** Although the derivation rule \((\rightarrow E_{\text{fail}})\) is clearly inspired by \( \text{fail} \leq A \rightarrow \text{fail} \), for all \( A \), or the logic rule

\[
\frac{\Gamma \vdash \bot}{\Gamma \vdash A}
\]

(ex falso quodlibet sequitur), we do not inhabit this rule with a term construct, as is done for example, in \( \Lambda \mu \) [12] and [1], and implicitly done for the systems above and rules \((\text{throw})\) and \((\text{halt})\). Rather, we limit its use to just \((\rightarrow E_{\text{fail}})\). Our treatment thereby better corresponds to the characteristic of aborting computations. If we would allow, as above, the rule

\[
\frac{\Gamma \vdash_{\text{fail}} M : A \mid n : A \rightarrow B, \Delta}{\Gamma \vdash_{\text{fail}} \text{panic} n(M) : C \mid n : A \rightarrow B, \Delta}
\]

by implicitly using the logical rule above, then it would be possible to assign an abortive computation any type, rather than just the one indication that computation has failed, and we could no longer be able to distinguish between exceptions and panic.

**Example 6.5** We have (essentially) restricted the use of fail to panic only. For example, the term

\[
\text{try} \ (\lambda xy.x) \ (\text{panic} m(N)) \ (\text{throw} n(L));
\]

\[
\text{catch} \ n(x) = P; \text{abort} \ m(x) = Q
\]

is not typeable in \( \vdash_{\text{fail}} \), since it would demand that the type for \( \lambda xy.x \) contains fail. It would be typeable if we relax the restriction, allowing fail as a normal type. Take the sub-term

\[
M = (\lambda xy.x) \ (\text{panic} m(N)) \ (\text{throw} n(L))
\]

which will panic. We can allow the throw and panic to return different types inside \( M \), as in Fig. 9. When we place this term inside the context of dealing with the catch on \( n \) and abort on \( m \), the special character of the rule \((\text{try})\) in \( \vdash_{\text{fail}} \) becomes evident; it allows the return type of exception handlers to differ from the type of the main term in case the latter is fail.
Remark that we do not consider rules like Example 6.7 abort is typeable under the restriction; see Fig. 10.

Lemma 6.8 cannot be sure that A

Proof: 

Using the conditional structure, the similar term

\[
\text{try if true then panic } m(N) \text{ else throw } n(L);
\]

is typeable under the restriction; see Fig. 10.

Our notion of type assignment is predictive in that we can show that terms typed with fail will raise a panic.

Lemma 6.6 i) If \( \Gamma \vdash_{\text{fail}} M : \text{fail} \mid \Delta \), then \( M \rightarrow^* \text{panic } n(N) \).

ii) If \( \Gamma \vdash_{\text{fail}} M : \text{fail} \mid \Delta \), then \( M \rightarrow^* \text{panic } n(N) \).

Proof: Straightforward by induction on the structure of derivations.

Notice that something similar also holds for type assignment in the \( \lambda \)-calculus (extended with type constants): if \( \Gamma \vdash M : \text{int} \), then \( M \) will run to an integer. Note that, because of the presence of throw, this property does not hold for \( \vdash_{\text{fail}} \).

So failing (having type fail) is now exclusively the domain of panic, as we intended from the outset; in particular, the type assignment system forces the type of the body of an abort to have type \( \perp \) as well, running the body of each abort has to result in a panic as well.

Example 6.7 Remark that we do not consider rules like

| \( \Gamma, x : A \vdash M : \text{fail} \mid \Delta \) | \( \Gamma, x : A \vdash M : \text{fail} \mid \Delta \) | \( \Gamma \vdash M : \text{fail} \mid \Delta \) | \( \Gamma \vdash \lambda x. M : \text{fail} \mid \Delta \) |
| \( \Gamma \vdash \lambda x. M : \lambda \rightarrow \text{fail} \mid \Delta \) | \( \Gamma \vdash \lambda x. M : \text{fail} \mid \Delta \) |

Moreover, assume we would add the first of the above two rules and assume we can derive:

| \( \Gamma, x : A \vdash_{\text{fail}} M : \text{fail} \mid \Delta \) | \( \Gamma \vdash_{\text{fail}} \lambda x. M : \text{fail} \mid \Delta \) | \( \Gamma \vdash N : \Delta \) | \( \Gamma \vdash_{\text{fail}} (\lambda x. M) N : \text{fail} \mid \Delta \) |
| \( \Gamma \vdash \lambda x. M : \lambda \rightarrow \text{fail} \mid \Delta \) |

Remark that now we cannot apply Lem. 5.4 to conclude \( \Gamma \vdash_{\text{fail}} M \{N / x\} : \text{fail} \mid \Delta \), since we cannot be sure that \( A = B \); therefore we would not be able to show soundness.

We can show that weakening and thinning are both admissible.

Lemma 6.8 (WEAKENING AND THINNING FOR \( \vdash_{\text{fail}} \)) The following rules are admissible:

\[
\begin{align*}
(Wk) : & \quad \frac{\Gamma \vdash_{\text{fail}} M : A \mid \Delta}{\Gamma' \vdash_{\text{fail}} M : A \mid \Delta'} \\
& \quad (\Gamma \subseteq \Gamma', \Delta \subseteq \Delta') \\
(Th) : & \quad \frac{\Gamma \vdash_{\text{fail}} M : A \mid \Delta}{\Gamma' \vdash_{\text{fail}} \lambda x M : A \mid \Delta'} \\
& \quad \{ x : B \in \Gamma \mid x \in \text{fn}(M) \}, \Delta' = \{ n : B \in \Delta \mid n \in \text{fn}(M) \} \\
\end{align*}
\]

Proof: Standard. \( \square \)

We can also show that type assignment is closed under term substitution.

Lemma 6.9 (SUBSTITUTION LEMMA FOR \( \vdash_{\text{fail}} \)) If \( \Gamma, x : C \vdash_{\text{fail}} M : A \mid \Delta \) and \( \Gamma \vdash_{\text{fail}} N : C \mid \Delta \), then \( \Gamma \vdash_{\text{fail}} M \{N / x\} : A \mid \Delta \).

Proof: By induction on the structure of terms.

\( (M \equiv c) : \text{ Then } A = \sigma(c); \text{ then also } \Gamma \vdash_{\text{fail}} c : \sigma(c) \mid \Delta, \text{ and } c \{N / x\} = c. \)
(M ≡ x): If Γ, x:C ⊢ n : A | Δ and Γ ⊢ n : N : C | Δ, then x:A ∈ Γ, x:C, so A = C. Also, x{N/x} = N, so Γ ⊢ n : x{N/x} : A | Δ.

(M ≡ y ≠ x): If Γ, x:C ⊢ n : A | Δ, then y:A ∈ Γ, so also Γ ⊢ y : A | Δ.

(M ≡ λy.M’): Then A = A’ → B’ and Γ, x:C, y:A’ ⊢ M’ : B’ | Δ. By induction, Γ, y:A’ ⊢ M’ : N : B’ | Δ. But then Γ ⊢ λy.M’ : N : A | Δ by (→I), so Γ ⊢ λy.M’(N/x) : A | Δ. Notice that λy.(M’(N/x)) = (λy.M’)(N/x).

(M ≡ PQ): Then either:
- there exists B such that Γ, x:C ⊢ n : B → A | Δ and Γ, x:C ⊢ Q : B | Δ. By induction both Γ ⊢ n : P{N/x} : B → A | Δ and Γ ⊢ Q{N/x} : B | Δ; then, by (¬E), we have Γ ⊢ n : P{N/x} Q{N/x} : A | Δ.
- A = fail and there exists B such that Γ, x:C ⊢ n : fail | Δ and Γ, x:C ⊢ Q : B | Δ. By induction both Γ ⊢ n : P{N/x} : fail | Δ and Γ ⊢ Q{N/x} : B | Δ; then, by (fail), we have Γ ⊢ n : P{N/x} Q{N/x} : fail | Δ.

Notice that P{N/x} Q{N/x} = PQ{N/x}.

(M ≡ if P then Q else R): Then either:
- Γ, x:C ⊢ n : P : bool | Δ, Γ, x:C ⊢ Q : A | Δ, and Γ, x:C ⊢ R : A | Δ, and by induction Γ ⊢ n : P{N/x} : bool | Δ, Γ ⊢ Q{N/x} : A | Δ, and Γ ⊢ R{N/x} : A | Δ. Then also Γ ⊢ n : if P{N/x} then Q{N/x} else R{N/x} : A | Δ.
- A = fail, Γ, x:C ⊢ n : fail | Δ, Γ, x:C ⊢ Q : B | Δ, and Γ, x:C ⊢ R : D | Δ, and by induction Γ ⊢ n : P{N/x} : fail | Δ, Γ ⊢ Q{N/x} : B | Δ, and Γ ⊢ R{N/x} : D | Δ. Then also Γ ⊢ n : if P{N/x} then Q{N/x} else R{N/x} : fail | Δ.

Notice that if P{N/x} then Q{N/x} else R{N/x} = (if P then Q else R){N/x}.

(M ≡ try P; catch n(y) = Q): Then there exists A_i, B_i such that Γ, x:C ⊢ n : P : A | Δ and Γ, x:C, y:A_i ⊢ Q_i : B_i | Δ, for all i ∈ n. By induction, Γ ⊢ n : P{N/x} : A | Δ and Γ, y:A_i ⊢ Q_i{N/x} : B_i | Δ (∀i ∈ n). We get Γ ⊢ n : try P{N/x}; catch n(y) = Q_i{N/x} : A | Δ by rule (try), and try P{N/x}; catch n(y) = Q_i{N/x} = (try P; catch n(y) = Q_i){N/x}.

(M ≡ throw n(P)): Then A ≠ fail, and there exists B, D such that n:B → D ∈ Δ, and Γ, x:C ⊢ n : P : B | Δ. By induction Γ ⊢ n : P{N/x} : B | Δ. Since n:B → D ∈ Δ, by rule (throw) we get Γ ⊢ n : throw n : P{N/x} : A | Δ. Notice that throw n{P{N/x}} = (throw n)(P){N/x}.

(M ≡ panic n(P)): Then A = fail and there exists B such that n:B → fail ∈ Δ, and Γ, x:C ⊢ n : P : B | Δ. By induction Γ ⊢ n : P{N/x} : B | Δ. Since n:B → fail ∈ Δ we get Γ ⊢ n : panic n : P{N/x} : fail | Δ by rule (panic). Notice that panic n{P{N/x}} = (panic n(P)){N/x}.

The main result we show for this system is the following soundness result. It states that running a program will either run normally, preserving the assigned type, or will run to a term that has type fail, so throws a panic.

Theorem 6.10 (Soundness for ⊢ for with respect to →*). If Γ ⊢ n : C | Δ and P →* Q, then either Γ ⊢ n : Q | Δ, or Γ ⊢ n : fail | Δ.

Proof: By induction on the definition →*; we focus on the single step reduction, and only show the interesting cases.

(β): Then P = (λx.M) N → M{N/x} = Q, and the derivation for P is constructed as follows:

\[ \frac{\Gamma, x:B ⊢ M : C | \Delta \quad (\rightarrow I)}{\Gamma ⊢ λx.M : B → C | \Delta} \quad \frac{\Gamma ⊢ n : B | \Delta \quad (\rightarrow E)}{\Gamma ⊢ (λx.M) N : C | \Delta} \]

(notice that it is impossible for (→E) to be applied last for (λx.M) N as fail cannot be
a type for $\lambda x. M$). In particular, then $\Gamma, x : B \vdash \text{tail} M : C \mid \Delta$ and $\Gamma \vdash \text{tail} N : B \mid \Delta$, and the result follows from Lem. 6.9.

(throw): Then $P = (\text{throw } n \, (N)) \, M \to \text{throw } n \, (N) = Q$, and the return type for the exception handler $n$ is not fail: then the derivation for $P$ looks like:

\[
\begin{array}{c}
\Gamma \vdash n \, (N) : D \to C \mid n \, : A \to B, \Delta \\
\Gamma \vdash \text{throw } n \, (N) : D \to C \mid n \, : A \to B, \Delta \\
\Gamma \vdash (\text{throw } n \, (N)) \, M : C \mid n \, : A \to B, \Delta
\end{array}
\]

Applying (throw) to $D$ we derive $\Gamma \vdash \text{throw } n \, (N) : C \mid n \, : A \to B, \Delta$.

(panic): Then $P = (\text{panic } n \, (N)) \, M \to \text{panic } n \, (N) = Q$, and the return type for the exception handler $n$ is fail; then the derivation for $P$ looks like:

\[
\begin{array}{c}
\Gamma \vdash n \, (N) : D \to C \mid n \, : A \to \text{fail}, \Delta \\
\Gamma \vdash \text{panic } n \, (N) : D \to C \mid n \, : A \to \text{fail}, \Delta \\
\Gamma \vdash (\text{panic } n \, (N)) \, M : D \mid n \, : A \to \text{fail}, \Delta
\end{array}
\]

Notice that we have a sub-derivation for $\Gamma \vdash \text{panic } n \, (N) : D \to C \mid n \, : A \to \text{fail}, \Delta$.

(try-throw): Then $P = \text{try } \text{throw } n \, (M) ; \, \text{catch } n \, (x) = N_1 \to N_1 \{M / x\} = Q$ and the derivation for $P$ is shaped as follows:

\[
\begin{array}{c}
\Gamma \vdash n \, (M) : A \mid n \, : A \to B, \Delta \\
\Gamma \vdash \text{throw } n \, (M) : A \mid n \, : A \to B, \Delta \\
\Gamma \vdash (\text{throw } n \, (M)) \, M : B \mid n \, : A \to B, \Delta
\end{array}
\]

where $C \neq \text{fail}$, and $B_i = C$ or $B_i = \text{fail}$, for each $i$. In particular, we have both $\Gamma \vdash \text{tail} M : A \mid n \, : A \to B, \Delta$ and $\Gamma, x : A_1 \vdash \text{tail} N_1 : C \mid \Delta$, so $B_i = C$. By Lem. 6.8, we can remove $n \, : A_1 \to B_i$ from the co-context for the first to obtain $\Gamma \vdash \text{tail} N_1 : A \mid \Delta$. Then, by Lem. 6.9, we obtain $\Gamma \vdash \text{panic } n \, (M) : A \mid \Delta$.

(try-panic): Then $P = \text{try } \text{panic } n \, (M) ; \, \text{abort } n \, (x) = N_1 \to N_1 \{M / x\} = Q$ and the derivation for $P$ is shaped as follows:

\[
\begin{array}{c}
\Gamma \vdash n \, (M) : A \mid n \, : A \to B, \Delta \\
\Gamma \vdash \text{panic } n \, (M) : A \mid n \, : A \to B, \Delta \\
\Gamma \vdash \text{panic } n \, (M) ; \, \text{abort } n \, (x) = n \, : \text{fail} \mid \Delta
\end{array}
\]

so $B_i = \text{fail}$. In particular, we have both $\Gamma \vdash \text{tail} M : A \mid n \, : A \to B, \Delta$ and $\Gamma, x : A_1 \vdash \text{tail} N_1 : \text{fail} \mid \Delta$. By Lem. 6.8, we can remove $n \, : A_1 \to B_i$ from the co-context for the first to obtain $\Gamma \vdash \text{panic } n \, (M) : A \mid \Delta$. Then, by Lem. 6.9, we obtain $\Gamma \vdash N_1 \{M / x\} : \text{fail} \mid \Delta$.

(try-normal): Then $P = \text{try } Q ; \, \text{handle } n \, (x) = M_i \to Q$ with $n \notin Q$. Then the derivation for $P$ is constructed as follows:

\[
\begin{array}{c}
\Gamma \vdash Q : C \mid n \, : A \to B, \Delta \\
\Gamma \vdash \text{try } Q ; \, \text{handle } n \, (x) = N \, : C \mid \Delta
\end{array}
\]

(notice that, by Lem. 6.6, $C \neq \text{fail}$). In particular, we have $\Gamma \vdash Q : C \mid n \, : A \to B, \Delta$; since $n \notin Q$, by Lem. 6.8 we can remove $n \, : A_1 \to B_i$ from the co-context to obtain $\Gamma \vdash Q : C \mid \Delta$.

(cond-true): Then $P = \text{if } \text{true} \text{ then } M \text{ else } N \to M = Q$. Since true can only be assigned bool,

\[\text{Remark that we cannot apply } (\to I) \text{ to the latter result.} \]
the derivation is constructed as follows:

\[
\begin{array}{c}
\Gamma \vdash \text{true} : \text{bool} | \Delta \\
\Gamma \vdash Q : A | \Delta \\
\Gamma \vdash N : B | \Delta
\end{array}
\]

(\text{cond})

and either:

\((A = B = C) \lor (A = C \land B = \text{fail})\): Then, in particular, \(\Gamma \vdash \text{fail} Q : C | \Delta\).

\((A = \text{fail} \land B = C)\): Then, in particular, \(\Gamma \vdash \text{fail} Q : \text{fail} | \Delta\).

\((\text{cond-panic})\): Then \(P = \text{if} false\) then \(M\) else \(N\) = \(Q\). Similar to the previous case.

\((\text{cond-throw})\): Then \(P = \text{if throw} n(R)\) then \(M\) else \(N\) = \(\text{throw} n(P) = Q\), and the derivation for \(P\) is constructed as:

\[
\begin{array}{c}
\Gamma \vdash P : E | n : E \rightarrow F, \Delta' \\
\Gamma \vdash \text{throw} n(R) : \text{bool} | n : E \rightarrow F, \Delta' \\
\Gamma \vdash M : B | \Delta \\
\Gamma \vdash N : C | \Delta
\end{array}
\]

(\text{cond})

for certain \(B\), \(C\), and \(D\). Then we can construct the derivation:

\[
\begin{array}{c}
\Gamma \vdash P : E | n : E \rightarrow F, \Delta' \\
\Gamma \vdash \text{throw} n(R) : D | n : E \rightarrow F, \Delta'
\end{array}
\]

(\text{throw})

\((\text{cond-panic})\): Then \(P = \text{if panic} n(R)\) then \(M\) else \(N\) = \(\text{panic} n(R) = Q\), and the derivation for \(P\) is constructed as:

\[
\begin{array}{c}
\Gamma \vdash \text{panic} n(R) : \text{fail} | \Delta \\
\Gamma \vdash M : B | \Delta \\
\Gamma \vdash N : C | \Delta
\end{array}
\]

(\text{cond})

for certain \(B\) and \(C\). Notice that we have a sub-derivation for \(\Gamma \vdash \text{panic} n(R) : \text{fail} | \Delta\).

\[\square\]

For the call-by-value system, we can show:

**Theorem 6.11 (Soundness for \(\vdash_{\text{fail}}\) with respect to \(\rightarrow_{\text{TRV}}\))** If \(\Gamma \vdash_{\text{fail}} P : C | \Delta\) and \(P \rightarrow_{\text{TRV}}^* Q\), then either \(\Gamma \vdash_{\text{fail}} Q : C | \Delta\), or \(\Gamma \vdash_{\text{fail}} Q : \text{fail} | \Delta\).

**Proof**: The proof is much like that for the previous result, with the addition of:

\((\text{throw}_V)\): Then \(\Delta = n : A \rightarrow C, \Delta'\), \(P = V(\text{throw} n(N)) \rightarrow \text{throw} n(N) = Q\), and the derivation for \(P\) is constructed as:

\[
\begin{array}{c}
\Gamma \vdash \text{throw} n(N) : E | n : A \rightarrow C, \Delta' \\
\Gamma \vdash N : A | n : A \rightarrow C, \Delta'
\end{array}
\]

(\text{throw})

\((\rightarrow_E)\)

We can construct the derivation for \(Q\):

\[
\begin{array}{c}
\Gamma \vdash \text{throw} n(N) : E | n : A \rightarrow C, \Delta'
\end{array}
\]

(\text{throw})

\((\text{panic}_V)\): Then \(P = V(\text{panic} n(N)) \rightarrow \text{panic} n(N) = Q\), and the derivation for \(P\) is constructed like:
\[
\begin{array}{c}
\Gamma \vdash V : \Delta \\
\Gamma \vdash \text{panic } n(N) : \text{fail} | \Delta \\
\hline
\Gamma \vdash V(\text{panic } n(N)) : \text{fail} | \Delta
\end{array}
\]

Notice that we have \( \Gamma \vdash \text{fail} \ \text{panic } n(N) : \text{fail} | \Delta \) in a sub-derivation.

\((M \to N \Rightarrow V M \to VN)\): By induction.

Conclusion

We have defined \( \lambda^\text{try} \), a natural extension to the \( \lambda \)-calculus by adding exception handling, and shown that it can be embedded into \( \lambda \mu \), preserving both \( \text{cbn} \) and \( \text{cbv} \) reduction. The normal notion of type assignment for \( \lambda^\text{try} \), here called the basic system, is also preserved by our mapping onto \( \lambda \mu \). Type assignment is not preserved, however, for the notion of type assignment that captures total program failure using exception handling.

We also have presented a notion of handling of exception and panic calls, together with a natural notion of type assignment, that cannot be represented in \( \lambda \mu \) or \( \lambda \mu\text{-top} \).

We thus have shown that, although a strong link between typeable exception handling and double negation elimination is evident, exception handling itself is a feature that is not naturally a part of calculi based on classical logic, since it is possible to define notions of type assignment that are natural for \( \lambda^\text{try} \), but are not founded on classical logic.

By letting go of the link between programming and logic, we have shown that it is possible to define handling of exception and panic calls for formal calculi in a computationally meaningful way.

Acknowledgements

I am greatly indebted to the students who, over the years, have worked on this and other problems related to classical logic and functional programming with me. A special mention is for Mihai-Radu-Niculce Popescu, Wil Fisher, Adela Baciu, James Griffiths, and Isaac van Bakel.

References


