

Program Analysis (70020)

Control Flow Analysis

Herbert Wiklicky

Department of Computing
Imperial College London

herbert@doc.ic.ac.uk
h.wiklicky@imperial.ac.uk

Autumn 2022

1/41

Control Flow Analysis

- ▶ Flow information is essential for the specification of Data Flow Analyses. In the case of the Monotone Framework, flow information is represented by the flow function **F**.
- ▶ WHILE language: flow information can be extracted directly from the program text. Procedure calls are performed by explicitly mentioning the name of a procedure.
- ▶ Not so trivial for more general languages e.g imperative languages with procedures as parameters, functional languages or object-oriented languages.
- ▶ A special analysis is required: **Control Flow Analysis**

2/41

The λ -Calculus

$N \in$ **Term** λ -terms
 $x \in$ **Var** variables

$N ::= x \mid (\lambda x.N) \mid (N_1 N_2)$

Substitution: $(\lambda x.M)N \longrightarrow_{\beta} M[x/N]$

$(\lambda x.x)z \longrightarrow_{\beta} z$
 $(\lambda x.x)(\lambda y.y) \longrightarrow_{\beta} (\lambda y.y)$

3/41

Syntax of Fun

$e \in$ **Exp** expressions (or labelled terms)
 $t \in$ **Term** terms (or unlabelled expressions)

$e ::= t^{\ell}$

$t ::= c \mid x \mid \text{fn } x \Rightarrow e_0 \mid e_1 e_2$
| if e_0 then e_1 else e_2 | $e_1 \text{ op } e_2$
| let $x = e_1$ in e_2

$((\text{fn } x \Rightarrow x^1)^2 (\text{fn } y \Rightarrow y^3)^4)^5$

4/41

An Example

```
let  f = fn x => x 1;  
     g = fn y => y + 2;  
     h = fn z => z + 3  
in   (f g) + (f h)
```

$(f\ g) + (f\ h) \longrightarrow ((\text{fn } x \Rightarrow x\ 1)\ g) + ((\text{fn } x \Rightarrow x\ 1)\ h)$
 $\longrightarrow (g\ 1) + (h\ 1)$
 $\longrightarrow ((\text{fn } y \Rightarrow y + 2)\ 1) + (\text{fn } z \Rightarrow z + 3)\ 1)$
 $\longrightarrow (1 + 2) + (1 + 3)$
 $\longrightarrow 7$

5/41

Evaluating Fun

$\rho \in \mathbf{Env}$	=	$\mathbf{Var} \mapsto \mathbf{Value}$	Environments
$v \in \mathbf{Value}$	=	$\mathbf{Constant} \cup \mathbf{Closure}$	Values
$\mathbf{Closure}$::=	$[(\text{fn } x \Rightarrow e_0), \rho]$	Closures

$\text{eval}(\rho, e) = v$

iff “ e evaluates to v in ρ ”

- ▶ $\text{eval}(\rho, e) = v$ can also be read as an specification for building an interpreter for the Fun language.
- ▶ We will use this specification just as a aid to help us understand the Control Flow Analysis.

6/41

Environment Rules I

$$\text{eval}(\rho, c^\ell) = c$$

$$\text{eval}(\rho, x^\ell) = \rho(x)$$

$$\text{eval}(\rho, (t_1^{\ell_1} \text{ op } t_2^{\ell_2})^\ell) = \text{eval}(\rho, t_1^{\ell_1}) \text{ op } \text{eval}(\rho, t_2^{\ell_2})$$

$$\text{eval}(\rho, (\text{if } t_0^{\ell_0} \text{ then } t_1^{\ell_1} \text{ else } t_2^{\ell_2})^\ell) = v$$

$$\text{where } v = \begin{cases} \text{eval}(\rho, t_1^{\ell_1}) & \text{for } \text{eval}(\rho, t_0^{\ell_0}) = \text{true} \\ \text{eval}(\rho, t_2^{\ell_2}) & \text{for } \text{eval}(\rho, t_0^{\ell_0}) = \text{false} \end{cases}$$

7/41

Environment Rules II

$$\text{eval}(\rho, (\text{fn } x \Rightarrow e_0)^\ell) = [(\text{fn } x \Rightarrow e_0), \rho] \quad \text{closure creation}$$

$$\text{eval}(\rho, (\text{let } x = t_1^{\ell_1} \text{ in } t_2^{\ell_2})^\ell) = \text{eval}(\rho[x \mapsto v_1], t_2^{\ell_2})$$

$$\text{where } v_1 = \text{eval}(\rho, t_1^{\ell_1})$$

$$\text{eval}(\rho, (t_1^{\ell_1} t_2^{\ell_2})^\ell) = \text{eval}(\rho_0[x \mapsto v_2], e_0) \quad \text{function application}$$

$$\text{where } \begin{aligned} \text{eval}(\rho, t_1^{\ell_1}) &= [(\text{fn } x \Rightarrow e_0), \rho_0] \wedge \\ \text{eval}(\rho, t_2^{\ell_2}) &= v_2 \end{aligned}$$

8/41

Control Flow Analysis (CFA)

As we allow variables/names to be bound/associated to/with **values** as well as **functions** (closures) any function application only makes sense in an environment ρ or context:

... $(f\ 3)$... or better ... $(f^{\ell_1}\ 3^{\ell_2})^{\ell_3}$...

It might be that $f \mapsto 3^{\ell'}$ (constant) or $f \mapsto (\text{fn } x \Rightarrow x^{\ell'})^{\ell''}$ (identity) or $f \mapsto (\text{fn } x \Rightarrow (x^{\ell'}\ x^{\ell''}))^{\ell'''}$ (doubling).

In our imperative setting WHILE we might also allow variables to point to programs, e.g. ... $| [p := S]^\ell | p |$... Then, e.g.

if b **then** $[p := S_1]^1$ **else** $[p := S_2]^2$; p

leads to the the question whether $(1, \text{init}(S_1))$ and/or $(1, \text{init}(S_2))$ should be in the **control flow**.

9/41

CFA and Functional Programs

Consider the following Fun program:

```
let  f = fn x => x 1;
     g = fn y => y + 2;
     h = fn z => z + 3
in   (f g) + (f h)
```

The aim of **Control Flow Analysis** is:

For each function application, which functions may be applied

10/41

Overview

- ▶ Control Flow Analysis
 - ▶ Abstract Domains and Specification
 - ▶ Constraint Generation
 - ▶ Constraint Solving Algorithm
- ▶ Control and Data Flow Analysis
- ▶ Context-Sensitive Analysis Concepts

11/41

0-CFA Analysis

We will define a **0-CFA Analysis**; the presentation requires two components:

- ▶ Abstract Domains
- ▶ Specification of the Analysis

The result of a 0-CFA analysis is a pair $(\hat{C}, \hat{\rho})$ where:

- ▶ \hat{C} is the **abstract cache** associating abstract values with each labelled program point.
- ▶ $\hat{\rho}$ is the **abstract environment** associating abstract values with each variable.

12/41

Abstract Domains

An **abstract value** \hat{v} is a set of **terms** of the form: $\text{fn } x \Rightarrow e_0$

$\hat{\rho} \in \widehat{\mathbf{Env}} = \mathbf{Var} \rightarrow \widehat{\mathbf{Val}}$ abstract environments

$\hat{v} \in \widehat{\mathbf{Val}} = \mathcal{P}(\mathbf{Term})$ abstract values

$\hat{\mathbf{C}} \in \widehat{\mathbf{Cache}} = \mathbf{Lab} \rightarrow \widehat{\mathbf{Val}}$ abstract caches

Compare this with the **Concrete Domain** (see before):

$\rho \in \mathbf{Env} = \mathbf{Var} \rightarrow \mathbf{Val}$ environments

$v \in \mathbf{Val} = \mathbf{Z} \cup \mathbf{Closure}$ values

$\mathbf{Closure} ::= [\text{fn } x \Rightarrow e_0, \rho]$ closures

13/41

Acceptable CFA

For the formulation of the **0-CFA** analysis we shall write

$$(\hat{\mathbf{C}}, \hat{\rho}) \models e$$

for when $(\hat{\mathbf{C}}, \hat{\rho})$ is an acceptable Control Flow Analysis of the expression e . Thus the relation “ \models ” has functionality

$$\models : (\widehat{\mathbf{Cache}} \times \widehat{\mathbf{Env}} \times \mathbf{Exp}) \rightarrow \{\text{true}, \text{false}\}$$

Our **Goal** therefore is:

If a sub-expression t^ℓ evaluates to a function (closure), then the function must be “predicted” by $\hat{\mathbf{C}}(\ell)$

14/41

CFA: Example

$$((\text{fn } x \Rightarrow x^1)^2 (\text{fn } y \Rightarrow y^3)^4)^5$$

	$(\widehat{C}_e, \widehat{\rho}_e)$	$(\widehat{C}'_e, \widehat{\rho}'_e)$	$(\widehat{C}''_e, \widehat{\rho}''_e)$
1	$\{\text{fn } y \Rightarrow y^3\}$	$\{\text{fn } y \Rightarrow y^3\}$	$\{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^3\}$
2	$\{\text{fn } x \Rightarrow x^1\}$	$\{\text{fn } x \Rightarrow x^1\}$	$\{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^3\}$
3	\emptyset	\emptyset	$\{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^3\}$
4	$\{\text{fn } y \Rightarrow y^3\}$	$\{\text{fn } y \Rightarrow y^3\}$	$\{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^3\}$
5	$\{\text{fn } y \Rightarrow y^3\}$	$\{\text{fn } y \Rightarrow y^3\}$	$\{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^3\}$
x	$\{\text{fn } y \Rightarrow y^3\}$	\emptyset	$\{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^3\}$
y	\emptyset	\emptyset	$\{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^3\}$
	√		√

15/41

Specification: Rules I

$$(\widehat{C}, \widehat{\rho}) \models_s c^\ell \text{ always}$$

$$(\widehat{C}, \widehat{\rho}) \models_s x^\ell \text{ iff } \widehat{\rho}(x) \subseteq \widehat{C}(\ell)$$

$$\begin{aligned} (\widehat{C}, \widehat{\rho}) \models_s (\text{if } t_0^{\ell_0} \text{ then } t_1^{\ell_1} \text{ else } t_2^{\ell_2})^\ell \\ \text{iff } (\widehat{C}, \widehat{\rho}) \models_s t_0^{\ell_0} \wedge \\ (\widehat{C}, \widehat{\rho}) \models_s t_1^{\ell_1} \wedge (\widehat{C}, \widehat{\rho}) \models_s t_2^{\ell_2} \wedge \\ \widehat{C}(\ell_1) \subseteq \widehat{C}(\ell) \wedge \widehat{C}(\ell_2) \subseteq \widehat{C}(\ell) \end{aligned}$$

$$\begin{aligned} (\widehat{C}, \widehat{\rho}) \models_s (\text{let } x = t_1^{\ell_1} \text{ in } t_2^{\ell_2})^\ell \\ \text{iff } (\widehat{C}, \widehat{\rho}) \models_s t_1^{\ell_1} \wedge (\widehat{C}, \widehat{\rho}) \models_s t_2^{\ell_2} \wedge \\ \widehat{C}(\ell_1) \subseteq \widehat{\rho}(x) \wedge \widehat{C}(\ell_2) \subseteq \widehat{C}(\ell) \end{aligned}$$

16/41

Specification: Rules II

$$\begin{aligned} (\widehat{C}, \widehat{\rho}) \models_s (t_1^{\ell_1} \text{ op } t_2^{\ell_2})^\ell \\ \text{iff } (\widehat{C}, \widehat{\rho}) \models_s t_1^{\ell_1} \wedge (\widehat{C}, \widehat{\rho}) \models_s t_2^{\ell_2} \end{aligned}$$

$$\begin{aligned} (\widehat{C}, \widehat{\rho}) \models_s (\text{fn } x \Rightarrow e_0)^\ell \\ \text{iff } \{\text{fn } x \Rightarrow e_0\} \subseteq \widehat{C}(\ell) \wedge (\widehat{C}, \widehat{\rho}) \models_s e_0 \end{aligned}$$

$$\begin{aligned} (\widehat{C}, \widehat{\rho}) \models_s (t_1^{\ell_1} t_2^{\ell_2})^\ell \\ \text{iff } (\widehat{C}, \widehat{\rho}) \models_s t_1^{\ell_1} \wedge (\widehat{C}, \widehat{\rho}) \models_s t_2^{\ell_2} \wedge \\ (\forall (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \widehat{C}(\ell_1) : \\ \widehat{C}(\ell_2) \subseteq \widehat{\rho}(x) \wedge \\ \widehat{C}(\ell_0) \subseteq \widehat{C}(\ell)) \end{aligned}$$

17/41

Constraint Generation

To implement the specification, we must generate a set of constraints from a given program. $C_*[[e_*]]$ is a set of **constraints** and **conditional constraints** of the form

$$lhs \subseteq rhs$$

$$\{t\} \subseteq rhs' \Rightarrow lhs \subseteq rhs$$

where rhs is of the form $C(\ell)$ or $r(x)$, and lhs is of the form $C(\ell)$, $r(x)$, or $\{t\}$, and all occurrences of t are of the form $\text{fn } x \Rightarrow e_0$.

18/41

Constraint-Based CFA I

$$(\widehat{\mathbf{C}}, \widehat{\rho}) \models_s (\text{fn } x \Rightarrow e_0)^\ell$$

$$\text{iff } \{\text{fn } x \Rightarrow e_0\} \subseteq \widehat{\mathbf{C}}(\ell) \wedge (\widehat{\mathbf{C}}, \widehat{\rho}) \models_s e_0$$

$$\mathcal{C}_\star[(\text{fn } x \Rightarrow e_0)^\ell] = \{\{\text{fn } x \Rightarrow e_0\} \subseteq \mathbf{C}(\ell)\} \cup \mathcal{C}_\star[e_0]$$

$$(\widehat{\mathbf{C}}, \widehat{\rho}) \models_s (t_1^{\ell_1} t_2^{\ell_2})^\ell \text{ iff } (\widehat{\mathbf{C}}, \widehat{\rho}) \models_s t_1^{\ell_1} \wedge (\widehat{\mathbf{C}}, \widehat{\rho}) \models_s t_2^{\ell_2} \wedge$$

$$(\forall (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \widehat{\mathbf{C}}(\ell_1) : \widehat{\mathbf{C}}(\ell_2) \subseteq \widehat{\rho}(x) \wedge \widehat{\mathbf{C}}(\ell_0) \subseteq \widehat{\mathbf{C}}(\ell))$$

$$\mathcal{C}_\star[(t_1^{\ell_1} t_2^{\ell_2})^\ell]$$

$$= \mathcal{C}_\star[t_1^{\ell_1}] \cup \mathcal{C}_\star[t_2^{\ell_2}]$$

$$\cup \{\{t\} \subseteq \mathbf{C}(\ell_1) \Rightarrow \mathbf{C}(\ell_2) \subseteq r(x) \mid t = (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \mathbf{Term}_\star\}$$

$$\cup \{\{t\} \subseteq \mathbf{C}(\ell_1) \Rightarrow \mathbf{C}(\ell_0) \subseteq \mathbf{C}(\ell) \mid t = (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \mathbf{Term}_\star\}$$

19/41

Constraint-Based CFA II

$$\mathcal{C}_\star[\mathbf{c}^\ell] = \emptyset$$

$$\mathcal{C}_\star[x^\ell] = \{r(x) \subseteq \mathbf{C}(\ell)\}$$

$$\mathcal{C}_\star[(\text{if } t_0^{\ell_0} \text{ then } t_1^{\ell_1} \text{ else } t_2^{\ell_2})^\ell] = \mathcal{C}_\star[t_0^{\ell_0}] \cup \mathcal{C}_\star[t_1^{\ell_1}] \cup \mathcal{C}_\star[t_2^{\ell_2}]$$

$$\cup \{\mathbf{C}(\ell_1) \subseteq \mathbf{C}(\ell)\}$$

$$\cup \{\mathbf{C}(\ell_2) \subseteq \mathbf{C}(\ell)\}$$

$$\mathcal{C}_\star[(\text{let } x = t_1^{\ell_1} \text{ in } t_2^{\ell_2})^\ell] = \mathcal{C}_\star[t_1^{\ell_1}] \cup \mathcal{C}_\star[t_2^{\ell_2}]$$

$$\cup \{\mathbf{C}(\ell_1) \subseteq r(x)\} \cup \{\mathbf{C}(\ell_2) \subseteq \mathbf{C}(\ell)\}$$

$$\mathcal{C}_\star[(t_1^{\ell_1} \text{ op } t_2^{\ell_2})^\ell] = \mathcal{C}_\star[t_1^{\ell_1}] \cup \mathcal{C}_\star[t_2^{\ell_2}]$$

20/41

Contrait Generation: Example I

$$\begin{aligned}
 \mathcal{C}_* \llbracket ((\text{fn } x \Rightarrow x^1)^2 (\text{fn } y \Rightarrow y^3)^4)^5 \rrbracket = \\
 & \mathcal{C}_* \llbracket (\text{fn } x \Rightarrow x^1)^2 \rrbracket \cup \mathcal{C}_* \llbracket (\text{fn } y \Rightarrow y^3)^4 \rrbracket \\
 & \cup \{ \{t\} \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(4) \subseteq r(x) \mid t = (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \mathbf{Term}_* \} \\
 & \cup \{ \{t\} \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(\ell_0) \subseteq \mathbf{C}(5) \mid t = (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \mathbf{Term}_* \}
 \end{aligned}$$

$$\begin{aligned}
 \mathcal{C}_* \llbracket (\text{fn } x \Rightarrow x^1)^2 \rrbracket = \\
 & \{ \{ \text{fn } x \Rightarrow x^1 \} \subseteq \mathbf{C}(2) \} \cup \mathcal{C}_* \llbracket x^1 \rrbracket = \\
 & \{ \{ \text{fn } x \Rightarrow x^1 \} \subseteq \mathbf{C}(2) \} \cup \{ r(x) \subseteq \mathbf{C}(1) \} = \\
 & \{ \{ \text{fn } x \Rightarrow x^1 \} \subseteq \mathbf{C}(2), r(x) \subseteq \mathbf{C}(1) \}
 \end{aligned}$$

$$\begin{aligned}
 \mathcal{C}_* \llbracket (\text{fn } y \Rightarrow y^3)^4 \rrbracket = & \{ \{ \text{fn } y \Rightarrow y^3 \} \subseteq \mathbf{C}(4) \} \cup \mathcal{C}_* \llbracket y^3 \rrbracket = \\
 & \{ \{ \text{fn } y \Rightarrow y^3 \} \subseteq \mathbf{C}(4), r(y) \subseteq \mathbf{C}(3) \}
 \end{aligned}$$

21/41

Contrait Generation: Example II

$$\begin{aligned}
 & \{ \{t\} \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(4) \subseteq r(x) \mid t = (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \mathbf{Term}_* \} \\
 = & \{ \text{fn } x \Rightarrow x^1 \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(4) \subseteq r(x), \\
 & \text{fn } y \Rightarrow y^3 \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(4) \subseteq r(y) \}
 \end{aligned}$$

$$\begin{aligned}
 & \{ \{t\} \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(\ell_0) \subseteq \mathbf{C}(5) \mid t = (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \mathbf{Term}_* \} \\
 = & \{ \text{fn } x \Rightarrow x^1 \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(1) \subseteq \mathbf{C}(5), \\
 & \text{fn } y \Rightarrow y^3 \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(3) \subseteq \mathbf{C}(5) \}
 \end{aligned}$$

22/41

Constraint Generation: Example III

$$\begin{aligned} \mathcal{C}_* \llbracket ((\text{fn } x \Rightarrow x^1)^2 (\text{fn } y \Rightarrow y^3)^4)^5 \rrbracket = \\ & \{ \{ \text{fn } x \Rightarrow x^1 \} \subseteq \mathbf{C}(2), \\ & \quad r(x) \subseteq \mathbf{C}(1), \\ & \quad \{ \text{fn } y \Rightarrow y^3 \} \subseteq \mathbf{C}(4), \\ & \quad r(y) \subseteq \mathbf{C}(3), \\ & \quad \{ \text{fn } x \Rightarrow x^1 \} \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(4) \subseteq r(x), \\ & \quad \{ \text{fn } x \Rightarrow x^1 \} \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(1) \subseteq \mathbf{C}(5), \\ & \quad \{ \text{fn } y \Rightarrow y^3 \} \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(4) \subseteq r(y), \\ & \quad \{ \text{fn } y \Rightarrow y^3 \} \subseteq \mathbf{C}(2) \Rightarrow \mathbf{C}(3) \subseteq \mathbf{C}(5) \} \end{aligned}$$

23/41

Constraint Solving

To solve the constraints, we use a graph-based formulation. The algorithm uses the following main **data structures**:

- ▶ a **worklist** W , i.e. a list of nodes whose outgoing edges should be traversed;
- ▶ a **data array** D that for each node gives an element of $\widehat{\mathbf{Val}}_*$; and
- ▶ an **edge array** E that for each node gives a list of constraints from which a list of the successor nodes can be computed.

24/41

Constraints Graph

The graph will have nodes $C(\ell)$ and $r(x)$ for $\ell \in \mathbf{Lab}_*$ and $x \in \mathbf{Var}_*$. Associated with each node p we have a data field $D[p]$ that initially is given by:

$$D[p] = \{t \mid (\{t\} \subseteq p) \in \mathcal{C}_*[[e_*]]\}$$

The graph will have edges for a subset of the constraints in $\mathcal{C}_*[[e_*]]$; each edge will be decorated with the constraint that gives rise to it:

- ▶ a constraint $p_1 \subseteq p_2$ gives rise to an edge from p_1 to p_2 , and
- ▶ a constraint $\{t\} \subseteq p \Rightarrow p_1 \subseteq p_2$ gives rise to an edge from p_1 to p_2 and an edge from p to p_2 .

25/41

Algorithm I

INPUT: $\mathcal{C}_*[[e_*]]$

OUTPUT: $(\hat{C}, \hat{\rho})$

METHOD: **Step 1: Initialisation**

$W := \text{nil};$

for q in Nodes do $D[q] := \emptyset;$

for q in Nodes do $E[q] := \text{nil};$

26/41

Algorithm II

Step 2: Building the graph

```
for  $cc$  in  $\mathcal{C}_*[[e_*]]$  do
  case  $cc$  of
     $\{t\} \subseteq p$ :  $\text{add}(p, \{t\})$ ;
     $p_1 \subseteq p_2$ :  $E[p_1] := \text{cons}(cc, E[p_1])$ ;
     $\{t\} \subseteq p \Rightarrow p_1 \subseteq p_2$ :
       $E[p_1] := \text{cons}(cc, E[p_1])$ ;
       $E[p] := \text{cons}(cc, E[p])$ ;
```

27/41

Algorithm III

Step 3: Iteration

```
while  $W \neq \text{nil}$  do
   $q := \text{head}(W)$ ;  $W := \text{tail}(W)$ ;
  for  $cc$  in  $E[q]$  do
    case  $cc$  of
       $p_1 \subseteq p_2$ :  $\text{add}(p_2, D[p_1])$ ;
       $\{t\} \subseteq p \Rightarrow p_1 \subseteq p_2$ :
        if  $t \in D[p]$  then  $\text{add}(p_2, D[p_1])$ ;
```

28/41

Algorithm IV

Step 4: Recording the solution

for ℓ in \mathbf{Lab}_* do $\widehat{C}(\ell) := D[C(\ell)]$;
 for x in \mathbf{Var}_* do $\widehat{\rho}(x) := D[r(x)]$;

USING: procedure $\text{add}(q,d)$ is
 if $\neg (d \subseteq D[q])$
 then $D[q] := D[q] \cup d$;
 $W := \text{cons}(q,W)$;

29/41

Example I

ρ	$D[\rho]$	$E[\rho]$
C(1)	\emptyset	$[\text{id}_x \subseteq C(2) \Rightarrow C(1) \subseteq C(5)]$
C(2)	id_x	$[\text{id}_y \subseteq C(2) \Rightarrow C(3) \subseteq C(5), \text{id}_y \subseteq C(2) \Rightarrow C(4) \subseteq r(y),$ $\text{id}_x \subseteq C(2) \Rightarrow C(1) \subseteq C(5), \text{id}_x \subseteq C(2) \Rightarrow C(4) \subseteq r(x)]$
C(3)	\emptyset	$[\text{id}_y \subseteq C(2) \Rightarrow C(3) \subseteq C(5)]$
C(4)	id_y	$[\text{id}_y \subseteq C(2) \Rightarrow C(4) \subseteq r(y), \text{id}_x \subseteq C(2) \Rightarrow C(4) \subseteq r(x)]$
C(5)	\emptyset	$[\]$
$r(x)$	\emptyset	$[r(x) \subseteq C(1)]$
$r(y)$	\emptyset	$[r(y) \subseteq C(3)]$

30/41

Example II

W	[C(4),C(2)]	[r(x),C(2)]	[C(1),C(2)]	[C(5),C(2)]	[C(2)]	[]
C(1)	\emptyset	\emptyset	id_y	id_y	id_y	id_y
C(2)	id_x	id_x	id_x	id_x	id_x	id_x
C(3)	\emptyset	\emptyset	\emptyset	\emptyset	\emptyset	\emptyset
C(4)	id_y	id_y	id_y	id_y	id_y	id_y
C(5)	\emptyset	\emptyset	\emptyset	id_y	id_y	id_y
r(x)	\emptyset	id_y	id_y	id_y	id_y	id_y
r(y)	\emptyset	\emptyset	\emptyset	\emptyset	\emptyset	\emptyset

31/41

Control Flow + Data Flow

Let **Data** be a set of *abstract data values* (i.e. abstract properties of booleans and arithmetic constants)

$$\hat{v} \in \widehat{\mathbf{Val}}_d = \mathcal{P}(\mathbf{Term} \cup \mathbf{Data}) \quad \text{abstract values}$$

For each constant $c \in \mathbf{Const}$ we need an element $d_c \in \mathbf{Data}$
 Similarly, for each operator $op \in \mathbf{Op}$ we need a total function

$$\widehat{op} : \widehat{\mathbf{Val}}_d \times \widehat{\mathbf{Val}}_d \rightarrow \widehat{\mathbf{Val}}_d$$

Typically, \widehat{op} will have a definition of the form:

$$\hat{v}_1 \widehat{op} \hat{v}_2 = \bigcup \{d_{op}(d_1, d_2) \mid d_1 \in \hat{v}_1 \cap \mathbf{Data}, d_2 \in \hat{v}_2 \cap \mathbf{Data}\}$$

for some function $d_{op} : \mathbf{Data} \times \mathbf{Data} \rightarrow \mathcal{P}(\mathbf{Data})$

32/41

Detection of Sign

$$\mathbf{Data}_{\text{sign}} = \{\text{tt}, \text{ff}, -, 0, +\}$$

$$d_{\text{true}} = \text{tt} \quad d_{\neq} = +$$

$\hat{\neq}$ is defined from:

d_+	tt	ff	-	0	+
tt	\emptyset	\emptyset	\emptyset	\emptyset	\emptyset
ff	\emptyset	\emptyset	\emptyset	\emptyset	\emptyset
-	\emptyset	\emptyset	$\{-\}$	$\{-\}$	$\{-, 0, +\}$
0	\emptyset	\emptyset	$\{-\}$	$\{0\}$	$\{+\}$
+	\emptyset	\emptyset	$\{-, 0, +\}$	$\{+\}$	$\{+\}$

33/41

Abstract Values I

$$(\hat{\mathbf{C}}, \hat{\rho}) \models_d (\text{fn } x \Rightarrow e_0)^\ell \text{ iff } \{\text{fn } x \Rightarrow e_0\} \subseteq \hat{\mathbf{C}}(\ell) \wedge (\hat{\mathbf{C}}, \hat{\rho}) \models_d e_0$$

$$\begin{aligned} (\hat{\mathbf{C}}, \hat{\rho}) \models_d (t_1^{\ell_1} t_2^{\ell_2})^\ell \\ \text{iff } (\hat{\mathbf{C}}, \hat{\rho}) \models_d t_1^{\ell_1} \wedge (\hat{\mathbf{C}}, \hat{\rho}) \models_d t_2^{\ell_2} \wedge \\ (\forall (\text{fn } x \Rightarrow t_0^{\ell_0}) \in \hat{\mathbf{C}}(\ell_1) : \\ \hat{\mathbf{C}}(\ell_2) \subseteq \hat{\rho}(x) \wedge \hat{\mathbf{C}}(\ell_0) \subseteq \hat{\mathbf{C}}(\ell)) \end{aligned}$$

$$\begin{aligned} (\hat{\mathbf{C}}, \hat{\rho}) \models_d (\text{if } t_0^{\ell_0} \text{ then } t_1^{\ell_1} \text{ else } t_2^{\ell_2})^\ell \\ \text{iff } (\hat{\mathbf{C}}, \hat{\rho}) \models_d t_0^{\ell_0} \wedge \\ (d_{\text{true}} \in \hat{\mathbf{C}}(\ell_0) \Rightarrow ((\hat{\mathbf{C}}, \hat{\rho}) \models_d t_1^{\ell_1} \wedge \hat{\mathbf{C}}(\ell_1) \subseteq \hat{\mathbf{C}}(\ell))) \wedge \\ (d_{\text{false}} \in \hat{\mathbf{C}}(\ell_0) \Rightarrow ((\hat{\mathbf{C}}, \hat{\rho}) \models_d t_2^{\ell_2} \wedge \hat{\mathbf{C}}(\ell_2) \subseteq \hat{\mathbf{C}}(\ell))) \end{aligned}$$

34/41

Abstract Values II

$$(\widehat{C}, \widehat{\rho}) \models_d c^\ell \text{ iff } \{d_c\} \subseteq \widehat{C}(\ell)$$

$$(\widehat{C}, \widehat{\rho}) \models_d x^\ell \text{ iff } \widehat{\rho}(x) \subseteq \widehat{C}(\ell)$$

$$\begin{aligned} (\widehat{C}, \widehat{\rho}) \models_d (\text{let } x = t_1^{\ell_1} \text{ in } t_2^{\ell_2})^\ell \\ \text{iff } (\widehat{C}, \widehat{\rho}) \models_d t_1^{\ell_1} \wedge (\widehat{C}, \widehat{\rho}) \models_d t_2^{\ell_2} \wedge \\ \widehat{C}(\ell_1) \subseteq \widehat{\rho}(x) \wedge \widehat{C}(\ell_2) \subseteq \widehat{C}(\ell) \end{aligned}$$

$$\begin{aligned} (\widehat{C}, \widehat{\rho}) \models_d (t_1^{\ell_1} \text{ op } t_2^{\ell_2})^\ell \\ \text{iff } (\widehat{C}, \widehat{\rho}) \models_d t_1^{\ell_1} \wedge (\widehat{C}, \widehat{\rho}) \models_d t_2^{\ell_2} \wedge \\ \widehat{C}(\ell_1) \widehat{\text{op}} \widehat{C}(\ell_2) \subseteq \widehat{C}(\ell) \end{aligned}$$

35/41

Example: Sign Detection

let $f = (\text{fn } x \Rightarrow (\text{if } (x^1 > 0^2)^3 \text{ then } (\text{fn } y \Rightarrow y^4)^5$
 $\text{else } (\text{fn } z \Rightarrow 25^6)^7)^8)^9$
in $((f^{10} 3^{11})^{12} 0^{13})^{14})^{15}$

C(1)	\emptyset
C(2)	\emptyset
C(3)	\emptyset
C(4)	\emptyset
C(5)	id_y
C(6)	\emptyset
C(7)	C_{25}

C(8)	$\{\text{id}_y, C_{25}\}$
C(9)	$\{\text{fn } x \dots\}^8$
C(10)	$\{\text{fn } x \dots\}^8$
C(11)	\emptyset
C(12)	$\{\text{id}_y, C_{25}\}$
C(13)	\emptyset

C(14)	\emptyset
C(15)	\emptyset
r(f)	$\{\text{fn } x \dots\}^8$
r(x)	\emptyset
r(y)	\emptyset
r(z)	\emptyset

C(1)	$\{+\}$
C(2)	$\{0\}$
C(3)	$\{\text{tt}\}$
C(4)	$\{0\}$
C(5)	id_y
C(6)	\emptyset
C(7)	C_{25}

C(8)	$\{\text{id}_y\}$
C(9)	$\{\text{fn } x \dots\}^8$
C(10)	$\{\text{fn } x \dots\}^8$
C(11)	$\{+\}$
C(12)	$\{\text{id}_y\}$
C(13)	$\{0\}$

C(14)	$\{0\}$
C(15)	$\{0\}$
r(f)	$\{\text{fn } x \dots\}^8$
r(x)	$\{+\}$
r(y)	$\{0\}$
r(z)	\emptyset

A pure 0-CFA analysis will not be able to discover that the

36/41

Context-Sensitive CFA

The Control Flow Analyses presented so far are imprecise in that they cannot distinguish the various instances of function calls from one another. In the terminology of Data Flow Analysis the 0-CFA analysis is **context-insensitive** and in the terminology of Control Flow Analysis it is **monovariant**.

To get a more precise analysis it is useful to introduce a mechanism that distinguishes different dynamic instances of variables and labels from one another. This results in a **context-sensitive** analysis and in the terminology of Control Flow Analysis the term **polyvariant** is used.

37/41

Example: Context

Consider the expression:

```
(let  f = (fn x=> x1)2
in   ((f3 f4)5 (fn y=> y6)7)8)9
```

The least 0-CFA analysis is given by $(\hat{C}_{id}, \hat{\rho}_{id})$:

38/41

0-CFA Solutions

$$\begin{aligned}\widehat{C}_{id}(1) &= \{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^6\} & \widehat{C}_{id}(2) &= \{\text{fn } x \Rightarrow x^1\} \\ \widehat{C}_{id}(3) &= \{\text{fn } x \Rightarrow x^1\} & \widehat{C}_{id}(4) &= \{\text{fn } x \Rightarrow x^1\} \\ \widehat{C}_{id}(5) &= \{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^6\} & \widehat{C}_{id}(6) &= \{\text{fn } y \Rightarrow y^6\} \\ \widehat{C}_{id}(7) &= \{\text{fn } y \Rightarrow y^6\} \\ \widehat{C}_{id}(8) &= \{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^6\} \\ \widehat{C}_{id}(9) &= \{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^6\} \\ \widehat{\rho}_{id}(f) &= \{\text{fn } x \Rightarrow x^1\} \\ \widehat{\rho}_{id}(x) &= \{\text{fn } x \Rightarrow x^1, \text{fn } y \Rightarrow y^6\} \\ \widehat{\rho}_{id}(y) &= \{\text{fn } y \Rightarrow y^6\}\end{aligned}$$

39/41

Expansion

Expand the program into

```
let f1 = (fn x1 => x1)
in let f2 = (fn x2 => x2)
   in (f1 f2) (fn y => y)
```

and then analyse the expanded expression: the 0-CFA analysis is now able to deduce that x_1 can only be bound to $\text{fn } x_2 \Rightarrow x_2$ and that x_2 can only be bound to $\text{fn } y \Rightarrow y$ so the overall expression will evaluate to $\text{fn } y \Rightarrow y$ only.

40/41

Further CFA Analyses

A more satisfactory solution to the problem is to extend the analysis with **context information** allowing it to distinguish between the various instances of variables and program points and still analyse the original expression.

Examples of such analyses include k -CFA analyses, uniform k -CFA analyses, polynomial k -CFA analyses (mainly of interest for $k > 0$) and the Cartesian Product Algorithm.