An Introduction to Control Flow Analysis

Benoît Montagu

https://epicure.gitlabpages.inria.fr/m2-sos/

SOS, Master Recherche Science Informatique, Univ Rennes

2024–2025

Introduction

Complex Control Flow (1/3)

Sometimes, it is difficult to know which function is called at some call site

For example, in an object oriented language, you could write:

```
1  abstract class A {
2    abstract public int m(int x);
3  }

4  class A1 extends A {
5    public int m(int x) { return x; }
6  }

7  class A2 extends A {
8    public int m(int x) { return 2*x; }
9  }
```

```
10 class C {
11   public int foo(boolean flag, int arg) {
12     A obj = null;
13     if (flag) obj = new A1();
14     else obj = new A2();
15     return obj.m(arg);
16   }
17 }
```

Complex Control Flow (1/3)

Sometimes, it is difficult to know which function is called at some call site

For example, in an object oriented language, you could write:

```
1  abstract class A {
2    abstract public int m(int x);
3  }

4  class A1 extends A {
5    public int m(int x) { return x; }
6  }

7  class A2 extends A {
8    public int m(int x) { return 2*x; }
9  }
```

```
10 class C {
11   public int foo(boolean flag, int arg) {
12     A obj = null;
13     if (flag) obj = new A1();
14     else obj = new A2();
15     return obj.m(arg);
16   }
17 }
```

On line 15, two programs can be executed: `A1.m` (line 5), or `A2.m` (line 8)

This depends on the value of the argument `flag` (line 11)

Complex Control Flow (2/3)

Another example in C, that involves function pointers:

```
1  int f1(int x) { return x; }

2  int f2(int x) { return 2*x; }

3  int foo(int flag, int arg) {
4    int (*f)(int);
5    if (flag) f = &f1;
6    else f = &f2;
7    return (*f)(arg);
8  }
```

Complex Control Flow (3/3)

The same example, in OCaml:

```
1 let f1 x = x
2 let f2 x = 2 * x

3 let foo flag arg =
4   let g = if flag then f1 else f2 in
5   g arg
```

Complex Control Flow (3/3)

The same example, in OCaml:

```
let f1 x = x
let f2 x = 2 * x

let foo flag arg =
  let g = if flag then f1 else f2 in
  g arg
```

A more complex example (in continuation passing style):

```
let rec fact_cps n =
  if n <= 0 then fun k -> k 1
  else
    let f = fact_cps (n-1) in
    fun k -> f (fun fact_n_1 -> k (n * fact_n_1))

let fact n = fact_cps n (fun result -> result)
```

Approximating control flow

Why do we want to know which functions can be called?

- To perform optimizations (function inlining, code specialization, ...)
- To determine whether a call might change memory
  (to enable more optimizations)
- To determine the stack consumption of a program
- To detect whether some exception might be raised
- To detect dead code with precision
- To be sure that some dangerous function cannot be called
- Analyze binary code
- ...

Approximating control flow

Why do we want to know which functions can be called?

- To perform optimizations (function inlining, code specialization, ...)
- To determine whether a call might change memory
  (to enable more optimizations)
- To determine the stack consumption of a program
- To detect whether some exception might be raised
- To detect dead code with precision
- To be sure that some dangerous function cannot be called
- Analyze binary code
- ...

This is a general, difficult problem: Control Flow Analysis (CFA)

The Control Flow Analysis Problem

Given a complete program *P*:

- For every call site in *P*, determine which functions might be called, and

The Control Flow Analysis Problem

Given a complete program *P*:

- For every call site in *P*, determine which functions might be called, and
- For every function in *P*, determine on which arguments it might be called

The Control Flow Analysis Problem

Given a complete program *P*:

- For every call site in *P*, determine which functions might be called, and
- For every function in *P*, determine on which arguments it might be called

In this course: we introduce 0-CFA (the simplest version of CFA)

- On a minimalistic language
- A definition of what is a correct solution
- A formulation based on set constraints
- The main arguments of the soundness proof
- A reconstruction of 0-CFA based on abstract interpretation
- Some extensions (very quickly)

Some References

Flemming Nielson, Hanne Riis Nielson, and Chris Hankin. ***Principles of Program Analysis.*** Springer Berlin Heidelberg, 1999. DOI: 10.1007/978-3-662-03811-6

Benoît Montagu and Thomas P. Jensen. **"Trace-Based Control-Flow Analysis".** In: *PLDI '21: 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation, Virtual Event, Canada, June 20-25, 20211.* Ed. by Stephen N. Freund and Eran Yahav. ACM, 2021, pp. 482–496. DOI: 10.1145/3453483.3454057

A Language with First-Class Functions

Our language of study

The untyped λ-calculus with *call by value* semantics

- Syntax:

$$
\begin{array}{rcll}
t & ::= & \mathrm{x} & \text{(variable)} \\
 & | & t\,t & \text{(application)} \\
 & | & \lambda \mathrm{x}\,.\,t & \text{(abstraction)}
\end{array}
$$

Our language of study

The untyped λ-calculus with *call by value* semantics

- Syntax:

$$
\begin{array}{rcll}
t & ::= & \mathrm{x} & \text{(variable)} \\
 & | & t\,t & \text{(application)} \\
 & | & \lambda \mathrm{x}\,.\,t & \text{(abstraction)} \\
 & | & (t)^{p} & \text{(annotation)}
\end{array}
$$

- The form $(t)^{p}$ is the term t *labelled* with the program point p
- Program points are akin to program locations (file/line/column) in the text of a program
- Program points identify subterms of the initial/source program
- The labels p do not have to be distinct

Our language of study

The untyped λ-calculus with *call by value* semantics

- Syntax:

$$
\begin{array}{rcll}
t & ::= & \mathsf{x} & \text{(variable)} \\
 & | & t\,t & \text{(application)} \\
 & | & \lambda \mathsf{x}\,.\,t & \text{(abstraction)} \\
 & | & (t)^{p} & \text{(annotation)}
\end{array}
$$

- The form $(t)^p$ is the term t *labelled* with the program point p
- Program points are akin to program locations (file/line/column) in the text of a program
- Program points identify subterms of the initial/source program
- The labels p do not have to be distinct
- We only consider "correctly labeled programs":
  - Each variable, abstraction and application is enclosed in an annotation
  - There is no annotation in an annotation: $\left((t)^{p_1}\right)^{p_2}$ is forbidden

Small-step semantics

Values: $v \quad ::= \quad \lambda x\,.\,t$

Substitution: $t_1[x \leftarrow t_2]$ (replaces every x in t_1 with t_2)

Call by value, left to right semantics, for correctly labeled terms:

$$\textsc{BetaV}\ \frac{}{\left(\lambda x\,.\,(t)^{p_0}\right)^{p_1}\ (v)^{p_2} \to t[x \leftarrow v]}$$

$$\textsc{AppCtxtL}\ \frac{t_1 \to t_1'}{t_1\ t_2 \to t_1'\ t_2} \qquad \textsc{AppCtxtR}\ \frac{t \to t'}{(v)^p\ t \to (v)^p\ t'} \qquad \textsc{AnnotCtxt}\ \frac{t \to t'}{(t)^p \to \left(t'\right)^p}$$

Exercise 2.1

Reduce to its normal form the following term

$$\left(\left(\left(\lambda f.\ \left(\lambda x.\ \left(f^{1}\ x^{2}\right)^{3}\right)^{4}\right)^{5}\ \left(\lambda x.\ \left(\lambda y.\ x^{6}\right)^{7}\right)^{8}\right)^{9}\ \left(\left(\lambda y.\ y^{10}\right)^{11}\ \left(\lambda z.\ z^{12}\right)^{13}\right)^{14}\right)^{15}$$

Exercises

Exercise 2.1

Reduce to its normal form the following term

$$\left(\left(\left(\lambda f.\ \left(\lambda x.\ \left(f^{1}\ x^{2}\right)^{3}\right)^{4}\right)^{5}\ \left(\lambda x.\ \left(\lambda y.\ x^{6}\right)^{7}\right)^{8}\right)^{9}\ \left(\left(\lambda y.\ y^{10}\right)^{11}\ \left(\lambda z.\ z^{12}\right)^{13}\right)^{14}\right)^{15}$$

Exercise 2.2 (At home)

Extend the language and its semantics with `let` *bindings as in OCaml.*

Exercise 2.3 (At home)

Extend the language and its semantics with integers, booleans, arithmetic expressions, arithmetic tests, and an `if...then...else` *construct.*

Exercise 2.4 (At home)

Extend the semantics with a new construct for recursive functions `fix` f x . *t that behaves like OCaml's* `let rec` f x $=$ *t* `in` f

0-CFA

Abstract objects computed by the 0-CFA analysis:

- **An abstract value** $\hat{v}$ is a finite set of values (with free variables) that syntactically occur in the source program
- **An abstract cache** $\hat{\mathrm{C}}$ maps labels to abstract values
  👉 Tells which values a program point might produce
- **An abstract environment** $\hat{\rho}$ maps variables to abstract values
  👉 Tells which values a variable might be instantiated with

Example

Consider the program:

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

reminder: $\left(\lambda x \,.\, (t)^{p_0}\right)^{p_1} (v)^{p_2} \to t[x \leftarrow v]$

Example

Consider the program:

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

reminder: $\left(\lambda x \,.\, (t)^{p_0}\right)^{p_1} (v)^{p_2} \to t[x \leftarrow v]$

$$\to \left(\left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

Example

Consider the program:

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

reminder: $\left(\lambda x \,.\, (t)^{p_0}\right)^{p_1} (v)^{p_2} \to t[x \leftarrow v]$

$$\to \left(\left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

$$\to \left(\lambda z \,.\, \left(\lambda x_2 \,.\, x_2^7\right)^3\right)^9$$

Example

Consider the program:

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

reminder: $\left(\lambda x \,.\, (t)^{p_0}\right)^{p_1} (v)^{p_2} \rightarrow t[x \leftarrow v]$

$$\rightarrow \left(\left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

$$\rightarrow \left(\lambda z \,.\, \left(\lambda x_2 \,.\, x_2^7\right)^3\right)^9$$

We have the cache and environment:

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Example

Consider the program:

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

reminder: $\left(\lambda x \,.\, (t)^{p_0}\right)^{p_1} (v)^{p_2} \rightarrow t[x \leftarrow v]$

$$\rightarrow \left(\left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

$$\rightarrow \left(\lambda z \,.\, \left(\lambda x_2 \,.\, x_2^7\right)^3\right)^9$$

We have the cache and environment:

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$

$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$

$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$

$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$

$$\hat{C}(7) = \emptyset$$

Example

Consider the program:

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

reminder: $\left(\lambda x \,.\, (t)^{p_0}\right)^{p_1} (v)^{p_2} \to t[x \leftarrow v]$

$$\to \left(\left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

$$\to \left(\lambda z \,.\, \left(\lambda x_2 \,.\, x_2^7\right)^3\right)^9$$

We have the cache and environment:

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$

$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$

$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$

$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$

$\hat{C}(7) = \emptyset$

👉 x_2^7 never produces a value

Example

Consider the program:

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

reminder: $\left(\lambda x \,.\, (t)^{p_0}\right)^{p_1} (v)^{p_2} \to t[x \leftarrow v]$

$$\to \left(\left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

$$\to \left(\lambda z \,.\, \left(\lambda x_2 \,.\, x_2^7\right)^3\right)^9$$

We have the cache and environment:

$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$ $\quad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$

$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\}$ $\quad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$

$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\}$ $\quad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$

$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$ $\quad$ 👉 z and x_2 are never instantiated

$\hat{C}(7) = \emptyset$

👉 x_2^7 never produces a value

Acceptability relation

Correct caches and environments for a term t are specified by the acceptability relation $(\hat{C}, \hat{\rho}) \models t$

$(\hat{C}, \hat{\rho}) \models t$ reads:

> "The abstract cache $\hat{C}$ and the abstract environment $\hat{\rho}$ correctly approximate the behaviour of the program t"

Acceptability relation

Correct caches and environments for a term t are specified by the acceptability relation $(\hat{C}, \hat{\rho}) \models t$

$(\hat{C}, \hat{\rho}) \models t$ reads:

> "The abstract cache $\hat{C}$ and the abstract environment $\hat{\rho}$ correctly approximate the behaviour of the program t"

$$\textsc{Var}\ \frac{\hat{\rho}(x) \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \models x^p}$$

Acceptability relation

Correct caches and environments for a term t are specified by the acceptability relation $(\hat{C}, \hat{\rho}) \models t$

$(\hat{C}, \hat{\rho}) \models t$ reads:

> "The abstract cache $\hat{C}$ and the abstract environment $\hat{\rho}$ correctly approximate the behaviour of the program t"

$$\textsc{Var}\ \frac{\hat{\rho}(x) \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \models x^p} \qquad \textsc{Lam}\ \frac{\{\lambda x.\ (t_0)^{p_0}\} \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \models (\lambda x.\ (t_0)^{p_0})^p}$$

Acceptability relation

Correct caches and environments for a term t are specified by the acceptability relation $(\hat{C}, \hat{\rho}) \models t$

$(\hat{C}, \hat{\rho}) \models t$ reads:

> "The abstract cache $\hat{C}$ and the abstract environment $\hat{\rho}$ correctly approximate the behaviour of the program t"

$$\textsc{Var}\ \frac{\hat{\rho}(x) \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \models x^p} \qquad \textsc{Lam}\ \frac{\{\lambda x.\ (t_0)^{p_0}\} \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \models (\lambda x.\ (t_0)^{p_0})^p}$$

$$\textsc{App}\ \frac{\begin{array}{c}(\hat{C}, \hat{\rho}) \models (t_1)^{p_1} \qquad (\hat{C}, \hat{\rho}) \models (t_2)^{p_2} \\ \forall (\lambda x.\ (t_0)^{p_0}) \in \hat{C}(p_1), \\ (\hat{C}, \hat{\rho}) \models (t_0)^{p_0} \quad \wedge \quad \hat{C}(p_2) \subseteq \hat{\rho}(x) \quad \wedge \quad \hat{C}(p_0) \subseteq \hat{C}(p)\end{array}}{(\hat{C}, \hat{\rho}) \models ((t_1)^{p_1}\ (t_2)^{p_2})^p}$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$\hat{\rho}(x_1) \subseteq \hat{C}(1)$ (VAR) at 1

Example

Consider the same program: $t = \left(\left((\lambda x_1 \,.\, x_1^1)^2 \ \left(\lambda y \,.\, (\lambda z \,.\, y^3)^4\right)^5\right)^6 \ (\lambda x_2 \,.\, x_2^7)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, (\lambda z \,.\, y^3)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, (\lambda z \,.\, y^3)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \qquad \text{(VAR) at 1}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \qquad \text{(LAM) at 2}$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \qquad \text{(VAR) at 1}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \qquad \text{(LAM) at 2}$$
$$\hat{\rho}(y) \subseteq \hat{C}(3) \qquad \text{(VAR) at 3}$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \qquad \text{(VAR) at 1}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \qquad \text{(LAM) at 2}$$
$$\hat{\rho}(y) \subseteq \hat{C}(3) \qquad \text{(VAR) at 3}$$
$$\{\lambda z \,.\, y^3\} \subseteq \hat{C}(4) \qquad \text{(LAM) at 4}$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \qquad \text{(VAR) at 1}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \qquad \text{(LAM) at 2}$$
$$\hat{\rho}(y) \subseteq \hat{C}(3) \qquad \text{(VAR) at 3}$$
$$\{\lambda z \,.\, y^3\} \subseteq \hat{C}(4) \qquad \text{(LAM) at 4}$$
$$\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\} \subseteq \hat{C}(5) \qquad \text{(LAM) at 5}$$

Example

Consider the same program: $t = \left(\left((\lambda x_1 \,.\, x_1^1)^2 \left(\lambda y \,.\, (\lambda z \,.\, y^3)^4 \right)^5 \right)^6 (\lambda x_2 \,.\, x_2^7)^8 \right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{ \lambda y \,.\, (\lambda z \,.\, y^3)^4 \right\} \qquad \hat{\rho}(x_1) = \left\{ \lambda y \,.\, (\lambda z \,.\, y^3)^4 \right\}$$
$$\hat{C}(2) = \left\{ \lambda x_1 \,.\, x_1^1 \right\} \qquad \hat{\rho}(y) = \left\{ \lambda x_2 \,.\, x_2^7 \right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{ \lambda x_2 \,.\, x_2^7 \right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{ \lambda z \,.\, y^3 \right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \quad \text{(VAR) at 1} \qquad \hat{C}(5) \subseteq \hat{\rho}(x_1) \wedge \hat{C}(1) \subseteq \hat{C}(6) \quad \text{(APP) at 6}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \quad \text{(LAM) at 2}$$
$$\hat{\rho}(y) \subseteq \hat{C}(3) \quad \text{(VAR) at 3}$$
$$\{\lambda z \,.\, y^3\} \subseteq \hat{C}(4) \quad \text{(LAM) at 4}$$
$$\{\lambda y \,.\, (\lambda z \,.\, y^3)^4\} \subseteq \hat{C}(5) \quad \text{(LAM) at 5}$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \quad \text{(VAR) at 1} \qquad \hat{C}(5) \subseteq \hat{\rho}(x_1) \wedge \hat{C}(1) \subseteq \hat{C}(6) \quad \text{(APP) at 6}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \quad \text{(LAM) at 2} \qquad \hat{\rho}(x_2) \subseteq \hat{C}(7) \quad \text{(VAR) at 7}$$
$$\hat{\rho}(y) \subseteq \hat{C}(3) \quad \text{(VAR) at 3}$$
$$\{\lambda z \,.\, y^3\} \subseteq \hat{C}(4) \quad \text{(LAM) at 4}$$
$$\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\} \subseteq \hat{C}(5) \quad \text{(LAM) at 5}$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \quad \text{(VAR) at 1} \qquad \hat{C}(5) \subseteq \hat{\rho}(x_1) \wedge \hat{C}(1) \subseteq \hat{C}(6) \quad \text{(APP) at 6}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \quad \text{(LAM) at 2} \qquad \hat{\rho}(x_2) \subseteq \hat{C}(7) \quad \text{(VAR) at 7}$$
$$\hat{\rho}(y) \subseteq \hat{C}(3) \quad \text{(VAR) at 3} \qquad \{\lambda x_2 \,.\, x_2^7\} \subseteq \hat{C}(8) \quad \text{(LAM) at 8}$$
$$\{\lambda z \,.\, y^3\} \subseteq \hat{C}(4) \quad \text{(LAM) at 4}$$
$$\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\} \subseteq \hat{C}(5) \quad \text{(LAM) at 5}$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \quad \text{(VAR) at 1} \qquad \hat{C}(5) \subseteq \hat{\rho}(x_1) \wedge \hat{C}(1) \subseteq \hat{C}(6) \quad \text{(APP) at 6}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \quad \text{(LAM) at 2} \qquad \hat{\rho}(x_2) \subseteq \hat{C}(7) \quad \text{(VAR) at 7}$$
$$\hat{\rho}(y) \subseteq \hat{C}(3) \quad \text{(VAR) at 3} \qquad \{\lambda x_2 \,.\, x_2^7\} \subseteq \hat{C}(8) \quad \text{(LAM) at 8}$$
$$\{\lambda z \,.\, y^3\} \subseteq \hat{C}(4) \quad \text{(LAM) at 4} \qquad \hat{C}(8) \subseteq \hat{\rho}(y) \wedge \hat{C}(4) \subseteq \hat{C}(9) \quad \text{(APP) at 9}$$
$$\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\} \subseteq \hat{C}(5) \quad \text{(LAM) at 5}$$

Example

Consider the same program: $t = \left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$

$$\hat{C}(1) = \hat{C}(5) = \hat{C}(6) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\} \qquad \hat{\rho}(x_1) = \left\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right\}$$
$$\hat{C}(2) = \left\{\lambda x_1 \,.\, x_1^1\right\} \qquad \hat{\rho}(y) = \left\{\lambda x_2 \,.\, x_2^7\right\}$$
$$\hat{C}(3) = \hat{C}(8) = \left\{\lambda x_2 \,.\, x_2^7\right\} \qquad \hat{\rho}(z) = \hat{\rho}(x_2) = \emptyset$$
$$\hat{C}(4) = \hat{C}(9) = \left\{\lambda z \,.\, y^3\right\}$$
$$\hat{C}(7) = \emptyset$$

Let us check all the constraints for $(\hat{C}, \hat{\rho}) \models t$

$$\hat{\rho}(x_1) \subseteq \hat{C}(1) \quad \text{(VAR) at 1} \qquad \hat{C}(5) \subseteq \hat{\rho}(x_1) \wedge \hat{C}(1) \subseteq \hat{C}(6) \quad \text{(APP) at 6}$$
$$\{\lambda x_1 \,.\, x_1^1\} \subseteq \hat{C}(2) \quad \text{(LAM) at 2} \qquad \hat{\rho}(x_2) \subseteq \hat{C}(7) \quad \text{(VAR) at 7}$$
$$\hat{\rho}(y) \subseteq \hat{C}(3) \quad \text{(VAR) at 3} \qquad \{\lambda x_2 \,.\, x_2^7\} \subseteq \hat{C}(8) \quad \text{(LAM) at 8}$$
$$\{\lambda z \,.\, y^3\} \subseteq \hat{C}(4) \quad \text{(LAM) at 4} \qquad \hat{C}(8) \subseteq \hat{\rho}(y) \wedge \hat{C}(4) \subseteq \hat{C}(9) \quad \text{(APP) at 9}$$
$$\{\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\} \subseteq \hat{C}(5) \quad \text{(LAM) at 5}$$

All the constraints are satisfied, therefore $(\hat{C}, \hat{\rho})$ is a valid solution for t!

Many solutions to the acceptability problem

For example, for the previous program:

- There is no constraint at all for $\hat{\rho}(z)$
- We can choose any value for $\hat{\rho}(x_2)$ and $\hat{C}(7)$ as long as $\hat{\rho}(x_2) \subseteq \hat{C}(7)$
- For $\hat{C}(8)$, we can choose any set that contains $\lambda x_2 \,.\, x_2^7$

A best solution

Proposition 3.1

For any program t, there exists $\hat{C}$ and $\hat{\rho}$ such that $(\hat{C}, \hat{\rho}) \models t$

A best solution

Proposition 3.1

For any program t, there exists $\hat{C}$ *and* $\hat{\rho}$ *such that* $(\hat{C}, \hat{\rho}) \models t$

Definition 1

For f_1 and f_2 in $A \to \wp(B)$, define: $f_1 \sqcap f_2 \triangleq \lambda a. f_1(a) \cap f_2(a)$

Proposition 3.2

If $(\hat{C}_1, \hat{\rho}_1) \models t$ *and* $(\hat{C}_2, \hat{\rho}_2) \models t$*, then* $(\hat{C}_1 \sqcap \hat{C}_2, \hat{\rho}_1 \sqcap \hat{\rho}_2) \models t$

Exercise 3.1 (At home)

Prove this proposition

A best solution

Proposition 3.1

For any program t, there exists $\hat{C}$ *and* $\hat{\rho}$ *such that* $(\hat{C}, \hat{\rho}) \models t$

Definition 1

For f_1 and f_2 in $A \to \wp(B)$, define: $f_1 \sqcap f_2 \triangleq \lambda a. f_1(a) \cap f_2(a)$

Proposition 3.2

If $(\hat{C}_1, \hat{\rho}_1) \models t$ *and* $(\hat{C}_2, \hat{\rho}_2) \models t$*, then* $(\hat{C}_1 \sqcap \hat{C}_2, \hat{\rho}_1 \sqcap \hat{\rho}_2) \models t$

Exercise 3.1 (At home)

Prove this proposition

Definition 2

For f_1 and f_2 in $A \to \wp(B)$, define: $f_1 \sqsubseteq f_2 \triangleq \forall a, f_1(a) \subseteq f_2(a)$

Theorem 3

For any program t, there exists a $\sqsubseteq$*-minimal solution* $(\hat{C}, \hat{\rho})$ *such that* $(\hat{C}, \hat{\rho}) \models t$

Constraint-based 0-CFA

Constraints

Problem: How can we compute the best solution?

Roadmap:

Program		Constraints		Solution
t	$\longrightarrow$	$\mathcal{C}[\![t]\!]$	$\longrightarrow$	$(\hat{\mathrm{C}}, \hat{\rho})$ such that $(\hat{\mathrm{C}}, \hat{\rho}) \models t$

Constraints $\mathscr{C}$ are finite sets of atomic constraints c of two forms:

Inclusion constraints:	$lhs \subseteq rhs$
Conditional constraints:	$\{\lambda x\,.\,t\} \subseteq rhs' \Rightarrow lhs \subseteq rhs$
where	$lhs ::= \{\lambda x\,.\,t\} \mid \mathrm{C}(p) \mid \mathrm{r(x)}$
	$rhs ::= \mathrm{C}(p) \mid \mathrm{r(x)}$

We write $\mathbf{Terms}(t)$ to denote the set of subterms of the program t

⚠ Constraints are just pieces of syntax

Constraints for 0-CFA

Let t be a program.

For any $t' \in \mathbf{Terms}(t)$, we define $\mathcal{C}[\![t']\!]$ by induction on t' as follows:

$$\mathcal{C}[\![x^p]\!] \triangleq \{r(x) \subseteq C(p)\}$$

Constraints for 0-CFA

Let t be a program.

For any $t' \in \mathbf{Terms}(t)$, we define $\mathcal{C}[\![t']\!]$ by induction on t' as follows:

$$\mathcal{C}[\![x^p]\!] \triangleq \{r(x) \subseteq C(p)\}$$

$$\mathcal{C}[\![(\lambda x.\ (t_0)^{p_0})^p]\!] \triangleq \mathcal{C}[\![(t_0)^{p_0}]\!] \cup \{\{\lambda x.\ (t_0)^{p_0}\} \subseteq C(p)\}$$

Constraints for 0-CFA

Let t be a program.

For any $t' \in \mathbf{Terms}(t)$, we define $\mathcal{C}[\![t']\!]$ by induction on t' as follows:

$$
\begin{array}{rcl}
\mathcal{C}[\![\mathsf{x}^p]\!] & \triangleq & \{\mathsf{r}(\mathsf{x}) \subseteq \mathsf{C}(p)\} \\
\mathcal{C}[\![\left(\lambda \mathsf{x}\,.\ (t_0)^{p_0}\right)^p]\!] & \triangleq & \mathcal{C}[\![(t_0)^{p_0}]\!] \cup \left\{\{\lambda \mathsf{x}\,.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p)\right\} \\
\mathcal{C}[\![\left((t_1)^{p_1}\ (t_2)^{p_2}\right)^p]\!] & \triangleq & \mathcal{C}[\![(t_1)^{p_1}]\!] \cup \mathcal{C}[\![(t_2)^{p_2}]\!] \\
 & & \cup \bigcup_{\lambda \mathsf{x}\,.\ (t_0)^{p_0} \in \mathbf{Terms}(t)} \left\{\{\lambda \mathsf{x}\,.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p_1) \Rightarrow \mathsf{C}(p_2) \subseteq \mathsf{r}(\mathsf{x})\right\} \\
 & & \cup \bigcup_{\lambda \mathsf{x}\,.\ (t_0)^{p_0} \in \mathbf{Terms}(t)} \left\{\{\lambda \mathsf{x}\,.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p_1) \Rightarrow \mathsf{C}(p_0) \subseteq \mathsf{C}(p)\right\}
\end{array}
$$

Constraints for 0-CFA

Let t be a program.

For any $t' \in \mathbf{Terms}(t)$, we define $\mathcal{C}[\![t']\!]$ by induction on t' as follows:

$$
\begin{array}{rcl}
\mathcal{C}[\![\mathsf{x}^p]\!] & \triangleq & \{\mathsf{r}(\mathsf{x}) \subseteq \mathsf{C}(p)\} \\
\mathcal{C}[\![\left(\lambda \mathsf{x}\,.\ (t_0)^{p_0}\right)^p]\!] & \triangleq & \mathcal{C}[\![(t_0)^{p_0}]\!] \cup \left\{\{\lambda \mathsf{x}\,.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p)\right\} \\
\mathcal{C}[\![\left((t_1)^{p_1}\ (t_2)^{p_2}\right)^p]\!] & \triangleq & \mathcal{C}[\![(t_1)^{p_1}]\!] \cup \mathcal{C}[\![(t_2)^{p_2}]\!] \\
 & & \cup \bigcup_{\lambda \mathsf{x}\,.\ (t_0)^{p_0} \in \mathbf{Terms}(t)} \left\{\{\lambda \mathsf{x}\,.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p_1) \Rightarrow \mathsf{C}(p_2) \subseteq \mathsf{r}(\mathsf{x})\right\} \\
 & & \cup \bigcup_{\lambda \mathsf{x}\,.\ (t_0)^{p_0} \in \mathbf{Terms}(t)} \left\{\{\lambda \mathsf{x}\,.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p_1) \Rightarrow \mathsf{C}(p_0) \subseteq \mathsf{C}(p)\right\}
\end{array}
$$

- There are constraints for every function bodies
- Applications do not generate constraints for the called functions

Constraints for 0-CFA

Let t be a program.

For any $t' \in \mathbf{Terms}(t)$, we define $\mathcal{C}[\![t']\!]$ by induction on t' as follows:

$$
\begin{array}{rcl}
\mathcal{C}[\![\mathsf{x}^p]\!] & \triangleq & \{\mathsf{r}(\mathsf{x}) \subseteq \mathsf{C}(p)\} \\
\mathcal{C}[\![\left(\lambda \mathsf{x}.\ (t_0)^{p_0}\right)^p]\!] & \triangleq & \mathcal{C}[\![(t_0)^{p_0}]\!] \cup \left\{\{\lambda \mathsf{x}.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p)\right\} \\
\mathcal{C}[\![\left((t_1)^{p_1}\ (t_2)^{p_2}\right)^p]\!] & \triangleq & \mathcal{C}[\![(t_1)^{p_1}]\!] \cup \mathcal{C}[\![(t_2)^{p_2}]\!] \\
 & & \cup \bigcup_{\lambda \mathsf{x}.\ (t_0)^{p_0} \in \mathbf{Terms}(t)} \left\{\{\lambda \mathsf{x}.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p_1) \Rightarrow \mathsf{C}(p_2) \subseteq \mathsf{r}(\mathsf{x})\right\} \\
 & & \cup \bigcup_{\lambda \mathsf{x}.\ (t_0)^{p_0} \in \mathbf{Terms}(t)} \left\{\{\lambda \mathsf{x}.\ (t_0)^{p_0}\} \subseteq \mathsf{C}(p_1) \Rightarrow \mathsf{C}(p_0) \subseteq \mathsf{C}(p)\right\}
\end{array}
$$

- There are constraints for every function bodies
- Applications do not generate constraints for the called functions

Remark

If $\mathrm{card}(\mathbf{Terms}(t)) = n$, *then* $\mathrm{card}(\mathcal{C}[\![t]\!]) = \mathcal{O}(n^2)$

Semantics of constraints

We define what it means for a constraint to be satisfied:

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho})[\![\{t\}]\!] &\triangleq \{t\} \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{C}(p)]\!] &\triangleq \hat{\mathsf{C}}(p) \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{r}(\mathsf{x})]\!] &\triangleq \hat{\rho}(\mathsf{x})
\end{aligned}
$$

Semantics of constraints

We define what it means for a constraint to be satisfied:

$$
\begin{array}{rcl}
(\hat{\mathsf{C}}, \hat{\rho})[\![\{t\}]\!] & \triangleq & \{t\} \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{C}(p)]\!] & \triangleq & \hat{\mathsf{C}}(p) \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{r}(\mathsf{x})]\!] & \triangleq & \hat{\rho}(\mathsf{x})
\end{array}
$$

$$
(\hat{\mathsf{C}}, \hat{\rho}) \models_c lhs \subseteq rhs \quad \triangleq \quad (\hat{\mathsf{C}}, \hat{\rho})[\![lhs]\!] \subseteq (\hat{\mathsf{C}}, \hat{\rho})[\![rhs]\!]
$$

Semantics of constraints

We define what it means for a constraint to be satisfied:

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho})[\![\{t\}]\!] &\triangleq \{t\} \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{C}(p)]\!] &\triangleq \hat{\mathsf{C}}(p) \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{r}(\mathsf{x})]\!] &\triangleq \hat{\rho}(\mathsf{x})
\end{aligned}
$$

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho}) \models_c lhs \subseteq rhs &\triangleq (\hat{\mathsf{C}}, \hat{\rho})[\![lhs]\!] \subseteq (\hat{\mathsf{C}}, \hat{\rho})[\![rhs]\!] \\
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \{t\} \subseteq rhs' \Rightarrow lhs \subseteq rhs &\triangleq (\hat{\mathsf{C}}, \hat{\rho}) \models_c \{t\} \subseteq rhs' \Rightarrow (\hat{\mathsf{C}}, \hat{\rho}) \models_c lhs \subseteq rhs
\end{aligned}
$$

Semantics of constraints

We define what it means for a constraint to be satisfied:

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho})[\![\{t\}]\!] &\triangleq \{t\} \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{C}(p)]\!] &\triangleq \hat{\mathsf{C}}(p) \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{r}(\mathsf{x})]\!] &\triangleq \hat{\rho}(\mathsf{x})
\end{aligned}
$$

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathit{lhs} \subseteq \mathit{rhs} &\triangleq (\hat{\mathsf{C}}, \hat{\rho})[\![\mathit{lhs}]\!] \subseteq (\hat{\mathsf{C}}, \hat{\rho})[\![\mathit{rhs}]\!] \\
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \{t\} \subseteq \mathit{rhs}' \Rightarrow \mathit{lhs} \subseteq \mathit{rhs} &\triangleq (\hat{\mathsf{C}}, \hat{\rho}) \models_c \{t\} \subseteq \mathit{rhs}' \Rightarrow (\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathit{lhs} \subseteq \mathit{rhs} \\
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathscr{C} &\triangleq \forall c \in \mathscr{C}, (\hat{\mathsf{C}}, \hat{\rho}) \models_c c
\end{aligned}
$$

Semantics of constraints

We define what it means for a constraint to be satisfied:

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho})[\![\{t\}]\!] &\triangleq \{t\} \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{C}(p)]\!] &\triangleq \hat{\mathsf{C}}(p) \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{r}(\mathsf{x})]\!] &\triangleq \hat{\rho}(\mathsf{x})
\end{aligned}
$$

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathit{lhs} \subseteq \mathit{rhs} &\triangleq (\hat{\mathsf{C}}, \hat{\rho})[\![\mathit{lhs}]\!] \subseteq (\hat{\mathsf{C}}, \hat{\rho})[\![\mathit{rhs}]\!] \\
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \{t\} \subseteq \mathit{rhs}' \Rightarrow \mathit{lhs} \subseteq \mathit{rhs} &\triangleq (\hat{\mathsf{C}}, \hat{\rho}) \models_c \{t\} \subseteq \mathit{rhs}' \Rightarrow (\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathit{lhs} \subseteq \mathit{rhs} \\
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathscr{C} &\triangleq \forall c \in \mathscr{C}, (\hat{\mathsf{C}}, \hat{\rho}) \models_c c
\end{aligned}
$$

Theorem 4

Assume that $\hat{\mathsf{C}}$ and $\hat{\rho}$ contain only variables/labels/terms found in t.
If $(\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathcal{C}[\![t]\!]$, then $(\hat{\mathsf{C}}, \hat{\rho}) \models t$

- We reduced the 0-CFA problem to a constraint satisfiability problem

Semantics of constraints

We define what it means for a constraint to be satisfied:

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho})[\![\{t\}]\!] &\triangleq \{t\} \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{C}(p)]\!] &\triangleq \hat{\mathsf{C}}(p) \\
(\hat{\mathsf{C}}, \hat{\rho})[\![\mathsf{r}(\mathsf{x})]\!] &\triangleq \hat{\rho}(\mathsf{x})
\end{aligned}
$$

$$
\begin{aligned}
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathit{lhs} \subseteq \mathit{rhs} &\triangleq (\hat{\mathsf{C}}, \hat{\rho})[\![\mathit{lhs}]\!] \subseteq (\hat{\mathsf{C}}, \hat{\rho})[\![\mathit{rhs}]\!] \\
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \{t\} \subseteq \mathit{rhs}' \Rightarrow \mathit{lhs} \subseteq \mathit{rhs} &\triangleq (\hat{\mathsf{C}}, \hat{\rho}) \models_c \{t\} \subseteq \mathit{rhs}' \Rightarrow (\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathit{lhs} \subseteq \mathit{rhs} \\
(\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathscr{C} &\triangleq \forall c \in \mathscr{C}, (\hat{\mathsf{C}}, \hat{\rho}) \models_c c
\end{aligned}
$$

Theorem 4

Assume that $\hat{\mathsf{C}}$ and $\hat{\rho}$ contain only variables/labels/terms found in t.
If $(\hat{\mathsf{C}}, \hat{\rho}) \models_c \mathcal{C}[\![t]\!]$, then $(\hat{\mathsf{C}}, \hat{\rho}) \models t$

- We reduced the 0-CFA problem to a constraint satisfiability problem
- Is it an equivalence?

Example

$$\Omega = \left(\left(\lambda x.\ (x^1\ x^2)^3\right)^4\ \left(\lambda y.\ (y^5\ y^6)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\right.$$

$$\left.\right\}$$

Example

$$\Omega = \left(\left(\lambda x\,.\,(x^{1}\,x^{2})^{3}\right)^{4}\left(\lambda y\,.\,(y^{5}\,y^{6})^{7}\right)^{8}\right)^{9}$$

(Ω is a diverging program)

$$\mathcal{C}[\![\Omega]\!] = \left\{ \; r(x) \subseteq C(1), \; \right\}$$

Example

$\Omega = \left(\left(\lambda x.\ (x^1\ x^2)^3\right)^4\ \left(\lambda y.\ (y^5\ y^6)^7\right)^8\right)^9$ (Ω is a diverging program)

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{ll} r(x) \subseteq C(1), & r(x) \subseteq C(2), \end{array}\right\}$$

Example

$\Omega = \left(\left(\lambda x.\ (x^1\, x^2)^3\right)^4 \left(\lambda y.\ (y^5\, y^6)^7\right)^8\right)^9$ (Ω is a diverging program)

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{ \begin{array}{ll} r(x) \subseteq C(1), & r(x) \subseteq C(2), \end{array} \right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$$\mathcal{C}[\![\Omega]\!] =$$

$$\left\{\begin{array}{cc} r(x) \subseteq C(1), & r(x) \subseteq C(2), \\ \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$$\mathcal{C}[\![\Omega]\!] =$$

$$\left\{\begin{array}{ll} \multicolumn{2}{c}{r(x) \subseteq C(1),} & \multicolumn{2}{c}{r(x) \subseteq C(2),} \\ \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\ \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(2) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(7) \subseteq C(3), \end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4 \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{cc} \mathsf{r}(x) \subseteq \mathsf{C}(1), & \mathsf{r}(x) \subseteq \mathsf{C}(2), \\ \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(3), \\ \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(3), \\ \multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4),} \end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{cc} \mathsf{r}(x) \subseteq \mathsf{C}(1), & \mathsf{r}(x) \subseteq \mathsf{C}(2), \\ \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(3), \\ \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(3), \\ \multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4),} \\ \multicolumn{2}{c}{\mathsf{r}(y) \subseteq \mathsf{C}(5),} \end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{cc}
\multicolumn{2}{c}{r(x) \subseteq C(1),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(2) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(7) \subseteq C(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4),} \\
\multicolumn{2}{c}{r(y) \subseteq C(5),} \qquad r(y) \subseteq C(6),
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{cc}
\multicolumn{2}{c}{r(x) \subseteq C(1),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(2) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(7) \subseteq C(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4),} \\
\multicolumn{2}{c}{r(y) \subseteq C(5),} \qquad r(y) \subseteq C(6),
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$$\mathcal{C}[\![\Omega]\!] =$$

$$\left\{\begin{array}{cc}
\mathsf{r}(x) \subseteq \mathsf{C}(1), & \mathsf{r}(x) \subseteq \mathsf{C}(2), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4),} \\
\mathsf{r}(y) \subseteq \mathsf{C}(5), & \mathsf{r}(y) \subseteq \mathsf{C}(6), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(7),
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$$\mathcal{C}[\![\Omega]\!] =$$

$$\left\{\begin{array}{cc}
\multicolumn{2}{c}{r(x) \subseteq C(1),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(2) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(7) \subseteq C(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4),} \\
\multicolumn{2}{c}{r(y) \subseteq C(5),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(6) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(3) \subseteq C(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(6) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(7) \subseteq C(7),
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$$\mathcal{C}[\![\Omega]\!] =$$

$$\left\{\begin{array}{cc}
\multicolumn{2}{c}{r(x) \subseteq C(1),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(2) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(7) \subseteq C(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4),} \\
\multicolumn{2}{c}{r(y) \subseteq C(5),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(6) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(3) \subseteq C(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(6) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(7) \subseteq C(7), \\
\multicolumn{2}{c}{\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(8),}
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ (x^1\, x^2)^3\right)^4 \left(\lambda y.\ (y^5\, y^6)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{cc}
\mathsf{r}(x) \subseteq \mathsf{C}(1), & \mathsf{r}(x) \subseteq \mathsf{C}(2), \\
\{\lambda x.\ (x^1\, x^2)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(x), & \{\lambda x.\ (x^1\, x^2)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(3), \\
\{\lambda y.\ (y^5\, y^6)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(y), & \{\lambda y.\ (y^5\, y^6)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(3), \\
\multicolumn{2}{c}{\{\lambda x.\ (x^1\, x^2)^3\} \subseteq \mathsf{C}(4),} \\
\mathsf{r}(y) \subseteq \mathsf{C}(5), & \mathsf{r}(y) \subseteq \mathsf{C}(6), \\
\{\lambda x.\ (x^1\, x^2)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(x), & \{\lambda x.\ (x^1\, x^2)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(7), \\
\{\lambda y.\ (y^5\, y^6)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(y), & \{\lambda y.\ (y^5\, y^6)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(7), \\
\multicolumn{2}{c}{\{\lambda y.\ (y^5\, y^6)^7\} \subseteq \mathsf{C}(8),}
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4 \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{ll}
\multicolumn{2}{c}{r(x) \subseteq C(1),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(2) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(7) \subseteq C(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4),} \\
\multicolumn{2}{c}{r(y) \subseteq C(5),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(6) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(3) \subseteq C(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(6) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(7) \subseteq C(7), \\
\multicolumn{2}{c}{\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(8),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4) \Rightarrow C(8) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4) \Rightarrow C(3) \subseteq C(9),
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{cc}
\multicolumn{2}{c}{\mathsf{r}(\mathsf{x}) \subseteq \mathsf{C}(1),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(\mathsf{x}), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(\mathsf{y}), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4),} \\
\multicolumn{2}{c}{\mathsf{r}(\mathsf{y}) \subseteq \mathsf{C}(5),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(\mathsf{x}), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(\mathsf{y}), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(7), \\
\multicolumn{2}{c}{\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(8),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(8) \subseteq \mathsf{r}(\mathsf{x}), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(9), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(8) \subseteq \mathsf{r}(\mathsf{y}), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(9)
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4 \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{cc}
\multicolumn{2}{c}{r(x) \subseteq C(1),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(2) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(7) \subseteq C(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4),} \\
\multicolumn{2}{c}{r(y) \subseteq C(5),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(6) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(3) \subseteq C(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(6) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(7) \subseteq C(7), \\
\multicolumn{2}{c}{\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(8),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4) \Rightarrow C(8) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4) \Rightarrow C(3) \subseteq C(9), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(4) \Rightarrow C(8) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(4) \Rightarrow C(7) \subseteq C(9)
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{ll}
\multicolumn{2}{c}{r(x) \subseteq C(1),} \\
\multicolumn{2}{c}{r(x) \subseteq C(2),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(2) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(1) \Rightarrow C(7) \subseteq C(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4),} \\
\multicolumn{2}{c}{r(y) \subseteq C(5),} \\
\multicolumn{2}{c}{r(y) \subseteq C(6),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(6) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(3) \subseteq C(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(6) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(7) \subseteq C(7), \\
\multicolumn{2}{c}{\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(8),} \\
\multicolumn{2}{c}{C(8) \subseteq r(x),} \\
\multicolumn{2}{c}{C(3) \subseteq C(9),} \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(4) \Rightarrow C(8) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(4) \Rightarrow C(7) \subseteq C(9)
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4 \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$$\mathcal{C}[\![\Omega]\!] =$$

$$\left\{\begin{array}{ll}
\mathsf{r}(x) \subseteq \mathsf{C}(1), & \mathsf{r}(x) \subseteq \mathsf{C}(2), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(3), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(3), \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4),} \\
\mathsf{r}(y) \subseteq \mathsf{C}(5), & \mathsf{r}(y) \subseteq \mathsf{C}(6), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(7), \\
\multicolumn{2}{c}{\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(8),} \\
\mathsf{C}(8) \subseteq \mathsf{r}(x), & \mathsf{C}(3) \subseteq \mathsf{C}(9), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(8) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(9)
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{ll}
\multicolumn{2}{c}{r(x) \subseteq C(1),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(2) \subseteq r(x), & \multicolumn{1}{c}{} \\
\multicolumn{2}{c}{C(2) \subseteq r(y),} \\
\multicolumn{2}{c}{\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(4),} \\
\multicolumn{2}{c}{r(y) \subseteq C(5),} \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(6) \subseteq r(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(5) \Rightarrow C(3) \subseteq C(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(6) \subseteq r(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(5) \Rightarrow C(7) \subseteq C(7), \\
\multicolumn{2}{c}{\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(8),} \\
\multicolumn{2}{c}{C(8) \subseteq r(x),} \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(4) \Rightarrow C(8) \subseteq r(y), & \multicolumn{1}{c}{}
\end{array}\right.$$

$$\left.\begin{array}{r}
r(x) \subseteq C(2), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq C(1) \Rightarrow C(3) \subseteq C(3), \\
C(7) \subseteq C(3), \\
\\
r(y) \subseteq C(6), \\
\\
\\
\\
C(3) \subseteq C(9), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq C(4) \Rightarrow C(7) \subseteq C(9)
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4 \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$$\mathcal{C}[\![\Omega]\!] =$$

$$\left\{\begin{array}{ll}
\mathsf{r}(x) \subseteq \mathsf{C}(1), & \mathsf{r}(x) \subseteq \mathsf{C}(2), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(3), \\
\mathsf{C}(2) \subseteq \mathsf{r}(y), & \mathsf{C}(7) \subseteq \mathsf{C}(3), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4), & \\
\mathsf{r}(y) \subseteq \mathsf{C}(5), & \mathsf{r}(y) \subseteq \mathsf{C}(6), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(8), & \\
\mathsf{C}(8) \subseteq \mathsf{r}(x), & \mathsf{C}(3) \subseteq \mathsf{C}(9), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(8) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(9)
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$$\mathcal{C}[\![\Omega]\!] =$$

$$\left\{\begin{array}{ll}
\mathsf{r}(x) \subseteq \mathsf{C}(1), & \mathsf{r}(x) \subseteq \mathsf{C}(2), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(x), & \\
\mathsf{C}(2) \subseteq \mathsf{r}(y), & \mathsf{C}(7) \subseteq \mathsf{C}(3), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4), & \\
\mathsf{r}(y) \subseteq \mathsf{C}(5), & \mathsf{r}(y) \subseteq \mathsf{C}(6), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(y), & \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(8), & \\
\mathsf{C}(8) \subseteq \mathsf{r}(x), & \mathsf{C}(3) \subseteq \mathsf{C}(9), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(8) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(9)
\end{array}\right\}$$

Example

$$\Omega = \left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4 \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9 \qquad (\Omega \text{ is a diverging program})$$

$\mathcal{C}[\![\Omega]\!] =$

$$\left\{\begin{array}{ll}
\mathsf{r}(x) \subseteq \mathsf{C}(1), & \mathsf{r}(x) \subseteq \mathsf{C}(2), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(1) \Rightarrow \mathsf{C}(2) \subseteq \mathsf{r}(x), & \\
\mathsf{C}(2) \subseteq \mathsf{r}(y), & \mathsf{C}(7) \subseteq \mathsf{C}(3), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(4), & \\
\mathsf{r}(y) \subseteq \mathsf{C}(5), & \mathsf{r}(y) \subseteq \mathsf{C}(6), \\
\{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(x), & \{\lambda x.\ \left(x^1\, x^2\right)^3\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(3) \subseteq \mathsf{C}(7), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(5) \Rightarrow \mathsf{C}(6) \subseteq \mathsf{r}(y), & \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(8), & \\
\mathsf{C}(8) \subseteq \mathsf{r}(x), & \mathsf{C}(3) \subseteq \mathsf{C}(9), \\
\{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(8) \subseteq \mathsf{r}(y), & \{\lambda y.\ \left(y^5\, y^6\right)^7\} \subseteq \mathsf{C}(4) \Rightarrow \mathsf{C}(7) \subseteq \mathsf{C}(9)
\end{array}\right\}$$

Minimal solution:

$$\mathsf{C}(1,2,5,6,8) = \mathsf{r}(x,y) = \{\lambda y.\ \left(y^5\, y^6\right)^7\}, \quad \mathsf{C}(4) = \{\lambda x.\ \left(x^1\, x^2\right)^3\}, \quad \mathsf{C}(3,7,9) = \emptyset$$

Solving the constraints

- There exists an algorithm the computes the minimal solution of $\mathcal{C}[\![t]\!]$ in $\mathcal{O}(n^3)$ worst case time complexity, where n is the size of t
- It works by propagating information in a graph that represents constraints
- The details are out of scope for this course

For more details, see the book
Principles of Program Analysis, Chapter 3 Section 4

Soundness of 0-CFA

Is the acceptability relation sound?

- We want a *theorem* saying that acceptable solutions $(\hat{C}, \hat{\rho})$ such that $(\hat{C}, \hat{\rho}) \models t$ "correctly approximate the behaviour of the program t"
- How can we state this?

Is the acceptability relation sound?

- We want a *theorem* saying that acceptable solutions $(\hat{C}, \hat{\rho})$ such that $(\hat{C}, \hat{\rho}) \models t$ "correctly approximate the behaviour of the program t"
- How can we state this?
- **Crux of the problem:**
  Abstract values are finite sets of values that occur in the program...

Is the acceptability relation sound?

- We want a *theorem* saying that acceptable solutions $(\hat{C}, \hat{\rho})$ such that $(\hat{C}, \hat{\rho}) \models t$ "correctly approximate the behaviour of the program t"
- How can we state this?
- **Crux of the problem:**
  Abstract values are finite sets of values that occur in the program...
  What concrete values are represented by those abstract values?

Is the acceptability relation sound?

- We want a *theorem* saying that acceptable solutions $(\hat{C}, \hat{\rho})$ such that $(\hat{C}, \hat{\rho}) \models t$ "correctly approximate the behaviour of the program t"
- How can we state this?
- **Crux of the problem:**
  Abstract values are finite sets of values that occur in the program...
  What concrete values are represented by those abstract values?
- **Intuition of the solution:**
  A free variables x in an abstract value can be replaced
  with any values drawn from $\hat{\rho}(x)$

Is the acceptability relation sound?

- We want a *theorem* saying that acceptable solutions $(\hat{C}, \hat{\rho})$ such that $(\hat{C}, \hat{\rho}) \models t$ "correctly approximate the behaviour of the program t"
- How can we state this?
- **Crux of the problem:**
  Abstract values are finite sets of values that occur in the program...
  What concrete values are represented by those abstract values?
- **Intuition of the solution:**
  A free variables x in an abstract value can be replaced
  with any values drawn from $\hat{\rho}(x)$
- Can we state this more formally?

Unfoldings

Unfolding relation:

$(t, \hat{\rho}) \models^{\emptyset}_{\mathsf{T}} t'$ means "term t' is obtained from t by unfolding definitions of $\hat{\rho}$"

Unfolding relation:

$(t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t'$ means "term t' is obtained from t by unfolding definitions of $\hat{\rho}$"

$$\frac{t \in \hat{\rho}(\mathrm{x}) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{\mathrm{x}\} \cup \mathrm{fv}\, t') = \emptyset}{(\mathrm{x}, \hat{\rho}) \models_{\mathsf{T}}^{X} t'} \qquad \frac{}{(\mathrm{x}, \hat{\rho}) \models_{\mathsf{T}}^{X} \mathrm{x}}$$

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{\mathrm{x}\} \cup X} t'}{(\lambda \mathrm{x}\,.\, t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda \mathrm{x}\,.\, t'} \qquad \frac{(t_1, \hat{\rho}) \models_{\mathsf{T}}^{X} t_1' \qquad (t_2, \hat{\rho}) \models_{\mathsf{T}}^{X} t_2'}{(t_1\, t_2, \hat{\rho}) \models_{\mathsf{T}}^{X} t_1'\, t_2'} \qquad \frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}{\left((t)^p, \hat{\rho}\right) \models_{\mathsf{T}}^{X} (t')^p}$$

- The structure of terms is preserved:
  only variables can be replaced with other terms
- The set X *forbids* unfolding some variables to prevent accidental captures/escapes of variables

Unfoldings: Examples

$$
\begin{aligned}
(x, \{x \mapsto \{\lambda z \,.\, z,\ \lambda y_1 \,.\, \lambda y_2 \,.\, y_1\}\}) &\models_{\top}^{\emptyset} \quad x \\
&\models_{\top}^{\emptyset} \quad \lambda z \,.\, z \\
&\models_{\top}^{\emptyset} \quad \lambda y_1 \,.\, \lambda y_2 \,.\, y_1
\end{aligned}
$$

Unfoldings: Examples

$$
\begin{aligned}
(x, \{x \mapsto \{\lambda z\,.\,z,\ \lambda y_1\,.\,\lambda y_2\,.\,y_1\}\}) &\models_{\top}^{\emptyset} \quad x \\
&\models_{\top}^{\emptyset} \quad \lambda z\,.\,z \\
&\models_{\top}^{\emptyset} \quad \lambda y_1\,.\,\lambda y_2\,.\,y_1
\end{aligned}
$$

$$
\begin{aligned}
(x, \{x \mapsto \{\lambda z\,.\,z,\ \lambda y\,.\,x\}\}) &\models_{\top}^{\emptyset} \quad \lambda z\,.\,z \\
&\models_{\top}^{\emptyset} \quad \lambda y\,.\,\lambda z\,.\,z \\
&\models_{\top}^{\emptyset} \quad \lambda y\,.\,\lambda y\,.\,\lambda z\,.\,z \\
&\models_{\top}^{\emptyset} \quad \lambda y\,.\,\lambda y\,.\,\lambda y\,.\,\lambda z\,.\,z \quad \ldots
\end{aligned}
$$

Unfoldings: Examples

$$
\begin{aligned}
(x, \{x \mapsto \{\lambda z\,.\,z,\ \lambda y_1\,.\,\lambda y_2\,.\,y_1\}\}) &\models_{\top}^{\emptyset} x \\
&\models_{\top}^{\emptyset} \lambda z\,.\,z \\
&\models_{\top}^{\emptyset} \lambda y_1\,.\,\lambda y_2\,.\,y_1
\end{aligned}
$$

$$
\begin{aligned}
(x, \{x \mapsto \{\lambda z\,.\,z,\ \lambda y\,.\,x\}\}) &\models_{\top}^{\emptyset} \lambda z\,.\,z \\
&\models_{\top}^{\emptyset} \lambda y\,.\,\lambda z\,.\,z \\
&\models_{\top}^{\emptyset} \lambda y\,.\,\lambda y\,.\,\lambda z\,.\,z \\
&\models_{\top}^{\emptyset} \lambda y\,.\,\lambda y\,.\,\lambda y\,.\,\lambda z\,.\,z \quad \ldots
\end{aligned}
$$

$$
\begin{aligned}
(x, \{x \mapsto \{\lambda z\,.\,x\}\}) &\models_{\top}^{\emptyset} x \\
&\models_{\top}^{\emptyset} \lambda z\,.\,x \\
&\models_{\top}^{\emptyset} \lambda z\,.\,\lambda z\,.\,x \\
&\models_{\top}^{\emptyset} \lambda z\,.\,\lambda z\,.\,\lambda z\,.\,x \quad \ldots
\end{aligned}
$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{\mathsf{x}\} \cup X} t'}{(\lambda \mathsf{x}\,.\,t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda \mathsf{x}\,.\,t'} \qquad \frac{t \in \hat{\rho}(\mathsf{x}) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{\mathsf{x}\} \cup \mathrm{fv}\, t') = \emptyset}{(\mathsf{x}, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{x\} \cup X} t'}{(\lambda x\,.\,t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda x\,.\,t'} \qquad \frac{t \in \hat{\rho}(x) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{x\} \cup \mathrm{fv}\, t') = \emptyset}{(x, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

$$(x, \{x \mapsto \{\lambda y\,.\,y\};\ y \mapsto \{\lambda z\,.\,z\}\}) \models_{\mathsf{T}}^{\emptyset} x$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{x\} \cup X} t'}{(\lambda x\,.\,t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda x\,.\,t'} \qquad \frac{t \in \hat{\rho}(x) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{x\} \cup \mathrm{fv}\, t') = \emptyset}{(x, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

$$(x, \{x \mapsto \{\lambda y\,.\,y\};\ y \mapsto \{\lambda z\,.\,z\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda z\,.\,z \qquad \text{y has escaped!}$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{x\} \cup X} t'}{(\lambda x \,.\, t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda x \,.\, t'} \qquad \frac{t \in \hat{\rho}(x) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{x\} \cup \mathrm{fv}\, t') = \emptyset}{(x, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

$$(x, \{x \mapsto \{\lambda y \,.\, y\};\ y \mapsto \{\lambda z \,.\, z\}\}) \models_{\mathsf{T}}^{\emptyset} x$$

$$\not\models_{\mathsf{T}}^{\emptyset} \lambda z \,.\, z \qquad \text{y has escaped!}$$

$$(x, \{x \mapsto \{\lambda y \,.\, x_2\};\ x_2 \mapsto \{y\};\ y \mapsto \{\lambda z \,.\, z, \lambda z \,.\, y\}\}) \models_{\mathsf{T}}^{\emptyset} x$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{x\} \cup X} t'}{(\lambda x \,.\, t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda x \,.\, t'} \qquad \frac{t \in \hat{\rho}(x) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{x\} \cup \mathrm{fv}\, t') = \emptyset}{(x, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

$$(x, \{x \mapsto \{\lambda y \,.\, y\};\ y \mapsto \{\lambda z \,.\, z\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda z \,.\, z \qquad \text{y has escaped!}$$

$$(x, \{x \mapsto \{\lambda y \,.\, x_2\};\ x_2 \mapsto \{y\};\ y \mapsto \{\lambda z \,.\, z, \lambda z \,.\, y\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, x_2$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{x\} \cup X} t'}{(\lambda x \,.\, t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda x \,.\, t'} \qquad \frac{t \in \hat{\rho}(x) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{x\} \cup \mathrm{fv}\, t') = \emptyset}{(x, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

$$(x, \{x \mapsto \{\lambda y \,.\, y\};\ y \mapsto \{\lambda z \,.\, z\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda z \,.\, z \qquad \text{y has escaped!}$$

$$(x, \{x \mapsto \{\lambda y \,.\, x_2\};\ x_2 \mapsto \{y\};\ y \mapsto \{\lambda z \,.\, z, \lambda z \,.\, y\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, x_2$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, y \qquad \text{y is captured!}$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{x\} \cup X} t'}{(\lambda x \,.\, t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda x \,.\, t'} \qquad \frac{t \in \hat{\rho}(x) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{x\} \cup \mathrm{fv}\, t') = \emptyset}{(x, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

$$(x, \{x \mapsto \{\lambda y \,.\, y\};\ y \mapsto \{\lambda z \,.\, z\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda z \,.\, z \qquad \text{y has escaped!}$$

$$(x, \{x \mapsto \{\lambda y \,.\, x_2\};\ x_2 \mapsto \{y\};\ y \mapsto \{\lambda z \,.\, z, \lambda z \,.\, y\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, x_2$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, y \qquad \text{y is captured!}$$
$$\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, \lambda z \,.\, z$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{x\} \cup X} t'}{(\lambda x \,.\, t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda x \,.\, t'} \qquad \frac{t \in \hat{\rho}(x) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{x\} \cup \mathrm{fv}\, t') = \emptyset}{(x, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

$$(x, \{x \mapsto \{\lambda y \,.\, y\};\ y \mapsto \{\lambda z \,.\, z\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda z \,.\, z \qquad \text{y has escaped!}$$

$$(x, \{x \mapsto \{\lambda y \,.\, x_2\};\ x_2 \mapsto \{y\};\ y \mapsto \{\lambda z \,.\, z, \lambda z \,.\, y\}\}) \models_{\mathsf{T}}^{\emptyset} x$$
$$\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, x_2$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, y \qquad \text{y is captured!}$$
$$\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, \lambda z \,.\, z$$
$$\not\models_{\mathsf{T}}^{\emptyset} \lambda y \,.\, \lambda z \,.\, y \qquad \text{y is captured!}$$

Unfoldings: Examples (continued)

Recall:

$$\frac{(t, \hat{\rho}) \models_{\mathsf{T}}^{\{x\} \cup X} t'}{(\lambda x \,.\, t, \hat{\rho}) \models_{\mathsf{T}}^{X} \lambda x \,.\, t'} \qquad \frac{t \in \hat{\rho}(x) \qquad (t, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t' \qquad X \cap (\{x\} \cup \mathrm{fv}\, t') = \emptyset}{(x, \hat{\rho}) \models_{\mathsf{T}}^{X} t'}$$

$$\begin{array}{rll} (x, \{x \mapsto \{\lambda y \,.\, y\};\ y \mapsto \{\lambda z \,.\, z\}\}) \models_{\mathsf{T}}^{\emptyset} & x & \\ \not\models_{\mathsf{T}}^{\emptyset} & \lambda z \,.\, z & y \text{ has escaped!} \end{array}$$

$$\begin{array}{rll} (x, \{x \mapsto \{\lambda y \,.\, x_2\};\ x_2 \mapsto \{y\};\ y \mapsto \{\lambda z \,.\, z, \lambda z \,.\, y\}\}) \models_{\mathsf{T}}^{\emptyset} & x & \\ \models_{\mathsf{T}}^{\emptyset} & \lambda y \,.\, x_2 & \\ \not\models_{\mathsf{T}}^{\emptyset} & \lambda y \,.\, y & y \text{ is captured!} \\ \models_{\mathsf{T}}^{\emptyset} & \lambda y \,.\, \lambda z \,.\, z & \\ \not\models_{\mathsf{T}}^{\emptyset} & \lambda y \,.\, \lambda z \,.\, y & y \text{ is captured!} \\ \models_{\mathsf{T}}^{\emptyset} & \lambda y \,.\, \lambda z \,.\, \lambda z \,.\, z & \end{array}$$

Abstract environments

- $(\hat{v}, \hat{\rho}) \models_{\mathsf{V}} v$ means "value v is obtained from $\hat{v}$ by unfolding definitions of $\hat{\rho}$"

$$\frac{v \in \hat{v} \qquad (v, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} v' \qquad \mathrm{fv}\, v' = \emptyset}{(\hat{v}, \hat{\rho}) \models_{\mathsf{V}} v'}$$

Abstract environments

- $(\hat{v}, \hat{\rho}) \models_{\mathsf{V}} v$ means "value v is obtained from $\hat{v}$ by unfolding definitions of $\hat{\rho}$"

$$\frac{v \in \hat{v} \qquad (v, \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} v' \qquad \mathrm{fv}\, v' = \emptyset}{(\hat{v}, \hat{\rho}) \models_{\mathsf{V}} v'}$$

- An environment ρ maps variables to *closed* values (*i.e.*, with no free variables)
- $\hat{\rho} \models_{\mathsf{E}} \rho$ means "environment ρ is obtained by unfolding definitions of $\hat{\rho}$"

$$\frac{\mathrm{dom}\, \rho \subseteq \mathrm{dom}\, \hat{\rho} \qquad \forall \mathsf{x} \in \mathrm{dom}\, \rho,\ (\hat{\rho}(\mathsf{x}), \hat{\rho}) \models_{\mathsf{V}} \rho(\mathsf{x})}{\hat{\rho} \models_{\mathsf{E}} \rho}$$

☞ An abstract environment denotes a set of concrete environments

Examples

$$
\begin{aligned}
\{x \mapsto \{\lambda z\,.\,z,\ \lambda y_1\,.\,\lambda y_2\,.\,y_1\}\} &\models_E \{\} \\
&\models_E \{x \mapsto \lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y_1\,.\,\lambda y_2\,.\,y_1\}
\end{aligned}
$$

Examples

$$
\begin{aligned}
\{x \mapsto \{\lambda z\,.\,z,\ \lambda y_1\,.\,\lambda y_2\,.\,y_1\}\} &\models_E \{\} \\
&\models_E \{x \mapsto \lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y_1\,.\,\lambda y_2\,.\,y_1\}
\end{aligned}
$$

$$
\begin{aligned}
\{x \mapsto \{\lambda z\,.\,z,\ \lambda y\,.\,x\}\} &\models_E \{\} \\
&\models_E \{x \mapsto \lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y\,.\,\lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y\,.\,\lambda y\,.\,\lambda z\,.\,z\} \\
&\models_E \ldots
\end{aligned}
$$

Examples

$$
\begin{aligned}
\{x \mapsto \{\lambda z\,.\,z,\ \lambda y_1\,.\,\lambda y_2\,.\,y_1\}\} &\models_E \{\} \\
&\models_E \{x \mapsto \lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y_1\,.\,\lambda y_2\,.\,y_1\}
\end{aligned}
$$

$$
\begin{aligned}
\{x \mapsto \{\lambda z\,.\,z,\ \lambda y\,.\,x\}\} &\models_E \{\} \\
&\models_E \{x \mapsto \lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y\,.\,\lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y\,.\,\lambda y\,.\,\lambda z\,.\,z\} \\
&\models_E \ldots
\end{aligned}
$$

$$
\begin{aligned}
\{x \mapsto \emptyset; y \mapsto \{\lambda z\,.\,z\}\} &\models_E \{\} \\
&\models_E \{y \mapsto \lambda z\,.\,z\}
\end{aligned}
$$

Examples

$$
\begin{aligned}
\{x \mapsto \{\lambda z\,.\,z,\ \lambda y_1\,.\,\lambda y_2\,.\,y_1\}\} &\models_E \{\} \\
&\models_E \{x \mapsto \lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y_1\,.\,\lambda y_2\,.\,y_1\}
\end{aligned}
$$

$$
\begin{aligned}
\{x \mapsto \{\lambda z\,.\,z,\ \lambda y\,.\,x\}\} &\models_E \{\} \\
&\models_E \{x \mapsto \lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y\,.\,\lambda z\,.\,z\} \\
&\models_E \{x \mapsto \lambda y\,.\,\lambda y\,.\,\lambda z\,.\,z\} \\
&\models_E \ldots
\end{aligned}
$$

$$
\begin{aligned}
\{x \mapsto \emptyset; y \mapsto \{\lambda z\,.\,z\}\} &\models_E \{\} \\
&\models_E \{y \mapsto \lambda z\,.\,z\}
\end{aligned}
$$

$$
\begin{aligned}
\{x \mapsto \{\lambda z\,.\,x\}; y \mapsto \{\lambda z\,.\,z\}\} &\models_E \{\} \\
&\models_E \{y \mapsto \lambda z\,.\,z\}
\end{aligned}
$$

Soundness 0-CFA

An environment acts on a term by substituting its free variables:

$$\mathsf{x}[\rho] \triangleq \begin{cases} \rho(\mathsf{x}) & \text{if } \mathsf{x} \in \operatorname{dom} \rho \\ \mathsf{x} & \text{otherwise} \end{cases}$$

$$\begin{aligned} (\lambda \mathsf{x} \,.\, t)[\rho] &\triangleq \lambda \mathsf{x} \,.\, (t[\rho \setminus \mathsf{x}]) \\ (t_1\ t_2)[\rho] &\triangleq (t_1[\rho])\ (t_2[\rho]) \\ (t)^p\,[\rho] &\triangleq (t[\rho])^p \end{aligned}$$

An environment acts on a term by substituting its free variables:

$$\mathrm{x}[\rho] \triangleq \begin{cases} \rho(\mathrm{x}) & \text{if } \mathrm{x} \in \operatorname{dom}\rho \\ \mathrm{x} & \text{otherwise} \end{cases}$$

$$\begin{aligned} (\lambda \mathrm{x}\,.\,t)[\rho] &\triangleq \lambda \mathrm{x}\,.\,(t[\rho \setminus \mathrm{x}]) \\ (t_1\ t_2)[\rho] &\triangleq (t_1[\rho])\ (t_2[\rho]) \\ (t)^p\,[\rho] &\triangleq (t[\rho])^p \end{aligned}$$

Theorem 5 (Soundness)

If $(\hat{\mathrm{C}}, \hat{\rho}) \models (t)^p$ *and* $\hat{\rho} \models_{\mathrm{E}} \rho$ *and* $\mathrm{fv}\,t \subseteq \operatorname{dom}\rho$ *and* $t[\rho] \to^* v$, *then* $\left(\hat{\mathrm{C}}(p), \hat{\rho}\right) \models_{\mathrm{V}} v$

An environment acts on a term by substituting its free variables:

$$x[\rho] \triangleq \begin{cases} \rho(x) & \text{if } x \in \operatorname{dom}\rho \\ x & \text{otherwise} \end{cases}$$

$$\begin{aligned} (\lambda x\,.\,t)[\rho] &\triangleq \lambda x\,.\,(t[\rho \setminus x]) \\ (t_1\ t_2)[\rho] &\triangleq (t_1[\rho])\ (t_2[\rho]) \\ (t)^p\,[\rho] &\triangleq (t[\rho])^p \end{aligned}$$

Theorem 5 (Soundness)

If $(\hat{C}, \hat{\rho}) \models (t)^p$ *and* $\hat{\rho} \models_E \rho$ *and* $\operatorname{fv} t \subseteq \operatorname{dom}\rho$ *and* $t[\rho] \to^* v$, *then* $\left(\hat{C}(p), \hat{\rho}\right) \models_V v$

Informal interpretation:

"if $(\hat{C}, \hat{\rho})$ is a valid 0-CFA solution for the program $(t)^p$,
if we replace the *inputs* (*i.e.*, the free variables) of t with values allowed by $\hat{\rho}$,
then the value produced by t belongs to the set of possible values for the label p"

Soundness 0-CFA

An environment acts on a term by substituting its free variables:

$$x[\rho] \triangleq \begin{cases} \rho(x) & \text{if } x \in \operatorname{dom}\rho \\ x & \text{otherwise} \end{cases}$$

$$\begin{aligned} (\lambda x\,.\,t)[\rho] &\triangleq \lambda x\,.\,(t[\rho \setminus x]) \\ (t_1\ t_2)[\rho] &\triangleq (t_1[\rho])\ (t_2[\rho]) \\ (t)^p\,[\rho] &\triangleq (t[\rho])^p \end{aligned}$$

Theorem 5 (Soundness)

If $(\hat{C}, \hat{\rho}) \models (t)^p$ *and* $\hat{\rho} \models_E \rho$ *and* $\operatorname{fv} t \subseteq \operatorname{dom}\rho$ *and* $t[\rho] \to^* v$, *then* $\left(\hat{C}(p), \hat{\rho}\right) \models_V v$

Informal interpretation:

"if $(\hat{C}, \hat{\rho})$ is a valid 0-CFA solution for the program $(t)^p$,
if we replace the *inputs* (*i.e.*, the free variables) of t with values allowed by $\hat{\rho}$,
then the value produced by t belongs to the set of possible values for the label p"

Corollary 6

If $(\hat{C}, \hat{\rho}) \models (t)^p$ *and* $\operatorname{fv} t = \emptyset$ *and* $t \to^* v$, *then* $\left(\hat{C}(p), \hat{\rho}\right) \models_V v$

Soundness of 0-CFA (continued)

The structure of the proof is similar to the soundness proof for the simply-typed λ-calculus (based preservation and progress)

Soundness of 0-CFA (continued)

The structure of the proof is similar to the soundness proof for the simply-typed λ-calculus (based preservation and progress)

Lemma 7 (Acceptability is invariant by reduction)

Assume $(\hat{\mathsf{C}}, \hat{\rho}) \models (t_1)^p$ *and* $(t_1, \hat{\rho}) \models^{\emptyset}_{\mathsf{T}} t_1'$*:*
If $t_1' \to t_2'$*, then there exists* t_2 *such that* $(\hat{\mathsf{C}}, \hat{\rho}) \models (t_2)^p$ *and* $(t_2, \hat{\rho}) \models^{\emptyset}_{\mathsf{T}} t_2'$

Soundness of 0-CFA (continued)

The structure of the proof is similar to the soundness proof for the simply-typed λ-calculus (based preservation and progress)

Lemma 7 (Acceptability is invariant by reduction)

Assume $(\hat{\mathrm{C}}, \hat{\rho}) \models (t_1)^p$ *and* $(t_1, \hat{\rho}) \models_{\mathrm{T}}^{\emptyset} t_1'$*:*
If $t_1' \to t_2'$*, then there exists* t_2 *such that* $(\hat{\mathrm{C}}, \hat{\rho}) \models (t_2)^p$ *and* $(t_2, \hat{\rho}) \models_{\mathrm{T}}^{\emptyset} t_2'$

Lemma 8 (Value acceptability)

Assume $(\hat{\mathrm{C}}, \hat{\rho}) \models (t)^p$ *and* $(t, \hat{\rho}) \models_{\mathrm{T}}^{\emptyset} v$ *and* $\mathrm{fv}\, v = \emptyset$*. Then,* $\left(\hat{\mathrm{C}}(p), \hat{\rho}\right) \models_{\mathrm{V}} v$

Example for Lemma 7

$$\hat{\rho}(x_1) = \left\{ \lambda y.\ (\lambda z.\, y^3)^4 \right\}$$
$$\hat{\rho}(x_2) = \emptyset$$
$$\hat{\rho}(y) = \left\{ \lambda x_2.\, x_2^7 \right\}$$
$$\hat{\rho}(z) = \emptyset$$

$$\hat{C}(9) = \left\{ \lambda z.\, y^3 \right\}$$

$$t_1' = \left(\left((\lambda x_1.\, x_1^1)^2 \left(\lambda y.\ (\lambda z.\, y^3)^4 \right)^5 \right)^6 (\lambda x_2.\, x_2^7)^8 \right)^9$$

Example for Lemma 7

$$\hat{\rho}(x_1) = \left\{ \lambda y.\ \left(\lambda z.\, y^3\right)^4 \right\} \qquad \hat{C}(9) = \left\{ \lambda z.\, y^3 \right\}$$
$$\hat{\rho}(x_2) = \emptyset$$
$$\hat{\rho}(y) = \left\{ \lambda x_2.\, x_2^7 \right\}$$
$$\hat{\rho}(z) = \emptyset$$

$$t_1' = \left(\left(\left(\lambda x_1.\, x_1^1\right)^2 \left(\lambda y.\ \left(\lambda z.\, y^3\right)^4 \right)^5 \right)^6 \left(\lambda x_2.\, x_2^7\right)^8 \right)^9 \qquad (t_1', \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t_1'$$

Example for Lemma 7

$$\hat{\rho}(x_1) = \left\{ \lambda y.\ \left(\lambda z.\, y^3\right)^4 \right\} \qquad \hat{C}(9) = \left\{ \lambda z.\, y^3 \right\}$$
$$\hat{\rho}(x_2) = \emptyset$$
$$\hat{\rho}(y) = \left\{ \lambda x_2.\, x_2^7 \right\}$$
$$\hat{\rho}(z) = \emptyset$$

$$t_1' = \left(\left(\left(\lambda x_1.\, x_1^1\right)^2 \left(\lambda y.\ \left(\lambda z.\, y^3\right)^4 \right)^5 \right)^6 \left(\lambda x_2.\, x_2^7\right)^8 \right)^9 \qquad (t_1', \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t_1'$$

$$\rightarrow \quad t_2' = \left(\left(\lambda y.\ \left(\lambda z.\, y^3\right)^4 \right)^6 \left(\lambda x_2.\, x_2^7\right)^8 \right)^9$$

Example for Lemma 7

$$\hat{\rho}(x_1) = \left\{\lambda y.\ (\lambda z.\, y^3)^4\right\} \qquad \hat{C}(9) = \left\{\lambda z.\, y^3\right\}$$
$$\hat{\rho}(x_2) = \emptyset$$
$$\hat{\rho}(y) = \left\{\lambda x_2.\, x_2^7\right\}$$
$$\hat{\rho}(z) = \emptyset$$

$$t_1' = \left(\left((\lambda x_1.\, x_1^1)^2\ \left(\lambda y.\ (\lambda z.\, y^3)^4\right)^5\right)^6\ (\lambda x_2.\, x_2^7)^8\right)^9 \qquad (t_1', \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t_1'$$

$$\rightarrow\ t_2' = \left(\left(\lambda y.\ (\lambda z.\, y^3)^4\right)^6\ (\lambda x_2.\, x_2^7)^8\right)^9 \qquad \left(\left(x_1^6\ (\lambda x_2.\, x_2^7)^8\right)^9, \hat{\rho}\right) \models_{\mathsf{T}}^{\emptyset} t_2'$$

Example for Lemma 7

$$\hat{\rho}(x_1) = \left\{\lambda y.\ (\lambda z.\, y^3)^4\right\} \qquad \hat{C}(9) = \left\{\lambda z.\, y^3\right\}$$
$$\hat{\rho}(x_2) = \emptyset$$
$$\hat{\rho}(y) = \left\{\lambda x_2.\, x_2^7\right\}$$
$$\hat{\rho}(z) = \emptyset$$

$$t_1' = \left(\left((\lambda x_1.\, x_1^1)^2\ \left(\lambda y.\ (\lambda z.\, y^3)^4\right)^5\right)^6\ (\lambda x_2.\, x_2^7)^8\right)^9 \qquad (t_1', \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t_1'$$

$$\to\ t_2' = \left(\left(\lambda y.\ (\lambda z.\, y^3)^4\right)^6\ (\lambda x_2.\, x_2^7)^8\right)^9 \qquad \left(\left(x_1^6\ (\lambda x_2.\, x_2^7)^8\right)^9, \hat{\rho}\right) \models_{\mathsf{T}}^{\emptyset} t_2'$$

$$\to\ t_3' = \left(\lambda z.\ (\lambda x_2.\, x_2^7)^3\right)^9$$

Example for Lemma 7

$$\hat{\rho}(x_1) = \left\{\lambda y.\ (\lambda z.\, y^3)^4\right\} \qquad \hat{C}(9) = \left\{\lambda z.\, y^3\right\}$$
$$\hat{\rho}(x_2) = \emptyset$$
$$\hat{\rho}(y) = \left\{\lambda x_2.\, x_2^7\right\}$$
$$\hat{\rho}(z) = \emptyset$$

$$t_1' = \left(\left((\lambda x_1.\, x_1^1)^2\ \left(\lambda y.\ (\lambda z.\, y^3)^4\right)^5\right)^6\ (\lambda x_2.\, x_2^7)^8\right)^9 \qquad (t_1', \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t_1'$$

$$\to\ t_2' = \left(\left(\lambda y.\ (\lambda z.\, y^3)^4\right)^6\ (\lambda x_2.\, x_2^7)^8\right)^9 \qquad \left(\left(x_1^6\ (\lambda x_2.\, x_2^7)^8\right)^9, \hat{\rho}\right) \models_{\mathsf{T}}^{\emptyset} t_2'$$

$$\to\ t_3' = \left(\lambda z.\ (\lambda x_2.\, x_2^7)^3\right)^9 \qquad \left((\lambda z.\, y^3)^9, \hat{\rho}\right) \models_{\mathsf{T}} t_3'$$

Example for Lemma 7

$$\hat{\rho}(x_1) = \left\{\lambda y.\ \left(\lambda z.\, y^3\right)^4\right\} \qquad \hat{C}(9) = \left\{\lambda z.\, y^3\right\}$$
$$\hat{\rho}(x_2) = \emptyset$$
$$\hat{\rho}(y) = \left\{\lambda x_2.\, x_2^7\right\}$$
$$\hat{\rho}(z) = \emptyset$$

$$t_1' = \left(\left(\left(\lambda x_1.\, x_1^1\right)^2 \left(\lambda y.\ \left(\lambda z.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2.\, x_2^7\right)^8\right)^9 \qquad (t_1', \hat{\rho}) \models_{\mathsf{T}}^{\emptyset} t_1'$$

$$\to\ t_2' = \left(\left(\lambda y.\ \left(\lambda z.\, y^3\right)^4\right)^6 \left(\lambda x_2.\, x_2^7\right)^8\right)^9 \qquad \left(\left(x_1^6\ \left(\lambda x_2.\, x_2^7\right)^8\right)^9, \hat{\rho}\right) \models_{\mathsf{T}}^{\emptyset} t_2'$$

$$\to\ t_3' = \left(\lambda z.\ \left(\lambda x_2.\, x_2^7\right)^3\right)^9 \qquad \left(\left(\lambda z.\, y^3\right)^9, \hat{\rho}\right) \models_{\mathsf{T}} t_3'$$

and by Lemma 8: $\left(\hat{C}(9), \hat{\rho}\right) \models_{\mathsf{V}} t_3'$

Some key lemmas for the proof of soundness for 0-CFA

Lemma 9 (Acceptability weakening)

If $(\hat{\mathsf{C}}, \hat{\rho}) \models (t)^{p_1}$ *and* $\hat{\mathsf{C}}(p_1) \subseteq \hat{\mathsf{C}}(p_2)$*, then* $(\hat{\mathsf{C}}, \hat{\rho}) \models (t)^{p_2}$

Lemma 10 (Value denotation weakening)

If $(\hat{v}_1, \hat{\rho}) \models_{\mathsf{V}} v$ *and* $\hat{v}_1 \subseteq \hat{v}_2$ *then* $(\hat{v}_2, \hat{\rho}) \models_{\mathsf{V}} v$

Lemma 11 (Term denotation weakening)

If $(t, \hat{\rho}) \models_{\mathsf{T}}^{X_1} t'$ *and* $X_2 \subseteq X_1$ *then* $(t, \hat{\rho}) \models_{\mathsf{T}}^{X_2} t'$

Lemma 12 (Term denotation substitution)

If $(t, \hat{\rho}) \models_{\mathsf{T}}^{X} t_1$ *and* $(\hat{\rho}(\mathsf{x}), \hat{\rho}) \models_{\mathsf{V}} t_2$ *and* $(t, \hat{\rho}) \models_{\mathsf{T}}^{X \setminus \{\mathsf{x}\}} t_1[\mathsf{x} \leftarrow t_2]$

Lemma 13 (Matching lemma)

If $\hat{\rho} \models_{\mathsf{E}} \rho$ *and* $X \cap \operatorname{dom} \rho = \emptyset$*, then* $(t, \hat{\rho}) \models_{\mathsf{T}}^{X} t[\rho]$

0-CFA as Abstract Interpretation

Theorem 5 (Soundness)

If $(\hat{\mathsf{C}}, \hat{\rho}) \models (t)^p$ *and* $\hat{\rho} \models_{\mathsf{E}} \rho$ *and* $\mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho$ *and* $t[\rho] \to^* v$, *then* $\left(\hat{\mathsf{C}}(p), \hat{\rho}\right) \models_{\mathsf{V}} v$

Some shortcomings about the standard presentation of 0-CFA:

- The soundness theorem only talks about the *final* value!
- The soundness theorem does not tell explicitly that $\hat{\rho}$ describes the possible instantiations of the variables that occur during evaluation!
- The rules give no explicit method to compute a solution
- There is no explanation of how to obtain the correct rules

Theorem 5 (Soundness)

If $(\hat{\mathsf{C}}, \hat{\rho}) \models (t)^p$ *and* $\hat{\rho} \models_{\mathsf{E}} \rho$ *and* $\mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho$ *and* $t[\rho] \to^* v$, *then* $\left(\hat{\mathsf{C}}(p), \hat{\rho}\right) \models_{\mathsf{V}} v$

Some shortcomings about the standard presentation of 0-CFA:

- The soundness theorem only talks about the *final* value!
- The soundness theorem does not tell explicitly that $\hat{\rho}$ describes the possible instantiations of the variables that occur during evaluation!
- The rules give no explicit method to compute a solution
- There is no explanation of how to obtain the correct rules

Abstract Interpretation: A *systematic* approach to design a static analysis:

- Is rooted in semantics
- Is guided by abstractions, in the form of Galois connections:

$$(A, \sqsubseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A^\sharp, \sqsubseteq^\sharp)$$

- Gives satisfactory answers to the 4 remarks from above

Small-step semantics

The small-step semantics is a *labelled transition system* (LTS)

It produces a **trace** of events of the form $t_1 \xrightarrow{tr}{}^* t_2$ that describes:

- which β-reductions have happened: $\beta(\lambda x\,.\,t,\, v)$
- which values were produced by a program point: $\mathrm{return}\,(p,\, v)$

The trace represents the *history* of the evaluation

Small-step semantics

The small-step semantics is a *labelled transition system* (LTS)

It produces a **trace** of events of the form $t_1 \xrightarrow{tr}{}^{*} t_2$ that describes:

- which β-reductions have happened: $\beta(\lambda x\,.\,t,\, v)$
- which values were produced by a program point: $\text{return}\,(p,\, v)$

The trace represents the *history* of the evaluation

$$\textsc{BetaV}\ \frac{}{(\lambda x\,.\,t)\,v \xrightarrow{\beta(\lambda x\,.\,t,\,v)} t[x \leftarrow v]} \qquad \textsc{Annot}\ \frac{}{(v)^{p} \xrightarrow{\text{return}(p,\,v)} v}$$

Small-step semantics

The small-step semantics is a *labelled transition system* (LTS)

It produces a **trace** of events of the form $t_1 \xrightarrow{tr}{}^{*} t_2$ that describes:

- which β-reductions have happened: $\beta(\lambda x\,.\,t,\, v)$
- which values were produced by a program point: $\text{return}\,(p,\, v)$

The trace represents the *history* of the evaluation

$$\textsc{BetaV}\ \frac{}{(\lambda x\,.\,t)\,v \xrightarrow{\beta(\lambda x\,.\,t,\,v)} t[x \leftarrow v]} \qquad \textsc{Annot}\ \frac{}{(v)^p \xrightarrow{\text{return}(p,\,v)} v}$$

$$\textsc{AppCtxtL}\ \frac{t_1 \xrightarrow{e} t_1'}{t_1\,t_2 \xrightarrow{e} t_1'\,t_2} \qquad \textsc{AppCtxtR}\ \frac{t \xrightarrow{e} t'}{v\,t \xrightarrow{e} v\,t'} \qquad \textsc{AnnotCtxt}\ \frac{t \xrightarrow{e} t'}{(t)^p \xrightarrow{e} \left(t'\right)^p}$$

Small-step semantics

The small-step semantics is a *labelled transition system* (LTS)

It produces a **trace** of events of the form $t_1 \xrightarrow{tr}{}^{*} t_2$ that describes:

- which β-reductions have happened: $\beta(\lambda x\,.\,t,\, v)$
- which values were produced by a program point: $\mathrm{return}\,(p,\, v)$

The trace represents the *history* of the evaluation

$$\textsc{BetaV}\ \frac{}{(\lambda x\,.\,t)\,v \xrightarrow{\beta(\lambda x\,.\,t,\,v)} t[x \leftarrow v]} \qquad \textsc{Annot}\ \frac{}{(v)^p \xrightarrow{\mathrm{return}(p,\,v)} v}$$

$$\textsc{AppCtxtL}\ \frac{t_1 \xrightarrow{e} t_1'}{t_1\,t_2 \xrightarrow{e} t_1'\,t_2} \qquad \textsc{AppCtxtR}\ \frac{t \xrightarrow{e} t'}{v\,t \xrightarrow{e} v\,t'} \qquad \textsc{AnnotCtxt}\ \frac{t \xrightarrow{e} t'}{(t)^p \xrightarrow{e} (t')^p}$$

$$\textsc{Refl}\ \frac{}{t \xrightarrow{\varepsilon}{}^{*} t} \qquad \textsc{Step}\ \frac{t_1 \xrightarrow{e} t_2 \qquad t_2 \xrightarrow{tr}{}^{*} t_3}{t_1 \xrightarrow{e +\!\!+ tr}{}^{*} t_3}$$

Exercises

Exercise 6.1

Reduce to its normal form the following term

$$\left(\left(\left(\lambda f\,.\,\left(\lambda x\,.\,\left(f^{1}\,x^{2}\right)^{3}\right)^{4}\right)^{5}\,\left(\lambda x\,.\,\left(\lambda y\,.\,x^{6}\right)^{7}\right)^{8}\right)^{9}\,\left(\left(\lambda y\,.\,y^{10}\right)^{11}\,\left(\lambda z\,.\,z^{12}\right)^{13}\right)^{14}\right)^{15}$$

What are the differences with the first semantics we gave in this course?

Roadmap

Abstract caches and environments

$$(\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$

Sets of traces

$$\wp(\mathcal{X} \to \mathcal{V}) \to \wp(\mathcal{T})$$

Roadmap

Abstract caches and environments

$$(\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$

Sets of traces

$$\wp(\mathcal{X} \to \mathcal{V}) \to \wp(\mathcal{T})$$

Roadmap

Abstract caches and environments

$$(\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$

Environments as inputs

$$(\mathcal{X} \to \wp(\mathcal{V})) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Sets of caches and sets of environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp(\mathcal{P} \to \wp(\mathcal{V})) \times \wp(\mathcal{X} \to \wp(\mathcal{V})))$$

Sets of caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))))$$

Sets of traces

$$\wp(\mathcal{X} \to \mathcal{V}) \to \wp(\mathcal{T})$$

Collecting Semantics

Recall: environments are maps from variables to closed values

Collecting semantics: $\mathbb{T}[\![t]\!] : \{\rho \mid \mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho\} \to \wp(\mathcal{T})$

$$\mathbb{T}[\![t]\!](\mathcal{I}) \triangleq \bigcup_{\rho \in \mathcal{I}} \left\{ tr \mid t[\rho] \xrightarrow{tr}{}^{*} v \right\}$$

Collecting Semantics

Recall: environments are maps from variables to closed values

Collecting semantics: $\mathbb{T}[\![t]\!] : \{\rho \mid \mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho\} \to \wp(\mathcal{T})$

$$\mathbb{T}[\![t]\!](\mathcal{I}) \triangleq \bigcup_{\rho \in \mathcal{I}} \left\{ tr \mid t[\rho] \xrightarrow{tr}{}^{*} v \right\}$$

The following inclusions are satisfied:

$$\mathbb{T}[\![\mathsf{x}^p]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathsf{return}\,(p,\, \rho(\mathsf{x}))\}$$

Collecting Semantics

Recall: environments are maps from variables to closed values

Collecting semantics: $\mathbb{T}[\![t]\!] : \{\rho \mid \mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho\} \to \wp(\mathcal{T})$

$$\mathbb{T}[\![t]\!](\mathcal{I}) \triangleq \bigcup_{\rho \in \mathcal{I}} \left\{ tr \mid t[\rho] \xrightarrow{tr}{}^{*} v \right\}$$

The following inclusions are satisfied:

$$\mathbb{T}[\![\mathsf{x}^p]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathsf{return}\,(p,\, \rho(\mathsf{x}))\}$$

$$\mathbb{T}[\![\,(\lambda \mathsf{x}\,.\,t)^p\,]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathsf{return}\,(p,\, (\lambda \mathsf{x}\,.\,t)[\rho])\}$$

Collecting Semantics

Recall: environments are maps from variables to closed values

Collecting semantics: $\mathbb{T}[\![t]\!] : \{\rho \mid \mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho\} \to \wp(\mathcal{T})$

$$\mathbb{T}[\![t]\!](\mathcal{I}) \triangleq \bigcup_{\rho \in \mathcal{I}} \left\{ tr \mid t[\rho] \xrightarrow{tr}{}^{*} v \right\}$$

The following inclusions are satisfied:

$$\mathbb{T}[\![\mathsf{x}^p]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathsf{return}\,(p,\, \rho(\mathsf{x}))\}$$

$$\mathbb{T}[\![\,(\lambda \mathsf{x}\,.\,t)^p\,]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathsf{return}\,(p,\, (\lambda \mathsf{x}\,.\,t)[\rho])\}$$

$$\mathbb{T}[\![\,((t_1)^{p_1}\ (t_2)^{p_2})^p\,]\!](\mathcal{I}) \subseteq$$

$$\left\{ tr_1 +\!\!+ \mathsf{return}\,(p_1,\, \lambda \mathsf{x}\,.\,(t_0)^{p_0}) \;\middle|\; tr_1 +\!\!+ \mathsf{return}\,(p_1,\, \lambda \mathsf{x}\,.\,(t_0)^{p_0}) \in \mathbb{T}[\![\,(t_1)^{p_1}\,]\!](\mathcal{I}), \right\}$$

Collecting Semantics

Recall: environments are maps from variables to closed values

Collecting semantics: $\mathbb{T}[\![t]\!] : \{\rho \mid \mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho\} \to \wp(\mathcal{T})$

$$\mathbb{T}[\![t]\!](\mathcal{I}) \triangleq \bigcup_{\rho \in \mathcal{I}} \left\{ tr \mid t[\rho] \xrightarrow{tr}{}^{*} v \right\}$$

The following inclusions are satisfied:

$$\mathbb{T}[\![\mathrm{x}^{p}]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathrm{return}\,(p,\, \rho(\mathrm{x}))\}$$

$$\mathbb{T}[\![\,(\lambda \mathrm{x}\,.\,t)^{p}\,]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathrm{return}\,(p,\, (\lambda \mathrm{x}\,.\,t)[\rho])\}$$

$$\mathbb{T}[\![\,((t_1)^{p_1}\ (t_2)^{p_2})^{p}\,]\!](\mathcal{I}) \subseteq$$

$$\left\{ \begin{array}{l} tr_1 +\!\!+ \mathrm{return}\,(p_1,\, \lambda \mathrm{x}\,.\,(t_0)^{p_0}) \\ +\!\!+\, tr_2 +\!\!+ \mathrm{return}\,(p_2,\, v_2) \end{array} \middle| \begin{array}{l} tr_1 +\!\!+ \mathrm{return}\,(p_1,\, \lambda \mathrm{x}\,.\,(t_0)^{p_0}) \in \mathbb{T}[\![\,(t_1)^{p_1}\,]\!](\mathcal{I}), \\ tr_2 +\!\!+ \mathrm{return}\,(p_2,\, v_2) \in \mathbb{T}[\![\,(t_2)^{p_2}\,]\!](\mathcal{I}), \end{array} \right\}$$

Collecting Semantics

Recall: environments are maps from variables to closed values

Collecting semantics: $\mathbb{T}[\![t]\!] : \{\rho \mid \mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho\} \to \wp(\mathcal{T})$

$$\mathbb{T}[\![t]\!](\mathcal{I}) \triangleq \bigcup_{\rho \in \mathcal{I}} \left\{ tr \mid t[\rho] \xrightarrow{tr}{}^{*} v \right\}$$

The following inclusions are satisfied:

$$\mathbb{T}[\![\mathrm{x}^{p}]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathrm{return}\,(p,\, \rho(\mathrm{x}))\}$$

$$\mathbb{T}[\![\,(\lambda \mathrm{x}\,.\,t)^{p}\,]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathrm{return}\,(p,\, (\lambda \mathrm{x}\,.\,t)[\rho])\}$$

$$\mathbb{T}[\![\,\left((t_1)^{p_1}\ (t_2)^{p_2}\right)^{p}\,]\!](\mathcal{I}) \subseteq$$

$$\left\{ \begin{array}{l} tr_1 +\!\!+ \mathrm{return}\left(p_1,\, \lambda \mathrm{x}\,.\,(t_0)^{p_0}\right) \\ +\!\!+\, tr_2 +\!\!+ \mathrm{return}\,(p_2,\, v_2) \\ +\!\!+\, \beta\left(\lambda \mathrm{x}\,.\,(t_0)^{p_0},\, v_2\right) \end{array} \middle| \begin{array}{l} tr_1 +\!\!+ \mathrm{return}\left(p_1,\, \lambda \mathrm{x}\,.\,(t_0)^{p_0}\right) \in \mathbb{T}[\![\,(t_1)^{p_1}\,]\!](\mathcal{I}), \\ tr_2 +\!\!+ \mathrm{return}\,(p_2,\, v_2) \in \mathbb{T}[\![\,(t_2)^{p_2}\,]\!](\mathcal{I}), \end{array} \right\}$$

Collecting Semantics

Recall: environments are maps from variables to closed values

Collecting semantics: $\mathbb{T}[\![t]\!] : \{\rho \mid \mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho\} \to \wp(\mathcal{T})$

$$\mathbb{T}[\![t]\!](\mathcal{I}) \triangleq \bigcup_{\rho \in \mathcal{I}} \left\{ tr \mid t[\rho] \xrightarrow{tr}{}^{*} v \right\}$$

The following inclusions are satisfied:

$$\mathbb{T}[\![\mathsf{x}^p]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathrm{return}\,(p,\, \rho(\mathsf{x}))\}$$

$$\mathbb{T}[\![\,(\lambda \mathsf{x}\,.\,t)^p\,]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathrm{return}\,(p,\, (\lambda \mathsf{x}\,.\,t)[\rho])\}$$

$$\mathbb{T}[\![\,\big((t_1)^{p_1}\ (t_2)^{p_2}\big)^p\,]\!](\mathcal{I}) \subseteq$$

$$\left\{ \begin{array}{l} tr_1 +\!\!+ \mathrm{return}\,\big(p_1,\, \lambda \mathsf{x}\,.\,(t_0)^{p_0}\big) \\ \quad +\!\!+ tr_2 +\!\!+ \mathrm{return}\,(p_2,\, v_2) \\ \quad +\!\!+ \beta\big(\lambda \mathsf{x}\,.\,(t_0)^{p_0},\, v_2\big) \\ \quad +\!\!+ tr_0 +\!\!+ \mathrm{return}\,(p_0,\, v_0) \end{array} \;\middle|\; \begin{array}{l} tr_1 +\!\!+ \mathrm{return}\,\big(p_1,\, \lambda \mathsf{x}\,.\,(t_0)^{p_0}\big) \in \mathbb{T}[\![\,(t_1)^{p_1}\,]\!](\mathcal{I}), \\ tr_2 +\!\!+ \mathrm{return}\,(p_2,\, v_2) \in \mathbb{T}[\![\,(t_2)^{p_2}\,]\!](\mathcal{I}), \\ tr_0 +\!\!+ \mathrm{return}\,(p_0,\, v_0) \in \mathbb{T}[\![\,(t_0)^{p_0}\,]\!](\mathcal{I}[\mathsf{x} \mapsto \{v_2\}]) \end{array} \right\}$$

where $\mathcal{I}[\mathsf{x} \mapsto S] = \{\rho[\mathsf{x} \mapsto v] \mid \rho \in \mathcal{I}, v \in S\}$

Collecting Semantics

Recall: environments are maps from variables to closed values

Collecting semantics: $\mathbb{T}[\![t]\!] : \{\rho \mid \mathrm{fv}\, t \subseteq \mathrm{dom}\, \rho\} \to \wp(\mathcal{T})$

$$\mathbb{T}[\![t]\!](\mathcal{I}) \triangleq \bigcup_{\rho \in \mathcal{I}} \left\{ tr \mid t[\rho] \xrightarrow{tr}{}^{*} v \right\}$$

The following inclusions are satisfied:

$$\mathbb{T}[\![\mathsf{x}^p]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathrm{return}\,(p,\, \rho(\mathsf{x}))\}$$

$$\mathbb{T}[\![\,(\lambda \mathsf{x}\,.\,t)^p\,]\!](\mathcal{I}) = \bigcup_{\rho \in \mathcal{I}} \{\mathrm{return}\,(p,\, (\lambda \mathsf{x}\,.\,t)[\rho])\}$$

$$\mathbb{T}[\![\,\big((t_1)^{p_1}\ (t_2)^{p_2}\big)^p\,]\!](\mathcal{I}) \subseteq$$

$$\left\{ \begin{array}{l} tr_1 +\!\!+ \mathrm{return}\,\big(p_1,\, \lambda \mathsf{x}\,.\,(t_0)^{p_0}\big) \\ \quad +\!\!+\, tr_2 +\!\!+ \mathrm{return}\,(p_2,\, v_2) \\ \quad +\!\!+\, \beta\big(\lambda \mathsf{x}\,.\,(t_0)^{p_0}\,,\, v_2\big) \\ \quad +\!\!+\, tr_0 +\!\!+ \mathrm{return}\,(p_0,\, v_0) \\ \quad +\!\!+\, \mathrm{return}\,(p,\, v_0) \end{array} \;\middle|\; \begin{array}{l} tr_1 +\!\!+ \mathrm{return}\,\big(p_1,\, \lambda \mathsf{x}\,.\,(t_0)^{p_0}\big) \in \mathbb{T}[\![\,(t_1)^{p_1}\,]\!](\mathcal{I}), \\ tr_2 +\!\!+ \mathrm{return}\,(p_2,\, v_2) \in \mathbb{T}[\![\,(t_2)^{p_2}\,]\!](\mathcal{I}), \\ tr_0 +\!\!+ \mathrm{return}\,(p_0,\, v_0) \in \mathbb{T}[\![\,(t_0)^{p_0}\,]\!](\mathcal{I}[\mathsf{x} \mapsto \{v_2\}]) \end{array} \right\}$$

where $\mathcal{I}[\mathsf{x} \mapsto S] = \{\rho[\mathsf{x} \mapsto v] \mid \rho \in \mathcal{I}, v \in S\}$

Roadmap

Abstract caches and environments

$$(\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$

Environments as inputs

$$(\mathcal{X} \to \wp(\mathcal{V})) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Sets of caches and sets of environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp(\mathcal{P} \to \wp(\mathcal{V})) \times \wp(\mathcal{X} \to \wp(\mathcal{V})))$$

Sets of caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))))$$

History

Sets of traces

$$\wp(\mathcal{X} \to \mathcal{V}) \to \wp(\mathcal{T})$$

From Traces to Caches and Environments

Set-valued functions form a complete lattice:

$$
\begin{array}{rcl}
\bot & \triangleq & \lambda k.\, \emptyset \\
\{k \mapsto S\} & \triangleq & \lambda k'.\, \text{if } k' = k \text{ then } S \text{ else } \emptyset \\
m_1 \,\dot{\cup}\, m_2 & \triangleq & \lambda k.\, m_1(k) \cup m_2(k) \\
m_1 \,\dot{\subseteq}\, m_2 & \triangleq & \forall k,\, m_1(k) \subseteq m_2(k)
\end{array}
$$

From Traces to Caches and Environments

Set-valued functions form a complete lattice:

$$\begin{array}{rcl} \bot & \triangleq & \lambda k.\, \emptyset \\ \{k \mapsto S\} & \triangleq & \lambda k'.\, \text{if } k' = k \text{ then } S \text{ else } \emptyset \\ m_1 \dot{\cup} m_2 & \triangleq & \lambda k.\, m_1(k) \cup m_2(k) \\ m_1 \dot{\subseteq} m_2 & \triangleq & \forall k,\, m_1(k) \subseteq m_2(k) \end{array}$$

Retrieving caches:

$$\begin{array}{rcl} \mathrm{cache}(\beta(\lambda x\,.\,t,\, v)) & \triangleq & \bot \\ \mathrm{cache}(\mathsf{return}\,(p,\, v)) & \triangleq & \{p \mapsto \{v\}\} \end{array} \qquad \begin{array}{rcl} \mathrm{cache}(\varepsilon) & \triangleq & \bot \\ \mathrm{cache}(tr_1 +\!\!+ tr_2) & \triangleq & \mathrm{cache}(tr_1) \dot{\cup} \mathrm{cache}(tr_2) \end{array}$$

From Traces to Caches and Environments

Set-valued functions form a complete lattice:

$$\begin{array}{rcl} \bot & \triangleq & \lambda k.\, \emptyset \\ \{k \mapsto S\} & \triangleq & \lambda k'.\, \text{if } k' = k \text{ then } S \text{ else } \emptyset \\ m_1 \,\dot\cup\, m_2 & \triangleq & \lambda k.\, m_1(k) \cup m_2(k) \\ m_1 \,\dot\subseteq\, m_2 & \triangleq & \forall k,\, m_1(k) \subseteq m_2(k) \end{array}$$

Retrieving caches:

$$\begin{array}{rcl} \mathrm{cache}(\beta(\lambda \mathsf{x}\,.\,t,\, v)) & \triangleq & \bot \\ \mathrm{cache}(\mathsf{return}\,(p,\, v)) & \triangleq & \{p \mapsto \{v\}\} \end{array} \qquad \begin{array}{rcl} \mathrm{cache}(\varepsilon) & \triangleq & \bot \\ \mathrm{cache}(tr_1 +\!\!+ tr_2) & \triangleq & \mathrm{cache}(tr_1) \,\dot\cup\, \mathrm{cache}(tr_2) \end{array}$$

Retrieving environments:

$$\begin{array}{rcl} \mathrm{env}(\beta(\lambda \mathsf{x}\,.\,t,\, v)) & \triangleq & \{\mathsf{x} \mapsto \{v\}\} \\ \mathrm{env}(\mathsf{return}\,(p,\, v)) & \triangleq & \bot \end{array} \qquad \begin{array}{rcl} \mathrm{env}(\varepsilon) & \triangleq & \bot \\ \mathrm{env}(tr_1 +\!\!+ tr_2) & \triangleq & \mathrm{env}(tr_1) \,\dot\cup\, \mathrm{env}(tr_2) \end{array}$$

History Abstraction

$$
\begin{array}{rcl}
\alpha_{\mathsf{h}} & : & \wp(\mathcal{T}) \to \wp(\mathcal{C} \times \mathcal{E}) \\
\alpha_{\mathsf{h}}(S) & \triangleq & \{(\mathrm{cache}(tr), \mathrm{env}(tr)) \mid tr \in S\}
\end{array}
$$

$$
\begin{array}{rcl}
\gamma_{\mathsf{h}} & : & \wp(\mathcal{C} \times \mathcal{E}) \to \wp(\mathcal{T}) \\
\gamma_{\mathsf{h}}(S) & \triangleq & \{tr \mid \mathrm{env}\, tr \sqsubseteq \hat{\rho},\ \mathrm{cache}\, tr \sqsubseteq \hat{\mathsf{C}},\ (\hat{\mathsf{C}}, \hat{\rho}) \in S\}
\end{array}
$$

$$
S_1 \sqsubseteq_{\mathsf{h}} S_2 \triangleq \forall (\hat{\mathsf{C}}_1, \hat{\rho}_1) \in S_1,\ \exists (\hat{\mathsf{C}}_2, \hat{\rho}_2) \in S_2,\ \hat{\mathsf{C}}_1 \dot{\subseteq} \hat{\mathsf{C}}_2 \wedge \hat{\rho}_1 \dot{\subseteq} \hat{\rho}_2
$$

We have a Galois connection:

$$
(\wp(\mathcal{T}), \subseteq) \underset{\alpha_{\mathsf{h}}}{\overset{\gamma_{\mathsf{h}}}{\leftrightarrows}} (\wp(\mathcal{C} \times \mathcal{E}), \sqsubseteq_{\mathsf{h}})
$$

Abstract Semantics After History Abstraction

Definition: $\mathbb{T}^{\sharp}_{\mathsf{h}}[\![t]\!] \triangleq \alpha_{\mathsf{h}} \circ \mathbb{T}[\![t]\!]$

Definition: $\mathbb{T}^{\sharp}_{\mathsf{h}}[\![t]\!] \triangleq \alpha_{\mathsf{h}} \circ \mathbb{T}[\![t]\!]$

The following inclusions are satisfied:

$$\mathbb{T}^{\sharp}_{\mathsf{h}}[\![\mathsf{x}^{p}]\!](\mathcal{I}) = \{(\{p \mapsto \{\rho(\mathsf{x})\}\}, \bot) \mid \rho \in \mathcal{I}\}$$

Definition: $\mathbb{T}^\sharp_{\mathsf{h}}[\![t]\!] \triangleq \alpha_{\mathsf{h}} \circ \mathbb{T}[\![t]\!]$

The following inclusions are satisfied:

$$\mathbb{T}^\sharp_{\mathsf{h}}[\![\mathsf{x}^p]\!](\mathcal{I}) = \{(\{p \mapsto \{\rho(\mathsf{x})\}\}, \bot) \mid \rho \in \mathcal{I}\}$$

$$\mathbb{T}^\sharp_{\mathsf{h}}[\![(\lambda \mathsf{x}\,.\,t)^p]\!](\mathcal{I}) = \{(\{p \mapsto \{(\lambda \mathsf{x}\,.\,t)[\rho]\}\}, \bot) \mid \rho \in \mathcal{I}\}$$

Definition: $\mathbb{T}^\sharp_{\mathsf{h}}[\![t]\!] \triangleq \alpha_{\mathsf{h}} \circ \mathbb{T}[\![t]\!]$

The following inclusions are satisfied:

$$\mathbb{T}^\sharp_{\mathsf{h}}[\![\mathsf{x}^p]\!](\mathcal{I}) = \{(\{p \mapsto \{\rho(\mathsf{x})\}\}, \bot) \mid \rho \in \mathcal{I}\}$$

$$\mathbb{T}^\sharp_{\mathsf{h}}[\![(\lambda \mathsf{x}\,.\,t)^p]\!](\mathcal{I}) = \{(\{p \mapsto \{(\lambda \mathsf{x}\,.\,t)[\rho]\}\}, \bot) \mid \rho \in \mathcal{I}\}$$

$$\mathbb{T}^\sharp_{\mathsf{h}}[\![\left((t_1)^{p_1}\ (t_2)^{p_2}\right)^p]\!](\mathcal{I}) \sqsubseteq_{\mathsf{h}} \left\{ \begin{array}{l} (\hat{\mathsf{C}}_1 \dot\cup \hat{\mathsf{C}}_2 \dot\cup \hat{\mathsf{C}}_0 \dot\cup \{p \mapsto \hat{\mathsf{C}}_0(p_0)\}, \\ \hat\rho_1 \dot\cup \hat\rho_2 \dot\cup \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\} \dot\cup \hat\rho_0) \end{array} \middle| \begin{array}{l} (\hat{\mathsf{C}}_1, \hat\rho_1) \in \mathbb{T}^\sharp_{\mathsf{h}}[\![(t_1)^{p_1}]\!](\mathcal{I}), \\ (\hat{\mathsf{C}}_2, \hat\rho_2) \in \mathbb{T}^\sharp_{\mathsf{h}}[\![(t_2)^{p_2}]\!](\mathcal{I}), \\ \lambda \mathsf{x}\,.\,(t_0)^{p_0} \in \hat{\mathsf{C}}_1(p_1), \\ (\hat{\mathsf{C}}_0, \hat\rho_0) \in \mathbb{T}^\sharp_{\mathsf{h}}[\![(t_0)^{p_0}]\!](\mathcal{I}[\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)]) \end{array} \right\}$$

where $\mathcal{I}[\mathsf{x} \mapsto S] = \{\rho[\mathsf{x} \mapsto v] \mid \rho \in \mathcal{I}, v \in S\}$

Roadmap

Abstract caches and environments

$$(\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$

Environments as inputs

$$(\mathcal{X} \to \wp(\mathcal{V})) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Sets of caches and sets of environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp(\mathcal{P} \to \wp(\mathcal{V})) \times \wp(\mathcal{X} \to \wp(\mathcal{V})))$$

Independent Attribute

Sets of caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))))$$

Sets of traces

$$\wp(\mathcal{X} \to \mathcal{V}) \to \wp(\mathcal{T})$$

Independent Attribute Abstraction

$$
\begin{array}{rcl}
\alpha_{\mathsf{ia}} & : & \wp(A \times B) \to \wp(A) \times \wp(B) \\
\alpha_{\mathsf{ia}}(S) & \triangleq & (\{a \mid (a,b) \in S\}, \{b \mid (a,b) \in S\})
\end{array}
$$

$$
\begin{array}{rcl}
\gamma_{\mathsf{ia}} & : & \wp(A) \times \wp(B) \to \wp(A \times B) \\
\gamma_{\mathsf{ia}}(S_A, S_B) & \triangleq & S_A \times S_B
\end{array}
$$

$$
(S_A, S_B) \sqsubseteq_{\mathsf{ia}} (S'_A, S'_B) \triangleq S_A \subseteq S'_A \wedge S_B \subseteq S'_B
$$

We have a Galois connection:

$$
(\wp(A \times B), \subseteq) \underset{\alpha_{\mathsf{ia}}}{\overset{\gamma_{\mathsf{ia}}}{\leftrightarrows}} (\wp(A) \times \wp(B), \sqsubseteq_{\mathsf{ia}})
$$

Composing Abstractions on Pairs

Given two Galois connections:

$$(A^\flat, \sqsubseteq_{A^\flat}) \underset{\alpha_A}{\overset{\gamma_A}{\leftrightarrows}} (A^\sharp, \sqsubseteq_{A^\sharp}) \quad \text{and} \quad (B^\flat, \sqsubseteq_{B^\flat}) \underset{\alpha_B}{\overset{\gamma_B}{\leftrightarrows}} (B^\sharp, \sqsubseteq_{B^\sharp})$$

$$\begin{array}{rcl} \langle \alpha_A, \alpha_B \rangle & : & A^\flat \times B^\flat \to A^\sharp \times B^\sharp \\ \langle \alpha_A, \alpha_B \rangle (a^\flat, b^\flat) & \triangleq & (\alpha_A(a^\flat), \alpha_B(b^\flat)) \end{array}$$

$$\begin{array}{rcl} \langle \gamma_A, \gamma_B \rangle & : & A^\sharp \times B^\sharp \to A^\flat \times B^\flat \\ \langle \gamma_A, \gamma_B \rangle (a^\sharp, b^\sharp) & \triangleq & (\gamma_A(a^\sharp), \gamma_B(b^\sharp)) \end{array}$$

$$(a_1^\flat, b_1^\flat) \sqsubseteq_{A^\flat \times B^\flat} (a_2^\flat, b_2^\flat) \triangleq a_1^\flat \sqsubseteq_{A^\flat} a_2^\flat \wedge b_1^\flat \sqsubseteq_{B^\flat} b_2^\flat$$

$$(a_1^\sharp, b_1^\sharp) \sqsubseteq_{A^\sharp \times B^\sharp} (a_2^\sharp, b_2^\sharp) \triangleq a_1^\sharp \sqsubseteq_{A^\sharp} a_2^\sharp \wedge b_1^\sharp \sqsubseteq_{B^\sharp} b_2^\sharp$$

We have a Galois connection:

$$(A^\flat \times B^\flat, \sqsubseteq_{A^\flat \times B^\flat}) \underset{\langle \alpha_A, \alpha_B \rangle}{\overset{\langle \gamma_A, \gamma_B \rangle}{\leftrightarrows}} (A^\sharp \times B^\sharp, \sqsubseteq_{A^\sharp \times B^\sharp})$$

Abstract Semantics After Independent Attribute Abstraction

Definition:

$$\mathbb{T}^\sharp_{\mathsf{ia}}[\![t]\!] \triangleq \langle \alpha_{\mathsf{ia}}, \alpha_{\mathsf{ia}} \rangle \circ \mathbb{T}^\sharp_{\mathsf{h}}[\![t]\!]$$

Abstract Semantics After Independent Attribute Abstraction

Definition:

$$\mathbb{T}^{\sharp}_{\mathsf{ia}}[\![t]\!] \triangleq \langle \alpha_{\mathsf{ia}}, \alpha_{\mathsf{ia}} \rangle \circ \mathbb{T}^{\sharp}_{\mathsf{h}}[\![t]\!]$$

The following inclusions are satisfied:

$$\mathbb{T}^{\sharp}_{\mathsf{ia}}[\![\mathsf{x}^{p}]\!](\mathcal{I}) = (\{\{p \mapsto \{\rho(\mathsf{x})\}\} \mid \rho \in \mathcal{I}\}, \{\bot\})$$

Abstract Semantics After Independent Attribute Abstraction

Definition:

$$\mathbb{T}^\sharp_{\mathsf{ia}}[\![t]\!] \triangleq \langle \alpha_{\mathsf{ia}}, \alpha_{\mathsf{ia}} \rangle \circ \mathbb{T}^\sharp_{\mathsf{h}}[\![t]\!]$$

The following inclusions are satisfied:

$$\mathbb{T}^\sharp_{\mathsf{ia}}[\![\mathsf{x}^p]\!](\mathcal{I}) = (\{\{p \mapsto \{\rho(\mathsf{x})\}\} \mid \rho \in \mathcal{I}\}, \{\bot\})$$

$$\mathbb{T}^\sharp_{\mathsf{ia}}[\![(\lambda \mathsf{x}\,.\,t)^p]\!](\mathcal{I}) = (\{\{p \mapsto \{(\lambda \mathsf{x}\,.\,t)[\rho]\}\} \mid \rho \in \mathcal{I}\}, \{\bot\})$$

Definition:

$$\mathbb{T}^\sharp_{\mathsf{ia}}[\![t]\!] \triangleq \langle \alpha_{\mathsf{ia}}, \alpha_{\mathsf{ia}} \rangle \circ \mathbb{T}^\sharp_{\mathsf{h}}[\![t]\!]$$

The following inclusions are satisfied:

$$\mathbb{T}^\sharp_{\mathsf{ia}}[\![\mathsf{x}^p]\!](\mathcal{I}) = (\{\{p \mapsto \{\rho(\mathsf{x})\}\} \mid \rho \in \mathcal{I}\}, \{\bot\})$$

$$\mathbb{T}^\sharp_{\mathsf{ia}}[\![(\lambda \mathsf{x}\,.\,t)^p]\!](\mathcal{I}) = (\{\{p \mapsto \{(\lambda \mathsf{x}\,.\,t)[\rho]\}\} \mid \rho \in \mathcal{I}\}, \{\bot\})$$

$$\begin{array}{l}
\mathbb{T}^\sharp_{\mathsf{ia}}[\![\left((t_1)^{p_1}\ (t_2)^{p_2}\right)^p]\!](\mathcal{I}) \sqsubseteq \\
\quad \text{let } (\hat{\mathsf{C}}_1, \hat{\rho}_1) = \mathbb{T}^\sharp_{\mathsf{ia}}[\![(t_1)^{p_1}]\!](\mathcal{I}) \text{ in} \\
\quad \text{let } (\hat{\mathsf{C}}_2, \hat{\rho}_2) = \mathbb{T}^\sharp_{\mathsf{ia}}[\![(t_2)^{p_2}]\!](\mathcal{I}) \text{ in} \\
\quad (\hat{\mathsf{C}}_1, \hat{\rho}_1) \sqcup (\hat{\mathsf{C}}_2, \hat{\rho}_2) \sqcup \\
\quad \bigsqcup_{\lambda \mathsf{x}\,.\,(t_0)^{p_0} \in \hat{\mathsf{C}}_1(p_1)} \text{let } (\hat{\mathsf{C}}_0, \hat{\rho}_0) = \mathbb{T}^\sharp_{\mathsf{ia}}[\![(t_0)^{p_0}]\!](\mathcal{I}[\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)]) \text{ in} \\
\qquad\qquad\qquad\qquad (\hat{\mathsf{C}}_0, \hat{\rho}_0) \sqcup (\{\{p \mapsto \hat{\mathsf{C}}_0(p_0)\}\}, \{\{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}\})
\end{array}$$

Roadmap

Abstract caches and environments

$$(\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$

Environments as inputs

$$(\mathcal{X} \to \wp(\mathcal{V})) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Map independent attribute

Sets of caches and sets of environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp(\mathcal{P} \to \wp(\mathcal{V})) \times \wp(\mathcal{X} \to \wp(\mathcal{V})))$$

Sets of caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))))$$

Sets of traces

$$\wp(\mathcal{X} \to \mathcal{V}) \to \wp(\mathcal{T})$$

Map Abstraction

This is similar to independent attribute on pairs

$$\begin{array}{rcl} \alpha_{\mathsf{m}} & : & \wp(A \to \wp(B)) \to (A \to \wp(B)) \\ \alpha_{\mathsf{m}}(S) & \triangleq & \lambda a.\ \bigcup_{f \in S} f(a) \end{array}$$

$$\begin{array}{rcl} \gamma_{\mathsf{m}} & : & (A \to \wp(B)) \to \wp(A \to \wp(B)) \\ \gamma_{\mathsf{m}}(f) & \triangleq & \{g \mid \forall a.\ g(a) \subseteq f(a)\} \end{array}$$

We have a Galois connection:

$$(\wp(A \to \wp(B)), \subseteq) \underset{\alpha_{\mathsf{m}}}{\overset{\gamma_{\mathsf{m}}}{\leftrightarrows}} (A \to \wp(B), \dot{\subseteq})$$

Abstract Semantics after Map Independent Attribute Abstraction

Definition:

$$\mathbb{T}^{\sharp}_{\mathsf{M}}[\![t]\!] \triangleq \langle \alpha_{\mathsf{m}}, \alpha_{\mathsf{m}} \rangle \circ \mathbb{T}^{\sharp}_{\mathsf{h}}[\![t]\!] \ : \ (\wp(\mathcal{X} \to \mathcal{V})) \to (\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))$$

Abstract Semantics after Map Independent Attribute Abstraction

Definition:

$$\mathbb{T}^{\sharp}_{\mathsf{M}}[\![t]\!] \triangleq \langle \alpha_{\mathsf{m}}, \alpha_{\mathsf{m}} \rangle \circ \mathbb{T}^{\sharp}_{\mathsf{h}}[\![t]\!] : (\wp(\mathcal{X} \to \mathcal{V})) \to (\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))$$

The following inclusions are satisfied:

$$\mathbb{T}^{\sharp}_{\mathsf{M}}[\![\mathsf{x}^{p}]\!](\mathcal{I}) = (\{p \mapsto \mathcal{I}(\mathsf{x})\}, \bot) \qquad \text{where } \mathcal{I}(\mathsf{x}) = \{\rho(\mathsf{x}) \mid \rho \in \mathcal{I}\}$$

Abstract Semantics after Map Independent Attribute Abstraction

Definition:

$$\mathbb{T}^\sharp_{\mathsf{M}}[\![t]\!] \triangleq \langle \alpha_{\mathsf{m}}, \alpha_{\mathsf{m}} \rangle \circ \mathbb{T}^\sharp_{\mathsf{h}}[\![t]\!] \;:\; (\wp(\mathcal{X} \to \mathcal{V})) \to (\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))$$

The following inclusions are satisfied:

$$\mathbb{T}^\sharp_{\mathsf{M}}[\![\mathsf{x}^p]\!](\mathcal{I}) \;=\; (\{p \mapsto \mathcal{I}(\mathsf{x})\},\, \bot) \qquad \text{where } \mathcal{I}(\mathsf{x}) = \{\rho(\mathsf{x}) \mid \rho \in \mathcal{I}\}$$

$$\mathbb{T}^\sharp_{\mathsf{M}}[\![\,(\lambda \mathsf{x}\,.\,t)^p\,]\!](\mathcal{I}) \;=\; (\{p \mapsto (\lambda \mathsf{x}\,.\,t)[\mathcal{I}]\},\, \bot) \qquad \text{where } t[\mathcal{I}] = \{t[\rho] \mid \rho \in \mathcal{I}\}$$

Definition:

$$\mathbb{T}^\sharp_{\mathsf{M}}[\![t]\!] \triangleq \langle \alpha_{\mathsf{m}}, \alpha_{\mathsf{m}} \rangle \circ \mathbb{T}^\sharp_{\mathsf{h}}[\![t]\!] \ : \ (\wp(\mathcal{X} \to \mathcal{V})) \to (\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))$$

The following inclusions are satisfied:

$$\mathbb{T}^\sharp_{\mathsf{M}}[\![\mathsf{x}^p]\!](\mathcal{I}) \ = \ (\{p \mapsto \mathcal{I}(\mathsf{x})\}, \bot) \qquad \text{where } \mathcal{I}(\mathsf{x}) = \{\rho(\mathsf{x}) \mid \rho \in \mathcal{I}\}$$

$$\mathbb{T}^\sharp_{\mathsf{M}}[\![\, (\lambda \mathsf{x} \,.\, t)^p \,]\!](\mathcal{I}) \ = \ (\{p \mapsto (\lambda \mathsf{x} \,.\, t)[\mathcal{I}]\}, \bot) \qquad \text{where } t[\mathcal{I}] = \{t[\rho] \mid \rho \in \mathcal{I}\}$$

$$\begin{array}{l}
\mathbb{T}^\sharp_{\mathsf{M}}[\![\, \left((t_1)^{p_1} \ (t_2)^{p_2}\right)^p \,]\!](\mathcal{I}) \ \sqsubseteq \\
\quad \text{let } (\hat{\mathsf{C}}_1, \hat{\rho}_1) = \mathbb{T}^\sharp_{\mathsf{M}}[\![\, (t_1)^{p_1} \,]\!](\mathcal{I}) \text{ in} \\
\quad \text{let } (\hat{\mathsf{C}}_2, \hat{\rho}_2) = \mathbb{T}^\sharp_{\mathsf{M}}[\![\, (t_2)^{p_2} \,]\!](\mathcal{I}) \text{ in} \\
\qquad (\hat{\mathsf{C}}_1, \hat{\rho}_1) \sqcup (\hat{\mathsf{C}}_2, \hat{\rho}_2) \sqcup \\
\qquad \bigsqcup_{\lambda \mathsf{x} \,.\, (t_0)^{p_0} \in \mathsf{C}_1(p_1)} \ \text{let } (\hat{\mathsf{C}}_0, \hat{\rho}_0) = \mathbb{T}^\sharp_{\mathsf{M}}[\![\, (t_0)^{p_0} \,]\!](\mathcal{I}[\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)]) \text{ in} \\
\qquad\qquad\qquad\qquad (\hat{\mathsf{C}}_0, \hat{\rho}_0) \sqcup \Big(\{p \mapsto \hat{\mathsf{C}}_0(p_0)\}, \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}\Big)
\end{array}$$

Roadmap

Abstract caches and environments

$$(\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$

Environments as inputs

$$(\mathcal{X} \to \wp(\mathcal{V})) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Map abstraction on inputs

Caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$$

Sets of caches and sets of environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp(\mathcal{P} \to \wp(\mathcal{V})) \times \wp(\mathcal{X} \to \wp(\mathcal{V})))$$

Sets of caches and environments

$$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))))$$

Sets of traces

$$\wp(\mathcal{X} \to \mathcal{V}) \to \wp(\mathcal{T})$$

From sets of functions to set-valued functions

Definition:

$$\begin{array}{rcl} \alpha_{\mathsf{m}_1} & : & \wp(A \to B) \to (A \to \wp(B)) \\ \alpha_{\mathsf{m}_1}(S) & \triangleq & \lambda a.\, \bigcup_{f \in S} \{f(a)\} \end{array}$$

$$\begin{array}{rcl} \gamma_{\mathsf{m}_1} & : & (A \to \wp(B)) \to \wp(A \to B) \\ \gamma_{\mathsf{m}_1}(f) & \triangleq & \{g \mid \forall a.\, g(a) \in f(a)\} \end{array}$$

We have a Galois connection:

$$(\wp(A \to B), \subseteq) \underset{\alpha_{\mathsf{m}_1}}{\overset{\gamma_{\mathsf{m}_1}}{\leftrightarrows}} (A \to \wp(B), \dot{\subseteq})$$

Abstract semantics after input abstraction: ∞CFA

Definition:

$$\mathbb{T}^{\sharp}_{\infty\mathsf{CFA}}[\![t]\!] \triangleq \mathbb{T}^{\sharp}_{\mathsf{M}}[\![t]\!] \circ \gamma_{\mathsf{m}_1} : (\mathcal{X} \to \wp(\mathcal{V})) \to (\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))$$

Abstract semantics after input abstraction: ∞CFA

Definition:

$$\mathbb{T}^{\sharp}_{\infty\mathrm{CFA}}[\![t]\!] \triangleq \mathbb{T}^{\sharp}_{\mathrm{M}}[\![t]\!] \circ \gamma_{\mathrm{m}_1} : (\mathcal{X} \to \wp(\mathcal{V})) \to (\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))$$

The following inclusions are satisfied:

$$\mathbb{T}^{\sharp}_{\infty\mathrm{CFA}}[\![\mathrm{x}^p]\!](\hat{\rho}) = (\{p \mapsto \hat{\rho}(\mathrm{x})\}, \bot)$$

Abstract semantics after input abstraction: ∞CFA

Definition:

$$\mathbb{T}^{\sharp}_{\infty\mathrm{CFA}}[\![t]\!] \triangleq \mathbb{T}^{\sharp}_{\mathrm{M}}[\![t]\!] \circ \gamma_{\mathrm{m}_1} : (\mathcal{X} \to \wp(\mathcal{V})) \to (\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))$$

The following inclusions are satisfied:

$$\mathbb{T}^{\sharp}_{\infty\mathrm{CFA}}[\![\mathrm{x}^p]\!](\hat{\rho}) = (\{p \mapsto \hat{\rho}(\mathrm{x})\}, \bot)$$

$$\mathbb{T}^{\sharp}_{\infty\mathrm{CFA}}[\![(\lambda \mathrm{x}\,.\,t)^p]\!](\hat{\rho}) = (\{p \mapsto (\lambda \mathrm{x}\,.\,t)[\gamma_{\mathrm{m}_1}(\hat{\rho})]\}, \bot) \qquad \text{where } t[\mathcal{I}] = \{t[\rho] \mid \rho \in \mathcal{I}\}$$

Abstract semantics after input abstraction: ∞CFA

Definition:

$$\mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![t]\!] \triangleq \mathbb{T}^\sharp_{\mathrm{M}}[\![t]\!] \circ \gamma_{\mathsf{m}_1} : (\mathcal{X} \to \wp(\mathcal{V})) \to (\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))$$

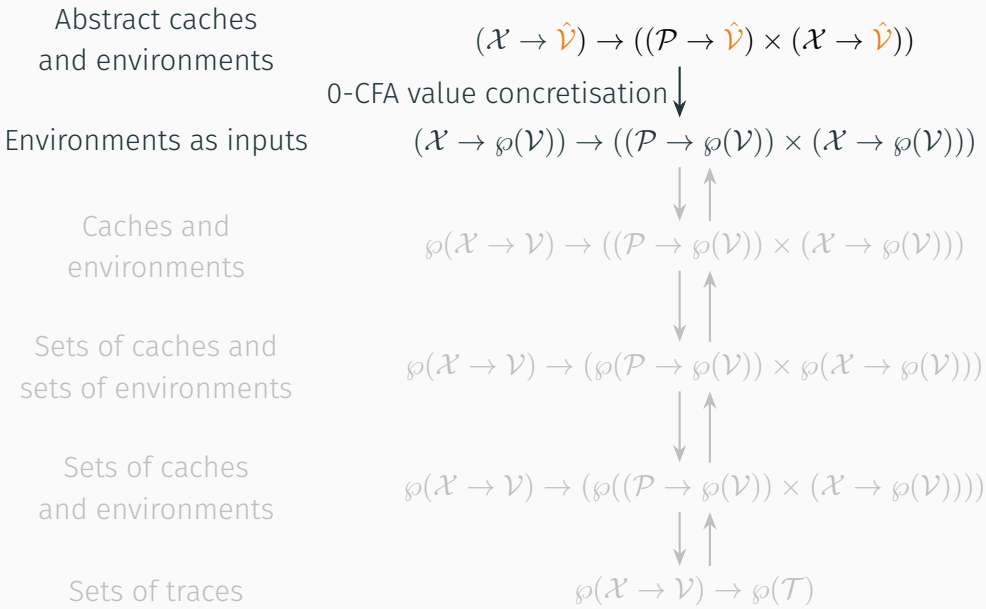
The following inclusions are satisfied:

$$\mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![\mathsf{x}^p]\!](\hat{\rho}) = (\{p \mapsto \hat{\rho}(\mathsf{x})\}, \bot)$$

$$\mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![(\lambda \mathsf{x}\,.\,t)^p]\!](\hat{\rho}) = (\{p \mapsto (\lambda \mathsf{x}\,.\,t)[\gamma_{\mathsf{m}_1}(\hat{\rho})]\}, \bot) \qquad \text{where } t[\mathcal{I}] = \{t[\rho] \mid \rho \in \mathcal{I}\}$$

$$\begin{array}{l}
\mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![\left((t_1)^{p_1}\ (t_2)^{p_2}\right)^p]\!](\hat{\rho}) \sqsubseteq \\
\quad \text{let } (\hat{\mathsf{C}}_1, \hat{\rho}_1) = \mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![(t_1)^{p_1}]\!](\hat{\rho}) \text{ in} \\
\quad \text{let } (\hat{\mathsf{C}}_2, \hat{\rho}_2) = \mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![(t_2)^{p_2}]\!](\hat{\rho}) \text{ in} \\
\qquad (\hat{\mathsf{C}}_1, \hat{\rho}_1) \sqcup (\hat{\mathsf{C}}_2, \hat{\rho}_2) \sqcup \\
\qquad \bigsqcup_{\lambda \mathsf{x}\,.\,(t_0)^{p_0} \in \hat{\mathsf{C}}_1(p_1)} \text{let } (\hat{\mathsf{C}}_0, \hat{\rho}_0) = \mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![(t_0)^{p_0}]\!](\hat{\rho}[\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)]) \text{ in} \\
\qquad\qquad (\hat{\mathsf{C}}_0, \hat{\rho}_0) \sqcup \left(\{p \mapsto \hat{\mathsf{C}}_0(p_0)\}, \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}\right)
\end{array}$$

Roadmap


Abstract caches and environments
$(\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$
0-CFA value concretisation
Environments as inputs
$(\mathcal{X} \to \wp(\mathcal{V})) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$
Caches and environments
$\wp(\mathcal{X} \to \mathcal{V}) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))$
Sets of caches and sets of environments
$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp(\mathcal{P} \to \wp(\mathcal{V})) \times \wp(\mathcal{X} \to \wp(\mathcal{V})))$
Sets of caches and environments
$\wp(\mathcal{X} \to \mathcal{V}) \to (\wp((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))))$
Sets of traces
$\wp(\mathcal{X} \to \mathcal{V}) \to \wp(\mathcal{T})$

0-CFA value abstraction

We reuse the unfolding relation from the first part of the course:

$$\begin{array}{rcl} \gamma^{\hat{\rho}}_{0\mathrm{CFA}} & : & \wp(\mathcal{V}) \to \wp(\mathcal{V} \cap \mathbf{Terms}(t)) \\ \gamma^{\hat{\rho}}_{0\mathrm{CFA}}(S) & \triangleq & \{v' \mid (v, \hat{\rho}) \models_{\mathrm{V}} v', v \in S\} \end{array}$$

$$S_1 \subseteq S_2 \;\Rightarrow\; \gamma^{\hat{\rho}}_{0\mathrm{CFA}}(S_1) \subseteq \gamma^{\hat{\rho}}_{0\mathrm{CFA}}(S_2)$$

There is no best abstraction!

Example: Take $\hat{\rho} = \{\mathrm{x}_1 \mapsto \lambda \mathrm{y}\,.\,\mathrm{y};\ \mathrm{x}_2 \mapsto \lambda \mathrm{y}\,.\,\mathrm{y}\}$

We have several minimal solutions to abstract the set $\{\lambda \mathrm{z}\,.\,\lambda \mathrm{y}\,.\,\mathrm{y}\}$:

- $\gamma^{\hat{\rho}}_{0\mathrm{CFA}}\{\lambda \mathrm{z}\,.\,\mathrm{x}_1\}$
- $\gamma^{\hat{\rho}}_{0\mathrm{CFA}}\{\lambda \mathrm{z}\,.\,\mathrm{x}_2\}$
- $\gamma^{\hat{\rho}}_{0\mathrm{CFA}}\{\lambda \mathrm{z}\,.\,\lambda \mathrm{y}\,.\,\mathrm{y}\}$

But they are not comparable!

Abstract Semantics for 0-CFA

We want:

$$\mathbb{T}^{\sharp}_{0\mathrm{CFA}}[\![t]\!] \;:\; (\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$

such that: $\mathbb{T}^{\sharp}_{\infty\mathrm{CFA}}[\![t]\!] \circ \gamma^{\hat{\rho}}_{0\mathrm{CFA}}(\hat{\rho}) \;\sqsubseteq\; \langle \gamma^{\hat{\rho}}_{0\mathrm{CFA}}, \gamma^{\hat{\rho}}_{0\mathrm{CFA}} \rangle \circ \mathbb{T}^{\sharp}_{0\mathrm{CFA}}[\![t]\!](\hat{\rho})$

We want:

$$\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![t]\!] \;:\; (\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$
$$\text{such that:} \quad \mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![t]\!] \circ \gamma^{\hat{\rho}}_{0\mathrm{CFA}}(\hat{\rho}) \;\sqsubseteq\; \langle \gamma^{\hat{\rho}}_{0\mathrm{CFA}}, \gamma^{\hat{\rho}}_{0\mathrm{CFA}} \rangle \circ \mathbb{T}^\sharp_{0\mathrm{CFA}}[\![t]\!](\hat{\rho})$$

It suffices that the following inclusions are satisfied:

$$\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\mathsf{x}^p]\!](\hat{\rho}) \;=\; (\{p \mapsto \hat{\rho}(\mathsf{x})\},\, \bot)$$

We want:

$$\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![t]\!] \;:\; (\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$
$$\text{such that:} \quad \mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![t]\!] \circ \gamma^{\hat{\rho}}_{0\mathrm{CFA}}(\hat{\rho}) \;\sqsubseteq\; \langle \gamma^{\hat{\rho}}_{0\mathrm{CFA}}, \gamma^{\hat{\rho}}_{0\mathrm{CFA}} \rangle \circ \mathbb{T}^\sharp_{0\mathrm{CFA}}[\![t]\!](\hat{\rho})$$

It suffices that the following inclusions are satisfied:

$$\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\mathsf{x}^p]\!](\hat{\rho}) \;=\; (\{p \mapsto \hat{\rho}(\mathsf{x})\},\, \bot)$$

$$\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\,(\lambda \mathsf{x}\,.\,t)^p\,]\!](\hat{\rho}) \;=\; (\{p \mapsto \lambda \mathsf{x}\,.\,t\},\, \bot)$$

We want:

$$\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![t]\!] \;:\; (\mathcal{X} \to \hat{\mathcal{V}}) \to ((\mathcal{P} \to \hat{\mathcal{V}}) \times (\mathcal{X} \to \hat{\mathcal{V}}))$$
$$\text{such that:}\quad \mathbb{T}^\sharp_{\infty\mathrm{CFA}}[\![t]\!] \circ \gamma^{\hat{\rho}}_{0\mathrm{CFA}}(\hat{\rho}) \;\sqsubseteq\; \langle \gamma^{\hat{\rho}}_{0\mathrm{CFA}}, \gamma^{\hat{\rho}}_{0\mathrm{CFA}} \rangle \circ \mathbb{T}^\sharp_{0\mathrm{CFA}}[\![t]\!](\hat{\rho})$$

It suffices that the following inclusions are satisfied:

$$\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\mathsf{x}^p]\!](\hat{\rho}) \;=\; (\{p \mapsto \hat{\rho}(\mathsf{x})\},\, \bot)$$

$$\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\,(\lambda \mathsf{x}\,.\,t)^p\,]\!](\hat{\rho}) \;=\; (\{p \mapsto \lambda \mathsf{x}\,.\,t\},\, \bot)$$

$$\begin{array}{l}
\mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\,((t_1)^{p_1}\ (t_2)^{p_2})^p\,]\!](\hat{\rho}) \;\sqsubseteq \\
\quad \text{let } (\hat{\mathsf{C}}_1, \hat{\rho}_1) = \mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\,(t_1)^{p_1}\,]\!](\hat{\rho}) \text{ in} \\
\quad \text{let } (\hat{\mathsf{C}}_2, \hat{\rho}_2) = \mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\,(t_2)^{p_2}\,]\!](\hat{\rho}) \text{ in} \\
\qquad (\hat{\mathsf{C}}_1, \hat{\rho}_1) \sqcup (\hat{\mathsf{C}}_2, \hat{\rho}_2) \sqcup \\
\qquad \bigsqcup_{\lambda \mathsf{x}\,.\,(t_0)^{p_0} \in \hat{\mathsf{C}}_1(p_1)} \text{let } (\hat{\mathsf{C}}_0, \hat{\rho}_0) = \mathbb{T}^\sharp_{0\mathrm{CFA}}[\![\,(t_0)^{p_0}\,]\!](\hat{\rho} \,\dot\cup\, \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}) \text{ in} \\
\qquad\qquad (\hat{\mathsf{C}}_0, \hat{\rho}_0) \sqcup \Big(\{p \mapsto \hat{\mathsf{C}}_0(p_0)\},\, \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}\Big)
\end{array}$$

Definition of 0-CFA

Definition:

$$
\begin{aligned}
&\mathbb{T}^\sharp[\![\cdot]\!] : \mathcal{T} \to (\mathcal{X} \to \wp(\mathcal{V})) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V}))) \\
&\triangleq \mathrm{lfp}\ \ \lambda f.\, \lambda t.\, \lambda \hat{\rho}. \\
&\qquad \text{match } t \text{ with} \\
&\qquad \mid \quad \mathsf{x}^p \ \Rightarrow\ (\{p \mapsto \hat{\rho}(\mathsf{x})\},\ \bot) \\
&\qquad \mid \quad (\lambda \mathsf{x}\,.\,t_0)^p \ \Rightarrow\ (\{p \mapsto \lambda \mathsf{x}\,.\,t_0\},\ \bot) \\
&\qquad \mid \quad \big((t_1)^{p_1}\ (t_2)^{p_2}\big)^p \ \Rightarrow \\
&\qquad\qquad \text{let } (\hat{\mathsf{C}}_1, \hat{\rho}_1) = f((t_1)^{p_1})(\hat{\rho}) \text{ in} \\
&\qquad\qquad \text{let } (\hat{\mathsf{C}}_2, \hat{\rho}_2) = f((t_2)^{p_2})(\hat{\rho}) \text{ in} \\
&\qquad\qquad (\hat{\mathsf{C}}_1, \hat{\rho}_1) \sqcup (\hat{\mathsf{C}}_2, \hat{\rho}_2) \sqcup \\
&\qquad\qquad \bigsqcup_{\lambda \mathsf{x}\,.\,(t_0)^{p_0} \in \hat{\mathsf{C}}_1(p_1)} \text{let } (\hat{\rho}_0) = f((t_0)^{p_0})(\hat{\mathsf{C}}, \hat{\rho} \dot{\cup} \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}) \text{ in} \\
&\qquad\qquad\qquad\qquad\qquad\qquad (\hat{\mathsf{C}}_0, \hat{\rho}_0) \sqcup \Big(\{p \mapsto \hat{\mathsf{C}}_0(p_0)\},\ \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}\Big)
\end{aligned}
$$

Definition of 0-CFA

Definition:

$$
\begin{aligned}
&\mathbb{T}^\sharp[\![\cdot]\!] : \mathcal{T} \to (\mathcal{X} \to \wp(\mathcal{V})) \to ((\mathcal{P} \to \wp(\mathcal{V})) \times (\mathcal{X} \to \wp(\mathcal{V})))\\
&\triangleq \mathrm{lfp}\ \ \lambda f.\, \lambda t.\, \lambda \hat{\rho}.\\
&\qquad \text{match } t \text{ with}\\
&\qquad \mid\ \ \mathsf{x}^p \ \Rightarrow\ (\{p \mapsto \hat{\rho}(\mathsf{x})\},\ \bot)\\
&\qquad \mid\ \ (\lambda \mathsf{x}\,.\,t_0)^p \ \Rightarrow\ (\{p \mapsto \lambda \mathsf{x}\,.\,t_0\},\ \bot)\\
&\qquad \mid\ \ \left((t_1)^{p_1}\ (t_2)^{p_2}\right)^p \ \Rightarrow\\
&\qquad\qquad \text{let } (\hat{\mathsf{C}}_1, \hat{\rho}_1) = f((t_1)^{p_1})(\hat{\rho}) \text{ in}\\
&\qquad\qquad \text{let } (\hat{\mathsf{C}}_2, \hat{\rho}_2) = f((t_2)^{p_2})(\hat{\rho}) \text{ in}\\
&\qquad\qquad (\hat{\mathsf{C}}_1, \hat{\rho}_1) \sqcup (\hat{\mathsf{C}}_2, \hat{\rho}_2) \sqcup\\
&\qquad\qquad \bigsqcup_{\lambda \mathsf{x}\,.\,(t_0)^{p_0} \in \hat{\mathsf{C}}_1(p_1)} \text{let } (\hat{\rho}_0) = f((t_0)^{p_0})(\hat{\mathsf{C}}, \hat{\rho} \dot{\cup} \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}) \text{ in}\\
&\qquad\qquad\qquad\qquad (\hat{\mathsf{C}}_0, \hat{\rho}_0) \sqcup \left(\{p \mapsto \hat{\mathsf{C}}_0(p_0)\},\ \{\mathsf{x} \mapsto \hat{\mathsf{C}}_2(p_2)\}\right)
\end{aligned}
$$

Why does this definition make sense?

Soundness of 0-CFA

Proposition 6.1

$$\mathbb{T}^{\sharp}_{0\mathrm{CFA}}[\![t]\!](\bot) \sqsubseteq \mathbb{T}^{\sharp}[\![t]\!](\bot)$$

Corollary 14

For the concretization γ that we have defined piece after piece:

$$\mathbb{T}[\![t]\!](\emptyset) \subseteq \gamma(\mathbb{T}^{\sharp}[\![t]\!](\bot))$$

Soundness of 0-CFA

Proposition 6.1

$$\mathbb{T}^{\sharp}_{0\mathrm{CFA}}[\![t]\!](\bot) \sqsubseteq \mathbb{T}^{\sharp}[\![t]\!](\bot)$$

Corollary 14

For the concretization γ that we have defined piece after piece:

$$\mathbb{T}[\![t]\!](\emptyset) \subseteq \gamma(\mathbb{T}^{\sharp}[\![t]\!](\bot))$$

- The proof follows from the soundness of all the abstractions we have used

Soundness of 0-CFA

Proposition 6.1

$$\mathbb{T}^{\sharp}_{0\mathrm{CFA}}[\![t]\!](\bot) \sqsubseteq \mathbb{T}^{\sharp}[\![t]\!](\bot)$$

Corollary 14

For the concretization γ that we have defined piece after piece:

$$\mathbb{T}[\![t]\!](\emptyset) \subseteq \gamma(\mathbb{T}^{\sharp}[\![t]\!](\bot))$$

- The proof follows from the soundness of all the abstractions we have used
- $\mathbb{T}^{\sharp}[\![t]\!]$ computes an abstraction of the traces produced by t, *i.e.*:
  - Which β-reductions might have been performed, and
  - Which values might have been produced at each program point

Soundness of 0-CFA

Proposition 6.1

$$\mathbb{T}^\sharp_{0\text{CFA}}[\![t]\!](\bot) \sqsubseteq \mathbb{T}^\sharp[\![t]\!](\bot)$$

Corollary 14

For the concretization γ that we have defined piece after piece:

$$\mathbb{T}[\![t]\!](\emptyset) \subseteq \gamma(\mathbb{T}^\sharp[\![t]\!](\bot))$$

- The proof follows from the soundness of all the abstractions we have used
- $\mathbb{T}^\sharp[\![t]\!]$ computes an abstraction of the traces produced by t, *i.e.*:
  - Which β-reductions might have been performed, and
  - Which values might have been produced at each program point
- $\mathbb{T}^\sharp[\![t]\!]$ is directly implementable!

  Fixpoint iteration builds a partial function of the so far computed results

  👉 Source code available on the course web page

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
```

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
Changes at iteration 2: ([ 2 -> { λx1.x1^1 }; 5 -> { λy.(λz.y^3)^4 } ], [])
```

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
Changes at iteration 2: ([ 2 -> { λx1.x1^1 }; 5 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 3: ([], [ x1 -> { λy.(λz.y^3)^4 } ])
```

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
Changes at iteration 2: ([ 2 -> { λx1.x1^1 }; 5 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 3: ([], [ x1 -> { λy.(λz.y^3)^4 } ])
Changes at iteration 4: ([ 1 -> { λy.(λz.y^3)^4 } ], [])
```

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
Changes at iteration 2: ([ 2 -> { λx1.x1^1 }; 5 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 3: ([], [ x1 -> { λy.(λz.y^3)^4 } ])
Changes at iteration 4: ([ 1 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 5: ([ 6 -> { λy.(λz.y^3)^4 } ], [])
```

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
Changes at iteration 2: ([ 2 -> { λx1.x1^1 }; 5 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 3: ([], [ x1 -> { λy.(λz.y^3)^4 } ])
Changes at iteration 4: ([ 1 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 5: ([ 6 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 6: ([], [ y -> { λx2.x2^7 } ])
```

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
Changes at iteration 2: ([ 2 -> { λx1.x1^1 }; 5 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 3: ([], [ x1 -> { λy.(λz.y^3)^4 } ])
Changes at iteration 4: ([ 1 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 5: ([ 6 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 6: ([], [ y -> { λx2.x2^7 } ])
Changes at iteration 7: ([ 4 -> { λz.y^3 } ], [])
```

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
Changes at iteration 2: ([ 2 -> { λx1.x1^1 }; 5 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 3: ([], [ x1 -> { λy.(λz.y^3)^4 } ])
Changes at iteration 4: ([ 1 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 5: ([ 6 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 6: ([], [ y -> { λx2.x2^7 } ])
Changes at iteration 7: ([ 4 -> { λz.y^3 } ], [])
Changes at iteration 8: ([ 9 -> { λz.y^3 } ], [])
```

Example #1

$$\left(\left(\left(\lambda x_1 \,.\, x_1^1\right)^2 \left(\lambda y \,.\, \left(\lambda z \,.\, y^3\right)^4\right)^5\right)^6 \left(\lambda x_2 \,.\, x_2^7\right)^8\right)^9$$

```
Changes at iteration 1: ([ 8 -> { λx2.x2^7 } ], [])
Changes at iteration 2: ([ 2 -> { λx1.x1^1 }; 5 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 3: ([], [ x1 -> { λy.(λz.y^3)^4 } ])
Changes at iteration 4: ([ 1 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 5: ([ 6 -> { λy.(λz.y^3)^4 } ], [])
Changes at iteration 6: ([], [ y -> { λx2.x2^7 } ])
Changes at iteration 7: ([ 4 -> { λz.y^3 } ], [])
Changes at iteration 8: ([ 9 -> { λz.y^3 } ], [])

Solution:
([ 1 -> { λy.(λz.y^3)^4 };  2 -> { λx1.x1^1 };      3 -> ∅;
   4 -> { λz.y^3 };         5 -> { λy.(λz.y^3)^4 }; 6 -> { λy.(λz.y^3)^4 };
   7 -> ∅;                  8 -> { λx2.x2^7 };      9 -> { λz.y^3 } ],
 [ x1 -> { λy.(λz.y^3)^4 }; x2 -> ∅;                y -> { λx2.x2^7 } ])
```

Example #2

$$\left(\left(\lambda x.\ \left(x^{1}\, x^{2}\right)^{3}\right)^{4}\ \left(\lambda y.\ \left(y^{5}\, y^{6}\right)^{7}\right)^{8}\right)^{9}$$

Example #2

$$\left(\left(\lambda x.\ \left(x^{1}\ x^{2}\right)^{3}\right)^{4}\ \left(\lambda y.\ \left(y^{5}\ y^{6}\right)^{7}\right)^{8}\right)^{9}$$

```
Changes at iteration 1:
([ 4 -> { λx.(x^1 x^2)^3 }; 8 -> { λy.(y^5 y^6)^7 } ], [])
```

Example #2

$$\left(\left(\lambda x.\ \left(x^{1}\ x^{2}\right)^{3}\right)^{4}\ \left(\lambda y.\ \left(y^{5}\ y^{6}\right)^{7}\right)^{8}\right)^{9}$$

```
Changes at iteration 1:
([ 4 -> { λx.(x^1 x^2)^3 }; 8 -> { λy.(y^5 y^6)^7 } ], [])
Changes at iteration 2: ([], [ x -> { λy.(y^5 y^6)^7 } ])
```

Example #2

$$\left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9$$

```
Changes at iteration 1:
([ 4 -> { λx.(x^1 x^2)^3 }; 8 -> { λy.(y^5 y^6)^7 } ], [])
Changes at iteration 2: ([], [ x -> { λy.(y^5 y^6)^7 } ])
Changes at iteration 3:
([ 1 -> { λy.(y^5 y^6)^7 }; 2 -> { λy.(y^5 y^6)^7 } ], [])
```

Example #2

$$\Big(\big(\lambda x.\ (x^1\, x^2)^3\big)^4\ \big(\lambda y.\ (y^5\, y^6)^7\big)^8\Big)^9$$

```
Changes at iteration 1:
([ 4 -> { λx.(x^1 x^2)^3 }; 8 -> { λy.(y^5 y^6)^7 } ], [])
Changes at iteration 2: ([], [ x -> { λy.(y^5 y^6)^7 } ])
Changes at iteration 3:
([ 1 -> { λy.(y^5 y^6)^7 }; 2 -> { λy.(y^5 y^6)^7 } ], [])
Changes at iteration 4: ([], [ y -> { λy.(y^5 y^6)^7 } ])
```

Example #2

$$\left(\left(\lambda x.\ \left(x^{1}\ x^{2}\right)^{3}\right)^{4}\ \left(\lambda y.\ \left(y^{5}\ y^{6}\right)^{7}\right)^{8}\right)^{9}$$

```
Changes at iteration 1:
([ 4 -> { λx.(x^1 x^2)^3 }; 8 -> { λy.(y^5 y^6)^7 } ], [])
Changes at iteration 2: ([], [ x -> { λy.(y^5 y^6)^7 } ])
Changes at iteration 3:
([ 1 -> { λy.(y^5 y^6)^7 }; 2 -> { λy.(y^5 y^6)^7 } ], [])
Changes at iteration 4: ([], [ y -> { λy.(y^5 y^6)^7 } ])
Changes at iteration 5:
([ 5 -> { λy.(y^5 y^6)^7 }; 6 -> { λy.(y^5 y^6)^7 } ], [])
```

Example #2

$$\left(\left(\lambda x.\ \left(x^1\, x^2\right)^3\right)^4\ \left(\lambda y.\ \left(y^5\, y^6\right)^7\right)^8\right)^9$$

```
Changes at iteration 1:
([ 4 -> { λx.(x^1 x^2)^3 }; 8 -> { λy.(y^5 y^6)^7 } ], [])
Changes at iteration 2: ([], [ x -> { λy.(y^5 y^6)^7 } ])
Changes at iteration 3:
([ 1 -> { λy.(y^5 y^6)^7 }; 2 -> { λy.(y^5 y^6)^7 } ], [])
Changes at iteration 4: ([], [ y -> { λy.(y^5 y^6)^7 } ])
Changes at iteration 5:
([ 5 -> { λy.(y^5 y^6)^7 }; 6 -> { λy.(y^5 y^6)^7 } ], [])

Solution:
([ 1 -> { λy.(y^5 y^6)^7 }; 2 -> { λy.(y^5 y^6)^7 }; 3 -> ∅;
   4 -> { λx.(x^1 x^2)^3 }; 5 -> { λy.(y^5 y^6)^7 }; 6 -> { λy.(y^5 y^6)^7 };
   7 -> ∅;                  8 -> { λy.(y^5 y^6)^7 }; 9 -> ∅ ],
 [ x -> { λy.(y^5 y^6)^7 }; y -> { λy.(y^5 y^6)^7 } ])
```

Soundness of the Acceptability Relation

Define $\quad (\hat{C}, \hat{\rho}) \Vdash t \triangleq \mathbb{T}^{\sharp}_{0CFA}[\![t]\!](\hat{\rho}) \sqsubseteq (\hat{C}, \hat{\rho})$

Soundness of the Acceptability Relation

Define $(\hat{C}, \hat{\rho}) \Vdash t \triangleq \mathbb{T}^{\sharp}_{0\mathrm{CFA}}[\![t]\!](\hat{\rho}) \sqsubseteq (\hat{C}, \hat{\rho})$

Then, the following implications are satisfied:

$$\frac{\hat{\rho}(x) \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \Vdash x^{p}} \qquad \frac{\{\lambda x.\ (t_0)^{p_0}\} \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \Vdash \left(\lambda x.\ (t_0)^{p_0}\right)^{p}}$$

$$\frac{\begin{array}{c}(\hat{C}, \hat{\rho}) \Vdash (t_1)^{p_1} \qquad (\hat{C}, \hat{\rho}) \Vdash (t_2)^{p_2} \\ \forall (\lambda x.\ (t_0)^{p_0}) \in \hat{C}(p_1), \\ (\hat{C}, \hat{\rho}) \Vdash (t_0)^{p_0} \quad \wedge \quad \hat{C}(p_2) \subseteq \hat{\rho}(x) \quad \wedge \quad \hat{C}(p_0) \subseteq \hat{C}(p)\end{array}}{(\hat{C}, \hat{\rho}) \Vdash \left((t_1)^{p_1}\ (t_2)^{p_2}\right)^{p}}$$

Soundness of the Acceptability Relation

Define $\quad (\hat{C}, \hat{\rho}) \Vdash t \triangleq \mathbb{T}^{\sharp}_{0\mathrm{CFA}}[\![t]\!](\hat{\rho}) \sqsubseteq (\hat{C}, \hat{\rho})$

Then, the following implications are satisfied:

$$\frac{\hat{\rho}(x) \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \Vdash x^p} \qquad \frac{\{\lambda x.\ (t_0)^{p_0}\} \subseteq \hat{C}(p)}{(\hat{C}, \hat{\rho}) \Vdash \left(\lambda x.\ (t_0)^{p_0}\right)^p}$$

$$\frac{\begin{array}{c}(\hat{C}, \hat{\rho}) \Vdash (t_1)^{p_1} \qquad (\hat{C}, \hat{\rho}) \Vdash (t_2)^{p_2} \\ \forall (\lambda x.\ (t_0)^{p_0}) \in \hat{C}(p_1), \\ (\hat{C}, \hat{\rho}) \Vdash (t_0)^{p_0} \quad \wedge \quad \hat{C}(p_2) \subseteq \hat{\rho}(x) \quad \wedge \quad \hat{C}(p_0) \subseteq \hat{C}(p)\end{array}}{(\hat{C}, \hat{\rho}) \Vdash \left((t_1)^{p_1}\ (t_2)^{p_2}\right)^p}$$

These are the same rules as the ones of the acceptability relation!

👉 This gives a semantic proof of the soundness for the rules of acceptability

Beyond 0-CFA

Limitations of 0-CFA

- **Context insensitive:** 0-CFA does not distinguish different instances of variables

$$\left(\mathsf{let}\, f = \left(\lambda x\,.\,x^{1}\right)^{2} \;\mathsf{in}\; \left(\left(f^{3}\, f^{4}\right)^{5}\; \left(\lambda y\,.\,y^{6}\right)^{7}\right)^{8}\right)^{9}$$

With the version based on constraints, we have:

$$\hat{C}(9) = \{\lambda x\,.\,x^{1}, \lambda y\,.\,y^{6}\} \qquad \longleftarrow \text{this is imprecise!}$$

ℹ Remark: with the version derived by abstract interpretation, we get:

$$\hat{C}(9) = \{\lambda y\,.\,y^{6}\}$$

Limitations of 0-CFA

- **Context insensitive:** 0-CFA does not distinguish different instances of variables

$$\left(\mathsf{let}\,\mathsf{f} = \left(\lambda \mathsf{x}\,.\,\mathsf{x}^{1}\right)^{2}\ \mathsf{in}\ \left(\left(\mathsf{f}^{3}\,\mathsf{f}^{4}\right)^{5}\ \left(\lambda \mathsf{y}\,.\,\mathsf{y}^{6}\right)^{7}\right)^{8}\right)^{9}$$

  With the version based on constraints, we have:

$$\hat{\mathsf{C}}(9) = \{\lambda \mathsf{x}\,.\,\mathsf{x}^{1}, \lambda \mathsf{y}\,.\,\mathsf{y}^{6}\} \qquad \longleftarrow \text{this is imprecise!}$$

  ℹ Remark: with the version derived by abstract interpretation, we get:

$$\hat{\mathsf{C}}(9) = \{\lambda \mathsf{y}\,.\,\mathsf{y}^{6}\}$$

- **Flow insensitive:** all parts of a program are analysed, even unreachable ones

$$\left(\begin{array}{l} \mathsf{let}\ \mathsf{omega} = \left(\left(\lambda \mathsf{x}_1\,.\ \left(\mathsf{x}_1^{1}\,\mathsf{x}_1^{2}\right)^{3}\right)^{4}\ \left(\lambda \mathsf{x}_2\,.\ \left(\mathsf{x}_2^{5}\,\mathsf{x}_2^{6}\right)^{7}\right)^{8}\right)^{9}\ \mathsf{in} \\ \left(\mathsf{omega}^{10}\ \left(\left(\lambda \mathsf{y}\,.\,\mathsf{y}^{11}\right)^{12}\ \left(\lambda \mathsf{z}\,.\,\mathsf{z}^{13}\right)^{14}\right)^{15}\right)^{16} \end{array}\right)^{17}$$

  With both versions of the analysis, we obtain: $\hat{\rho}(\mathsf{y}) = \{\lambda \mathsf{z}\,.\,\mathsf{z}^{13}\}$

Extensions

Many aspects were not covered in this course! To cite a few:

- Context sensitivity: k-CFA, polymorphic splitting, ...
- Reachability-based CFA
- Recursive functions
- Booleans, conditionals, arithmetic
- Algebraic datatypes
- Imperative features
- Object oriented features
- Laziness
- Non-structural control flow:
  - Exceptions
  - Continuations/`callcc`
  - Delimited continuations/coroutines
  - Effect handlers
- Concurrency
- Reflexion

Open Questions for CFA

- Relational domains for CFA?
- Modular analysis?
- Scalable analysis?
  $\mathcal{O}(n^3)$ does not scale ☹

Some ongoing research at Inria Rennes:

- 👉 *Salto* project: static analysis for OCaml programs
  Based on a variant of CFA, designed using abstract interpretation