

AAA616: Program Analysis

Lecture 8 — Control-Flow Analysis

Hakjoo Oh
2026 Fall

Control-Flow Analysis (CFA)

- In functional or object-oriented languages, the program's control flows are not explicit from the program syntax.
- Control-flow analysis is a static analysis that computes for each subexpression the set of functions that it could evaluate to.

Example 1

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

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

Example 2

$(\text{let } g = (\text{fun } f \ x \Rightarrow (f^1 \ (\text{fn } y \Rightarrow y^2)^3)^4)^5 \text{ in } (g^6 \ (\text{fn } z \Rightarrow z^7)^8)^9)^{10}$

1	{ fun f x => (f (fn y => y)) }
2	∅
3	{ fn y => y }
4	∅
5	{ fun f x => (f (fn y => y)) }
6	{ fun f x => (f (fn y => y)) }
7	∅
8	{ fn z => z }
9	∅
10	∅
f	{ fun f x => (f (fn y => y)) }
g	{ fun f x => (f (fn y => y)) }
x	{ fn y => y, fn z => z }
y	∅
z	∅

Language

$e \rightarrow$	t^l	expressions (labelled terms)
$t \rightarrow$	n	terms (unlabelled expressions)
	x	
	$\text{fn } x \Rightarrow e_0$	
	$\text{fun } f \ x \Rightarrow e_0$	
	$e_1 \ e_2$	
	$\text{if } e_0 \text{ then } e_1 \text{ else } e_2$	
	$\text{let } x = e_1 \text{ in } e_2$	
	$e_1 \text{ op } e_2$	

The 0-CFA Analysis

- 0-CFA aims to compute an abstract state of the form:

$$S \in \mathbf{State} = (\mathbf{Label} \cup \mathbf{Var}) \rightarrow 2^{\mathbf{Term}}$$

- Two steps:
 - ① Generate equations over the state
 - ② Solve the equations

Generating Equations

From the program

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

generate the equation as follows:

$$\begin{aligned} \mathcal{C}(((\text{fn } x \Rightarrow x^1)^2 (\text{fn } y \Rightarrow y^3)^4)^5) = \{ \\ & \{\text{fn } x \Rightarrow x^1\} \subseteq S(2), \\ & S(x) \subseteq S(1), \\ & \{\text{fn } y \Rightarrow y^3\} \subseteq S(4), \\ & S(y) \subseteq S(3), \\ & \{\text{fn } x \Rightarrow x^1\} \subseteq S(2) \implies S(4) \subseteq S(x), \\ & \{\text{fn } x \Rightarrow x^1\} \subseteq S(2) \implies S(1) \subseteq S(5), \\ & \{\text{fn } y \Rightarrow y^3\} \subseteq S(2) \implies S(4) \subseteq S(y), \\ & \{\text{fn } y \Rightarrow y^3\} \subseteq S(2) \implies S(3) \subseteq S(5), \\ & \} \end{aligned}$$

Two types of equations:

$$lhs \subseteq rhs, \quad \{t\} \subseteq rhs' \implies lhs \subseteq rhs$$

Generating Equations

$$\begin{aligned}
 \mathcal{C}(n^l) &= \emptyset \\
 \mathcal{C}(x^l) &= \{S(x) \subseteq S(l)\} \\
 \mathcal{C}((\text{fn } x \Rightarrow e_0)^l) &= \{\{\text{fn } x \Rightarrow e_0\} \subseteq S(l)\} \cup \mathcal{C}(e_0) \\
 \mathcal{C}((\text{fun } f \ x \Rightarrow e_0)^l) &= \{\{\text{fun } f \ x \Rightarrow e_0\} \subseteq S(l)\} \cup \mathcal{C}(e_0) \\
 &\quad \cup \{\{\text{fun } f \ x \Rightarrow e_0\} \subseteq S(f)\} \\
 \mathcal{C}((t_1^{l_1} \ t_2^{l_2})^l) &= \mathcal{C}(t_1^{l_1}) \cup \mathcal{C}(t_2^{l_2}) \\
 &\quad \cup \{\{t\} \subseteq S(l_1) \implies S(l_2) \subseteq S(x) \\
 &\quad \quad | \ t = (\text{fn } x \Rightarrow t_0^{l_0}) \in \mathbf{Term}\} \\
 &\quad \cup \{\{t\} \subseteq S(l_1) \implies S(l_0) \subseteq S(l) \\
 &\quad \quad | \ t = (\text{fn } x \Rightarrow t_0^{l_0}) \in \mathbf{Term}\} \\
 &\quad \cup \{\{t\} \subseteq S(l_1) \implies S(l_2) \subseteq S(x) \\
 &\quad \quad | \ t = (\text{fun } f \ x \Rightarrow t_0^{l_0}) \in \mathbf{Term}\} \\
 &\quad \cup \{\{t\} \subseteq S(l_1) \implies S(l_0) \subseteq S(l) \\
 &\quad \quad | \ t = (\text{fun } f \ x \Rightarrow t_0^{l_0}) \in \mathbf{Term}\} \\
 \mathcal{C}((\text{if } t_0^{l_0} \text{ then } t_1^{l_1} \text{ else } t_2^{l_2})^l) &= \\
 \mathcal{C}((\text{let } x=t_1^{l_1} \text{ in } t_2^{l_2})^l) &= \\
 \mathcal{C}((t_1^{l_1} \text{ op } t_2^{l_2})^l) &=
 \end{aligned}$$

Solving the Equations

$$\begin{aligned} \mathcal{C}(((\text{fn } x \Rightarrow x^1)^2 \ (\text{fn } y \Rightarrow y^3)^4)^5) = \{ \\ & \{\text{fn } x \Rightarrow x^1\} \subseteq S(2), \\ & S(x) \subseteq S(1), \\ & \{\text{fn } y \Rightarrow y^3\} \subseteq S(4), \\ & S(y) \subseteq S(3), \\ & \{\text{fn } x \Rightarrow x^1\} \subseteq S(2) \implies S(4) \subseteq S(x), \\ & \{\text{fn } x \Rightarrow x^1\} \subseteq S(2) \implies S(1) \subseteq S(5), \\ & \{\text{fn } y \Rightarrow y^3\} \subseteq S(2) \implies S(4) \subseteq S(y), \\ & \{\text{fn } y \Rightarrow y^3\} \subseteq S(2) \implies S(3) \subseteq S(5), \\ & \} \end{aligned}$$

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

Solving the Equation

solve(C, S) =
 let $S' = \mathbf{update}(C, S)$
 if $\forall a. S'(a) \subseteq S(a)$ then S
 else **solve**(C, S')

update(C, S) =
 for c in C :
 if $c = (\{t\} \subseteq S(a))$:
 $S(a) := S(a) \cup \{t\}$
 if $c = (S(a_1) \subseteq S(a_2))$:
 $S(a_2) := S(a_2) \cup S(a_1)$
 if $c = (\{t\} \subseteq S(a_1) \implies S(a_2) \subseteq S(a_3))$:
 if $t \in S(a_1)$ then $S(a_3) := S(a_3) \cup S(a_2)$
 return S

Limitation

$(\text{let } f = (\text{fn } x \Rightarrow x^1)^2 \text{ in } ((f^3 \ f^4)^5 \ (\text{fn } y \Rightarrow y^6)^7)^8)^9$

1	{ fn x => x ¹ , fn y => y ⁶ }
2	{ fn x => x ¹ }
3	{ fn x => x ¹ }
4	{ fn x => x ¹ }
5	{ fn x => x ¹ , fn y => y ⁶ }
6	{ fn y => y ⁶ }
7	{ fn y => y ⁶ }
8	{ fn x => x ¹ , fn y => y ⁶ }
9	{ fn x => x ¹ , fn y => y ⁶ }
f	{ fn x => x ¹ }
x	{ fn x => x ¹ , fn y => y ⁶ }
y	{ fn y => y ⁶ }

The result says that the overall expression (label 9) may evaluate to two functions but only $\text{fn } y \Rightarrow y^6$ is possible in the real execution.

Summary

- 0-CFA: context-insensitive control-flow analysis.
 - ① Derive a set of equations
 - ② Solve the equations
- Possible extension: k -CFA