02/26/21 Recitation Notes

17-355/17-665/17-819: Program Analysis (Spring 2021)
Jeremy Lacomis

1 Reminders

- Homework 3 is due next **Tuesday, March 02, 2021 at 11:59pm EST**.

2 Program Analysis Correctness

In this recitation we will prove properties of a *Parity Analysis*. A parity analysis tracks if the value of an integer is odd or even at a program point.

Remember, to define a dataflow analysis, we need the following:

- A lattice $(L, \sqsubseteq)$. For parity analysis, $L = \{\top, O, V, \bot\}$ and $\bot \sqsubseteq \{O, V\} \sqsubseteq \top$ where $O \sqcup V = \top$
- An abstraction function α. For parity analysis, $\alpha : \mathbb{Z} \mapsto L$ and we define it as follows:

$$\alpha(n) = \begin{cases} V \text{ when } n \text{ is an even integer } (n \in \{2k : k \in \mathbb{Z}\}) \\ O \text{ when } n \text{ is an odd integer } (n \in \{2k+1 : k \in \mathbb{Z}\}) \end{cases}$$

- a flow function f_P
- initial dataflow analysis assumptions σ_0, in this case σ_0 maps all variables' initial states to $\top$.

2.1 Local (Un)soundness Proof

Remember from class that to prove the global soundness it is enough to show that the flow function is monotonic and locally sound. Assume that we have already proven monotonicity and we want to prove or disprove the following (incorrect) flow function for parity analysis.

$$f_P[\![a := b]\!](\sigma) = \sigma[a \mapsto O]$$

Remember, a flow function f is locally sound iff $P \vdash c_i \rightsquigarrow c_{i+1}$ and $\alpha(c_i) \sqsubseteq \sigma_{n_i}$ and $f[\![P[n_i]]\!](\sigma_{n_i}) = \sigma_{n_{i+1}} \Rightarrow \alpha(c_{i+1}) \sqsubseteq \sigma_{n_{i+1}}$

Proof. Case $f_P[\![a := 2]\!](\sigma_{n_i})$.

Assume $c_i = E, n$ and $\alpha(E) \sqsubseteq \sigma_{n_i}$

$\sigma_{n_{i+1}} = f_P[\![a := 2]\!](\sigma_{n_i}) = \sigma_{n_i}[a \mapsto O]$ (by definition)

$c_{i+1} = E[a \mapsto 2], n+1$ (by rule *step-assign*)

$\alpha(c_{n_{i+1}}) = \alpha(E[a \mapsto 2]) = \alpha(E)[a \mapsto \alpha_s(2)] = \alpha(E)[a \mapsto V]$ (by definition of α and α_s.)

Notice that $\alpha(E) \sqsubseteq \sigma_{n_i}$ by assumption, but $\alpha(c_{i+1}) = \alpha(E)[a \mapsto V] \not\sqsubseteq \sigma_{n_i}[a \mapsto O]$ because $\sqsubseteq$ is defined piecewise and $V \not\sqsubseteq {}_s O$. Therefore $\alpha(c_i) \sqsubseteq \sigma_{n_i} \wedge f_P[\![P[n_i]]\!](\sigma_{n_i}) = \sigma_{n_{i+1}} \not\Rightarrow \alpha(c_{i+1}) \sqsubseteq \sigma_{n_{i+1}}$ □

2.2 A Real Parity Flow Function

Now consider the following (correct) flow function.

$$f_P[\![a := b * c]\!](\sigma) = \begin{cases} \sigma[a \mapsto \bot] & \text{if } \sigma(b) = \bot \vee \sigma(c) = \bot \\ \sigma[a \mapsto O] & \text{if } \sigma(b) = O \wedge \sigma(c) = O \\ \sigma[a \mapsto V] & \text{if } (\sigma(b) = V \wedge \sigma(c) \neq \bot) \vee (\sigma(b) \neq \bot \wedge \sigma(c) = V) \\ \sigma[a \mapsto \top] & \text{if } (\sigma(b) = \top \wedge \sigma(c) \notin \{V, \bot\}) \vee (\sigma(b) \notin \{V, \bot\} \wedge \sigma(c) = \top) \end{cases}$$

2.3 Termination

To prove termination of an analysis we must prove that there are no infinite descending chains in the analysis lattice and that the flow functions are monotonic. Since our lattice is of finite height 2, we know we do not have any infinite descending chains.

Monotonicity A function f is *monotonic* $\iff \sigma_1 \sqsubseteq \sigma_2 \Rightarrow f(\sigma_1) \sqsubseteq f(\sigma_2)$

Proof. of monotonicity of the above flow function

Assume $\sigma_1 \sqsubseteq \sigma_2$
$\sigma_1(b) \sqsubseteq_s \sigma_2(b)$ and $\sigma_1(c) \sqsubseteq_s \sigma_2(c)$ (Since $\sqsubseteq$ is defined point-wise)

Case $(\sigma_1(b) = V \wedge \sigma_1(c) \neq \bot) \vee (\sigma_1(b) \neq \bot \wedge \sigma_1(c) = V)$

Since $\sigma_1(b) \sqsubseteq_s \sigma_2(b)$ and $\sigma_1(c) \sqsubseteq_s \sigma_2(c)$:
$(\sigma_2(b) \in \{V, \top\} \wedge \sigma_2(c) \neq \bot) \vee (\sigma_2(c) \in \{V, \top\} \wedge \sigma_2(b) \neq \bot)$

$$\therefore f_P[\![a := b * c]\!](\sigma_2) = \begin{cases} \sigma_2[a \mapsto V] & \text{if } (\sigma_2(b) = V \wedge \sigma_2(c) \neq \bot) \vee \\ & \quad (\sigma_2(c) = V \wedge \sigma_2(b) \neq \bot) \\ \sigma_2[a \mapsto \top] & \text{otherwise} \end{cases}$$

Since $\sqsubseteq$ is defined point-wise, $V \sqsubseteq_s V$, $V \sqsubseteq_s \top$, and $\sigma_1 \sqsubseteq \sigma_2$, we get
$f_P[\![a := b * c]\!](\sigma_1) = \sigma_1[a \mapsto V] \sqsubseteq f_P[\![a := b * c]\!](\sigma_2)$

□

2.3.1 Correctness

Now let's try showing that the above function is locally sound. Remember, a flow function f is locally sound iff $P \vdash c_i \rightsquigarrow c_{i+1}$ and $\alpha(c_i) \sqsubseteq \sigma_{n_i}$ and $f[\![P[n_i]]\!](\sigma_{n_i}) = \sigma_{n_{i+1}} \Rightarrow \alpha(c_{i+1}) \sqsubseteq \sigma_{n_{i+1}}$

Proof. of local soundness of the above flow function
Assume $f_P\ c_i = E, n$ and $\alpha(E) \sqsubseteq \sigma_{n_i}$
Then $c_{i+1} = E[a \mapsto m], n + 1$ for some m such that $E(b) * E(c) = m$ by rule *step-arith*
Now $\alpha(c_{i+1}) = \alpha(E[a \mapsto m]) = \alpha(E)[a \mapsto \alpha_s(m)]$ by the definitions of α and α_s

Case $m \in \{2k : k \in \mathbb{Z}\}$
Then $\alpha_s(m) = V$ and $E(b)$ is even or $E(c)$ is even
Thus $(\alpha_s(E(b)) = V \wedge \alpha_s(E(c)) \neq \bot) \vee$
$(\alpha_s(E(c)) = V \wedge \alpha_s(E(b)) \neq \bot)$

Since $\alpha(E) \sqsubseteq \sigma_{n_i}$, we get
$(\alpha_s(E(b)) = V \sqsubseteq_s \sigma_{n_i}(b) \wedge \alpha_s(E(c)) \neq \bot \sqsubseteq_s \sigma_{n_i}(c)) \vee$
$(\alpha_s(E(c)) = V \sqsubseteq_s \sigma_{n_i}(c) \wedge \alpha_s(E(b)) \neq \bot \sqsubseteq_s \sigma_{n_i}(b))$

From this we get $(\sigma_{n_i}(b) \in \{V, \top\} \wedge \sigma_{n_i}(c) \neq \bot) \vee (\sigma_{n_i}(c) \in \{V, \top\} \wedge \sigma_{n_i}(b) \neq \bot)$

$$\therefore \sigma_{n_{i+1}} = f_P[\![a := b * c]\!](\sigma_{n_i}) = \begin{cases} \sigma_{n_i}[a \mapsto V] & \text{if } (\sigma_{n_i}(b) = V \wedge \sigma_{n_i}(c) \neq \bot) \vee \\ & \quad (\sigma_{n_i}(c) = V \wedge \sigma_{n_i}(b) \neq \bot) \\ \sigma_{n_i}[a \mapsto \top] & \text{otherwise} \end{cases}$$

Since $\sqsubseteq$ is defined point-wise, $\alpha(E) \sqsubseteq \sigma_{n_i}$, $V \sqsubseteq_s V$, and $V \sqsubseteq_s \top$, we get
$\alpha(c_{i+1}) = \alpha(E)[a \mapsto V] \sqsubseteq \sigma_{n_{i+1}}$

Case $m \in \{2k + 1 : k \in \mathbb{Z}\}$
[Similar to the previous case and left up to the reader to prove as an exercise]

□