

1 Source Language

$\langle \text{statement} \rangle ::= \langle \text{statement} \rangle \langle \text{statement} \rangle$
 $\quad | \text{ 'if' } (\langle \text{expression} \rangle) \{ \langle \text{statement} \rangle \} \text{ 'else' } \{ \langle \text{statement} \rangle \}$
 $\quad | \text{ 'return' } \langle \text{expression} \rangle \text{ ';'}$
 $\quad | \langle \text{expression} \rangle \text{ ';'}$

$\langle \text{expression} \rangle ::= \langle \text{variable} \rangle \mid \langle \text{literal} \rangle$
 $\quad | (\langle \text{expression} \rangle)$
 $\quad | \langle \text{expression} \rangle \langle \text{binop} \rangle \langle \text{expression} \rangle$
 $\quad | \langle \text{unop} \rangle \langle \text{expression} \rangle$

$\langle \text{binop} \rangle ::= \text{ '+' } \mid \text{ '-' } \mid \text{ '*' } \mid \text{ '/' } \mid \text{ '%'}$
 $\quad | \text{ '&&' } \mid \text{ '||' }$
 $\quad | \text{ '&' } \mid \text{ '|' } \mid \text{ '<<' } \mid \text{ '>>' }$
 $\quad | \text{ '==' } \mid \text{ '<=' } \mid \text{ '>=' } \mid \text{ '<' } \mid \text{ '>' }$

2 Symbolic Execution

2.1 Expressions

$$\frac{}{\langle S; v \rangle \Downarrow \langle S; v \rangle} \text{ LITERAL}$$

2.2 Statements

$$\frac{\langle S; e \rangle \Downarrow \langle S'; s \rangle}{\langle S; e \rangle \Downarrow \langle S'; \emptyset \rangle} \text{ EXPRESSION}$$

$$\frac{\langle S; c_1 \rangle \Downarrow \langle S_1; s_1 \rangle \quad \langle S_1; c_2 \rangle \Downarrow \langle S_2; s_2 \rangle}{\langle S; c_1 \ c_2 \rangle \Downarrow \langle S_2; s_2 \rangle} \text{ SEQUENCE}$$

$$\frac{\begin{array}{l} \langle S; e \rangle \Downarrow \langle S_1; g_1 \rangle \quad g(S) \not\Rightarrow g_1 \quad g(S) \not\Rightarrow \neg g_1 \\ \langle S_1[g \mapsto g(S_1) \wedge g_1]; c_1 \rangle \Downarrow \langle S_2; s_2 \rangle \\ \langle S_1[g \mapsto g(S_1) \wedge \neg g_1]; c_1 \rangle \Downarrow \langle S_3; s_3 \rangle \\ S' = \langle (g_1 ? g(S_2) : g(S_3)); (g_1 ? \rho(S_2) : \rho(S_3)); (g_1 ? \mu(S_2) : \mu(S_3)) \rangle \end{array}}{\langle S; \text{if } e \ \{ \ c_1 \} \ \text{else} \ \{ \ c_2 \} \rangle \Downarrow \langle S'; \emptyset \rangle} \text{ IFELSE}$$

$$\frac{\langle S; e \rangle \Downarrow \langle S_1; g_1 \rangle \quad g(S) \Rightarrow g_1 \quad \langle S_1; c_1 \rangle \Downarrow \langle S_2; s \rangle}{\langle S; \text{if } e \ \{ \ c_1 \} \ \text{else} \ \{ \ c_2 \} \rangle \Downarrow \langle S_2; \emptyset \rangle} \text{ IFTRUE}$$

$$\frac{\langle S; e \rangle \Downarrow \langle S_1; g_1 \rangle \quad g(S) \Rightarrow \neg g_1 \quad \langle S_1; c_2 \rangle \Downarrow \langle S_2; s \rangle}{\langle S; \text{if } e \ \{ \ c_1 \} \ \text{else} \ \{ \ c_2 \} \rangle \Downarrow \langle S_2; \emptyset \rangle} \text{ IFFALSE}$$

2.3 Memory

$$\frac{\rho(S)[x] = s}{\langle S; x \rangle \Downarrow \langle S; s \rangle} \text{VAR}$$

$$\frac{x \notin \text{dom } \rho(S)}{\langle S; \tau \ x \rangle \Downarrow \langle S[\rho \mapsto (\rho(S), (x \rightarrow \emptyset))]; s \rangle} \text{DECLARELOCAL}$$

$$\frac{x \notin \text{dom } \rho(S) \quad \langle S; e \rangle \Downarrow \langle S'; s \rangle}{\langle S; \tau \ x = e \rangle \Downarrow \langle S'[\rho \mapsto (\rho(S'), (x \rightarrow s))]; s \rangle} \text{DECLAREASSIGNLOCAL}$$

$$\frac{\langle S; e_1 \rangle \Downarrow \langle S_1; \text{ptr } x \rangle \quad x \in \text{dom } \rho(S_1) \quad \langle S_1; e_2 \rangle \Downarrow \langle S_2; s \rangle}{\langle S; *e_1 = e_2 \rangle \Downarrow \langle S_2[\rho \mapsto (\rho(S_2), (x \rightarrow s))]; s \rangle} \text{UPDLOCAL}$$

$$\frac{\langle S; e_1 \rangle \Downarrow \langle S_1; s_1 \rangle \quad s_1 \neq \text{ptr } x \quad \langle S_1; e_2 \rangle \Downarrow \langle S_2; s_2 \rangle}{\langle S; *e_1 = e_2 \rangle \Downarrow \langle S_2[\mu \mapsto (\mu(S_2), (s_1 \rightarrow s_2))]; s_2 \rangle} \text{UPDGLOBAL}$$

$$\frac{\langle S; e \rangle \Downarrow \langle S'; \text{ptr } x \rangle \quad \rho(S')[x] = s}{\langle S; *e \rangle \Downarrow \langle S'; s \rangle} \text{SELLOCAL}$$

$$\frac{\langle S; e \rangle \Downarrow \langle S'; \text{ptr } x \rangle \quad \rho(S')[x] = s}{\langle S; *e \rangle \Downarrow \langle S'; s \rangle} \text{SELGLOBAL}$$