LOGICAL ENCODING OF PROGRAMS

$\{P\}\ S\ \{Q\}$ is VALID

iff

FOL formula is VALID

---

simple programming language

$P ::= x := a \quad (x \leftarrow a)$

(a: arithmetic expression)

| if b then P_1 else P_2

| $P_1 ; P_2$

The set of variables is V

a state $s : V \to \mathbb{Z}$

$\langle P, s \rangle \to s'$

Transition Relations

$T(V, V')$

$T(s, s')$

e.g. $x := x + 1$

$V = \{x\}$

$V' = \{x'\}$ $\quad V'' = \{x''\}$

transition relation

$\{(n, n+1) \mid n \in \mathbb{Z}\}$

$T(x, x')$

$T(0, 1)$ ✓

$T(1, 0)$

FOL formulas in LIA (linear integer arithmetic)

$$\varphi := a_1 = a_2 \mid a_1 \leq a_2 \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \neg\varphi \mid \exists x.\, \varphi \mid \forall x.\, \varphi$$

$c_0 + c_1 x_1 + c_2 x_2 + \cdots + c_n x_n$ ($c_i \in \mathbb{Z}$, x_i are variables)

e.g. $2x + 3y \geq 0 \wedge x + z < 10$

e.g. $x + y > 0$

$m = \{x \mapsto 1,\ y \mapsto 2\}$

$m \models x + y > 0$

Encoding the transition relation

① $x := a$

e.g. $x := x+1$

x	x'
0	1
1	2
⋮	⋮

$x' = x+1$

$M = \{x' \mapsto 1, x \mapsto 0\}$

Encoding $x := a$ $\quad enc(x := a)$

$$\varphi \equiv x' = a \wedge \bigwedge_{y \neq x, y \in V} y' = y$$

E.g. $x := x+y$

$V = \{x, y\}$

$$T(x, y, x', y') \equiv x' = x+y \wedge y' = y$$

Encoding if b then P_1 else P_2

$$enc(\text{if } b \text{ then } P_1 \text{ else } P_2) = (b \Rightarrow enc(P_1)) \wedge (\neg b \Rightarrow enc(P_2))$$

E.g. if $x > 0$ then $x := x+1$ else $x := y$

$$enc(\text{if} \ldots) \equiv (x > 0 \Rightarrow x' = x+1 \wedge y' = y) \wedge (x \leq 0 \Rightarrow x' = y \wedge y' = y)$$

E.g. $x := x+1 \; ; \; y := y+1$

$$\exists x'', y''. \left(\begin{array}{l} x'' = x+1 \wedge \\ y'' = y \end{array} \right) \wedge \left(\begin{array}{l} y' = y''+1 \\ \wedge \, x' = x'' \end{array} \right)$$

$$T_1(x, y, x', y') \equiv x' = x+1 \wedge y' = y$$

$$T_2(x, y, x', y') \equiv y' = y+1 \wedge x' = x$$

$T_1(x, y, x'', y'') \wedge T_2(x'', y'', x', y')$

General form:

$$enc(P_1 ; P_2) \equiv$$
$$\exists V''.\ T_1(V, V'') \wedge T_2(V'', V')$$

where $T_1(V, V') = enc(P_1)$

$T_2(V, V') = enc(P_2)$

Soundness / completeness of encoding

$s, s' : V \to \mathbb{Z}$

$m : V \cup V' \to \mathbb{Z}$

Soundness: Fix a program P.

Let $m \models enc(P)$

$s = \{v \mapsto m(v) \mid v \in V\}$

$s' = \{v \mapsto m(v') \mid v \in V\}$

Then $\langle P, s \rangle \to s'$

Completeness: Let $\langle P, s \rangle \to s'$

Let $m = \{v \mapsto s(v) \mid v \in V\}$

$\cup \{v' \mapsto s'(v) \mid v \in V\}$

$m \models enc(P)$

VERIFICATION

$\{\phi\}\ P\ \{\psi\}$

represented in LIA, e.g. $x > 0$

for any state $s \in \phi$, if $\langle P, s\rangle \to s'$ then $s' \in \psi$

$$\boxed{\phi \wedge enc(P) \Longrightarrow \psi'}$$ is VALID

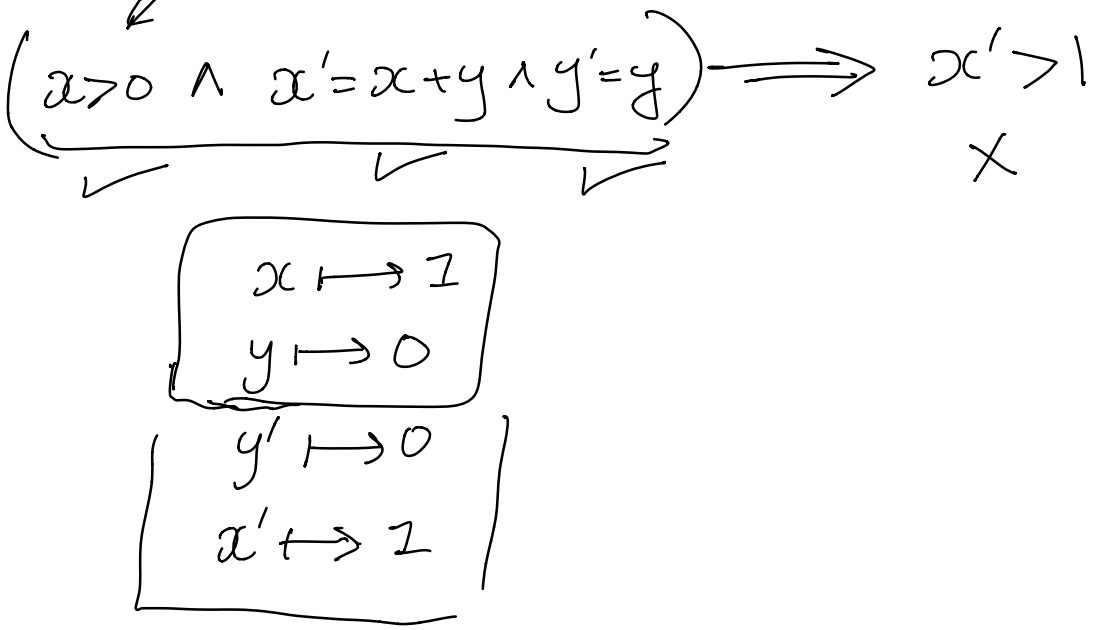
iff

$\{\phi\}\ P\ \{\psi\}$ is VALID / TRUE

E.g. $\{x > 0\}\ x := x + 1\ \{x > 1\}$

$$(x > 0 \wedge x' = x + 1) \Longrightarrow x' > 1$$

E.g. $\{x>0\}\ x := x+y\ \{x>1\}$


$(x>0 \wedge x'=x+y \wedge y'=y) \Longrightarrow x'>1$
X
$x \mapsto 1$
$y \mapsto 0$
$y' \mapsto 0$
$x' \mapsto 1$

programs of the form

$$P_{pre}\ ;\ \text{while } b \text{ do } P_{body}$$

$$T_{pre}(V, V') \wedge \left(\bigwedge_{i=1}^{n} b^i \wedge T_{body}(V^i, V^{i+1}) \right) \wedge \neg b^{n+1}$$

loop exit

"symbolic execution"

"bounded model checking"