VERIFICATION WITH HORN CLAUSES

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

loop free

encode P as a transition relation $T(v,v')$

$$\phi \land T(v,v') \implies \psi'$$

$\{x > 0\}$

$y := x$

$z := x + y$

$\{z > 0\}$

$$\frac{\{\phi\}\ P_1\ \{\chi\} \qquad \{\chi\}\ P_2\ \{\psi\}}{\{\phi\}\ P_1 ;\ P_2\ \{\psi\}}$$

$\{x>0\}\ y := x\ \{x>0 \land y>0\}$

$\{x>0 \land y>0\}\ z := x+y\ \{z>0\}$

① $\{x>0\}\ y := x\ \{r(x,y,z)\}$

② $\{r(x,y,z)\}\ z := x+y\ \{z>0\}$

Find an interp. of $r(x,y,z)$ s.t. both of the above are valid Hoare triples

$$C_1 \triangleq \forall V, V'.\ x > 0 \land enc(y := x) \implies r(x', y', z')$$

$y' = x$
$\land\ x' = x$
$\land\ z' = z$

$C_2 \triangleq \forall V, V' . \, r(x,y,z) \wedge enc(z := x+y) \Longrightarrow z' > 0$

Q: Is $C_1 \wedge C_2$ SAT

$M \models C_1 \wedge C_2$

interpretation for $r(x,y,z)$

$p \wedge q \wedge r \Longrightarrow s$ Horn Clause

Constrained Horn clauses (CHC)

general form:

$$\underbrace{\underbrace{r_1(V_1) \wedge r_2(V_2) \wedge r_3(V_3)}_{\text{unknown relations}} \wedge \cdots \wedge \varphi}_{\text{BODY}} \Rightarrow \underbrace{H_c}_{\text{HEAD}}$$

formula with no unknowns

head of the clause

$C = \{c_1, \ldots, c_n\}$

C is SAT iff there is an interpretation of unknown relations that make all clauses VALID

LOOPs

$P ::= P_{pre} \; ; \; \text{while } \underline{b} \text{ do } P_{body}$

before loop

loop body

loop free

invariant

1 $\{\phi\}\; P_{pre}\; \{I\}$ initiation

2 $\{I \wedge b\}\; P_{body}\; \{I\}$ consecution

3 $\{I \wedge \neg b\}\; \text{skip}\; \{\psi\}$ safety

GOAL: $\{\phi\}\; P\; \{\psi\}$

drop $\forall V, V'$ for clarity

$C_1 \triangleq \phi \wedge enc(P_{pre}) \Longrightarrow I(V')$

$C_2 \triangleq I(V) \wedge b \wedge enc(P_{body}) \Longrightarrow I(V')$

$C_3 \triangleq I(V) \wedge \neg b \Longrightarrow \psi$

$\{x \geq 0 \wedge y > 0\}$

$r := x$
$q := 0$

P_{pre}

$V = \{x, y, r, q\}$

while $r \geq y$ b

$r = r - y$
$q = q + 1$

P_{body}

$\{x = y * q + r \wedge 0 \leq r < y\}$

$\{x \geq 0 \wedge y > 0\}\; P_{pre}\; \{I\}$

$I = x = y*q + r \wedge r \geq 0$

initiation

$x \geq 0 \wedge y > 0 \wedge enc(P_{pre}) \Longrightarrow I(V')$

consecution

$I(V) \wedge r \geq y \wedge enc(P_{body}) \Longrightarrow I(V')$

safety

$I(V) \wedge r < y \Longrightarrow (x = y*q + r \wedge 0 \leq r < y)$

$$\{ x = y * q + r \land r \geq 0 \land r \geq y \}$$

$$r = r - y$$

$$q = q + 1$$

$$\{ x = y * q + r \land r \geq 0 \}$$

```
mc(p):
    if p > 100
        r := p - 10

    else
        p1 := p + 11
        p2 := mc(p1)
        r := mc(p2)
```

$$\{\text{true}\} \quad mc(p) \quad \{ r \geq 91 \}$$

$mc(p, r)$

C_1 (base case)

$$p > 100 \land r = p - 10 \implies mc(p, r)$$

C_2 (recursion)

$$p \leq 100 \land p_1 = p + 11 \land mc(p_1, p_2) \land mc(p_2, r) \implies mc(p, r)$$

safety $\quad mc(p, r) \implies r \geq 91$

Q: Find a definition of

$mc(p, r)$

$\{x > 0\}$

① if $x > 5$

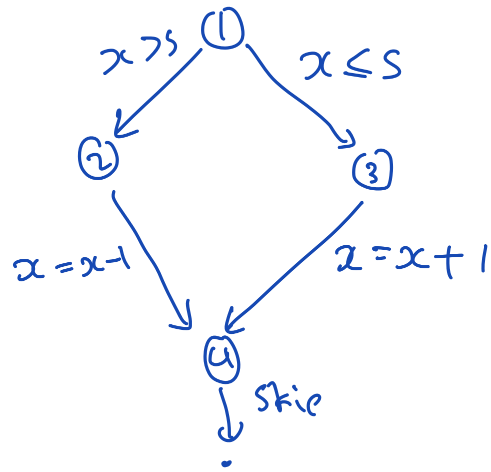
② $x = x - 1$

else

③ $x = x + 1$

④ skip

$\{x > 0\}$



$$I_1(x) \wedge x > 5 \Longrightarrow I_2(x)$$

$$I_1(x) \wedge x \leq 5 \Longrightarrow I_3(x)$$

$$I_2(x) \wedge x' = x - 1 \Longrightarrow I_4(x')$$

$$I_3(x) \wedge x' = x + 1 \Longrightarrow I_4(x')$$

$$x > 0 \Longrightarrow I_1(x)$$

$$I_4(x) \Longrightarrow x > 0$$