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

loop-free

trans(v, v')

$$\phi \wedge \text{trans}(v, v') \Rightarrow \psi'$$

E.g. $\{x > 0\}$

① $y := x$;

② $z := x + y$;

$\{z > 0\}$

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

unknown formula ψ

$\{x > 0\}\ y := x\ \{r(x, y, z)\}$

$\{r(x, y, z)\}\ z := x + y\ \{z > 0\}$

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

① $\{x>0\}\ y:=x\ \{x>0 \wedge y>0\}$

② $\{x>0 \wedge y>0\}\ z:=x+y\ \{z>0\}$

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

$y'=x$
$\wedge\ x'=x$
$\wedge\ z'=z$

uninterpreted.

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

Is $C_1 \wedge C_2$ satisfiable?

$$M \models C_1 \wedge C_2$$

an interpretation of the relation "r"

Horn clauses (or constrained Horn clauses)

$$\underbrace{\underbrace{r_1(\vec{v}_1) \wedge r_2(\vec{v}_2) \wedge \dots \wedge r_{n-1}(\vec{v}_{n-1})}_{\text{unknown relations}} \wedge \varphi}_{\text{BODY}} \Longrightarrow \underbrace{H_c}_{\text{HEAD}}$$

standard interpreted formula enc$(\dots)$

either relation or interpreted formula

$$C = \{c_1, c_2, \dots, c_n\}$$

C is satisfiable if there is an interpretation of r_i that makes the clauses VALID

Loops

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

loop-free

prove that $\{\phi\} P \{\psi\}$

① the invariant is true when we finish P_{pre}

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

② the invariant must remain true as the loop executes

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

③ when the loop exits, postcondition is satisfied

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

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

$$\left.\begin{array}{ll} ① & r := x \\ ② & q := 0 \end{array}\right\} P_{pre}$$

③ while $\boxed{r \geq y}$ b

$$\left.\begin{array}{ll} ④ & r := r - y \\ ⑤ & q := q + 1 \end{array}\right\} P_{body}$$

⑥ skip

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

$$C_1 \triangleq x \geq 0 \wedge y > 0 \wedge enc(P_{pre}) \Longrightarrow I(x', y', r', q')$$

$$C_2 \triangleq I(x, y, r, q) \wedge r \geq y \wedge enc(P_{body}) \Longrightarrow I(x', y', r', q')$$

$$C_3 \triangleq I(x, y, r, q) \wedge \underbrace{r < y}_{\neg b} \Longrightarrow \begin{pmatrix} x = y * q + r \wedge \\ 0 \leq r < y \end{pmatrix}$$

Every statement P will have a line number $L(P)$

$L_1(P)$ the line number of the next stmt

$L_2(P)$ the other possible line number

$$encH(x := a) = I_i(V) \wedge enc(x := a) \Rightarrow I_j(V')$$

$$L(x := a) = i \qquad L_1(x := a) = j$$

$$\{I_i(V)\}\ x := a\ \{I_j(V)\}$$

$$encH(\text{if } b \text{ then } P_1 \text{ else } P_2) =$$

$$I_i(V) \wedge b \Rightarrow I_j(V)$$

$$I_i(V) \wedge \neg b \Rightarrow I_k(V)$$

$$L(P) = i, \quad L_1(P) = j, \quad L_2(P) = k$$

$$encH(\text{while } b \text{ do } P) =$$

$$I_i(V) \wedge b \Rightarrow I_j(V)$$

$$I_i(V) \wedge \neg b \Rightarrow I_k(V)$$

$$\{\phi\} \ldots\ldots \{\psi\}$$

$$\phi \Rightarrow I_1(V)$$

$$I_{ex}(V) \Rightarrow \psi$$

E.g. $\{x>0\}$

① if $x>5$

② $\quad x = x-1$

else

③ $\quad x = x+1$

④ skip;

$\{x>0\}$

① $I_1(x) \wedge x>5 \Longrightarrow I_2(x)$ then

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

② $I_2(x) \wedge x' = x-1 \Longrightarrow I_4(x')$

③ $I_3(x) \wedge x' = x+1 \Longrightarrow I_4(x')$

$x>0 \Longrightarrow I_1(x)$

$I_4(x) \Longrightarrow x>0$

$\underline{mc(p)}$: // McCarthy 91

if $p > 100$

$r := p - 10$

else

$p_1 := p + 11$

$p_2 := mc(p_1)$

$r := mc(p_2)$

$$\{true\}\ r := mc(p)\ \{r \geq 91\}$$

---

treat $mc(p, r)$ as a relation in FOL

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

$$\underbrace{p \leq 100 \wedge p_1 = p + 11 \wedge mc(p_1, p_2) \wedge mc(p_2, r) \implies mc(p, r)}_{\text{Encode } mc(p,r)}$$

$$\underbrace{true}_{\text{pre}} \wedge mc(p, r) \implies \underbrace{r \geq 91}_{\text{post}}$$