CLASS 9  HOARE TRIPLES p+2

Last time:
{p35} print n
specific
σ = {p35} no bug when run in
σ = {p35} but might not terminate
{p35 < t3}

Examples

\[
\begin{align*}
q &\geq 03 \quad y := \sqrt{x} \{ y = \sqrt{3} \\
q &\geq 03 \quad y := \sqrt{x} \{ y \geq 0 \}
\end{align*}
\]

Loops
\[
W \equiv \text{while } i \neq 0 \text{ do } i := i - 1 \text{ od}
\]

\[
\begin{align*}
\{ i \geq 03 \} \quad W \{ i = 03 \} &\quad \text{doesn't terminate} \\
\forall i &\quad \{ i \geq 03 \} \quad W \{ i = 03 \} \\
\forall i &\quad \{ i < 0 \} \quad W \{ i = 03 \} \\
\{ i < 0 \} &\quad \{ i \geq 03 \} \quad \text{valid for partial correctness}
\end{align*}
\]
\textbf{Alg: } \text{while } i \geq 0 \text{ do }
\begin{align*}
&i := i-1 \text{ mod } d \\
&T_0 := \{ i \geq 0 \Rightarrow i = 0 \} \quad \text{if } i \text{ starts } < 0
&i := \max(i_0, i) \\
&T_0 := \{ i \geq 0 \Rightarrow i = 0 \} \quad \text{if } i_0 < 0 \Rightarrow i = i_0
&i \text{ is unchanged}
\end{align*}

\begin{align*}
&T_3 \quad \text{also correct}
&\text{while } i > 0 \text{ do } \text{false}
&T_3 \quad \text{invariant}
\end{align*}

\text{Invariant: } i := 0; s := 0 \\
\text{Need that } s = \sum(i) \text{ to add range on } i
\text{ guarantee}
Why notate like that?
because \( 0 \leq i \leq n \) and \( 5 = \text{sum}(i) \)
is needed by next piece of code:
\[
\{ \text{for} \ i = 0; \ s1 = 0; \text{while} \ i < n \text{ do} \text{printf} 5 \}
\]
needed here

If \( \{ p^3 \ s1 \ q^3 \} \) and \( \{ q^3 \ s2 \ r^3 \} \) are valid
then so is \( \{ p^3 \ s1 \cdot s2 \cdot r^3 \} \)
sequence rule
gets justified by analyzing semantics of
triples and sequences

---

Reasoning about assignments - Two techniques
\( \{ \text{given} \} \ x := e \ 3 \ \text{infer} \ x := e \) forward
\( \{ \text{infer} \} \ x := e \ \{ \text{given} \} \) backward
given predicate for \( P(x) \)

\[ F = \{ P(e) \} \quad \text{x := e} \quad \{ P(x) \} \quad \text{by \textit{asg} rule} \]

\( e \) is even \( x \) is even

\[ F = \{ 2+k \text{ is even} \} \quad \text{x := 2 + k} \quad \{ x \text{ is even} \} \]

\( 2 + 5 \text{ is even} \quad \text{x := 2 + 5} \quad \{ x \text{ is even} \} \]

Semantics: If \( \sigma \models P(e) \) then \( M(x := e, \sigma) \models P(x) \)

\text{Asg Lemma}

\[ \text{clg notation} \]

\[ R(x, k) = x = \text{sum}(0, k) \]

\[ \{ R(s, k + 1) \} \quad k := k + 1 \quad \{ R(s, k) \} \]

\[ s = 0 + t + 1 + k + 1 \quad s = 0 + t + 2 + \ldots + k \]

\[ \{ R(s + k + 1, k + 1) \} \quad s := s + k + 1 \quad \{ R(s, k + 1) \} \]

\[ s + k + 1 = 0 + t + \ldots + k + 1 \quad s = 0 + t + \ldots + k + 1 \]

both k's

\[ \text{clg ed} \]

\[ \{ R(s + k + k) \} \quad s := s + k \quad \{ R(s, k) \} \]

\[ k := k + 1 \quad \{ R(s + k, k) \} \]
Changing preconditions/postconditions of given triples \( H \) \( S \) \{9\}

\( \{x \geq 0\} y = x \{x \geq 0\} \)

If we know \( \{x \geq 0\} y = x \{y \geq 0\} \)
then changing \( x \geq 0 \) to \( x \geq 0 \) is ok

\( S = \{x \geq 0\} \rightarrow S = \{x \geq 0\} \)

precondition strengthening new prop. satisfied by smaller set of states

If \( q \Rightarrow r \) then \( q \) is stronger than \( r \)
\( r \) is weaker than \( q \)
(real is "stronger than or equal to"
"weaker than or equal to")

If \( q \Rightarrow r \) then \( q \) stronger than \( q \Rightarrow r \)
\( q \Rightarrow r \) stronger than \( q \Rightarrow r \)
\( q \) and \( r \) are actually of equal strength
$p \rightarrow q$

sets of states

$\sigma_1 = p$

and

$\sigma_1 \not\in p \land \sigma_1 \notin q$

neither $p \rightarrow q$

nor $q \rightarrow p$

$\sigma_2 \in p$ and $\sigma_2 \notin q$

$\sigma_3 \notin q$ and $\sigma_3 \in \overline{p}$

Preconditions can always be strengthened

If $p' \rightarrow p$ and $\{p35|9\}$

then $\{p'38|9\}$

Postconditions can always be weakened

If $p35(|9)$ and $9 \rightarrow 9'$

then $\{p38|9,3\}$
Doesn't mean you always want to str. pre. weaker pos...

sequence of nested circles

\[
\begin{align*}
G_1 & \\
G_2 & \\
G_3 &
\end{align*}
\]

\[
\text{Stronger takes } \ r_1 \to r_2 \to r_3 \to r_4
\]

\[
\text{Satisfying set of states gets smaller}
\]

\(\emptyset\) is the strongest In limit, we get to \(\emptyset\)

Set of states
False is strongest pred.

Expanding \(r_4 \to r_3 \to r_2 \to r_1\) on weakening

Limit is \(\sum\) all states True
Which set \(T\)?

\(T\) is the weakest predicate
easier for pair to fix bugs

ok when \( x > 0 \) bug gets

\[ \{ x \geq 0 \} \land \{ q \} \]

fails when \( x = 0 \):

\[ \{ x \geq 0 \} \land \{ q \} \]

oh yes, I meant\n
\( x > 0 \) don't do that

weak \[ \{ p \} \land \{ y \geq 0 \} \]

post \[ \{ p \} \land \{ y \geq 0 \} \]

but if this one \[ \{ p \} \land \{ y \geq 0 \} \]

leads to \( y = 0 \)

It's a feature, less satisfying for users