Class 16 CS 536 Thu 3/18

Today - from last section
They behind loop invariants
Then full proofs (no outlines)

Loop rule

\[ P \Rightarrow S \{ P \} \]

\[ \text{line } P \text{ while } B \text{ do } S \text{ od } P \Rightarrow B \]

Why invariants - why not wp / sp?

- Because they might not be verifiable in a finite way

Say we start spec. of \( W \) in the loop

in state \( \sigma_0 \)

\[
\begin{align*}
\text{stop} \quad \text{while test } \sigma_0 \quad 0 \text{ iterations} \\
\text{at} \quad \forall i \quad \sigma_i = M(S_0, \sigma_0) \quad 1 \text{ iteration } P \Rightarrow S \{ P \} \\
\text{after } B \quad \sigma_i = M(S_1, \sigma_i) \quad 2 \text{ iterations } P \Rightarrow S \{ P \} \\
\sigma_k = B \quad k \text{ iterations} \\
\text{sp of } W = (P \Rightarrow B) \cup Q \Rightarrow B \Rightarrow Q \Rightarrow B
\end{align*}
\]
Use invariants to approximate \( wp(sp) \)

\[ (p \land B) \land S \land sp(p \land B, S) \]

\( p \land B \) imply \( sp \) loop body

\[ \{ wp(S, p) \} S \land p \]

\( p \land B \) approximates \( wp \) of loop body

For entire loop, \( p \) is approx to \( wp, sp \)

\[ \{ p \land B \} W \land \{ p \land B \} \]

sp of loop implies

\[ sp(p \lor w) \Rightarrow p \land \neg B \]

\[ \{ p \land B \} \]

wp of \( w \lor p \land B \)

\[ p \Rightarrow wp(w, p \land B) \]
On to class 16 - full proofs + outlines, proof rule for triple Hilbert style proof \[ \text{assumption} \]

\[ \text{judgment} \]

\[ \text{reason} \]

\[ \text{each reason can} \]

\[ \text{appeal to earlier judgment} \]

We've seen that we can get multiple proofs of same conclusion using different programs (little differences)

\[ \text{conclusion} \]

\[ S = \text{sum}(0, n) \]

\[ S = \text{sum}(0, k) \land k = n \]

\[ S = \text{sum}(1, k+1) \land k+1 = n \]

Slight diff's in initialization

\[ S = \text{sum}(0, k-1) \land k-1 = n \]

Test + body

\[ S = \text{sum}(0, j) \land j = n \]

\[ S = \text{sum}(0, j+1) \land j+1 = n \]

et cetera
Also, proofs can differ in what order they present lines just need to refer to earlier lines (orders not significant) seq 1, 2 seq 2, 1

Can often prove things in > 1 way
\[ p \rightarrow \text{wp}(x_1 = e, q) \]
\[ p \rightarrow p \rightarrow \text{wp}(x_1 = e, q) \]
\[ p \rightarrow \text{wp}(x_1 = e, q) \]
\[ \text{pred logic} \]
\[ \text{pre. stmt} 1 \]

\[ p \rightarrow \text{wp}(x_1 = e, q) \]
\[ \text{sp(p,x_1 = e)} \]
\[ \text{pred logic} \]
\[ \text{post. stmt. 1, 2} \]

Sequences — take up of both starts or one of each
Full proof outlines

Formal proofs are long, involve a lot of rewriting.

Use full proof outlines to cut down on text.

Full proof outline expands to formal proof.

Exp. not unique, typically.

Full outline includes a triple for every proof line (except predicate logic).

Every triple in outline must be provable using the pf. rules.

For weakening & strengthening, we write the two predicates next to each other.

\[ \begin{cases} n \geq 0, k = 0; & n \geq 0, k = 0 \Rightarrow s = 0 \Rightarrow n \geq 0, k = 0 \\{ \text{pr} \} \text{ } n \geq 0 \Rightarrow s = 0 \end{cases} \]

Predicate on left must imply predicate on right (predicate logic).
1. \{n \geq 0 \} \land k = 0 \iff n \geq 0 \land k = 0

2. \{n > 0 \} \land k = 0 \iff n > 0 \land k = 0

3. \{n > 0 \} \land k = 0 \iff \{n > 0 \} \land k = 0

4. \{n > 0 \} \land k = 0 \iff \{n > 0 \} \land k = 0

5. \{n > 0 \} \land k = 0 \iff \{n > 0 \} \land k = 0

6. \{n > 0 \} \land k = 0 \iff \{n > 0 \} \land k = 0

\text{seq 1, 2, 3, 4, 5, 6}

\{n > 0 \} \land k = 0 \iff \{n > 0 \} \land k = 0

1. \{p_i \mid [0/5] \} \land s = 0 \iff \{p_i \mid [0/5] \} \land s = 0

2. \{p_i \mid [0/5] \} \land s = 0 \iff \{p_i \mid [0/5] \} \land s = 0

3. n > 0 \land p_i \mid [0/5] \land s = 0 \iff \{p_i \mid [0/5] \} \land s = 0

4. n > 0 \land p_i \mid [0/5] \land s = 0 \iff \{p_i \mid [0/5] \} \land s = 0

5. n > 0 \land p_i \mid [0/5] \land s = 0 \iff \{p_i \mid [0/5] \} \land s = 0

\text{seq 4, 1}

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

\[ P_i \mid [0/5] \land s = \text{sum}(0, k) \]

\[ P_i \mid [0/5] \land [0/5] = 0 \leq k \leq n \land n = \text{sum}(0, k) \]

\[ P_i \mid [0/5] \land [0/5] = 0 \leq 0 \leq n \land n = \text{sum}(0, 0) \]