CSC410

Azadeh Farzan

Fall 2020
How do we deal with large programs?
Modularity!
This is Hoare Triple:

\[
\{ p \} \ S \ \{ q \}
\]

S: is a program.
Hoare Triples are like the lego pieces for proofs!
Axioms and Rules of Hoare Logic
AXIOM 1: SKIP

\[
\{p\} \text{ skip} \{p\}
\]

AXIOM 2: ASSIGNMENT

\[
\{p[u := t]\} \ u := t \ \{p\}
\]
Example

\{\text{true}\} \quad x := 1 \quad \{x > 0\}

\{y > 0\} \quad x := y \quad \{x > 0\}
3.3 Verification

Clearly, all three formulas are true in the sense of partial correctness. Also \{ x = 2 \land \forall i \geq 2: a[i] = 1 \} is true in the sense of partial correctness. This correctness formula states that every computation of \( S \) that begins in a state which satisfies \( x = 2 \land \forall i \geq 2: a[i] = 1 \), diverges. Namely, if there existed a finite computation, its final state would satisfy \( false \) which is impossible.

\[ \square \]

Partial Correctness

As we have seen in Examples 3.1 and 3.2, reasoning about correctness formulas in terms of semantics is not very convenient. A much more promising approach is to reason directly on the level of correctness formulas. Following Hoare [1969], we now introduce a proof system, called \( PW \), allowing us to prove partial correctness of \( while \) programs in a syntax-directed manner, by induction on the program syntax.

**PROOF SYSTEM PW:**
This system consists of the group of axioms and rules 1–6.

**AXIOM 1: SKIP**
\[
\{ p \} \text{skip} \{ p \}
\]

**AXIOM 2: ASSIGNMENT**
\[
\{ p [u := t] \} \quad u := t \{ p \}
\]

**RULE 3: COMPOSITION**
\[
\{ p \} S_1 \{ r \}, \quad \{ r \} S_2 \{ q \}
\]

\[
\{ p \} S_1; \quad S_2 \{ q \}
\]

**RULE 4: CONDITIONAL**
\[
\{ p \land B \} S_1 \{ q \}, \quad \{ p \land \neg B \} S_2 \{ q \}
\]

if \( B \) then \( S_1 \) else \( S_2 \) fi \{ q \}

**RULE 5: LOOP**
\[
\{ p \land B \} S \{ p \}
\]

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

while \( B \) do \( S \) od \{ q \}
3.3 Verification

Clearly, all three formulas are true in the sense of partial correctness. Also \(\{x = 2 \land \forall i \geq 2: a[i] = 1\}\) \(S\{\text{false}\}\) is true in the sense of partial correctness. This correctness formula states that every computation of \(S\) that begins in a state which satisfies \(x = 2 \land \forall i \geq 2: a[i] = 1\), diverges. Namely, if there existed a finite computation, its final state would satisfy \(\text{false}\) which is impossible. \(\square\)

Partial Correctness

As we have seen in Examples 3.1 and 3.2, reasoning about correctness formulas in terms of semantics is not very convenient. A much more promising approach is to reason directly on the level of correctness formulas. Following Hoare [1969], we now introduce a proof system, called \(PW\), allowing us to prove partial correctness of \(\text{while}\) programs in a syntax-directed manner, by induction on the program syntax.

PROOF SYSTEM \(PW\):

This system consists of the group of axioms and rules 1–6.

**AXIOM 1: SKIP**

\[\{p\}\ \text{skip}\ \{p\}\]

**AXIOM 2: ASSIGNMENT**

\[\{p[i]:=t\}\ u:=t\ \{p\}\]

**RULE 3: COMPOSITION**

\[\{p\}\ S_1\ \{r\},\ \{r\}\ S_2\ \{q\}\ \{p\}\ S_1;\ S_2\ \{q\}\]

**RULE 4: CONDITIONAL**

\[\{p \land B\}\ S_1\ \{q\},\ \{p \land \neg B\}\ S_2\ \{q\}\ \{p\}\ \text{if}\ B\ \text{then}\ S_1\ \text{else}\ S_2\ \text{fi}\ \{q\}\]

**RULE 5: LOOP**

\[\{p \land B\}\ S\ \{p\}\ \{p\}\ \text{while}\ B\ \text{do}\ S\ \text{od}\ \{p\}\ \land \neg B\]

\[\{p \land B\}\ S\ \{p\}\ \{p\}\ \text{while}\ B\ \text{do}\ S\ \text{od}\ \{p\}\ \land \neg B\]
RULE 5: LOOP

\[
\begin{align*}
\{p \land B\} & \quad S \quad \{p\} \\
\{p\} & \quad \textbf{while} \quad B \quad \textbf{do} \quad S \quad \textbf{od} \quad \{p \land \neg B\}
\end{align*}
\]
RULE 6: CONSEQUENCE

\[ p \rightarrow p_1, \{p_1\} \quad S \quad \{q_1\}, \quad q_1 \rightarrow q \]

\[ \{p\} \quad S \quad \{q\} \]
Quotient-Remainder
Example
And one more rule for total correctness ...
RULE 7: LOOP II

\[
\{ p \land B \} \ S \ \{ p \}, \\
\{ p \land B \land t = z \} \ S \ \{ t < z \}, \\
p \rightarrow t \geq 0
\]

\[
\{ p \} \ \text{while} \ B \ \text{do} \ S \ \text{od} \ \{ p \land \neg B \}
\]