Hoare logic

while programs;
Hoare logic proof system, operational semantics, soundness of Hoare proof system

Midterm

- Midterm exam on October 26th, in class. (for 1h)
- Topics include all that we have done so far plus the topics in the next two/three lectures on Hoare logic, operational semantics, and soundness of Hoare logic (for while programs).

While - programs

$$S ::= \underline{\text{skip}} \mid u := t \mid S_1 ; S_2 \mid \underline{\text{if}}\ B\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2 \mid \underline{\text{while}}\ B\ \underline{\text{do}}\ S_1\ \underline{\text{od}}$$

$$\vdash_{HL} \{p\}\ S\ \{q\}$$

A1. $\{p\}\ \mathrm{skip}\ \{p\}$

A2. $\{p[t/u]\}\ u := t\ \{p\}$

sound because
$p[t/u] = wpre(p, u := t)$

A3.

$$\frac{\{p\}\ S_1\ \{r\} \qquad \{r\}\ S_2\ \{q\}}{\{p\}\ S_1 ; S_2\ \{q\}}$$

A4.

$$\frac{\{p \wedge B\}\ S_1\ \{q\} \qquad \{p \wedge \neg B\}\ S_2\ \{q\}}{\{p\}\ \text{if } B \text{ then } S_1 \text{ else } S_2\ \{q\}}$$

A5.

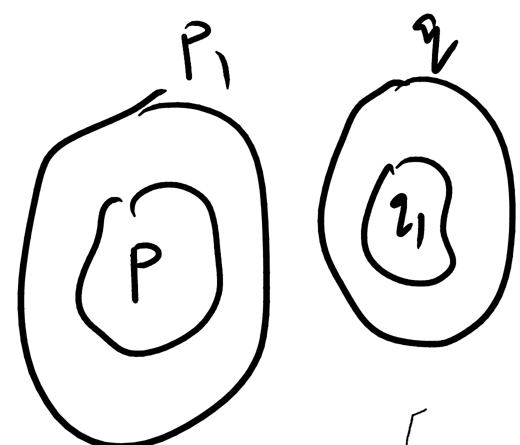
$$\frac{\{p \wedge B\}\ S\ \{p\}}{\{p\}\ \underline{\text{while}}\ B\ \underline{\text{do}}\ S\ \underline{\text{od}}\ \{p \wedge \neg B\}}$$

Loop

A6

$$\frac{p \Rightarrow p_1 \quad q_1 \Rightarrow q \quad \{p_1\} S \{q_1\}}{\{p\}\ S\ \{q\}}$$

Consequence



α

$\{\text{true}\}\ \text{skip}\ \{\alpha\}$

$DIV \equiv quo := 0 ; rem := x ; S_0$

$S_0 \equiv \underline{\text{while}}\ rem \geq y\ \underline{\text{do}}\ rem := rem - y;\ quo := quo + 1$

$\{x \geq 0 \wedge y \geq 0\}\ DIV\ \{\underline{quo.y + rem = x \wedge \cancel{\ } 0 \leq rem < y}\}$

$LI : p : \underline{quo.y + rem = x \wedge rem \geq 0}$

$A : \{\underline{x \geq 0 \wedge y \geq 0}\}\ quo := 0; \underline{rem := x}\ \{p\}$

$B : \{\underline{p \wedge rem \geq y}\}\ rem := rem - y\ ; quo := quo + 1;$
$\{p\}$

$\{quo \cdot y + x = x \wedge x \geq 0\}$ $rem := x$ $\{p\}$ Axiom

$\{0 \cdot y + x = x \wedge x \geq 0\}$ $quo := 0$ $\{quo \cdot y + x = x \wedge x \geq 0\}$ Axiom

$\{0 \cdot y + x = x \wedge x \geq 0\}$ $quo := 0;\ rem := x$ $\{p\}$ Sequence rule

Since $x \geq 0 \wedge y \geq 0 \Rightarrow 0 \cdot y + x = x \wedge x \geq 0$

$\{x \geq 0 \wedge y \geq 0\}$ $quo := 0;\ rem := x$ $\{p\}$ ~~Generalization~~ Consequence

A

Assume you prove B

From B and the loop rule:

$$\{P\}\ \underline{\text{while}}\ rem \geq y\ \underline{\text{do}}\ rem := rem - y;\ quo := quo + 1;\ \{P\}$$

$$\{P \wedge \neg(rem \geq y)\}$$

From A & B sequence-rule

$$\{x \geq 0 \wedge y \geq 0\}\ DIV\ \{P \wedge \neg(rem \geq y)\}$$

By rule of consequence, since

$$P \wedge \neg(rem \geq y) \Rightarrow quo \cdot y + rem = x \wedge 0 \leq rem < y$$

$$\{x \geq 0 \wedge y \geq 0\}\ DIV\ \{quo \cdot y + rem = x \wedge 0 \leq rem < y\}$$

$DIV \equiv quo := 0 \; ; \; rem := x \; ; \; S_0$

$S_0 \equiv \underline{\text{while}} \; (rem \geq y) \; \underline{\text{do}} \; rem := rem - y \; ; \; quo := quo + 1 \; ; \; \underline{\text{od}}$

To prove

$\{x \geq 0 \wedge y \geq 0\} \; DIV \; \{quo \cdot y + rem = x \wedge 0 \leq rem < y\}$

Let loop inv p be

$p \equiv quo \cdot y + rem = x \wedge rem \geq 0$

1. $\{quo \cdot y + x = x \wedge x \geq 0\}$ rem := x $\{P\}$ [Assign axiom]

2. $\{0 \cdot y + x = x \wedge x \geq 0\}$ quo := 0 $\{quo \cdot y + x = x \wedge x \geq 0\}$ [Assign axiom]

3. By composition rule, from 1 and 2

$\{0 \cdot y + x = x \wedge x \geq 0\}$ quo := 0 ; rem := x $\{P\}$

4. Since $x \geq 0 \wedge y \geq 0 \Rightarrow 0 \cdot y + x = x \wedge x \geq 0$ ← (proof omitted)

by consequence rule

$\{x \geq 0 \wedge y \geq 0\}$ quo := 0 ; rem := x $\{P\}$ (A)

5. $\{(quo+1)y + rem = x \wedge rem \geq 0\}$ quo := quo + 1 $\{P\}$ [Assign axiom]

6. $\{(quo+1)y + rem - y = x \wedge rem - y \geq 0\}$ rem := rem - y $\{(quo+1)y + rem = x \wedge rem \geq 0\}$

[Assign axiom]

7. By composition rule and 5 and 6:

$\{(quo+1)y + rem - y = x \wedge rem - y \geq 0\}$

rem := rem − y;

quo := quo + 1

$\{p\}$

8. Since $p \wedge rem \geq y \Rightarrow (quo+1)y + rem - y = x \wedge rem - y \geq 0$

by consequence rule

$\{p \wedge rem \geq y\}$ rem := rem − y; quo := quo + 1 $\{p\}$ B

9. By loop rule; 8

$\{p\}$ <u>while</u> (rem ≥ y) <u>do</u> rem := rem − y; quo := quo + 1 <u>od</u>

$\{p \wedge \neg(rem \geq y)\}$

10. By composition rule, 4 and 9

$\{x \geq 0 \wedge y \geq 0\}$ DIV $\{P \wedge \neg(\text{rem} \geq y)\}$

11. Since $P \wedge \neg(\text{rem} \geq y) \Rightarrow \text{quo} \cdot y + \text{rem} = x \wedge 0 \leq \text{rem} < y$

by consequence rule,

$\{x \geq 0 \wedge y \geq 0\}$ DIV $\{\text{quo} \cdot y + \text{rem} = x \wedge 0 \leq \text{rem} < y\}$

QED.