

6. Exercise sheet *Semantics and Verification of Software WS0809*

Due to Monday, 1 Dec. 2008, before the exercise course begins.

Exercise 6.1:

(2 points)

Prove the following partial correctness result using Hoare logic:

$$\{x = i \wedge y = j\} x := x + y; y := x - y; x := x - y \{x = j \wedge y = i\}.$$

Solution

Let

$$\underbrace{\{x = i \wedge y = j\}}_A \quad \underbrace{x := x + y}_{c_1}; \quad \underbrace{y := x - y}_{c_2}; \quad \underbrace{x := x - y}_{c_3} \quad \underbrace{\{x = j \wedge y = i\}}_B.$$

$$\begin{array}{c} \text{(asgn)} \frac{}{\{A_2\}c_2\{A_3\}} \quad \text{(asgn)} \frac{}{\{A_3\}c_3\{B\}} \\ \text{(seq)} \frac{}{\{A_2\}c_2; c_3\{B\}} \\ \text{(asgn)} \frac{}{\{A_1\}c_1\{A_2\}} \\ \text{(seq)} \frac{}{\{A_1\}c_1; c_2; c_3\{B\}} \\ \text{(cons)} \frac{\models A \Rightarrow A_1}{\{A\}c_1; c_2; c_3\{B\}} \end{array}$$

where A_3, A_2, A_1 are defined as follows:

$$\begin{aligned} A_3 &= B[x \mapsto x - y] = (x - y = j \wedge y = i) \\ A_2 &= A_3[y \mapsto x - y] = (x - (x - y) = j \wedge x - y = i) \\ A_1 &= A_2[x \mapsto x + y] = (x + y - (x + y - y) = j \wedge x + y - y = i) \\ &\Leftrightarrow (x = i \wedge y = j) = A \end{aligned}$$

This completes the proof. □

Exercise 6.2:

(2+3 points)

- (a) Develop a proof rule for statements of the form **for** $x := a_1$ **to** a_2 **do** c where $x \in \mathbf{Var}$, $a_1, a_2 \in \mathbf{AExp}$, and $c \in \mathbf{Cmd}$ (without assuming the presence of a **while** statement in the programming language).
- (b) Using this rule (and the known proof system), establish the validity of the following partial correctness property:

$$\{y \geq 0\} z := 0; \mathbf{for} \ x := 1 \ \mathbf{to} \ y \ \mathbf{do} \ z := z + x \left\{ z = \frac{y(y+1)}{2} \right\}$$

Solution

(a) Derive from the corresponding *while*-statement:

$$\mathbf{for } x := a_1 \mathbf{ to } a_2 \mathbf{ do } c \equiv x := a_1; \mathbf{ while } x \leq a_2 \mathbf{ do } (c; x := x + 1)$$

$$\begin{array}{c} \frac{\frac{\frac{\{A \wedge x \leq a_2\} c \{A[x \mapsto x + 1]\}}{\{A[x \mapsto x + 1]\} x := x + 1 \{A\}}}{\{A \wedge x \leq a_2\} c; x := x + 1 \{A\}}}{\frac{\{A[x \mapsto a_1]\} x := a_1 \{A\}}{\{A[x \mapsto a_1]\} x := a_1; \mathbf{ while } x \leq a_2 \mathbf{ do } (c; x := x + 1) \{A \wedge x > a_2\}}} \\ \Rightarrow \frac{\{A \wedge x \leq a_2\} c \{A[x \mapsto x + 1]\}}{\{A[x \mapsto a_1]\} \mathbf{ for } x := a_1 \mathbf{ to } a_2 \mathbf{ do } c \{A \wedge x > a_2\}} \end{array}$$

(b) Choose loop invariant:

$$C \equiv (y \geq 0 \wedge x \leq y + 1 \wedge z = \frac{x*(x-1)}{2})$$

For the body of the **for** statement:

$$\vdash \{C[x \mapsto x + 1][z \mapsto z + x]\} z := z + x \{C[x \mapsto x + 1]\}$$

Precondition and postcondition valid:

$$\begin{array}{l} C \wedge x \leq a_2 \\ \equiv (y \geq 0 \wedge x \leq y + 1 \wedge z = \frac{x*(x-1)}{2} \wedge x \leq y) \\ \Leftrightarrow (y \geq 0 \wedge x \leq y \wedge z = \frac{x*(x-1)}{2}) \end{array}$$

$$\begin{array}{l} C[x \mapsto x + 1][z \mapsto z + x] \\ \equiv (y \geq 0 \wedge x + 1 \leq y + 1 \wedge z + x = \frac{x*(x+1)}{2}) \\ \Leftrightarrow (y \geq 0 \wedge x \leq y \wedge z = \frac{x*(x+1)}{2} - x) \\ \Leftrightarrow (y \geq 0 \wedge x \leq y \wedge z = \frac{x*(x-1)}{2}) \end{array}$$

$$\text{Together: } C \wedge x \leq a_2 \Leftrightarrow C[x \mapsto x + 1][z \mapsto z + x]$$

$$\Rightarrow \vdash \{C \wedge x \leq a_2\} z := z + x \{C[x \mapsto x + 1]\} \quad (\text{for the body})$$

$$\Rightarrow \vdash \{C[x \mapsto 1]\} \mathbf{ for } x := 1 \mathbf{ to } a_2 \mathbf{ do } z := z + x \{C \wedge x > a_2\}$$

$$\Rightarrow \vdash \{C[x \mapsto 1][z \mapsto 0]\} z := 0; \mathbf{ for } x := 1 \mathbf{ to } a_2 \mathbf{ do } z := z + x \{C \wedge x > a_2\}$$

where

$$\begin{array}{l} C[x \mapsto 1][z \mapsto 0] \\ \equiv (y \geq 0 \wedge 1 \leq y + 1 \wedge 0 = \frac{1*(0)}{2}) \\ \Leftrightarrow (y \geq 0) \equiv A \end{array}$$

and $C \wedge x > a_2$

$$\begin{array}{l} \equiv (y \geq 0 \wedge x \leq y + 1 \wedge z = \frac{x*(x-1)}{2} \wedge x > y) \\ \Leftrightarrow (y \geq 0 \wedge x = y + 1 \wedge z = \frac{y*(y+1)}{2}) \\ \Rightarrow z = \frac{y*(y+1)}{2} \equiv B \end{array}$$

$$\Rightarrow \vdash \{A\} c \{B\} \quad (\text{the PCP from the exercise})$$

Exercise 6.3:**(1+0.5+0.5+3 points)**

(a) Show that the *greatest common divisor* of two positive integers $i, j \in \mathbb{Z}$, denoted by $\text{gcd}(i, j)$, has the following properties:

$$(i) \quad i > j \Rightarrow \text{gcd}(i, j) = \text{gcd}(i - j, j),$$

$$(ii) \quad \text{gcd}(i, j) = \text{gcd}(j, i), \text{ and}$$

$$(iii) \quad \text{gcd}(i, i) = i.$$

(b) Using the Hoare rules, prove that the statement $c \in \mathbf{Cmd}$ given by

$$\mathbf{while} \neg(x = y) \mathbf{do} \mathbf{if} x \leq y \mathbf{then} y := y - x \mathbf{else} x := x - y,$$

satisfies the following partial correctness property:

$$\{x = i \wedge y = j \wedge i \geq 1 \wedge j \geq 1\} c \{x = \text{gcd}(x, y) = \text{gcd}(i, j)\}.$$

Solution

For $i, j \geq 1$: $\text{gcd}(i, j) := \max(D(i) \cap D(j))$ where $D(i) := \{k \geq 1 \mid \exists i' \geq 1 \text{ such that } k \cdot i' = i\}$.

(a) (i) For $i > j \geq 1$:

$$k \in D(i) \cap D(j)$$

$$\Leftrightarrow \exists i' > j' \geq 1 \text{ such that } k \cdot i' = i \text{ and } k \cdot j' = j$$

$$\Rightarrow \exists i' > j' \geq 1 \text{ such that } k \cdot (i' - j') = i - j \text{ and } k \cdot j' = j$$

$$\Leftrightarrow k \in D(i - j) \cap D(j)$$

$$\Rightarrow \text{gcd}(i, j) = \text{gcd}(i - j, j)$$

$$(ii) \quad \text{gcd}(j, i) = \max(D(i) \cup D(j)) = \max(D(j) \cup D(i)) = \text{gcd}(j, i)$$

$$(iii) \quad \text{gcd}(i, i) = \max(D(i) \cup D(i)) = \max D(i) = i$$

$$\text{since } 1 \cdot i = i \text{ and thus } i \in D(i)$$

(b) To show: $\vdash \{A\} c \{B\}$ where

(go bottom up)

$$A \equiv \{x = i \wedge y = j \wedge i \geq 1 \wedge j \geq 1\}$$

$$c \equiv \mathbf{while} \neg(x = y) \mathbf{do} \mathbf{if} x \leq y \mathbf{then} y := y - x \mathbf{else} x := x - y$$

$$B \equiv \{x = \text{gcd}(x, y) = \text{gcd}(i, j)\}$$

Loop invariant: $C \equiv (k = \text{gcd}(i, j) = \text{gcd}(x, y))$ (that is, $\text{gcd}(x, y)$ is invariant!)

$$(6) \vdash \{y - x > 0 \wedge k = \text{gcd}(x, y - x) = \text{gcd}(i, j)\} y := y - x \{k = \text{gcd}(x, y) = \text{gcd}(i, j) \wedge y > 0\}$$

$$(7) \vdash \{x - y > 0 \wedge k = \text{gcd}(x - y, y) = \text{gcd}(i, j)\} x := x - y \{k = \text{gcd}(x, y) = \text{gcd}(i, j) \wedge x > 0\}$$

with *cons* rule and (a)(i) and (a)(ii):

$$\models A \Rightarrow A' \quad : \quad \models y \geq x \wedge \neg(x = y) \wedge k = \dots \Rightarrow y - x > 0 \wedge k = \text{gcd}(x, y - x) = \text{gcd}(i, j)$$

$$\models A \Rightarrow A' \quad : \quad \models x \geq y \wedge \neg(x = y) \wedge k = \dots \Rightarrow x - y > 0 \wedge k = \text{gcd}(x - y, y) = \text{gcd}(i, j)$$

$$\models B' \Rightarrow B \quad : \quad \models k = \dots \wedge y > 0 \Rightarrow k = \dots$$

$$\models B' \Rightarrow B \quad : \quad \models k = \dots \wedge x > 0 \Rightarrow k = \dots$$

$$(4) \vdash \{x \leq y \wedge \neg(x = y) \wedge k = \dots\} y := y - x \{k = \dots\}$$

$$(5) \vdash \{\neg(x \leq y) \wedge \neg(x = y) \wedge k = \dots\} x := x - y \{k = \dots\}$$

with *if* rule:

(3) $\vdash \{\neg(x = y) \wedge k = \dots\} \text{ if } x \leq y \text{ then } y := y - x \text{ else } x := x - y \{k = \dots\}$

with *while* rule:

(2) $\vdash \overbrace{\{k = \dots\}}^A \text{ c } \overbrace{\{x = y \wedge k = \dots\}}^{\neg b}$

with *cons* rule and (a)(iii):

$\models A \Rightarrow A' \quad : \quad \models x = i \wedge y = j \wedge x \geq 1 \wedge y \geq 1 \Rightarrow k = \text{gcd}(x, y) = \text{gcd}(i, j)$

$\models B' \Rightarrow B \quad : \quad \models x = y \wedge k = \text{gcd}(x, y) = \text{gcd}(i, j) \Rightarrow x = \text{gcd}(x, y) = \text{gcd}(i, j)$

(1) $\vdash \{A\} \text{ c } \{B\}$

$$\frac{\frac{\overline{\text{(6) asgn}}}{\text{(4) cons}} \quad \frac{\overline{\text{(7) asgn}}}{\text{(5) cons}}}{\text{(3) if}}}{\frac{\text{(2) while}}{\text{(1) cons}}}$$

□