Semantics and Verification of Software
apl. Prof. Dr. Thomas Noll
Benjamin Kaminski Christoph Matheja

# Exersice Sheet 6

## Sample Solution

## Task 1: Partial Correctness Properties

### (a)

The required partial correctness property is

$$\{n > 2 \wedge \text{even}\,(n)\}\, c\, \{\exists q, p.\ n = q + p \wedge \text{prime}\,(q) \wedge \text{prime}\,(p)\}$$

Where $\text{even}\,(n)$ and $\text{prime}\,(n)$ are defined as follows:

- $\text{even}\,(n) = \exists z.\ n = 2 \cdot z$
- $\text{prime}\,(n) = n > 1 \wedge \forall k.\ \underbrace{(\exists l.\ l \geq 1 \wedge n = k \cdot l)}_{\text{“}k \text{ is divisor of } n\text{”}} \rightarrow (k = 1 \vee k = n)$

### (b)

The existence of a suitable program $c$ does not imply Goldbach's conjecture, as the postcondition is only fulfilled if $c$ terminates which is not guaranteed by partial correctness.

## Task 2: Relative Completeness

### (a)

| Program $c$ | $wp\,(c,\ B)$ |
|---|---|
| skip | $B$ |
| $x := a$ | $B[x \mapsto a]$ |
| $c_1;\ c_2$ | $wp\,(c_1,\ wp\,(c_2,\ B))$ |
| if $b$ then $c_1$ else $c_2$ | $(b \wedge wp\,(c_1,\ B)) \vee (\neg b \wedge wp\,(c_2,\ B))$ |
| while $b$ do $c'$ | $(\neg b \wedge B) \vee (b \wedge wp\,(c',\ wp\,(\text{while } b \text{ do } c',\ B)))$ <br> $\equiv \bigwedge_{i \in \mathbb{N}} F_i$, where <br> $F_{i+1} = (\neg b \wedge B) \vee (b \wedge wp\,(F_i,\ B))$ and <br> $F_0 = \text{true}$ |

## (b)

We will proof by induction on the structure of the syntax of c that the Hoare logic is relatively complete.

**Induction Base:**

$c \triangleq \text{skip}$ Trivial by the rule

$$\frac{}{\{B\}\,\text{skip}\,\{B\}}\ (\text{skip})$$

$c \triangleq c := a$ Trivial by the rule

$$\frac{}{\underbrace{\{B\,[x \mapsto a]\}}_{wp(x:=a,\ B)}\ x := a\,\{B\}}\ (\text{asgn})$$

**Induction Hypothesis:**

$\vdash \{wp\,(c,\ B)\}\,c\,\{B\}$ holds for any program c.

**Induction Step:**

$c \triangleq c_1;\ c_2$

By induction hypothesis, we know that $\vdash \{wp\,(c_2,\ B)\}\,c_2\,\{B\}$ holds.
Furthermore, by induction hypothesis, we have
$\vdash \underbrace{\{wp\,(c_1,\ wp\,(c_2,\ B))\}}_{=wp(c_1;\ c_2,\ B)}\,c_1\,\{wp\,(c_2,\ B)\}$.

Then we obtain a proof using the (seq)-rule:

$$\frac{\{wp\,(c_1;\ c_2,\ B)\}\,c_1\,\{wp\,(c_2,\ B)\} \qquad \{wp\,(c_2,\ B)\}\,c_2\,\{B\}}{\{wp\,(c_1;\ c_2,\ B)\}\,c_1;\ c_2\,\{B\}}\ (\text{seq})$$

$\underline{c \triangleq \text{if } b \text{ then } c_1 \text{ else } c_2}$

By induction hypothesis, we have $\vdash \{wp\,(c_1,\ B)\}\, c_1\, \{B\}$ and $\vdash \{wp\,(c_2,\ B)\}\, c_2$
We then obtain the following proof:

$$\circledast$$

$$\frac{\models ((b \wedge wp\,(c,\ B)) \Rightarrow wp\,(c_1,\ B)) \quad \vdash \{wp\,(c_1,\ B)\}\, c_1\, \{B\} \quad \models (B \Rightarrow B)}{\{b \wedge wp\,(c,\ B)\}\, c_1\, \{B\}}\ (\text{cons})$$

$$\circledast\circledast$$

$$\frac{\models ((\neg b \wedge wp\,(c,\ B)) \Rightarrow wp\,(c_2,\ B)) \quad \vdash \{wp\,(c_2,\ B)\}\, c_2\, \{B\} \quad \models (B \Rightarrow B)}{\{\neg b \wedge wp\,(c,\ B)\}\, c_2\, \{B\}}\ (\text{cons})$$

$$\frac{\circledast \quad \circledast\circledast}{\{wp\,(c,\ B)\}\ \text{if } b \text{ then } c_1 \text{ else } c_2\, \{B\}}\ (\text{if})$$

$\underline{c \triangleq \text{while } b \text{ do } c'}$

By induction hypothesis, we have $\vdash \{wp\,(c,\ A)\}\, c'\, \{A\}$ for any assertion A.
In particular, we may choose $A = wp\,(\text{while } b \text{ do } c',\ B)$. Then
$\circledast$

$$\frac{\dfrac{\models (A \wedge b \Rightarrow A) \quad \vdash \{wp\,(c',\ A)\}\, c'\, \{A\} \quad \models (A \Rightarrow A)}{\{A \wedge b\}\, c'\, \{A\}}\ (\text{cons})}{\{A\}\ \text{while } b \text{ do } c'\, \{A \wedge \neg b\}}\ (\text{while})$$

$$\frac{\models (A \Rightarrow A) \quad \circledast \quad \models ((A \wedge \neg b) \Rightarrow B)}{\{wp\,(\text{while } b \text{ do } c',\ B)\}\ \text{while } b \text{ do } c'\, \{B\}}\ (\text{cons})$$

In each case we found a prove showing that $\vdash \{wp\,(c,\ B)\}\, c\, \{B\}$ holds.

## Task 3: Strongest Postconditions

### (a)

Let $A, B \in Assn,\ I \in Int$(Interpretation).
Then the strongest postcondition can be defined as

$$sp^I[\![c,\ A]\!] = \bigcap_{\models^I\{A\}c\{B\}} B^I = \left\{\sigma' \in \Sigma \mid \exists\sigma.\sigma \models^I A \wedge \mathfrak{C}[\![c]\!]\sigma = \sigma'\right\}$$

**(b)**

| Program $c$ | $sp\,(c,\ A)$ |
|---|---|
| skip | $A$ |
| $x := a$ | $\exists z.\ (x = a\,[x \mapsto z]) \wedge A\,[x \mapsto z]$ |
| $c_1;\ c_2$ | $sp\,(c_2,\ sp\,(c_1,\ A))$ |
| if $b$ then $c_1$ else $c_2$ | $sp\,(c_1,\ A \wedge b) \vee sp\,(c_2,\ A \wedge \neg b)$ |
| while $b$ do $c'$ | $sp\,(\text{while } b \text{ do } c',\ sp\,(c',\ A \wedge b)) \vee (A \wedge \neg b)$<br>$\equiv \bigwedge_{i\in\mathbb{N}} F_i$, where<br>$F_{i+1} = (\neg b \to A) \wedge (b \to sp\,(c,\ F_i))$ and<br>$F_0 = \text{true}$ |

**(c)**

$$\begin{aligned}
& sp\,(x := 2 \cdot x;\ y := x + 2;\ z := y + x,\ x = 1) \\
= \ & sp\,(y := x + 2;\ z := y + x,\ sp\,(x := 2 \cdot x,\ x = 1)) \\
= \ & sp\,(y := x + 2;\ z := y + x,\ \exists z_1.\ (x := (2 \cdot x)\,[x \mapsto z_1]) \wedge (x = 1)\,[x \mapsto z_1]) \\
= \ & sp\,(y := x + 2;\ z := y + x,\ \exists z_1.\ (x := 2 \cdot z_1) \wedge (z_1 = 1)) \\
= \ & sp\,(z := y + x,\ sp\,(y := x + 2,\ \exists z_1.\ (x := 2 \cdot z_1) \wedge (z_1 = 1))) \\
= \ & sp\,(z := y + x,\ \exists z_2.\ (y := (x + 2)\,[y \mapsto z_2]) \wedge \\
& (\exists z_1.\ (x := 2 \cdot z_1) \wedge (z_1 = 1))\,[y \mapsto z_2]) \\
= \ & sp\,(z := y + x,\ \exists z_2.\ (y := (x + 2)) \wedge (\exists z_1.\ (x := 2 \cdot z_1) \wedge (z_1 = 1))) \\
= \ & \exists z_3.\ (z := (y + x)\,[z \mapsto z_3]) \wedge \\
& (\exists z_2.\ (y := (x + 2)) \wedge (\exists z_1.\ (x := 2 \cdot z_1) \wedge (z_1 = 1)))\,[z \mapsto z_3] \\
= \ & \exists z_3.\ (z := (y + x)) \wedge (\exists z_2.\ (y := (x + 2)) \wedge (\exists z_1.\ (x := 2 \cdot z_1) \wedge (z_1 = 1)))
\end{aligned}$$

**(d)**

We first compute $wp^I\,(c,\ \text{false})$ and $sp^I\,(c,\ \text{false})$ for any $I \in Int$:

$$sp^I\,(c,\ \text{false}) = \left\{\sigma' \in \Sigma \mid \exists \sigma.\sigma \models^I \text{false} \wedge \mathfrak{C}[\![c]\!]\sigma = \sigma'\right\} = \emptyset = \text{false}$$
$$wp^I\,(c,\ \text{false}) = \underbrace{\left\{\sigma \in \Sigma_\perp \mid \mathfrak{C}[\![c]\!]\sigma \models^I \text{false}\right\}}_{=:A}$$

We then have to show that

$$\begin{array}{ll} & \models \{wp\,(c,\ sp\,(c,\ \text{false}))\}\,c\,\{sp\,(c,\ wp\,(c,\ \text{false}))\} \\ \Leftrightarrow & \models \{wp\,(c,\ \text{false})\}\,c\,\{sp\,(c,\ wp\,(c,\ \text{false}))\} \\ \Leftrightarrow & \models \{A\}\,c\,\{sp\,(c,\ A)\} \qquad \text{(this is always true, see (a))} \end{array}$$

Therefore, the statement is correct.