Semantics and Types - Assignment 3

Mikkel Willén
bmq419

March 6, 2024

Task 3.1

We derive the triple

$$\{n \geq 0 \wedge d > 0\}\ \texttt{DIV}\ \{n = q \times d + r \wedge 0 \leq r \wedge r < d\}$$

in Hoare logic by fully annotating the program.

$\{n \geq 0 \wedge d > 0\}$
$\{n = 0 \times d + n \wedge n + d > 0\}$ $\dagger_1$
$r := n$
$\{n = 0 \times d + r \wedge r + d > 0\}$
$q := 0$
$\{n = q \times d + r \wedge r + d > 0\}$
$\texttt{while}\ r > 0\ \texttt{do}$
  $\{n = q \times d + r \wedge r + d > 0 \wedge r > 0\}$
  $\{n = (q+1) \times d + (r - d) \wedge (r - d) + d > 0\}$ $\dagger_2$
  $r := r - d$
  $\{n = (q+1) \times d + r \wedge r + d > 0\}$
  $q := q + 1$
  $\{n = q \times d + r \wedge r + d > 0\}$
$\{n = q \times d + r \wedge r + d > 0 \wedge \neg(r > 0)\}$
$\texttt{if}\ r < 0\ \texttt{then}$
  $\{n = q \times d + r \wedge r + d > 0 \wedge \neg(r > 0) \wedge r < 0\}$
  $\{n = (q-1) \times d + (r + d) \wedge (r + d) + d > 0 \wedge \neg(r > 0)\}$ $\dagger_3$
  $r := r + d$
  $\{n = (q-1) \times d + r \wedge r + d > 0 \wedge \neg(r > 0)\}$
  $q := q - 1$
  $\{n = q \times d + r \wedge r + d > 0 \wedge \neg(r > 0)\}$
  $\{n = q \times d + r \wedge 0 \leq r \wedge r < d\}$ $\dagger_4$
$\texttt{else}$
  $\{n = q \times d + r \wedge r + d > 0 \wedge \neg(r > 0) \wedge \neg(r < 0\}$
  $\{n = q \times d + r \wedge 0 \leq r \wedge r < d\}$ $\dagger_5$
  $\texttt{skip}$
  $\{n = q \times d + r \wedge 0 \leq r \wedge r < d\}$
$\{n = q \times d + r \wedge 0 \leq r \wedge r < d\}$

We will now prove each of the semantic reasonings marked with a †.

$\dagger_1 : \overbrace{n \geq 0}^{(1)} \wedge \overbrace{d > 0}^{(2)} \Rightarrow \overbrace{n = q \times d + r}^{(a)} \wedge \overbrace{r + d > 0}^{(b)}$

Here (a) is a simple reduction, and (b) follows directly from (1) and (2).

$\dagger_2 : \overbrace{n = q \times d + r}^{(1)} \wedge \overbrace{r + d > 0}^{(2)} \wedge \overbrace{r > 0}^{(3)} \Rightarrow \overbrace{n = (q+1) \times d + (r-d)}^{(a)} \wedge \overbrace{(r-d) + d > 0}^{(b)}$

(a) follows from (1), since $q \times d + d + r - d = q \times d + r = n$. (b) follow from (3) since $(r - d) + d = r > 0$.

$$\dagger_3 : \overbrace{n = q \times d + r}^{(1)} \wedge \overbrace{r + d > 0}^{(2)} \wedge \overbrace{\neg(r > 0)}^{(3)} \wedge \overbrace{r < 0}^{(4)} \Rightarrow \overbrace{n = (q-1) \times d + (r+d)}^{(a)} \wedge \overbrace{(r+d) + d > 0}^{(b)} \wedge \overbrace{\neg(r > 0)}^{(c)}$$

(a) follows from (1), since $q \times d - d + r + d = q \times d + r = n$. (b) follows from (2) and (3), since (3) says that $\neg(r > 0)$ which means that $r \leq 0$, which means that $d > 0$ for (2) to hold and so $r + 2d > 0$. (c) follows from (3).

$$\dagger_4 : \overbrace{n = q \times d + r}^{(1)} \wedge \overbrace{r + d > 0}^{(2)} \wedge \overbrace{\neg(r > 0)}^{(3)} \Rightarrow \overbrace{n = q \times d + r}^{(a)} \wedge \overbrace{0 \leq r}^{b} \wedge \overbrace{r < d}^{c}$$

(a) is the same as (1). (b) follows from (3) since $\neg(r > 0) = r \leq 0$. (c) follows from (2) and (3), since (3) says that $\neg(r > 0)$ which means that $r \leq 0$, which means that $d > 0$ for (2) to hold, and so $r \leq 0 < d$

$$\dagger_5 : \overbrace{n = q \times d + r}^{(1)} \wedge \overbrace{r + d > 0}^{(2)} \wedge \overbrace{\neg(r > 0)}^{(3)} \wedge \overbrace{\neg(r < 0)}^{(4)} \Rightarrow \overbrace{n = q \times d + r}^{(a)} \wedge \overbrace{0 \leq r}^{b} \wedge \overbrace{r < d}^{c}$$

This is the same as $\dagger_4$ and we do not need to use (4).

Task 3.2

Theorem 3.7 *If* $\vdash \{A\}\ c\ \{B\}$, *then* $\models \{A\}\ c\ \{B\}$

$$\text{Case } \mathcal{H} = \text{H-R}{\small\text{EPEAT}} \frac{\overset{\mathcal{H}_0}{\{A \vee (B \wedge \neg b)\}\ c_0\ \{B\}}}{\{A\}\ \textbf{repeat}\ c_0\ \textbf{until}\ b\ \{B \wedge b\}}$$

By inner induction on derivations, we want to prove, that for any σ'' such that $\sigma'' \models B$ and derivation $\mathcal{E}'$ of $\langle \textbf{repeat}\ c_0\ \textbf{until}\ b, \sigma'' \rangle \downarrow \sigma'$, we must have $\sigma' \models B \wedge b$.

$$\text{Case } \mathcal{E}' = \text{EC-R}{\small\text{EPEAT}}\text{T} \frac{\overset{\mathcal{E}'_0}{\langle c_0, \sigma'' \rangle \downarrow \sigma'} \quad \overset{\mathcal{E}'_1}{\langle b, \sigma' \rangle \downarrow \textbf{true}}}{\langle \textbf{repeat}\ c_0\ \textbf{until}\ b, \sigma'' \rangle \downarrow \sigma'}$$

By Lemma 3.1 on $\mathcal{E}'_1$ we get that $\sigma' \models b$, and then by outer IH on $\mathcal{H}_0$ with $\mathcal{E}'_0$ we get $\sigma' \models B$ and so we have that $\sigma' \models B \wedge b$.

$$\text{Case } \mathcal{E}' = \text{EC-R}{\small\text{EPEAT}}\text{T} \frac{\overset{\mathcal{E}'_0}{\langle c_0, \sigma'' \rangle \downarrow \sigma'''} \quad \overset{\mathcal{E}'_1}{\langle b, \sigma''' \rangle \downarrow \textbf{false}} \quad \overset{\mathcal{E}'_2}{\langle \textbf{repeat}\ c_0\ \textbf{until}\ b, \sigma''' \rangle \downarrow \sigma'}}{\langle \textbf{repeat}\ c_0\ \textbf{until}\ b, \sigma'' \rangle \downarrow \sigma'}$$

By Lemma 3.1 on $\mathcal{E}'_1$ we get that $\sigma''' \not\models b$ i.e., that $\sigma''' \models \neg b$. By outer IH on $\mathcal{H}_0$ with $\mathcal{E}'_0$ we get that $\sigma''' \models B$ and we have that $\sigma''' \models B \wedge \neg b$. But then, by inner IH on $\mathcal{E}'_2$, we get that $\sigma' \models B \wedge b$.

To complete the case, we simply take σ'' as σ and $\mathcal{E}'$ as $\mathcal{E}$ in the above result.

Task 3.3

a)

Given the Completeness Theorem, we can claim that if the Hoare Triple $\vdash \{\textbf{false}\}\ c\ \{B\}$ is logically valid, then it is provable in Hoare logic.

b)

By structural induction on c, we first show that $\vdash \{\textbf{false}\}\ c\ \{\textbf{false}\}$.

$$\text{Case } \mathcal{H} = \text{H-S}{\small\text{KIP}} \frac{}{\{\textbf{false}\}\ \textbf{skip}\ \{\textbf{false}\}}$$

Here $c = \textbf{skip}$ and it holds trivially, since the state does not change.

$$\text{Case } \mathcal{H} = \text{H-A}{\small\text{SSIGN}} \frac{}{\{\textbf{false}[a/X]\}\ X := a\ \{\textbf{false}\}}$$

Here $c = (X := a)$ and the only possible shape of $\mathcal{E}$ is

$$\mathcal{E} = \text{EC-ASSIGN}\frac{\overset{\mathcal{E}_0}{\langle a, \sigma\rangle \downarrow n}}{\langle X := a, \sigma\rangle \downarrow \sigma[X \mapsto n]}$$

so $\sigma' = \sigma[X \mapsto n]$, and we can use Lemma 3.6 ($\Rightarrow$) on $\mathcal{E}_0$ and that $\sigma \vdash \mathbf{false}[a/X]$, gives us $\mathbf{false}[a/X] \vdash b$.

$$\text{Case } \mathcal{H} = \text{H-SEQ}\frac{\overset{\mathcal{H}_0}{\{\mathbf{false}\}\ c_0\ \{C\}} \quad \overset{\mathcal{H}_1}{\{C\}\ c_1\ \{\mathbf{false}\}}}{\{\mathbf{false}\}\ c_0; c_1\{\mathbf{false}\}}$$

Here $c = (c_0; c_1)$ and by IH on $\mathcal{H}_0$ and $\mathcal{H}_1$ it also holds for any C.

$$\text{Case } \mathcal{H} = \text{H-IF}\frac{\overset{\mathcal{H}_0}{\{\mathbf{false} \wedge b\}\ c_0\ \{\mathbf{false}\}} \quad \overset{\mathcal{H}_1}{\{\mathbf{false} \wedge \neg b\}\ c_0\ \{\mathbf{false}\}}}{\{\mathbf{false}\}\ \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1\ \{\mathbf{false}\}}$$

By IH on $\mathcal{H}_0$ and $\mathcal{H}_1$ we get that it holds, and we have that $\mathbf{false} \wedge b = \mathbf{false}$ and $\mathbf{false} \wedge \neg b = \mathbf{false}$.

$$\text{Case } \mathcal{H} = \text{H-CONSEQ}\frac{\vDash \mathbf{false} \Rightarrow A' \quad \overset{\mathcal{H}_0}{\{A'\}\ c\ \{B'\}} \quad \vDash B' \Rightarrow \mathbf{false}}{\{\mathbf{false}\}\ c\ \{\mathbf{false}\}}$$

By IH on $\mathcal{H}_0$ we get $\{\mathbf{false}\}\ c\ \{\mathbf{false}\}$.

If we combine these rules with the **Consequence** rule to strengthen the postcondition from **false** to B

$$\text{H-CONSEQ}\frac{\vDash \mathbf{false} \Rightarrow \mathbf{false} \quad \{\mathbf{false}\}\ c\ \{\mathbf{false}\} \quad \vDash \mathbf{false} \Rightarrow B}{\{\mathbf{false}\ c\ \{B\}}$$

Since the antecedent $\{\mathbf{false}\}\ c\ \{\mathbf{false}\}$ was proven for any command c in the structural induction and $\mathbf{false} \Rightarrow B$, we can use the **consequence** rule to derive $\{\mathbf{false}\}\ c\ \{B\}$.