Program Verification

Hoare Logic of partial and total correctness

1. Derive the following specifications of partial correctness using tableaux:

   a) $\{x > 0\} y \leftarrow x + 1 \{y > 1\}$

   b) $\{x > 1\} z = 1;\ y \leftarrow x;\ y \leftarrow y - z \{y > 0 \ \wedge \ x > y\}$

   c) $\{\mathsf{true}\} y \leftarrow x;\ y \leftarrow x + x + y \{y = 3 \times x\}$

   d) $\{\mathsf{true}\}$`if x > y then z ←  y else z ← x` $\{z = min(x, y)\}$.

   e) $\{\mathsf{true}\}$`if x > y then z ← x else z ← y` $\{z = max(x, y)\}$.

   f) $\{x_0 > 0 \ \wedge \ y_0 > 0\} z \leftarrow 0;$ `while` $y \leq x$ `do` $(z \leftarrow z+1; x \leftarrow x-y)\{z = x_0/y_0 \wedge x = x_0 \% y_0\}$, where x_0 and y_0 are initial values of x and y, respectively.

   g) $\{x \geq 0\} z \leftarrow x; y \leftarrow 0;$ `while` $\neg z = 0$ `do` $(y \leftarrow y + 1; z \leftarrow z - 1)\{x = y\}$.

   h) $\{y \geq 0\} w \leftarrow 0; z \leftarrow 0;$ `while` $\neg w = y$ `do` $(z \leftarrow z + x; w \leftarrow w + 1)\{z = x \times y\}$.

   i) $\{y = y_0 \ \wedge \ y \geq 0\}\ z \leftarrow 0;$ `while` $\neg y = 0$ `do` $(z \leftarrow z + x; y \leftarrow y - 1)\{z = x \times y_0\}$, where y_0 is the initial value of y.

2. Show that:

$$s \models \varphi[E/x] \quad \Leftrightarrow \quad s[\mathcal{A}[\![E]\!]s/x] \models \varphi$$

3. Show that this rule can be derived from the system $\mathcal{H}$

   $[if'_p\ ]$

$$\frac{\{\varphi_1\}\, C_1\, \{\psi\} \qquad \{\varphi_2\}\, C_2\, \{\psi\}}{\{(B \to \varphi_1) \ \wedge \ (\neg B \to \varphi_2)\}\, \mathtt{if}\, B\, \mathtt{then}\, C_1\, \mathtt{else}\, C_2\, \{\psi\}}$$

4. Derive the following specifications of partial correctness using tableaux:

   a) $\{x = 0 \ \wedge \ 1 \leq m\}$ `for` $n \leftarrow 1$ `until` m `do` $x \leftarrow x + n\ \{x = m \times (m + 1) div 2\}$. ($\varphi$ is $x = (n - 1) \times n\, div 2$).

   b) $\{n \geq 1\}\ p \leftarrow 0;$ `for` $x \leftarrow 1$ `until` n `do` $p \leftarrow p + m\ \{p = m \times n\}$

   c) $\{a[x] = x \ \wedge \ a[y] = y\}\ r \leftarrow a[x];\ a[x] \leftarrow a[y];\ a[y] \leftarrow r\ \{a[x] = y \ \wedge \ a[y] = x\}$

5. Derive the following specifications of total correctness:

   a) $\{y > 0\}$ `while` $y \leq r$ `do` $(r \leftarrow r - y;\ q \leftarrow q + 1\ )\{\mathsf{true}\}$

   b) $\{x \geq 0\} z \leftarrow x; y \leftarrow 0,$ `while` $\neg z = 0$ `do` $(y \leftarrow y + 1; z \leftarrow z - 1)\{x = y\}$.

   c) $\{y \geq 0\} w \leftarrow 0; z \leftarrow 0;$ `while` $\neg w = y$ `do` $(z \leftarrow z + x; w \leftarrow w + 1)\{z = x \times y\}$.

   d) $\{y = y_0 \ \wedge \ y \geq 0\}\ z \leftarrow 0;$ `while` $\neg y = 0$ `do` $(z \leftarrow z + x; y \leftarrow y - 1)\{z = x \times y_0\}$, where y_0 is the initial value of y.