

Verificação Formal de Software - Exercícios

Lógica de Hoare para correção parcial e total

1. Considerando o sistema de correção parcial dada no curso, deduz as seguintes asserções usando precondições fracas e *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) $\{\text{true}\}y = x; y \leftarrow x + x + y\{y = 3 \times x\}$
- d) $\{\text{true}\}\leftarrow \text{if } x > y \text{ then } z \leftarrow y \text{ else } z \leftarrow x \{z = \min(x, y)\}.$
- e) $\{\text{true}\}\text{if } x > y \text{ then } z \leftarrow x \text{ else } z \leftarrow y \{z = \max(x, y)\}.$
- f) $\{x_0 > 0 \wedge y_0 > 0\}z \leftarrow 0; \text{while } y \leq x \text{ do } (z \leftarrow z + 1; x \leftarrow x - y)\{z = x_0 \text{ div } y_0 \wedge x = x_0 \text{ mod } y_0\}$, onde x_0 e y_0 são os valores iniciais de x e y , respectivamente.
- g) $\{x \geq 0\}z \leftarrow x; y \leftarrow 0; \text{while } \neg z = 0 \text{ do } (y \leftarrow y + 1; z \leftarrow z - 1)\{x = y\}.$
- h) $\{y \geq 0\}w \leftarrow 0; z \leftarrow 0; \text{while } \neg w = y \text{ do } (z \leftarrow z + x; w \leftarrow w + 1)\{z = x \times y\}.$
- i) $\{y = y_0 \wedge y \geq 0\}z \leftarrow 0; \text{while } \neg y = 0 \text{ do } (z \leftarrow z + x; y \leftarrow y - 1)\{z = x \times y_0\}$, onde y_0 é o valor inicial de y .

2. Mostra que, para qualquer asserção φ , variável x , expressão aritmética E e estado s :

$$s \models \varphi[E/x] \quad \text{se e só se} \quad s[\mathcal{A}[E]/x] \models \varphi$$

3. Mostra que a regra seguinte se pode deduzir do sistema de inferência dado para a correção parcial.

$[if'_p]$

$$\frac{\{\varphi_1\} C_1 \{\psi\} \quad \{\varphi_2\} C_2 \{\psi\}}{\{(B \rightarrow \varphi_1) \wedge (\neg B \rightarrow \varphi_2)\} \text{ if } B \text{ then } C_1 \text{ else } C_2 \{\psi\}}$$

4. Considerando o sistema de dedução para a correção total dada no curso, deduz as seguintes asserções usando precondições fracas e *tableaux*:

- a) $\{y > 0\} \text{ while } y \leq r \text{ do } (r \leftarrow r - y; q \leftarrow q + 1)\{\top\}$
- b) $\{x \geq 0\}z \leftarrow x; y \leftarrow 0; \text{while } \neg z = 0 \text{ do } (y \leftarrow y + 1; z \leftarrow z - 1)\{x = y\}.$
- c) $\{y \geq 0\}w \leftarrow 0; z \leftarrow 0; \text{while } \neg w = y \text{ do } (z \leftarrow z + x; w \leftarrow w + 1)\{z = x \times y\}.$
- d) $\{y = y_0 \wedge y \geq 0\}z \leftarrow 0; \text{while } \neg y = 0 \text{ do } (z \leftarrow z + x; y \leftarrow y - 1)\{z = x \times y_0\}$, onde y_0 é o valor inicial de y .

5. Considerando a semântica axiomática para a correção parcial dada no curso, deduz as seguintes asserções usando precondições fracas e *tableaux*:

- a) $\{a[x] = x \wedge a[y] = y\} r := a[x]; a[x] := a[y]; a[y] := r \{a[x] = y \wedge a[y] = x\}$

6. Considera o sistema \mathcal{H}_g (o sistema de inferência para a lógica de Hoare sem a regra da consequência) e as funções VCG, VC e wp apresentadas nas aulas.

- (a) Aplica o algoritmo VCGen definido nas aulas para calcular as condições de verificação do seguinte programa (acrescenta o correspondente invariante I):

```
{y=i, y>=0}  
  while y!= 0 do {I}  
    z:=z + 1;  
    y:=y-1  
  {z=z+i}
```