Introduction to Computer Science
Jacobs University Bremen
Dr. Jürgen Schönwälder

Module: CH-232
Date: 2021-11-26
Due: 2021-12-03

ICS 2021 Problem Sheet #12

Problem 12.1: *correctness of exponentiation algorithm* (1+2+2+2+1+1+1 = 10 points)

Prove step-by-step the partial correctness and the total correctness of the following algorithm using Hoare Logic. Our claim is that the algorithm calculates x^n for integers x and n.

```
1:  K := n
2:  P := x
3:  Y := 1
4:  while K > 0 do
5:      if K mod 2 = 0 then
6:          P := P × P
7:          K := K/2
8:      else
9:          Y := Y × P
10:         K := K − 1
11:     fi
12: od
```

a) Define a suitable precondition and a suitable postcondition.

b) Add annotations for partial correctness.

c) Derive verification conditions for partial correctness.

d) Prove the partial correctness verification conditions.

e) Add additional annotations for total correctness.

f) Derive or update verification conditions for total correctness.

g) Prove the total correctness verification conditions.

Solution:

a) Translation into Hoare language constructs with preconditions and postconditions

Precondition: $\{x \in \mathbb{Z} \wedge n \in \mathbb{N}\}$

```
1:  K := n
2:  P := x
3:  Y := 1
4:  while K > 0 do
5:      if K mod 2 = 0 then
6:          P := P × P
7:          K := K/2
8:      else
9:          Y := Y × P
10:         K := K − 1
11:     fi
12: od
```

Postcondition: $\{Y = x^n\}$

b) We have to add an annotation before the while command (due to the sequence rule) and we have to add an annotation before the body of the while loop (the loop invariant).

Precondition: $\{x \in \mathbb{Z} \wedge n \in \mathbb{N}\}$

1: $K := n$
2: $P := x$
3: $Y := 1$
4: $\{(K \geq 0) \wedge (Y \times P^K = x^n)\}$
5: **while** $K > 0$ **do**
6: $\quad \{(K \geq 0) \wedge (Y \times P^K = x^n)\}$
7: $\quad$ **if** $K \bmod 2 = 0$ **then**
8: $\quad\quad P := P \times P$
9: $\quad\quad K := K/2$
10: $\quad$ **else**
11: $\quad\quad Y := Y \times P$
12: $\quad\quad K := K - 1$
13: $\quad$ **fi**
14: **od**

Postcondition: $\{Y = x^n\}$

c) Deriving verification conditions for partial correctness. We obtain the first verification condition from the precondition and the sequence of assignments leading to the annotation before the while loop:

$$x \in \mathbb{Z} \wedge n \in \mathbb{N} \Longrightarrow (n \geq 0) \wedge (1 \times x^n = x^n) \tag{VC1}$$

We obtain two more verification conditions by applying the rule for the while command:

$$(K \geq 0) \wedge (Y \times P^K = x^n) \Longrightarrow (K \geq 0) \wedge (Y \times P^K = x^n) \tag{VC2}$$

$$(K \geq 0) \wedge (Y \times P^K = x^n) \wedge (K \leq 0) \Longrightarrow (Y = x^n) \tag{VC3}$$

Now we have to add verification conditions for the body of the while loop, i.e., the conditional command. The starting condition is $\{(K \geq 0) \wedge (Y \times P^K = x^n) \wedge (K > 0)\}$ and we need to show that after the conditional command $\{(K \geq 0) \wedge (Y \times P^K = x^n)\}$ holds. Applying the rule for conditional commands, we get the following two additional verification conditions:

$$\begin{aligned}(K \geq 0) \wedge (Y \times P^K = x^n) \wedge (K > 0) \wedge (K \bmod 2 = 0)& \\ \Longrightarrow (K/2 \geq 0) \wedge (Y \times (P \times P)^{K/2} = x^n)&\end{aligned} \tag{VC4}$$

$$\begin{aligned}(K \geq 0) \wedge (Y \times P^K = x^n) \wedge (K > 0) \wedge (K \bmod 2 = 1)& \\ \Longrightarrow (K - 1 \geq 0) \wedge (Y \times P \times P^{K-1} = x^n)&\end{aligned} \tag{VC5}$$

d) Proof of the verification conditions: VC1 is trivially true since $n \in \mathbb{N}$ implies that $n \geq 0$ and obviously $1 \times x^n = x^n$. VC2 is also trivially true since the statement on the left and right side of the implication is identical.

For VC3, we have:

$$\begin{aligned}(K \geq 0) \wedge (Y \times P^K = x^n) \wedge (K \leq 0) &\Longrightarrow (K = 0) \wedge (Y \times P^K = x^n) \\ &\Longrightarrow (Y \times P^0 = x^n) \\ &\Longrightarrow (Y \times 1 = x^n) \\ &\Longrightarrow (Y = x^n)\end{aligned}$$

For VC4, we have:

$$\begin{aligned}(K \geq 0) \wedge (Y \times P^K = x^n) \wedge (K > 0) \wedge (K \bmod 2 = 0) &\Longrightarrow (K > 0) \wedge (K \bmod 2 = 0) \wedge (Y \times P^K = x^n) \\ &\Longrightarrow (K/2 > 0) \wedge (Y \times P^{2(K/2)} = x^n \\ &\Longrightarrow (K/2 > 0) \wedge (Y \times (P \times P)^{K/2} = x^n)\end{aligned}$$

For VC5, we have:

$$\begin{aligned}(K \geq 0) \wedge (Y \times P^K = x^n) \wedge (K > 0) \wedge (K \bmod 2 = 1) &\Longrightarrow (K > 0) \wedge (K \bmod 2 = 1) \wedge (Y \times P^K = x^n) \\ &\Longrightarrow (K - 1 \geq 0) \wedge (Y \times P^K = x^n) \\ &\Longrightarrow (K - 1 \geq 0) \wedge (Y \times P \times P^{K-1} = x^n)\end{aligned}$$

e) We have to add a variant E that decreases on each iteration of the while loop. In this case, we can simply define $E = K$.

Precondition: $\{x \in \mathbb{Z} \land n \in \mathbb{N}\}$

1: $K := n$
2: $P := x$
3: $Y := 1$
4: $\{(K \geq 0) \land (Y \times P^K = x^n)\}$
5: **while** $K > 0$ **do**
6: $\quad \{(K \geq 0) \land (Y \times P^K = x^n)\}$
7: $\quad [K]$
8: $\quad$ **if** $K \bmod 2 = 0$ **then**
9: $\quad\quad P := P \times P$
10: $\quad\quad K := K/2$
11: $\quad$ **else**
12: $\quad\quad Y := Y \times P$
13: $\quad\quad K := K - 1$
14: $\quad$ **fi**
15: **od**

Postcondition: $\{Y = x^n\}$

---

f) We have to add the following verification condition

$$(Y \times P^K = x^n) \land (K > 0) \Longrightarrow (K \geq 0) \tag{VC6}$$

and we have to extend VC4 and VC5:

$$\begin{aligned}(K \geq 0) \land (Y \times P^K = x^n) \land (K > 0) \land (K \bmod 2 = 0) \land (K = m)& \\ \Longrightarrow (K/2 \geq 0) \land (Y \times (P \times P)^{K/2} = x^n) \land (K/2 < m)& \quad \text{(VC4')} \\ (K \geq 0) \land (Y \times P^K = x^n) \land (K > 0) \land (K \bmod 2 = 1) \land (K = m)& \\ \Longrightarrow (K - 1 \geq 0) \land (Y \times P \times P^{K-1} = x^n) \land (K - 1 < m)& \quad \text{(VC5')}\end{aligned}$$

g) VC6 is trivially true since $K > 0$ implies $K \geq 0$. We already know that the VC4 and VC5 are true so we only have to show that $(K = m) \Longrightarrow (K/2 < m)$ and $(K = m) \Longrightarrow (K - 1 < m)$. This implications are both obviously true.

Marking:

a) - *0.5pt for a reasonable precondition*
- *0.5pt for a reasonable postcondition*

b) - *1pt for a suitable annotation before the while loop*
- *1pt for a suitable loop invariant*

c) - *0pt for VC1 (this is trivial)*
- *0.5pt for each of VC2, VC3, VC4, VC5*

d) - *0.5pt for both VC1 and VC2*
- *0.5pt for each of VC3, VC4, VC5*

e) - *1pt for a correct variant*

f) - *0.2pt for VC6*
- *0.4pt each for VC4' and VC5'*

g) - *0.2pt for VC6*
- *0.4pt each for VC4' and VC5'*