Secure and Dependable Systems
Jacobs University Bremen
Dragi Kamov

Course: CO21-320203
March 14th, 2019

Homework 2

Problem 2.1

Solution:

a) **Translate the C function into Hoare language constructs and define the precondition and the postcondition of the function** $exp()$

precondition { $(n >= 0)$ }

```
K := n
P := x
Y := 1
WHILE (K > 0) DO
IF (K % 2 = 0) THEN
P := P * P
K := K / 2
ELSE
Y := Y * P
K := K - 1
FI
OD
```

postcondition{ $y = x^n$ }

b) **Add annotations for partial correctness**

precondition { $(n >= 0)$ }

```
K := n
P := x
Y := 1
  {(K = n) ∧ (P = x) ∧ (Y = 1)}
WHILE (K > 0) DO
  {(Y ∗ exp(P,K) == exp(x,n))}
IF (K % 2 = 0) THEN
P := P * P
K := K / 2
ELSE
Y := Y * P
K := K - 1
FI
OD
```

postcondition{ $Y * exp(P, K) == exp(x, n)$ }

c) **Derive verification conditions for partial correctness**

$(n >= 0) \rightarrow ((K = n) \wedge (P = x) \wedge (Y = 1))$
$((K = n) \wedge (P = x) \wedge (Y = 1)) \rightarrow (Y * exp(P, K) == exp(x, n))$
$(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (K\%2 == 0) \rightarrow (Y * exp(P, K) == exp(x, n))$
$(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (K\%2\,! = 0) \rightarrow (Y * exp(P, K) == exp(x, n))$

d) **Prove the partial correctness verification conditions**

$\{n >= 0\}$ K = n; P = x; Y = 1 $\{(K = n) \wedge (P = x) \wedge (Y = 1)\}$
Substitution method
$\{(n >= 0)\}\{(n = (n \wedge x) = (x \wedge 1) = 1)\}$
$(n >= 0) \rightarrow (T \wedge T \wedge T)$ Tautology method
$(n >= 0) \rightarrow (T)$

$\{(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (K\%2 == 0)\} P = P * P, K = K/2 \{Y * exp(P, K) == exp(x, n)\}$
Substitution method
$\{(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (K\%2 == 0)\}\{Y * exp(P^2, K/2) == exp(x, n)\}$
$((Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (K\%2 == 0)) \rightarrow (Y * exp(P, K) == exp(x, n))$
The following is holding true by implication, given that the loop invariant is true.

$\{(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (K\%2 \,! = 0)\}$ Y = Y * P; K = K - 1 $\{Y * exp(P, K) == exp(x, n)\}$
$\{(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (K\%2 \,! = 0)\}\{Y * P * exp(P, K - 1) == exp(x, n)\}$
Multiplicative identity.
$((Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (K\%2 \,! = 0)) \rightarrow (Y * exp(P, K) == exp(x, n))$
The following is holding true by implication, given that the loop invariant is true.

e) **Add additional annotations for total correctness**

precondition $\{ \ n >= 0 \ \}$

```
  {(K = n) ∧ (P = x) ∧ (Y = 1)}
K := n
P := x
Y := 1
WHILE (K > 0) DO
  {(Y * exp(P,K) == exp(x,n)) ∧ ((( K % 2 = 0 ) ∨ (K % 2 != 0)) ∧ (K >= 0))}
 IF (K % 2 = 0) THEN
P := P * P
K := K / 2
ELSE
Y := Y * P
K := K - 1
FI
OD
```

postcondition$\{ \ Y * exp(P, K) == exp(x, n) \wedge (K >= 0) \ \}$

f) **Derive or update verification conditions for total correctness**

$(n >= 0) \rightarrow ((K = n) \wedge (P = x) \wedge (Y = 1))$
$((K = n) \wedge (P = x) \wedge (Y = 1)) \rightarrow (Y * exp(P, K) == exp(x, n) \wedge (K > 0))$
$(Y * exp(P, K) == exp(x, n)) \rightarrow ((K\%2 == 0) \vee (K\%2 \,! = 0))$
$(K\%2 == 0) \rightarrow (Y * exp(P, K) == exp(x, n) \wedge (K >= 0))$
$(K\%2 \,! = 0) \rightarrow (Y * exp(P, K) == exp(x, n) \wedge (K >= 0))$

g) **Prove the total correctness verification conditions**

$\{((Y * exp(P, K) == exp(x, n)) \wedge ((K\%2 == 0) \vee (K\%2 \,! = 0) \wedge (K > 0))\} \ \{(Y * exp(P, K) == exp(x, n))\}$
1. The loop terminates.
2. For the program to terminate, K must be less than 0 at some point in time. And since K is decreasing with each step the program is going to terminate.
K decreases in the following two ways:
1) If K is even, then K gets divided by half. .
2) If K is odd, then K gets decremented by 1, which is quite obviously decreasing.