Secure and Dependable Systems
Jacobs University Bremen
Fezile Manana

Course: CO21-320203
13th March 2019

Homework 2

Problem 2.1

a) Precondition $\Rightarrow \{(n \geqslant 0)\}$

```
1: K := n
2: P := x
3: Y := 1
4: While (K > 0) DO
5:   IF (K % 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 $\Rightarrow \{Y = x^n\}$

b) Precondition $\Rightarrow \{(n \geqslant 0)\}$

```
1: K := n
2: P := x
3: Y := 1
     {(K = n ∧ P = x ∧ Y = 1)}
4: While (K > 0) DO
     {(Y * exp(P, K) == exp(x, n))}
5:   IF (K % 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 $\Rightarrow \{Y * exp(P, K) == exp(x, n)\}$

c)
- Assignments on lines 1, 2, and 3:
  $(n >= 0) \rightarrow (K = n \wedge P = x \wedge Y = 1)$

- While loop:
  $(K = N \wedge P = X \wedge Y = 1) \rightarrow (Y * exp(P, K) = exp(x, n))$
  $(Y * exp(P, K) = exp(x, n) \wedge \neg(K > 0)) \rightarrow (Y = exp(x, n))$
  Final statement takes if statement into consideration which leads to two different validation conditions.
  $\{Y * exp(P, K) = exp(x, n) \wedge K > 0\}$ IF K % 2 = 0 THEN C 1 ELSE C 2 FI $\{Y * exp(P, K) = exp(x, n)\}$
  $(Y * exp(P, K) = exp(x, n) \wedge K > 0 \wedge K\%2 = 0) \rightarrow (Y * exp(P * P, K/2) = exp(x, n))$
  $(Y * exp(P, K) = exp(x, n) \wedge K > 0 \wedge \neg(K\%2 = 0)) \rightarrow ((Y * P) * exp(P, K - 1) = exp(x, n))$

d) $\underline{(n >= 0) \rightarrow (K = n \wedge P = x \wedge Y = 1)}$

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

$\underline{(K = N \wedge P = X \wedge Y = 1) \rightarrow (Y * exp(P, K) = exp(x, n))}$

$\{N = n \wedge X = x \wedge N \geqslant 0\} K := n, P := x, Y := 1 \{K = n \geqslant 0 \wedge P = x \wedge Y = 1\}$
Substitution: $\{N = n \wedge P = x\}\{n = n \geqslant 0 \wedge x = x \wedge 1 = 1\}$
$(N = n \wedge P = x) \rightarrow (K = n \geqslant 0 \wedge P = x \wedge Y = 1)$

Loop invariant: $(Y * exp(P, K) = exp(x, n))$
P = Q = invariant

If $K\%2 = 0$ then
$\{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0 \wedge K\%2 = 0\} P := P * P, K := K/2 \{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0\}$
$\{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0 \wedge K\%2 = 0\}\{exp(Y * (P * P), K/2) = exp(x, n) \wedge K/2 \geqslant 0\}$
$(Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0 \wedge K\%2 = 0) \rightarrow (Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0)$

else
$\{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0 \wedge \neg K\%2 = 0\} Y := Y * exp(P, K) := K - 1 \{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0\}$
$\{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0 \wedge \neg K\%2 = 0\}\{Y * P * exp(P, K-1) = exp(x, n) \wedge K-1 \geqslant 0\}$
$(Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0 \wedge \neg K\%2 = 0) \rightarrow (Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0)$

$\underline{(K = N \wedge P = X \wedge Y = 1) \rightarrow (Y * exp(P, K) = exp(x, n)):}$

$\{K = n > 0 \wedge P = x \wedge Y = 1\}\{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0\}$
$K = n > 0 \wedge P = x \wedge Y = 1 \rightarrow 1 * exp(x, n) = xn \wedge K \geqslant 0$
$(K = n > 0 \wedge P = x \wedge Y = 1) \rightarrow (Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0)$

$\underline{(Y * exp(P, K) = exp(x, n) \wedge \neg(K > 0)) \rightarrow (Y = exp(x, n)):}$

$\{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0 \wedge \neg(K > 0)\}\{Y = exp(x, n)\}$
$\{Y * exp(P, K) = exp(x, n) \wedge K \geqslant 0 \wedge \neg(K > 0)\}\{Y * (exp(P, 0) = 1) = exp(x, n)\}$
$(Y * PK = exp(x, n) \wedge K \geqslant 0 \wedge \neg(K > 0)) \rightarrow (Y = exp(x, n))$

$\underline{(Y * exp(P, K) = exp(x, n) \wedge K > 0 \wedge K\%2 = 0) \rightarrow (Y * exp(P * P, K/2) = exp(x, n))}$
$\{(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge (k\%2)\} P = P * P, K = K/2 \{Y * exp(P, K) == exp(x, n)\}$
$\{(Y * exp(P, K) == exp(x, n))\}\{Y * exp(P^2, K/2) == exp(x, n)\}$
$((Y * exp(P, K) == exp(x, n))) \rightarrow (Y * exp(P, K) == exp(x, n))$

$\underline{(Y * exp(P, K) = exp(x, n) \wedge K > 0 \wedge \neg(K\%2 = 0)) \rightarrow ((Y * P) * exp(P, K - 1) = exp(x, n))}$
$\{(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge \neg(k\%2)\} Y = Y * P, K = K - 1 \{Y * exp(P, K) == exp(x, n)\}$
$\{(Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge \neg(k\%2)\}\{Y * P * exp(P, K - 1) == exp(x, n)\}$
$((Y * exp(P, K) == exp(x, n)) \wedge (K > 0) \wedge \neg(k\%2)) \rightarrow (Y * exp(P, K) == exp(x, n))$

e) Precondition $\Rightarrow \{(n \geqslant 0)\}$

```
1: K := n
2: P := x
3: Y := 1
     {(K = n ∧ P = x ∧ Y = 1)}
4: While (K > 0 DO
     {(Y * exp(P, K) == exp(x, n)}
     [K]
5:   IF (K % 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 $\Rightarrow \{Y * exp(P, K) == exp(x, n) \wedge (K >= 0)\}$

f) Assignments on lines 1, 2, and 3:
$(n >= 0) \rightarrow (K = n \wedge P = x \wedge Y = 1)$
While loop:
$(K = N \wedge P = X \wedge Y = 1) \rightarrow (Y * exp(P, K) = exp(x, n))$
$(Y * exp(P, K) = exp(x, n) \wedge \neg(K > 0)) \rightarrow (Y = exp(x, n))$
Final statement takes if statement into consideration which leads to two different validation conditions.
$\{Y * exp(P, K) = exp(x, n) \wedge K > 0\}$IF K % 2 = 0 THEN C 1 ELSE C 2 FI $\{Y * exp(P, K) = exp(x, n)\}$

$(Y * exp(P, K) = exp(x, n) \wedge K > 0) \rightarrow (K \geqslant 0)$
$(Y * exp(P, K) = exp(x, n) \wedge K > 0 \wedge K = n \wedge K\%2 = 0) \rightarrow (Y * exp(P * P, K/2) = exp(x, n) \wedge K/2 < n)$
$(Y * exp(P, K) = exp(x, n) \wedge K > 0 \wedge K = n \wedge \neg(K\%2 = 0)) \rightarrow ((Y * P) * exp(P, K - 1) = exp(x, n) \wedge K - 1 < n)$

g) $\underline{(Y * exp(P, K) = exp(x, n) \wedge K > 0) \rightarrow (K \geqslant 0)}$

Given that $K > 0$, then $K \geqslant 0$.

$\underline{(Y * exp(P, K) = exp(x, n) \wedge K > 0 \wedge K = n \wedge K\%2 = 0) \rightarrow (Y * exp(P * P, K/2) = exp(x, n) \wedge K/2 < n)}$

K is decreasing as $K/2$ rounds down K.

$\underline{(Y * exp(P, K) = exp(x, n) \wedge K > 0 \wedge K = n \wedge \neg(K\%2 = 0)) \rightarrow ((Y * P) * exp(P, K - 1) = exp(x, n) \wedge K - 1}$

Trivially K is decreasing as $K - 1$ decrements K, and will terminate.