Introduction to Computer Science
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: CH-232-A
Date: 2019-11-29
Due: 2019-12-06

ICS 2019 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.