

ICS 2020 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  $K \bmod 2 = 0$  then
6:      $P := P \times P$ 
7:      $K := K/2$ 
8:   else
9:      $Y := Y \times P$ 
10:     $K := K - 1$ 
11:  fi
12: od
```

- Define a suitable precondition and a suitable postcondition.
- Add annotations for partial correctness.
- Derive verification conditions for partial correctness.
- Prove the partial correctness verification conditions.
- Add additional annotations for total correctness.
- Derive or update verification conditions for total correctness.
- Prove the total correctness verification conditions.