

### SADS 2020 Problem Sheet #3

**Problem 3.1:** *correctness of exponentiation algorithm* (1+1+2+1+2+1+1+1 = 10 points)

Prove step-by-step the partial correctness and the total correctness of the following function  $f()$  using Hoare Logic. Our claim is that the function  $f(x, n)$  calculates  $x^n$  for integers  $x$  and  $n$ .

```
#include <stdio.h>
#include <stdlib.h>

int f(int x, int n)
{
    int k = n;
    int p = x;
    int y = 1;

    while (k > 0) {
        if (k % 2 == 0) {
            p = p * p;
            k /= 2;
        } else {
            y = y * p;
            k--;
        }
    }

    return y;
}

int main(int argc, char *argv[])
{
    if (argc != 3) {
        return EXIT_FAILURE;
    }

    printf("%d\n", f(atoi(argv[1]), atoi(argv[2])));
    return EXIT_SUCCESS;
}
```

- a) Translate the C function into Hoare language.
- b) Define a suitable precondition and a suitable postcondition.
- c) Add annotations for partial correctness.
- d) Derive verification conditions for partial correctness.
- e) Prove the partial correctness verification conditions.
- f) Add additional annotations for total correctness.
- g) Derive or update verification conditions for total correctness.
- h) Prove the total correctness verification conditions.