Exam Program Correctness, June 18th 2014, 9:00-12:00h.

- This exam consists of three problems. Problem 1 is worth 20 points, problem 2 is worth 30 points, and problem 3 is worth 40 points. You get 10 points for not misspelling your name and student number.
- Give complete annotations, and linear proofs. Use a pen. Do not use a pencil!
- The exam is a closed book exam. You are not allowed to use the reader, slides, notes, or any other material.
- Do not hand in scratch paper!

Problem 1 (20 pt).
(a) Prove the correctness of the following conditional command (where z, a, and n are variables of the type $\mathbb{N}$):

$\{z \cdot a^{2\cdot(n \textbf{ div } 2)+n} \textbf{ mod } 2 = Z \ \wedge \ n \geq 0\}$
if n **mod** $2 = 1$ **then**
  $z := z * a$;
end;
$a := a * a$;
$n := n$ **div** 2;
$\{z \cdot a^n = Z \ \wedge \ n \geq 0\}$

(b) Prove the correctness of the following program fragment

var $n, x, y, z : \mathbb{Z}$;
  $\{P : n \geq 0 \ \wedge \ (x+y)^n = Z\}$
$z := 1$;
while $n \neq 0$ **do**
  if n **mod** $2 = 1$ **then**
    $z := z * (x + y)$
  end;
  $x := x * x + 2 * x * y$;
  $y := y * y$;
  $n := n$ **div** 2;
end;
  $\{Q : z = Z\}$

Problem 2 (30 pt). Design and prove the correctness of a command S that satisfies

const $n : \mathbb{N}$, $a :$ **array** $[0..n)$ **of** $\mathbb{Z}$;
var $x : \mathbb{Z}$;
  $\{P :$ **true**$\}$
S
  $\{Q : x = \Sigma(\text{Max}\{a[j] \mid j : 0 \leq j \leq i\} \mid i : 0 \leq i < n)\}$.

The time complexity of the command S must be linear in n. Start by defining (a) suitable helper function(s) and the corresponding recurrence(s). It is allowed to use the constants $-\infty$ and/or $+\infty$ in your program.

Problem 3 (40 pt). Given is a two-dimensional array a that is *increasing* in both indices. Consider the following specification:

const $n, w : \mathbb{N}$, $a :$ **array** $[0..n)$ **of** $\mathbb{N}$;
var $k : \mathbb{N}$;
  $\{P : \ Z = \#\{(i,j) \mid i,j : 0 \leq i \leq j < n \ \wedge \ a[i,j] = w\}\ \}$
S
  $\{Q : \ k = Z\}$

(a) Make a sketch in which you clearly indicate where the array is high, low, and how a contour line goes.

(b) Define a function $F(x, y)$ that can be used to compute Z. Determine the relevant recurrences for $F(x, y)$, including the base cases.

(c) Design a command S that has a linear time complexity in n. Prove the correctness of your solution.