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

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** $2;$
$\{z \cdot a^n = Z \ \wedge\ n \geq 0\}$

Solution:

$\{z \cdot a^{2\cdot(n \textbf{ div } 2)+n \textbf{ mod } 2} = Z \ \wedge\ n \geq 0\}$
if n **mod** $2 = 1$ **then**
$\{n \textbf{ mod } 2 = 1 \ \wedge\ z \cdot a^{2\cdot(n \textbf{ div } 2)+n \textbf{ mod } 2} = Z \ \wedge\ n \geq 0\}$
(∗ substitution; logic ∗)
$\{z \cdot a^{2\cdot(n \textbf{ div } 2)+1} = Z \ \wedge\ n \geq 0\}$
(∗ calculus ∗)
$\{z \cdot a \cdot a^{2\cdot(n \textbf{ div } 2)} = Z \ \wedge\ n \geq 0\}$
$z := z * a;$
$\{z \cdot a^{2\cdot(n \textbf{ div } 2)} = Z \ \wedge\ n \geq 0\}$
else
$\{n \textbf{ mod } 2 = 0 \ \wedge\ z \cdot a^{2\cdot(n \textbf{ div } 2)+n \textbf{ mod } 2} = Z \ \wedge\ n \geq 0\}$
(∗ substitution; logic ∗)
$\{z \cdot a^{2\cdot(n \textbf{ div } 2)} = Z \ \wedge\ n \geq 0\}$
end; (∗ collect branches ∗)
$\{z \cdot a^{2\cdot(n \textbf{ div } 2)} = Z \ \wedge\ n \geq 0\}$
(∗ calculus ∗)
$\{z \cdot (a^2)^{n \textbf{ div } 2} = Z \ \wedge\ n \textbf{ div } 2 \geq 0\}$
$a := a * a;$
$n := n$ **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;
$\{Q : z = Z\}$

Solution: problem 1(a) suggests the invariant: $J :\ n \geq 0 \ \wedge\ z \cdot (x + y)^n = Z$. In the body of the loop, n is decreased. So, we choose the variant function vf$= n \in \mathbb{Z}$. The invariant states that $n \geq 0$, so $J \wedge B \Rightarrow \text{vf} \geq 0$. The remaining proof obligations are verified in the following annotation:

$\{P : n \geq 0 \ \wedge\ (x+y)^n = Z\}$
(∗ calculus ∗)
$\{n \geq 0 \ \wedge\ 1 \cdot (x+y)^n = Z\}$

$z := 1;$

$\{J :\ n \geq 0 \ \wedge\ z \cdot (x+y)^n = Z\}$

while $n \neq 0$ **do**

$\{z \cdot (x+y)^n = Z \ \wedge\ n = V > 0\}$
(∗ calculus ∗)
$\{z \cdot (x+y)^{2 \cdot (n \textbf{ div } 2) + n \textbf{ mod } 2} = Z \ \wedge\ n = V > 0\}$

if n **mod** $2 = 1$ **then**

$\{n \textbf{ mod } 2 = 1 \ \wedge\ z \cdot (x+y)^{2 \cdot (n \textbf{ div } 2) + n \textbf{ mod } 2} = Z \ \wedge\ n = V > 0\}$
(∗ substitution; calculus; logic ∗)
$\{z \cdot (x+y) \cdot (x+y)^{2 \cdot (n \textbf{ div } 2)} = Z \ \wedge\ n = V > 0\}$

$z := z * (x+y)$

$\{z \cdot (x+y)^{2 \cdot (n \textbf{ div } 2)} = Z \ \wedge\ n = V > 0\}$

else

$\{n \textbf{ mod } 2 = 0 \ \wedge\ z \cdot (x+y)^{2 \cdot (n \textbf{ div } 2) + n \textbf{ mod } 2} = Z \ \wedge\ n = V > 0\}$
(∗ substitution; calculus; logic ∗)
$\{z \cdot (x+y)^{2 \cdot (n \textbf{ div } 2)} = Z \ \wedge\ n = V > 0\}$

end; (∗ collect branches ∗)

$\{z \cdot (x+y)^{2 \cdot (n \textbf{ div } 2)} = Z \ \wedge\ n = V > 0\}$
(∗ calculus ∗)
$\{z \cdot ((x+y)^2)^{n \textbf{ div } 2} = Z \ \wedge\ n = V > 0\}$
(∗ calculus ∗)
$\{z \cdot (x^2 + 2 \cdot x \cdot y + y^2)^{n \textbf{ div } 2} = Z \ \wedge\ n = V > 0\}$

$x := x * x + 2 * x * y;$

$\{z \cdot (x + y^2)^{n \textbf{ div } 2} = Z \ \wedge\ n = V > 0\}$

$y := y * y;$

$\{z \cdot (x+y)^{n \textbf{ div } 2} = Z \ \wedge\ n = V > 0\}$
(∗ calculus ∗)
$\{z \cdot (x+y)^{n \textbf{ div } 2} = Z \ \wedge\ 0 \leq n \textbf{ div } 2 < V\}$

$n := n$ **div** $2;$

$\{z \cdot (x+y)^n = Z \ \wedge\ 0 \leq n < V\}$
$\{J \ \wedge\ \text{vf} < V\}$

end;

$\{z \cdot (x+y)^n = Z \ \wedge\ n = 0\}$
(∗ $x+y)^0 = 1$ ∗)
$\{Q : z = Z\}$

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

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

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.

Solution: We start by rewriting the postcondition $Q: \ x = S(n)$, where

$$S(k) = \Sigma(\text{Max}\{a[j] \mid j : 0 \le j \le i\} \mid i : 0 \le i < k)$$

Clearly, $S(0) = 0$ (sum over empty domain). For $k \ge 0$ we find:

$$\begin{array}{rcl} S(k+1) & = & \Sigma(\text{Max}\{a[j] \mid j : 0 \le j \le i\} \mid i : 0 \le i < k+1) \\ & = & \{i < k+1 \text{ so } i < k \vee i = k\} \\ & & \Sigma(\text{Max}\{a[j] \mid j : 0 \le j \le i\} \mid i : 0 \le i < k) + \text{Max}\{a[j] \mid j : 0 \le j \le k\} \\ & = & S(k) + M(k+1) \end{array}$$

where $M(k) = \text{Max}\{a[j] \mid j : 0 \le j < k\}$. Clearly $M(0) = -\infty$ (maximum over empty domain) and $M(k+1) = M(k) \textbf{ max } a[k]$ (for $0 \le k < n$).

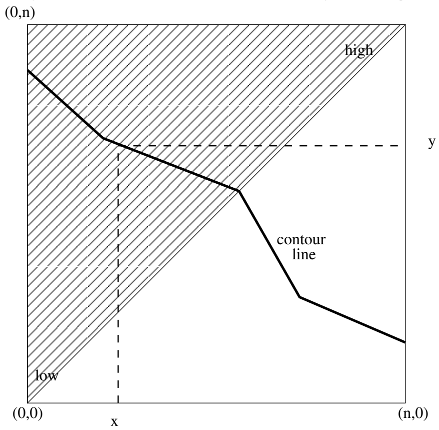
We choose the invariant $J: \ x = S(k) \ \wedge \ y = M(k) \ \wedge \ 0 \le k \le n$ and guard $B: \ k \ne n$. From $J \wedge \neg B$ clearly follows $Q: \ x = s(n)$. We choose the variant function vf$= n - k \in \mathbb{Z}$. The invariant states that $k \le n$, so $J \wedge B \Rightarrow \text{vf} \ge 0$. The remaining proof obligations are verified in the following annotation:

$$\begin{array}{l}
\quad \{P : \textbf{true}\} \\
\qquad (* \ n \in \mathbb{N} \ *) \\
\quad \{0 = S(0) \ \wedge \ -\infty = M(0) \ \wedge \ 0 \le 0 \le n\} \\
k := 0; \ x := 0; \ y := -\infty; \\
\quad \{J: \ x = S(k) \ \wedge \ y = M(k) \ \wedge \ 0 \le k \le n\} \\
\textbf{while } k \ne n \textbf{ do} \\
\qquad \{x = S(k) \ \wedge \ y = M(k) \ \wedge \ 0 \le k < n \ \wedge \ n - k = V\} \\
\qquad\quad (* \ 0 \le k < n; \text{ use recurrences } *) \\
\qquad \{x + M(k+1) = S(k+1) \ \wedge \ y \textbf{ max } a[k] = M(k+1) \ \wedge \ 0 \le k < n \ \wedge \ n - k = V\} \\
\quad y := y \textbf{ max } a[k]; \\
\qquad \{x + M(k+1) = S(k+1) \ \wedge \ y = M(k+1) \ \wedge \ 0 \le k < n \ \wedge \ n - k = V\} \\
\qquad\quad (* \text{ substitution; calculus } *) \\
\qquad \{x + y = S(k+1) \ \wedge \ y = M(k+1) \ \wedge \ 0 \le k+1 \le n \ \wedge \ n - (k+1) < V\} \\
\quad x := x + y; \\
\qquad \{x = S(k+1) \ \wedge \ y = M(k+1) \ \wedge \ 0 \le k+1 \le n \ \wedge \ n - (k+1) < V\} \\
\quad k := k + 1; \\
\qquad \{x = S(k) \ \wedge \ y = M(k) \ \wedge \ 0 \le k \le n \ \wedge \ n - k < V\} \\
\qquad \{J \ \wedge \ \text{vf} < V\} \\
\textbf{end}; \\
\quad \{x = S(k) \ \wedge \ y = M(k) \ \wedge \ k = n\} \\
\quad \{Q : x = S(n)\}
\end{array}$$

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

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

(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.

Solution: $F(x,y) = \#\{(i,j) \mid i,j : x \le i \le j < y\ \wedge\ a[i,j] = w\}$
It is clear that $F(x,y) = 0$ if $x \ge y$ (empty domain). We can shrink the region that corresponds with $F(x,y)$ by incrementing x or decrementing y.

$$\begin{array}{rcl} F(x,y) & = & \#\{(i,j) \mid i,j : x \le i \le j < y\ \wedge\ a[i,j] = w\} \\ & = & \{x \le i \text{ so } x+1 \le i \vee i = x\} \\ & & \#\{(i,j) \mid i,j : x+1 \le i \le j < y\ \wedge\ a[i,j] = w\} + \#\{j \mid j : x \le j < y\ \wedge\ a[x,j] = w\} \\ & = & \{\text{definition } F\} \\ & & F(x+1,y) + \#\{j \mid j : x \le j < y\ \wedge\ a[x,j] = w\} \\ & = & \{a[x,j]\uparrow,\ a[x,y-1] \text{ maximal; } \textbf{if } a[x,y-1] < w \text{ then } a[x,j] < w \text{ (for } x \le j < y)\} \\ & & F(x+1,y) \end{array}$$

$$\begin{array}{rcl} F(x,y) & = & \#\{(i,j) \mid i,j : x \le i \le j < y\ \wedge\ a[i,j] = w\} \\ & = & \{j < y \text{ so } j < y-1 \vee j = y-1\} \\ & & \#\{(i,j) \mid i,j : x \le i \le j < y-1\ \wedge\ a[i,j] = w\} + \#\{i \mid i : x \le i \le y-1\ \wedge\ a[i,y-1] = w\} \\ & = & \{\text{definition } F\} \\ & & F(x,y-1) + \#\{i \mid i : x \le i \le y-1\ \wedge\ a[i,y-1] = w\} \\ & = & \{a[i,y-1]\uparrow,\ a[x,y-1] \text{ minimal; } \textbf{if } a[x,y-1] \ge w \text{ then } a[i,y-1] > w \text{ (for } x < i \le y-1)\} \\ & & F(x,y-1) + \text{ord}(a[x,y-1] = w) \end{array}$$

In conclusion, we found the following recurrence relation:

$$\begin{array}{rcl} x \ge y & \Rightarrow & F(x,y) = 0 \\ 0 \le x < y \le n\ \wedge\ a[x,y-1] < w & \Rightarrow & F(x,y) = F(x+1,y) \\ 0 \le x < y \le n\ \wedge\ a[x,y-1] = w & \Rightarrow & F(x,y) = F(x,y-1) + 1 \\ 0 \le x < y \le n\ \wedge\ a[x,y-1] > w & \Rightarrow & F(x,y) = F(x,y-1) \end{array}$$

(c) Design a command S that has a linear time complexity in n. Prove the correctness of your solution.
Solution: It is clear that we can rewrite the predondition as $P: \ Z = F(0, n)$. The standard invariant for this type of problem is:

$$J: \ Z = k + F(x, y) \ \wedge \ 0 \leq x \leq n \ \wedge \ 0 \leq y \leq n$$

We choose the guard $B: \ x < y$, such that $\neg B \equiv x \geq y$. In that case $F(x, y) = 0$, so $J \ \wedge \ \neg B \Rightarrow Q: \ k = Z$. In the body of the loop we will increment x and decrement y. The guard says $x < y$, so we can choose $\text{vf} = y - x \in \mathbb{Z}$. Clearly, $J \wedge B \Rightarrow \text{vf} \geq 0$. The remaining proof obligations are verified in the following annotation:

$\{P : Z = F(0, n)\}$
  (* $n \in \mathbb{N}$; calculus *)
$\{Z = 0 + F(0, n) \ \wedge \ 0 \leq 0 \leq n \ \wedge \ 0 \leq 0 \leq n\}$
$k := 0; \ x := 0; \ y := y;$
$\{J: \ Z = k + F(x, y) \ \wedge \ 0 \leq x \leq n \ \wedge \ 0 \leq y \leq n\}$
while $x < y$ **do**
  $\{Z = k + F(x, y) \ \wedge \ 0 \leq x < y \leq n \ \wedge \ y - x = V\}$
  if $a[x, y - 1] < w$ **then**
    $\{a[x, y - 1] < w \ \wedge \ Z = k + F(x, y) \ \wedge \ 0 \leq x < y \leq n \ \wedge \ y - x = V\}$
      (* recurrence, case $0 \leq x < y \leq n \ \wedge \ a[x, y - 1] < w$, so $F(x, y) = F(x + 1, y)$ *)
    $\{Z = k + F(x + 1, y) \ \wedge \ 0 \leq x < y \leq n \ \wedge \ y - x = V\}$
      (* $x < y \leq n \Rightarrow x + 1 \leq n$; calculus; logic *)
    $\{Z = k + F(x + 1, y) \ \wedge \ 0 \leq x + 1 \leq n \ \wedge \ 0 \leq y \leq n \ \wedge \ y - (x + 1) < V\}$
  $x := x + 1;$
    $\{Z = k + F(x, y) \ \wedge \ 0 \leq x \leq n \ \wedge \ 0 \leq y \leq n \ \wedge \ y - x < V\}$
  else if $a[x, y - 1] > w$ **then**
    $\{a[x, y - 1] > w \ \wedge \ Z = k + F(x, y) \ \wedge \ 0 \leq x < y \leq n \ \wedge \ y - x = V\}$
      (* recurrence, case $0 \leq x < y \leq n \ \wedge \ a[x, y - 1] > w$, so $F(x, y) = F(x, y - 1)$ *)
    $\{Z = k + F(x, y - 1) \ \wedge \ 0 \leq x < y \leq n \ \wedge \ y - x = V\}$
      (* $0 \leq x < y \leq n \Rightarrow 0 \leq y - 1$; calculus; logic *)
    $\{Z = k + F(x, y - 1) \ \wedge \ 0 \leq x \leq n \ \wedge \ 0 \leq y - 1 \leq n \ \wedge \ (y - 1) - x < V\}$
  $y := y - 1;$
    $\{Z = k + F(x, y) \ \wedge \ 0 \leq x \leq n \ \wedge \ 0 \leq y \leq n \ \wedge \ y - x < V\}$
  else (* remaining case is $a[x, y - 1] = w$ *)
    $\{a[x, y - 1] = w \ \wedge \ Z = k + F(x, y) \ \wedge \ 0 \leq x < y \leq n \ \wedge \ y - x = V\}$
      (* recurrence, case $0 \leq x < y \leq n \ \wedge \ a[x, y - 1] = w$, so $F(x, y) = F(x, y - 1) + 1$ *)
    $\{Z = k + 1 + F(x, y - 1) \ \wedge \ 0 \leq x < y \leq n \ \wedge \ y - x = V\}$
  $k := k + 1;$
    $\{Z = k + F(x, y - 1) \ \wedge \ 0 \leq x < y \leq n \ \wedge \ y - x = V\}$
      (* $0 \leq x < y \leq n \Rightarrow 0 \leq y - 1$; calculus; logic *)
    $\{Z = k + F(x, y - 1) \ \wedge \ 0 \leq x \leq n \ \wedge \ 0 \leq y - 1 \leq n \ \wedge \ (y - 1) - x < V\}$
  $y := y - 1;$
    $\{Z = k + F(x, y) \ \wedge \ 0 \leq x \leq n \ \wedge \ 0 \leq y \leq n \ \wedge \ y - x < V\}$
  end; (* collect branches *)
  $\{J \ \wedge \ \text{vf} < V\}$
end;
$\{Z = k + F(x, y) \ \wedge \ 0 \leq x \leq n \ \wedge \ 0 \leq y \leq n \ \wedge \ x \geq y\}$
  {recurrence, case $x \geq y$, so so $F(x, y) = 0$; logic *)
$\{Q : Z = k\}$