Answers Exam Program Correctness, May 6th 2015.

Problem 1 ($2 \times 10 = 20$ pt). Declared is the variable $x : \mathbb{Z}$.
(a) Design an annotated command S_0 that satisfies the Hoare triple:

$$\{\ x = X\ \}\ \ S_0\ \ \{\ x > 0\ \wedge\ (x = 2 \cdot X + 1\ \vee\ x = -2 \cdot X)\ \}$$

(b) Design an annotated command S_1 that satisfies the reverse Hoare triple:

$$\{\ x > 0\ \wedge\ (x = 2 \cdot X + 1\ \vee\ x = -2 \cdot X)\ \}\ \ S_1\ \ \{\ x = X\ \}$$

Answers:

(a)
$\{x = X\}$
if $x \geq 0$ **then**
$\{x \geq 0\ \wedge\ x = X\}$
(∗ calculus ∗)
$\{2 \cdot x + 1 > 0\ \wedge\ 2 \cdot x + 1 = 2 \cdot X + 1\}$
$x := 2 * x + 1;$
$\{x > 0\ \wedge\ x = 2 \cdot X + 1\}$
(∗ logic ∗)
$\{x > 0\ \wedge\ (x = 2 \cdot X + 1\ \vee\ x = -2 \cdot X)\}$
else
$\{x < 0\ \wedge\ x = X\}$
(∗ calculus ∗)
$\{-2 \cdot x > 0\ \wedge\ -2 \cdot x = -2 \cdot X\}$
$x := -2 * x;$
$\{x > 0\ \wedge\ x = -2 \cdot X\}$
(∗ logic ∗)
$\{x > 0\ \wedge\ (x = 2 \cdot X + 1\ \vee\ x = -2 \cdot X)\}$
end; (∗ collect branches ∗)
$\{x > 0\ \wedge\ (x = 2X + 1\ \vee\ x = -2X)\}$

(b)
$\{x > 0\ \wedge\ (x = 2 \cdot X + 1\ \vee\ x = -2 \cdot X)\}$
if x **mod** $2 = 0$ **then**
$\{x \textbf{ mod } 2 = 0\ \wedge\ x > 0\ \wedge\ (x = 2 \cdot X + 1\ \vee\ x = -2 \cdot X)\}$
(∗ $x \textbf{ mod } 2 = 0 \Rightarrow x \neq 2 \cdot X + 1$ ∗)
$\{x = -2X\}$
(∗ calculus ∗)
$\{(-x) \textbf{ div } 2 = X\}$
$x := (-x) \textbf{ div } 2;$
$\{x = X\}$
else
$\{x \textbf{ mod } 2 \neq 0\ \wedge\ x > 0\ \wedge\ (x = 2 \cdot X + 1\ \vee\ x = -2 \cdot X)\}$
(∗ $x \textbf{ mod } 2 \neq 0 \Rightarrow x \neq -2 \cdot X$ ∗)
$\{x = 2 \cdot X + 1\}$
(∗ calculus ∗)
$\{(x - 1) \textbf{ div } 2 = X\}$
$x := (x - 1) \textbf{ div } 2;$
$\{x = X\}$
end; (∗ collect branches ∗)
$\{x = X\}$

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

$$\begin{array}{l}
\textbf{const } n : \mathbb{N}, \quad a : \textbf{ array } [0..n) \textbf{ of } \mathbb{Z}; \\
\textbf{var } s : \mathbb{Z}; \\
\quad \{ P : \textbf{ true } \} \\
T \\
\quad \{ Q : s = \Sigma(\Sigma(a[j] \cdot a[k] \mid j,k : i \leq j \leq k < n) \mid i : 0 \leq i < n) \} .
\end{array}$$

The time complexity of the command T must be linear in n. Start by defining (a) suitable helper function(s) and the corresponding recurrence(s).

Answer: We start by introducing $F(x) = \Sigma(\Sigma(a[j] \cdot a[k] \mid j,k : i \leq j \leq k < n) \mid i : x \leq i < n)$ such that we can rewrite the postcondition as

$$Q : \; s = F(0)$$

Note that we found $F(x)$ by replacing the the constant 0 (lower bound index i) by the variable x. Replacing the upper bound n by x does not work, since the inner expression is then hard (impossible) to initialize.

It is clear that $F(n) = 0$ (sum over empty domain). In a loop, we will decrement x, so we are interested in a recurrence for $F(x-1)$.

$$\begin{array}{ll}
 & F(x-1) \\
= & \{ \text{ definition } F \} \\
 & \Sigma(\Sigma(a[j] \cdot a[k] \mid j,k : i \leq j \leq k < n) \mid i : x-1 \leq i < n) \\
= & \{ \textbf{ assume } 0 < x \leq n; \text{ split } x \leq i \text{ or } i = x-1 \ \} \\
 & \Sigma(\Sigma(a[j] \cdot a[k] \mid j,k : i \leq j \leq k < n) \mid i : x \leq i < n) \ + \ \Sigma(a[j] \cdot a[k] \mid j,k : x-1 \leq j \leq k < n) \\
= & \{ \text{ definition } F \} \\
 & F(x) \ + \ \Sigma(a[j] \cdot a[k] \mid j,k : x-1 \leq j \leq k < n) \\
= & \{ \textbf{ introduce } G(x) = \Sigma(a[j] \cdot a[k] \mid j,k : x \leq j \leq k < n) \ \} \\
 & F(x) + G(x-1)
\end{array}$$

It is clear that $G(n) = 0$ (sum over empty domain). We are interested in a recurrence for $G(x-1)$.

$$\begin{array}{ll}
 & G(x-1) \\
= & \{ \text{ definition } G \} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x-1 \leq j \leq k < n) \\
= & \{ \textbf{ assume } 0 < x \leq n; \text{ split } x \leq j \text{ or } j = x-1 \ \} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x \leq j \leq k < n) \ + \ \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \leq k < n) \\
= & \{ \text{ definition } G; \text{ calculus} \} \\
 & G(x) \ + \ a[x-1] \cdot \Sigma(a[j] \mid k : x-1 \leq k < n) \\
= & \{ \textbf{ introduce } H(x) = \Sigma(a[k] \mid k : x \leq k < n) \ \} \\
 & G(x) \ + \ a[x-1] \cdot H(x-1)
\end{array}$$

It is clear that $H(n) = 0$ (sum over empty domain). We are interested in a recurrence for $H(x-1)$.

$$\begin{array}{ll}
 & H(x-1) \\
= & \{ \text{ definition } H \} \\
 & \Sigma(a[k] \mid k : x-1 \leq k < n) \\
= & \{ \textbf{ assume } 0 < x \leq n; \text{ split } x \leq k \text{ or } k = x-1 \ \} \\
 & \Sigma(a[j] \mid j : x \leq k < n) \ + \ a[x-1] \\
= & \{ \text{ definition } H \} \\
 & H(x) \ + \ a[x-1]
\end{array}$$

We now introduce the invariant $J : \; s = F(x) \ \wedge \ g = H(x) \ \wedge \ h = H(x) \ \wedge \ 0 \leq x \leq n$.
Clearly, we choose the guard $B : \; x \neq 0$, such that $J \ \wedge \ \neg B \Rightarrow s = F(0) \equiv Q$.
For the variant function we choose $\mathsf{vf} = x \in \mathbb{Z}$. Clearly $J \Rightarrow \mathsf{vf} = x \geq 0$.

Initialization of the invariant is easy:

$\{$ **true** $\}$
  (* base cases recurrences; $n \in \mathbb{N}$ *)
$\{ 0 = F(n) \wedge 0 = G(n) \wedge 0 = H(n) \wedge 0 \leq n \leq n \}$.
$s := 0;\ g := 0;\ h := 0;\ x := n;$
$\{J :\ s = F(x) \wedge g = G(x) \wedge h = H(x) \wedge 0 \leq x \leq n \}$

We now turn to the derivation of the body of the while-loop.

$\{J \wedge B \wedge \mathsf{vf} = V\}$
  (* definitions J, B, and vf *)
$\{s = F(x) \wedge g = G(x) \wedge h = H(x) \wedge 0 < x = V \leq n\}$
  (* $0 < x \leq n$; use recurrence $H(x-1)$ *)
$\{s = F(x) \wedge g = G(x) \wedge h + a[x-1] = H(x-1) \wedge 0 < x = V \leq n\}$
$h := h + a[x-1];$
$\{s = F(x) \wedge g = G(x) \wedge h = H(x-1) \wedge 0 < x = V \leq n\}$
  (* $0 < x \leq n$; recurrence $G(x-1) = G(x) + a[x-1] \cdot H(x-1)$; substitution *)
$\{s = F(x) \wedge g + a[x-1] \cdot h = G(x-1) \wedge h = H(x-1) \wedge 0 < x = V \leq n\}$
$g := g + a[x-1] * h;$
$\{s = F(x) \wedge g = G(x-1) \wedge h = H(x-1) \wedge 0 < x = V \leq n\}$
  (* $0 < x \leq n$; recurrence $F(x-1) = F(x) + G(x-1)$; substitution *)
$\{s + g = F(x-1) \wedge g = G(x-1) \wedge h = H(x-1) \wedge 0 < x = V \leq n\}$
$s := s + g;$
$\{s = F(x-1) \wedge g = G(x-1) \wedge h = H(x-1) \wedge 0 < x = V \leq n\}$
  (* prepare $x := x - 1$; calculus *)
$\{s = F(x-1) \wedge g = G(x-1) \wedge h = H(x-1) \wedge 0 \leq x-1 \leq n \wedge x-1 < V\}$
$x := x - 1;$
$\{J \wedge \mathsf{vf} < V :\ s = F(x) \wedge g = G(x) \wedge h = H(x) \wedge 0 \leq x \leq n \wedge x < V\}$

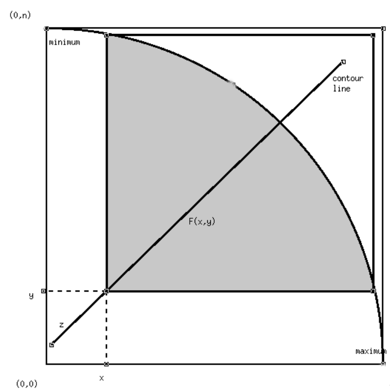
We completed the proof. We found the following program fragment:

const $n : \mathbb{N}$, $a :$ **array** $[0..n)$ **of** $\mathbb{Z}$;
var $s,\ g,\ h,\ x : \mathbb{Z}$;
  $\{ P :$ **true** $\}$
  $s := 0;$
  $g := 0;$
  $h := 0;$
  $x := n;$
    $\{J :\ s = F(x) \wedge g = G(x) \wedge h = H(x) \wedge 0 \leq x \leq n \}$
      (* $\mathsf{vf} = x$ *)
  while $x \neq 0$ **do**
    $h := h + a[x-1];$
    $g := g + a[x-1] * h;$
    $s := s + g;$
    $x := x - 1;$
  end;
    $\{Q :\ z = F(0)\}$

Problem 3 (40 pt). Given is a two-dimensional array a that is *ascending* in its first argument and *decreasing* in its second argument. Consider the following specification:

$$
\begin{array}{l}
\textbf{const } n,\ w : \mathbb{N}, \quad a: \ \textbf{array } [0..n) \ \textbf{ of } \mathbb{N}; \\
\quad \textbf{var } z : \mathbb{N}; \\
\qquad \{P: \ Z = \#\{(i,j) \mid i,j : 0 \le i \ \wedge \ 0 \le j \ \wedge \ i^2 + j^2 \le n^2 \ \wedge \ a[i,j] = w\} \ \} \\
\quad U \\
\qquad \{Q: \ Z = z\}
\end{array}
$$

(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.

Answer: We define $F(x, y) = \#\{(i, j) \mid i, j : x \le i \ \wedge \ y \le j \ \wedge \ i^2 + j^2 \le n^2 \ \wedge \ a[i, j] = w\}$.
It is clear that $x^2 + y^2 > n^2 \Rightarrow F(x, y) = 0$. To reduce the size of the shaded area (see sketch), we need to increment x or increment y. We first have a look at an increment of x:

$\quad F(x, y)$
$=$ { definition F}
$\quad \#\{(i, j) \mid i, j : x \le i \ \wedge \ y \le j \ \wedge \ i^2 + j^2 \le n^2 \ \wedge \ a[i, j] = w\}$
$=$ { **assume** $x^2 + y^2 \le n$; so domain non-empty; split $i = x$ or $x + 1 \le i$ }
$\quad \#\{(i, j) \mid i, j : x + 1 \le i \ \wedge \ y \le j \ \wedge \ i^2 + j^2 \le n \ \wedge \ a[i, j] = w\} +$
$\quad \#\{j \mid j : y \le j \ \wedge \ x^2 + j^2 \le n^2 \ \wedge \ a[x, j] = w\}$
$=$ { definition F }
$\quad F(x + 1, y) \ + \ \#\{j \mid j : y \le j \ \wedge \ x^2 + j^2 \le n^2 \ \wedge \ a[x, j] = w\}$
$=$ { $a[x, j]$ is decreasing in j; $a[x, y]$ is maximal; **assume** $a[x, y] \le w$; then $a[x, j] < w$ for $j > y$ }
$\quad F(x + 1, y) + \mathsf{ord}(a[x, y] = w)$

Next we investigate an increment of y:

$\quad F(x, y)$
$=$ { definition F}
$\quad \#\{(i, j) \mid i, j : x \le i \ \wedge \ y \le j \ \wedge \ i^2 + j^2 < n^2 \ \wedge \ a[i, j] = w\}$
$=$ { **assume** $x^2 + y^2 \le n$; so domain non-empty; split $j = y$ or $y + 1 \le j$ }
$\quad \#\{(i, j) \mid i, j : x \le i \ \wedge \ y + 1 \le j \ \wedge \ i^2 + j^2 < n^2 \ \wedge \ a[i, j] = w\} +$
$\quad \#\{i \mid i : x \le i \ \wedge \ i^2 + y^2 < n^2 \ \wedge \ a[i, y] = w\}$
$=$ { definition F}
$\quad F(x, y + 1) \ + \ \#\{i \mid i : x \le i \ \wedge \ i^2 + y^2 < n^2 \ \wedge \ a[i, y] = w\}$
$=$ { $a[i, y]$ is ascending in i; $a[x, y]$ is minimal; **assume** $a[x, y] > w$; then $a[i, y] > w$ for $i \ge x$ }
$\quad F(x, y + 1)$

In conclusion, we found the following recurrence relation for $F(x, y)$:

$$\begin{array}{rcl} x^2 + y^2 > n & \Rightarrow & F(x, y) = 0 \\ x^2 + y^2 \le n^2 \ \wedge \ a[x, y] \le w & \Rightarrow & F(x, y) = F(x + 1, y) + \mathsf{ord}(a[x, y] = w) \\ x^2 + y^2 \le n^2 \ \wedge \ a[x, y] > w & \Rightarrow & F(x, y) = F(x, y + 1) \end{array}$$

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

Answer: The precondition can be rewritten as $P: \ Z = F(0, 0)$. We introduce the variables $x, y : \mathbb{N}$, the invariant, guard, and variant function:

$$\begin{array}{rcl} J & : & Z = z + F(x, y) \\ B & : & x^2 + y^2 \le n^2 \\ \mathsf{vf} & = & n^2 - x^2 - y^2 \in \mathbb{Z} \end{array}$$

Clearly, $J \ \wedge \ \neg B \Rightarrow Z = z$. It is also clear that $B \Rightarrow \mathsf{vf} \ge 0$. The invariant is easy to initialize:

$\{P: \ Z = F(0, 0) \ \}$
  (∗ calculus ∗)
$\{ \ Z = 0 + F(0, 0) \ \}$.
$z := 0; \ x := 0; \ y := 0;$
$\{J: \ Z = z + F(x, y) \ \}$

We now turn to the derivation of the body of the while-loop.

$\{J \ \wedge \ B \ \wedge \ \mathsf{vf} = V\}$
  (∗ definitions J, B, and vf ∗)
$\{Z = z + F(x, y) \ \wedge \ x^2 + y^2 \le n^2 \ \wedge \ n^2 - x^2 - y^2 = V\}$
if $a[x, y] \le w$ **then**
  $\{a[x, y] \le w \ \wedge \ Z = z + F(x, y) \ \wedge \ x^2 + y^2 \le n^2 \ \wedge \ n^2 - x^2 - y^2 = V\}$
    (∗ recurrence $x^2 + y^2 \le n^2 \ \wedge \ [a, y] \le w \Rightarrow F(x, y) = F(x + 1, y) + \mathsf{ord}(a[x, y] = w)$ ∗)
  $\{Z = z + \mathsf{ord}(a[x, y] = w) + F(x, y) \ \wedge \ n^2 - x^2 - y^2 = V\}$
 $z := z + \mathsf{ord}(a[x, y] = w);$
  $\{Z = z + F(x, y) \ \wedge \ n^2 - x^2 - y^2 = V\}$
    (∗ prepare $x := x + 1$; note that $x \ge 0$, since $x \in \mathbb{N}$ ∗)
  $\{Z = z + F(x, y) \ \wedge \ n^2 - (x + 1)^2 - y^2 = V\}$
 $x := x + 1;$
  $\{Z = z + F(x, y) \ \wedge \ n^2 - x^2 - y^2 < V\}$
else
  $\{a[x, y] > w \ \wedge \ Z = z + F(x, y) \ \wedge \ x^2 + y^2 \le n^2 \ \wedge \ n^2 - x^2 - y^2 = V\}$
    (∗ recurrence $x^2 + y^2 \le n^2 \ \wedge \ [a, y] > w \Rightarrow F(x, y) = F(x, y + 1)$ ∗)
  $\{Z = z + F(x, y + 1) \ \wedge \ \ \wedge \ n^2 - x^2 - y^2 = V\}$
    (∗ prepare $y := y + 1$; note that $y \ge 0$, since $y \in \mathbb{N}$ ∗)
  $\{Z = z + F(x, y) \ \wedge \ n^2 - x^2 - (y + 1)^2 < V\}$
 $y := y + 1;$
  $\{Z = z + F(x, y) \ \wedge \ n^2 - x^2 - y^2 < V\}$
end; (∗ collect branches ∗)
$\{J \ \wedge \ \mathsf{vf} < V: \ Z = z + F(x, y) \ \wedge \ n^2 - x^2 - y^2 < V\}$

We completed the proof. We found the following program fragment:

const $n,\ w : \mathbb{N}, \quad a:$ **array** $[0..n)$ **of** $\mathbb{N}$;
var $x,\ y,\ z : \mathbb{N}$;
  $\{P:\ Z = \#\{(i,j) \mid i,j : 0 \le i \ \wedge\ 0 \le j \ \wedge\ i^2 + j^2 \le n^2 \ \wedge\ a[i,j] = w\}\ \}$
$x := 0;$
$y := 0;$
$z := 0;$
  $\{J:\ Z = z + \#\{(i,j) \mid i,j : x \le i \ \wedge\ y \le j \ \wedge\ i^2 + j^2 \le n^2 \ \wedge\ a[i,j] = w\}\ \}$
    $(*\ \mathsf{vf} = n^2 - x^2 - y^2\ *)$
while $x * x + y * y \le n * n$ **do**
  if $a[x,y] \le w$ **then**
    $z := z + \mathsf{ord}(a[x,y] = w);$
    $x := x + 1;$
  else
    $y := y + 1;$
  end;
end;
  $\{Q:\ Z = z\}$