Uitwerking Programmacorrectheid, 26 april 2007

Tijdsduur 3 uur. Gesloten boek.

Opgave 1 (12 %). Gegeven is een functie $g : \mathbb{Z} \to \mathbb{Z}$ en getallen $n, w \in \mathbb{N}$. Gegeven is dat er getallen $k \in \mathbb{N}$ bestaan waarvoor $g(k) > w$.

Specificeer een commando T ter bepaling van het kleinste getal $k \in \mathbb{N}$ waarvoor $g(k) > w$. Geef bij voorkeur één die biregulier is (dwz. zowel preregulier als postregulier).

Uitwerking. Een bireguliere specificatie:

$$
\begin{array}{l}
\textbf{const } w, n : \mathbb{N} \ ; \\
\textbf{var } k : \mathbb{Z} \ ; \\
\quad \{ \ P : \ M = \mathtt{Min}\,\{ i \in \mathbb{N} \mid g(i) > w \} \ \wedge \ M < \infty \} \\
T \\
\quad \{ \ Q : \ k = M \} \ \ .
\end{array}
$$

De declaraties van w en de variabele (bv. k) zijn nodig (n is overbodig).

Opgave 2 (48 %). Gegeven is een functie $h : \mathbb{Z}^2 \to \mathbb{Z}$ die zwak stijgend is in beide argumenten. Bepaal een commando T dat voldoet aan

$$
\begin{array}{l}
\textbf{const } m : \mathbb{N}, \ c : \mathbb{Z} \ ; \\
\textbf{var } z : \mathbb{Z} \ ; \\
\quad \{ \ P : \ Z = \#\{ (i,j) \mid 0 \le j \le i < m \ \wedge \ h(i,j) > c \} \ \} \\
T \\
\quad \{ \ Q : \ Z = z \ \} \ \ .
\end{array}
$$

(a: 24 %) Maak een schets van het te onderzoeken gebied. Geef aan hoe de hoogtelijn loopt, en waar je de resterende rechthoek legt. Definieer een geschikte functie en bepaal recurrente betrekkingen daarvoor, zodanig dat Z daarmee berekend kan worden.
(b: 24 %) Bepaal een commando S dat aan bovenstaande specificatie voldoet. Voer hiertoe het volledige stappenplan uit. Bij de stappen 1 en 3 hoef je geen lineaire bewijzen te geven, je moet daar alleen aangeven wat de bewijsverplichtingen zijn en waarom daaraan voldaan wordt.

Uitwerking. (a) Het zoekgebied is de driehoek tussen de horizontale x-as, de verticale lijn $x = m$ en de diagonaal $x = y$. De hoogtelijn van h loopt van zuidoost naar noordwest (of omgekeerd). Maak nu zelf de schets. Je zou de diagonaal $x = y$ ook als een hoogtelijn kunnen opvatten, maar die hoeft niet gezocht te worden. We volgen daarom in het te ontwikkelen commando de hoogtelijn van h.

Omdat we binnen het zoekgebied willen beginnen, beginnen we in het zuidoosten, dus in het punt $(m, 0)$. De resterende rechthoek ligt dus ten noordwesten van het inspectiepunt. Het punt (i, j) ligt ten noordwesten van (x, y) als $i < x$ en $j > y$. Het ligt onder of op de diagonaal als $j \le i$. Om de goede vorm van P te krijgen, definiëren we daarom:

$$F(x,y) = \#\{ (i,j) \mid y \le j \le i < x \ \wedge \ h(i,j) > c \} \ .$$

Merk op, dat we hier niet hoeven te eisen dat $0 \le y$ of $x \le m$. Desgewenst kun je dat in deel (b) aan de invariant toevoegen.

De preconditie wordt $P : Z = F(m, 0)$. Wegens leeg domein geldt:

(Fin) $\qquad x \le y \quad \Rightarrow \quad F(x,y) = 0 \ .$

We gaan nu op zoek naar recurrente betrekkingen voor $F(x, y)$, waarbij we x willen verlagen en/of y willen verhogen.

$$
\begin{array}{ll}
 & F(x,y) \\
= & \{ \text{ definitie } F \ \} \\
 & \#\{(i,j) \mid y \le j \le i < x \ \wedge \ h(i,j) > c\} \\
= & \{ \ i < x-1 \text{ of } i = x-1\text{; splitsen } \} \\
 & \#\{(i,j) \mid y \le j \le i < x-1 \ \wedge \ h(i,j) > c\} \\
 & + \#\{j \mid y \le j \le x-1 \ \wedge \ h(x-1,j) > c\} \\
= & \{ \text{ herken definitie } F \ \} \\
 & F(x-1,y) + \#\{j \mid y \le j \le x-1 \ \wedge \ h(x-1,j) > c\} \\
= & \{ \text{ Stel } h(x-1,y) > c. \text{ Omdat } h \text{ zwak stijgend is, is dan} \\
 & \quad \text{ook } h(x-1,j) > c \text{ voor } j \ge y \ \} \\
 & F(x-1,y) + \#\{j \mid y \le j \le x-1\} \\
= & \{ \text{ Stel } y < x. \text{ Goed tellen. } \} \\
 & F(x-1,y) + x - y \ .
\end{array}
$$

Voor het verhogen van y, gaan we na dat:

$$
\begin{array}{ll}
 & F(x,y) \\
= & \{ \text{ definitie } F \ \} \\
 & \#\{(i,j) \mid y \le j \le i < x \ \wedge \ h(i,j) > c\} \\
= & \{ \ j = y \text{ of } y+1 \le j\text{; splitsen, herken definitie } F \ \} \\
 & F(x,y+1) + \#\{i \mid y \le i < x \ \wedge \ h(i,y) > c\} \\
= & \{ \text{ Stel } h(x-1,y) \le c. \text{ Omdat } h \text{ zwak stijgend is, is dan} \\
 & \quad \text{ook } h(i,y) \le c \text{ voor } i < x \ \} \\
 & F(x,y+1) + \#\{i \mid \mathit{false}\} \\
= & \{ \text{ Tellen. } \} \\
 & F(x,y+1) \ .
\end{array}
$$

We hebben aldus de recurrente betrekkingen

(RBx) $\quad y < x \ \wedge \ h(x-1,y) > c \quad \Rightarrow \quad F(x,y) = F(x-1,y) + x - y \ ,$
(RBy) $\quad h(x-1,y) \le c \quad \Rightarrow \quad F(x,y) = F(x,y+1) \ .$

(b) Stap 1. We kiezen J en B volgens

$J: \quad Z = z + F(x,y) \ ,$
$B: \quad y < x \ .$

De formule (Fin) impliceert nu $J \wedge \neg B \ \Rightarrow \ Q : Z = z$.

Stap 2. Initialisatie.

$$
\begin{array}{l}
\quad \{ \ P: \ Z = F(m,0)\} \\
\quad \{ \ Z = 0 + F(m,0)\} \\
z := 0 \ ; \ x := m \ ; \ y := 0 \ ; \\
\quad \{ \ J: \ Z = z + F(x,y)\} \ \ .
\end{array}
$$

Stap 3. We kiezen $\mathit{vf} = x - y$. Wegens $B: y < x$ geldt $J \wedge B \ \Rightarrow \ \mathit{vf} \ge 0$.

Stap 4.

$$
\begin{array}{l}
\quad \{ \ J \wedge B \ \wedge \ \mathrm{vf} = V\} \\
\quad \{ \ Z = z + F(x,y) \ \wedge \ y < x \ \wedge \ x - y = V\} \\
\textbf{if } h(x-1,y) > c \textbf{ then} \\
\qquad \{ \ h(x-1,y) > c \ \wedge \ Z = z + F(x,y) \ \wedge \ y < x \ \wedge \ x - y = V\} \\
\qquad \quad (* \ \text{(RBx) en rekenen} \ *) \\
\qquad \{ \ Z = z + x - y + F(x-1,y) \ \wedge \ x - 1 - y < V\} \\
\quad z := z + x - y \ ; \\
\qquad \{ \ Z = z + F(x-1,y) \ \wedge \ x - 1 - y < V\} \\
\quad x := x - 1 \ ; \\
\qquad \{ \ J \wedge \mathrm{vf} < V: \quad Z = z + F(x,y) \ \wedge \ x - y < V\}
\end{array}
$$

$$
\begin{array}{l}
\textbf{else} \\
\qquad \{\ h(x-1,y) \le c\ \wedge\ Z = z + F(x,y)\ \wedge\ y < x\ \wedge\ x - y = V\} \\
\qquad\quad (*\ \text{(RBy) en rekenen}\ *) \\
\qquad \{\ Z = z + F(x, y+1)\ \wedge\ x - (y+1) < V\} \\
\quad y := y + 1\ ; \\
\qquad \{\ J \wedge \mathrm{vf} < V :\quad Z = z + F(x,y)\ \wedge\ x - y < V\} \\
\textbf{end} \quad (*\ \text{verzamelen}\ *) \\
\quad \{\ J \wedge \mathrm{vf} < V\}\ \ .
\end{array}
$$

Stap 5. Samenvatting.

$$
\begin{array}{l}
\quad \{\ P :\ Z = F(m,0)\} \\
z := 0\ ;\ x := m\ ;\ y := 0\ ; \\
\quad \{\ J :\ Z = z + F(x,y)\} \\
\textbf{while}\ y < x\ \textbf{do} \quad (*\ \mathrm{vf} : x - y\ *) \\
\quad \textbf{if}\ h(x-1,y) > c\ \textbf{then} \\
\qquad z := z + x - y\ ; \\
\qquad x := x - 1\ ; \\
\quad \textbf{else} \\
\qquad y := y + 1\ ; \\
\quad \textbf{end} \\
\textbf{end} \\
\quad \{\ Q : Z = z\}\ \ .
\end{array}
$$

Opgave 3 (40 %). Bepaal een commando T dat voldoet aan

$$
\begin{array}{l}
\textbf{const}\ n : \mathbb{N},\ a, b : \textbf{array}[0\ .\ .\ n)\ \textbf{of}\ \mathbb{Z}\ ; \\
\textbf{var}\ x : \mathbb{Z}_\infty\ ; \\
\quad \{\ \mathit{true}\ \} \\
T \\
\quad \{\ Q :\ x = \mathtt{Max}\,(a[i] + b[j] \mid i, j : 0 \le i \le j < n)\ \}
\end{array}
$$

(a: 20 %) Bepaal recurrente betrekkingen voor

$$A(k) = \mathtt{Max}\,(a[i] + b[j] \mid i, j : 0 \le i \le j < k)\ ,$$

en voor eventuele andere nuttige hulpfuncties, zodanig dat $A(n)$ daarmee berekend kan worden.
(b: 20 %) Bepaal een commando T dat aan bovenstaande specificatie voldoet. Voer hiertoe het volledige stappenplan uit. Bij de stappen 1 en 3 hoef je geen lineaire bewijzen te geven, je moet daar alleen aangeven wat de bewijsverplichtingen zijn en waarom daaraan voldaan wordt.

Uitwerking. Vergelijk opgave 7.14 uit de syllabus. Er geldt $A(0) = -\infty$ wegens leeg domain. We vinden verder:

$$
\begin{array}{cl}
 & A(k) \\
= & \{\ \text{definitie}\ \} \\
 & \mathtt{Max}\,(a[i] + b[j] \mid i, j : 0 \le i \le j < k) \\
= & \{\ \text{Stel } k > 0.\ \text{Dan } j < k-1 \text{ of } j = k-1;\ \text{splitsen; herken } A\ \} \\
 & A(k-1)\ \textbf{max}\ \mathtt{Max}\,(a[i] + b[k-1] \mid i : 0 \le i \le k-1) \\
= & \{\ \text{distributie van optelling over Max}\ \} \\
 & A(k-1)\ \textbf{max}\ (\mathtt{Max}\,(a[i] \mid i : 0 \le i \le k-1) + b[k-1]) \\
= & \{\ \text{rekenen, definitie } C \text{ hieronder}\ \} \\
 & A(k-1)\ \textbf{max}\ (C(k) + b[k-1])\ ,
\end{array}
$$

waarbij

$$C(k) = \mathtt{Max}\,(a[i] \mid i : 0 \le i < k)\ .$$

Hiervoor geldt $C(0) = -\infty$ wegens leeg domein. We vinden verder

$$\begin{array}{ll} & C(k) :\ \mathtt{Max}\,(a[i] \mid i : 0 \le i < k) \\ = & \{\ \text{Stel } k > 0.\ \text{Dan } i < k-1 \text{ of } i = k-1 \ge 0;\ \text{splitsen}\ \} \\ & C(k-1)\ \mathbf{max}\ a[k-1]\ . \end{array}$$

Dit bewijst

$$\begin{array}{lll} k > 0 & \Rightarrow & A(k) = A(k-1)\ \mathbf{max}\ (C(k) + b[k-1]) \\ & \wedge & C(k) = C(k-1)\ \mathbf{max}\ a[k-1]\ . \end{array}$$

Stap 1. We zien nu dat $Q : z = A(n)$. We gebruiken hulpvariabelen $y, k : \mathbb{Z}$ met de invariant en guard volgens

$$\begin{array}{ll} J: & x = A(k)\ \wedge\ y = C(k)\ \wedge\ 0 \le k \le n\ , \\ B: & k \ne n\ . \end{array}$$

Het is duidelijk dat $J \wedge \neg B$ impliceert dat $Q : x = A(n)$.
Stap 2. Initialisatie.

$$\begin{array}{l} \quad \{\ \mathit{true}\ \} \\ \quad \{\ -\infty = A(0)\ \wedge\ -\infty = C(0)\ \wedge\ 0 \le 0 \le n\} \\ x := -\infty\ ;\ y := -\infty\ ;\ k := 0\ ; \\ \quad \{\ J :\quad x = A(k)\ \wedge\ y = C(k)\ \wedge\ 0 \le k \le n\}\ \ . \end{array}$$

Stap 3. We nemen $\mathit{vf} = n - k$. Omdat J het conjunct $k \le n$ bevat, geldt $J\ \wedge\ B\ \Rightarrow\ \mathit{vf} \ge 0$.
Stap 4. De body van de lus:

$$\begin{array}{l} \quad \{\ J \wedge B \wedge \mathrm{vf} = V\} \\ \quad \{\ x = A(k)\ \wedge\ y = C(k)\ \wedge\ 0 \le k \le n\ \wedge\ k \ne n\ \wedge\ n - k = V\} \\ \quad\ (*\ C(k+1) = C(k)\ \mathbf{max}\ a[k]\ *) \\ \quad \{\ x = A(k)\ \wedge\ y\ \mathbf{max}\ a[k] = C(k+1)\ \wedge\ 0 \le k < n\ \wedge\ n - k = V\} \\ y := y\ \mathbf{max}\ a[k]\ ; \\ \quad \{\ x = A(k)\ \wedge\ y = C(k+1)\ \wedge\ 0 \le k < n\ \wedge\ n - k = V\} \\ \quad\ (*\ A(k+1) = A(k)\ \mathbf{max}\ (C(k+1) + b[k])\ *) \\ \quad \{\ x\ \mathbf{max}\ (y + b[k]) = A(k+1)\ \wedge\ y = C(k+1) \\ \quad\quad \wedge\ 0 \le k+1 \le n\ \wedge\ n - (k+1) < V\} \\ x := x\ \mathbf{max}\ (y + b[k])\ ; \\ \quad \{\ x = A(k+1)\ \wedge\ y = C(k+1)\ \wedge\ 0 \le k+1 \le n\ \wedge\ n - (k+1) < V\} \\ k := k + 1\ ; \\ \quad \{\ J\ \wedge\ \mathrm{vf} < V :\quad x = A(k)\ \wedge\ y = C(k)\ \wedge\ 0 \le k \le n\ \wedge\ n - k < V\}\ \ . \end{array}$$

Stap 5. Samenvatting.

$$\begin{array}{l} \quad \{\ \mathit{true}\ \} \\ x := -\infty\ ;\ y := -\infty\ ;\ k := 0\ ; \\ \quad \{\ J :\quad x = A(k)\ \wedge\ y = C(k)\ \wedge\ 0 \le k \le n\} \\ \mathbf{while}\ k \ne n\ \mathbf{do}\quad (*\ \mathrm{vf} : n - k\ *) \\ \quad y := y\ \mathbf{max}\ a[k]\ ; \\ \quad x := x\ \mathbf{max}\ (y + b[k])\ ; \\ \quad k := k + 1\ ; \\ \mathbf{end} \\ \quad \{\ Q :\quad x = A(n)\}\ \ . \end{array}$$

In dit commando wordt de body n keer uitgevoerd. Het is dus veel efficienter dan programma's die alle paren (i, j) met $0 \le i \le j < n$ langs gaan (er zijn $\frac{1}{2}n(n+1)$ paren).