Uitwerking Programmacorrectheid, 21 april 2008

Tijdsduur 3 uur. Gesloten boek.

Geef in alle gevallen volledige en volledig correcte annotaties. Behandel elke herhaling met het volledige stappenplan.

Opgave 1 (18 %). Bepaal een geannoteerd commando S dat voldoet aan

$$
\begin{array}{l}
\textbf{var } i,j,k:\mathbb{Z} \\
\quad \{\ P:\ (X \le i \ \vee\ X \le j \ \vee\ X \le k) \ \wedge\ i \le Y \ \wedge\ j \le Y \ \wedge\ k \le Y \\
\qquad\quad \wedge\ i+j+k = Z \ \} \\
S \\
\quad \{\ Q: X \le i \le Y \ \wedge\ j = Z \ \} \ .
\end{array}
$$

Aanwijzing. Je mag de operatoren **min** en **max** gebruiken, desgewenst herhaaldelijk. Eén van de twee komt hier goed van pas.

Uitwerking.

$$
\begin{array}{l}
\quad \{\ P:\ (X \le i \ \vee\ X \le j \ \vee\ X \le k) \ \wedge\ i \le Y \ \wedge\ j \le Y \ \wedge\ k \le Y \\
\qquad\quad \wedge\ i+j+k = Z \ \} \\
\qquad (*\ \ X \text{ is } \le \text{ tenminste een van de drie en dus } \le \text{ de grootste;} \\
\qquad\quad \text{de grootste van de drie is ook } \le Y \ \ *) \\
\quad \{\ X \le \max\{i,j,k\} \le Y \ \wedge\ i+j+k = Z \ \} \\
\textbf{var } m:\mathbb{Z} \\
m := \max\{i,j,k\} \ ; \ // \text{ of } m := i \ \textbf{max} \ j \ \textbf{max} \ k \ ; \\
\quad \{\ X \le m \le Y \ \wedge\ i+j+k = Z \ \} \\
j := i+j+k \ ; \\
\quad \{\ X \le m \le Y \ \wedge\ j = Z \ \} \\
i := m \ ; \\
\quad \{\ Q: X \le i \le Y \ \wedge\ j = Z \ \} \ .
\end{array}
$$

Opgave 2 (34 %). Gegeven zijn twee arrays volgens

$$\textbf{const } n:\mathbb{N} \ ; \quad a,b : \textbf{array } [0\ .\ .\ n) \textbf{ of } \mathbb{R} \ .$$

Bepaal een commando S ter berekening van

$$\Sigma(a[i]\cdot b[j] \mid i,j:\ 0 \le j \le i < n) \ .$$

De tijdscomplexiteit van commando S dient $\mathcal{O}(n)$ te zijn.
Geef eerst een formele specificatie.

Uitwerking. Stel $A(k) = \Sigma(a[i]\cdot b[j] \mid i,j:\ 0 \le j \le i < k)$. Er geldt $A(0) = 0$ wegens leeg domein. Voor $k \ge 0$ vinden we:

$$
\begin{array}{cl}
 & A(k+1) \\
= & \{ \text{ definitie } A \text{ met } k+1 \text{ ipv } k \ \} \\
 & \Sigma(a[i]\cdot b[j] \mid i,j:\ 0 \le j \le i < k+1) \\
= & \{ \text{ afsplitsen } i<k \text{ en } i=k\text{; gebruik } k \ge 0 \ \} \\
 & A(k) + \Sigma(a[k]\cdot b[j] \mid j:\ 0 \le j \le k) \\
= & \{ \text{ distributie en definitie } C(k+1) \text{ hieronder } \} \\
 & A(k) + a[k]\cdot C(k+1) \ ,
\end{array}
$$

waarbij $C(k) = \Sigma(b[j] \mid j:\ 0 \le j < k)$. Er geldt weer $C(0) = 0$ en voor $k \ge 0$ geldt analoog dat $C(k+1) = C(k) + b[k]$.

Waardering: 20 punten voor correcte recurrente betrekkingen inclusief beide basisgevallen; 14 punten voor correct stappenplan als er twee functies met recurrente betrekkingen van de goede structuur zijn.

We gebruiken de formele specificatie

$$\begin{array}{l} \quad \{\ P:\ true\ \} \\ \textbf{var}\ x:\mathbb{R} \\ S \\ \quad \{\ Q:\ x=A(n)\ \}\ \ . \end{array}$$

Stap 1. We gebruiken hulpvariabelen $k:\mathbb{Z}$ en $y:\mathbb{R}$, en kiezen:

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

Bewijs:

$$\begin{array}{ll} & J\ \wedge\ \neg B \\ \Rightarrow & \{\ \text{definities } J \text{ en } B\text{, weglaten conjuncten}\ \} \\ & x=A(k)\ \wedge\ k=n \\ \Rightarrow & \{\ \text{invullen}\ \} \\ & Q:\quad x=A(n)\ . \end{array}$$

Stap 2. Initialisatie:

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

Stap 3. We kiezen $vf=n-k$. De onderbegrenzing $vf\ge 0$ volgt uit het conjunct $k\le n$ van de invariant.

Stap 4. Body.

$$\begin{array}{l} \quad \{\ J\ \wedge\ B\ \wedge\ \mathrm{vf}=V\ \} \\ \quad \{\ 0\le k\le n\ \wedge\ x=A(k)\ \wedge\ y=C(k)\ \wedge\ k\ne n\ \wedge\ n-k=V\ \} \\ \quad \{\ 0\le k< n\ \wedge\ x=A(k)\ \wedge\ y=C(k)\ \wedge\ n-k=V\ \} \\ \qquad (*\ \text{de recurrente betrekking voor } C(k+1)\ *) \\ \quad \{\ 0\le k< n\ \wedge\ x=A(k)\ \wedge\ y+b[k]=C(k+1)\ \wedge\ n-k=V\ \} \\ y:=y+b[k]\ ; \\ \quad \{\ 0\le k< n\ \wedge\ x=A(k)\ \wedge\ y=C(k+1)\ \wedge\ n-k=V\ \} \\ \qquad (*\ \text{de recurrente betrekking voor } A(k+1)\text{; rekenen }\ *) \\ \quad \{\ 0\le k+1\le n\ \wedge\ x+a[k]\cdot y=A(k+1)\ \wedge\ y=C(k+1) \\ \qquad\quad \wedge\ n-(k+1)<V\ \} \\ x:=x+a[k]\cdot y\ ; \\ \quad \{\ 0\le k+1\le n\ \wedge\ x=A(k+1)\ \wedge\ y=C(k+1)\ \wedge\ n-(k+1)<V\ \} \\ k:=k+1\ ; \\ \quad \{\ J\ \wedge\ \mathrm{vf}<V:\quad 0\le k\le n\ \wedge\ x=A(k)\ \wedge\ y=C(k)\ \wedge\ n-k<V\ \}\ \ . \end{array}$$

Stap 5. Samenvatting.

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

Opgave 3 (48 %). Gegeven zijn constanten m, $c : \mathbb{Z}$, en een functie $h : \mathbb{Z}^2 \to \mathbb{Z}$ die zwak dalend is in zijn beide argumenten. Bepaal een commando S ter bepaling van het aantal paren (i, j) met $i \geq 0$ en $i^2 \leq j < m$ en $h(i, j) > c$.
(a: 6 %) Geef een formele specificatie voor commando S.
(b: 24 %) Maak een schets van het te onderzoeken gebied, rekening houdend met de gegeven ongelijkheden. Geef aan waar berg en dal liggen, hoe de hoogtelijn loopt, en waar je het resterende zoekgebied legt. Definieer een functie waar Z mee berekend kan worden. Bepaal recurrente betrekkingen voor deze functie.
(Je hebt geen vierkantswortels nodig.)
(c: 18 %) Bepaal een commando S dat aan bovenstaande specificatie voldoet.

Uitwerking. (a)

$$
\begin{array}{l}
\textbf{const } m, c : \mathbb{Z} \\
\quad \{\ P : Z = \#\{(i,j) \mid i,j :\ 0 \leq i \ \wedge\ i^2 \leq j < m \ \wedge\ h(i,j) > c\}\ \} \\
\textbf{var } z : \mathbb{Z} \\
S \\
\quad \{\ Q : Z = z\ \}\ \ .
\end{array}
$$

(b) Teken een dalparabool voor de vergelijking $i^2 = j$ met de top in de oorsprong, afgesneden ter hoogte $y = m$. Het gaat om het binnengebied van de afgesnede parabool, en dan rechts van de y-as. De berg ligt in de oorsprong. Naar het oosten en noorden toe wordt het lager. De hoogtelijn ligt NW-ZO. We leggen het resterend zoekgebied ten ZO van de testpositie en definiëren dus:

$$F(x, y) = \#\{(i, j) \mid i, j :\ x \leq i \ \wedge\ i^2 \leq j < y \ \wedge\ h(i, j) > c\}\ .$$

De preconditie is nu $P : Z = F(0, m)$. Er geldt $F(x, y) = 0$ als $y \leq x^2$ wegens leeg domein. Immers: $x \leq i \ \wedge\ i^2 \leq j < y$ impliceert $x^2 \leq j < y$ en dus $x^2 < y$.

We maken het zoekgebied kleiner door x te verhogen (oostwaartse stap) of y te verlagen (zuidwaartse stap).

$$
\begin{array}{cl}
 & F(x,y) \\
= & \{\ \text{definitie } F \text{ en afsplitsen } i = x \text{ dan wel } x+1 \leq i\ \} \\
 & F(x+1,y) + \#\{j \mid x^2 \leq j < y \ \wedge\ h(x,j) > c\} \\
= & \{\ h(x,j) \text{ is zwak dalend in } j;\ \textbf{stel } h(x,y-1) > c; \\
 & \quad \text{dan is } h(x,j) > c \text{ voor alle } j \text{ met } j < y\ \} \\
 & F(x+1,y) + \#\{j \mid x^2 \leq j < y\} \\
= & \{\ \textbf{stel } x^2 \leq y;\ \text{tellen}\ \} \\
 & F(x+1,y) + y - x^2\ .
\end{array}
$$

Dit bewijst

(RB1) $\qquad x^2 \leq y \ \wedge\ h(x, y-1) > c \quad \Rightarrow \quad F(x, y) = F(x+1, y) + y - x^2\ .$

De zuidwaartse stap gaat volgens:

$$
\begin{array}{cl}
 & F(x,y) \\
= & \{\ \text{definitie } F \text{ en afsplitsen } j = y-1 \text{ dan wel } j < y-1\ \} \\
 & F(x,y-1) + \#\{i \mid x \leq i \ \wedge\ i^2 \leq y-1 \ \wedge\ h(i,y-1) > c\} \\
= & \{\ h(i,y-1) \text{ is zwak dalend in } i;\ \textbf{stel } h(x,y-1) \leq c; \\
 & \quad \text{dan is } h(i,y-1) \leq c \text{ voor alle } i \text{ met } x \leq i\ ;\ \text{leeg domein}\ \} \\
 & F(x,y-1)\ .
\end{array}
$$

Dit bewijst

(RB2) $\qquad h(x, y-1) \leq c \quad \Rightarrow \quad F(x, y) = F(x, y-1)\ .$

Stap 1. We kiezen

$$J: \quad Z = F(x,y) + z \ ,$$
$$B: \quad x^2 < y \ .$$

Er geldt:

$$\begin{array}{ll} & J \ \wedge \ \neg B \\ \equiv & \{ \text{ definities } J,\ B, \text{ bepaling ontkenning } \} \\ & Z = F(x,y) + z \ \wedge \ y \le x^2 \\ \Rightarrow & \{ \ F(x,y) = 0, \text{ zie boven; rekenen } \} \\ & Q: \ Z = z \ . \end{array}$$

Stap 2. Initialisatie.

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

Stap 3. We kiezen (bv) $\mathrm{vf} = y - x$.

$$\begin{array}{ll} & J \wedge B \\ \Rightarrow & \{ \text{ definitie } B \text{ en rekenen } \} \\ & x \le x^2 < y \\ \Rightarrow & \{ \text{ rekenen } \} \\ & y - x \ge 0 \ . \end{array}$$

Stap 4. De body:

$$\begin{array}{l} \quad \{ \ J \wedge B \wedge \mathrm{vf} = V : \quad Z = F(x,y) + z \ \wedge \ x^2 < y \ \wedge \ y - x = V \ \} \\ \textbf{if} \ \ h(x, y-1) > c \ \ \textbf{then} \\ \qquad \{ \ h(x,y-1) > c \ \wedge \ Z = F(x,y) + z \ \wedge \ x^2 < y \ \wedge \ y - x = V \ \} \\ \qquad\quad (* \ \ (\mathrm{RB1}) \text{ en rekenen } \ *) \\ \qquad \{ \ Z = F(x+1, y) + y - x^2 + z \ \wedge \ y - (x+1) < V \ \} \\ \quad z := y - x^2 + z \ ; \\ \qquad \{ \ Z = F(x+1,y) + z \ \wedge \ y - (x+1) < V \ \} \\ \quad x := x + 1 \ ; \\ \qquad \{ \ J \ \wedge \ \mathrm{vf} < V : \quad Z = F(x,y) + z \ \wedge \ y - x < V \ \} \\ \textbf{else} \\ \qquad \{ \ h(x,y-1) \le c \ \wedge \ Z = F(x,y) + z \ \wedge \ x^2 < y \ \wedge \ y - x = V \ \} \\ \qquad\quad (* \ \ (\mathrm{RB2}) \text{ en rekenen } \ *) \\ \qquad \{ \ Z = F(x, y-1) + z \ \wedge \ (y-1) - x < V \ \} \\ \quad y := y - 1 \ ; \\ \qquad \{ \ J \ \wedge \ \mathrm{vf} < V : \quad Z = F(x,y) + z \ \wedge \ y - x < V \ \} \\ \textbf{end} \quad (* \ \text{verzamel de takken} \ *) \\ \quad \{ \ J \ \wedge \ \mathrm{vf} < V \} \ \ . \end{array}$$

Stap 5. Samenvatting.

$$\begin{array}{l} \quad \{ \ P : Z = F(0,m) \ \} \\ x := 0 \ ; \ y := m \ ; \ z := 0 \ ; \\ \quad \{ \ J: \ Z = F(x,y) + z \ \} \\ \textbf{while} \ \ x^2 < y \ \ \textbf{do} \quad (* \ \ \mathrm{vf} : y - x \ \ *) \\ \quad \textbf{if} \ \ h(x,y-1) > c \ \ \textbf{then} \\ \qquad z := y - x^2 + z \ ; \ x := x + 1 \ ; \\ \quad \textbf{else} \ \ y := y - 1 \ \ \textbf{end} \\ \textbf{end} \\ \quad \{ \ Q: \ Z = z \ \} \ \ . \end{array}$$

Slotopmerking. In de expressies voor de functies A en F uit opgaven 2 en 3 komen *gebonden* variabelen i en j voor. Die moeten *niet* als *programmavariabelen* gebruikt worden, want dan loopt de argumentatie zeker in het honderd.