Uitwerking Programmacorrectheid, 14 april 2009

Tijdsduur 3 uur. Gesloten boek.

Geef in alle gevallen volledig en correct geannoteerde commando's. Behandel elke herhaling met het volledige stappenplan. Geef bij de stappen 1 telkens een geannoteerd lineair bewijs. Bij de stappen 3 is het voldoende de bewijsverplichting te geven met een goed argument waarom hieraan voldaan wordt.

Opgave 1 (20 %). Bepaal een geannoteerd commando S dat voldoet aan

$$
\begin{array}{l}
\textbf{var } p, q : \mathbb{Z} \\
\quad \{ \ P: \ X \geq 0 \ \wedge \ (p = X + 3 \ \vee \ p = -X) \ \wedge \ p^2 + q = Y \ \} \\
S \\
\quad \{ \ Q: \ p = X \ \wedge \ p^2 + q = Y \ \} \ .
\end{array}
$$

Uitwerking.

$$
\begin{array}{l}
\quad \{ \ P: \ X \geq 0 \ \wedge \ (p = X + 3 \ \vee \ p = -X) \ \wedge \ p^2 + q = Y \ \} \\
\quad \{ \ (p - 3 = X \geq 0 \ \vee \ -p = X \geq 0) \ \wedge \ p^2 + q = Y \ \} \\
\textbf{if } p \geq 3 \ \textbf{ then} \\
\qquad \{ \ p \geq 3 \ \wedge \ (p - 3 = X \geq 0 \ \vee \ -p = X \geq 0) \ \wedge \ p^2 + q = Y \ \} \\
\qquad\quad (* \ \ p \geq 3 \text{ geeft } -p < 0 \text{, dus tweede disjunct vervalt } \ *) \\
\qquad \{ \ p - 3 = X \ \wedge \ p^2 + q = Y \ \} \\
\qquad \{ \ p - 3 = X \ \wedge \ (p - 3 + 3)^2 + q = Y \ \} \\
\quad p := p - 3 \\
\qquad \{ \ p = X \ \wedge \ (p + 3)^2 + q = Y \ \} \\
\qquad \{ \ p = X \ \wedge \ p^2 + 6 \cdot p + 9 + q = Y \ \} \\
\quad q := 6 \cdot p + 9 + q \\
\qquad \{ \ p = X \ \wedge \ p^2 + q = Y \ \} \\
\textbf{else} \\
\qquad \{ \ p < 3 \ \wedge \ (p - 3 = X \geq 0 \ \vee \ -p = X \geq 0) \ \wedge \ p^2 + q = Y \ \} \\
\qquad\quad (* \ \ p < 3 \text{ geeft } p - 3 < 0 \text{, dus eerste disjunct vervalt } \ *) \\
\qquad \{ \ -p = X \ \wedge \ (-p)^2 + q = Y \ \} \\
\quad p := -p \\
\qquad \{ \ Q: \ p = X \ \wedge \ p^2 + q = Y \ \} \\
\textbf{end} \quad (* \text{ verzamel de takken } *) \\
\quad \{ \ Q \ \} \ .
\end{array}
$$

Merk op, dat de preconditie impliceert dat $p \geq 3 \ \vee \ p \leq 0$. De guard $p \geq 3$ kan daarom ook vervangen worden door $p \geq 2$ of $p \geq 1$. De guards $p > 3$ en $p \geq 0$ zijn echter foutief.

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

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

De tijdscomplexiteit van commando S dient $\mathcal{O}(n)$ te zijn.
Bepaal eerst geschikte hulpfuncties en recurrente betrekkingen daarvoor.
Geef een formele specificatie voordat je met het stappenplan begint.

Uitwerking. Definieer

$$L(k) = \Sigma(a[i] \cdot b[j] \mid i, j : \ 0 \leq i < j < k) \ .$$

Er geldt $L(0) = 0$, omdat de som over een leeg domein 0 is. Verder is

$$\begin{array}{ll} & L(k+1) \\ = & \{ \text{ definitie } L(k); \text{ splitsen: } j < k \text{ of } j = k \ \} \\ & L(k) + \Sigma(a[i] \cdot b[k] \mid i : \ 0 \le i < k) \\ = & \{ \text{ distributie van } b[k]; \text{ definitie } E(k) \text{ hieronder } \} \\ & L(k) + E(k) \cdot b[k] \ , \end{array}$$

waarbij $E(k)$ gedefinieerd is door

$$E(k) = \Sigma(a[i] \mid i : \ 0 \le i < k) \ .$$

Weer geldt $E(k) = 0$ wegens leeg domein. Als $k \ge 0$ is geldt:

$$\begin{array}{ll} & E(k+1) \\ = & \{ \text{ definitie } E(k); \text{ splitsen: } i < k \text{ of } i = k; \text{ gebruik } k \ge 0 \ \} \\ & E(k) + a[k] \ . \end{array}$$

We hebben dus $L(0) = E(0) = 0$, en voor $k \ge 0$:

$$\begin{array}{l} L(k+1) = L(k) + E(k) \cdot b[k] \ , \\ E(k+1) = E(k) + a[k] \ . \end{array}$$

We kiezen de specificatie:

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

Stap 1. We kiezen hulpvariabelen $k : \mathbb{Z}$ en $y : \mathbb{R}$, en de invariant en guard volgens

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

Hiervoor geldt:

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

Stap 2. Initialisatie:

$$\begin{array}{l} \quad \{ \ P : \ \mathit{true} \ \} \qquad (* \ \text{basisgevallen} \ *) \\ \quad \{ \ 0 = L(0) \ \wedge \ 0 \le 0 \le n \ \wedge \ 0 = E(0) \ \} \\ x := 0 \ ; \ k := 0 \ ; \ y := 0 \\ \quad \{ \ J : \quad x = L(k) \ \wedge \ 0 \le k \le n \ \wedge \ y = E(k) \ \} \ \ . \end{array}$$

Stap 3. We kiezen de variante functie $\mathit{vf} = n - k$. Er geldt $J \wedge B \ \Rightarrow \ \mathit{vf} \ge 0$ omdat $J \ \Rightarrow \ k \le n$.

Stap 4. De body van de lus:

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

Stap 5. Samenvatting.

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

De tijdscomplexiteit is van orde n, omdat de variante functie $\mathit{vf} = n - k$ initieel gelijk is aan n en de initialisatie en de lusbody verder geen lussen bevatten.

Opgave 3 (46 %). Gegeven zijn constanten m, $c : \mathbb{Z}$, en een functie $h : \mathbb{Z}^2 \to \mathbb{Z}$ die zwak dalend is in zijn eerste argument en zwak stijgend is in zijn tweede argument.

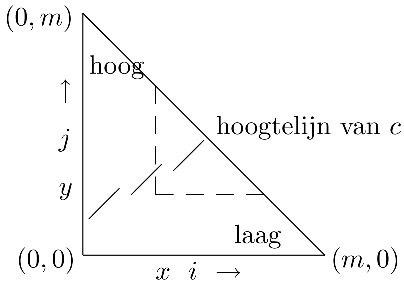
Bepaal een commando S ter bepaling van het aantal paren (i, j) met $i \ge 0$ en $j \ge 0$ en $i + j < m$ en $h(i, j) > c$.

(a: 26 %) 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 het gevraagde aantal mee berekend kan worden. Bepaal recurrente betrekkingen voor deze functie, inclusief basisgeval(len).

(b: 4 %) Geef een formele specificatie voor commando S.

(c: 16 %) Bepaal voor dit probleem een correct commando S met tijdscomplexiteit $\mathcal{O}(m)$.

Uitwerking.



Functie h daalt naar het oosten en stijgt naar het noorden. De berg ligt dus in het noordwesten, het dal in het zuidoosten. De hoogtelijn loopt dus van zuidwest naar noordoost. We leggen het resteren zoekgebied ten noordoosten van het zoekpunt (x, y), omdat we dan in het hoekpunt in het zuidwesten beginnen kunnen.

We definiëren daarom:

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

De gezochte waarde is dus $F(0,0)$.

Als $m \le x+y$, dan geldt $x \le i \;\wedge\; y \le j \;\Rightarrow\; m \le i+j$, zodat het domein van de verzameling leeg is. Dit impliceert:

$$m \le x+y \;\Rightarrow\; F(x,y) = 0 \;.$$

We zoeken nu naar recurrente betrekkingen voor $F(x,y)$ waarbij x en/of y verhoogd wordt. Voor het verhogen van x krijgen we:

$$\begin{array}{cl}
 & F(x,y) \\
= & \{\text{ definitie } F\text{; splitsen; } i = x \text{ of } x+1 \le i\text{; herken } F\ \} \\
 & F(x+1,y) + \#\{j \mid j : y \le j \;\wedge\; x+j < m \;\wedge\; h(x,j) > c\,\} \\
= & \{\ h(x,j) \text{ stijgt in } j\ ;\ h(x,y) \text{ is dus de laagste;} \\
 & \quad \textbf{stel } h(x,y) > c\ ;\ \text{dan is } h(x,j) > c \text{ voor alle } j \ge y\ \} \\
 & F(x+1,y) + \#\{j \mid j : y \le j < m - x\,\} \\
= & \{\ \textbf{stel } x+y \le m\text{; tellen } *) \\
 & F(x+1,y) + m - x - y \;.
\end{array}$$

Voor het verlagen van y krijgen we:

$$\begin{array}{cl}
 & F(x,y) \\
= & \{\text{ definitie } F\text{; splitsen; } j = y \text{ of } y+1 \le j\text{; herken } F\ \} \\
 & F(x,y+1) + \#\{i \mid i :\ x \le i \;\wedge\; i+y < m \;\wedge\; h(i,y) > c\,\} \\
= & \{\ h(i,y) \text{ daalt in } i\ ;\ h(x,y) \text{ is dus de hoogste;} \\
 & \quad \textbf{stel } h(x,y) \le c\ ;\ \text{dan is } h(i,y) \le c \text{ voor alle } i \ge x\ \} \\
 & F(x,y+1) \;.
\end{array}$$

Dit bewijst de recurrente betrekkingen

(1) $\quad x+y \le m \;\wedge\; h(x,y) > c \;\Rightarrow\; F(x,y) = F(x+1,y) + m - x - y \;,$

(2) $\quad h(x,y) \le c \;\Rightarrow\; F(x,y) = F(x,y+1) \;.$

We kiezen de specificatie:

$$\begin{array}{l}
\quad \{\ P :\ Z = F(0,0)\ \} \\
\textbf{var } z : \mathbb{Z} \\
S \\
\quad \{\ Q :\ Z = z\ \} \;.
\end{array}$$

Stap 1. We gebruiken hulpvariabelen x, $y : \mathbb{Z}$, en de invariant en guard volgens:

$$\begin{array}{ll}
J : & Z = z + F(x,y) \;, \\
B : & x + y < m \;.
\end{array}$$

Dan geldt

$$\begin{array}{cl}
 & J \;\wedge\; \neg B \\
\equiv & \{\text{ definities, uitwerken ontkenning }\} \\
 & Z = z + F(x,y) \;\wedge\; m \le x+y \\
\Rightarrow & \{\text{ dan is } F(x,y) = 0\text{, zie boven }\} \\
 & Q :\ Z = z \;.
\end{array}$$

Stap 2. Initialisatie.

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

Stap 3. We kiezen de variante functie $vf = m - x - y$. Hiervoor geldt $J \wedge B \Rightarrow vf \geq 0$ omdat $B \equiv x + y < m$.

Stap 4. De body van de lus wordt:

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

Stap 5. Samenvatting.

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

De tijdscomplexiteit is van orde m, omdat de variante functie $vf = m - x - y$ initieel gelijk is aan m en de initialisatie en de lusbody geen lussen bevatten.