Uitwerking Programmacorrectheid
24 augustus 2007

Tijdsduur 3 uur. Gesloten boek.

Opgave 1 (15 %). Bepaal een geannoteerd commando S dat voldoet aan

$$
\begin{array}{l}
\textbf{const}\ n : \mathbb{Z} \\
\textbf{var}\ k : \mathbb{Z} \\
\quad \{\ P :\ k = X\ \} \\
S \\
\quad \{\ Q :\ k \leq n\ \wedge\ (k = X + 1\ \vee\ k = 2 \cdot n - X)\ \}\ \ .
\end{array}
$$

Uitwerking. Omdat n een constante is, mag het commando geen toekenning(en) aan n bevatten. Omdat X een specificatieconstante is, mag die *niet* in het commando voorkomen.

$$
\begin{array}{l}
\quad \{\ P :\ k = X\ \} \\
\textbf{if}\ k + 1 \leq n\ \textbf{then} \\
\qquad \{\ k = X\ \wedge\ k + 1 \leq n\}\ \ (*\ \text{rekenen}\ *) \\
\qquad \{\ k + 1 \leq n\ \wedge\ k + 1 = X + 1\ \} \\
\quad k := k + 1 \\
\qquad \{\ k \leq n\ \wedge\ k = X + 1\ \} \\
\textbf{else} \\
\qquad \{\ k = X\ \wedge\ n < k + 1\}\ \ (*\ n \leq k, \text{ rekenen}\ *) \\
\qquad \{\ 2 \cdot n - k \leq n\ \wedge\ 2 \cdot n - k = 2 \cdot n - X\ \} \\
\quad k := 2 \cdot n - k \\
\qquad \{\ k \leq n\ \wedge\ k = 2 \cdot n - X\ \} \\
\textbf{end}\quad (*\ \text{verzamel de takken}\ *) \\
\quad \{\ (k \leq n\ \wedge\ k = X + 1)\quad \vee\quad (k \leq n\ \wedge\ k = 2 \cdot n - X\ \} \\
\qquad (*\ \text{distributiviteit}\ *) \\
\quad \{\ Q :\ k \leq n\ \wedge\ (k = X + 1\ \vee\ k = 2 \cdot n - X)\ \}\ \ .
\end{array}
$$

Opgave 2 (40 %). Er is een groep personen met de nummers $0 \leq i \leq n$. Gegeven is een afhankelijkheidsrelatie $a(i, j)$ tussen de personen, die transitief is, dwz. voldoet aan $a(i, j)\ \wedge\ a(j, k)\ \Rightarrow\ a(i, k)$. Gegeven is tevens $\neg\, a(0, n)$ en $0 < n \leq 2^r$ (ten overvloede: $\neg$ staat voor **not**).

Ontwerp een geannoteerd commando S ter bepaling van een persoon met nummer p waarvoor geldt $\neg\, a(p, p + 1)$. Dit commando dient in ten hoogste r stappen te termineren.

$$
\begin{array}{l}
\textbf{const}\ n, r \in \mathbb{N} \\
\quad \{\ P :\ \neg\, a(0, n)\ \wedge\ 0 < n \leq 2^r\ \wedge\ (\forall\, i, j, k : a(i, j) \wedge a(j, k)\ \Rightarrow\ a(i, k))\ \} \\
\textbf{var}\ p : \mathbb{Z} \\
S \\
\quad \{\ Q :\ \neg\, a(p, p + 1)\}\ \ .
\end{array}
$$

Laat ook zien, dat je commando inderdaad in ten hoogste r stappen termineert. Voer het volledige stappenplan uit.

Uitwerking. De preconditie hangt alleen van constanten af. We zullen hem dus verderop weglaten, wanneer we hem niet nodig hebben. Het idee van de oplossing is de transitiviteit te herschrijven tot $\neg a(i, k)\ \Rightarrow\ \neg a(i, j) \vee \neg a(j, k)$.

Stap 1. We introduceren gehele variabelen q en s met de invariant J en guard B volgens:

J: $p < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - p \leq 2^s$,
B: $p + 1 \neq q$.

Er geldt:

$$
\begin{array}{ll}
& J \wedge \neg B \\
\equiv & \{ \text{ invullen, ontkenning uitwerken } \} \\
& p < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - p \leq 2^s \ \wedge \ p + 1 = q \\
\Rightarrow & \{ \text{ invullen en conjuncten weglaten } \} \\
& Q : \ \neg\, a(p, p+1) \ .
\end{array}
$$

Stap 2. Initialisatie.

$$
\begin{array}{l}
\quad \{ \ P \ \} \\
\quad \{ \ 0 < n \ \wedge \ \neg\, a(0,n) \ \wedge \ n - 0 \leq 2^r \ \} \\
p := 0 \ ; \ q := n \ ; \ s := r \ ; \\
\quad \{ \ J : \quad p < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - p \leq 2^s \ \} \ .
\end{array}
$$

Stap 3. Om terminatie in ten hoogste r stappen te bewijzen, nemen we $vf = s$. Correctheidsbewijs:

$$
\begin{array}{ll}
& J \wedge B : \quad p < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - p \leq 2^s \ \wedge \ p + 1 \neq q \\
\Rightarrow & \{ \text{ rekenen, } 2^s \geq 1 \text{ en dus: } \} \\
& s \geq 0 \ .
\end{array}
$$

Stap 4. We gebruiken een hulpvaribele $m : \mathbb{Z}$:

$$
\begin{array}{l}
\quad \{ \ J \ \wedge \ B \ \wedge \ vf = V \ \} \\
\quad \{ \ p < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - p \leq 2^s \ \wedge \ p + 1 \neq q \ \wedge \ s = V \ \} \\
\qquad (* \text{ voorbereiding van halvering van het zoekgebied } *) \\
\quad \{ \ p < (p+q) \ \mathbf{div} \ 2 < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - (p+q) \ \mathbf{div} \ 2 \leq 2^{s-1} \\
\qquad \wedge \ (p+q) \ \mathbf{div} \ 2 - p \leq 2^{s-1} \ \wedge \ s - 1 < V \ \} \\
m := (p+q) \ \mathbf{div} \ 2 \ ; \ s := s - 1 \\
\quad \{ \ p < m < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - m \leq 2^s \ \wedge \ m - p \leq 2^s \ \wedge \ s < V \ \} \\
\mathbf{if} \ a(p,m) \ \mathbf{then} \\
\qquad \{ \ a(p,m) \ \wedge \ p < m < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - m \leq 2^s \\
\qquad\quad \wedge \ m - p \leq 2^s \ \wedge \ s < V \ \} \\
\qquad\quad (* \ a(i,j) \text{ is transitief volgens } P \ *) \\
\qquad \{ \ m < q \ \wedge \ \neg\, a(m,q) \ \wedge \ q - m \leq 2^s \ \wedge \ s < V \ \} \\
\quad p := m \ ; \\
\qquad \{ \ J \ \wedge \ vf < V : \quad p < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - p \leq 2^s \ \wedge \ s < V \ \} \\
\mathbf{else} \\
\qquad \{ \ \neg\, a(p,m) \ \wedge \ p < m < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - m \leq 2^s \\
\qquad\quad \wedge \ m - p \leq 2^s \ \wedge \ s < V \ \} \\
\qquad\quad (* \text{ weglaten conjuncten } *) \\
\qquad \{ \ p < m \ \wedge \ \neg\, a(p,m) \ \wedge \ m - p \leq 2^s \ \wedge \ s < V \ \} \\
\quad q := m \ ; \\
\qquad \{ \ J \ \wedge \ vf < V : \quad p < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - p \leq 2^s \ \wedge \ s < V \ \} \\
\mathbf{end} \quad (* \text{ verzamel de takken } *) \\
\quad \{ \ J \ \wedge \ vf < V \ \} \ .
\end{array}
$$

Stap 5. Samenvatting en conclusie.

$$
\begin{array}{l}
\quad \{ \ P \ \} \\
p := 0 \ ; \ q := n \ ; \ s := r \ ; \\
\quad \{ \ J : \quad p < q \ \wedge \ \neg\, a(p,q) \ \wedge \ q - p \leq 2^s \ \} \\
\mathbf{while} \ p + 1 \neq q \ \mathbf{do} \quad (* \ vf \ = s \ *) \\
\quad m := (p+q) \ \mathbf{div} \ 2 \ ; \ s := s - 1 \ ; \\
\quad \mathbf{if} \ a(p,m) \ \mathbf{then} \ \ p := m \ \mathbf{else} \ \ q := m \ \ \mathbf{end} \\
\mathbf{end} \quad \{ \ Q : \neg\, a(p, p+1) \ \} \ .
\end{array}
$$

Omdat $s \geq 0$ blijft en in elke stap met 1 verlaagd wordt, is het aantal stappen kleiner of gelijk aan de beginwaarde r van s.

Opgave 3 (45 %). Gegeven is een functie $h : \mathbb{N}^2 \to \mathbb{Z}$ die sterk dalend in zijn eerste argument en zwak stijgend in zijn tweede argument is. Bepaal een commando S ter bepaling van het aantal paren (i, j) met $i + j \leq m$ en $h(i, j) = c$ voor een gegeven getal c, volgens de specificatie

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

(a: 25 %) Maak een schets van het te onderzoeken gebied. Geef aan waar berg en dal liggen, 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: 20 %) Bepaal een commando S dat aan bovenstaande specificatie voldoet. Voer hiertoe het volledige stappenplan uit.

Uitwerking. (a) Het gaat om de punten in de rechthoekige driehoek met rechthoekszijden langs de x-as en de y-as, en de schuine zijde met de vergelijking $x + y = m$ (inclusief de rand). Het dal ligt in de oostpunt, de berg in de noordpunt van de driehoek. De hoogtelijn gaat dus ongeveer van zuidwest naar noordoost. We leggen de resterende rechthoek ten noordoosten van het inspectiepunt en definiëren dus

$$F(x, y) = \#\{(i, j) \mid x \leq i \ \wedge \ y \leq j \ \wedge \ i + j \leq m \ \wedge \ h(i, j) = c\}\ .$$

Er geldt

(basis) $\quad x + y > m \quad \Rightarrow \quad F(x, y) = 0$

wegens leeg domein.

Voor het verhogen van x berekenen we:

$$\begin{array}{cl} & F(x, y) \\ = & \{\ \text{splitsen: } i \geq x + 1 \text{ of } i = x\ \} \\ & F(x + 1, y) + \#\{j \mid y \leq j \ \wedge \ x + j \leq m \ \wedge \ h(x, j) = c\} \\ = & \{\ h(x, j) \geq h(x, y) \text{ omdat } h(x, \_) \text{ zwak stijgend is.} \\ & \quad \textbf{Stel}\ \ h(x, y) > c. \text{ Dan is ook } h(x, j) > c \text{ voor alle } j \geq y\ \} \\ & F(x + 1, y)\ . \end{array}$$

Voor het verhogen van y berekenen we:

$$\begin{array}{cl} & F(x, y) \\ = & \{\ \text{splitsen: } j \geq y + 1 \text{ of } j = y\ \} \\ & F(x, y + 1) + \#\{i \mid x \leq i \ \wedge \ i + y \leq m \ \wedge \ h(i, y) = c\} \\ = & \{\ h(i, y) < h(x, y) \text{ voor } i > x \text{ omdat } h(\_, y) \text{ sterk dalend is.} \\ & \quad \textbf{Stel}\ \ h(x, y) \leq c. \text{ Dan is } h(i, y) < c \text{ voor alle } i > x. \\ & \quad \textbf{Stel}\ \ x + y \leq m. \text{ Dan telt } (x, y) \text{ zelf mee indien } h(x, y) = c.\ \} \\ & F(x, y + 1) + ord(h(x, y) = c)\ . \end{array}$$

We krijgen aldus de recurrente betrekkingen:

(RBx) $\quad h(x, y) > c \quad \Rightarrow \quad F(x, y) = F(x + 1, y)\ ,$
(RBy) $\quad x + y \leq m \ \wedge \ h(x, y) \leq c \quad \Rightarrow \quad F(x, y) = F(x, y + 1) + ord(h(x, y) = c)\ .$

(b) Implementatie.

Stap 1. We kiezen als invariant en guard:

$$\begin{aligned} &J: \quad Z = z + F(x,y)\ , \\ &B: \quad x + y \le m\ . \end{aligned}$$

Bewijs:

$$\begin{aligned} & \quad J \wedge \neg B \\ \equiv & \quad \{ \text{ definities, uitwerken ontkenning} \} \\ & \quad Z = z + F(x,y) \ \wedge\ x + y > m \\ \Rightarrow & \quad \{ \text{ (basis) en rekenen } \} \\ & \quad Q: \quad Z = z\ . \end{aligned}$$

Stap 2. Initialisatie:

$$\begin{aligned} & \quad \{\ P:\ Z = \#\{(i,j) \in \mathbb{N}^2 \mid i + j \le m \ \wedge\ h(i,j) = c\} \\ & \qquad (*\ \text{definitie } F \text{ en rekenen } *) \\ & \quad \{\ Z = 0 + F(0,0)\ \} \\ & z := 0\ ;\ x := 0\ ;\ y := 0\ ; \\ & \quad \{\ J: Z = z + F(x,y)\ \}\ \ . \end{aligned}$$

Stap 3. We nemen $vf = m - x - y$. De guard B impliceert dat $vf \ge 0$ is.

Stap 4.

$$\begin{aligned} & \quad \{\ J \ \wedge\ B \ \wedge\ \mathrm{vf} = V\ \} \\ & \quad \{\ Z = z + F(x,y) \ \wedge\ x + y \le m \ \wedge\ m - x - y = V\ \} \\ & \textbf{if } h(x,y) > c \textbf{ then} \\ & \qquad \{\ h(x,y) > c \ \wedge\ Z = z + F(x,y) \ \wedge\ x + y \le m \ \wedge\ m - x - y = V\ \} \\ & \qquad\quad (*\ \text{(RBx), rekenen, en weglaten conjuncten } *) \\ & \qquad \{\ Z = z + F(x+1,y) \ \wedge\ m - (x+1) - y < V\ \} \\ & \quad x := x + 1\ ; \\ & \qquad \{\ J \ \wedge\ \mathrm{vf} < V: \quad Z = z + F(x,y) \ \wedge\ m - x - y < V\ \} \\ & \textbf{else} \\ & \qquad \{\ h(x,y) \le c \ \wedge\ Z = z + F(x,y) \ \wedge\ x + y \le m \ \wedge\ m - x - y = V\ \} \\ & \qquad\quad (*\ \text{(RBy), rekenen, en weglaten conjuncten } *) \\ & \qquad \{\ Z = z + \mathrm{ord}(h(x,y) = c) + F(x,y+1) \ \wedge\ m - x - (y+1) < V\ \} \\ & \quad z := z + \mathrm{ord}(h(x,y) = c)\ ; \\ & \qquad \{\ Z = z + F(x,y+1) \ \wedge\ m - x - (y+1) < V\ \} \\ & \quad y := y + 1\ ; \\ & \qquad \{\ J \ \wedge\ \mathrm{vf} < V: \quad Z = z + F(x,y) \ \wedge\ m - x - y < V\ \} \\ & \textbf{end} \quad (*\ \text{verzamel de takken } *) \\ & \quad \{\ J \ \wedge\ \mathrm{vf} < V\ \}\ \ . \end{aligned}$$

Stap 5. Samenvatting.

$$\begin{aligned} & \quad \{\ P:\ Z = \#\{(i,j) \in \mathbb{N}^2 \mid i + j \le m \ \wedge\ h(i,j) = c\} \\ & z := 0\ ;\ x := 0\ ;\ y := 0\ ; \\ & \quad \{\ J: Z = z + F(x,y)\ \} \\ & \textbf{while } x + y \le m \textbf{ do} \quad (*\ \mathrm{vf} = m - x - y\ *) \\ & \quad \textbf{if } h(x,y) > c \textbf{ then} \\ & \qquad x := x + 1\ ; \\ & \quad \textbf{else} \\ & \qquad z := z + \mathrm{ord}(h(x,y) = c)\ ; \\ & \qquad y := y + 1\ ; \\ & \quad \textbf{end} \\ & \textbf{end} \quad \{\ Q:\ Z = z\ \}\ \ . \end{aligned}$$