Uitwerking Programmacorrectheid, 29 juni 2007

Tijdsduur 3 uur. Gesloten boek.

Opgave 1 (15 %). Gegeven is een programmavariabele $m : \mathbb{Z}$. Beschouw de specificaties

(1) $\{\ m = X\ \}\quad U\quad \{\ X < m < X + 5\ \}$.
(2) $\{\ X < m < X + 5\ \}\quad V\quad \{\ m = X\ \}$.

(a) Beschrijf deze twee commando's in het nederlands.
(b) Geef een geannoteerd commando dat aan één van beide specificaties voldoet.
(c) Geef aan waarom er geen commando kan zijn dat aan de andere specificatie voldoet.

Uitwerking. (a) Als de variabele m vóór uitvoering van U de waarde X heeft, dan wijzigt U de waarde van m zo dat na afloop $X < m < X + 5$ geldt.. Met andere woorden, U verhoogt m met een getal $g \in \{1, 2, 3, 4\}$. Uitwerkingen, dat vóór uitvoering van U de conditie $m = X$ moet gelden en dat na uitvoering $X < m < X + 5$ moet gelden, zijn niet precies genoeg.

Commando V gokt de waarde van X, waarvan (in de preconditie) gegeven is dat hij voldoet aan $m - 5 < X < m$, en maakt m daaraan gelijk.

(b)
$\{m = X\}$
$(*$ rekenen (er zijn meer mogelijkheden) $*)$
$\{X < m + 1 < X + 5\}$
$m := m + 1$
$\{X < m < X + 5\}$.

(c) De preconditie is equivalent met $m - 5 < X < m$. Dit legt X niet eenduidig vast: X kan $m - 1$ maar ook $m - 2$ zijn (of ...). Het is dus niet mogelijk aan m een waarde te geven die aan *elke* dergelijke X gelijk is.

Opgave 2 (40 %). Ontwerp een commando T met logaritmische complexiteit dat voldoet aan

const $n : \mathbb{N}^+$, $a :$ `array` $[0\ ..\ n]$ **of** $\mathbb{Z}$
var $i : \mathbb{Z}$
$\{\ P : a[0] < a[n] + 5\ \}$
T
$\{\ Q : 0 \le i < n\ \wedge\ a[i] < a[i + 1] + 5\ \}$.

Voer 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. Lineair zoeken is niet efficient genoeg. Bewijzen van lineaire zoekprogramma's gaan meestal fout, omdat er niet gegeven is dat er een i is die aan Q voldoet. Dit zou je apart uit de preconditie moeten bewijzen. Onbewezen (en verkeerd bewezen) versies vam linear search leveren geen punten op. Bij het onderstaande binaire zoekprogramma volgt het echter uit het correctheidsbewijs van het programma.

Stap 1. We gebruiken een hulpvariabele $j : \mathbb{Z}$ en de invariant en guard volgens

J : $\quad 0 \le i < j \le n\ \wedge\ a[i] < a[j] + 5$
B : $\quad i + 1 \neq j$.

$J \wedge \neg B$ impliceert Q, want $\neg B$ geeft $j = i + 1$ en als we $j := i + 1$ in J invullen krijgen we Q.

Stap 2. Initialisatie.

$$
\begin{array}{l}
\quad \{P : a[0] < a[n] + 5\ \} \\
\qquad (*\ n \in \mathbb{N}^+ \text{ geeft } n > 0\ *) \\
\quad \{0 \le 0 < n \le n\ \wedge\ a[0] < a[n] + 5\} \\
i := 0\ ;\ j := n \\
\quad \{J :\ 0 \le i < j \le n\ \wedge\ a[i] < a[j] + 5\}\ .
\end{array}
$$

Stap 3. We nemen (bv) $vf = j - i$. Te bewijzen dat $J \wedge B \Rightarrow vf \ge 0$. Dit geldt omdat $i < j$ uit J volgt.

Stap 4.

$$
\begin{array}{l}
\quad \{J \wedge B \wedge vf = V\} \\
\quad \{0 \le i < j \le n\ \wedge\ a[i] < a[j] + 5\ \wedge\ i + 1 \ne j\ \wedge\ j - i = V\} \\
\qquad (*\ \text{zie onder}\ *) \\
\quad \{0 \le i < (i + j)\ \mathbf{div}\ 2 < j \le n\ \wedge\ a[i] < a[j] + 5\ \wedge\ j - i = V\} \\
m := (i + j)\ \mathbf{div}\ 2\ ; \\
\quad \{0 \le i < m < j \le n\ \wedge\ a[i] < a[j] + 5\ \wedge\ j - i = V\} \\
\mathbf{if}\ \ a[i] < a[m] + 5\ \ \mathbf{then} \\
\qquad \{a[i] < a[m] + 5\ \wedge\ 0 \le i < m < j \le n\ \wedge\ a[i] < a[j] + 5 \\
\qquad\quad \wedge\ j - i = V\} \\
\qquad\quad (*\ \text{rekenen}\ *) \\
\qquad \{0 \le i < m \le n\ \wedge\ a[i] < a[m] + 5\ \wedge\ m - i < V\} \\
\quad j := m\ ; \\
\qquad \{J \wedge vf < V :\ 0 \le i < j \le n\ \wedge\ a[i] < a[j] + 5\ \wedge\ j - i < V\} \\
\mathbf{else} \\
\qquad \{a[m] + 5 \le a[i]\ \wedge\ 0 \le i < m < j \le n\ \wedge\ a[i] < a[j] + 5 \\
\qquad\quad \wedge\ j - i = V\} \\
\qquad\quad (*\ \text{rekenen en}\ a[m] < a[m] + 5 \le a[i] < a[j] + 5\ *) \\
\qquad \{0 \le m < j \le n\ \wedge\ a[m] < a[j] + 5\ \wedge\ j - m < V\} \\
\quad i := m\ ; \\
\qquad \{J \wedge vf < V :\ 0 \le i < j \le n\ \wedge\ a[i] < a[j] + 5\ \wedge\ j - i < V\} \\
\mathbf{end}\quad (*\ \text{verzamel postcondities}\ *) \\
\quad \{J \wedge vf < V\}\ .
\end{array}
$$

Rest ons nog op te merken dat

$$
\begin{array}{ll}
 & i < j\ \wedge\ i + 1 \ne j \\
\Rightarrow & i + 2 \le j \\
\Rightarrow & i < i + 1 = (i + i + 2)\ \mathbf{div}\ 2 \le (i + j)\ \mathbf{div}\ 2 \\
 & \wedge\ \ (i + j)\ \mathbf{div}\ 2 \le (j - 2 + j)\ \mathbf{div}\ 2 = j - 1 < j \\
\Rightarrow & i < (i + j)\ \mathbf{div}\ 2 < j\ .
\end{array}
$$

Stap 5. Samenvatting.

$$
\begin{array}{l}
\quad \{P : a[0] < a[n] + 5\ \} \\
i := 0\ ;\ j := n \\
\quad \{J :\ 0 \le i < j \le n\ \wedge\ a[i] < a[j] + 5\} \\
\mathbf{while}\ \ i + 1 \ne j\ \ \mathbf{do}\quad (*\ \ vf : j - i\ *) \\
\qquad m := (i + j)\ \mathbf{div}\ 2\ ; \\
\qquad \mathbf{if}\ \ a[i] < a[m] + 5\ \ \mathbf{then}\ j := m \\
\qquad \mathbf{else}\ \ i := m\ \ \mathbf{end} \\
\mathbf{end} \\
\quad \{Q : 0 \le i < n\ \wedge\ a[i] < a[i + 1] + 5\ \}\ .
\end{array}
$$

Opgave 3 (45 %). Gegeven is een functie $h : \mathbb{Z}^2 \to \mathbb{Z}$ die zwak stijgend in zijn eerste argument en zwak dalend in zijn tweede argument is. Commando S wordt gespecificeerd door

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

(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. 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.

(a) De berg ligt in het oosten, het dal in het noorden. De hoogtelijn loopt dus zuidwest-noordoost. We beginnen in de oorsprong en volgen hem naar het noordoosten. De resterende rechthoek ligt dus in het noordoosten. We definiëren derhalve

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

Wegens leeg domein geldt:

(basis) $\quad x \ge m\ \vee\ y \ge n\ \ \Rightarrow\ \ F(x,y) = 0\ .$

We bepalen twee recurrente betrekkingen met domeinsplitsing. Eerst in i:

$$\begin{array}{ll} & F(x,y) \\ = & \{\ \text{splits in } i \ge x+1 \text{ en } i = x\ \} \\ & F(x+1,y) + \#\{i \mid x = i < m\ \wedge\ (\exists\, j : y \le j < n\ \wedge\ h(i,j) = c)\} \\ = & \{\ \textbf{Stel } x < m\ \wedge\ y < n\ \wedge\ h(x,y) \le c. \\ & \quad \text{Er geldt } h(x,j) \le h(x,y) \text{ voor alle } j \ge y. \\ & \quad \text{Als } h(x,y) = c, \text{ dan kunnen we } (i,j) = (x,y) \text{ nemen.} \\ & \quad \text{Als } h(x,y) < c, \text{ dan is } h(x,j) \le h(x,y) < c \text{ voor alle } j \ge y \text{ omdat} \\ & \quad h(x,j) \text{ zwak dalend in } j \text{ is, en dus is } h(x,j) \ne c \text{ voor deze } j.\ \} \\ & F(x+1,y) + ord(h(x,y) = c)\ . \end{array}$$

Domeinsplitsing in j geeft:

$$\begin{array}{ll} & F(x,y) \\ = & \{\ \textbf{Stel}\ \ y < n.\ \text{Splits in } j \ge y+1 \text{ en } j = y\ \} \\ & \#\{i \mid x \le i < m\ \wedge\ (h(i,y) = c\ \vee\ (\exists\, j : y+1 \le j < n\ \wedge\ h(i,j) = c))\} \\ = & \{\ \textbf{Stel } h(x,y) > c. \text{ Dan is } h(i,y) \ge h(x,y) > c \text{ voor alle } i \ge x \text{ omdat} \\ & \quad h(i,y) \text{ zwak stijgend in } i \text{ is, en dus is } h(i,y) \ne c \text{ voor deze } i.\ \} \\ & \#\{i \mid x \le i < m\ \wedge\ (\exists\, j : y+1 \le j < n\ \wedge\ h(i,j) = c)\} \\ = & \{\ \text{definitie } F\ \} \\ & F(x,y+1)\ . \end{array}$$

Deze bewijst de regels:

$$\begin{array}{ll} \text{(rec1)} & x < m\ \wedge\ y < n\ \wedge\ h(x,y) \le c \\ & \quad \Rightarrow\ \ F(x,y) = F(x+1,y) + ord(h(x,y) = c)\ , \\ \text{(rec2)} & y < n\ \wedge\ h(x,y) > c\ \ \Rightarrow\ \ F(x,y) = F(x,y+1)\ . \end{array}$$

(b) Stap 1. We introduceren hulpvariabelen $x,\ y : \mathbb{Z}$ en nemen invariant en guard volgens:

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

$J \wedge \neg B$ impliceert Q, omdat formule (basis) dan $F(x,y) = 0$ geeft.

Stap 2. Initialisatie.

$\{P : \ Z = \#\{i \mid 0 \le i < m \ \wedge \ (\exists\, j : 0 \le j < n \ \wedge \ h(i,j) = c)\}$
$\quad (*$ definitie F en rekenen $*)$
$\{Z = 0 + F(0,0)\}$
$z := 0 \ ; \ x := 0 \ ; \ y := 0 \ ;$
$\{J : \ Z = z + F(x,y)\}$.

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

Stap 4.

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
$\{Z = z + F(x,y) \ \wedge \ x < m \ \wedge \ y < n \ \wedge \ m + n - x - y = V\}$
if $h(x,y) \le c$ **then**
$\quad \{h(x,y) \le c \wedge Z = z + F(x,y) \ \wedge \ x < m \ \wedge \ y < n$
$\qquad \wedge \ m + n - x - y = V\}$
$\qquad (*$ (rec1) $*)$
$\quad \{Z = z + ord(h(x,y) = c) + F(x+1,y) \ \wedge \ m + n - (x+1) - y < V\}$
$\quad z := z + ord(h(x,y) = c) \ ;$
$\quad \{Z = z + F(x+1,y) \ \wedge \ m + n - (x+1) - y < V\}$
$\quad x := x + 1 \ ;$
$\quad \{J \wedge vf < V : \quad Z = z + F(x,y) \ \wedge \ m + n - x - y < V\}$
else
$\quad \{h(x,y) > c \wedge Z = z + F(x,y) \ \wedge \ x < m \ \wedge \ y < n$
$\qquad \wedge \ m + n - x - y = V\}$
$\qquad (*$ (rec2) $*)$
$\quad \{Z = z + F(x,y+1) \ \wedge \ m + n - x - (y+1) < V\}$
$\quad y := y + 1 \ ;$
$\quad \{J \wedge vf < V : \quad Z = z + F(x,y) \ \wedge \ m + n - x - y < V\}$
end $\quad (*$ verzamel postcondities $*)$
$\{J \wedge vf < V\}$.

Stap 5. Samenvatting.

$\{P : \ Z = \#\{i \mid 0 \le i < m \ \wedge \ (\exists\, j : 0 \le j < n \ \wedge \ h(i,j) = c)\}$
$z := 0 \ ; \ x := 0 \ ; \ y := 0 \ ;$
$\{J : \ Z = z + F(x,y)\}$
while $x < m \wedge y < n$ **do** $\quad (*$ $vf : m + n - x - y$ $*)$
$\quad$ **if** $h(x,y) \le c$ **then**
$\qquad z := z + ord(h(x,y) = c) \ ;$
$\qquad x := x + 1 \ ;$
$\quad$ **else** $y := y + 1$ **end**
end
$\{Q : Z = z\}$.