Uitwerking Toets Programmacorrectheid, 11 maart 2011

Tijdsduur 2 uur. Gesloten boek. Geef voor alle commando's correcte en volledige annotaties.

Opgave 1 (15 %). Gegeven zijn programmavariabelen $n, t : \mathbb{Z}$. Bepaal één geannoteerde toekenning S die voldoet aan

$$
\begin{array}{l}
\quad \{n = Y + 1 \ \wedge \ t = X + 2 \cdot Y\} \\
S \\
\quad \{n = X - 2 \ \wedge \ t = X + 2 \cdot Y\} \ .
\end{array}
$$

Uitwerking.

$$
\begin{array}{l}
\quad \{n = Y + 1 \ \wedge \ t = X + 2 \cdot Y\} \\
\qquad (* \ \text{We hebben behoefte aan } X - 2 \text{ uitgedrukt in } n \text{ en } t : \\
\qquad\quad X - 2 = t - 2 \cdot Y - 2 = t - 2 \cdot (Y + 1) = t - 2 \cdot n \ \ *) \\
\quad \{ \ t - 2 \cdot n = X - 2 \ \wedge \ t = X + 2 \cdot Y\} \\
n := t - 2 \cdot n \ ; \\
\quad \{ \ n = X - 2 \ \wedge \ t = X + 2 \cdot Y\}
\end{array}
$$

Opgave 2 (35 %). Gegeven is de programmavariabele $n : \mathbb{Z}$. Bepaal een geannoteerd conditioneel commando U dat voldoet aan

$$
\begin{array}{l}
\quad \{P : \ n = X \ \} \\
U \\
\quad \{Q : \ n \geq 0 \ \wedge \ (n + X = 0 \ \vee \ 3 \cdot n \leq X + 1 < 3 \cdot n + 3) \ \} \ .
\end{array}
$$

Uitwerking. We hebben $Q \equiv (Q1 \vee Q2)$ voor

$$
\begin{array}{ll}
Q1 : & n \geq 0 \ \wedge \ n + X = 0 \ , \\
Q2 : & n \geq 0 \ \wedge \ 3 \cdot n \leq X + 1 < 3 \cdot n + 3.
\end{array}
$$

We streven naar één van beide disjuncten van de postconditie:

$$
\begin{array}{l}
\quad \{P : \ n = X \ \} \\
\textbf{if} \ \ n \leq 0 \ \ \textbf{then} \\
\qquad \{ \ n = X \ \wedge \ n \leq 0 \ \} \\
\qquad\ \ (* \ \text{rekenen} \ *) \\
\qquad \{ \ -n \geq 0 \ \wedge \ (-n) + X = 0 \ \} \\
\quad n := -n \\
\qquad \{ \ Q1 : n \geq 0 \ \wedge \ n + X = 0 \ \} \\
\textbf{else} \\
\qquad \{ \ n = X \ \wedge \ n > 0 \ \} \\
\qquad\ \ (* \ \text{rekenen} \ *) \\
\qquad \{ \ (n + 1) \ \textbf{div} \ 3 \geq 0 \ \wedge \ (n + 1) \ \textbf{div} \ 3 = (X + 1) \ \textbf{div} \ 3 \ \} \\
\quad n := (n + 1) \ \textbf{div} \ 3 \ ; \\
\qquad \{ \ n \geq 0 \ \wedge \ n = (X + 1) \ \textbf{div} \ 3 \ \} \\
\qquad\ \ (* \ \text{definitie } \textbf{div} \ *) \\
\qquad \{ \ Q2 : \ n \geq 0 \ \wedge \ 3 \cdot n \leq X + 1 < 3 \cdot n + 3 \ \} \\
\textbf{end} \quad (* \ \text{verzamel de takken, gebruik } Q \equiv (Q1 \vee Q2) \ *) \\
\quad \{ \ Q : \ n \geq 0 \ \wedge \ (n + X = 0 \ \vee \ 3 \cdot n \leq X + 1 < 3 \cdot n + 3) \ \} \ .
\end{array}
$$

Opgave 3 (50 %). Gegeven is de declaratie

$$\textbf{const } n : \mathbb{N} \,,\ a : \ \textbf{array } [0\ .\ .\ n) \textbf{ of } \mathbb{Z} \ .$$

Er geldt

$$P_0 : \quad \forall\, i : 0 \le i < n \ \Rightarrow\ a[i] \ge 1 \ .$$

De functie $f : \mathbb{N} \to \mathbb{Z}$ voldoet aan de recurrente betrekkingen:

$$f(k) = 0 \ \text{ als } n \le k,$$
$$f(k) = 1 + k \cdot f(k + a[k]) \ \text{ als } 0 \le k < n.$$

Bepaal een commando T dat $f(k)$ berekent volgens de specificatie

$$\begin{array}{l} \textbf{var } k, x : \mathbb{Z} \ ; \\ \quad \{P :\ k \ge 0 \ \wedge\ X = f(k)\} \\ T \\ \quad \{Q :\ X = x\} \ . \end{array}$$

Gebruik hiertoe een hulpvariabele $y : \mathbb{Z}$ en een herhaling met de invariant

$$J : \quad k \ge 0 \ \wedge\ X = x + y \cdot f(k) \ .$$

Voer het volledige stappenplan uit. Geef bij de stappen 1 en 3 geannoteerde lineaire bewijzen.

Uitwerking.
Stap 1. Finalisatie. In verband met de definitie van f kiezen we de guard

$$B : \quad k < n \ .$$

Aan de bewijsverplichting $J \wedge \neg B \ \Rightarrow\ Q$ wordt voldaan wegens

$$\begin{array}{ll} & J \ \wedge\ \neg B \\ \equiv & \{ \text{ definities } J \text{ en } B, \text{ uitwerking ontkenning } \} \\ & k \ge 0 \ \wedge\ X = x + y \cdot f(k) \ \wedge\ n \le k \\ \Rightarrow & \{ \text{ definitie: } f(k) = 0 \text{ voor } k \ge n; \text{ rekenen } \} \\ & Q : X = x \ . \end{array}$$

Stap 2. Initialisatie.

$$\begin{array}{l} \textbf{var } k, x : \mathbb{Z} \ ; \\ \quad \{P :\ k \ge 0 \ \wedge\ X = f(k)\} \\ \qquad (*\ \text{rekenen } *) \\ \quad \{\ k \ge 0 \ \wedge\ X = 0 + 1 \cdot f(k)\} \\ x := 0 \ ; \\ \quad \{\ k \ge 0 \ \wedge\ X = x + 1 \cdot f(k)\} \\ y := 1 \ ; \\ \quad \{\ J : \quad k \ge 0 \ \wedge\ X = x + y \cdot f(k)\} \ \ . \end{array}$$

Stap 3. We kiezen de variante functie $vf = n - k$. Er geldt $J \wedge B \ \Rightarrow\ vf \ge 0$ wegens

$$\begin{array}{ll} & J \ \wedge\ B \\ \Rightarrow & \{ \text{ definitie } B, \text{ weglaten } J \ \} \\ & k < n \\ \Rightarrow & \{ \text{ dus } vf = n - k > 0 \text{ en dus } \} \\ & vf \ge 0. \end{array}$$

Stap 4. Body van de lus.

$$
\begin{array}{l}
\quad \{\ J \ \wedge\ B \ \wedge\ \mathrm{vf} = V\ \} \\
\quad \{\ k \geq 0 \ \wedge\ X = x + y \cdot f(k) \ \wedge\ k < n \ \wedge\ n - k = V\ \} \\
\qquad (*\ \text{definitie } f(k) \text{ voor } 0 \leq k < n \text{ geeft} \\
\qquad\qquad X = x + y \cdot (1 + k \cdot f(k + a[k])); \text{ distributiviteit } *) \\
\quad \{\ 0 \leq k < n \ \wedge\ X = (x + y) + (y \cdot k) \cdot f(k + a[k]) \ \wedge\ n - k = V\ \} \\
x := x + y\ ; \\
\quad \{\ 0 \leq k < n \ \wedge\ X = x + (y \cdot k) \cdot f(k + a[k]) \ \wedge\ n - k = V\ \} \\
y := y \cdot k\ ; \\
\quad \{\ 0 \leq k < n \ \wedge\ X = x + y \cdot f(k + a[k]) \ \wedge\ n - k = V\ \} \\
\qquad (*\ P_0 \text{ geeft } a[k] \geq 1 \text{ wegens } 0 \leq k < n; \text{ rekenen } *) \\
\quad \{\ k + a[k] \geq 0 \ \wedge\ X = x + y \cdot f(k + a[k]) \ \wedge\ n - (k + a[k]) < V\ \} \\
k := k + a[k]\ ; \\
\quad \{\ J \ \wedge\ \mathrm{vf} < V : \quad k \geq 0 \ \wedge\ X = x + y \cdot f(k) \ \wedge\ n - k < V\ \} \ .
\end{array}
$$

Stap 5. Samenvatting.

$$
\begin{array}{l}
\quad \{P :\ k \geq 0 \ \wedge\ X = f(k)\} \\
x := 0\ ; \\
y := 1\ ; \\
\quad \{\ J : \quad k \geq 0 \ \wedge\ X = x + y \cdot f(k)\ \} \\
\textbf{while}\ \ k < n\ \ \textbf{do} \qquad (*\ \mathrm{vf} = n - k\ *) \\
\quad x := x + y\ ; \\
\quad y := y \cdot k\ ; \\
\quad k := k + a[k]\ ; \\
\textbf{end} \\
\quad \{\ Q : X = x\ \} \ .
\end{array}
$$