Uitwerking Toets Programmacorrectheid, 8 maart 2007

Tijdsduur 2 uur. Gesloten boek.

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

$$\begin{array}{l} \{j = Y + 5 \ \wedge \ k = X + 3 \cdot Y\} \\ S \\ \{j = X \ \wedge \ k = X + 3 \cdot Y\} \ . \end{array}$$

Uitwerking. NB Je mag niet meer dan één toekenning gebruiken.

$$\begin{array}{l} \{j = Y + 5 \ \wedge \ k = X + 3 \cdot Y\} \\ \quad (* \text{ rekenen, } X = k - 3 \cdot Y = k - 3 \cdot (j - 5) = k + 15 - 3 \cdot j \ *) \\ \{k + 15 - 3 \cdot j = X \ \wedge \ k = X + 3 \cdot Y\} \\ j := k + 15 - 3 \cdot j \\ \{j = X \ \wedge \ k = X + 3 \cdot Y\} \ . \end{array}$$

Een vaak gemaakte fout: uit $Y = (k - X)$ **div** 3 mag je niet afleiden dat $3 \cdot Y = k - X$. Immers 5 **div** $3 = 1$ en $5 \neq 3 \cdot 1$.

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

$$\begin{array}{l} \{X \geq 0 \ \wedge \ (2 \cdot m = 1 - X \ \vee \ m = X + 3)\} \\ U \\ \{m = X\} \ . \end{array}$$

Uitwerking.

$$\begin{array}{l} \{X \geq 0 \ \wedge \ (2 \cdot m = 1 - X \ \vee \ m = X + 3)\} \\ \quad (* \text{ distributie } X \geq 0, \text{ bereken } X \ *) \\ \{1 - 2 \cdot m = X \geq 0 \ \vee \ m - 3 = X \geq 0\} \\ \textbf{if} \ \ m \geq 3 \ \ \textbf{then} \quad (* \text{ de guards } m \geq 1 \text{ en } m \geq 2 \text{ zijn ook correct } *) \\ \quad \{m \geq 3 \ \wedge \ (1 - 2 \cdot m = X \geq 0 \ \vee \ m - 3 = X \geq 0)\} \\ \quad\quad (* \ 1 - 2 \cdot m < 0, \text{ dus eerste disjunct vervalt; weglaten conjunct } *) \\ \quad \{m - 3 = X\} \\ \quad m := m - 3 \\ \quad \{m = X\} \\ \textbf{else} \\ \quad \{m < 3 \ \wedge \ (1 - 2 \cdot m = X \geq 0 \ \vee \ m - 3 = X \geq 0)\} \\ \quad\quad (* \ m - 3 < 0, \text{ dus tweede disjunct vervalt; weglaten conjunct } *) \\ \quad \{1 - 2 \cdot m = X\} \\ \quad m := 1 - 2 \cdot m \\ \quad \{m = X\} \\ \textbf{end} \\ \quad \{\text{verzamel de takken } m = X\} \ . \end{array}$$

Een soms gemaakte fout: de specificatieconstante X mag niet in het programma, en dus ook niet als guard van het **if** commando, voorkomen. Anders was de oplossing $U : m := X$ wel zo gemakkelijk (hoewel dit geen conditioneel commando is).

Opgave 3 (50 %). De functie $f : \mathbb{Z} \to \mathbb{Z}$ is gegeven door de recurrente betrekkingen:

$$\begin{array}{l} f(x) = 0 \ \text{ als } x < 0, \\ f(x) = 3 \cdot f(x - 5) + x \ \text{ als } x \geq 0 \ . \end{array}$$

Bepaal een commando T dat voldoet aan

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

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

$$J : \quad X = y \cdot f(k) + z \ .$$

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

Uitwerking. De functie f mag niet in het programma voorkomen. Anders was de toekenning $z := f(k)$ wel zo eenvoudig.

Stap 1. We kiezen $B : \ k \geq 0$. Te bewijzen is nu $J \wedge \neg B \ \Rightarrow \ Q$.

$$
\begin{array}{ll}
 & J \ \wedge \ \neg B \\
\equiv & \quad \{ \text{ definities } J \text{ en } B, \text{ uitwerken negatie } \} \\
 & X = y \cdot f(k) + z \ \wedge \ k < 0 \\
\Rightarrow & \quad \{ \text{ definitie van } f(k) \text{ bij } k < 0 \ \} \\
 & X = y \cdot 0 + z \\
\equiv & \quad \{ \text{ rekenen en definitie } Q \ \} \\
 & Q : \quad X = z \ .
\end{array}
$$

Let wel: in een geannoteerd lineair bewijs staan er geen accolades om de predicaten. De implicatie ($\Rightarrow$) mag niet door equivalentie ($\equiv$) vervangen worden, want $X = y \cdot 0 + z$ impliceert niet dat $k < 0$.

Stap 2. Initialisatie.

$$
\begin{array}{l}
\quad \{P : \quad X = f(k)\} \\
\qquad (* \text{ voorbereiding toekenningen } *) \\
\quad \{X = 1 \cdot f(k) + 0\} \\
y := 1 \ ; \ z := 0 \quad (* \text{ simultane toekenning } *) \\
\quad \{J : \quad X = y \cdot f(k) + z\} \ .
\end{array}
$$

Stap 3. We kiezen $vf = k$. Te bewijzen is $J \wedge B \ \Rightarrow \ vf \geq 0$. Bewijs:

$$
\begin{array}{ll}
 & J \ \wedge \ B \\
\equiv & \quad \{ \text{ definitie } B \ \} \\
 & J \ \wedge \ k \geq 0 \\
\Rightarrow & \quad \{ \text{ weglaten conjunct, } vf = k \ \} \\
 & vf \geq 0 \ .
\end{array}
$$

Stap 4. De body.

$$
\begin{array}{l}
\quad \{J \wedge B \wedge \mathrm{vf} = V\} \\
\qquad (* \ \text{ definities } *) \\
\quad \{X = y \cdot f(k) + z \ \wedge \ k \geq 0 \ \wedge \ k = V\} \\
\qquad (* \text{ definitie } f(k) \text{ voor } k \geq 0 \ *) \\
\quad \{X = y \cdot (3 \cdot f(k-5) + k) + z \ \wedge \ k = V\} \\
\qquad (* \text{ rekenen, voorbereiding } k := k - 5 \ *) \\
\quad \{X = y \cdot 3 \cdot f(k-5) + y \cdot k + z \ \wedge \ k - 5 < V\} \\
z := y \cdot k + z \ ; \\
\quad \{X = y \cdot 3 \cdot f(k-5) + z \ \wedge \ k - 5 < V\} \\
y := y \cdot 3 \ ; \\
\quad \{X = y \cdot f(k-5) + z \ \wedge \ k - 5 < V\} \\
k := k - 5 \ ; \\
\quad \{J \ \wedge \ \mathrm{vf} < V : \quad X = y \cdot f(k) + z \ \wedge \ k < V\} \ .
\end{array}
$$

Stap 5. Samenvatting.

$$
\begin{array}{l}
\quad \{P: \quad X = f(k)\} \\
y := 1\ ;\ z := 0 \\
\quad \{J: \quad X = y \cdot f(k) + z\} \quad (* \ \mathrm{v}f : k \ *) \\
\textbf{while}\ \ k \geq 0\ \ \textbf{do} \\
\quad z := y \cdot k + z\ ; \\
\quad y := y \cdot 3\ ; \\
\quad k := k - 5\ ; \\
\textbf{end} \\
\quad \{Q: \quad X = z\}\ \ .
\end{array}
$$