Uitwerking Toets PCor, 5 maart 2008

Tijdsduur 2 uur. Gesloten boek.

Opgave 1 (40 %). Gegeven zijn programmavariabelen $i, k : \mathbb{Z}$. Bepaal een geannoteerd commando S dat voldoet aan

$$\begin{array}{l} \quad \{\ P :\ i = X\ \wedge\ k = Y\ \wedge\ X + Y \geq 0\ \} \\ S \\ \quad \{\ Q : i \geq 0\ \wedge\ ((i = X\ \wedge\ k = X - Y)\ \vee\ (i = Y\ \wedge\ k = X + Y))\ \}\ . \end{array}$$

Aanwijzing: herschrijf Q eerst in de vorm $Q \equiv Q0 \vee Q1$.

Uitwerking 1. Wegens distributiviteit van $\wedge$ over $\vee$ geldt: $Q \equiv Q0 \vee Q1$ voor

$$\begin{array}{ll} Q0 : & i = X \geq 0\ \wedge\ k = X - Y\ , \\ Q1 : & i = Y \geq 0\ \wedge\ k = X + Y\ . \end{array}$$

De test $X \geq 0$ is fout omdat X niet in het commando mag voorkomen. Wegens $i = X$ vooraf, kunnen we $Q0$ alleen waar maken als $i \geq 0$ vooraf geldt. We testen dit dus:

$$\begin{array}{l} \quad \{\ P :\ i = X\ \wedge\ k = Y\ \wedge\ X + Y \geq 0\ \} \\ \textbf{if}\ \ i \geq 0\ \ \textbf{then} \\ \qquad \{\ i = X\ \wedge\ k = Y\ \wedge\ X + Y \geq 0\ \wedge\ i \geq 0\ \} \\ \qquad\quad (*\ \text{toewerken naar } Q0\ *) \\ \qquad \{\ i = X \geq 0\ \wedge\ i - k = X - Y\ \} \\ \quad k := i - k\ ; \\ \qquad \{\ Q0 :\ i = X \geq 0\ \wedge\ k = X - Y\ \} \\ \textbf{else} \\ \qquad \{\ i = X\ \wedge\ k = Y\ \wedge\ X + Y \geq 0\ \wedge\ i < 0\ \} \\ \qquad\quad (*\ \text{wegens } X = i < 0 \text{ en } X + Y \geq 0, \text{ geldt } Y \geq 0\ *) \\ \qquad \{\ i = X\ \wedge\ i + k = X + Y\ \wedge\ Y \geq 0\ \} \\ \quad k := i + k\ ; \\ \qquad \{\ i = X\ \wedge\ k = X + Y\ \wedge\ Y \geq 0\ \} \\ \qquad\quad (*\ \text{toewerken naar } Q1\ *) \\ \qquad \{\ k - i = Y \geq 0\ \wedge\ k = X + Y\ \} \\ \quad i := k - i\ ; \\ \qquad \{\ Q1 :\ i = Y \geq 0\ \wedge\ k = X + Y\ \} \\ \textbf{end} \quad (*\ \text{verzamel de takken}\ *) \\ \quad \{\ Q :\ \ Q0 \vee Q1\ \}\ . \end{array}$$

Opgave 2 (60 %). De functie $f : \mathbb{Z} \to \mathbb{Z}$ voldoet aan de recurrente betrekkingen:

$$\begin{array}{l} f(0) = 0 \\ f(7 \cdot n + r) = 2 \cdot f(n) + r\ \ \text{als}\ \ 0 \leq r < 7 \end{array}$$

Bepaal een commando T dat voldoet aan

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

Gebruik hiertoe een hulpvariabele $y : \mathbb{Z}$ en een herhaling met een invariant die het conjunct $y \cdot f(n) + x = Z$ bevat.

Voer het volledige stappenplan uit. Geef bij stap 1 een geannoteerd lineair bewijs. Geef bij stap 3 de bewijsverplichting en een sluitende argumentatie of een lineair bewijs.

Uitwerking 2. Stap 1. We kiezen:

$$\begin{array}{ll} J: & y \cdot f(n) + x = Z \ \wedge \ n \geq 0 \ , \\ B: & n \neq 0 \ . \end{array}$$

Te bewijzen: $J \ \wedge \ \neg B \ \Rightarrow \ Q$.

$$\begin{array}{ll} & J \ \wedge \ \neg B: \quad y \cdot f(n) + x = Z \ \wedge \ n \geq 0 \ \wedge \ n = 0 \\ \Rightarrow & \{ \text{ invullen } n = 0, \text{ weglaten conjuncten } \} \\ & y \cdot f(0) + x = Z \\ \equiv & \{ \text{ definitie } f(0) = 0, \text{ rekenen en herkennen } Q \ \} \\ & Q: \ x = Z \ . \end{array}$$

Stap 2. Initialisatie:

$$\begin{array}{l} \{ \ P: \quad f(n) = Z \ \wedge \ n \geq 0 \ \} \\ \quad (* \ \text{rekenen} \ *) \\ \{ \ 1 \cdot f(n) + 0 = Z \ \wedge \ n \geq 0 \ \} \\ y := 1 \ ; \ x := 0 \ ; \\ \{ \ J: \quad y \cdot f(n) + x = Z \ \wedge \ n \geq 0 \ \} \ . \end{array}$$

Stap 3. We kiezen $vf = n$. Te bewijzen is nu $J \wedge B \ \Rightarrow \ vf \geq 0$. Dit volgt direct uit het feit dat J het conjunct $n \geq 0$ bevat.

Stap 4.

$$\begin{array}{l} \{ \ J \ \wedge \ B \ \wedge \ vf = V \ \} \\ \{ \ y \cdot f(n) + x = Z \ \wedge \ n \geq 0 \ \wedge \ n \neq 0 \ \wedge \ n = V \ \} \\ \{ \ y \cdot f(n) + x = Z \ \wedge \ n > 0 \ \wedge \ n = V \ \} \\ \quad (* \ \text{deling met rest } n = 7 \cdot (n \ \mathbf{div} \ 7) + n \ \mathbf{mod} \ 7 \ *) \\ \{ \ y \cdot f(7 \cdot (n \ \mathbf{div} \ 7) + n \ \mathbf{mod} \ 7) + x = Z \ \wedge \ 0 \leq n \ \mathbf{mod} \ 7 < 7 \\ \quad \wedge \ n > 0 \ \wedge \ n = V \ \} \\ \quad (* \ \text{definitie } f \text{ en distributie van } y \cdot \ *) \\ \{ \ y \cdot 2 \cdot f(n \ \mathbf{div} \ 7) + y \cdot (n \ \mathbf{mod} \ 7) + x = Z \ \wedge \ n > 0 \ \wedge \ n = V \ \} \\ x := y \cdot (n \ \mathbf{mod} \ 7) + x \ ; \\ \{ \ y \cdot 2 \cdot f(n \ \mathbf{div} \ 7) + x = Z \ \wedge \ n > 0 \ \wedge \ n = V \ \} \\ \quad (* \ \text{eigenschap } \mathbf{div}, \text{ voorbereiden toekenning aan } n \ *) \\ \{ \ y \cdot 2 \cdot f(n \ \mathbf{div} \ 7) + x = Z \ \wedge \ n \ \mathbf{div} \ 7 \geq 0 \ \wedge \ n \ \mathbf{div} \ 7 < V \ \} \\ y := y \cdot 2 \ ; \ n := n \ \mathbf{div} \ 7 \ ; \\ \{ \ y \cdot f(n) + x = Z \ \wedge \ n \geq 0 \ \wedge \ n < V \ \} \\ \quad (* \ \text{keuzes } J \text{ en } vf \ *) \\ \{ \ J \ \wedge \ vf < V \ \} \ . \end{array}$$

Stap 5. Samenvatting.

$$\begin{array}{l} \{ \ P: \quad f(n) = Z \ \wedge \ n \geq 0 \ \} \\ y := 1 \ ; \ x := 0 \ ; \\ \{ \ J: \quad y \cdot f(n) + x = Z \ \wedge \ n \geq 0 \ \} \\ \mathbf{while} \ \ n \neq 0 \ \ \mathbf{do} \quad (* \ vf : n \ *) \\ \quad x := y \cdot (n \ \mathbf{mod} \ 7) + x \ ; \\ \quad y := y \cdot 2 \ ; \ n := n \ \mathbf{div} \ 7 \ ; \\ \mathbf{end} \\ \{ \ Q : x = Z \ \} \ . \end{array}$$