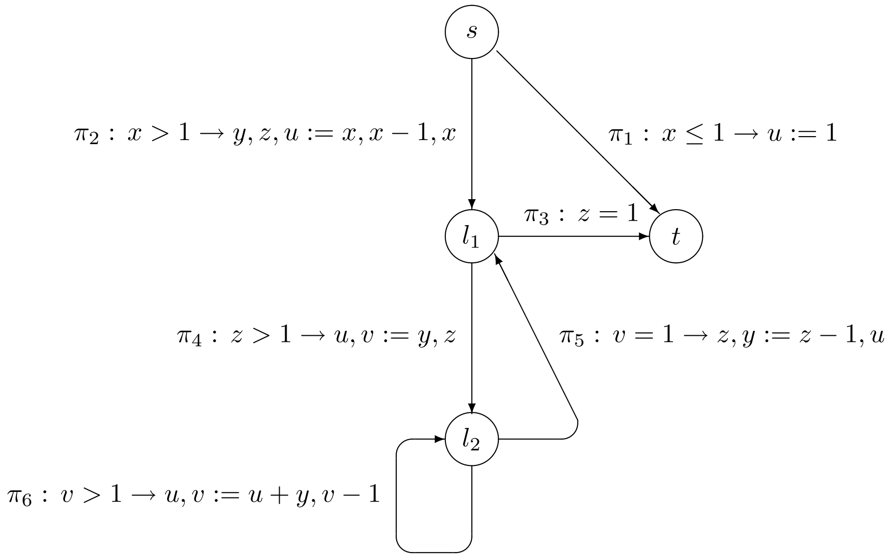
Ulrich Hannemann Jan Bredereke

Übungsserie 1

Beispiellösung

Lösungentwicklung[1] zu Aufgabe 1.2

Für das folgende Programm P soll gezeigt werden, daß $\models \{(x \geq 0)\}\, P\, \{(u = x!)\}$ gilt.



Wir wenden die Methode von Floyd entsprechend Definition 3.2 an. Dazu soll ein Zusicherungsnetz für P gefunden werden, welches induktiv ist und konsistent zu $\varphi \stackrel{\text{def}}{=} (x \geq 0)$ und $\psi \stackrel{\text{def}}{=} (u = x!)$ ist. Unser Zustandsraum besteht aus dem Vektor $\overline{y} \stackrel{\text{def}}{=} (u, v, x, y, z)$.

Wie arbeitet das Programm? Dazu betrachten wir einen Lauf mit einem frei gewählten Eingabewert für x, etwa $x = 4$. Nicht genau bekannte Werte werden durch $\perp$ dargestellt.

$$\begin{aligned}
&\langle s, (\perp, \perp, 4, \perp, \perp)\rangle \to \langle l_1, (4, \perp, 4, 4, 3)\rangle \to \langle l_2, (4, 3, 4, 4, 3)\rangle \to \\
&\langle l_2, (8, 2, 4, 4, 3)\rangle \to \langle l_2, (12, 1, 4, 4, 3)\rangle \to \langle l_1, (12, 1, 4, 12, 2)\rangle \to \\
&\langle l_2, (12, 2, 4, 12, 2)\rangle \to \langle l_2, (24, 1, 4, 12, 2)\rangle \to \langle l_1, (24, 1, 4, 24, 1)\rangle \to \\
&\langle t, (24, 1, 4, 24, 1)\rangle
\end{aligned}$$

Dabei beobachten wir

- In l_1 wird auf Abbruch getestet, u und y haben stets den gleichen Wert, im Beispiel die aufsteigende Folge $4, 12, 24$ – oder $x, x(x-1), x(x-1)((x-1)-1)$.
- Knoten l_2 führt eine Multiplikation durch: Beim Eintritt in den Knoten werden als Multiplikatoren u und v übergeben, dann wird π_6 so lange durchlaufen, bis $v = 1$ gilt. In diesem Fall enthält u gerade das Produkt der Anfangswerte.

[1] Fragen, Ergänzungen, Korrekturen (falls nötig) bitte per mail an die Veranstalter.

Schritt 1 Als erstes werden Prädikate für den Start- bzw. Zielknoten gewählt. Insbesondere für die Konsistenzprüfung ist es sinnvoll, hier die Vor- bzw. Nachbedingung einzusetzen. Also:

$$\mathcal{Q}_s(\bar{y}) \stackrel{\text{def}}{=} x \geq 0$$
$$\mathcal{Q}_t(\bar{y}) \stackrel{\text{def}}{=} u = x!$$

Damit wäre der Konsistenzbeweis erfüllt, denn

$$\models \varphi \rightarrow \mathcal{Q}_s \text{ und}$$
$$\models \mathcal{Q}_t \rightarrow \psi$$

gelten trivialerweise.

Allein durch diese Wahl ist aber bereits die erste Verifikationsbedingung überprüfbar, da es eine Transition von s nach t gibt. Wir zeigen also

$$V_{\pi_1} : \models \mathcal{Q}_s \wedge x \leq 1 \rightarrow \mathcal{Q}_t \circ (u := 1).$$

Sei also σ ein Zustand mit $\sigma \models \mathcal{Q}_s \wedge x \leq 1$. Aus $\sigma \models x \geq 0 \wedge x \leq 1$ folgt $\sigma \models x = 0 \vee x = 1$. Zu zeigen ist, daß dann $(\sigma : u \mapsto 1) \models u = x!$ gilt, bzw. $\sigma \models x! = 1$. Da aber $0! \stackrel{\text{def}}{=} 1$ und $1! = 1$ gilt, ist auch $\models x = 0 \vee x = 1 \rightarrow x! = 1$ gültig.

Schritt 2 Als nächsten Schritt entwickeln wir das Prädikat $\mathcal{Q}_{l_1}$. Für den Fall $z = 1$ ist die Transition π_3 zu nehmen, d.h., daß in diesem Fall $u = x!$ sein muss. Wie oben beobachtet, wird in u der gesuchte Wert $x!$ aufgebaut durch Multiplikation mit einem absteigenden Faktor - z. Somit lässt sich als Zwischenbeschreibung für u ein Term entwickeln, der aussagt, daß $x!$ berechnet wird und alle Multiplikatoren kleiner oder gleich z noch fehlen. Ferner beobachten wir noch, daß in den Transitionen zu l_1 jeweils sichergestellt wird, daß die Variablen u und y den gleichen Wert bekommen. Somit können wir als Prädikat für l_1 festlegen:

$$\mathcal{Q}_{l_1} \stackrel{\text{def}}{=} y = u \wedge u = \frac{x!}{z!}.$$

An dieser Stelle sind zwei weitere Verifikationsbedingungen zu prüfen, die zu von l_1 wegführenden Transitionen gehören. Wir zeigen also

$$V_{\pi_2} : \models \mathcal{Q}_s \wedge x > 1 \rightarrow \mathcal{Q}_{l_1} \circ (u, y, z := x, x, x - 1).$$

Sei also σ ein Zustand mit $\sigma \models \mathcal{Q}_s \wedge x > 1$. Aus $x \geq 0 \wedge x > 1$ folgt $x > 1$. Zu zeigen ist

$$\sigma \models u = y \wedge u = \frac{x!}{z!} \circ (u, y, z := x, x, x - 1),$$

also

$$\sigma \models x = x \wedge x = \frac{x!}{(x-1)!}$$

Da $\sigma(x) > 1$ ist $\frac{x!}{(x-1)!}$ definiert und $x = \frac{x!}{(x-1)!}$ gültig. Somit ist also V_{π_2} wahr.

Außerdem überprüfen wir π_3:

$$V_{\pi_3} : \models \mathcal{Q}_{l_1} \wedge z = 1 \rightarrow \mathcal{Q}_t.$$

Diese Verifikationsbedingung ist einfach:

$$y = u \wedge u = \frac{x!}{z!} \wedge z = 1$$

impliziert direkt $u = x!$.

Schritt 3 Nun fehlt noch ein Prädikat für l_2. Bei Betrachtung eines Programmlaufs stellen wir fest, daß der Wert von y insgesamt v-mal auf den Anfangswert von u addiert wird und somit zur Rückgabe" (Transition nach l_1) gerade $u = z * y$ gilt. Dieses Multiplizieren durch wiederholtes Aufaddieren kann durch den Term $u = y * (z - v + 1)$ charakterisiert werden. Die Werte von x, y und z bleiben unverändert, die Beziehung $y = \frac{x!}{z!}$ kann (und muß) also übernommen werden. Definieren wir also

$$\mathcal{Q}_{l_2} \stackrel{\text{def}}{=} y = \frac{x!}{z!} \wedge u = y * (z - v + 1).$$

Mit diesem Prädikat sind drei Verifikationsbedingungen zu überprüfen.

$$V_{\pi_4} : \models \mathcal{Q}_{l_1} \wedge z > 1 \rightarrow \mathcal{Q}_{l_2} \circ (u, v := y, z).$$

Sei also σ ein Zustand mit $\sigma \models \mathcal{Q}_{l_1} \wedge z > 1$, also $\sigma \models y = u \wedge u = \frac{x!}{z!} \wedge z > 1$. Zu zeigen ist

$$\sigma \models y = \frac{x!}{z!} \wedge u = y * (z - v + 1) \circ (u, v := y, z),$$

also

$$\sigma \models y = \frac{x!}{z!} \wedge y = y * (z - z + 1).$$

Wegen $\models y = u \wedge u = \frac{x!}{z!} \rightarrow y = \frac{x!}{z!}$ ist dies unmittelbar erfüllt, V_{π_4} ist also gültig.

$$V_{\pi_6} : \models \mathcal{Q}_{l_2} \wedge v > 1 \rightarrow \mathcal{Q}_{l_2} \circ (u, v := u + y, v - 1).$$

Sei also σ ein Zustand mit $\sigma \models \mathcal{Q}_{l_2} \wedge v > 1$, also $\sigma \models y = \frac{x!}{z!} \wedge u = y * (z - v + 1) \wedge v > 1$. Zu zeigen ist

$$\sigma \models y = \frac{x!}{z!} \wedge u = y * (z - v + 1) \circ (u, v := u + y, v - 1),$$

also

$$\sigma \models y = \frac{x!}{z!} \wedge u + y = y * (z - (v - 1) + 1).$$

Dabei gilt $\sigma \models y = \frac{x!}{z!}$ unmittelbar, und weil $\sigma \models u = y * (z - v + 1) \rightarrow u + y = y * (z - v + 2)$ gilt, ist auch diese Verifkationsbedingung gültig (wegen $v > 1$ gilt $y * (z - (v - 1) + 1) = y * (z - v + 2)$.

Es bleibt noch

$$V_{\pi_5} : \models \mathcal{Q}_{l_2} \wedge v = 1 \rightarrow \mathcal{Q}_{l_1} \circ (z, y := z - 1u).$$

Sei also σ ein Zustand mit $\sigma \models \mathcal{Q}_{l_2} \wedge v = 1$, also $\sigma \models y = \frac{x!}{z!} \wedge u = y * (z - v + 1) \wedge v = 1$. Zu zeigen ist

$$\sigma \models y = u \wedge u = \frac{x!}{z!} \circ (z, y = z - 1, u),$$

also

$$\sigma \models u = u \wedge u = \frac{x!}{(z-1)!}.$$

Hier taucht jetzt ein kleines Problem auf: Wir wissen, daß

$$\sigma \models y = \frac{x!}{z!} \wedge u = y * z$$

gilt, da $v = 1$, somit $\sigma \models u = \frac{x! * z}{z!}$. Der letzte Schritt, um den Beweis zu führen, nämlich $\models \frac{x!}{(z-1)!} = \frac{x! * z}{z!}$, gilt aber nur, falls $z \geq 1$ ist. Somit muß die Zusicherung für l_2 noch ergänzt werden.

$$\mathcal{Q}'_{l_2} \stackrel{\text{def}}{=} y = \frac{x!}{z!} \wedge u = y * (z - v + 1) \wedge z \geq 1$$

Mit diesem Prädikat ist die Verifikationsbedingung V_{π_5} gültig. Durch die Änderung müssen jetzt aber die Bedingungen V_{π_4} und V_{π_6} erneut bewiesen werden. Auf V_{π_6} hat die neue Wahl von $\mathcal{Q}'_{l_2}$ keine Auswirkung, da z nicht in die Transition involviert ist. Die Verifikationsbedingung V_{π_4} ändert sich, es ist zu zeigen, daß

$$\models (y = u \wedge u = \frac{x!}{z!} \wedge z > 1) \rightarrow (y = \frac{x!}{z!} \wedge u = y * (z - v + 1) \wedge z \geq 1) \circ (u, v := y, z)$$

gültig ist. Da aber $\models z > 1 \rightarrow z \geq 1$ gilt, ist auch diese Verifikationsbedingung gültig.

Zusammenfassung Für das Programm P ist ein Zusicherungsnetz definiert als

$$\begin{array}{ll}
\mathcal{Q}_s(\bar{y}) & \stackrel{\text{def}}{=} x \geq 0 \\
\mathcal{Q}_{l_1} & \stackrel{\text{def}}{=} y = u \wedge u = \frac{x!}{z!} \\
\mathcal{Q}'_{l_2} & \stackrel{\text{def}}{=} y = \frac{x!}{z!} \wedge u = y * (z - v + 1) \wedge z \geq 1 \\
\mathcal{Q}_t(\bar{y}) \stackrel{\text{def}}{=} & u = x!
\end{array}$$

Dieses Zusicherungsnetz ist induktiv und konsistent bezüglich $\langle (x \geq 0), (u = x!) \rangle$. Somit gilt $\models \{(x \geq 0)\}\, P\, \{(u = x!)\}$.