Ludwig-Maximilians-Universität München SS 2006
Institut für Informatik Übungsblatt 3
Prof. Dr. M. Wirsing, M. Hammer, A. Rauschmayer

Informatik II Musterlösung

Zu jeder Aufgabe ist eine Datei abzugeben, deren Name rechts in der Aufgabenüberschrift steht. Stellen Sie die Dateien in ein extra Verzeichnis (mit beliebigem Namen) und packen Sie dieses zu einem ZIP-Archiv. Geben Sie dieses, wie üblich, per UniWorx ab.

Aufgabe 3-1 **Programmäquivalenz** (`progequiv.txt`, 6 Punkte)

Zwei Programme $\mathtt{P}_1$ und $\mathtt{P}_2$ heissen äquivalent, wenn für beliebige Formeln φ, ψ gilt:

$\{\varphi\}\ \mathtt{P}_1\ \{\psi\}$ ist im Hoare-Kalkül herleitbar gdw. $\{\varphi\}\ \mathtt{P}_2\ \{\psi\}$ im Hoare-Kalkül herleitbar ist.

a) Beweisen Sie: Die beiden Programme

```
if (B1) {
    if (B2) {
        S1
    } else {
        S2
    }
} else {
    S2
}
```

und

```
if (B1 && B2) {
    S1
} else {
    S2
}
```

sind äquivalent.

Lösung: Wir bezeichnen das erste Programm als $\mathtt{P}_1$, das zweite als $\mathtt{P}_2$. Um $\mathtt{P}_1$ abzuleiten, benötigen wir:

$$\dfrac{\dfrac{\{\varphi \wedge \mathtt{B1} \wedge \mathtt{B2}\}\ \mathtt{S1}\ \{\psi\} \qquad \{\varphi \wedge \mathtt{B1} \wedge \neg\mathtt{B2}\}\ \mathtt{S2}\ \{\psi\}}{\{\varphi \wedge \mathtt{B1}\}\ \mathtt{if\ (B2)}\dots\ \{\psi\}}\text{(Falluntersch)} \qquad \{\varphi \wedge \neg\mathtt{B1}\}\ \mathtt{S2}\ \{\psi\}}{\{\varphi\}\ \mathtt{P}_1\ \{\psi\}}\text{(Falluntersch)}$$

Zu zeigen sind also die drei Beweisverpflichtungen:

$$\{\varphi \wedge \mathtt{B1} \wedge \mathtt{B2}\}\ \mathtt{S1}\ \{\psi\} \tag{1.1}$$
$$\{\varphi \wedge \mathtt{B1} \wedge \neg\mathtt{B2}\}\ \mathtt{S2}\ \{\psi\} \tag{1.2}$$
$$\{\varphi \wedge \neg\mathtt{B1}\}\ \mathtt{S2}\ \{\psi\} \tag{1.3}$$

Dies ist äquivalent zu:

$$\{\varphi \wedge \mathtt{B1} \wedge \mathtt{B2}\}\ \mathtt{S1}\ \{\psi\} \tag{1.1}$$
$$\{(\varphi \wedge \mathtt{B1} \wedge \neg\mathtt{B2}) \vee (\varphi \wedge \neg\mathtt{B1})\}\ \mathtt{S2}\ \{\psi\} \tag{1.2'}$$

Für $\mathtt{P}_2$ benötigen wir:

$$\dfrac{\{\varphi \wedge \mathtt{B1} \wedge \mathtt{B2}\}\ \mathtt{S1}\ \{\psi\} \qquad \{\varphi \wedge \neg(\mathtt{B1} \wedge \mathtt{B2})\}\ \mathtt{S2}\ \{\psi\}}{\{\varphi\}\ \mathtt{P}_2\ \{\psi\}}\text{(Falluntersch)}$$

Die produziert die Beweisverpflichtungen:

$$\{\varphi \wedge \texttt{B1} \wedge \texttt{B2}\}\ \texttt{S1}\ \{\psi\} \tag{2.1}$$
$$\{\varphi \wedge \neg(\texttt{B1} \wedge \texttt{B2})\}\ \texttt{S2}\ \{\psi\} \tag{2.2}$$

1.1 und 2.1 sind identisch. Die Vorbedingungen von 1.2' und 2.2 sind äquivalent:

$$\begin{aligned}
& (\varphi \wedge \texttt{B1} \wedge \neg\texttt{B2}) \vee (\varphi \wedge \neg\texttt{B1}) \\
\Leftrightarrow\ & \varphi \wedge ((\texttt{B1} \wedge \neg\texttt{B2}) \vee \neg\texttt{B1}) \\
\Leftrightarrow\ & \varphi \wedge (\neg\texttt{B2} \vee \neg\texttt{B1}) \\
\Leftrightarrow\ & \varphi \wedge \neg(\texttt{B1} \wedge \texttt{B2})
\end{aligned}$$

Damit sind $\texttt{P}_1$ und $\texttt{P}_2$ äquivalent.

Aufgabe 3-2 **Hoare-Kalkül** (`hoare.txt`, 10 Punkte)

Betrachten Sie das folgende Programm `P`:

```
while (i != n) {
    s = s + i + 1;
    i = i + 1;
}
```

Als Nachbedingung fordern wir

$$\texttt{s} = \sum_{j=0}^{\texttt{n}} j$$

a) Finden Sie eine Vorbedingung, so dass partielle Korrektheit gilt, *nicht* jedoch totale Korrektheit!

Lösung: Damit partielle, aber nicht totale Korrektheit gilt, darf der Schleifenrumpf nicht terminieren. Dies erreichen wir z.B. mit der Vorbedingung $\texttt{i} > \texttt{n}$.

b) Finden Sie eine geeignete Schleifeninvariante und weisen Sie vermittels des Hoare-Kalküls nach, dass dies tatsächlich eine Invariante ist. (Geeignet bedeutet, dass die Nachbedingung tatsächlich folgt.)

Lösung: Als Invariante bietet sich sofort

$$I \equiv \texttt{s} = \sum_{j=0}^{\texttt{i}} j$$

an. Der Nachweis ist einfach, hier die formelle Version:

$$\dfrac{\dfrac{\dfrac{}{\left\{\texttt{s}+\texttt{i}+1 = \sum_{j=0}^{\texttt{i+1}} j\right\}\ \texttt{s = s + i + 1;}\ \left\{\texttt{s} = \sum_{j=0}^{\texttt{i+1}} j\right\}}\text{(Zuw)} \quad \dfrac{}{\left\{\texttt{s} = \sum_{j=0}^{\texttt{i+1}} j\right\}\ \texttt{i = i + 1;}\ \left\{\texttt{s} = \sum_{j=0}^{\texttt{i}} j\right\}}\text{(Zuw)}}{\dfrac{\left\{\texttt{s}+\texttt{i}+1 = \sum_{j=0}^{\texttt{i+1}} j\right\}\ \texttt{s = s + i + 1; i = i + 1;}\ \left\{\texttt{s} = \sum_{j=0}^{\texttt{i}} j\right\}}{\left\{\texttt{s} = \left(\sum_{j=0}^{\texttt{i}} j\right) + (i+1) - (i+1)\right\}\ \texttt{s = s + i + 1; i = i + 1;}\ \left\{\texttt{s} = \sum_{j=0}^{\texttt{i}} j\right\}}\text{(Abschw)}}\text{(Seq)}}{\left\{\texttt{s} = \sum_{j=0}^{\texttt{i}} j\right\}\ \texttt{s = s + i + 1; i = i + 1;}\ \left\{\texttt{s} = \sum_{j=0}^{\texttt{i}} j\right\}}\text{(Abschw)}$$

Im Wesentlichen ist nur zweimal die Zuweisungsregel auf die Invariante anzuwenden, und dann mit etwas Rechnerei (legitimiert durch die Abschwächungsregel) die Invarianteneigenschaft sicherzustellen.

c) Beweisen sie die totale Korrektheit von

$$\{\mathtt{s} = 0 \wedge \mathtt{i} = 0 \wedge \mathtt{n} > 0\}\ \mathtt{P}\ \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{n}} j\right\}$$

Hinweis: Um in einer ASCII-Datei Summenzeichen darstellen zu können, verwenden Sie für $\sum_{i=0}^{n} i$ die Notatation „`sum(i=0, n, i)`“ (alternativ, für LaTeX-Fans: „`\sum_{i=0}^{n} i`“).

Lösung: Wiederum müssen wir die Invariante verstärken, damit die Fundiertheit des „Abstandsterms“ $\mathtt{n} - \mathtt{i}$ aus ihr folgt:

$$I \equiv \mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} \leq \mathtt{n}$$

Analog zum Nachweis der Invariante oben prüfen wir die neue Invariante, und erhalten:

$$\left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} + 1 \leq \mathtt{n}\right\}\ \texttt{s = s + i + 1; i = i + 1;}\ \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} \leq \mathtt{n}\right\}$$

Dies können wir mit der Abschwächungsregel wie folgt umschreiben:

$$\dfrac{\dfrac{\dfrac{\left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} + 1 \leq \mathtt{n}\right\}\ \texttt{s = s + i + 1; i = i + 1;}\ \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} \leq \mathtt{n}\right\}}{\left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} < \mathtt{n}\right\}\ \texttt{s = s + i + 1; i = i + 1;}\ \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} \leq \mathtt{n}\right\}}\,(\text{Abschw})}{\left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} \leq \mathtt{n} \wedge \mathtt{i} \neq \mathtt{n}\right\}\ \texttt{s = s + i + 1; i = i + 1;}\ \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} \leq \mathtt{n}\right\}}\,(\text{Abschw})}{\mathbf{F_p} \equiv \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} \leq \mathtt{n} \wedge \mathtt{i} \neq \mathtt{n}\right\}\ \texttt{\{s = s + i + 1; i = i + 1;\}}\ \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} \leq \mathtt{n}\right\}}\,(\text{Block})$$

Jetzt müssen wir noch den Abstiegsterm beweisen (mit $\alpha \equiv \mathtt{n} - (\mathtt{i} + 1) = z - 1$):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\{\mathtt{n} - (\mathtt{i}+1) = z - 1\}\ \texttt{s = s + i + 1;}\ \{\alpha\}}\,(\text{Zuw}) \quad \dfrac{}{\{\alpha\}\ \texttt{i = i + 1;}\ \{\mathtt{n} - \mathtt{i} = z - 1\}}\,(\text{Zuw})}{\{\mathtt{n} - (\mathtt{i}+1) = z - 1\}\ \texttt{s = s + i + 1; i = i + 1;}\ \{\mathtt{n} - \mathtt{i} = z - 1\}}\,(\text{Seq})}{\{\mathtt{n} - \mathtt{i} = z\}\ \texttt{s = s + i + 1; i = i + 1;}\ \{\mathtt{n} - \mathtt{i} = z - 1\}}\,(\text{Abschw})}{\{I \wedge \mathtt{i} \neq \mathtt{n} \wedge \mathtt{n} - \mathtt{i} = z\}\ \texttt{s = s + i + 1; i = i + 1;}\ \{\mathtt{n} - \mathtt{i} < z\}}\,(\text{Abschw})}{\mathbf{F_t} \equiv \{I \wedge \mathtt{i} \neq \mathtt{n} \wedge \mathtt{n} - \mathtt{i} = z\}\ \texttt{\{s = s + i + 1; i = i + 1;\}}\ \{\mathtt{n} - \mathtt{i} < z\}}\,(\text{Block})$$

Damit können wir die Regel für totale Korrektheit anwenden:

$$\dfrac{\dfrac{\mathbf{F_t} \qquad \mathbf{F_p}}{\left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j\right\}\ P\ \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \neg(\mathtt{i} \neq \mathtt{n})\right\}}\,(\text{Iteration}_{\text{total}})}{\{\mathtt{s} = 0 \wedge \mathtt{i} = 0 \wedge \mathtt{n} > 0\}\ \mathtt{P}\ \left\{\mathtt{s} = \sum_{j=0}^{\mathtt{n}} j\right\}}\,(\text{Abschw})$$

Es lohnt sich, die letzte Abschwächungsregel noch einmal genau zu betrachen: Sie darf angewendet werden, weil sowohl

$$\mathtt{s} = 0 \wedge \mathtt{i} = 0 \wedge \mathtt{n} > 0 \implies \mathtt{s} = \sum_{j=0}^{\mathtt{i}} j$$

als auch

$$\mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \neg(\mathtt{i} \neq \mathtt{n}) \implies \mathtt{s} = \sum_{j=0}^{\mathtt{i}} j \wedge \mathtt{i} = \mathtt{n} \implies \mathtt{s} = \sum_{j=0}^{\mathtt{n}} j$$

gelten, wie sich leicht nachrechnen lässt.

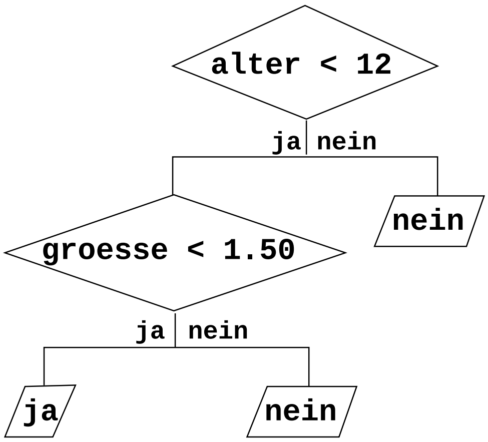
Aufgabe 3-3 **Kontrollflussdiagram** (`kindersitz.{ps,pdf,jpg,png}`, 4 Punkte)

Gegeben sei folgende Regelung:

> Kinder unter 12 Jahren müssen in einem altersgerechten Kindersitz (wörtlich: "amtlich genehmigte Rückhalteeinrichtung") sitzen, ausser wenn sie bereits 1,50 Meter oder größer sind. Dabei ist auch der vorgesehene Sicherheitsgurt anzulegen.

Erstellen Sie ein Kontrollflussdiagramm, welches anhand von Alter und Größe einer Person entscheidet, ob ein Kindersitz notwendig ist.

Lösung:



Abgabe: Per UniWorx, bis spätestens Montag, den 22.5.2006 um 9:00 Uhr.