7. Übung zur
Konstruktion fehlerfreier Software

Frank Pilhofer

Montag 13-14 Uhr

0. Satz formulieren

Am Ende des Programmstücks wird die Schleifenvariable i wieder gelöscht, daher können in der Postbedingung keine Aussagen über diese Variable mehr gemacht werden. Die einzig mögliche Aussage ist $sum = \sum_{i=1}^{n} x(i)$.

Insgesamt läßt sich folgender Satz beweisen:

$$\left\{n \in N \wedge \forall_{i=1}^{n} : x(i) \in R\right\} P \left\{sum = \sum_{i=1}^{n} x(i) \wedge n \in N \wedge \forall_{i=1}^{n} : x(i) \in R\right\}$$

wobei P das Programmsegment ist.

1. Satz beweisen

Zunächst wird das Programmstück in drei Teile zerlegt, die Initialisierung, die Schleife und das Schlußstück:

P_1 : declare (*sum*,*R*,0); declare (*i*,*Z*,0)
P_2 : while $i<n$ do $i:=i+1$; $sum=sum+x(i)$ endwhile
P_3 : release *i*

1. Schritt (Initialisierung): Zu beweisen ist

$$\left\{n \in N \wedge \forall_{i=1}^{n} : x(i) \in R\right\} P_1 \left\{sum = \sum_{j=1}^{i} x(j) \wedge 0 \le i \le n \wedge i \in Z \wedge n \in N\right\}$$

Es ist

$$\begin{aligned}
&\left(\text{declare}(sum, R, 0); \text{declare}(i, Z, 0)\right).\left\{n \in N \wedge \forall_{i=1}^{n} : x(i) \in R\right\} \\
= \quad &\left(\text{declare}(i, Z, 0)\right).\left\{n \in N \wedge \forall_{i=1}^{n} : x(i) \in R \wedge sum \in R \wedge sum = 0\right\} \\
= \quad &\left\{n \in N \wedge \forall_{i=1}^{n} : x(i) \in R \wedge sum \in R \wedge sum = 0 \wedge i \in Z \wedge i = 0\right\} \\
\Rightarrow \quad &\left\{n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\}
\end{aligned}$$

2. Schritt (Durchlauf der Schleife). Zu beweisen ist $\{B \wedge I\} S \{I\}$, also

$$\left\{B \wedge n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\} S \left\{n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\}$$

Es ist

$$\begin{aligned}
&\left(i := i+1; sum := sum + x(i)\right).\left\{i < n \wedge n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\} \\
= \quad &\left(i := i+1; sum := sum + x(i)\right).\left\{n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i < n\right\} \\
= \quad &\left(sum := sum + x(i)\right).\left\{n \in N \wedge sum = \sum_{j=1}^{i-1} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\} \\
= \quad &\left\{n \in N \wedge sum = x(i) + \sum_{j=1}^{i-1} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\} \\
= \quad &\left\{n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\}
\end{aligned}$$

3. Schritt (Terminieren der Schleife). Zu beweisen ist $\{I \wedge \overline{B}\} \Rightarrow P$, also

$$\left\{\overline{B} \wedge n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\} \Rightarrow \left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\}$$

Es ist

$$\begin{aligned}
&\left\{\overline{i < n} \wedge n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\} \\
= \quad &\left\{i \ge n \wedge n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\} \\
= \quad &\left\{i = n \wedge n \in N \wedge sum = \sum_{j=1}^{i} x(j) \wedge i \in Z\right\} \\
= \quad &\left\{i = n \wedge n \in N \wedge sum = \sum_{j=1}^{n} x(j) \wedge i \in Z\right\} \\
\Rightarrow \quad &\left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\}
\end{aligned}$$

Aus den Schritten 1, 2 und 3 folgt mit Beweisregel (W2):

$$\{n \in N\}(P_1; P_2)\left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\}$$

4. Schritt (Abschluß)

Es bleibt zu zeigen: $\left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j) \wedge i \in Z \wedge 0 \le i \le n\right\} P_3 \left\{sum = \sum_{i=1}^{n} x(i) \wedge n \in N\right\}$

Die release-Anweisung löscht alle Informationen über i und läßt alle anderen Variablen unverändert. Der eben genannte Satz gilt daher.

5. Schritt (qed)

Aus dem Schluß nach Schritt 3 und Schritt 4 folgt mit Beweisregel F1:

$$\{n \in N\}(P_1; P_2; P_3) = W\left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j)\right\}$$

womit die Korrektheit des Programmsegments bewiesen ist.

2. Umfassende Vorbedingung

Gesucht ist eine umfassende Vorbedingung zu $\{V\}P\left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j)\right\}$.

Es ist $\left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j)\right\} P_3 \left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j)\right\}$ und

$$\left\{n \in N \wedge \left(\left(i \ge n \wedge sum = \sum_{j=1}^{n} x(j)\right) \vee \left(0 \le i < n \wedge sum = \sum_{j=1}^{i} x(j)\right)\right)\right\} P_2 \left\{n \in N \wedge sum = \sum_{j=1}^{n} x(j)\right\}$$

und $\{n \in N\} P_1 \left\{n \in N \wedge \left(\left(i \ge n \wedge sum = \sum_{j=1}^{n} x(j)\right) \vee \left(0 \le i < n \wedge sum = \sum_{j=1}^{i} x(j)\right)\right)\right\}$, daher ist $\{n \in N\}$ eine umfassende Vorbedingung zur obigen Postbedingung.