9. Übung zur
Konstruktion fehlerfreier Software

Frank Pilhofer

Montag 13-14 Uhr

Verifikation einer Korrektheitsaussage

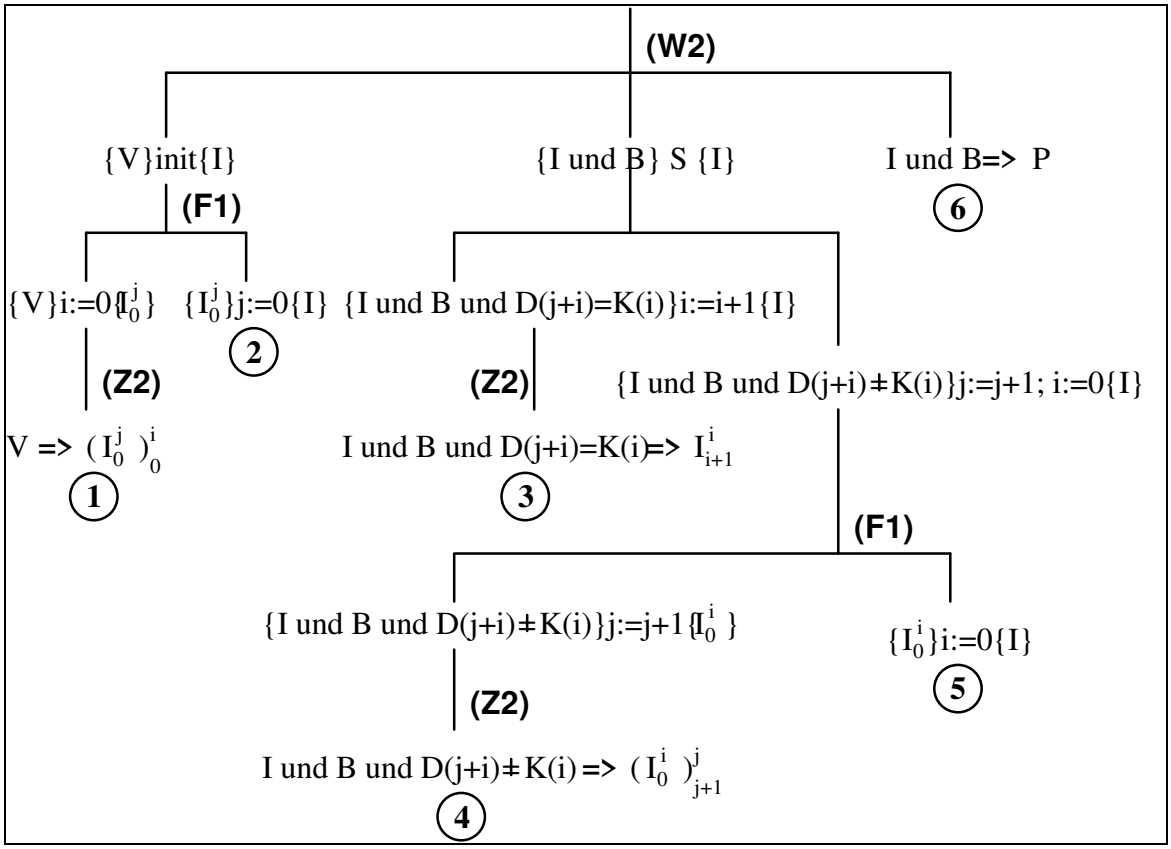
```
{V}
i:=0; j:=0
while i<n und j≤M-N do
      if D(j+i)=K(i) then i:=i+1 else j:=j+1; i:=0 endif
invariant I
endwhile
{P}
```

V: $N, M \in Z \text{ und } 0 \le N \le M+1$

P: $\begin{cases} N, M, j \in Z \wedge \wedge_{k=0}^{j-1}\left(\vee_{a=0}^{N-1} D(k+a) \neq K(a)\right) \wedge \\ j = M-N+1 \vee 0 \le j \le M-N \wedge \wedge_{a=0}^{i-1} D(j+a) = K(a) \end{cases}$

I: $\begin{cases} N, M, j, i \in Z \wedge 0 \le i \le N \wedge \wedge_{k=0}^{j-1}\left(\vee_{a=0}^{N-1} D(k+a) \neq K(a)\right) \wedge \\ j = M-N+1 \vee 0 \le j \le M-N \wedge \wedge_{a=0}^{i-1} D(j+a) = K(a) \end{cases}$

Aufteilung in Einzelimplikationen



Nun müssen die Einzelimplikationen bewiesen werden.

①

Es ist I_0^j = $\begin{cases} N,M,0,i \in Z \wedge 0 \le i \le N \wedge \\ \left(0 = M-N+1 \vee 0 \le M-N \wedge \wedge_{a=0}^{i-1} D(a) = K(a)\right) \end{cases}$

und $\left(I_0^j\right)_0^i$ = $\begin{cases} N,M \in Z \wedge 0 \le N \wedge \\ \left(0 = M-N+1 \vee 0 \le M-N\right) \end{cases}$

= $\begin{cases} N,M \in Z \wedge 0 \le N \wedge \\ \left(N = M+1 \vee N \le M\right) \end{cases}$ = $N,M \in Z \wedge 0 \le N \le M+1$

= V

②

gilt sofort nach (Z2)

③

Es ist $I \wedge i < N \wedge j \le M-N \wedge D(j+i) = K(i)$

= $\begin{cases} N,M,j,i \in Z \wedge 0 \le i < N \wedge \wedge_{k=0}^{j-1}\left(\vee_{a=0}^{N-1} D(k+a) \ne K(i)\right) \wedge \\ \left(0 \le j \le M-N \wedge \wedge_{a=0}^{i}\left(D(j+a) = K(a)\right)\right) \end{cases}$

= $\begin{cases} N,M,j,i \in Z \wedge 1 \le i+1 \le N \wedge \wedge_{k=0}^{j-1}\left(\vee_{a=0}^{N-1} D(k+a) \ne K(i)\right) \wedge \\ \left(0 \le j \le M-N \wedge \wedge_{a=0}^{i}\left(D(j+a) = K(a)\right)\right) \end{cases}$

$\Rightarrow$

= $\begin{cases} N,M,j,i+1 \in Z \wedge 0 \le i+1 \le N \wedge \wedge_{k=0}^{j-1}\left(\vee_{a=0}^{N-1} D(k+a) \ne K(a)\right) \wedge \\ \left(j = M-N+1 \vee 0 \le j \le M-N \wedge \wedge_{a=0}^{i}\left(D(j+a) = K(a)\right)\right) \end{cases}$

= I_{i+1}^i

④

Es ist I_0^i

= $\begin{cases} N,M,0,j \in Z \wedge 0 \le N \wedge \wedge_{k=0}^{j-1}\left(\vee_{a=0}^{N-1} D(k+a) \ne K(a)\right) \wedge \\ \left(j = M-N+1 \vee 0 \le j \le M-N\right) \end{cases}$

und daher ist $\left(I_0^i\right)_{j+1}^j$

= $\begin{cases} N,M,0,j+1 \in Z \wedge 0 \le N \wedge \wedge_{k=0}^{j}\left(\vee_{a=0}^{N-1} D(k+a) \ne K(a)\right) \wedge \\ j+1 = M-N+1 \vee 0 \le j+1 \le M-N \end{cases}$

= $\begin{cases} N,M,j \in Z \wedge 0 \le N \wedge \wedge_{k=0}^{j}\left(\vee_{a=0}^{N-1} D(k+a) \ne K(a)\right) \wedge \\ -1 \le j \le M-N \end{cases}$

Auf der anderen Seite ist $I \wedge i < N \wedge j \le M-N \wedge D(j+i) \ne K(i)$

= $\begin{cases} N,M,i,j \in Z \wedge 0 \le i \wedge 0 \le N \wedge i < N \wedge \wedge_{k=0}^{j}\left(\vee_{a=0}^{N-1} D(k+a) \ne K(a)\right) \wedge \\ 0 \le j \le M-N \wedge \wedge_{a=0}^{i-1} D(j+a) = K(a) \end{cases}$

$\Rightarrow$ $\left(I_0^i\right)_{j+1}^j$

⑤

gilt sofort nach (Z2)

⑥

Es gilt $I \wedge \overline{B} \Rightarrow I$. Nun ist

$$
\begin{array}{lll}
I & = & \left\{ \begin{array}{l} N, M, j, i \in Z \wedge 0 \le i \le N \wedge \wedge_{k=0}^{j-1} \left(\vee_{a=0}^{N-1} D(k+a) \neq K(a) \right) \wedge \\ \quad j = M - N + 1 \vee 0 \le j \le M - N \wedge \wedge_{a=0}^{i-1} D(j+a) = K(a) \end{array} \right. \\
& \Rightarrow & \left\{ \begin{array}{l} \quad N, M, j \in Z \wedge \wedge_{k=0}^{j-1} \left(\vee_{a=0}^{N-1} D(k+a) \neq K(a) \right) \wedge \\ j = M - N + 1 \vee 0 \le j \le M - N \wedge \wedge_{a=0}^{i-1} D(j+a) = K(a) \end{array} \right. \\
& = & P
\end{array}
$$

Damit ist die Korrektheit des gesamten Programmstücks gezeigt.

Zu den Fragen:
3. Die Implikationen der Teilschritte ①, ② und ⑤ sind äquivalent, die anderen nicht.
4. Solche Programmstücke suchen eine bestimmte Teilkette in einer langen Kette.