

Diskrete Mathematik

Teil Verifikation

Sebastian Iwanowski
FH Wedel

Kap. 3: Verifikation von Schleifen

Verifikation und Konstruktion von Schleifen

Definition einer Schleife:

```
while Schleifenbedingung do  
    Rumpfanweisung
```

Schleifenbedingung muss eine **logische** Funktion sein, die nur von Variablen abhängen darf, die mit Werten belegt sind.

Funktionsweise:

- 1) Zunächst wird **Schleifenbedingung** ausgewertet.
- 2) Wenn **Schleifenbedingung** falsch ist, wird die Schleife sofort beendet.
Wenn **Schleifenbedingung** wahr ist, wird **Rumpfanweisung** ausgeführt.
Dann wird bei Schritt 1) fortgefahren.

Verifikation von Schleifen

Verifikationstechnik:

W	{	<pre> {Vorbedingung} while Schleifenbedingung do {Eintrittsbedingung} Rumpfanweisung {Austrittsbedingung} {Nachbedingung} </pre>	φ β φ_i S ψ_i ψ
---	---	--	---

Definition:

Es sei φ_i die Eintrittsbedingung vor der i-ten Ausführung der Rumpfanweisung und ψ_i die Austrittsbedingung nach der i-ten Ausführung der Rumpfanweisung. Die Schleife werde nach k Ausführungen beendet.

Dann gilt:

- 1) $\varphi_1 \Leftrightarrow \varphi \wedge \beta$ $\{\varphi_1\}$ Rumpfanweisung $\{\psi_1\}$
- 2) $\varphi_2 \Leftrightarrow \psi_1 \wedge \beta$ $\{\varphi_2\}$ Rumpfanweisung $\{\psi_2\}$
- .
- i) $\varphi_i \Leftrightarrow \psi_{i-1} \wedge \beta$ $\{\varphi_i\}$ Rumpfanweisung $\{\psi_i\}$
- .
- k) $\varphi_k \Leftrightarrow \psi_{k-1} \wedge \beta$ $\{\varphi_k\}$ Rumpfanweisung $\{\psi_k\}$
- k+1) $\psi \Leftrightarrow \psi_k \wedge \neg\beta$ $\{\varphi_k\}$ Rumpfanweisung $\{\psi_k\}$

Problem:

Es ist unklar, wie groß k ist, d.h. wie viele Zwischenbedingungen φ_i und ψ_i es gibt.

Verifikation von Schleifen

Verifikationstechnik:

W	{	{Vorbedingung}	φ
		while Schleifenbedingung do	β
		{Eintrittsbedingung}	φ_i
		Rumpfanweisung	S
		{Austrittsbedingung}	ψ_i
		{Nachbedingung}	ψ

Gegeben ψ , berechne φ : Wie findet man die **schwächste** Vorbedingung P für φ ?

Beobachtung:

- 0) Sei P_0 die schwächste Vorbedingung, falls die Schleife gar nicht durchlaufen wird.
- 1) Sei P_1 die schwächste Vorbedingung, falls die Schleife genau einmal durchlaufen wird.
- i) Sei P_i die schwächste Vorbedingung, falls die Schleife genau i-mal durchlaufen wird.

Lösung: Dann gilt: $P = P_0 \vee P_1 \vee \dots \vee P_i \vee \dots$

potentiell unendlich viele!

Problem: Im allgemeinen Fall könnten sich die P_i 's alle unterscheiden !

Damit kann keine allgemeine Lösungstechnik angegeben werden !

Verifikation von Schleifen

Verifikationstechnik:

	{Vorbedingung}	φ
W	while Schleifenbedingung do	β
	{Eintrittsbedingung}	φ_i
	Rumpfanweisung	S
	{Austrittsbedingung}	ψ_i
	{Nachbedingung}	ψ

Aufgaben, die bei Zuweisungen und Verzweigungen gelöst wurden:

Berechnung der schwächsten Vorbedingung: Gegeben ψ , berechne φ

Berechnung der stärksten Nachbedingung: Gegeben φ , berechne ψ

Das ist hier zu schwierig !

Einfachere Aufgabe:

Gegeben φ und ψ :

Beweise, dass gilt: $\{\varphi\} W \{\psi\} !$

Verifikation von Schleifen

Wesentliche Schritte bei der Verifikation von Schleifen:

Invariantenbestimmung (Hauptarbeit):

- 1) **Beweise eine Aussage über den Wert der Schleifenvariablen nach Durchlauf der Schleife in Abhängigkeit von der Durchlaufzahl i .**

Variantenbestimmung (meist leichte, aber wichtige Zusatzarbeit):

- 2) **Beweise, dass die Schleife irgendwann zum Ende kommt.**

Folgerung (meist unmittelbar):

- 3) **Die Nachbedingung ψ ergibt sich aus dem Belegungswert der Variablen (1), wenn die Schleife zum Ende gekommen ist (2)**

Verifikation von Schleifen

Wesentliche Schritte bei der Verifikation von Schleifen:

Invariantenbestimmung (Hauptarbeit):

1) Beweise eine Aussage über den Wert der Schleifenvariablen nach Durchlauf der Schleife in Abhängigkeit von der Durchlaufzahl i .

Beweistechnik: Vollständige Induktion über i :

Seien x_1, \dots, x_j die Variablen, die in der Rumpfanweisung verändert werden:

- a) Unterscheide die Belegungswerte dieser Variablen nach i bzw. $i+1$ Schleifendurchläufen:
 x_{1i}, \dots, x_{ji} ist der Wert nach i Schleifendurchläufen.
 $x_{1,i+1}, \dots, x_{j,i+1}$ ist der Wert nach $i+1$ Schleifendurchläufen.
- b) Setze die verschiedenen Belegungszustände in Beziehung zueinander (gemäß Programm), verwende die Induktionsannahme für i und folgere die Induktionsbehauptung für $i+1$

*Die Bedingungen für die Belegungswerte heißen **Invariante** der Schleife.*

Verifikation von Schleifen

Wesentliche Schritte bei der Verifikation von Schleifen:

Variantenbestimmung (meist leichte, aber wichtige Zusatzarbeit):

2) **Beweise, dass die Schleife irgendwann zum Ende kommt.**

Hierfür muss β vom Belegungswert mindestens einer der Variablen x_1, \dots, x_j abhängen!
*Eine solche Variable heißt **Variante** der Schleife.*

Folgerung (meist unmittelbar):

3) **Die Nachbedingung ψ ergibt sich aus dem Belegungswert der Variablen (1), wenn die Schleife zum Ende gekommen ist (2)**

Das ergibt sich in der Regel unmittelbar, weil die Invariantenbedingungen in 1) entsprechend formuliert werden.

Regelfall: In ψ wird eine Aussage über den Belegungszustand von in der Schleife veränderten Variablen gemacht.

Sonderfall: Falls in ψ noch andere Zusammenhänge gefordert werden, sollte das in 1) und 2) vorbereitet werden, indem weitere Hilfsgrößen definiert werden.