Kapitel L:V

V. Erweiterungen und Anwendungen zur Logik

Terminierung

Der Nachweis der totalen Korrekheit eines Programms erfordert neben der bisher betrachteten partiellen Korrektheit den Nachweis seiner Terminierung des Programmes.

Wann ist Terminierung ein Problem?

- In Zuweisungen, falls der arithmetische Ausdruck nicht berechenbar ist (z.B. Division durch 0, nicht initialisierte Variable),
- in bedingten Anweisungen, falls die Bedingung nicht entschieden werden kann oder falls die Anweisungen im *then*-Teil oder im *else*-Teil nicht terminieren,
- in Anweisungsfolgen, falls eine Anweisung darin nicht terminiert,
- aber vor allem in Schleifen.

➜ Wir beschränken uns auf Terminierungsbeweise für Schleifen.

Bemerkungen:

- Ausser in Schleifen kann die Terminierung garantiert werden, indem man die Art der arithmetischen oder booleschen Ausdrücke auf einfache Formen beschränkt (Addition, Subtraktion von 1, also $x := x + 1;$ und Test auf 0, also $\texttt{if}\ (x = 0) \ldots$).

Terminierung

Terminierung von Schleifen

Eine Schleife

$$\texttt{while}\ (B)\ \texttt{do}\ S$$

terminiert unter der Vorbedingung P genau dann, wenn jede Ausführung von S terminiert und wenn eine Invariante I_T der Schleife existiert und ein ganzzahliger arithmetischer Ausdruck T existiert, so dass folgende Aussagen gelten:

1. $\{P\} \Rightarrow \{I_T\}$ ist gültige Abschwächung.
2. $\{T \leq 0$ *und* $I_T\} \Rightarrow \{$*nicht* $B\}$ ist gültige Abschwächung.
3. $\{T = t + 1$ *und* I_T *und* $B\}\ S\ \{T = t$ *und* $I_T\}$ ist gültige Hoare-Formel.

t ist ein Bezeichner für eine ganzzahlige Variable, die weder in T noch in der Schleife vorkommt, d.h. nicht in B und nicht in S.

T heißt auch Terminierungsfunktion oder *Variante* der Schleife.

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife

Schleife:

$\{a, b \in \mathbf{Z}$ *und* $x = a$ *und* $y = b$ *und* $a \geq 0\} = \{P\}$

```
while (x > 0) do
   begin
      x := x − 1;
      y := y + 1;
   end
```

Invariante I: $(x, y \in \mathbf{Z}$ *und* $x + y = a + b$ *und* $x \geq 0)$ (für part. Korrektheit)
Invariante I_T: $(x, y \in \mathbf{Z})$
Schleifenbedingung B: $(x > 0)$
Ganzzahliger Ausdruck T: x

Nachweis: $\{P\} \quad \Rightarrow \quad \{I_T\}$ ✓

Nachweis: $\{T \leq 0$ *und* $I_T\} \quad \Rightarrow \quad \{$*nicht* $B\}$ ✓

Nachweis: T ganzzahlig wegen Invariante ✓

Bemerkungen:

- Für eine Schleife

```
while (x > 25) do
   begin
      x := x - 1;
      y := y + 1;
   end
```

  wählt man als ganzzahligen Ausdruck T: $x - 25$

  Wichtig ist die Existenz einer unteren Schranke für T und das streng monotone Fallen des Wertes von T mit jedem Schleifendurchlauf.

- Als Invariante für die Terminierung kann häufig die Invariante (oder ein Teil hiervon) aus dem Nachweis der partiellen Korrektheit gewählt werden. Mit ihr läßt sich meist sofort die Beschränktheit der Werte der Variante T nachweisen.

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife (Fortsetzung)

Nachweis der Invarianz von I_T und der Dekrementierung von T

$\{a, b \in \mathbf{Z}$ *und* $x = a$ *und* $y = b$ *und* $a \geq 0\}$

```
while (x > 0) do
  begin
    x := x - 1;
    y := y + 1;
  end
```

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife (Fortsetzung)

Nachweis der Invarianz von I_T und der Dekrementierung von T

$\{a, b \in \mathbf{Z}$ *und* $x = a$ *und* $y = b$ *und* $a \geq 0\}$

$\Rightarrow \{x, y \in \mathbf{Z}\}$

`while` $(x > 0)$ `do`

$\{x = t + 1$ *und* $x, y \in \mathbf{Z}$ *und* $x > 0\}$

`begin`

$\{x = t + 1$ *und* $x, y \in \mathbf{Z}$ *und* $x > 0\}$

$x := x - 1;$

$y := y + 1;$

$\{x = t$ *und* $x, y \in \mathbf{Z}\}$

`end`

$\{x = t$ *und* $x, y \in \mathbf{Z}\}$

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife (Fortsetzung)

Nachweis der Invarianz von I_T und der Dekrementierung von T

$\{a, b \in \mathbf{Z}$ *und* $x = a$ *und* $y = b$ *und* $a \geq 0\}$

$\Rightarrow \{x, y \in \mathbf{Z}\}$

`while` $(x > 0)$ `do`

$\{x = t + 1$ *und* $x, y \in \mathbf{Z}$ *und* $x > 0\}$

`begin`

$\{x = t + 1$ *und* $x, y \in \mathbf{Z}$ *und* $x > 0\}$

$\Rightarrow \{x - 1 = t$ *und* $(x - 1), y \in \mathbf{Z}\}$

$x := x - 1;$

$\{x = t$ *und* $x, y \in \mathbf{Z}\}$

$\Rightarrow \{x = t$ *und* $x, (y + 1) \in \mathbf{Z}\}$

$y := y + 1;$

$\{x = t$ *und* $x, y \in \mathbf{Z}\}$

`end`

$\{x = t$ *und* $x, y \in \mathbf{Z}\}$

Terminierung

Formaler Nachweis der Terminierung von Schleifen

- Insgesamt sind fünf Nachweise erforderlich:
  1. (Terminierung des Schleifenrumpfes)
  2. Folgerbarkeit einer Invarianten I_T aus der Vorbedingung der Schleife
  3. Ganzzahligkeit von T
  4. Folgerbarkeit der Nicht-Gültigkeit der Schleifenbedingung aus $T \leq 0$ und der Invarianten I_T
  5. Nachweis der Invarianz von I_T und Nachweis der Dekrementierung von T

  Für (2) und (5) sind Herleitungen anzugeben, (3) muss aus I_T gefolgert werden.

- Die Invariante I_T muss nicht mit der Invarianten für den Nachweis der partiellen Korrektheit der Schleife übereinstimmen, häufig sind sie aber sehr ähnlich.

Beachte:

Die Gestalt der Hoare-Regel für die Schleife erlaubt keinen gleichzeitigen Nachweis von partieller Korrektheit und Terminierung.

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife

Gegeben sei das folgende Programm mit den angegebenen Vor- und Nachbedingungen:

$\{n \in \mathbf{N}_0\}$

```
begin
    i := 0;
    x := 0;
    {n ∈ N_0 und i = 0 und x = 0}
    while (i < n) do
        begin
            i := i + 1;
            x := x + i;
        end
end
```

$\{n \in \mathbf{N}_0$ *und* $x = \sum_{i=0}^{n} i\}$

Prüfen Sie, ob die Schleife terminiert.

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife (Fortsetzung)

Kandidaten für Variante T:
i, x oder arithmetische Ausdrücke hiermit, da nur sie in der Schleife verändert werden.

Kandidat $T = n - i$

- Nachweis der Abschwächung von $\{T \leq 0$ *und* $I_T\}$ zu $\{$*nicht* $B\}$:

  $\{n - i \leq 0\} \Rightarrow \{$*nicht* $i < n\}$ ✓

  Eine Invariante wird hier also außer für die Ganzzahligkeit gar nicht benötigt.

- Nachweis der Ganzzahligkeit ➜ Invariante

  T ganzzahlig, da mit n initialisiert durch Vorbedingung und $i := 0;$ und T nur durch $i := i + 1;$ in der Schleife verändert.

  Also Invariante I_T: $(n, i \in \mathbf{N}_0)$

  I_T ist Teil der Invarianten $\{n, i \in \mathbf{N}_0$ *und* $i \leq n$ *und* $x = \frac{1}{2}i(i+1)\}$ aus dem Nachweis der partiellen Korrektheit. Dadurch kann der Nachweis für die partielle Korrektheit für den Nachweis der Terminierung teilweise recycled werden. Das erleichtert die Arbeit!

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife (Fortsetzung)

- Verifikation von S mit Vorbedingung $\{T = t + 1$ *und* I_T *und* $B\}$ zur Nachbedingung $\{T = t$ *und* $I_T\}$
  (t bezeichnet eine Variable, die nicht im Programm vorkommt)

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

while $(i < n)$ do

  begin

    $i := i + 1;$

    $x := x + i;$

  end

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife (Fortsetzung)

- Verifikation von S mit Vorbedingung $\{T = t + 1$ *und* I_T *und* $B\}$ zur Nachbedingung $\{T = t$ *und* $I_T\}$
  (t bezeichnet eine Variable, die nicht im Programm vorkommt)

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

$\Rightarrow \{n, i \in \mathbf{N}_0\}$

`while` $(i < n)$ `do`

$\{n - i = t + 1$ *und* $n, i \in \mathbf{N}_0$ *und* $i < n\}$

`begin`

$\{n - i = t + 1$ *und* $n, i \in \mathbf{N}_0$ *und* $i < n\}$

$i := i + 1;$

$x := x + i;$

$\{n - i = t$ *und* $n, i \in \mathbf{N}_0\}$

`end`

$\{n - i = t$ *und* $n, i \in \mathbf{N}_0\}$

Terminierung

Beispiel für den Nachweis der Terminierung einer Schleife (Fortsetzung)

- Verifikation von S mit Vorbedingung $\{T = t + 1$ *und* I_T *und* $B\}$ zur Nachbedingung $\{T = t$ *und* $I_T\}$
  (t bezeichnet eine Variable, die nicht im Programm vorkommt)

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$
$\Rightarrow \{n, i \in \mathbf{N}_0\}$
`while` $(i < n)$ `do`
  $\{n - i = t + 1$ *und* $n, i \in \mathbf{N}_0$ *und* $i < n\}$
  `begin`
    $\{n - i = t + 1$ *und* $n, i \in \mathbf{N}_0$ *und* $i < n\}$
    $\Rightarrow \{n - (i + 1) = t$ *und* $n, (i + 1) \in \mathbf{N}_0\}$
    $i := i + 1;$
    $\{n - i = t$ *und* $n, i \in \mathbf{N}_0\}$
    $x := x + i;$
    $\{n - i = t$ *und* $n, i \in \mathbf{N}_0\}$
  `end`
  $\{n - i = t$ *und* $n, i \in \mathbf{N}_0\}$

Damit folgt insgesamt, dass die Schleife terminiert.

Terminierung

Informeller Nachweis der Terminierung von Schleifen

Auch dieser Nachweis verwendet einen Ausdruck T über den Variablen des Programms als Variante.

- Insgesamt sind vier Nachweise erforderlich:
  1. (Terminierung des Schleifenrumpfes)
  2. Ganzzahligkeit von T
  3. Dekrementierung (bzw. Inkrementierung) von T in jedem Schleifendurchlauf
  4. Nachweis von Schranken für T (z.B. $\{T \geq \text{bound}\}$ ist invariant), aus deren Verletzung auch die Verletzung der Schleifenbedingung folgt.

  Für (2),(3),(4) wird informell mit Ganzzahligkeit von Variablen und Veränderungen durch Anweisungen des Programmstückes argumentiert. Für (4) wird die Invariante aus dem Nachweis der partiellen Korrektheit ausgenutzt.

➜ Sind die beiden Formulierungen gleichwertig?

Bemerkungen:

- Für in den Werten streng monoton fallende Ausdrücke T benötigt man natürlich nur eine untere Schranke, für in den Werten streng monoton wachsende Ausdrücke T eine oberen Schranke.
- Dieser Nachweis wird im Teil der Inkrementierung von T weniger streng formal durchgeführt und ebenso im Bereich der Folgerbarkeit der Ungültigkeit der Schleifenbedingung bei Überschreiten der Schranke.

Terminierung

Beispiel für den alternativen Nachweis der Terminierung einer Schleife

Gegeben sei das folgende Programm mit den angegebenen Vor- und Nachbedingungen:

$\{n \in \mathbf{N}_0\}$

```
begin
    i := 0;
    x := 0;
    {n ∈ N_0 und i = 0 und x = 0}
    while (i < n) do
        begin
            i := i + 1;
            x := x + i;
        end
end
```

$\{n \in \mathbf{N}_0$ *und* $x = \sum_{i=0}^{n} i\}$

Prüfen Sie, ob die Schleife terminiert.

Terminierung

Beispiel für den alternativen Nachweis der Terminierung einer Schleife (Fortsetzung)

Kandidat für die Variante: $T = i$

- T ist ganzzahlig, da i mit 0 in $i := 0;$ initialisiert und nur durch $i := i + 1;$ in der Schleife verändert wird.
- T wächst mit jedem Durchlauf durch den Schleifenrumpf um den Wert 1, da i im Schleifenrumpf nur durch $i := i + 1;$ verändert wird.
- (T ist nach unten beschränkt wegen Zusicherung $i = 0$ vor und Inkrementierung von i in der Schleife.)

  T ist nach oben beschränkt durch n, da $n \geq i$ Teil der Invariante aus dem Nachweis der partiellen Korrektheit ist und n unverändert bleibt.

  Die Verletzung der Schleifenbedingung bei Überschreiten von n durch T ist offensichtlich.

➜ Damit folgt insgesamt, dass die Schleife terminiert.

Bemerkungen:

- T muss hier nicht so eingeschränkt gewählt werden. Durch Subtraktion der Variante vom Maximalwert bei monoton wachsenden Ausdrücken oder des Minimalwertes von der Variante bei monoton fallenden Ausdrücken kann man eine Variante mit den alten Anforderungen herstellen.
- Anstelle einer formalen Herleitung wird hier durch *Hinschauen* die kontinuierliche Veränderung von T nachgewiesen.
- Auf einen Nachweis, dass bei Erreichen der Schranken durch T die Schleifenbedingung nicht mehr erfüllt wird, kann man häufig ganz verzichten. Die Variante und ihre Schranke können in solchen Fällen so gewählt werden, dass sie die Schleifenbedingung bilden.
- Für den Nachweis der Beschränktheit von T nutzt man intensiv die Invariante aus dem Beweis der partiellen Korrektheit und argumentiert mit offensichtlichen Eigenschaften.
- Grundsätzlich ist dieser alternative Nachweis also unter Verwendung der Invarianten der partiellen Korrektheit ein vollständiger Nachweis der Terminierung. Er ist weniger formal, da auf exakte Begründungen verzichtet wird und Überzeugung durch Augenschein an die Stelle tritt.

Terminierung

Terminierung: Ein Problem?

- Manche Schleifen terminieren immer!

$\{a > 0$ *und* $b > 0\}$

`while` $(a \neq b)$ `do`

  `begin`

    `while` $(a > b)$ `do`

      $a := a - b;$

    `while` $(b > a)$ `do`

      $b := b - a;$

  `end`

Terminierung

Terminierung: Ein Problem?

- Manche Schleifen terminieren immer!

$\{a > 0$ *und* $b > 0\}$

```
while (a ≠ b) do
   begin
      while (a > b) do
         a := a − b;
      while (b > a) do
         b := b − a;
   end
```

- Manche Schleifen terminieren nicht immer!

$\{a > 0$ *und* $b > 0\}$

```
while (a ≠ b) do
   begin
      while (a ≥ b) do
         a := a − b;
      while (b > a) do
         b := b − a;
   end
```

Terminierung

Terminierung: Ein Problem? (Fortsetzung)

- Für manche Schleifen ist nicht bekannt, ob sie terminieren!

  $\{n \in \mathbf{N}$ *und* $n > 0$ *und* $x = n\}$

  $\texttt{while}\ (x \neq 1)\ \texttt{do}$

  $\quad \texttt{if}\ (x\ \text{gerade})\ \texttt{then}$

  $\quad\quad x := x/2;$

  $\quad \texttt{else}$

  $\quad\quad x := 3 * x - 1;$

  (Collatz-Problem)

➜ Die Frage nach der Terminierung von Schleifen ist unentscheidbar.

Bemerkungen:

- Das Collatz-Problem betrifft Zahlenfolgen, die nach einem einfachen Bildungsgesetz konstruiert werden:

  1. Beginne mit irgendeiner natürlichen Zahl $n > 0$.
  2. Ist n gerade, so nimm als nächste Zahl $n/2$.
  3. Ist n ungerade, so nimm als nächste Zahl $3n + 1$.

  Die so erhaltenen Zahlenfolgen endeten bei allen getesteten Auswahlen für n in dem Zyklus 4,2,1.

  Die Collatz-Vermutung lautet daher:

  > Jede so konstruierte Zahlenfolge endet im Zykel 4,2,1 egal, mit welcher positiven natürlichen Zahl man beginnt.

  Aufgrund des Bildungsgesetzes für die Zahlenfolge nennt man diese Vermutung auch die (3n + 1)-Vermutung. Die im Schleifenrumpf berechnete Funktion in x heißt Ulam's Funktion.
  [Wikipedia, 2009]

- Für den Nachweis der Unentscheidbarkeit kann man die Arbeitsschritte einer universellen Turingmaschine im Schleifenrumpf beschreiben und in der Schleifenbedingung überprüfen, ob die Rechnung der Turingmaschine terminiert (Halteproblem).

Terminierung

Nicht-Terminierung von Schleifen

Eine Schleife

$$\texttt{while}\ (B)\ \texttt{do}\ S$$

terminiert nicht, wenn eine Zusicherung I_{NT} existiert, so dass folgende Aussagen gelten:

1. Es gibt Eingaben, so dass $\{B$ *und* $I_{NT}\}$ vor der Schleife gültig ist.
2. $\{B$ *und* $I_{NT}\}$ ist Invariante der Schleife.

I_{NT} bezeichnet eine nur in bestimmten Eingabesituationen gültige Zusicherung.

Beim Nachweis der partiellen Korrektheit und der Terminierung müssen die verwendeten Zusicherungen in allen denkbaren Zuständen des Programmes an den entsprechenden Stellen gelten.

Bemerkungen:

- Durch Nachweise für Nicht-Terminierung von Schleifen kann man Hinweise für notwendige Änderungen der Spezifikation erlangen.
- Durch Nachweise für Nicht-Terminierung von Schleifen zeigt man die Anwesenheit eines Fehlers, aber nicht die Abwesenheit!

Terminierung

Beispiel Nicht-Terminierung von Schleifen

Vorbedingung P: $\{x < y$ *und* $x \geq 0\}$

Gesucht ist verschärfte Vorbedingung R mit $\{R\} \Rightarrow \{P\}$

(Verschärfte Vorbedingung repräsentiert spezielle Wertebelegung für x und y.)

$\{x < y$ *und* $x \geq 0\}$

while $(x < y)$ do

$x := x * x + 5 * x;$

Terminierung

Beispiel Nicht-Terminierung von Schleifen

Vorbedingung P: $\{x < y$ *und* $x \geq 0\}$

Gesucht ist verschärfte Vorbedingung R mit $\{R\} \Rightarrow \{P\}$

(Verschärfte Vorbedingung repräsentiert spezielle Wertebelegung für x und y.)

$\{x < y$ *und* $x \geq 0\}$

$\{x < y$ *und* $x = 0\} = \{R\}$

`while` $(x < y)$ `do`

$x := x * x + 5 * x;$

(Genaugenommen muss $\{R\}$ eine Verschärfung der Spezifikation des Programmes sein.)

Terminierung

Beispiel Nicht-Terminierung von Schleifen

Vorbedingung P: $\{x < y$ *und* $x \geq 0\}$

Gesucht ist verschärfte Vorbedingung R mit $\{R\} \Rightarrow \{P\}$

(Verschärfte Vorbedingung repräsentiert spezielle Wertebelegung für x und y.)

Invariante $I_{NT} = R$

$\{x < y$ *und* $x \geq 0\}$

$\{x < y$ *und* $x = 0\} = \{R\}$

$\Rightarrow \{x < y$ *und* $x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

`while` $(x < y)$ `do`

$x := x * x + 5 * x;$

(Genaugenommen muss $\{R\}$ eine Verschärfung der Spezifikation des Programmes sein.)

Terminierung

Beispiel Nicht-Terminierung von Schleifen

Vorbedingung P: $\{x < y$ *und* $x \geq 0\}$

Gesucht ist verschärfte Vorbedingung R mit $\{R\} \Rightarrow \{P\}$

(Verschärfte Vorbedingung repräsentiert spezielle Wertebelegung für x und y.)

Invariante $I_{NT} = R$

$\{x < y$ *und* $x \geq 0\}$

$\{x < y$ *und* $x = 0\} = \{R\}$

$\Rightarrow \{x < y$ *und* $x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

`while` $(x < y)$ `do`

$\{x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

$x := x * x + 5 * x;$

$\{x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

(Genaugenommen muss $\{R\}$ eine Verschärfung der Spezifikation des Programmes sein.)

Terminierung

Beispiel Nicht-Terminierung von Schleifen

Vorbedingung P: $\{x < y$ *und* $x \geq 0\}$

Gesucht ist verschärfte Vorbedingung R mit $\{R\} \Rightarrow \{P\}$

(Verschärfte Vorbedingung repräsentiert spezielle Wertebelegung für x und y.)

Invariante $I_{NT} = R$

$\{x < y$ *und* $x \geq 0\}$

$\{x < y$ *und* $x = 0\} = \{R\}$

$\Rightarrow \{x < y$ *und* $x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

`while` $(x < y)$ `do`

$\{x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

$\Rightarrow \{x * x + 5 * x = 0$ *und* $x * x + 5 * x < y\}$

$x := x * x + 5 * x;$

$\{x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

(Genaugenommen muss $\{R\}$ eine Verschärfung der Spezifikation des Programmes sein.)

Terminierung

Beispiel Nicht-Terminierung von Schleifen

Vorbedingung P: $\{x < y$ *und* $x \geq 0\}$

Gesucht ist verschärfte Vorbedingung R mit $\{R\} \Rightarrow \{P\}$

(Verschärfte Vorbedingung repräsentiert spezielle Wertebelegung für x und y.)

Invariante $I_{NT} = R$

$\{x < y$ *und* $x \geq 0\}$

$\{x < y$ *und* $x = 0\} = \{R\}$

$\Rightarrow \{x < y$ *und* $x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

`while` $(x < y)$ `do`

$\{x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

$\Rightarrow \{x * x + 5 * x = 0$ *und* $x * x + 5 * x < y\}$

$x := x * x + 5 * x;$

$\{x = 0$ *und* $x < y\} = \{R$ *und* $B\}$

(Genaugenommen muss $\{R\}$ eine Verschärfung der Spezifikation des Programmes sein.)

➜ Schleife terminiert also nicht für Anfangswert $x = 0$.