Beweis von Programmeigenschaften

Tut ein Programm das, was es soll?

Eine Studie von 1991 zeigt, daß bei Projekten in der Größenordnung von 405 Arbeitsjahren aufwärts

- Projektmanagement ca. 16-18%
- Dokumentation 30 - 33 %
- Codierung nur 20 - 12 % und
- analytische Qualitätssicherung 34 - 37 %

der Arbeit ausmacht. (Liggesmeyer et al. in: Informatik-Spektrum Band 21, Heft 5, 1998)

Qualitätssicherung

- formale Techniken: Verifikation und symbolischer Test
- statistische Analyse: Reviews
- systematische Prüftechniken: dynamischer Test

Eine Grundlage für formale Techniken ist der Induktionsbeweis.

Schleifeninvariante

Wir wollen feststellen, ob eine Aussage $S(n)$ für alle positiven ganzen Zahlen n wahr ist.

Wir denken dabei an eine Schleife mit n als Laufvariable. Die Aussage $S(n)$ soll immer an einem bestimmten Punkt der Schleife wahr sein. Wenn sie das ist, heißt sie Schleifeninvariante.

- bei welchem Schritt in der Schleife soll die Aussage $S(n)$ wahr sein?
- welche Aussage interessiert uns?

Induktionsbeweis

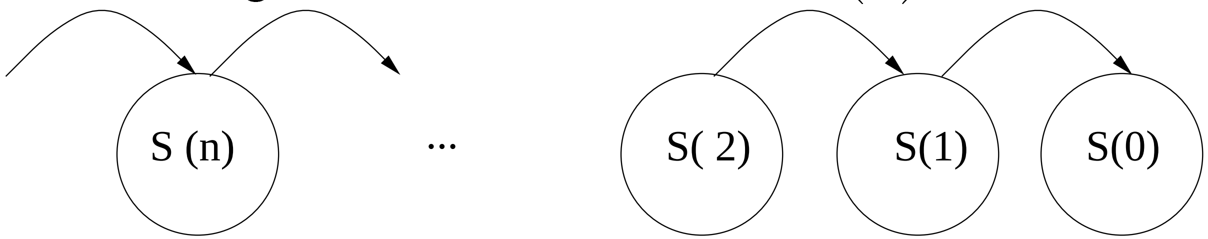
Induktionsanfang: Meist ist die Aussage $S(0)$ der Induktionsanfang. Gilt die Aussage für $n = 0$? Es kann aber statt 0 irgendeine Zahl b sein, so daß $S(n)$ nur für $n \geq b$ bewiesen wird.

Induktionsschritt: Zu beweisen ist, daß aus $S(n)$ logisch folgt, daß $S(n+1)$ gilt. Wir nehmen also an, daß $S(n)$ wahr ist. Dies ist die *Induktionsannahme*. Dann zeigen wir, daß dann auch $S(n+1)$ wahr ist. Gilt $S(n)$ nicht, ist die Aussage ohnehin wahr.

Die logische Implikation – aus A folgt B – ist wahr, wenn

- A falsch ist oder
- B wahr ist oder
- A und B beide wahr sind.

In einem Induktionsbeweis zeigen wir also, daß $S(0)$ wahr ist. Dann zeigen wir, daß, falls $S(n)$ wahr ist, auch $S(n+1)$ wahr ist.



Jede Instanz der Aussage $S(n)$ hängt von der Aussage über den nächst niedrigeren Wert von n ab.

Warum geht das?

Wie kann denn dieser Induktionsschritt funktionieren? Die Argumentation geht auf zwei alternative Arten.

- Wir wollen wissen, ob $S(a)$ für irgendein a gilt. Wenn $a = 0$, dann haben wir beim Induktionsanfang den Beweis schon geführt. Wenn $a > 0$, dann gelangen wir durch eine Kette dahin: $S(0)$ impliziert $S(1)$, $S(1)$ impliziert $S(2)$ und so weiter bis $S(a)$. Egal, welchen Wert a hat, irgendwann erreichen wir ihn.

- Wir können auch mit einem Gegenbeispiel argumentieren, warum der Induktionsschritt Sinn macht. Nehmen wir mal an, a wäre die kleinste Zahl, bei der $S(n)$ nicht gilt. Dann ist also $S(a-1)$ noch wahr, aber $S(a)$ nicht. Dies ist ein Widerspruch! (Die Implikation "aus A folgt B" ist falsch, wenn A wahr ist und B ist falsch.) Unsere Annahme, es gäbe ein a, so daß für $n > a$ gilt, daß $S(n)$ falsch ist, führt zu einem Widerspruch. Es gibt also kein a, ab dem $S(n)$ falsch ist, wenn alles davor wahr ist.

Induktionsbeweis am Beispiel der Selektionssortierung

Warum funktioniert unser Programm? Wir haben zwei Schleifen ineinander geschachtelt. Können wir über diese Schleifen irgendeine Aussage machen?

Schleifeninvariante vor Eintritt in die Schleife.

Aussage innere Schleife S(n): Wenn wir 4) mit n als Wert von j erreichen, ist der Wert der Variablen x der kleinste Wert im Feld $a[]$ von $a[i]$ bis $a[n-1]$ und k dessen Position.

Aussage äußere Schleife: bis i ist das Feld sortiert und nach i gibt es keine Position, in der ein Wert ist, der kleiner als irgendein Wert vor i ist.

innere Schleife

1. $x = a[i]$

2. $j = i + 1$

3. Aussage $S(n)$, wobei wir uns mit n auf den Zähler j der Schleife beziehen. Wir sagen deshalb nicht einfach $S(j)$, weil wir in der Argumentation manchmal j verändern, während n gleich bleibt. Hier betrachten wir den Zustand direkt vor der Abbruchbedingung der Schleife.

4. $j \geq a.length$?

5. $x \geq a[j]$?

6. $k = j; x = a[j];$

7. $j + +;$

Wenn die Frage 4) mit "ja beantwortet wird, verlassen wir die Schleife. Wenn die Frage 5) mit "nein" beantwortet wird, gehen wir zu Anweisung 7).

Induktionsanfang

Es gibt nun einen natürlichen Induktionsanfang, nämlich, wenn wir das erste Mal in die Schleife hineingeraten. Dann ist $x = a[i]$ und $j = i + 1$.

Also müssen wir zuerst zeigen, daß für $n = i + 1$ unsere Aussage gilt: $S(i + 1)$. Ausformuliert heißt das:

"x ist der kleinste Wert im Feld von $a[i]$ bis $a[i]$."

Dies ist wahr, denn

- $x = a[i]$ wurde ja gerade in 2) gesetzt
- später kommen wir nicht noch einmal in die Situation, daß $n = i + 1$, weil ja in 7) j inkrementiert wird.

Implikation

A	->	B
w	f	f
w	w	w
f	w	w
f	w	f

Insbesondere gilt die Implikation also,

- wenn A falsch ist – egal, wie B ist
- wenn B wahr ist – egal wie A ist

S(n) --> S(n+1)
w

n >= a.length

w
S(n) --> S (n+1)

w

A --> B

f

n < a.length

w
S(n) --> S(n+1)

w

w

A --> B

w w

a[n] >= x

also bleibt x
also ist x kleinster Wert

a[n] < x

also x= a[n]
also ist x kleinster Wert

Induktionsschritt

Wenn $S(i+1)$ gilt, dann wollen wir weiter für $n \geq i+1$ beweisen, $S(n) \rightarrow S(n+1)$.

- $n \geq a.length$ bewirkt Verlassen der Schleife, also kein Erreichen der Schleifeninvariante mit $n+1$. D.h.:

  $S(n+1)$:

  in 4): $j == n+1 \rightarrow$

  $a[k] == x \& i \leq k \leq n-1 \& \forall z \not\exists y : a[z] == y \& y < x$

  $j == n+1$ ist falsch, $S(n+1)$ also wahr.

  Wenn $S(n+1)$ wahr ist, ist $S(n) \rightarrow S(n+1)$ wahr.

- $n < a.length$

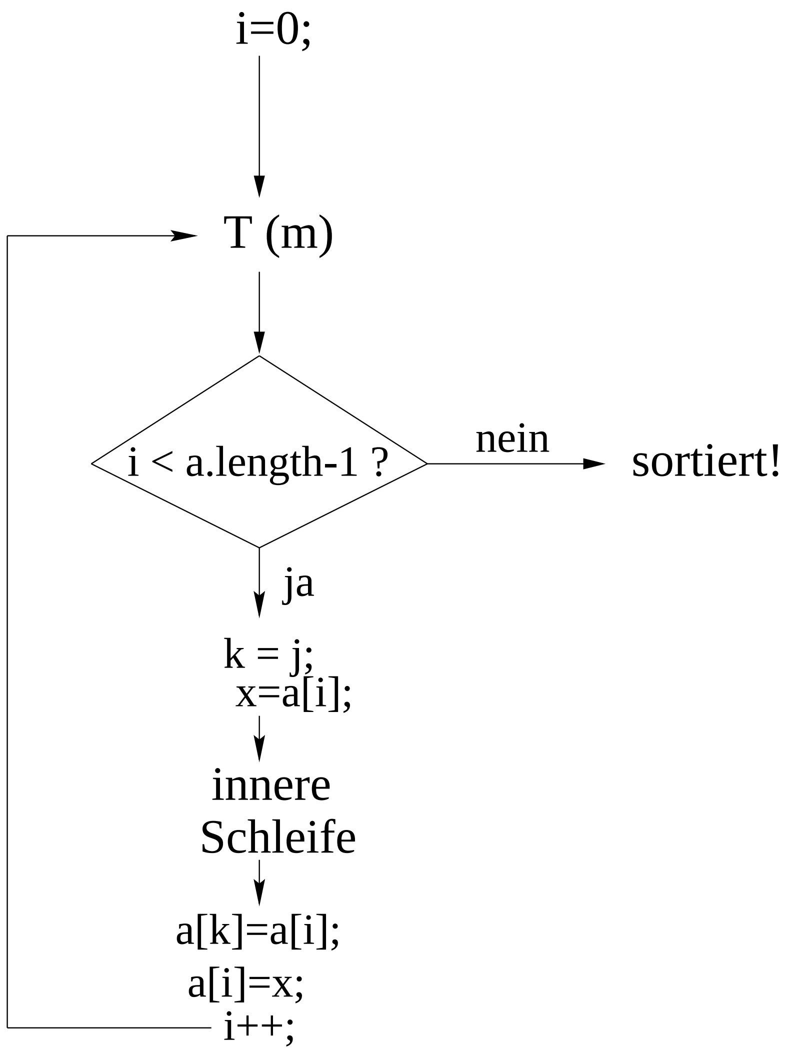
  Wir werden also den Test in 4) mit $n+1$ als Wert von j erreichen. Ist x dann der kleinste Wert des Feldes von $a[i]$ bis $a[n]$? Dazu betrachten wir zwei Fälle, je nach Ausgang des Test in 5).

- Wenn $a[n]$ nicht kleiner ist als der kleinste Wert im Feld von $a[i]$ bis $a[n-1]$, dann wird in 6) der Wert von x nicht geändert. Dann ist also x der kleinste Wert auch bei $n+1$.
- Wenn $a[n]$ kleiner ist als der bisher kleinste Wert im Feld von $a[i]$ bis $a[n-1]$, dann erhält x in 6) den Wert $a[n]$. Dann ist also x der kleinste Wert bei $n+1$.

j wird in 7) inkrementiert und dann erreichen wir den entscheidenden Punkt, die Schleifeninvariante. Gerade dann gilt die Aussage $S(n+1)$.

Wir haben also gezeigt, daß $S(n+1)$, wenn $S(n)$ unter der Annahme, daß $S(i+1)$.

äußere Schleife



Beweis der äußeren Schleife

Aussage $T(m)$: Wenn wir den Schleifentest, $i \geq a.length - 1$, mit m als dem Wert der Variablen i erreichen, dann gilt

a) Das Feld ist von $a[i]$ bis $a[m-1]$ sortiert, d.h. $a[0] \leq a[1] \leq ... \leq a[m-1]$.

b) Alle Werte von $a[m]$ bis zum Ende des Feldes sind mindestens so groß wie jeder beliebige Wert von $a[0]$ bis $a[m-1]$.

Induktionsanfang

$m = 0$ ist der Anfang, wie durch $int\ i = 0$ angegeben.

$T(0)$: "das Feld ist von $a[0]$ bis $a[-1]$ sortiert."

Es gibt gar keine Elemente in $a[0]$ bis $a[-1]$. Über die leere Menge kann man beliebige Aussagen treffen – sie sind alle wahr. Also sind die nicht vorhandenen Elemente sortiert und kleiner als die Elemente in $a[0]$ bis zum Feldende. $T(0)$ ist also wahr.

T(m) --> T(m+1)
w

m+1 >= a.length-1
w
T(m) --> T (m+1)
w
A --> B
f

m < a.length-1
w
T(m) --> T(m+1)
w w
A --> B
w w

a)
weil T(m):
a[0] bis a[m-1] sortiert

weil S(n):
x ist kleinster Wert in
a[m] bis a[a.length-1]

jetzt a[m]=x!

b)
weil T(m):
alle y in a[m] bis a[a.lenght-1]
alle z in a[0] bis a[m-1]: y>=z

jetzt: a[m]=x
i++
dann gilt:
alle y in a[m+1] bis a[a.length-1]
alle z in a[0] bis a[m]: y>=z

m >=a.length-1
w
T(m) --> T(m+1)
w w
A --> B
f

Induktionsschritt

Für $m > 0$ nehmen wir an, daß $T(m)$ wahr ist, und wollen zeigen, daß dann auch $T(m+1)$ wahr ist.

- Wenn wir den Schleifentest, $i \geq a.length - 1$, nicht mit $m+1$ als Wert von i erreichen, ist der erste Teil der Implikation ("Wenn wir den Schleifentest ... erreichen") falsch und damit $T(m+1)$ sowieso wahr.

- Betrachten wir also den Fall, wenn m kleiner als $a.length - 1$ und größer als 0 ist.
  - Teil a) der Aussage $T(m+1)$
    Hat i den Wert m, so wird in der inneren Schleife – wie durch $S(m)$ bewiesen – der kleinste Wert in $a[m]$ bis zum Feldende gefunden. Dieses kleinste Element wird der neue Wert von x an der Position $a[k]$.
    Weil $T(m)$ gilt, ist $a[0]$ bis $a[m-1]$ sortiert. Jetzt speichern wir das kleinste Element des Feldrestes an die richtige Stelle im sortierten Teil.
    Also ist Teil a) der Aussage $T(m+1)$ wahr.
  - Teil b) der Aussage.
    Für $i = m$ gilt, daß alle Elemente im unsortierten Teil $a[m]$ bis Feldende größer oder gleich groß einem jeden beliebigen Element in $a[0]$ bis $a[m-1]$ sind. Wir haben aus dem unsortierten Rest das kleinste Element herausgenommen. Kein Element im unsortierten Teil des Felds ist kleiner als dies. Verkürzen wir den unsortierten Teil ($i{+}{+}$), dann bleiben darin immer noch nur Elemente, die nicht kleiner sind als ein Element im nunmehr verlängerten sortierten Teil $a[0]$ bis $a[m]$.

In anderen Worten: “alle Elemente in $a[m+1]$ bis Feldende sind mindestens so groß wie jeder beliebige Wert eines Elementes in $a[0]$ bis $a[m]$.” Also ist Teil b) der Aussage $T(m+1)$ wahr.

- Wenn nun $m \geq a.length - 1$ ist, verlassen wir die äußere Schleife und damit das Programm. Zu $T(m+1)$ kommen wir nicht mehr, d.h. weil der erste Teil der Aussage von $T(m+1)$ falsch ist, ist $T(m+1)$ wahr. Da $T(m)$ gilt, ist das Feld von $a[0]$ bis $a[m-1]$ sortiert (Teil a) der Aussage). $T(m)$ ist mindestens so groß wie irgendein Element in $a[0]$ bis $a[m-1]$ (Teil b) der Aussage). Damit ist das Feld insgesamt sortiert.

Das Programm entspricht also tatsächlich dem Modell der Sortierung, das durch die Aussagen $S(n)$ und $T(m)$ charakterisiert ist.