

6. Rekursive Funktionen und Induktion

6.1 Rekursive Funktionen

- Definition rekursiver Funktionen
- Terminierung

6.2 Beweisen durch Induktion

6.3 Fundierte Relationen

6.1 Rekursive Funktionen

Rekursive Funktionen können in PVS nicht einfach wie nicht-rekursive Funktionen definiert werden, da der zu definierende Name im Rumpf der Definition (der rechten Seite nach dem =) nicht verwendet werden kann.

Alternative 1: Deklaration des Funktionsnamens als uninterpretiertes Funktionssymbol, gefolgt von einer *Formel*, die die Rekursionsgleichung enthält und als Axiom anzusehen ist.

```
fakt : [nat -> nat]
fakt_ax : AXIOM
      fakt(n) = IF n=0 THEN 1 ELSE n * fakt(n-1) ENDIF
```

Alternative 2: Explizite rekursive Definition mit Angabe des Schlüsselworts RECURSIVE vor dem Resultat-Typ

```
fakt(n: nat): RECURSIVE nat =
      IF n=0 THEN 1 ELSE n * fakt(n-1) ENDIF
...

```

Rekursive Funktion: Axiom oder Definition?

Axiome sind einfacher hinzuschreiben, sind aber potentiell gefährlich:

Axiome können inkonsistent sein!

Es ist daher sicherer, eine definitorische Form der Rekursion zu benutzen.

Definitionen sollen *konservative Erweiterungen* einer Theorie sein:

Theorie , d.h. die Menge der beweisbaren Aussagen ("Theoreme"), soll durch Hinzunahme einer Definition nicht vergrößert werden.

PVS erzwingt bei Definitionen diese Eigenschaft, insbesondere durch die Forderung, dass alle Funktionen als *total* nachgewiesen werden.

Totale rekursive Funktionen

In der 'normalen' Prädikatenlogik werden alle Funktionen als *total* vorausgesetzt.

Partialität entsteht in natürlicher Weise bei rekursiven Funktionen.

~> Logik muß mit partiellen Funktionen umgehen können.

Mögliche Alternativen: z.B.

- Mehrwertige Logik (z.B. 3-wertig: wahr, falsch, unbestimmt ('bottom')); siehe "Logic of Computable Functions", LCF)
- Logik partieller Funktionen
Problem z.B.: was bedeutet All-Quantifizierung über ein nur partiell definiertes Prädikat?

Die Alternativen haben ihre eigenen Probleme; PVS unterstützt (direkt) keine.

Frage: wie sieht es aus mit Funktionen, die inhärent partiell sind?

Z.B. für Division über reellen Zahlen: Division durch 0?

Rekursive Funktionen: Terminierung

PVS erlaubt es in vielen Fällen, inhärent partielle Funktionen auf ihren tatsächlichen Definitionsbereich einzuschränken und damit total zu machen.

↪ Erweiterung des Typsystems um *Sub-* oder *Untertypen* (kommt später)

Für nicht-rekursive Funktionen ist die Forderung nach Totalität unproblematisch (warum?).

Für rekursiv definierte Funktionen erzwingt PVS den Nachweis der Terminierung:

In der Syntax: In der rekursiven Definition muß eine *Maßfunktion* angegeben werden:

```
fakt(n: nat): RECURSIVE nat =  
    IF n=0 THEN 1 ELSE n * fakt(n-1) ENDIF  
MEASURE x
```

x steht hier für die Identität (LAMBDA (x:nat): x)

Generell: bei Angabe der Maßfunktion kann Lambda-Bindung fortgelassen werden, es genügt Angabe des Rumpfs der Funktion.

Rekursive Funktionen: Terminierung (2)

In der Semantik: Die Maßfunktion bildet das Rekursionsargument in eine geordnete Menge ab.

Im einfachsten Fall (wie hier): Abbildung in die Menge der natürlichen Zahlen.

Bezüglich der Maßfunktion müssen die Argumente der rekursiven Aufrufe im Funktionsrumpf kleiner werden.

Wenn es ein kleinstes Element in der Maßmenge gibt, folgt aus der Bedingung, dass die Rekursion terminiert.

PVS generiert hierfür während der Typüberprüfung eine *Terminierungs-TCC* - hier:

```
fakt_TCC: OBLIGATION
  FORALL (n: nat): NOT n=0 IMPLIES n-1 < n
```

Die TCC enthält als Vorbedingung die zutreffende Bedingung

~> Herstellen des richtigen Kontexts für den Beweis

~> TCCs (“*type correctness conditions*”) werden in Kürze allgemein behandelt.

Induktion

Warum braucht man Induktion?

1. *Ein Induktionsaxiom/-schema schließt Nichtstandard-Modelle aus*

(s.o. Logik höherer Stufe)

Ein *Induktionsschema* steht für eine (unendliche) Menge von (PL1-)Instanzen des Induktionsprinzips; ein Induktionsaxiom (in der Form einer PL2-Formel) drückt dasselbe etwas direkter (und sauberer) aus.

2. Mit Hilfe von *Induktion als Beweisprinzip* können Aussagen bewiesen werden, die anders (d.h. in PL1) nicht bewiesen werden können.

Z.B. Prinzip der *mathematischen Induktion* über den natürlichen Zahlen Nat

Beispiel: Peano-Arithmetik

Die Peano-Arithmetik (elementare Arithmetik; nach dem ital. Mathematiker Peano, 1889) ist die Theorie der natürlichen Zahlen mit Addition und Multiplikation, $\mathcal{N}_{+,*}$, definiert durch das Axiomensystem PA :

$$\forall x. \neg(0 = s(x)) \quad (\text{constr})$$

$$\forall x, y. s(x) = s(y) \Rightarrow x = y \quad (\text{inj})$$

$$\forall x. x + 0 = x \quad (\text{add0})$$

$$\forall x, y. x + s(y) = s(x + y) \quad (\text{add1})$$

$$\forall x. x * 0 = 0 \quad (\text{mul0})$$

$$\forall x, y. x * s(y) = x * y + x \quad (\text{mul1})$$

$$\forall P : (\mathcal{N} \rightarrow Bool). \quad (\text{induct})$$

$$P(0) \wedge (\forall x. P(x) \Rightarrow P(s(x))) \Rightarrow \forall x. P(x)$$

plus Axiome über Gleichheit

Peano-Arithmetik (2)

Das Axiom (induct) definiert das *Induktionsprinzip* für natürliche Zahlen:

Um eine Formel $\forall x.Q(x)$ zu beweisen, muß gezeigt werden

- (i) $Q(0)$ (Induktions-Anfang)
- (ii) $Q(s(x))$ unter der Annahme $Q(x)$, für beliebiges x (Induktions-Schritt)

Man kann zeigen, daß obige Axiomatisierung \mathcal{N}_{+*} bis auf Isomorphie charakterisiert.

Die in PA gültigen Sätze sind nicht rekursiv aufzählbar.

Insbesondere ist also PA nicht entscheidbar.

Es gibt entscheidbare Untertheorien von PA , z.B. die *Presburger-Arithmetik*, die nur lineare Arithmetik (keine Multiplikation) enthält.

Peano-Arithmetik: Beispielbeweis

Beweise die Formel $Q := \forall x. (x + 1 = 1 + x)$ aus den Axiomen PA :

Beweisstruktur:

$$\frac{\frac{\frac{PA \vdash IA}{PA \vdash IA \wedge IS} \quad PA \vdash IS}{PA, (IA \wedge IS \Rightarrow Q) \vdash Q} \quad PA, Q \vdash Q}{PA, \forall P. P(0) \wedge (\forall x. Px \Rightarrow P(s(x))) \Rightarrow \forall x. P(x) \vdash Q}^{(*)}$$

Bei dem Schritt $(*)$ ist für P einzusetzen die Funktion

$$\sigma := \lambda z. (z + 1 = 1 + z)$$

Dadurch wird $P(0)$ zum Induktions-Anfang:

$$IA := 0 + 1 = 1 + 0$$

$\forall x. P(x) \Rightarrow P(s(x))$ wird zum Induktions-Schritt

$$IS := \forall x. (x + 1 = 1 + x \Rightarrow s(x) + 1 = 1 + s(x))$$

$\forall x. P(x)$ wird gleich der zu beweisenden Formel Q :

$$\forall x. x + 1 = 1 + x$$

Peano-Arithmetik: Beispielbeweis (2)

Die einzigen verbleibenden Beweisziele sind:

$$PA \vdash IA$$

und

$$PA \vdash IS$$

Sie lassen sich mit Hilfe der übrigen Axiome beweisen, d.h. ohne Anwendung von Induktion.

Bemerkung: Formal gesehen ist der Beweis nur in PL2 möglich, aber Elemente der PL2 werden nur für die Instantiierung der Induktionsformel (und für die zugehörigen Inferenzen) benötigt; der Rest des Beweises ist dann wie in einem “normalen” PL1-Beweis.

Induktion in PVS

In PVS ist der Typ `nat` vorgegeben, ebenso die zugehörige Formel für Induktion über `nat`.

(Streng genommen handelt es sich in PVS hierbei *nicht* um ein Axiom.)

```
p: VAR pred[nat]
```

```
nat_induction: LEMMA
```

```
(p(0) AND (FORALL j: p(j) IMPLIES p(j+1)))  
  IMPLIES (FORALL i: p(i))
```

Alternativ könnte die Formel über `p` all-quantifiziert geschrieben werden.

Induktionsbeweise in PVS

In PVS ist es (in der Regel) nicht notwendig, die Induktionsformel explizit zu instantiieren mit einem passenden Prädikat.

Stattdessen: Beweiserkommando `induct`

`(induct "n")`

– generiert für eine Zielformel die entsprechenden Unterziele Induktionsanfang und Induktionsschritt, entsprechend der zugehörigen Induktionsformel (Beispiele für andere Typen kommen später)

Für einen Induktionsbeweis ist die wichtigste Entscheidung: welches ist das Induktionsargument?

Im einfachsten Fall: `trivial` (wenn es nur einen Kandidaten gibt)

6.3 Fundierte Relationen

Eine Relation \succ auf einer Menge S heißt *fundiert* (engl. *well-founded*), falls jede nichtleere Teilmenge M von S wenigstens ein bezgl. \succ minimales Element m enthält, d.h. es kein $x \in M$ mit $m \succ x$ gibt.

Eine Menge S mit einer fundierten Relation \succ heißt *fundiert* (oder *wohlfundiert*) bezgl. \succ .

Satz: Es sind äquivalent:

- (i) \succ ist fundierte Relation auf S .
- (ii) Es gibt in S keine unendliche absteigende Kette

$$x_1 \succ x_2 \succ \dots \succ x_n \succ \dots$$

Beweis:

(i) \Rightarrow (ii): Angenommen, es gibt eine unendliche Kette $x_1 \succ x_2 \succ \dots$

Sei $M = \{x_1, x_2, \dots\}$. Für jedes $x_i \in M$ gibt es ein bzgl. \succ kleineres Element (x_{i+1}), daher hat M kein minimales Element.

Fundierte Relationen (Forts.)

Beweis: (i) \Leftarrow (ii):

Angenommen, \succ ist auf S nicht fundiert. Dann gibt es wenigstens eine nichtleere Teilmenge M von S ohne minimales Element. Eine unendliche absteigende Kette kann wie folgt konstruiert werden:

(a) x_1 wird willkürlich aus M gewählt (existiert, da M nicht leer ist).

(b) Für x_i wähle ein x_{i+1} , so daß $x_i \succ x_{i+1}$ – muß jeweils existieren, da es kein minimales Element gibt. \square

Lemma: Eine fundierte Relation ist irreflexive und asymmetrisch.

Bemerkung: Eine fundierte Relation muß nicht transitiv sein, d.h. keine Ordnungsrelation sein.

Die meisten hier benutzten fundierten Relationen sind jedoch Ordnungsrelationen.

Beispiele für fundierte Relationen:

- (1) Die leere Relation ist fundiert.
- (2) Die übliche Ordnungsrelation $>$ auf natürlichen Zahlen Nat
- (3) Die folgende Relation auf Nat ist fundiert, aber nicht transitiv:

$$n \succ m \text{ g.d.w. } m = suc(n)$$

- (3) Die *lexikographische Ordnung* $>^2$ auf $Nat \times Nat$:

$$(m_1, m_2) >^2 (n_1, n_2) \text{ g.d.w. } m_1 > n_1 \text{ oder } m_1 = n_1 \wedge m_2 > n_2$$

Allgemein läßt sich eine lexikographische Ordnung auf Tupeln angeben, wenn jeweils eine fundierte Ordnung für jede Komponente gegeben ist.

- (4) Die Teillisten-Relation auf linearen Listen:

$$l_1 < l_2 \text{ falls } l_1 \text{ ein "Endstück" von } l_2 \text{ ist}$$

Allgemein sind Teilstruktur-Relationen auf induktiv definierten Datenstrukturen fundiert (mehr hierzu später).

Fundierte Relationen (2)

Nachweis der Fundiertheit mit Hilfe von Abbildungen:

Gegeben Mengen S und M mit einer fundierten Relation $>_M$ auf M , weiterhin eine Abbildung $f : S \rightarrow M$ (“Maßfunktionen”).

Eine Relation $>_S$ auf S wird definiert (induziert) durch

$$x >_S y \iff f(x) >_M f(y) \text{ für alle } x, y \in S$$

Satz: Die Relation $>_S$ ist fundiert.

Beispiele:

- Jede Abbildung in Nat mit Ordnungsrelation $>$
- Längenfunktion über linearen Listen
- Höhenfunktion über Bäumen
- Anzahl der Blätter von Bäumen

All diese Funktionen sind “Zählfunktionen”.

Fundierte Relationen (3)

Fundierte (Ordnungs-)Relationen sind wichtig für

- den Nachweis der Terminierung für rekursiv definierte Funktionen (s. oben),
- als Grundlage für Induktionsbeweise.

Nachweis der Terminierung von Funktionen über fundierte Relationen entspricht der gebräuchlichsten Art der informellen Begründung, weshalb ein Programm terminiert (z.B.: ein Zähler wird so lange monoton verändert, bis ein Abbruchkriterium erfüllt ist).

Die Charakterisierung fundierter Relationen über minimale Elemente kann als Beweisprinzip statt eines Induktionsbeweises genutzt werden.

Induktion über fundierten Relationen

Eine fundierte Relation kann herangezogen werden zur Definition eines Induktionssprinzips:

fundierte oder Noethersche Induktion

benannt nach der Mathematikerin Amalie Emmy (“Emily”) Noether (1882–1935)

Satz (Noethersche Induktion): Sei \prec eine fundierte Relation auf einer Menge S . Um eine Eigenschaft P für alle $x \in S$ nachzuweisen (d.h. $\forall x : S. P(x)$), genügt es zu zeigen:

$$\forall x : S. (\forall y : S. y \prec x \Rightarrow P(y)) \Rightarrow P(x)$$

Beweis: Angenommen, die Menge A der Elemente aus S , für die P nicht gilt, ist nicht-leer. Dann hat sie ein kleinstes Element, m . Nach Definition gilt $P(y)$ für alle $y \prec m$, nach Voraussetzung muß dann auch $P(m)$ gelten, im Widerspruch zur Annahme. Daher muß A leer sein, d.h. P gilt für alle $x \in S$. \square

Induktion über fundierte Relationen (2)

Beispiel für Noethersche Induktion:

“vollständige Induktion” über natürlichen Zahlen:

Um $\forall x : \text{Nat. } P(x)$ zu beweisen, genügt es zu zeigen:

$$\forall x : \text{Nat. } [\forall y : \text{Nat. } y < x \Rightarrow P(y)] \Rightarrow P(x)$$

Bemerkung: der Basis-Fall $P(0)$ ist “automatisch” abgedeckt (wieso?).

Weitere Beispiele kommen (in Kürze) bei der Behandlung induktiver Datenstrukturen.

Fundierte Relationen in PVS

Die Eigenschaft, fundiert zu sein, kann in PVS als Prädikat (höherer Stufe) über Relationen ausgedrückt werden:

```
< : VAR pred[[T,T]]
```

```
p : VAR pred[T]
```

```
x, y, z : VAR T
```

```
well_founded?(<): bool =
```

```
  (FORALL p: (EXISTS x: p(x))
```

```
    IMPLIES (EXISTS y: p(y) AND
```

```
      (FORALL z: p(z) IMPLIES (NOT z < y))))
```

Der PVS-Prelude enthält allgemeine Formulierungen für fundierte Relationen und fundierte Induktion. Diese erfordern bisher noch nicht behandelte Konstrukte und werden später vorgestellt.