Grundlagen der Programmierung (Vorlesung 10)

Ralf Möller, FH-Wedel

- Vorige Vorlesung: Prädikatenlogik
- Inhalt dieser Vorlesung
  - Prädikatenlogik mit speziellen Theorien
    - natürliche Zahlen, ganze Zahlen, reelle Zahlen
  - Elemente von Programmiersprachen:
    - Variablen, Felder
- Lernziele
  - Grundlagen der systematischen Programmentwicklung

Noch einmal: Funktionen

- In der Semantik der Prädikatenlogik:
  - Spezifikation von I_A durch: $f^A = \{ (x, y), (y, z), ...\}$
  - Schreibweise: $f(x) = y$ (x heißt Argument oder Parameter, y heißt Wert)
- Extensionale Definition problematisch da Tupelmenge potentiell unendlich
- Daher: Angabe der Tupelmenge durch Prädikatenlogische Formel (Beispiel)
  - $f^A = \{ (x, y) \mid y = x + 2 \}$
  - Schreibweise: $f(x) = x + 2$

Prädikate als Boole'sche Funktionen

- Prädikatsnamen bezeichnen Mengen von Tupeln:
  - Struktur $(U_A, . ^{A})$
  - Beispiel: $U_A = \{u, v, w\}$
  - Beispiel: $P^A = \{ (u, v), (v, w) \}$
- Darstellung von Prädikaten als Funktionen:
  - Beispiel: $P : U_A \times U_A \rightarrow B$ $\qquad B = \{ 0, 1 \}$
  - $P^A = \{ (u, v, 1), (v, w, 1),$
    $(u, w, 0), (u, u, 0), (v, v, 0), (v, u, 0),$
    $(w, u, 0), (w, v, 0), (w, w, 0) \}$

Prädikatenlogik für „Arithmetik“

- Festlegung des Universums der Struktur
- Definition von Prädikaten mit Hilfe von „eingebauten“, vorausgesetzten Funktionen

Zahlen

N_0	auch: N	unsigned int , cardinal: natürliche Zahlen ab 0
N_1		natürliche Zahlen ab 1
Z		Intg, integer: ganze Zahlen
R		real, float: reelle Zahlen

Operationen auf natürlichen Zahlen

elementare Prädikate	$= : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{B}$
	$\neq : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{B}$
elementare Operationen	$+1 : \mathsf{N}_0 \longrightarrow \mathsf{N}_0$
	$-1 : \mathsf{N}_0 \longrightarrow \mathsf{N}_0$
Arithmetik	$+ : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{N}_0$
	$- : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{N}_0$
	$\cdot : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{N}_0$
	$\mathsf{div} : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{N}_0$
	$\mathsf{mod} : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{N}_0$

$+,\cdot$ totale Funktionen

$-$,div,mod partielle Funktionen

Algebraische Axiome für +, *

- Einselemente
- Kommutativität
- Distributivität
- Assoziativität
- ....

- Axiome ermöglichen Umformulierungen von Termen

Weitere „eingebaute“ Prädikate

Vergleiche

$$\geq : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{B}$$
$$> : \mathsf{N}_0 \times \mathsf{N}_0 \longrightarrow \mathsf{B}$$

$\geq, >$ totale Funktionen

Wie hängen die Funktionen und Prädikate zusammen?

- Festlegung der Eigenschaften durch sog. Axiome
- Aus den durch Axiome festgelegten Eigenschaften sind Folgerungen ($\models$) möglich
- Menge von Axiomen heißt auch "Theorie"
- Üblich: Notation der Axiome als Formeln
- Zusammenhang zwischen "$\rightarrow$" und " $\models$ "

Ungleichungen Rechnen mit Ungleichungen

i, j, k seien ganze Zahlen

Axiome:

transitiv	$i \leq j \wedge j \leq k \quad \rightarrow \quad i \leq k$
reflexiv	$i \leq i$
antisymmetrisch	$i \leq j \wedge j \leq i \quad \rightarrow \quad i = j$
	$i \leq j \wedge 0 \leq k \quad \rightarrow \quad i * k \leq j * k$
transitiv	$i < j \wedge j < k \quad \rightarrow \quad i < k$

Weitere Axiome:

$$\neg(i < i)$$

$$\neg(i < j \wedge j < i)$$

$$i < j \quad \rightarrow \quad i + k < j + k$$

$$i < j \wedge 0 \leq k \quad \rightarrow \quad i * k \leq j * k$$

$$i < j \wedge 0 < k \quad \rightarrow \quad i * k < j * k$$

$$i < j \quad \rightarrow \quad i + 1 \leq j$$

Noch einmal: Natürliche Zahlen

- Wir betrachten Strukturen $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$
- Ausgezeichnete Menge N (auch N_0 genannt) der natürlichen Zahlen einschließlich 0, $N \subseteq U_\mathcal{A}$
- Annahme: Prädikat N zum Test, ob ein Objekt $n \in U_\mathcal{A}$ aus N ist

Vereinbarung von abkürzenden Schreibweisen

- $\forall\, n \in N\, .\, P(n)$ für $\forall\, n\, (N(n) \rightarrow P(n))$ (dto. für Z)
- $\forall\, a \leq n \leq b\, .\, P(n)$ für $\forall\, n\, (((N(n) \wedge (a \leq n)) \wedge (n \leq b)) \rightarrow P(n))$
- $\forall\, x \in M\, .\, F(x)$

- $\exists\, n \in N\, .\, P(n)$ für $\exists\, n\, (N(n) \wedge P(n))$ (dto. für Z)
- $\exists\, a \leq n \leq b\, .\, P(n)$ für $\exists\, n\, (((N(n) \wedge (a \leq n)) \wedge (n \leq b)) \wedge P(n))$
- $\exists\, x \in M\, .\, F(x)$

Beispiel

Aussage	*„alle Aldi-PCs sind schlecht gebaut"*
Grundmenge	PCs
elementare Prädikate	$vonAldi(x)$
	$gut(x)$
Formel	mit All–Quantor
	$\forall\, pc \in PCs \bullet vonAldi(pc) \Rightarrow \neg gut(pc)$

Aussage	*„es gibt eine gerade Primzahl"*
Grundmenge	N_0
elementare Prädikate	$gerade(x)$
	$prim(x)$
Formel	mit Existenz–Quantor
	$\exists\, n \in \mathsf{N}_0 \bullet gerade(n) \wedge prim(n)$

Tautologien/Gesetze (1)

(1) $\forall\, i \in \{\,\} \bullet P(i) \quad \leftrightarrow \quad \text{true}$

(2) $\exists\, i \in \{\,\} \bullet P(i) \quad \leftrightarrow \quad \text{false}$

(3) $\exists\, i \in M \bullet \neg P(i) \quad \leftrightarrow \quad \neg\forall\, i \in M \bullet P(i)$

$\forall\, i \in M \bullet \neg P(i) \quad \leftrightarrow \quad \neg\exists\, i \in M \bullet P(i)$

Verallgemeinerung von de Morgan

(4) $\forall\, i \in M \bullet P(i) \wedge j \in M \quad \rightarrow \quad P(j)$

(5) $j \in M \wedge P(j) \quad \rightarrow \quad \exists\, i \in M \bullet P(i)$

Tautologien/Gesetze (2)

(1a) $\forall\, a \le i < a \bullet P(i) \;\leftrightarrow\; \text{true}$

(2a) $\exists\, a \le i < a \bullet P(i) \;\leftrightarrow\; \text{false}$

(3a) $\exists\, a \le i < b \bullet \neg P(i) \;\leftrightarrow\; \neg\forall\, a \le i < b \bullet P(i)$

$\forall\, a \le i < b \bullet \neg P(i) \;\leftrightarrow\; \neg\exists\, a \le i < b \bullet P(i)$

(4a) $\forall\, a \le i < b \bullet P(i) \land a \le j < b \;\rightarrow\; P(j)$

(5a) $a \le j < b \land P(j) \;\rightarrow\; \exists\, a \le i < b \bullet P(i)$

(6a) $\forall\, a \le i < b \bullet P(i) \land \forall\, b < i < c \bullet P(i)$
$\leftrightarrow\; \forall\, a \le i < c \bullet P(i)$

Grundmenge	$i \in S$
Intervall	häufiger Sonderfall von Mengen: Intervall aus den ganzen Zahlen
Notation	$a \leq i < b$
alternative Notation	für Formeln mit Quantoren
	$\forall\, a \leq i < b \bullet P(i)$ — halb offenes Intervall
	$\forall\, a \leq i \leq b \bullet P(i)$ — abgeschlossenes Intervall
	$\forall\, a \leq i \bullet P(i)$ — unbeschränktes Intervall
Felder	f : array $[0\,..\,n-1]$ of $\mathit{Element}$
	f ist eine Variable zum Speichern einer ganzen Menge von Werten
Referenzierung	$f[i], f(i), f_i$ — Zugriff auf i-te Element in f
Indexbereich	ein Intervall (hier $0 \leq i < n$)

Beispiele für Prädikate mit $\forall$-Quantoren

gegeben zwei Felder a und b
vom Typ $\mathsf{array}\ [0\,..\,n-1]\ \mathsf{of}\ \mathsf{Z}$

Aufgabe Wie sehen die zugehörigen Prädikate aus?

(1) a ist eine exakte Kopie von b, alle Elemente sind gleich

(2) Für alle i ist das i-te Element von a kleiner als das i-te Element von b

(3) Jedes Element von a ist kleiner als jedes Element von b

(4) Wenn die Elemente von a in aufsteigender Reihenfolge sortiert sind, so auch die Elemente von b

(5) Alle Elemente von a sind untereinander verschieden

(6) Jedes Element von a ist von jedem Element von b verschieden

Beispiele	für Prädikate mit $\exists$- und $\forall$-Quantoren
gegeben	zwei Felder a und b vom Typ $\mathsf{array}\ [0\,..\,n-1]\ \mathsf{of}\ \mathsf{Z}$
Aufgabe	Wie sehen die zugehörigen Prädikate aus?
(1)	Einige Elemente von a sind ungleich 0
(2)	das Feld a ist nicht in aufsteigender Reihenfolge sortiert
(3)	mindestens ein Element von a ist größer als alle Elemente von b
(4)	Jedes Element von b ist eine Kopie eines Elements von a

(5) b enthält alle Zahlen von 0 bis $n-1$ (eine Permutation aller Zahlen von 0 bis $n-1$)

(6) b zeigt die numerische Ordnung von a an, d.h. $b[0]$ ist der Index auf das kleinste Element von a, $b[1]$ der Index auf das zweitkeinste Element usw.

(7) Wenn alle Elemente in a paarweise verschieden sind, dann enthält b die Elemente von a in sortierter Reihenfolge

(8) b enthält die Elemente von a in sortierter Reihenfolge

Negation	von Prädikaten mit Quantoren
Aussage	*„alle Aldi-PCs sind schlecht gebaut“*
Frage	Welche der folgenden Aussagen ist die Negation dieser Aussage
(1)	Alle nicht-Aldi-PCs sind gut gebaut
(2)	Alle Aldi-PCs sind gut gebaut
(3)	Einige Aldi-PCs sind gut gebaut
(4)	Einige Aldi-PCs sind schlecht gebaut
(5)	Einige nicht-Aldi-PCs sind schlecht gebaut
(6)	Einige nicht-Aldi-PCs sind gut gebaut

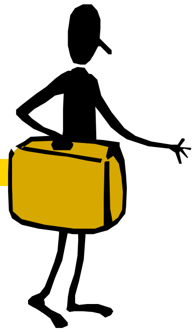
Algorithmen vs. Funktionen

- Statt extensionaler Spezifikation einer Funktion
- Spezifikation mit Hilfe einer Formel bzw. eines Prädikates (intensionale Spezifikation)
- Algorithmen berechnen Funktionen
- Berechnungsvorschrift (ggf. für jeden möglichen Parameter) erforderlich (-> Algorithmus)
- Berechnungsvorschrift u.U. nicht einfach zu finden (-> Korrektheit, Vollständigkeit, Terminierung)
- Systematische Entwicklung notwendig

Algorithmen

- Verwendung einer beliebigen Menge von "Variablen" {x, y, z, ...}
- Elementare Anweisungen
  - Zuweisung (Bsp. "x := 2")
  - Fallunterscheidung
  - Schleife
- Algorithmus: Sequenz von elementaren Anweisungen
- Idee: Nach Ausführung des Algorithmus steht Funktionswert in festgelegter Variable

Zusammenfassung, Kernpunkte



- Prädikatenlogik mit Axiomen z.B. für natürliche Zahlen
- Elemente von Programmiersprachen
  - Variablen, Felder
- Spezifikationen

Was kommt beim nächsten Mal?

- Elemente von Programmiersprachen:
  - Kontrollstrukturen
- Verifikation von Programmen