Diskrete Mathematik 2

FS 2013

Contents

1 1. Woche **1**

1.1 Semesterablauf(?) 1

1.2 Quantifizierung 1

1.3 Semantik 3

2 2. Woche **4**

1 1. Woche

1.1 Semesterablauf(?)

- Arithmetik in $\mathbb{Z}$

- Modulares Rechnen

- Gruppen

- RSA

- Quantifizierung

- Induktion
    - Rekurision
    - Invarianten

- Kein Laptop

- Zwischenpruefung: 30.04.2013 (1 Stunde)

- 5. Maerz 2013 Unterricht nur bis 18:20

- Buecher:

    - Gries/Schneider
      A logical approach to Discrete Math
      Springer, 1993

    - Jean Gallier
      Discrete Math
      Springer, 2010

    - Struckermann/Waetiger
      Mathematik fuer Informatiker
      Spektrum, 2007

1.2 Quantifizierung

$$\mathbb{N} = \begin{cases} \{\underline{0}, 1, 2, ...\} \ (?) \\ \{1, 2, ...\} \ (?) \end{cases}$$

$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + ... + n^2$

$\sum_{i=1}^{-1} i^2 = \begin{cases} ungueltig\ (?) \\ 1^2\ (?) \\ 1^2 + 0^2 + (-1)^2\ (?) \\ 0\ (\rightarrow ja,\ Neutrales\ Element) \end{cases}$

$\sum_{i=1}^{n} i^2 + 1 = 1^2 + 2^2 + ... + n^2 + 1$ (?)

$\sum_{i=1}^{n} (i^2 + 1) = (1^2 + 1) + (2^2 + 1) + ... + (n^2 + 1)$ (?)

$\sum_{\substack{i=1 \\ odd(i)}}^{n} i^2 = 1^2 + 3^2 + ... + n^2$, falls $odd(n)$, sonst $(n-1)^2$

$\prod_{i=1}^{n} i^2 = 1^2 * 2^2 * ... * n^2$

$\prod_{i=1}^{-1} i^2 = 1$ (neutrales Element)

(Java ==)

$\forall_{i=0}^{n-1} (b[i] == 0) = (b[0] == 0) \wedge (b[1] == 0) \wedge ... \wedge (b[n-1] == 0)$

$\exists_{i=0}^{n-1} (b[i] == 0) = (b[0] == 0) \vee (b[1] == 0) \vee ... \vee (b[n-1] == 0)$

$\sum_{i=1}^{n} i^2 = (\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n : i^2)$

$(\sum i : \mathbb{N}, j : \mathbb{N} \mid 1 \leqslant i \leqslant 2 \wedge 1 \leqslant j \leqslant 3 : i^j)$

$(\circ\, v_1 : T_1, ..., v_n : T_n \mid R : P)$

- $\circ : T \times T \rightarrow T$ (wobei T ein Typ ist)

Bsp: $+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
$+(3, 4) = 7$

$a \circ b = b \circ a$ fuer alle a,b : T (Symmetrie)(Kommutativitaet) — ABELSCHES MONOID
$(a \circ b) \circ c = a \circ (b \circ c)$ fuer alle a,b,c : T (Assoziativitaet)
$u \circ a = a = a \circ u$
es gibt ein u : T, so dass fuer alle a : T (neutrales Element) — MONOID

$\circ$	T	u
$+ \sum$	$\mathbb{Z}$	0
$* \prod$	$\mathbb{Z}$	1
$\forall$	$\mathbb{B}$	$true$
$\exists$	$\mathbb{B}$	$false$

String mit Konkatenation nicht-abelsches Monoid
$("a" + "b") + "c"\ equals\ "a" + ("b" + "c")$
$"a" + ""\ equals\ "a"$
$"a" + "b"\ !equals\ "b" + "a"$ (nicht equals)

- $T_1, ..., T_n$ Datentypen

- $V_1, ..., V_n$ Variablen

alle paarweise verschieden

V_i vom Typ: T_i

- R : boolescher Ausdruck, kann $V_1 ... V_n$ enthalten, Bereich (Range)

- P : beliebiger Ausdruck vom Typ T, kann $V_1 ... V_n$ enthalten, Koerper (Body)

Typ der Quantifizierung : T

$(\forall i : \mathbb{N} \mid 0 \leqslant i \leqslant n : b[i] = 0)$ und das Ganze ist : $\mathbb{B}$
$(\circ\, V_1 : T_1 \mid R : P)$ wobei $T_1 : \mathbb{N}, P : \mathbb{B}$

$\wedge : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$

$P : T_1 \times T_2 \times ... \times T_n \to T$

1.3 Semantik

Bsp: $(+i : \mathbb{Z} \mid -1 \leqslant i \leqslant 2 : i^2)$

1. Fall (Topf $\neq \emptyset$)

Von $\mathbb{Z}$ alle Zahlen ausfiltern (-1,0,1,2) (Menge)

$\to^{1^2}$ $((-1)^2, 1^2, 0^2, 2^2)(1, 1, 0, 4)$ (Multimenge)

$\to 2^2 + 1^2 + (-1)^2 + 0^2$

2. Fall (Topf = 0)

$\to$ Topf leer $\to$ Resultat: Neutrales Element (von +) $\to 0$

Beispiele:

1) $(+\, i : \mathbb{N} \mid 0 \leqslant i \leqslant 4 : i * 8) = (0 * 8) + (1 * 8) + ...$

2) $(*\, i : \mathbb{N} \mid 0 \leqslant i \leqslant 3 : i + 1) = (0 + 1) * (1 + 1) * ...$

3) $(\wedge\, i : \mathbb{N} \mid 0 \leqslant i \leqslant 2 : i * d \neq 6) = (0 * d) \neq 6 \wedge (1 * d) \neq 6 \wedge ...$

4) $(\vee\, i : \mathbb{N} \mid 0 \leqslant i \leqslant 21 : b[i] = 0) = b[0] = 0 \vee b[1] = 0 \vee ...$

5) $(\sum k : \mathbb{N} \mid k^2 = 4 : k^2) = 2$

6) $(\sum k : \mathbb{Z} \mid k^2 = 4 : k^2) = 2 + (-2) = 0$

---

2 2. Woche

$(\circ\, v_1 : T_1, ..., v_n : T_n \mid R : P)$

E1: $\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^2)$

- Wert haengt von n ab, nicht von i

$n = 3 :$ 0 1 2

$0^2 + 1^2 + 2^2 = 5$

$n = 0 :$ kein i

0 (neutral +)

E2: $(\sum j : \mathbb{Z} \mid 0 \leqslant j < n : j^2)$

$n = 3 \rightarrow 5$

$n = 0 \rightarrow 0$

E1: $(\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^2)$

E3: $(\sum i\, ① : \mathbb{Z} \mid 0 \leqslant i\, ② < n : i^2\, ③) + 1\, ④$

$(\leftarrow\rightarrow)$: Gueltigkeitsbereich von i (scope)

i tritt hier 4 mal auf (occurs)

Auftreten (occurances) 1, 2, 3 gebunden
Auftreten 4 frei
2 und 3 gebunden an 1
2 und 3 angewandte Auftreten (applied)
1 bindende, deklarierende Auftreten (binding)

Eine Variable heisst frei in einem Ausdruck E (expresion), falls sie in E frei vorkommt.

$FV(E) =$ Menge der freie Variablen von E

$FV(E_3) = \{'n', 'i'\}$ (Die Variablennamen und nicht die Werte der Variablen)

$x, y : \mathbb{Z}$
$x = 3, y = 5$
$\{x, y\} = \{3, 5\}$

$x = y = 3$
$\{x, y\} = \{3\}$

$x + y * 2$
$y, 2 : *$ Operator
dann das Resultat mit x und $+$ Operator

E4: $(\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^2) * (\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^3)$

$FV(E_4) = \{'n'\}$

E5: $(\prod n \mid k \leqslant n \leqslant l : (\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^2) * (\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^3))$

$FV(E_5) = \{'k', 'l'\}$

E6: $(\sum i : \mathbb{Z} \mid 0 \leqslant i \leqslant (\sum i : \mathbb{Z} \mid 2 \leqslant i < 3 : i^2) : i^2)$