# Diskrete Mathematik 2

FS 2013

# Contents

# 1 Semesterablauf(?)

- Arithmetik in $\mathbb{Z}$

- Modulares Rechnen

- Gruppen

- RSA

- Quantifizierung

- Induktion
    - Rekurision
    - Invarianten

---

- Kein Laptop

- Zwischenpruefung: 30.04.2013 (1 Stunde)

---

- Buecher:

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

    - Jean Gallier
      Discrete Math
      Springer, 2010

    - Struckermann/Waetiger
      Mathematik fuer Informatiker
      Spektrum, 2007

---

# 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) — 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 $T_1 : \mathbb{N}, P : \mathbb{B}$

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

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

---

# 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)

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

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

2. Fall (Topf = 0)

$\rightarrow$ Topf leer $\rightarrow$ Resultat: Neutrales Element (von +) $\rightarrow$ 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) $(\sum k : \mathbb{Z} \mid k^2 = 4 : k^2) = 2 + (-2) = 0$

### 3.1 This is a subsection