
Diskrete Mathematik 2

FS 2013

Contents

1	Erste Woche	1
1.1	Semesterablauf	1
1.2	Quantifizierung	1
1.3	Semantik	3
2	Zweite Woche	4
2.1	Freie/Gebundene Variablen	4
3	Dritte Woche	6
3.1	Saetze zur Quantifizierung	6
4	Vierte Woche	8
4.1	???	8
4.2	Anwendung	9

1 Erste Woche

1.1 Semesterablauf

- Arithmetik in \mathbb{Z}
- Modulares Rechnen
- Gruppen
- RSA
- Quantifizierung
- Induktion
 - Rekursion
 - Invarianten

-
- Kein Laptop
 - Zwischenprüfung: 30.04.2013 (1 Stunde)
 - 5. März 2013 Unterricht nur bis 18:20

-
- Bücher:
 - 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

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

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

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

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

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

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

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

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

(Java ==)

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

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

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

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

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

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

$$\text{Bsp: } + : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$+(3, 4) = 7$$

$$\text{ABELSCHES MONOID} \left\{ \begin{array}{l} a \circ b = b \circ a \text{ fuer alle } a, b : T \text{ (Symmetrie) (Kommutativitaet)} \\ \text{MONOID} \left\{ \begin{array}{l} (a \circ b) \circ c = a \circ (b \circ c) \text{ fuer alle } a, b, c : T \text{ (Assoziativitaet)} \\ u \circ a = a = a \circ u \\ \text{es gibt ein } u : T, \text{ so dass fuer alle } a : T \text{ (neutrales Element)} \end{array} \right. \end{array} \right.$$

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

String mit Konkatination: Nicht-abelsches Monoid

$(\text{"a"} + \text{"b"}) + \text{"c"} \text{ equals } \text{"a"} + (\text{"b"} + \text{"c"})$

$\text{"a"} + \text{""} \text{ equals } \text{"a"}$

$\text{"a"} + \text{"b"} \text{ !equals } \text{"b"} + \text{"a"} \text{ (nicht equals)}$

- T_1, \dots, T_n Datentypen

- V_1, \dots, V_n Variablen

alle paarweise verschieden

V_i vom Typ: T_i

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

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

Typ der Quantifizierung : T

$(\forall i : \mathbb{N} \mid 0 \leq i \leq n : b[i] = 0)$ und das Ganze ist : \mathbb{B}

$(\circ V_1 : T_1 \mid R : P)$ wobei $T_1 : \mathbb{N}, P : \mathbb{B}$

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

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

1.3 Semantik

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

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:

$$1) (+ i : \mathbb{N} \mid 0 \leq i < 4 : i * 8) = (0 * 8) + (1 * 8) + \dots$$

$$2) (* i : \mathbb{N} \mid 0 \leq i < 3 : i + 1) = (0 + 1) * (1 + 1) * \dots$$

$$3) (\wedge i : \mathbb{N} \mid 0 \leq i < 2 : i * d \neq 6) = ((0 * d) \neq 6) \wedge ((1 * d) \neq 6) \wedge \dots$$

$$4) (\vee i : \mathbb{N} \mid 0 \leq i < 21 : b[i] = 0) = (b[0] == 0) \vee (b[1] == 0) \vee \dots$$

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

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

2 Zweite Woche

2.1 Freie/Gebundene Variablen

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

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

- Wert haengt von n ab, nicht von i

$$n = 3 : \quad 0 \quad 1 \quad 2$$

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

$n = 0$: kein i

$$0 \text{ (neutral +)}$$

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

$$n = 3 \rightarrow 5$$

$$n = 0 \rightarrow 0$$

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

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

i tritt hier 4 mal auf (occurs)

Auftreten (occurrences) $\textcircled{1}, \textcircled{2}, \textcircled{3}$ gebunden

Auftreten $\textcircled{4}$ frei

$\textcircled{2}$ und $\textcircled{3}$ gebunden an $\textcircled{1}$

$\textcircled{2}$ und $\textcircled{3}$ angewandte Auftreten (applied)

$\textcircled{1}$ 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)

$$x, y : \mathbb{Z}$$

$$x = 3, y = 5$$

$$\{x, y\} = \{3, 5\}$$

$$x = y = 3$$

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

$$x + y * 2$$

$$y, 2 : * \text{ Operator}$$

dann das Resultat mit x und $+$ Operator

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

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

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

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

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

$$FV(E_6) = \emptyset$$

Ein Ausdruck E ohne freie Variablen ($FV(E) = \emptyset$ oder $\{ \}$) heisst geschlossen

$$(\sum i : \mathbb{Z} \mid 1 \leq i < 2 : (\sum j : \mathbb{Z} \mid 1 \leq j < 3 : i + j))$$

i zuerst:

$$i : \quad \quad \quad \begin{matrix} 1 \\ (\sum j : \mathbb{Z} \mid 1 \leq j < 3 : 1 + j) \end{matrix} + \begin{matrix} 2 \\ (\sum j : \mathbb{Z} \mid 1 \leq j < 3 : 2 + j) \end{matrix}$$

$$j : \quad \begin{matrix} 1 & 2 & 3 \\ ((1 + 1) + (1 + 2) + (1 + 3)) \end{matrix} + \begin{matrix} 1 & 2 & 3 \\ ((2 + 1) + (2 + 2) + (2 + 3)) \end{matrix}$$

j zuerst:

$$j : \quad \quad \quad \begin{matrix} 1 & 2 & 3 \\ (\sum i : \mathbb{Z} \mid 1 \leq i < 2 : ((i + 1) + (i + 2) + (i + 3))) \end{matrix}$$

$$i : \quad \quad \quad \begin{matrix} 1 \\ ((1 + 1) + (1 + 2) + (1 + 3)) \end{matrix} + \begin{matrix} 2 \\ ((2 + 1) + (2 + 2) + (2 + 3)) \end{matrix}$$

3 Dritte Woche

3.1 Sätze zur Quantifizierung

Satz (Dummy renaming)

$$(\circ v \mid R : P) = (\circ w \mid R[v \leftarrow w] : P[v \leftarrow w])$$

Voraussetzung: $w \notin FV(R) \cup FV(P)$

Dabei: $E[v \leftarrow F]$ bezeichnet exakt denselben Ausdruck wie E , aber alle freien Auftreten von v ersetzt durch (F) .

wobei E, F : Ausdruck, v : Variable

$$\text{Bsp: } (i + 5)[i \leftarrow j + 3] = (j + 3) + 5$$

wobei $(i + 5) : E$, $[i : v, j + 3 : F]$

$$(i * 5)[i \leftarrow j + 3] = (j + 3) * 5$$

$$(\sum i \mid \text{true} : i^2)[i \leftarrow j + 3] = (\sum i \mid \text{true} : i^2)$$

$$(\sum i \mid \text{true} : i^2) = (\sum j \mid \text{true} : j^2)$$

$$= (\sum j \mid true[i \leftarrow j] : i^2[i \leftarrow j])$$

$$= (\sum j \mid true : j^2)$$

$$42[i \leftarrow j + 3] = 42 \text{ "Man kann die Bedeutung des Universums nicht aendern."}$$

Es ist ein Unterschied, ob die Ersetzung innerhalb oder ausserhalb einer Quantifizierung angegeben wird.

$$(\sum i \mid true : i^2)[i \leftarrow j + 3]$$

Hier sollen alle freien Auftreten von Variable i in $(\sum i \mid true : i^2)$ durch $j + 3$ ersetzt werden.
Aber alle Auftreten von i sind in diesem Ausdruck gebunden, also ist nichts zu ersetzen.

Dummy renaming sagt aus, dass wir die gebundenen Auftreten einer Variablen innerhalb einer Quantifizierung konsistent umbenennen duerfen, solange wir dabei keine freien Variablen einfangen.

$$\begin{aligned} & (\sum i \mid 1 \leq i \leq n : i^2) \\ &= (\sum j \mid 1 \leq i \leq n[i \leftarrow j] : i^2[i \leftarrow j]) \\ &= (\sum j \mid 1 \leq j \leq n : j^2) \end{aligned}$$

Hier sind die Ersetzungen innerhalb der Quantifizierung.
Und beachten Sie: im Teilausdruck $1 \leq i \leq n$ ist die Variable i frei,
daher liefert $1 \leq i \leq n[i \leftarrow j]$ den Ausdruck $1 \leq j \leq n$

Im Gesamtausdruck $(\sum i \mid true : i^2)$ sind alle Auftreten von i hingegen gebunden.
Aber in diesem Ausdruck wollen wir auch nicht ersetzen, sondern eben in den beiden Teilausdruecken.

Ein Auftreten einer Variablen kann in einem Teilausdruck frei sein, aber im Gesamtausdruck gebunden.
Ob ein Auftreten frei oder gebunden ist, hängt immer vom betrachteten (Teil-)Ausdruck ab.

$$\text{Bsp: } (\sum i \mid 1 \leq i \leq n : i^2)$$

$$\text{wobei } i : v, (1 \leq i \leq n) : R, i^2 : P$$

$$= (\sum j \mid (1 \leq i \leq n)[i \leftarrow j] : i^2[i \leftarrow j])$$

$$\text{wobei } j : w$$

$$= (\sum j \mid 1 \leq j \leq n : j^2)$$

Aber: Vorsicht:

$$\begin{aligned} & (\sum i : \mid 1 \leq i \leq n : i^2) \\ & n = 0, \quad 0(\text{neutral}+) \\ & n = 1, \quad 1 \end{aligned}$$

haengt von n ab

\neq

$(\sum n : | 1 \leq n \leq n : n^2)$
 ∞ undefiniert

haengt nicht von n ab

4 Vierte Woche

4.1 ???

$$(\sum i \mid 0 \leq i \leq n : i^2)[n \leftarrow n^2] = (\sum i \mid 0 \leq i \leq n^2 : i^2)$$

$(\sum i \mid 0 \leq i \leq n : i^2)[n \leftarrow i + 1] \neq (\sum i \mid 0 \leq i \leq i + 1 : i^2)$
 freies Auftreten von i wird gefangen \rightarrow name clash

$$\begin{aligned} & (\sum i \mid 0 \leq i \leq n : i^2)[n \leftarrow i + 1] \\ &= (\sum j \mid 0 \leq j \leq n : j^2)[n \leftarrow i + 1] \\ &= (\sum j \mid 0 \leq j \leq i + 1 : j^2) \end{aligned}$$

Empty range

$(\circ v \mid false : P) = u_\circ$ (Neutrales Element)

One point

Voraussetzung: $v \notin FV(E)$

$$(\circ v \mid v = E : P) = P[v \leftarrow E]$$

$$\text{Bsp. } (\sum i \mid i = j + 3 : i^2) = i^2[i \leftarrow j + 3] = (j + 3)^2$$

$$(\sum i \mid i = j + i + 3 : i^2) \neq i^2[i \leftarrow j + i + 3] = (j + i + 3)^2$$

Split-off term

$$(\circ i \mid 0 \leq i < n + 1 : P) = (\circ i \mid 0 \leq i < n : P) \circ P[i \leftarrow n]$$

$$\begin{aligned} \text{Bsp. } (\sum i \mid 0 \leq i < n + 1 : i^2) &= (\sum i \mid 0 \leq i < n : i^2) + n^2 \\ 0^2 + 1^2 + \dots + (n - 1)^2 + n^2 &= (0^2 + 1^2 + \dots + (n - 1)^2) + n^2 \end{aligned}$$

$$\begin{aligned}
n = 0 : \\
(\circ i \mid 0 \leq i < 1 : P) &= (\circ i \mid 0 \leq i < 0 : P) \circ P[i \leftarrow 0] \\
i = 0 : \\
P[i \leftarrow 0] \text{ (One point)} &= u_{\circ} \circ P[i \leftarrow 0]
\end{aligned}$$

4.2 Anwendung

Praedikat

$i + 1 > j : Bool$ macht Aussage ueber Werte von freien Variablen

Feld $b[0...n-1]$ mit ganzen Zahlen; $n \geq 0$

" b enthaelt eine -1 ." \rightarrow bedeutet mindestens

$$(\exists i : \mathbb{N} \mid 0 \leq i < n : b[i] = -1)$$

" b enthaelt genau eine -1 ."

$$(\exists i : \mathbb{N} \mid 0 \leq i < n : (b[i] = -1) \wedge (\forall j : \mathbb{N} \mid (0 \leq j < n) \wedge (j \neq i) : b[j] \neq -1))$$

=

$$1 = (\sum i : \mathbb{N} \mid (0 \leq i < n) \wedge (b[i] = -1 : 1))$$

&&

" b enthaelt keine -1 ."

$$(\forall i : \mathbb{N} \mid 0 \leq i < n : b[i] \neq -1)$$

=

$$\neg(\exists i : \mathbb{N} \mid 0 \leq i < n : b[i] = -1)$$
