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 Saetze zur Quantifizierung (Fortsetzung) . . . 8
4.2 Anwendung . . . 9

5 Fuenfte Woche **10**
5.1 Magisches Quadrat . . . 10
5.2 Mathematische Induktion . . . 10

6 Sechste Woche **12**
6.1 Vollstaendige Induktion . . . 12

7 Siebte Woche **16**
7.1 Zahlentheorie . . . 16

1 Erste 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

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

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

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

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

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

$\sum_{\substack{i=1 \\ odd(i)}}^{n} i^2 = 1^2 + 3^2 + ... + n^2$, 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: $+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
$+(3, 4) = 7$

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

$\circ$	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 $T_1 : \mathbb{N}, P : \mathbb{B}$

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

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

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)

$\rightarrow^{1^2}$ $((-1)^2, 1^2, 0^2, 2^2)(1, 1, 0, 4)$ (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) $(+\, i : \mathbb{N} \mid 0 \leqslant i < 4 : i * 8) = (0 * 8) + (1 * 8) + ...$

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

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

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

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 Zweite Woche

2.1 Freie/Gebundene Variablen

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

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

- Wert haengt von n ab, nicht von i

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

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

$n = 0$: kein i

0 (neutral +)

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

$n = 3 \rightarrow 5$

$n = 0 \rightarrow 0$

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

$FV(E_6) = \emptyset$

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

---

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

<u>i zuerst:</u>

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

$j:$ $\quad ((\overset{1}{(1+1)} + \overset{2}{(1+2)} + \overset{3}{(1+3)}) + (\overset{1}{(2+1)} + \overset{2}{(2+2)} + \overset{3}{(2+3)}))$

<u>j zuerst:</u>

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

$i:$ $\quad \overset{1}{((1+1) + (1+2) + (1+3))} + \overset{2}{((2+1) + (2+2) + (2+3))}$

---

3 Dritte Woche

3.1 Saetze zur Quantifizierung

<u>Satz</u> (Dummy renaming)

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

<u>Voraussetzung:</u> $w \notin FV(R) \cup FV(P)$

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

wobei E, F : Ausdruck, v : Variable

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

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

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

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

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

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

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

$42[i \leftarrow j+3] = 42$ "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.

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

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

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.

Bsp: $(\sum i \mid 1 \leqslant i \leqslant n : i^2)$

wobei $i : v$, $(1 \leqslant i \leqslant n) : R$, $i^2 : P$

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

wobei $j : w$

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

<u>Aber:</u> Vorsicht:

$(\sum i : \mid 1 \leqslant i \leqslant n : i^2)$
$n = 0, \qquad 0(neutral+)$
$n = 1, \qquad 1$

haengt von n ab

$\neq$

$(\sum n : \mid 1 \leqslant n \leqslant n : n^2)$
∞ undefiniert

haengt <u>nicht</u> von n ab

---

4 Vierte Woche

4.1 Saetze zur Quantifizierung (Fortsetzung)

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

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

$(\sum i \mid 0 \leqslant i < n : i^2)[n \leftarrow i + 1]$
$= (\sum j \mid 0 \leqslant j < n : j^2)[n \leftarrow i + 1]$
$= (\sum j \mid 0 \leqslant j < i + 1 : j^2)$

<u>Empty range</u>

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

<u>One point</u>

Voraussetzung: $v \notin FV(E)$

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

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

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

<u>Split-off term</u>

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

Bsp. $(\sum i \mid 0 \leqslant i < n + 1 : i^2) \quad = (\sum i \mid 0 \leqslant i < n : i^2) + n^2$
$0^2 + 1^2 + ... + (n-1)^2 + n^2 \quad = (0^2 + 1^2 + ... + (n-1)^2) + n^2$

$n = 0:$

$(\circ\, i \mid 0 \leqslant i < 1 : P) = (\circ\, i \mid 0 \leqslant i < 0 : P) \circ P[i \leftarrow 0]$

$i = 0:$

$P[i \leftarrow 0]$ (One point) $= u_\circ$(empty range) $\circ P[i \leftarrow 0]$

4.2 Anwendung

Praedikat

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

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

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

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

"b enthaelt genau eine -1."

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

$=$

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

"b enthaelt keine -1."

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

$=$

$\neg(\exists i : \mathbb{N} \mid 0 \leqslant i < n : b[i] = -1) \rightarrow (\neg$ ("b enthaelt mindestens eine -1."))

$\neg(\exists v \mid R : P) = (\forall v \mid R : \neg P)$

$\neg(\forall v \mid R : P) = (\exists v \mid R : \neg P)$

de Morgan

$$\begin{aligned}\neg(\exists v \mid R : P) &= \neg(P_0 \vee P_1 \vee ... \vee P_{n-1} \vee P_n)\\ &= ((\neg P_0) \wedge (\neg P_1) \wedge ...(\neg P_n))\\ &= (\forall v \mid R : \neg P)\end{aligned}$$

---

5 Fuenfte Woche

5.1 Magisches Quadrat

Uebungsblatt 2, Aufgabe 3

$k, i : 1 \leqslant k \leqslant n, 1 \leqslant i \leqslant n$

1) $$\begin{aligned}(\exists M : \mathbb{N} \mid true : (\forall i \mid 1 \leqslant i \leqslant n : &(\sum k \mid 1 \leqslant k \leqslant n : Q[i,k]) = M\\ &\wedge(\sum k \mid 1 \leqslant k \leqslant n : Q[k,i]) = M\\ &\wedge(\sum k \mid 1 \leqslant k \leqslant n : Q[k,k]) = M\\ &\wedge(\sum k \mid 1 \leqslant k \leqslant n : Q[k,(n+1)-k)]) = M\\ &\wedge(\forall m : N \mid 1 \leqslant m \leqslant n^2 :\\ &\quad (\exists i,j \mid 1 \leqslant i < n \wedge 1 \leqslant j < n : m = Q[i,j])))\end{aligned}$$

2) $M = \frac{\sum_{i=1}^{n^2} i}{n}$

$n * M = (\sum i \mid 1 \leqslant i \leqslant n^2 : i)$

$M = \frac{(\sum i \mid 1 \leqslant i \leqslant n^2 : i)}{n} = \frac{n^2 * (n^2+1)}{2*n} = \frac{n*(n^2+1)}{2}$

5.2 Mathematische Induktion

$(\mathbb{B} : Boolean)$

Sei $P : \mathbb{N} \rightarrow \mathbb{B}$
zu zeigen:
$(\forall n : \mathbb{N} \mid true : P(n))$

Beispiel

$P(n) : n^3 + 5 * n$ ist ein Vielfaches von 6

z ist Vielfaches von 6 heisst:
$(\exists i : \mathbb{Z} \mid true : i * 6 = z)$

$0^3 + 5 * 0 = 0(\text{Zeuge}) * 6$
$1^3 + 5 * 1 = 1 * 6$

$2^3 + 5 * 2 = 3 * 6$ (Muss bei allen *true* zurueck geben!!)

Idee: Induktionsprinzip

Man zeigt:

1) $P(0)$
2) $P(n) \Rightarrow P(n+1)$ fuer alle $n : \mathbb{N}$

$P(0)$ gilt: Wegen 1)

$(P(0) \wedge (P(0) \Rightarrow P(1)) \Rightarrow P(1)$
wegen 2) mit $n = 0$

$(P(1) \wedge (P(1) \Rightarrow P(2)) \Rightarrow P(2)$
wegen 2) mit $n = 1$

Damit gilt $P(n)$ fuer alle $n : \mathbb{N}$

Unser Beispiel

1) Induktionsanfang (Base case)
zu zeigen: $P(0)$
$0^3 + 5 * 0 = 0(\text{Zeuge}) * 6$

2) Induktionsschritt (inductive step)
zu zeigen: $P(n) \Rightarrow P(n+1)$ fuer alle $n : \mathbb{N}$

Sei n eine beliebige natuerliche Zahl.

Annahme: Es gaelte $P(n) : n^3 + 5 * n$, dass heisst $n^3 + 5 * n = 6 * r$, mit $r : \mathbb{Z}$, ist vielfaches von 6.
zu zeigen: (unter dieser Annahme) $P(n+1) : (n+1)^3 + 5 * (n+1)$ ist vielfaches von 6.
das heisst: $(n+1)^3 + 5 * (n+1) = 6 * s$, mit $s : \mathbb{Z}$

$(n+1)^3 + 5 * (n+1)$

<Arith>

$= (n^3 + 3 * n^2 + 3 * n + 1) + (5 * n + 5)$

<Arith + Kaninchen>

$= (n^3 + 5 * n) + (3 * n^2 + 3 * n + 6)$

<Annahme>

$= 6 * r + 3 * n^2 + 3 * n + 6$

<Arith + Kaninchen>

$= 6 * r + 3 * n * (n+1) + 6$

<n*(n+1) ist gerade>

$= 6 * r + 3 * (2 * t) + 6$

<Arith>

$= 6 * (r + t + 1)$ (Zeuge) ✓

Modus ponens

p	q	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
f	f	w
f	w	w
w	f	w
w	w	w

$(p \Rightarrow r) \wedge (\neg p \Rightarrow s)$

$\equiv (p \wedge r) \vee (\neg p \wedge s)$

Sei p. Dann

$$\begin{array}{ll} & (p \Rightarrow r) \wedge (\neg p \Rightarrow s) \\ = & \quad r \quad \wedge \quad true \\ = & \quad r \end{array}$$

$$\begin{array}{ll} & (p \wedge r) \vee (\neg p \wedge s) \\ = & \quad r \quad \vee \quad false \\ = & \quad r \end{array}$$

Sei $\neg p$ Analog

---

6 Sechste Woche

6.1 Vollstaendige Induktion

Arbeitsblatt 1 - Aufgabe 1

$(P(0) \wedge (\forall n : \mathbb{N} \mid : P(n) \Rightarrow P(n+1)) \Rightarrow (\forall n : \mathbb{N} \mid : P(n))$

wobei $P(0)$: Base Case
$(\forall n : \mathbb{N} \mid : P(n) \Rightarrow P(n+1))$: Iductive Case
$(\forall n : \mathbb{N} \mid : P(n))$: Ziel der Induktion

Complete Induction

$P(0)$
$(P(0) \wedge (P(0) \Rightarrow P(1))) \Rightarrow P(1)$
$(P(0) \wedge P(1) \wedge (P(0) \wedge P(1) \Rightarrow P(2))) \Rightarrow P(2)$
$(P(0) \wedge P(1) \wedge P(2) \wedge (P(0) \wedge P(1) \wedge P(2) \Rightarrow P(3))) \Rightarrow P(3)$

$(P(0) \wedge (\forall n : \mathbb{N} \mid : (\forall k : \mathbb{N} \mid k \leqslant n : P(k)) \Rightarrow P(n+1)) \Rightarrow (\forall n : \mathbb{N} \mid : P(n))$

Aufgabe 2

Sei $k : \mathbb{N}$, $k \geqslant 0$

$(P(k) \wedge (\forall n : \mathbb{N} \mid n \geqslant k : P(n) \Rightarrow P(n+1)) \Rightarrow (\forall n : \mathbb{N} \mid n \geqslant k : P(n))$

Fibonacci

$fib : \mathbb{N} \to \mathbb{N}$

A $fib(0) = 0$
B $fib(1) = 1$
C $fib(n) = fib(n-1) + fib(n-2)$, $n \geqslant 2$

Satz Fuer alle $n : \mathbb{N}$ gilt:

$P(n) : (\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n : fib(i)) = f(n+2) - 1$

Beweis

1) Induktionsanfang: zu zeigen: $P(0)$, also

$(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant 0 : fib(i)) = f(0+2) - 1$

$(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant 0 : fib(i))$

$<$ empty range, neutral $+$ $>$

$= 0$

$fib(0+2) - 1$

$<$ arith $>$

$= fib(2) - 1$

$<$ C mit $n = 2$ $>$

$= fib(0) + fib(1) - 1$

$<$ A, B $>$

$= 0 + 1 - 1$

$<$ arith $>$

$= 0$

2) Induktionsschritt:

Sei n eine beliebige natuerliche Zahl

Annahme: $(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n : fib(i)) = fib(n+2) - 1$

zu zeigen: $(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n+1 : fib(i)) = fib(n+3) - 1$

$(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n+1 : fib(i))$

$<$ range split (split-off term) $>$

$= (\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n : fib(i)) + fib(n+1)$

$<$ Annahme $>$

$= fib(n+2) - 1 + fib(n+1)$

$<$ arith $>$

$= (fib(n+2) + fib(n+1)) - 1$

$<$ C, mit $n+3 \geqslant 2$ $>$

$= fib(n+3) - 1$

□

Satz:

Fuer alle $n : \mathbb{N}$ mit $n \geqslant 3$ gilt:

$2n + 1 < 2^n$

Beweis

1) IA

$2 * 3 + 1 < 2^3 \equiv 7 < 8$ ✓

2) IS

Sei n eine beliebige natuerliche Zahl mit $n \geqslant 3$
Annahme Es gelte: $2n + 1 < 2^n$
zu zeigen: Es gilt: $2(n+1) + 1 < 2^(n+1)$

Beweis

$2(n+1)+1$

$\quad < \text{arith} >$

$= (2n+1)+2$

$\quad < \text{Annahme} >$

$\Rightarrow (2n+1)+2 < 2^n + 2$

$\leqslant$

$2^n + 2^n$

$\quad < \text{arith} >$

$= 2^n + 1$ ✓

$2 * 2 * ... * 2 = 2^n$
(n mal)

$pow1(n) = (\prod i : \mathbb{N} \mid 1 \leqslant i \leqslant n : 2)$

$pow2(n) \begin{cases} 2^0 = 1 \\ 2^n = 2 * 2^{n-1}, \text{ fuer } n > 0 \end{cases}$

```
int pow1(int n){
        int p=1;
        for(int i=1; i<=n; i++){
                p*=2;
        }
        return p;
}

int pow2(int n){
        return (n==0)? 1: 2*pow2(n-1);
}
```

<u>Satz:</u> Fuer alle $n : \mathbb{N}$ gilt: $pow1(n) = pow2(n)$

<u>Beweis</u> Aufgabe!

$x < y \Rightarrow x \leqslant y$

$x \leqslant y \Rightarrow x < y \vee x = y$

$p \Rightarrow p \vee q$

---

7 Siebte Woche

7.1 Zahlentheorie

Teilbarkeit

$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$, $c, b : \mathbb{Z}$

$c \backslash b \equiv (\exists k : \mathbb{Z} \,|\, : b = k * c)$

$c \backslash b$: "c teilt b"
"b ist teilbar durch c"
"c ist Teiler von b"
"b ist Vielfaches von c"

Beispiel:

$7 \backslash 13 = false$
$(-7) \backslash 14 = true$
nicht einheitlich in Literatur $\begin{cases} 0 \backslash 14 = false \\ 0 \backslash 0 = true \text{ (es existiert kein } k) \end{cases}$

Satz $b, c, d : \mathbb{Z}$

(1) $c \backslash c$ (Reflektivitaet)
(2) $c \backslash 0$
(3) $1 \backslash b$
(4) $c \backslash 1 \Rightarrow c = 1 \vee c = -1$
(5) $d \backslash c \wedge c \backslash b \Rightarrow d \backslash b$ (Transitivitaet)
(6) $b \backslash c \wedge c \backslash b \Rightarrow b = c \vee b = -c$
auf $\mathbb{Z}$ also nicht antisymmetrisiert, auf $\mathbb{N}$ aber schon
(7) $b \backslash c \Rightarrow b \backslash (c * d)$
(8) $b \backslash c \Rightarrow (b * d) \backslash (c * d)$
(9) $1 < b \wedge b \backslash c \Rightarrow \neg(b \backslash (c + 1))$

(1) und (5) und (6) heisst: \-Relation ist eine partielle Ordnung auf $\mathbb{N}$ (aber nicht auf $\mathbb{Z}$)

Beweis:

(1) zu zeigen: es gibt $k : \mathbb{Z}$ mit $c = k * c$
Waehle $k = 1 : \mathbb{Z}$
(2) $0 = k * c, k = 0 : \mathbb{Z}$
(3) $b = k * 1, k = b : \mathbb{Z}$
(4) $1 = k * c = 1 * 1 = (-1) * (-1) \Rightarrow c = 1 \vee c = -1$
(5)
$d \backslash c$, also gibt es $k_1 : \mathbb{Z}$ mit $c = k1 * d$
$c \backslash b$, also gibt es $k_2 : \mathbb{Z}$ mit $b = k2 * c$
aber $b = k_2 * c = k_2 * (k_1 * d) = (k_2 * k_1) * d$
also gibt es $k = k_1 * k_2 : \mathbb{Z}$ mit$b = k * d$, also $d \backslash b$
(6)
$b \backslash c$, also gibt es $k_1 : \mathbb{Z}$ mit $c = k1 * b$

$c \backslash b$, also gibt es $k_2 : \mathbb{Z}$ mit $b = k2 * c$
also $b = k_2 * c = k_2 * (k_1 * b) = (k_2 * k_1) * b$
also $b - (k_2 * k_1) * b = 0$
also $b - (1 - k_2 * k_1) = 0$
also $b = 0 \vee 1 - k_2 * k_1 = 0$
also $b = 0 \vee k_2 * k_1 = 1$
also $b = 0 \vee k_2 = k_1 = 1 \vee k_2 = k_1 = -1$
also $b = 0 \vee c = b \vee c = -b$
mit $b = 0$ ist $c = b$
