Diskrete Strukturen und Logik

WiSe 2007/08 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

Diskrete Strukturen und Logik Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- Kombinatorik: Die Kunst des Zählens
- algebraische Strukturen

Kombinatorik

- Summenregel
- Produktregel
- Inklusions-/ Exklusionsprinzip
- Funktionenanzahlen

Summenregel I

Satz: Sind A und B disjunkte endliche Mengen, so gilt:

$$|A \cup B| = |A| + |B|.$$

Beweis: Die Aussage ist trivial für $|B| = 0$, also $B = \emptyset$.

Die Aussage ist ebenso klar für $|B| = 1$, also $B = \{a\}$ für ein $a \notin A$. (*)

Im IS nehmen wir an, die Aussage würde für alle B mit $|B| \leq n$ gelten.

Betrachte ein B mit $|B| = n + 1$. Also ist $B \neq \emptyset$.

Wähle $b \in B$ willkürlich, aber fest. Auf $B' = B \setminus \{b\}$ lässt sich die IV anwenden.

$\rightsquigarrow |A \cup B'| = |A| + |B'|$.

Wegen (*) gilt $|A \cup B| = |(A \cup B' \cup \{b\}| = |A| + (|B'| + 1) = |A| + |B' \cup \{b\}| = |A| + |B|$. $\rightsquigarrow$ Beh.

Summenregel Interpretation

Manchmal ist es hilfreich für das Verständnis, Mengen möglicher Versuchsausgänge eines Experimentes zu betrachten.

Angenommen, wir könnten für einen Versuch die möglichen (endlich vielen) Ergebnisse in zwei Typen klassifizieren: Typ A bzw. B.
Das soll bedeuten, dass jeder Versuchsausgang vom Typ A oder vom Typ B ist, aber nicht von beiden Typen.

Gibt es $\mathrm{n_A}$ viele Ausgänge vom Typ A und $\mathrm{n_B}$ viele vom Typ B, dann gibt es $\mathrm{n} = \mathrm{n_A} + \mathrm{n_B}$ viele Versuchsausgänge insgesamt.

Summenregel II (allgemein)

Satz: Sei $k \in \mathbb{N}$ und $A_1, \ldots, A_k$ seien endliche, paarweise disjunkte Mengen. Dann gilt:

$$\left| \bigcup_{i=1}^{k} A_i \right| = \sum_{i=1}^{k} |A_i| \,.$$

Beweis: Die Aussage stimmt für $k \leq 1$.

Angenommen, sie gilt für Vereinigungen von höchstens $k-1$ Mengen, $k \geq 1$. Dann gilt:

$$\begin{aligned}
\left|\bigcup_{i=1}^{k} A_i\right| &= \left|\left(\bigcup_{i=1}^{k-1} A_i\right) \cup A_k\right| \\
&= \left|\left(\bigcup_{i=1}^{k-1} A_i\right)\right| + |A_k| \\
&= \sum_{i=1}^{k-1} |A_i| + |A_k|
\end{aligned}$$

Produktregel

Satz: Sind A und B endliche Mengen, so gilt:

$$|A \times B| = |A| \times |B|.$$

Für Mengen $A_1, \ldots, A_k$, $k \in \mathbb{N}$, definieren wir rekursiv:

$$\bigtimes_{i=1}^{k} A_i = \begin{cases} \{\emptyset\}, & k = 0 \\ A_1, & k = 1 \\ \left(\bigtimes_{i=1}^{k-1} A_i\right) \times A_k, & k > 1 \end{cases}$$

Satz: Sei $k \in \mathbb{N}$ und $A_1, \ldots, A_k$ seien endliche Mengen. Dann gilt:

$$\left| \bigtimes_{i=1}^{k} A_i \right| = \prod_{i=1}^{k} |A_i| \,.$$

Beweis: völlig analog zur Summenregel durch *verschachtelte Induktion*:

also: 1. Induktion über k und

2. im Induktionsschritt Induktion über die Mächtigkeit der zweiten Menge; diese "innere Induktion" ist im Beweis des vorigen Satzes "versteckt".

Nachtrag: gerichtete Bäume

Ein *gerichteter Baum* hat folgende Eigenschaften:
Seine *Wurzel* hat als einziger Knoten Ingrad null.
Seine *Blätter* haben als einzige Knoten Ausgrad null.
Alle Knoten außer der Wurzel haben Ingrad eins; der unmittelbare Vorgängerknoten heißt auch *Elternknoten*.
Alle Knoten außer den Blättern haben Ausgrad ungleich null; die unmittelbaren Nachfolgerknoten heißen auch *Kindknoten*.

Satz: Es gibt genau einen gerichteten Pfad von der Wurzel zu jedem Knoten.
Beweis: Betrachte zwei Pfade p, p' von der Wurzel zu einem Knoten x.
Angenommen, der knotenweise Vergleich der zwei Pfade "von hinten" liefert einen Knoten y, der bzgl. p bzw. bzgl. p' zwei verschiedene Vorgänger z und z' hätten.
Dann hätte y einen Ingrad echt größer als Eins, Widerspruch ! Also sind p und p' identisch.

Baumdiagramme

Die Produktregel kann man sich mit einem *Baumdiagramm* veranschaulichen.
(Achtung: *gerichtete Bäume*)

Beispiel: Wie viele Binärzahlen mit drei Ziffern gibt es ?
Da drei Entscheidungen zu fällen sind (für jede Ziffer eine), haben Pfade von der Wurzel bis zu den Blättern stets die Länge drei.
Da es sich um binäre Entscheidungen jeweils handelt, hat jeder Knoten, der kein Blatt ist, zwei Kinder.
Durch Abzählen der Blätter sehen wir die Lösung: acht.
Dies liefert auch die Produktregel: $|\{0,1\} \times \{0,1\} \times \{0,1\}| = 2^3 = 8$.

Ein ausführliches Beispiel

In einigen (älteren) Programmiersprachen beginnt jeder Variablenname mit einem der 26 Buchstaben des Alphabets.
Anschließend folgen bis zu sieben weitere Zeichen, wovon jeder entweder ein Buchstabe oder eine der Ziffern 0 bis 9 ist.
Wie viele verschiedene Variablennamen gibt es ?
Wir können die Menge A der Variablennamen in 8 disjunkte Teilmengen aufteilen: A_i bezeichne all Variablennamen der Länge i, $i = 1, \ldots, 8$.
Summenregel $\rightsquigarrow |A| = |A_1| + |A_2| + |A_3| + |A_4| + |A_5| + |A_6| + |A_7| + |A_8|$.
Offensichtlich gilt: $|A_1| = 26$.
Die Menge der Buchstaben und Ziffern hat nach der Summenregel 36 Elemente.
Die Produktregel liefert: $|A_i| = 26 \cdot 36^{i-1}$.

Eine hilfreiche Formel: die *geometrische Reihe*

Satz: Für Zahlen a und $n \in \mathbb{N}$ gilt:

$$\sum_{i=0}^{n} a^i = \frac{a^{n+1} - 1}{a - 1}.$$

Beweis: per Induktion: IA $n = 0$ ✓. Zum IS; betrachte $n > 0$:

$$\sum_{i=0}^{n} a^i = \left(\sum_{i=0}^{n-1} a^i\right) + a^n = \frac{a^n - 1}{a - 1} + \frac{a^{n+1} - a^n}{a - 1} = \frac{a^{n+1} - 1}{a - 1}.$$

Das liefert im vorigen Beispiel:

$$A = 26 \cdot \left(\sum_{i=0}^{7} 36^i\right) = 26 \cdot \frac{36^8 - 1}{35} \approx 10^{12}.$$

Ein leichtes Korollar: Potenzen

Wir können das (kartesische) Mengenprodukt von gleichen Mengen auch in Potenzschreibweise notieren, d.h.:

$$M^n = \underbrace{M \times \cdots \times M}_{n \text{ mal}}$$

M^n beinhaltet also alle n-Tupel von Elementen aus M.

Übung: Definieren Sie *Mengepotenz*en genauer induktiv !

Folgerung: $|M^n| = |M|^n$. Beweis: Produktgesetz

Inklusions-Exklusionsprinzip | Venn-Diagramme an der Tafel

Satz: Seien A und B endliche Mengen. Dann gilt:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Beweis: Führe einen Induktionsbeweis über die Größe von B.
IA: $|B| = 0 \rightsquigarrow B = \emptyset \rightsquigarrow A \cap B = \emptyset \rightsquigarrow |A| = |A \cup B| = |A| + |B| - |A \cap B| = |A| + 0 - 0$.
IV: Wir nehmen an, die Aussage gelte für Mengen B der Größe höchstens n.
IS: Sei B eine Menge mit $n + 1 \geq 1$ Elementen. Der Fall $A \cap B = \emptyset$ ist durch die Summenregel abgedeckt. Wähle daher $b \in A \cap B$ beliebig, aber fest.
Auf $B' = B \setminus \{b\}$ können wir die Induktionsvoraussetzung anwenden.
$\rightsquigarrow |A \cup B'| = |A| + |B'| - |A \cap B'|$.
Ferner ist (1) $A \cup B = A \cup B'$ und (2) $(A \cap B') \cap \{b\} = \emptyset$. Wegen (2) liefert die Summenregel für $A \cap B = (A \cap B') \cup \{b\}$: $|(A \cap B') \cup \{b\}| = |(A \cap B')| + 1$. Also:

$$\begin{aligned} |A \cup B| &= |A \cup B'| \\ &= |A| + |B'| - |A \cap B'| \\ &= |A| + (|B| - 1) - (|A \cap B| - 1) \\ &= |A| + |B| - |A \cap B| \end{aligned}$$

Inklusions-Exklusionsprinzip: ein Beispiel

Wie viele Folgen der Länge acht über der Menge $\{0,1\}$ fangen mit Null an oder enden mit 11 ?

$$A = \{w \in \{0,1\}^8 \mid \exists x \in \{0,1\}^7 : w = (0,x)\}$$
$$B = \{w \in \{0,1\}^8 \mid \exists y \in \{0,1\}^6 : w = (y,1,1)\}$$
$$A \cap B = \{w \in \{0,1\}^8 \mid \exists z \in \{0,1\}^5 : w = (0,z,1,1)\}$$

$$\rightsquigarrow |A \cup B| = |A| + |B| - |A \cap B| = 2^7 + 2^6 - 2^5 = 160.$$

Inklusions-Exklusionsprinzip II

Satz: Es seien A, B, C endliche Mengen. Dann gilt:

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|.$$

Beweis: $|(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$

$= |A| + |B| + |C| - |A \cap B| - |(A \cap C) \cup (B \cap C)|$

$= |A| + |B| + |C| - |A \cap B| - (|A \cap C| + |B \cap C| - |A \cap B \cap C|)$

Ein Induktionsbeweis ist viel aufwändiger (siehe Meinel-Buch).

Die Formel lässt sich weiter verallgemeinern.
Man muss immer wieder alternierend “zuviel gezählte” Elemente abziehen bzw. zuviel abgezogene Elemente draufzählen.

Inklusions-Exklusionsprinzip III

Zum Formulieren des allgemeinen Prinzips benötigen wir noch eine Schreibweise: Für eine Menge A und eine natürliche Zahl k (meist: $0 \leq \ell \leq |A|$) bezeichnet

$$\binom{A}{\ell}$$

die *Menge der ℓ-elementigen Teilmengen* von A.

Satz: Es seien $A_0, \ldots, A_{k-1}$ endliche Mengen. Dann gilt:

$$\left| \bigcup_{i=0}^{k-1} A_i \right| = \sum_{\ell=1}^{k} (-1)^{k-\ell-1} \left(\sum_{I \in \binom{[k]}{\ell}} \left| \bigcap_{j \in I} A_j \right| \right)$$

Wenn man das I-E-Prinzip nicht beachtet. . .

Studenten haben 28 Vorlesungswochen.
Häufig entfallen davon sowieso noch eine je Semester.
Es verbleiben also noch 26 Wochen.
M.a.W.: Studenten haben das halbe Jahre frei, also 183 Tage frei.
Wir müssen noch berücksichtigen, dass die Wochenenden auch frei sind.
Das sind weitere 52 freie Tage. $\rightsquigarrow$ 232 Tage sind frei.
Auch fleißige Studenten arbeiten an 8 der 24 Stunden des Tages nicht, d.h. an einem Drittel des Jahres, das sind rund 121 Tage. M.a.W.: 354 Tage sind arbeitsfrei. Von den verbleibenden 11 Arbeitstagen sind noch die Feiertage abzuziehen: 3 Tage Weihnachten, 2 Tage Ostern, 2 Tage Pfingsten, 1 Tag Nationalfeiertag, 1 Tag der Arbeit. Es verbleiben noch zwei Arbeitstage, und das sind Rosenmontag und Faschingsdienstag.

Funktionenanzahlen I

Schreibweise: B^A ist die Menge aller Funktionen von A nach B.

Satz: Für endliche Mengen A, B gilt: $|B^A| = |B|^{|A|}$.

Beweis: Jedem Element aus A können $|B|$ verschiedene Elemente zugeordnet werden. Die Zuordnung der Elemente aus B erfolgt unabhängig für verschiedene Elemente aus A. Mit einfacher Induktion über die Größe von A folgt daher:

$$\left|B^A\right| = \underbrace{|B| \cdots |B|}_{|A| \text{ mal}} = |B|^{|A|}.$$

Potenzmengen

Ähnlich wie in der letzten Vorlesung gilt auch im endlichen Fall:
Satz: Für jede endliche Menge M gilt: 2^M und $\{0,1\}^M$ sind gleichmächtig.
Beweis: über Indikatorfunktion χ_N zu $N \subseteq M$

Aus dem Zusammenhang mit Indikatorfunktionen folgt unmittelbar:
Satz: Für jede endliche Menge M gilt: $\left|2^M\right| = 2^{|M|}$.

Binomialkoeffizienten

Gilt $\mathfrak{n} = |\mathfrak{A}|$, so schreiben wir auch:

$$\left(\begin{array}{c} \mathfrak{n} \\ \ell \end{array} \right) := \left| \left(\begin{array}{c} \mathfrak{A} \\ \ell \end{array} \right) \right|$$

und nennen den linken Ausdruck *Binomialkoeffizienten*, gelesen $\mathfrak{n}$ *über* ℓ.

Binomialkoeffizienten—ein kombinatorischer Beweis

Satz: $\sum_{\ell=0}^{n} \binom{n}{\ell} = 2^n$.

Beweis: Wir führen einen *kombinatorischen Beweis*:
Es sei A eine n-elementige Menge.
Für die Potenzmenge wissen wir: $\left|2^A\right| = 2^n$.
Die Potenzmenge lässt sich bezüglich der Mächtigkeit in Klassen einteilen.
Daher liefert die Summenformel:

$$\left|\bigcup_{\ell=0}^{n} \binom{A}{\ell}\right| = \sum_{\ell=0}^{n} \left|\binom{A}{\ell}\right| = \sum_{\ell=0}^{n} \binom{n}{\ell} = 2^n.$$

Ein Induktionsbeweis ist viel aufwändiger (siehe Meinel-Buch).

Funktionenanzahlen II

Erinnerung: Fakultätsfunktion

Satz: Es sei A eine endliche Menge. Die Anzahl der injektiven Funktionen $f : A \to A$ beträgt $(|A|)!$.

Beweis: per Induktion über die Mächtigkeit von A
Für $A = \emptyset$ stimmt es; die einzige Funktion in $\emptyset^\emptyset$ ist injektiv. (Warum ?)
Betrachte eine n-elementige Menge A, $n \geq 1$.
Wähle $a, b \in A$ beliebig. $A' = A \setminus \{a\}$ und $A'' = A \setminus \{b\}$ sind gleichmächtig.
Nach IV gibt es $(n-1)!$ viele Injektionen von $[n-1]$ nach $[n-1]$.
Jede dieser Injektionen g liefert, komponiert mit Bijektionen $\phi : [n-1] \to A'$ und $\psi : [n-1] \to A''$ eine Injektion f von A nach A mit $f(a) = b$ vermöge $f(x) = \psi(g(\phi^{-1}(x)))$ für $x \in A'$.
Umgekehrt liefert jede Injektion f von A nach A mit $f(a) = b$ eine Injektion $g : [n-1] \to [n-1]$ mit $g(j) = \psi^{-1}(f(\phi(j)))$.

Die Summenformel liefert nun die Behauptung (für "unser" $a \in A$):

$$\begin{aligned} |\{f : A \to A \mid f \text{ ist injektiv}\}| &= \left| \bigcup_{b \in A} \{f : A \to A \mid f \text{ ist injektiv} \wedge f(a) = b\} \right| \\ &= \sum_{b \in A} |\{f : A \to A \mid f \text{ ist injektiv} \wedge f(a) = b\}| \\ &= \sum_{b \in A} (n-1)! = |A|(n-1)! = n! \end{aligned}$$

Auch hier gäbe es ein alternatives kombinatorisches Argument:

Betrachte $A = \{a_1, \ldots, a_n\}$.

Dem ersten Element a_1 können n verschiedene Elemente zugeordnet werden.

Wegen der Injektivität können dem zweiten Element a_2 nur noch $n-1$ verschiedene Elemente zugeordnet werden usw.

Dem letzten Element a_n kann dann nur noch ein Element zugeordnet werden.