Universität
Augsburg
University

Diskrete Strukturen und Logik

Vorlesung 02: Grundlagen

Prof. Dr. Tobias Mömke
Universität Augsburg

4. November 2020

Diskrete Strukturen und Logik

Inzidenzsystem

Seien S, T Mengen und $I \subseteq S \times T$ eine Relation zwischen S und T ("Inzidenz").

Dann ist (S, T, I) ein **Inzidenzsystem**.

Seien $a \in S$ und $b \in T$:

- a und b sind inzident, genau dann wenn $(a, b) \in I$
- Sonst: a und b sind nicht-inzident

Beispiel: Graph

Zweifaches Abzählen

Satz

Sei (S, T, I) ein Inzidenzsystem. Für $a \in S$ und $b \in T$,

$r(a)$: *Anzahl zu a inzidenter Elemente aus T*

$r(b)$: *Anzahl zu b inzidenter Elemente aus S*

Dann gilt

$$\sum_{a \in S} r(a) = \sum_{b \in T} r(b)$$

Beweis. Sei
$S = \{a_1, a_2, \ldots, a_m\}$ für ein $m \in \mathbb{N}^*$ und
$T = \{b_1, b_2, \ldots, b_n\}$ für ein $n \in \mathbb{N}^*$.

$m \times n$ Matrix $M = (m_{ij})$ (Inzidenzmatrix):

$$m_{ij} = \begin{cases} 1 & \text{falls } (a_i, b_j) \in I \\ 0 & \text{sonst} \end{cases}$$

$r(a_i)$: Anzahl Einsen in Zeile i
$r(b_j)$: Anzahl Einsen in Spalte j

$$\sum_{a \in S} r(a) \quad \text{und} \quad \sum_{b \in T} r(b)$$

Summe **aller** Einsen in allen Zeilen respektive Spalten.
Formal: Bijektionen zwischen Summen und Anzahl der Einsen. $\square$

Beispiel

$S = T = [8]$
i, j inzident, falls i Teiler von j, also $i|j$.

Fortsetzung vom Beispiel

Frage

Wie viele Teiler hat eine Zahl von 1 bis 8 **im Durchschnitt**?

Was heißt das formal?
Sei $t(n)$ die Anzahl der Teiler von n. Dann ist der Durchschnitt

$$\bar{t}(n) = \frac{1}{n} \sum_{j=1}^{n} t(j)$$

Beispiel: $\bar{t}(8) = 1/8 \cdot \sum_{i=1}^{8} t(i)$

n	1	2	3	4	5	6	7	8
$\bar{t}(n)$	1	3/2	5/3	2	2	16/7	5/2	

Was ist $\bar{t}$ für beliebige n?

Teiler nach Spalten zählen:

$$\tau = \sum_{i=1}^{n} t(i)$$

und daher $\bar{t}(n) = \tau/n$.
Stattdessen: Wir zählen nach Zeilen.

Zeile i: Eins bei allen Vielfachen von i

Problem:

Teiler nach Spalten zählen:

$$\tau = \sum_{i=1}^{n} t(i)$$

und daher $\overline{t}(n) = \tau/n$.
Stattdessen: Wir zählen nach Zeilen.

Zeile i: Eins bei allen Vielfachen von i

Problem:

i teilt nicht immer n.
Z.B. für $n = 8$ und $i = 3$: $8/3 = 2 + 2/3$, aber nur 2 Einsen

Gaußklammern

Notation

Sei $x \in \mathbb{R}$ beliebig.
Obere Gaußklammer (ceiling):
$\lceil x \rceil$ ist die kleinste Zahl $a \in \mathbb{Z}$ mit $a \geq x$.

Untere Gaußklammer (floor):
$\lfloor y \rfloor$ ist die größte Zahl $b \in \mathbb{Z}$ mit $b \leq y$.

Beispiele:

$$\begin{aligned}
\lfloor 3.5 \rfloor &= \\
\lceil 3.5 \rceil &= \\
\lfloor -3 \rfloor &= \\
\lceil 2 \rceil &= \\
\lfloor -3.5 \rfloor &= \\
\lceil -3.5 \rceil &=
\end{aligned}$$

Zurück zum Beispiel

Erinnerung: Zeile i hat Eins für vielfache von i.
Anzahl der Einsen in Zeile i: $\lfloor n/i \rfloor$

Zweifaches Abzählen:

$$\bar{t}(n) = \frac{1}{n}\sum_{j=1}^{n} t(j) = \frac{1}{n}\sum_{i=1}^{n} \lfloor n/i \rfloor \sim \frac{1}{n}\sum_{i=1}^{n} \frac{n}{i} = \sum_{i=1}^{n} \frac{1}{i} = H_n$$

Zeichen $\sim$: nicht genau gleich, es gibt einen Fehler.

Größe des Fehlers innerhalb $\sum_{i=1}^{n} \frac{n}{i}$: Pro Summand höchstens 1
Summe der Fehler: höchstens n (Es gibt n Summandenden.)
Wir teilen durch n.

Daher insgesamt: Fehler höchstens 1, d.h.,

$$\frac{1}{n}\sum_{i=1}^{n} \lfloor i/n \rfloor \leq \frac{1}{n}\sum_{i=1}^{n} i/n \leq \frac{1}{n}\sum_{i=1}^{n} \lfloor i/n \rfloor + 1$$

Zusammenfassung

Für jedes n: Durchschnittliche Anzahl der Teiler zwischen $H_n - 1$ und H_n
Später: Harmonische Zahl H_n etwa $\ln n$.

Im Vergleich: Kryptographie basiert auf Schwierigkeit zu faktorisieren!

Diskrete Strukturen und Logik

Binomialkoeffizienten

(Wiederholung aus Vorkurs)

Gegeben: Menge M.
Potenzmenge $\mathcal{P}(M)$: Menge aller Teilmengen von M
Menge von Mengen $\mathcal{P}_k(M)$: k-elementige Teilmengen von M, d.h.

$$\mathcal{P}_k(M) = \{S \subseteq M : |S| = k\}$$

Binomialkoeffizienten:

$$\binom{n}{k} = |\mathcal{P}_k|$$

Beispiel: Anzahl der Möglichkeiten, 4 von 10 Vorlesungen auszuwählen.

Stirling Zahlen zweiter Art

Wir betrachten:
Mengen-Partition von n-Menge in k disjunkte Blöcke.
Kurz: **k-Mengen-Partition**

Anzahl möglicher k-Mengen-Partitionen: **Stirling-Zahlen zweiter Art**

$$S_{n,k} := |\{P \subseteq \mathcal{P}([n]) : |P| = k \text{ und } P \text{ ist Partition von } [n]\}|$$

Beispiel: $S_{5,2} = 15$

Zahl-Partitionen

Sei $n \in \mathbb{N}^*$.

k-Zahl-Partition von n:

$$n_1, n_2, \ldots, n_k \text{ mit } n_i \geq 1 \text{ für } 1 \leq i \leq k, \text{ so dass } n_1 + n_2 + \cdots + n_k = n.$$

Anzahl der möglichen k-Partitionen: $P_{n,k}$

Beispiel: $P_{8,4} = 5$

Reihenfolge

Bei Mengen-Partitionen und Zahl-Partitionen:

Reihenfolge spielt keine Rolle.

Beispiel:

$$\{\{a, b\}, \{c\}\} = \{\{c\}, \{a, b\}\}$$

$$3 + 1 + 1 = 1 + 1 + 3$$

Geeordnete Mengen- und Zahlpartitionen:

Zähle jede Reihenfolge einzeln.

Beispiel: Geeordnete 3-Zahl-Partitionen von 4:
$1 + 1 + 2, 1 + 2 + 1, 2 + 1 + 1$
Beachte: Wir unterscheiden nicht unterschiedliche Vorkommen gleicher Zahlen.
(Also $1' + 1'' + 2$ und $1'' + 1' + 2$ zählen nur ein Mal).

Werkzeuge

Berechnung der Zählkoeffizienten:

Wir brauchen

- k-Permutationen
- Fallende Faktorielle
- Steigend Faktorielle

Permutationen

Definition

Sei M eine endliche Menge. Eine **Permutation** von M ist eine **bijektive** Funktion

$$\sigma\colon M \to M$$

Beispiel für $M = [4] = \{1, 2, \ldots, 4\}$:

n	1	2	3	4
$\sigma(n)$	2	1	4	3

Anzahl Permuationen

Satz

Sei M eine m-Mengen. Es gibt $m!$ viele Permutationen von M.

Beweis. Ohne Beschränkung der Allgemeinheit: $M = [m]$.
Für $m = 1$: Einzige Abbildung ist Identität, $m! = 1$.
Induktion: Angenommen $n!$ Permutationen für n-Menge.
Wir zeigen: $(n+1)!$ Permutationen für $n+1$-Menge.

- $n + 1$ Möglichkeiten, $\sigma(1)$ zu wählen.
- Danach: Anzahl der Bijektionen $[n+1] \setminus \{1\} \to [n+1] \setminus \{\sigma(1)\}$
  Bijektionen $f : M \setminus \{1\} \to [n], g : [n+1] \setminus \{\sigma(1)\} \to [n]$, betrachte $g^{-1} \circ \sigma' \circ f$
  Daher äquivalent: Betrachte Bijektionen $\sigma' : [n] \to [n]$
- Nach Induktionsvoraussetzung: $n!$ Permutationen für jede der $n + 1$ Möglichkeiten

Damit insgesamt: $(n+1) \cdot n! = (n+1)!$ Permutationen $\square$

k-Permutationen

Definition

Sei M eine endliche Menge mit $|M| = m$ und $k \in \mathbb{N}$, $k \leq m$. Eine k-Permutation von M ist eine Permutation von U für $U \in \mathcal{P}_k$.

Also Permuationen der k-Elementigen Teilmengen von M.
Ähnlich zur Anzahl der Permuationen:

- m Möglichkeiten, das erste Element zu wählen
- $m - 1$ Möglichkeiten, das zweite Element zu wählen
- $\ldots$
- $m - k + 1$ Möglichkeiten, das k-te Element zu wählen

Insgesamt: $m \cdot m - 1 \cdot \ldots \cdot m - k + 1$ Möglichkeiten.
Beweis: Übung

Faktorielle

Definition

Fallende Faktorielle:

$$n^{\underline{k}} := n \cdot n - 1 \cdot \ldots \cdot n - k + 1$$

Steigende Faktorielle:

$$n^{\overline{k}} := n \cdot n + 1 \cdot \ldots \cdot n + k - 1$$

Das Wort “Fakultät” (z.B. $n!$) hat den gleichen Urspung; man sagt “n factorial” auf englisch.

Damit gilt: Es gibt $n^{\underline{k}}$ k-Permutationen.

Zurück zum Zählen

Zusammenfassung:

Anzahl Teilmengen: 2^n
Anzahl k-Teilmengen: $\binom{n}{k}$
Anzahl Permutationen: $n!$
Anzahl k-Permutationen: $n^{\underline{k}}$

Geeordnete Teilmengen und k-Mengen-Partitionen

Satz

*Es gibt $k!\binom{n}{k}$ **geordnete** k-Teilmengen einer n-Menge M.*

Beweis: Es gibt $\binom{n}{k}$ verschiedene k-Teilmengen und $k!$ Reihenfolgen für jede Auswahl.
(Wirklich formal: Benutze Bijektionen und Produktregel.) $\square$

Satz

*Es gibt $k!S_{n,k}$ **geordnete** k-Mengen-Partitionen einer n-Menge M.*

Beweis:
$S_{n,k}$ ist Anzahl ungeordneter k-Mengen-Partitionen, für jede Auswahl $k!$ Möglichkeiten. $\square$

Zurück zu Binomialkoeffizienten

Interessante Einsicht:

$$\text{Geordnete } k\text{-Untermengen} = k\text{-Permutationen von } M$$

Daher:

$$k!\binom{n}{k} = n^{\underline{k}}$$

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}$$

Geordnete Zahl-Partitionen

Erinnerung:

Wir unterscheiden $3+1+1$ und $1+1+3$, aber nicht
$1'+1''+3$ und $1''+1'+3$.

Anzahl geeordneter Zahl-Partitionen von $3, 1, 1$: 3 (und nicht 6).

Satz

Die Anzahl der geeordneten k-Zahl-Partitionen von n ist $\binom{n-1}{k-1}$.

Beweis.

Beispiel

Sei $n = 6$ und $k = 3$

$$\binom{5}{2} = 10$$

geordnete k-Zahl-Partitionen von n.

Multimenge

Menge:

Gleiche Elemente werden nur ein Mal gezählt. Beispiel:

$$\{a, a, b, c\} = \{a, b, c\}$$

Multimenge: Gleiche Schreibweise, aber mehrfach gezählt.

$$\{a, a, b, c\} \neq \{a, b, c\}$$

Die **Vielfachheit** von a ist 2 und die Vielfachheit von b ist 1.

Mächtigkeit einer Multimenge: Summe der Vielfachheiten

Konvention: Wenn nicht dazu gesagt, Menge.
Nur Multimenge, wenn explizit gesagt.

k-Multimengen

k-Multimenge über Menge M: Multimenge N, Mächtigkeit $|N| = k$, jedes Element von M.
Beispiel: $\{a, b, b, c, c, d, d, d\}$ ist 8-Multimenge über $\{a, b, c, d\}$.

Satz

Die Anzahl der k-Multimengen über einer n-Menge ist

$$\frac{n^{\overline{k}}}{k!}\,.$$

Erinnerung: $n^{\overline{k}} = n \cdot (n+1) \cdot \ldots \cdot (n+k-1)$
Beweis.