

Diskrete Strukturen:

TL;DR

(Version: 3. März 2020)

Anmerkung: Kann Fehler enthalten. Ich übernehme keinerlei Haftung. Falls jemand Fehler findet, sagt mir bitte Bescheid, dann verbessere ich das aus. Das Dokument ist unfertig. Gerne dürft ihr mir Ergänzungen zukommen lassen. Nicht als Lerngrundlage nehmen (das Ding heißt TL;DR).

Robyn Källe

Kombinatorik

Urnenmodell:

- mit Zurücklegen, mit Reihenfolge

$$\mathcal{M} := \{(s_1, \dots, s_k) \in [n]^k\}$$

$$|\mathcal{M}| = n^k$$

- mit Zurücklegen, ohne Reihenfolge

$$\mathcal{M} := \{(s_1, \dots, s_k) \in [n]^k \mid s_1 \leq s_2 \leq \dots \leq s_k\}$$

$$|\mathcal{M}| = \binom{k+n-1}{k}$$

- ohne Zurücklegen, mit Reihenfolge

$$\mathcal{M} := \{(s_1, \dots, s_k) \in [n]^k \mid |\{s_1, \dots, s_k\}| = k\}$$

$$|\mathcal{M}| = n^{\underline{k}} := \frac{n!}{(n-k)!}$$

- ohne Zurücklegen, ohne Reihenfolge

$$\mathcal{M} := \{(s_1, \dots, s_k) \in [n]^k \mid s_1 < s_2 < \dots < s_k\}$$

$$|\mathcal{M}| = \binom{n}{k}$$

Grundprinzipien:

- Summenregel

$$\left| \biguplus_{i \in I_0} A_i \right| = \sum_{i \in I_0} |A_i|$$

- Union Bound

$$\left| \bigcup_{i \in I_0} A_i \right| \leq \sum_{i \in I_0} |A_i|$$

- Produktregel

$$|A_1 \times \dots \times A_n| = \prod_{i \in [n]} |A_i|$$

- Siebformel

$$\left| \bigcup_{i \in [n]} A_i \right| = \sum_{\substack{I \subseteq [n]: \\ I \neq \emptyset}} (-1)^{|I|+1} \cdot \left| \bigcap_{i \in I} A_i \right|$$

- $|A| = m \cdot |B|$, falls $\forall b \in B: f^{-1}(b) = m$

$$\text{für } f: A \rightarrow B$$

- Schubfachprinzip

$$\text{für } f: A \rightarrow B: \exists b \in B \text{ mit } |f^{-1}(b)| \geq \lceil |A|/|B| \rceil$$

- Doppeltes Abzählen

$$\text{für jedes } R \subseteq S \times T \text{ gilt: } \sum_{s \in S} |\{t \in T \mid (s,t) \in R\}| = \sum_{t \in T} |\{s \in S \mid (s,t) \in R\}|$$

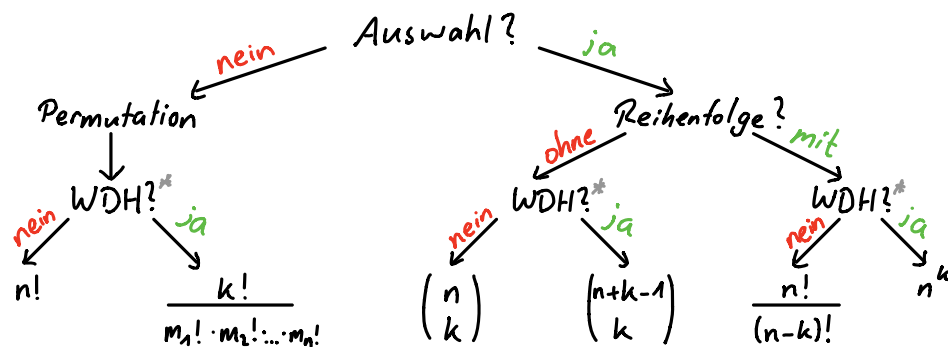
Goldene Tabelle:

k Bälle $\rightarrow$ n Urnen	beliebig viele ("beliebig")	höchstens 1 ("injektiv")	mindestens 1 ("surjektiv")	genau 1 ("bijektiv")	... pro Urne
Beides	n^k	$n^{\underline{k}}$	$n! \cdot S_{k,n}$	$k!$	
Nur Urnen	$\binom{k+n-1}{k}$	$\binom{n}{k}$	$\binom{k-1}{n-1}$	1	
Nur Bälle	$\sum_{i=0}^n S_{k,i}$	1	$S_{k,n}$	1	
Nichts	$\sum_{i=0}^n P_{k,i}$	1	$P_{k,n}$	1	

... unterscheidbar

Credit: Carlos Camino

Welche Formel soll ich nehmen?



*WDH: „Treten Elemente mehrfach auf?“

Credit: Daniel Jung (YouTube)

Zahlpartitionen von n in k Summanden:

$$\cdot |\{(s_1, \dots, s_k) \in \mathbb{N}_0^k \mid s_1 + \dots + s_k = n\}| = \binom{n+k-1}{n}$$

$$\cdot |\{(s_1, \dots, s_k) \in \mathbb{N}_0^k \mid s_1 + \dots + s_k \leq n\}| = \binom{n+k}{n}$$

$$\cdot |\{(s_1, \dots, s_k) \in \mathbb{N}^k \mid s_1 + \dots + s_k = n\}| = \binom{n-1}{k-1}$$

$$\cdot |\{(s_1, \dots, s_k) \in \mathbb{N}^k \mid s_1 + \dots + s_k = n, s_1 \leq \dots \leq s_k\}|$$

$$= |P_{n,k}| \quad \text{mit} \quad |P_{n,k}| = |P_{n-1,k-1}| + |P_{n-k,k}|$$

$$\cdot |P_{n,n}| = 1$$

$$\cdot |P_{n+1,0}| = 0$$

$$\cdot |P_{n,k}| = 0 \quad \text{falls} \quad k > n$$

Stirling Zahlen 2. Art: „sodass jede Box mind. 1 Element enthält“

n Elemente in k nicht-unterscheidbare Boxen:

$$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k} \quad \text{rekursiv berechnen, bis: } S_{0,0} = 1, S_{m,0} = 0, S_{m,m} = 1$$

$$S_{m,1} = 1$$

n Elemente in k unterschiedliche Boxen:

$$k! \cdot S_{n,k}$$

Partitionen von $[n]$ in λ_i -viele, i -elementige Klassen:

$$\frac{n!}{(1!)^{\lambda_1} \dots (n!)^{\lambda_n} \cdot \lambda_1! \dots \lambda_n!}$$

Algebra

Gruppen:

$G \cong \langle G, \cdot, 1 \rangle$ ist eine Gruppe, falls:

Grundmenge G
Gruppenoperation $\cdot$
neutrales Element 1

0. $\cdot : G \times G \rightarrow G$ (abgeschlossen)

1. $\forall a, b, c: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (assoziativ)

2. $\forall a: a \cdot 1 = 1 \cdot a = a$ (Neutrales)

3. $\forall a \exists b: a \cdot b = b \cdot a = 1$ (Inverses)

G ist kommutativ, falls:

4. $\forall a, b: a \cdot b = b \cdot a$ (kommutativ)

Falls G kommutativ ist, wird die Additive Schreibweise für G verwendet:

$$G \cong \langle G, +, 0 \rangle$$

• $\mathbb{Z}_n := \{0, 1, 2, \dots, n\}$, $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid \text{ggT}(x, n) = 1\}$

• $|\mathbb{Z}_n^*| =: \varphi(n) = n \cdot \prod_{\substack{p \in \mathbb{P} \\ p|n}} (1 - p^{-1})$

falls $n \in \mathbb{P}$: $\varphi(n) = n - 1$, falls $\text{ggT}(m, n) = 1$: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

falls $n \in \mathbb{P}, k \in \mathbb{N}$: $\varphi(n^k) = n^{k-1} (n - 1)$

• Eine Gruppe ist zyklisch, wenn sie von einem einzigen Element erzeugt wird: $G = \langle x \rangle$

sei G die Gruppe $\langle \mathbb{Z}, +, 1 \rangle$

wähle $x \in G$. Was ist die kleinste Untergruppe von G , die x enthält?

$$\hookrightarrow \langle x \rangle = \{ \dots, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, \dots \}$$

→ eine Gruppe mit x muss auch das Inverse von x enthalten (weil Gruppe)

→ muss neutrales Element enthalten

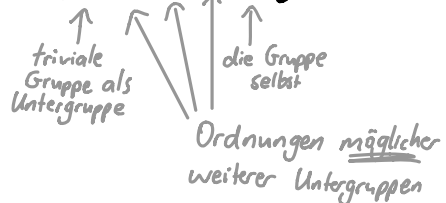
→ muss unter " $\cdot$ " abgeschlossen sein (+ alle Inverse von x^i)

= "die von x generierte Gruppe"

- Sei $H \leq G$ und $|G| < \infty$: dann $|H| \mid |G|$ (die Ordnung von H teilt $|G|$)

Beispiel: $\langle \mathbb{Z}_{29}^*, \cdot_{29}, 1 \rangle$ $\varphi(29) = 28 = 2 \cdot 14 = 2 \cdot 2 \cdot 7$ (da 29 prim)

$\rightarrow \forall H \leq G: |H| \in \{1, 2, 7, 14, 28\}$



- Ordnung eines Elements a herausfinden:

1. $|\mathbb{Z}_n^*|$ bestimmen

2. Teiler T von $|\mathbb{Z}_n^*|$ herausfinden

3. Sei n das neutrale Element, $t \in T$:

$$\left. \begin{array}{l} \text{falls } a^t = e : \text{ord}(a) = t \quad (\text{multiplikativ}) \\ \text{falls } t \cdot a = e : \text{ord}(a) = t \quad (\text{additiv}) \end{array} \right\} \text{ und falls } \neg \exists t' \in T \text{ mit } t' < t \text{ und } a^{t'} = e \text{ bzw. } t' \cdot a = e$$

- Gibt es ein Element a mit $\text{ord}(a) = 0$ in G ?

$\hookrightarrow 0 \mid |G|$? $\rightarrow$ falls nein: nein, sonst: wie oben vorgehen

- „Berechnen Sie a^k mit $a, k = \text{absurd hohe Zahlen}$.“

$\hookrightarrow$ in jeder Gruppe gilt: $a^k = a^{k \bmod |G|}$

Beispiel: $987^{911} \bmod 911$ berechnen:

$$987^{911} \equiv_{911} 987^{911 \bmod \varphi(911)} = 987^{911 \bmod 910} = 987^1 \equiv_{911} 76$$

- Falls $G = \langle g \rangle$ und $|G| < \infty$: Erzeuger $E := \{g^k \mid k \in \mathbb{Z}_{|G|}^*\}$, $|E| = \varphi(|G|)$

- Falls $G = \langle g \rangle$:

- $\forall H \leq G$: H ist zyklisch

- G ist kommutativ

- Falls $|G| \in \mathbb{P}$: Gruppe zyklisch

- $\mathbb{Z}_n^*$ ist Menge der Erzeuger von $\langle \mathbb{Z}_n, +_n, 0 \rangle$

- Zeigen, dass a ein Erzeuger von $G = \langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$ ist:
 1. Primteiler T von $|\mathbb{Z}_n^*|$ bestimmen
 2. Falls gilt: $\forall t \in T: a^{\frac{|\mathbb{Z}_n^*|}{t}} \neq_p 1$ dann ist a Erzeuger von G (gdw.-Bedingung)
- Anzahl der Erzeuger einer zyklischen Gruppe G_z : $\varphi(|G_z|)$
- Inverses bestimmen: EEA

Graphen

Digraphen:

- $\forall u, v \in E: u(E \cup E^{-1})v \rightarrow G$ ist zusammenhängend
- $\forall u, v \in E: uE^*v, vE^*u \rightarrow G$ ist stark zusammenhängend
- $G[U]$ (stark) zshgd. $\rightarrow U \subseteq V$ ist (starke) zshg.-Komponente
- es gibt kein U' mit $U \subsetneq U' \subseteq V$, sodass $G[U']$ eine (starke) zshg.-Komponente ist
 $\rightarrow U$ ist maximale (starke) zshg.-Komponente
- es gibt Bijektion $\beta: V_G \rightarrow V_H: G$ und H sind isomorph („Knotenumbenennung“)

Einfache Graphen:

- Realisierbarkeit einer Gradfolge:
 - Summe d. Knotengrade ungerade $\Rightarrow G$ existiert nicht
 - $|\{v \in V \mid \deg(v) \text{ ungerade}\}|$ ungerade $\Rightarrow G$ existiert nicht
 - Havel-Hakimi-Algorithmus
- Bipartit?
 - G ist bipartit $\Leftrightarrow G$ enthält keinen Kreis ungerader Länge
- Zusammenhängend?
 - G ist zshgd. $\Rightarrow |E| \geq |V| - 1, \quad \Delta(G) + \delta(G) + 1 \geq |V| \Rightarrow G$ ist zshgd.
- Baum?
 - G ist zshgd. und $|V| = |E| + 1 \Leftrightarrow G$ ist Baum
 - G ist kreisfrei und $|V| = |E| + 1 \Leftrightarrow G$ ist Baum
 - G ist zshgd. und kreisfrei $\Leftrightarrow G$ ist Baum
 - $u, v \in V$ sind durch genau einen einfachen Pfad in G verbunden $\Leftrightarrow G$ ist Baum
 - G ist zshgd. $\Rightarrow G$ enthält Spannbaum
 - G ist Baum $\Rightarrow |V| = |E| + 1$

- **Eulertour?**

- G ist zshgd. und $\forall v \in V: \deg(v) \text{ gerade} \Rightarrow G$ besitzt Eulertour

- **Hamiltonkreis?**

- $\forall v \in V: \deg(v) \geq \frac{1}{2}|V|$ und $|V| \geq 3 \Rightarrow G$ besitzt Hamiltonkreis

- **Planar?**

- G ist planar $\Leftrightarrow G$ ist nicht (Major von) $K_{3,3}$ oder K_5

- $f = |E| - |V| + 2$

- G ist planar und hat $|V| \geq 3$ Knoten $\Rightarrow |E| \leq 3 \cdot |V| - 6$

- **Färbbarkeit?**

- $\chi(G) \leq |V|$
 - $\chi(G) \leq 1 + \max\{\deg(v) \mid v \in V\}$
- } gilt für alle einfachen Graphen

- G ist planar $\Rightarrow \chi(G) \leq 4$ (4-Farben-Satz)

- $\chi(G) \leq 2 \Leftrightarrow G$ ist bipartit

- $E \neq \emptyset \Rightarrow \chi(G) > 1$

- $\chi(K_n) = n$ $\chi(K_{m,n}) = 2$ $\chi(C_{2k}) = 2$ $\chi(C_{2k+1}) = 3$
- z.B. K_5 z.B. $K_{3,3}$ z.B. C_4 z.B. C_3
- 

- **Kreis?**

- G ist zshgd. und hat $n \geq 2$ Knoten und hat n oder mehr Kanten $\rightarrow G$ hat Kreis

Matchings:

- Heiratssatz: Es gibt ein Matching $M \subseteq E$ in $G(A \cup B, E)$

$$\Leftrightarrow$$

$$\Gamma(X) \geq |X| \quad \text{mit} \quad \Gamma(X) = \bigcup_{x \in X} \Gamma(x)$$

- Matchings mit Präferenzen: Gale-Shapley-Algorithmus

Adjazenzmatrizen:

- Summe: $C_{i,j} := A_{i,j} + B_{i,j}$

$$\begin{pmatrix} 1 & 2 & 0 \\ 3 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 1 \\ -2 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

- Multiplikation: $C_{i,j} := \sum_{t \in M_3} A_{i,t} \cdot B_{t,j}$

$$\begin{pmatrix} 1 & 2 & 0 \\ 3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + 2 \cdot 3 + 0 \cdot 1 & 1 \cdot (-1) + 2 \cdot 1 + 0 \cdot 0 \\ 3 \cdot 0 + 0 \cdot 3 + 1 \cdot 1 & 3 \cdot (-1) + 0 \cdot 1 + 1 \cdot 0 \end{pmatrix}$$

- Random-Surfer-Modell