

# **Diskrete Strukturen**

## **WS 21/22**

### **aufgeschrieben und verarbeitet**

### **von: Milena Serbinova**

Diese Zusammenfassung wurde von einer Studentin erstellt,  
basierend auf der Vorlesung aus dem Wintersemester  
2020/21.

Einige der in diesem Skript enthaltenen Bilder sind  
Screenshots aus den Vorlesungsfolien. Hier sind nur jene  
Themen drin, welche im WS 21/22 behandelt wurden.

Ich garantiere weder Richtigkeit noch Vollständigkeit, im  
Zweifel hat immer die Vorlesung Recht!

# KONTINUIERLICH

(nicht auf separate Werte beschränkt)

# DISKRET

(bestimme Werte)

Discrete Mengen → endlich viele Elemente

## GRAPHENTHEORIE

Eigenschaften von Graphen

## LOGIK

Syntax und Semantik logischer Formeln

# DISKRETE STRUKTUREN

- Reihenfolge der Objekte spielt keine Rolle
  - $x \in M$  Element von  $M$
  - $x \notin M$  extensionale  $M := \{0, a, 2\}$
  - implizit oder explizit ↗  
intensionale  $\{x \mid x \in R\}$
  - die leere Menge  $\{\}$

- $M_1 = M_2 \Rightarrow M_1 \subseteq M_2$  und  $M_2 \subseteq M_1$
- $M_1 \Delta M_2$  (symmetrische Differenz)
- Mächtigkeit / Kardinalität  $|M|$



endliche Menge  $|M| < \infty$

unendliche Menge  $|M| = \infty$

## RUSSELSCHE ANTONOMIE

Man kann einen Barbier als einen definieren, der all jene und nur jene rasiert, die sich nicht selbst rasieren.  
Die Frage ist: Rasiert der Barbier sich selbst?

- $nS \cup S$ , wenn  $S = \{\emptyset, \{\}\}$
- $\Omega$  Universum / Grundmenge  $\bar{A}$  Komplement
- Potenzmenge  $P(M) := 2^M := \{A \mid A \subseteq M\}$   $P(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$
- $P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
- $P(\emptyset) = \{\emptyset\}$
- $P(\{a\}) = \{\emptyset, \{a\}\}$
- $P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $P(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
- $P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$
- $P(P(\{a\})) = \{\emptyset, \{\emptyset\}, \{\{a\}\}, \{\emptyset, \{a\}\}\}$

$$|M| = k \quad |P(M)| = 2^k$$

$$\{1, 2, 3\} \rightarrow \{\{1\}, \{2, 3\}\}, \{\{1\}, \{2\}, \{3\}\}, \dots$$

$$\emptyset \notin P$$

$$\mathbb{Q} := \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N} \right\}$$

## DIAGONALISIERUNG

$$\begin{array}{l} 1: 0, 0, 0, 0, \dots \\ 2: 0, 1, 1, 5, \dots \\ 3: 0, 4, 1, 4, 2, \dots \\ x = 0, 2, 2, \dots \in \mathbb{R} \end{array}$$

Noch mehr Standardäquivalenzen für Mengenvariablen  $A, B, C$ .

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C) \\ A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C) \\ A &= A \cup (A \cap B) \\ A &= A \cap (A \cup B) \\ A \Delta B &= (A \setminus B) \cup (B \setminus A) \end{aligned}$$

► Mit definiertem Universum  $\Omega$ :

$$\begin{array}{ll} A \cap \bar{A} = \emptyset & \bar{A} = A \\ A \cup \bar{A} = \Omega & \bar{A} \cup B = \bar{A} \cap B \\ A \setminus B = A \cap \bar{B} & \bar{A} \cap B = \bar{A} \cup B \end{array}$$

## De Morgan

## MENGENAUSDRÜCKE

- $\cap$
  - $\cup$
  - $P()$
  - $\setminus$
  - $\Delta$
- TERME

- $\bar{A} = \Omega \setminus A$  äquivalent
- $A = A \cup A = A \cup \emptyset = A \cap A$
- $\emptyset = A \cap \emptyset$
- $A \cup B = B \cup A$  (Kommutativität)
- $(A \cup B) \cup C = (A \cup C) \cup B$  (Assoziativität)



Venn-Diagramm

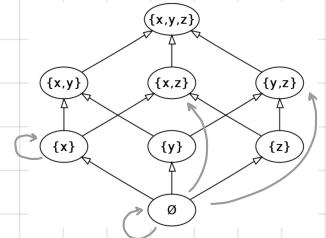


Karnaugh-Veitch-Diagramm



$$(A \cap B) \cup C$$

Potenzmenge = Hasse-Diagramm





# BINÄRE RELATION

2-stellige Relation ( $R \subseteq A \times B$ )  $\leq, <, =$

# GRAPHEN

$\Rightarrow$  Gerichteter Graph (Digraph)

$$\leq_{\text{IN}}^{-1}$$

inverse  
Relation

Infixnotation  
 $3 \leq_{\text{IN}} 5$

bipartit

$$V = A \cup B$$

$$A \cap B = \emptyset$$

$$E \subseteq A \times B \cup B \times A \quad (\text{es gibt nur Kanten zwischen } A \text{ und } B)$$

ein Kreis mit

3 + 4 einer geraden Anzahl an Kanten

Partitionsklasse

vollständig bipartit



nicht vollständig

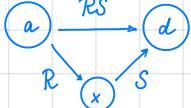
## RELATIONALES PRODUKT

von  $R$  und  $S$   $\Rightarrow RS \subseteq A \times D$

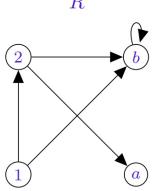
$$R \subseteq A \times B$$

$$RS = \{(a, d) \mid \text{es gibt } x \in B \cap C \text{ mit } (a, x) \in R \text{ und } (x, d) \in S\}$$

$$RS = T_{1,4} \quad (R \bowtie_{z=1} S)$$



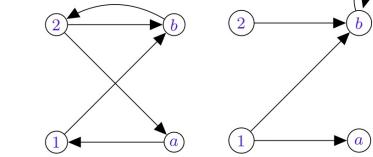
Verkettung von  $R$  und  $S$



$$R$$

$$S$$

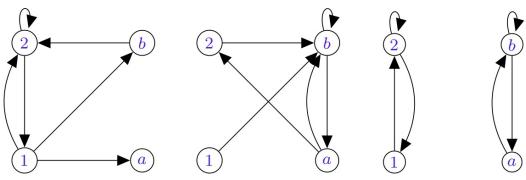
$$RR$$



$$RS$$

$$SR$$

$$SS$$



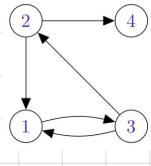
$$\bullet R^0 := Id_A := \{(a, a) \mid a \in A\} \quad R \subseteq A \times A$$

$$\bullet R^1 := \text{Identität} \quad R = R^0 R$$

$$\bullet R^2 := RR = R^1 R \quad \text{reursive Berechnung}$$

$$\bullet R^{k+1} := R^k R = R R^k = \underbrace{R R \dots R}_{k+1 \text{ mal}}$$

$$\bullet R^{-1} = \{(b, a) \mid (a, b) \in R\}$$



$$R \bowtie_{z=1} S \Rightarrow$$

$$R = \{(1, b), (b, b), (1, 2), (2, b), (2, a), (2, a)\}$$

$$(1, 2), (2, b), (2, a), (1, 2), (b, b), (b, 2), (a, 1)\}$$

	1	b	2	a
1	b	b		
b	b	b		
2	a	a	b	
a			b	a

$$R \bowtie_{z=1} R$$

$$R^0$$

$$R^1$$

$$R^2$$

$$R^3$$

$$R^0$$

$$R^1$$

$$$$

- 1)  $(s, t) \in R^*$ : Es gibt einen Pfad von  $s$  nach  $t$  in Graph  $G_R$   
 2)  $(s, t) \in R^{\leq n-1}$ : Es gibt einen Pfad von  $s$  nach  $t$  in Graph  $G_R$ , der höchstens  $n-1$  Schritte macht



Sei  $s, \dots, u, \dots, t$  ein Pfad von  $s$  nach  $t$ , der den Knoten  $u$  zweimal enthält. Dann erhält man durch Entfernen des "nutzlosen" Teilstücks von  $u$  nach  $u$ , einen neuen, kürzeren Pfad  $s, \dots, u, \dots, t$ , der  $u$  einmal weniger enthält. Durch wiederholte Anwendung dieser Regel erhält man einen **einfachen Pfad** von  $s$  nach  $t$ . Jeder einfache Pfad von GR besteht aus höchstens  $n - 1$  Schritten, da er sonst mindestens einen Knoten zweimal besucht.

$$(s, t) \in R^* \Rightarrow$$

gdw. es gibt einen Pfad von  $s$  nach  $t$  in  $G_R$

gdw. es gibt einen einfachen Pfad

gdw. es gibt einen Pfad der höchstens  $n-1$  Schritte macht

$$\text{gdw. } (s, t) \in R^{\leq n-1}$$

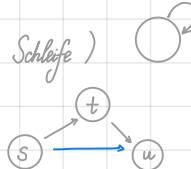
$R$  sei:  $R_0 \not\subseteq R$

- reflexiv falls  $\text{Id}_A \subseteq R$  (Jeder Knoten hat eine Schleife)

$$\bullet (R^*)^* = (R^+)^* = (R^+)^+ = R^*$$

$$\bullet (R^+)^+ = R^+$$

- transitiv falls  $(s, t) \in R$  und  $(t, u) \in R \rightarrow (s, u) \in R$



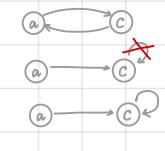
- symmetrisch  $(s, t) \in R \rightarrow (t, s) \in R$

asymmetrisch  $(s, t) \in R \rightarrow (t, s) \notin R$

antisymmetrisch

$(s, t) \in R$  und

$$(t, s) \in R$$



$$R: =_{\mathbb{Z}}; \leq_{\mathbb{Z}}; \neq_{\mathbb{R}}; \geq_{\mathbb{N}}$$

$|_{\mathbb{Z}}$  mit  $a|_{\mathbb{Z}} b$  definiert durch  $\frac{b}{a} \in \mathbb{Z}$

$\equiv_m$  mit  $a \equiv_m b$  definiert durch  $m|(a-b) \Rightarrow \frac{a-b}{m} \equiv_1 1$

" $a$  teilt  $b$ "

$$\frac{b}{a} \in \mathbb{Z}$$

$$5 \equiv_4 1$$

Prefix  $u \leq_p v$  falls  $w \in \Sigma^*$  mit  $uw = v$

Suffix  $u \leq_s v$  falls  $w \in \Sigma^*$  mit  $wu = v$

Indfix (Faktor)  $u \leq_i v$  falls  $w, w' \in \Sigma^*$  mit  $wuw' = v$

konjugiert  $u \cong_c v$  falls  $w, w' \in \Sigma^*$  mit  $u = ww'$  und

Boothaus

Hausboot

$v = w'w$

## ÄQUIVALENZ RELATIONEN

$=_{\mathbb{Z}}, \equiv_m, \equiv_c$  reflexiv, symmetrisch, transativ

Kongruenz modulo  $k$  (derselbe Rest bei Division durch  $m$ )  $5 \equiv_4 14$

Aquivalenzklasse  $[a]_R = \{b \in A \mid aRb\}$

$\checkmark a \in [a]_R$

$$[1]_{=_{\mathbb{Z}}} = \{1\}$$

$\checkmark [a]_R = [b]_R \Leftarrow aRb$

$$[-5]_{=_{\mathbb{Z}}} = 3\mathbb{Z} + 1 = \{ \dots, -5, -2, 1, 4, \dots \}$$

$\checkmark [a]_R \cap [b]_R \Leftarrow (a, b) \notin R$

Quotient

$$A/R = \{[a]_R \mid a \in R\}$$

Menge aller Aquivalenzklassen (eine Partition von  $A$ )

$$\mathbb{Z}/=_{\mathbb{Z}} = \{[x] \mid x \in \mathbb{Z}\}$$

$$\mathbb{Z}/\equiv_3 = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$$



$2^k$  Kästchen



$\leq_{\mathbb{Z}}, \subseteq, |_{\mathbb{N}}, \leq_{\text{s.p.i.}}$  reflexiv, antisymmetrisch, transativ

unvergleichbar

## ORDNUNGS RELATIONEN

ordnen Objekte teilweise (partiell)

$$a, b \in \mathbb{Z} \Rightarrow a \leq_{\mathbb{Z}} b$$

$$a, b \in \mathbb{N} \nRightarrow a |_{\mathbb{N}} b$$

$(\frac{b}{a} \notin \mathbb{N})$

## TOTALE ORDNUNG (Totalordnung)

strikte / strenge Varianten: reflexiv  $\rightarrow$  irreflexiv

$$<_{\mathbb{Z}} = \leq_{\mathbb{Z}} \setminus \text{Id}_{\mathbb{Z}}$$

Antisymmetrie  $\rightarrow$  Symmetrie

$$a R b \rightarrow a S b$$

oder

## PARTIELLE ORDNUNG

(Halbordnung)

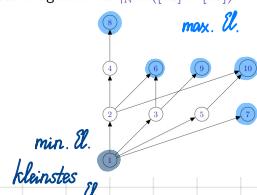
## HASSE-DIAGRAMM

reflexiv und transitiv

$$\{1 \dots 10\}$$

1	2	3
1 (1,1)		(2,3)
2		
3		
4		
5		

Beispiel: Hasse-Diagramm zu  $\mathbb{N} \cap ([10] \times [10])$



$m \in A$  ist ein maximales Element bzgl.  $R$ , falls  $\rightarrow$  keine Kanten zu einem anderen Element

duale Begriffe

$m \in A$  ist das größte Element bzgl.  $R$ , falls  $aRm$  für jedes  $a \in A$  gilt

ist  $R$  total  $\rightarrow$  max = größte



Mit  $R$  ist auch  $R^{-1}$  eine Ordnung  
von  $A$  auf  $B$

für jedes

Funktion (Abbildung)  $R \subseteq A \times B$ :  $a \in A$  existiert genau ein  $b \in B$  mit  $(a,b) \in R$

von  $A$  nach  $B$ im( $f$ ) Zielmengewann immer  $a R b' \rightarrow b = b'$  $f: A \rightarrow B$ Bildmenge ( $\{f(a) \mid a \in A\} \subseteq B$ ) $f(X) = \{f(a) \mid a \in X\}$ , wenn  $X \subseteq A$  $f(a)$  steht für das eindeutige  $b \in B$ Urbildmenge  $\text{dom}(f) = f^{-1}(Y)$ , wenn  $Y \subseteq B$  $|B|^A|$  die Anzahl der möglichen Funktionen  $|B^A|$ die Menge aller Funktionen von  $A$  nach  $B$ :  $B^A := \{f: A \rightarrow B\}$  $f = \bigcup_{i=1}^k f_i \Leftrightarrow f(a_1, \dots, a_k)$ 

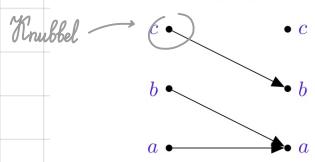
Stelligkeit / Arilität

=  $k$ -äre Funktion  
nulleare Funktion $f: \bigcup_{i=1}^k A_i \rightarrow B$  $f: \{\cdot\} \rightarrow B$ 

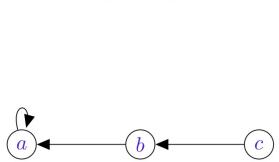
## VISUALISIERUNG:

Beispiel:  $f = \{(a,a), (b,a), (c,b)\} \subseteq A \times A$  für  $A = \{a, b, c\}$ 

Als Funktion:



Als Relation:



v injektiv

$f(a) = f(a') \rightarrow a = a'$

$f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = ax + b$

$f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2$

(Äquivalent:  $|f^{-1}(\{b\})| \leq 1$  für jedes  $b \in B$ )

nicht injektiv

v surjektiv

für jedes  $b \in B$  ein  $a \in A$  mit  $f(a) = b$  gibt

$f: \mathbb{Z} \rightarrow \mathbb{Z}, n \mapsto 2n$

$f: \mathbb{Z} \rightarrow \mathbb{Z}, n \mapsto n+1$

(nur gerade Zahlen  $\Rightarrow$  nicht surjektiv)

surjektiv

v bijektiv

Permutation

 $f: A \rightarrow A$  für jedes  $b \in B$ Äquivalent:  $|f^{-1}(\{b\})| = 1$ 

→

Umkehrfunktion /

Inverse  $f^{-1} = \{(b,a) \mid b \in B, a \in f^{-1}(\{b\})\} \subseteq A^B$ die Menge aller Funktionen  $B \rightarrow A$ 

partielle Funktion

nicht injektiv

nicht surjektiv

nicht injektiv

nicht inj

$$3) (f \circ f^{-1}) = \text{Id}_B$$

$$\begin{array}{l} f: B \rightarrow A \\ b \in B \\ a = f^{-1}(b) \end{array} \Rightarrow \begin{array}{l} b \in f(\{a\}) \\ b = f(a) = f(f^{-1}(b)) = (f \circ f^{-1})(b) \end{array}$$

$$4) \begin{array}{l} g: A \rightarrow B \\ (g \circ f^{-1}) = \text{Id}_B \end{array} \Rightarrow g = (f^{-1})^{-1} = f$$

$$\begin{array}{l} f = \text{Id}_B \circ f = (g \circ f^{-1}) \circ f = \\ = g \circ (f^{-1} \circ f) = g \circ \text{Id}_A = g \end{array}$$

# KARDINALITÄT

Satz von Cantor-Bernstein-Schröder

$$\begin{array}{l} f: A \rightarrow B \text{ injektiv} \Rightarrow h: A \rightarrow B \text{ bijektiv} \\ g: B \rightarrow A \end{array}$$

$$\text{es folgt: } |A| = |B| \text{ wenn } \begin{array}{l} f: A \rightarrow B \\ g: B \rightarrow A \end{array}$$

$$\begin{array}{l} |A| < |B| \text{ wenn } \begin{array}{l} f: A \rightarrow B \\ \text{aber nicht injektiv} \end{array} \\ g: B \rightarrow A \end{array}$$

abzählbare Menge  $|A| \leq |N|$

unabzählbare Menge  $|A| > |N|$

$$\checkmark |N| = |N \times N| \text{ mittels der Bijektion}$$

$$f: N \times N \rightarrow N, (n, m) \mapsto \frac{1}{2}(m+n-1)(m+n-2) + m$$

Kardinalzahl  $|A|$   $A$  ist abzählbar, wenn jedes  $a \in A$  mit einer eindeutigen Identifikationsnummer zu versehen ist

Satz von Cantor  $|A| < |\mathcal{P}(A)|$

mit  $f: A \rightarrow \mathcal{P}(A), a \mapsto \{a\}$  folgt  $|A| < |\mathcal{P}(A)| \rightarrow$  Diagonalisierung:

wir nehmen an, dass  $g: A \rightarrow \mathcal{P}(A)$  bijektiv ist

$$\text{setze } M = \{a \in A \mid a \notin g(a)\} \subset \mathcal{P}(A)$$

da  $g$  angeblich bijektiv, gibt es ein  $m \in A$  mit  $g(m) = M$

$$\text{Aber: } m \in M \text{ gdw. } m \notin g(m) = M \Rightarrow \text{S}$$

$\mathbb{R}$  überabzählbar (nicht abzählbar)

Beweis: DIAGONALISIERUNG (Widerspruchsbeweis)

$$\text{Annahme: } \mathbb{R} \text{ abzählbar } g: \mathbb{R} \rightarrow N [0,1]$$

$$1: 0, \underline{5} 0 0 0 \dots$$

$$2: 0, 1 \underline{4} 6 3 \dots$$

$$3: 0, 3 \underline{4} 1 7 \dots$$

$$4: 0, 4 2 6 \underline{8} \dots$$

Behauptung:  $g$  nicht surjektiv

$$x = 0, 6 5 2 g \dots \in \mathbb{R}$$

nicht in der Liste (untersch. sich von der  $i$ -Zahl in der Liste in  $i$ -Nachkommastelle)  $\Rightarrow \mathbb{R}$  nicht abzählbar

- Ist  $f$  injektiv, dann ist  $g: A \rightarrow f(A), a \mapsto f(a)$  bijektiv.
  - Ist  $f: A \rightarrow A$  injektiv und  $A$  endlich, dann ist  $f$  bijektiv.
  - Ist  $f: A \rightarrow A$  surjektiv und  $A$  endlich, dann ist  $f$  bijektiv.
  - Sind  $f: A \rightarrow B$  und  $g: B \rightarrow C$  injektiv/surjektiv, dann auch  $(g \circ f)$ .
  - Ist  $(g \circ f)$  surjektiv, dann auch  $g$ .
  - Ist  $(g \circ f)$  injektiv, dann auch  $f$ .
  - $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$  und  $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$ .
  - $f(X \cup Y) = f(X) \cup f(Y)$ , aber  $f(X \cap Y) \subseteq f(X) \cap f(Y)$ .
- $f$  ist genau dann injektiv, wenn stets  $f(X \cap Y) = f(X) \cap f(Y)$  gilt.

$B$  mindestens so mächtig wie  $A$

- $|A| \leq |B| \Rightarrow$  es gibt eine Injektion  $f: A \rightarrow B$
- $|A| \oplus |B| \Rightarrow$  es gibt eine Bijektion  $f: A \rightarrow B$
- $|A| < |B| \Rightarrow$  es gibt eine Injektion  $f: A \rightarrow B$ , aber keine Bijektion  $g: A \rightarrow B$

$$\left[ \begin{array}{l} |A| \leq |B| \Rightarrow |A| \leq |C| \\ |B| \leq |C| \end{array} \right]$$

Komposition injektiver Funktion ist injektiv

gerade Zahlen

$$\text{BEISPIELE: } \checkmark |N| = |2N| \text{ mittels } \begin{array}{l} N \rightarrow 2N, n \mapsto 2n \text{ inj.} \\ 2N \rightarrow N, n \mapsto n \text{ inj.} \end{array}$$

$$\checkmark |N| = |\mathbb{Q}| \text{ oder } 2N \rightarrow N, n \mapsto \frac{n}{2} \text{ inj.}$$

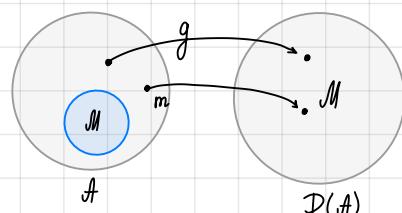
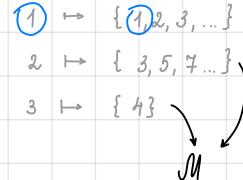
$$\checkmark |N| = |\mathbb{Z}| \text{ mittels der Bijektion } f: \mathbb{Z} \rightarrow N, z \mapsto \begin{cases} 2z+1, & z \geq 0 \\ -2z, & \text{sonst} \end{cases}$$

Hilbert'sches Hotel

In einem Hotel mit endlich vielen Zimmern können keine Gäste mehr aufgenommen werden, sobald alle Zimmer belegt sind.

Hilberts Hotel hat unendlich viele Zimmer (durchnummiert mit natürlichen Zahlen bei 1 beginnend). Man könnte nun annehmen, dass dasselbe Problem auch hier auftreten würde, nämlich dann, wenn alle Zimmer durch (unendlich viele) Gäste belegt sind.

Es gibt jedoch einen Weg, Platz für einen weiteren Gast zu machen, obwohl alle Zimmer belegt sind. Der Gast von Zimmer 1 geht in Zimmer 2, der Gast von Zimmer 2 geht in Zimmer 3, der von Zimmer 3 nach Zimmer 4 usw. Damit wird Zimmer 1 frei für den neuen Gast. Da die Anzahl der Zimmer unendlich ist, gibt es keinen „letzten“ Gast, der nicht ein weiteres Zimmer umziehen könnte. Wiederholt man das, erhält man Platz für eine beliebige, aber endliche Zahl neuer Gäste. Es ist sogar möglich, Platz für abzählbar unendlich viele neue Gäste zu machen: Der Gast von Zimmer 1 geht wie vorher in Zimmer 2, der Gast von Zimmer 2 aber in Zimmer 4, der von Zimmer 3 in Zimmer 6 usw. Kurz gesagt, jeder Gast multipliziert seine Zimmernummer mit 2, um die neue zu erhalten. Damit werden alle Zimmer mit ungerader Nummer frei für die abzählbar unendlich vielen Neuankömmlinge. Wenn dies nacheinander geschehen würde, würde es bei einer unendlichen Anzahl von Gästen und einer unendlichen Anzahl von Zimmern unendlich lange dauern.



$$\left. \begin{array}{l} \forall z \in [0,1]: \exists i \in \mathbb{N}: z = f_i \\ x \in [0,1], \text{ aber } x \neq \text{alle } f_i \end{array} \right\} \Rightarrow \mathbb{R} \text{ nicht abzählbar}$$

$A$  endlich  
 $|A| = k$   
 $|\mathcal{P}(A)| = 2^k > k$

• Noch mehr Beispiele:

- $\{0, 1\}^* = |\mathbb{N}|$  wegen Bijektion  $\{0, 1\}^* \rightarrow \mathbb{N}, w \mapsto (1w)_2$ , wobei  $(w)_2$  die Zahl mit binärer Darstellung  $w$  bezeichnet.
- $|A^*| = |\mathbb{N}|$  für jede endliche Menge  $A$ .
- Die Menge der C/Java/Python-Programme ist abzählbar.
- $|\mathbb{N}| < |[0, 1]|$  wegen  $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |\{0, 1\}^{\mathbb{N}}| = |[0, 1]|$
- $|(0, 1)| = |[1, \infty)|$  wegen Bijektion  $[1, \infty) \rightarrow (0, 1], x \mapsto 1/x$
- $|(0, 1)| = |\mathbb{R}|$
- $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| = |\mathbb{R}^\mathbb{R}|$
- $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$

Satz von Cantor

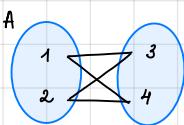
Multimenge  $\{ \cdot \}_M$  Vollfachheit wichtig  $\{ \cdot \}_M$   
Reihenfolge unwichtig

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

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

$$\{a, b, c, a\}_M = \{(a, 2), (b, 1), (c, 1), (d, 0)\}$$

wie oft  
 $j$



bipartit

$$V = A \cup B \text{ mit } A \cap B = \emptyset \quad (V = A \uplus B)$$

$$E \subseteq A \times B \cup B \times A \quad (\text{nur Kanten zwischen } A \text{ und } B)$$

charakteristische Funktion von  $f$   
 $\{0, 1\}^\Omega$  in der Menge  
(nicht in der Menge)

Für  $|A| < |B|$ : bilde eine Ungleichungskette

$$|A| \leq |C_1| \leq \dots \leq |C_n| \leq |B|$$

wobei mindestens ein Glied nicht nur  $\leq$  sondern auch  $<$  erfüllt.

• Für  $|C_i| \leq |C_{i+1}|$  gebe eine Injektion an (Spezialfall:  $C_i \subseteq C_{i+1}$ ).

• Für  $|C_i| < |C_{i+1}|$  benutze den Satz von Cantor.

Beweise  $|A| < |B|$

direkter Beweis  
gebe eine Bijektion  
 $A \rightarrow B$  oder  $B \rightarrow A$  an

indirekter Beweis  
der Satz von CBS  
gebe Injektionen  
 $A \rightarrow B$  und  $B \rightarrow A$  an

# DIGRAPHEN

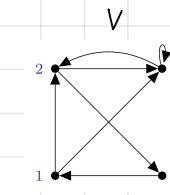
- für  $U \subseteq V$ :  $G[U]$  für  $(U, E \cap (U \times U))$  (von  $U$  induzierter Teilgraph)
- $H = (V_H, E_H)$  - Teilgraph von  $G(V_G, E_G)$ , falls  $V_H \subseteq V_G$  und  $E_H \subseteq E_G$
- $G$  ist zusammenhängend, falls  $u(E \cup E^{-1})^* v$  für alle  $u, v \in V$  gilt
- $G$  ist stark zusammenhängend, falls  $u E^* v$  und  $v E^* u$  für alle  $u, v \in V$  gilt
- $\Rightarrow$  (starke) Zusammenhangskomponente  
maximale (starke) Zusammenhangskomponente, falls es kein  $U'$  mit  $U \subseteq U' \subseteq V$  gibt, so dass  $G[U']$  selbst eine Zusammenhangskomponente ist  $\rightarrow$



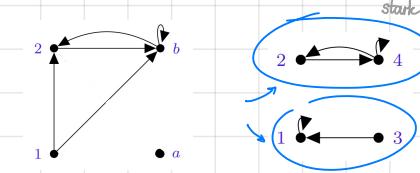
a verb. mit b, c  
b ...  
c ...

$$U = \{a, z, b\}$$

~ gerichtet



$$G[V]$$



$$G[U]$$

nicht stark zusammenhängend,  
da es gibt  $1 \rightarrow b$ , aber kein  $b \rightarrow 1$

KREIS (zyklus) - ein Pfad mit  $l \geq 1$  und  $v_0 = v_l$

einfacher Kreis ( $\{v_0, v_1, \dots, v_l\} = l$ ) enthält keine weiteren Kreise

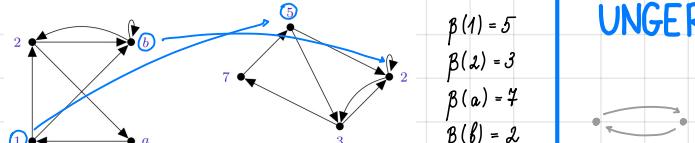
SCHLEIFE (Schlinge) - Selbstkante

kreisfrei = azyklisch

- DAG - directed acyclic graph

Äquivalenz:

ISOMORPHIE ~ STRUKTURGLEICH



$$(u, v), (v, u) \in E \subseteq V \times V \quad \{u, v\} \in E \subseteq \binom{V}{2}$$

$$\binom{V}{2} := \{ \{u, v\} \subseteq V \mid u \neq v \} \quad \text{Menge aller 2-elementigen Teilmengen}$$

$$\Gamma(u) = \{v \in V \mid \{u, v\} \in E\} \quad \text{Knotengrad}$$

Vorgänger, Nachfolger  $\rightarrow$  Nachbarschaft

Indikatorfunktion  $f: \mathbb{N} \rightarrow \{0, 1\}$

Kontinuumshypothese  $\exists M \subset \mathbb{N} \subset |M| < |\mathbb{R}|$

Turing'sche Halteproblem

@milesasrb

unentscheidbar

Beweise  $|A| = |B|$

direkter Beweis

gebe eine Bijektion  
 $A \rightarrow B$  oder  $B \rightarrow A$  an

indirekter Beweis

der Satz von CBS  
gebe Injektionen  
 $A \rightarrow B$  und  $B \rightarrow A$  an

f:  $\Omega \rightarrow \{0, 1\}$

f:  $\Omega \rightarrow \{0, 1\}$

von  $A$

in der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

(nicht in der Menge)

f

in

der Menge

**KREIS** - ein Pfad mit  $l \geq 3$  und  $v_0 = v_l$

einfacher Kreis ( $|\{v_0, v_1, \dots, v_{l-1}\}| = l$ ) besteht aus mind. 3 Knoten



kein Kreis (triviale Kreise werden ausgeschlossen)

Beweis:

$G = (A \cup B, E)$  - sei ein bipartiter Graph, der einen Kreis  $v_0, v_1, v_2, \dots, v_l$  mit  $v_0 \in A$  hat. Dann muss gelten:  $v_1 \in B, v_2 \in A$  usw.  $\Rightarrow v_l \in B$  weil  $l$  ungerade ist. Dies kann jedoch nicht sein, da  $v_l = v_0 \in A$ .

## BIPARTIT

gdw der einfache Graph keinen Kreis ungerader Länge enthält

weitere Graphklassen:

- **Multigraph** mehr als eine Kante von  $u$  nach  $v$
- **Hypergraph**  $E \subseteq P(V)$  Hyperkante verbindet mehrere Knoten gleichzeitig
- **Knoten-/Kantenbeschrifteter Graph**

Spezielle (einfache) Graphen:

- **Vollständiger Graph**  $K_n := ([n], \binom{[n]}{2})$
- **Kreisgraph**  $C_n := ([n], \{(i, (i \bmod n) + 1) \mid i \in [n]\})$

Jeder Knoten entweder hat 2 nicht leere Teilläume oder ist ein Blatt oder

- **Pfadgraph**  $P_n := ([n], \{\{i, i+1\} \mid i \in [n-1]\})$  für  $n \geq 3$
- **Perfekter Binärbaum** der Höhe  $h$

$$B_h := (\{0,1\}^h, \{\{u, ux\} \mid u \in \{0,1\}^{h-1}, h \in \mathbb{N}_0 : B_h \text{ hat } 2^h \text{ Blätter}$$

$$\text{hat } 2^h \text{ Blätter}$$

INDUKTIONSBeweIS

Induktionsbasis / -behauptung / -annahme

$2^{h+1} - 1$  Knoten

$\deg(u) \leq 1$

$$\sum_{i=1}^n i = \binom{n}{2} = \frac{n(n+1)}{2}$$

kleiner Gauß

$$K_1, K_2, K_3, K_4, K_5$$

$$C_3, C_4, C_5$$

Hyperwürfel der Dimension  $n$

$$Q_n := \{(0,1)^n, \{(u,v) \mid \sum_{i=1}^n |u_i - v_i| = 1\} \text{ mit } Q_0 := \{(\emptyset)\}, Q_1$$

$$Q_2, Q_3, Q_4$$



## GRADFOLGE

LEMMA Handschlaglemma

$$G = (V, E)$$

$$(\deg(v_1), \deg(v_2), \dots, \deg(v_n)) \text{ für } V = \{v_1, v_2, v_3, \dots, v_n\}$$

$$2|E| = \sum_{i \in [n]} \deg(v_i)$$

jeder Graph hat eine gerade Anzahl von Knoten ungeraden Grades

## GRADFOLGEN

- Welche Tupeln von Zahlen sind die Gradfolge eines Graphen?
- Lemma: Es gibt einen einfachen Graphen mit  $n$  Knoten und Gradfolge  $(d_1, \dots, d_n)$ , gdw. es einen einfachen Graphen mit  $n-1$  Knoten und Gradfolge  $\text{sort}(d_1, \dots, d_n, d_{n-1}) = (d_1, \dots, d_{n-1}, d_n - 1)$  gibt.

Dabei bezeichnet  $\text{sort}(t)$  das Tupel, das man aus  $t$  erhält, indem man die Komponenten von  $t$  aufsteigend sortiert.

Algorithmus von Havel-Hakimi

• Einiger: Aufsteigend sortierte Gradfolge  $(d_1, d_2, \dots, d_n)$ .

• Falls  $d_1 < 0$  oder  $d_n > n-1$ : Abbruch, es existiert kein entsprechender Graph.

• Falls  $d_1 = 0$ : Gib  $(\emptyset, \emptyset)$  zurück.

• Sonst:

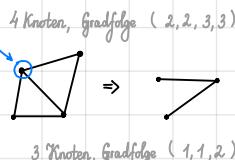
Setze  $(d_1, \dots, d_n) - 1 := (d_2, \dots, d_n, d_{n-1} - 1, \dots, d_{n-1} - 1)$ .

Bestimme eine Permutation  $\pi: [n-1] \rightarrow [n-1]$ , so dass  $(d_{\pi(1)}, \dots, d_{\pi(n-1)})$  wieder aufsteigend sortiert ist.

Bestimme rekursiv, soweit möglich, einen Graphen  $G' = ([n-1], E')$  mit  $\deg(v) = d_{\pi(i)}$ .

Gib  $G = ([n], E)$  mit  $E = \{(v, u), \pi(v) \mid (u, v) \in E'\} \cup \{(v, n-1), \dots, (v, n-d_n)\}$  zurück.

Knoten mit dem höchsten Grad



3 Knoten, Gradfolge (1, 1, 2)

(1, 1, 2, 3, 4, 4, 5) ist realisierbar

gdw (0, 1, 1, 2, 3, 3) ist realisierbar

gdw (0, 0, 1, 1, 2) ist realisierbar

gdw (0, 0, 0, 0) ist realisierbar

• top-down Reduktion der Gradfolge  
bottom-up Konstruktion

• BÄUME

- Beispiele:
  - ( $\Leftrightarrow$ ) Ist in  $G$  der Knoten mit maximalem Grad  $d_n$  genau mit Knoten der Grade  $d_{n-1}, d_{n-2}, \dots, d_{n-1}$  verbunden, dann erhält man durch Entfernen dieses Knotens einen Graphen  $G'$  mit der (unsortierten) Gradfolge  $(d_1, \dots, d_{n-1}, d_n - 1, \dots, d_{n-1} - 1)$ .

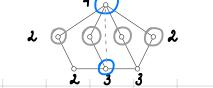
• Beispiel:



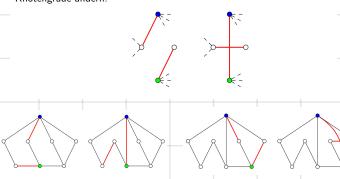
Ist in  $G$  der Knoten mit maximalem Grad  $d_n$  nicht genau mit Knoten der Grade  $d_{n-1}, d_{n-2}, \dots, d_{n-1}$  verbunden, dann tauscht man Nachbarn so lange aus, bis dies der Fall ist.

Und entfernt dann erst den Knoten mit maximalem Grad.

• Beispiel:

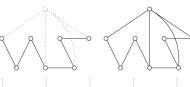


Idee: „Grün“ soll neuer Nachbar von „Blau“ werden, ohne dass sich die Knotengrade ändern.



( $\Leftarrow$ ): Hat man andererseits einen einfachen Graphen  $G'$  zu der unsortierten Gradfolge  $(d_1, \dots, d_n, d_{n-1}, d_n, d_{n-1}, \dots, d_{n-1} - 1)$  bereits gefunden, dann fügt man einfach einen neuen Knoten hinzu und verbindet diesen mit Knoten der Grade  $d_{n-1}, d_n - 1, \dots, d_{n-1} - 1$ .

• Beispiel:



ein einfacher Graph  $G = (V, E)$ , der zusammenhängend und kreisfrei ist

ein Knoten  $v \in V$  mit  $\deg(v) = 1$  - Blatt, alle anderen Knoten - innere Knoten

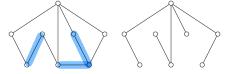
ein Graph, dessen maximale Zusammenhangskomponenten Bäume sind - Wald

BEWEIS S. 452

Sei  $G = (V, E)$  ein (einfacher Graph):

ein Taufgraph  $T = (V, E')$  mit  $E' \subseteq E$ , Jeder zusammenhängende Graph sollte daher einen Spannbaum besitzen: man entfernt einfach jede Kante, die nicht für den Zusammenhang notwendig ist.

der selbst ein Baum ist - Spannbaum



Ein Graph lässt sich durch einen Baum realisieren, wenn

fest gewählter Wurzel  $r \in V$

$G = (V, E, r)$

• Die Höhe  $h_G(v)$  eines Knotens  $v$  in  $G$  ist sein Abstand zu  $r$

• Die Höhe von  $G$  wird mit  $h(G) = \max \{h_G(v) \mid v \in V\}$

•  $u \in V \rightarrow \{u, v\} \in E$  und  $h_G(v) = h_G(u) + 1$  bezeichnet

Vater Kind

wir müssen zeigen, dass es zwischen 2 beliebigen Kindern nicht einen einfachen Pfad gibt

Widerspruch:  $G$  ist nicht zusammenhängend

$\Rightarrow$  in  $G$  existieren 2 Knoten  $u, w$ , die durch einen Pfad verbunden sind

aber  $h_G(u) = h_G(w)$  ist, ist auch jedes  $G = (V, E')$  kreisfrei, Widerspruch

•  $|V| = \sum_{v \in V} |V|_v = \sum_{v \in V} (|E| + 1) = |E| + l$

Height = 4

Height = 4

graph  $G(V, E)$  äquivalent:
 

- 1)  $|V| = |E| + 1$  schen beweisen
- 2) Nachg. per Induktion:  $G$  enthält einen Kreis  $\Rightarrow$  entfernen wir eine beliebige Kante
- 3)  $G' = (V, E')$  und  $|V| - 2$  Knoten kann jedoch nicht zusammenhängend sein  $\Rightarrow$  der Graph ist zwingend (4. Schritt)
- aus  $|V| = |E| + 1 \Rightarrow l = 1$ , d.h.  $G$  ist zwingend
- 2) Widerspruch: es gibt zwei Knoten  $u, w$ , die durch zwei unterschiedliche Pfade  $V_1, V_2, \dots, V_k$  und  $V'_1, V'_2, \dots, V'_k$  verbunden waren.  $V_1 = V'_1, V_2 = V'_2, \dots, V_k = V'_k = w$ . S. 455

• 1-4 sind für einen einfachen Graphen  $G(V, E)$  äquivalent:
 

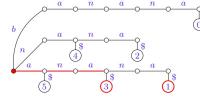
- 1)  $G$  ist ein Baum
- 2)  $G$  ist zusammenhängend und  $|V| = |E| + 1$
- 3)  $G$  ist kreisfrei und  $|V| = |E| + 1$
- 4) zwei beliebige Knoten  $u, v$  sind durch genau einen Pfad verbunden

- $u E^* v$  ( $E^*$  ist eine partielle Ordnung auf  $V$  mit dem minimalen Element  $v$ )
- Torfahre Nachfahre
- für  $u \in V$  ist  $(uE^*, E \cap (\Sigma^h), u)$  der durch  $u$  induzierte Teilbaum von  $G$

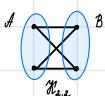
### SUFFIXBAUM

- Muss man in einem gegebenen Text  $t \in \Sigma^*$  wiederholte nach Vorkommen von Wörtern  $u, v \in \Sigma^*$  suchen, so kann die Suche mittels eines Suffixbaums beschleunigt werden:
  - Der Suffixbaum zu  $t$  hat als Knoten alle Inhalte von  $\{t\}$ , wobei  $s$  ein künstliches Endsymbol ist.
  - Zwei Inhalte  $u, v$  von  $t$  sind durch eine Kante verbunden, wenn es ein  $x \in \Sigma \cup \{s\}$  mit  $u = ux$  gibt.
  - Jedes Blatt  $uS$  ist mit dem Startindex  $|t| - |u|$  von  $u$  bzgl.  $t$  beschriftet.

Beispiel:  $t = \text{banana}$  (Knotenbezeichner als Kantenlabel)

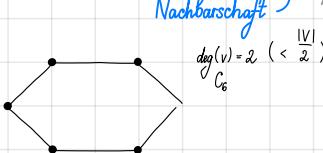


$K_{n,m}$  - ein vollständiger biparter Graph, dessen Knotenmenge  $V$  die disjunkte Vereinigung von  $A$  ( $|A|=n$ ) und  $B$  ( $|B|=m$ ) ist, mit Knotenmenge aus  $\{a, b\}$  ( $a \in A, b \in B$ )



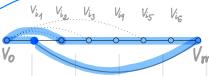
$G = (V, E)$  mit  $|V| \geq 3$  besitzt einen Hamiltonkreis, wenn in  $G$  jeder Knoten mind. den Grad  $\frac{|V|}{2}$  hat hinreichende (nicht notwendige) Bedingung

$$\deg(v), \deg(u) \geq \frac{|V|}{2} \rightarrow \{v\} \cap \Gamma(u) \neq \emptyset$$



Sei  $G = (V, E)$  ein solcher Graph. Setze  $n = |V|$ . Dann ist  $G$  zusammenhängend: Würde  $G$  in mindestens zwei max. Zshgskomponenten zerfallen, so hätte die kleinste max. Zshgskomponente höchstens  $\frac{n}{2}$  Knoten und damit jeder Knoten höchstens Grad  $\frac{n}{2} - 1$ .

Sei  $\pi = v_0, v_1, \dots, v_m$  ein längster einfacher Pfad in  $G$ ; dann muss jeder Nachbar von  $v_0$  auf  $\pi$  liegen, ebenso jeder Nachbar von  $v_m$ ; ansonsten wäre  $\pi$  nicht maximal.

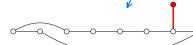


Sind  $0 < i_1 < \dots < i_k \leq m$  die Positionen der Nachbarn von  $v_0$  bzgl.  $\pi$ ; es gilt nach Annahme  $\deg(v_0) = k \geq \frac{n}{2}$ .

Einer der Knoten  $v_{i_1-1}, \dots, v_{i_k-1}$  muss ein Nachbar von  $v_m$  sein: ansonsten könnte  $v_m$  nur noch maximal Grad  $n-1-k \leq n-1-\frac{n}{2} < \frac{n}{2}$  besitzen, was unserer Annahme widerspricht.

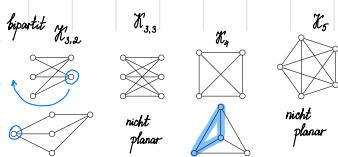
Wir finden also ein  $j \in [k]$  mit  $\{v_0, v_{i_j}\}, \{v_{i_j-1}, v_m\} \in E$ .

Würde ein Knoten  $v_i$  auf  $\pi$  einen Nachbarn  $w$  besitzen, der nicht auf  $\pi$  liegt, dann könnte  $w$  bei  $v_i$  zu einem Pfad öffnen, welcher zusammen mit  $w$  einen längeren Pfad als  $\pi$  ergeben würde.



Da  $G$  zusammenhängend ist, muss jeder Knoten von  $G$  bereits auf  $\pi$  liegen, d.h.  $\pi$  ist ein Hamiltonkreis.

## PLANARE GRAPHEN



**I**Basis: Im Fall  $n=0$  folgt  $|E|=|V|=0$ , also ist  $G$  ein Baum mit  $f=1$ , also gilt  $|E|+|V|-1=1-|V|+1=|V|=2$ .

**I**Schritt: Sei  $n \in \mathbb{N}_0$  beliebig fixiert.

falls der Graph sich in der (zwei-dimensionalen) Zeichenebene ohne Kantenüberschneidungen zeichnen lässt

**Eulersche Polyederformel (EPF)**  $f - |E| + |V| = 2$   
! Die umschließende Fläche wird mitgezählt

$(G \text{ zshg. } |E| \geq |V|-1) \Rightarrow \text{Induktion nach } n = |E| - |V| + 1 \in \mathbb{N}_0$

**I**Beweis: Die EPF gilt für jeden zshg. planaren Graph  $G = (V, E)$  mit  $|E| - |V| + 1 = 1 - |V| + 1 = 2$ .

**I**Annahme: Die EPF gilt für jeden zshg. planaren Graph  $G = (V, E)$  mit  $|E| - |V| + 1 \leq n$ .

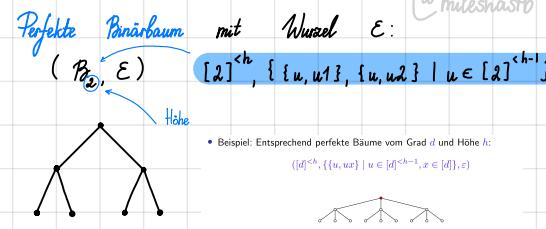
$f = 1$

**(1 Zshgskomp)**

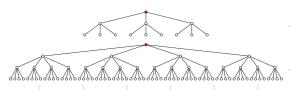
daran 1 für umschl. Fläche

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

**(Anzahl der Flächen)**

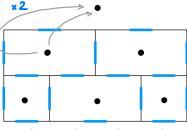


• Beispiel: Entsprechend perfekte Bäume vom Grad  $d$  und Höhe  $h$ :  $\{[d]^{h-1}, \{u, vx\} | u \in [d]^{h-1}, v \in [d], v \in \{x\}\}$



## EULERTOURNEN

Pfade, in denen alle Kanten nur einmal vorkommen



$(v_0 = v_t)$  EulerTour  $(v_0 \neq v_t)$  Eulerpfad

$$|\{v_0, v_1\}, \{v_1, v_2\}, \dots, \{v_{t-1}, v_t\}| = |E|$$

**SATZ:** Ein zusammenhängender einfacher Graph  $G = (V, E)$  besitzt genau dann eine Eulertour, wenn jeder Knoten geraden (positiven) Knotengrad hat.

**BEWEIS:** Sei  $u \in V$  beliebig fixiert

Für jede Kante, die bzgl. der Eulertour von  $u$  wegführt, muss es auch genau eine Kante geben, welche bzgl.  $u$  hinführt. Also hat  $u$  geraden Grad.

**BEWEIS:** Ein zusammenhängender einfacher Graph  $G = (V, E)$ , in dem jeder Knoten geraden Grad hat, besitzt eine Eulertour ( $|E| = k$ )

**Basis:** Sei  $k=3$  (mit weniger Knoten gibt es mindestens einen Knoten mit ungeradem Grad). Jeder zshg. Graph mit 3 Knoten ist isomorph zum  $C_3$  und besitzt eine Eulertour.

**I:** Sei  $k \geq 3$  beliebig fixiert ( $k \in \mathbb{N}$ )

**IA:** Jeder zshg. Graph  $G = (V, E)$  mit  $|E| \leq k$  und nur geraden Knotengraden besitzt eine Eulertour

**Behauptung:** Jeder zshg. Graph  $G = (V, E)$  mit  $|E| = k+1$  und nur geraden Knotengraden besitzt eine Eulertour

**Beweis:** Sei  $G = (V, E)$  zshg. mit  $|E| = k+1$  und nur geraden Knotengraden. Fixiere eine beliebige Kante  $\{u, w\} \in E$ . Sei  $G' = (V, E \setminus \{u, w\})$ .

Wir behaupten: es gibt in  $G'$  einen Pfad von  $u$  nach  $w$ .

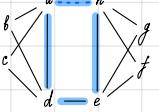
**Beweis:** Die Zshgskomponente von  $u$  in  $G'$  erhält eine gerade Anzahl von Knoten mit ungeradem Grad (Handschlaglemma)  $|E'| = \frac{\sum \deg u}{2}$

Da  $u$  und  $w$  die einzigen Knoten mit ungeradem Grad sind, muss  $w$  zur Zshgskomponente von  $u$  gehören.

Es folgt, dass mindestens ein Pfad von  $u$  nach  $w$  führt.

Es gibt somit in  $G'$  einen einfachen Pfad  $v_0, \dots, v_t$  von  $u$  nach  $w$ , zusammen mit  $\{u, w\}$  somit einen Kreis

$$K = v_0, v_1, \dots, v_t, v_0$$

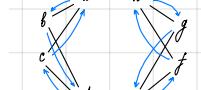


1. Fall:

Sei  $G''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden. Andernfalls hat jeder Knoten in  $G''$  geraden Grad.

Für jede der max. Zshgskomponenten von  $G''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.



Wir erhalten eine Eulertour für ganz  $G$ , indem wir die Eulertouren  $K_i$  anstelle ihrer Startknoten in  $K$  substituieren.



$n_1 = \text{adeba}, n_2 = \text{abeta}, n_3 = \text{eghfe}$   
Eulertour:  $(\text{adeba})(\text{eghfe})(\text{abeta})$

2. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

2. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

3. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

4. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

5. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

6. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

7. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

8. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

9. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

10. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

11. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

12. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

13. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

14. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

15. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

16. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

17. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Annahme; wir dürfen annehmen, dass  $K_i$  jeweils in einem Knoten von  $K$  beginnt.

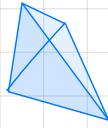
18. Fall:

Sei  $G'''$  der Graph, der aus  $G$  durch Entfernen der Kante  $v$  entsteht.  $G'''$  enthält höchstens  $k$  Knoten (tatsächlich sogar höchstens  $k-2$  Knoten).

Falls  $G'''$  gar keine Kanten mehr enthält, haben wir bereits eine Eulertour ( $K$ ) gefunden.

Für jede der max. Zshgskomponenten von  $G'''$  finden wir daher eine Eulertour  $K_i$  nach Ann

# POLYEDER



	$ E $	$ V $
$f$	4	4
	6	4
	-	+
	4	4
	$= 2$	

	$ E $	$ V $
5	8	5
	-	+
	5	5
	$= 2$	

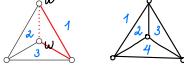
  

	$ E $	$ V $
6	12	8
	-	+
	8	8
	$= 2$	



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

IBeweis: Da  $|E| \geq |V|$ , muss  $G$  einen Kreis  $\kappa$  enthalten. Entfernen einer beliebigen Kante  $\{u, w\}$  von  $\kappa$  aus  $G$  führt auf  $G' = G \setminus \{\{u, w\}\}$ ; dabei werden die durch  $\{u, w\}$  getrennten Flächen zu einer Fläche vereinigt.



$G'$  ist noch zshg. und planar, hat eine Kante weniger als  $G$  und unterteilt die Ebene in  $f-1$  Flächen. Nach Induktionsannahme gilt  $(f-1) - (|E|-1) + |V| = 2$ , also auch  $f - |E| + |V| = 2$ .

- falls der Graph zshg.  $\rightarrow k=1$
- falls der Graph nicht zshg.  $\rightarrow f - |E| + |V| - k = 1$

EPF für planare Graphen mit  $k$  max.

Zuskomponenten  $f - |E| + |V| = 1 + k$

Für jeden planaren Graphen  $G = (V, E)$  gilt

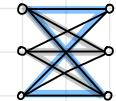
- $f - |E| + |V| \geq 2$
- $|E| \leq 3|V| - 6$ , falls  $|V| \geq 3$ , da

Jede Fläche wird durch mindestens 3 Kanten definiert; dabei zählen wir jede Kante aber doppelt, d.h.  $|E| \geq \frac{2}{3}f$  bzw.  $f \leq \frac{3}{2}|E|$ . Damit

$$2 \leq f - |E| + |V| \leq \frac{2}{3}|E| - |E| + |V| \sim -\frac{1}{3}|E| + |V|$$

- Es gibt mind. einen Knoten  $u \in V$  mit  $\deg(u) \leq 5$ , da:

$K_{3,3}$ : jeder Kreis besteht aus mindestens 4 Kanten, da alle Kreise in bipartiten Graphen gerade Länge haben.  
In einer überschneidungsfreien Darstellung des  $K_{3,3}$  müsste jede Fläche durch mindestens 4 Kanten begrenzt sein.  
Es müsste also  $\frac{4}{2}f \leq |E| = 9$  gelten und damit  $f - |E| + |V| \leq \frac{9}{2} - 9 + 6 = 1,5 < 2$



$K_5$ :  $|V| = 5$  also  $10 = |E| > 3|V| - 6 = 9$   
 $|E| = 10$  ( $|E| \leq 3|V| - 6$ )

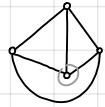
$H$  ist ein Minor von  $G$ , falls man aus  $G$  schrittweise mittels:

- ▷ Entfernen von Kanten
- ▷ Entfernen von Knoten mit Grad 0
- ▷ Kantenkontraktion

einen zu  $H$  isomorphen Graphen erzeugen kann

LEMMA  $x(G) \leq \frac{1}{2} + \sqrt{2|E| + \frac{1}{4}}$

Vier-Farben-Satz (planare Graphen)



Ein einfacher Graph  $G = (V, E)$  ist genau dann planar, wenn weder  $K_5$  noch  $K_{3,3}$  ein Minor von  $G$  ist

$K_5$  noch  $K_{3,3}$

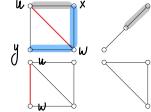
min. Knotengrad 3

min. Knotengrad 4

Sei  $G = (V, E)$  ein einfacher Graph. Fixiere eine beliebige Kante  $e = \{u, w\} \in E$ . Dann schreibt man  $G/e$  für den einfachen Graphen, den man aus  $G$  erhält, indem man  $u$  mit  $w$  identifiziert:

$$G/e = (V - \{w\}, E \cap \binom{V - \{w\}}{2}) \cup \{\{u, x\} \mid \{w, x\} \in E\}$$

Man sagt, dass  $G/e$  aus  $G$  durch die Kantenkontraktion von  $e$  gewonnen wird.



# KNOTENFÄRBUNG

$$G = (V, E)$$

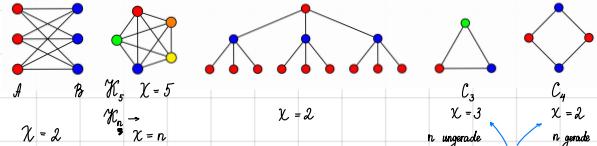
Eine Abbildung  $c: V \rightarrow \mathbb{N}$  ist eine Knotenfärbung von  $G$ , falls  $c(u) \neq c(w)$  für jede Kante  $\{u, w\} \in E$  gilt

Die Anzahl der von  $c$  verwendeten Farben ist  $lc(V)$

Die chromatische Zahl  $x(G)$  von  $G$  ist die minimale Anzahl von Farben, für die es eine Knotenfärbung von  $G$  gibt, d.h.

$$x(G) := \min \{ lc(V) \mid c: V \rightarrow \mathbb{N} \text{ Knotenfärbung von } G \}$$

Bäume:



- $x(G) \leq |V|$  für jeden einfachen Graphen
- $x(G) \leq 2$  gdw.  $G$  bipartit ist (keine Kanten  $\Rightarrow 1$  oder 0)
- $x(G) > 1$ , sobald  $E \neq \emptyset$
- $x(K_n) = n$ ,  $x(K_{m,n}) = 2$ ,  $x(C_{2k}) = 2$ ,  $x(C_{2k+1}) = 3$
- $x(G) \leq 1 + \max_{v \in V} \deg(v)$

# MATCHING

partielle Funktion  $f: S \hookrightarrow P$  maximal 1 Kante  $e \in E$  für alle  $e, e' \in M$

Ein Matching  $M$  heißt perfekt, wenn es für alle  $v \in V$  ein  $m \in M$  gibt, so dass  $v \in m$  ( $|M| = \frac{|V|}{2}$ ) ( $s_i, p_i \in V$ )

SATZ Sei  $G = (A \cup B, E)$  ein einfacher bipartiter Graph mit  $|A| \leq |B|$

Es gibt ein Matching  $M \subseteq E$  mit  $|M| = |A|$  gdw. jede Knotenteilmenge  $X \subseteq A$  mindestens  $|X|$  Nachbarn (in  $B$ ) besitzt

nicht realisierbar

LOGIK: Jeder Graph mit Gradfolge  $(3, 4, 5)$  besitzt eine Eulertour - wahr

# MATRIZEN

$m \times n$  - Matrix über einer Menge  $D$ :  $M \in D^{m \times n}$

Summe  $C = A + B \in \mathbb{R}^{m \times n}$

$$C_{ij} = A_{ij} + B_{ij}$$

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

Zeilenvektor  $D^{1 \times n}$

Spaltenvektor  $D^{m \times 1}$

**Multplikation**  $C = A \cdot B \in \mathbb{R}^{k \times n}$

$$A \in \mathbb{R}^{m \times k}, B \in \mathbb{R}^{k \times n}$$

**Skalprodukt** des  $i$ -ten Zeilenvektors und des  $j$ -ten Spaltenvektors

**nicht kommutativ!**

$$C_{ij} := \sum_{t \in [m]} A_{it} \cdot B_{tj}$$

$$\begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + 2 \cdot 3 + 0 \cdot 1 & 1 \cdot (-1) + 2 \cdot 1 + 0 \cdot 0 \\ 2 \cdot 0 + 0 \cdot 3 + 1 \cdot 1 & 2 \cdot (-1) + 0 \cdot 1 + 1 \cdot 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 1 & -2 \end{pmatrix}$$

# ADJAZENZ

MATRIX

**LEMMA** Für  $k \in \mathbb{N}$  ist  $(\mathcal{A}_G^k)_{ij}$  die Anzahl der verschiedenen  $k$ -Schritt-Pfade von  $v_i$  nach  $v_j$

INDUKTIONSBEWEIS

Sei  $\Phi_{ij}^k$  die Menge aller  $k$ -Schritt-Pfade von  $v_i$  nach  $v_j$ :  $(\mathcal{A}_G^k)_{ij} = |\Phi_{ij}^k|$  für alle  $k \in \mathbb{N}$

INDUKTIONSBASIS:  $k=1$  - 1-Schritt-Pfade entsprechen exakt den Kanten von  $G$ . Also gilt  $(\mathcal{A}_G^1)_{ij} = |\Phi_{ij}^1|$

INDUKTIONSSCHRITT: Sei  $k \in \mathbb{N}$  beliebig fixiert

INDUKTIONSAHNAMHE: Es gilt  $(\mathcal{A}_G^k)_{ij} = |\Phi_{ij}^k|$

INDUKTIONSBEHÄUPTUNG:  $(\mathcal{A}_G^{k+1})_{ij} = |\Phi_{ij}^{k+1}|$

Beweis der IB:  $(\mathcal{A}_G^{k+1})_{ij} = (\mathcal{A}_G^k \cdot \mathcal{A}_G^1)_{ij} = \sum_{m \in [n]} (\mathcal{A}_G^k)_{i,m} \cdot (\mathcal{A}_G^1)_{m,j}$  |  $\Phi_{ij}^{k+1}| = \sum_{m \in [n]} |\Phi_{i,m}^k| |\Phi_{m,j}^1| = \sum_{m \in [n]} (\mathcal{A}_G^k)_{i,m} \cdot (\mathcal{A}_G^1)_{m,j} = (\mathcal{A}_G^{k+1})_{ij}$

$\Phi_{ij}^{k+1} = \bigcup_{m \in [n]} \Phi_{i,m}^k \Phi_{m,j}^1$ , da wir die  $k+1$ -Schritt-Pfade nach dem vorletzten Knoten  $v_m$  partitionieren können.

# LOGIK

Inferenz Wenn  $A$  w, dann  $B$  w ( $A \rightarrow B$ )

Annahme (Prämissen, Antezedens, Hypothese)

logische Inferenz mit Variablen (Platzhalter für Aussagen)

Aussagenlogik

Prädikatenlogik (erster Stufe)

propositional

first-order logic (FOL)

Boolesche Werte

1,0

Belegung - eine Funktion  $\beta: V' \rightarrow \{0,1\}$  mit  $V' \subseteq V$

$k$  Variablen  $\rightarrow 2^k$  Werte

eine zu  $F$  passende Belegung  $\beta: V' \rightarrow \{0,1\}$  heißt minimal, falls  $V_F = V'$

Semantik von  $F$ :  $[F](\beta) = 0/1$   $F$  ist unter  $\beta$  falsch / wahr

$p \rightarrow q \not\Rightarrow \neg p \rightarrow \neg q \rightarrow: 1 \rightarrow 0 f$

$\oplus$

entweder, oder

$p$	$q$	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	1

$\leftrightarrow$

gdw.

$0$	$1$	$1$
1	0	1
1	1	0

Disjunktion  $\vee$  OR  
Konjunktion  $\wedge$  UND

$\cdot$  Exklusiv-Oder

XOR

wenn  $F$ , dann  $G$ , sonst  $H$

$\sim (AnB) \cup (\bar{A}n\bar{B})$

$\cdot$  Biconditional

$\leftrightarrow$

$\cdot$  If-Then-Else

ITE ( $F, G, H$ )

Es gibt mögliche binäre Operatoren und  $2^k$  Operatoren der Arität  $k$

Tautologie  $\neq$  wahr

$\checkmark$

$F$  sei (allgemein) gültig, wenn für jede Belegung  $\beta$ , die zu  $F$  passt, gilt  $[F](\beta) = 1$

**LEMMA**

eine Formel  $F$  ist gültig gdw für jede minimale Belegung  $\beta$ , die zu  $F$  passt, gilt  $[F](\beta) = 1$

$\checkmark$

$\neq$

$\neq$  falsch

$\checkmark$

$\neq$

$\neq$  widersprüchlich, wenn für jede Belegung  $\beta$ , die zu  $F$  passt, gilt  $[F](\beta) = 0$

**LEMMA**

eine Formel  $F$  ist gültig gdw für jede minimale Belegung  $\beta$ , die zu  $F$  passt, gilt  $[F](\beta) = 0$

$\checkmark$

$\neq$

$\neq$  Widerspruch

$\checkmark$

$\neq$  erfüllbar, wenn es eine Belegung  $\beta$  gibt, die zu  $F$  passt, und  $[F](\beta) = 1$

das Erfüllbarkeitsproblem (satisfiability problem, SAT)

- Ist  $F$  erfüllbar?

$F$  und  $G$  sind logisch äquivalent ( $F \equiv G$ ) gdw für jede Belegung  $\beta$ , die zu  $F$  und zu  $G$  passt, gilt:  $[F](\beta) = [G](\beta)$

(zwei verschiedene Schreibweisen derselben Aussage)

**LEMMA**

Lemma: Sei  $V_{F,G}$  die Menge der Variablen, die in  $F$  oder  $G$  vorkommen.  $F$  und  $G$  sind äquivalent genau dann, wenn für jede Belegung  $\beta: V_{F,G} \rightarrow \{0,1\}$  gilt:  $[F](\beta) = [G](\beta)$ .

$\checkmark$  folgt aus  $F$

$F \models G$  -  $F \rightarrow G$  ist gültig

Implication

gültig = korrekt

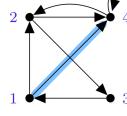
Annahme  $\vdash$

$F \rightarrow G$  Konklusion

Idempotenz

$F \vee F \equiv F$

$F \wedge F \equiv F$



$$A_G = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Es gibt 2 Pfade der Länge von  $v_1$  zu  $v_2$

$$A_G^2 = \begin{pmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

$$A_G^3 = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 2 & 1 & 3 \end{pmatrix}$$

# AUSSAGEN LOGIK

## SYNTAX

legt fest, welche Zeichenketten wohlgeformte Ausdrücke (Formeln) sind ( $F \equiv G$  syntaktisch äquivalent)

besteht aus einem Vokabular (der festlegt, welche Zeichen in Ausdrücken vorkommen dürfen) und einer Menge von Formationsregeln (die festlegen, welche Zeichenketten über dem Vokabular zulässig oder wohlgeformt sind)

Das Vokabular setzt sich aus folgenden Zeichenklassen zusammen:

- Wahrheitkonstanten: true, false
- Unendliche Menge  $V$  von Aussagenvariablen:  $p, q, r, s, t, \dots$
- Logische Operatoren:  $\neg, \wedge, \vee, \rightarrow$
- Hilfsymbole:  $(, )$

Die Formationsregeln sind:

- Regel 0: true und false sind Formeln.
- Regel 1: Eine Aussagenvariable ist eine Formel.
- Regel 2: Ist  $F$  eine Formel, dann ist auch  $\neg F$  eine Formel.
- Regel 3: Sind  $F$  und  $G$  Formeln, dann sind  $(F \wedge G)$ ,  $(F \vee G)$  und  $(F \rightarrow G)$  ebenfalls Formeln.
- Regel 4: Ein Ausdruck ist nur dann eine Formel, wenn er durch Anwendung der oben stehenden Regeln konstruiert werden kann.

## Backus-Naur-Form (BNF)

$F ::= \text{true} \mid \text{false} \mid p \mid \neg F \mid (F \vee F) \mid (F \wedge F) \mid (F \rightarrow F)$  mit  $p \in V$

atomare Formel

## SYNTAXBAUM

- geordneter Wurzelbaum

Teiformel - Zeichenkette, die als vollständig und zusammenhängend vorkommt

Talkbaum

Bindungsregeln:



atomare Teiformel

Bindungsstärke:  $\neg$  bindet stärker als  $\wedge$

Bindungsstärke:  $\wedge$  bindet stärker als  $\vee$

Bindungsstärke:  $\vee$  bindet stärker als  $\rightarrow$

- $F \leftrightarrow G \equiv (F \rightarrow G) \wedge (G \rightarrow F)$
- $F \oplus G \equiv (F \vee G) \wedge (\neg F \vee \neg G)$

## Aquivalenzumformung $\Rightarrow$

**Ersetzbarkeitstheorem:** Seien  $F, G, H$  aussagenlogische Formeln mit  $F \equiv G$  und  $F$  eine Teilformel von  $H$ .

Sei  $H'$  eine aussagenlogische Formel, welche aus  $H$  entsteht, indem man ein beliebiges Vorkommen von  $F$  in  $H$  durch  $G$  ersetzt.

Dann gilt  $H \equiv H'$ .

@ miles hasb

literale

$\{ p, \neg p \mid p \in V \}$

## NORMALFORM:

- konjunktiver KNF  $\bigwedge_{i=1}^m (\bigvee_{j=1}^{m_i} L_{i,j}) \quad \neg p \wedge (p \vee r) \wedge (p \vee q)$
- disjunktiver DNF  $\bigvee_{i=1}^m (\bigwedge_{j=1}^{m_i} L_{i,j}) \quad r \vee (\neg p \wedge q)$

$$\begin{aligned} p^0 &:= \neg p \quad \text{negative literal} \\ p^1 &:= p \quad \text{positive literal} \end{aligned}$$

Erfüllbarkeitsäquivalent  $F \equiv_e G$  (es gibt eine erfüllende Belegung  $\beta_F$  für  $F$  bzw. es gibt eine erfüllende Belegung  $\beta_G$  für  $G$  gilt)

▷ Beispiel:  $F = (p_1 \wedge p_2) \vee (p_3 \wedge p_4) \vee \dots \vee (p_{2k-1} \wedge p_{2k})$

- KNF zu  $F$  besteht aus  $2^k$  verschiedenen Disjunktionen von Literalen (sog. Klauseln), ist also exponentiell länger als  $F$ .
- Erfüllbarkeitsäquivalente Formel mittels Hilfsvariablen wird nur um konstanten Faktor länger.

$$\begin{aligned} q_0 &\leftarrow q_1 \vee q_2 \equiv (q_0 \rightarrow q_1 \vee q_2) \wedge (q_1 \wedge q_2 \rightarrow q_0) \equiv \\ q_1 &\leftarrow p_1 \wedge p_2 \equiv (\neg q_0 \vee (q_1 \vee q_2)) \wedge (\neg(q_1 \wedge q_2) \vee q_0) \equiv \\ q_2 &\leftarrow p_3 \wedge p_4 \equiv (\neg q_0 \vee q_1 \vee q_2) \wedge (\neg q_1 \vee \neg q_2 \vee q_0) - \text{KNF} \end{aligned}$$

Für jede Formel  $F$  gibt es eine Formel in KNF und in DNF

▷ Wahrheitstafel:

			$((p \rightarrow q) \wedge (\neg p \rightarrow r))$
$p$	$q$	$r$	
0	0	0	1
0	0	1	1
0	1	0	1
1	0	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

▷ KNF:

$$ITE(p, q, r) \equiv K_F = (p \vee q \vee r) \wedge (p \vee \neg q \vee r) \vee (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r)$$

▷ DNF:

$$ITE(p, q, r) \equiv D_F = (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$$

$(F \wedge F)$	$\equiv F$	(Idempotenz)
$(F \vee F)$	$\equiv F$	
$(F \wedge G)$	$\equiv (G \wedge F)$	(Kommutativität)
$(F \vee G)$	$\equiv (G \vee F)$	
$((F \wedge G) \wedge H)$	$\equiv (F \wedge (G \wedge H))$	(Assoziativität)
$((F \vee G) \vee H)$	$\equiv (F \vee (G \vee H))$	
$(F \wedge (F \vee G))$	$\equiv F$	(Absorption)
$(F \vee (F \wedge G))$	$\equiv F$	
$(F \wedge (G \vee H))$	$\equiv ((F \wedge G) \vee (F \wedge H))$	(Distributivität)
$(F \vee (G \wedge H))$	$\equiv ((F \vee G) \wedge (F \vee H))$	
$\neg \neg F$	$\equiv F$	(Doppelnegation)
$\neg(F \wedge G)$	$\equiv (\neg F \vee \neg G)$	(deMorgan)
$\neg(F \vee G)$	$\equiv (\neg F \wedge \neg G)$	
$(F \wedge \neg F)$	$\equiv \text{false}$	(Triviale Kontradiktion)
$(F \vee \neg F)$	$\equiv \text{true}$	(Triviale Tautologie)
$(F \wedge \text{false})$	$\equiv \text{false}$	(Dominanz)
$(F \vee \text{true})$	$\equiv \text{true}$	
$(F \wedge \text{true})$	$\equiv F$	(Identität)
$(F \vee \text{false})$	$\equiv F$	

**OPERATOR-BASIS** Zu jeder beliebigen Booleschen Funktion  $f: \{0,1\}^n \rightarrow \{0,1\}$  gibt es eine Formel  $F$  in DNF mit  $V_F = \{p_1, p_2, \dots, p_n\}$ , so dass  $[F](B) = f(\beta(p_1), \beta(p_2), \dots, \beta(p_n))$  für jede zu  $F$  passende Belegung  $\beta$   $\Rightarrow$  (Operator-) Basis  $\{\wedge, \vee, \neg\}$  (vollständige Menge)  $(F \wedge G) \equiv \neg(\neg F \vee \neg G)$

$$\begin{aligned} \text{NAND } \bar{\wedge} \quad (F \bar{\wedge} G) &:= \neg(F \wedge G) & \text{nicht assoziativ} \\ \text{NOR } \bar{\vee} \quad (F \bar{\vee} G) &:= \neg(F \vee G) \end{aligned}$$

$$\neg F \equiv \neg(\neg F \wedge F) \equiv (F \bar{\wedge} F)$$

$$(F \vee G) \equiv \neg(\neg F \wedge \neg G) \equiv ((F \bar{\wedge} F) \bar{\vee} (G \bar{\wedge} G))$$

$\{\vee, \wedge\}$  keine Basis

$\{\rightarrow, \text{false}\}, \{\rightarrow, \neg\}$  vollständig

## KLAUSEL

ist eine Disjunktion von literalen  $(p \vee \neg q), (p \vee q \vee r), p \dots$

$$\{\neg p, p, \neg q, r\} \sim \neg p \wedge (p \vee \neg q \vee r)$$

## OLR

one-line rule: falls  $\{L\} \in \mathcal{K}$ , dann soll  $L = \text{true}$

## PLR

pure-line rule: falls nur  $L$  in  $\mathcal{K}$  auftritt, aber  $\neg L$  nicht, dann soll  $L = \text{true}$

## Wissenrepräsentation

- Wissen wird durch  $\rightarrow$  Implikationen dargestellt - Regeln
- Konjunktion von Regeln - Wissensbasis
- Ziel

$\{s\} \xrightarrow{s=\text{true}} \dots$

## RESOLUTION

Def.: Resolventenbildung

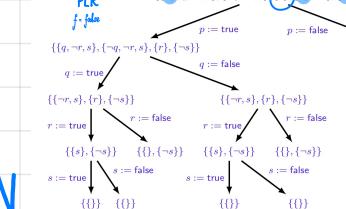
Für Literal  $L$ , Klauseln  $K_1, K_2$  mit  $L \in K_1, \bar{L} \in K_2$  gilt:

$$K_1, K_2 \vdash (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\bar{L}\})$$

Resolvent

DPLL: Suche nach einer erfüllenden Belegung

DPLL: Davis-Putnam-Logemann-Loveland



nur eine literal pro Schritt

$$\begin{array}{c} \{p\} \quad \{\neg p\} \\ \diagdown \quad \diagup \\ \{\neg p, q, r\} \quad \{\neg p, \neg s, t\} \\ \diagup \quad \diagdown \\ p \wedge \neg p = \text{false} \end{array}$$

## GRUNDPRINZIPIEN

$$\bullet \text{ SUMMENREGEL} \quad A \cap B = \emptyset \rightarrow |A \cup B| = |A| + |B|$$

$$\bullet \text{ PRODUKTREGEL} \quad |A \times B| = |A| \cdot |B|$$

$$\bullet \text{ SCHUBFACHPRINZIP} \quad f: A \rightarrow B \quad |A| = \sum_{b \in B} |\bar{f}^{-1}(b)| \leq |B| \max_{b \in B} |\bar{f}^{-1}(b)|$$

$$\text{A, B - endlich} \quad \max_{b \in B} |\bar{f}^{-1}(b)| \geq \frac{|A|}{|B|}$$

$$\bullet \text{ DOPPELTES ABZHÄLEN} \quad 2|E| = \sum_{v \in V} \deg(v)$$

## KOMBINATORIK

beschäftigt sich mit den (effizienten) Zählen komplizierter Mengen

$$A = \{p_1, p_2, p_3\}$$

$$B = \{f, m\}$$

$$\sum_{s \in S} |\{t \in T \mid (s, t) \in R\}| = \sum_{t \in T} |\{s \in S \mid (s, t) \in R\}|$$

Ziehen aus einer Urne:  $n$  Kugeln insgesamt  
 $k$  Kugeln werden hintereinander gezogen

- Zurücklegen + Reihenfolge

- Zurücklegen - Reihenfolge

+ Zurücklegen - Reihenfolge

+ Zurücklegen + Reihenfolge

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

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

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

$$M_{n,k} := \{(s_1, s_2, \dots, s_k) \in [n]^k\} - n^k \text{ Möglichkeiten}$$

- Zurücklegen  
+ Reihenfolge
- $A_{n,k} := \{(s_1, s_2, \dots, s_k) \in [n]^k \mid |\{s_1, s_2, \dots, s_k\}| = k\}$
- $k$ -Tupel mit  $k$  verschiedenen Einträgen aus  $[n] = \{1, 2, \dots, n\}$
- falls  $k > n$ , dann  $|A_{n,k}| = 0$  ( $A_{n,k} = \emptyset$ )
  - falls  $k = 0 \leq n$ , dann  $|A_{n,0}| = 1$  ( $A_{n,0} = \{\()\}$ )
- $|A_{n,k}| = n \cdot |A_{n-1, k-1}|$ , wobei  $|A_{n,0}| = 1$
- $|A_{n,k}| = n \cdot (n-1) \cdot \dots \cdot (n-k+1) = \frac{n!}{(n-k)!}$

## BINOMIALFORMEL

$$(1+x)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k$$

Tandemdistanz Identität  $= \sum_{i=0}^k \binom{m}{i} \binom{n}{k-i}$

- + Zurücklegen  
- Reihenfolge

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

Aufsteigend sortierte  $k$ -Tupel über  $[n]$  mit Wiederholungen

$D_{k,n} := \{(k_1, \dots, k_n) \in \mathbb{N}_0^n \mid k_1 + k_2 + \dots + k_n = k\}$ 

$k_i$  zählt Vorkommen von Wert  $i$

$n = 5, k = 6$

$C_{5,6} \ni (1, 1, 2, 4, 5, 5) \Leftrightarrow (2, 1, 0, 1, 2) \in D_{6,5}$

$D_{k,n} := \{(s_1, \dots, s_k) \in \mathbb{N}_0^k \mid s_1 + s_2 + \dots + s_k = n\}$

maximal  $k$  Einträge  $|E_{n,k}| = |D_{n,k+1}| = \binom{n+k}{n}$

# VERTEILUNGS PROBLEME

$\text{obj} - kd +$

Wieviele Möglichkeiten gibt es,  $n$  Euro unter  $k$  Kindern zu verteilen, so dass jedes Kind mindestens 1 Euro erhält?

Die Euros sind nicht unterscheidbar, Kinder aber schon.

$G_{n,k} := \{(s_1, \dots, s_k) \in \mathbb{N}^k \mid s_1 + \dots + s_k = n\}$

$s_1 + \dots + s_k = n$

sortierte Zählsktoren mit  $k$  Komponenten und Summe  $n$

$|G_{n,k}| = \binom{n-1}{k-1}$

Jedes Tupel  $(s_1, \dots, s_k)$  kann geschrieben werden als

$a = \underbrace{s_1}_{\geq 1} + \underbrace{s_2}_{\geq 1} + \dots + \underbrace{s_k}_{\geq 1} = n$

Damit wird das Tupel einzigartig durch die Plus-Zeichen bestimmt, die die  $s_i$  trennen.

$\sum_{k=1}^n |G_{n,k}| = \sum_{k=1}^n \binom{n-1}{k-1} = 2^{n-1}$

# ALGEBRA

• größter gemeinsamer Teiler ggT

$\text{ggT}(a, b) := \max \{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}$ 
 $= \prod_{p \in \mathbb{P}} p^{\min\{v_p(a), v_p(b)\}}$

• kleinstes gemeinsames Vielfaches kgV

$\text{kgV}(a, b) := \min \{m \in \mathbb{N} \mid a \mid m \wedge b \mid m\}$ 
 $= \prod_{p \in \mathbb{P}} p^{\max\{v_p(a), v_p(b)\}}$

$a \cdot b = \text{kgV}(a, b) \cdot \text{ggT}(a, b)$

- Zurücklegen  
- Reihenfolge

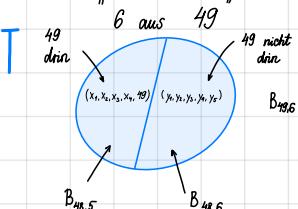
$\{s_1, s_2, \dots, s_k \subseteq [n] \mid |\{s_1, s_2, \dots, s_k\}| = k\} =: \binom{[n]}{k}$

- $k$ -elementige Teilmenge von  $[n]$
- $B_{n,k} := \{(s_1, s_2, \dots, s_k) \in [n]^k \mid s_1 < s_2 < \dots < s_k\}$
- Aufsteigend sortierte  $k$ -Tupel mit  $k$  verschiedenen Einträgen aus  $[n]$
- Jedes  $(s_1, s_2, \dots, s_k)$  kann auf  $k!$  unterschiedliche Arten umsortiert werden
- $|B_{n,k}| = \frac{|A_{n,k}|}{k!} = \binom{[n]}{k} = \frac{n!}{(n-k)!k!}$
- für  $0 \leq k \leq n$

## BINOMINALLKOEFFIZIENT

$\binom{n}{k} := \begin{cases} \frac{n!}{(n-k)!k!} & \text{falls } 0 \leq k \leq n \\ 0 & \text{sonst} \end{cases}$

$\binom{n}{n-k} = \binom{n}{k}$



$|B_{49,6}| = |B_{48,5}| + |B_{48,6}|$

$|B_{n,k}| = |B_{n-1, k-1}| + |B_{n-1, k}|$

mit  $|B_{n,0}| = 1$  und  $|B_{n,n}| = 1$

$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Elemente

$|D_{k,n}| = \binom{n+k-1}{n} = |C_{n,k}|$ 

Ziehungen  
fü r jedes Element

## STIRLING-ZAHLEN

### 2. ART

Wie viele Möglichkeiten gibt es,  $k$  (Weihnachts)-Geschenke unter  $n$  Kindern zu verteilen, so dass jedes Kind mindestens ein Geschenk erhält?

Kinder und Geschenke sind unterscheidbar

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

$k=6, n=4 \quad (3, 1, 3, 2, 2, 4) \quad |F_{n,n}| = n!$

$(3, 1, 3, 2, 2, 4) \mapsto (\underbrace{\{2\}}_{\text{Kinder}}, \underbrace{\{4, 5\}}_{\text{geschenke}}, \underbrace{\{1, 3\}}_{\text{geschenke}}, \underbrace{\{6\}}_{\text{geschenke}})$ 

geordnete Partition

Wieviele Möglichkeiten gibt es,  $k$  Geschenke in  $n$  Päckchen aufzuteilen, so dass jedes Päckchen mindestens ein Geschenk enthält?

Die Päckchen sind nicht unterscheidbar

$\{2\}, \{4, 5\}, \{1, 3\}, \{6\}$ 

ungeordnete Partition

Stirling-Zahl 2. Art  $S_{n,k} \rightarrow$  Klassen  
↓ Objekte

$|F_{n,k}| = n! \cdot S_{n,k}$

$S_{n,k} = S_{n-1, k-1} + k \cdot S_{n-1, k}$ 

$n > k > 0$

$S_{n,0} = 0$

$S_{n,n} = 1$

$\begin{array}{ll} |P_{n,k}| = |P_{n-1, k-1}| + |P_{n-k, k}| & \text{für } k > 0 \\ |P_{n,0}| = 0 & \text{für } n > 0 \\ |P_{n,k}| = 0 & \text{für } k > n \end{array}$

Partitionen von  $n$

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

• Teilbarkeitsrelation auf  $\mathbb{Z}$ :

a teilt b (ohne Rest)

$a \mid b \text{ gdw } \frac{b}{a} \in \mathbb{Z}$

• Primzahlen ( $P$  ist abzählbar unendlich  $|P| = |\mathbb{N}|$ )

$|P| = \{p \in \mathbb{N} \mid p > 1 \wedge \forall n \in \mathbb{N}: n \mid p \rightarrow (n=1 \vee n=p)\}$

• Primfaktorzerlegung von  $n \in \mathbb{N}$ :

$n = \prod_{p \in P} p^{v_p(n)}$ 

mit  $v_p(n) := \max \{k \in \mathbb{N}_0 \mid p^k \mid n\}$

$12 = 2^2 \cdot 3$

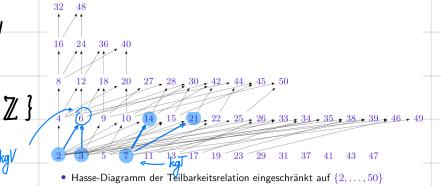
• Modulo N: Rest bei ganzzahliger Division durch N

$a \bmod N := \min \{r \in \mathbb{Z} \mid \frac{a-r}{N} \in \mathbb{Z}\} = a - \lfloor \frac{a}{N} \rfloor \cdot N \in \mathbb{Z}$

$a \equiv_N b \sim a \bmod N = b$

$\{z \in \mathbb{Z} \mid z \equiv_N k\} = [k]_N = k + N\mathbb{Z} = \{k + Nz \mid z \in \mathbb{Z}\}$

$-1 \bmod 6 = -1 - \lfloor \frac{-1}{6} \rfloor = -1 - (-1) \cdot 6 = 5$



• Hasse-Diagramm der Teilbarkeitsrelation eingeschränkt auf {2, ..., 50}

• ggV(a, b): kleinste Zahl, die von a und b erreicht werden kann.

• ggT(a, b): größte Zahl, die von a und b erreicht werden kann.

# TEILERFREMDE

(koprime) Reste modulo N  $\mathbb{Z}_N^* := \{ k \in \mathbb{Z} \mid \text{ggT}(k, N) = 1 \}$

$\mathbb{Z}_{15}^* = \{ 1, 2, 4, 7, 8, 11, 13, 14 \}$

$\varphi(N) = |\mathbb{Z}_N^*|$

$\varphi(15) = |\mathbb{Z}_{15}^*| = |\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$

ggT finden:  $\text{ggT}(a, b) = \text{ggT}(b, a) = \text{ggT}(-a, b) = \text{ggT}(a, -b) = \text{ggT}(-a, -b)$   $0 \leq a \leq b$   
 Es gilt  $b \bmod a = b - ka$  für  $k = \lfloor b/a \rfloor$

1)  $\text{ggT}(a, b) = b$  falls  $a=0$   
 2)  $\text{ggT}(a, b) = \text{ggT}(b \bmod a, a)$  für  $0 < a < b$ , da Damit:  $d \mid a \wedge d \mid b \Leftrightarrow d \mid a \wedge d \mid (b - ka)$

# ERWEITERTER EUKLIDISCHE ALGORITHMUS

## EUKLIDISCHE ALGORITHMUS

$$g = \text{ggT}(45, 63) \stackrel{!}{=} 45 \cdot 3 + 63 \cdot (-2) = g$$

$a \leq b$	$\lfloor b/a \rfloor$	$d$	$\beta$	$a \leq b$	$\lfloor b/a \rfloor$	$d$	$\beta$
45	1	3	-2	5	48	9	-19
18	2	-2	1	3	5	1	2
9	18	-	1	0	2	3	-1
				1	2	1	1
					-		0

G ist endlich, falls  $|G| < \infty$

multipaktiv

$$G \cong \langle G, \cdot, 1 \rangle$$

Beispiele:

- $\langle \mathbb{Z}, +, 0 \rangle$  0) ist eine Gruppe, falls  $\text{G ist eine Gruppe, falls}$
  - Inverse:  $-a$  1)  $\forall a, b, c : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - $\langle n\mathbb{Z}, +, 0 \rangle$  2)  $\forall a : a \cdot 1 = 1 \cdot a = a$
  - für  $n \in \mathbb{N}$  3)  $\forall a \exists b : a \cdot b = b \cdot a = 1$  es existiert
  - $n\mathbb{Z}$  - ganzzahlig 4)  $\forall a, b : a \cdot b = b \cdot a$
  - Helfende von n Untergruppe
- Grundmenge:  $\mathbb{Z}_n^* = \{ x \in \mathbb{Z}_n \mid \text{ggT}(x, n) = 1 \}$
- Gruppenoperation:  $a \cdot_n b = (a \cdot b) \bmod n$
- Neutrales: 1
- Inverse:  $d \bmod n$  invers zu  $a$  mit  $1 = \text{ggT}(a, n) = d \cdot a + \beta \cdot n$

# PERMUTATION

$$f: A \rightarrow A$$

- PERMUTATION von A

( $S_A$  - die Menge aller Permutationen)

(nicht kommutativ)

Lemma:  $(\mathbb{Z}_n, +_n, 0)$  ist eine kommutative Gruppe ( $n > 0$ ):

• Abgeschlossen:  $a +_n b = (a + b) \bmod n \in \mathbb{Z}_n$  nach Definition von modn.

• Assoziativ: Seien  $a, b, c \in \mathbb{Z}_n$ .

Dann gilt  $(a +_n b) +_n c = (a + b - kn) + c \bmod n = (a + b + c) \bmod n$ .

Symmetrisch folgt  $a +_n (b +_n c) = (a + b + c) \bmod n$ .

• Neutrales:  $0 +_n 0 = (0 + 0) \bmod n = 0 \bmod n = 0$  für  $a \in \mathbb{Z}_n \setminus \{0\}$ .

• Inverses:  $a +_n 0 = (a + 0) \bmod n = a \bmod n = a$  für  $a \in \mathbb{Z}_n \setminus \{0\}$ .

• Kommutativ:  $a +_n b = (a + b) \bmod n = (b + a) \bmod n = b +_n a$ .

# ORDNUNG EINES ELEMENTS

Setze dann  $\langle a \rangle := \{ a^k \mid k \in \mathbb{Z} \} = \{ \dots, (\bar{a}^1)^3, (\bar{a}^1)^2, \bar{a}^1, 1, a, a^2, a^3, \dots \}$

und  $\text{ord}(a) := \min \{ k \in \mathbb{N} \mid a^k = 1 \}$  (mit  $\min \emptyset := \infty$ )

- $\text{ord}(a)$  Ordnung von a und ist die kleinste positive Zahl mit  $a^k = 1$  (e)
- a wird ein Erzeuger von G genannt, falls  $\langle a \rangle = G$

additiv:  $\langle G, +, 0 \rangle$ :  $0a = 0$

$$(k+1)a := a + (ka)$$

$$(-(k+1))a := (-a) + ((-k)a)$$

zyklische

für  $G \cong \langle G, \cdot, 1 \rangle$  eine Gruppe,  $a \in G$  und  $k \in \mathbb{N}$ .

$$a^0 := 1$$

$$a^{k+1} := a \cdot (a^k)$$

$$\bar{a}^{(k+1)} := (\bar{a}^{-1}) \cdot (\bar{a}^k)$$

$$(a^k)^l = a^{kl} = (a^l)^k \quad a^k a^l = a^{k+l}$$

$$\langle a \rangle = \langle \bar{a}^{-1} \rangle$$

$$\text{ord}(a) = \text{ord}(\bar{a}^{-1})$$

Hilfsausage

LEMMA  $\varphi(N) = |\mathbb{Z}_N^*| = N \prod_{p \in P: p \mid N} (1 - \frac{1}{p})$

$$\varphi(15) = 15 \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{3}\right) =$$

$$\varphi(p) = p-1 \quad p \in P = (5-1)(3-1) = 8$$

```
# has: 0 <= a <= b
def euclid(a,b):
    if a == 0:
        return b
    return euclid(b % a, a)
```

@milesasrb

# ERWEITERTER EUKLIDISCHE ALGORITHMUS

ggT

$$\begin{aligned} \text{ggT}(a, b) &= L \cdot a + \beta \cdot b \\ 1) \quad b \bmod a &= 0, \text{ falls } L = 1, \beta = 0 \\ 2) \quad \text{ggT}(a, b) &= (\beta' - \lfloor b/a \rfloor L') a + L' b \\ \text{damit: } d \mid a \wedge d \mid b &\Leftrightarrow d \mid a \wedge d \mid (b - ka) \end{aligned}$$

G ist endlich, falls  $|G| < \infty$

multipaktiv

$$G \cong \langle G, \cdot, 1 \rangle$$

Beispiele:

- $\langle \mathbb{Z}, +, 0 \rangle$  0) ist eine Gruppe, falls  $\text{G ist eine Gruppe, falls}$
- Inverse:  $-a$  1)  $\forall a, b, c : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

- $\langle n\mathbb{Z}, +, 0 \rangle$  2)  $\forall a : a \cdot 1 = 1 \cdot a = a$
- für  $n \in \mathbb{N}$  3)  $\forall a \exists b : a \cdot b = b \cdot a = 1$  es existiert

- $n\mathbb{Z}$  - ganzzahlig 4)  $\forall a, b : a \cdot b = b \cdot a$

- Helfende von n Untergruppe

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

Gruppenoperation:  $a \cdot_n b = (a \cdot b) \bmod n$

Neutrales: 1

Inverse:  $d \bmod n$  invers zu  $a$  mit

$$1 = \text{ggT}(a, n) = d \cdot a + \beta \cdot n$$

•  $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$  - multiplicative Gruppe modulo  $n \geq 2$

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

Gruppenoperation:  $a \cdot_n b = (a \cdot b) \bmod n$

Neutrales: 1

Inverse:  $d \bmod n$  invers zu  $a$  mit

$$1 = \text{ggT}(a, n) = d \cdot a + \beta \cdot n$$

Untergruppe

•  $\langle \mathbb{Z}_6, +_6, 0 \rangle$

•  $\langle \mathbb{Z}_9^*, \cdot_9, 1 \rangle$

•  $\langle \mathbb{Z}/12\mathbb{Z}, +_{12}, 0 \rangle$

•  $\langle \mathbb{Z}/13\mathbb{Z}, +_{13}, 0 \rangle$

•  $\langle \mathbb{Z}/15\mathbb{Z}, +_{15}, 0 \rangle$

•  $\langle \mathbb{Z}/21\mathbb{Z}, +_{21}, 0 \rangle$

•  $\langle \mathbb{Z}/25\mathbb{Z}, +_{25}, 0 \rangle$

•  $\langle \mathbb{Z}/35\mathbb{Z}, +_{35}, 0 \rangle$

•  $\langle \mathbb{Z}/49\mathbb{Z}, +_{49}, 0 \rangle$

•  $\langle \mathbb{Z}/65\mathbb{Z}, +_{65}, 0 \rangle$

•  $\langle \mathbb{Z}/91\mathbb{Z}, +_{91}, 0 \rangle$

•  $\langle \mathbb{Z}/119\mathbb{Z}, +_{119}, 0 \rangle$

•  $\langle \mathbb{Z}/169\mathbb{Z}, +_{169}, 0 \rangle$

•  $\langle \mathbb{Z}/289\mathbb{Z}, +_{289}, 0 \rangle$

•  $\langle \mathbb{Z}/481\mathbb{Z}, +_{481}, 0 \rangle$

•  $\langle \mathbb{Z}/841\mathbb{Z}, +_{841}, 0 \rangle$

•  $\langle \mathbb{Z}/1681\mathbb{Z}, +_{1681}, 0 \rangle$

•  $\langle \mathbb{Z}/3361\mathbb{Z}, +_{3361}, 0 \rangle$

•  $\langle \mathbb{Z}/6721\mathbb{Z}, +_{6721}, 0 \rangle$

•  $\langle \mathbb{Z}/13441\mathbb{Z}, +_{13441}, 0 \rangle$

•  $\langle \mathbb{Z}/26881\mathbb{Z}, +_{26881}, 0 \rangle$

•  $\langle \mathbb{Z}/53761\mathbb{Z}, +_{53761}, 0 \rangle$

•  $\langle \mathbb{Z}/107521\mathbb{Z}, +_{107521}, 0 \rangle$

•  $\langle \mathbb{Z}/215041\mathbb{Z}, +_{215041}, 0 \rangle$

•  $\langle \mathbb{Z}/430081\mathbb{Z}, +_{430081}, 0 \rangle$

•  $\langle \mathbb{Z}/860161\mathbb{Z}, +_{860161}, 0 \rangle$

•  $\langle \mathbb{Z}/1720321\mathbb{Z}, +_{1720321}, 0 \rangle$

•  $\langle \mathbb{Z}/3440641\mathbb{Z}, +_{3440641}, 0 \rangle$

•  $\langle \mathbb{Z}/6881281\mathbb{Z}, +_{6881281}, 0 \rangle$

•  $\langle \mathbb{Z}/13762561\mathbb{Z}, +_{13762561}, 0 \rangle$

•  $\langle \mathbb{Z}/27525121\mathbb{Z}, +_{27525121}, 0 \rangle$

•  $\langle \mathbb{Z}/55050241\mathbb{Z}, +_{55050241}, 0 \rangle$

•  $\langle \mathbb{Z}/110100481\mathbb{Z}, +_{110100481}, 0 \rangle$

•  $\langle \mathbb{Z}/220200961\mathbb{Z}, +_{220200961}, 0 \rangle$

•  $\langle \mathbb{Z}/440401921\mathbb{Z}, +_{440401921}, 0 \rangle$

•  $\langle \mathbb{Z}/880803841\mathbb{Z}, +_{880803841}, 0 \rangle$

•  $\langle \mathbb{Z}/1761607681\mathbb{Z}, +_{1761607681}, 0 \rangle$

•  $\langle \mathbb{Z}/3523215361\mathbb{Z}, +_{3523215361}, 0 \rangle$

•  $\langle \mathbb{Z}/7046430721\mathbb{Z}, +_{7046430721}, 0 \rangle$

•  $\langle \mathbb{Z}/14092861441\mathbb{Z}, +_{14092861441}, 0 \rangle$

•  $\langle \mathbb{Z}/28185722881\mathbb{Z}, +_{28185722881}, 0 \rangle$

•  $\langle \mathbb{Z}/56371445761\mathbb{Z}, +_{56371445761}, 0 \rangle$

•  $\langle \mathbb{Z}/112742891521\mathbb{Z}, +_{112742891521}, 0 \rangle$

•  $\langle \mathbb{Z}/225485783041\mathbb{Z}, +_{225485783041}, 0 \rangle$

•  $\langle \mathbb{Z}/450971566081\mathbb{Z}, +_{450971566081}, 0 \rangle$

•  $\langle \mathbb{Z}/901943132161\mathbb{Z}, +_{901943132161}, 0 \rangle$

•  $\langle \mathbb{Z}/1803886264321\mathbb{Z}, +_{1803886264321}, 0 \rangle$

•  $\langle \mathbb{Z}/3607772528641\mathbb{Z}, +_{3607772528641}, 0 \rangle$

•  $\langle \mathbb{Z}/7215545057281\mathbb{Z}, +_{7215545057281}, 0 \rangle$

•  $\langle \mathbb{Z}/14431090114561\mathbb{Z}, +_{14431090114561}, 0 \rangle$

•  $\langle \mathbb{Z}/28862180229121\mathbb{Z}, +_{28862180229121}, 0 \rangle$

•  $\langle \mathbb{Z}/57724360458241\mathbb{Z}, +_{57724360458241}, 0 \rangle$

•  $\langle \mathbb{Z}/115448720916481\mathbb{Z}, +_{115448720916481}, 0 \rangle$

•  $\langle \mathbb{Z}/230897441832961\mathbb{Z}, +_{230897441832961}, 0 \rangle$

•  $\langle \mathbb{Z}/461794883665921\mathbb{Z}, +_{461794883665921}, 0 \rangle$

•  $\langle \mathbb{Z}/923589767331841\mathbb{Z}, +_{923589767331841}, 0 \rangle$

•  $\langle \mathbb{Z}/1847179534663681\mathbb{Z}, +_{1847179534663681}, 0 \rangle$

•  $\langle \mathbb{Z}/3694359069327361\mathbb{Z}, +_{3694359069327361}, 0 \rangle$

•  $\langle \mathbb{Z}/7388718138654721\mathbb{Z}, +_{7388718138654721}, 0 \rangle$

•  $\langle \mathbb{Z}/14777436277309441\mathbb{Z}, +_{14777436277309441}, 0 \rangle$

•  $\langle \mathbb{Z}/29554872554618881\mathbb{Z}, +_{29554872554618881}, 0 \rangle$

•  $\langle \mathbb{Z}/59109745109237761\mathbb{Z}, +_{59109745109237761}, 0 \rangle$

•  $\langle \mathbb{Z}/118219490218475521\mathbb{Z}, +_{118219490218475521}, 0 \rangle$

•  $\langle \mathbb{Z}/236438980436951041\mathbb{Z}, +_{236438980436951041}, 0 \rangle$

•  $\langle \mathbb{Z}/472877960873902081\mathbb{Z}, +_{472877960873902081}, 0 \rangle$

•  $\langle \mathbb{Z}/945755921747804161\mathbb{Z}, +_{945755921747804161}, 0 \rangle$

•  $\langle \mathbb{Z}/1891511843495608321\mathbb{Z}, +_{1891511843495608321}, 0 \rangle$

•  $\langle \mathbb{Z}/3783023686991216641\mathbb{Z}, +_{3783023686991216641}, 0 \rangle$

•  $\langle \mathbb{Z}/7566047373982433281\mathbb{Z}, +_{7566047373982433281}, 0 \rangle$

•  $\langle \mathbb{Z}/15132094747964866561\mathbb{Z}, +_{15132094747964866561}, 0 \rangle$

•  $\langle \mathbb{Z}/30264189495929733121\mathbb{Z}, +_{30264189495929733121}, 0 \rangle$

•  $\langle \mathbb{Z}/60528378991859466241\mathbb{Z}, +_{6052837899185946624$

Beispiel: -  $\text{ord}((1,2,3)) = 3$  in  $\langle S_3, \circ, \text{Id} \rangle$  da:

$$(1,2,3)^3 = ((1,2,3) \circ (1,2,3)) \circ (1,2,3) = (1,3,2) \circ (1,2,3) = (1)(2)(3) = \text{Id}$$

-  $\text{ord}(5) = 6$  in  $\langle \mathbb{Z}_7^*, \cdot_7, 1 \rangle$  da:

$$\begin{aligned} 5^6 &= (5 \cdot_7 5) \cdot_7 5^4 = 4 \cdot_7 5^4 \\ &= (4 \cdot_7 5) \cdot_7 5^3 = 6 \cdot_7 5^3 \\ &= (6 \cdot_7 5) \cdot_7 5^2 = 2 \cdot_7 5^2 \\ &= (2 \cdot_7 5) \cdot_7 5 = 3 \cdot_7 5 \\ &= 1 \end{aligned}$$

$$0, \dots, \mathbb{Z}_n = 0 \dots n-1$$

$$5 \equiv_7 -2$$

$$5^k \equiv_7 (-2)^k$$

$$\langle \mathbb{Z}_6, +_6, 0 \rangle, a = 1$$

$$\langle \mathbb{Z}_6, +_6, 0 \rangle, a = 2$$

$$\langle \mathbb{Z}_9^*, \cdot_9, 1 \rangle, a = 2$$

$$\langle \mathbb{Z}_9^*, \cdot_9, 1 \rangle, a = 4$$

$$\text{ord}(1) = 6$$

$$\text{ord}(2) = 3$$

$$\text{ord}(3) = 6$$

$$\text{ord}(4) = 3$$

-  $\text{ord}(4) = 3$  in  $\langle \mathbb{Z}_6, +_6, 0 \rangle$  da  $(4 +_6 4) +_6 4 = 2 +_6 4 = 0$

-  $\text{ord}(4) = \infty$  in  $\langle \mathbb{Z}, +, 0 \rangle$  da  $\langle 4 \rangle = 4\mathbb{Z} = \{4k \mid k \in \mathbb{Z}\}$

Länge des Kreises  $\langle a \rangle$

$$1) a^{\text{ord}(a)} = a^{\text{ord}(a)-1} a = 1$$

$$a^{-1} = a^{\text{ord}(a)-1}$$

$$4) |\langle a \rangle| = \text{ord}(a)$$

$$2) a^k = a^{k \bmod \text{ord}(a)} \quad \text{für } k \in \mathbb{Z}$$

$$3) \langle a \rangle = \{1, a, a^2, \dots, a^{\text{ord}(a)-1}\}$$

$$5) a^k = a^{k \bmod \text{ord}(a)} = 1 \text{ gdw. } k \bmod \text{ord}(a) = 0 \text{ gdw. } \text{ord}(a) | k$$

$$\langle S_3, \circ, \text{Id} \rangle, a = (1, 2, 3)$$

$$\langle \mathbb{Z}_7^*, \cdot_7, 1 \rangle, a = 5$$

$$\langle \mathbb{Z}_6, +_6, 0 \rangle, a = 4$$

$$\langle \mathbb{Z}_{12}, +_{12}, 0 \rangle, a = 3$$

$$\langle \mathbb{Z}_{11}, \cdot_{11}, 1 \rangle$$

$$\langle S_6, \circ, \text{Id} \rangle, a = (1, 2, 3, 4, 5, 6)$$

$$\langle \mathbb{Z}_{10}, \cdot_{10}, 1 \rangle$$

$$\langle \mathbb{Z}_9^*, \cdot_9, 1 \rangle$$

$$\langle \mathbb{Z}_8^*, \cdot_8, 1 \rangle$$

$$\langle \mathbb{Z}_7^*, \cdot_7, 1 \rangle$$

$$\langle \mathbb{Z}_6^*, \cdot_6, 1 \rangle$$

$$\langle \mathbb{Z}_5^*, \cdot_5, 1 \rangle$$

$$\langle \mathbb{Z}_4^*, \cdot_4, 1 \rangle$$

$$\langle \mathbb{Z}_3^*, \cdot_3, 1 \rangle$$

$$\langle \mathbb{Z}_2^*, \cdot_2, 1 \rangle$$

$$\langle \mathbb{Z}, +, 0 \rangle$$

$$\langle \mathbb{Q}, +, 0 \rangle$$

$$\langle \mathbb{R}, +, 0 \rangle$$

$$\langle \mathbb{C}, +, 0 \rangle$$

$$\langle \mathbb{H}, +, 0 \rangle$$

$$\langle \mathbb{A}, +, 0 \rangle$$

$$\langle \mathbb{B}, +, 0 \rangle$$

$$\langle \mathbb{D}, +, 0 \rangle$$

$$\langle \mathbb{E}, +, 0 \rangle$$

$$\langle \mathbb{F}, +, 0 \rangle$$

$$\langle \mathbb{G}, +, 0 \rangle$$

$$\langle \mathbb{H}, +, 0 \rangle$$

$$\langle \mathbb{I}, +, 0 \rangle$$

$$\langle \mathbb{J}, +, 0 \rangle$$

$$\langle \mathbb{K}, +, 0 \rangle$$

$$\langle \mathbb{L}, +, 0 \rangle$$

$$\langle \mathbb{M}, +, 0 \rangle$$

$$\langle \mathbb{N}, +, 0 \rangle$$

$$\langle \mathbb{O}, +, 0 \rangle$$

$$\langle \mathbb{P}, +, 0 \rangle$$

$$\langle \mathbb{Q}, +, 0 \rangle$$

$$\langle \mathbb{R}, +, 0 \rangle$$

$$\langle \mathbb{S}, +, 0 \rangle$$

$$\langle \mathbb{T}, +, 0 \rangle$$

$$\langle \mathbb{U}, +, 0 \rangle$$

$$\langle \mathbb{V}, +, 0 \rangle$$

$$\langle \mathbb{W}, +, 0 \rangle$$

$$\langle \mathbb{X}, +, 0 \rangle$$

$$\langle \mathbb{Y}, +, 0 \rangle$$

$$\langle \mathbb{Z}, +, 0 \rangle$$

$$\langle \mathbb{A}, +, 0 \rangle$$

$$\langle \mathbb{B}, +, 0 \rangle$$

$$\langle \mathbb{C}, +, 0 \rangle$$

$$\langle \mathbb{D}, +, 0 \rangle$$

$$\langle \mathbb{E}, +, 0 \rangle$$

$$\langle \mathbb{F}, +, 0 \rangle$$

$$\langle \mathbb{G}, +, 0 \rangle$$

$$\langle \mathbb{H}, +, 0 \rangle$$

$$\langle \mathbb{I}, +, 0 \rangle$$

$$\langle \mathbb{J}, +, 0 \rangle$$

$$\langle \mathbb{K}, +, 0 \rangle$$

$$\langle \mathbb{L}, +, 0 \rangle$$

$$\langle \mathbb{M}, +, 0 \rangle$$

$$\langle \mathbb{N}, +, 0 \rangle$$

$$\langle \mathbb{O}, +, 0 \rangle$$

$$\langle \mathbb{P}, +, 0 \rangle$$

$$\langle \mathbb{Q}, +, 0 \rangle$$

$$\langle \mathbb{R}, +, 0 \rangle$$

$$\langle \mathbb{S}, +, 0 \rangle$$

$$\langle \mathbb{T}, +, 0 \rangle$$

$$\langle \mathbb{U}, +, 0 \rangle$$

$$\langle \mathbb{V}, +, 0 \rangle$$

$$\langle \mathbb{W}, +, 0 \rangle$$

$$\langle \mathbb{X}, +, 0 \rangle$$

$$\langle \mathbb{Y}, +, 0 \rangle$$

$$\langle \mathbb{Z}, +, 0 \rangle$$

$$\langle \mathbb{A}, +, 0 \rangle$$

$$\langle \mathbb{B}, +, 0 \rangle$$

$$\langle \mathbb{C}, +, 0 \rangle$$

$$\langle \mathbb{D}, +, 0 \rangle$$

$$\langle \mathbb{E}, +, 0 \rangle$$

$$\langle \mathbb{F}, +, 0 \rangle$$

$$\langle \mathbb{G}, +, 0 \rangle$$

$$\langle \mathbb{H}, +, 0 \rangle$$

$$\langle \mathbb{I}, +, 0 \rangle$$

$$\langle \mathbb{J}, +, 0 \rangle$$

$$\langle \mathbb{K}, +, 0 \rangle$$

$$\langle \mathbb{L}, +, 0 \rangle$$

$$\langle \mathbb{M}, +, 0 \rangle$$

$$\langle \mathbb{N}, +, 0 \rangle$$

$$\langle \mathbb{O}, +, 0 \rangle$$

$$\langle \mathbb{P}, +, 0 \rangle$$

$$\langle \mathbb{Q}, +, 0 \rangle$$

$$\langle \mathbb{R}, +, 0 \rangle$$

$$\langle \mathbb{S}, +, 0 \rangle$$

$$\langle \mathbb{T}, +, 0 \rangle$$

$$\langle \mathbb{U}, +, 0 \rangle$$

$$\langle \mathbb{V}, +, 0 \rangle$$

$$\langle \mathbb{W}, +, 0 \rangle$$

$$\langle \mathbb{X}, +, 0 \rangle$$

$$\langle \mathbb{Y}, +, 0 \rangle$$

$$\langle \mathbb{Z}, +, 0 \rangle$$

$$\langle \mathbb{A}, +, 0 \rangle$$

$$\langle \mathbb{B}, +, 0 \rangle$$

$$\langle \mathbb{C}, +, 0 \rangle$$

$$\langle \mathbb{D}, +, 0 \rangle$$

$$\langle \mathbb{E}, +, 0 \rangle$$

$$\langle \mathbb{F}, +, 0 \rangle$$

$$\langle \mathbb{G}, +, 0 \rangle$$

$$\langle \mathbb{H}, +, 0 \rangle$$

$$\langle \mathbb{I}, +, 0 \rangle$$

$$\langle \mathbb{J}, +, 0 \rangle$$

$$\langle \mathbb{K}, +, 0 \rangle$$

$$\langle \mathbb{L}, +, 0 \rangle$$

$$\langle \mathbb{M}, +, 0 \rangle$$

$$\langle \mathbb{N}, +, 0 \rangle$$

$$\langle \mathbb{O}, +, 0 \rangle$$

$$\langle \mathbb{P}, +, 0 \rangle$$

$$\langle \mathbb{Q}, +, 0 \rangle$$

$$\langle \mathbb{R}, +, 0 \rangle$$

$$\langle \mathbb{S}, +, 0 \rangle$$

$$\langle \mathbb{T}, +, 0 \rangle$$

$$\langle \mathbb{U}, +, 0 \rangle$$

$$\langle \mathbb{V}, +, 0 \rangle$$

$$\langle \mathbb{W}, +, 0 \rangle$$

$$\langle \mathbb{X}, +, 0 \rangle$$

$$\langle \mathbb{Y}, +, 0 \rangle$$

$$\langle \mathbb{Z}, +, 0 \rangle$$

$$\langle \mathbb{A}, +, 0 \rangle$$

$$\langle \mathbb{B}, +, 0 \rangle$$

$$\langle \mathbb{C}, +, 0 \rangle$$

$$\langle \mathbb{D}, +, 0 \rangle$$

$$\langle \mathbb{E}, +, 0 \rangle$$

$$\langle \mathbb{F}, +, 0 \rangle$$

$$\langle \mathbb{G}, +, 0 \rangle$$

$$\langle \mathbb{H}, +, 0 \rangle$$

$$\langle \mathbb{I}, +, 0 \rangle$$

$$\langle \mathbb{J}, +, 0 \rangle$$

$$\langle \mathbb{K}, +, 0 \rangle$$

$$\langle \mathbb{L}, +, 0 \rangle$$

$$\langle \mathbb{M}, +, 0 \rangle$$

$$\langle \mathbb{N}, +, 0 \rangle$$

$$\langle \mathbb{O}, +, 0 \rangle$$

$$\langle \mathbb{P}, +, 0 \rangle$$

$$\langle \mathbb{Q}, +, 0 \rangle$$

$$\langle \mathbb{R}, +, 0 \rangle$$

$$\langle \mathbb{S}, +, 0 \rangle$$

$$\langle \mathbb{T}, +, 0 \rangle$$

$$\langle \mathbb{U}, +, 0 \rangle$$

$$\langle \mathbb{V}, +, 0 \rangle$$

$$\langle \mathbb{W}, +, 0 \rangle$$

$$\langle \mathbb{X}, +, 0 \rangle$$

$$\langle \mathbb{Y}, +, 0 \rangle$$

$$\langle \mathbb{Z}, +, 0 \rangle$$

$$\langle \mathbb{A}, +, 0 \rangle$$

$$\langle \mathbb{B}, +, 0 \rangle$$

$$\langle \mathbb{C}, +, 0 \rangle$$

$$\langle \mathbb{D}, +, 0 \rangle$$

$$\langle \mathbb{E}, +, 0 \rangle$$

$$\langle \mathbb{F}, +, 0 \rangle$$

$$\langle \mathbb{G}, +, 0 \rangle$$

$$\langle \mathbb{H}, +, 0 \rangle$$

$$\langle \mathbb{I}, +, 0 \rangle$$

$$\langle \mathbb{J}, +, 0 \rangle$$

$$\langle \mathbb{K}, +, 0 \rangle$$

$$\langle \mathbb{L}, +, 0 \rangle$$

$$\langle \mathbb{M}, +, 0 \rangle$$

$$\langle \mathbb{N}, +, 0 \rangle$$

$$\langle \mathbb{O}, +, 0 \rangle$$

$$\langle \mathbb{P}, +, 0 \rangle$$

$$\langle \mathbb{Q}, +, 0 \rangle$$

$$\langle \mathbb{R}, +, 0 \rangle$$

$$\langle \mathbb{S}, +, 0 \rangle</math$$