PERSONAL - Diskrete Strukturen

Mengenlehre

- es gilt:

    - $\emptyset \subseteq M$
    - wenn $M \subseteq \emptyset$, dann $M = \emptyset$
    - wenn $M_1 \subseteq M_2$, dann $M_1 \cap M_2 \neq \emptyset$
    - wenn $M_1 = M_2$, dann $M_1 \subseteq M_2$ und $M_2 \subseteq M_1$
- **Differenz** und **symmetrische Differenz**:
    - $M_2 \backslash M_1$: Elemente der Menge M_2, ohne Elemente, die auch in M_1 sind
    - $M_1 \Delta M_2$: Elemente, die nur in eines der beiden, aber nicht in beiden Mengen sind
        - $M_1 \Delta M_2 = M_2 \Delta M_1 = (M_1 \backslash M_2) \cup (M_2 \backslash M_1)$
- **Kardinalität einer Menge** $|M|$: bestimmt die **Anzahl** der (*unterschiedlichen*) Elemente einer Menge
- **Mengenoperationen**:
    - Schnitt $\cap$
        - wenn $M_1 \cap M_2 = \emptyset$, dann sind die Mengen **disjunkt**
    - Vereinigung $\cup$
- **Universum** Ω, **Komplement** $\overline{A} = \Omega \backslash A$
- **Potenzmenge** 2^M / $\mathcal{P}(M)$: alle **Teilmengen** von M
    - *Kardinalität der Potenzmenge*: $2^{|M|}$
- **Partition**: Menge von **disjunkten, nicht leeren Teilmengen** von M, **deren Vereinigung genau** M **ergibt**
- **Kartesisches Produkt**: $A \times B = \{(a, b) \mid a \in A, b \in B\}$
    - Menge aller Paare, deren ersten Komponente ein Element aus A und deren zweiten ein Element aus B ist
    - $|A \times B| = |A| * |B|$
    - **nicht kommutativ**
- **"k-Tupel"**: $A^k = \{(a_1, ..., a_k) \mid a_1, ..., a_k \in A\}$

Standardäquivalenzen

- $A = A \cup A$
- $A = A \cap A$
- $A = A \cup \emptyset$
- $\emptyset = A \cap \emptyset$
- $A \cup B = B \cup A$
- $A \cap B = B \cap A$
- $A \cup (B \cup C) = (A \cup B) \cup C$

- $A \cap (B \cap C) = (A \cap B) \cap C$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
- $A = A \cup (A \cap B)$
- $A = A \cap (A \cup B)$
- $A \,\Delta\, B = (A \setminus B) \cup (B \setminus A)$

Standardäquivalenzen mit definiertem Universum

- $A \cap \overline{A} = \emptyset$
- $A \cup \overline{A} = \Omega$
- $A \setminus B = A \cap \overline{B}$
- $\overline{\overline{A}} = A$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Wörter und Sprachen

- **Alphabet**: Σ
- **Menge aller endlichen Wörter** Σ^*: $\bigcup_{k \in \mathbb{N}_0} \Sigma^k$
  - "*Menge aller endlichen Tupel mit Einträgen aus einem Alphabet* Σ"
- **Wort** = Tupel
  - **leeres Wort** ϵ = leeres Tupel
- **Sprache**: $L \subseteq \Sigma^*$

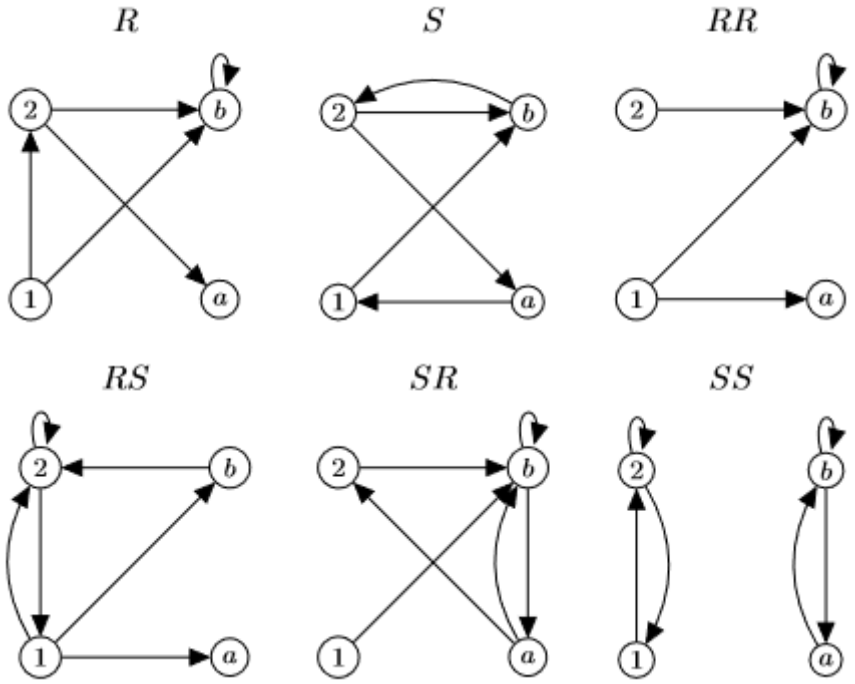
Binäre Relationen

- 2-stellige Relationen $R \subseteq A \times B$
  - *Infix-Notation*: aRb für $(a, b) \in R$

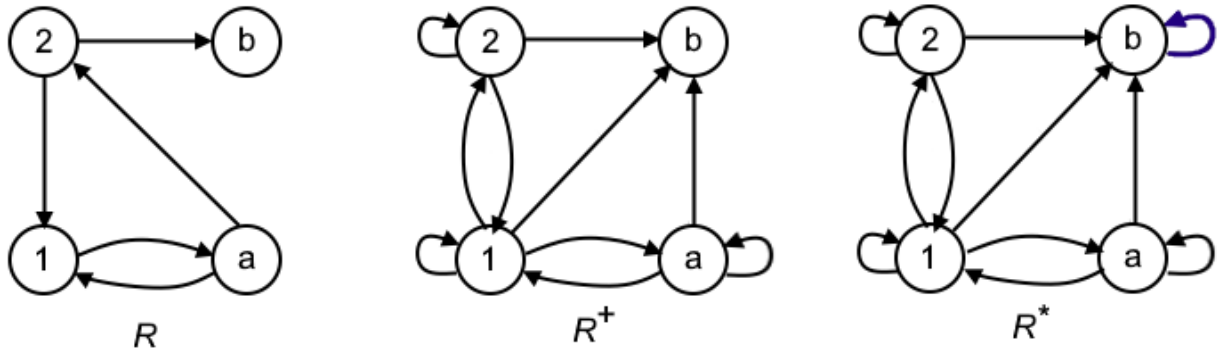
Relationales Produkt

- $R^0 = \mathrm{Id}_A = \{(a, a) \mid a \in R\}$
- $R^1 = R^0 R = R$

- $R^2 = R^1 R = RR$ (*"Pfade mit 2 Schritte"*)



- **transitive Hülle**: $R^+ = \bigcup_{k \in \mathbb{N}} R^k$ (*alle Pfade, die mindestens einen Schritt machen*)
- **reflexiv-transitive Hülle**: $R^* = R^0 \cup R^k$ (*alle Pfade, die mindestens einen Schritt machen, und auch Pfade der Länge 0 / Selbstschleifen*)

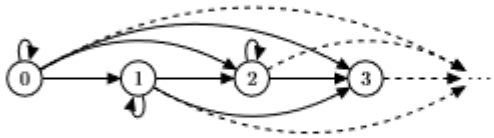


Eigenschaften von binären Relationen

- eine binäre Relation $R \subseteq A \times A$ ist...
  - ...**reflexiv**, falls $\mathrm{Id}_A \subseteq R$ (*jeder Knoten hat eine Schleife*)
  - ...**symmetrisch**, falls für jedes $(s,t) \in R$ auch $(t,s) \in R$ gilt (*zwischen je zwei Knoten gibt es entweder keine oder beide Kanten*)
  - ...**asymmetrisch**, falls für jedes $(s,t) \in R$ immer $(t,s) \notin R$ gilt (***keine Schleifen*** *+ zwischen je zwei verschiedenen Knoten gibt es höchstens eine Kante*)
  - ...**antisymmetrisch**, falls für jedes $(s,t) \in R$ und $(t,s) \in R$ auch $s = t$ gilt (***Schleifen erlaubt*** *+ zwischen je zwei verschiedenen Knoten gibt es höchstens eine Kante*)
  - ...**transitiv**, falls für jedes $(s,t) \in R$ und $(t,u) \in R$ auch $(s,u) \in R$ gilt (*kommt man mit genau zwei Schritten von s nach u, dann auch mit genau einem*)
- **partielle Ordnungen**: reflexiv, antisymmetrisch, transitiv (*z.B.* $|_{\mathbb{N}}$)

- **totale Ordnungen**: partielle Ordnung + für alle $a, b \in R$ gilt entweder aRb oder bRa
- $m \in A$ ist ein **maximales Element** bzgl. R, wenn es **keine Kanten zu einem anderen Element** gibt
  - *analog*: minimal
- *Darstellung*: Hasse-Diagramme
  ▷ **Beispiel:** $\leq_{\mathbb{N}_0}$

  Statt

  nur

- $m \in A$ ist das **größte Element** bzgl. R, wenn es **keine Kanten zu einem anderen Element** gibt und **von jedem anderen Knoten eine Kante zu** m existiert (*z.B. 1 in* $|_{\mathbb{N}}^{-1}$)
  - *analog*: kleinstes Element (*z.B. 1 in* $|_{\mathbb{N}}$)
- **(!)** mit R ist R^{-1} auch eine Ordnung

- **Äquivalenzrelationen**: reflexiv, symmetrisch, transitiv (*z.B.* $\leq_{\mathbb{Z}}$)
  - **Äquivalenzklasse** eines Objekts a bzgl. R: $[a]_R = \{b \in A \mid aRb\}$
    - z.B. $[1]_{=\mathbb{Z}} = \{1\}$, $[-5]_{\equiv_3} = \{3\mathbb{Z} + 1\}$
    - es gilt:
      - $a \in [a]_R$
      - $[a]_R = [b]_R$ für aRb
      - $[a]_R \cap [b]_R = \emptyset$ für $(a, b) \notin R$
  - **Quotient** von A bzgl. R: Menge aller Äquivalenzklassen $A/R = \{[a]_R \mid a \in A\}$
    - z.B. $\mathbb{Z}/\equiv_3 = \{3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2\}$

Funktionen

- **totale Funktion**: eine Relation $R \subseteq A \times B$, wobei es für jedes $a \in A$ **genau ein** $b \in B$ mit $(a, b) \in R$ gibt
  - *Menge aller Funktionen von A nach B*: $B^A = \{f : A \to B\}$ mit $|B^A| = |B|^{|A|}$
- **partielle Funktion**: eine Relation $R \subseteq A \times B$, wobei es für jedes $a \in A$ **höchstens ein** $b \in B$ mit $(a, b) \in R$ gibt
- **Komposition (g nach f)**: $(g \circ f)(x) = g(f(x))$

- aus $f : A \to B$ und $g : B \to C$ folgt $g \circ f : A \to C$

Eigenschaften von Funktionen

- eine Funktion $f : A \to B$ ist...
  - ...**injektiv**, falls aus $f(a) = f(a')$ stets $a = a'$ folgt (*für jedes $b \in B$ gibt es **höchstens ein Urbild***)
  - ...**surjektiv**, falls für jedes $b \in B$ ein $a \in A$ mit $f(a) = b$ gibt (*für jedes $b \in B$ gibt es **mindestens ein Urbild***)
  - ...**bijektiv**, falls sie sowohl injektiv, als auch surjektiv ist (*für jedes $b \in B$ gibt es **genau ein Urbild***)

Kardinalität von Mengen

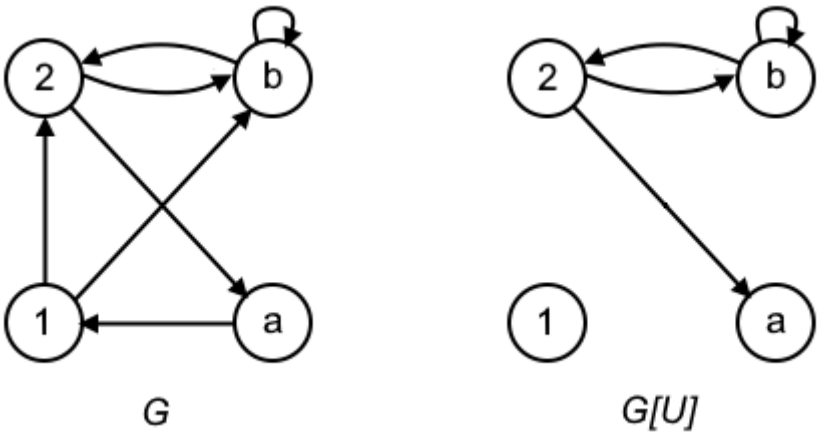
- $|A| \leq |B|$ falls es eine **Injektion** $f : A \to B$ gibt
- $|A| = |B|$ falls es eine **Bijektion** $f : A \to B$ gibt
- $|A| < |B|$ falls es eine **Injektion** $f : A \to B$, aber **keine Injektion** $g : B \to A$ gibt
- **Satz von Cantor**:
  - sind $f : A \to B$ und $g : B \to A$ **injektiv**, dann ist $h : A \to B$ **bijektiv** ($|A| = |B|$)

Graphen

Gerichtete Graphen (Digraphen)

- $G = (V, E)$
  - G - Digraph
  - V - Knotenmenge, $|V|$ - Anz. Knoten
    - *Endliche Graphen*: Wenn $|V|$ endlich, ist G endlich
  - $E \subseteq V \times V$ - Kantenmenge, $|E|$ - Anz. Kanten
    - jede Kante ist ein *Tupel* (u, v)
- *Bipartite Graphen*: $V = A \dot{\cup} B$ (A und B disjunkt)
- *Pfad*: je zwei aufeinander folgende Knoten sind durch eine gerichtete Kante aus E verbunden
  - *Länge eines Pfades*: Anzahl der Kanten
  - *einfacher Pfad*: kein Knoten taucht mehrmals auf
  - **(!) In einem endlichen Digraphen hat ein einfacher Pfad maximal die Länge $|V| - 1$**
- *Teilgraph* $G[U]$ (*von U induzierter Teilgraph*, $U \subseteq V$)

- Beispiel: $U = \{a, 2, b\}$



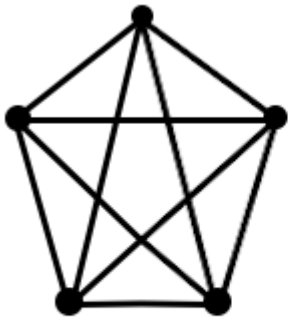
- $H = (V_H, E_H)$ **ist Teilgraph von** $G = (V_G, E_G)$**, wenn** $V_H \subseteq V_G \wedge E_H \subseteq E_G$

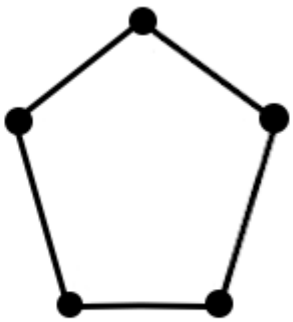
- *Zusammenhang und Zusammenhangskomponente*
  - G - zusammenhängend, wenn $u(E \cup E^{-1})^* v \; \forall u, v \in V$
    - es existiert einen Weg zwischen jedem u und v, wenn G *ungerichtet* wäre
    - $U \subseteq V$ ist eine *Zusammenhangskomponente von G*, wenn $G[U]$ *zusammenhängend ist*
    - **(*) hinreichende Bedingung:** wenn die Summe aus minimalem und maximalem Knotengrad größer oder gleich $n - 1$ ist, ist der Graph zusammenhängend
      - *generell, ohne Beweis*: prüfe anhand des maximalen Grades, ob der Knoten mit minimalem Grad irgendwie durch einen Pfad mit dem Knoten mit maximalem Grad verbunden ist
  - G - stark zusammenhängend, wenn $uE^* v \; \forall u, v \in V$
    - es existiert einen *Weg* zwischen jedem u und v im *gerichteten* Graph G
    - $U \subseteq V$ ist eine *starke Zusammenhangskomponente von G*, wenn $G[U]$ *stark zusammenhängend ist*
    - *isolierte Knoten sind starke Zusammenhangskomponenten*
    - **(!) jeder stark zusammenhängende Graph** G **mit** n **Knoten hat mindestens** n **Kanten**
- *Kreise*
  - Pfad mit $l \geq 1$, der in Knoten u beginnt und in u endet
  - *einfache Kreise*: kein Knoten taucht mehrmals auf
    - m.a.W *der Kreis enthält keinen kleineren Kreis*
  - ein Graph ohne Kreise heist azyklisch (kreisfrei)
- *Vorgänger und Nachfolger*
  - *Nachfolger* von u: $uE = \{v \in V | uEv\}$
  - *Vorgänger* von v: $Ev = \{u \in V | uEv\}$
- *Isomorphie*

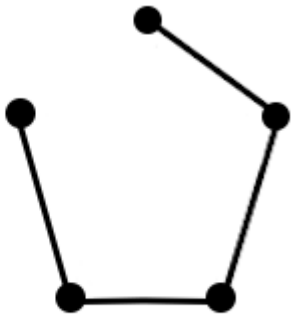
- $G \cong H$, wenn man die Knoten von G in H umbenennen kann ($V_G \to V_H$), so dass *die Kanten erhalten bleiben*
- **(!) Isomorphie $\cong$ ist eine Äquivalenzrelation**
- isomorphe Graphen haben dieselbe Gradfolge (*sortiert*), jedoch kann es sein, dass 2 nicht-isomorphe Graphen dieselbe Gradfolge haben

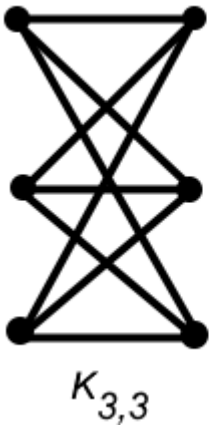
Ungerichtete und einfache Graphen

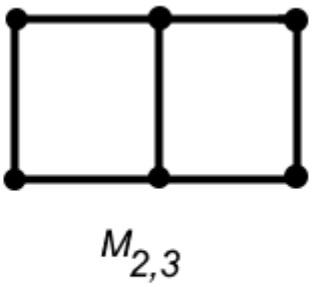
- $G = (V, E)$ ungerichtet, wenn E *symmetrisch* (wenn es zwischen zwei Knoten entweder gar keine oder beide Kanten existieren)
  - in einem ungerichteten Graph hat ein Kreis mind. Länge 3 ($l \geq 3$)
- *einfacher Graph*: endlicher, ungerichteter Digraph ohne Schleifen *(E symmetrisch, irreflexiv)*
  - **Satz**: ein **einfacher** Graph ist genau dann **bipartit**, wenn er **keinen Kreis ungerader Länge** enthält
- spezielle einfache Graphen:
  - Vollständiger Graph K_n
  - Kreisgraph C_n ($n \geq 3$)
  - Pfadgraph P_n
  - Vollständiger Bipartiter Graph $K_{m,n}$ ($m \leq n$)
  - Perfekter Binärbaum B_h (h - Höhe)

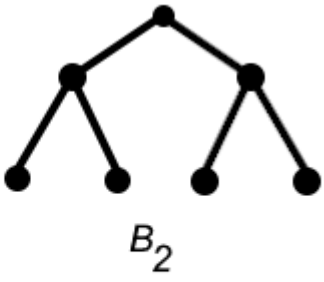












- **(!) Eigenschaften**:

- für jeden **einfachen zshgd.** Graphen gilt: $|E| \geq |V| - 1$ bzw. $|V| \leq |E| + 1$
  - "jeder zshgd. Graph hat **mindestens** $|V| - 1$ **Kanten**"
  - "jeder zshgd. Graph hat **höchstens** $|E| + 1$ **Knoten**"
- jeder **einfache** Graph mit $|E| \geq |V|$ und $|V| \geq 3$ enthält einen **Kreis**
  - G kreisfrei, wenn $|V| \geq |E| + 1$
  - wenn G **kreisfrei** ist, dann ist G **bipartit**, falls $|E| \geq 1$
- **Handschlaglemma**: $2|E| = \sum_{i \in [n]} deg(v_i)$ (*Anzahl der Kanten eines Graphen ist gleich mit der Hälfte der Summe aller Knotengrade*)
  - ein Graph mit $|V| > \frac{1}{2} \sum_{i \in [n]} d_i + 1$ kann **nicht zusammenhängend** sein (*da sonst* $|V| > |E| + 1$ *gilt und der Graph nicht genug Kanten hat*)
    - dies bedeutet jedoch nicht, dass ein Graph mit $|V| \leq \frac{1}{2} \sum_{i \in [n]} d_i + 1$ zshgd. ist

Bäume

- **einfache** Graphen, die sowohl **zshgd**., als auch **kreisfrei** sind
  - *Knoten mit* $deg(v) = 1$: "Blatt"
  - *andere Knoten*: "innere Knoten"
- **(!) Eigenschaften**:
  - $|E| = |V| - 1$ **bzw.** $|V| = |E| + 1$
  - jeder Baum mit $|V| \geq 2$ hat **mindestens 2 Blätter**
  - jeder zshgd. Graph hat **mindestens einen Spannbaum**

Perfekte Binärbaume

- **(!) Eigenschaften**:
  - ein Baum der Höhe h hat 2^h Blätter
  - ein Baum der Höhe h hat $2^{h+1} - 1$ Knoten

Wurzelbäume

- Bäume mit einer **Wurzel** (*root*), von welcher man jeden anderen Knoten erreichen kann
- Höhe = Tiefe = Level = Abstand eines Knoten u von der Wurzel r (root)
  - *Höhe eines Baumes*: max. Abstand zw. Wurzel und einem Blatt
  - *Schreibweise*:
    - uEv (u Vater von v, v Kind von u)
    - uE^*v (u Vorfahrer von v, v Nachfahrer von u)

Gradfolge

- Havel-Hakimi-Algorithmus

Hamiltonkreise und Eulertouren

- **Hamiltonkreis**: jeder **Knoten** wird **genau einmal** besucht
  - *(!) Existenz* (*hinreichend; es gibt auch Hamiltonkreise, wo diese Bedingung verletzt wird*): jeder Knoten in einem einfachen Graph mit $|V| \geq 3$ hat mindestens Grad $\frac{|V|}{2}$
- **Eulertour**: jede **Kante** wird **genau einmal** besucht
  - *(!) Existenz*: jeder Knoten in einem **einfachen, zshgd.** Graph hat **geraden** Grad

Planarität

- ein einfacher Graph ist **planar**, wenn man ihn so zeichnen kann, dass sich **keine Kanten überschneiden**
- **(!) Eulerische Polyederformel (EPF) für zshgd., planare Graphen (I)**: $f - |E| + |V| = 2$ (f: *Anzahl der Flächen*)
  - **(!) die umschließenede Fläche wird mitgezählt!**
- **(!) Eulerische Polyederformel für planare Graphen mit k maximale Zshgskomponenten (II)**: $f - |E| + |V| = 1 + k$
- **(!) Eigenschaften jedes planaren Graphen**:
  - $f - |E| + |V| \geq 2$ (*laut I und II*)
  - $|E| \leq 3|V| - 6$ für $|V| \geq 3$
  - **Satz von Kuratowski**: ein Graph ist genau dann planar, wenn er weder K_5, noch $K_{3,3}$ als Minor enthält
    - G hat mindestens 5 Knoten mit mindestens Grad 4 oder mindestens 6 Knoten mit mindestens Grad 3 $\rightarrow$ G ist **nicht** planar
  - wenn eine Fläche f durch mindestens n Kanten definiert ist: $|E| \geq \frac{n}{2} f$ bzw. $f \leq \frac{2}{n}|E|$
    - wenn eine Fläche f durch genau n Kanten definiert ist: $|E| = \frac{n}{2} f$ bzw. $f = \frac{2}{n}|E|$

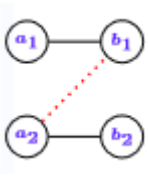
Knotenfärbung

- $\chi(G)$: minimale Anzahl der Farben, für die es eine Knotenfärbung für den Graphen G gibt
- **(!) Eigenschaften**:
  - *für einfache Graphen*: $\chi(G) \leq |V|$
  - *für bipartite Graphen*: $\chi(G) \leq 2$
  - *wenn* $E \neq \emptyset$: $\chi(G) > 1$
  - *Vier-Farben-Satz*: für jeden planaren Graphen gilt $\chi(G) \leq 4$
- **überprüfe, ob ein Graph bipartit ist**:
  - färbe einen Knoten in einer Farbe
  - färbe Nachbar mit einer anderen Farbe

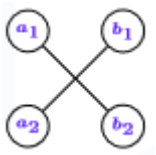
- wenn Widerspruch (*2 benachbarte Knoten haben selbe Farbe*) $\rightarrow$ G ist **nicht** bipartit

Heiratssatz, Gale-Shapley-Algorithmus

- Matchings existieren in bipartiten Graphen $G = (A \dot{\cup} B, E)$
  - **Definition**: ein Matching $M \subseteq E$ ist eine **Teilmenge** der Kanten E eines Graphen G, so dass **keine zwei Kanten aus** M **einen gemeinsamen Knoten** haben ($\forall e, e' \in M \ : \ |e \cap e'| \neq 1$)
  - **perfektes Matching**: jeder Knoten wurde gematcht ($|M| = |V|/2$)
- **Heiratssatz**: $\exists$ Matching $\leftrightarrow |\Gamma(X)| \geq |X|$ mit $\Gamma(X) = \bigcup_{x \in X} \Gamma(x)$ (X - beliebige Knotenmenge in A, $\Gamma(X)$ - Nachbarn von X in B)
  - jede Knotenteilmenge X in A hat mind. $|X|$ Nachbarn in B
- **Matchings mit Präferenzen**
  $b_1 \prec_{a_1} b_2, \quad b_2 \prec_{a_2} b_1, \quad a_1 \prec_{b_1} a_2, \quad a_1 \prec_{b_2} a_2$
  - *instabiles Matching*: $f(a) \prec_a f(a') \ \wedge \ a' \prec_{f(a')} a$ (*a bevorzugt den Partner von a' und der Partner von a' bevorzugt a* $\rightarrow$ *a und f(a') würden ihren aktuellen Partner verlassen*)

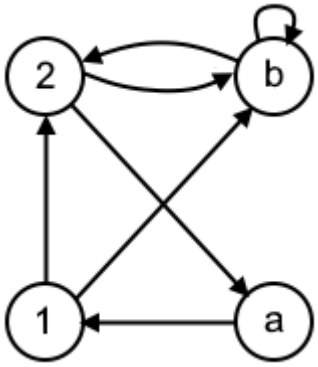
  - *stabiles Matching*

Matrizen

- $M \in D^{m \times n}$: Matrix M mit m Zeilen und n Spalten über eine Menge D
  - $D^{1 \times n}$: Zeilenvektoren
  - $D^{n \times 1}$: Spaltenvektoren
- **(!) Summe C zweier Matrizen A, B**: $C_{i,j} = A_{i,j} + B_{i,j}$ mit $C = A + B \in \mathbb{R}^{m \times n}$
  - addiere den Eintrag an Position i, j in A mit den Eintrag an derselben Position i, j in B, speichere Ergebnis an Position i, j in neuer Matrix C
- **(!) Multiplikation zweier Matrizen**:
  - es seien zwei Matrizen $A \in \mathbb{R}^{a \times b}$ und $B \in \mathbb{R}^{b \times c}$
  - das Ergebnis deren Multiplikation ist $C = A \cdot B \in \mathbb{R}^{a \times c}$
    - Ergebnis der Multiplikation hat **Zeilenanzahl von A** und **Spaltenanzahl von B**
    - $C_{i,j}$ ist das **Skalarprodukt** des **i-ten Zeilenvektors** und **j-ten Spaltenvektors**

- **(!) Adjazenzmatrizen**
  - $(A_G^k)i, j$: Anzahl der verschiedenen k-Schritt-Pfade von v_i nach v_j in G
    - A_G^0: 1 auf Diagonale von oben links nach unten rechts, sonst 0
- **Random-Surfer-Modell**
  - (P_G^k): Wahrscheinlichkeit, von v_i zu v_j in genau k Schritte zu kommen
    - $P_{i,j} = \frac{1}{|v_i E|}$ (*1 / Anzahl der Nachfolger von* v_i), wenn v_i Nachfolger hat
    - sonst, $P_{i,j} = 0$
  - Beispiel:



    - $P_G = \begin{pmatrix} 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 1/2 & 1/2 \\ 1 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 1/2 \end{pmatrix}, P_G^2 = \begin{pmatrix} 0 & 1/4 & 1/4 & 1/2 \\ 1/2 & 1/4 & 0 & 1/4 \\ 0 & 1/2 & 0 & 1/2 \\ 0 & 1/4 & 1/4 & 1/2 \end{pmatrix}, \ldots$

Aussagelogik

- **Logik**: untersucht, welche **Inferenzen** korrekt sind
- **Inferenz**: Aussage der Form "Wenn **A** wahr ist, dann ist **B** auch wahr"
  - A: Annahme
  - B: Konklusion
- **Vokabular** besteht aus:
  - `true` und `false`
  - **Unendliche Menge von Aussagevariablen** V: p, q, r etc.
  - **Operatoren**: $\wedge$, $\vee$, $\rightarrow$, $\neg$ etc.
  - **Hilfssymbole**: $(,)$
- **Logische Operatoren - Schreibweise**:

Operator	DS	ERA
Konjunktion	$\wedge$	*
Disjunktion	$\vee$	+

Operator	DS	ERA
Negation	$\neg$	$\overline{a}$

- **(!) Regeln**:
  1. `true` **und** `false` sind Formeln
  2. **Variablen** sind Formeln
  3. Ist F eine Formel, so ist $\neg F$ **auch** eine Formel
  4. Sind F und G Formeln, so sind $(F \wedge G), (F \vee G), (F \to G)$ **auch** Formeln
- **Terminalsymbole**: Symbole, die man **nicht ersetzen** kann (z.B. p, q)
- V_F: Menge aller in F vorkommenden Variablen
- G ist **Teilformel** von F, wenn G **vollständig und zshgd.** in F vorkommt
  - Beispiel: Teilformeln zu $F = ((p \vee \neg q) \wedge \neg(q \vee \neg\neg r))$
    - $p, q, \neg q, (p \vee \neg q), r, \neg r, \neg\neg r, (q \vee \neg\neg r), \neg(q \vee \neg\neg r), ((p \vee \neg q) \wedge \neg(q \vee \neg\neg r))$
- **Bindungsregeln (Reihenfolge stark $\to$ schwach)**: $\neg, \wedge, \vee, \to$
  - $\neg p \wedge q \equiv (\neg p \wedge q)$
  - $p \wedge q \to r \equiv ((p \wedge q) \to r)$
  - $p \wedge q \vee r \wedge s \equiv ((p \wedge q) \vee (r \wedge s))$
- **Belegung** $\beta : V' \to \{0, 1\}$ mit $V' \subseteq V$
  - Abbildung, die jeder **Aussagenvariablen** V' einen Wahrheitswert 0 bzw. 1 zuordnet
  - minimal, wenn $V' = V_F$
- **Bedeutung / Wahrheitswert von F**: $[F](\beta)$ oder $[F]$:
  - $$[F](\beta) = \begin{cases} 1 & \text{falls } F = true \\ 0 & \text{falls } F = false \\ \beta(p) & \text{falls } F = p \text{ für } p \in V \\ 1 - [G](\beta) & \text{falls } F = \neg G \\ \max\{[G](\beta), [H](\beta)\} & \text{falls } F = G \vee H \\ \min\{[G](\beta), [H](\beta)\} & \text{falls } F = G \wedge H \\ \max\{1 - [G](\beta), [H](\beta)\} & \text{falls } F = G \to H \end{cases}$$
- **Erf**$_G$: Menge aller minimalen Belegungen β, die G erfüllen
- Eine Formel ist...
  - ...eine **Tautologie** / **(allgemein)gültig**, wenn sie in allen Welten **wahr** ist (*für jede Belegung β gilt* $[F](\beta) = 1$) (*Test*: prüfe in Wahrheitstabelle, ob Spalte für F nur 1 enthält)
    - z.B. $p \vee \neg p$
  - ...ein **Widerspruch** / **unerfüllbar**, wenn sie in allen Welten **falsch** ist (*für jede Belegung β gilt* $[F](\beta) = 0$) (*Test*: prüfe in Wahrheitstabelle, ob Spalte für F nur 0 enthält)

        - z.B. $p \wedge \neg p$
    - ...**erfüllbar**, wenn es mindestens eine Belegung β mit $[F](\beta) = 1$ gibt (*Test*: prüfe in Wahrheitstabelle, ob Spalte für F mindestens ein 1 enthält)
        - z.B. $p \rightarrow q$
- F gültig $\leftrightarrow \neg F$ unerfüllbar
    - F unerfüllbar $\leftrightarrow \neg F$ gültig
- F nicht gültig $\leftrightarrow \neg F$ erfüllbar
    - F erfüllbar $\leftrightarrow \neg F$ nicht gültig
- F nicht gültig, aber erfüllbar $\leftrightarrow \neg F$ nicht gültig, aber erfüllbar

Wahrheitstabellen

Negation

G	$\neg G$
1	0
0	1

Konjunktion

G	H	$G \wedge H$
0	0	0
0	1	0
1	0	0
1	1	1

Disjunktion

G	H	$G \vee H$
0	0	0
0	1	1
1	0	1
1	1	1

Implikation

G	H	$G \rightarrow H$
0	0	1
0	1	1
1	0	0
1	1	1

XOR

F	G	$F \oplus G$
0	0	0
0	1	1
1	0	1
1	1	0

GDW/XNOR

F	G	$F \leftrightarrow G$
0	0	1
0	1	0
1	0	0
1	1	1

F	G	H	ITE(F, G, H)
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Logische Äquivalenzen

- $F \equiv G$ genau dann, wenn für jede mögliche Belegung β für F und G die Gleichung $[F](\beta) = [G](\beta)$ gilt
    - wenn F und G äquivalent sind, heißt das, dass F und G zwei unterschiedliche Schreibweise für die selben Formeln sind / **F und G sind semantisch gleich**
        - *Test*: prüfe in Wahrheitstabelle, ob für $F \leftrightarrow G$ die Spalte für $\leftrightarrow$ nur 1 enthält

Logische Inferenzen

- Formel der Gestalt $F \rightarrow G$ (*"F impliziert G"*) (*korrekt, wenn sie gültig ist*)
- $F \models G$ (*"G folgt aus F"*) bezeichnet, dass $F \rightarrow G$ **gültig** ist

Beziehungen

- $F \equiv G$, wenn Erf$_F$ = Erf$_G$ (Belegungen, die F erfüllen, **gleich** mit Belegungen, die G erfüllen)

- $F \models G$, wenn $\text{Erf}_F \subseteq \text{Erf}_G$ (Belegungen, die F erfüllen, **unter** den Belegungen, die G erfüllen)
- F ist **gültig**, wenn...
  - ...$\neg F$ ein *Widerspruch* ist
  - ...$F \equiv true$
  - ...$true \models F$ (*anders* $\models F$) ($1 \rightarrow a$ *nur dann gültig, wenn a = 1*)
- F ist **widersprüchlich**, wenn...
  - ...$\neg F$ eine *Tautologie* ist
  - ...$F \equiv false$
  - ...$F \models false$ ($a \rightarrow 0$ *nur dann gültig, wenn a = 0*)

Äquivalenzumformungen

- Idempotenz
  - $F \wedge F \equiv F$
  - $F \vee F \equiv F$
- Kommutativität
  - $F \wedge G \equiv G \wedge F$
  - $F \vee G \equiv G \vee F$
- Assoziativität
  - $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$
  - $(F \vee G) \vee H \equiv F \vee (G \vee H)$
- Absorption
  - $F \wedge (F \vee G) \equiv F$
  - $F \vee (F \wedge G) \equiv F$
- Distributivität
  - $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
  - $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
- Doppelnegation
  - $\neg\neg F \equiv F$
- De Morgan
  - $\neg(F \wedge G) \equiv \neg F \vee \neg G$
  - $\neg(F \vee G) \equiv \neg F \wedge \neg G$
- Triviale Kontradiktion / Tautologie
  - $F \wedge \neg F \equiv false$

- $F \vee \neg F \equiv true$

- Dominanz
  - $F \wedge false \equiv false$
  - $F \vee true \equiv true$
- Identität
  - $F \wedge true \equiv F$
  - $F \vee false \equiv F$
- Implikation
  - $F \rightarrow G \equiv \neg F \vee G$
- Bikonditional (*gdw, iff*)
  - $F \leftrightarrow G \equiv (F \rightarrow G) \wedge (G \rightarrow F) \equiv \neg(F \oplus G)$
- XOR
  - $F \oplus G \equiv (F \vee G) \wedge (\neg F \vee \neg G) \equiv (F \wedge \neg G) \vee (\neg F \wedge G)$

KNF und DNF

- **Literale** L: $\{p, \neg p\}$ (*einzelne Variablen und deren Negationen*)
- **KNF**: $(L \vee ... \vee L) \wedge ... \wedge (L \vee ... \vee L)$
  - erfüllbar, wenn **alle** *Konjunkte* erfüllbar sind
  - jede Formel ist in KNF übertragbar
    1. Entferne $\rightarrow$, $\leftrightarrow$ und $\oplus$ mit **Umformung**
    2. Wende **deMorgan** an
    3. Wende **Distributivität** an
- **DNF**: $(L \wedge ... \wedge L) \vee ... \vee (L \wedge ... \wedge L)$
  - erfüllbar, wenn **mindestens** ein *Disjunkt* erfüllbar ist
  - jede Formel ist in DNF übertragbar
    1. Entferne $\rightarrow$, $\leftrightarrow$ und $\oplus$ mit **Umformung**
    2. Wende **deMorgan** an
    3. Wende **Distributivität** an

Kanonische DNF und Kanonische KNF

- **K. DNF** (*1-Werte*)

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

$$\text{ITE}(p,q,r) \equiv D_F = \quad (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r)$$
$$(p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$$

- **K. KNF** (*0-Werte*) (*wenn KV-Diagramm, wähle 0-Werte und negiere sie*)

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

$$\text{ITE}(p,q,r) \equiv K_F = \quad (p \vee q \vee r) \wedge (p \vee \neg q \vee r)$$
$$(\neg p \vee q \vee r) \wedge (\neg p \vee q \wedge \neg r)$$

Aufstellen einer KNF-Formel erfüllbarkeitsäquivalent zu F

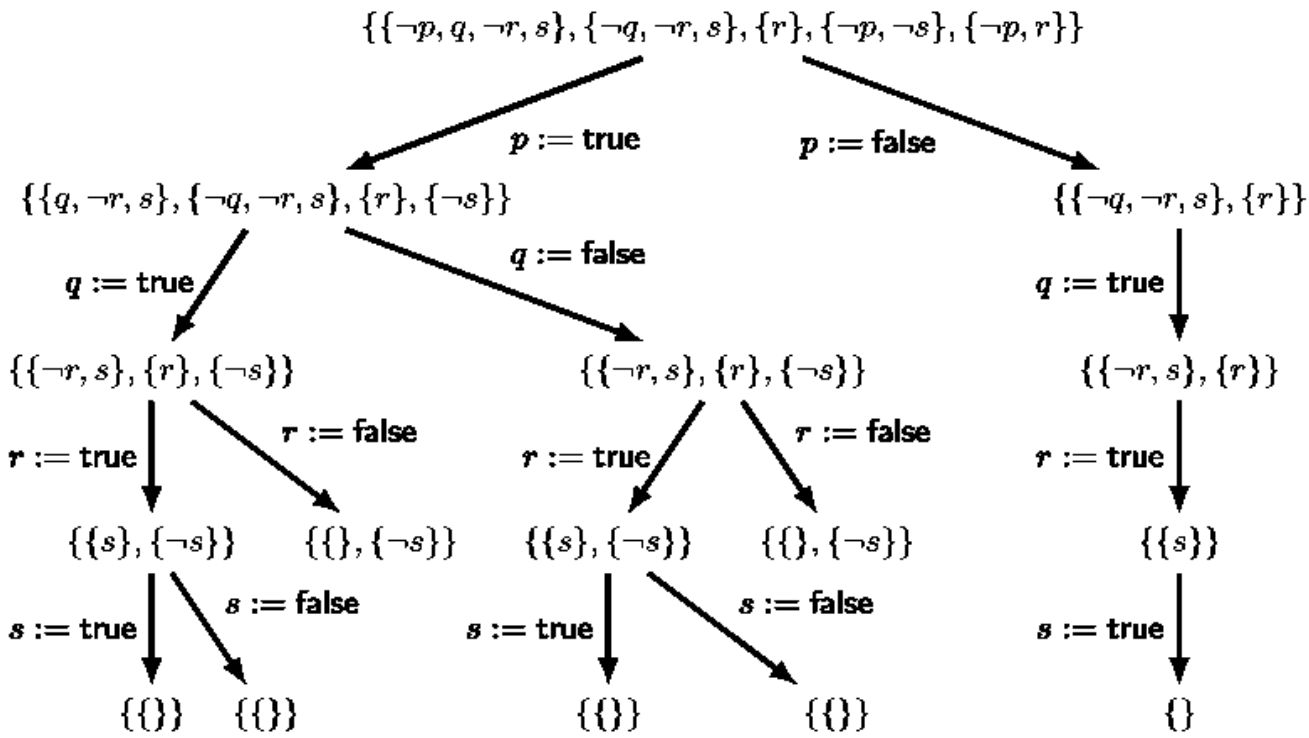
- stelle **Syntaxbaum** von F auf, notiere Wurzel als T
- für jede **Teilformel** (*nichtterminale Knoten*), notiere sie als T_i mit $T_i \leftrightarrow T_{i_1} \cdot T_{i_2}$ (wobei i_1 und i_2 die Kinder von T_i sind) bzw. $T_i \leftrightarrow \neg T_{i_1}$ (*wenn nur Negation*)
- die **finale Klausel** hat die Form $T \wedge (T \leftrightarrow T_i \cdot T_j) \wedge \ldots$
- wende **Umformungsregeln** an, um KNF zu erreichen

Weitere Operatoren

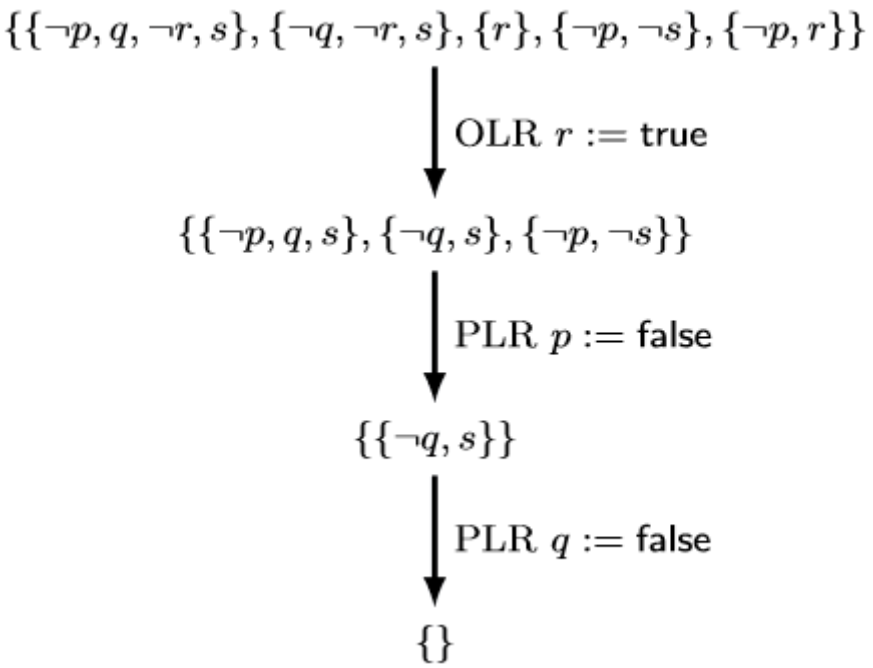
Name	Operator und Syntax	Äquivalent zu...
NAND	$F \overline{\wedge} G$	$\neg(F \wedge G)$
NOR	$F \overline{\vee} G$	$\neg(F \vee G)$

DPLL: Davis-Putnam-Logemann-Loveland für Formeln in KNF

- auf **Erfüllbarkeit** ausgerichtet
- berechnet eine **erfüllende Belegung**, die weiterhin als **Zertifikat der Erfüllbarkeit** verwendet werden kann



- **Optimierungen (*Priorität hoch* $\rightarrow$ *niedrig*)**:
  - OLR (*one-literal rule*): Wenn $\exists$ eine Klausel, die nur L enthält, setze L auf true
  - PLR (*pure-literal rule*): Wenn nur L und nie $\overline{L}$ in jedwelcher Formel auftritt, setze L auf $true$
  - Caching / Memoization: bereits behandelte Klauselmengen können ignoriert werden

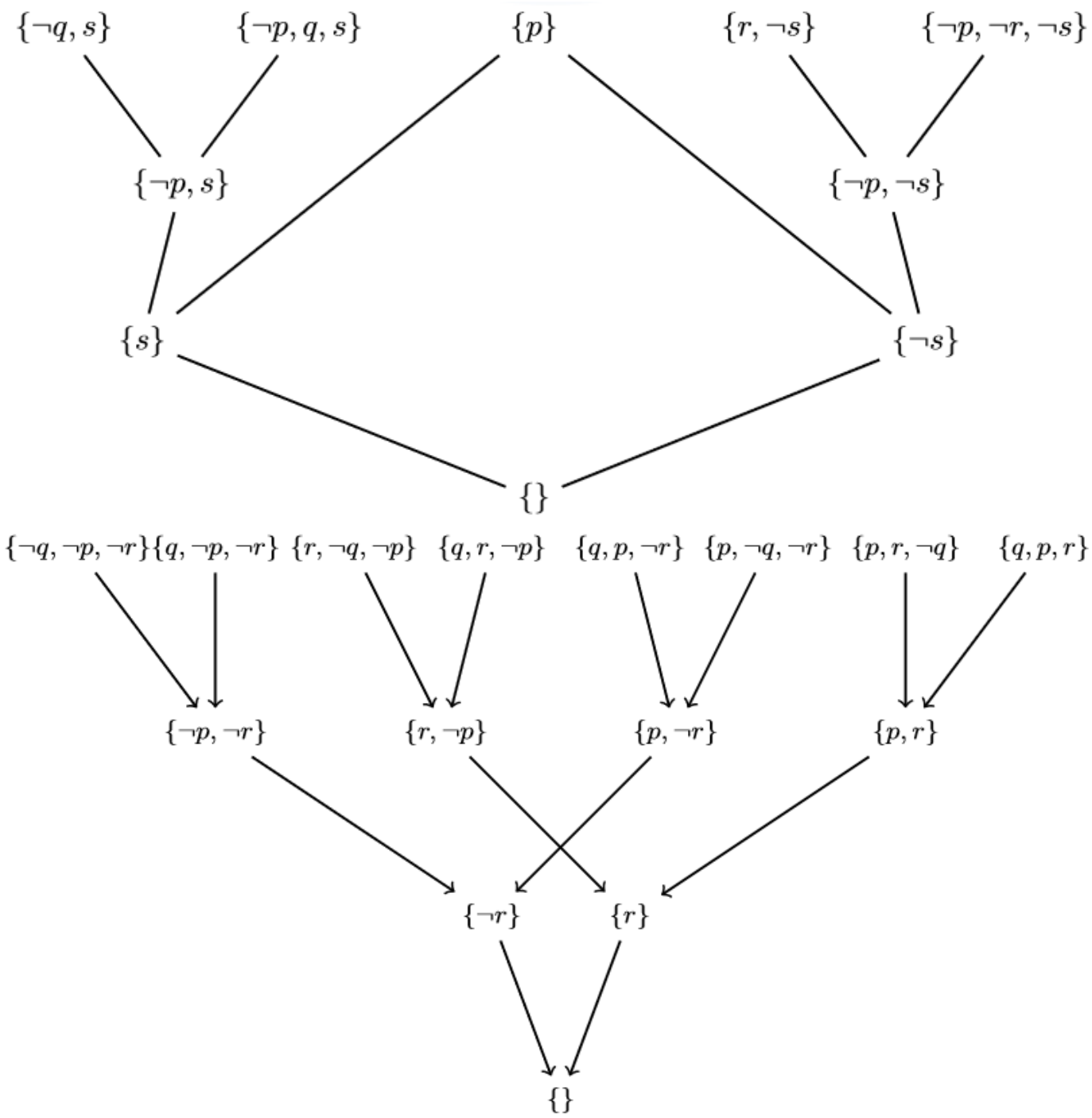


Resolution

- auf **Unerfüllbarkeit** ausgerichtet
- berechnet **Zertifikat der Unerfüllbarkeit**

1. Suche zwei Mengen K_1 und K_2, wo $L \in K_1$ **und** $\overline{L} \in K_2$ (*genau ein Literal!*)

2. Füge die **Vereinigung dieser Mengen ohne L bzw. $\overline{L}$** zur neuen Klauselmenge hinzu
3. Wiederhole, bis die **leere Klauselmenge** $\square$ bzw. {{}} resolviert wird



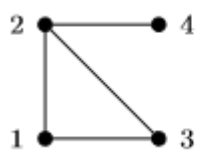
- *Anzahl der möglichen Formeln für n Literale*: $4^n = 2^{2n}$

Kombinatorik

Kombinatorische Grundprinzipien

- **Summenregel**:
  - wenn $A \cap B = \emptyset$, dann $|A \cup B| = |A| + |B|$
  - wenn $A \cap B \neq \emptyset$, dann $|A \cup B| = |A| + |B| - |A \cap B|$

- **Produktregel**:
  - $|A \times B|$ = $|A| * |B|$ (*kann mit beliebig vielen Mengen erweitert werden*)
  - analog $|\{a,b\}^n| = 2^n$
- (+) Regeln können *zusammen angewendet* werden: $|A \times (B \cup C)| = |A| * (|B| + |C|)$ für $(B \cap C) = \emptyset$
- **generelle Mengenregeln**:
  - für $f : A \to B$, wo jedes Element aus B genau m Urbilder in A hat, gilt $|A| = m|B|$
  - wenn f bijektiv, gilt $|A| = |B|$
- **Schubfachprinzip / pigeon-hole principle**:
  - falls man n Objekte auf m Mengen verteilt ($n, m > 0$) und n **größer** als m ist, dann gibt es mindestens eine Menge, in der mehr als ein Objekt landet
  - falls man n Objekte auf m Mengen verteilt ($n, m > 0$) und n **kleiner** als m ist, dann gibt es mindestens eine Menge, in der kein Objekt landet
  - **Verschärfung**: verteilt man n Elemente auf k Mengen, gibt es mindestens eine Menge, in der sich zumindest $\lceil \frac{n}{k} \rceil$ Objekte befinden
  - **Beispiele**:
    - in einer Gruppe von 3 Personen haben mindestens 2 das gleiche Geschlecht: $2 = \lceil 3/2 \rceil$
    - in einer Gruppe von 13 Personen haben mindestens 2 Personen im selben Monat Geburtstag: $2 = \lceil 13/12 \rceil$
    - es gibt in Deutschland mindestens 415 Menschen, die exakt die gleiche Anzahl von Haaren auf dem Kopf haben: $415 = \lceil 83.000.000/200.000 \rceil$, wobei die Einwohnerzahl Deutschlands 83 Mio. beträgt und die durschnittliche Anzahl der Haare auf dem Kopf 200.000 ist
- **Beweistechnik** - **Doppeltes Abzählen**:
  - *Inzidenzmatrix*: die Summe der Spalten ($\sum_{v \in V} deg(v)$) ist gleich mit der Summe der Zeilen ($2|E|$) $\to$ Beweis des Handschlaglemmas ($2|E| = \sum_{v \in V} deg(v)$)



I	1	2	3	4
$\{1,2\}$	1	1	0	0
$\{1,3\}$	1	0	1	0
$\{2,3\}$	0	1	1	0
$\{2,4\}$	0	1	0	1

- **Inklusion und Exklusion**
  - z.B. $n = 3$: $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$

Ziehen aus einer Urne: Formeln

- k Elemente aus einer n-elementigen Menge

	mit Zurücklegen	ohne Zurücklegen
geordnet (mit Reihenfolge)	n^k	$\frac{n!}{(n-k)!}$
ungeordnet (ohne Reihenfolge)	$\binom{k+n-1}{k}$	$\binom{n}{k}$

- *Urne mit n Kugeln, ziehe k Kugeln...*
- **Ohne** Zurücklegen, **Mit** Reihenfolge: $A_{n,k} := \{(s_1, ..., s_k) \in [n]^k | |\{s_1, ..., s_k\}| = k\}$
  - $|A_{n,k}| = \frac{n!}{(n-k)!}$
  - "*k-Tupel mit k verschiedenen Einträgen aus $[n]$*"
  - *Tupel ohne Duplikate*
- **Ohne** Zurücklegen, **Ohne** Reihenfolge: $B_{n,k} := \{(s_1, ..., s_k) \in [n]^k : s_1 < s_2 < ... < s_k\}$
  - $|B_{n,k}| = \binom{n}{k} = \frac{n!}{k!(n-k)!}$
  - "*Aufsteigend sortierte k-Tupel mit k verschiedenen Einträgen aus $[n]$*"
  - *eindeutige Menge*
- **Mit** Zurücklegen, **Ohne** Reihenfolge: $C_{n,k} := \{(s_1, ..., s_k) \in [n]^k : s_1 \leq s_2 \leq ... \leq s_k\}$
  - $|C_{n,k}| = \binom{n+k-1}{k}$
  - **(!)** $|C_{n,k}| = |D_{k,n}|$
  - "*Aufsteigend sortierte k-Tupel über $[n]$ mit Wiederholungen*"
  - *Multimenge*
- **Mit** Zurücklegen, **Mit** Reihenfolge: $\{(s_1, ..., s_k) \in [n]^k\}$
  - Anz. Möglichkeiten = n^k
  - *Tupel mit Duplikate*

Beispielsaufgaben: Ziehen aus einer Urne

- Wie viele mögliche Lottoziehungen gibt es (n Bälle, k Ziehungen)? $\rightarrow |B_{n,k}|$ (**ohne** Zurücklegen, **ohne** Reihenfolge)
- Ein Wettbewerb vergibt einen ersten, einen zweiten, ... und einen k-ten Preis. Wie viele Möglichkeiten gibt es, die Preise unter den n Wettbewerbsteilnehmer zu verteilen? $\rightarrow |A_{n,k}|$ (**ohne** Zurücklegen, **mit** Reihenfolge)
- Wie viele Möglichkeiten gibt es, k Fußballspiele auf n Austragungsorte zu verteilen? $\rightarrow n^k$ (**mit** Zurücklegen, **mit** Reihenfolge)
- Wie viele Möglichkeiten gibt es, k Euro unter n Personen zu verteilen? $\rightarrow |C_{n,k}|$ (**mit** Zurücklegen, **ohne** Reihenfolge)

Beispielsaufgaben: Möglichkeiten, Buchstaben umzuordnen

- Möglichkeiten, die Buchstaben in ABCDEFGH umzuordnen, so, dass ABC erhalten bleibt

    - gesamte Anzahl an Buchstaben: $8 \rightarrow$ Anz. Möglichkeiten, alle Buchstaben umzuordnen, ohne zu beachten, dass ABC erhalten bleibt = $8!$
    - betrachte ABC als 1 Einheit $\rightarrow$ 5 einzelne Buchstaben, 1 Paar ABC $\rightarrow$ Anz. Möglichkeiten, alle Buchstaben umzuordnen, ohne dass das Paar ABC verloren geht = $6! = 720$
- Anz. der erhaltenen Wörter aus Permutation von "hallo"
    - wenn man l_1 und l_2 als unterschiedliche Buchstaben betrachten würde: $5! = 120$ (Wortlänge)
    - jedes Wort würde $2!$ mal auftreten $\rightarrow$ gesuchter Wert = $5!/2! = 60$
- Anz. der erhaltenen Wörter aus Permutation von "bewundernswert"
    - selbes Prinzip $\rightarrow 14!/(3! * 2! * 2! * 2!) = 14!/48 = 1.816.214.400$

Stirling-Zahlen 2. Art

- **Definition**: **Anzahl Partitionen** von n Elementen ($[n]$) **in** k **nicht leere Klassen**
    - m.a.W. **Anzahl der Äquivalenzrelationen** über $[n]$ **mit genau** k **Klassen**
- **Notation**: $S_{n,k} = \left\{ {n \atop k} \right\}$
- **Formeln**:
    - *rekursiv*: $S_{n,k} = S_{n-1,k-1} + k * S_{n-1,k}$
        - *Base Cases*: $S_{n,0} = 0$, $S_{0,0} = 1$ und $S_{n,n} = 1$
    - *geschlossen*: $S_{n,k} = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n$

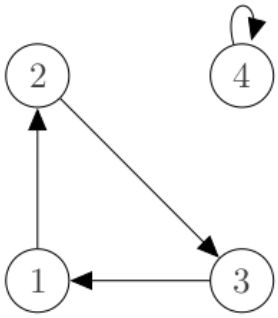
Anzahl Partitionen bei vorgegebener Klassengröße

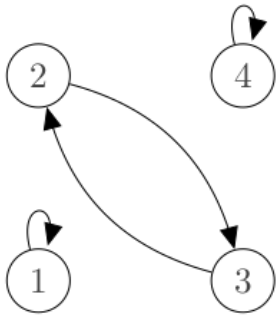
λ_1	λ_2	λ_3	Partitionen
0	0	1	$\{\{1,2,3\}\}$
1	1	0	$\{\{1\},\{2,3\}\}, \{\{2\},\{1,3\}\}, \{\{3\},\{1,2\}\}$
3	0	0	$\{\{1\},\{2\},\{3\}\}$

- es gilt $\sum_{i=1}^{n} i * \lambda_i = n$
    - z.B. $1 * 3 = 1 * 1 + 2 * 1 = 3 * 1$
- **Anzahl der Partitionen von** $[n]$ **mit** λ_i **vielen** i**-elementigen Klassen** = $\frac{n!}{(1!)^{\lambda_1} * \ldots * (n!)^{\lambda_n} * \lambda_1! * \ldots * \lambda_n!}$

Stirling-Zahlen 1. Art

- **Zykelschreibweise**: die einzelnen Tupel beschreiben die Kreise im Graph

$f = (1\,2\,3)\,(4) =$ 

$g = (1)\,(2\,3)\,(4) =$ 

- **Definition**: **Anzahl Permutationen** von n Elementen ($[n]$) **mit genau k Zyklen**
- **Notation**: $s_{n,k} = \begin{bmatrix} n \\ k \end{bmatrix}$
- **Formel**: $s_{n,k} = s_{n-1,k-1} + (n-1) * s_{n-1,k}$
  - *Base Cases*: $s_{n,0} = 0$, $s_{0,0} = 1$ und $s_{n,n} = 1$

Zählvektoren

- $|D_{n,k}| = |C_{k,n}| := |\{(s_1, ..., s_k) \in \mathbb{N}_0^k | s_1 + ... + s_k = n\}| = \binom{n+k-1}{n} = \binom{n+k-1}{k-1}$
  - "*Zählvektoren mit k Einträgen und Summe genau n*"
  - *Eselsbrücke*: entspricht der Menge der *Wörter*, die "*n Strichen und $k-1$ Kommata haben*"
- $|E_{n,k}| = |D_{n,k+1}| :=:= |\{(s_1, ..., s_k) \in \mathbb{N}_0^k | s_1 + ... + s_k \leq n\}| = \binom{n+k}{n}$
  - "*Zählvektoren mit k Einträgen und Summe höchstens n*"
- $|F_{n,k}| := |\{(s_1, ..., s_k) \in [n]^k || \{s_1, ..., s_k\}| = n\}|$ (*n - Anzahl der Klassen, k - Anzahl der Objekte*)
  - *rekursiv*: $|F_{n,k}| = n! * S_{k,n}$
  - *geschlossen*: $|F_{n,k}| = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^k$
- $|G_{n,k}| := |\{(s_1, ..., s_k) \in \mathbb{N}^k | s_1 + ... + s_k = n\}| = \binom{n-1}{k-1}$
  - "*sortierte Zählvektoren mit k Komponenten und Summe genau n*"
  - *Eselsbrücke*: entspricht der Anzahl der Möglichkeiten, $k-1$ Pluszeichen aus insgesamt $n-1$ Pluszeichen zu wählen
  - ***geordnete** Zahlpartition*
- $|P_{n,k}| := |\{(s_1, ..., s_k) \in \mathbb{N}^k | s_1 + ... + s_k = n, s_1 \leq ... \leq s_k\}|$ (*Partitionen von n*)
  - $|P_{n,k}| = |P_{n-1,k-1}| + |P_{n-k,k}|$ für $k > 0$
  - $|P_{n,0}| = 0$ für $n > 0$
  - $|P_{n,k}| = 0$ für $k > n$
  - $|P_{0,0}| = 1$
  - $|P_{n,n}| = 1$
- $|H_{n,k}| := |\{(s_1, ..., s_k) \in \mathbb{N}_0^k | s_1 + ... + s_k = n, s_1 \leq ... \leq s_k\}| = |P_{n+k,k}|$

- *Anzahl der Zahlpartitionen von n in k positive Summanden*
- ***ungeordnete** Zahlpartition*

Beispielsaufgaben: Verteilungsprobleme

- Wie viele Möglichkeiten gibt es, k Weihnachtsgeschenke unter n Kindern zu verteilen, so dass jedes Kind mindestens ein Geschenk erhält?
  - Sowohl die Kinder als auch die Geschenke sind **unterscheidbar**! $\rightarrow |F_{n,k}|$ (***geordnete** Partition von $[n]$ in k Klassen*)
- Wie viele Möglichkeiten gibt es, k Weihnachtsgeschenke in n Päckchen aufzuteilen, so dass jedes Päckchen mindestens ein Geschenk enthält?
  - Die Päckchen sind **nicht unterscheidbar**, die Geschenke sind **unterscheidbar** $\rightarrow S_{n,k}$ (***ungeordnete** Partition von $[n]$ in k Klassen*)
- Wie viele Möglichkeiten gibt es, n Euromünzen unter k Kindern zu verteilen, so dass jedes Kind mindestens eine Münze erhält?
  - Die Münzen sich **nicht unterscheidbar**, die Kinder sind **unterscheidbar** $\rightarrow |G_{n,k}|$
- Wie viele Möglichkeiten gibt es, n Euromünzen in k Päckchen aufzuteilen, so dass jedes Päckchen mindestens eine Münze enthält?
  - Sowohl die Münzen, als auch die Päckchen sind **nicht unterscheidbar**! $\rightarrow |P_{n,k}|$
- Wie viele Möglichkeiten gibt es, n Euro in k Päckchen aufzuteilen, wenn Päckchen auch 0 Euro enthalten dürfen? $\rightarrow |H_{n,k}| = |P_{n+k,k}|$

Binomialkoeffizient, Binomialformel und Vandermondesche Identität

- **Binomialkoeffizient**: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$: Anzahl der k-Elementigen Teilmengen einer n-Elementigen Menge
- **Binomialformel**: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$
- **Vandermondische Identität**: $\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$

Rechenregel für Binomialkoeffizienten

- **Pascalsche Identität**: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
- **Symmetrie**: $\binom{n}{k} = \binom{n}{n-k}$
- **Zeilensumme**: $\sum_{i=0}^{n} \binom{n}{i} = 2^n$
- **Spaltensumme**:$\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1}$
- **Diagonalsumme**: $\sum_{i=0}^{n} \binom{n+i}{i} = \binom{n+k+1}{k}$

Algebra und Gruppentheorie

Teilbarkeit und Primfaktorzerlegung

- **Teilbarkeitsrelation** (*a ist Teiler von b*)
  - $a|b \leftrightarrow \frac{b}{a} \in \mathbb{Z}$ (a **teilt** b **ohne Rest**)
- **Primzahlen** (*alle Zahlen, deren Teiler nur 1 und sich selbst sind*)
  - $\mathbb{P} = \{p \in \mathbb{N} | p > 1 \wedge \forall n \in \mathbb{N} : n|p \rightarrow (n = 1 \vee n = p)\}$
  - jedes p größer als 1 und wenn n Teiler von p ist, dann, dann ist n entweder 1 oder p

GGT und KGV

- **ggT(a, b)**:
  - $\prod_{p \in \mathbb{P}} p^{min\{v_p(a), v_p(b)\}}$
  - **Produkt jedes Primfaktors** der beiden Zahlen mit dem jeweiligen **minimalen Exponenten** (*impl. 0 wenn nicht vorhanden in einem der beiden Zerlegungen*)
- **kgV(a, b)**:
  - $\prod_{p \in \mathbb{P}} p^{max\{v_p(a), v_p(b)\}}$
  - **Produkt jedes Primfaktors** der beiden Zahlen mit dem jeweiligen**maximalen Exponenten**
- $a * b = ggT(a, b) * kgV(a, b)$

Modulorechnung

- $a \mod N = a - \lfloor \frac{a}{N} \rfloor * N \in \mathbb{Z}_N$, mit $\mathbb{Z}_N := \{0, ..., N - 1\}$
- Wichtige Gruppen (*allgemein*):
  - $\mathbb{Z}_N := \{0, ..., N - 1\}$ (*alle möglichen Ergebnisse modulo N*)
  - $\mathbb{Z}_N^* := \{1..., N - 1\}$ (*teilerfremde Ergebnisse modulo N*)
  - $[N] := \{1, ..., N\}$ (*Menge aller natürlichen Zahlen von 1 bis N inkl.*)

Restklassen und Kongruenzen

- **Restklasse** $[a]_m$ von $a \mod m$: Menge (*Äquivalenzklasse*) aller Zahlen, die bei **Division** durch m ($m \in \mathbb{Z} \wedge m \neq 0$) **denselben Rest** lassen wie a
  - $[a]_m = a + m\mathbb{Z}$
  - $(a \mod m) = (k \mod m)$ für ein beliebiges $k \in Z$
- **Kongruenz modulo m** $\equiv_m$: Zwei Zahlen a und b sind **kongruent** modulo m, wenn sie bei der **Division** durch m **beide denselben Rest** haben
  - beide Zahlen unterscheiden sich um ein **ganzzahliges Vielfaches** von m
  - *alt. Schreibweise*: $a \equiv b \mod m$

Erweiterter Euklidischer Algorithmus (EEA)

- **Verfahren**:

    - **von oben nach unten**: bestimme $\lfloor b/a \rfloor$, trage Wert von a in unteren Zeile für b und den Rest $b \mod a$ für a ein
        - wiederhole so lange, bis $b \mod a = 0$
    - **von unten nach oben**: setze $\alpha = 1$ und $b = 0$, dann trage Wert von α_{alt} in der oberen Zeile für β und $\beta_{alt} - \lfloor b/a \rfloor_{current} * \alpha_{alt}$ für α ein
        - wiederhole bis zur obersten Zeile
- **multiplikatives Inverse** von a in $\langle Z_n^*, \cdot_n, 1 \rangle$: $\alpha \mod n$
- **Test auf ggT**: $ggT(a, b) = a * \alpha + b * \beta$
    - *Beispiel*: $a = 5, b = 911$

a	b	$\lfloor b/a \rfloor$	α	β	
5	911	182	-182	1	$-182 = 0 - 182 \cdot 1$
911 − 5·182 = 1	5	–	1	0	

ggT(5, 911)

Teilerfremde Reste modulo N und Primzahltest

- **Teilerfremde Reste modulo** N: $\mathbb{Z}_N^* := \{k \in \mathbb{Z}_N | ggT(k, N) = 1\}$
    - **Menge** aller Zahlen aus $\mathbb{Z}_N$, deren **größten gemeinsamen Teiler** mit N **1** ist / **teilerfremd** zu N sind
    - *Beispiel*: $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$
- **Eulerische Phi-Funktion**: $\varphi(N) := |\mathbb{Z}_N^*| = N * \prod_{p \in \mathbb{P}: p|N} (1 - p^{-1})$
    - **Kardinalität der Menge der teilerfremden Reste** einer Zahl modulo N
        - berechnet, indem man N mit $1 - 1/p$ für jeden **einzelnen** Primfaktor multipliziert
    - **(!)** $\varphi(p) := p - 1$ für $p \in \mathbb{P}$ (*alle Zahlen von 1 bis* $p - 1$)
    - **(!)** $\varphi(m * n) = \varphi(m) * \varphi(n)$ für $ggT(m, n) = 1$
        - *gilt auch für mehr als zwei Faktoren, dann* $ggT(a, b, c, ...) = 1$
    - *Beispiel*: $\varphi(15) = 15 * (1 - \frac{1}{5}) * (1 - \frac{1}{3}) = (5 - 1)(3 - 1) = 8$
- **Primzahltest**: $a^{p-1} \equiv 1 \mod p$
    - für $N > 2$, wähle $1 \leq a < N$ und prüfe:
        - wenn $a^{N-1} \equiv 1 \mod N$, kann N eine Primzahl sein (*oder auch nicht, siehe Carmichael-Zahlen*)
        - wenn **nicht** $a^{N-1} \equiv 1 \mod N$, ist N definitiv **keine** Primzahl

Modulorechnung

- **Rechenregeln**:

- $(a+b) \mod n = ((a \mod n) + (b \mod n)) \mod n$
- $(a \cdot b) \mod n = ((a \mod n) \cdot (b \mod n)) \mod n$
- $(a \mod n) \mod n = a \mod n$

Gruppen

Allgemeine Definition

- eine Menge G mit **innerer Verknüpfung** $G \times G \to G$ heißt **Gruppe**, falls folgendes gilt:
  1. *Abgeschlossenheit*: $G \times G \to G$
  2. *Assoziativität*: $\forall\, a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$
  3. *neutrales Element*: $\exists\, e \in G : e \circ a = a = a \circ e$ (*eindeutig!*)
  4. *Inverses*: $\forall\, a \in G\ \exists\, b \in G : a \circ b = e = b \circ a$ mit $b = a^{-1}$ (*eindeutig!*)
- eine Gruppe heißt **abelsch**, wenn diese **kommutativ** ist ($\forall a, b \in G : a + b = b + a$)
- **(!) Eigenschaften einer Gruppe** $\mathbb{G} = \langle \mathbb{G}, \cdot, 1 \rangle$:
  - das **Neutrale** ist **eindeutig**
  - das **Inverse** ist **eindeutig**
  - $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$
  - **Kürzungsregel**: Falls $ab = ac$ oder $ba = ca$, dann $b = c$
  - $b = c$ **gdw.** $ab = ac$ für ein beliebiges $a \in \mathbb{G}$
  - $b \neq c$ **gdw.** $ab \neq ac$ für ein beliebiges $a \in \mathbb{G}$

Ordnung eines Elements

- *es gilt hier* $\mathbb{G} = \langle \mathbb{G}, \cdot, 1 \rangle$
- **Ordnung eines Elements**: kleinste Zahl $k \in \mathbb{N}$, so dass a^k das neutrale Element als Ergebnis hat ($a \in \mathbb{G}$)
  - $ord(a) := min\{k \in \mathbb{N} | a^k = 1\}$
    - $min\emptyset := \infty$
    - *(*) für additive Gruppen*: $ord(a) := min\{k \in \mathbb{N} \mid ka = 0\}$
  - **(!)** $ord(a) = ord(a^{-1})$
  - **(!)** $ord(a)$ **muss** Teiler von $|\mathbb{G}|$ sein
- **Erzeugnis von** a: $\langle a \rangle := \{a^k | k \in \mathbb{Z}\} = \{...(a^{-1})^2, (a^{-1})^1, 1, a^1, a^2, ...\}$
  - *(*) für additive Gruppen*: $\langle a \rangle := \{ka \mid k \in \mathbb{Z}\}$
  - **(!)** $\langle a \rangle = \langle a^{-1} \rangle$
  - **(!)** $ord(a) = |\langle a \rangle|$
- **Erzeuger von** $\mathbb{G}$: a ist ein Erzeuger von $\mathbb{G}$, wenn $\langle a \rangle = \mathbb{G}$

- **(!)** *um ein Element mit Ordnung d zu finden*: wenn g ein Erzeuger von $\mathbb{G}$ ist (daraus $ord(g) = |\mathbb{G}|$), dann gilt für jeden Teiler $d \mid ord(g)$, dass $g^{ord(g)/d}$ Ordnung d hat

- **Gruppenexponent von** $\mathbb{G}$: $\lambda_{\mathbb{G}} = kgV(\{ord(a) \mid a \in \mathbb{G}\})$
  - $\lambda_{\mathbb{G}}$ teilt $\mathbb{G}$ ohne Rest

- **(!) Eigenschaften**:
  - $a^{ord(a)} = 1$
  - $a^{-1} = a^{ord(a)-1}$
  - $a^k = a^{k \mod ord(a)}$ für jedes $k \in \mathbb{Z}$
  - $a^k = a^{k \mod |\mathbb{G}|}$ für jedes $k \in \mathbb{Z}$
  - $a^k = a^{k \mod \lambda_{\mathbb{G}}}$ für jedes $k \in \mathbb{Z}$
  - $\langle a \rangle = \{1, a, a^2, ..., a^{ord(a)-1}\}$
  - $|\langle a \rangle| = ord(a)$
  - $a^k = a^{k \mod ord(a)} = 1$ **gdw.** $k \mod ord(a) = 0$ **gdw.** $ord(a) \mid k$
  - $a^{|\mathbb{G}|} = 1$ **für alle** $a \in \mathbb{G}$, also $|\mathbb{G}| \mod ord(a) = 0$
  - $a^{\lambda_{\mathbb{G}}} = 1$ **für alle** $a \in \mathbb{G}$

- **(!) Satz von Euler**:
  - Sei $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$, dann gilt $1 = a^{|\mathbb{Z}_n^*|} = a^{\varphi(n)}$
  - *alternativ*: $a^{\varphi(n)} \equiv_n 1$, falls $ggT(a, n) = 1$

- **(!) Kleiner Fermatscher Satz**:
  - Sei $\langle \mathbb{Z}_p^*, \cdot_p, 1 \rangle$ für $p \in \mathbb{P}$, dann gilt $1 = a^{|\mathbb{Z}_p^*|} = a^{\varphi(p)} = a^{p-1}$
  - *alternativ*: $a^{p-1} \equiv_p 1$, falls $ggT(a, p) = 1$

Veranschaulichung der Ordnung

- $G_{r_a} = (\mathbb{G}, \{(x, xa) | x \in \mathbb{G}\})$
- $x\ \langle a \rangle$: Kreis in G_{r_a}, der x enthält
- **(!) Eigenschaften**:
  - *Länge des Kreises*: $ord(a)$
    - jeder Kreis hat die **gleiche Länge**
  - *Anzahl der Kreisen*: $|\mathbb{G}|\ /\ ord(a)$
- **(?) Allgemeine Regel**: für alle $k \geq 3$ gilt...
  - ...$\mathbb{Z}_{2^k}^*$ (*teilerfremde Gruppe einer Zweierpotenz*) ist **nie zyklisch**, wird aber **stets durch 2 Elemente** erzeugt, wobei eines die **Ordnung** 2^{k-2}, das andere die **Ordnung 2** hat
  - ...der **Gruppenexponent** λ von $\mathbb{Z}_{2^k}^*$ ist stets 2^{k-2}

        - z.B: für $\mathbb{Z}_{16}^*$ sind die Erzeuger beispielsweise 3 und 7 ($ord(3) = 4$, $ord(7) = 2$) und der Gruppenexponent ist 4
    - $\mathbb{Z}_2^*$ und $\mathbb{Z}_4^*$ sind **zyklisch**

Untergruppen

- **Untergruppe** H: nicht leere **Teilmenge** von $\mathbb{G}$, die bezüglich der Operation $\cdot$ selbst eine **Gruppe** definiert
- **Bezeichnung**: $H \leq \mathbb{G}$
- **(!) Eigenschaften**:
    - H erbt das Neutrale und die Inversen von $\mathbb{G}$
    - $H \leq \mathbb{G}$ gdw. $\forall a, b \in H : ab^{-1} \in H$
- **(!) Satz von Lagrange**: $|H|$ ist stets ein **Teiler** von $|\mathbb{G}|$ für $H \leq \mathbb{G}$

Symmetrische Gruppen

- jedes **Tupel** beschreibt einen **Kreis** in $G_f = ([n], f)$
    - Zykel können beliebig angeordnet werden, Fixpunkte (*Kreise bzw. Tupel der Länge 1*) müssen nicht angegeben werden: $(2)(1,3,5)(4) = (3,5,1)(4)(2) = (5,1,3)$
    - *Beispiel*: Für $\pi = [5] \to [5]$ in $\langle S_5, \circ, Id_{[5]} \rangle$ mit $\pi(1) = 2, \pi(2) = 4, \pi(3) = 5, \pi(4) = 1, \pi(5) = 3$ folgt $\pi = (1,2,4)(3,5)$
- $l_a(x) = ax$ und $r_a(x) = xa$ sind **Permutationen auf** x
- **(!) Eigenschaften**:
    - $|S_n| = n!$
    - $ord(\pi)$ = kgV der **Zykellängen**
        - *Beispiel (oberes)*: $ord(\pi) = kgV(\{3,2\}) = 6$
    - λ_S = kgV **aller** möglichen Zykellängen
        - *Beispiel für* S_5^*: $\lambda = kgV(\{1,2,3,4,5\}) = 60$
    - **Inverse eines Zyklus**: Zyklus umdrehen ($(1,2,3)^{-1} = (3,2,1)$)

Zyklische Gruppen

- **Zyklische Gruppen**: Gruppen, die von einem einzigen Element a erzeugt werden
    - $\langle a \rangle = \mathbb{G}$
    - a: **Generator** von $\mathbb{G}$
    - jede zyklische Gruppe ist **kommutativ** ($a^k \cdot a^l = a^{k+l} = a^l \cdot a^k$)
- **(!) Eigenschaften**:
    - a ist ein **Erzeuger** von $\mathbb{G}$ gdw. $a^{|\mathbb{G}|/p} \neq 1$ für **jeden Primfaktor** p von $|\mathbb{G}|$

- jede Gruppe mit $|\mathbb{G}| \in \mathbb{P}$ ist **zyklisch**
- jede **Untergruppe** $H \leq \mathbb{G}$ einer zyklischen Gruppe ist **zyklisch**
- $\lambda = |\mathbb{G}|$

~ The End!