Theoretische Informatik

Mathematische Grundlagen

Patrick Horster
Universität Klagenfurt
Informatik – Systemsicherheit

Allgemeines

- In diesem einführenden Kapitel werden zunächst elementare Grundlagen kurz aufgezeigt, die als bekannt vorausgesetzt werden oder leicht einzusehen sind (evtl. Nacharbeiten).
- Sie dienen im Wesentlichen zum Verständnis und zur Vereinheitlichung der Schreibweise, um eine gemeinsame Basis für die Vorlesung „Theoretische Informatik“ zu legen.
- Diese Einführung erhebt keinen Anspruch auf Vollständigkeit. Zudem dient sie nicht als Ersatz für die in den Vorlesungen eingeführten Notationen.
- Obwohl wir bemüht sind, keine Fehler zu machen, freuen wir uns über jede Fehlermeldung. Erforderliche Korrekturen werden unmittelbar eingearbeitet, die aktualisierten Unterlagen stehen Ihnen dann zeitnahe in der gewohnten Form zur Verfügung.

Inhalt

- Mengen
- Relationen und Funktionen
- Relationen und ihre Darstellungen
- Abschlusseigenschaften
- Endliche und unendliche Mengen
- Elementare Beweistechniken

Mengen 1

- Eine Menge ist eine Sammlung von Objekten.
- Die vier Buchstaben a, b, c und d bestimmen eine Menge L, L = {a, b, c, d}.
- Die Objekte heißen Elemente, b ist ein Element von L, e ist kein Element von L. Schreibweise: $b \in L$, $e \notin L$.
- Wiederholungen sind nicht relevant: {a, b, c, d, a, b} = {a, b, c, d}.
- Reihenfolge ist ohne Bedeutung: {a, b, c, d} = {a, c, d, b}.
- |M| bezeichnet die Kardinalität der Menge M, |L| = 4.
- Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente enthalten.
- Elemente einer Menge haben i.A. keine Beziehung zueinander.
- {1, rot, {c, gelb}} ist eine Menge mit drei Elementen: 1, rot und der Menge {c, gelb}.
- Mengen können auch nur ein Element besitzen (unäre Mengen): {I} ist die Menge, die nur das Element I besitzt.

Mengen 2

- Die Menge ohne Elemente heißt leere Menge, die mit $\varnothing$ bezeichnet wird; $|\varnothing| = 0$.
- Es gibt nur eine leere Menge, jede andere Menge heißt nichtleer.
- Endliche Mengen können in der Form {Aufzählung der Elemente} dargestellt werden (prinzipiell); bei unendlichen Mengen ist dies unmöglich!
- Trotzdem bezeichnen
  - $\mathbb{N} := \{0, 1, 2, 3, ...\}$ die Menge der natürlichen Zahlen und
  - $\mathbb{Z} := \{... , -3, -2, -1, 0, 1, 2, 3, ...\}$ die Menge der ganzen Zahlen.
- Mengen können aber auch mit Bezug zu anderen Mengen und Beschreibungen der Eigenschaften angegeben werden:
  $B := \{x \mid x \in A, x \text{ hat Eigenschaft } P\}$.
  Dabei ist A i.d.R. eine bereits definierte Menge und P eine wohldefinierte Eigenschaft.

Mengen 3

- Beispiele:
  - $2\mathbb{N} := \{n \mid n \in \mathbb{N}, n \text{ ist durch 2 teilbar}\} = \{0, 2, 4, 6, ...\}$,
    Menge der geraden natürlichen Zahlen.
  - $2\mathbb{N}+1 := \{n \mid n \in \mathbb{N}, n-1 \text{ ist durch 2 teilbar}\} = \{1, 3, 5, 7, ...\}$,
    Menge der ungeraden natürlichen Zahlen.
  - $\mathbb{P} := \{p \mid p \in \mathbb{N}, p \text{ besitzt genau zwei Teiler aus } \mathbb{N} \text{ (1 und p)}\}$,
    Menge der Primzahlen.
- Eine Menge A ist Teilmenge einer Menge B, falls für alle $x \in A$ gilt $x \in B$. Schreibweise: $A \subseteq B$
- Beispiele: $2\mathbb{N} \subseteq \mathbb{N}$, $2\mathbb{N}+1 \subseteq \mathbb{N}$
- Ist A eine Teilmenge von B, aber $A \neq B$, so ist A eine echte Teilmenge von B. Schreibweise: $A \subset B$
- Beispiel: $\{2, 3, 5, 7, 11, 13\} \subset \mathbb{P}$
- Für jede Menge A gilt $\varnothing \subseteq A$, da jedes Element aus $\varnothing$ (es gibt keines) auch Element aus A ist.

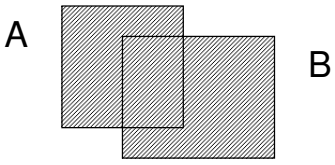
Mengen 4

- Um zu zeigen, dass zwei Mengen A und B gleich sind, reicht es zu zeigen, dass sowohl $A \subseteq B$ als auch $B \subseteq A$. Dazu reicht es zu zeigen, dass für ein beliebiges $a \in A$ auch $a \in B$ und für ein beliebiges $b \in B$ auch $b \in A$ ist.
- Sind zwei Mengen A und B gegeben, so können durch Mengenoperationen neue Mengen gebildet werden:

- Vereinigung:

  $A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$

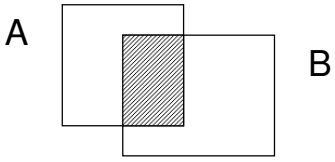
  $\{1,3,5\} \cup \{3,5,7\} = \{1,3,5,7\}$



- Durchschnitt:

  $A \cap B := \{x \mid x \in A \text{ und } x \in B\}$

  $\{1,3,5\} \cap \{3,5,7\} = \{3,5\}$

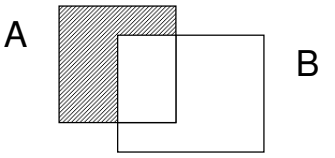


Mengen 5

- Differenz:

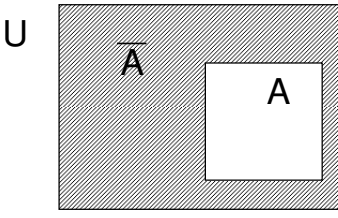
  $A - B := \{x \mid x \in A \text{ und } x \notin B\}$

  $\{1,3,5\} - \{3,5,7\} = \{1\}$



- Komplement:

  Ist $A \subseteq U$, so heißt $\overline{A} := U - A$
  das Komplement von A bzgl. U.



- Beim Komplement wird auf die übergeordnete Menge U häufig kein (besonderer) Bezug genommen.
- Sprechweise: Universum U.

Mengen 6

Sind A, B und C Mengen, dann gelten die folgenden Regeln:

- Idempotenz:
  $A \cup A = A$
  $A \cap A = A$
- Assoziativität:
  $(A \cup B) \cup C = A \cup (B \cup C)$
  $(A \cap B) \cap C = A \cap (B \cap C)$
- Distributivität:
  $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
  $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
- Regeln von DeMorgan:
  $A - (B \cup C) = (A - B) \cap (A - C)$
  $A - (B \cap C) = (A - B) \cup (A - C)$
- Kommutativität:
  $A \cup B = B \cup A$
  $A \cap B = B \cap A$
- Absorption:
  $A \cap (A \cup B) = A$
  $A \cup (A \cap B) = A$

Mengen 7

- Ist A das zu B und C gehörende Universum, so schreiben wir (ohne Bezug zu A, falls dieser aus dem Kontext ersichtlich ist):
  $\overline{B \cup C} = \overline{B} \cap \overline{C}$
  $\overline{B \cap C} = \overline{B} \cup \overline{C}$
  Übung: Beweisen Sie die Korrektheit der Regeln von DeMorgan.
- Zwei Mengen A und B heißen disjunkt, falls sie keine gemeinsamen Elemente besitzen, damit gilt dann $A \cap B = \emptyset$.
- Durchschnitt und Vereinigung können auch für mehr als zwei Mengen festgelegt werden. Ist S eine Sammlung von Mengen, so schreiben wir US (für die Vereinigung der Mengen in S).
  $S = \{\{a, b\}, \{b, c\}, \{c, d\}\} \Rightarrow US = \{a, b\} \cup \{b, c\} \cup \{c, d\} = \{a, b, c, d\}$
  $S = \{\{n\} \mid n \in \mathbb{N}\} \Rightarrow US = \mathbb{N}$
- Allgemein gilt: $US = \{x \mid x \in T \text{ für (wenigstens) eine Menge } T \in S\}$
- Entsprechendes gilt für ∩S: $\cap S = \{x \mid x \in T \text{ für jede Menge } T \in S\}$

Mengen 8

- Die Menge aller Teilmengen einer Menge A heißt Potenzmenge von A. Schreibweisen: 2^A oder $\mathcal{P}(A)$.
- Die Potenzmenge von {c, d} besteht aus {c, d}, {c}, {d} und $\emptyset$, somit gilt $2^{\{c,\,d\}} = \{\emptyset,\{c\},\{d\},\{c,\,d\}\}$.
- Eine Partition Π (Zerlegung) einer nichtleeren Menge A ist eine Teilmenge von 2^A, so dass $\emptyset \notin \Pi$ und jedes Element aus A in genau einer Menge von Π liegt.
- Formale Darstellung:

  $\Pi \subseteq 2^A$ heißt Partition von A : $\Leftrightarrow$ (1) $\wedge$ (2)

  (1) $\emptyset \notin \Pi$

  (2) $(\forall\, a \in A)\ (\exists_1\, T \in \Pi)\ a \in T$
- Bemerkung:
  Der Allquantor $\forall$ (für alle) und der Existenzquantor $\exists$ (es existiert wenigstens ein) sollten bekannt sein. Durch die Bezeichnung $\exists_1$ legen wir die Eindeutigkeit fest (es existiert genau ein).

Mengen 9

- Π ist eine Partition von A, falls Π eine Menge von Teilmengen von A ($\Pi \subseteq \mathcal{P}(A)$) mit den folgenden drei Eigenschaften ist:
  1. $M \in \Pi \Rightarrow M \neq \emptyset$
  2. $M_1, M_2 \in \Pi, M_1 \neq M_2 \Rightarrow M_1 \cap M_2 = \emptyset$
  3. $U\Pi = A$
- Beispiele:
  - {{a, b},{c},{d}} ist eine Partition von {a, b, c, d},
  - {2$\mathbb{N}$, 2$\mathbb{N}$+1} ist eine Partition von $\mathbb{N}$.
  - {2$\mathbb{N}$, 2$\mathbb{N}$+1, $\mathbb{P}$} und {2$\mathbb{N}$, $\mathbb{P}$} sind keine Partitionen von $\mathbb{N}$.
- Hinweis:
  Hinterfragen Sie die Beziehungen, insbesondere solche, die unklar erscheinen. Betrachten Sie geeignete Beispiele und machen Sie sich mit der schriftlichen Anwendung vertraut. Schriftliche Übungen sind dazu ein geeignetes Hilfsmittel.

Relationen und Funktionen 1

- Die Mengen {2, 3} und {3, 2} sind ununterscheidbar. Wird die Reihenfolge berücksichtigt, so resultieren geordnete Paare (a, b).
  - $a \neq b \Rightarrow (a, b) \neq (b, a)$
  - $(a, b) = (c, d) \Rightarrow a = c$ und $b = d$
- $A \times B := \{(a, b) \mid a \in A, b \in B\}$ heißt kartesisches Produkt.
  - $\{1, 2, 3\} \times \{a, b\} = \{(1,a), (1,b), (2,a), (2,b), (3,a), (3,b)\}$
- Eine Teilmenge ρ von $A \times B$ heißt binäre Relation über A und B.
  - $\{(1,a), (2,b), (3,a)\}$ ist eine binäre Relation über $\{1, 2, 3\} \times \{a, b\}$.
  - $\{(i, j) \mid i, j \in \mathbb{N}, i < j\}$ ist die „kleiner Relation“ auf $\mathbb{N}$.
- Allgemein:
  Sind $a_1, ..., a_n$ ($n \in \mathbb{N}$) beliebige (nicht notwendig verschiedene) Objekte, dann heißt $(a_1, ..., a_n)$ geordnetes n-Tupel.
  a_i, $i \in [1:n] = \{1, 2, ..., n\}$, heißt i-te Komponente.
  $(b_1, ..., b_m) = (a_1, ..., a_n) \Leftrightarrow$ ($m = n$ und $a_i = b_i$ für $i \in [1:n]$)

Relationen und Funktionen 2

- (a,a), (a,a,a), (a,(a,a)), ((a,a),a) sind paarweise verschieden.
- Sind $A_1, ..., A_n$ Mengen, dann bezeichnet $A_1 \times \cdots \times A_n$ die Menge aller geordneten n-Tupel $(a_1, ..., a_n)$, $a_i \in A_i$.
- Sind alle A_i gleich A, so schreiben wir statt $A \times \cdots \times A$ auch A^n.
  $A^0 := \varnothing$, $A^* := \bigcup_{i=0}^{\infty} A^i$, $A^+ := \bigcup_{i=1}^{\infty} A^i$
- $\mathbb{N}^2$ bezeichnet die Menge aller geordneten Paare natürlicher Zahlen.
- Eine n-näre Relation über Mengen $A_1, ..., A_n$ ist eine Teilmenge von $A_1 \times \cdots \times A_n$.
- Verzichten wir auf die Klammerbildung, so schreiben wir anstelle von $A \times B$ (kontextabhängig) auch AB.
- Beispiel: $A = \{a\}$, $B = \{c, d\}$
  $AB = \{ac, ad\}$, $A^+ = \{a, aa, aaa, ...\}$,
  $B^+ = \{c, d, cc, cd, dc, dd, ccc, \ldots\}$

Relationen und Funktionen 3

- Es seien A und B Mengen, $\rho \subseteq A \times B$ (eine Relation).
  - Def(ρ) := {a ∈ A | (∃ b ∈ B) (a, b) ∈ ρ} heißt Definitionsbereich von ρ.
  - Bild(ρ) := {b ∈ B | (∃ a ∈ A) (a, b) ∈ ρ} heißt Bildbereich von ρ.
  - Schreibweise: a ρ b ⇔ (a, b) ∈ ρ
- f := (A, B, ρ) heißt Korrespondenz, wobei
  - A der Vorbereich von f, (Argumentbereich, Definitionsbereich)
  - B der Bildbereich von f, (Wertebereich, Nachbereich)
  - Def(f) = Def(ρ) und
  - Bild(f) = Bild(ρ) ist.
- f heißt partielle Funktion :⇔ ρ ist rechtseindeutig
  Schreibweise: f: A ⇢ B (f muss nicht für alle a ∈ A definiert sein)
- f heißt totale Funktion :⇔ (ρ rechtseindeutig und Def(f) = A)
  Statt totale Funktion wird oft auch (einfach) Funktion gesagt.
  Schreibweise: f: A ⟶ B (f ist für alle a ∈ A definiert)
- Die Begriffe Funktion und Abbildung werden synonym verwendet.

Relationen und Funktionen 4

- Beispiele:
  - S := {s | s ist Stadt in Österreich}
  - L := {*l* | *l* ist Bundesland in Österreich}
  - R_1 := {(x, y) | x ∈ S, y ∈ L, x ist Stadt in y}
  - R_2 := {(x, y) | x ∈ L, y ∈ S, y ist Stadt in x}
  - R_3 := {(x, y) | x ∈ S, y ∈ L, x ist Hauptstadt von y}

  - f = (S,L,R_1) ist eine Funktion, da jede Stadt (Postleitzahl unterscheidet gleiche Namen) in genau einem Bundesland liegt.
  - (L,S,R_2) ist keine Funktion, da in einem Bundesland i.d.R. mehrerer Städte liegen.
  - g = (S,L,R_3) ist eine partielle Funktion.
    Def(g) = {h | h ist Hauptstadt in einem Bundesland}.

Relationen und Funktionen 5

- Sei f = (A, B, ρ) eine partielle Funktion, dann ist für a $\in$ A möglicherweise der Wert f(a) nicht definiert.
  Daher treffen wir die folgende Vereinbarung:

$$f(a) := \begin{cases} b \in B, \text{ falls } a \in \text{Def}(f) \text{ und } a \rho b \\ \text{nicht definiert, sonst} \end{cases}$$

- Oft wird für „nicht definiert“ ein neues Objekt eingeführt:
  - Bezeichnung: „$\perp$“ oder „div“ oder „$\uparrow$“.
  - Es ergibt sich (die kanonische Erweiterung):
    $f : A \cup \{\perp\} \rightarrow B \cup \{\perp\}$
- Ist f: A $\rightarrow$ B und A' $\subseteq$ A, dann bezeichnet f(A') := {f(a) | a $\in$ A'} das Bild (Menge von Funktionswerten) von A' unter f.
  Mit A = {-2,-1,0,1,2,3} und f(x) := x^2 erhalten wir f(A) = {0,1,4,9}.

Relationen und Funktionen 6

- Spezielle Funktionen sind von besonderem Interesse:
  - f : A $\rightarrow$ B heißt injektiv (one-to-one),
    falls für alle a, a' $\in$ A mit a $\neq$ a' gilt: f(a) $\neq$ f(a').
    g: L $\rightarrow$ S, g(x) = Hauptstadt von x ist injektiv.
  - f : A $\rightarrow$ B heißt surjektiv (onto),
    falls für alle b $\in$ B (wenigstens) ein a $\in$ A mit f(a) = b existiert.
    g ist nicht surjektiv (nicht jede Stadt ist Hauptstadt).
  - f : A $\rightarrow$ B heißt bijektiv $\Leftrightarrow$ f ist injektiv und surjektiv.
    Ist H := S die Menge der Hauptstädte, dann ist g: L $\rightarrow$ H bijektiv.
- Zu jeder binären Relation R $\subseteq$ A $\times$ B existiert eine inverse Relation $R^{-1} \subseteq B \times A$, definiert durch (b, a) $\in R^{-1}$:$\Leftrightarrow$ (a, b) $\in$ R.
- R_1 und R_2 sind zueinander inverse Relationen.
  - (S,L,R_1) ist eine Funktion
  - (L,S,R_2) ist keine Funktion

Relationen und Funktionen 7

- Ist $f : A \to B$ bijektiv $\Rightarrow$ $f^{-1} : B \to A$ bijektiv.
  - $f^{-1}(f(a)) = a$ für alle $a \in A$
  - $f(f^{-1}(b)) = b$ für alle $b \in B$
- Wir wissen: $\{a\} \neq (a)$, aber es existiert eine einfache Bijektion (bijektive Abbildung) f zwischen einelementigen Mengen und geordneten 1-Tupeln: $f(\{a\}) = (a)$.
- Solche Bijektionen (bijektive Funktionen) heißen natürliche Isomorphismen – sie berechtigen dazu, {a}, (a) und a im entsprechenden Kontext als identisch anzusehen.
- Beispiele:
  - Für Mengen A und B gibt es den natürlichen Isomorphismus h von $2^{A \times B}$ (Menge aller binären Relationen auf A und B) auf die Menge $\{f \mid f \text{ ist Funktion von A nach } 2^B\}$.
  - Es sei $R \subseteq A \times B$, dann ist h(R) die Funktion $f : A \to 2^B$, so dass $f(a) := \{b \mid b \in B, (a, b) \in R\}$.

Relationen und Funktionen 8

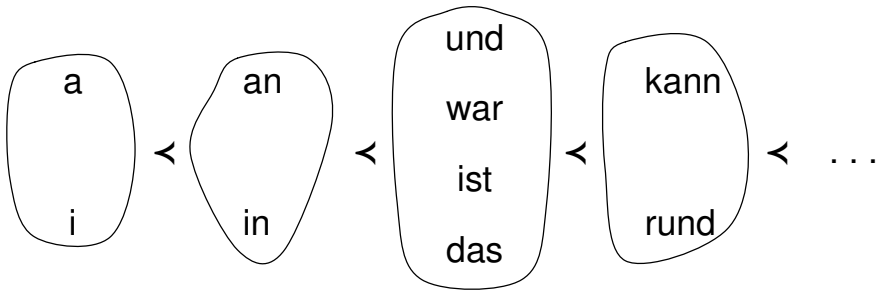
- Beispiele (Fortsetzung):
  - L sei die Menge aller Länder in Österreich.
  - $R \subseteq L \times L$, $(\ell_1, \ell_2) \in R \Leftrightarrow \ell_1, \ell_2$ sind benachbart.
  - $f : L \to 2^L$, $f(l) = \{\ell' \mid \ell' \in L, \ell \text{ und } \ell' \text{ sind benachbart}\}$.
- Manchmal interessiert die Umkehrung einer Funktion $f : A \to B$ auch dann, wenn die Funktion f nicht bijektiv ist.
  Zu einem Wert $b \in B$ interessiert uns dann die Urbildmenge.

  Idee: Betrachte $f^{-1} \subseteq B \times A$ (die Umkehrung der Funktion f) als Funktion von B nach 2^A unter Benutzung des natürlichen Isomorphismus.
- Sind Q und R binäre Relationen, dann bezeichne $Q \circ R$ (kurz QR) ihre Komposition.

  $Q \circ R := \{(a, b) \mid \exists\, c \text{ mit } (a, c) \in Q \text{ und } (c, b) \in R\}$
- Sind $f : A \to B$ und $g : B \to C$ Funktionen, dann ist $h = f \circ g$ eine Funktion, $h : A \to C$ mit $h(a) := f \circ g(a) := g(f(a))$.

Relationen und ihre Darstellung 1

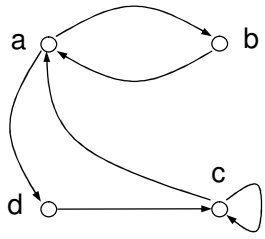
- Wir betrachten Relationen $R \subseteq A \times A$.
- Beispiele:
  a) Kleiner-Relation < (auf natürlichen Zahlen)
     ... < 2 < 3 < 4 < ...
  b) Größer-Relation >
     ... > 10 > 9 > 8 > 7 > ... (auf natürlichen Zahlen)
  c) Kürzer-Relation $\prec$ (auf Wörtern)



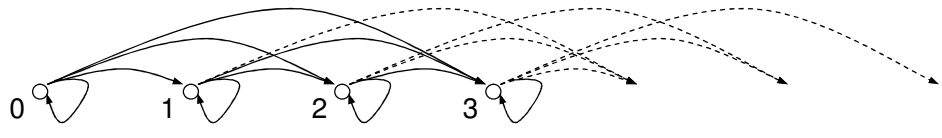
Relationen und ihre Darstellung 2

- $R \subseteq A \times A$ kann durch einen Graphen repräsentiert werden: a als Knoten ○ mit der Bezeichnung a, $(a,b) \in R$ als gerichtete Kante zwischen den Knoten a und b: 

- Beispiele:
  a) R = {(a,b), (b,a), (a,d), (d,c), (c,c), (c,a)}



  b) $\leq : \{(i,j) \mid i, j \in \mathbb{N}, i \leq j\}$, der zugehörige Graph ist unendlich



Relationen und ihre Darstellung 3

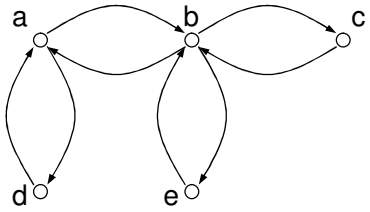
- $R \subseteq A \times A$ heißt reflexiv $:\Leftrightarrow (\forall\, a \in A)\ (a, a) \in R$

  a) ist nicht reflexiv

  b) ist reflexiv

- $R \subseteq A \times A$ heißt symmetrisch $:\Leftrightarrow ((a,b) \in R \ \Rightarrow\ (b,a) \in R)$
- Beispiele:

  a) $R = \{(a,b), (b,a), (a,d), (d,a), (b,c), (c,b), (b,e), (e,b)\}$ ist symmetrisch.

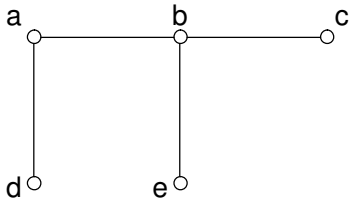


  b) „Freundschaft“ ist (i.d.R.) symmetrisch, nicht reflexiv.

  c) {(a,b) | a, b Personen mit demselben Vater} ist symmetrisch und reflexiv.

Relationen und ihre Darstellung 4

- Symmetrische Relationen können als ungerichtete Graphen dargestellt werden.



- $R \subseteq A \times A$ heißt antisymmetrisch $:\Leftrightarrow$
  $((a,b) \in R, a \neq b) \ \Rightarrow\ (b,a) \notin R)$
- Beispiel:

  P sei die Menge aller Personen

  {(a,b) | a, b ∈ P, a ist Vater von b} ist antisymmetrisch.

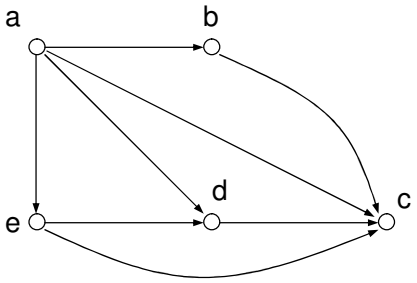
  Es gibt Relationen, die sind weder symmetrisch noch antisymmetrisch:

  {(a,b) | a, b ∈ P, a ist Bruder von b}, etwa fünf Geschwister, davon zwei ♂ und drei ♀.

Relationen und ihre Darstellung 5

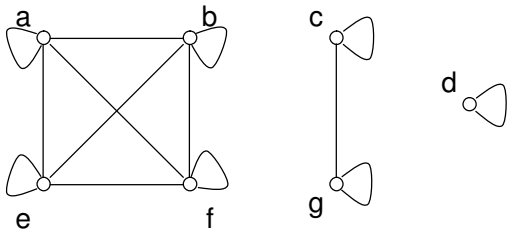
- $R \subseteq A \times A$ heißt transitiv $:\Leftrightarrow ((a,b), (b,c) \in R) \Rightarrow (a,c) \in R)$
  $\{(a,b) \mid a, b \in P$, a ist Vorfahre von b$\}$ ist transitiv

- $<$, $>$ und $\prec$ (kürzer) sind transitiv.
  Für den zugehörigen Graphen gilt dann:
  Gibt es eine Folge von Pfeilen $a \to b \to c \to ... \to z$,
  dann gibt es auch einen von a nach z ($a \to z$).



Relationen und ihre Darstellung 6

- R heißt Äquivalenzrelation $:\Leftrightarrow$ R ist reflexiv, symmetrisch und transitiv.
- Eine Äquivalenzrelation kann durch einen ungerichteten Graphen repräsentiert werden, der Graph besteht aus Äquivalenzklassen.
- [a] bezeichnet die Äquivalenzklasse, in der $a \in A$ liegt.
- $[a] := \{b \mid (a,b) \in R\}$ bzw. $[a] := \{b \mid (b,a) \in R\}$
- Beispiel: R = { (a,a),(b,b),(e,e),(f,f),(a,b),(b,a),(a,e),(e,a),(b,e),
  (e,b),(b,f),(f,b),(c,c),(g,g),(c,g),(g,c),(d,d)}



- Hier ergeben sich drei Äquivalenzklassen (Cluster) – so genannte Zusammenhangskomponenten.

Relationen und ihre Darstellung 7

Satz A1: (Beweis: Übung)
Es sei R eine Äquivalenzrelation auf A, dann bilden die Äquivalenzklassen von R eine Partition von A.

- Ist eine Äquivalenzrelation gegeben, so können wir immer die korrespondierende Partition konstruieren.
- Beispiel:
  - R = {(a,b) | a, b ∈ P, a und b haben dieselben Eltern}
  - Äquivalenzklassen sind (hier) Gruppen von Geschwistern.
- Satz 1.1 kann auch umgekehrt werden:
  Jede Partition bestimmt eine Äquivalenzrelation.

  Π sei eine Partition von A.

  {(a,b) | a, b ∈ A, a, b sind in derselben Teilmenge von Π} ist Äquivalenzrelation.
- Hieraus resultiert wiederum ein natürlicher Isomorphismus zwischen Äquivalenzrelationen auf A und Partitionen von A.

Relationen und ihre Darstellung 8

- R heißt partielle Ordnung (PO) auf A :⇔
  R ist reflexiv, antisymmetrisch und transitiv.
- Eine partielle Ordnung $R \subseteq A \times A$ heißt totale Ordnung :⇔
  (∀ a, b ∈ A) gilt: (a,b) ∈ R oder (b,a) ∈ R).
- Beispiele:
  - R = {(a,b) | a,b ∈ P, a ist Vorfahre von b} ist eine partielle Ordnung (falls wir (a,a) ∈ R akzeptieren).
  - R ist keine totale Ordnung, da Geschwister keine „Vorfahrenbeziehung“ haben.
  - ≤ ist eine totale Ordnung auf ℕ.
- $R \subseteq A \times A$; eine Folge $(a_1, ..., a_n)$, $n \geq 1$, mit $(a_i,a_{i+1}) \in R$, $i = 1(1)n-1$, heißt Kette in R.
- Die Kette $(a_1, ..., a_n)$ heißt Zykel, falls $a_i \neq a_j$, $i \neq j$, und $(a_n,a_1) \in R$.
- Ein Zykel $(a_1, ..., a_n)$ heißt trivial, falls $n = 1$, sonst nichttrivial.

Relationen und ihre Darstellung 9

Satz A2:

Es sei $R \subseteq A \times A$. R ist eine partielle Ordnung $\Leftrightarrow$ R ist reflexiv, transitiv und R hat keine nichttrivialen Zykel.

Beweis:

„$\Rightarrow$“ Jede partielle Ordnung ist reflexiv und transitiv. Annahme: R habe einen nichttrivialen Zykel $(a_1, ..., a_n)$ mit $n \geq 2 \Rightarrow (a_n,a_1) \in R \Rightarrow$ (da R transitiv ist) $(a_1,a_n) \in R \Rightarrow$ R ist nicht antisymmetrisch $\Rightarrow$ R ist keine partielle Ordnung. Widerspruch.

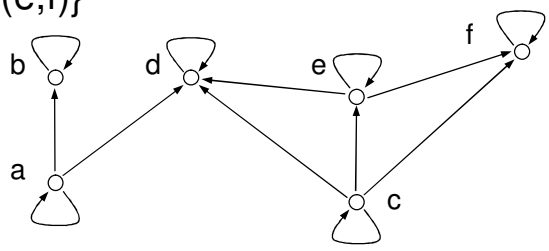
„$\Leftarrow$“ R hat keine nichttrivialen Zykel $\Rightarrow$ R ist antisymmetrisch, denn mit $a \neq b$ und $(a,b) \in R$ und $(b,a) \in R \Rightarrow (a,b)$ ist nichttrivialer Zykel. Damit ist R reflexiv, transitiv und antisymmetrisch, und somit ist R eine partielle Ordnung.

- Betrachten wir (partielle oder totale) Ordnungen, dann stellt sich unmittelbar die Frage nach einem minimalen bzw. maximalen Element. So ist etwa 0 das kleinste (minimale) Element der natürlichen Zahlen bzgl. der Kleiner-Relation.

Relationen und ihre Darstellung 10

- Es sei $R \subseteq A \times A$ eine partielle Ordnung. $a \in A$ heißt minimal, wenn $(b,a) \in R$ genau dann, falls $b = a$.
- Beispiel:

  R = {(a,a), (b,b), (a,b), (d,d), (a,d), (c,c), (c,d), (e,e), (c,e), (e,d), (f,f), (c,f), (e,f)}



  a und c sind minimale Elemente der partiellen Ordnung R.

- Jede endliche partielle Ordnung besitzt wenigstens ein minimales Element.
- Eine unendliche partielle Ordnung kann ein minimales Element besitzen.

Relationen und ihre Darstellung 11

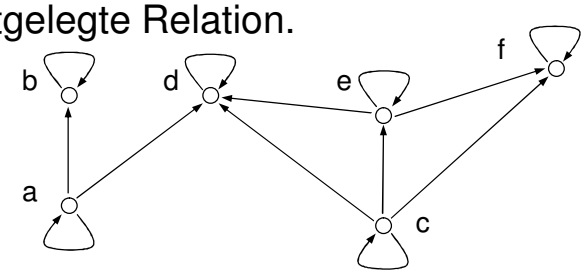
- Beispiele:
  - In $\mathbb{N}$ ist 0 das minimale Element.
  - In $\mathbb{Z}$ existiert kein minimales Element.
  - Es sei S eine beliebige Menge von Mengen,
    $R_S := \{(A,B) \mid A, B \in S, A \subseteq B\}$ ist PO auf S.
  - Ein minimales Element existiert nicht notwendiger Weise:
    Betrachte etwa $S = \{\{x \mid x \in \mathbb{R}, 0 \leq x \leq 1/n\} \mid n = 1, 2, \ldots\}$
  - Es kann mehrere minimale Elemente geben:
    Betrachte etwa $S = \{\{a\}, \{b\}, \{a,b\}\}$
- Infixnotation:
  - Statt $(a,b) \in R$ schreiben wir auch $a\ R\ b$,
  - i.d.R. schreiben wir $a = b$ anstelle von $(a,b) \in =$.
  - Vorteile bei Transitivität: $a\ R\ b\ R\ c \Rightarrow a\ R\ c$.

Abschlusseigenschaften 1

- Wir erinnern uns:
  Die Menge $\mathbb{N}$ ist abgeschlossen bezüglich der Addition, denn für alle $a, b \in \mathbb{N}$ gilt $a+b \in \mathbb{N}$.
- $\mathbb{N}$ ist nicht abgeschlossen bezüglich der Subtraktion.
  Es existieren $a, b \in \mathbb{N}$ mit $a-b \notin \mathbb{N}$.
- Die Menge $\mathbb{Z}$ ist abgeschlossen bezüglich der Subtraktion, denn für alle $a, b \in \mathbb{Z}$ gilt $a-b \in \mathbb{Z}$.
- Sei D eine Menge, $n \geq 0$, $R \subseteq D^{n+1}$ eine Relation.
  Eine Teilmenge $B \subseteq D$ heißt abgeschlossen unter R, falls $b_{n+1} \in B$ wenn $b_1, \ldots, b_n \in B$ und $(b_1, \ldots, b_{n+1}) \in R$.
- Übung:
  Es sei $D = \{a, b, c, d, e, f\}$ und R die durch den folgenden Graphen festgelegte Relation. Bestimmen Sie eine Teilmenge $B \subseteq D$ mit $|B| \geq 3$, für die B unter R abgeschlossen ist.

Abschlusseigenschaften 2

- Sei D eine Menge, $n \geq 0$, $R \subseteq D^{n+1}$ eine Relation.
  Eine Teilmenge $B \subseteq D$ heißt abgeschlossen unter R, falls für $b_1, ..., b_n \in B$ und $(b_1, ..., b_{n+1}) \in R$ auch $b_{n+1} \in B$ gilt.
- Beispiel:
  Es sei D = {a, b, c, d, e, f} und R die durch den folgenden Graphen festgelegte Relation.



  B_1 = {a, b, d} ist abgeschlossen unter R (trivial), B_2 = {a, b, c} ist nicht abgeschlossen unter R (warum?).
- Übung: Bestimmen Sie die kleinste unter R abgeschlossene Teilmenge $B \subseteq D$ mit $|B| \geq 3$ und $\{a, e\} \subseteq B$.

Abschlusseigenschaften 3

- Eigenschaften der Form: „Die Menge B ist abgeschlossen unter den Relationen $R_1, ..., R_m$“ heißt Abschlusseigenschaft von B.
- Beispiel:
  Sei $D = 2^{\mathbb{N}}$, n = 2, $(X,Y,Z) \in R \Leftrightarrow Z = X \cap Y$
  $B := \{\{x \in \mathbb{N} \mid a \leq x \leq b\} \mid a, b \in \mathbb{N}\}$ ist abgeschlossen unter R.
- Da Relationen Mengen sind, können sie auch unter Relationen abgeschlossen sein.
- Beispiele: Es sei D eine Menge.
  - Q sei eine ternäre Relation auf D^2, $Q \subseteq (D \times D)^3$, so dass
    $Q = \{((a,b), (b,c), (a,c)) \mid a, b, c \in D\}$
    $R \subseteq D \times D$ ist abgeschlossen unter Q $\Leftrightarrow$ R ist transitiv,
    Transitivität ist also eine Abschlusseigenschaft.
  - Q' := {(a,a) | a ∈ D} ist eine unäre Relation auf D^2,
    dann ist $R \subseteq D \times D$ abgeschlossen unter Q' $\Leftrightarrow$ R ist reflexiv.
  - Ist R sowohl transitiv als auch reflexiv, dann ist $R \subseteq D \times D$ abgeschlossen unter Q und Q'.

Abschlusseigenschaften 4

- Bemerkung:
  Der Begriff „Abschluss unter einer Funktion f“
  ist verträglich mit der bisher definierten Abschlusseigenschaft:
  Betrachte f: $D^n \to D$ als Relation $R \subseteq D^{n+1}$.
- Beispiel:
  - D sei eine Menge, $n \geq 0$, $f : D^n \to D$.
  - $B \subseteq D$ ist abgeschlossen unter f, falls $f(b_1, ..., b_n) \in B$ für alle $b_1, ..., b_n \in B$.
  - z.B. $D = \mathbb{Z}$, $B = \mathbb{N}$, f: Addition von n Elementen.
- Wir erinnern uns:
  - Die Menge $\mathbb{N}$ ist abgeschlossen bezüglich der Addition, denn für alle $a, b \in \mathbb{N}$ gilt $a + b \in \mathbb{N}$.
  - $\mathbb{N}$ ist nicht abgeschlossen bezüglich der Subtraktion; es existieren $a, b \in \mathbb{N}$ mit $a - b \notin \mathbb{N}$.
  - Die Menge $\mathbb{Z}$ ist abgeschlossen bezüglich der Subtraktion, denn für alle $a, b \in \mathbb{Z}$ gilt $a - b \in \mathbb{Z}$.

Abschlusseigenschaften 5

- Bemerkung:
  Eine häufig verwendete Abschlusseigenschaften bzgl. einer Eigenschaft P ist die kleinste (abgeschlossene) Obermenge:

  A sei eine Menge. Bestimme „die kleinste“ Menge B mit $A \subseteq B$ und B erfüllt die Eigenschaft P (B ist abgeschlossen unter P).

Satz A3: (ohne Beweis)

Es seien P eine (durch Relationen auf D definierte) Abschlusseigenschaft und $A \subseteq D$. Dann gibt es eine eindeutig bestimmte minimale Menge B, $A \subseteq B$, die P genügt.

Spezialfall von Satz A3:

Die reflexive, transitive Hülle R^* von $R \subseteq A \times A$, ist der Abschluss von R unter den Relationen Q und Q'.

- $Q = \{((a,b), (b,c), (a,c)) \mid a, b, c \in A\}$
- $Q' = \{(a,a) \mid a \in A\}$

Abschlusseigenschaften 6

R^* ist die minimale reflexive, transitive Relation mit $R \subseteq R^*$.

- Beispiel:
  R = {(a,b) | Bus hält an a und später an b}
  R^* = {(a,b) | b ist von a mittels Bus erreichbar}

Satz A4:

Für die reflexive, transitive Hülle R^* einer binären Relation R gilt:
$R^* = R \cup \{(a,b) \mid$ es gibt eine Kette in R von a nach b$\}$
(beachte, dass es hier eine triviale „Kette“ von a nach a gibt)

- Bemerkung:
  Bezüglich der Reflexivität, Transitivität und der Symmetrie existieren weitere Abschlusseigenschaften (8 sind möglich), z.B.
  - R^+ ist die transitive Hülle von R.
  - ...
  - Die reflexive, symmetrische, transitive Hülle von R ist eine Äquivalenzrelation.

Endliche und unendliche Mengen 1

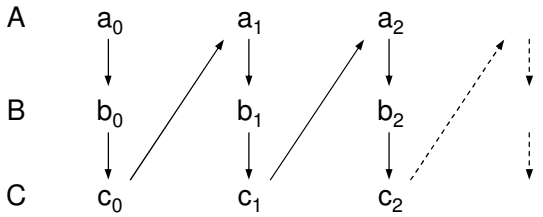
- Basischarakterisierung einer endlichen Menge A ist die Kardinalität |A| (# der Elemente, #: Zeichen für Anzahl).
- Sind A und B endliche Mengen mit $A \subseteq B$, so gilt $|A| \leq |B|$, ist $A \subset B$, so gilt $|A| < |B|$.
- Erweiterung auf unendliche Mengen ist komplexer: Gibt es mehr (natürliche) Vielfache von 17, {0,17,34,51, ...} = A_{17n}, als (natürliche) Quadratzahlen, {0,1,4,9,16, ...} = A_{nn} ?
- Zwei Mengen A und B heißen gleichmächtig, falls eine Bijektion $f : A \rightarrow B$ (und somit $f^{-1}: B \rightarrow A$) existiert.
- „Gleichmächtig“ ist eine symmetrische Relation, es ist sogar eine Äquivalenzrelation.
- {8, rot, {$\emptyset$,b}} und {1,2,3} sind gleichmächtig,
- f(8) = 1, f(rot) = 2, f({$\emptyset$,b}) = 3
- A_{17n} und A_{nn} sind gleichmächtig: $f(17n) = n^2$.

Endliche und unendliche Mengen 2

- Allgemein:
  - Menge A ist endlich, falls es ein $n \in \mathbb{N}$ gibt, so dass A und [1:n] gleichmächtig sind, d.h. $|A| = n$. Ist $A = \emptyset$, so ist $|A| = 0$.
  - Eine Menge ist unendlich, falls sie nicht endlich ist.
  - $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, A_{17n}, A_{nn} sind unendlich.
  - Nicht alle unendlichen Mengen sind gleichmächtig.
  - Eine Menge heißt
    abzählbar unendlich, falls sie gleichmächtig zu $\mathbb{N}$ ist.
    abzählbar, falls sie endlich oder abzählbar unendlich ist.
  - Eine Menge, die nicht abzählbar ist, heißt überabzählbar.
  - Es gibt verschiedene Techniken, um zu zeigen, dass A abzählbar unendlich ist.
  - Direkte Weg: Angabe einer Bijektion zwischen einer abzählbar unendlichen Menge B (nichtnotwendig $\mathbb{N}$) und A.

Endliche und unendliche Mengen 3

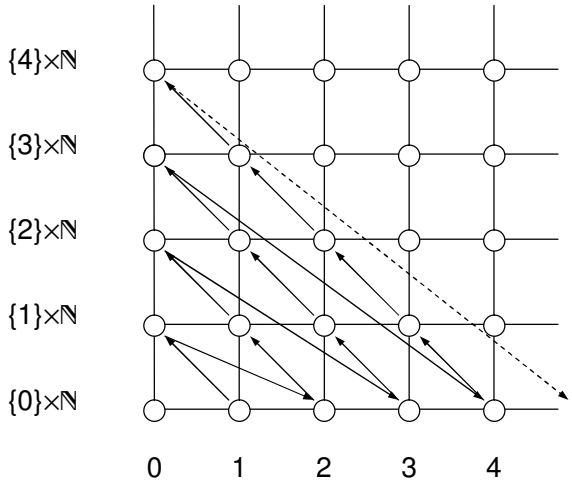
  - Ist B gleichmächtig zu $\mathbb{N}$, B gleichmächtig zu A
    $\Rightarrow$ A gleichmächtig zu $\mathbb{N}$.
  - Ist A eine unendliche Teilmenge einer abzählbar unendlichen Menge B, dann ist A abzählbar unendlich.
  - Die Vereinigung endlich vieler abzählbar unendlicher Mengen ist abzählbar unendlich.
- Beispiel:
  A, B und C seien disjunkte abzählbar unendliche Mengen,
  $A = \{a_0, a_1, a_3, ...\}$, $B = \{b_0, b_1, b_2, ...\}$, $C = \{c_0, c_1, c_2, ...\}$
  $A \cup B \cup C = \{a_0, b_0, c_0, a_1, b_1, c_1, ...\}$



Endliche und unendliche Mengen 4

- Die Idee kann genutzt werden, um zu zeigen, dass die Vereinigung unendlich vieler abzählbar unendlicher Mengen abzählbar unendlich ist.
- Beispiel:

  $\mathbb{N}\times\mathbb{N} = \{0\}\times\mathbb{N} \cup \{1\}\times\mathbb{N} \cup \{2\}\times\mathbb{N} \cup \ldots$



Endliche und unendliche Mengen 5

0. Runde: (0,0)
1. Runde: (0,1), (1,0)
2. Runde: (0,2), (1,1), (2,0)
3. Runde: (0,3), (1,2), (2,1), (3,0)
4. Runde: (0,4), (1,3), (2,2), (3,1), (4,0)

   ...

n. Runde: (0,n), (1,n–1), (2,n–2), . . . , (n–1,1), (n,0)

In der n-ten Runde werden alle Paare $(i,j) \in \mathbb{N}\times\mathbb{N}$ mit $i+j = n$ besucht.

- Hieraus resultiert eine so genannte Gödelisierung, dabei handelt es sich um eine bijektive Abbildung (hier: $\mathbb{N}\times\mathbb{N} \leftrightarrow \mathbb{N}$) zwischen abzählbar unendlichen Mengen.
- Wir werden (später) Techniken betrachten, mit denen wir die Überabzählbarkeit von Mengen beweisen werden.

Elementare Beweistechniken 1

- Die vollständigen Induktion ist ein wichtigsten Hilfsmittel, um Beweise zu führen. Wir betrachten das Basisprinzip:
- Sei A eine Menge natürlicher Zahlen, so dass
  - 1. $0 \in A$
  - 2. Aus $\{0,1,2, ...,n\} \subseteq A$ folgt $n+1 \in A$
  - Dann gilt: $A = \mathbb{N}$.
- Nutze dies, um zu zeigen: Für alle $n \in \mathbb{N}$ gilt die Eigenschaft P.
- Prinzipielle Vorgehensweise: $A = \{n \mid P \text{ ist wahr für alle } n\}$
  1. Induktionsanfang: Zeige: $0 \in A$, d.h. P ist wahr für 0.
  2. Induktionsvoraussetzung (Hypothese): Es sei $n \geq 0$ beliebig aber fest. P gelte für alle natürlichen Zahlen 0,1, ..., n.
  3. Induktionsschritt: Zeige unter Verwendung der Hypothese (Induktionsvoraussetzung), dass P auch für n+1 wahr ist.
- Damit ist dann $A = \mathbb{N}$ und P gilt für alle $n \in \mathbb{N}$.

Elementare Beweistechniken 2

Satz A5:

Für jede endliche Menge A gilt: $|2^A| = 2^{|A|}$.

Beweis:

Wir führen den Beweis per Induktion über die Kardinalität von A.

1. $|A| = 0$, d.h. $A = \emptyset$
   $2^{|A|} = 2^0 = 1$; $2^A = \{\emptyset\} \Rightarrow |2^A| = 1$
2. Sei $n \geq 0$, es gelte $|2^A| = 2^{|A|}$ für alle $|A| \leq n$.
3. $|A| = n+1$, da $n \geq 0$ enthält A wenigstens ein Element a.
   Sei $B := A - \{a\} \Rightarrow |B| = n$ und es gilt $|2^B| = 2^{|B|} = 2^n$.
   2^A kann in zwei disjunkte Mengen von Mengen zerlegt werden: in solche, die a enthalten und in solche, die a nicht enthalten.
   $2^A = 2^B \cup \{C \cup \{a\} \mid C \in 2^B\} \Rightarrow |2^A| = 2^n + 2^n = 2^{n+1}$.

- Ein anderes – in vielen Anwendungen nichttriviales – Hilfsmittel zu Beweisführung ist das so genannte Schubfachprinzip.

Elementare Beweistechniken 3

- Sind A und B nichtleere Mengen mit |A| > |B|, dann existiert keine injektive Funktion von A nach B. Verteilen wir die Elemente aus A auf |B| Schubfächer, so enthält wenigstens ein Schubfach mehr als ein Element. Beweis: Induktion über |B|.

Satz A6:

R sei eine binäre Relation auf der endlichen Menge A. Gibt es beliebig lange Ketten in R, dann existiert auch ein Zykel in R.

Beweis:

- Existieren beliebig lange Ketten $\Rightarrow$ es existiert eine Kette $(a_1, ..., a_n)$ für ein $n > |A|$.
- Schubfachprinzip: $f : \{1, ..., n\} \rightarrow A$ mit $f(i) = a_i$ kann nicht injektiv sein. Es gibt also i und j, $1 \leq i < j \leq n$, mit $f(i) = f(j)$.
- Sei $k > 0$ die kleinste Zahl für die $f(m) = f(m+k)$ ist; so ein m muss für $1 \leq m < n$ existieren.
- Dann ist $(a_m, a_{m+1}, ..., a_{m+k-1})$ ein Zykel; für $k = 1$ ergibt sich der triviale Zykel (a_m).

Elementare Beweistechniken 4

- In Beweisen werden wir das Diagonalisierungsprinzip einsetzen, es dient häufig dazu, Widerspruchsbeweise zu führen.
  - R sei eine binäre Relation auf der Menge A.
  - $D = \{a \mid a \in A, (a,a) \notin R\}$ sei die Diagonalmenge von R.
  - Für jedes $a \in A$ sei $R_a := \{b \mid b \in A, (a,b) \in R\}$.
  - Damit gilt: $D \neq R_a$ für alle $a \in R$.

Satz A7: (Cantor 1845-1918)

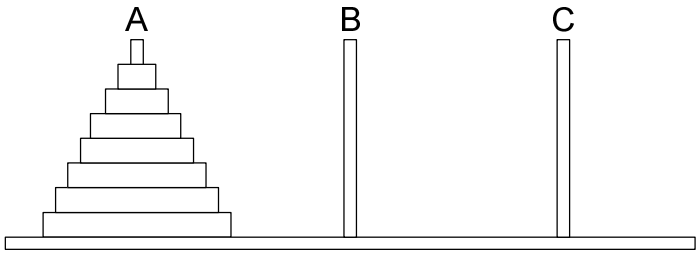
Die Menge $2^{\mathbb{N}}$ ist überabzählbar.

Beweis:

- Annahme: $2^{\mathbb{N}}$ ist abzählbar unendlich. Dann existiert eine Bijektion $f : \mathbb{N} \rightarrow 2^{\mathbb{N}}$, $2^{\mathbb{N}} = \{S_0, S_1, S_2, ...\}$ mit $f(i) = S_i$, $i \in \mathbb{N}$.
- Betrachte die Diagonalmenge $D = \{n \in \mathbb{N} \mid n \notin S_n\} \in 2^{\mathbb{N}}$, womit ein $k \in \mathbb{N}$ existieren müsste mit $D = S_k$.
- Es gilt dann entweder $k \in S_k$ oder $k \notin S_k$.
  $k \in S_k$: $D = \{n \in \mathbb{N} \mid n \notin S_n\} \Rightarrow k \notin D$, aber $D = S_k$, womit $k \notin S_k$.
  $k \notin S_k$: $k \in D$, aber $D = S_k \Rightarrow k \in S_k$.
- Hiermit gilt: $2^{\mathbb{N}}$ ist überabzählbar.

Elementare Beweistechniken 5

- Türme von Hanoi: Existiert ein Verfahren, um die Scheiben von A nach C zu transportieren? Dabei darf B benutzt werden, es darf aber niemals eine größere Scheibe auf einer kleineren liegen.



- Hier kann leicht ein Existenzbeweis (per Induktion über die Anzahl n der Scheiben) erbracht werden.
  - Induktionsanfang (n = 1) und Hypothese (n = k) trivial.
  - n = k+1: Transportiere die obersten k Scheiben von A nach B (wg. Hypothese), transportiere die unterste größte Scheibe von A nach C. Transportiere die verbleibenden k Scheiben von B nach C.
- Nun wissen wir lediglich: Für alle n existiert eine Lösung.

Elementare Beweistechniken 6

- Von besonderer Bedeutung sind konstruktive Beweise, bei denen explizite Verfahren angegeben werden.
- Als Beispiel betrachten wir k-reguläre (ungerichtete) Graphen, bei denen der Grad (Anzahl der Kanten die den Knoten als Endpunkt haben) eines jeden Knoten k ist.

Satz A8:

Für jede gerade Zahl $n \in 2\mathbb{N}+2$ existiert ein Graph G = (V,E) mit n Knoten, so dass G 3-regulär ist.

Beweis:

Die Anzahl (n > 0) der Knoten in G = (V,E) sei gerade, n = 2k. Wir bezeichnen die Knoten mit V = (1,2,...,2k). Die ungerichteten Kanten resultieren aus folgender Konstruktion:

$E = \{ \{i, i+1\} \mid 1 \leq i \leq 2k-1\} \cup \{ \{2k, 1\} \} \cup \{ \{i, i+k\} \mid 1 \leq i \leq k\}$

- Übung: Skizzieren Sie den resultierenden Graph für n = 2k = 10.