Grundlagen der Theoretischen Informatik

Till Mossakowski

Fakultät für Informatik
Otto-von-Guericke Universität
Magdeburg

Wintersemester 2014/15

Notation für Wörter

$|w|_a$ is die Anzahl der Vorkommen von a in w
Beispiel: $|abba|_a = 2$

Zwei Mengen A und B heißen *disjunkt*, falls sie keine gemeinsamen Elemente enthalten, d.h., falls $A \cap B = \emptyset$.

Eine Teilmenge Π der Potenzmenge 2^A einer nicht-leeren Menge A heißt *Partition* von A, falls gilt

- jedes Element von Π ist nicht leer
- $B, C \in \Pi, B \neq C \Rightarrow B \cap C = \emptyset$
- jedes Element von A ist in einer der Mengen in Π enthalten

Eine *Folge* von Objekten ist eine Auflistung dieser Objekte in einer bestimmten Ordnung.

Ein *geordnetes n-Tupel* ist eine Folge von n Objekten. Wir schreiben

$$(a_1, a_2, \ldots, a_n)$$

Das i-te Objekt a_i der Folge wird als *i-te Komponente* bezeichnet. Ein *geordnetes Paar* ist ein geordnetes 2-Tupel.

Das *kartesische Produkt* $A_1 \times A_2 \times \cdots \times A_n$ von n Mengen $A_1, \ldots, A_n$ ist die Menge aller geordneten n-Tupel $(a_1, a_2, \ldots, a_n)$ mit $a_i \in A_i$ für alle $i = 1, \ldots, n$.

Relationen und Funktionen

Eine *n-stellige Relation* auf den Mengen $A_1, \ldots, A_n$ ist eine Teilmenge von $A_1 \times A_2 \times \cdots \times A_n$.

Eine 1-stellige Relation heißt *unäre Relation*, eine 2-stellige Relation heißt *binäre Relation*.

Eine *Funktion* von A nach B ist eine binäre Relation mit der Eigenschaft: Für jedes Element a aus A gibt es genau ein geordnetes Paar mit a als erster Komponente.

$$f : A \to B$$
$$a \mapsto f(a)$$

Eine *partielle Funktion* von A nach B ist eine binäre Relation mit der Eigenschaft: Für jedes Element a aus A gibt es höchstens ein geordnetes Paar mit a als erster Komponente.

Eine Funktion $f : A_1 \times A_2 \times \cdots \times A_n \to B$
mit $f(a_1, a_2, \ldots, a_n) = b$ heißt *n-stellige Funktion*. b heißt *Funktionswert*, die a_i werden *Argumente* genannt.

Eine Funktion $f : A \to B$ heißt *injektiv*, falls verschiedene Elemente aus A auf verschiedene Elemente aus B abgebildet werden, d.h., aus $a, a' \in A, a \neq a'$ folgt $f(a) \neq f(a')$, f heißt *surjektiv*, falls es für jedes $b \in B$ ein $a \in A$ gibt, so dass $b = f(a)$, und f heißt *bijektiv*, falls f sowohl injektiv als auch surjektiv ist.

Binäre Relationen

Eine binäre Relation $R \subseteq A \times A$ heißt *reflexiv*, falls $(a, a) \in R$ für alle $a \in A$,

R heißt *symmetrisch* falls aus $(a, b) \in R$ folgt, dass $(b, a) \in R$,

R heißt *transitiv* falls aus $(a, b), (b, c) \in R$ folgt, dass auch $(a, c) \in R$,

und R heißt *antisymmetrisch*, falls aus $(a, b) \in R$, $(b, a) \in R$ folgt, dass $a = b$.

Eine binäre Relation, die reflexiv, transitiv und symmetrisch ist, heißt *Äquivalenzrelation*.

Sei $R \subseteq A \times A$ eine Äquivalenzrelation.

$$[a]_R = \{b \mid (a, b) \in R\}$$

heißt die *Äquivalenzklasse* von a bezüglich R.

Satz:
Die Äquivalenzklassen einer Äquivalenzrelation $R \subseteq A \times A$ bilden eine Partition von A.

Eine binäre Relation $R \subseteq A \times A$, die reflexiv, transitiv und antisymmetrisch ist, heißt *partielle Ordnung* oder auch *Halbordnung* auf A. Sie heißt *totale Ordnung*, wenn für alle $a,b \in A, a \neq b$, entweder $(a,b) \in R$ oder $(b,a) \in R$.

Die *inverse Relation* einer binären Relation $R \subseteq A \times B$ ist die Relation

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

Ein *Pfad* in einer binären Relation $R \subseteq A \times A$ ist eine Folge $(a_1, a_2, \ldots, a_n)$ für ein $n \geq 1$, so dass $(a_i, a_{i+1}) \in R$ für alle $i = 1, \ldots, n-1$. Ein Pfad heißt *einfacher Pfad*, falls alle a_i verschieden sind. Ein Pfad $(a_1, a_2, \ldots, a_n)$ hat *Länge* $n-1$.

Ein *Kreis* in einer binären Relation $R \subseteq A \times A$ ist eine Folge $(a_1, a_2, \ldots, a_n)$ für ein $n \geq 1$, so dass $(a_i, a_{i+1}) \in R$ für alle $i = 1, \ldots, n-1$ und ferner $(a_n, a_1) \in R$. Ein Kreis heißt *einfacher Kreis*, falls alle a_i verschieden sind. Ein Kreis $(a_1, a_2, \ldots, a_n)$ hat *Länge* n.

Sei $R \subseteq V \times V$ eine binäre Relation.

Die *reflexive Hülle* von R ist die Relation

$$R \cup \{(a,a) \mid a \in V\}$$

Die *transitive Hülle* von R ist die Relation

$$R \cup \{(a,b) \mid a,b \in V \text{ und es gibt einen Pfad positiver Länge von } a \text{ nach } b \text{ in } R\}$$

Die *reflexive, transitive Hülle* von R ist die Relation

$$R^* = \{(a,b) \mid a,b \in V \text{ und es gibt Pfad von } a \text{ nach } b \text{ in } R\}$$

Natürliche Bijektionen

Bestimmte Bijektionen, die besonders einfach sind, nennen wir natürliche Bijektionen.

Beispiele:

$$\phi : \mathbb{N} = \{1,2,\ldots\} \to \{\{n\} \mid n \in \mathbb{N}\}$$

$$\phi(k) = \{k\}$$

$$\phi : A \times B \times C \to (A \times B) \times C$$
$$\phi(a,b,c) = ((a,b),c)$$

$$\phi : 2^{A \times B} \to \{f \mid f \text{ ist eine Funktion von } A \text{ nach } 2^B\}$$

$$\phi(R) = f : A \to 2^B, \text{ wobei}$$
$$f(a) = \{b \mid b \in B \text{ und } (a,b) \in R\}$$

Abzählbarkeit

Welche Menge enthält mehr Elemente?

$\{0,17,34,51,68,\ldots\}$ oder $\{0,14,28,42,56,\ldots\}$

$\{0,1,2,3,4,5,\ldots\}$ oder $\{0,2,4,6,8,10,\ldots\}$

Zwei Mengen A und B heißen *gleichmächtig*, wenn es eine bijektive Funktion $f : A \to B$ gibt.

Eine Menge heißt *endlich*, wenn sie gleichmächtig ist zu $\{1,2,\ldots,n\}$ für ein $n \in \mathbb{N}$. Sie heißt *unendlich*, wenn sie nicht endlich ist.

Mit $|A|$ bezeichnen wir die Anzahl der Elemente einer endlichen Menge A.

Eine Menge heißt *abzählbar unendlich*, wenn sie gleichmächtig ist zu $\mathbb{N}$.

Satz:
$\mathbb{N} \times \mathbb{N}$ *ist abzählbar unendlich.*

Satz:
Die Vereinigungsmenge abzählbar unendlich vieler abzählbar unendlicher Mengen ist abzählbar unendlich.

Eine unendliche Menge, die nicht abzählbar unendlich ist, heißt *überabzählbar*.

Satz:
$2^{\mathbb{N}}$ *ist überabzählbar.*

Satz: [Georg Cantor]
$\mathbb{R}$ *ist überabzählbar.*

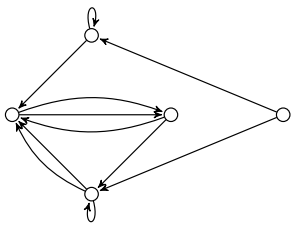
Graphen

Ein (gerichteter) *Multigraph* $G = (V, E)$ besteht aus einer Menge von *Knoten* V und einer Menge von *Kanten* E und zugehörigen Funktionen $source : E \to V$ und $target : E \to V$, die jeder Kante $e \in E$ einen initialen Knoten $source(e)$ und einen terminalen Knoten $target(e)$ zuordnen.

Zwei oder mehr Kanten mit gleichen initialen und terminalen Knoten heißen *Mehrfachkanten*.

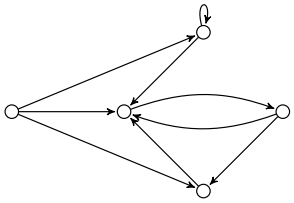
Eine Kante e mit $source(e) = target(e)$ heißt *Schlinge*.

Veranschaulicht werden Graphen durch eine Menge von Punkten, den Knoten, zwischen denen Linien, die Kanten, verlaufen. Die terminalen Knoten werden dabei durch Pfeilspitzen gekennzeichnet.



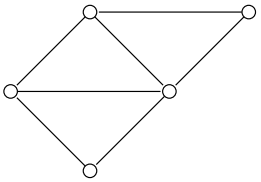
Ein (gerichteter) *Graph* ist ein (gerichteter) Multigraph ohne Mehrfachkanten. Die Kantenmenge E können wir nun als Teilmenge von $V \times V$ auffassen.

Gerichtete Graphen sind in natürlicher Weise isomorph zu binären Relationen auf den Knotenmengen.



Ein *ungerichteter Graph* besteht aus einer Menge von Knoten V und einer Menge von Kanten E, deren Elemente zweielementige Teilmengen von V sind.

Bei einem ungerichteten Graphen sind die Knoten einer Kante nicht ausgezeichnet. Ferner gibt es keine Schlingen.



Ein *Pfad* in einem (gerichteten) Multigraphen $G = (V, E)$ ist eine Folge $v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n$ für ein $n \geq 0$, wobei $v_i \in V$ für alle $i = 0, \ldots, n$ und $e_j \in E$ mit $source(e_j) = v_{j-1}$ und $target(e_j) = v_j$ für für alle $j = 1, \ldots, n$.

Ein Pfad $v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n$ heißt *einfacher Pfad*, falls $v_0, \ldots, v_n$ paarweise verschieden sind.

Ein Pfad $v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n$ heißt *Kreis*, falls $v_0 = v_n$.

Ein Kreis $v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n$ heißt *einfacher Kreis*, falls $v_1, \ldots, v_n$ paarweise verschieden sind.

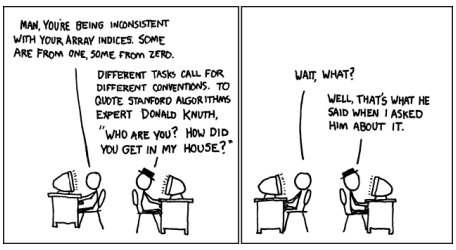
Ein *Pfad* in einem ungerichteten Graphen $G = (V, E)$ ist eine Folge $v_0, v_1, \ldots, v_n$ für ein $n \geq 0$, wobei $\{v_i, v_{i+1}\} \in E$ für alle $i = 0, \ldots, n-1$.

Ein Pfad in einem ungerichteten Graphen heißt *einfacher Pfad*, falls $v_0, \ldots, v_n$ paarweise verschieden sind.

Ein Pfad $v_0, v_1, \ldots, v_n$ in einem ungerichteten Graphen heißt *Kreis*, falls $n \geq 3$ und $v_0 = v_n$.

Ein Kreis in einem ungerichteten Graphen heißt *einfacher Kreis*, falls $v_1, \ldots, v_n$ paarweise verschieden sind.

Ein ungerichteter oder gerichteter Graph heißt *azyklisch*, falls er keinen Kreis enthält.



xkcd.com

Ein ungerichteter Graph heißt *zusammenhängend*, falls je zwei Knoten des Graphen durch einen Pfad verbunden sind.

Der *Ausgangsgrad* eines Knotens v in einem Multigraphen ist die Anzahl der Kanten, für die v initialer Knoten ist, also $|\{e \in E \mid source(e) = v\}|$.

Der *Eingangsgrad* eines Knotens v in einem Multigraphen ist die Anzahl der Kanten, für die v terminaler Knoten ist, also $|\{e \in E \mid target(e) = v\}|$.

Der *Grad* eines Knotens v in einem ungerichteten Graphen ist $|\{e \in E \mid v \in e\}|$.

Ein *Baum* ist ein zusammenhängender, azyklischer ungerichteter Graph.

Ein *Wurzelbaum* ist ein Baum, der einen ausgezeichneten Knoten enthält, der *Wurzel* genannt wird. Die von der Wurzel verschiedenen Knoten vom Grad 1 werden *Blätter* genannt.

In einem Wurzelbaum lassen sich die Kanten von der Wurzel zu den Blättern orientieren. Bezüglich dieser Orientierung gibt es für alle Knoten außer der Wurzel genau einen Vorgänger, der *Elterknoten* genannt wird, und für alle Knoten außer den Blättern Nachfolger, die *Kinder* genannt werden.

Ein Wurzelbaum heißt *geordneter Wurzelbaum*, falls unter den Kindern jedes Knotens eine Ordnung festgelegt ist.

O-Notation

Seien $f : \mathbb{N} \to \mathbb{R}$ und $g : \mathbb{N} \to \mathbb{R}$ zwei Funktionen, so dass $f(n) \geq 0$ und $g(n) \geq 0$ für alle $n \in \mathbb{N}$ gilt.

$f(n) = O(g(n))$ wenn es n_0 und eine positive Konstante c gibt, so dass $f(n) \leq c \cdot g(n)$ für alle $n \geq n_0$.

$f(n) = \Omega(g(n))$ wenn es n_0' und eine positive Konstante c' gibt, so dass $f(n) \geq c' \cdot g(n)$ für alle $n \geq n_0'$.

$f(n) = \Theta(g(n))$ wenn $f(n) = O(g(n))$ und $f(n) = \Omega(g(n))$.

Beweise und Beweistechniken

$$\underset{\textit{Hypothese}}{H} \quad \Rightarrow \quad \underset{\textit{Konklusion}}{K}$$

wenn H gilt, dann gilt auch K

wenn H, dann K

aus H folgt K

H impliziert K

H ist hinreichend für K

K ist notwendig für H

H nur dann, wenn K

$$\neg H \quad \Leftarrow \quad \neg K$$

Beweistechniken

- Deduktiver Beweis
- Indirekter Beweis: Beweis der Kontraposition
- Beweis durch Widerspruch (reductio ad absurdum)
  - Diagonalisierung
- Induktion
  - vollständige Induktion
  - strukturelle Induktion
- Existenzbeweis
  - Beispiel („Beweis durch Gegenbeispiel“)
  - Konstruktionsverfahren
  - Probabilistische Methode
- Schubfachprinzip

Deduktive Beweise

Satz: *Die Summe dreier aufeinanderfolgender natürlicher Zahlen ist durch 3 teilbar.*

Seien $a = n$, $b = n+1$ und $c = n+2$ die drei Zahlen. Dann gilt

$$\begin{aligned} a+b+c &= n+(n+1)+(n+2) \\ &= 3n+3 \\ &= 3(n+1) \end{aligned}$$

Also ist $a+b+c$ durch 3 teilbar.

Indirekte Beweise

Satz: *Sei $a \in \mathbb{N}$. Wenn a^2 gerade ist, dann ist auch a gerade.*

Wir zeigen: Falls a ungerade ist, so ist auch a^2 ungerade:

Falls a ungerade ist, so ist $a = 2n-1$ für ein $n \in \mathbb{N}$.
Dann ist $a^2 = 4n^2 - 4n + 1$. Da $4n^2 - 4n$ gerade ist,
ist a^2 also ungerade.

Beweise durch Widerspruch

Satz: *Es gibt unendlich viele Primzahlen.*

Nehmen wir an, die Anzahl der Primzahlen sei endlich. Sagen wir, es gäbe k Primzahlen $p_1, p_2, \ldots, p_k$. Betrachte

$$p_1 \cdot p_2 \cdots p_k + 1$$

Diese Zahl ist durch keine der k Primzahlen teilbar, also muss es Primzahlen geben, die wir nicht mitgezählt haben. Widerspruch!

Diagonalisierung

Satz: $2^{\mathbb{N}}$ *ist überabzählbar.*

Nehmen wir an, es gäbe eine Abzählung

$$2^{\mathbb{N}} = \{R_1, R_2, R_3, \ldots\}$$

Betrachten wir

$$D = \{n \in \mathbb{N} \mid n \notin R_n\}$$

Es ist $D \in 2^{\mathbb{N}}$, aber D ist von allen Mengen in der Aufzählung $R_1, R_2, R_3, \ldots$ verschieden. Widerspruch!

Induktive Beweise

$$A = \{n \in \mathbb{N} \mid E \text{ gilt für } n\}$$

Falls

(1) $1 \in A$

(2) für alle $n \in \mathbb{N}$ gilt: $n \in A \Rightarrow n+1 \in A$

dann ist $A = \mathbb{N}$.

(1) *Induktionsverankerung*:
E gilt für $n = 1$

(2) *Induktionsannahme*:
Für beliebiges, aber festes n gilt E

(3) *Induktionsschritt*:
Falls die Induktionsannahme gilt, dann gilt E auch für $n+1$

Satz: $1+3+5+\cdots+2n-1 = n^2$ *für alle* $n \in \mathbb{N}$.

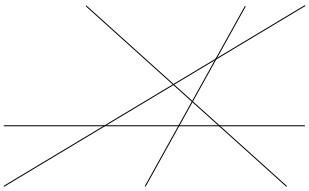
Induktionsverankerung:
Für $n = 1$ gilt $1 = 1^2$.

Induktionsschritt:

$$\begin{aligned} 1+3+5+\cdots+2n-1+2(n+1)-1 &= n^2+2(n+1)-1 \\ &= n^2+2n+1 \\ &= (n+1)^2 \end{aligned}$$

wobei die Gleichheit in der ersten Zeile nach Induktionsannahme gilt.

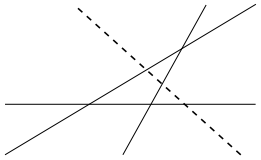
Anordnungen von Geraden (allgemeine Lage):
Gegeben seien n Geraden in der Ebene, so dass es unter diesen keine zwei parallelen Geraden gibt und keine drei, die sich in einem Punkt schneiden. Die Geraden unterteilen die Ebene in disjunkte Regionen.



Satz: *Die Anzahl der Regionen in einer Anordnung von n Geraden mit obigen Eigenschaften ist* $1+n(n+1)/2$.

Induktionsverankerung:
Eine Gerade unterteilt die Ebene in zwei Regionen.

Induktionsschritt:
Gegeben seien nun $n+1 \geq 2$ Geraden, die unsere Bedingungen erfüllen. Wir entfernen eine der Geraden. Die entstehende Anordnung besitzt nach Induktionsannahme $1+n(n+1)/2$ Regionen.



Wir fügen nun die entfernte Gerade ℓ wieder hinzu. Dadurch werden manche Regionen in zwei Regionen unterteilt. Wieviele? Eine mehr als es Schnittpunkte zwischen ℓ und den übrigen Geraden gibt. Es gibt n solche Schnittpunkte und somit wächst die Anzahl der Regionen um $n+1$:

$$1+n(n+1)/2+n+1 = 1+(n+1)((n+1)+1)/2$$

Variationen:

Falls

(1) $1 \in A$

(2) für alle $n \in \mathbb{N}$ gilt: $\{1,2,\ldots,n\} \subseteq A \Rightarrow n+1 \in A$

dann ist $A = \mathbb{N}$.

Falls

(1) $k \in A$

(2) für alle $n \in \{k, k+1, \ldots\}$ gilt: $n \in A \Rightarrow n+1 \in A$

dann ist $\{k, k+1, \ldots\} \subseteq A$.

Strukturelle Induktion

(1) Jede Zahl ist ein Ausdruck

(2) Falls E_1 und E_2 Ausdrücke sind, dann ist E_1+E_2 ein Ausdruck

(3) Falls E ein Ausdruck ist, dann ist (E) ein Ausdruck

Satz: *Jeder Ausdruck enthält die gleiche Anzahl von öffnenden und schließenden Klammern.*

Induktionsverankerung:
Eine Zahl enthält weder öffnende noch schließende Klammern.

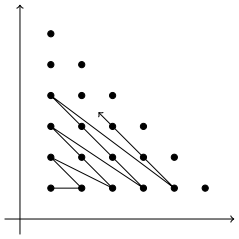
Induktionsschritt:
Falls der Ausdruck von der Form E_1+E_2 ist, so enthalten E_1 und E_2 nach Induktionsannahme jeweils gleichviele öffnende und schließende Klammern, also auch E_1+E_2.

Falls der Ausdruck von der Form (E) ist, so enthält E nach Induktionsannahme gleichviele öffnende und schließende Klammern. Da (E) von jeder Sorte genau eine Klammer mehr enthält als E, gilt die Behauptung auch für (E).

Konstruktive Beweise

Satz: $\mathbb{N} \times \mathbb{N}$ *ist abzählbar unendlich.*

$$f((i,j)) = \tfrac{1}{2}(\,(i+j)^2 - 3i - j) + 1$$



Die Probabilistische Methode

Man weist die Existenz eines Objekts mit einer bestimmten Eigenschaft nach, indem man zeigt, dass die Wahrscheinlichkeit, dass ein zufällig erzeugtes Objekt diese Eigenschaft besitzt, positiv ist.

Sei $G = (V,E)$ ein Graph und $\Pi = \{U, V-U\}$ eine Partition von V. Eine Kante $e \in E$ heißt *Schnittkante* bezüglich Π, falls ein Endknoten von e in U und der andere in $V-U$ liegt.

Satz: *Für jeden Graphen $G = (V,E)$ gibt es eine Partition von V, bezüglich derer die Anzahl der Schnittkanten mindestens $\frac{1}{2}|E|$ ist.*

Wähle eine Partition zufällig, indem jeder Knoten mit Wahrscheinlichkeit $\frac{1}{2}$ der Menge U zugeschlagen wird.

X_e Indikatorzufallsvariable dafür, dass e eine Schnittkante ist.

$$\mathbf{E}[X_e] = \tfrac{1}{2}$$

$$X = \sum_{e \in E} X_e$$

Wegen der Linearität des Erwartungswertes ist

$$\mathbf{E}[X] = \tfrac{1}{2}|E|$$

Also muss es eine Partition geben mit mindestens $\frac{1}{2}|E|$ Schnittkanten.

Schubfachprinzip

Seien A und B endliche Mengen und sei $|A| > |B|$. Dann gibt es keine injektive Funktion von A nach B.

Satz: *Sei $G = (V,E)$ ein gerichteter Graph mit n Knoten. Dann enthält G einen Kreis genau dann wenn G einen Pfad der Länge mindestens n enthält.*

„Beweise“ ohne Worte

Satz: [Pythagoras]
Im rechtwinkligen Dreieck ist die Summe der Kathetenquadrate gleich dem Hypothenusenquadrat.