Aussagen

Aussagen sind Sätze die wahr oder falsch sind.

p	q	$p \wedge q$	$p \lor q$	$\neg q$	$p \rightarrow q$ w	$p \leftrightarrow q$
f	f	f	f	w	w	w
f	w	f	w	w	w	f
w	f	f	w	f	f	f
w	w	w	w	f	w	w

Tautologie Wahrheitswerteverlauf konstant w

Kontradiktion Wahrheitswerteverlauf konstant f

Äquivalenz wenn $p \leftrightarrow$ Tautologie ist. $p \equiv q$

Disjunkt Zwei Mengen $X \cap Y = \emptyset$

Atom die bzgl \leq minimalen Elemente von B/\perp

Mengen

"Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens" Cantor Von jedem Objekt steht fest, ob es zur Menge gehört oder nicht.

Wunsch 0 $x \in A : \neg(x = x) = \emptyset$ die leere Menge

Wunsch 1 " $x \in y$ " x ein Element von y oder nicht.

Wunsch 2 $B = x \in A : p(x)wahr$ B aus wahren p(x) aus A

Wunsch 3 $x = y : \leftrightarrow \forall z : (z \in x \leftrightarrow z \in y).$

Wunsch 4 $y : \leftrightarrow \forall z : (z \in x \to z \in y)[x \subseteq y]$

Teilmengen A Teilmenge von B $\leftrightarrow \forall x: (x \in A \to x \in B) :\Rightarrow A \subseteq B$ A Obermenge von B $\leftrightarrow \forall x: (x \in B \to x \in A) :\Rightarrow A \supseteq B$ Folglich $A = B \leftrightarrow A \subseteq B \land B \subseteq A$ Schnittmenge von A und B: $A \cap B = x: x \in A \land x \in B$ Vereinigungsmenge von A und B: $A \cup B = x: x \in A \lor x \in B$ Seien A,B Mengen, dann sei $A/B := x \in A : x \notin B = A \triangle B$

Relationen

Eine Relation von Mengen A nach B ist eine Teilmenge R von AxB. $(x, y) \in R$: x steht in einer Relation R zu y; auch xRy

binäre Relation

- All relation $R := AxA \subseteq AxA$
- Nullrelation $R := \emptyset \subseteq AxA$
- Gleichheitsrelation R := (x, y)...x = y
- $A = R; R := ((x, y) \in \mathbb{R}x\mathbb{R}, x \le y)$
- $A = \mathbb{Z}; R := \{(x,y) \in \mathbb{Z}x\mathbb{Z} : x \text{ ist Teiler von y} \}$ kurz: x—y

Eigenschaften von Relationen Sei $R \in AxA$ binäre Relation auf A

- Reflexiv \leftrightarrow xRx $\forall x \in A$
- symmetrisch \leftrightarrow xRy \rightarrow yRx
- Antisymmetrisch \leftrightarrow xRy $\land yRx \rightarrow x = y$
- $\bullet \ \ {\rm Transitiv} \ \leftrightarrow \ {\rm xRy} \ \land \ {\rm yRz} \ \rightarrow \ {\rm xRz}$
- totale Relation \leftrightarrow xRy \lor yRx $\forall x, y \in A$

R heißt:

- Äquivalenz
relation \leftrightarrow R reflexiv, symmetrisch und transitiv
- Ordnung \leftrightarrow R reflexiv, antisymmetrisch und transitiv
- \bullet Totalordnung \leftrightarrow R Ordnung und total
- Quasiordnung \leftrightarrow R reflexiv und transitiv

Äqivalenzrelation $\sim \text{Sei } C_{\wp}(A)$. C heißt Partition/Klasse von A, falls gilt:

- $\bigcup C = A$ d.h. jedes $x \in A$ liegt in (min) einem $y \in C$
- $\emptyset \not\in C$ d.h. jedes $y \in C$ enthält (min) ein Element von A
- $x \cap y = \emptyset$ f.a. $x \notin y$ aus C

Ein Graph G=(V,E) ist ein Paar bestehend aus einer Menge V und $E\subseteq (x,y:x\neq y \text{ aus V})$. Zu $a,b\in V$ heißt eine Folge $P=x_1,...,x_n$ von paarweise verschiedenen Ebenen mit $a=x_0,b=x_j;x_{j-1},x_i\in Ea*i\in b*j$ ein a,b-Weg der Länge l oder Weg a nach b. Durch $a\sim b$ gibt es einen a,b-Weg in G, wird eine Äquivalenzrelation auf V definiert, denn:

- " \sim reflexiv": es ist $x \sim x$, denn P = x ist ein x,x-Weg in G
- " \sim symmetrisch": aus $x \sim y$ folgt, es gibt einen x,y-Weg \rightarrow es gibt einen y,x-Weg $y \sim x$
- " \sim transitiv": aus $x \sim y$ und $y \sim x$ folgt, es gibt einen x,y-Weg und einen y,x-Weg

(Halb) Ordnungen Sei leq eine Ordnung auf X. Sei $A \subseteq X, b \in X$

- b minimal in $A \leftrightarrow b \in A$ und $(c \le b \to c = bf.a.c \in A)$
- b maximal in $A \leftrightarrow b \in A$ und $(b < c \rightarrow b = cf.a.c \in A)$
- b kleinstes Element in A \leftrightarrow b \in A und (b < cf.a.c \in A)
- b größtes Element in $A \leftrightarrow b \in A$ und $(c \leq bf.a.c \in A)$
- b untere Schranke von A \leftrightarrow b < cf.a.c \in A
- b obere Schranke von A \leftrightarrow c \leq bf.a.c \in A
- b kleinste obere Schranke von A \leftrightarrow b ist kleinstes Element von ($b' \in X$: b' obere Schranke von A) auch Supremum von A: $\vee A = b$
- b größte untere Schranke von A \leftrightarrow b ist das größte Element von ($b' \in X$: b' untere Schranke von A) auch Infinum von A; $\land A = b$

kleinstes und größtes Element sind jew. eindeutig bestimmt (falls existent)

Wohlordnungssatz Jede Menge lässt sich durch eine Ordnung so ordnen, dass jede nichtleere Teilmenge von X darin ein kleinstes Element ist.

Induktion

Menge M heißt induktiv : $\leftrightarrow \emptyset \in M \land \forall X \in M, \{X^+ \in M\}$. Ist O eine Menge von induktiven Mengen, $O \pm O$ dann ist auch $\bigcap O$ induktiv. Insbesondere ist der Durchschnitt zweier induktiver Mengen induktiv.

Induktion I Sei $p(n) \in \mathbb{N}$. Gelte p(0) und $p(n) \to p(n^+)$ f.a. $n \in \mathbb{N}$ dann ist p(n) wahr f.a. $n \in \mathbb{N}$.

Induktion II Sei $p(n) \in \mathbb{N}$, gelte $\{ \forall x < n : p(x) \} \to p(n)$ f.a. $n \in \mathbb{N}$. Damit ist p(n) wahr für alle $n \in \mathbb{N}$.

Funktionen

Eine Relation $f\subseteq AxB$ heißt Funktion $f:A\to B$ ("A nach B") falls es zu jedem $x\in A$ genau ein $y\in B$ mit $(x,y)\in f$ gibt. Satz: $f:A\to B, g:A\to B$, dann gilt $f=g\leftrightarrow f(x)=g(x)$. Sei $f:A\to B$ Funktion, f heißt:

- injektiv \leftrightarrow jedes y aus B hat höchstens ein Urbild $(f(x)=f(y)\to x=y)$
- subjektiv \leftrightarrow jedes y aus B hat wenigstens ein Urbild f(x) = y
- bijektiv ↔ jedes y aus B hat genau ein Urbild; injektiv und surjektiv

Ist $f: A \to B$ bijektiv, dann ist auch $f^{-1} \subseteq BxA$ bijektiv, die Umkehrfunktion von f. Mit $f: A \to B$, $g: B \to C$, wird durch $(g \circ f)(x) := g(f(x))$ eine Funktion $g \circ f: A \to C$ definiert.

Satz: ist $f:A\to B$ bijektiv, so ist f^{-1} eine Funktion B nach A. Mengen A,B, heißen gleichmächtig $(|A|=|B|\equiv A\cong B)$ falls Bijektion von A nach B. Eine Menge A heißt endlich, wenn sie gleichmächtig zu einer natürlichen Zahl ist; sonst heißt A unendlich. Eine Menge A heißt Deckend-unendlich, falls es eine Injektion $f:A\to B$ gibt die nicht surjektiv ist. A heißt höchstens so mächtig wie B, falls es eine Injektion von A nach B gibt: $|A|\leq |B|$ bzw $A\preceq B$ (Quasiordnung).

Für zwei Mengen A,B gilt $|A| \leq |B|$ oder $|B| \leq |A|$. Eine Relation f heißt partielle Bijektion (oder Matching), falls es Teilmengen $A' \subseteq A$ und $B' \subseteq B$ gibt sodass f eine Bijektion von A' nach B' gibt.

Kontinuitätshypothese Aus $|\mathbb{N}| \leq |A| \leq |\mathbb{R}|$ folgt $|A| = |\mathbb{N}|$ oder $|A| = |\mathbb{R}|$ (keine Zwischengrößen).

Gruppen, Ringe, Körper

Eine Operation auf eine Menge A ist eine Funktion $f:AxA \to A$; schreibweise xfy. Eine Menge G mit einer Operation \circ auf G heißt Gruppe, falls gilt:

- $a \circ (b \circ c) = (a \circ b) \circ c$ freie Auswertungsfolge
- es gibt ein neutrales Element $e \in G$ mit $a \circ e = a$ und $e \circ a = a$ f.a. $a \in G$
- $\forall a \in G \exists b \in G : \{a \circ b = e\} \lor \{b \circ a = e\}; b = a^{-1}$

kommutativ/abelsch, falls neben 1.,2. und 3. außerdem gilt:

• $a \circ b = b \circ a$ f.a. $a, b \in G$

Eine Bijektion von X nach X heißt Permutation von X. (S_X, \circ) ist eine Gruppe.

Zwei Gruppen (G, \circ_G) und (H, \circ_H) heißen isomorph, falls es einen Isomorphismus $(G, \circ_G) \cong (H, \circ_H)$ von (G, \circ_G) nach (H, \circ_H) gibt.

Addition von \mathbb{N} +: $\mathbb{N}x\mathbb{N} \to \mathbb{N}$ wird definiert durch:

- m+0 := m f.a. $m \in \mathbb{N}$ (0 ist neutral)
- m+n sei schon definiert f.a. $m \in \mathbb{N}$ und $n \in \mathbb{N}$
- $m + n^+ := (m + n)^+$ f.a. $m, n \in \mathbb{N}$

Multiplikation $* : \mathbb{N}x\mathbb{N} \to \mathbb{N}$ wird definiert durch:

- m * 0 := 0 f.a. $m \in \mathbb{N}$
- $m * n^+ = m * n + m$ f.a. $n \in \mathbb{N}$

ganze Zahlen \mathbb{Z} Durch $(a,b) \sim (c,d) \leftrightarrow a+d=b+c$ wird eine Äquivalenzrelation auf $\mathbb{N}x\mathbb{N}$ definiert. Die Äquivalenzklassen bzgl \sim heißen ganze Zahlen (Bezeichnung \mathbb{Z} . Wir definieren Operationen +, * auf \mathbb{Z} durch:

- $[(a,b)]_{/\sim} + [(c,d)]_{/\sim} = [(a+c,b+d)]_{/\sim}$
- $\bullet \ \ [(a,b)]_{/\sim} * [(c,d)]_{/\sim} = [(ac+bd,ad+bc)]_{/\sim}$

Satz: \mathbb{Z} ist eine abelsche Gruppe (+ assoziativ, enthält neutrales Element, additiv Invers).

Ein Ring R ist eine Menge mit zwei Operationen $+, *: \mathbb{R}x\mathbb{R} \to \mathbb{R}$ mit:

- a + (b + c) = (a + b) + c f.a. $a, b, c \in \mathbb{R}$
- Es gibt ein neutrales Element $O \in \mathbb{R}$ mit O + a = a + O = O f.a. $a \in \mathbb{R}$
- zu jedem $a \in \mathbb{R}$ gibt es ein $-a \in \mathbb{R}$ mit a + (-a) = -a + a = 0
- a+b=b+a f.a. $a,b\in\mathbb{R}$
- a * (b * c) = (a * b) * c f.a. $a, b, c \in \mathbb{R}$
- a * (b + c) = a * b + a * c f.a. $a, b, c \in \mathbb{R}$

R heißt Ring mit 1, falls:

• es gibt ein $1 \in \mathbb{R}$ mit a * 1 = 1 * a = a f.a. $a \in \mathbb{R}$

R heißt kommutativ, falls:

• a * b = b * a f.a. $a, b \in \mathbb{R}$

Ein kommutativer Ring mit $1 \neq O$ heißt Körper, falls:

- zu jedem $a \in \mathbb{R}$ gibt es ein $a^{-1} \in \mathbb{R}$ mit $a * a^{-1} = 1$
- Ist \mathbb{R} ein Körper, so ist $\mathbb{R}^* = \mathbb{R}/(0)$ mit * eine abelsche Gruppe.
- \mathbb{Z} mit + und * ist ein kommutativer Ring mit $1 \neq 0$ aber kein Körper
- $\mathbb{Q}, \mathbb{C}, \mathbb{R}$ mit + und * ist ein Körper

Zerlegen in primäre Elemente Jede ganze Zahl n > 0 lässt sich bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen darstellen.

Konstruktion von rationalen Zahlen aus \mathbb{Z} Sei $M = \mathbb{Z}x(\mathbb{Z}/0)$ die Menge von Brüchen. Durch $(a,b) \sim (c,d) \leftrightarrow ad = bc$ wird Äquivalenzrelation auf M durchgeführt. Definiere Operationen +,* auf \mathbb{Q} wie folgt:

- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{b*d}$ (wohldefiniert)
- \bullet $\frac{a}{b} * \frac{c}{d} = \frac{a*c}{b*d}$

Satz: ℚ mit +,* ist ein Körper.

Ring der formalen Potenzreihe Sei k ein Körper. Eine Folge $(a_0,a_1,...,a:n) \in K^{\mathbb{N}}$ mit Einträgen aus K heißt formale Potenzreihe K[[x]]. Die Menge aller Polynome wird mit K[x] bezeichnet. K[[x]] wird mit +,* zu einem kommutativen Ring mit $1 \neq 0$

- $+: (a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$
- *: $(a_0, a_1, ...) + (b_0, b_1, ...) = (c_0, c_1, ...)$ mit $c_K = \sum_{i=a}^k a_i * b_{k-i}$

B mit $\vee, \wedge, \bar{}$ seien boolesche Algebren. Sie heißen isomorph, falls es einen Isomorphismus von B nach \dot{B} gibt, d.h. eine Bijektion $\phi: B \to \dot{B}$ mit:

- $\phi(a \vee b) = \phi(a)\dot{\vee}\phi(b)$
- $\phi(a \wedge b) = \phi(a)\dot{\wedge}\phi(b)$
- $\phi(\bar{a}) = \phi(\bar{a})$

Lemma: Sei B mit \vee , \wedge , eine boolesche Algebra, dann gilt:

- $a \lor T = T$ f.a. $a \in B$
- $a \land \bot = \bot$ f.a. $a \in B$
- $a \lor b$ ist obere Schranke von a,b, d.h. $a \le a \lor b,$ dann $a \lor (a \lor b) = a \lor b$
- $a \lor b$ ist kleinste obere Schranke, d.h. $a \le z$ und $b \le z$ folgt $a \lor b \le z$

Diskrete Wahrscheinlichkeitsräume

Ein Wahrscheinlichkeitsraum ist ein Paar (Ω,p) bestehend aus einer endlichen Menge Ω und einer Funktion $p:\Omega \to [0,1] \in \mathbb{R}$ mit $\sum_{\omega \in \Omega} p(\omega) = 1$. Jeder derartige p heißt Verteilung auf Ω . Die Elemente aus Ω heißen Elementarereignis, eine Teilmenge A von Ω heißt ein Ereignis; seine Wahrscheinlichkeit ist definiert durch $p(A) := \sum_{\omega inA} p(\omega)$. $A = \emptyset$ und jede andere Menge $A \subseteq \Omega$ mit p(A) = 0 heißt unmöglich (unmögliches Ereignis). $A = \Omega$ und jede andere Menge $A \subseteq \Omega$ mit p(A) = 1 heißt sicher (sicheres Ereignis). Es gilt für Ereignisse $A, B, A_1, ..., A_k$:

- $A \subseteq B \to p(A) \le p(B)$
- $p(A \cup B) \rightarrow p(A) + p(B) p(A \cap B)$
- disjunkt $(A_i \cap A_J = \emptyset \text{ für } i \neq j)$ so gilt $p(A_1 \cup ... \cup A_k) = p(A_1) + ... + p(A_k)$
- $p(\Omega/A) :=$ Gegenereignis von A = 1 p(A)
- $p(A_1, ..., A_k) \le p(A_1) + ... + p(A_k)$

 (Ω, p) heißt Produktraum von $(\Omega_1, p_1), \dots, A, B \in \Omega$ heißen (stochastisch) unabhängig, falls $p(A \cap B) = p(A) * p(B)$.

Bedingte Wahrscheinlichkeiten $B \subseteq \Omega$ ("bedingtes Ereignis") mit p(B) > 0, dann ist

 $p_B:B\to [0,1]; p_B(\omega)=\frac{p(\omega)}{p(B)}$ eine Verteilung auf B. Für $A\subseteq \Omega$ gilt

 $\begin{array}{l} - G(A \cap B) = \sum p_B(\omega) = \sum \frac{p(\omega)}{p(B)} = \frac{p(A \cap B)}{p(B)} := p(A|B) \\ \text{bedingte Wahrscheinlichkeit von A unter B.} \\ p(A|B) = \frac{p(B|A)*p(A)}{p(B)} \end{array}$

Erwartung, Varianz, Covarianz Erwartungswert $E(X) = \sum_{\omega \in \Omega} X(\omega) p(\omega)$ Linearität von E: E(x+y) = E(x) + E(y) und $E(\alpha x) = \alpha E(x)$. Varianz von X: $Var(X) = E((X^2) - E(X))^2$) Covarianz: Cov(X,Y) = E((X-E(X))*(Y-E(Y))) Verschiebungssatz: Cov(X,Y) = E(X*Y) - E(X)*E(Y) $Var(X) = Cov(X,X) = E(X*X) - E(X)*E(Y) - (E(X))^2$ Sind X,Y stochastisch unabhängig ZVA, so ist E(X)*E(Y) = E(X*Y); folglich Cov(X,Y) = 0 Bernoulliverteilt falls P(X=1) = P und P(X=0) = 1 - P,

 $\begin{array}{l} \textbf{Binominalkoeffizienten} \quad \text{N sei Menge, dann ist} \\ \binom{N}{k} := (x \subseteq N : \text{x hat genau k Elemente} \; (|x| = k)) \; \text{für } k \in \mathbb{N}. \\ \binom{N}{0} := (\emptyset), \; \binom{N}{n} = N \to \binom{n}{0} = \binom{n}{n} = 1 \; \binom{n}{0} = 1, \\ \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} = \frac{n!}{k!(n-k)!} \end{array}$

 $p \in [0,1]$. $E(X) = \sum x * p(X = x) = 1 * p(X = 1) = p$

Hypergeometrische Verteilung Beispiel: Urne mit zwei Sorten Kugeln; N Gesamtzahl der Kugeln, M Gesamtzahl Kugeln Sorte 1, N-M Gesamtzahl Kugeln Sorte 2, $n \leq N$ Anzahl Elemente einer Stichprobe. X Anzahl der Kugeln Sorte 1 in einer zufälligen n-elementigen Stichprobe.

$$p(X = k) = \frac{\binom{M}{k} \binom{N-M}{n-k}}{\binom{N}{n}}$$

$$E(X) = \sum_{x=0}^{M} \frac{\binom{M}{k} \binom{N-M}{n-k}}{\binom{N}{n}} = \dots = n * \frac{M}{N}$$
$$Var(X) = E(X^2) - E(X)^2 = n * \frac{M}{N} (1 - \frac{M}{N}) \binom{N-n}{N-1}$$

Elementare Graphentheorie

G=(V,E) heißt Graph mit Eckenmenge V(G)=V und Kantenmenge $E(G)=E\subseteq x,y:x\neq y\in V$. Für $(a,b)\in V(G)$ heißt $d_G(a,b)=min(l:$ es gibt einen a,b-Weg der Länge l) Abstand von a nach b. G heißt zusammenhängend, wenn G höchstens eine Komponente besitzt.

- $d_G(x,y) = 0 \leftrightarrow x = y$ f.a. $x,y \in V(G)$
- $d_G(x,y) = d_G(y,x)$ f.a. $x,y \in V(F)$
- $d_G(x,z) \le d_G(x,y) + d_G(y,z)$) f.a. $x, y, z \in V(G)$

< ist Ordnung, denn:

- *G* < *G*
- $H \le G \land G \le H \to H = G$
- $H < G \land G = L \rightarrow H < L$

Ein Teilgraph H des Graphen G heißt aufspannend, falls V(H) = V(G). Weiter $N_G(x) := x \in V(G) : xy \in E(G)$ die

Menge der nachbarn von x in G. Hier gilt: $|N_G(x) = d_G(x)|$. In jedem Graph G gilt $\sum_{x \in V(G)} d_G(x) = 2|E(G)|$. Der Durchschnittsgrad von G ist somit $d(\bar{G}) = \frac{1}{|V(G)|} \sum d_G(x) = \frac{2|E(G)|}{|V(G)|}$. Ein Graph ist ein Baum wenn "G ist minimal zusammenhängend und kreisfrei"

- G ist kreisfrei und zusammenhängend
- G kreisfrei und |E(G)| = |V(G)| 1
- G zusammenhängend und |E(G)| = |V(G)| 1

Breitensuchbaum von G falls $d_F(z,x)=d_G(z,x)$ f.a. $z\in V(G)$. Tiefensuchbaum von G falls für jede Kante zy gilt: z liegt auf dem y,x-Weg in T oder y liegt auf dem z,t-Weg in T. Satz: Sei G zusammenhängender Graph $x\in V(G)$. (X) sind $x_0,...,x_{e-1}$ schon gewählt und gibt es ein $+\in (0,...,e-1)$ so, dass x_+ einen Nachbarn y in V(G) $(x_0,...,x_{e-1})$, so setze $x_e=y$ und f(e):=t; iteriere mit e+1 statt e. Dann ist $T:=(x_0,...,x_e,x_j*x_{f(j)}:j\in 1,...,e)$ ein Spannbaum

- $\bullet \ \ f(e)$ wird in + stets größtmöglich gewählt, so ist T ein Tiefensuchbaum

Spannbäume minimaler Gewichte Sei G zuständiger Graph, $\omega: E(G) \to \mathbb{R}$; Setze $F = \emptyset$. Solange es eine Kante $e \in E(G)/F$ gibt so, dass $F \lor (e)$ kreisfrei ist, wähle e mit minimalem Gewicht $\omega(e)$, setzte $F = F \lor e$, iterieren. Das Verfahren endet mit einem Spannbaum T = G(F) minimalen Gewichts.

Das Traveling Salesman Problem Konstruiere eine Folge $x_0,...,x_m$ mit der Eigenschaft, dass jede Kante von T genau zweimal zum Übergang benutzt wird, d.h. zu $e \in E(T)$ existieren $i \neq j$ mit $e = x_i x_{i+1}$ und $e = x_j x_{j+1}$ und zu jedem k existieren $e \in E(T)$ mit $e = x_k x_{k+1}$. Das Gewicht dieser Folge sei $\sum \omega(x_i x_{i+1}) = 2\omega(T)$. Eliminiere Mehrfachnennungen in der Folge. Durch iteration erhält man einen aufspannenden Kreis mit $\omega(X) \leq 2\omega(T)$.

Färbung & bipartit Eine Funktion $f:V(G)\to C$ mit $|C|\le k$ heißt k-Färbung, falls $f(x)\ne f(y)$ für $xy\in E(G)$. Ein Graph heißt bipartit mit den Klassen A,B falls $(x\in A\land y\in B)\lor (x\in B\land y\in A)$. Mit Bipartitheit gilt G hat ein Matching von $A\leftrightarrow |N_G(X)|\le |X|$ für alle $X\subseteq A$.