Aussagen

Aussagen sind Sätze die wahr oder falsch sind, d.h. der Wahrheitswert ist wahr oder falsch.

Verknüpfungen von Aussagen Seien p und q Aussagen, dass sind folgende Sätze auch Aussagen - $p \wedge q$ "und" - $p \vee q$ "oder" - $\neg p$ "nicht" - $p \rightarrow q$ "impliziert" - $p \leftrightarrow q$ "genau dann wenn"

Wahrheitswerteverlauf — p — q — $p \wedge q$ — $p \vee q$ — $\neg q$ — $p \rightarrow q$ — $p \leftrightarrow q$ — — — — — — — — — — — — — — — — — — 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 —

Aussagenlogische Variablen Variable die den Wert w oder f annimmt

Aussagenlogische Formel Verknüpfung aussagenloser Variablen nach obrigen Muster

Belegung Zuordnung von w/f an jede Variable einer aussagenlogischer Formel

Wahrheitswerteverlauf Wahrheitswert der Aussagenformel in Abhängigkeit von der Belegung der Variable

Tautologie Formel deren Wahrheitswerteverlauf konstant w ist

Kontradiktion Formel deren Wahrheitswerteverlauf konstant f ist

Kontraposition $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow p)$ ist eine Tautologie

Modus Potens $(p \vee (p \rightarrow q)) \rightarrow q$ ist eine Tautologie

Äquivalenz Zwei Formeln p,q sind äquivalent (bzw logisch äquivalent) wenn $p \leftrightarrow$ Tautologie ist. Man schreibt $p \equiv q$. Die Formel p impliziert die Formel q, wenn $p \rightarrow q$ eine Tautologie ist

Regeln

- $p \wedge q \equiv q \wedge p$ (Kommutativ)
- $p \vee q \equiv q \vee p$ (Kommutativ)
- $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ (Assoziativ)
- $p \vee (q \vee r) \equiv (p \vee q) \vee$ (Assoziativ)
- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ (Distributiv)
- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (Distributiv)
- $\neg(\neg q) \equiv q$ (Doppelte Verneinung)
- $\neg(p \wedge q) \equiv (\neg p) \wedge (\neg q)$ (de Morgansche)

Aussagenformen in einer Variable x aus dem Universum U heißen Prädikate von U. Aussagenformen in n Variablen $x_1, ..., x_n$ aus dem Universum U heißen "n-stellige Prädikate" von U.
Seien p,q Prädikate über U

- $(\forall x : (p(x) \wedge q(x))) \leftrightarrow (\forall x : p(x) \wedge \forall x : q(x))$
- $\exists x : (p(x) \vee q(x)) \leftrightarrow (\exists x : p(x) \vee \exists x : q(x))$
- $\neg(\forall x : p(x)) \leftrightarrow \exists x : \neg p(x)$
- $\neg(\exists x : p(x)) \leftrightarrow \forall x : \neg p(x)$

Achtung: Verschiedenartige Quantoren dürfen nicht getauscht werden! gleichartige Quantoren dürfen getauscht werden

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 Es gibt eine Menge. Ist A irgendeine Menge, so ist $x \in A : \neg(x = x)$ eine Menge ohne Elemente, die sogenannte leere Menge $\emptyset$.

Wunsch 1 "$x \in y$" soll Aussagenform über dem Universum U aller Mengen sein. D.h. für je zwei Mengen x und y ist entweder x ein Element von y oder nicht. D.h. "$x \in y$" ist ein 2-stelliges Prädikat über U.

Wunsch 2 Ist p(x) ein Prädikat über U, so soll es eine Menge geben, die aus genau denjenigen Mengen x besteht, für die p(x) wahr ist. Bezeichnung $x : p(x)"ist - wahr"$. Danach gäbe es eine Menge M, die aus genau denjenigen Mengen x mit $x \notin x$ besteht: $M = x : x \notin x$.

Wunsch 2' Ist A eine Menge und p(x) ein Prädikat über U, dann gilt es eine Menge B die aus genau denjenigen Mengen x aus A besteht, für die p(x) wahr ist. Bezeichnung: $B = x \in A : p(x) wahr$. Folgerung: die Gesamtheit aller Mengen ist selbst keine Menge, sonst findet man einen Widerspruch wie oben.

Wunsch 3 Zwei Mengen x,y sind genau dann gleich wenn sie diesselben Elemente enthalten. D.h. $x = y :\leftrightarrow \forall z : (z \in x \leftrightarrow z \in y)$. Somit gilt für zwei Prädikate p(x), q(x) über U und jede Menge A: $x \in A : p(x) wahr = x \in A : q(x) wahr$ genau dann, wen q(x), p(x) den gleichen Wahrheitswert für jedes x aus A haben.

Wunsch 4 Zu jeder Menge A gibt es eine Menge B, die aus genau denjenigen Mengen besteht, die Teilmengen von A sind. Dabei ist x eine Teilmenge von $y :\leftrightarrow \forall z : (z \in x \rightarrow z \in y) [x \subseteq y]$ $B = x : x \subseteq A = \wp(A)$ B heißt Potentmenge von A

Teilmengen

A Teilmenge von B $\leftrightarrow \forall x : (x \in A \rightarrow x \in B) :\Rightarrow A \subseteq B$ A Obermenge von B $\leftrightarrow \forall x : (x \in B \rightarrow x \in A) :\Rightarrow A \supseteq B$ Folglich $A = B \leftrightarrow A \subseteq B \wedge B \subseteq A$ Schnittmenge von A und B: $A \cap B = x : x \in A \wedge x \in B$ Vereinigungsmenge von A und B: $A \cup B = x : x \in A \vee x \in B$
Sei eine Menge (von Mengen) dann gibt es eine Menge die aus genau den Mengen besteht, die in jeder Menge von A enthalten sind (außer $A = \emptyset$). Ebenso gibt es Mengen die aus genau den Mengen besteht, die in wenigstens einer Menge aus A liegen. Die Existenz dieser Menge wird axiomatisch gefordert in ZFC:$UA = x : \exists z \in A : x \in z$

Seien A,B Mengen, dann sei $A/B := x \in A : x \notin B = A \triangle B$
De Moorgansche Regel: $\overline{A \cup B} = \overline{A} \cap \overline{B}$ und $\overline{A \cap B} = \overline{A} \cup \overline{B}$
Das geordnete Paar (x,y) von Mengen x,y ist definiert durch $x, x, y := x, y$ A und B Mengen: $AxB := (x, y) : x \in A \wedge y \in B$

Relationen

$A = Peter, Paul, Marry$ und
$B = C++, Basic, Lisp : R \subseteq AxB$, etwa (Peter,c++),(Paul, C++), (Marry,Lisp). Seien A,B Mengen: Eine Relation von A nach B ist eine Teilmenge R von AxB. $(x, y) \in R$: x steht in einer Relation R zu y; auch xRy Ist A=B, so heißt R auch binäre Relation auf A

binäre Relation

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

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

- Reflexiv $\leftrightarrow$ xRx $\forall x \in A$
- Symetrisch $\leftrightarrow xRy \rightarrow yRx$
- Antisymetrisch $\leftrightarrow xRy \wedge yRx \rightarrow x = y$
- Transitiv $\leftrightarrow xRy \wedge yRz \rightarrow xRz$
- totale Relation $\leftrightarrow xRy \vee yRx \forall x, y \in A$
- R heißt Äquivalenzrelation $\leftrightarrow$ R reflexiv, symetrisch und transitiv
- R heißt Ordnung $\leftrightarrow$ R reflexiv, antisymetrisch und transitiv
- R heißt Totalordnung $\leftrightarrow$ R Ordnung und total
- R heißt Quasiordnung $\leftrightarrow$ R reflexiv und transitiv

Äqivalenzrelation Sei A Menge, $C\wp(A)$ Menge von teilmengen von A. C heißt Partition von A, falls gilt: 1. $UC = A$ d.h. jedes $x \in A$ liegt in (wenigstens) einem $y \in C$ 2. $\emptyset \notin C$ d.h. jedes $y \in C$ enthält (wenigstens) ein Element von A 3. $X \cap Y = \emptyset$ f.a. $X \notin Y$ aus C
Zwei Mengen $X \cap Y = \emptyset$ heißten disjunkt. Satz: Sei $\sim$ Äquivalenzrelation auf A. Für $x \in A$ betrachtet $[x]_{/\sim} := y \in A : y \sim x$. Dann ist $[x]_{/\sim} : x \in A = C_{/\sim}$ Partition von A. Die Elemente $[x]_{/\sim}$ von $C_{/\sim}$ heißen Äquivalenzklassen. Die Elemente von C heißten Teile, Klassen oder Partitionen. Somit ist $\equiv (modm)$ eine Äquivalenzrelation. Ihre Äquivalenzklassen heißen Restklassen mod m
Ein Graph $G = (V, E)$ ist ein Paar bestehend aus einer Menge V und $E \subseteq (x, y : x \neq y$ 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
- "$\sim$ symetrisch": 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

Die Äquivalenzklassen von $\sim_G$ erzeugen die Zusammenhangskomponenten von G
Satz: Sei C eine Partition von A, dann wird durch $x \sim_G y \leftrightarrow$ es gibt ein $X \in C$ mit $x, y \in X$ eine Äquivalenzrelation auf A definiert.

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

- b minimal in A $\leftrightarrow b \in A$ und $(c \leq b \rightarrow c = bf.a.c \in A)$
- b maximal in A $\leftrightarrow b \in A$ und $(b \leq c \rightarrow b = cf.a.c \in A)$
- b kleinstes Element in A $\leftrightarrow b \in A$ und $(b \leq cf.a.c \in A)$
- b größtes Element in A $\leftrightarrow b \in A$ und $(c \leq bf.a.c \in A)$
- b untere Schranke von A $\leftrightarrow b \leq cf.a.c \in A$
- 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 Infinium von A; $\wedge A = b$

kleinstes und größtes Element sind jew. eindeutig bestimmt (falls existent)
Satz: Sei X Menge. $\subseteq$ ist Ordnung auf $\wp(X)$. Ist $O \subseteq \wp(X)$, so ist $supO = \bigcup O$ und $infO = \bigcap O$
Satz: Die Teilbarkeitsrelation — ist Ordnung auf den natürlichen Zahlen $\mathbb{N}$. Es gibt $sup(a, b) = kgV(a, b)$ (kleinstes gemeinsames Vielfaches) und $inf(a, b) = ggT(a, b)$ (größtes gemeinsames Vielfaches)

Hesse Diagramm Darstellung einer Ordnung $\subseteq$ auf X 1. Im Fall $x \subseteq y$ zeichne x "unterhalb" von y in die Ebene 2. Gilt $x \subseteq y(x \neq y)$ und folgt aus $x \subseteq z \subseteq y$ stets $x = z$ oder $y = z$ so wird x mit y "verbunden"

Zoonsche Lemma Zu jeder Menge und für jede Ordnung $\leq$ auf X mit der Eigenschaft, dass jede nicht-leere Kette nach der beschränkt ist, gibt es ein maximales Element.

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

Induktion

X ist eine Menge, $X := X \vee X$ M Menge heißt induktiv $:\leftrightarrow \emptyset \in M \wedge \forall X \in M\ X^+ \in M$.
Ist O eine Menge von induktiven Mengen, $O \pm O$ dann ist auch $\bigcap O$ induktiv. Insbesondere ist der Durchschnitt zweier induktiver Mengen induktiv. Es gibt eine induktive Menge M: $M = \bigcap A \in \wp(M) : Ainduktiv$. Sei M' irgendeine (andere) induktive Menge $\rightarrow M \cap M'$ ist induktive Teilmenge von M. $\mathbb{N}_M$ ist der Durchschnitt über alle induktiven Teilmengen von M $\mathbb{N}_M \subseteq M \cap M' \subseteq M'$. Folglich ist $\mathbb{N}_m$ Teilmenge jeder induktiven Menge.

Satz I (Induktion I) Sei $p(n)$ ein Prädikat über $\mathbb{N}$. Gelte $p(0)$ und $p(n) \rightarrow p(n^+)$ f.a. $n \in \mathbb{N}$ dann ist $p(n)$ wahr f.a. $n \in \mathbb{N}$. Schreibe $x = y :\leftrightarrow x \in y \vee x = y$

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

Funktionen

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

- f heißt injektiv $\leftrightarrow$ jedes y aus B hat höchstens ein Urbild
- f heißt subjektiv $\leftrightarrow$ jedes y aus B hat wenigstens ein Urbild
- f heißt bijektiv $\leftrightarrow$ jedes y aus B hat genau ein Urbild

Ist $f : A \rightarrow B$ bijektive Funktion, dann ist auch $f^{-1} \subseteq BxA$ bijektiv von B nach A, die Umkehrfunktion von f. Man nennt f dann Injektion, Surjektion bzw Bijektion

- f injektiv $\leftrightarrow (f(x) = f(y) \rightarrow x = y)$ f.a. $x, y \in A$ oder $(x \neq y \rightarrow f(x) \neq f(y))$
- f surjektiv $\leftrightarrow$ Zu jedem $x \in B$ existiert ein $x \in A$ mit $f(x) = y$
- f bijektiv $\leftrightarrow$ f injektiv und surjektiv

Sind $f : A \rightarrow B$ und $g : B \rightarrow C$ Funktionen, so wird durch $(g \circ f)(x) := g(f(x))$ eine Funktion $g \circ f : A \rightarrow C$ definiert, die sog. Konkatenation/Hintereinanderschaltung/Verkettung/Verkopplung von f und g (gesprochen "g nach f").
Satz: $f : A \rightarrow B, g : B \rightarrow C$ sind Funktionen. Sind f,g bijektiv, so ist auch $g \circ f : A \rightarrow C$ bijektiv
Satz: ist $f : A \rightarrow B$ 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. $\cong$ ist auf jeder Menge von Mengen eine Äquivalenzrelation

- "$\cong$ reflexiv": $A \cong A$, denn $f : A \rightarrow A, f(x) = X$, ist Bijektion von A nach A
- "$\cong$ symmetrisch": Aus $A \cong B$ folgt Bijektion von A nach B $\rightarrow B \cong A$
- "$\cong$ transitiv": Aus $A \cong B$ und $B \cong C$ folgt $A \cong C$

$|A| = |A| : |A|$ ist die Kordinalität von A, d.h. die kleinste zu A gleichmächtige Ordinalzahl. Eine Ordinalzahl ist eine e-transitive Menge von e-transitiven Mengen. Eine Menge X heißt e-transitiv, wenn aus $a \in b$ und $b \in c$ stets $a \in c$ folgt. Sei $A := \mathbb{N}$ und $B = 0, 2, 4, ... = n \in \mathbb{N} : 2|n$, dann sind A und B gleichmächtig, denn $f : A \rightarrow B, f(x) = 2x$ ist 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 $f : A \rightarrow B$ gibt die nicht surjektiv ist.
Satz: A unendlich $\leftrightarrow$ A deckend-unendlich A,B sind Mengen. A heißt höchstens so mächtig wie B, falls es eine Injektion von A nach B gibt. $|A| \leq |B|$ bzw $A \preceq B$. $\preceq$ ist Quasiordnung auf jeder Menge von Mengen.

- "$\preceq$ reflexiv": Injektion von A nach A
- "$\preceq$ transitiv": $A \preceq B$ und $B \preceq C$ folgt Injektion $f : A \rightarrow B$ und $g : B \rightarrow C$. Verkopplung $g \circ f \rightarrow A \preceq C$

Satz (Vergleichbarkeitssatz): Für zwei Mengen A,B gilt $|A| \leq |B|$ oder $|B| \leq |A|$. Eine Relation f von A nach B 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.
Sei M die Menge aller Matchings von A nach B und wie jede Menge durch $\subseteq$ geordnet. Sei $K \subseteq M$ eine Kette von Matchings. K besitzt eine obere Schranke $(\bigcup K)$ in M. Seien $(x, y); (x', y')$ zwei Zuordnungspfeile aus $\bigcup K$, zeige $x \neq x'$ und $y \neq y'$ dann folgt Matching. Jede Kette von Matchings benutzt eine obere Schranke, die ebenfalls ein Matching ist $\rightarrow$ es gibt ein maximales Matching von A nach B, etwa h. Im Fall $(x \in A, y \in B$ mit $(x, y) \in h)$ ist h eine Injektion von A nach B, d.h. $|A| \subseteq |B|$ andernfalls $y \in B, x \in A$ mit $x, y \in h$ ist h^{-1} eine Injektion von B nach A, d.h. $|B| \subseteq |A|$.
Satz (Cantor/Schröder/Bernstein): Für zwei Mengen A,B gilt: Aus $|A| \subseteq |B|$ und $|B| \subseteq |A|$ folgt $|A| = |B|$.
Satz (Cantor): Für jede Menge X gilt: $|X| \leq \wp(X)$ und $|X| \neq |\wp(X)|$. Z.B. ist $|\mathbb{N}| < |\mathbb{R}|$; zu $|\mathbb{N}|$ gleichmächtige Mengen nennt man abzählbar; unendliche nicht-abzählbare Mengen nennt man überzählbar.

Kontinuitätshypothese

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

Seien M,I zwei Mengen. Eine Funktion $f : I \to M$ von I nach M heißt auch Familie über der Indexmenge I auf M. Schreibweise $(m_i)_{i \in I}$ wobei $m_i = f(i)$. Familien über $I = \mathbb{N}$ heißen Folgen (bzw. unendliche Folgen). Eine (endliche) Folge ist eine Familie über einer endlichen Indexmenge I. Funktionen von $1, ..., n$ in einer Menge A ($a_q, ..., a_n \in A$) heißen n-Tupel. Für eine Mengenfamilie $(A_i)_{i \in A}$ sei ihr Produkt durch $\prod A_i = (f :$ Funktion von I nach $\bigcup A_i$ mit $f(i) \in A_i$ f.a. $i \in I)$. Ist allgemein $A_i = A$ konstant, so schreibe $\prod A_i = A^I = f : I \to R$. Bezeichnung auch $2^{\mathbb{N}}$.

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 $e \in G$ mit $a \circ e = a$ und $e \circ a = a$ f.a. $a \in G$. e heißt neutrales Element von G und ist eindeutig bestimmt
- zu jedem $a \in G$ existiert ein $b \in G$ mit $a \circ b = e$ und $b \circ a = e$; wobei e ein neutrales Element ist. b ist durch a eindeutig bestimmt, denn gäbe es noch ein $c \in G$ mit $a \circ c = e$ folgt $b = b \circ e$. Schreibweise für dieses eindeutig durch a bestimmte b: a^{-1}

Eine Gruppe G mit $\circ$ wird auch mit $(G, \circ)$ bezeichnet. Sie heißt kommutativ bzw abelsch, falls neben 1.,2. und 3. außerdem gilt:

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

Das neutrale Element aus 2. wird mit 1 bezeichnet. Im Fall der abelschen Gruppe benutzt man gerne "additive Schreibung": "+" statt "$\circ$" und "0" statt "1" (Bsp: $1 * a = a * 1 = a$). 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 von $(G, \circ_G)$ nach $(H, \circ_H)$ gibt (bzw. von G nach H). Schreibweise $(G, \circ_G) \cong (H, \circ_H)$

- "$\cong$ reflexiv": $G \cong G$, denn id_G ist ein Isomorphismus
- "$\cong$ symmetrisch": aus $G \cong G$ folgt: es existiert ein bijektiver Homomorphismus
- "$\cong$ transitiv": sei $G \cong H$ und $H \cong J \to$ es gibt einen Isomorphismus $\phi : G \to H$ und $\psi : H \to J \to \phi \circ \psi : G \to J \to$ J ist bijektiv. $\phi \circ G$ ist Homomorphismus von G nach J und bijektiv also Isomorph

Satz: Jede Gruppe $(G, \circ)$ ist zu einer Untergruppe von $(S_G, \circ)$ isomorph

Arithmetik 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 ein gutes $n \in \mathbb{N}$
- $m + n^+ := (m + n)^+$ f.a. $m, n \in \mathbb{N}$

Satz: $m + n = n + m$ f.a. $m, n \in \mathbb{N}$ (Beweis induktiv über m)
Satz: $l + (m + n) = (l + m) + n$ f.a. $l, m, n \in \mathbb{N}$ (Klammern sind neutral bzgl +)
Satz (Streichungsregel): aus $a + n = b + n$ folgt $a = b$ f.a. $a, b, n \in \mathbb{N}$

Analog: 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. $n \in \mathbb{N}$

Es gilt:

- $m * n = n * m$ f.a. $n \in \mathbb{N}$
- $m * (n * l) = (m * n) * l$ f.a. $m, n \in \mathbb{N}$
- $m * 1 = 1 * m = m$ f.a. $m \in \mathbb{N}$
- $a * n = b * n \to a = b$ f.a. $a, b \in \mathbb{N}, n \in \mathbb{N}/0$
- $a * (b + c) = a * b + a * c$ (Distributivgesetz)

Die ganzen 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 $\mathbb{Z}$, Bsp $17 = [(17, 0)]_{/\sim}$). Wir definieren Operationen +, * auf $\mathbb{Z}$ durch:

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

Zu zeigen ist: Die auf der rechten Seite definierten Klassen hängen nicht von der Wahl der "Repräsentanten" der Klassen auf der linken Seite ab (Wohldefiniert).
Formal (für +): $[(a, b)]_{/\sim} = [(a', b')]_{/\sim}$ und $[(c, d)]_{/\sim} = [(c', d')]_{/\sim}$ impliziert $[(a, b)]_{/\sim} + [(c, d)]_{/\sim} = [(a' + c', b' + d')]_{/\sim}$. Aus der Vss konstant kommt $a + b' = b + a'$ und $c + d' = c' + d$. Dann folgt $a + c + b' + d' = b + d + a' + c'$, also $(a + c, b + d) \sim (a' + c', b' + d')$.
Satz: $\mathbb{Z}$ ist eine abelsche Gruppe (+ assoziativ, enthält neutrales Element, additiv Invers). $[(a, 0)]_{/\sim}$ wird als a notiert. $-[(a, 0)]_{/\sim} = [(0, a)]_{/\sim}$ wird als -a notiert.
Anordnung: $[(a, b)]_{/\sim} \subseteq [(c, d)]_{/\sim} \leftrightarrow a + d \leq b + c$
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 $a * a^{-1} = a^{-1} * a = 1$

Bemerkung: O kann kein multiplikativ inverses haben.

- 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

Division mt Rest in $\mathbb{Z}$

Satz: Zu $a, b \in \mathbb{Z}, b \neq 0$, gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $a = q * b + r$ und $0 \leq q < |b|$ (d.h. $\mathbb{Z}$ ist ein euklidischer Ring). (Beweis über Induktion)

Zerlegen in primäre Elemente

Satz: Jede ganze Zahl $n > 0$ lässt sich bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen darstellen.
Beweis-Existenz mit Annahme: Der Satz gilt nicht, dann gibt es eine kleinste Zahl n die sich nicht als Produkt von Primzahlen schreiben lässt $\to$ n weder Primzahl noch 1 $\to n = m * l$ für $m, l > 1 \to$ m und l sind Produkte von Primzahlen $\to m * l =$ Produkt von Primzahlen.
Eindeutigkeit mit Annahme: es gibt ein $n > 0$ ohne eindeutige Primfaktorzerlegung (PFZ)$\to$ es gibt ein kleinstes $n > 0$ ohne eindeutige PFZ. Kommt eine Primzahl p in beiden Zerlegungen vor, so hat auch $\frac{n}{p}$ zwei verschiedene PFZen.
Man erhält die PFZ von $n' = (1_1 - p_1) * b$ aus den PFZen von $q_1 - p_1$ und b.. -¿ Eindeutig bestimmbar.

Arithmetik im Restklassenring in $\mathbb{Z}$

Sei $m > 1$ gegeben, $a \equiv$ b mod m $\leftrightarrow m|a - b$ def. Relation auf $\mathbb{Z}$. Die Äquivalenzklasse zu a wird mit $\bar{a}$ bezeichnet, d.h. $\bar{a} = [a]_{\text{mod m}} = x \in \mathbb{Z} : x \equiv$ a mod m, $\mathbb{Z}_m = \bar{a} : a \in \mathbb{Z}$. Sei dazu $\bar{a} \in \mathbb{Z}_m$ beliebig.
Division mit Rest $\to$ es gibt eindeutig bestimmt q,r mit $a = q * m + r$ und $0 \leq r < m \to a - r = q * m \to m|a - r \to a \equiv$ r mod m $\to \bar{a} = \bar{r}$.
Also tritt $\bar{a}$ in der Liste $\bar{0}, \bar{1}, ..., \overline{m-1}$ auf. Aus $0 \leq i < j \leq m - 1$ folgt $\bar{i} \neq \bar{j}$. In der Liste $\bar{0}, \bar{1}, ..., \overline{m-1}$ gibt es daher keine Wiederholungen $\to |\mathbb{Z}_M| = m$.
Wir definieren Operationen +,* auf $\mathbb{Z}_m$ durch $\bar{a} + \bar{b} := \overline{a + b}$ und $\bar{a} * \bar{b} := \overline{a * b}$ für $a, b \in \mathbb{Z}$. Wohldefiniert: aus $\bar{a} = \bar{a'}$ und $\bar{b} = \bar{b'}$ folgt $\overline{a + b} = \overline{a' + b'}$. Analog für Multiplikation.
Eigenschaften von $\mathbb{Z}$ mit +,* werden auf $\mathbb{Z}$ mit +,* "vererbt", z.B. Distributivgesetz.

Satz: Sei $m \geq 2$ dann ist $\mathbb{Z}_m$ mit +,* ein kommutativer Ring mit $\bar{1} \neq \bar{0}$. Genau dann ist $\mathbb{Z}_m$ sogar ein Körper, wenn m eine Primzahl ist.
Satz: Genau dann gibt es einen Körper mit n ELementen, wenn n eine Primzahl ist. D.h.. wenn $n = p^a$ ist für eine Primzahl p und $a \geq 1$.

Konstruktion von $\mathbb{Q}$ 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. Schreibweise für die Äquivalenzklassen $\frac{a}{b}$ Die Elemente von $\mathbb{Q} : \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0$ heißten rationale Zahlen. Definiere Operationen +,* auf $\mathbb{Q}$ wie folgt:

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

Satz: $\mathbb{Q}$ mit +,* ist ein Körper.
Durch $\frac{a}{b} \leq \frac{c}{d}$ wird eine totale Ordnung auf $\mathbb{Q}$ definiert.
Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$ mit Dedchin-Schnitten.

Ring der formalen Potenzreihe Sei k ein Körper (oder nur ein Ring mit 1+0). Eine Folge $(a_0, a_1, ..., a:n) \in K^{\mathbb{N}}$ mit Einträgen aus K heißt formale Potenzreihe. Die Folge (0,1,0,0,...) wird mit x bezeichnet. Statt $K^{\mathbb{N}}$ schreibt man $K[[x]]$. $(0_0, a_1, a_2, ...)$ heißt Polynom in x, falls es ein $d \in \mathbb{N}$ gibt mit $a_j = 0$ f.a. $j < n$. Die Menge aller Polynome wird mit $K[x]$ bezeichnet.
Satz: $K[[x]]$ wird mit +,* wie folgt zu einem kommutativen Ring mit $1 \neq 0$

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

Die formale Potenzreihe $(a, 0, 0, 0, ...)$ wird ebenfalls mit a bezeichnet.
Die bzgl $\leq$ minimalen Elemente von $B/\perp$ heißen Atom von B.
Satz: Sei $b \in B/\perp$ und $a_1, ..., a_k$ diejenigen Atome a mit $a \leq b$, dann ist $b = a_1 \vee a_2 \vee ... \vee a_k$.
B mit $\vee, \wedge, ^-$ und $\dot{B}$ mit $\dot{\vee}, \dot{\wedge}, \dot{^-}$ 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:

- $\phi(a \vee b) = \phi(a) \dot{\vee} \phi(b)$ f.a. $a, b \in B$
- $\phi(a \wedge b) = \phi(a) \dot{\wedge} \phi(b)$ f.a. $a, b \in B$
- $\phi(\bar{a}) = \dot{\bar{\phi(a)}}$ f.a. $a \in B$

Satz (Stone): Ist B mit $\vee, \wedge, ^-$ eine boolesche Algebra, B endlich und A die Menge ihrer Atome, so ist B isomorph zur booleschen Algebra $\wp(A)$ mit $\cap, \cup, \dot{^-}$, wobei $\dot{\bar{X}} = A/X$. Also ist in jeder Teilmenge X von A Bild eines Elements von B unter ϕ.
Satz: $\perp$, T sind durch die Bedingung 3 eindeutig bestimmt.
Satz: $\bar{a}$ ist durch die Bedingung 1,2,4 eindeutig bestimmt.
Lemma: Sei B mit $\vee, \wedge, ^-$ eine boolesche Algebra, dann gilt:

- Dominanz
  - $a \vee T = T$ f.a. $a \in B$
  - $a \wedge \perp = \perp$ f.a. $a \in B$
- Absorption
  - $a \vee (a \wedge b) = a$ f.a. $a, b \in B$
  - $a \wedge (a \vee b) = a$ f.a. $a, b \in B$
- Streichungsregel
  - $a \wedge x = b \wedge x \to a = b$ f.a. $a, b, c \in B$
  - $a \wedge \bar{x} = b \wedge \bar{x} \to a = b$ f.a. $a, b, x \in B$
- Assoziativität
  - $a \vee (b \vee c) = (a \vee b) \vee c$ f.a. $a, b, c \in B$
  - $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ f.a. $a, b, c \in B$
- De Moorgansche Regel
  - $a \bar{\vee} b = \bar{a} \wedge \bar{b}$ f.a. $a, b \in B$
  - $a \bar{\wedge} b = \bar{a} \vee \bar{b}$ f.a. $a, b \in B$

Satz: Durch $a \leq b :\leftrightarrow a \vee b = b$ wird eine Ordnung auf der booleschen Algebra B mit $\vee, \wedge, ^-$ definiert ($a \vee b = supa, b$; $a \wedge b = infa, b$)
Es gilt $a \vee b = b \to a \wedge b = a \wedge (a \vee b) = a$

- $a \vee b$ ist obere Schranke von a, b, d.h. $a \leq a \vee b$, dann $a \vee (a \vee b) = a \vee b$
- $a \vee b$ ist kleinste obere Schranke, d.h. $a \leq z$ und $b \leq z$ folgt $a \vee b \leq z$

Sind $B, \dot{B}$ isomorph, so schreibe $B \cong \dot{B}$. Daraus folgt $\dot{B} \cong B$ und aus $B \cong \dot{B}$ und $\dot{B} \cong \ddot{B}$ folgt $B \cong \ddot{B}$. Weiterhin besitzt jede boolesche Algebra mit genau n Atomen genau 2^n viele Elemente (denn sie ist isomorph zur booleschen Algebra).
Beispiel: Sei X eine endliche Menge von Variablen. Eine aussagenlogische Formel F in X ist:

- atomar: "x" mit $x \in X$ oder "f" oder "w" oder
- zusammengesetzt: $(P \vee Q), (P \wedge Q), (\neg P)$ aus den Formeln P,Q

Der Wahrheitswert von F unter der Belegung $\beta : X \to f, w$ ergibt sich wie in Kapitel 1. Bezeichnung für den Wahrheitswert von F unter $\beta : W_F(\beta)$. Es gibt $2^{|x|}$ Belegungen. Der Wahrheitswerteverlauf ist die so definierte Funktion $W_F : f, w^X \to f, w$. Folglich gibt es $2^{2^{|x|}}$ verschiedene Wahrheitswertverläufe für logische Formeln. Formeln F, F' heißen äquivalent, falls $W_F = W_{F'} \to$ es gibt $2^{2^{|x|}}$ verschiedene Äquivalenzklassen aussagenlogischer Formeln in X. Die Äquivalenzklassen werden mit $[F]_{/\equiv}$ bezeichnet.
Sei $B := ([F]_{/\equiv}$: F aussagenlogische Formel in X) die Menge aller Äquivalenzklassen aussagenlogischer Formeln in X.

- $[P]_{/\equiv} \vee [Q]_{/\equiv} = [(P \vee Q)]_{/\equiv}$
- $[P]_{/\equiv} \wedge [Q]_{/\equiv} = [(P \wedge Q)]_{/\equiv}$
- $\bar{[P]}_{/\equiv} = [-(P)]_{/\equiv}$

liefert die boolesche Algebra auf B

- $\perp = [f]_{/\equiv}$ = Menge der Kontradiktionen von X
- $T = [w]_{/\equiv}$ = Menge der Tautologien von X

Ordnung $\leq$ auf B: $[P]_{/\equiv} \leq [Q]_{/\equiv} \leftrightarrow [P]_{/\equiv} \wedge [Q]_{/\equiv} \to$ Die Atome von B sind genau die Klassen zu Formel P mit $W_p^{-1}(w) = 1$. Kanonische Repräsentanten für diese Atome sind die Min-Terme. Zu jeder aussagenlogischen Formel f kann man die Atome $[P]_{/\equiv}$ mit $[P]_{/\equiv} \leq [F]_{/\equiv}$ betrachten, wobei P Min-Terme sind.
Satz: Jede Formel ist äquivalent zu einer Formel in DNF (disjunkte normal Form)
Coatome der booleschen Algebra B mit $\vee, \wedge, ^-$:= Atome der dualen booleschen Algebra B mit $\vee, \wedge, ^-$
Ist $b \in B$ und $a_1, ..., a_k$ die Coatome a mit $b \leq a$ so gibt $b = a_1 \wedge ... \wedge a_k$. Max-Terme sind "$x_1 \vee ... \vee x_k$" und alle j die durch Ersetzung einiger x_j durch $\neg x_j$ daraus hervorgehen und sind die kanonische Repräsentation der Coatome von B.
Satz: Jede aussagenlogische Formel ist äquivalent zu einer Formel in konjunktiver Normalform (KNF), d.h. zu einer Formel $P_1 \wedge ... \wedge P_n$, worin die P_j Max-Terme sind.

Diskrete Wahrscheinlichkeitsräume

Ein (endlicher, diskreter) 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 (Wahrscheinlichkeits-) Verteilung auf Ω. Die Elemente aus Ω heißen Elementarereignis, eine Teilmenge A von Ω heißt ein Ereignis; seine Wahrscheinlichkeit ist definiert durch $p(A) := \sum_{\omega in A} p(\omega)$. $A = \emptyset$ 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 $A, B, A_1, ..., A_k$:

- $A \subseteq B \to p(A) \leq p(B)$ denn $p(A) = \sum p(\omega) \leq \sum p(\omega) = p(B)$
- $p(A \cup B) \to p(A) + p(B) - p(A \cap B)$
- Sind $A_1, ..., A_k$ paarweise disjunkt (d.h. $A_i \cap A_J = \emptyset$ für $i \neq j$) so gilt $p(A_1 \cup ... cup A_k) = p(A_1) + ... + p(A_k)$
- $p(\Omega/A) :=$ Gegenereignis von $A = 1 - p(A)$
- $p(A_1, ..., A_k) \leq p(A_1) + ... + p(A_k)$

Beispiel: Würfelwurf

- ungezinkt:
  - $\Omega = 1, 2, 3, 4, 5, 6$
  - $p = (\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6})$
  - d.h. $p(\omega) = \frac{1}{6}$ f.a. $\omega \in \Omega$
- gezinkt:
  - $\Omega = 1, 2, 3, 4, 5, 6$
  - $p = (\frac{1}{4}, \frac{1}{10}, \frac{1}{5}, \frac{1}{4}, \frac{1}{10}, \frac{1}{10}) = (25\%, 10\%, 20\%, 25\%, 10\%, 10\%)$

- $p(\omega \in \Omega : \omega gerade) = p(2,4,6) = p(2)+p(4)+p(6) = \frac{1}{10}+\frac{1}{4}+\frac{1}{10} = \frac{9}{20}$

Satz: Sind $(\Omega, p_1), ..., (\Omega, p_m)$ Wahrscheinlichkeitsräume so ist durch $p((\omega_1, ..., \omega_m)) = \prod p_i(\omega_i)$ eine Verteilung auf $\Omega = \Omega_1 x ... x \Omega_m = (\omega_1, ..., \omega_m) : \omega \in \Omega, f.a.i \in 1, ..., m$. Für $A_1 \subseteq \Omega_1, A_2 \subseteq \Omega_2, ..., A_m \subseteq \Omega_m$ gilt $p(A_1 x ... x A_m) = \prod p_i(A_i)$. (Ω, p) heißt Produktraum von $(\Omega_1, p_1), ...$
(Ω, p) Wahrscheinlichkeitsraum; $A, B \in \Omega$ heißen (stochastisch) unabhängig, falls $p(A \cap B) = p(A) * p(B)$. Bespiel: $p(A \cap B) = p(i,j) = p_1 i * p_2 j = p(A) * p(B)$ für das Ereignis "der 1. Würfel zeigt i, der 2. Würfel zeigt j"

Bedingte Wahrscheinlichkeiten

(Ω, p) Wahrscheinlichkeitsraum, $B \subseteq \Omega$ ("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, denn $\sum p_b(\omega) = \sum \frac{p(\omega)}{p(B)} = \frac{1}{p(B)} \sum p(\omega) = \frac{1}{p(B)} p(B) = 1$. p_B ist die durch B bedingte Verteilung. Für $A \subseteq \Omega$ gilt $p_B(A \cap B) = \sum p_B(\omega) = \sum \frac{p(\omega)}{p(B)} = \frac{p(A \cap B)}{p(B)} := p(A|B)$ ("p von A unter B") bedingte Wahrscheinlichkeit von A unter B.
Satz (Bayer): $p(A|B) = \frac{p(B|A)*p(A)}{p(B)}$ wobei $p_A, p_B \geq 0$
Satz (Totale Wahrscheinlichkeit): Seien $A_1, ..., A_k$ paarweise disjunkt, $\bigcup A_j = \Omega, p(A_i) > 0, B \subseteq \Omega$, dann gilt $p(B) = \sum p(B|A_i) * p(A_i)$.
Satz (Bayer, erweitert): $A_1, ..., A_k, B$ wie eben, $p(B) > 0$. Für $i \in 1, ..., k$ gilt $p(A_i|B) = \frac{p(B|A_i)*p(A_i)}{\sum p(B|A_j)*p(A_j)}$
Bespiel: In einem Hut liegen drei beidseitig gefärbte Karten. Jemand zieht ("zufällig") eine Karte und leg sie mit einer ("zufälligen") Seite auf den Tisch. Karten rot/rot, rot/blau und blau/blau. Gegeben er sieht rot, wie groß ist die Wahrscheinlichkeit, dass die andere Seite auch rot ist? p(unten rot — oben rot) = p(unten rot und oben rot)/p(oben rot) = $\frac{p\binom{r}{r}}{p(\binom{r}{r}\binom{r}{b})} = \frac{\frac{2}{6}}{\frac{3}{6}} = \frac{2}{3}$
Eine Funktion $X : \Omega \to \mathbb{R}$ heißt (reellwertige) Zufallsvariable. Weil Ω endlich ist, ist auch $X(\Omega) = X(\omega) : \omega \in \Omega \subseteq \mathbb{R}$ endlich. Durch $p_x(x) := p(X = x) := p(\omega \in \Omega : X(\omega) = x)$ wird ein Wahrscheinlichkeitsraum $(X(\Omega), p_x)$ definiert; denn $\sum p_x(x) = p(\Omega) = 1$. p_x heißt die von X induzierte Verteilung. $X(\Omega)$ ist meist erheblich kleiner als Ω. Beispiel: Augensumme beim Doppelwurf:
$X : \Omega \to \mathbb{R}, X((i,j)) = i + j \to X(\Omega) = 2, 3, 4, ..., 12$
Satz: Seien $(\Omega_1, p_1), (\Omega_2, p_2)$ Wahrscheinlichkeitsräume und (Ω, p) ihr Produktraum. Sei $X : \Omega_1 \to \mathbb{R}, Y : \Omega_2 \to \mathbb{R}$, fasse X,Y als ZVA in Ω zusammen $X((\omega_1, \omega_2)) = X(\omega_1)$ und $Y((\omega_1, \omega_2)) = Y(\omega_2)$; d.h. X,Y werden auf Ω "fortgesetzt". Dann sind X,Y stochastisch unabhängig in (Ω, p) (und $p(X = x) = p_1(X = x), p(Y = y) = p_2(Y = y))$.

Erwartungswert, Varianz, Covarianz

Sei $X : \Omega \to \mathbb{R}$ ZVA im Wahrscheinlichkeitsraum (Ω, p).
$E(X) = \sum_{x \in X(\Omega)} xp(X = x) = \sum_{winOmega} X(\omega)p(\omega)$ "E verhält sich wie Integral"; E(x) heißt Erwartungswert von x. Linearität des Erwartungswertes: $E(x + y) = E(x) + E(y)$ und $E(\alpha x) = \alpha E(x)$. Ist $X : \Omega \to \mathbb{R}$ konstant gleich c, so ist $E(x) = \sum x * p(X = x) = c * p(X = x) = c * 1 = c$. Die Varianz von X: $Var(X) = E((X - E(X))^2)$ heißt Varianz von X (um E(X)). Die Covarianz:
$Cov(X,Y) = E((X - E(X)) * (Y - E(Y)))$ heißt Covarianz von X und Y. Der Verschiebungssatz:
$Cov(X,Y) = E(X * Y) - E(X) * E(Y)$ $Var(X) = Cov(X,X) = E(X * X) - E(X)E(X) = E(X^2) - (E(X))^2$
Seien X,Y stochastisch unabhängig
$(\leftrightarrow p(X = x \wedge Y = y) = p(X = x) * p(Y = y))$
$E(X) * E(Y) = \sum_{x \in X(\Omega)} x * p(X = x) * \sum_{y \in Y(\Omega)} y * p(Y = y) = \sum_{x \in X(\Omega)} \sum_{y \in Y(\Omega)} xy * p(X = x)p(Y = y) = \sum_{Z \in \mathbb{R}} z * p(X * Y = Z) = E(X * Y)$. Sind X,Y stochastisch unabhängig ZVA, so ist $E(X) * E(Y) = E(X * Y)$; folglich $Cov(X,Y) = 0$
Satz: Seien X,Y ZVA, dann gilt
$Var(X + Y) = Var(x) + Var(Y) + 2 * Cov(X,Y)$. Sind insbesondere X,Y unabhängig gilt:
$Var(X + Y) = Var(X) + Var(Y)$.
Sei (Ω, p) Wahrscheinlichkeitsraum, $X : \Omega \to \mathbb{R}$ Zufallsvariable heißt Bernoulliverteilt im Parameter p falls $p(X = 1) = p$ und $p(X = 0) = 1 - p$, $p \in [0,1]$.
$E(X) = \sum x * p(X = x) = 1 * p(X = 1) = p$ Für $X : \Omega \to 0, 1$ ist $X^2 = X$:
$Var(X) = E(X^2) - E(X)^2 = p - p^2 = p(1 - p) = p * q$

Binominalkoeffizienten

Sei N eine Menge, dann ist $\binom{N}{k} := (x \subseteq N :$ x hat genau k Elemente $(|x| = k))$ für $k \in \mathbb{N}$. Für $n \in \mathbb{N}$ sei $\binom{n}{k} := |(\binom{1,...,k}{k})$.
Satz: $\binom{n}{0} = nn = 1$ f.a. $n \geq 0$ $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ f.a. $n \geq 0, k \geq 1, k \geq n - 1$
Jede n-elementige Menge N ist $\binom{N}{0} = (\emptyset), \binom{N}{n} = N \to \binom{n}{0} = \binom{n}{n} = 1$. Den zweiten Teil der Behauptung zeigt man induktiv über n.

Binominalsatz

$(a + b)^n = \sum_{k=0}^{n} a^k b^{n-k}$ für $a, b \in \mathbb{R}$. Für $n \in \mathbb{N}$ sei $n! = n(n-1)(n-2)... * 3 * 2 * 1 = \prod i$; für $n \in \mathbb{N}$ und $k \geq 0$ sei $[\binom{n}{k}] = \frac{n!}{k!(n-k)!}$
Satz: $\binom{n}{0} = \binom{n}{n} = 1$ für jedes $n \in \mathbb{N}$, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ für $k \geq 1$ und $k \leq n - 1$. Zweiter Teil:
$[\binom{n-1}{k}] + [\binom{n-1}{k-1}] = \frac{n!}{k!(n-k)!} = [\binom{n}{k}]$. Also stimmen die Rekursionsgleichungen von $\binom{n}{k}$ und $[\binom{n}{k}]$ überein sowie $\binom{n}{k} = [\binom{n}{k}]$. Folglich ist die Anzahl k-elementiger Teilmengen eine n-elementige Menge gleich $\frac{n!}{k!(n-k)!}$.
Seien $X_1, ..., X_n$ unabhängige ZVAen, alle X_i seien Bernoulli-Verteilt im Parameter $p[0,1]$, d.h. $p(X_1 = 1) = p$, $p(X_i = 0) = (1 - p)$. Dann ist $X_i = X_1 + X_2 + ... + X_n$ ebenfalls reelwertige ZVA. Im Fall $X_i : \Omega \to 0, 1$ ist $X : \Omega \to 0, 1, ..., n$. Die Verteilung von X ergibt sich wie folgt, für $k \in 0, 1, ..., n$: $p(X = k) = \binom{n}{k} * p^k (1 - p)^{n-k}$
Eine ZVA heißt binominalverteilt in den Parametern n und p falls gilt: $p(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}$ für $k \in 0, 1, ..., n$; schreibe $X \sim L(n,p)$. Sonst ist X Bernoulliverteilt (genau dann wenn $X \sim L(1,p)$).

Erwartungswert und Varianz

Sei $X \sim L(n,p)$
OBdA $X = X_1, + ... + X_n$ wobei X_i unabhängig und Bernoulliverteilt. $E(X) = n * p$, $E(X_i) = p$
$Var(X) = n * p * (1 - p)$, $Var(X_i) = p * (1 - p)$

Multinominalverteilung

$\binom{N}{k_1, ..., k_n}$ sei Menge der Abbildungen $f : N \to 1, ..., r$ mit $k1, ..., k_r \geq 0$, $k_1 + ... + k_r = |\mathbb{N}|$ und $f^{-1}[j] = k_j \binom{n}{k_1, ..., k_r} = |\binom{N}{k_1, ..., k_r}$.

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.
$p(X = k) = \frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}}$ Eine ZVA $X : \Omega \to \mathbb{R}$ heißt hypergeometrisch Verteilt in den Parametern M,N,n falls $p(X = k)$ für alle $k \geq 0, k \geq M$ gilt.
$E(X) = \sum_{x=0}^{M} \frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}} = ... = n * \frac{M}{N}$
$Var(X) = E(X^2) - E(X)^2 = ... = n * \frac{M}{N}(1 - \frac{M}{N})(\binom{N-n}{N-1})$

Elementare Graphentheorie

$G = (V,E)$ heißt Graph mit Eckenmenge $V(G) = V$ und Kantenmenge $E(G) = E \subseteq x, y : x \neq y \in V$. Veranschaulichung als Punkte in der Ebene (V) mit "Verknüpfungslinien" von x nach y. Bsp $G = (1, 2, 3, 4, 12, 13, 14, 15, 16)$.
$P = x_0, ..., x_e$ Folge pw verschiedener Ecken mit $x_{i-1}, ..., x_i \in E(k)$ für $i \in 1, ..., l$ heißt ein Weg von x_0 nach x_e der Länge l. 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. Falls es keinen a,b-Weg gibt, definiere $d_G(a,b) = +\infty$.
$a \sim b \leftrightarrow$ es gibt einen a,b-Weg in G wird eine Äquivalenzrelation auf V(G) definiert. DIe Äquivalenzklassen heißen (Zusammenhangs-) Komponenten von G.
G heißt zusammenhängend, wenn G höchstens eine Komponente besitzt. $d_G : V(G)xV(G) \leftrightarrow \mathbb{R}_{\geq 0}$ ist eine Matrix

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

Für $A \subseteq V(G)$ sei $G[A] := (A, x, y \in E(G) : x, y \in A)$. Für $F \subseteq E(G)$ sei $G[F] := (V(G), F)$. $G[A]$ bzw $G[F]$ heißt von A bzw F induzierte Teilgraph. Ein Graph H mit $V(H) \subseteq V(G)$ und $E(H) \subseteq E(G)$ heißt Teilgraph von G, schreibweise $H \leq G$. $\leq$ ist Ordnung, denn:

- $G \leq G$

- $H \leq G \wedge G \leq H \rightarrow H = G$
- $H \leq G \wedge G = L \rightarrow H \leq L$

Ist $P = x_0, ..., x_p$ Weg, so heißt auch der Teilgraph ein Weg von x_0 nach x_e. Graphen G, H heißen isomorph, falls es einen Isomorphismus von V(G) nach V(H) gibt. Das heißt eine Bijektion. $V(G) \rightarrow V(H)$ mit
$f(x)f(y) \in E(H) \leftrightarrow x, y \in E(G)$. Es gilt:

- $G \cong G$
- $G \cong H \rightarrow H \cong G$
- $G \cong H \wedge H \cong L \rightarrow G \cong L$

Eine Folge $C = x_0, x_1, ..., x_{l-1}$ von Ecken mit $x_i, x_{i+1} \in E(G)$ für $i \in 0, ..., l-2$ und $x_{l-1}x_0 \in E(G)$ heißt Kreis in G der Länge l, falls $x_0, ..., x_{l-1}$ pw verschieden sind. Bsp: Kreis der Länge 5.
Ein Teilgraph H des Graphen G (also $H \leq G$) heißt aufspannend, falls $V(H) = V(G)$. Für eine Ecke $x \in V(G)$ sei $d_G(x) = |x, y \in E(G), y \in V(G)|$ die Anzahl der mit x indizierten Kanten, der sogenannte Grad von x in 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 zusammenhängend und G-e nicht zusammenhängend für jedes $e \in E(G)$ "G ist minimal zusammenhängend" Graph G ist ein Baum wenn G kreisfrei und Graph G+xy nicht kreisfrei für jedes $xy \notin E(G)$ G ist Baum, wenn

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

Jeder Baum mit wenigstens einer Ecke besitzt eine Ecke vom Grad ≤ 1, ein sog. Blatt ("jeder Baum besitzt ein Blatt").
$\rightarrow E(G) = |V(G)| - 1$ für jeden Baum also
$d(G) = \frac{2|V(G)|-2}{|V(G)|} < 2$.
G Wald $\leftrightarrow$ die Komponenten von G sind Bäume
G Baum $\leftrightarrow$ G ist zusammenhängender Wald
Ein Teilgraph H von G heißt Teilbaum von G, falls H ein Baum ist. Ein aufspannender Teilbaum von G heißt Spannbaum von G. G zusammenhängend $\leftrightarrow$ G Spannbaum.
Ein Spannbaum T von G heißt Breitensuchbaum von G bei $x \in V(G)$ falls $d_F(z, x) = d_G(z, x)$ f.a. $z \in V(G)$.
Ein Spannbaum T von G heißt Tiefensuchbaum von G bei $x \in V(G)$ 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

- (X) wird in + stets kleinstmöglich gewählt, so ist T ein Breitensuchbaum
- wird in (X) + stets größtmöglich gewählt, so ist T ein Tiefensuchbaum

Spannbäume minimaler Gewichte

G Graph, $F \subseteq E(G)$ heißt kreisfrei, falls G(F) kreisfrei ist.
Lemma (Austauschlemma für Graphen): Seien F, F' zwei kreisfreie Kantenmengen in Graph G und $|F| < |F'|$, dann gibt es ein $e \in F'/F$ so, dass $F \vee e$ kreisfrei ist.
G, $\omega : E(G) \rightarrow \mathbb{R}$ (Gewichtsfunktion an den Kanten). Für $F \subseteq E(G)$ sei $\omega(F) = \sum \omega(e)$, speziell $\omega(\emptyset) = 0$.
Für einen Teilgraphen H von G sei $\omega(G) = \omega(E(G))$. Ein Spannbaum minimalen Gewichts ist ein Spannbaum T von G mit $\omega(T) \leq \omega(S)$ für jeden Spannbaum S von G.
Satz (Kruskal): Sei G zuständiger Graph, $\omega : E(G) \rightarrow \mathbb{R}$; Setze $F = \emptyset$. Solange es eine Kante $e \in E(G)/F$ gibt so, dass $F \vee (e)$ kreisfrei ist, wähle e mit minimalem Gewicht $\omega(e)$, setzte $F = F \vee e$, iterieren. Das Verfahren endet mit einem Spannbaum $T = G(F)$ minimalen Gewichts.
Beweis: Weil G endlich ist endet das Verfahren mit einem maximal kreisfreien Graphen T. Seien $e_1, ..., e_n$ die Kanten von T in der Reihenfolge ihres Erscheinens, sei S Spannbaum minimalen Gewichts und $f_1, ..., f_m$ die Kanten in Reihenfolge aufsteigenden Gewichts. Angenommen (redactio ad absurdum) $\omega(T) > \omega(S)$. Dann gibt es ein $i \in 1, ..., m$ mit $\omega(e_i) > \omega(f_i)$. Wähle i kleinstmöglich, dann ist $F = e_1, ..., e_{i-1}$ und $F' = f_1, ..., f_i$ kreisfrei. Nach Austauschlemma gibt es ein $f \in F'/F$ so, dass $F \vee f$ kreisfrei ist. Also ist f ein Kandidat bei der Auswahl von e_i gewesen, also $\omega(e_i) \leq \omega(f)$ (Fehler!). Folglich ist $\omega(T) \leq \omega(S) \Rightarrow \omega(T) = \omega(S)$ also T und S Spannbaum mit minimalen Gewichten.

Das Traveling Salesman Problem

G sei Graph (vollständig) auf n Ecken, d.h. $xy \in E(G) \forall x \neq y$ aus V(G) und $\omega * E(G) \rightarrow \mathbb{R}$. Finde aufspannenden Kreis C von G minimalen Gewichts. Zusatzannahme (metrische TSP) $\omega(xz) \leq \omega(xy) + \omega(yz)$. Finde einen aufspannenden Kreis C, der um einen Faktor von höchstens zwei von einem aufspannenden Kreis D minimalen Gewichts abweicht ($\omega(C) \leq 2\omega(D)$) sog. Approximationsalgorithmus mit Gütefaktor $\leq$.

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. Gibt es $i \neq j$ mit $x_j = x_i$ so streiche x aus der Folge. Das Gewicht der neuen Folge ist maximal so groß wie das Gewicht der alten. Durch iteration erhält man einen aufspannenden Kreis mit $\omega(X) \leq 2\omega(T)$. Sei e Kante von D $\rightarrow D - e = S$ ist aufspanndender Weg $\rightarrow \omega(T) \leq w(D - e) \leq \omega(D)$.

G Graph, $k \geq 0$. Eine Funktion $f : V(G) \rightarrow C$ mit $|C| \leq k$ heißt k-Färbung, falls $f(x) \neq f(y)$ für $xy \in E(G)$. G heißt k-färbbar, falls G eine k-Färbung besitzt. Das kleinste $k \geq 0$ für das G k-färbbar ist heißt dramatische Zahl von G, Bezeichnung $X(G)$.

Satz (Tuga): Sei $k \geq 2$ und G ein Graph ohne Kreise eine Lösung $l \equiv 1 mod k$, dann ist G k-faltbar. G 2-färbbar $\leftrightarrow$ G hat keine Kreise ungerader Länge. Ein Graph heißt bipartit mit den Klassen A,B falls $(x \in A \wedge y \in B) \vee (x \in B \wedge y \in A)$ für alle $xy \in E(G)$ gilt. Genau dann ist G bipoartit mit gewissen Klassen A,B wenn G 2-färbbar ist.

Satz (Hall): Sei G bipartit mit Klassen A,B. Dann gilt G hat ein Matching von A $\leftrightarrow |N_G(X)| \leq |X|$ für alle $X \subseteq A$.

Satz: "$\rightarrow$" sei M Matching von A in G
$\rightarrow |N_G(X)| \leq N_{G[M]}(X) = |X|$. "$\leftarrow$" Induktiv über $|V(G)|$.
Ein schneller Zeuge für die Existenz eines Matchings von A im bipartiten Graphen G mit Klassen A,B ist das Matching selbst. Ein schneller Zeuge für die nicht-existenz eines Matchings ist ein $X \subseteq A$ mit $|N_G(X)| < |X|$.

Das Entscheidungsproblem "hat ein bipartiter Graph ein Matching?" ist im NP und zugleich in co-NP. Also ist auch Problem "ist ein Graph 2-färbbar?" in NP und co-NP. Das Problem "ist ein Graph 3-färbbar" ist in NP. Es ist sogar NP-vollständig, d.h. jedes Problem in NP (jedes Entscheidungsproblem mit schnellen Zeugen für Ja) lässt sich in Polynomalzeit in dieses Färbungsproblem überführen.