

# Diskrete Mathematik

Patrick Bucher & Lukas Arnold

14. Juni 2017

## Inhaltsverzeichnis

<b>1 Foundations</b>	<b>2</b>	4.2 Induktionsbeweis . . . . .	4
1.1 Operationen . . . . .	2	4.3 Schlussregeln / Inferenzregeln . . . . .	5
1.2 Prioritäten der Operationen . . . . .	2	<b>5 Counting</b>	<b>5</b>
1.3 Tautologie & Kontraktion . . . . .	2	5.1 Produktregel . . . . .	5
1.4 Logische Äquivalenzgesetze . . . . .	2	5.2 Summenregel . . . . .	5
1.5 Äquivalenzgesetze . . . . .	2	5.3 Einschluss-/Ausschlussprinzip . . . . .	5
1.6 Quantifikatoren . . . . .	3	5.4 Verallgemeinertes Schubfachprinzip . . . . .	5
1.7 Negation von Quantifikatoren . . . . .	3	5.5 Permutationen . . . . .	5
1.8 Beweise . . . . .	3	5.6 Anzahl Permutationen . . . . .	5
<b>2 Basic Structures</b>	<b>3</b>	5.7 Kombinationen . . . . .	5
2.1 Mengen . . . . .	3	5.8 Anzahl Kombinationen . . . . .	5
2.2 Spezielle Mengen . . . . .	3	5.9 Binomialkoeffizienten . . . . .	5
2.3 Mengenoperationen . . . . .	3	5.10 Binomialsatz . . . . .	5
2.4 Rechenregeln für Mengen . . . . .	3	<b>6 Diskrete Wahrscheinlichkeitsrechnung</b>	<b>5</b>
2.5 Definition von Funktionen . . . . .	3	6.1 Wahrscheinlichkeit nach Laplace . . . . .	5
2.6 Arten von Funktionen . . . . .	3	6.2 Komplement der Wahrscheinlichkeit . . . . .	5
2.7 Zusammengesetzte Funktion . . . . .	3	6.3 Additionsregel . . . . .	5
2.8 Umkehrfunktion . . . . .	3	6.4 Bedingte Wahrscheinlichkeit . . . . .	5
2.9 <i>ceiling</i> und <i>floor</i> -Funktion . . . . .	3	6.5 Unabhängige Ereignisse . . . . .	5
2.10 Folgen . . . . .	3	6.6 Satz der totalen Wahrscheinlichkeit . . . . .	5
2.11 Reihen . . . . .	3	6.7 Satz von Bayes . . . . .	5
2.12 Summenformeln . . . . .	3	6.8 Binomialverteilung . . . . .	5
<b>3 Fundamentals</b>	<b>3</b>	6.9 Hypergeometrische Verteilung . . . . .	6
3.1 Wachstum von Funktionen . . . . .	3	6.10 Poissonverteilung . . . . .	6
3.2 Exponentialfunktionen . . . . .	4	6.11 Verteilung einer Zufallsvariablen . . . . .	6
3.3 Logarithmusfunktionen . . . . .	4	6.12 Erwartungswert einer Zufallsvariable . . . . .	6
3.4 Komplexität von Algorithmen . . . . .	4	6.13 Unabhängigkeit von Zufallsvariablen . . . . .	6
3.5 Zahlen und Division . . . . .	4	6.14 Varianz einer Zufallsvariable . . . . .	6
3.6 Primzahl . . . . .	4	6.15 Standardabweichung einer Zufallsvariable . . . . .	6
3.7 Mersenne Primes . . . . .	4	<b>7 Advanced Counting Techniques</b>	<b>6</b>
3.8 Primzahlsatz . . . . .	4	7.1 Rekursionsbeziehungen . . . . .	6
3.9 ggT und kgV . . . . .	4	7.2 Erzeugende Funktion . . . . .	6
3.10 Kongruenz . . . . .	4	7.3 Anzahl Derangements . . . . .	6
3.11 Addition zweier Matrizen . . . . .	4	<b>8 Zahlentheorie</b>	<b>6</b>
3.12 Multiplikation einer Matrix mit einer Zahl . . . . .	4	8.1 Division mit Rest . . . . .	6
3.13 Multiplikation von Matrizen . . . . .	4	8.2 Kongruenz modulo $n$ . . . . .	6
3.14 Transponierte Matrix . . . . .	4	8.3 Euklidischer Algorithmus . . . . .	6
3.15 Symmetrie einer Matrix . . . . .	4	8.4 Diophantische Gleichung . . . . .	6
3.16 Einheitsmatrix . . . . .	4	8.5 erweiterter Euklidischer Algorithmus . . . . .	6
3.17 Inverse Matrix . . . . .	4	8.6 Chinesischer Restsatz . . . . .	6
3.18 Boolesches Produkt zweier Matrizen . . . . .	4	8.7 Eulersche $\phi$ -Funktion . . . . .	6
<b>4 Reasoning</b>	<b>4</b>	8.8 Primzahl . . . . .	6
4.1 Beweismethoden . . . . .	4	8.9 kleiner Satz von Fermat . . . . .	6
		8.10 Primzahltest von Wilson . . . . .	6

8.11 Restklassen . . . . .	6
8.12 Rechenregeln für das modulare Rechnen .	7
8.13 Potenzieren modulo $n$ . . . . .	7
8.14 Square and Multiply Algorithm . . . . .	7
8.15 Nullteiler . . . . .	7
8.16 Inverse Elemente . . . . .	7
8.17 Primitive Elemente / Erzeugende . . . . .	7
8.18 Einwegfunktionen . . . . .	7
8.19 Modulare Quadratwurzeln . . . . .	7
8.20 diskrete Logarithmus . . . . .	7
8.21 Diffie-Hellmann Schlüsselvereinbarung .	7
8.22 Symmetrische Verschlüsselung . . . . .	7
8.23 Asymmetrische Verschlüsselung . . . . .	7
8.24 Satz von Euler . . . . .	7

<b>9 Graphentheorie</b>	<b>7</b>
9.1 Grade . . . . .	7
9.2 Isomorphe Graphen . . . . .	7
9.3 Vollständiger Graph . . . . .	7
9.4 Eigenschaften eines Baumes . . . . .	8
9.5 Vollständige bipartite Graphen . . . . .	8
9.6 Page-Rank-Algorithmus . . . . .	8
9.7 Matrizen . . . . .	8
9.8 Wege und Kreise . . . . .	8
9.9 Planare Graphen . . . . .	8
9.10 Satz von Euler . . . . .	8
9.11 Satz von Kuratovsky . . . . .	8
9.12 Färbungen . . . . .	8
9.13 Dekompositionsgleichung . . . . .	8
9.14 Gerüste / Spannbäume . . . . .	8

## 1 Foundations

### 1.1 Operationen

Negation	$\neg p$	<i>Verneinung</i>
Konjunktion	$p \wedge q$	<i>Und-Verknüpfung</i>
Disjunktion	$p \vee q$	<i>Oder-Verknüpfung</i>
EXOR	$p \oplus q$	<i>Exklusiv-Oder</i>
Implikation	$p \rightarrow q$	<i>falls <math>p</math> dann <math>q</math></i>
Bikonditional	$p \leftrightarrow q$	<i><math>p</math> genau dann wenn <math>q</math></i>

### 1.2 Prioritäten der Operationen

$\neg$	$\wedge$	$\vee$	$\oplus$	$\rightarrow$	$\leftrightarrow$
1	2	3	4	5	6

### 1.3 Tautologie & Kontraktion

Tautologie	$p \vee \neg p$	<i>immer wahre Aussage</i>
Kontraktion	$p \wedge \neg p$	<i>immer falsche Aussage</i>

### 1.4 Logische Äquivalenzgesetze

Identität	$p \wedge \mathbf{T} \equiv p$	$p \vee \mathbf{F} \equiv p$
Dominanz	$p \vee \mathbf{T} \equiv \mathbf{T}$	$p \wedge \mathbf{F} \equiv \mathbf{F}$
Negation	$p \vee \neg p \equiv \mathbf{T}$	$p \wedge \neg p \equiv \mathbf{F}$
Assoziativ 1	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	
Assoziativ 2	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	
Distributiv 1	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	
Distributiv 2	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	
De Morgan's 1	$\neg(p \wedge q) \equiv \neg p \vee \neg q$	
De Morgan's 2	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	

### 1.5 Äquivalenzgesetze

$p \rightarrow q$	$\equiv$	$\neg p \vee q$
$p \rightarrow q$	$\equiv$	$\neg q \rightarrow \neg p$
$p \vee q$	$\equiv$	$\neg p \rightarrow q$
$p \wedge q$	$\equiv$	$\neg(p \rightarrow \neg q)$
$\neg(p \rightarrow q)$	$\equiv$	$p \wedge \neg q$
$p \leftrightarrow q$	$\equiv$	$(p \rightarrow q) \wedge (q \rightarrow p)$
$p \leftrightarrow q$	$\equiv$	$\neg p \leftrightarrow \neg q$
$p \leftrightarrow q$	$\equiv$	$(p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q)$	$\equiv$	$p \leftrightarrow \neg q$
$p \rightarrow (q \wedge r)$	$\equiv$	$(p \rightarrow q) \wedge (p \rightarrow r)$
$(p \vee q) \rightarrow r$	$\equiv$	$(p \rightarrow r) \wedge (q \rightarrow r)$
$p \rightarrow (q \vee r)$	$\equiv$	$(p \rightarrow q) \vee (p \rightarrow r)$
$(p \wedge q) \rightarrow r$	$\equiv$	$(p \rightarrow r) \vee (q \rightarrow r)$
$p \oplus q$	$\equiv$	$(p \vee q) \wedge (\neg p \vee \neg q)$
$\neg(p \oplus q)$	$\equiv$	$(p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \oplus q)$	$\equiv$	$p \leftrightarrow q$

## 1.6 Quantifikatoren

For All	$\forall$	für alle $x$ aus $P$ wahr
Exists	$\exists$	für mindestens ein $x$ aus $P$ wahr
Not Exists	$\neg\exists$	für alle $x$ aus $P$ falsch
Not For All	$\neg\forall$	für mindestens ein $x$ aus $P$ falsch

## 1.7 Negation von Quantifikatoren

$\neg\exists x P(x)$	$\equiv$	$\forall x \neg P(x)$
$\neg\forall x P(x)$	$\equiv$	$\exists x \neg P(x)$

## 1.8 Beweise

direkter Beweis	$p \rightarrow q$
indirekter Beweis	$\neg q \rightarrow \neg p$
Widerspruch	$\neg p \rightarrow q$
Vorgehen Widerspruch	$(\neg p \rightarrow \mathbf{f}) \Rightarrow (p \rightarrow \mathbf{w})$

## 2 Basic Structures

### 2.1 Mengen

$\mathbb{N} = \{1, 2, \dots\}$   
 $\mathbb{N}_0 = \{0, 1, 2, \dots\}$   
 $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$   
 $\mathbb{Z}^+ = \{1, 2, \dots\}$   
 $\mathbb{Q} = \{p/q | p \in \mathbb{Z} \wedge q \in \mathbb{N}\}$   
 $\mathbb{R}$ : die Menge der reellen Zahlen  
 $\mathbb{C}$ : die Menge der komplexen Zahlen

### 2.2 Spezielle Mengen

Teilmenge:	$A \subset B \equiv \forall x (x \in A \rightarrow x \in B)$
Leere Menge:	$\emptyset \subset A$ gilt für jede Menge $A$
Kardinalität:	$ S $ beschreibt Anzahl Elemente von $A$
Potenzmenge:	$P(S) = 2^S = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
Kreuzprodukt:	$A \times B = \{(a, b)   a \in A \wedge b \in B\}$

### 2.3 Mengenoperationen

Komplement:	$A^c = \overline{A} = \{m \in M : m \notin A\}$
Durchschnitt:	$A \cap B = \{m \in M   m \in A \wedge m \in B\}$
Vereinigung:	$A \cup B = \{m \in M   m \in A \vee m \in B\}$
Differenz:	$B - A = \{m \in M   m \in B \wedge m \notin A\}$

### 2.4 Rechenregeln für Mengen

Kommutativgesetz	$A \cup B = B \cup A$
Kommutativgesetz	$A \cap B = B \cap A$
Assoziativgesetz	$A \cup (B \cap C) = (A \cup B) \cap C$
Assoziativgesetz	$A \cap (B \cup C) = (A \cap B) \cup C$
Distributivgesetz	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Distributivgesetz	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
De Morgan's Gesetz	$\overline{A \cup B} = \overline{A} \cap \overline{B}$
De Morgan's Gesetz	$\overline{A \cap B} = \overline{A} \cup \overline{B}$

## 2.5 Definition von Funktionen

$$f : X \rightarrow Y \quad x \mapsto f(x) \quad f : x \mapsto f(x)$$

$$f(x) := \begin{cases} 5 & \text{für } x < 0 \\ x^2 + 5 & \text{für } x \in [0, 2] \\ 0.5x + 8 & \text{für } x > 2 \end{cases}$$

## 2.6 Arten von Funktionen

injektiv	auf jedes Element in $Y$ zeigt höchstens ein Pfeil
surjektiv	auf jedes Element in $Y$ zeigt mindestens ein Pfeil
bijektiv	auf jedes Element in $Y$ zeigt genau ein Pfeil

## 2.7 Zusammengesetzte Funktion

$$g : X \rightarrow U \quad x \mapsto g(x)$$

$$f : U \rightarrow Y \quad u \mapsto f(u)$$

$$F = f \circ g : X \rightarrow Y \quad x \mapsto f(g(x))$$

## 2.8 Umkehrfunktion

$$y = f(x) \quad x = f^{-1}(y)$$

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$$

$$(f^{-1} \circ f)(y) = f^{-1}(f(y)) = y$$

## 2.9 ceiling und floor-Funktion

$$\lceil \cdot \rceil : \mathbb{R} \rightarrow \mathbb{Z}, x \mapsto \lceil x \rceil = \min\{n \in \mathbb{Z} | x \leq n\}$$

$$\lfloor \cdot \rfloor : \mathbb{R} \rightarrow \mathbb{Z}, x \mapsto \lfloor x \rfloor = \max\{n \in \mathbb{Z} | n \leq x\}$$

## 2.10 Folgen

harmonisch	$a_k = 1/k$
geometrisch	$a_k = a_0 * q^k$
arithmetisch	$a_k = a_0 + (k * d)$

## 2.11 Reihen

harmonisch	$\sum_{k=1}^n 1/k$
geometrisch	$a_0 * \sum_{k=0}^{n-1} q^k = a_0 \frac{q^n - 1}{q - 1}$
arithmetisch	$\sum_{k=0}^{n-1} (a_0 + kd) = n \frac{a_0 + a_{n-1}}{2}$

## 2.12 Summenformeln

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}$$

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=1}^n k^3 = \frac{n^2(n+1)^2}{4}$$

$$\sum_{k=0}^n x^k, |x| < 1 = \frac{1}{1-x}$$

$$\sum_{k=1}^n kx^{k-1}, |x| < 1 = \frac{1}{(1-x)^2}$$

## 3 Fundamentals

### 3.1 Wachstum von Funktionen

$f =$  "sehr komplizierte Funktion"  
 $g =$  "einfachere Funktion"  
 $|f(x)| \leq C|g(x)|, \forall x > k$   
 $f(x) = \mathcal{O}(g(x))$

### 3.2 Exponentialfunktionen

$$\begin{aligned} a^r * a^s &= a^{r+s} \\ \frac{a^r}{a^s} &= a^{r-s} \\ (a^r)^s &= (a^s)^r = a^{r*s} \end{aligned}$$

### 3.3 Logarithmusfunktionen

$$\begin{aligned} \log_a(u * v) &= \log_a(u) + \log_a(v) \\ \log_a\left(\frac{u}{v}\right) &= \log_a(u) - \log_a(v) \\ \log_a(u^v) &= v * \log_a(u) \end{aligned}$$

### 3.4 Komplexität von Algorithmen

konstant	$\mathcal{O}(1)$
logarithmisch	$\mathcal{O}(\log n)$
linear	$\mathcal{O}(n)$
n log n	$\mathcal{O}(n * \log n)$
polynomial	$\mathcal{O}(n^b)$
exponentiell	$\mathcal{O}(b^n), b > 1$
faktorielle	$\mathcal{O}(n!)$

### 3.5 Zahlen und Division

$$\begin{aligned} a|b \wedge a|c &\rightarrow a|(b + c) \\ a|b &\rightarrow \forall c(a|bc) \\ a|b \wedge b|c &\rightarrow a|c \end{aligned}$$

### 3.6 Primzahl

$$\nexists a(a|n \wedge (1 < a < n))$$

### 3.7 Mersenne Primes

$$M_n = 2^p - 1, p \in \text{"Primzahlen"}$$

### 3.8 Primzahlsatz

$$\pi(x) \approx \frac{x}{\ln(x)}$$

### 3.9 ggT und kgV

$$\begin{aligned} a &= dq + r, \text{ wobei } (0 \leq r < d) \\ q &= a \text{ div } d \text{ und } r = a \bmod d \\ ab &= ggT(a, b) * kgV(a, b) \end{aligned}$$

### 3.10 Kongruenz

$$a \equiv b \bmod m, m|(a - b)$$

### 3.11 Addition zweier Matrizen

$$A+B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{bmatrix}$$

### 3.12 Multiplikation einer Matrix mit einer Zahl

$$\alpha A = \begin{bmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \cdots & \alpha a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \cdots & \alpha a_{mn} \end{bmatrix}$$

### 3.13 Multiplikation von Matrizen

$$A \times B = C \quad \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix}$$

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \quad \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}$$

$$c_{11} = (a_{11} * b_{11}) + (a_{12} * b_{21}) + \cdots + (a_{1n} * b_{m1})$$

### 3.14 Transponierte Matrix

$A^T$  durch Vertauschen von Zeilen und Spalten

### 3.15 Symmetrie einer Matrix

ist symmetrisch, falls  $A^T = A$   
ist antisymmetrisch, falls  $A^T = -A$

### 3.16 Einheitsmatrix

$I_n$  ist eine Matrix bei der alle Elemente auf der Diagonalen Eins und alle anderen Null sind

### 3.17 Inverse Matrix

$$A^{-1} * A = A * A^{-1} = I_n$$

### 3.18 Boolesches Produkt zweier Matrizen

$$A \odot B = [c_{ij}], \text{ wobei } c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \cdots \vee (a_{in} \wedge b_{nj})$$

## 4 Reasoning

### 4.1 Beweismethoden

Direkter Beweis	$p \rightarrow q$
Beweis durch Kontraposition	$\neg q \rightarrow \neg p$
Beweis durch Widerspruch	$\neg p \rightarrow q$

### 4.2 Induktionsbeweis

Induktionshypothese	$P(k)$
Induktionsverankerung	$P(1)$
Induktionsschritt	$P(k) \rightarrow P(k+1)$
$[P(1) \wedge \forall k(P(k) \rightarrow P(k+1))] \rightarrow \forall n P(n)$	

### 4.3 Schlussregeln / Inferenzregeln

Modus ponens	$((p \rightarrow q) \wedge p) \rightarrow q$
Modus tollens	$((\neg q \wedge (p \rightarrow q))) \rightarrow \neg p$
Hypothetischer Syllogismus	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
Disjunktiver Syllogismus	$((p \vee q) \wedge \neg p) \rightarrow q$
Addition	$p \rightarrow (p \vee q)$
Simplifikation	$(p \wedge q) \rightarrow p$
Konjunktion	$((p) \wedge (q)) \rightarrow p \wedge q$
Resolution	$((p \wedge q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$

## 5 Counting

### 5.1 Produktregel

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$$

### 5.2 Summenregel

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$$

### 5.3 Einschluss-/Ausschlussprinzip

für 2 Mengen:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

für 3 Mengen:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

### 5.4 Verallgemeinertes Schubfachprinzip

Falls man  $N$  Objekte auf  $k$  Schubfächer verteilt, dann gibt es wenigstens ein Schubfach, welches mindestens  $\lceil N/k \rceil$  Objekte enthält

### 5.5 Permutationen

geordnete Anordnung von  $r$  der  $n$  Elemente

### 5.6 Anzahl Permutationen

Bedingung	$0 \leq r \leq n \in \mathbb{N}$
ohne Wiederholung	$P(n, r) = \frac{n!}{(n-r)!}$
mit Wiederholung	$P(n, r) = n^r$

### 5.7 Kombinationen

ungeordnete Auswahl von  $r$  dieser  $n$  Elemente

### 5.8 Anzahl Kombinationen

Bedingung	$0 \leq r \leq n \in \mathbb{N}$
ohne Wiederholung	$C(n, r) = \frac{n!}{r!(n-r)!} = \binom{n}{r}$
mit Wiederholung	$C(n, r) = \frac{n!}{r!(n-r)!} = \binom{n+r-1}{r}$

### 5.9 Binomialkoeffizienten

$$\binom{\alpha}{k} = \frac{\alpha * (\alpha-1) * \dots * (\alpha-k+1)}{k!}$$

$$C(n, k) = \binom{n}{k} = \binom{n}{n-k} = C(n, n-k)$$

### 5.10 Binomialsatz

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$$

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$$

$$\sum_{k=0}^n 2^k \binom{n}{k} = 3^n$$

$$\sum_{k=0}^n \binom{r}{k} \binom{s}{n-k} = \binom{r+s}{n}$$

## 6 Diskrete Wahrscheinlichkeitsrechnung

### 6.1 Wahrscheinlichkeit nach Laplace

$$p(A) = \frac{|A|}{|S|} = \frac{\text{Anzahl guenstige}}{\text{Anzahl moegliche}}$$

### 6.2 Komplement der Wahrscheinlichkeit

$$p(\bar{A}) = 1 - p(A)$$

### 6.3 Additionsregel

$$p(A_1 \cup A_2) = p(A_1) + p(A_2) - p(A_1 \cap A_2)$$

### 6.4 Bedingte Wahrscheinlichkeit

$$p(A|B) = \frac{p(A \cap B)}{p(B)}$$

### 6.5 Unabhängige Ereignisse

$$p(A|B) = \frac{p(A \cap B)}{p(B)} = \frac{p(A)p(B)}{p(B)} = p(A)$$

### 6.6 Satz der totalen Wahrscheinlichkeit

$$p(A) = \sum_{i=1}^k p(A \cap B_i) = \sum_{i=1}^k p(A|B_i) \cdot p(B_i)$$

$$p(A|C) = \frac{1}{p(C)} \sum_{i=1}^k p(A \cap (B_i \cap C))$$

$$p(A|C) = \sum_{i=1}^k p(A|B_i) \cdot p(B_i|C)$$

Spezialfall für 2 Mengen:

$$p(A) = p(A|B) \cdot p(B) + p(A|\bar{B}) \cdot p(\bar{B})$$

### 6.7 Satz von Bayes

$$p(B_j|A) = \frac{p(A|B_j) \cdot p(B_j)}{p(A)} = \frac{p(A|B_j) \cdot p(B_j)}{\sum_{i=1}^k p(A|B_i) \cdot p(B_i)}$$

Spezialfall für 2 Mengen:

$$p(B|A) = \frac{p(A|B) \cdot p(B)}{p(A|B) \cdot p(B) + p(A|\bar{B}) \cdot p(\bar{B})}$$

### 6.8 Binomialverteilung

$$B(k|n, p) = B_{n,p}(k) = C(n, k) p^k (1-p)^{n-k}$$

$$B(k|n, p) = \binom{n}{k} p^k (1-p)^{n-k}$$

Bedingung:

$$p = M/N \text{ und } n \leq M/10 \leq (N-M)/10$$

## 6.9 Hypergeometrische Verteilung

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

## 6.10 Poissonverteilung

$$f(k) = \frac{u^k}{k!} e^{-u}$$

Bedingung:

$$u = np \text{ und } p \leq 0.1, n \geq 100$$

## 6.11 W'keitsverteilung einer Zufallsvariablen

$$\{(r, p(X=r)) | \forall r \in X(S)\}$$

## 6.12 Erwartungswert einer Zufallsvariable

$$E(C) = \sum_{s \in S} X(s) \cdot p(s) = \sum_{r \in X(S)} r \cdot p(X=r)$$

## 6.13 Unabhängigkeit von Zufallsvariablen

$$\forall r_1 \in \mathbb{R} \text{ und } \forall r_2 \in \mathbb{R} \text{ gilt } p(X(s) = r_1 \wedge Y(s) = r_2) = p(X(s) = r_1) \cdot p(Y(s) = r_2)$$

## 6.14 Varianz einer Zufallsvariable

$$V(X) = \sum_{s \in S} (X(s) - E(X))^2 \cdot p(s)$$

$$V(X) = \sum_{r \in X(S)} (r - E(X))^2 \cdot p(X=r)$$

## 6.15 Standardabweichung einer Zufallsvariable

$$\sigma(X) = \sqrt{V(X)}$$

## 7 Advanced Counting Techniques

### 7.1 Rekursionsbeziehungen

$$a_n = f(a_{n-1}, a_{n-2}, \dots, a_2, a_1), \forall n \geq n_0, n_0 \in \mathbb{N}^+$$

### 7.2 Erzeugende Funktion

$$G(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 x^0 + a_1 x^1 + a_2 x^2 + \dots$$

### 7.3 Anzahl Derangements

$$D_n = n! \left[ 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!} \right]$$

## 8 Zahlentheorie

### 8.1 Division mit Rest

$$A = q * n + r \text{ wobei } 0 \leq r < |n|$$

### 8.2 Kongruenz modulo n

$$a \equiv b \pmod{n} \iff n | (a - b)$$

$$\iff \exists q : a - b = q * n$$

$$\iff \exists q : a = b + q * n$$

## 8.3 Euklidische Algorithmus

$$\begin{array}{rclcl} 963 & = & 4 & * & 218 & + & 91 \\ 218 & = & 2 & * & 91 & + & 36 \\ 91 & = & 2 & * & 36 & + & 19 \\ 36 & = & 1 & * & 19 & + & 17 \\ 19 & = & 1 & * & 17 & + & 2 \\ 17 & = & 8 & * & 2 & + & 1 \\ 8 & = & 2 & * & 1 & + & 0 \end{array}$$

## 8.4 Diophantischer Gleichung

$$n_1 * x + n_2 * y = n$$

## 8.5 erweiterter Euklidischer Algorithmus

$$\begin{array}{rclcl} 67 & - & 1 & 0 \\ 24 & 2 * & 0 & 1 \\ 19 * & 1 & 1 * & -2 * & 19 = 67 \% 24 \\ 5 & 4 & -1 & 3 & 2 = 67 \text{ div } 24 \\ 4 & 1 & 4 & -11 & 1 = 1 - 2 * 0 \\ 1 & & -5 & 14 & -2 = 0 - 2 * 1 \end{array}$$

## 8.6 Chinesischer Restsatz

$$M_i = \frac{m}{m_i}$$

$$M_i * y_i \equiv 1 \pmod{m_i}$$

$$x = \sum_{i=1}^k r_i * M_i * y_i$$

## 8.7 Eulersche $\phi$ -Funktion

$$\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$$

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n | x > 0 \text{ und } \text{ggT}(x, n) = 1\}$$

$$|\mathbb{Z}_n^*| := \text{Anzahl Elemente in } \mathbb{Z}_n^*$$

$$\phi : \mathbb{N} \rightarrow \mathbb{N}, n \mapsto |\mathbb{T}_n^*| =: \phi(n)$$

$$\begin{array}{rcl} \phi(p) & = & p - 1 \\ \phi(p * q) & = & (p - 1) * (q - 1) \\ \phi(m) & = & (p_1 - 1) * p_1^{r_1-1} * (p_2 - 1) * p_2^{r_2-1} * \dots \end{array}$$

## 8.8 Primzahl

$$n = p_1^{e_1} * p_2^{e_2} * p_3^{e_3} * \dots * p_n^{e_n}$$

## 8.9 kleiner Satz von Fermat

$$m^p \pmod{p} = m \pmod{p}$$

## 8.10 Primzahltest von Wilson

falls  $(n-1)! + 1$  durch  $n$  teilbar ist

## 8.11 Restklassen

$$[r] = \{x \in \mathbb{Z} | x \equiv r \pmod{n}\}$$

## 8.12 Rechenregeln für das modulare Rechnen

$$\begin{aligned} a \oplus_n b &= b \oplus_n a = a + b \mod n = R_n(a + b) \\ a \odot_n b &= b \odot_n a = a * b \mod n = R_n(a * b) \\ a \odot_n (b \oplus_n c) &= (a \odot_n b) \oplus_n (a \odot_n c) \end{aligned}$$

## 8.13 Potenzieren modulo n

$$x^m = x^{2*k+l} = x^{2*k} * x^l = (x^k)^2 * x^l$$

## 8.14 Square and Multiply Algorithm

1. Exponent binär schreiben
2. Q bedeutet quadrieren und M multiplizieren
3. Ersetze 1 durch QM und 0 durch Q
4. das erste (links) QM streichen
5. Reihenfolge von Quadrieren und Multiplizieren
6. Exponent einsetzen
7. entsprechend Quadrieren und Multiplizieren
8. immer wieder modular reduzieren

## 8.15 Nullteiler

$$\begin{aligned} a \in \mathbb{Z}_n, a \neq 0, b \in \mathbb{Z}_n, b \neq 0 \\ \text{falls } a \odot_n b = 0, \text{ dann ist } a \text{ Nullteiler von } \mathbb{Z}_n \end{aligned}$$

## 8.16 Inverse Elemente

$$\begin{aligned} \mathbb{Z}_n^* &= \{a \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1\} \\ a^{-1} &= R_p(a^{p-2}) = a^{p-2} \mod p, (p = \text{Primzahl}) \end{aligned}$$

## 8.17 Primitive Elemente / Erzeugende

falls jedes Element  $a \in \mathbb{Z}_p^*$  eine Potenz von  $z$  ist

## 8.18 Einwegfunktionen

$$\begin{aligned} \text{Quadrieren modulo } n & x \mapsto x^2 \mod n \\ \text{Potenzieren modulo } n & x \mapsto x^e \mod n \\ \text{Exponentialfunktion modulo } p & x \mapsto b^x \mod p \end{aligned}$$

$n = pq$  (Multiplikation zweier Primzahlen)

## 8.19 Modulare Quadratwurzeln

$$\begin{aligned} \sqrt{a} \mod n &= \{x \in \mathbb{Z}_n^* \mid x^2 = a \mod n\} \\ \Rightarrow \text{Für ein } a \text{ kann es mehrere Quadratwurzeln geben} \end{aligned}$$

## 8.20 diskrete Logarithmus

$$\exp_b(k) = b^k \mod p$$

## 8.21 Diffie-Hellmann Schlüsselvereinbarung

1. Wähle zwei natürliche Zahlen  $p$  und  $s$
2.  $A$  wählt eine Zufallszahl  $a < p$   
 $A$  berechnet  $\alpha = s^a \mod p$   
 $A$  sendet  $\alpha$  über einen Kanal an  $B$
3.  $B$  wählt eine Zufallszahl  $b < p$   
 $B$  berechnet  $\beta = s^b \mod p$   
 $B$  sendet  $\beta$  über einen Kanal an  $A$
4.  $A$  berechnet  $\beta^a \mod p = s^{b*a} \mod p$
5.  $B$  berechnet  $\alpha^b \mod p = s^{b*a} \mod p$
6. Beide haben den gemeinsamen Schlüssel

## 8.22 Symmetrische Verschlüsselung

Verschlüsselungsfunktion  $f$ , Schlüssel  $k$ , Klartext  $m$ , Geheimtext  $c$ , Entschlüsselungsfunktion  $f^*$

$$\begin{aligned} m \mapsto c &= f(k, m) \text{ und } c \mapsto m = f^*(k, c) \\ \text{Bedingung: } f^*(k, f(k, m)) &= m \end{aligned}$$

## 8.23 Asymmetrische Verschlüsselung

privater Schlüssel  $d = d_T$ , öffentlicher Schlüssel  $e = e_T$ , Klartext  $m$ , Geheimtext  $c$

$$\begin{aligned} m \mapsto c &= f_e(m) \text{ und } c \mapsto m' = f_d(c) \\ \text{Bedingung: } m' &= f_d(c) = f_d(f_e(m)) = m \end{aligned}$$

## 8.24 Satz von Euler

$$m^{k\phi(n)+1} \mod n = m^{k(p-1)(q-1)+1} \mod n = m$$

## 9 Graphentheorie

### 9.1 Grade

$$\begin{aligned} \text{Eckengrad} & \sum_{v \in V} \deg(v) = 2 * |E| \\ \text{Maximalgrad} & \Delta(G) = \max_{v \in V(G)} \deg(v) \\ \text{Maximalgrad} & \delta(G) = \min_{v \in V(G)} \deg(v) \end{aligned}$$

Spezielle Ecken:

$$\begin{aligned} \text{isolierte Ecke} & \deg(v) = 0 \\ \text{Endecke} & \deg(v) = 1 \end{aligned}$$

### 9.2 Isomorphe Graphen

isomorph, falls es eine Bijektion  $f : V \rightarrow V'$   
 $\{u, v\} \in E \Leftrightarrow \{f(u), f(v)\} \in E'$

### 9.3 Vollständiger Graph

Vollständiger Graph mit  $n$  Knoten: genau eine Kante zwischen je zwei Knoten ( $m$  Kanten).

$$m = \binom{n}{2} = \frac{(n-1)n}{2}$$

## 9.4 Eigenschaften eines Baumes

Baum mit  $n$  Knoten  $n - 1$  Kanten  
 Baum mit  $i$  inneren Knoten  $n = m \cdot i + 1$  Knoten  
 $m$ -facher Baum der Höhe  $h$  höchstens  $m^h$  Blätter

## 9.5 Vollständige bipartite Graphen

Bedingung:  $U \cup W = V$  und  $U \cap W = \emptyset$

1. keine Kante zwischen Knoten aus  $U$
2. keine Kante zwischen Knoten aus  $W$
3. Knoten aus sind genau durch eine Kante verbunden
4.  $\forall u \in U, u$  ist mit jedem Knoten aus  $W$  verbunden
5.  $\forall w \in W, w$  ist mit jedem Knoten aus  $U$  verbunden

## 9.6 Page-Rank-Algorithmus

Gewicht der Seite  $PR_i$  in einem Netz mit  $N$  Seiten  
 Dämpfungsfaktor  $d$  mit  $0 \leq d \leq 1$   
 $C_j$  von Seite  $j$  abgehende Links

$$PR_i = \frac{1-d}{N} + d \cdot \sum_j \frac{PR_j}{C_j}$$

## 9.7 Matrizen

$n$  Ecken,  $m$  Kanten

**Adjazenzmatrix**  $A(G)$   $n \times n$  - Matrix  
 mit Anzahl Kanten zwischen den Ecken

**Inzidenzmatrix**  $B(G)$   $n \times m$  - Matrix  
 Ecke liegt auf Kante (0 oder 1)

**Gradmatrix**  $D(G)$   $n \times n$  - Diagonal-Matrix  
 Grade der Knoten auf der Diagonalen

## 9.8 Wege und Kreise

Anzahl Wege der Länge  $l$  von Knoten  $i$  zu  $j$   
 Eintrag  $(i, j)$  von  $A(G)^l$  (Adjazenzmatrix hoch  $l$ )

Weg	Folge von Kanten
Kreis	gleicher Anfangs- und Endpunkt
einfacher Kreis	jede Kante höchstens einmal
Eulerweg	jede Kante genau einmal
Eulerkreis	jede Kante genau einmal
Hamiltonweg	jeden Knoten genau einmal
Hamiltonkreis	jeden Knoten genau einmal

*Satz von Dirac*  
 ein Graph mit  $n \geq 3$  Knoten mit  $\text{Grad} \geq n/2$  hat einen Hamiltonkreis

*Satz von Ore*  
 ein Graph mit  $n \geq 3$  mit  $\deg(v) + \deg(u) \geq n$  für jedes Paar  $u, v$  von nicht benachbarten Ecken hat einen Hamiltonkreis

## 9.9 Planare Graphen

wenn er sich ohne Kantenkreuzungen zeichnen lässt

## 9.10 Satz von Euler

Für ein zusammenhängender, planarer Graph mit  $|V|$  Knoten,  $|E|$  Kanten und  $|R|$  Regionen gilt:

$$2 = |V| - |E| + |R|$$

## 9.11 Satz von Kuratovsky

Ein Graph ist genau dann nicht planar, wenn er einen Untergraphen vom Typ  $K_{3,3}$  oder  $K_5$  enthält

## 9.12 Färbungen

$c: V \rightarrow C$  so dass  $c(u) \neq c(v)$  falls  $\{u, v\} \in E$

Abschätzung:  $1 \leq \chi(G) \leq \Delta(G) + 1$

Anzahl mögliche Färbungen mit  $x$  Farben:

Graph mit $E = \emptyset$	$P(G, x) = x^n$
Vollständiger Graph	$P(K_n, x) = x * \dots * (x - n + 1)$
Baum	$P(T_n, x) = x * (x - 1)^{n-1}$

## 9.13 Dekompositionsgleichung

Graph  $G = (V, E)$  mit Kante  $e = a, b$

$G - e$	Graph $G$ unter Weglassung der Kante $e$
$G_e$	Graph $G$ mit zusammengezogener Kante $e$ unter Weglassung aller parallelen Kanten

Anzahl Färbungen von  $G$  mit  $x$  Farben:  
 $P(G, x) = P(G - e, x) - P(G_e, x)$

*Ziel:*

Rückführung des Graphen auf Bäume und vollständige Graphen mit erchenbarer Anzahl von Färbungen

*Chromatische Zahl eines Graphen:*

$$\chi(G) = \min\{x \in \mathbb{N} : P(G, x) > 0\}$$

## 9.14 Gerüste / Spannbäume

zusammenhängender, kreisfreier Unterbaum, der alle Knoten aus  $V$  enthält

$G - e$	Graph $G$ unter Weglassung der Kante $e$
$G/e$	Graph $G$ unter Zusammenziehung der Kante $e$ und Weglassen aller Schlingen

Anzahl der Gerüste des Graphen:

$$G: t(G) = t(G - e) + t(G/e)$$

*Ziel:*

Rückführung des Graphen  $G$  auf Kreise und Bäume mit bekannter/erchenbarer Anzahl Gerüste