

Diskrete Mathematik

Patrick Bucher & Lukas Arnold

2. Juni 2017

Inhaltsverzeichnis

1 Foundations	1
1.1 Operationen	1
1.2 Prioritäten der Operationen	1
1.3 Tautologie & Kontraktion	1
1.4 Logische Äquivalenzgesetze	2
1.5 Äquivalenzgesetze	2
1.6 Quantifikatoren	2
1.7 Negation von Quantifikatoren	2
1.8 Beweise	2
2 Basic Structures	2
2.1 Mengen	2
2.2 Spezielle Mengen	2
2.3 Mengenoperationen	2
2.4 Rechenregeln für Mengen	2
2.5 Definition von Funktionen	2
2.6 Arten von Funktionen	2
2.7 Zusammengesetzte Funktion	2
2.8 Umkehrfunktion	2
2.9 Folgen	3
2.10 Reihen	3
2.11 Summenformeln	3
3 Fundamentals	3
3.1 Wachstum von Funktionen	3
3.2 Exponentialfunktionen	3
3.3 Logarithmusfunktionen	3
3.4 Komplexität von Algorithmen	3
3.5 Zahlen und Division	3
3.6 Primzahl	3
3.7 Mersenne Primes	3
3.8 Primzahlsatz	3
3.9 ggT und kgV	3
3.10 Kongruenz	3
4 Diskrete Wahrscheinlichkeitsrechnung	3
4.1 Wahrscheinlichkeit nach Laplace	3
4.2 Komplement der Wahrscheinlichkeit	3
4.3 Additionsregel	3
4.4 Bedingte Wahrscheinlichkeit	3
4.5 Unabhängige Ereignisse	3
4.6 Satz der totalen Wahrscheinlichkeit	3
4.7 Satz von Bayes	3
4.8 Binomialverteilung	4
4.9 Hypergeometrische Verteilung	4
4.10 Poissonverteilung	4

4.11 Verteilung einer Zufallsvariablen	4
4.12 Erwartungswert einer Zufallsvariable	4
4.13 Varianz einer Zufallsvariable	4
4.14 Standardabweichung einer Zufallsvariable	4

5 Advanced Counting Techniques	4
5.1 Rekursionsbeziehungen	4
5.2 Erzeugende Funktion	4
5.3 Ein- / Ausschlussprinzip	4
5.4 Anzahl Derangements	4

6 Zahlentheorie	4
6.1 Division mit Rest	4
6.2 Kongruenz modulo n	4
6.3 Euklidischer Algorithmus	4
6.4 Diophantische Gleichung	4
6.5 erweiterter Euklidischer Algorithmus	4
6.6 Chinesischer Restsatz	4
6.7 Eulersche ϕ -Funktion	4
6.8 Primzahl	4
6.9 kleiner Satz von Fermat	4
6.10 Primzahltest von Wilson	4

7 Graphentheorie 1	5
7.1 (Ecken)grade	5
7.2 Wichtige Graphen	5
7.3 Baum	5
7.4 Page-Rank-Algorithmus	5
7.5 Matrizen	5
7.6 Wege und Kreise	5

8 Graphentheorie 2	5
---------------------------	----------

9 Graphentheorie 3	5
---------------------------	----------

1 Foundations

1.1 Operationen

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

1.2 Prioritäten der Operationen

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

1.3 Tautologie & Kontraktion

Tautologie	$p \vee \neg p$	immer wahre Aussage
Kontraktion	$p \wedge \neg p$	immer falsche Aussage

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}	$= \{p/q \mid p \in \mathbb{Z} \wedge q \in \mathbb{N}\}$
\mathbb{R} :	die Menge der reellen Zahlen
\mathbb{C} :	die Menge der komplexen Zahlen

2.2 Spezielle Menegen

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 Elmenete von A
Potenzmenge:	$P(S) = 2^S = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
Kreuzprodukt:	$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

2.3 Mengenoperationen

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

2.4 Rechenregeln für Mengen

Kommutativgesetz	$A \cup B = B \cup A$
Kommutativgesetz	$A \cap B = B \cap A$
Assoziativgesetz	$A \cup (B \cup C) = (A \cup B) \cup C$
Assoziativgesetz	$A \cap (B \cap C) = (A \cap B) \cap C$
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 Faktionen

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

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

$$\begin{aligned} g : X &\rightarrow U & x &\mapsto g(x) \\ f : U &\rightarrow Y & u &\mapsto g(u) \\ F = f \circ g : X &\rightarrow Y & x &\mapsto f(g(x)) \end{aligned}$$

2.8 Umkehrfunktion

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

$$\begin{aligned} (f^{-1} \circ f)(x) &= f^{-1}(f(x)) = x \\ (f^{-1} \circ f)(y) &= f^{-1}(f(y)) = y \end{aligned}$$

2.9 Folgen

$$\begin{aligned} \text{harmonisch} & \quad a_k = 1/k \\ \text{geometrisch} & \quad a_k = a_0 * q^k \\ \text{arithmetisch} & \quad a_k = a_0 + (k * d) \end{aligned}$$

2.10 Reihen

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

2.11 Summenformeln

$$\begin{aligned} \sum_{k=1}^n k & \quad \frac{n*(n+1)}{2} \\ \sum_{k=1}^n k^2 & \quad \frac{n(n+1)(2n+1)}{6} \\ \sum_{k=1}^n k^3 & \quad \frac{n^2(n+1)^2}{4} \\ \sum_{k=0}^n x^k, |x| < 1 & \quad \frac{1}{1-x} \\ \sum_{k=1}^n kx^{k-1}, |x| < 1 & \quad \frac{1}{(1-x)^2} \end{aligned}$$

3 Fundamentals

3.1 Wachstum von Funktionen

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

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

$$\begin{aligned} \text{konstant} & \quad O(1) \\ \text{logarithmisch} & \quad O(\log n) \\ \text{linear} & \quad O(n) \\ n \log n & \quad O(n * \log n) \\ \text{polynomial} & \quad O(n^b) \\ \text{exponentiell} & \quad O(b^n), b > 1 \\ \text{faktorielle} & \quad O(n!) \end{aligned}$$

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

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

4 Diskrete Wahrscheinlichkeitsrechnung

4.1 Wahrscheinlichkeit nach Laplace

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

4.2 Komplement der Wahrscheinlichkeit

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

4.3 Additionsregel

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

4.4 Bedingte Wahrscheinlichkeit

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

4.5 Unabhängige Ereignisse

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

4.6 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:

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

4.7 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:

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

4.8 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:

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

4.9 Hypergeometrische Verteilung

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

4.10 Poissonverteilung

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

Bedingung:

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

4.11 W'keitsverteilung einer Zufallsvariablen

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

4.12 Erwartungswert einer Zufallsvariable

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

4.13 Varianz einer Zufallsvariable

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

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

4.14 Standardabweichung einer Zufallsvariable

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

5 Advanced Counting Techniques

5.1 Rekursionsbeziehungen

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

5.2 Erzeugende Funktion

$$G(x) = \sum_{k=0}^{\infty} a_k x^k$$

5.3 Ein- / Ausschlussprinzip

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

5.4 Anzahl Derangements

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

6 Zahlentheorie

6.1 Division mit Rest

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

6.2 Kongruenz modulo n

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

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

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

6.3 Euklidische Algorithmus

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

6.4 Diophantischer Gleichung

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

6.5 erweiterter Euklidischer Algorithmus

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

6.6 Chinesischer Restsatz

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

$$M_i * y_1 \equiv 1 \pmod{m_i}$$

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

6.7 Eulersche ϕ -Funktion

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

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

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

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

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

6.8 Primzahl

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

6.9 kleiner Satz von Fermat

$$m^p \bmod p = m \bmod p$$

6.10 Primzahltest von Wilson

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

7 Graphentheorie 1

7.1 (Ecken)grade

Eckengrad: $\sum_{v \in V} \deg(v) = 2 \cdot |E|$

Maximalgrad: $\Delta(G) = \max_{v \in V(G)} \deg(v)$

Maximalgrad: $\delta(G) = \min_{v \in V(G)} \deg(v)$

7.2 Wichtige Graphen

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

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

7.3 Baum

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.

7.4 Page-Rank-Algorithmus

Gewicht der Seite PR_i in einem Netz mit N Seiten, Dämpfungsfaktor d ($[0; 1]$), C_j von Seite j abgehende Links:

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

7.5 Matrizen

n Ecken, m Kanten

Adjazenzmatrix $A(G)$: $n \times n$ -Matrix (Knoten/Knoten) mit Anzahl Kanten zwischen den Ecken.

Inzidenzmatrix $B(G)$: $n \times m$ -Matrix (Knoten/Kanten) mit 1 (Knoten liegt auf Kante) oder 0 (Knoten *nicht* auf Kante)

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

7.6 Wege und Kreise

Weg: Folge von Kanten $e_1 = a, b, e_2 = b, c, \dots$

Kreis: Weg mit übereinstimmendem Anfangs- und Endpunkt (Länge > 0)

einfacher Kreis: jede Kante kommt höchstens einmal vor
TODO: p.49/62

Eulerweg: Weg, der jede Kante einmal durchläuft

Eulerkreis: Kreis, der jede Kante einmal durchläuft

Hamiltonweg: Weg, der jeden Knoten einmal durchläuft
Hamiltonkreis: Kreis, der jeden Knoten einmal durchläuft

Satz von Dirac: ein Graph mit $n \geq 3$ Knoten mit Grad $\geq n/2$ hat einen Hamiltonkreis.

Satz von Ore: TODO p. 62

8 Graphentheorie 2

TODO: Päd

9 Graphentheorie 3

TODO: Päd