Diskrete Mathematik

Patrick Bucher & Lukas Arnold

5. Juni 2017

Inhaltsverzeichnis

1 Foundations

1.1 Operationen

Negation	$\neg p$	*Verneinung*
Konkunktion	$p \wedge q$	*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	$p \wedge \neg q$	*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

$$
\begin{aligned}
p \rightarrow q &\equiv \neg p \vee q \\
p \rightarrow q &\equiv \neg q \rightarrow \neg p \\
p \vee q &\equiv \neg p \rightarrow q \\
p \wedge q &\equiv \neg(p \rightarrow \neg q) \\
\neg(p \rightarrow q) &\equiv p \wedge \neg q \\
\\
p \leftrightarrow q &\equiv (p \rightarrow q) \wedge (q \rightarrow p) \\
p \leftrightarrow q &\equiv \neg p \leftrightarrow \neg q \\
p \leftrightarrow q &\equiv (p \wedge q) \vee (\neg p \wedge \neg q) \\
\neg(p \leftrightarrow q) &\equiv p \leftrightarrow \neg q \\
\\
p \rightarrow (q \wedge r) &\equiv (p \rightarrow q) \wedge (p \rightarrow r) \\
(p \vee q) \rightarrow r &\equiv (p \rightarrow r) \wedge (q \rightarrow r) \\
p \rightarrow (q \vee r) &\equiv (p \rightarrow q) \vee (p \rightarrow r) \\
(p \wedge q) \rightarrow r &\equiv (p \rightarrow r) \vee (q \rightarrow r) \\
\\
p \oplus q &\equiv (p \vee q) \wedge (\neg p \vee \neg q) \\
\neg(p \oplus q) &\equiv (p \wedge q) \vee (\neg p \wedge \neg q) \\
\neg(p \oplus q) &\equiv p \leftrightarrow q
\end{aligned}
$$

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

2 Basic Structures

2.1 Mengen

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

2.2 Spezielle Menegen

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

2.3 Mengenoperationen

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

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 Fuktionen

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

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

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

$g : X \to U$	$x \mapsto g(x)$
$f : U \to Y$	$u \mapsto g(u)$
$F = f \circ g : X \to Y$	$x \mapsto f(g(x))$

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 Folgen

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

2.10 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	$\sum_{k=0}^{n-1} (a_0 + kd) = n \frac{a_0 + a_{n-1}}{2}$

2.11 Summenformeln

$\sum_{k=1}^{n} k$	$\frac{n*(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{n} x^k, \lvert x\rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{n} kx^{k-1}, \lvert x\rvert < 1$	$\frac{1}{(1-x)^2}$

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

$a^r * a^s = a^{r+s}$
$\frac{a^r}{a^s} = a^{r-s}$
$(a^r)^s = (a^s)^r = a^{r*s}$

3.3 Logarithmusfunktionen

$log_a(u * v) = log_a(u) + log_a(v)$
$log_a(\frac{u}{v}) = log_a(u) - log_a(v)$
$log_a(u^v) = v * log_a(u)$

3.4 Komplexität von Algorithmen

konstant	$O(1)$
logarithmisch	$O(logn)$
linear	$O(n)$
n log n	$O(n * logn)$
polynomial	$O(n^b)$
exponentiell	$O(b^n), b > 1$
faktorielle	$O(n!)$

3.5 Zahlen und Division

$a|b \wedge a|c \rightarrow a|(b + c)$
$a|b \rightarrow \forall c(a|bc)$
$a|b \wedge b|c \rightarrow a|c$

3.6 Primzahl

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

3.7 Mersenne Primes

$M_n = 2^p - 1, p \in$ ”*Primzahlen*“

3.8 Primzahlsatz

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

3.9 ggT und kgV

$a = dq + r$, wobei $(0 \leq r < d)$
$q = a$ div d und $r = a$ mod d
$ab = ggT(a, b) * kgV(a, b)$

3.10 Kongruenz

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

4 Diskrete Wahrscheinlichkeitsrechnung

4.1 Wahrscheindlichkeit nach Laplace

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

4.2 Komplement der Wahrscheindlichkeit

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

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 Wahrscheindlichkeit

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

Spezialfall für 2 Mengen:
$p(A) = p(A|B) \cdot p(B) + p(A|\overline{B}) \cdot p(\overline{B})$

4.7 Satz von Bayes

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

Spezialfall für 2 Mengen:
$p(B|A) = \frac{P(A|B)\ p(B)}{p(A|B) \cdot p(B) + p(A|\neg B) \cdot p(\overline{B})}$

4.8 Binomialverteilung

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

Bedingung:
$p = M/N$ und $n <= M/10 <= (N - M)/10$

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:
$u = np$ und $p <= 0.1, n >= 100$

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

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

5 Advanced Counting Techniques

5.1 Rekursionsbeziehungen

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

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

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

6 Zahlentheorie

6.1 Division mit Rest

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

6.2 Kongruenz modulo n

$$\begin{aligned} a \equiv b(\mod n) &\iff n|(a-b) \\ &\iff \exists q : a - b = q * n \\ &\iff \exists q : a = b + q * n \end{aligned}$$

6.3 Euklidsche Algorithmus

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

6.4 Diophantischer Gleichung

$n_1 * x + n_2 * y = n$

6.5 erweiterter Euklidsche Algorithmus

67	**-**	**1**	**0**	
24	2 *	**0**	**1**	
19 *	1	1 *	-2 *	*19 = 67 % 24*
5	4	-1	3	*2 = 67 div 24*
4	1	4	-11	*1 = 1 - 2 * 0*
1		-5	14	*-2 = 0 - 2 * 1*

6.6 Chinesischer Restsatz

$M_i = \frac{m}{m_i}$
$M_i * y_1 \equiv 1(\mod m_i)$
$x = \sum_{i=1}^{k} r_i * M_i * y_i$

6.7 Eulersche ϕ-Funktion

$\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$
$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n | x > 0$ und $ggT(x, n) = 1\}$
$|\mathbb{Z}_n^*| :=$ Anzahl Elemente in $\mathbb{Z}_n^*$

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

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

6.8 Primzahl

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

6.9 kleiner Satz von Fermat

$m^p \mod p = m \mod p$

6.10 Primzahltest von Wilson

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

6.11 Restklassen

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

6.12 Rechenregeln für modularen Rechnen

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

6.13 Potenzieren modulo n

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

6.14 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 Multipliziere
6. Exponent einsetzten
7. entsprechend Quadrieren und Multiplizieren
8. immer wieder modular reduzieren

6.15 Nullteiler

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

6.16 Inverse Elemente

$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | ggT(a, n) = 1\}$
$a^{-1} = R_p(a^{p-2}) = a^{p-2} \mod p$, ($p$ = Primzahl)

6.17 Primitive Elemente / Erzeugende

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

6.18 Einwegfunktionen

Quadrieren modulo n	$x \mapsto x^2 \mod n$
Potenzieren modulo n	$x \mapsto x^e \mod n$
Exponentialfunktion modulo p	$x \mapsto b^x \mod p$

6.19 Modulare Quadratwurzeln

$\sqrt{a} \mod n = \{x \in \mathbb{Z}_n^* | x^2 = a \mod n\}$
=> Für ein a kann es mehrere Quadratwurzeln geben

6.20 diskrete Logarithmus

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

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

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

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

- Weg: Folge von Kanten $e_1 = a, b, e_2 = b, c, \ldots$
- Kreis: Weg mit übereinstimmendem Anfangs- und Endpunkt (Länge > 0)
- einfacher Kreis: jede Kante kommt höchstens einmal vor
- 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: 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.

8 Graphentheorie 2

8.1 Satz von Euler

Für ein zusammenhängender, planarer Graph G mit $|V|$ Knoten, $|E|$ Kanten und $|R|$ Regionen gilt:
$2 = |V| - |E| + |R|$

8.2 Satz von Kuratovsky

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

8.3 Färbungen

Anzahl mögliche Färbungen des Graphen G mit x Farben: $P(G, x)$

- Graph G mit n Knoten und leerer Kantenmenge: $P(G, x) = x^n$
- Vollständiger Graph G mit n Knoten: $P(K_n, x) = x \cdot (x-1) \cdot (x-2) \cdots (x-n+1)$
- Baum mit n Knoten: $P(T_n, x) = x \cdot (x-1)^{n-1}$

8.4 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 G auf Bäume (T) und vollständige Graphen (K) mit errechenbarer Anzahl von Färbungen

Chromatische Zahl eines Graphen: $\chi(G) = min\{x \in \mathbb{N} : P(G,x) > 0\}$ (das kleinste x, wofür das chromatische Polynom P eine positive Zahl liefert)

8.5 Gerüste

- Gerüst oder Spannbaum eines Graphen $G = (V, E)$: zusammenhängender, kreisfreier Unterbaum, der alle Knoten aus V enthält.
- Baum: 1 Gerüst
- Kreis mit n Kanten: je ein Gerüst durch Entfernung einer Kante (n Gerüste)
- $G - e$: 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/errechenbarer Anzahl Gerüste

9 Graphentheorie 3

TODO: Pädu