Diskrete Mathematik

Patrick Bucher & Lukas Arnold

5. Juni 2017

| Inhaltsverzeichnis | | | | | $4.11\ \ W'ke its verteilung\ einer\ Zufalls variablen\ .$ | | 4 |
|--------------------|------|--|---|---|--|--|---------------|
| | | and a the man | • | | | Erwartungswert einer Zufallsvariable | 4 |
| 1 | | ndations | 2 | | | Varianz einer Zufallsvariable | 4 |
| | 1.1 | Operationen | 2 | | 4.14 | Standardabweichung einer Zufallsvariable | 4 |
| | 1.2 | Prioritäten der Operationen | 2 | _ | | | |
| | 1.3 | Tautologie & Kontraktion | 2 | 5 | | inced Counting Techniques | 4 |
| | 1.4 | Logische Äquivalenzgesetze | 2 | | | Rekursionsbeziehungen | 4 |
| | 1.5 | Äquivalenzgesetze | 2 | | | Erzeugende Funktion | 4 |
| | 1.6 | Quantifikatoren | 2 | | | Ein- / Ausschlussprinzip | 4 |
| | 1.7 | Negation von Quantifikatoren | 2 | | 5.4 | Anzahl Derangements | 4 |
| | 1.8 | Beweise | 2 | • | 7-61 | a walka a sui a | |
| 2 | Rac | ic Structures | 2 | 6 | | entheorie Division mit Rest | 4 4 |
| _ | 2.1 | | 2 | | | Kongruenz modulo n | 4 |
| | | Mengen | | | | | |
| | 2.2 | Spezielle Menegen | 2 | | | Euklidsche Algorithmus | 4 |
| | 2.3 | Mengenoperationen | 2 | | | Diophantischer Gleichung | 4 |
| | 2.4 | Rechenregeln für Mengen | 2 | | | erweiterter Euklidsche Algorithmus | 4 |
| | 2.5 | Definition von Fuktionen | 3 | | | Chinesischer Restsatz | 4 |
| | 2.6 | Arten von Funktionen | 3 | | | Eulersche ϕ -Funktion | 5 |
| | 2.7 | Zusammengesetzte Funktion | 3 | | | Primzahl | 5 |
| | 2.8 | Umkehrfunktion | 3 | | 6.9 | kleiner Satz von Fermat | 5 |
| | 2.9 | Folgen | 3 | | 6.10 | Primzahltest von Wilson | 5 |
| | 2.10 | Reihen | 3 | | | | |
| | | Summenformeln | 3 | 7 | - | hentheorie 1 | 5 |
| | | | | | | (Ecken)grade | 5 |
| 3 | Fun | damentals | 3 | | 7.2 | Wichtige Graphen | 5 |
| | 3.1 | Wachstum von Funktionen | 3 | | 7.3 | Baum | 5 |
| | 3.2 | Exponentialfunktionen | 3 | | 7.4 | Page-Rank-Algorithmus | 5 |
| | 3.3 | Logarithmusfunktionen | 3 | | 7.5 | Matrizen | 5 |
| | 3.4 | Komplexität von Algorithmen | 3 | | 7.6 | Wege und Kreise | 5 |
| | 3.5 | Zahlen und Division | 3 | | | | |
| | 3.6 | Primzahl | 3 | 8 | Grap | hentheorie 2 | 5 |
| | 3.7 | Mersenne Primes | 3 | | | | |
| | 3.8 | Primzahlsatz | 3 | 9 | Grap | hentheorie 3 | 5 |
| | 3.9 | ggT und kgV | 3 | | | | |
| | | Kongruenz | 3 | | | | |
| 4 | | | | | | | |
| 4 | | wrete Wahrscheinlichkeitsrechnung Wahrscheindlichkeit nach Laplace | 3 | | | | |
| | 4.1 | | 3 | | | | |
| | 4.2 | Komplement der Wahrscheindlichkeit | 3 | | | | |
| | 4.3 | Additionsregel | 3 | | | | |
| | 4.4 | Bedingte Wahrscheinlichkeit | 3 | | | | |
| | 4.5 | Unabhängige Ereignisse | 4 | | | | |
| | 4.6 | Satz der totalen Wahrscheindlichkeit | 4 | | | | |
| | 4.7 | Satz von Bayes | 4 | | | | |
| | 4.8 | Binomialverteilung | 4 | | | | |
| | 4.9 | Hypergeometrische Verteilung | 4 | | | | |
| | 4.10 | Poissonverteilung | 4 | | | | |

1 Foundations

1.1 Operationen

| Negation | $\neg p$ | Verneinung |
|---------------|-----------------------|---------------------|
| Konkunktion | $p \wedge q$ | Und-Verknüpfung |
| Disjunktion | $p \lor q$ | 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

1.3 Tautologie & Kontraktion

Tautologie $p \lor \neg p$ immer wahre Aussage Kontraktion $p \land \neg q$ immer falsche Aussage

1.4 Logische Äquivalenzgesetze

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

1.5 Äquivalenzgesetze

$$p \rightarrow q \equiv \neg p \lor q$$

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

$$p \lor q \equiv \neg p \rightarrow q$$

$$p \land q \equiv \neg (p \rightarrow \neg q)$$

$$\neg (p \rightarrow q) \equiv p \land \neg q$$

$$p \leftrightarrow q \equiv (p \rightarrow q) \land (q \rightarrow p)$$

$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$

$$p \leftrightarrow q \equiv (p \land q) \lor (\neg p \land \neg q)$$

$$\neg (p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

$$p \leftrightarrow q \equiv (p \land q) \lor (\neg p \land \neg q)$$

$$\neg (p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

$$p \rightarrow (q \land r) \equiv (p \rightarrow q) \land (p \rightarrow r)$$

$$(p \lor q) \rightarrow r \equiv (p \rightarrow r) \land (q \rightarrow r)$$

$$p \rightarrow (q \lor r) \equiv (p \rightarrow q) \lor (p \rightarrow r)$$

$$(p \land q) \rightarrow r \equiv (p \rightarrow q) \lor (p \rightarrow r)$$

$$(p \land q) \rightarrow r \equiv (p \rightarrow q) \lor (p \rightarrow r)$$

$$(p \land q) \rightarrow r \equiv (p \land q) \lor (\neg p \lor \neg q)$$

$$\neg (p \oplus q) \equiv (p \land q) \lor (\neg p \land \neg q)$$

$$\neg (p \oplus q) \equiv p \leftrightarrow q$$

1.6 Quantifikatoren

For All \forall für alle \mathbf{x} aus \mathbf{P} wahr

Exists \exists für mindestens ein \mathbf{x} aus \mathbf{P} wahr

Not Exists $\neg \exists$ für alle \mathbf{x} aus \mathbf{P} falsch

Not For All $\neg \forall$ für mindestens ein \mathbf{x} aus \mathbf{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

 $\begin{array}{ll} \text{direkter Beweis} & p \rightarrow q \\ \text{indirekter Beweis} & \neg q \rightarrow \neg p \\ \text{Widerspruch} & \neg p \rightarrow q \\ \textit{Vorgehen Widerspruch} & (\neg p \rightarrow \mathbf{f}) \Rightarrow (p \rightarrow \mathbf{w}) \end{array}$

2 Basic Structures

2.1 Mengen

$$\begin{split} \mathbb{N} &= \{1,2,\dots\} \\ \mathbb{N}_0 &= \{0,1,2,\dots\} \\ \mathbb{Z} &= \{\dots,-1,0,1,2,\dots\} \\ \mathbb{Z}^+ &= \{1,2,\dots\} \\ \mathbb{Q} &= \{p/q|p \in Z \land q \in N\} \\ \mathbb{R} \text{: die Menge der komplexen Zahlen} \\ \mathbb{C} \text{: die Menge der komplexen Zahlen} \end{split}$$

2.2 Spezielle Menegen

Teilmenge: $A \subset B \equiv \forall x (x \in A \to x \in B)$ Leere Menge: $\emptyset \subset A \ gilt \ fiir \ jede \ Menge \ A$ Kardinalität: |S| beschreibt Anzahl Elmenete von APotenzmenge: $P(S) = 2^S = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ Kreuzprodukt: $A \times B = \{(a, b) | a \in A \land b \in B\}$

2.3 Mengenoperationen

 $\begin{array}{ll} \text{Komplement:} & A^c = \overline{A} = \{m \in M : m \notin A\} \\ \text{Durchschnitt:} & A \cap B = \{m \in M | m \in A \wedge m \in B\} \\ \text{Vereinigung:} & A \cup B = \{m \in M | m \in A \vee m \in B\} \\ \text{Differenz:} & B - A = \{m \in M | m \in B \wedge m \notin A\} \\ \end{array}$

2.4 Rechenregeln für Mengen

 $\begin{array}{lll} \text{Kommutativgesetz} & A \cup B = B \cup A \\ \text{Kommutativgesetz} & A \cap B = B \cap A \\ \text{Assoziativgesetz} & A \cup (B \cup C) = (A \cup B) \cup C \\ \text{Assoziativgesetz} & A \cap (B \cap C) = (A \cap B) \cap C \\ \text{Distributivgesetz} & A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ \text{De Morgan's Gesetz} & \overline{A \cup B} = \overline{A} \cap \overline{B} \\ \text{De Morgan's Gesetz} & \overline{A \cap B} = \overline{A} \cup \overline{B} \\ \end{array}$

2.5 Definition von Fuktionen

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

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

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

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

2.8 Umkehrfunktion

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

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

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

2.11 Summenformeln

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

3 Fundamentals

3.1 Wachstum von Funktionen

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

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

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

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

$$\not\exists a(a|n^{(1)} < a < n)$$

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 $(0 \le r < d)$
 $q = a$ 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

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

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

Bedingung:

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

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:

$$u = np \text{ und } p \le 0.1, n \ge 100$$

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

$$\begin{array}{l} V(X) = \sum_{s \in S} (X(s) - E(X))^2 \cdot p(s) \\ V(X) = \sum_{r \in X(S)} (r - E(X))^2 \cdot p(X = r) \end{array}$$

4.14 Standardabweichung einer Zufallsvariable

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

5 Advanced Counting Techniques

5.1 Rekursionsbeziehungen

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

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

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

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 Euklidsche Algorithmus

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 $2 = 67 \text{ div } 24$
4 1 4 -11 $1 = 1 - 2 * 0$
1 -5 14 -2 = 0 - 2 * 1

6.6 Chinesischer Restsatz

$$\begin{aligned} M_i &= \frac{m}{m_i} \\ M_i * y_1 &\equiv 1 \pmod{m_i} \\ x &= \sum_{i=1}^k r_i * M_i * y_i \end{aligned}$$

6.7 Eulersche ϕ -Funktion

$$\begin{split} & \mathbb{Z}_n := \{0,1,2,\dots,n-1\} \\ & \mathbb{Z}_n^* := \{x \in \mathbb{Z}_n | x > 0 \text{ und } ggT(x,n) = 1\} \\ & |\mathbb{Z}_n^*| := \text{Anzahl Elemente in } \mathbb{Z}_n^* \\ & \phi : \mathbb{N} \to \mathbb{N}, n \mapsto |\mathbb{T}_n^*| =: \phi(n) \\ & \phi(p) &= p-1 \\ & \phi(p*q) &= (p-1)*(q-1) \\ & \phi(m) &= (p_1-1)*p_1^{r_1-1}*(p_2-1)*p_2^{r_2-1}*\dots \end{split}$$

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

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

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). ... $\binom{n}{n}$ $\binom{(n-1)n}{n}$

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

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

- ullet 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 $e_1 = a, b, e_2 = b, c, \dots$
- 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

TODO: Pädu

9 Graphentheorie 3

TODO: Pädu