

# Diskrete Mathematik

Patrick Bucher & Lukas Arnold

18. Mai 2017

## Inhaltsverzeichnis

<b>1 Foundations</b>	<b>1</b>
1.1 Operationen . . . . .	1
1.2 Prioritäten der Operationen . . . . .	1
1.3 Tautologie & Kontraktion . . . . .	1
1.4 Logische Äquivalenzgesetze . . . . .	1
1.5 Äquivalenzgesetze . . . . .	2
1.6 Quantifikatoren . . . . .	2
1.7 Negation von Quantifikatoren . . . . .	2
1.8 Beweise . . . . .	2
<b>2 Basic Structures</b>	<b>2</b>
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 . . . . .	2
2.10 Reihen . . . . .	2
2.11 Summenformeln . . . . .	3
<b>3 Fundamentals</b>	<b>3</b>
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
<b>4 Diskrete Wahrscheinlichkeitsrechnung</b>	<b>3</b>
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 . . . . .	3
4.9 Hypergeometrische Verteilung . . . . .	3
4.10 Poissonverteilung . . . . .	4

4.11 W'keitsverteilung einer Zufallsvariablen . . . . .	4
4.12 Erwartungswert einer Zufallsvariable . . . . .	4
4.13 Varianz einer Zufallsvariable . . . . .	4
4.14 Standardabweichung einer Zufallsvariable . . . . .	4

## 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

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

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

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

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

## 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

$$\begin{aligned} \neg\exists x P(x) &\equiv \forall x \neg P(x) \\ \neg\forall x P(x) &\equiv \exists x \neg P(x) \end{aligned}$$

## 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 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 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 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

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

## 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

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

## 2.10 Reihen

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

## 2.11 Summenformeln

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

## 3 Fundamentals

### 3.1 Wachstum von Funktionen

TODO

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

### 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

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

## 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

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

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

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

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**

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