

Diskrete Mathematik | DMI

Zusammenfassung

INHALTSVERZEICHNIS

1. Aussagenlogik	2
1.1. Glossar	2
1.2. Formeln	2
1.3. Rechenregeln	3
2. Prädikatenlogik	3
2.1. Glossar	3
3. Beweisen	3
3.1. Induktion	3
3.1.1. Techniken	4
4. Direkte, iterative und rekursive Berechnungen	4
4.1. Glossar	4
5. Mengen	4
5.1. Glossar	4
5.2. Rechenregeln	4
6. Formeln, Abbildungen, Relationen	5
6.1. Glossar	5
7. Modulo-Rechnen	5
7.1. Glossar	6
7.2. Rechenregeln	6
7.3. Primfaktorenzerlegung	6
7.4. Euklidischer Algorithmus	6
7.4.1. Beispiel	6
7.5. Erweiterter Euklidischer Algorithmus	7
7.5.1. Beispiel	7
7.6. Kleiner Fermat	7
7.7. Satz von Euler	7
7.7.1. Euler'sche φ -Funktion (Totient)	7
7.7.1.1. Rechenregeln	8
7.8. RSA Verschlüsselung	8

1. AUSSAGENLOGIK

1.1. GLOSSAR

<i>Begriff</i>	<i>Bedeutung</i>
Aussage	<ul style="list-style-type: none"> – Feststellender Satz, dem eindeutig «wahr» oder «falsch» zugeordnet werden kann – Symbole wie A, B, C... werden dafür verwendet
Aussagenlogische Form	– Kombination von Aussagen, verknüpft durch Junktoren
Aussageform	– Aussagen verknüpft mit Variablen
Normalform	– Standardisierte Aussagenlogische Formen (Formeln)
Negationsnormalform	– \neg steht ausschliesslich direkt vor Aussagen oder Konstanten
Verallgemeinerte Disjunktion	<ul style="list-style-type: none"> – Einzelne Aussage oder Negation – wahr oder falsch – Disjunktion $A \vee B$, falls A und B selbst verallgemeinerte Disjunktionen sind
Verallgemeinerte Konjunktion	<ul style="list-style-type: none"> – Einzelne Aussage oder Negation – wahr oder falsch – Konjunktion $A \wedge B$, falls A und B selbst verallgemeinerte Konjunktionen sind
Disjunktive Normalform	– Disjunktion von (oder eine einzelne) verallgemeinerten Konjunktionen
Konjunktive Normalform	– Konjunktion von (oder eine einzelne) verallgemeinerten Disjunktionen
Kontradiktion	– Immer falsch
Tautologie	– Immer wahr
Junktoren (/Konnektoren)	<ul style="list-style-type: none"> – \neg Negation – \wedge Konjunktion – \vee Disjunktion (einschliessliches oder!) – \Rightarrow Implikation – \Leftrightarrow Äquivalenz
Abtrennungsregel	– $(A \wedge (A \Rightarrow B)) \Rightarrow B$
Bindungsstärke	– \neg vor \wedge, \vee vor $\Rightarrow, \Leftrightarrow$

1.2. FORMELN

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$$

$$(A \Leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$$

$$\neg(A \Rightarrow B) \Leftrightarrow A \wedge \neg B$$

$$A \vee (\neg A \wedge B) \Leftrightarrow A \vee B$$

$$\text{Abtrennungsregel: } A \wedge (A \Rightarrow B) \Rightarrow B$$

1.3. RECHENREGELN

Begriff	Bedeutung
Kommutativität	<ul style="list-style-type: none"> – $(A \wedge B) \Leftrightarrow (B \wedge A)$ – $(A \vee B) \Leftrightarrow (B \vee A)$
Assoziativität	<ul style="list-style-type: none"> – $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$ – $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$
Distributivität	<ul style="list-style-type: none"> – $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ – $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
Absorption	<ul style="list-style-type: none"> – $A \vee (A \wedge B) \Leftrightarrow A$ – $A \wedge (A \vee B) \Leftrightarrow A$
Idempotenz	<ul style="list-style-type: none"> – $A \vee A = A$ – $A \wedge A = A$
Doppelte Negation	– $\neg(\neg A) \Leftrightarrow \neg\neg A \Leftrightarrow A$
Konstanten	<ul style="list-style-type: none"> – W=wahr – F=falsch
???	– $(A \Rightarrow B \Rightarrow C) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow C)$
de Morgan	<ul style="list-style-type: none"> – $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ – $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

2. PRÄDIKATENLOGIK

2.1. GLOSSAR

Begriff	Bedeutung
Subjekt	– «Konkretes Ding» / Stellvertreter einer Variable
Prädikat	<ul style="list-style-type: none"> – «Eigenschaft», zB «ist eine Primzahl» – Prädikate werden oft wie Funktionen geschrieben. Ist P ein Prädikat, dann bedeutet $P(x)$, dass x das Prädikat erfüllt. $P(x)$ ist eine Aussageform.
Quantor	<ul style="list-style-type: none"> – \forall Allquantor (Für alle) – \exists Existenzquantor (Es existiert)

3. BEWEISEN

TODO: MEHR BEWEISE

3.1. INDUKTION

$$A(1) \wedge (A(n) \Rightarrow A(n+1)) \Rightarrow A(m), m \in \mathbb{N}$$

Beispiel: $2 \mid (6^n)$

- 1) Verankerung: $n = 0$
 - $2 \mid (6^0)$
- 2) Induktionsschritt $n \rightarrow n+1$
 - $2 \mid (6^{n+1})$
 - a) Induktionsannahme: $2 \mid (6^n)$
 - b) Behauptung: $2 \mid (6^{n+1})$

c) Beweis: Verwendung der Annahme, um Richtigkeit der Behauptung zu zeigen

3.1.1. Techniken

- 1) Direkter Beweis $f(n) = f_1(n) = f_2(n) = \dots = f_m(n) = g(n)$
- 2) Differenz gleich Null $f(n) - g(n) = 0 \Rightarrow f(n) = g(n)$
- 3) Äquivalenzumformung
- 4) Dritte Grösse (vereinfachen) $g(n) = h(n) = f(n)$

4. DIREKTE, ITERATIVE UND REKURSIVE BERECHNUNGEN

4.1. GLOSSAR

Begriff	Bedeutung
Folge	– Nummerierte Liste von Objekten (Folgegliedern)
Reihe	– Summe von Folgegliedern einer Zahlenfolge

5. MENGEN

5.1. GLOSSAR

Begriff	Bedeutung
Aufzählend	– $\{1, 2, 3\}$
Beschreibend	– $\{x \in \mathbb{N}^+ \mid x < 4\}$
Mächtigkeit	– Anzahl Elemente einer Menge – $ M $
Potenzmenge	– Menge aller Teilmengen einer Menge – $P(M)$ – $ P(M) = 2^{ M }$
Kartesisches Produkt	– $A \times B = \{(a, b) \mid a \in A, b \in B\}$

5.2. RECHENREGELN

Für die Mengen A und B in der Obermenge M gelten die folgenden Aussagen:

$$\overline{\overline{A}} = A$$

$$A \cap \overline{A} = \emptyset$$

$$A \cup \overline{A} = M$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

6. FORMELN, ABBILDUNGEN, RELATIONEN

6.1. GLOSSAR

Begriff	Bedeutung
Funktion/Abbildung	<ul style="list-style-type: none"> – Zuordnung, die jedem Element der Definitionsmenge D genau ein Element einer Zielmenge Z zuordnet. – Injektive Relation – $f : D \rightarrow Z$ – Abbildungen mit mehreren Argumenten: $f : A \times B \rightarrow Z, f(a, b) = y$
Graph	<ul style="list-style-type: none"> – Menge von Paaren $(x, f(x))$ – $G \in D \times Z$
Relation	<ul style="list-style-type: none"> – Teilmenge des Kartesischen Produktes mehrerer Mengen – $A = \prod_{i=1}^n A_i, A_i = n_i \Rightarrow A = \prod_{i=1}^n n_i$ – Kleiner-Relation: $R_{<} = \{(a, b) \mid a \in A, b \in B, a < b\}$ – Gleich-Relation: $R_{=} = \{(a, b) \mid a \in A, b \in B, a = b\}$ – Kleiner-Gleich-Relation: $R_{\leq} = R_{=} \cup R_{<} = \{(a, b) \mid a \in A, b \in B, a \leq b\}$
Surjektiv	– Alle Elemente der Definitions- und Zielmenge sind «verknüpft» / jedes Element der Bildmenge kommt als Bild vor
Injektiv	<ul style="list-style-type: none"> – Alle Inputs haben eindeutige Outputs – $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
Bijektiv	– Surjektiv und Injektiv
Reflexiv	<ul style="list-style-type: none"> – Alle Elemente von A stehen zu sich selbst in Beziehung – $a \in A \Rightarrow (a, a) \in R$ – $A \Leftrightarrow A$
Symmetrisch	<ul style="list-style-type: none"> – $(a, b) \in R \wedge (b, a) \in R$ – $(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A)$
Transitiv	<ul style="list-style-type: none"> – $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$ – $(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)$
Äquivalenzrelation	<ul style="list-style-type: none"> – reflexiv, symmetrisch und transitiv – $\Leftrightarrow, =$
Irreflexiv	– $a \in A \Rightarrow \neg(a, a) \in R$
Asymmetrisch	– $(a, b) \in R \Rightarrow \neg(b, a) \in R$
Antisymmetrisch	– $((a, b) \in R) \wedge ((b, a) \in R) \Rightarrow a = b$
Ordnungsrelation	<ul style="list-style-type: none"> – reflexiv, antisymmetrisch und transitiv – \leq
Symmetrische Differenz	<ul style="list-style-type: none"> – $A \Delta B = \{x \in G \mid (x \in A \cup B) \wedge \neg(x \in A \cap B)\}$ – $A \Delta B = (A \cup B) \setminus (A \cap B)$ – $(A \Delta B) \Delta C = A \Delta (B \Delta C)$

7. MODULO-RECHNEN

Die Modulo-Relation ist eine **Äquivalenzrelation** auf \mathbb{Z} .

7.1. GLOSSAR

Begriff	Bedeutung
Teiler-Relation	<ul style="list-style-type: none"> Für $a, b \in \mathbb{Z}$ ist die Teiler-Relation $b \mid a \Leftrightarrow T(b, a) \Leftrightarrow \exists q \in \mathbb{Z} : bq = a$ $b \mid a \Leftrightarrow -b \mid a$ $b \mid a \Leftrightarrow b \mid -a$ Ordnungsrelation auf \mathbb{N}
Modulo-Relation	Für $a, q, r \in \mathbb{Z}$ ist die Modulo-Relation $R_q(a, r) \Leftrightarrow q \mid a - r \Leftrightarrow a \equiv r \pmod{q}$
\sim	<ul style="list-style-type: none"> «relates to» $a \sim b \Leftrightarrow (a, b) \in R$
Quotient, Rest	<p>Zu jeder Zahl $a \in \mathbb{Z}$ und jeder Zahl $b \in \mathbb{Z}$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $a = q * b + r, 0 \leq r < b$</p> <p>Bsp: $7 = 2 * 3 + 1$</p> <p>q heisst Quotient</p> <p>r heisst Rest</p>
Restklassen	<ul style="list-style-type: none"> $[b]_q = \{a \in \mathbb{Z} \mid a \equiv b \pmod{q}, q > 0\}$ $\mathbb{Z}_q = \{[0]_q, [1]_q, [2]_q, \dots, [q-1]_q\} = \underbrace{\{0, 1, 2, 3, \dots, q-1\}}_{\text{Vereinfachung}}$
Multiplikatives Inverses	Für $a \in \mathbb{Z}_q$ ist $b \in \mathbb{Z}_q$ das multiplikative inverse von a , wenn $a * b \equiv 1 \pmod{q}$
Nullteiler	Wenn für $a, b \in \mathbb{Z}_q : ab \equiv 0 \pmod{q}$ und $a \not\equiv 0 \pmod{q} \wedge b \not\equiv 0 \pmod{q}$, heissen a, b Nullteiler

7.2. RECHENREGELN

- $(a + b) \pmod{n} = ((a \pmod{n}) + (b \pmod{n})) \pmod{n}$
- $(a - b) \pmod{n} = ((a \pmod{n}) - (b \pmod{n})) \pmod{n}$
- $(a * b) \pmod{n} = ((a \pmod{n}) * (b \pmod{n})) \pmod{n}$
- $a^d \pmod{n} = (a^{d-x} * a^x) \pmod{n} = ((a^{d-x} \pmod{n}) * (a^x \pmod{n})) \pmod{n}$

7.3. PRIMFAKTORENZERLEGUNG

Begriff	Bedeutung
$\text{ggT}(a, b)$	$\max\{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}$
$\text{kgV}(a, b)$	<ul style="list-style-type: none"> $\min\{m \in \mathbb{N} \mid a \mid m \wedge b \mid m\}$ $\frac{ab}{\text{ggT}(a, b)}$
Teilerfremd	<ul style="list-style-type: none"> Zwei Zahlen $a, b \in \mathbb{N}$ heissen Teilerfremd, wenn $\text{ggT}(a, b) = 1$ Sei $p \in \mathbb{N}$ eine Primzahl und $q \in \mathbb{N}, q < p, q \neq 0$ dann ist $\text{ggT}(p, q) = 1$

7.4. EUKLIDISCHER ALGORITHMUS

Seien $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$

Initialisierung: Setze $x := a, y := b$ und $q := x, r := x - q * y$ (d.h. bestimme q und r so, dass $x = q * y + r$ ist)

Wiederhole bis $r = 0$ ist

Ergebnis: $y = \text{ggT}(a, b)$

7.4.1. Beispiel

$\text{ggT}(122, 72), a = 122, b = 72$

– Init: $x_0 = a = 122, y_0 = b = 72$

– Iteration:

	$x_i = y_{i-1}$	$y_i = r_{i-1}$	$q_i = x_i \text{ div } y_i$	$r_i = x_i \bmod y_i = x_i - q_i * y_i$
$i = 0$	122	72	1	50
$i = 1$	72	50	1	22 Muster: $r_{i+1} < r_i$
$i = 2$	50	22	2	6
$i = 3$	22	6	3	4
$i = 4$	6	4	1	2
$i = 5$	4	$2 = \text{ggT}(122, 72)$	2	0 (immer 0 am Schluss)

7.5. ERWEITERTER EUKLIDISCHER ALGORITHMUS

Seien $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$

Initialisierung: Setze $x := a, y := b, q := x \div y, r := x - q * y, (u, s, v, t) = (1, 0, 0, 1)$ (d.h. bestimme q und r so, dass $x = q * y + r$ ist)

Wiederhole bis $r = 0$ ist

Ergebnis: $y = \text{ggT}(a, b) = s * a + t * b$

Wenn $\text{ggT}(a, b) = 1$ ist, dann folgt: $t * v \equiv 1 \bmod a$

7.5.1. Beispiel

$\text{ggT}(99, 79)$

i	$x = y_{-1}$	$y = r_{-1}$	$q = x \div y$	$r = x_i - q_i * y_i$	$u = s_{-1}$	$s = u_{-1} - q_{-1} * s_{-1}$	$v = t_{-1}$	$t = v_{-1} - q_{-1} * t_{-1}$
$i = 0$	99	79	1	20	1	0	0	1
$i = 1$	79	20	3	19	0	1	1	-1
$i = 2$	20	19	1	1	1	-3	-1	4
$i = 3$	19	1	19	0	-3	4	4	-5

Daraus folgend:

- $\text{ggT}(99, 79) + 1 + 4 * 99 + (-5) * 79 \Leftrightarrow 396 - 395 = 1$
- -5 ist mult. Inv. von 79 in \mathbb{Z}_{99}
- 4 ist mult. Inv. von 99 in \mathbb{Z}_{79}

7.6. KLEINER FERMAT

Sei $p \in \mathbb{N}$ eine Primzahl und $x \in \mathbb{Z} \setminus \{0\}$ mit $\text{ggT}(x, p) = 1$

Dann ist: $x^{p-1} \equiv 1 \bmod p$

Daraus folgend:

$$\begin{aligned}
 x^{p-1} &\equiv 1 \bmod p & | \quad ()^n \\
 \Leftrightarrow x^{n(p-1)} &\equiv 1 \bmod p & | \quad * x \\
 \Leftrightarrow x^{1+n(p-1)} &\equiv x \bmod p \\
 \Leftrightarrow x^{1 \bmod (p-1)} &\equiv x \bmod p
 \end{aligned}$$

7.7. SATZ VON EULER

Sei $n \in \mathbb{N} \setminus \{0\}$ und $z \in \mathbb{Z}$ mit $\text{ggT}(z, n) = 1$. Dann ist $z^{\varphi(n)} \equiv 1 \bmod n$.

7.7.1. Euler'sche φ -Funktion (Totient)

Sei $n \in \mathbb{N} \setminus \{0\}$ und $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \text{ hat ein multiplikatives Inverses in } \mathbb{Z}_n\}$. Dann heisst $\varphi(n)$:

$$\begin{aligned}
 \varphi(n) &= \text{Anz. Elemente in } \mathbb{Z}_n \text{ mit mult. Inversen} \\
 &= \text{Anz. Zahlen } 1 \leq q \leq n \text{ mit } \text{ggT}(q, n) = 1 \\
 &= |\mathbb{Z}_n^*|
 \end{aligned}$$

Falls p Primzahl ist, dann ist $\varphi(p) = p - 1$

7.7.1.1. Rechenregeln

- 1) Sei $n \in \mathbb{N}$ eine Primzahl, dann $\varphi(n) = n - 1$
- 2) Sei $n \in \mathbb{N}$ eine Primzahl und $p \in \mathbb{N} \setminus \{0\}$, dann $\varphi(n^p) = n^{p-1} * (n - 1)$
- 3) Seien $m, n \in \mathbb{N} \setminus \{0\}$ und $\text{ggT}(m, n) = 1$, dann $\varphi(n * m) = \varphi(n) * \varphi(m)$

7.8. RSA VERSCHLÜSSELUNG

- 1) Wähle 2 Primzahlen p, q
- 2) Berechne $n = p * q$
- 3) Berechne $\varphi(n) = (p - 1)(q - 1)$
- 4) Wähle a, b so, dass $a * b \equiv 1 \pmod{\varphi(n)}$
- 5) Vergesse $p, q, \varphi(p * q)$. Brauchen wir nicht und riskieren nur, dass uns jemand hackt

Public key ist nun n, b , Private key ist n, a

Sidenote: Fürs Alphabet muss n grösser sein als 26