Mathematik für die angewandte Informatik

Marcel Schubert

08.07.2024

Contents

Einleitung

Zusammenfassung mathematischer Begriffe und Konzepte für die angewandte Informatik. Die hier zusammengestellte Informationen beruhen auf Unterlagen der Hochschule, Büchern und dem Internet. Das Urheberrecht liegt bei den Autoren.

Chapter 1

Diskrete Mathematik

1.1 Mengen

(**Mengendefinition** nach Cantor): Eine Menge ist "eine Zusammenfassung von bestimmten, wohl unterschiedenen Objekten der Anschauung oder des Denkens, welche die Elemente der Menge genannt werden, zu einem Ganzen". (1.1)

(**Teilmengen**): Sind A und B Mengen und sind alle Elemente von A auch Elemente von B, so ist A eine Teilmenge von B. Wir schreiben $A \subset B$ (zu lesen als: "A ist enthalten in B"). (1.2)

Zwei Mengen A und B sind genau dann **gleich**, wenn sowohl die Inklusion $A \subset B$ als auch die Inklusion $B \subset A$ gelten. Formal: $A = B \leftrightarrow A \subset B \wedge B \subset A$ (1.3)

(**Mächtigkeit**): Die Mächtigkeit einer Menge M ist die Anzahl ihrer Elemente. Formal: $|M|$, zu lesen als: "die Mächtigkeit von M". (1.4)

(**Potenzmenge**): Wir bezeichnen die Menge aller Teilmengen einer Menge M als Potenzmenge von M und schreiben P(M) für diese Menge. (1.5)

Die **Potenzmenge einer endlichen Menge M** mit n Elementen besteht aus genau 2^n Elementen, $|P(M)| = 2^{|M|}$ (1.6)

1.1.1 Mächtigkeit unendlicher Mengen

(**Abzählbar Unendlich**): Mengen A und B heissen gleich mächtig, wenn es eine bijektive Abbildung von A nach B gibt. Die Mächtigkeit der Menge der natürlichen Zahlen heisst abzählbar unendlich. (1.7)

Die Menge der natürlichen Zahlen und die Menge der ganzen Zahlen sind gleich mächtig. (1.8)

Die Menge der natürlichen Zahlen und die Menge der rationalen Zahlen sind gleich mächtig. (1.9)

1.1.2 Vereinigung, Durchschnitt

(**Vereinigung**): Wenn A und B Mengen sind, dann bezeichnen wir: Die Vereinigung von A und B ist die Menge mit allen Objekten, die Element von A oder Element von B sind. Die Vereinigung von A und B wird mit $A \cup B$ bezeichnet. Es ist $A \cup B = \{x | x \in A \wedge x \in B\}$. (1.10)

(**Durchschnitt**): Der Durchschnitt von A und B ist die Menge mit allen Objekten, die sowohl Element von A als auch Element von B sind. Anstelle von Durchschnitt werden auch die Bezeichnungen Schnittmenge oder nur Schnitt verwendet. Die Schnittmenge von A und B wird mit $A \cap B$ bezeichnet. Die formale Definition ist $A \cap B = \{x | x \in A \vee x \in B\}$ (1.11)

Rechengesetze :

Kommutativgesetz:	$A \cap B = B \cap A$	
Assoziativgesetz:	$A \cap (B \cap C) = (A \cap B) \cap C$	
Idempotenzgesetz:	$A \cap A = A$	(1.12)
Verschmelzungsgesetz:	$A \cup (A \cap B) = A$	
Distributivgesetz:	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	

1.1.3 Komplement und Differenz

(**Komplement**): Sei A eine Teilmenge einer Obermenge M. Dann heisst die Menge $\bar{A} = \{x \in M | x \notin A\}$ das Komplement von A bezüglich der Obermenge M (1.13)

(**Differenz**): Die Differenz von zwei Mengen A und B besteht aus allen Elementen von A, die nicht in B sind, und wird definiert durch $A \backslash B = \{x \in A | x \notin B\}$ (1.14)

$$
\begin{aligned}
\bar{\bar{A}} &= A \\
A \cap \bar{A} &= \varnothing \\
A \cup \bar{A} &= M \\
A \bar{\cap} B &= \bar{A} \cup \bar{B} \\
A \bar{\cup} B &= \bar{A} \cap \bar{B}
\end{aligned} \tag{1.15}
$$

1.1.4 Bindungsstärke

Das Komplement besitzt die grösste Bindungsstärke, gefolgt von den anderen Mengen-Operatoren Vereinigung, Durchschnitt und Mengendifferenz. Es gilt: $^{-}$vor $\cup, \cap, \backslash$ (1.16)

1.1.5 Folgen und Reihen

Eine **Folge** ist eine nummerierte Liste von Objekten (Zahlenfolgegliedern, Zahlen) e.g. $(a_k)_{k=0\cdots n} = (a_0, \cdots, a_n)$ (1.17)

Eine **Reihe** ist die Summer von Folgengliedern einer Zahlenfolge e.g. $\sum_{k=1}^{n} a_k = a_1 + \cdots + a_n$ (1.18)

1.1.6 Kartesisches Produkt

Das kartesische Produkt von zwei Mengen A und B wird definiert als die Menge aller (geordneten) Paare, deren erste Komponente aus der Menge A stammt und deren zweite Komponente aus der Menge B oder veralgemeinert: $A_1 \times \cdots \times A_n = \{(a_1, \cdots, a_n) | a_1 \in A_1, \cdots, a_n \in A_n\}$ (1.19)

1.1.7 Relation

$$A = \prod_{i=1}^{n} A_i = A_i \times \cdot \times A_i \implies R \subset A \tag{1.20}$$

Ein Beispiel ist etwa eine Liste, in der für die Studierenden ihre Abteilung und ihre im Herbstsemester belegten Kurse. Eine binäre Relationen zwischen 2 gleichen Mengen heisst:

1. **reflexiv**, genau dann wenn alle Elemente von A zu sich selbst in Beziehung stehen. $\forall a \in A \implies (a, a) \in R$
2. **symmetrisch**, wenn mit (a,b) auch (b,a) in der Relation enthalten ist
3. **transitiv**, wenn aus (a,b) und (b,c) folgt, dass auch (a,c)
4. **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist.

Eine nicht leere, nicht reflexive, aber symmetrische und transitive Relation kann es nicht geben.

Datenbanken

TODO

Teilerrelation und Modulo

(**Teiler-Relation**): Für $a, b \in \mathbb{Z}$ heisst die Relation $b|a \Leftrightarrow T(b, a) \Leftrightarrow \exists q \in \mathbb{Z} : b \cdot q = a$ die Teiler-Relation (teilt-Relation). Es gilt $b|a \Leftrightarrow -b|a \wedge b|a \Leftrightarrow b| - a$ (1.21)

(**Modulo**): Aus der Teiler-Relation wird die Modulo-Relation abgeleitet. $R_q(a, r) \Leftrightarrow q|a - r \Leftrightarrow a \equiv r \mod q$. Die modulo Relation ist eine Äquivalenzrelation. (1.22)

Restklassen

Die Modulo-Relation teilt die ganzen Zahlen auf in disjunkte Teilmengen, in die so genannten Restklassen.

Die Menge $[a]_q = \{x \in \mathbb{Z} | x \equiv a \mod q, 0 \leq a < q\}$, also die Menge aller ganzen Zahlen mit gleichem Rest bei der Division durch q, bezeichnen wir als Restklasse von a modulo q. Wir bezeichnen die Menge der Restklassen modulo q auch als $\mathbb{Z}_q$. (1.23)

Sei $q \in \mathbb{Z} \backslash \{0\}$. Dann ist die Addition und die Multiplikation in den natürlichen Zahlen verträglich mit der modulo-Relation mod q. Die Addition und die Multiplikation in den natürlichen Zahlen überträgt sich daher auf die Restklassen. (1.24)

(**Zyklische Gruppen**): Man bezeichnet die aus den Restklassen modulo q gebildete Menge $\mathbb{Z}_q$ als zyklische Gruppe, weil die Restklassen sich zyklisch wiederholen. (1.25)

TODO more Zyklisches Stuff Kleiner Fermat, Multiplikatives Inverses, Satz von euler, chinesischer restsatz $q = 2 \implies \mathbb{Z}_2 = \{[0]_2, [1]_2\} \implies [0]_2 = \{\cdots, -176, -93, 0, \cdots\}, [1]_1 = \cdots$

Division mit Rest

Wenn $a, b \in \mathbb{Z}$ sind, b$b > 0$ ist und $a = q \cdot b + r$ ist mit $q, r \in \mathbb{Z}$ und $0 \leq r < b$, dann heisst r der Rest der Division von a durch b. Es ist dann $a \equiv r \mod b$ (1.26)

1.1.8 Naive Mengenlehre

Die hier definierten Mengen sind als Zusammenfassung von bestimmten, wohl unterschiedenen Objekten anzusehen. Eine derart einfache Definition von Mengen führt aber auf Widersprüche (Antinomien) und wurde daher als die naive Mengenlehre bezeichnet. Heute wird die Mengenlehre mit Hilfe von Axiomen definiert. Dadurch werden diese Widersprüche vermieden. Ein berühmtes Beispiel für eine Antinomie ist das Barbier-Paradox. Man kann einen Barbier als einen definieren, der all jene und nur jene rasiert, die sich nicht selbst rasieren. Die Frage ist: Rasiert der Barbier sich selbst? Wenn der Barbier sich selbst rasiert, ist er kein Barbier mehr, weil er ja nur die rasiert, die sich nicht selbst rasieren. Wenn der Barbier sich nicht selbst rasiert, muss er sich aber selbst rasieren, weil er ja alle rasiert, die sich nicht selbst rasieren, also in dem Fall auch sich selbst.

(**Abstrakte Mengendefinition**): Sei M die Menge aller Mengen, die sich nicht selbst als Element enthalten. Wenn M sich nicht selbst enthält, dann enthält M sich selbst.
Für sinnvolle Anwendungen wird verboten, dass Mengen sich selbst enthalten dürfen. (1.27)

1.2 Aussagenlogik

- Eine **Aussage** ist ein feststellender Satz, dem eindeutig einer der beiden Wahrheitswerte wahr oder falsch zugeordnet werden kann.
- **Aussagenlogische Formeln** verknüpfen Aussagen mit Hilfe von Junktoren.
- Eine **Kontradiktion** ist eine logische Aussage, die nie wahr ist. Alle Zeilen der Wahrheitstafel ergeben falsch.
- Eine **Tautologie** ist eine logische Aussage, die immer wahr ist. Alle Zeilen der Wahrheitstafel ergeben wahr.
- Die **Rechenregeln** für aussagenlogische Formeln sind: Kommutativität, Assoziativität, Distributivität, Absorption, Idempotenz, doppelte Negation, de Morgan, Regeln für die logischen Konstanten wahr und falsch.
- Jede aussagenlogische Formel kann in verschiedene **Negationsnormalformen**, **konjunktive** und **disjunktive Normalformen** umgewandelt werden.
- Aus einer Wahrheitstafel abgeleitete Normalformen lassen sich mit Hilfe der Rechenregeln oder mit **Karnaugh-Veitch-Diagrammen** vereinfachen.

1.2.1 Bindungsstärke

Die Bindungsstärke legt fest, welche Junktoren in aussagenlogischen Formeln zuerst ausgeführt werden. Das Nicht hat die grösste Bindungsstärke, gefolgt von den beiden Junktoren Und und Oder. Die kleinste Bindungsstärke besitzen die Implikation und die Äquivalenz. Bei der Bindungsstärke gilt also:

1. $\neg$
2. $\wedge$ and $\vee$ (1.28)
3. $\Rightarrow$ and $\Leftrightarrow$

1.2.2 Aussagenlogische Formeln

Sind A, B und C aussagenlogische Formeln mit $A \implies B \implies C$, dann bedeutet dies $A \implies B \wedge B \implies C$

1.2.3 De-Morgan

Für beliebige Aussagen A und B gilt:

$$\begin{aligned} \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B \\ \neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B \end{aligned} \tag{1.29}$$

1.2.4 Prädikatenlogik

$$\begin{aligned} \forall x \in W, \quad & R(x) \Leftrightarrow \neg\exists x \in W, \neg R(x) \\ \exists x \in W, \quad & \neg R(x) \Leftrightarrow \neg\forall x \in W, R(x) \end{aligned} \tag{1.30}$$

1.2.5 Normalformen

Aussagenlogische Formeln sind beliebig kompliziert, um diese übersichtlicher zu gestalten bringt man sie in eine Normalform.

Eine aussagenlogische Formel steht in Negationsnormalform, wenn die Negation nur direkt vor Aussagen oder Konstanten steht (1.31)

Eine verallgemeinerte Konjunktion ist eine Aussage oder seine Negation, oder einer der logischen Konstanten T=wahr und F=falsch, oder eine Konjunktion $A \wedge B$ falls diese selbst verallgemeinterte Konjunktionen sind. (1.32)

Die Aussage A liegt in disjunktiver Normalform vor, wenn sie eine verallgemeinerte Konjunktion ist, oder wenn sie eine Disjunktion von verallgemeinerten Konjunktionen ist. (1.33)

Eine verallgemeinerte Disjunktion ist eine einzelne Aussage oder seine Negation (also A oder $\neg A$) oder eine der logischen Konstanten T=wahr und F=falsch oder die Disjunktion $A \vee B$, falls A und B selbst verallgemeinerte Disjunktionen sind. Die Aussage A liegt in konjunktiver Normalform vor, wenn sie eine verallgemeinerte Disjunktion ist, oder wenn sie eine Konjunktion von verallgemeinerten Disjunktionen ist.

Diese Definitionen mögen auf den ersten Blick verwirren, sind aber eigentlich einfach und dienen dazu, komplizierte Bedingungen zu analysieren. Um die Beispielaussage A in disjunktiver Normalform zu schreiben, haben wir die Zeilen der Wahrheitstabelle ausgewertet, in denen die Aussage A richtig ist. Um die Beispielaussage A in konjunktiver Normalform zu schreiben, werten wir jetzt die Zeilen der Wahrheitstabelle aus, in denen die Aussage A falsch ist.

1.2.6 Karnaught-Veitch

Aussagenlogische Formeln können auch mit Karnaugh-Veitch-Diagrammen vereinfacht werden. Aus der Wahrheitstafel wird eine disjunktive oder eine konjunktive Normalform abgeleitet und in das Karnaugh-Veitch-Diagramm eingetragen. Im Diagramm werden die einzelnen Aussagen zu Blöcken zusammengefasst, die mit einfacheren Aussagen charakterisiert werden können. Es werden verschiedene Methoden angewendet. Wir gehen hier nur auf die Minterm-Methode ein. Das Vorgehen für n Aussagen ist folgendermassen:

1. Ein Diagramm mit 2^n Zellen erzeugen und beschriften, hier bei n=3:

	B	B	$\neg B$	$\neg B$
A				
$\neg A$				
	C	$\neg C$	$\neg C$	C

Figure 1.1: A figure caption

Die Randbeschriftungen müssen so gewählt werden, dass 2 benachbarte Zellen sich genau in einer Aussage unterscheiden.

2. Aus einer Wahrheitstabelle die Wahrheitswerte ablesen und in das Diagramm eintragen. Hier verwenden wir das Beispiel 16. Eine disjunktive Normalform kann an der Wahrheitstabelle abgelesen werden und gleich in das Karnaugh-Veitch-Diagramm eingetragen werden. Am einfachsten trägt man zuerst die Wahrheitswerte ein, die am wenigsten häufig auftreten, hier also die falsch-Werte

A	B	C	G
w	w	w	w
w	w	f	f
w	f	w	w
w	f	f	f
f	w	w	w
f	w	f	f
f	f	w	w
f	f	f	w

Figure 1.2: A figure caption

Nachdem die einen Wahrheitswerte vollständig eingetragen wurden (hier also 3 f-Werte), werden alle anderen Zellen auf den anderen Wahrheitswert gesetzt (hier werden die 5 w-Werte ergänzt).

	B	B	$\neg B$	$\neg B$
A	w	f	f	w
$\neg A$	w	f	w	w
	C	$\neg C$	$\neg C$	C

Figure 1.3: A figure caption

3. Blockbildung im Karnaugh-Veitch-Diagramm
   (a) Alle benachbarten w-Felder zu horizontalen oder vertikalen Blöcken zusammenfassen, die die Grösse einer 2er-Potenz besitzen.
   (b) Hierbei gelten Zellen auch über den Rand als benachbart.
   (c) Bei der MinTerm-Methode müssen alle w-Zellen durch solche Blöcke überdeckt werden, ohne dass eine f-Zelle überdeckt wird. Es können w-Zellen mehrfach überdeckt werden. In dem Beispiel können wir den 4er-Block C und den 2er-Block $\neg A \wedge \neg B$ nehmen und erhalten bei der Vereinfachung mit dem Karnaugh-Veitch-Diagramm als Ergebnis

1.3 Beweise

1. Direkte Beweise $A \implies B$
2. Indirekte Beweise $\neg B \implies \neg A$
3. Widerspruchsbeweis = reductio ad absurdum $A \wedge \neg B \implies F$
4. Vollständige Induktion $A(1) \wedge (A(n) \implies A(n+1)) \implies A(m), m \in \mathbb{N}$
5. Vollständige Fallunterscheidung $A \leftrightarrow A_1 \vee \cdots A_n$ und es gilt $(A_n \implies B)$ dann $A \implies B$
6. Schubfachprinzip: Wenn n+1 Gegenstände (Objekte) auf n Schubladen (Kategorien) verteilt werden, dann befinden sich in mindestens einem Schubfach 2 Gegenstände
7. Diagonalverfahren (Georg Cantor): Anzahl rationaler Zahlen ist genau so gross wie die Anzahl der natürlichen Zahlen.

1.3.1 Vollständige Induktion

1. **Verankerung**: Es wird geprüft, ob $A(n)$ für den ersten Wert stimmt. Ob also die Aussage $A(n_0)$ gilt.
2. **Induktionsschritt**: $n \to n+1$, Es wird gezeigt dass wenn $A(n)$ gilt auch $A(n+1)$ gilt. $A(n) \implies A(n+1)$
   (a) **Induktionsannahme**: $A(n)$ sei richtig für n
   (b) **Induktionsbehauptung**: $A(n+1)$
   (c) **Induktionsbeweis**: Mit der Aussage $A(n)$ die Richtigkeit der Behauptung $A(n+1)$ zeigen.

Für die Lösung von Induktionsbeweise können allen voran zwischen 4 gängigen Techniken gewählt werden. Hier mit dem Beispiel $f(n) = g(n)$:

1. Direkter Beweis für einfache Fälle bspws. Fällen bei denen sich g(n) nicht vereinfachen lässt. $f(n) = f_1(n) = f_m(n) = g(n)$
2. Differenz gleich Null für die Fälle, in denen die erste Technik zu kompliziert scheint. $f(n) - g(n) = 0$
3. Äquivalenzumformungen für die Fälle, in denen auf der linken Seite gleiche Faktoren (z.B. 6, oder (n+1)) auftreten wie auf der rechten Seite.
4. Dritte Grösse für die Fälle, in denen sich g(n) vereinfachen lässt (zum Beispiel durch Ausmultiplizieren), nach dem Grundsatz "Sind zwei Grössen einer dritten gleich, dann sind sie auch untereinander gleich".

1.3.2 Direkter Beweis

Bei einem direkten Beweis wird die Behauptung aus den allgemein geltenden Grundlagen direkt abgeleitet. In der Sprache der Aussagenlogik können wir das so formulieren: Sei A(n) eine Aussage für eine natürliche Zahl n und B(n) eine Formel, die wahr ist, wenn A(n) wahr ist. Bei einem direkten Beweis versucht man also die Aussage $A(n) \implies B(n)$ direkt zu zeigen.

1.4 Axiome Natürlicher Zahlen

1. Null ist eine natürliche Zahl.
2. Zu jeder natürlichen Zahl n gibt es genau einen Nachfolger n0, der auch eine natürliche Zahl ist.
3. Null ist nicht Nachfolger einer natürlichen Zahl.
4. Jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl.
5. Die Menge der natürlichen Zahlen ist die kleinste Menge, die die Zahl Null und mit jeder natürlichen Zahl auch ihren Nachfolger enthält.

(1.34)

1.5 Sonstige Formeln

$$\text{Arithmetische Summenformel } \sum_{k=1}^{n} k = \frac{1}{2}n(n+1) \text{ for } n \in \mathbb{N}, n >= 1 \tag{1.35}$$

(Euklid) Die Menge der Primzahlen ist unendlich. (1.36)

1.6 Euklidischer Algorithmus

1.6.1 Erweiterter Euklidischer Algorithmus

Chapter 2

Lineare Algebra

2.1 Normalform

2.1.1 Hessische Normalform

2.2 Cramersche Regel

2.3 Gauss-Jordan

Chapter 3

Analysis

3.1 Ableitungen

3.2 Integration

3.3 Kurvendiskussion

Stationäre Punkte bei $f^{'}(x) = 0$, wobei:

1. $f^{''}(x) < 0 \implies$ lokale Maxima
2. $f^{''}(x) > 0 \implies$ lokale Minima
3. $f^{''}(x) = 0 \implies$ Unentschieden
4. $f^{''}(x) = 0 \wedge f^{'''}(x) \neq 0 \implies$ Wendestelle

3.4 Taylor

3.5 Fourier

3.6 Trigonometrische Funktionen

Add Images here

3.6.1 Spezielle Funktionswerte

$$\begin{aligned} \sin(\frac{\pi}{6}) = \frac{1}{2}, \sin(\frac{\pi}{4}) = \frac{\sqrt{2}}{2}, \sin(\frac{\pi}{3}) = \frac{\sqrt{3}}{2} \\ \cos(\frac{\pi}{6}) = \frac{\sqrt{3}}{2}, \cos(\frac{\pi}{4}) = \frac{\sqrt{2}}{2}, \cos(\frac{\pi}{3}) = \frac{1}{2} \end{aligned} \tag{3.1}$$

3.6.2 Additionstheoreme und Produktformeln

$$\begin{aligned}
\sin(a \pm b) &= \sin(a)\cos(b) \pm \cos(a)\sin(b) \\
\cos(a \pm b) &= \cos(a)\cos(b) \mp \sin(a)\sin(b) \\
\cos(a)\cos(b) &= \frac{1}{2}(\cos(a-b) + \cos(a+b)) \\
\sin(a)\sin(b) &= \frac{1}{2}(\cos(a-b) - \cos(a+b)) \\
\cos(a)\sin(b) &= \frac{1}{2}(\sin(a+b) - \sin(a-b))
\end{aligned} \tag{3.2}$$

Doppelwinkeltheorem

$$\begin{aligned}
1 &= \cos^2(x) + \sin^2(x) \\
\cos(2x) &= \cos^2(x) - \sin^2(x) \\
\sin(2x) &= 2\sin(x)\cos(x)
\end{aligned} \tag{3.3}$$

Chapter 4

Statistik

4.1 Lineare Regression

Chapter 5

Informationen und Codierung

5.1 RSA

5.2 DH

Chapter 6

Data Science / Datenwissenschaft

Chapter 7

Systeme

7.1 Paralellisierung

7.2 Netzwerke