

HANSER



Leseprobe

zur

„Theoretischen Informatik, 4.A.“

von Dirk W. Hoffmann

ISBN (Buch): 978-3-446-45793-5

ISBN (E-Book): 978-3-446-45794-2

Weitere Informationen und Bestellungen unter
<http://www.hanser-fachbuch.de/978-3-446-45793-5>

sowie im Buchhandel

© Carl Hanser Verlag, München



Vorwort

Für die meisten Menschen ist die Informatik fest mit der Entstehungsgeschichte des Computers verbunden; einer Technik, die von außen betrachtet keinen Grenzen zu unterliegen scheint. Wir erleben seit Jahren eine schier ungebremste Entwicklung und sind längst daran gewöhnt, dass der Computer von heute schon morgen überholt ist. Dass sich hinter der Computertechnik eine tiefgründige Wissenschaft verbirgt, die all die großen Erfolge erst möglich macht, bleibt vielen Menschen verborgen. Die Rede ist von der theoretischen Informatik.

In der Grundlagenausbildung hat die theoretische Informatik ihren festen Platz eingenommen. Viele Studierende begegnen ihr mit gemischten Gefühlen und von manchen wird sie gar als bedrohlich empfunden. Mitverantwortlich für diese Misere sind die historischen Wurzeln der theoretischen Informatik. Entstanden aus der Mathematik, wird sie häufig in einer Präzision dargestellt, die in der Informatik ihresgleichen sucht. Manch ein Leser verirrt sich schnell in einem Gewirr aus Definitionen, Sätzen und Beweisen, das die Sicht auf die eigentlichen Konzepte und Methoden unfreiwillig verdeckt. Dass die theoretische Informatik weder schwer noch trocken sein muss, versuche ich mit diesem Buch zu beweisen.

Die folgenden Kapitel werden von zwei Leitmotiven getragen. Zum einen möchte ich die grundlegenden Konzepte, Methoden und Ergebnisse der theoretischen Informatik vermitteln, ohne diese durch einen zu hohen Abstraktionsgrad zu vernebeln. Hierzu werden die Problemstellungen durchweg anhand von Beispielen motiviert und die Grundideen der komplizierteren Beweise an konkreten Probleminstanzen nachvollzogen. Zum anderen habe ich versucht, den Lehrstoff in vielerlei Hinsicht mit Leben zu füllen. An zahlreichen Stellen werden Sie Anmerkungen und Querbezüge vorfinden, die sich mit der historischen Entwicklung dieser einzigartigen Wissenschaftsdisziplin beschäftigen.

Bei allen Versuchen, einen verständlichen Zugang zu der nicht immer einfachen Materie zu schaffen, war es mir ein Anliegen, keinen Verlust an Tiefe zu erleiden. Das Buch ist für den Bachelor-Studiengang konzipiert und deckt die typischen Lehrinhalte ab, die im Grundstudium an den hiesigen Hochschulen und Universitäten unterrichtet werden.

Vorwort zur vierten Auflage

Mittlerweile ist die *Theoretische Informatik* in der vierten Auflage erschienen, und ich bedanke mich an dieser Stelle bei allen Lesern, von denen ich seit dem Erscheinen der drit-

ten Auflage eine Rückmeldung erhalten habe. Namentlich erwähnen möchte ich Dr. Klaus Fiedler für seine zahlreichen Hinweise zur Verbesserung des Manuskripts, Mareike Bockholt und Keno Wehr für wichtige Bemerkungen zu Ogdens Lemma und Prof. Dr.-Ing. Martin Eisemann für wertvolle Anmerkungen zur Erzeugung der Chomsky-Normalform.

Karlsruhe, im Mai 2018

Dirk W. Hoffmann

Symbolwegweiser



Definition



Satz, Lemma, Korollar



Leichte Übungsaufgabe



Mittelschwere Übungsaufgabe



Schwere Übungsaufgabe

Lösungen zu den Übungsaufgaben

In wenigen Schritten erhalten Sie die Lösungen zu den Übungsaufgaben:

1. Gehen Sie auf die Seite www.dirkwhoffmann.de/TH
2. Geben Sie den neben der Aufgabe abgedruckten Webcode ein
3. Die Musterlösung wird als PDF-Dokument angezeigt



Inhaltsverzeichnis

1	Einführung	11
1.1	Was ist theoretische Informatik?	11
1.2	Zurück zu den Anfängen	14
1.2.1	Die Mathematik in der Krise	14
1.2.2	Metamathematik	18
1.2.3	Die ersten Rechenmaschinen	22
1.2.4	Der Computer wird erwachsen	24
1.2.5	Berechenbarkeit versus Komplexität	26
1.3	Theoretische Informatik heute	32
1.4	Übungsaufgaben	34
2	Mathematische Grundlagen	37
2.1	Grundlagen der Mengenlehre	38
2.1.1	Der Mengenbegriff	38
2.1.2	Mengenoperationen	41
2.2	Relationen und Funktionen	44
2.3	Die Welt der Zahlen	52
2.3.1	Natürliche, rationale und reelle Zahlen	52
2.3.2	Von großen Zahlen	55
2.3.3	Die Unendlichkeit begreifen	57
2.4	Rekursion und induktive Beweise	65
2.4.1	Vollständige Induktion	66
2.4.2	Strukturelle Induktion	68
2.5	Übungsaufgaben	70
3	Logik und Deduktion	81
3.1	Aussagenlogik	82
3.1.1	Syntax und Semantik	82
3.1.2	Normalformen	91
3.1.3	Beweistheorie	96
3.1.3.1	Hilbert-Kalkül	98
3.1.3.2	Resolutionskalkül	104
3.1.3.3	Tableaukalkül	109
3.1.4	Anwendung: Hardware-Entwurf	112

3.2	Prädikatenlogik	117
3.2.1	Syntax und Semantik	118
3.2.2	Normalformen	122
3.2.3	Beweistheorie	124
3.2.3.1	Resolutionskalkül	130
3.2.3.2	Tableaukalkül	135
3.2.4	Anwendung: Logische Programmierung	138
3.3	Logikerweiterungen	145
3.3.1	Prädikatenlogik mit Gleichheit	146
3.3.2	Logiken höherer Stufe	147
3.3.3	Typentheorie	149
3.4	Übungsaufgaben	150
4	Formale Sprachen	161
4.1	Sprache und Grammatik	162
4.2	Chomsky-Hierarchie	168
4.3	Reguläre Sprachen	170
4.3.1	Definition und Eigenschaften	170
4.3.2	Pumping-Lemma für reguläre Sprachen	172
4.3.3	Satz von Myhill-Nerode	174
4.3.4	Reguläre Ausdrücke	176
4.4	Kontextfreie Sprachen	179
4.4.1	Definition und Eigenschaften	179
4.4.2	Normalformen	179
4.4.2.1	Chomsky-Normalform	179
4.4.2.2	Backus-Naur-Form	181
4.4.3	Pumping-Lemma für kontextfreie Sprachen	182
4.4.4	Entscheidungsprobleme	186
4.4.5	Abschlusseigenschaften	188
4.5	Kontextsensitive Sprachen	191
4.5.1	Definition und Eigenschaften	191
4.5.2	Entscheidungsprobleme	192
4.5.3	Abschlusseigenschaften	193
4.6	Phrasenstruktursprachen	193
4.7	Übungsaufgaben	195
5	Endliche Automaten	201
5.1	Begriffsbestimmung	202
5.2	Deterministische Automaten	204
5.2.1	Definition und Eigenschaften	204
5.2.2	Automatenminimierung	206
5.3	Nichtdeterministische Automaten	208

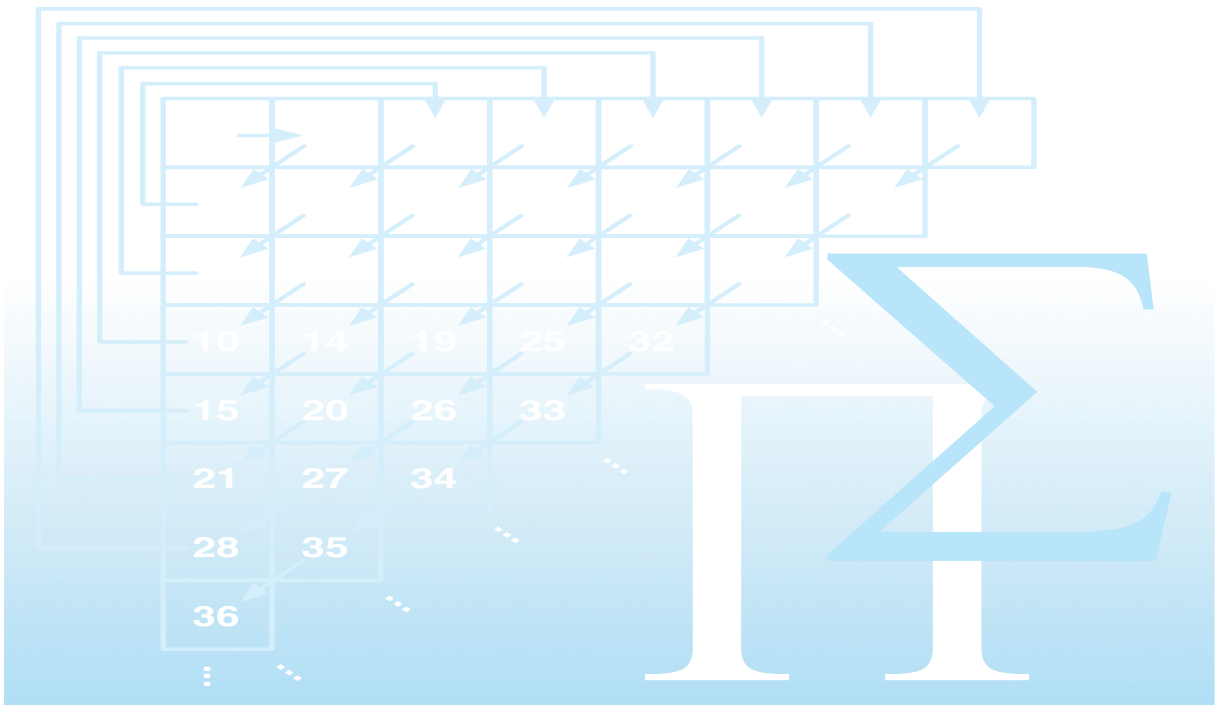
5.3.1	Definition und Eigenschaften	208
5.3.2	Satz von Rabin, Scott	210
5.3.3	Epsilon-Übergänge	212
5.4	Automaten und reguläre Sprachen	216
5.4.1	Automaten und reguläre Ausdrücke	217
5.4.2	Abschlusseigenschaften	218
5.4.3	Entscheidungsprobleme	220
5.4.4	Automaten und der Satz von Myhill-Nerode	221
5.5	Kellerautomaten	223
5.5.1	Definition und Eigenschaften	223
5.5.2	Kellerautomaten und kontextfreie Sprachen	226
5.5.3	Deterministische Kellerautomaten	228
5.6	Transduktoren	230
5.6.1	Definition und Eigenschaften	230
5.6.2	Automatenminimierung	231
5.6.3	Automatensynthese	233
5.6.4	Mealy- und Moore-Automaten	234
5.7	Petri-Netze	238
5.8	Zelluläre Automaten	243
5.9	Übungsaufgaben	246
6	Berechenbarkeitstheorie	253
6.1	Berechnungsmodelle	254
6.1.1	Loop-Programme	254
6.1.2	While-Programme	260
6.1.3	Goto-Programme	264
6.1.4	Primitiv-rekursive Funktionen	269
6.1.5	Turing-Maschinen	277
6.1.5.1	Einband-Turing-Maschinen	277
6.1.5.2	Einseitig und linear beschränkte Turing-Maschinen	285
6.1.5.3	Mehrspur-Turing-Maschinen	286
6.1.5.4	Mehrband-Turing-Maschinen	286
6.1.5.5	Maschinenkomposition	288
6.1.5.6	Universelle Turing-Maschinen	289
6.1.5.7	Zelluläre Turing-Maschinen	293
6.1.6	Alternative Berechnungsmodelle	295
6.1.6.1	Registermaschinen	296
6.1.6.2	Lambda-Kalkül	300
6.2	Church'sche These	302
6.3	Entscheidbarkeit	309
6.4	Akzeptierende Turing-Maschinen	312

6.5	Unentscheidbare Probleme	319
6.5.1	Halteproblem	319
6.5.2	Satz von Rice	322
6.5.3	Reduktionsbeweise	325
6.5.4	Das Post'sche Korrespondenzproblem	326
6.5.5	Weitere unentscheidbare Probleme	330
6.6	Übungsaufgaben	333
7	Komplexitätstheorie	341
7.1	Algorithmische Komplexität	342
7.1.1	O-Kalkül	349
7.1.2	Rechnen im O-Kalkül	352
7.2	Komplexitätsklassen	356
7.2.1	P und NP	359
7.2.2	PSPACE und NPSpace	365
7.2.3	EXP und NEXP	367
7.2.4	Komplementäre Komplexitätsklassen	369
7.3	NP-Vollständigkeit	371
7.3.1	Polynomielle Reduktion	371
7.3.2	P-NP-Problem	372
7.3.3	Satz von Cook	373
7.3.4	Reduktionsbeweise	380
7.4	Übungsaufgaben	386
A	Notationsverzeichnis	397
B	Abkürzungsverzeichnis	401
C	Glossar	403
	Literaturverzeichnis	419
	Namensverzeichnis	423
	Sachwortverzeichnis	425

2 Mathematische Grundlagen

In diesem Kapitel werden Sie ...

- die Cantor'sche Definition der Menge ergründen,
- die grundlegenden Eigenschaften von Relationen und Funktionen kennen lernen,
- die natürlichen, rationalen und reellen Zahlen untersuchen,
- den systematischen Umgang mit der Unendlichkeit erlernen,
- induktive Definitionen und Beweise verstehen.



2.1 Grundlagen der Mengenlehre

2.1.1 Der Mengenbegriff



Georg Cantor
(1845 – 1918)

Abbildung 2.1: Der deutsche Mathematiker Georg Cantor wurde am 3. März 1845 in Sankt Petersburg geboren. Nach seiner Ausbildung in Zürich, Göttingen und Berlin folgte er einem Ruf an die Universität Halle, an der er über 40 Jahre lang lehrte und forschte. Cantor gehört zu den bedeutendsten Mathematikern des späten neunzehnten und frühen zwanzigsten Jahrhunderts. Mit seiner *Mannigfaltigkeitslehre* begründete er die Mengenlehre und legte mit dem Begriff der *Kardinalität* den Grundstein für den Umgang mit der Unendlichkeit. Der Begriff der *Abzählbarkeit* geht genauso auf Cantor zurück wie die *Diagonalisierungsmethode*, mit deren Hilfe sich viele Erkenntnisse der theoretischen Informatik auf anschauliche Weise erklären lassen. Im Alter von 39 Jahren erkrankt Cantor an manischer Depression – ein Leiden, das ihn bis zu seinem Lebensende begleiten sollte. Kurz nach seinem siebzigsten Geburtstag wird er nach einem erneuten Krankheitsausbruch in die Universitätsklinik Halle eingewiesen. Dort stirbt Georg Cantor am 6. Januar 1918 im Alter von 72 Jahren.

Wir beginnen unseren Streifzug durch die Grundlagen der Mathematik mit einem Abstecher in das Gebiet der Mengenlehre. Für jeden von uns besitzt der Begriff der *Menge* eine intuitive Interpretation, die nicht zuletzt durch unser Alltagsleben geprägt ist. So fassen wir die 22 Akteure auf dem Fußballplatz wie selbstverständlich zu zwei Elfergruppen zusammen und wissen auch in anderen Lebenslagen Äpfel von Birnen zu unterscheiden. Die Zusammenfassung einer beliebigen Anzahl von Dingen bezeichnen wir als *Menge* und jedes darin enthaltene Objekt als *Element*.



Definition 2.1 (Mengendefinition nach Cantor)

„Unter einer *Menge* verstehen wir jede Zusammenfassung M von bestimmten wohl unterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die *Elemente* von M genannt werden) zu einem Ganzen.“
(Georg Cantor)

Dies ist der Originalwortlaut, mit dem der deutsche Mathematiker Georg Cantor (Abbildung 2.1) im Jahr 1885 den Mengenbegriff formulierte [13]. Die hierauf begründete mathematische Theorie wird als *Cantor'sche Mengenlehre* bezeichnet. Ebenfalls üblich sind die Begriffe der *anschaulichen*, *intuitiven* oder *naiven Mengenlehre*, um sie von den später entwickelten, streng axiomatisch definierten Mengenbegriffen abzugrenzen.

Wir schreiben $a \in M$, um auszudrücken, dass a ein Element von M ist. Entsprechend drückt die Notation $a \notin M$ aus, dass a nicht zu M gehört. Die abkürzende Schreibweise $a, b \in M$ bzw. $a, b \notin M$ besagt, dass sowohl a als auch b Elemente von M sind bzw. beide nicht zu M gehören. Zwei Mengen M_1 und M_2 gelten als gleich ($M_1 = M_2$), wenn sie exakt dieselben Elemente enthalten. Im Umkehrschluss existiert für zwei ungleiche Mengen M_1 und M_2 stets ein Element in M_1 oder M_2 , das nicht in der anderen Menge enthalten ist. Wir schreiben in diesem Fall $M_1 \neq M_2$. Offensichtlich gilt für jedes Objekt a und jede Menge M entweder $a \in M$ oder $a \notin M$.

Im Gegensatz zur umgangssprachlichen Bedeutung des Begriffs der Menge spielt es im mathematischen Sinn keine Rolle, ob darin wirklich

viele Objekte zusammengefasst sind. Wir reden selbst dann von einer Menge, wenn diese überhaupt keine Elemente enthält. Für diese *leere Menge* ist das spezielle Symbol \emptyset reserviert.

Mengen können ein einzelnes Objekt niemals mehrfach beinhalten und genauso wenig besitzen ihre Elemente einen festen Platz; Mengen sind inhärent ungeordnet. Im Übungsteil dieses Kapitels werden Sie sehen, dass der Mengenbegriff trotzdem stark genug ist, um geordnete Zusammenfassungen zu modellieren, die zudem beliebig viele Duplikate enthalten dürfen.

In der Praxis haben sich zwei unterschiedliche Schreibweisen etabliert, um die Elemente einer Menge zu definieren:

■ Aufzählende Beschreibung

Die Elemente einer Menge werden explizit aufgelistet. Selbst unendliche Mengen lassen sich aufzählend (enumerativ) beschreiben, wenn die Elemente einer unmittelbar einsichtigen Regelmäßigkeit unterliegen. Die nachstehenden Beispiele bringen Klarheit:

$$\mathbb{N} := \{0, 1, 2, 3, \dots\}$$

$$\mathbb{N}^+ := \{1, 2, 3, 4, \dots\}$$

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

$$M_1 := \{0, 2, 4, 6, 8, 10, \dots\}$$

$$M_2 := \{0, 1, 4, 9, 16, 25, \dots\}$$

\mathbb{N} heißt die Menge der *natürlichen Zahlen* oder die Menge der *nicht-negativen ganzen Zahlen*. \mathbb{N}^+ beginnt mit der 1 und wird die Menge der *positiven ganzen Zahlen* genannt. \mathbb{Z} ist die Menge der *ganzen Zahlen*. M_1 enthält alle geraden natürlichen Zahlen und die Menge M_2 die Quadrate der ganzen Zahlen.

■ Deskriptive Beschreibung

Die Mengenzugehörigkeit eines Elements wird durch eine charakteristische Eigenschaft beschrieben. Genau jene Elemente sind in der Menge enthalten, auf die die Eigenschaft zutrifft.

$$M_3 := \{n \in \mathbb{N} \mid n \bmod 2 = 0\}$$

$$M_4 := \{n^2 \mid n \in \mathbb{N}\}$$

Demnach enthält die Menge M_3 alle Elemente $n \in \mathbb{N}$, die sich ohne Rest durch 2 dividieren lassen, und die Menge M_4 die Werte n^2 für alle natürlichen Zahlen $n \in \mathbb{N}$. Die Mengen M_3 und M_4 sind damit nichts anderes als eine deskriptive Beschreibung der im vorherigen Beispiel eingeführten Mengen M_1 und M_2 .

Auf den ersten Blick scheint der Mengenbegriff intuitiv erfassbar zu sein, auf den zweiten entpuppt er sich als komplexes Gebilde. Bereits im Einführungskapitel konnten wir den Cantor'schen Mengenbegriff mithilfe der *Russell'schen Antinomie* als widersprüchlich entlarven.

Damit die Mathematik nicht auf wackligen Füßen steht, wurde mit der *axiomatischen Mengenlehre* eine formale Theorie geschaffen, die Inkonsistenzen der Russell'schen Art beseitigen soll. Einen wichtigen Grundstein legte der deutsche Mathematiker Ernst Zermelo, als er im Jahr 1907 ein entsprechendes Axiomensystem formulierte. Die *Zermelo-Mengenlehre* bestand aus insgesamt 7 Axiomen, die noch umgangssprachlich formuliert waren [111]. Das System wurde 1921 von Abraham Fraenkel um das Ersetzungsaxiom und 1930 von Zermelo um das Fundierungsaxiom ergänzt [32, 112]. Die 9 Axiome bilden zusammen die *Zermelo-Fraenkel-Mengenlehre*, kurz ZF, wie sie heute in weiten Teilen der Mathematik Verwendung findet (Abbildung 2.2).

Wird ZF zusätzlich um das *Auswahlaxiom* (*axiom of choice*) erweitert, so entsteht die ZFC-Mengenlehre (*Zermelo-Fraenkel with Choice*). Das zusätzliche zehnte Axiom besagt das Folgende: Ist M eine Menge von nichtleeren Mengen, dann gibt es eine Funktion f , die aus jeder Menge $M' \in M$ genau ein Element auswählt. Das Auswahlaxiom ist unabhängig von allen anderen. 1937 zeigte Kurt Gödel, dass es sich widerspruchsfrei zu den ZF-Axiomen hinzufügen lässt [37]. 1963 kam Paul Cohen zu dem erstaunlichen Ergebnis, dass die Negation des Auswahlaxioms die Widerspruchsfreiheit von ZF ebenfalls nicht zerstört [23].

Mit dem ehemaligen Mengenbegriff von Cantor hat die axiomatische Mengenlehre nur wenig gemein. Sie gehört heute zu den schwierigsten Teilgebieten der Mathematik und nur wenigen ist es vergönnt, sie vollständig zu durchdringen.

■ Axiom der Bestimmtheit (Zermelo, 1908)

$$\forall x \forall y (x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y))$$

„Ist jedes Element einer Menge M gleichzeitig Element von N und umgekehrt, ist also gleichzeitig $M \subset N$ und $N \subset M$, so ist immer $M = N$. Oder kürzer: jede Menge ist durch ihre Elemente bestimmt.“

■ Axiom der leeren Menge (Zermelo, 1908)

$$\exists x \forall y y \notin x$$

„Es gibt eine (uneigentliche) Menge, die ‚Nullmenge‘ \emptyset , welche gar keine Elemente enthält.“

■ Axiom der Paarung (Zermelo, 1908)

$$\forall x \forall y \exists z \forall u (u \in z \leftrightarrow u = x \vee u = y)$$

„Sind a, b irgend zwei Dinge des Bereichs, so existiert immer eine Menge $\{a, b\}$, welche sowohl a als [auch] b , aber kein von beiden verschiedenes Ding x als Element enthält.“

■ Axiom der Vereinigung (Zermelo, 1908)

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists (w \in x) z \in w)$$

„Jeder Menge T entspricht eine Menge $\bigcup T$ (die ‚Vereinigungsmenge‘ von T), welche alle Elemente der Elemente von T und nur solche als Elemente enthält.“

■ Axiom der Aussonderung (Zermelo, 1908)

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge \varphi(z))$$

„Durch jede Satzfunktion $f(x)$ wird aus jeder Menge m eine Untermenge m_f ausgesondert, welche alle Elemente x umfasst, für die $f(x)$ wahr ist. Oder: Jedem Teil einer Menge entspricht selbst eine Menge, welche alle Elemente dieses Teils enthält.“

■ Axiom des Unendlichen (Zermelo, 1908)

$$\exists x (\emptyset \in x \wedge \forall (y \in x) \{y\} \in x)$$

„Der Bereich enthält mindestens eine Menge Z , welche die Nullmenge als Element enthält und so beschaffen ist, dass jedem ihrer Elemente a ein weiteres Element der Form $\{a\}$ entspricht.“

■ Axiom der Potenzmenge (Zermelo, 1908)

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$$

„Jeder Menge m entspricht eine Menge $\mathcal{P}m$, welche alle Untermengen von m als Elemente enthält, einschließlich der Nullmenge und m selbst.“

■ Axiom der Ersetzung (Fraenkel, 1922)

$$(\forall (a \in x) \exists_1 b \varphi(a, b)) \rightarrow (\exists y \forall b (b \in y \leftrightarrow \exists (a \in x) \varphi(a, b)))$$

„Ist M eine Menge und wird jedes Element von M durch ein Ding des Bereichs \mathfrak{B} ersetzt, so geht M wiederum in eine Menge über.“

■ Axiom der Fundierung (Zermelo, 1930)

$$\forall x (x \neq \emptyset \rightarrow \exists (y \in x) x \cap y = \emptyset)$$

„Jede (rückschreitende) Kette von Elementen, in welcher jedes Glied Element des vorangehenden ist, bricht mit endlichem Index ab bei einem Urelement. Oder, was gleichbedeutend ist: Jeder Teilbereich T enthält wenigstens ein Element t_0 , das kein Element t in T hat.“

■ Optional: Axiom der Auswahl (Zermelo, 1904)

$$(\forall (u, v \in x) (u \neq v \rightarrow u \cap v = \emptyset) \wedge \forall (u \in x) u \neq \emptyset) \rightarrow \exists y \forall (z \in x) \exists_1 (w \in z) w \in y$$

„Ist T eine Menge, deren sämtliche Elemente von \emptyset verschiedene Mengen und untereinander elementfremd sind, so enthält ihre Vereinigung $\bigcup T$ mindestens eine Untermenge S_1 , welche mit jedem Element von T ein und nur ein Element gemein hat.“

Abbildung 2.2: Axiome der Zermelo-Fraenkel-Mengenlehre

Von den ganzen Zahlen \mathbb{Z} wissen wir, dass sie sich mit den Vergleichsoperatoren \leq und \geq in eine Ordnung bringen lassen. Mengen lassen sich mithilfe der *Teil- oder Untermengenbeziehung* \subseteq und der *Obermengenbeziehung* \supseteq auf ähnliche Weise ordnen:

$$M_1 \subseteq M_2 \Leftrightarrow \text{Aus } a \in M_1 \text{ folgt } a \in M_2$$

$$M_1 \supseteq M_2 \Leftrightarrow M_2 \subseteq M_1$$

Beachten Sie, dass die Teilmengenbeziehung nach dieser Definition immer auch dann gilt, wenn die linke Menge überhaupt keine Elemente enthält. Mit anderen Worten: Die leere Menge \emptyset ist eine Teilmenge jeder anderen Menge. Des Weiteren ist jede Menge auch eine Teilmenge von sich selbst. Folgerichtig gelten die Beziehungen $\emptyset \subseteq M$, $M \supseteq \emptyset$, $M \subseteq M$ und $M \supseteq M$.

Mithilfe der eingeführten Operatoren können wir die Mengengleichheit wie folgt charakterisieren:

$$M_1 = M_2 \Leftrightarrow M_1 \subseteq M_2 \text{ und } M_2 \subseteq M_1$$

Zusätzlich vereinbaren wir die Operatoren \subset (*echte Teilmenge*) und \supset (*echte Obermenge*):

$$M_1 \subset M_2 \Leftrightarrow M_1 \subseteq M_2 \text{ und } M_1 \neq M_2$$

$$M_1 \supset M_2 \Leftrightarrow M_1 \supseteq M_2 \text{ und } M_1 \neq M_2$$

Offensichtlich gilt für die weiter oben eingeführten Mengen die Beziehung $M_1 \subset \mathbb{N} \subset \mathbb{Z}$. Dagegen gilt weder $M_1 \subset M_2$ noch $M_2 \subset M_1$.

2.1.2 Mengenoperationen

Bestehende Mengen lassen sich durch die Anwendung von *Mengenoperationen* zu neuen Mengen verknüpfen. In den nachstehenden Betrachtungen seien M_1 und M_2 Teilmengen einer nichtleeren *Universal- bzw. Trägermenge* T . Die *Vereinigungsmenge* $M_1 \cup M_2$ und die *Schnittmenge* $M_1 \cap M_2$ sind wie folgt definiert:

$$M_1 \cup M_2 := \{a \mid a \in M_1 \text{ oder } a \in M_2\}$$

$$M_1 \cap M_2 := \{a \mid a \in M_1 \text{ und } a \in M_2\}$$

Zwei Mengen M_1 und M_2 heißen *disjunkt*, falls $M_1 \cap M_2 = \emptyset$ gilt.

Die Definition lässt sich auf die Vereinigung bzw. den Schnitt beliebig vieler Mengen verallgemeinern. Für die endlich vielen Mengen

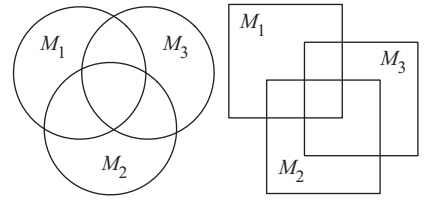
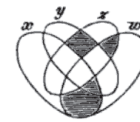
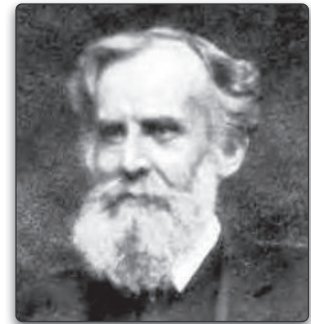


Abbildung 2.3: Venn-Diagramme sind ein anschauliches Hilfsmittel, um Beziehungen zwischen Mengen zu visualisieren. Eine Menge wird durch eine Fläche beschrieben, die durch einen geschlossenen Linienzug begrenzt wird. Jeder diskrete Punkt innerhalb der Fläche entspricht einem Element der Menge.



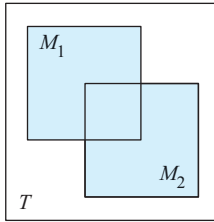
Viergliedriges Venn-Diagramm aus der Originalarbeit von 1881



John Venn (1834 – 1923)

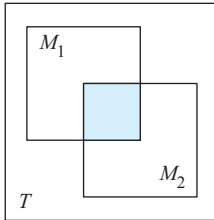
Abbildung 2.4: Das Venn-Diagramm wurde im Jahr 1881 durch den britischen Logiker und Philosophen John Venn eingeführt [101, 102]. Es bildet heute die am häufigsten eingesetzte Darstellungsform für die bildliche Repräsentation einer Menge.

■ Vereinigung



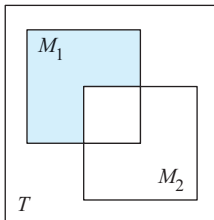
$$M_1 \cup M_2$$

■ Schnitt



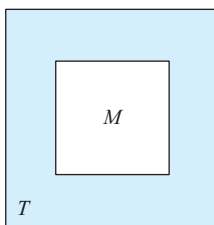
$$M_1 \cap M_2$$

■ Differenz



$$M_1 \setminus M_2$$

■ Komplement



$$\bar{M}$$

M_1, \dots, M_n bzw. die unendlich vielen Mengen M_1, M_2, \dots vereinbaren wir die folgende Schreibweise:

$$\bigcup_{i=1}^n M_i := M_1 \cup \dots \cup M_n \quad \text{bzw.} \quad \bigcup_{i=1}^{\infty} M_i := M_1 \cup M_2 \cup \dots$$

$$\bigcap_{i=1}^n M_i := M_1 \cap \dots \cap M_n \quad \text{bzw.} \quad \bigcap_{i=1}^{\infty} M_i := M_1 \cap M_2 \cap \dots$$

Zusätzlich definieren wir die *Differenzmenge* $M_1 \setminus M_2$ sowie die *Komplementärmenge* \bar{M} wie folgt:

$$M_1 \setminus M_2 := \{a \mid a \in M_1 \text{ und } a \notin M_2\}$$

$$\bar{M} := T \setminus M$$

Viele Mengenbeziehungen lassen sich intuitiv mithilfe von *Venn-Diagrammen* veranschaulichen. Die Elemente einer Menge werden durch diskrete Punkte und die Mengen selbst als geschlossene Gebiete in der Ebene repräsentiert (vgl. Abbildungen 2.3 bis 2.5).

Die Vereinigungs-, Schnitt- und Komplementoperatoren begründen zusammen die *Mengenalgebra*. In der entstehenden algebraischen Struktur gilt eine Reihe von Gesetzen, die sich direkt aus der Definition der Operatoren ergeben. Insbesondere lassen sich die folgenden vier Verknüpfungsregeln ableiten:

■ Kommutativgesetze

$$M_1 \cup M_2 = M_2 \cup M_1$$

$$M_1 \cap M_2 = M_2 \cap M_1$$

■ Distributivgesetze

$$M_1 \cup (M_2 \cap M_3) = (M_1 \cup M_2) \cap (M_1 \cup M_3)$$

$$M_1 \cap (M_2 \cup M_3) = (M_1 \cap M_2) \cup (M_1 \cap M_3)$$

■ Neutrale Elemente

$$M \cup \emptyset = M$$

$$M \cap T = M$$

■ Inverse Elemente

$$M \cup \bar{M} = T$$

$$M \cap \bar{M} = \emptyset$$

Abbildung 2.5: Elementare Mengenoperationen

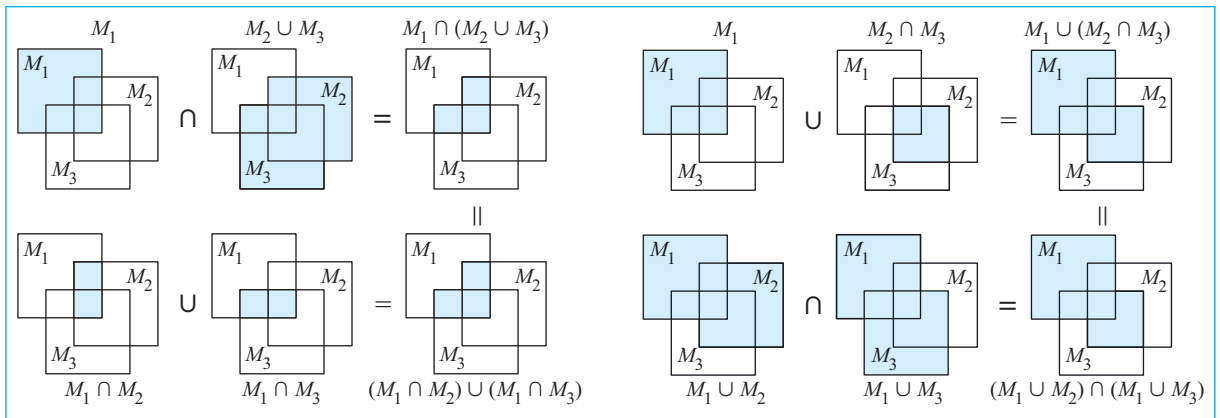


Abbildung 2.6: Veranschaulichung der Distributivgesetze anhand von Venn-Diagrammen

Von den vorgestellten Verknüpfungsregeln bedürfen nur die beiden Distributivgesetze eines zweiten Blickes, um sich von deren Richtigkeit zu überzeugen. Die Venn-Diagramme in Abbildung 2.6 liefern eine grafische Begründung für diese Regeln.

Die Mengenalgebra ist ein Spezialfall einer *booleschen Algebra* (Abbildung 2.7) [49]. Damit übertragen sich alle Gesetzmäßigkeiten, die in einer booleschen Algebra gelten, in direkter Weise auf die Mengenalgebra. Hierunter fallen insbesondere die folgenden Verknüpfungsregeln:

■ Assoziativgesetze

$$M_1 \cup (M_2 \cup M_3) = (M_1 \cup M_2) \cup M_3$$

$$M_1 \cap (M_2 \cap M_3) = (M_1 \cap M_2) \cap M_3$$

■ Idempotenzgesetze

$$M \cup M = M$$

$$M \cap M = M$$

■ Absorptionsgesetze

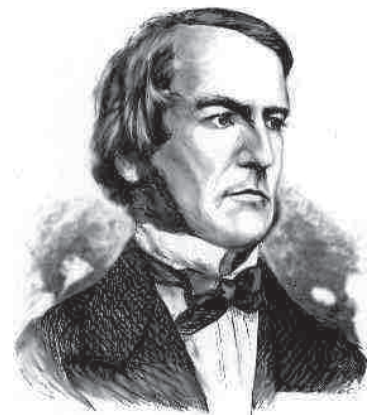
$$M_1 \cup (M_1 \cap M_2) = M_1$$

$$M_1 \cap (M_1 \cup M_2) = M_1$$

■ Gesetze von De Morgan (Abbildung 2.8)

$$\overline{M_1 \cup M_2} = \overline{M_1} \cap \overline{M_2}$$

$$\overline{M_1 \cap M_2} = \overline{M_1} \cup \overline{M_2}$$



George Boole
(1815 – 1864)

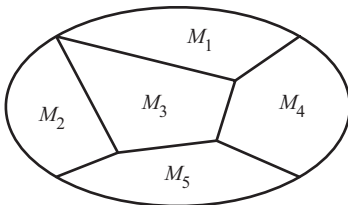
Abbildung 2.7: Der britische Mathematiker und Philosoph George Boole zählt zu den einflussreichsten Logikern des neunzehnten Jahrhunderts. Mit seinem historischen Werk *The laws of thought* legte er 1854 den Grundstein der mathematischen Logik [9]. Die nach ihm benannte boolesche Algebra ist die mathematische Grundlage für die Funktionsweise und die Konstruktion aller modernen Computeranlagen.

„The contrary of an aggregate is the compound of the contraries of the aggregants: the contrary of a compound is the aggregate of the contraries of the components.“



Augustus De Morgan (1806 – 1871)

Abbildung 2.8: Die Gesetze von De Morgan sind nach dem britischen Mathematiker Augustus De Morgan benannt, der neben George Boole als einer der bedeutendsten Mitbegründer der mathematischen Logik gilt. Auch in anderen Bereichen der Mathematik hat De Morgan Maßgebliches geleistet. Im Laufe seines Lebens verfasste er bedeutende Arbeiten in den Bereichen der Arithmetik und der Trigonometrie.



$$M = M_1 \cup \dots \cup M_5, M_i \neq \emptyset \text{ für } 1 \leq i \leq 5, \\ M_i \cap M_k = \emptyset \text{ für } i \neq k, 1 \leq i, k \leq 5$$

Abbildung 2.9: Eine Partition teilt eine Menge in paarweise disjunkte Äquivalenzklassen auf.

■ **Auslöschungsgesetze**

$$M \cup T = T \\ M \cap \emptyset = \emptyset$$

■ **Gesetz der Doppelnegation**

$$\overline{\overline{M}} = M$$

Zum Schluss wollen wir eine wichtige Mengenoperation einführen, die uns an zahlreichen Stellen in diesem Buch begegnen wird. Gemeint ist die Vereinigung aller Teilmengen zu einer neuen Menge 2^M . Diese wird als *Potenzmenge* bezeichnet und lässt sich mit der eingeführten Nomenklatur wie folgt charakterisieren:

$$2^M := \{M' \mid M' \subseteq M\}$$

Offensichtlich gelten für alle Mengen M die Beziehungen $\emptyset \in 2^M$ und $M \in 2^M$. Für eine nichtleere Menge M besitzt die Potenzmenge damit mindestens 2 Elemente.

Eine Teilmenge $P \subseteq 2^M$ ist eine *Partition* von M , wenn jedes Element aus M in einer und nur einer Menge aus P liegt. Die Elemente aus P werden als *Äquivalenzklassen* bezeichnet (vgl. Abbildung 2.9).

2.2 Relationen und Funktionen

Eine *Relation* setzt verschiedene Objekte in eine wohldefinierte Beziehung zueinander. Wir schreiben $x \sim_R y$, um auszudrücken, dass die Elemente x und y bezüglich der Relation R in Beziehung stehen. Um das Gegenteil auszudrücken, schreiben wir $x \not\sim_R y$. Die eingeführte Notation mag den Anschein erwecken, dass wir mit dem Relationenbegriff ein neues mathematisches Konzept einführen. Die folgenden Definitionen zeigen aber, dass sich die Relationentheorie vollständig auf den Schultern der Mengenlehre errichten lässt:

 **Definition 2.2 (Kartesisches Produkt)**

Sei M eine beliebige Menge. Die Menge

$$M \times M := \{(x, y) \mid x, y \in M\}$$

nennen wir das *kartesische Produkt* von M .



Definition 2.3 (Relation)

Sei M eine beliebige Menge. Jede Menge R mit

$$R \subseteq M \times M$$

heißt Relation in M . Wir schreiben $x \sim_R y$ für $(x, y) \in R$ und $x \not\sim_R y$ für $(x, y) \notin R$.

Dieser Definition folgend, ist das kartesische Produkt $M \times M$ die Menge aller geordneten Paare (x, y) von Elementen aus M . Jede Relation können wir als diejenige Teilmenge von $M \times M$ auffassen, die für alle x, y mit $x \sim_R y$ das Tupel (x, y) enthält.

Relationen lassen sich auf verschiedene Weise beschreiben. Ist die Grundmenge M endlich, so werden neben der mathematisch geprägten Mengenschreibweise (vgl. Abbildung 2.10 oben) insbesondere die folgenden Darstellungen bemüht:

■ Graph-Darstellung

Die Elemente von M werden als Knoten in Form eines Punktes oder Kreises repräsentiert und jedes Element $(x, y) \in R$ als gerichtete Verbindungslinie (Pfeil) eingezeichnet. Elemente der Form (x, x) werden durch eine Schlinge symbolisiert, die den Knoten x mit sich selbst verbindet.

■ Matrix-Darstellung

In dieser Darstellung wird eine Relation durch eine binäre Matrix repräsentiert, die für jedes Element aus M eine separate Zeile und Spalte enthält. Jedes Matrixelement entspricht einem bestimmten Tupel (x, y) des kartesischen Produkts $M \times M$. Gilt $x \sim y$, so wird der Matrixkoeffizient an der betreffenden Stelle auf 1 gesetzt. Alle anderen Koeffizienten sind gleich 0.

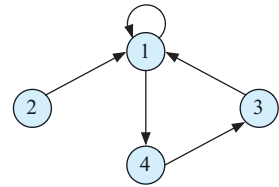
Abbildung 2.10 stellt die verschiedenen Repräsentationsformen gegenüber. Da jede Darstellung über individuelle Vor- und Nachteile verfügt, werden wir uns im Folgenden nicht auf eine einzige Repräsentation beschränken, sondern individuell auf die jeweils passende Darstellungsform zurückgreifen.

Viele praxisrelevante Relationen besitzen immer wiederkehrende, charakteristische Eigenschaften. Die folgenden *Relationenattribute* helfen, das Chaos zu ordnen:

■ Mengendarstellung

$$R := \left\{ \begin{array}{l} (1, 1), \\ (1, 4), \\ (2, 1), \\ (3, 1), \\ (4, 3) \end{array} \right\}$$

■ Graph-Darstellung



■ Tabellarische Darstellung

	1	2	3	4
1	1	0	0	1
2	1	0	0	0
3	1	0	0	0
4	0	0	1	0

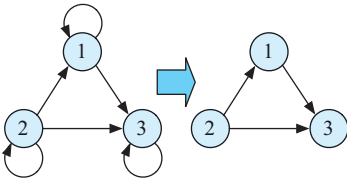
Adjazenztafel

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

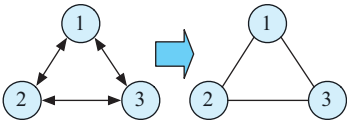
Adjazenzmatrix

Abbildung 2.10: Für die Beschreibung von Relationen haben sich verschiedene Darstellungsformen etabliert.

■ Reflexivität



■ Symmetrie



■ Transitivität

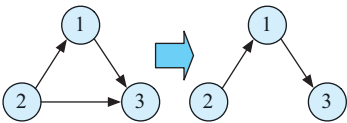


Abbildung 2.11: Vereinfachte Darstellung reflexiver, symmetrischer und transitiver Relationen



Definition 2.4 (Relationenattribute)

Eine Relation R in der Menge M heißt

- *reflexiv* in M , falls $x \sim x$ für alle $x \in M$ gilt,
- *irreflexiv* in M , falls $x \not\sim x$ für alle $x \in M$ gilt,
- *symmetrisch* in M , falls aus $x \sim y$ stets $y \sim x$ folgt,
- *asymmetrisch* in M , falls aus $x \sim y$ stets $y \not\sim x$ folgt,
- *antisymmetrisch* in M , falls aus $x \sim y$ und $y \sim x$ stets $x = y$ folgt,
- *transitiv* in M , falls aus $x \sim y$ und $y \sim z$ stets $x \sim z$ folgt,
- *linkstotal* in M , falls für alle $x \in M$ ein $y \in M$ existiert mit $x \sim y$,
- *rechtstotal* in M , falls für alle $y \in M$ ein $x \in M$ existiert mit $x \sim y$,
- *linkseindeutig* in M , falls aus $x \sim z$ und $y \sim z$ stets $x = y$ folgt,
- *rechtseindeutig* in M , falls aus $x \sim y$ und $x \sim z$ stets $y = z$ folgt.

Stellen wir eine Relation R als Graph oder in Form einer Adjazenzmatrix dar, so lassen sich viele der eingeführten Attribute auf den ersten Blick erkennen. Eine Relation R ist genau dann reflexiv, wenn alle Knoten des Relationengraphen mit einer Schlinge versehen sind, und eine symmetrische Relation liegt genau dann vor, wenn jede Kante in beiden Richtungen mit einer Pfeilspitze abschließt. Ähnliches gilt für die tabellarische Darstellung. Eine Relation R ist genau dann reflexiv, wenn in der Adjazenzmatrix sämtliche Koeffizienten der Hauptdiagonalen gleich 1 sind, und die Symmetrieeigenschaft ist gegeben, wenn die linke untere und die rechte obere Hälfte spiegelsymmetrisch zur Hauptdiagonalen liegen.

Für reflexive, symmetrische oder transitive Relationen R wird der Relationengraph gewöhnlich in einer vereinfachten Darstellung notiert (vgl. Abbildung 2.11). Reflexive Relationen werden dann ohne Schlingen gezeichnet und symmetrische Relationen durch einen ungerichteten Graph repräsentiert; an die Stelle der Doppelpfeile treten in diesem Fall einfache Linienverbindungen. Ähnliche Vereinfachungen gelten für transitive Relationen, die aus Gründen der Übersichtlichkeit um unnötige Kanten befreit werden dürfen. Eine Kante zwischen zwei Knoten x und y darf immer dann entfallen, wenn x und y bereits über andere Kanten miteinander verbunden sind.

Sachwortverzeichnis

Symbole

μ -Operator, 274
 μ -Rekursion, 274
 μ -rekursive Funktion, 275, 411
3SAT, 380, 403
4er-Nachbarschaft, 244
8er-Nachbarschaft, 244

A

Abbildung, 50
Ableitungsrelation, 96
Abschwächungsregel, 98
Absolute Adressierung, 296
Abstraktion, 300
Abtrennungsregel, 17
Abzählbare Sprache, 310
Abzählbarkeit, **59**, 310, 403
Ackermann-Funktion, 56, 403
Addierer
 Carry-look-ahead-, 116
 Carry-ripple-, 114
Adressierung
 absolute, 296
 indirekte, 296
 unmittelbare, 296
Äquivalenz, 87
Akkumulator, 296
AKS-Algorithmus, 33
Akzeptierende Turing-Maschine, 312
Akzeptierender Automat, 203, 403
Akzeptor, 203, 403
 Minimierung, 206
 Turing-, 312
Algorithmische Komplexität, 342
Algorithmus
 CYK-, 186, 405
 effektiver, 27

effizienter, 27
Gilmore-, 128, 407
Las-Vegas-, 32
Monte-Carlo-, 32
randomisierter, 32
rekursiver, 271
Robinson-, 131, 414
Strassen-, 391
Allgemeingültigkeit, 85, 403
 prädikatenlogische, 122
Allgemeinster Unifikator, 131, 403
Alphabet, 162
Antinomie, 403
 Russell'sche, **17**, 39, 415
Antivalenzoperator, 83
Äquivalenz, 87
 -klasse, 44
 -operator, 83
 -problem, 163, 403
 -relation, 49
Arbeitsband, 292
Asymptotische Komplexität, 350
Asymptotisches Wachstum, 403
Atomare Aussage, 82, 404
Atomare Formel, 83
Aufzählbare Sprache, 310
Aufzählbarkeit, 310
Ausdruck
 regulärer, 26, **176**, 217, 414
Ausgabealphabet
 von Transduktoren, 230
Ausgabeband, 296
Ausgabefunktion, 230
Ausgabeschaltnetz, 233
Aussage
 atomare, 82, 404
Aussagenlogik, 23, **82**, 404
 Normalformen, 91
Auswahlaxiom, 39

Automat

äquivalenter, 206
akzeptierender, 203, 403
DEA, 204, 405
deterministischer, 204
endlicher, 25, **201**, 406
Keller-, 223, 409
linearer, 244
Mealy-, 203, **234**, 411
Moore-, 203, **234**, 411
NEA, 209, 411
nichtdeterministischer, 208
Potenzmengen-, 211, 413
Produkt-, 219
reduzierter, 206
übersetzender, 203, 230
zellulärer, **243**, 252, 418
Automatenminimierung, 404
 von Akzeptoren, 206
 von Transduktoren, 231
Automatensynthese, 233, 404
Automatentheorie, 25, 201
Axiom, 35, 404
Axiome
 von Peano, 52

B

Backtracking, 145
Backus-Naur-Form, 181, 404
 erweiterte, 181
Bandalphabet
 von Turing-Maschinen, 279
Bandplatzfunktion, 365
Bar-Hillel-Theorem, 185
Barbier-Paradoxon, 34, 404
Basis, 306
BCD-Code, 249
Befehlszähler, 296

- Belegung, 84
 Berechenbarkeit, **254**, 302, 404
 Goto-, 266
 Loop-, 256
 Turing-, 281, 417
 While-, 261
 Berechenbarkeitstheorie, 253, 404
 Berechnungsmodell, 254, 404
 Beweis
 direkter, 66
 durch Widerspruch, 66
 induktiver, 65
 Beweistheorie
 aussagenlogische, 96
 prädikatenlogische, 124
 Biberfunktion, 337
 Bijektive Funktion, 51
 Bild, 51
 Binärbaum, 68
 balancierter, 68
 saturierter, 68
 Binäre Codierung, 282
 Binäre Suche, 387
 Binomialkoeffizient, 79
 Binomischer Lehrsatz, 79
 Bisimulation, **206**, **231**, 405
 Blättermenge, 68
 Blank-Symbol, 279
 Boolesche Algebra, 43
 Boolesche Funktion, 85
 Brute-Force-Methode, 363
- C**
- Cantor'sche Paarungsfunktion, 61, 75
 Cantor-Maschine, 312
 Carry bit, 114
 Carry-look-ahead-Addierer, 116
 Carry-ripple-Addierer, 114
 CD, 248
 Charakteristische Funktion, 309, 405
 Chomsky-Hierarchie, 25, **168**, 405
 Chomsky-Normalform, 179, 405
 Church'sche These, 254, **302**, 308, 405
 Church-Rosser-Eigenschaft, 301
 CLIQUE, 383
 Co-Komplexität, 369, 405
- COBOL, 24
 Code
 einschrittiger, 231
 Codierung
 binäre, 282
 unäre, 282
 Collatz-Funktion, 78
 Cook
 Satz von, **373**, 383
 Cook, Satz von, 415
 CYK-Algorithmus, 186, 405
- D**
- Datenspur, 287
 DEA, 204, 405
 Deadlock, 242
 Dedekind'scher Schnitt, 54
 Deduktion, 81
 Deduktionsbeweis, 66
 Definition
 rekursive, 65
 Definitionsmenge, 50
 Deklarative Programmierung, 138
 Deterministischer Automat, 204
 Diagonalisierung, 38, 405
 Diagonalisierungsargument, 62
 Diagonalsprache, 338
 Differenzmenge, 42
 Dirichlet'sches Schubfachprinzip, 90, 406
 Disjunktion, 82
 Disjunktive Form, 406
 Disjunktive Minimalform, 95
 Disjunktive Normalform, 95, 406
 kanonische, 93
 Distributivgesetz, 42, 98
 Divide and conquer, 356
 DNA computing, 308
 DNF, 94
 DVD, 248
 Dyck-Sprache, 165, 227
 Dynamische Logik, 295
 Dynamische Programmierung, **186**, **346**, 406
- E**
- Ebene
 Meta-, 82
 Objekt-, 82
 Einband-Turing-Maschine, 277
 Eingabealphabet
 von ε -Automaten, 213
 von DEAs, 204
 von Kellerautomaten, 224
 von NEAs, 209
 von Transduktoren, 230
 von Turing-Maschinen, 279
 Eingabeband, 296
 Einschrittiger Code, 231
 Element, 38
 Elementaroperatoren, 89
 Endlicher Automat, 25, **201**, 406
 Endlichkeitsproblem, 162, 406
 Endrekursion, 272
 Endzustand
 von ε -Automaten, 213
 von DEAs, 204
 von NEAs, 209
 von Turing-Maschinen, 279
 Enigma, 23
 Entscheidbare Sprache, 313
 Entscheidbarkeit, 19, **309**, 406
 Semi-, 309, 416
 Epsilon-Übergang, 212, 213, 406
 Erfüllbarkeit, 406
 aussagenlogische, 85
 prädikatenlogische, 122
 Erfüllbarkeitsäquivalenz, 123, 406
 Erreichbarkeitsanalyse, 241
 Euklidische Axiome, 15
 Euler-Kreis, 29
 EXP, 367, 406
- F**
- Faktorisierungsregel, 134
 Faktum
 in Prolog, 138
 Ferritkernspeicher, 24
 Fibonacci-Folge, 390
 Finalzustand

von ε -Automaten, 213
 von DEAs, 204
 von NEAs, 209
 von Turing-Maschinen, 279
 Fixpunkt, 208
 -operator, 301
 Fleißiger Biber, 337
 Flipflop, 233
 Formale Sprache, 25, **162**, 406
 Formales System, 12, 35, 407
 Formel
 aussagenlogische, 82
 bereinigte, 119
 erfüllbarkeitsäquivalente, 123
 geschlossene, 119
 prädikatenlogische, 119
 Formulario-Projekt, 53
 FORTRAN, 24
 Funktion, **44**, 50
 μ -rekursive, 275, 411
 Ackermann-, 56, 403
 bijektive, 51
 boolesche, 85
 charakteristische, 309, 405
 injektive, 51
 partielle, **51**, 258, 412
 platzkonstruierbare, 366
 primitiv-rekursive, 269, 413
 surjektive, 51
 totale, 51, 417
 unberechenbare, 319
 zeitkonstruierbare, 361
 Funktions
 -variable, 147
 Funktionstabelle, 85
 Funktionswert, 51

G
 Gegenbeispiel, 109
 Generative Grammatik, 25
 Gilmore-Algorithmus, 128, 407
 Gleichheitsrelation, 47
 Gödelisierung, 291, 407
 Gödelnummer, **291**, 321, 339, 407
 Goto-Berechenbarkeit, 266
 Goto-Programm, 264, 407

Goto-Sprache, 264, 407
 Grad
 von Polynomen, 353
 Grammatik, 162–164, 407
 eindeutige, 167
 generative, 25
 kontextfreie, 168, **179**, 409
 kontextsensitive, 168, **191**, 410
 mehrdeutige, 167
 rechtslineare, 170
 reguläre, 168, **170**, 414
 Gray-Code, 231
 Greibach-Normalform, 197, 407
 Grundinstanz, 127, 407
 Grundlagenkrise, 14
 Grundmenge, 120
 Grundsubstitution, 120

H

Halteproblem, 21, **319**, 407
 allgemeines, 320
 auf leerem Band, 322, 408
 spezielles, 339, 416
 Hamilton-Kreis, 30
 Hamilton-Problem, 364, 408
 Hardware-Entwurf, 112
 Haskell, 300
 Head recursion, 272
 Herbrand
 Satz von, 126, 415
 Herbrand-Interpretation, 126, 408
 Herbrand-Modell, 126, 408
 Herbrand-Universum, 125, 408
 Hilbert-Kalkül, 98, 408
 Hilbert-Wüste, 76
 Hilberts Hotel, 61
 Horn-Formel, 143
 Hülle
 Kleene'sche, 162
 reflexiv-transitive, 47, 48
 transitive, 47
 Huffman-Normalform, 234

I

Identität, 47

Ignorabimus, 19
 Imaginäre Einheit, 71
 Implikation, 82
 Indirekte Adressierung, 296
 Individuenbereich, 120
 Induktion
 strukturelle, 68, 416
 vollständige, **66**, 418
 Induktionsaxiom, 408
 Induktiver Beweis, 65
 Injektive Funktion, 51
 Instanzen, 99
 Interpretation, **84**, **120**, 408
 Herbrand-, 126, 408
 Inverses Element, 42
 Inzidenzmatrix, 239, 408
 Irrationale Zahl, 54
 Isomorphie, 212
 Iterationslemma, 185

K

Kalkül, 12, 35, **96**, 408
 Hilbert-, 98, 408
 Lambda-, 300
 Resolutions-, **104**, 130, 414
 Tableau-, **109**, 135, 416
 Widerspruchs-, 97, 418
 Kapazität, 241
 Kardinalität, 38, 58
 Kardinalzahl, 64, 408
 Kartesisches Produkt, 44
 KDNF, 93
 Kelleralphabet, 224
 Kellerautomat, 223, 409
 deterministischer, 228, 229
 Kellerspeicher, 409
 Kettenregel, 180
 KKNF, 93
 Klausel, 95, 409
 leere, 95
 Klauseldarstellung, 95
 Kleene
 Satz von, 264, 415
 Kleene'sche Hülle, 162
 Kleene'sche Normalform, **268**, 304, 409
 KNF, 94

- Königsberger Brückenproblem, 29, 409
 Kollisionsfreiheit, 135
 Kommutativgesetz, 42
 Komplementärautomat, 218
 Komplementärmenge, 42
 Komplexe Zahl, 71
 Komplexitätsklasse, 29, **356**, 409
 komplementäre, 369, 405
 Komplexitätstheorie, 341, 409
 Komposition, 270
 Konfiguration, 409
 globale, 244
 lokale, 244
 von ε -Automaten, 213
 von DEAs, 205
 von Kellerautomaten, 225
 von NEAs, 210
 von Petri-Netzen, 239
 von Turing-Maschinen, 280
 Konjunktion, 82
 Konjunktive Form, 409
 Konjunktive Minimalform, 95
 Konjunktive Normalform, 95, 409
 kanonische, 93
 Konklusion, 98
 Kontextfreie Grammatik, 168, **179**, 409
 Kontextfreie Sprache, **179**, 226, 410
 Kontextsensitive Grammatik, 168, **191**,
 410
 Kontextsensitive Sprache, 191, 410
 Kontinuum, 64
 Kontinuumshypothese, 64
 Kontraposition, 98
 Konversionsregel, 300
 Kopfrekursion, 272
 Kopfzelle, 293
 Korrektheit, 96
 Korrespondenzproblem, 326, 413
 binäres, 340
 modifiziertes, 328
- L**
- Lambda-Kalkül, 300
 Lambda-Term, 300
 Landau-Symbole, 349, 410
 Las-Vegas-Algorithmus, 32
 Last-In-First-Out, 224
 Latch, 233
 Laufzeitfunktion, 359
 LBA-Problem
 erstes, 318
 zweites, 318
 Lebendigkeit
 von Petri-Netzen, 241
 Leere Klausel, 95
 Leere Menge, 39
 Leerheitsproblem, 162, 410
 LIFO, 224
 Lineare Rekursion, 272
 Lineare Suche, 387
 Linearer Automat, 244
 Linksableitung, 165, 410
 Literal, 92, 410
 Logik, 81, 410
 Aussagenlogik, 23, **82**, 404
 dynamische, 295
 höherer Stufe, 147, 410
 Prädikatenlogik, 117, 413
 Logikminimierung, 95
 Logische Folgerung, 87
 Logische Programmierung, 138
 Logizismus, 16, 35
 Loop-Berechenbarkeit, 256
 Loop-Programm, 254, 410
 Loop-Sprache, 254, 410
- M**
- Mächtigkeit, 58, 410
 Makro, 257
 Marke, 238, 412
 Markenindex, 265
 Markierungsgleichung, 241
 Maschinenkomposition, 288
 Matrix, 122
 Maxterm, 92, 411
 Mealy-Automat, 203, **234**, 411
 Mehrband-Turing-Maschine, 286
 Mehrdeutigkeitsproblem, 411
 Mehrspur-Turing-Maschine, 286
 Menge, 38
 disjunkte, 41
 leere, 39
 Null-, 40
 unentscheidbare, 319
 wohlgeordnete, 72
 Mengenalgebra, 42
 Mengenlehre, 16
 axiomatische, 39
 Cantor'sche, 38
 Fraenkel-, 39
 Zermelo-Fraenkel-, 39
 Mengenoperation, 41
 Metaebene, 82
 Millennium-Probleme, 32
 Minimalform, 95
 disjunktive, 95
 konjunktive, 95
 Minimierung, 404
 Logik-, 95
 von Akzeptoren, 206
 von Transduktoren, 231
 Minterm, 92, 411
 Miranda, 300
 ML, 300
 Modell, **84**, **121**, 411
 Herbrand-, 126, 408
 Modellrelation, **84**, 120, 121
 Modus barbara, 150
 Modus ponens, 17, **98**, 411
 Monte-Carlo-Algorithmus, 32
 Moore-Automat, 203, **234**, 411
 Moore-Nachbarschaft, 244
- N**
- Nachbarschaft
 Moore-, 244
 Von-Neumann-, 244
 Nachbarschaftsfunktion
 von zellulären Automaten, 243
 Natürliche Zahl, 39, 52
 NEA, 209, 411
 Negation, 82
 Negationsnormalform, 122, 411
 Nerode-Relation, 175
 Neutrales Element, 42
 NEXP, 367, 411
 Nichtdeterministischer Automat, 208
 Nichtterminal, 163

- Nonterminal, 163, 164
 Normalform, 92, 179
 aussagenlogische, 91
 Chomsky-, 179, 405
 disjunktive, 406
 Greibach-, 197, 407
 Huffman-, 234
 kanonische
 disjunktive, 93
 konjunktive, 93
 Kleene'sche, **268**, 304, 409
 konjunktive, 409
 Negations-, 122, 411
 prädikatenlogische, 122
 NP, 359, 411
 NP-hart, 372, 412
 NP-vollständig, 31, **371**, 412
 NPSPACE, 365, 412
 Nullmenge, **40**
- O**
- O-Kalkül, 349
 O-Notation, 349, 412
 Obermenge, 41
 Objektebene, 82
 ODER-Operator, 82
 Ogdens Lemma, 185
 Operator, 51, 55
 Operatorensystem
 vollständiges, 89
 Orakel, 364
 Ordnung
 lineare, 50
 partielle, 50
 totale, 50
 Ordnungsrelation, 50
- P**
- P, 359, 412
 P-NP-Problem, 372, 412
 Paarungsfunktion, **61**, 258, 412
 Cantor'sche, 61, 75
 Palindromsprache, 196, 226
 Parikh-Vektor, 239, 412
 Paritätsbit, 246
 Paritätscode, 246
 Partielle Funktion, **51**, 258, 412
 Partition, 44
 Peano-Axiome, 52, 412
 Petri-Netz, 238, 412
 Pfad
 geschlossener, 109
 offener, 109
 vollständiger, 110
 widerspruchsfreier, 109
 widersprüchlicher, 109
 Phrasenstrukturgrammatik, 168
 Phrasenstruktursprache, 193
 Pigeonhole principle, 90, 406
 Platzkonstruierbare Funktion, 366
 Polynom, 353
 Polynomielle Reduktion, 371, 413
 Pop-Operation, 224
 Positionsspur, 287
 Post'sche Tag-Maschine, 295
 Post'sches Korrespondenzproblem, 326, 413
 binäres, 340
 modifiziertes, 328
 Potenzmenge, 44
 Potenzmengenautomat, 211, 413
 Prädikat, 117
 -variable, 147
 Prädikatenlogik, 117, 413
 Normalformen, 122
 zweiter Stufe, 147
 Prämisse, 98
 Pränex-Form, 122, 413
 Primitiv-rekursive Funktion, 269, 413
 Primitive Rekursion, 269, 413
 Principia Mathematica, 17, 18
 Problem
 unentscheidbares, 319
 Produktautomat, 219
 Produktion, 164
 Programm, 296
 Goto-, 264, 407
 Loop-, 254, 410
 While-, 260, 418
 Programmierung
 deklarative, 138
 dynamische, **186**, **346**, 406
 logische, 138
 Prolog, 413
 PSPACE, 365, 414
 Pumping-Lemma, 185, 414
 für kontextfreie Sprachen, 182
 für reguläre Sprachen, 172
 Push-Operation, 224
- Q**
- Quantenrechner, 308
- R**
- Rabin und Scott
 Satz von, 210, 415
 Rad des Theodorus, 65
 Random access machine, 296
 Randomisierter Algorithmus, 32
 Rationale Zahl, 53
 Rechtsableitung, 165, 414
 Rechtslineare Grammatik, 170
 Reduktion, 414
 polynomielle, 371, 413
 Reduktionsbeweis, 325, 380
 Reelle Zahl, 54
 Regel, 35, 164
 in Prolog, 138
 Registermaschine, 296, 414
 verallgemeinerte, 296
 Reguläre Grammatik, 168, **170**, 414
 Reguläre Sprache, **170**, 216, 414
 Regulärer Ausdruck, 26, **176**, 217, 414
 Rekurrenzgleichung, 390
 Rekursion, 65
 μ -, 274
 lineare, 272
 primitive, 269, 413
 verschachtelte, 272
 verzweigende, 272
 wechselseitige, 272
 Rekursiv aufzählbare Sprache, 310
 Rekursive Definition, 65
 Relation, 44
 Ableitungs-, 96
 Äquivalenz-, 49
 inverse, 47
 Ordnungs-, 50

Relationenattribut, 45
 Relationenprodukt, 47
 Resolutionsbaum, 105
 Resolutionskalkül, 414
 aussagenlogisches, 104
 prädikatenlogisches, 130
 Resolutionsregel, 105
 Resolvente, 105
 Rice
 Satz von, 322, 415
 Robinson-Algorithmus, 131, 414
 Rucksackproblem, 186, **342**, 415
 Russell'sche Antinomie, **17**, 39, 415

S

SAT, 415
 Satz
 von Cantor, 64, 415
 von Cook, **373**, 383, 415
 von Herbrand, 126, 415
 von Kleene, 264, 415
 von Myhill-Nerode, 174, 221
 von Rabin und Scott, 210, 415
 von Rice, 322, 415
 von Savitch, 367, 415
 Savitch
 Satz von, 367, 415
 Schaltnetz, 233
 Ausgabe-, 233
 Übergangs-, 233
 Schaltwerk, 25, 233
 Scheme, 300
 Schleife
 While-, 260
 Schleifensatz, 185
 Schlussregel, 416
 Schnittmenge, 41
 Schubfachprinzip, 90, 406
 Selbstabbildung, 51
 Semantik, 82, 416
 Semi-entscheidbare Sprache, 313
 Semi-entscheidbarkeit, 313
 Semi-Entscheidbarkeit, 309, 416
 Semi-Thue-System, 169
 Sicherheit
 von Petri-Netzen, 241

Sierpinski-Dreieck, 245, 252
 Skolem-Form, 123, 416
 Speicher, 296
 Speichervektor, 255
 Spezielles Halteproblem, 339, 416
 Sprache
 abzählbar, 310
 Diagonal-, 338
 entscheidbare, 313
 formale, 25, **162**, 406
 Goto-, 264, 407
 inhärent mehrdeutige, 167
 kontextfreie, **179**, 226, 410
 kontextsensitive, 191, 410
 Loop-, 254, 410
 Palindrom-, 196, 226
 Phrasenstruktur-, 193
 reguläre, **170**, 216, 414
 rekursiv aufzählbare, 310
 semi-entscheidbare, 313
 unentscheidbare, 319
 While-, 260, 418
 Stack, 224, 259
 Stapel, 224, 259
 Startkonfiguration, 245
 Startsymbol, 164
 Startvariable, 164
 Startzustand
 von ϵ -Automaten, 213
 von DEAs, 204
 von Kellerautomaten, 224
 von NEAs, 209
 von Transduktoren, 230
 von Turing-Maschinen, 279
 Stirling-Zahl, 73
 Strassen-Algorithmus, 391
 Strukturelle Induktion, 68, 416
 Substitution, 119
 Substitutionstheorem, 89
 Suche
 binäre, 387
 lineare, 387
 Surjektive Funktion, 51
 Syllogismus, 150
 Syntax, 82, 416
 Syntaxbaum, 167, 416
 Synthese
 von Automaten, 233, 404, 416

T

Tableau
 geschlossenes, 110
 offenes, 110
 vollständiges, 110
 widerspruchsfreies, 110
 Tableukalkül, 416
 aussagenlogisches, 109
 prädikatenlogisches, 135
 Tag-Maschine, 295
 Tail recursion, 272
 Taubenschlagprinzip, 90, 406
 Tautologie, 416
 aussagenlogische, 85
 prädikatenlogische, 122
 Teile-und-herrsche-Prinzip, 356
 Teilformel, 83
 Teilmenge, 41
 Terminal, 163
 Terminalalphabet, 164
 Terminierungsmenge, 261
 Thue-System, 169
 Totale Funktion, 51, 417
 Totalordnung, 50
 Trägermenge, 41
 Transduktor, 203, **230**, 248, 417
 Minimierung, 231
 Transistor, 24
 Turing-Akzeptor, 312
 Turing-Berechenbarkeit, 281, 417
 Turing-Bombe, 23
 Turing-Maschine, 20, **277**, 417
 akzeptierende, 312
 Einband-, 277
 einseitig beschränkte, 285
 Komposition, 288
 linear beschränkte, 285
 Mehrband-, 286
 Mehrspur-, 286
 universelle, 289, 418
 zelluläre, 293
 Turing-Test, 279

U

Überabzählbarkeit, 59, 417

Übergangsfunktion, 255
 Übergangsrelation, 314
 Übergangsschaltnetz, 233
 Übersetzender Automat, 203, 230
 Umkehrabbildung, 51
 Unäre Codierung, 282
 Unberechenbarkeit, 319, 417
 UND-Operator, 82
 Unendlichkeit, 57
 Unentscheidbarkeit, 319, 417
 Unerfüllbarkeit, 85, 417
 Unifikation, 130, 417
 Unifikator, 130, 418
 allgemeinster, 131, 403
 Universalmenge, 41
 Universelle Turing-Maschine, 289, 418
 Universum, 120
 Herbrand-, 125, 408
 Unmittelbare Adressierung, 296
 Untermenge, 41
 Up-Arrow-Notation, 56, 418
 Urbild, 51

V

Variable, 82, 164
 Funktions-, 147
 Prädikat-, 147
 Venn-Diagramm, 41, 42
 Vereinigungsmenge, 41
 Verklemmungsfreiheit
 von Petri-Netzen, 242
 Verschachtelte Rekursion, 272
 Verzweigende Rekursion, 272

Vollständige Induktion, **66**, 418
 Vollständiges Operatorensystem, 89
 Vollständigkeit, 18, 96
 Von-Neumann-Nachbarschaft, 244

W

Wahrheitstabelle, 85
 Wahrheitstafel, 85
 Wechselseitige Rekursion, 272
 While-Berechenbarkeit, 261
 While-Programm, 260, 418
 While-Schleife, 260
 While-Sprache, 260, 418
 Widerspruchsbeweis, 66
 Widerspruchsfreiheit, 19
 Widerspruchskalkül, 97, 418
 Wohlordnung, 72
 Wort, 162
 Wortproblem, 162, 418
 Wurzelschnecke, 65

X

XOR-Operator, 83

Z

Z3, 22
 Zahl
 ganze, 39, 53
 große, 55
 irrationale, 54
 natürliche, 39, 52

 nichtnegative, 39
 positive, 39
 rationale, 53
 reelle, 54
 Zeichen, 162
 Zeitkonstruierbare Funktion, 361
 Zelle, 243
 Zellmenge, 243
 Zelluläre Turing-Maschine, 293
 Zellulärer Automat, **243**, 252, 418
 Zentraleinheit, 296
 Zermelo-Fraenkel-Mengenlehre, 39
 Zermelo-Mengenlehre, 39
 Zielmenge, 50
 Zustand, 202
 äquivalenter, 206
 Zustandsband, 292
 Zustandsmenge
 von ε -Automaten, 213
 von DEAs, 204
 von Kellerautomaten, 224
 von NEAs, 209
 von Transduktoren, 230
 von Turing-Maschinen, 279
 von zellulären Automaten, 243
 Zustandsübergangsdigramm, 202
 Zustandsübergangsfunktion
 von ε -Automaten, 213
 von DEAs, 204
 von Kellerautomaten, 224
 von NEAs, 209
 von Transduktoren, 230
 von Turing-Maschinen, 279
 von zellulären Automaten, 243