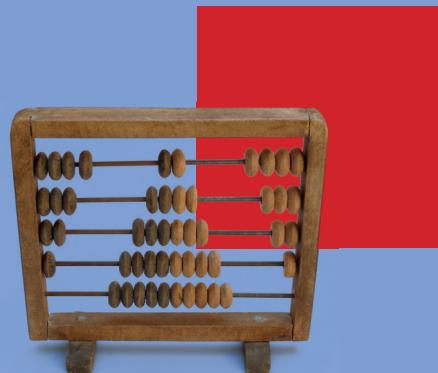


dirk w. HOFFMANN



# THEORETISCHE INFORMATIK



HANSER



Bleiben Sie einfach auf dem Laufenden:  
[www.hanser.de/newsletter](http://www.hanser.de/newsletter)

Sofort anmelden und Monat für Monat  
die neuesten Infos und Updates erhalten.

---

Dirk W. Hoffmann

# Theoretische Informatik

Mit 258 Bildern, 22 Tabellen und 78 Aufgaben

HANSER

---

## Autor

Prof. Dr. Dirk W. Hoffmann, Hochschule Karlsruhe, Fakultät für Informatik

Alle in diesem Buch enthaltenen Programme, Verfahren und elektronischen Schaltungen wurden nach bestem Wissen erstellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund ist das im vorliegenden Buch enthaltene Programm-Material mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor und Verlag übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

## Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dieses Werk ist urheberrechtlich geschützt.

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Buches, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren), auch nicht für Zwecke der Unterrichtsgestaltung – mit Ausnahme der in den §§ 53, 54 URG genannten Sonderfälle –, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© 2009 Carl Hanser Verlag München

Lektorat: Dipl.-Ing. Erika Hotho

Herstellung: Dipl.-Ing. Franziska Kaufmann

Covergestaltung: Stephan Rönigk

Datenbelichtung, Druck und Bindung: Kösel, Krugzell

Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702

Printed in Germany

ISBN 978-3-446-41511-9

[www.hanser.de/computer](http://www.hanser.de/computer)

# Vorwort

---

Für viele 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.

Karlsruhe, im Dezember 2008

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](http://www.dirkwhoffmann.de/TH)
2. Geben Sie einen der im Buch abgedruckten Webcodes ein
3. Die Musterlösung wird als PDF-Dokument angezeigt

# Inhaltsverzeichnis

---

<b>1 Einführung</b>	<b>11</b>
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 Die ersten Rechenmaschinen . . . . .	22
1.2.3 Der Computer wird erwachsen . . . . .	24
1.2.4 Berechenbarkeit versus Komplexität . . . . .	26
1.3 Theoretische Informatik heute . . . . .	32
1.4 Übungsaufgaben . . . . .	34
<b>2 Mathematische Grundlagen</b>	<b>37</b>
2.1 Grundlagen der Mengenlehre . . . . .	38
2.1.1 Der Mengenbegriff . . . . .	38
2.1.2 Mengenoperationen . . . . .	40
2.2 Relationen und Funktionen . . . . .	43
2.3 Die Welt der Zahlen . . . . .	51
2.3.1 Natürliche, rationale und reelle Zahlen . . . . .	51
2.3.2 Von großen Zahlen . . . . .	54
2.3.3 Die Unendlichkeit begreifen . . . . .	56
2.4 Rekursion und induktive Beweise . . . . .	64
2.4.1 Vollständige Induktion . . . . .	65
2.4.2 Strukturelle Induktion . . . . .	67
2.5 Übungsaufgaben . . . . .	69
<b>3 Logik und Deduktion</b>	<b>77</b>
3.1 Aussagenlogik . . . . .	78
3.1.1 Syntax und Semantik . . . . .	78
3.1.2 Normalformen . . . . .	87
3.1.3 Beweistheorie . . . . .	92
3.1.3.1 Hilbert-Kalkül . . . . .	93
3.1.3.2 Resolutionskalkül . . . . .	101
3.1.3.3 Tableaukalkül . . . . .	105
3.1.4 Anwendung: Hardware-Entwurf . . . . .	108
3.2 Prädikatenlogik . . . . .	113

3.2.1	Syntax und Semantik . . . . .	114
3.2.2	Normalformen . . . . .	118
3.2.3	Beweistheorie . . . . .	120
3.2.3.1	Resolutionskalkül . . . . .	126
3.2.3.2	Tableaukalkül . . . . .	131
3.2.4	Anwendung: Logische Programmierung . . . . .	134
3.3	Logiken höherer Stufe . . . . .	141
3.4	Übungsaufgaben . . . . .	144
<b>4</b>	<b>Formale Sprachen</b>	<b>153</b>
4.1	Sprache und Grammatik . . . . .	154
4.2	Chomsky-Hierarchie . . . . .	160
4.3	Reguläre Sprachen . . . . .	162
4.3.1	Definition und Eigenschaften . . . . .	162
4.3.2	Pumping-Lemma für reguläre Sprachen . . . . .	164
4.3.3	Reguläre Ausdrücke . . . . .	166
4.4	Kontextfreie Sprachen . . . . .	169
4.4.1	Definition und Eigenschaften . . . . .	169
4.4.2	Normalformen . . . . .	169
4.4.2.1	Chomsky-Normalform . . . . .	169
4.4.2.2	Backus-Naur-Form . . . . .	171
4.4.3	Pumping-Lemma für kontextfreie Sprachen . . . . .	172
4.4.4	Entscheidungsprobleme . . . . .	176
4.4.5	Abschlusseigenschaften . . . . .	178
4.5	Kontextsensitive Sprachen . . . . .	181
4.5.1	Definition und Eigenschaften . . . . .	181
4.5.2	Entscheidungsprobleme . . . . .	182
4.5.3	Abschlusseigenschaften . . . . .	183
4.6	Rekursiv aufzählbare Sprachen . . . . .	183
4.7	Übungsaufgaben . . . . .	185
<b>5</b>	<b>Endliche Automaten</b>	<b>191</b>
5.1	Begriffsbestimmung . . . . .	192
5.2	Deterministische Automaten . . . . .	194
5.2.1	Definition und Eigenschaften . . . . .	194
5.2.2	Automatenminimierung . . . . .	196
5.3	Nichtdeterministische Automaten . . . . .	198
5.3.1	Definition und Eigenschaften . . . . .	198
5.3.2	Satz von Rabin, Scott . . . . .	200
5.3.3	Epsilon-Übergänge . . . . .	203
5.4	Automaten und reguläre Sprachen . . . . .	206
5.4.1	Abschlusseigenschaften . . . . .	208

5.4.2	Entscheidungsprobleme . . . . .	210
5.5	Kellerautomaten . . . . .	211
5.5.1	Definition und Eigenschaften . . . . .	211
5.5.2	Kellerautomaten und kontextfreie Sprachen . . . . .	214
5.5.3	Deterministische Kellerautomaten . . . . .	216
5.6	Transduktoren . . . . .	218
5.6.1	Definition und Eigenschaften . . . . .	218
5.6.2	Automatenminimierung . . . . .	219
5.6.3	Automatensynthese . . . . .	221
5.6.4	Mealy- und Moore-Automaten . . . . .	222
5.7	Petri-Netze . . . . .	226
5.8	Zelluläre Automaten . . . . .	231
5.9	Übungsaufgaben . . . . .	234
<b>6</b>	<b>Berechenbarkeitstheorie</b> . . . . .	<b>241</b>
6.1	Berechnungsmodelle . . . . .	242
6.1.1	Loop-Programme . . . . .	242
6.1.2	While-Programme . . . . .	248
6.1.3	Goto-Programme . . . . .	252
6.1.4	Primitiv-rekursive Funktionen . . . . .	257
6.1.5	Turing-Maschinen . . . . .	265
6.1.5.1	Einband-Turing-Maschinen . . . . .	265
6.1.5.2	Einseitig und linear beschränkte Turing-Maschinen . . . . .	273
6.1.5.3	Mehrspur-Turing-Maschinen . . . . .	274
6.1.5.4	Mehrband-Turing-Maschinen . . . . .	274
6.1.5.5	Maschinenkomposition . . . . .	276
6.1.5.6	Universelle Turing-Maschinen . . . . .	277
6.1.5.7	Zelluläre Turing-Maschinen . . . . .	281
6.1.6	Alternative Berechnungsmodelle . . . . .	283
6.1.6.1	Registermaschinen . . . . .	284
6.1.6.2	Lambda-Kalkül . . . . .	288
6.2	Church'sche These . . . . .	290
6.3	Akzeptierende Turing-Maschinen . . . . .	297
6.4	Entscheidbarkeit . . . . .	303
6.5	Unentscheidbare Probleme . . . . .	307
6.5.1	Halteproblem . . . . .	307
6.5.2	Satz von Rice . . . . .	310
6.5.3	Reduktionsbeweise . . . . .	313
6.5.4	Das Post'sche Korrespondenzproblem . . . . .	314
6.5.5	Weitere unentscheidbare Probleme . . . . .	318
6.6	Übungsaufgaben . . . . .	321

<b>7 Komplexitätstheorie</b>	<b>329</b>
7.1 Algorithmische Komplexität . . . . .	330
7.1.1 O-Kalkül . . . . .	337
7.1.2 Rechnen im O-Kalkül . . . . .	340
7.2 Komplexitätsklassen . . . . .	344
7.2.1 P und NP . . . . .	347
7.2.2 PSPACE und NPSPACE . . . . .	352
7.2.3 EXP und NEXP . . . . .	353
7.2.4 Komplementäre Komplexitätsklassen . . . . .	355
7.3 NP-Vollständigkeit . . . . .	357
7.3.1 Polynomielle Reduktion . . . . .	357
7.3.2 P-NP-Problem . . . . .	358
7.3.3 Satz von Cook . . . . .	359
7.3.4 Reduktionsbeweise . . . . .	366
7.4 Übungsaufgaben . . . . .	372
<b>A Notationsverzeichnis</b>	<b>383</b>
<b>B Abkürzungsverzeichnis</b>	<b>387</b>
<b>C Glossar</b>	<b>389</b>
<b>Literaturverzeichnis</b>	<b>417</b>
<b>Namensverzeichnis</b>	<b>423</b>
<b>Sachwortverzeichnis</b>	<b>425</b>

# 1 Einführung

---

„Wir müssen wissen. Wir werden wissen.“

David Hilbert

## 1.1 Was ist theoretische Informatik?

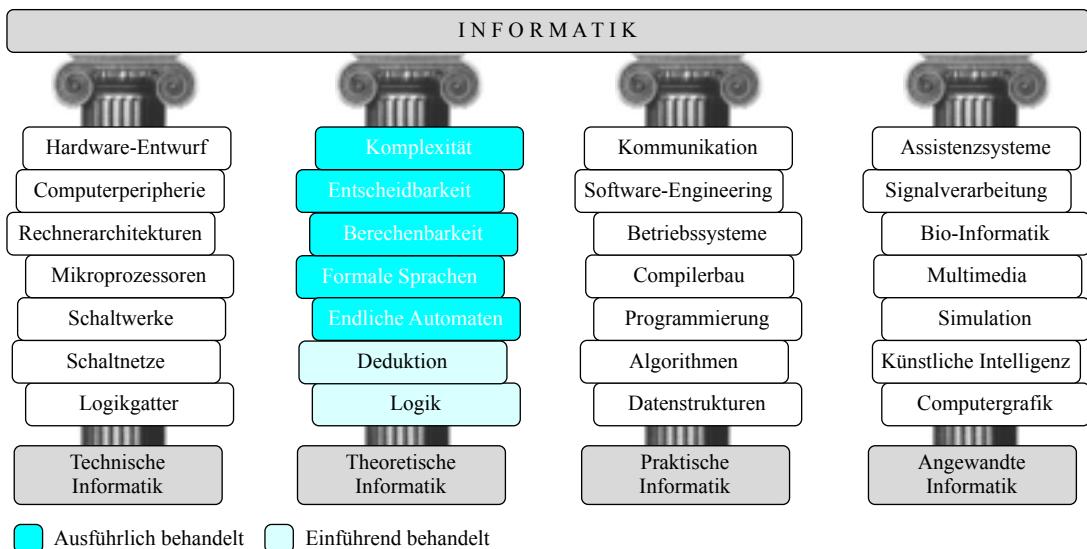
Kaum eine andere Technologie hat unser tägliches Leben so rasant und nachhaltig verändert wie der Computer. Unzählige Bereiche des täglichen Lebens werden inzwischen von Bits und Bytes dominiert – selbst solche, die noch vor einigen Jahren als elektronikfreie Zone galten. Die Auswirkungen dieser Entwicklung sind bis in unser gesellschaftliches und kulturelles Leben zu spüren und machen selbst vor der deutschen Sprache keinen Halt. Vielleicht haben auch Sie heute schon *gemailt*, *gesimst* oder *gegoogelt* (Abbildung 1.1). Die Digitalisierung unserer Welt ist in vollem Gange und eine Abschwächung der eingeschlagenen Entwicklung zumindest mittelfristig nicht abzusehen.

Die in der Retrospektive einzigartige Evolution der Computertechnik ist eng mit der Entwicklung der Informatik verbunden. Als naturwissenschaftliche Fundierung der Computertechnik untersucht sie die Methoden und Techniken, die eine digitale Welt wie die unsere erst möglich machen. In der gleichen Geschwindigkeit, in der Computer die Welt eroberten, konnte sich die Informatik von einer Nischendisziplin der Mathematik und Elektrotechnik zu einer eigenständigen Grundlagenwissenschaft entwickeln. War sie zu Anfang auf wenige Kernbereiche beschränkt, so präsentiert sich die Informatik mittlerweile als eine breit gefächerte Wissenschaftsdisziplin. Heute existieren Schnittstellen in die verschiedensten Bereiche wie die Biologie, die Medizin und sogar die bildenden Künste.

In Abbildung 1.2 sind die vier Säulen dargestellt, von denen die Informatik gegenwärtig getragen wird. Eine davon ist die theoretische Informatik. Sie beschäftigt sich mit den abstrakten Konzepten und Methoden, die sich hinter den Fassaden moderner Computersysteme verbergen. Die theoretische Informatik ist vor der technischen Informatik die älteste Kernsäule und hat ihren direkten Ursprung in der Mathematik.



**Abbildung 1.1:** Die zunehmende Technisierung des Alltagslebens macht auch vor der deutschen Sprache keinen Halt. Im Jahre 2004 schaffte es das neudeutsche Verb *googeln* in den Duden [97]. Dort finden sich auch die Worte *mailen*, *simsen* und *downloaden* wieder.



**Abbildung 1.2:** Die vier Säulen der Informatik

Trotz ihres relativen Alters hat dieser Zweig der Informatik nichts von seiner ursprünglichen Bedeutung verloren. Er bildet das konzeptionelle Fundament, auf dem die anderen Bereiche der Informatik solide ruhen und aus dessen Wissensfundus sie schöpfen.

Betrachten wir die inhaltlichen Themen der modernen theoretischen Informatik genauer, so lassen sich diese in die folgenden Teilgebiete untergliedern (vgl. Abbildung 1.3):

#### ■ Logik und Deduktion (Kapitel 3)

Die Logik ist ein Teilbereich der Mathematik, der sich mit grundlegenden Fragestellungen mathematischer Theorien beschäftigt. Im Mittelpunkt steht die Untersuchung *formaler Systeme (Kalküle)*, in denen Aussagen durch die Anwendung fest definierter Regeln auf eine kleine Menge vorgegebener Axiome abgeleitet werden. Die formale Logik spielt nicht nur in der theoretischen Informatik eine Rolle. Zum einen gibt sie uns in Form der Aussagenlogik ein Instrumentarium an die Hand, mit dem wir jede erdenkliche Hardware-Schaltung formal beschreiben und analysieren können. Zum anderen lässt sich mit der Prädikatenlogik und den Logiken höherer Stufe das Verhalten komplexer Hardware- und Software-Systeme exakt spezifizieren und in Teilen verifizieren.

### ■ Formale Sprachen (Kapitel 4)

Die Theorie der formalen Sprachen beschäftigt sich mit der Analyse, der Klassifikation und der generativen Erzeugung von Wortmengen. Künstliche Sprachen sind nach festen Regeln aufgebaut, die zusammen mit dem verwendeten Symbolvorrat eine formale Grammatik bilden. Die zugrunde liegende Theorie gibt uns die Methoden und Techniken an die Hand, die für den systematischen Umgang mit modernen Programmiersprachen und dem damit zusammenhängenden Compilerbau unabdingbar sind. Viele Erkenntnisse aus diesem Bereich haben ihre Wurzeln in der Linguistik und stoßen dementsprechend auch außerhalb der Informatik auf reges Interesse.

### ■ Automatentheorie (Kapitel 5)

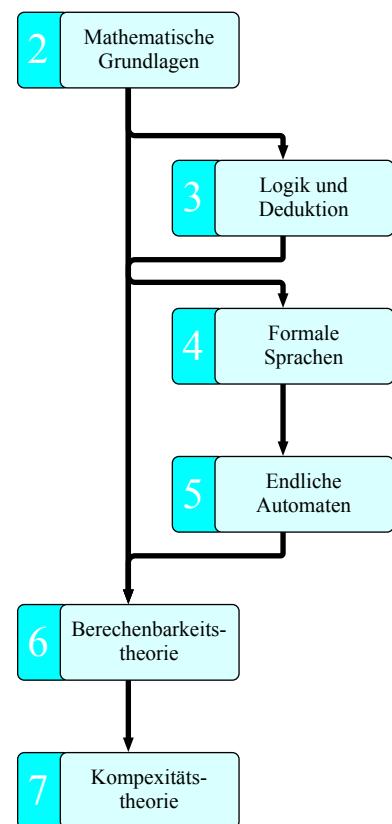
Hinter dem Begriff des endlichen Automaten verbirgt sich ein abstraktes Maschinenmodell, das sich zur Modellierung, zur Analyse und zur Synthese zustandsbasierter Systeme eignet. Auf der obersten Ebene untergliedern sich endliche Automaten in Akzeptoren und Transduktoren. Erstere zeigen einen engen Bezug zu den formalen Sprachen, Letztere spielen im Bereich des Hardware-Entwurfs eine dominierende Rolle. Sie sind das mathematische Modell, mit dem sich das zeitliche Verhalten synchron getakteter Digitalschaltungen exakt beschreiben und analysieren lässt.

### ■ Berechenbarkeitstheorie (Kapitel 6)

Die Berechenbarkeitstheorie beschäftigt sich mit grundlegenden Untersuchungen über die algorithmische Lösbarkeit von Problemen. Die Bedeutung dieses Teilgebiets der theoretischen Informatik ist zweigeteilt. Zum einen wird das gesamte Gebiet der Algorithmentechnik durch die Definition formaler Berechnungsmodelle auf einen formalen Unterbau gestellt. Zum anderen ermöglicht uns die systematische Vorgehensweise, die Grenzen der prinzipiellen Berechenbarkeit auszuloten.

### ■ Komplexitätstheorie (Kapitel 7)

Während die Berechenbarkeitstheorie Fragen nach der puren Existenz von Algorithmen beantwortet, versucht die Komplexitätstheorie die Eigenschaften einer Lösungsstrategie quantitativ zu erfassen. Algorithmen werden anhand ihres Speicherplatzbedarfs und Zeitverbrauchs in verschiedene Komplexitätsklassen eingeteilt, die Rückschlüsse auf deren praktische Verwertbarkeit zulassen. Die Ergebnisse dieser Theorie beeinflussen den gesamten Bereich der modernen Software- und Hardware-Entwicklung.



**Abbildung 1.3:** Kapitelübersicht. Die Pfeile deuten an, wie die einzelnen Kapitel inhaltlich zusammenhängen.

1. Axiom:

*„Zu zwei Punkten gibt es genau eine Gerade, auf der sie liegen.“*



2. Axiom:

*„Jede gerade Strecke zwischen zwei Punkten lässt sich eindeutig verlängern.“*



3. Axiom:

*„Zu einem Punkt und einer Strecke kann man genau einen Kreis konstruieren.“*



4. Axiom:

*„Alle rechten Winkel sind gleich.“*



5. Axiom:

*„Zu einer Geraden und einem Punkt außerhalb der Geraden gibt es genau eine Gerade, die durch den Punkt geht und parallel zur ersten Geraden ist.“*



Euklid von Alexandria  
(ca. 365 v. Chr. – ca. 300 v. Chr.)

**Abbildung 1.4:** Die euklidischen Axiome

## 1.2 Zurück zu den Anfängen

Bevor wir uns ausführlich mit den Begriffen und Methoden der theoretischen Informatik beschäftigen, wollen wir in einem historischen Streifzug herausarbeiten, in welchem Umfeld ihre Teilgebiete entstanden sind und in welchem Zusammenhang sie heute zueinander stehen.

### 1.2.1 Die Mathematik in der Krise

Die theoretische Informatik hat ihre Wurzeln in der Mathematik. Ihre Geschichte beginnt mit der *Grundlagenkrise*, die Anfang des zwanzigsten Jahrhunderts einen Tiefpunkt in der mehrere tausend Jahre alten Historie der Mathematik markierte. Um die Geschehnisse zu verstehen, die die älteste aller Wissenschaften in ihren Grundfesten erschütterten, wollen wir unseren Blick zunächst auf das achtzehnte Jahrhundert richten. Zu dieser Zeit war die Mathematik schon weit entwickelt, jedoch noch lange nicht die abstrakte Wissenschaft, wie wir sie heute kennen. Fest in der realen Welt verankert, wurde sie vor allem durch Problemstellungen der physikalischen Beobachtung vorangetrieben. Zahlen waren nichts weiter als Messgrößen für reale Objekte und weit von den immateriellen Gedankengebilden der modernen Zahlentheorie entfernt. So wenig wie die Mathematik als eigenständige Wissenschaft existierte, so wenig gab es den reinen Mathematiker.

Im neunzehnten Jahrhundert änderte sich die Sichtweise allmählich in Richtung einer abstrakteren Mathematik. Zahlen und Symbole wurden von ihrer physikalischen Interpretation losgelöst betrachtet und entwickelten sich langsam, aber beharrlich zu immer abstrakter werdenden Größen. Mit der geänderten Sichtweise war es nun möglich, eine Gleichung der Form

$$c^2 = a^2 + b^2 \quad (1.1)$$

völlig unabhängig von ihrer pythagoreischen Bedeutung zu betrachten. In ihrer abstraktesten Interpretation lässt sie sich als mathematisches Spiel begreifen, das uns erlaubt, die linke Seite durch die rechte zu ersetzen. Die Variablen  $a$ ,  $b$  und  $c$  degradieren in diesem Fall zu inhaltsleeren Größen, die in keinerlei Bezug mehr zu den Seitenlängen eines rechtwinkligen Dreiecks stehen.

Dass es richtig war, das mathematische Gedankengerüst von seiner physikalischen Interpretation zu trennen, wurde durch die Physik selbst untermauert. So machte die zu Beginn des zwanzigsten Jahrhunderts auf-

„Wenn es sich darum handelt, die Grundlagen einer Wissenschaft zu untersuchen, so hat man ein System von Axiomen aufzustellen, welche eine genaue und vollständige Beschreibung derjenigen Beziehungen enthalten, die zwischen den elementaren Begriffen jener Wissenschaft stattfinden. Die aufgestellten Axiome sind zugleich die Definitionen jener elementaren Begriffe und jede Aussage innerhalb des Bereiches der Wissenschaft, deren Grundlagen wir prüfen, gilt uns nur dann als richtig, falls sie sich mittelst einer endlichen Anzahl logischer Schlüsse aus den aufgestellten Axiomen ableiten lässt. Bei näherer Betrachtung entsteht die Frage, ob etwa gewisse Aussagen einzelner Axiome sich untereinander bedingen und ob nicht somit die Axiome noch gemeinsame Bestandteile enthalten, die man beseitigen muss, wenn man zu einem System von Axiomen gelangen will, die völlig voneinander unabhängig sind.“

Vor allem aber möchte ich unter den zahlreichen Fragen, welche hinsichtlich der Axiome gestellt werden können, dies als das wichtigste Problem bezeichnen, zu beweisen, dass dieselben untereinander widerspruchsfrei sind, d.h., dass man aufgrund derselben mittelst einer endlichen Anzahl von logischen Schlüssen niemals zu Resultaten gelangen kann, die miteinander in Widerspruch stehen.“



David Hilbert  
(1862 – 1943)

**Abbildung 1.5:** Auszug aus Hilberts historischer Millenium-Rede auf dem internationalen Kongress der Mathematiker in Paris

keimende Quantenmechanik deutlich, dass die damals wie heute merkwürdig anmutenden Effekte der Elementarteilchenphysik nur mit Hilfe abstrakter Modelle präzise erfasst werden können. Viele mathematische Konstrukte wie z. B. der *Hilbertraum* oder die *abstrakte Gruppe* konnten nachträglich zur Beschreibung der Natur eingesetzt werden, obwohl diese nichts mit unserer makroskopischen Anschauung gemeinsam haben.

Die zunehmende Abstraktion ließ Raum für Fragen zu, die sich in einer physikalisch interpretierten Mathematik nicht stellen. Interpretieren wir z. B. die *euklidischen Axiome* (Abbildung 1.4) ausschließlich im Sinne der klassischen Geometrie, so erscheinen sie als reine Selbstverständlichkeit. Sie decken sich mit den Erfahrungen, die wir in der makroskopischen Welt täglich machen und kaum jemand würde auf die Idee kommen, an ihnen zu zweifeln. Entsprechend lange galten die Axiome als unantastbar.

Die Situation ändert sich, sobald wir die Mathematik als ein abstraktes Wechselspiel von Symbolen und Regeln betreiben. Lösen wir uns von der intuitiven Interpretation der euklidischen Axiome, so stellt sich



Gottlob Frege  
(1848 – 1925)

**Abbildung 1.6:** Gottlob Frege. Der im mecklenburgischen Wismar geborene Mathematiker zählt zu den Mitbegründern der mathematischen Logik und der analytischen Philosophie. Im Jahre 1879 eröffnete Frege mit seiner berühmten *Begriffschrift* einen axiomatischen Zugang zur Logik [34]. Er führt darin die grundlegenden Konzepte und Begriffe ein, die wir auch heute noch in der Prädikatenlogik (Abschnitt 3.2) und den Logiken höherer Stufe (Abschnitt 3.3) verwenden. Sein Begriffsgerüst war deutlich weiter entwickelt als die Syllogismen des Aristoteles – der bis dato präzisesten Form des logischen Schließens. Die meiste Zeit seines Lebens war Frege ein überzeugter Verfechter des *Logizismus*. Er vertrat die Auffassung, dass die Mathematik ein Teil der Logik sei. In diesem Sinne müssen sich alle Wahrheiten auf eine Menge von Axiomen zurückführen lassen, die nach Freges Worten „*eines Beweises weder fähig noch bedürftig*“ seien. Er stand damit in einer Gegenposition zu anderen Mathematikern seiner Zeit, von denen viele die Logik als isoliertes Teilgebiet der Mathematik begriffen.

die Frage, ob diese ein vollständiges und widerspruchsfreies Gebilde ergeben. Im Jahre 1899 gelang es David Hilbert, diese Frage positiv zu beantworten. Er postulierte ein Axiomensystem, aus dem sich alle Sätze der euklidischen Geometrie ableiten lassen, ohne die verwendeten Symbole mit einer speziellen Interpretation zu versehen [45].

Inspiriert von den Anfangserfolgen stand die Mathematik um die Jahrhundertwende vollends im Zeichen der axiomatischen Methode. Das Führen eines Beweises wurde als der Prozess verstanden, Sätze durch die Anwendung wohldefinierter Schlussregeln aus einer kleineren Menge vorgegebener, *a priori* als wahr definierter Axiome abzuleiten. Eine spezielle Interpretation der Symbole war dazu weder erforderlich noch in jedem Fall angestrebt. Die Mathematik wurde zu einem Schachspiel, in dem die Regeln die Partie bestimmen und nicht die Bedeutung der Figuren. Hilberts axiomatische Methode birgt das Maß an Ehrlichkeit und Klarheit in sich, nach der Mathematiker von jeher streben: Sie ist frei von Interpretationsspielräumen jeglicher Art.

Der deutsche Mathematiker David Hilbert war kein Unbekannter. Bereits zu Lebzeiten wurde er als Ikone gefeiert und beeinflusste wie kein anderer die Mathematik des beginnenden zwanzigsten Jahrhunderts. Im Jahre 1900 hielt Hilbert auf dem internationalen Kongress der Mathematiker in Paris eine wegweisende Rede, an der sich die weitere Stoßrichtung der gesamten Mathematik über Jahre hinweg orientieren sollte (vgl. Abbildung 1.5). In seiner Ansprache trug er 23 ungelöste Probleme vor, die für die Mathematik von immenser Wichtigkeit, aber bis dato eben ungelöst waren. Bereits an zweiter Stelle forderte Hilbert die Weltgemeinschaft dazu auf, einen Beweis für die Widerspruchsfreiheit der arithmetischen Axiome zu liefern. Ein solcher Beweis ist von tragender Bedeutung für die gesamte Mathematik, da nahezu alle ihre Teilbereiche auf der Theorie der Zahlen aufbauen. Solange die Widerspruchsfreiheit nicht garantiert werden kann, besteht die Möglichkeit, dass sich sowohl die Gleichung  $1 + 1 = 2$  als auch die Gleichung  $1 + 1 \neq 2$  aus den Axiomen ableiten lassen. Die Auswirkungen wären von fatalistischem Ausmaß für alle Bereiche der Mathematik.

Bereits kurze Zeit später sollte die Wissenschaftsgemeinde erleben, wie real eine solche Gefahr wirklich war. Der deutsche Mathematiker Gottlob Frege (Abbildung 1.6) spürte sie am eigenen Leib, als er im Jahre 1902 ein formales Axiomensystem für ein Teilgebiet der Mathematik aufstellte, das auf den ersten Blick so intuitiv und einfach erscheint wie kaum ein anderes. Die Rede ist von der *Mengenlehre*. Der zweite Band seiner „Grundgesetze der Arithmetik“ schließt mit dem folgenden Nachwort [32, 33]:

*„Einem wissenschaftlichen Schriftsteller kann kaum etwas Unerwünschteres begegnen, als dass ihm nach Vollendung einer Arbeit eine der Grundlagen seines Baues erschüttert wird.“*

Doch wodurch wurde Freges Arbeit so grundlegend erschüttert, dass er sein gesamtes Werk gefährdet sah? Die Antwort ist in einem Brief von Bertrand Russell zu finden, den er im Jahre 1902 an Frege schickte – just zu der Zeit, als dieser sein mathematisches Werk vollendete. Aufbauend auf den Begriffen der naiven Mengenlehre definierte Russell die Menge aller Mengen, die sich nicht selbst als Element enthalten:

$$M := \{M' \mid M' \notin M'\} \quad (1.2)$$

Die Definition von  $M$  ist mit der damals verwendeten Mengendefinition von Georg Cantor vereinbar, führt bei genauerer Betrachtung jedoch unweigerlich zu einem Widerspruch. Da für jedes Element  $a$  und jede Menge  $M$  entweder  $a \in M$  oder  $a \notin M$  gilt, muss auch  $M$  entweder in sich selbst enthalten sein oder nicht. Die Definition von  $M$  offenbart uns jedoch das folgende erstaunliche Ergebnis:

$$M \in M \Rightarrow M \notin M, \quad M \notin M \Rightarrow M \in M \quad (1.3)$$

Der als *Russell'sche Antinomie* bekannte Widerspruch entlarvte den Cantor'schen Mengenbegriff als in sich widersprüchlich und lies Freges Gedankengerüst wie ein Kartenhaus in sich zusammenstürzen. Die Geschehnisse unterstrichen nachhaltig, wie wichtig eine widerspruchsfreie Fundierung der Mathematik tatsächlich war.

Zu den ersten, die sich der neugeborenen Herausforderung stellten, gehörten die britischen Mathematiker Bertrand Russell und Alfred North Whitehead. Sie starteten den Versuch, ein widerspruchsfreies Fundament zu errichten, auf dem die Mathematik für alle Zeiten einen sicheren Halt finden sollte. Nach zehn Jahren intensiver Arbeit war das Ergebnis greifbar: Die *Principia Mathematica* waren fertiggestellt (vgl. Abbildung 1.7). In einem dreibändigen Werk unternahmen Russell und Whitehead den Versuch, weite Bereiche der Mathematik mit den Mitteln der elementaren Logik formal herzuleiten. Ein großer Teil des Werks ist der *Typentheorie* gewidmet; einer widerspruchsfreien Konstruktion des Mengenbegriffs, mit dem die Art von Selbstbezug vermieden wird, die wenige Jahre zuvor die Mathematik in ihre größte Krise stürzte. Heute gilt die Typentheorie der Principia als überholt. An ihre Stelle tritt der formale axiomatische Aufbau der Mengenlehre durch Ernst Zermelo und Abraham Fraenkel, der die Russell'sche Antinomie ebenfalls beseitigt [31, 102].

Die mathematische Widerspruchsfreiheit ist eine unabdingbare Eigenschaft des mathematischen Schließens. Fehlt sie, so verkommt jedes formale System zu einem wertlosen Gedankengebilde. Warum dies so ist, wollen wir im Folgenden kurz begründen. Nehmen wir an, es gebe eine Aussage  $R$ , für die sich sowohl  $R$  als auch ihre Negation  $\neg R$  innerhalb des Kalküls ableiten lassen. Die Situation erscheint wenig bedrohlich, wenn es sich um eine Aussage handelt, die uns nicht weiter interessiert. Eventuell ist  $R$  eine Aussage der Russell'schen Art, die uns ohnehin suspekt erscheint. Können wir den Kalkül vielleicht trotzdem sinnvoll einsetzen, wenn wir Aussagen dieser Form schlicht außen vor lassen?

Dass sich widersprüchliche Aussagen in einem Kalkül nicht isoliert betrachten lassen, liegt an den Schlussregeln der klassischen Logik. In Kapitel 3 werden Sie erlernen, wie sich das Theorem

$$\neg P \rightarrow (P \rightarrow Q)$$

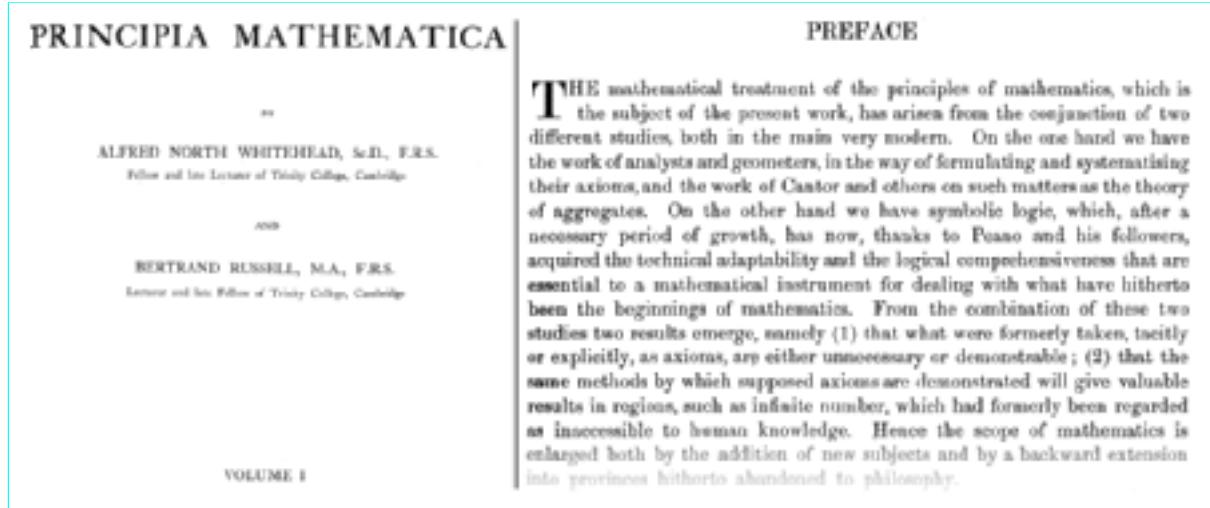
aus den elementaren Axiomen der Logik herleiten lässt. In Worten besagt es: Ist  $P$  falsch, so folgt aus der Wahrheit von  $P$  die Wahrheit von  $Q$ . Substituieren wir  $R$  für  $P$ , so erhalten wir das Theorem

$$\neg R \rightarrow (R \rightarrow Q).$$

Da  $\neg R$  eine wahre Aussage ist, lässt sich mit Hilfe der *Abtrennungsregel (Modus ponens)* das Theorem

$$R \rightarrow Q$$

herleiten. Nach Voraussetzung ist  $R$  ebenfalls wahr, so dass eine erneute Anwendung der Abtrennungsregel das Theorem  $Q$  hervorbringt. Da die Wahl von  $Q$  keinen Einschränkungen unterliegt, können wir eine beliebige Aussage für  $Q$  substituieren. Kurzum: In einem widersprüchlichen Kalkül lassen sich ausnahmslose alle Aussagen als wahr beweisen.



**Abbildung 1.7:** Die *Principia Mathematica* von Bertrand Russell und Alfred North Whitehead ist eines der berühmtesten mathematischen Werke unserer Geschichte. Die Principia, erstmals erschienen in den Jahren 1910 bis 1913, stand ganz im Zeichen des Hilbertprogramms. Auf über 1800 Seiten, verteilt auf 3 Bände, unternahmen die Autoren den Versuch, alle mathematischen Erkenntnisse aus einer kleinen Menge von Axiomen systematisch herzuleiten.

Die Principia stand ganz im Zeichen des *Hilbertprogramms* und war in puncto Präzision jedem anderen Werk ihrer Zeit weit voraus. Sie fasste einen mathematischen Beweis als eine Folge von Regelanwendungen auf, durch die eine Aussage in endlich vielen Schritten aus einer festgelegten Menge von Axiomen abgeleitet wurde.

Durch die zunehmende Beschäftigung mit den verschiedensten formalen Systemen entstand im Laufe der Zeit eine Meta-Mathematik, die sich nicht mit der Ableitung von Sätzen *innerhalb* eines Kalküls beschäftigt, sondern mit Sätzen, die Aussagen *über* den Kalkül treffen. Drei Fragestellungen rückten in diesem Zusammenhang in das Zentrum des Interesses:

#### ■ Vollständigkeit

Ein formales System heißt *vollständig*, wenn jede wahre Aussage, die in der Notation des Kalküls formuliert werden kann, innerhalb desselben beweisbar ist. Mit anderen Worten: Für jede wahre Aussage  $P$  muss es eine endliche Kette von Regelanwendungen geben, die  $P$  aus den Axiomen deduziert. Beachten Sie, dass uns ein vollständiger Kalkül nicht preisgeben muss, wie eine solche Kette zu finden ist. Die Vollständigkeit garantiert lediglich deren Existenz.

### ■ Widerspruchsfreiheit

Ein formales System heißt *widerspruchsfrei*, wenn für eine Aussage  $P$  niemals gleichzeitig  $P$  und die Negation von  $P$  (geschrieben als  $\neg P$ ) abgeleitet werden kann. Auf die immense Bedeutung der Widerspruchsfreiheit eines Kalküls sind wir weiter oben bereits eingegangen. Erfüllt ein formales System diese Eigenschaft nicht, so könnte es kaum wertloser sein. Es würde uns gestatten, jede beliebige Aussage zu beweisen.

### ■ Entscheidbarkeit

Ein formales System heißt *entscheidbar*, wenn ein systematisches Verfahren existiert, mit dem für jede Aussage entschieden werden kann, ob sie innerhalb des Kalküls beweisbar ist. Hinter der Eigenschaft der Entscheidbarkeit verbirgt sich nichts Geringeres als der Wunsch nach einer mechanisierten Mathematik. Wäre z. B. die Zahlentheorie vollständig und entscheidbar, so ließe sich für jede wahre zahlentheoretische Aussage auf maschinellem Wege ein Beweis konstruieren. Der Traum eines jeden Mathematikers würde wahr.

Hilbert war überzeugt, dass eine vollständige, widerspruchsfreie und entscheidbare Axiomatisierung der Mathematik möglich sei. Im Jahre 1929 wurden seine Hoffnungen durch die Arbeiten des jungen Mathematikers Kurt Gödel zusätzlich genährt, als dieser in seiner Promotionschrift die Vollständigkeit der Prädikatenlogik erster Stufe bewies [35]. Es war also möglich, einen Kalkül zu konstruieren, in dem sich jede wahre prädikatenlogische Formel in endlich vielen Schritten aus den Axiomen ableiten lässt. In diesen Tagen glaubte man das Hilbertprogramm auf einem guten Weg und es schien nur eine Frage der Zeit zu sein, bis aus Hilberts Vermutungen Gewissheit werden würde.

1930 war das Jahr, in dem die Entwicklung eine abrupte Kehrtwende nehmen sollte. Am 8. September bekräftigte Hilbert vor der Versammlung Deutscher Naturforscher und Ärzte in seiner Heimatstadt Königsberg seine tiefe Überzeugung, dass es in der Wissenschaft keine unlösbareren Probleme gibt. Ein Auszug aus seiner Rede wurde in Form einer Radioansprache ausgestrahlt. Sie schließt mit den berühmten Worten:

*„Wir dürfen nicht denen glauben, die heute mit philosophischer Miene und überlegenem Tone den Kulturuntergang prophezeien und sich in dem Ignorabimus gefallen. Für uns gibt es kein Ignorabimus, und meiner Meinung nach auch für die Naturwissenschaft überhaupt nicht. Statt des törichten Ignorabimus heiße im Gegenteil unsere Lösung: Wir müssen wissen, wir werden wissen.“*

*„Ignoramus et ignorabimus.“*  
(Wir wissen es nicht und wir werden es niemals wissen)



Emil Heinrich Du Bois-Reymond  
(1818 – 1896)

*„Für uns gibt es kein Ignorabimus.“*  
Mit diesem Satz bekräftigte David Hilbert seine Haltung, dass es in den Naturwissenschaften keine unbeweisbaren Wahrheiten gibt. Der Begriff *Ignorabimus* wurde durch den deutschen Gelehrten Emil Heinrich Du Bois-Reymond geprägt. Durch seine Leipziger Rede vor der Versammlung Deutscher Naturforscher und Ärzte löste er im Jahre 1872 einen Richtungsstreit aus, der auf Jahre hinweg zu kontroversen Diskussionen in der Wissenschaftsgemeinde führen sollte. Er vertrat die Meinung, dass Begriffe wie das Bewusstsein niemals mit naturwissenschaftlichen Methoden erklärbar sein werden. Kurzum: Die Wissenschaft besitzt unüberwindbare Grenzen. „Ich werde jetzt, wie ich glaube, in sehr zwingender Weise darten, dass nicht allein bei dem heutigen Stand unserer Kenntnis das Bewusstsein aus seinen materiellen Bedingungen nicht erklärbar ist, was wohl jeder zugibt, sondern dass es auch der Natur der Dinge nach aus diesen Bedingungen nicht erklärbar sein wird.“ [8].

Der Unvollständigkeitsbeweis ist nicht nur aufgrund seiner inhaltlichen Tragweite von Bedeutung. Auch die trickreiche Beweisführung, mit der Gödel sein Resultat erzielte, zeugt von der Tiefgründigkeit des Ergebnisses. Gödel konnte zeigen, dass mathematische Schlussregeln, die Aussagen über Zahlen machen, selbst als Zahl verstanden werden konnten. Damit war es möglich, die Ebene der Zahlentheorie mit ihren Meta-Ebenen zu vermischen. Aussagen sind nichts anderes als Zahlen, die selbst Aussagen über Zahlen tätigen. Auf diese Weise gelang es Gödel, Meta-Aussagen wie „*Aussage XYZ ist beweisbar*“ innerhalb des Systems zu codieren. Um die Unvollständigkeit zu beweisen, wandte Gödel einen Trick an, der an die Russell'sche Antinomie erinnert. Er konstruierte Aussagen, die auf sich selbst Bezug nehmen und so eine Meta-Aussage über sich selbst beinhalten. Es gelang ihm, eine Formel zu konstruieren, die der Meta-Aussage „*Diese Formel ist nicht beweisbar*“ entspricht. Ist die Formel wahr, so lässt sie sich nicht beweisen und das zugrunde liegende Axiomensystem ist unvollständig. Ist sie falsch, so würde ein Beweis für eine falsche Aussage existieren und das Axiomensystem wäre nicht widerspruchsfrei. Mit anderen Worten: Erfüllt ein Axiomensystem die Eigenschaft der Widerspruchsfreiheit, so ist es zwangsläufig unvollständig.

Der Unvollständigkeitsatz zeigte zudem, dass die Widerspruchsfreiheit eines hinreichend aussagekräftigen formalen Systems nicht innerhalb des Systems selbst bewiesen werden kann. Gödel nutzte aus, dass in einem widersprüchlichen System alle Aussagen wahr sind, d. h., ein Kalkül ist genau dann widerspruchsfrei, wenn es eine einzige Aussage gibt, die nicht bewiesen werden kann. Gödel konnte jedoch zeigen, dass eine Aussage der Form „*es existiert eine unbeweisbare Aussage*“ ebenfalls nicht innerhalb des Systems bewiesen werden kann.

Die Hilbert'sche Rede ist im Originalton erhalten und ein unschätzbares Dokument der Zeitgeschichte. Sie zeigt nachdrücklich, wie überzeugt er von der Durchführbarkeit seines ehrgeizigen Programms wirklich war.

Zum Zeitpunkt seiner Rede wusste Hilbert noch nichts von den Ereignissen, die sich am Vortag an anderer Stelle in Königsberg abspielten. Es war die große Stunde eines vierundzwanzigjährigen Mathematikers, der mit der Präsentation seines Unvollständigkeitssatzes die Mathematik aus den Angeln hob. Derselbe Kurt Gödel, der kurze Zeit zuvor die Vollständigkeit der Prädikatenlogik bewies, konnte zeigen, dass die Arithmetik aus fundamentalen Überlegungen heraus unvollständig sein musste. Seine Ergebnisse waren so allgemein, dass sie auf jedes axiomatische System angewendet werden konnten, das ausdrucksstark genug ist, um die Zahlentheorie zu formalisieren. Damit war nicht nur gezeigt, dass der logische Apparat der Principia Mathematica unvollständig war, sondern auch, dass jeder Versuch, die Principia oder ein ähnliches System zu vervollständigen, von Grund auf zum Scheitern verurteilt ist. Gödel versetzte dem Hilbertprogramm einen schweren Schlag, von dem es sich nie erholen sollte.

Gödels Arbeit verwies die Mathematik zweifelsohne in ihre Grenzen, ließ jedoch Hilberts dritte Vermutung außen vor. Auch wenn wir nicht in der Lage sind, einen widerspruchsfreien und zugleich vollständigen Kalkül für die Theorie der Zahlen zu konstruieren, so könnte die Frage nach der Entscheidbarkeit eines Kalküls dennoch positiv beantwortet werden. Der Unvollständigkeitsbeweis schließt nicht aus, dass ein systematisches Verfahren existiert, das für jede Aussage bestimmt, ob es innerhalb des Systems beweisbar ist oder nicht.

Die Hoffnung, dass zumindest diese letzte Frage positiv beantwortet werden könnte, wurde im Jahre 1936 vollends zerstört, als der britische Mathematiker Alan Turing seine grundlegende Arbeit „*On computable numbers, with an application to the Entscheidungsproblem*“ der Öffentlichkeit präsentierte (Abbildung 1.8). Turings Arbeit ist für die theoretische Informatik aus zweierlei Gründen von Bedeutung. Zum einen gelang es ihm als einer der Ersten, die Grenzen der Berechenbarkeit formal zu erfassen und das Entscheidungsproblem negativ zu beantworten; die Jagd nach dem mathematischen Perpetuum Mobile war zu Ende. Zum anderen konstruierte Turing für seinen Beweis ein abstraktes Maschinenmodell, das dem Funktionsprinzip moderner Computer bereits sehr nahe kam. Aus heutiger Sicht bildet das gedankliche Gebilde der *Turing-Maschine* die Nahtstelle zwischen der abstrakten Mathematik des frühen zwanzigsten Jahrhunderts und der Welt der realen Rechenmaschinen. In gewissem Sinne ersann Turing den *missing link*, der die Mathematik in Form des Computers zum Leben erweckte.

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO  
THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

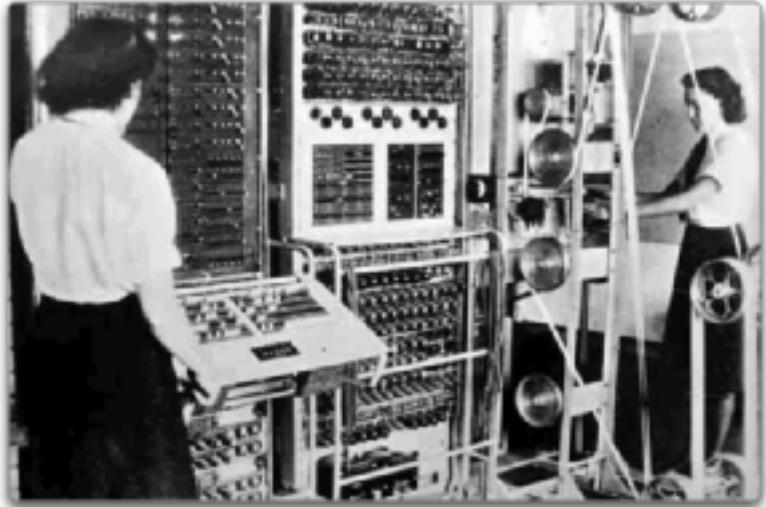
The “computable” numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbersome technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

**Abbildung 1.8:** Im Jahre 1936 postulierte Alan Turing ein abstraktes Maschinenmodell, das die theoretische Informatik bis heute prägt [90]. Mit der *Turing-Maschine* legte er das formale Fundament, auf dem weite Teile der modernen Berechenbarkeitstheorien beruhen.

Turings theoretische Ergebnisse bilden den Kern der modernen Berechenbarkeitstheorie, die in der Informatik die gleiche Bedeutung besitzt wie die Relativitätstheorie in der Physik. Sie weist uns fundamentale Grenzen auf, die wir dem technologischen Fortschritt zum Trotz niemals überwinden können.

In der Tat existieren etliche reale Problemstellungen, die mit mechanisierten Verfahren nicht zu lösen sind. Ein Beispiel ist das *Halteproblem*, das wir in Kapitel 6 in all seinen Facetten untersuchen werden. Es besagt grob, dass kein mechanisiertes Verfahren existiert, mit dem wir immer korrekt entscheiden können, ob ein gegebenes Programm unter einer bestimmten Eingabe anhalten oder unendlich lange laufen wird. Die Unentscheidbarkeit des Halteproblems ist der Grund, dass selbst die modernsten Software-Compiler nicht zuverlässig entscheiden können, ob ein Programm eine Endlosschleife enthält oder nicht. Die Suche nach

**Abbildung 1.9:** Die Colossus Mark II war eine Spezialkonstruktion des britischen Militärs, die im Zweiten Weltkrieg zur Dechiffrierung des deutschen Nachrichtenverkehrs eingesetzt wurde. Ein Prototyp der Maschine, die Mark I, wurde im Dezember 1943 fertiggestellt, ein halbes Jahr später ging die erste Mark II in Betrieb. Bis zum Ende des Kriegs wurden insgesamt 10 Colossus-Rechner gebaut. Zu ihrer Zeit bestach die Maschine durch moderne Technik. Anstelle von elektrischen Relais verarbeiteten die britischen Ingenieure schneller schaltende Triodenröhren. Mit der Colossus gelang es den Briten, den deutschen Code in wenigen Stunden zu brechen.



einem entsprechenden Algorithmus wäre vergebens; die Arbeit von Turing lehrt uns, dass ein solcher aus fundamentalen Überlegungen heraus nicht existieren kann. In Kapitel 6 werden wir uns mit der Berechenbarkeitstheorie im Detail auseinandersetzen und auch den Aufbau und die Funktionsweise der Turing-Maschine ausführlich kennen lernen.

## 1.2.2 Die ersten Rechenmaschinen

Die folgenden Jahre standen ganz im Zeichen der aufkeimenden Computertechnik. Im Jahre 1941 konstruierte Konrad Zuse mit der Z3 einen voll funktionsfähigen Rechner aus ca. 2000 elektromechanischen Relais. Die Maschine wurde mit einer Taktfrequenz von 5 bis 10 Hertz betrieben, kam auf ein Gesamtgewicht von ca. 1000 kg und besaß eine Leistungsaufnahme von 4000 Watt. Rückblickend gehört der Bau der Z3 zu den bedeutendsten Meilensteinen auf dem Weg in das Informationszeitalter.

In den kommenden Jahren diktierte der politische Umbruch den Lauf der Dinge. Der aufkeimende Zweite Weltkrieg holte die Wissenschaft in die reale Welt zurück – eine Welt, in der Not und Furcht keinen Platz für „mathematische Spielereien“ ließen. Turing, der mit seinem abstrakten Rechnermodell ein paar Jahre zuvor die Grenzen der Berechenbarkeit auslotete, konnte sich den weltgeschichtlichen Ereignissen nicht entziehen. Auch für ihn war die Zeit gekommen, sich aus der theoretischen Gedankenwelt zu verabschieden. Zusammen mit einer Reihe anderer

Wissenschaftler begab sich Turing nach Bletchley Park, einem idyllischen Landsitz in der Grafschaft Buckinghamshire. Dort suchte er als Mitglied eines geheimen Konsortiums im Dienst der britischen Regierung nach Möglichkeiten, um den militärischen Verschlüsselungscodes der deutschen Truppen zu brechen.

Während des Zweiten Weltkriegs chiffrierte die deutsche Wehrmacht den Nachrichtenverkehr mit Hilfe der *Enigma* – einer Maschine, die auf dem Prinzip der *polyalphabetischen Substitution* beruht [6,47]. Obwohl die Funktionsweise aus heutiger Sicht primitiv erscheint, hätte die manuelle Dechiffrierung mehrere Monate in Anspruch genommen.

Um den deutschen Nachrichtenverkehr zeitnah zu entschlüsseln, konstruierten die britischen Wissenschaftler mit der *Colossus* eine Rechenmaschine, die auf das Brechen des Enigma-Codes spezialisiert war (Abbildung 1.9). Nach anfänglichen Schwierigkeiten gelang es den Briten schließlich, die Funksprüche der deutschen Truppen in nur noch wenigen Stunden zu entschlüsseln. Für Turing hatte der Bau der *Colossus* einen ganz besonderen Aspekt, denn obwohl sich die Maschine in vielen Punkten von seinem abstrakten Maschinenmodell unterschied, wurde ein großer Teil seiner Idee plötzlich real. Realer als ihm wahrscheinlich selbst lieb war, denn natürlich hatte auch er sich unter den gegebenen Umständen gewünscht, dass eine *Colossus* nie hätte gebaut werden müssen.

Die *Colossus* war kein Computer im heutigen Sinne, da sie für die Lösung einer ganz speziellen Aufgabe konzipiert war. Die erste voll funktionsfähige Rechenmaschine, die nahezu allen Definitionen des modernen Computer-Begriffs standhält, war der *Electronic Numerical Integrator and Computer*, kurz ENIAC (Abbildungen 1.10 bis 1.12). Der Rechnerklotz wurde unter der Leitung von J. Presper Eckert und John W. Mauchly an der Moore School of Electrical Engineering der University of Pennsylvania gebaut und im Jahr 1946 der Öffentlichkeit vorgestellt [39, 86]. Die ENIAC beeindruckte bereits aufgrund ihrer Größe. Sie bestand aus insgesamt 30 Einheiten, die U-förmig über eine eigens errichtete Halle verteilt angeordnet waren. Die ca. 18.000 verbauten Vakuumröhren der knapp 30 Tonnen wiegenden Apparatur verursachten eine Leistungsaufnahme von sagenhaften 174.000 Watt.

Intern arbeiten alle Computer im Binärsystem, d. h., jede interne Berechnung lässt sich auf eine Folge von Verknüpfungen der Binärziffern 0 und 1 zurückführen. Formal lassen sich die Vorgänge innerhalb eines Computers mit Hilfe der *Aussagenlogik* beschreiben – einem Teilgebiet der mathematischen Logik, das bereits sehr gut untersucht war, bevor der erste Computer das Konstruktionslabor verließ. Damit wur-



U.S.-Armee-Foto

**Abbildung 1.10:** Teilansicht der ENIAC (linke Raumhälfte)



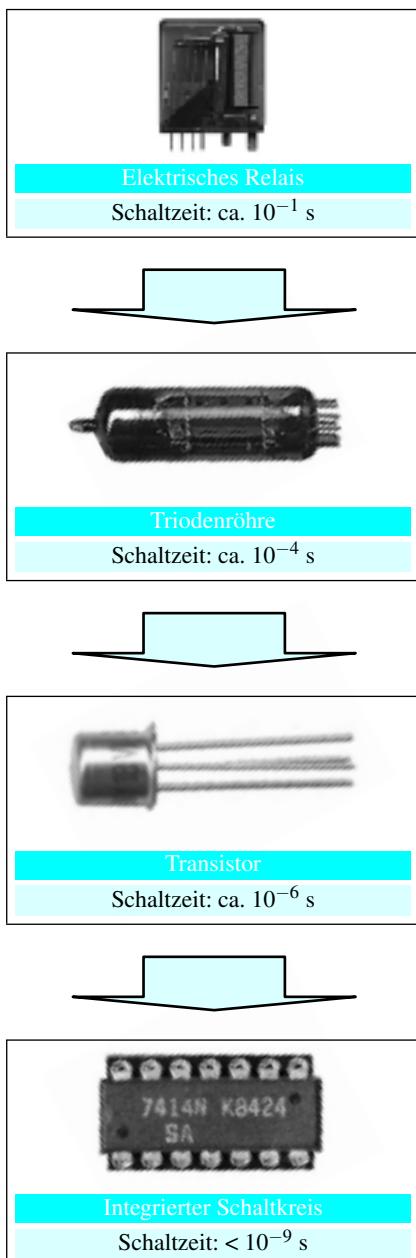
U.S.-Armee-Foto

**Abbildung 1.11:** Teilansicht der ENIAC (rechte Raumhälfte)



U.S.-Armee-Foto

**Abbildung 1.12:** ENIAC-Techniker beim Austausch einer defekten Trioden-Röhre



**Abbildung 1.13:** Von der ersten Rechenmaschine bis zum Supercomputer erlebte die Schaltkreis-Technik drei große Technologiewechsel.

de die mathematische Logik, die zu Beginn des Jahrhunderts die große Krise der Mathematik auslöste, plötzlich zur treibenden Kraft in der rasanten Fortentwicklung der Rechnertechnik. Seither ist die Logik nicht von der Informatik zu trennen. Sie war und ist die formale Grundlage für die Spezifikation, den Entwurf und die Analyse digitaler Hardware-Schaltungen. Kapitel 3 ist vollständig der Logik gewidmet und wird die grundlegende Bedeutung für die moderne Informatik aufzeigen.

Natürlich war es von der ENIAC bis zum modernen Computer noch ein langer Weg. Zur damaligen Zeit waren Rechenanlagen mit Triodenröhren bestückt, die den Entwicklern neben ihrer enormen Leistungsaufnahme vor allem wegen ihrer vergleichsweise geringen Zuverlässigkeit Kopfzerbrechen bereiteten. Erst durch die Erfindung des *Transistors* konnte die Computertechnik in Leistungsbereiche vordringen, die wir heute als selbstverständlich erachten (vgl. Abbildung 1.13). Der erste praxistaugliche Transistor wurde im Jahr 1948 von den Bell Laboratories in New York vorgestellt, allerdings sollten noch ein paar Jahre vergehen, bis er die alte Vakuumröhre vollständig verdrängen konnte. Der erste Computer auf Transistor-Basis wurde an der Manchester University Anfang der Fünfzigerjahre gebaut. Dem 1953 fertiggestellten Prototyp folgte eine deutlich erweiterte Variante, die zwei Jahre später in Betrieb genommen werden konnte.

### 1.2.3 Der Computer wird erwachsen

Der Übergang von der Röhre zum Transistor machte den Weg für die Computer der *zweiten Generation* frei. Die Technologietransition wurde von weiteren wichtigen Entwicklungen begleitet: Steuer- und Rechenwerke nahmen an Komplexität zu und bis dato fortschrittliche Konzepte wie die Verwendung indizierbarer Register oder der Einsatz von Gleitkomma-Hardware gehörten schnell zum Stand der Technik. Ferner hielt der *Ferritkernspeicher* Einzug, der bereits mehrere Kilobyte Daten aufnahm, allerdings in mühevoller Handarbeit gefertigt werden musste.

Die zunehmende Leistungsfähigkeit der konstruierten Computersysteme führte zu einer kontinuierlichen Veränderung in ihrer Bedienung. Wurden die Rechenmaschinen in den Pioniertagen noch direkt auf der Hardware-Ebene programmiert, arbeiteten auf den Computern der zweiten Generation bereits rudimentäre Betriebssysteme. Zeitgleich nahm die Entwicklung von Programmiersprachen an Fahrt auf. 1957 wurde der erste FORTRAN-Compiler ausgeliefert und 1960 die Programmiersprache COBOL verabschiedet. Verschiedene Spezialanwendungen sind auch heute noch in diesen Sprachen programmiert.

Hand in Hand mit der Evolution der Programmiersprachen wuchsen neue Teilbereiche heran, zu denen auch die Theorie der *formalen Sprachen* gehört. Dieser Teilbereich bündelt alle Methoden und Techniken, die sich mit dem Umgang mit künstlichen Sprachkonstrukten beschäftigen. Er stellt das theoretische Grundgerüst zur Verfügung, auf dem der moderne Compilerbau beruht [3].

Die Forschung auf diesem Gebiet wurde insbesondere durch die Arbeiten von Noam Chomsky (Abbildung 1.14) inspiriert, der im Jahre 1957 die *generative Linguistik* begründete [17]. Diese besagt im Kern, dass natürliche Sprachen elementaren Regeln unterliegen, die von uns unbewusst in der Analyse und Konstruktion von Sätzen eingesetzt werden. Auf diese Weise gelang es Chomsky zu erklären, dass wir richtige und falsche Sätze auch dann unterscheiden können, wenn wir sie noch nie in unserem Leben vorher gehört haben. Darauf hinaus führten Chomskys Arbeiten zu dem Ergebnis, dass die von Menschen gesprochenen Sprachen auf der unteren Ebene fast alle den gleichen Regeln unterliegen. Im Zuge seiner Analyse führte er den Begriff der *generativen Grammatik* ein, der kurze Zeit später Einzug in die theoretische Informatik hielt. Auch wenn Chomsky bei seiner Arbeit stets natürliche Sprachen im Sinn hatte, schuf er genau das Begriffsgerüst, das für den systematischen Umgang mit Computersprachen unabdingbar ist. In Kapitel 4 werden wir uns ausführlicher mit der Theorie der formalen Sprachen beschäftigen und die aus Sicht der Informatik wichtigsten Ergebnisse zusammenfassen.

Eng verwandt mit dem Gebiet der formalen Sprachen ist die *Automatentheorie*. In der Informatik beschreibt der Begriff des *endlichen Automaten* ein abstraktes Modell eines Zustandsübergangssystems, das in vielen Aspekten den Turing-Maschinen ähnelt, aber nicht an deren Ausdrucksstärke herankommt. Endliche Automaten stehen in einer engen Beziehung zu den formalen Sprachen, da sich die meisten Sprachklassen in ein äquivalentes Automatenmodell überführen lassen. In diesem Sinne wird der endliche Automat zu einer konkreten Beschreibungsform einer formalen Sprache. Moderne Compiler setzen Software-Implementierungen endlicher Automaten ein, um die Syntax eines Programmtextes zu überprüfen; Textverarbeitungen bedienen sich dieser Methodik, um Suchtexte in großen Texten effizient aufzuspüren.

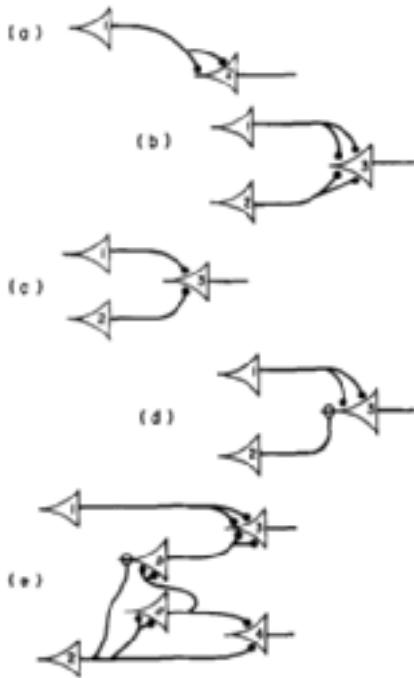
Auch im Bereich des Hardware-Entwurfs spielt der endliche Automat eine zentrale Rolle. So lässt sich jede getaktete Hardware-Schaltung in einen funktional äquivalenten endlichen Automaten übersetzen und auf diese Weise einer formalen Analyse unterziehen. Umgekehrt beschreibt jeder endliche Automat eine Hardware-Schaltung und lässt sich automatisiert in ein *Schaltwerk* transformieren. Neben der Aussagenlo-

„There are two central problems in the descriptive study of language. One primary concern of the linguist is to discover simple and 'revealing' grammars for natural language. At the same time, by studying the properties of such successful grammars are clarifying the basic conceptions that underlie them, he hopes to arrive at a general theory of linguistic structure.“ [16]



Noam Chomsky  
(1928)

**Abbildung 1.14:** Viele Erkenntnisse über formale Sprachen gehen auf die Arbeiten des amerikanischen Linguisten Noam Chomsky zurück. Bereits in den frühen Jahren seiner akademischen Laufbahn suchte Chomsky einen theoretischen Zugang zur Linguistik. Ein Kernelement seiner Herangehensweise war die Verwendung formaler Grammatiken – Meta-Sprachen, die einen rekursiven Aufbau der Sprachausdrücke aus einer Menge von Grundelementen erlauben. Der formale Charakter seiner Methodik machte es erstmals möglich, mathematisch präzise Aussagen über linguistische Sprachen zu treffen. Insbesondere gelang es Chomsky, Sprachen anhand gewisser Eigenschaften ihrer Meta-Sprache in verschiedene Typklassen einzuteilen. Die entstehende *Chomsky-Hierarchie* gehört heute zu den wichtigsten Klassifikationsmerkmalen formaler Sprachen.

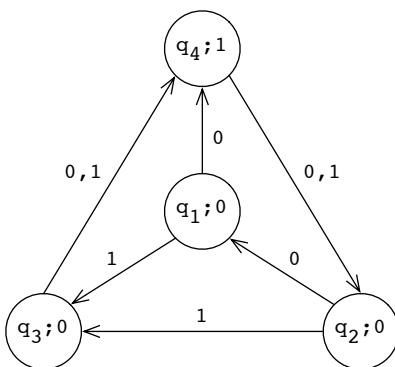


**Abbildung 1.15:** Nervennetze von McCulloch und Pitts [66]

gik ist die Automatentheorie die zweite tragende Säule des gesamten Hardware-Entwurfs. Aufgrund der großen Bedeutung widmet sich Kapitel 5 ausschließlich diesem Teilgebiet der theoretischen Informatik.

Im Gegensatz zu vielen anderen Begriffen der theoretischen Informatik ist die Entstehungsgeschichte des endlichen Automaten nicht an ein einzelnes Ereignis gebunden. Vielmehr haben wir es mit einem Begriff zu tun, der in einem evolutionären Prozess Schritt für Schritt entwickelt wurde. Zu den bemerkenswertesten Vorgängern zählen die *Nervennetze*, die im Jahre 1943 von Warren McCulloch und Walter Pitts zur Untersuchung neuronaler Strukturen eingeführt wurden (vgl. Abbildung 1.15). Die Arbeit ist für die Entwicklung des Automatenbegriffs in zweierlei Hinsicht von Bedeutung. Zum einen finden wir im Neuronenmodell von McCulloch und Pitts bereits viele Konzepte vor, die auch den modernen endlichen Automaten auszeichnen. Zum andere besaß die Arbeit für viele andere Wissenschaftler eine geradezu inspirierende Wirkung. So auch für den US-amerikanischen Mathematiker Stephen Cole Kleene, der das Nervennetz im Jahre 1956 zu einem allgemeinen Zustandsübergangsmodell weiterentwickelte [58]. In diesem Zusammenhang führte Kleene die *regulären Ausdrücke* ein, die bis heute die Standardnotation für die Beschreibung von Suchmustern bilden. Weiterer bedeutende Beiträge zur Automatentheorie wurden nahezu zeitgleich von George H. Mealy und Edward F. Moore publiziert [67, 70]. Aus Moores Arbeit stammt unter anderem das grafische Transitionsmodell, das wir auch heute noch zur Darstellung endlicher Automaten verwenden (vgl. Abbildung 1.16).

Den vielleicht größten Beitrag zur Automatentheorie lieferten Michael Oser Rabin und Dana Scott im Jahre 1959. Unter anderem sorgten sie für eine klare Abgrenzung zwischen endlichen Automaten und Turing-Maschinen. Hierzu wiesen sie nach, dass sich die zahlreichen, im Laufe der Zeit entstandenen Automatenmodelle allesamt aufeinander abbilden lassen und damit eine geringere Ausdrucksstärke besitzen als die Turing-Maschine. Des Weiteren führten sie das Konzept des Nichtdeterminismus ein, mit dem sie eine völlig neue Denkrichtung im Bereich der Berechenbarkeitstheorie schufen. Im Jahre 1976 wurden Rabin und Scott für ihre bedeutende Arbeit mit dem Turing-Award ausgezeichnet (Tabelle 1.1).



**Abbildung 1.16:** Endlicher Automat aus der Originalarbeit von Moore [70]

## 1.2.4 Berechenbarkeit versus Komplexität

Die zunehmende Rechenleistung machte es in der zweiten Hälfte des zwanzigsten Jahrhunderts möglich, auch komplexe Probleme computer-

Jahr	Preisträger	Jahr	Preisträger	Jahr	Preisträger
1966	Alan J. Perlis		Dennis M. Ritchie	2000	Andrew Chi-Chih Yao
1967	Maurice V. Wilkes	1984	Niklaus E. Wirth	2001	Ole-Johan Dahl,
1968	Richard Hamming	1985	Richard M. Karp		Kristen Nygaard
1969	Marvin Minsky	1986	John E. Hopcroft, Robert E. Tarjan	2002	Leonard M. Adleman Ronald L. Rivest,
1970	James H. Wilkinson	1987	John Cocke		Adi Shamir
1971	John McCarthy	1988	Ivan Sutherland	2003	Alan Kay
1972	Edsger W. Dijkstra	1989	William Kahan	2004	Vinton G. Cerf, Robert E. Kahn
1973	Charles W. Bachman	1990	Fernando J. Corbató		Peter Naur
1974	Donald E. Knuth	1991	Robin Milner	2005	Frances E. Allen
1975	Allen Newell, Herbert A. Simon	1992	Butler W. Lampson	2006	Edmund M. Clarke, E. Allen Emerson, Joseph Sifakis
1976	Michael O. Rabin, Dana S. Scott	1993	Juris Hartmanis, Richard E. Stearns		
1977	John Backus	1994	Edward Feigenbaum, Raj Reddy		
1978	Robert W. Floyd	1995	Manuel Blum		
1979	Kenneth E. Iverson	1996	Amir Pnueli		
1980	C. Antony R. Hoare	1997	Douglas Engelbart		
1981	Edgar F. Codd	1998	Jim Gray		
1982	Stephen A. Cook	1999	Frederick P. Brooks, Jr.		
1983	Ken Thompson,				



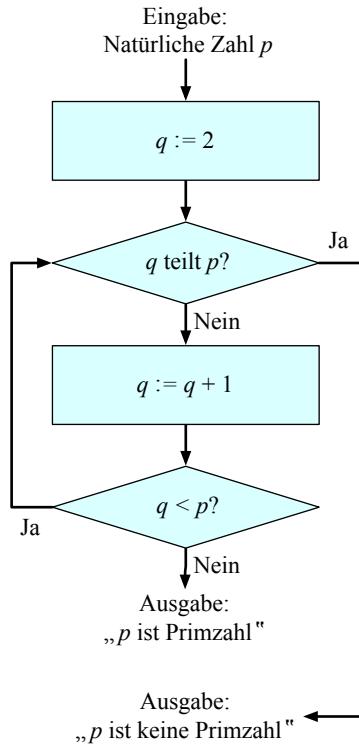
**Tabelle 1.1:** Der Turing-Award existiert seit 1966 und wird seitdem jährlich vergeben. Er ist die höchste Auszeichnung im Bereich der Informatik und hat eine ähnliche Bedeutung wie der Nobelpreis in anderen Wissenschaftsdisziplinen.

gestützt zu bearbeiten. Die Forschung auf dem Gebiet der Algorithmentechnik nahm an Fahrt auf und brachte immer neue Rechenvorschriften hervor, mit denen Probleme aus ganz unterschiedlichen Anwendungsbereichen maschinell gelöst werden konnten. Mit der Fähigkeit, immer größere Eingabemengen verarbeiten zu können, rückten die Laufzeit und der Platzverbrauch eines Programms stärker in das Bewusstsein der Soft- und Hardware-Entwickler. Damit ein Algorithmus für die Lösung praktischer Probleme eingesetzt werden konnte, musste er nicht nur *effektiv* sein, d. h. stets das korrekte Ergebnis berechnen, sondern auch *effizient*. Anders als in den Pioniertagen der theoretischen Informatik, in denen die Berechenbarkeitstheorie zu ihrer vollen Blüte heranreifte, war es nicht mehr länger ausreichend, die prinzipielle Lösbarkeit eines Problems zu zeigen. Eine algorithmische Lösung war faktisch nutzlos, wenn ein Computer mehrere Jahre oder Jahrzehnte für ihre Ausführung benötigte.

■ Problem



■ Algorithmus



**Abbildung 1.17:** Das Problem PRIME lässt sich auf einfache Weise lösen, indem wir die Eingabe  $p$  nacheinander durch alle Zahlen  $q$  mit  $2 \leq q < p$  teilen. Geht die Division niemals ohne Rest auf, so ist  $p$  eine Primzahl. Während das Programm für kleine Zahlen praktikabel arbeitet, nimmt die Rechenzeit für größere Werte von  $p$  drastisch zu. Kurzum: Der abgebildete Algorithmus ist effektiv, aber nicht effizient.

Die praktische Verwertbarkeit von Algorithmen lenkte die Aufmerksamkeit der Wissenschaftsgemeinde langsam, aber sicher von der Berechenbarkeitstheorie weg und hin zur Komplexitätstheorie. Die Grundlagen für die Untersuchung der Laufzeit- und Platzkomplexität von Algorithmen wurden in den Sechzigerjahren geschaffen [21, 27] und nachhaltig durch die Arbeit von Juris Hartmanis und Richard Stearns aus dem Jahre 1965 beeinflusst [41]. Mit ihren mathematisch präzisen Komplexitätsuntersuchungen von Turing-Maschinen legten die beiden US-amerikanischen Computerwissenschaftler den Grundstein für die formale Komplexitätstheorie, wie wir sie heute kennen.

Eine kleine Auswahl konkreter Beispiele soll verdeutlichen, mit welchen Fragestellungen sich dieser Zweig der theoretischen Informatik im Kern befasst. Als Erstes betrachten wir mit PRIME ein Problem der Zahlentheorie, das Mathematiker seit tausenden von Jahren beschäftigt. Für eine beliebige natürliche Zahl  $p$  gilt es zu entscheiden, ob es sich um eine Primzahl handelt oder nicht. Dass PRIME lösbar ist, liegt auf der Hand, schließlich können wir die Zahl  $p$  als Primzahl identifizieren, indem wir  $p$  nacheinander durch alle potenziellen Faktoren dividieren. Abbildung 1.17 fasst die Vorgehensweise in einem Flussdiagramm zusammen. Obwohl der konstruierte Algorithmus für alle Eingabewerte die korrekte Antwort liefert, nimmt die Rechenzeit für größere Eingabewerte dramatisch zu. Bezeichnet  $n$  die Anzahl der Bits in der Binärdarstellung von  $p$ , so müssen im schlimmsten Fall  $2^n$  Divisionen berechnet werden, bis der Algorithmus terminiert. Selbst wenn wir eine Billion Einzeldivisionen pro Sekunde ausführen könnten, stünde das Ergebnis für eine 128-Bit-Binärzahl erst nach ca.  $10^{19}$  Jahren fest. Wir müssten damit länger auf die Antwort warten, als unser Universum jemals existieren wird.

Als Nächstes wenden wir uns mit SAT einem Problem der Aussagenlogik zu (vgl. Abschnitt 3.2). Konkret geht es um die Frage, ob wir die Variablen einer aussagenlogischen Formel  $F$  so mit den Wahrheitswerten 1 (wahr) und 0 (falsch) belegen können, dass  $F$  wahr wird. Eine Formel mit dieser Eigenschaft heißt *erfüllbar (satisfiable)*.

Genau wie PRIME lässt sich auch SAT verblüffend einfach lösen. Da eine Formel  $F$  nur endlich viele aussagenlogische Variablen enthält und diese ausschließlich die Werte 1 oder 0 annehmen können, ist die Anzahl der möglichen Variablenbelegungen endlich. Somit können wir die Erfüllbarkeit einer Formel  $F$  entscheiden, indem wir alle Belegungskombinationen der Reihe nach durchprobieren (vgl. Abbildung 1.18). Genau dann, wenn wir eine Kombination finden, für die  $F$  den Wahrheitswert 1 annimmt ( $F \equiv 1$ ), erfährt der Erfüllbarkeitstest eine positive Antwort. Wie schon im Falle von PRIME ist der gefundene Algorith-

mus effektiv, aber nicht effizient. Bezeichnet  $n$  die Anzahl der aussagenlogischen Variablen in  $F$ , so müssen im schlimmsten Fall alle  $2^n$  Wertekombinationen betrachtet werden, um eine zuverlässige Aussage über die Erfüllbarkeit von  $F$  zu treffen.

Das Problem SAT spielt in der theoretischen Informatik eine weit größere Rolle, als es der ein oder andere Leser an dieser Stelle vermuten mag. In Abschnitt 7.3.3 werden wir zeigen, dass viele Algorithmen auf das Erfüllbarkeitsproblem reduziert werden können, indem der Programmablauf in eine aussagenlogische Formel hineincodiert wird. In diesem Sinne wird sich SAT als Universalproblem erweisen, aus dem sich viele Ergebnisse der modernen Komplexitätstheorie direkt ableiten lassen.

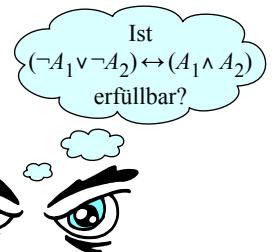
Obwohl die gesamte theoretische Informatik in der zweiten Hälfte des zwanzigsten Jahrhunderts durch die Erkenntnis geprägt war, dass ein praktisch verwertbarer Algorithmus nicht nur effektiv, sondern auch effizient arbeiten muss, waren die Fortschritte auf dem Gebiet der Algorithmentechnik unterschiedlicher Natur. Einige Probleme konnten mit Algorithmen gelöst werden, die auch für große Eingabelängen sehr schnell zu einem Ergebnis führten, andere widersetzen sich vehement einer effizienten Lösung. Es schien, als ob die untersuchten Problemstellungen individuelle Schwierigkeitsgrade besäßen, die selbst mit den größten Anstrengungen nicht umgangen werden konnten.

Wissenschaftler reagierten mit der Definition von *Komplexitätsklassen*, in die sich die untersuchten Problemstellungen anhand ihrer bisher bekannten Lösungsstrategien einordnen ließen. Die weiter oben eingeführten Algorithmen zur Lösung von PRIME und SAT sind sogenannte *Exponentialzeitalgorithmen*, da ihre Rechenzeit exponentiell mit dem Größenparameter  $n$  ansteigt. Probleme, für die ausschließlich Exponentialzeitalgorithmen bekannt sind, gelten in der Praxis als unlösbar.

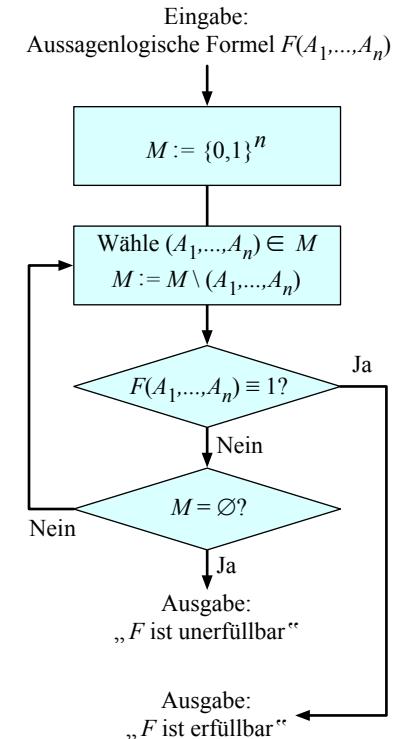
Eine ungleich größere Bedeutung besitzen die *Polynomialzeitalgorithmen*, deren Rechenzeit durch ein Polynom  $p(n)$  nach oben begrenzt ist. Da Polynome für steigende Werte von  $n$  deutlich langsamer gegen unendlich streben als Exponentielfunktionen, setzen viele Experten die Existenz eines Polynomialzeitalgorithmus mit der praktischen Lösbarkeit eines Problems gleich.

Welche Komplexität sich hinter einem spezifischen Problem verbirgt, ist diesem nicht unmittelbar anzusehen und bereits kleine Veränderungen der Fragestellung können zu einer schlagartigen Änderung der Problemkomplexität führen. Wir wollen dieses Phänomen am Beispiel des Königsberger Brückenproblems ergründen, das sich mit der Frage beschäftigt, ob in einem gegebenen Graph  $G$  ein *Euler-Kreis* existiert.

#### ■ Problem

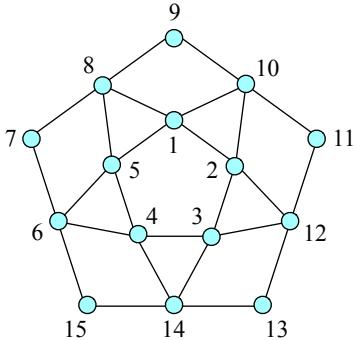


#### ■ Algorithmus

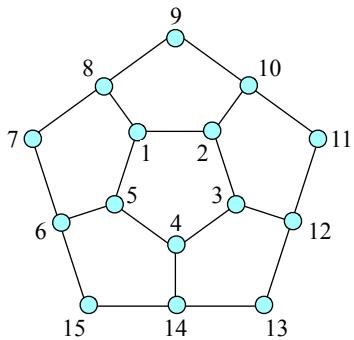


**Abbildung 1.18:** Das Problem SAT lässt sich lösen, indem der Funktionswert von  $F$  nacheinander für sämtliche Variablenbelegungen ausgerechnet wird. Da die Anzahl der Belegungen exponentiell mit der Anzahl der Variablen zunimmt, bleibt die praktische Anwendung dieser Methode auf Formeln mit wenigen Variablen beschränkt. Genau wie im Falle von PRIME ist der Algorithmus effektiv, aber nicht effizient.

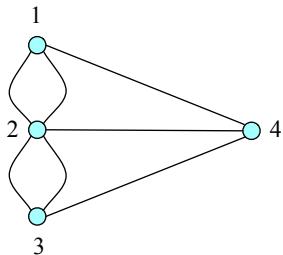
## ■ Graph 1



## ■ Graph 2



## ■ Graph 3



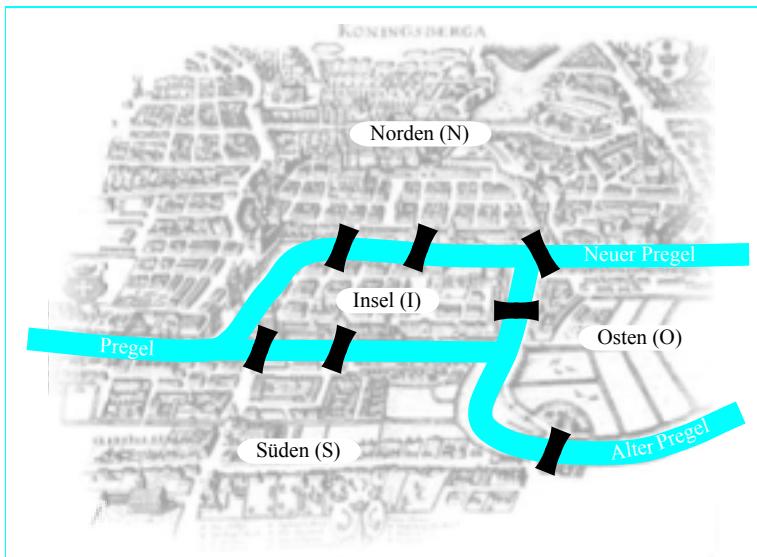
**Abbildung 1.19:** Hinter dem Königsberger Brückenproblem versteckt sich eine elementare Graph-Eigenschaft, die sich anhand des Euler-Kriteriums effizient nachweisen lässt. Von den dargestellten Graphen erfüllt nur der erste das Euler-Kriterium.

Plakativ gesprochen liegt ein solcher genau dann vor, wenn wir  $G$  auf einem Rundweg so durchlaufen können, dass alle Kanten genau einmal besucht werden. 1736 bewies der Schweizer Mathematiker Leonhard Euler, dass ein solcher Kreis genau dann existiert, wenn jeder Knoten eine gerade Anzahl ausgehender Kanten besitzt [7, 29].

Damit können wir das Problem für einen beliebigen Graphen mit  $n$  Knoten in linearer Zeit lösen, indem wir nacheinander die Anzahl der ausgehenden Kanten bestimmen. Genau dann, wenn wir in einem der Knoten eine ungerade Anzahl vorfinden, ist die Antwort negativ; einen Euler-Kreis kann es in diesem Fall nicht geben. Abbildung 1.19 demonstriert das Vorgehen anhand zweier Beispielgraphen, von denen nur der erste das Euler-Kriterium erfüllt. In den anderen Graphen existiert kein Euler-Kreis, da gleich mehrere Knoten eine ungerade Anzahl ausgehender Kanten aufweisen.

Euler motivierte seine Ergebnisse, indem er auf die besondere geografische Lage der Stadt Kaliningrad, das frühere Königsberg, zurückgriff. Die ehemalige Hauptstadt Ostpreußens wird durch den Fluss Pregel in vier Gebiete unterteilt, die zu Eulers Zeiten über 7 Brücken miteinander verbunden waren (vgl. Abbildung 1.20). Euler konnte mit Hilfe seiner Untersuchungen beweisen, dass es unmöglich war, Königsberg auf einem Rundweg zu erkunden, der jede Brücke exakt einmal besucht. Hierzu brauchte er nichts weiter zu tun, als die Kartentopologie in einen Graphen zu übersetzen, in dem jedes Stadtgebiet einem Knoten und jede Brücke einer Kante entspricht. Den entstehenden Graphen haben wir bereits kennen gelernt: Er ist mit dem dritten Beispiel aus Abbildung 1.19 identisch. Da dieser Graph keinen Euler-Kreis besitzt, kann es im ehemaligen Königsberg keinen entsprechenden Rundgang geben.

Für die Komplexitätstheorie ist das Königsberger Brückenproblem von großer Bedeutung, da eine geringfügige Abwandlung ein faktisch unlösbares Problem entstehen lässt. Es wurde im Jahre 1859 von Sir William Hamilton formuliert und ist dem Königsberger Brückenproblem zum Verwechseln ähnlich. Für einen gegebenen Graphen  $G$  ist zu entscheiden, ob wir diesen auf einem Rundweg so durchlaufen können, dass alle Knoten genau einmal besucht werden. Einen Weg mit dieser Eigenschaft bezeichnen wir als *Hamilton-Kreis*. Bezogen auf die Stadt-karte von Königsberg lautet das Hamilton-Problem wie folgt: Gibt es einen Rundweg durch die Stadt, so dass kein Stadtteil zweimal betreten wird? In unserem konkreten Beispiel reicht ein gezielter Blick, um einen Hamilton-Kreis zu erkennen. Starten wir beispielsweise im Norden, so gelangen wir über die Pregel-Insel in den südlichen Stadtteil. Anschließend können wir über den östlichen Teil in den Norden zurückkehren, ohne die Insel erneut zu betreten.



**Abbildung 1.20:** Im achtzehnten Jahrhundert wurde die Stadt Königsberg durch den Fluss Pregel in vier Gebiete aufgeteilt, die durch sieben Brücken miteinander verbunden waren. Bekannt wurde das Stadtbild durch den Schweizer Mathematiker Leonhard Euler, der es zur Veranschaulichung eines von ihm gelösten Graphenproblems benutzte. Er motivierte seine Arbeit mit der Frage, ob Königsberg auf einem Rundweg erkundet werden kann, auf dem jede Brücke genau einmal überquert wird. Im Jahre 1736 bewies er, dass ein solcher Weg nicht existiert. Mit seinen Untersuchungen begründete Euler die Graphentheorie, die heute sowohl in der theoretischen als auch in der praktischen Informatik ihren festen Platz eingenommen hat.

Obwohl die Lösung des Hamilton-Problems für kleine Graphen wie eine Fingerübung wirkt, ist es noch niemandem gelungen, einen deterministischen Polynomialzeitalgorithmus dafür zu formulieren. Ob ein solcher Algorithmus überhaupt existieren kann, ist gegenwärtig unbekannt. Um es vorwegzunehmen: Die Chancen, dass sich das Hamilton-Problem auf realen Rechenanlagen in Polynomialzeit lösen lässt, stehen aus heutiger Sicht nicht allzu gut, da es in die Klasse der *NP-vollständigen* Probleme fällt.

Die Klasse der NP-vollständigen Probleme ist eine Teilmenge der Klasse NP. Probleme aus NP zeichnen sich dadurch aus, dass eine potenzielle Lösung sehr einfach auf Korrektheit geprüft werden kann, das Finden derselben jedoch ungleich schwerer ist. Am Beispiel des Hamilton-Problems lässt sich diese Eigenschaft besonders gut beobachten. Ist eine Sequenz von Knoten vorgegeben, so können wir leicht feststellen, ob diese einen Hamilton-Kreis beschreibt. Die Berechnung der Knotensequenz gestaltet sich dagegen deutlich komplexer. Die Teilmenge der NP-vollständigen Probleme vereint alle Elemente aus NP, die mächtig genug sind, um damit alle anderen NP-Probleme ebenfalls zu lösen. Sie gehören damit zu den schwersten Problemen überhaupt und eine effiziente Lösung eines einzigen NP-vollständigen Problems würde die effiziente Lösbarkeit aller anderen Probleme aus NP nach sich ziehen.

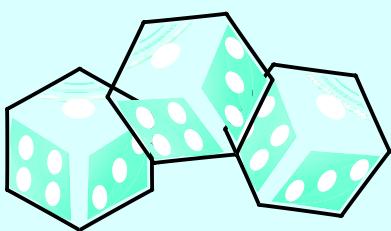
Für diesen Moment soll uns diese vage Beschreibung des Vollständigkeitsbegriffs genügen. Eine genaue Definition werden wir in Kapitel 7

Die Rechenzeit eines Exponentialzeitalgorithmus nimmt so schnell zu, dass seine Praxistauglichkeit deutlich eingeschränkt ist. Um größere Eingaben verarbeiten zu können, wurden für viele Probleme *randomisierte Algorithmen* entwickelt. Diese verfolgen die Grundidee, eine gewünschte Eigenschaft nicht für *alle*, sondern nur für die *meisten* Eingaben zu garantieren. Auf diese Weise entstehen Algorithmen, die aus theoretischer Sicht Lücken aufweisen, in der Praxis aber gute Ergebnisse liefern. Randomisierte Algorithmen lassen sich in zwei Klassen einteilen:

*Las-Vegas-Algorithmen* berechnen immer das korrekte Ergebnis, konsumieren für vereinzelte Eingaben jedoch überproportional viel Rechenzeit. In diese Gruppe fällt der bekannte Sorteralgorithmus Quicksort. Im statistischen Mittel benötigt dieser  $n \cdot \log n$  Operationen, um eine Liste mit  $n$  Elementen zu sortieren. Bei einer ungünstigen Werteverteilung steigt die Laufzeit dagegen quadratisch mit der Anzahl der zu sortierenden Elementen an.

*Monte-Carlo-Algorithmen* garantieren für alle Eingaben die gleiche Laufzeitkomplexität, liefern dafür in manchen Fällen eine falsche Antwort. Mit dem Primzahltest von Robert Solovay und Volker Strassen enthält diese Klasse einen Algorithmus, der vor allem im Zusammenhang mit RSA-Kryptosystemen einen hohen Bekanntheitsgrad erreichte [85].

Der Primzahltest ist deutlich schneller als alle nicht-randomisierten Verfahren, in einzelnen Fällen werden jedoch auch faktorisierbare Zahlen als Primzahl klassifiziert.



nachholen, sobald das zum Verständnis notwendige Begriffsgerüst geschaffen wurde. So viel vorweg: Ob überhaupt ein NP-vollständiges Problem existiert, war lange Zeit unbekannt. Erst im Jahre 1971 gelang Stephen Cook und Leonid Levin unabhängig voneinander der Nachweis, dass das weiter oben skizzierte SAT-Problem NP-vollständig ist [24, 63, 64].

Ein Jahr später wies Richard Karp die NP-Vollständigkeit von 20 weiteren Problemen nach [52] und das im Jahre 1979 publizierte Buch von Michael Garey und David Johnson enthält bereits eine Zusammenfassung von ca. 300 NP-vollständigen Problemen. Können wir für nur ein einziges einen Polynomialzeitalgorithmus konstruieren, so sind alle anderen NP-vollständigen Probleme auf einen Schlag ebenfalls in Polynomialzeit lösbar. Damit steht fest: Sollte ein solcher Algorithmus tatsächlich irgendwann gefunden werden, wären seine Auswirkungen bis in alle Teilbereiche der Informatik hinein spürbar.

Die steigende Anzahl gefundener Probleme, die sich vehement einer effizienten Lösbarkeit entziehen, nährt jedoch in vielen Experten die Vermutung, dass es unmöglich ist, einen Polynomialzeitalgorithmus für ein NP-vollständiges Problem zu finden. Ein mathematischer Beweis dafür steht aber bis heute aus und wir dürfen gespannt sein, was die zukünftige Forschung in diesem Bereich an Überraschungen hervorbringen wird.

## 1.3 Theoretische Informatik heute

Die theoretische Informatik gehört zu den wenigen Teilgebieten der Informationswissenschaft, die über einen gefestigten Stoffumfang verfügen. Insbesondere im Vergleich mit der sich kontinuierlich wandelnden Software-Technik wirken die Erkenntnisse und Methoden überaus stabil. Trotzdem handelt es sich bei der theoretischen Informatik keinesfalls um einen abgeschlossenen Wissenschaftszweig und viele Problemstellungen sind nach wie vor ungelöst.

Eine davon ist die endgültige Klärung der weiter oben diskutierten Frage, ob sich NP-vollständige Probleme auf realen Rechenanlagen in Polynomialzeit lösen lassen. Dieses *P-NP-Problem* ist von so großer Bedeutung, dass es in die Riege der *7 Millennium-Probleme* aufgenommen wurde (Abbildung 1.21). Diese wurden am 24. Mai 2000 in Paris vorgestellt; in derselben Stadt, in der David Hilbert hundert Jahre zuvor in seiner historischen Rede die 23 dringlichsten Probleme der Mathematik formulierte. Die Forschung auf diesem Gebiet ist durchaus attraktiv.

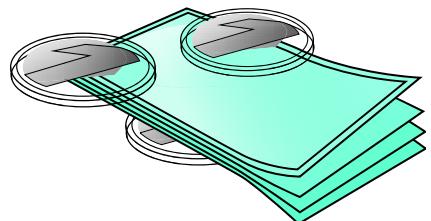
Für jedes der 7 Millennium-Probleme hat das in Cambridge beheimatete Clay Mathematics Institute (CMI) ein Preisgeld von einer Million US-Dollar ausgelobt.

Wie auch immer die Antwort auf das P-NP-Problem lauten wird: Die Folgen sind nicht nur positiver Natur. Gelingt es, die heute mehrheitlich gehegte Vermutung zu bestätigen, dass sich NP-vollständige Probleme nicht in Polynomialzeit lösen lassen, so wäre die Existenz theoretisch beantwortbarer, aber praktisch unlösbarer Fragestellungen gesichert. Wir wüssten dann, dass Probleme wie das Hamilton'sche niemals effizient gelöst werden können. Doch auch die gegenteilige Antwort würde uns Kopfzerbrechen bereiten, da sich viele sicherheitskritische Algorithmen auf die praktische Unlösbarkeit NP-vollständiger Probleme stützen. Sollten wir jemals in der Lage sein, auch nur eine einzige NP-vollständige Fragestellung in Polynomialzeit zu beantworten, so ließen sich neben dem Hamilton-Problem auch Algorithmen aus dem Gebiet der Kryptographie effizient lösen. Die im Internetzeitalter so unabdingbar gewordene Verschlüsselung stände mit einem Schlag auf wackligen Füßen.

Wie Sie sehen, ist die theoretische Informatik weit mehr als mathematische Spielerei. Sie besitzt weitreichende Konsequenzen, die sich in alle Bereiche der Informatik auswirken. Dass die theoretische Informatik keine tote Wissenschaft ist, wird durch Ergebnisse der jüngsten Zeit untermauert. Eines davon bezieht sich auf das weiter oben eingeführte Problem PRIME, also auf die Frage, ob es sich bei einer gegebenen Zahl  $p$  um eine Primzahl handelt oder nicht. Obwohl Primzahlen seit tausenden von Jahren intensiv untersucht werden, wurde die Komplexität von PRIME erst im Jahr 2002 vollständig geklärt. In diesem Jahr gelang es den indischen Computerwissenschaftlern Manindra Agrawal, Neeraj Kayal und Nitin Saxena, einen polynomiellen Algorithmus für PRIME zu konstruieren [2]. Der AKS-Algorithmus erzeugte ein Echo weit über die Wissenschaftsgemeinde hinaus. Sogar die New York Times publizierte einen Artikel über die „New Method Said to Solve Key Problem in Math“ [79].

Die Arbeit von Agrawal, Kayal und Saxena ist aus zweierlei Gründen von Bedeutung. Zum einen zeigt sie, dass wir mit unseren Vermutungen oft falsch liegen. Viele Wissenschaftler waren vor 2002 der Überzeugung, dass für das Problem PRIME kein Polynomialzeitalgorithmus existiert. Zum anderen demonstriert sie, wie groß unsere Wissenslücken im Fundament der Informatik noch immer sind. Die Ansicht, wir hätten es hier mit einer vollständig untersuchten, in sich abgeschlossenen Wissenschaft zu tun, trügt. Ganz im Gegenteil: Die theoretische Informatik lebt!

*„Suppose that you are organizing housing accommodations for a group of four hundred university students. Space is limited and only one hundred of the students will receive places in the dormitory. To complicate matters, the Dean has provided you with a list of pairs of incompatible students, and requested that no pair from this list appear in your final choice. This is an example of what computer scientists call an NP-problem, since it is easy to check if a given choice of one hundred students proposed by a coworker is satisfactory (i.e., no pair taken from your coworker's list also appears on the list from the Dean's office), however the task of generating such a list from scratch seems to be so hard as to be completely impractical. [...] This apparent difficulty may only reflect the lack of ingenuity of your programmer. In fact, one of the outstanding problems in computer science is determining whether questions exist whose answer can be quickly checked, but which require an impossibly long time to solve by any direct procedure. Problems like the one listed above certainly seem to be of this kind, but so far no one has managed to prove that any of them really are so hard as they appear; i.e., that there really is no feasible way to generate an answer with the help of a computer. [...]“*



**Abbildung 1.21:** Für die endgültige Klärung des P-NP-Problems lobte das Clay Mathematics Institute im Jahre 2000 ein Preisgeld von einer Million US-Dollar aus.



In diesem Kapitel haben Sie erfahren, wie der Logizismus die Mathematik zu Beginn des zwanzigsten Jahrhunderts verändert hat. Die zuvor physikalisch geprägte Mathematik wurde durch *formale Systeme* verdrängt, die sich aus *Axiomen* und *Regeln* zusammensetzen. Ein Theorem ist bewiesen, wenn es sich durch die Anwendung einer endlichen Folge von Regelanwendungen aus den Axiomen herleiten lässt. In einem solchen *Kalkül* wird das Führen eines mathematischen Beweises zu einem mechanischen Prozess.

Um das Gesagte mit Leben zu füllen, wollen wir ein konkretes formales System betrachten. Es stammt aus Douglas Hofstadters Meisterwerk *Gödel, Escher, Bach* und gibt einen erstklassigen Eindruck von der Grundidee des logischen Schließens [49]:

**Aufgabe 1.4**  
  
**Webcode**  
**1904**

- Axiome
  - 1. **MI** ist ein Satz
- Schlussregeln
  - 1. Mit **xI** ist auch **xIU** ein Satz
  - 2. Mit **Mx** ist auch **Mxx** ein Satz
  - 3. In jedem Satz darf **III** durch **U** ersetzt werden
  - 4. In jedem Satz darf **UU** entfernt werden

In dem soeben definierten *MIU-System* lässt sich z. B. der Satz **MUIIU** wie folgt beweisen:

<b>MI</b>	(Axiom)
→ <b>MI</b>	(Regel 2)
→ <b>MIII</b>	(Regel 2)
→ <b>MUI</b>	(Regel 3)
→ <b>MUIU</b>	(Regel 1)
→ <b>MUIUUI</b>	(Regel 2)
→ <b>MUIIU</b>	(Regel 4)

- a) Lassen sich die Sätze **MIU** und **MIIIIU** innerhalb des Kalküls ableiten?
- b) Ist die Reihenfolge der angewendeten Regeln immer eindeutig bestimmt?
- c) Versuchen Sie zu ermitteln, ob sich der Satz **MU** aus den Axiomen ableiten lässt. Konstruieren Sie einen Beweis in Form einer konkreten Ableitungssequenz oder begründen Sie, warum ein solcher Beweis nicht existieren kann.



## 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. Er gilt als der Begründer der 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 Jahre 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 abzutrennen.

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 Sinne 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 also 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. Wie die folgenden Beispiele demonstrieren, können auch unendliche Mengen aufzählend (enumerativ) beschrieben werden, wenn die Elemente einer unmittelbar einsichtigen Regelmäßigkeit unterliegen.

$$\mathbb{N} = \{1, 2, 3, 4, \dots\} \quad (2.1)$$

$$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\} \quad (2.2)$$

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \quad (2.3)$$

$$M_1 = \{2, 4, 6, 8, 10, \dots\} \quad (2.4)$$

$$M_2 = \{0, 1, 4, 9, 16, 25, \dots\} \quad (2.5)$$

$\mathbb{N}$  heißt die Menge der *natürlichen Zahlen* oder die Menge der *positiven ganzen Zahlen*.  $\mathbb{N}_0$  enthält zusätzlich die Zahl null und wird die Menge der *nichtnegativen 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.

$$M_3 := \{n \in \mathbb{N} \mid n \bmod 2 = 0\} \quad (2.6)$$

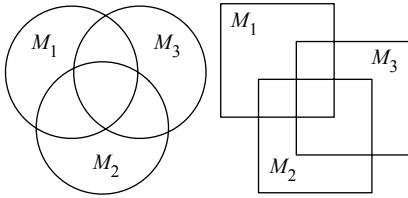
$$M_4 := \{n^2 \mid n \in \mathbb{N}_0\} \quad (2.7)$$

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 nichtnegativen Zahlen  $n \in \mathbb{N}_0$ . 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 mit Hilfe 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 Jahre 1907 ein entsprechendes Axiomensystem formulierte. Die *Zermelo-Mengenlehre* bestand aus insgesamt 7 Axiomen, die noch umgangssprachlich formuliert waren [102]. Das System wurde 1921 von Abraham Fraenkel um das Ersetzungssaxiom und 1930 von Zermelo um das Fundierungssaxiom ergänzt [31, 103]. Die 9 Axiome bilden zusammen die *Zermelo-Fraenkel-Mengenlehre*, kurz ZF, wie sie heute in weiten Teilen der Mathematik Verwendung findet.

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 [36]. 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.



**Abbildung 2.2:** *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.

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

$$M_1 \subseteq M_2 : \Leftrightarrow \text{Aus } a \in M_1 \text{ folgt } a \in M_2 \quad (2.8)$$

$$M_1 \supseteq M_2 : \Leftrightarrow M_2 \subseteq M_1 \quad (2.9)$$

Beachten Sie, dass die Teilmengenbeziehung nach dieser Definition immer auch dann gilt, wenn  $M$  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  $M \supseteq M$ .

Mit Hilfe der eingeführten Operatoren können wir die Mengengleichheit wie folgt charakterisieren:

$$M_1 = M_2 \Leftrightarrow M_1 \subseteq M_2 \text{ und } M_2 \subseteq M_1 \quad (2.10)$$

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

$$M_1 \subset M_2 : \Leftrightarrow M_1 \subseteq M_2 \text{ und } M_1 \neq M_2 \quad (2.11)$$

$$M_1 \supset M_2 : \Leftrightarrow M_1 \supseteq M_2 \text{ und } M_1 \neq M_2 \quad (2.12)$$

Offensichtlich gilt für die weiter oben eingeführten Mengen die Beziehung  $M_1 \subset \mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z}$ . Dagegen gilt weder  $M_1 \subset M_2$  noch  $M_2 \subset M_1$ .



Viergliedriges  
Venn-Diagramm  
aus der Original-  
arbeit von 1881



John Venn (1834 – 1923)

**Abbildung 2.3:** Das Venn-Diagramm wurde im Jahre 1881 durch den britischen Logiker und Philosophen John Venn eingeführt [93, 94]. Es bildet heute die am häufigsten eingesetzte Darstellungsform für die bildliche Repräsentation einer Menge.

## 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:

$$M_1 \cup M_2 := \{a \mid a \in M_1 \text{ oder } a \in M_2\} \quad (2.13)$$

$$M_1 \cap M_2 := \{a \mid a \in M_1 \text{ und } a \in M_2\} \quad (2.14)$$

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

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

$$\bigcup_{i=1}^n M_i := M_1 \cup \dots \cup M_n \quad \text{bzw.} \quad \bigcup_{i=1}^{\infty} M_i := M_1 \cup M_2 \cup \dots \quad (2.15)$$

$$\bigcap_{i=1}^n M_i := M_1 \cap \dots \cap M_n \quad \text{bzw.} \quad \bigcap_{i=1}^{\infty} M_i := M_1 \cap M_2 \cap \dots \quad (2.16)$$

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

$$M_1 \setminus M_2 := \{a \mid a \in M_1 \text{ und } a \notin M_2\} \quad (2.17)$$

$$\overline{M} := T \setminus M \quad (2.18)$$

Viele Mengenbeziehungen lassen sich intuitiv mit Hilfe 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 2.2 bis 2.4).

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

$$M_1 \cup M_2 = M_2 \cup M_1 \quad (2.19)$$

$$M_1 \cap M_2 = M_2 \cap M_1 \quad (2.20)$$

#### ■ Distributivgesetze

$$M_1 \cup (M_2 \cap M_3) = (M_1 \cup M_2) \cap (M_1 \cup M_3) \quad (2.21)$$

$$M_1 \cap (M_2 \cup M_3) = (M_1 \cap M_2) \cup (M_1 \cap M_3) \quad (2.22)$$

#### ■ Neutrale Elemente

$$M \cup \emptyset = M \quad (2.23)$$

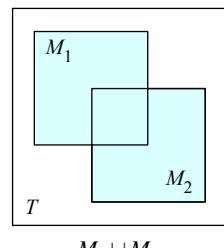
$$M \cap T = M \quad (2.24)$$

#### ■ Inverse Elemente

$$M \cup \overline{M} = T \quad (2.25)$$

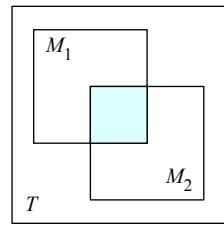
$$M \cap \overline{M} = \emptyset \quad (2.26)$$

#### ■ Vereinigung



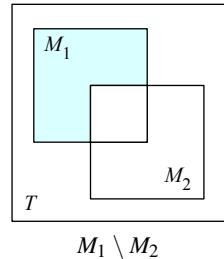
$$M_1 \cup M_2$$

#### ■ Schnitt



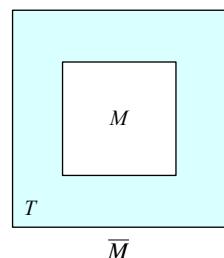
$$M_1 \cap M_2$$

#### ■ Differenz



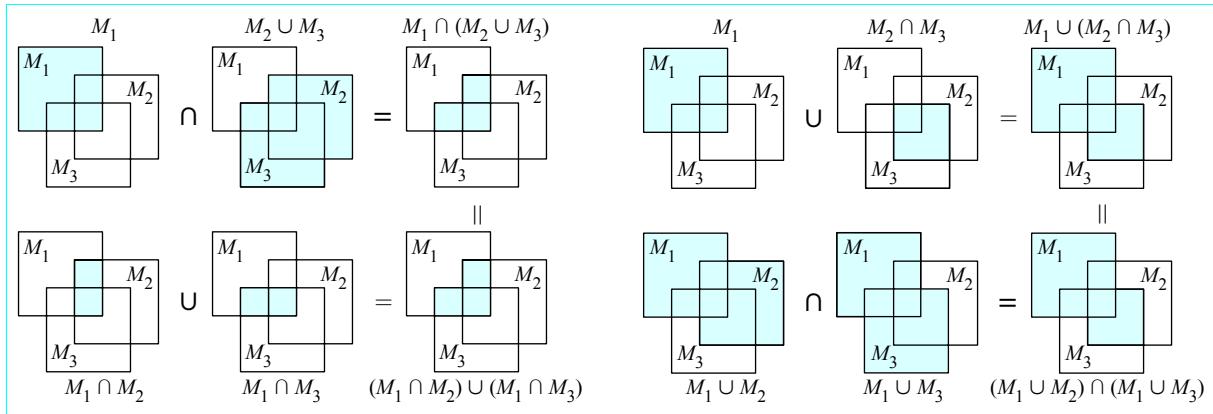
$$M_1 \setminus M_2$$

#### ■ Komplement



$$\overline{M}$$

**Abbildung 2.4:** Elementare Mengenoperationen



**Abbildung 2.5:** 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 2.5 liefern eine grafische Begründung für diese Regeln.

Die Mengenalgebra ist ein Spezialfall einer *booleschen Algebra* (Abbildung 2.6) [48]. Damit übertragen sich alle Gesetzmäßigkeiten, die in einer booleschen Algebra gelten, in direkter Weise auf die Mengenalgebra. Hierunter fallen insbesondere die folgenden Verknüpfungsregeln:



George Boole (1815 – 1864)

**Abbildung 2.6:** Der britische Mathematiker und Philosoph George Boole zählt zu den einflussreichsten Logikern des neunzehnten Jahrhunderts. Mit seinem aus heutiger Sicht 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.

#### ■ Assoziativgesetze

$$M_1 \cup (M_2 \cup M_3) = (M_1 \cup M_2) \cup M_3 \quad (2.27)$$

$$M_1 \cap (M_2 \cap M_3) = (M_1 \cap M_2) \cap M_3 \quad (2.28)$$

#### ■ Idempotenzgesetze

$$M \cup M = M \quad (2.29)$$

$$M \cap M = M \quad (2.30)$$

#### ■ Absorptionsgesetze

$$M_1 \cup (M_1 \cap M_2) = M_1 \quad (2.31)$$

$$M_1 \cap (M_1 \cup M_2) = M_1 \quad (2.32)$$

#### ■ Gesetze von De Morgan (Abbildung 2.7)

$$\overline{M_1 \cup M_2} = \overline{M_1} \cap \overline{M_2} \quad (2.33)$$

$$\overline{M_1 \cap M_2} = \overline{M_1} \cup \overline{M_2} \quad (2.34)$$

■ Auslöschungsgesetze

$$M \cup T = T \quad (2.35)$$

$$M \cap \emptyset = \emptyset \quad (2.36)$$

■ Gesetz der Doppelnegation

$$\overline{\overline{M}} = M \quad (2.37)$$

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:

$$2^M := \{M' \mid M' \subseteq M\} \quad (2.38)$$

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 2.8).

## 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  $\not\sim_R y$ . Die eingeführte Notation mag den Anschein erwecken, dass wir mit dem Relationenbegriff ein neues mathematisches Konzept einführen. Die folgenden Definitionen machen jedoch deutlich, dass sich die Relationentheorie vollständig auf dem Grundgerüst der Mengenlehre errichten lässt:



### Definition 2.2 (Kartesisches Produkt)

Sei  $M$  eine beliebige Menge. Die Menge

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

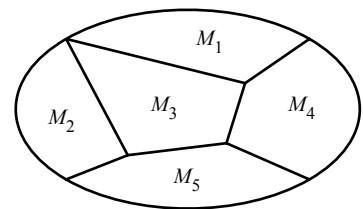
nennen wir das *kartesische Produkt* von  $M$ .

„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 2.7:** Die Gesetze von De Morgan sind nach dem britischen Mathematiker Augustus De Morgan benannt. Neben George Boole gilt er als einer der bedeutendsten Mitbegründer der mathematischen Logik. De Morgans Werk geht jedoch weit über den Bereich der formalen Logik hinaus. So wurde z. B. auch der Begriff der *vollständigen Induktion* (Abschnitt 2.4.1) von ihm geprägt und das Beweisprinzip durch seine Arbeiten auf eine formale Basis gestellt.



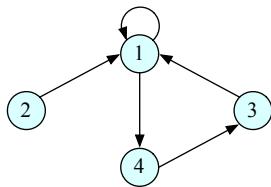
$$M = M_1 \cup \dots \cup M_5, \\ M_i \cap M_k = \emptyset \text{ für } i \neq k, 1 \leq i, k \leq 5$$

**Abbildung 2.8:** Eine Partition teilt eine Menge in paarweise disjunkte Äquivalenzklassen auf.

■ Mengendarstellung

$$R := \{ (1,1), (1,4), (2,1), (3,1), (4,3) \}$$

■ 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 2.9:** Für die Beschreibung von Relationen haben sich verschiedene Darstellungsformen etabliert.



### 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 2.9 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 Verbindungsleitung (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 2.9 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:



### Definition 2.4 (Relationenattribute)

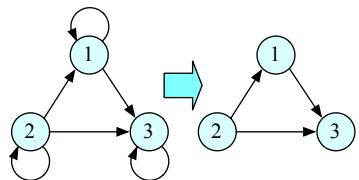
Eine Relation  $R$  in der Menge  $M$  heißt

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

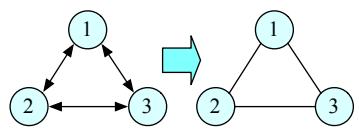
Stellen wir eine Relation  $R$  als Graph oder in Form einer Adjazenzmatrix dar, so lassen sich viele der eingeführten Attribute auf den ersten Blick erkennen. Eine Relation  $R$  ist genau dann reflexiv, wenn alle Knoten des Relationengraphen mit einer Schlinge versehen sind; eine symmetrische Relation 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. 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 2.10). 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. Aufgrund der Transitivität kann eine Kante zwischen zwei Knoten  $x$  und  $y$  immer dann entfallen, wenn  $x$  und  $y$  bereits über andere Kanten miteinander verbunden sind.

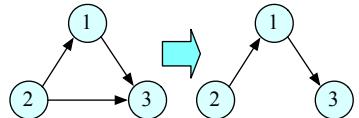
#### ■ Reflexivität



#### ■ Symmetrie



#### ■ Transitivität



**Abbildung 2.10:** Vereinfachte Darstellung reflexiver, symmetrischer und transiver Relationen

**Reflexivität**

„Für alle  $x \in M$  gilt  $x \sim x$ “

$$R \text{ ist reflexiv} \Leftrightarrow R^0 \subseteq R$$

**Irreflexivität**

„Für alle  $x \in M$  gilt  $x \not\sim x$ “

$$R \text{ ist irreflexiv} \Leftrightarrow R^0 \cap R = \emptyset$$

**Symmetrie**

„Aus  $x \sim y$  folgt  $y \sim x$ “

$$R \text{ ist symmetrisch} \Leftrightarrow R = R^{-1}$$

**Asymmetrie**

„Aus  $x \sim y$  folgt  $y \not\sim x$ “

$$R \text{ ist asymmetrisch} \Leftrightarrow R \cap R^{-1} = \emptyset$$

**Antisymmetrie**

„Aus  $x \sim y$  und  $y \sim x$  folgt  $x = y$ “

$$R \text{ ist antisymmetrisch} \Leftrightarrow R \cap R^{-1} \subseteq R^0$$

**Transitivität**

„Aus  $x \sim y$  und  $y \sim z$  folgt  $x \sim z$ “

$$R \text{ ist transitiv} \Leftrightarrow R \cdot R \subseteq R$$

**Tabelle 2.1:** Alternative Charakterisierung einiger Relationenattribute

Genau wie Mengen lassen sich auch Relationen durch die Anwendung elementarer Operationen zu neuen Relationen verknüpfen. Wichtig für unsere Betrachtungen sind vor allem die Berechnung des *Relationenprodukts* sowie die Bildung der inversen Relation.

**Definition 2.5 (Relationenprodukt, inverse Relation)**

$R$  und  $S$  seien zwei Relationen in  $M$ . Das *Relationenprodukt*  $R \cdot S$  und die *inverse Relation*  $R^{-1}$  sind wie folgt definiert:

$$\begin{aligned} R \cdot S &:= \{(x, y) \mid \text{es existiert ein } z \text{ mit } x \sim_R z \text{ und } z \sim_S y\} \\ R^{-1} &:= \{(y, x) \mid (x, y) \in R\} \end{aligned}$$

Ferner treffen wir die folgenden Vereinbarungen:

$$R^0 := \{(x, x) \mid x \in R\}$$

$$R^n := R \cdot R^{n-1}$$

Entsprechend dieser Definition ist das Wertepaar  $(x, y)$  genau dann ein Element des Relationenprodukts, wenn  $x$  und  $y$  über ein drittes Zwischenelement  $z$  in Beziehung stehen. Offensichtlich gelten für drei beliebige Relationen  $S$ ,  $R$  und  $T$  in einer Menge  $M$  die folgenden Beziehungen:

$$R \cdot (S \cdot T) = (R \cdot S) \cdot T \quad (2.39)$$

$$R \cdot R^0 = R \quad (2.40)$$

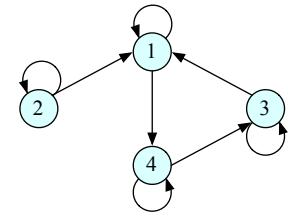
$R^0$  ist das neutrale Element des Relationenprodukts und wird als *Gleichheitsrelation* oder *Identität* bezeichnet. Mit Hilfe der eingeführten Operationen lassen sich die weiter oben definierten Relationenattribute elegant charakterisieren. Für eine beliebige Relation  $R$  gelten die in Tabelle 2.1 zusammengefassten Beziehungen.

In vielen Anwendungsfällen ist es notwendig, eine gegebene Relation  $R$  um ein oder mehrere Attribute aus Definition 2.4 anzureichern. Hierzu wird  $R$  in eine größere Relation eingehüllt, die  $R$  als Teilmenge enthält. Von besonderer Bedeutung sind die *transitive* und die *reflexiv transitive Hülle* von  $R$ :

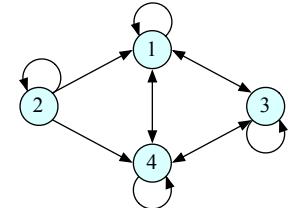
**Definition 2.6 (Transitive Hülle)**

Sei  $R$  eine beliebige Relation in  $M$ . Die *transitive Hülle*  $R^+$  ist die kleinste Relation, die  $R$  einschließt und die Eigenschaften der Transitivität erfüllt.

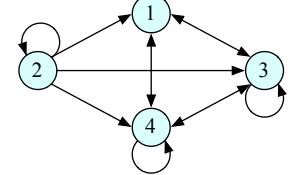
$$R_0 \cup R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cup \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$



$$(R_0 \cup R)^2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$



$$(R_0 \cup R)^3 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$



**Abbildung 2.11:** Iterative Berechnung der reflexiv transitiven Hülle



### Definition 2.7 (Reflexiv transitive Hülle)

Sei  $R$  eine beliebige Relation in  $M$ . Die *reflexiv transitive Hülle*  $R^*$  ist die kleinste Relation, die  $R^+$  einschließt und zusätzlich die Eigenschaften der Reflexivität erfüllt.

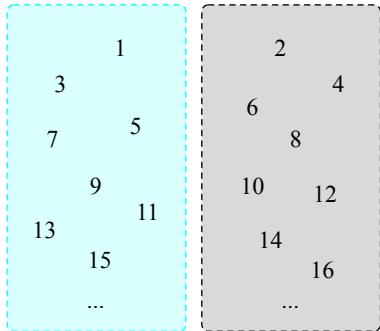
Aus der gegebenen Definition erschließt sich sofort die folgende Überlegung:  $x \sim_{R^+} y$  gilt genau dann, wenn ein  $k \in \mathbb{N}$  und Elemente  $z_1, \dots, z_k$  mit der folgenden Eigenschaft existieren:

$$x \sim_R z_1, z_1 \sim_R z_2, \dots, z_k \sim_R y \quad (2.41)$$

Damit lassen sich die transitive und die reflexiv transitive Hülle in direkter Weise auf das Relationenprodukt reduzieren. Es gelten die folgenden Beziehungen:

$$R^+ = \bigcup_{i=1}^{\infty} R^i, \quad R^* = \bigcup_{i=0}^{\infty} R^i \quad (2.42)$$

- $\{(x,y) \mid x, y \in \mathbb{N}, x \bmod 2 = y \bmod 2\}$



**Abbildung 2.12:** Äquivalenzrelationen partitionieren die Grundmenge in paarweise disjunkte Äquivalenzklassen.

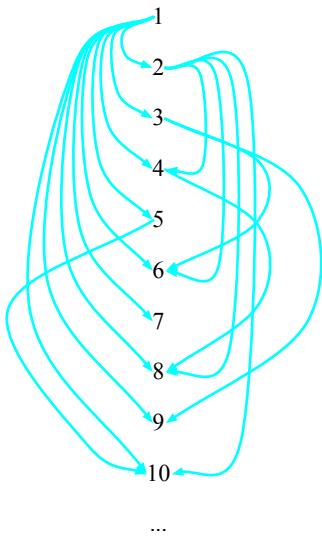
Ist  $R$  eine Relation in einer endlichen Menge  $M$  mit  $n$  Elementen, so können wir die Gleichungen auf die folgende Form reduzieren:

$$R^+ = \bigcup_{i=1}^n R^i, \quad R^* = \bigcup_{i=0}^n R^i = (R_0 \cup R)^n \quad (2.43)$$

In dieser Form können wir die Gleichungen verwenden, um die transitive bzw. die reflexiv transitive Hülle zu erzeugen. Für die Berechnung von  $R^*$  fügen wir zunächst die Elemente von  $R^0$  zu  $R$  hinzu. Auf diese Weise wird  $R$  zu einer reflexiven Relation. Anschließend reichern wir die Menge um neue Wertpaare  $(x,y)$  an, indem wir die Relation so lange mit sich selbst multiplizieren, bis ein Fixpunkt erreicht ist. Die reflexiv transitive Hülle ist berechnet, wenn keine neuen Wertpaare mehr hinzukommen.

Stellen wir die Relation  $R$  in Form einer Adjazenzmatrix dar, so lässt sich das Relationenprodukt durch eine modifizierte Matrizenmultiplikation erzeugen. Die Modifikation besteht darin, alle Produktkoeffizienten ungleich 0 als 1 in die Ergebnismatrix einzutragen. Hierdurch ist sichergestellt, dass die Multiplikation zweier Matrizen wieder eine binäre Matrix ergibt. Abbildung 2.11 demonstriert die Berechnung anhand eines konkreten Beispiels.

- $\{(x,y) \mid y = n \cdot x \text{ für ein } n \in \mathbb{N}\}$



**Abbildung 2.13:** Ordnungsrelationen erzeugen eine (partielle) Hierarchie auf den Elementen der Grundmenge.

Wir werden nun die weiter oben eingeführten Attribute nutzen, um Relationen genauer zu klassifizieren. Die folgenden Klassen werden uns im Rest dieses Buchs immer wieder aufs Neue begegnen:

#### ■ Äquivalenzrelationen

Eine Relation  $R$  ist eine *Äquivalenzrelation*, wenn sie gleichzeitig *reflexiv*, *symmetrisch* und *transitiv*

ist. Jede Äquivalenzrelation in einer Menge  $M$  besitzt die Eigenschaft, die Elemente aus  $M$  in Äquivalenzklassen einzuteilen. Hierzu wird jedes Element  $x \in M$  der Äquivalenzklasse

$$[x]_\sim := \{y \mid x \sim y\} \quad (2.44)$$

zugeordnet. Die Reflexivität, Symmetrie und Transitivität führt dazu, dass die Äquivalenzklassen paarweise disjunkt sind. Die Menge der Äquivalenzklassen ist also eine Partition von  $M$ .

Die folgenden beiden Beispiele sind Äquivalenzrelationen in den natürlichen Zahlen:

$$R_1 := \{(x,y) \mid x, y \in \mathbb{N}, x \bmod 2 = y \bmod 2\}$$

$$R_2 := \{(x,x) \mid x \in \mathbb{N}\}$$

Die Relation  $R_1$  separiert die Menge der natürlichen Zahlen in die Klasse der geraden Zahlen und die Klasse der ungeraden Zahlen (vgl. Abbildung 2.12). Hinter der Relation  $R_2$  verbirgt sich nichts anderes als die bekannte Gleichheitsrelation ( $=$ ). In diesem Fall bildet jedes Element  $x$  seine eigene Äquivalenzklasse.

### ■ Ordnungsrelationen

Eine Relation  $R$  ist eine *Ordnungsrelation*, wenn sie gleichzeitig

*reflexiv, transitiv* und *antisymmetrisch*

ist. Die folgenden beiden Beispiele sind Ordnungsrelationen in den natürlichen Zahlen:

$$R_1 := \{(x, y) \mid x \leq y\}$$

$$R_2 := \{(x, y) \mid y = n \cdot x \text{ für ein } n \in \mathbb{N}\}$$

Die Relation  $R_1$  entspricht der bekannten Kleiner-gleich-Relation.  $R_2$  setzt zwei Zahlen  $x$  und  $y$  genau dann in Relation zueinander, wenn  $y$  ein ganzzahliges Vielfaches von  $x$  ist. Alle Ordnungsrelationen besitzen die Eigenschaft, die Elemente einer Menge in eine hierarchische Ordnung zu bringen. Die Definition lässt dabei ausdrücklich zu, dass zwei Elemente  $x$  und  $y$  in überhaupt keiner Beziehung zueinander stehen. Beispielsweise gilt für das obige Beispiel weder  $2 \sim_{R_2} 3$  noch  $3 \sim_{R_2} 2$  (vgl. Abbildung 2.13). Ordnungen mit dieser Eigenschaft werden auch als *partielle Ordnung* bezeichnet. Gilt dagegen, wie im Fall von  $R_1$ , für zwei beliebige Elemente  $x$  und  $y$  entweder die Beziehung  $x \sim y$  oder  $y \sim x$ , so sprechen wir von einer *Totalordnung* oder einer *linearen Ordnung*.

Neben den Äquivalenz- und Ordnungsrelationen existiert eine weitere wichtige Relationenklasse, die bisher gänzlich unerwähnt blieb. Die Rede ist von der Klasse der *Funktionen* (*Abbildungen*).



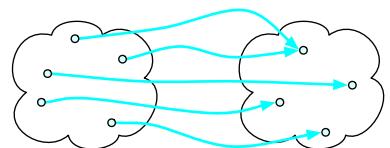
### Definition 2.8 (Funktion)

Mit  $M$  und  $N$  seien zwei beliebige nichtleere Mengen gegeben. Unter einer *Funktion* oder einer *Abbildung*

$$f : M \rightarrow N \tag{2.45}$$

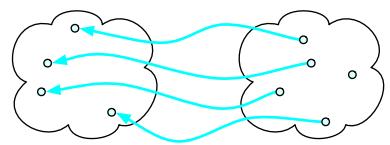
verstehen wir eine Vorschrift, die jedem Element  $x$  der *Definitionsmenge*  $M$  höchstens ein Element  $f(x)$  der *Zielmenge*  $N$  zuordnet.

### ■ Surjektivität



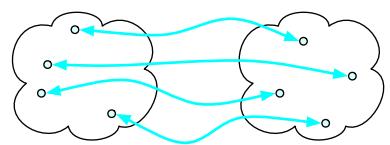
Ausnahmslos jedes Element der Zielmenge ist das Bild eines oder mehrerer Elemente der Definitionsmenge.

### ■ Injektivität



Es liegt eine umkehrbar eindeutige Zuordnung vor. Die Bilder zweier unterschiedlicher Elemente der Definitionsmenge sind stets verschieden.

### ■ Bijektivität



Die Eigenschaften der Surjektivität und Injektivität sind gleichermaßen erfüllt. Es besteht eine Eins-zu-eins-Zuordnung zwischen den Elementen der Definitionsmenge und der Zielmenge.

**Abbildung 2.14:** Surjektive, injektive und bijektive Funktionen

```

log.c
1  unsigned foo ( unsigned x )
2  {
3      int y = 0;
4      while (x != 1) {
5          x >>= 1;
6          y++;
7      }
8      return y;
9  }

```

**Abbildung 2.15:** Logarithmenberechnung in der Programmiersprache C

Der Funktionsbegriff wird in der theoretischen Informatik anders definiert als in der Mathematik. Dort ist eine Funktion eine Zuordnungsvorschrift, die ausnahmslos jedes Element der Definitionsmenge auf ein Element der Zielmenge abbildet. Mit anderen Worten: In der klassischen Mathematik sind alle Funktionen total. Der Begriff der partiellen Funktion wurde in der theoretischen Informatik eingeführt, um Programme zu beschreiben, die für gewisse Eingabewerte nicht terminieren. Als Beispiel betrachten wir die in Abbildung 2.15 dargestellte C-Funktion `foo`. Für  $x > 0$  berechnet sie den ganzzahlig gerundeten Zweierlogarithmus des Eingabewerts  $x$ . Für  $x = 0$  ist der Ausgabewert undefiniert, da das Programm in eine Endlosschleife gerät. Mit Hilfe von partiellen Funktionen lässt sich das Programmverhalten problemlos beschreiben:

$$f(x) : x \mapsto \lfloor \log_2 x \rfloor \quad \text{für } x > 0$$

Trotzdem besteht zwischen partiellen und totalen Funktionen kein wirklich fundamentaler Unterschied. Wir können jede partielle Funktion auf eine totale Funktion zurückführen, indem wir die Zielmenge um ein zusätzliches Symbol  $\perp$  anreichern, das wir als Bildelement für alle undefinierten Funktionswerte verwenden.



### Definition 2.9 (Funktion (Fortsetzung))

Eine Funktion  $f : M \rightarrow N$  heißt

- *total*, wenn für jedes  $x \in M$  ein Element  $f(x) \in N$  existiert.
- *partiell*, wenn sie für mindestens ein  $x \in M$  undefiniert ist.

Das Element  $f(x)$  heißt der *Funktionswert* von  $f$  an der Stelle  $x$  bzw. das *Bild* von  $x$ . Analog heißt  $x$  das *Urbild* von  $f(x)$ . Formal verbirgt sich hinter einer Funktion  $f : M \rightarrow N$  nichts anderes als eine rechtseindeutige Relation  $R_f \subseteq M \times N$ . Die bekannte Schreibweise  $f : x \mapsto y$  drückt aus, dass die Funktion  $f$  das Element  $x$  auf das Element  $y$  abbildet, und ist gleichbedeutend mit der relationalen Notation  $x \sim_{R_f} y$ . Gilt  $N \subseteq M$ , so sprechen wir von einer *Selbstabbildung*. Funktionen der Form  $f : M^n \rightarrow M$  werden häufig als  $n$ -stellige *Operatoren* bezeichnet. In der Mathematik werden totale Funktionen anhand ihrer Abbildungseigenschaften wie folgt klassifiziert:



### Definition 2.10 (Surjektivität, Injektivität, Bijektivität)

Sei  $f : M \rightarrow N$  eine totale Funktion.  $f$  heißt

- *surjektiv*, falls für alle  $y \in N$  ein  $x \in M$  mit  $f(x) = y$  existiert,
- *injektiv*, falls aus  $f(x) = f(y)$  stets  $x = y$  folgt,
- *bijektiv*, falls  $f$  sowohl injektiv als auch surjektiv ist.

Grob gesprochen besitzen surjektive Funktionen die Eigenschaft, die Zielmenge vollständig auszuschöpfen, d. h., jedes Element besitzt mindestens ein Urbild in der Definitionsmenge. Injektive Funktionen zeichnen sich dadurch aus, dass jedes Element der Zielmenge höchstens ein Urbild besitzt. Diese Eigenschaft ist die Voraussetzung, um aus einer Abbildung  $f$  die *Umkehrabbildung*  $f^{-1}$  zu konstruieren, die jedem Element  $f(x)$  sein Urbild  $x$  zuordnet. Entsprechend werden injektive Funktionen auch als *umkehrbar eindeutig* oder einfach nur als *umkehrbar* bezeichnet. Eine bijektive Funktion  $f$  erfüllt beide Eigenschaften gleichzeitig, so dass für jedes Element  $x$  der Definitionsmenge genau ein Element  $y$  der Zielmenge mit  $f(x) = y$  existiert. Mit anderen Worten: Bijektive Funktionen stellen eine Eins-zu-eins-Zuordnung zwischen Definitionsmenge und Zielmenge her. Abbildung 2.14 fasst die Eigenschaften surjektiver, injektiver und bijektiver Funktionen grafisch zusammen.

## 2.3 Die Welt der Zahlen

### 2.3.1 Natürliche, rationale und reelle Zahlen

Im vorherigen Abschnitt haben wir mit der Menge  $\mathbb{N} = \{1, 2, 3, \dots\}$  die *natürlichen Zahlen* eingeführt. Der Umgang mit dieser Menge scheint uns in die Wiege gelegt, schließlich entspringt sie einer angeborenen Fähigkeit des Menschen: dem Abzählen von Dingen. Auch wenn uns die natürlichen Zahlen auf den ersten Blick völlig vertraut erscheinen, wollen wir sie an dieser Stelle durch eine formale Definition charakterisieren. Nur so sind wir in der Lage, auf den zweiten Blick aufkeimende, scheinbare Widersprüche im Ansatz zu ersticken.

Die am weitesten verbreitete Definition der natürlichen Zahlen geht auf den italienischen Mathematiker Giuseppe Peano zurück (Abbildung 2.16). Dieser lieferte im Jahre 1892 eine formale Beschreibung, die aus insgesamt fünf Axiomen besteht [73]:



#### Definition 2.11 (Axiomatisierung der natürlichen Zahlen)

Die Menge der natürlichen Zahlen  $\mathbb{N}$  ist durch die folgenden fünf *Peano-Axiome* charakterisiert:

- P1) 1 ist eine natürliche Zahl.
- P2) Jede natürliche Zahl  $n$  hat genau einen Nachfolger  $\text{succ}(n)$ .
- P3) 1 ist kein Nachfolger einer natürlichen Zahl.
- P4) Die Nachfolger zweier verschiedener natürlicher Zahlen sind ebenfalls verschieden.
- P5) Enthält eine Teilmenge  $M \subseteq \mathbb{N}$  die Zahl 1 und zu jedem Element  $n$  auch ihren Nachfolger  $\text{succ}(n)$ , so gilt  $M = \mathbb{N}$ .

Das Peano-Axiom P4 ist gleichbedeutend mit der Aussage, dass keine natürliche Zahl existiert, die mehr als einen Vorgänger besitzt.

Die Menge der natürlichen Zahlen ist bezüglich der Addition und der Multiplikation abgeschlossen, d. h., für zwei beliebige Zahlen  $a, b \in \mathbb{N}$  liegen auch die Summe  $a + b$  sowie das Produkt  $a \cdot b$  in  $\mathbb{N}$ . Aufgrund des einseitig beschränkten Zahlenbereichs besitzt die Gleichung

$$a + x = b \quad (2.46)$$

*„Questions that pertain to the foundations of mathematics, although treated by many in recent times, still lack a satisfactory solution. Ambiguity of language is philosophy's main source of problems. That is why it is of the utmost importance to examine attentively the very words we use.“*



Giuseppe Peano (1858 – 1932)

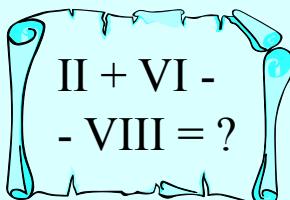
**Abbildung 2.16:** Der Italiener Giuseppe Peano gilt als einer der Wegbereiter der mathematischen Logik und der axiomatischen Methode. Peano war ein Akkurateur seines Faches und ein Verfechter symbolischer Sprachen. Nur diese verfügten seiner Ansicht nach über die nötige Präzision, um mathematische Sachverhalte prägnant und unmissverständlich zu formulieren. Unter anderem gehen die heute immer noch gebräuchlichen Symbole  $\cup$ ,  $\cap$ ,  $\in$  und  $\exists$  auf die Arbeiten von Peano zurück. Einen großen Teil seines wissenschaftlichen Engagements widmete er dem *Formulario-Projekt* – einem groß angelegten Vorhaben zur Formalisierung des mathematischen Wissens. Heute ist der Name Peano fest mit den fünf Axiomen verbunden, die uns die formale Grundlage für den Umgang mit den natürlichen Zahlen liefern.

In der modernen Mathematik ist die Null nicht wegzudenken. Ohne sie würden weder die elementaren Regeln der Arithmetik funktionieren noch wären wir in der Lage, Dezimalzahlen eindeutig zu notieren. Der Umgang mit ihr ist uns heute so vertraut, dass sie keinerlei Sonderstellung mehr bedarf. Kurzum: Die Null ist zu einer Zahl wie jede andere geworden.

Vor diesem Hintergrund verwundert es immer wieder, dass sie erst sehr spät ihren Platz in der Arithmetik fand. Babylonier, Ägypter, Griechen und Römer kannten kein Symbol für die Null und entsprechend schwer war es, in den verwendeten Zahlensystemen zu rechnen. Wahrscheinlich verhinderte ihre innerste Bedeutung den unvoreingenommenen Umgang mit dieser Zahl. Null stand für „nichts“ und jede Definition einer entsprechenden Zahl schien diese Eigenschaft ad absurdum zu führen.

Das geistige Fundament der Zahl Null, wie wir sie heute verstehen und verwenden, wurde in Indien im fünften bis siebten Jahrhundert n. Chr. geschaffen. Über Persien gelangte sie nach Europa und über den Himalaja nach China.

Das Rechnen mit der Null sollte die Mathematiker noch über Jahre beschäftigen. Der indische Mathematiker und Astronom Brahmagupta war der Meinung, null geteilt durch null ergäbe null. Andere Mathematiker waren der Auffassung, dass eine Zahl unverändert bleibt, wenn sie durch null dividiert wird. Erst die Infinitesimalrechnung von Leibniz und Newton lieferte schließlich das mathematische Instrumentarium, um das unendlich Kleine zu beherrschen [12].



jedoch nur für  $a < b$  eine Lösung in  $\mathbb{N}$ . Abhilfe schafft die Menge der *ganzen Zahlen*  $\mathbb{Z}$ , die  $\mathbb{N}$  in den negativen Zahlenbereich fortsetzt:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \quad (2.47)$$

In dieser Menge können wir Gleichung (2.46) für beliebige Werte von  $a$  und  $b$  lösen. Genau wie die natürlichen Zahlen sind auch die ganzen Zahlen bezüglich der Addition und der Multiplikation abgeschlossen. Dagegen ist die Division nur in Ausnahmefällen möglich. Der Wunsch, die Gleichung

$$a \cdot x = b \quad (2.48)$$

für beliebige Werte  $a, b \in \mathbb{Z}$  zu lösen, bringt uns auf direktem Weg zu den *rationalen Zahlen*  $\mathbb{Q}$ :

$$\mathbb{Q} := \{x \mid x = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0\} \quad (2.49)$$

Jede rationale Zahl  $a \in \mathbb{Q}$  lässt sich als unendlicher periodischer Dezimalbruch der Form

$$x = \underbrace{a_k \dots a_1 a_0}_{Vorkommastellen}, \underbrace{a_{-1} a_{-2} \dots a_{-l}}_{Nachkommastellen}, \underbrace{\overline{a_{-l-1} a_{-l-2} \dots a_{-m}}}_{Periode} \quad (2.50)$$

überführen und jede Zahl der Form (2.50) in der Form  $\frac{p}{q}$  mit  $p, q \in \mathbb{Z}$  darstellen. Kurzum: Die Menge der rationalen Zahlen ist mit der Menge der unendlichen periodischen Dezimalbrüche identisch. In diesen sind die endlichen Dezimalzahlbrüche als Spezialfall enthalten; sie entsprechen einem periodischen Dezimalbruch mit der Periode 0.

Die Menge der rationalen Zahlen verfügt über zwei wesentliche Eigenschaften. Zum einen sind die natürlichen und die ganzen Zahlen Teilmengen von  $\mathbb{Q}$ . Zum anderen können wir in dieser Menge uneingeschränkt rechnen. Für zwei beliebige rationale Zahlen liegen die Summe, die Differenz, das Produkt und der Quotient ebenfalls wieder in  $\mathbb{Q}$ . Es gelten die folgenden Rechenregeln:

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} : \frac{c}{d} = \frac{ad}{bc} \quad (2.51)$$

Die gewonnene Bewegungsfreiheit, die wir in der Menge der rationalen Zahlen genießen, wirft die Frage auf, ob eine erneute Erweiterung des Zahlenbereichs sinnvoll ist. Die Antwort lautet „ja“, da die Menge  $\mathbb{Q}$  – obwohl sie jedes noch so kleine Intervall mit unendlich vielen Elementen überdeckt – Lücken besitzt. Ein Beispiel einer solchen Lücke ist die Zahl  $\sqrt{2}$ . Von dieser wissen wir zunächst nur, dass sie mit sich

selbst multipliziert das Ergebnis 2 liefert. Den ungefähren Wert von  $\sqrt{2}$  können wir ebenfalls beziffern:

$$\sqrt{2} \approx 1,41421 \quad (2.52)$$

Wir können uns der Zahl  $\sqrt{2}$  durch die Angabe weiterer Nachkommastellen beliebig nähern. Jeder Versuch,  $\sqrt{2}$  exakt niederzuschreiben, ist jedoch von vorneherein zum Scheitern verurteilt. Schuld daran ist die Eigenschaft dieser Zahl, unendlich viele, unregelmäßig auftretende Nachkommaziffern zu besitzen. Mit anderen Worten:  $\sqrt{2}$  besitzt keine periodische Dezimalbruchdarstellung und ist damit keine rationale Zahl. Diese Erkenntnis ist keinesfalls neu. Bereits Euklid von Alexandria konnte mit einem einfachen Widerspruchsargument zeigen, dass sich  $\sqrt{2}$  nicht in Form eines Dezimalbruchs darstellen lässt und damit außerhalb von  $\mathbb{Q}$  liegen muss [28].

Schließen wir die Lücken in der Menge  $\mathbb{Q}$  durch die Hinzunahme aller Zahlen mit einer unendlichen, nichtperiodischen Dezimalbruchdarstellung, so erhalten wir die Menge der *reellen Zahlen*  $\mathbb{R}$ .

$$\mathbb{R} := \{x \mid x \text{ besitzt eine unendliche Dezimalbruchdarstellung}\} \quad (2.53)$$

Die Differenzmenge  $\mathbb{R} \setminus \mathbb{Q}$  heißt die Menge der *irrationalen Zahlen*. Neben der Zahl  $\sqrt{2}$  enthält  $\mathbb{R} \setminus \mathbb{Q}$  weitere bekannte Größen. Beispiele sind die Kreiszahl  $\pi$  und die Euler'sche Konstante  $e$ .

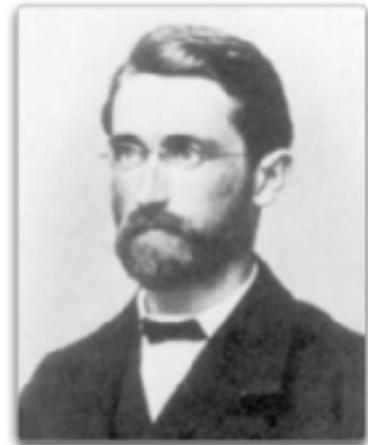
Die soeben gegebene Definition der reellen Zahlen ist recht vage formuliert und im mathematischen Sinne nur bedingt belastbar. Aus diesem Grund wurden in der Vergangenheit erhebliche Anstrengungen unternommen, die Definition von  $\mathbb{R}$  zu präzisieren. Einen formalen und gleichzeitig anschaulichen Zugang zu den reellen Zahlen liefernte der deutsche Mathematiker Julius Dedekind im Jahre 1872 (Abbildung 2.17). Dedekind ging von der Idee aus, dass die Zahlengerade durch jeden ihrer Punkte in eine linke und eine rechte Seite unterteilt wird. In entsprechender Weise lässt sich jeder Punkt durch zwei Mengen  $L$  und  $R$  mit  $\mathbb{Q} = L \cup R$  und  $l < r$  für alle  $l \in L$  und alle  $r \in R$  beschreiben. Das Tupel  $(L|R)$  wird als *Dedekind'scher Schnitt* bezeichnet und steht stellvertretend für ein Element aus  $\mathbb{R}$ :

$$\begin{aligned} \frac{1}{3} &= (\{x \in \mathbb{Q} \mid x \leq \frac{1}{3}\} \mid \{x \in \mathbb{Q} \mid x > \frac{1}{3}\}) \\ \sqrt{2} &= (\{x \in \mathbb{Q} \mid x^2 < 2\} \mid \{x \in \mathbb{Q} \mid x^2 > 2\}) \end{aligned}$$

Obwohl jeder Schnitt ausschließlich aus rationalen Zahlen besteht, ist es uns gelungen, jede reelle Zahl eindeutig zu identifizieren.

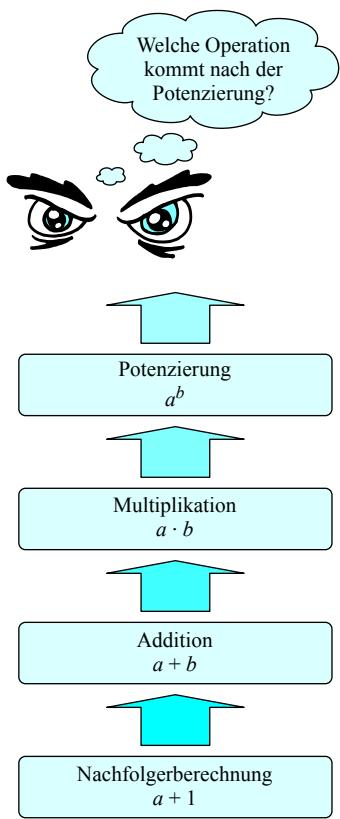
Die Dedekind'schen Schnitte sind nicht das einzige Modell, um die reellen Zahlen greifbar zu machen. Andere Formalisierungen bedienen sich

„Die Zahlen sind freie Schöpfungen des menschlichen Geistes, sie dienen als Mittel, um die Verschiedenheit der Dinge leichter und schärfer aufzufassen.“ [26]



Richard Dedekind (1831 – 1916)

**Abbildung 2.17:** Im Jahre 1872 veröffentlichte der deutsche Mathematiker Richard Dedekind seine einflussreiche Definition der reellen Zahlen [25]. Seither gehören die Dedekind'schen Schnitte zu den wichtigsten Hilfsmitteln für den formalen Umgang mit dieser Zahlenmenge.



**Abbildung 2.18:** Hierarchie der arithmetischen Operatoren

des Prinzips der Intervallschachtelung oder definieren die reellen Zahlen, wie einst von Georg Cantor vorgeschlagen, als Äquivalenzklasse rationaler Cauchy-Folgen [44].

### 2.3.2 Von großen Zahlen

Standen in unseren bisherigen Untersuchungen die Zahlen im Mittelpunkt, wollen wir uns in diesem Abschnitt ausführlicher mit den *Operatoren* beschäftigen, ohne die jegliche Mathematik ein langweiliges Unterfangen wäre. Wir werden eine Reihe von Betrachtungen vornehmen, die für den reinen Mathematiker exotisch wirken mögen, im Bereich der Berechenbarkeitstheorie aber eine bedeutende Rolle spielen.

Für die folgenden Betrachtungen setzen wir als Grundmenge die natürlichen Zahlen  $\mathbb{N}$  voraus. Die mit Abstand einfachste Operation auf einer Zahl  $a \in \mathbb{N}$  ist die Berechnung des Nachfolgers  $\text{succ}(a) = 1 + a$ . Dass  $\text{succ}(a)$  für alle Zahlen  $a \in \mathbb{N}$  existiert, garantiert uns das zweite Peano-Axiom.

Unwesentlich komplexer ist die Addition. Im Grunde genommen handelt es sich dabei um keine neue Operation, da wir die Berechnung von  $a + b$  auf die wiederholte Anwendung der Nachfolgeoperation  $(1 + a)$  reduzieren können:

$$a + b = \underbrace{1 + (1 + (1 + (\dots + (1 + a)))))}_{b \text{ Kopien von } 1} \quad (2.54)$$

$$= 1 + (a + (b - 1)) \quad (2.55)$$

Die nächsthöhere Operation ist die Multiplikation. Analog zu den Gleichungen (2.54) und (2.55) können wir die Produktbildung auf die Addition zurückführen:

$$a \cdot b = \underbrace{a + (a + (a + (\dots + (a + a)))))}_{b \text{ Kopien von } a} \quad (2.56)$$

$$= a + (a \cdot (b - 1)) \quad (2.57)$$

Die wiederum nächsthöhere Operation ist die Potenzierung. Wir können dem eingeschlagenen Schema treu bleiben und die Potenz  $a^b$  wie folgt berechnen:

$$a^b = \underbrace{a \cdot (a \cdot (a \cdot (\dots \cdot (a \cdot a)))))}_{b \text{ Kopien von } a} \quad (2.58)$$

$$= a \cdot (a^{b-1}) \quad (2.59)$$

$\text{ack}(n, m)$	$m = 0$	$m = 1$	$m = 2$	$m = 3$	$m = 4$
$n = 0$	1	2	3	4	5
$n = 1$	2	3	4	5	6
$n = 2$	3	5	7	9	11
$n = 3$	5	13	29	61	125
$n = 4$	13	65533	$2^{65536} - 3$	$2^{2^{65536} - 3}$	$\text{ack}(3, 2^{2^{65536} - 3})$
$n = 5$	65533	$\text{ack}(4, 65533)$	$\text{ack}(4, \text{ack}(5, 1))$	$\text{ack}(4, \text{ack}(5, 2))$	$\text{ack}(4, \text{ack}(5, 3))$
$n = 6$	$\text{ack}(4, 65533)$	$\text{ack}(5, \text{ack}(5, 1))$	$\text{ack}(5, \text{ack}(6, 1))$	$\text{ack}(5, \text{ack}(6, 2))$	$\text{ack}(5, \text{ack}(6, 3))$

**Tabelle 2.2:** Ein kleiner Auszug aus der Wertetabelle der Ackermann-Funktion

Die arithmetischen Operationen scheinen ganz offensichtlich eine Hierarchie zu bilden (vgl. Abbildung 2.18). Doch wie geht diese Hierarchie nach oben weiter? Konkreter formuliert: Welche mathematische Operation kommt nach der Potenzierung? Dass den meisten von uns die Antwort auf diese Frage nicht auf der Zunge liegt, hat einen triftigen Grund: Der klassischen Mathematik fehlen Symbole, mit denen sich arithmetische Operationen höherer Grade niederschreiben lassen.

Der US-amerikanische Computerwissenschaftler Donald E. Knuth löste das Problem im Jahre 1976 durch die Einführung der *Up-Arrow-Notation* [59]. Mit dem  $\uparrow$ -Operator schuf er die Möglichkeit, Funktionen verschiedener Grade nach einem einheitlichen Schema zu benennen:

$$a \uparrow^n b := \begin{cases} a^b & \text{falls } n = 1 \\ 1 & \text{falls } b = 0 \\ a \uparrow^{n-1} (a \uparrow^n (b-1)) & \text{sonst} \end{cases} \quad (2.60)$$

Die Definition folgt exakt dem gleichen Konstruktionsprinzip, das uns bereits die Potenzierung auf die Multiplikation (Gleichung (2.59)), die Multiplikation auf die Addition (Gleichung (2.57)) und die Addition schließlich auf die Nachfolgeoperation (Gleichung (2.55)) reduzierten ließ.

Eine bekannte Funktion, die das Schema der herausgearbeiteten Berechnungsvorschrift aufgreift, ist die *Ackermann-Funktion* [1]. Sie wurde von dem deutschen Mathematiker Wilhelm Ackermann im Jahre 1928 publiziert und wird uns in Kapitel 6 als Hilfsmittel dienen, um die unterschiedliche Ausdrucksstärke von Loop- und While-Programmen zu beweisen. Die heute gebräuchliche Darstellungsform unterscheidet

sich von jener der Originalarbeit. Sie geht auf den deutschen Mathematiker Hans Hermes zurück und ist durch die folgende rekursive Definition gegeben [43]:

$$\text{ack}(0, m) = m + 1 \quad (2.61)$$

$$\text{ack}(n, 0) = \text{ack}(n - 1, 1) \quad (2.62)$$

$$\text{ack}(n, m) = \text{ack}(n - 1, \text{ack}(n, m - 1)) \quad (2.63)$$

Gleichung (2.63) enthält den gleichen rekursiven Kern, auf dem auch die Definition des  $\uparrow$ -Operators beruht. Entsprechend sind wir in der Lage, die Ackermann-Funktion mit Hilfe des  $\uparrow$ -Operators auszudrücken. Es gelten die folgenden Beziehungen:

$$\text{ack}(1, m) = 2 + (m + 3) - 3 \quad (2.64)$$

$$\text{ack}(2, m) = 2 \cdot (m + 3) - 3 \quad (2.65)$$

$$\text{ack}(3, m) = 2 \uparrow (m + 3) - 3 \quad (2.66)$$

$$\text{ack}(4, m) = 2 \uparrow\uparrow (m + 3) - 3 \quad (2.67)$$

$$\text{ack}(5, m) = 2 \uparrow\uparrow\uparrow (m + 3) - 3 \quad (2.68)$$

$$\text{ack}(6, m) = 2 \uparrow\uparrow\uparrow\uparrow (m + 3) - 3 \quad (2.69)$$

...

$$\text{ack}(n, m) = 2 \underbrace{\uparrow\uparrow \dots \uparrow}_{(n-2)\text{-mal}} (m + 3) - 3 \quad (2.70)$$

Wie die Gleichungen (2.64) bis (2.70) offenbaren, verbirgt sich hinter dem harmlos anmutenden Rekursionsschema eine trickreiche Konstruktion. Die Ackermann-Funktion ist eine Art Universalfunktion, die die gesamte Operatorenhierarchie in sich vereint. Da der erste Parameter den Grad der auszuführenden Operation bestimmt, nimmt die Funktion selbst für kleine Parameter riesige Werte an. Tabelle 2.2 vermittelt einen Eindruck über das Wachstumsverhalten. Obwohl die Tabelle nur wenige Felder umfasst, konnten die Funktionswerte nicht überall in ihrer Dezimaldarstellung eingetragen werden. So entspricht der Wert  $\text{ack}(4, 2)$  bereits einer ca. 20.000-stelligen Zahl.

### 2.3.3 Die Unendlichkeit begreifen

In diesem Abschnitt wenden wir uns einem Thema zu, das in der theoretischen Informatik eine übergeordnete Rolle spielt und etliche Generationen von Mathematikern vor scheinbar unüberwindbare Rätsel stellte (vgl. Abbildung 2.19). Die Rede ist von der Unendlichkeit. Wir werden uns an diesen Begriff in zwei Schritten herantasten. Zunächst werden

*„Wir werden uns nicht mit Streitigkeiten über das Unendliche ermüden, denn bei unserer Endlichkeit wäre es verkehrt.“*



(René Descartes)  
(1596 – 1650)

*„Wir haben keine Vorstellung eines unendlichen Raumes.“*



(Gottfried Wilhelm Leibniz)  
(1646 – 1716)

*„So protestiere ich gegen den Gebrauch einer unendlichen Größe.“*



(Carl Friedrich Gauß)  
(1777 – 1855)

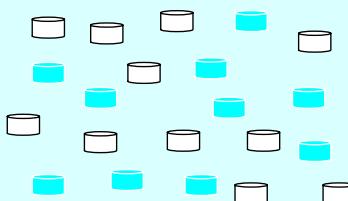
**Abbildung 2.19:** Der Begriff der Unendlichkeit stellte viele Mathematikergenerationen vor scheinbar unüberwindliche Rätsel. Erst die Arbeiten von Georg Cantor lieferten das notwendige Instrumentarium, um das Unendliche systematisch zu erfassen und beherrschbar zu machen.

wir definieren, was sich hinter dem nebulösen Terminus der Unendlichkeit genau verbirgt. Anschließend werden wir zeigen, dass Unendlichkeit nicht gleich Unendlichkeit ist. Sie mögen es vielleicht schon vermuten: Es gibt derer unendlich viele.

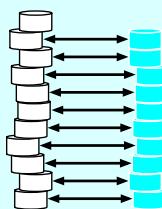
In der Mathematik ist die Unendlichkeit allgegenwärtig und in vielen Situationen scheint uns deren Anwesenheit nicht weiter zu stören. Wir gehen wie selbstverständlich mit der Menge der natürlichen Zahlen  $\mathbb{N}$  oder der Menge der ganzen Zahlen  $\mathbb{Z}$  um, obwohl wir niemals in der Lage sein werden, alle Zahlen niederzuschreiben. Auf die Frage, wie viele Elemente die Mengen  $\mathbb{N}$  und  $\mathbb{Z}$  wirklich besitzen, antworten wir fast schon reflexartig mit der Antwort „unendlich“. Viele von uns plagt dabei das Gefühl, dass die Menge der ganzen Zahlen  $\mathbb{Z}$  mehr Elemente enthalten müsste als die Menge der natürlichen Zahlen  $\mathbb{N}$ . Alle Elemente von  $\mathbb{N}$  sind schließlich in  $\mathbb{Z}$  enthalten, nicht jedoch umgekehrt. Damit ist an der Zeit, uns Gedanken zu machen, wie wir den schwer greifbaren Begriff der Unendlichkeit bändigen können.

Der Schlüssel für den Umgang mit dem Unendlichen liegt in der Be- trachtung der *Mächtigkeit* (*Kardinalität*) einer Menge  $M$ . Diese wird

Die Idee, die Gleichmächtigkeit zweier Mengen über die Existenz einer bijektiven Zuordnung zu entscheiden, ist kein Kunstprodukt der Mathematik. In Wirklichkeit ist uns das verwendete Prinzip vertrauter, als es auf den ersten Blick erscheinen mag. So setzen wir diese Methode in vielen Alltagssituationen unbewusst ein, um das vergleichsweise aufwendige Zählen großer Gegenstandsmengen zu umgehen. Auch Kinder, die des Rechnens noch überhaupt nicht mächtig sind, bedienen sich dieses Prinzips.



Um z. B. festzustellen, ob in einer Menge von Spielsteinen mehr blaue oder mehr weiße Steine enthalten sind, ist es ausreichend, diese farblich zu separieren und anschließend zu stapeln:



In der neuen Darstellung lässt sich mit einem einzigen Blick erkennen, dass die weißen Steine in der Überzahl sind. Beachtlich an dieser Methode ist vor allem die Tatsache, dass wir die Mächtigkeit zweier Mengen vergleichen können, ohne die konkrete Anzahl ihrer Elemente zu bestimmen. Erst hierdurch sind wir in der Lage, die Vorgehensweise auf Mengen mit unendlich vielen Elementen zu übertragen.

mit  $|M|$  bezeichnet und entspricht für endliche Mengen schlicht der Anzahl ihrer Elemente.

$$M_1 = \emptyset \Rightarrow |M_1| = 0 \quad (2.71)$$

$$M_2 = \{\square, \diamond, \circ\} \Rightarrow |M_2| = 3 \quad (2.72)$$

$$M_3 = \{2, 3, 5\} \Rightarrow |M_3| = 3 \quad (2.73)$$

Die Mengen  $M_2$  und  $M_3$  sind *gleichmächtig*, da sie die gleiche Anzahl an Elementen enthalten. In diesem Fall sind wir in der Lage, die Elemente beider Mengen eindeutig einander zuzuordnen. Für unser Beispiel könnte die Zuordnung folgendermaßen aussehen:

$$\square \mapsto 2, \quad \diamond \mapsto 3, \quad \circ \mapsto 5 \quad (2.74)$$

Stimmt die Anzahl der Elemente nicht überein, so ist jeder Versuch, eine derartige Zuordnung herzustellen, zum Scheitern verurteilt. Damit sind wir in der Lage, den Begriff der Mächtigkeit an die Existenz einer entsprechenden Abbildung zu knüpfen:



### Definition 2.12 (Mengenvergleiche)

Mit  $M_1$  und  $M_2$  seien zwei beliebige Mengen gegeben.  $M_1$  und  $M_2$  heißen *gleichmächtig*, geschrieben als

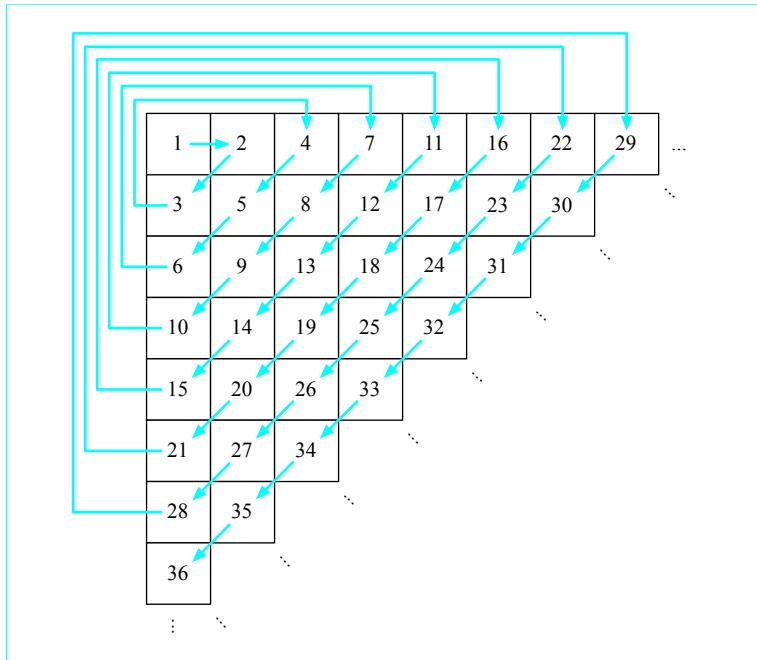
$$|M_1| = |M_2|,$$

wenn eine bijektive Abbildung  $f : M_1 \rightarrow M_2$  existiert. Jede unendliche Menge  $M$  heißt

- *abzählbar*, falls  $|M| = |\mathbb{N}|$ , und
- *überabzählbar*, falls  $|M| \neq |\mathbb{N}|$  gilt.

Zwei unendliche Mengen sind per Definition genau dann gleichmächtig, wenn sich ihre Elemente jeweils umkehrbar eindeutig einander zuordnen lassen. Auf den ersten Blick erscheint die Herangehensweise als unnatürlich und unnötig umständlich. Auf den zweiten Blick wird deutlich, dass die Definition darauf verzichtet, die Elemente einer Menge explizit zu zählen. Damit sind wir in der Lage, auch dann die Kardinalität zweier Mengen zu vergleichen, wenn diese unendlich viele Elemente enthalten.

Plakativ gesprochen drückt der Begriff der *Abzählbarkeit* aus, dass wir die Elemente einer unendlichen Menge durchnummrieren können. Mit welcher Nummer wir die einzelnen Elemente konkret belegen, spielt



**Abbildung 2.20:** Die abgebildete Paarungsfunktion ordnet jedem Tupel  $(p, q) \in \mathbb{N}^2$  eine Zahl  $\pi_{\mathbb{N}}(p, q) \in \mathbb{N}$  zu. Die Abbildung ist bijektiv und beweist, dass  $\mathbb{N}$  und  $\mathbb{N}^2$  gleichmächtig sind.

dabei keine Rolle – einzig die Existenz einer solchen Zuordnung macht eine Menge abzählbar. Überabzählbare Mengen besitzen diese Eigenschaft nicht, d. h., jeder Versuch, ihre Elemente durchzunummerieren, muss scheitern. Dass es solche Mengen überhaupt gibt, ist keinesfalls selbstverständlich.

Im Folgenden werden wir zeigen, dass solche Mengen tatsächlich existieren und sich sogar systematisch aus abzählbaren Mengen konstruieren lassen. Die Cantor'sche Definition der Kardinalität wird sich dabei als äußerst wertvoll erweisen, da wir hierüber in der Lage sind, die konstruierten Mengen miteinander zu vergleichen. Wie wir gleich sehen werden, hält die Unendlichkeit einige Überraschungen für uns bereit.

Als Erstes betrachten wir die beiden Mengen  $\mathbb{N}$  und  $\mathbb{Z}$ . Obwohl  $\mathbb{N}$  eine echte Teilmenge von  $\mathbb{Z}$  ist, lassen sich beide bijektiv aufeinander abbilden. Die folgende Zuordnung ist eine von – Sie werden es ahnen – unendlich vielen Möglichkeiten:

$$f : x \mapsto \begin{cases} -2x & \text{falls } x < 0 \\ 2x + 1 & \text{falls } x \geq 0 \end{cases} \quad (2.75)$$

Die Mengen der natürlichen und der ganzen Zahlen erweisen sich in der Tat als gleichmächtig. Doch damit nicht genug. Auch die Menge der ra-

*Hilberts Hotel* ist ein Gedankenspiel, das eine verblüffende Eigenschaft der Unendlichkeit anschaulich demonstriert [15]. Im Kern geht es um die Frage, ob in einem Hotel mit unendlich vielen Zimmern selbst dann ein neuer Gast aufgenommen werden kann, wenn es restlos ausgebucht ist.



Unter normalen Umständen würde Ihnen jeder Portier mit Schulterzucken begegnen. In Hilberts Hotel ist es dagegen kein Problem, ein freies Zimmer zu beschaffen. Um einen neuen Gast aufzunehmen, müssen wir lediglich alle bisherigen Gäste bitten, aus ihrem Zimmer mit der Nummer  $n$  in das Zimmer mit der Nummer  $n + 1$  zu wechseln. Auf diese Weise wird das Zimmer mit der Nummer 1 frei, in das wir unseren neuen Gast einquartieren können.



Das Gedankenspiel stellt unsere menschliche Intuition auf eine harte Probe und mag zunächst mehr Verwirrung stiften als Klarheit schaffen. Auf den zweiten Blick wird deutlich, dass wir einen zusätzlichen Gast genau deshalb aufnehmen können, weil die Mengen  $\mathbb{N}$  und  $\mathbb{N} \setminus \{1\}$  gleichmächtig sind. Wenn jeder Gast sein Nachbarzimmer bezieht, entspricht dies der Anwendung der Funktion  $f : n \mapsto n + 1$ , die  $\mathbb{N}$  bijektiv auf die Menge  $\mathbb{N} \setminus \{1\}$  abbildet.

tionalen Zahlen  $\mathbb{Q}$  lässt sich bijektiv auf  $\mathbb{N}$  abbilden. Wie dies aussehen kann, ist in Abbildung 2.20 skizziert. Alle Elemente von  $\mathbb{Q}$  sind in einer Matrix angeordnet, die sich unendlich weit nach rechts und nach unten ausbreitet.  $\frac{x}{y} \in \mathbb{Q}$  können wir eindeutig einem Element der Matrix zuordnen, indem wir  $x$  mit der Spalte und  $y$  mit der Zeile des entsprechenden Felds identifizieren. Wie die Abbildung zeigt, sind wir in der Lage, jedes Matrixelement  $(x, y)$  mit einer eindeutigen Nummer  $\pi_{\mathbb{N}}(x, y)$  zu belegen, indem wir im Feld  $(1, 1)$  beginnen und uns anschließend diagonal zwischen der oberen und der linken Seite hin- und herbewegen. Die entstehende Abbildung  $\pi_{\mathbb{N}} : \mathbb{N}^2 \rightarrow \mathbb{N}$  heißt *Cantor'sche Paarungsfunktion* und lässt sich über die nachstehende Formel direkt berechnen:

$$\pi_{\mathbb{N}}(x, y) = y + \sum_{i=1}^{x+y-2} i = 1 + \frac{(x+y)^2 - 3x - y}{2} \quad (2.76)$$

Über die Existenz einer bijektiven Zuordnung zwischen  $\mathbb{N}$  und  $\mathbb{Q}$  haben wir gezeigt, dass beide Mengen die gleiche Mächtigkeit besitzen.

Mit Hilfe der Cantor'schen Paarungsfunktion lassen sich weitere Mengen als gleichmächtig identifizieren. Durch die rekursive Anwendung sind wir z. B. in der Lage, nicht nur jedem Paar  $(x, y) \in \mathbb{N}^2$ , sondern auch jedem Tripel  $(x, y, z) \in \mathbb{N}^3$  ein eindeutiges Element in  $\mathbb{N}$  zuzuordnen. Hierzu definieren wir die Funktion  $\pi_{\mathbb{N}}^3 : \mathbb{N}^3 \rightarrow \mathbb{N}^2$  wie folgt:

$$\pi_{\mathbb{N}}^3(x, y, z) := \pi_{\mathbb{N}}(\pi_{\mathbb{N}}(x, y), z) \quad (2.77)$$

Führen wir den Gedanken in dieser Richtung fort, so erhalten wir mit

$$\pi_{\mathbb{N}}^1(x_1) := x_1 \quad (2.78)$$

$$\pi_{\mathbb{N}}^{n+1}(x_1, \dots, x_n, x_{n+1}) := \pi_{\mathbb{N}}(\pi_{\mathbb{N}}^n(x_1, \dots, x_n), x_{n+1}) \quad (2.79)$$

eine bijektive Abbildung von  $\mathbb{N}^n$  auf  $\mathbb{N}$ . Damit ist bewiesen, dass der  $n$ -dimensionale Zahlenraum  $\mathbb{N}^n$  stets die gleiche Mächtigkeit besitzt wie die Grundmenge  $\mathbb{N}$  selbst – unabhängig davon, wie groß wir die Dimension  $n \in \mathbb{N}$  auch wählen.

An dieser Stelle drängt sich unweigerlich die Frage auf, wie eine Menge  $M$  beschaffen sein muss, um mächtiger zu sein als die Menge der natürlichen Zahlen  $\mathbb{N}$ . In der Tat haben wir mit den reellen Zahlen  $\mathbb{R}$  eine solche Menge weiter oben bereits eingeführt. Die Überabzählbarkeit der reellen Zahlen wurde von Georg Cantor erstmals im Jahre 1874 formal gezeigt [14]. Der Beweis ist vergleichsweise abstrakt und nicht einfach zu verstehen.

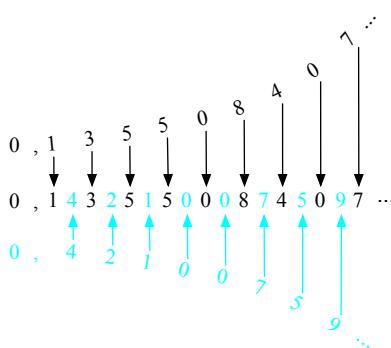
1877 bewies er seine Aussage erneut – diesmal auf verblüffend einfache Weise. Den Kern des Beweises bildet das von ihm entwickelte *Diagona-*

$f(1) =$	0	,	5	4	9	0	0	7	5	8	...
$f(2) =$	0	,	7	1	4	4	5	6	6	3	...
$f(3) =$	0	,	7	4	3	9	6	1	4	2	...
$f(4) =$	0	,	2	3	1	1	1	7	4	5	...
$f(5) =$	0	,	2	7	9	7	7	4	0	0	...
$f(6) =$	0	,	3	8	6	4	8	7	2	8	...
$f(7) =$	0	,	5	6	0	6	9	3	7	4	...
$f(8) =$	0	,	2	1	3	4	4	9	9	9	...
$\vdots$	$\ddots$										

**Abbildung 2.21:** Das Diagonalisierungsargument. Gäbe es eine bijektive Abbildung von den natürlichen auf die reellen Zahlen, so müsste sich die (unendlich lange) Ziffernfolge jeder reellen Zahl in einer Zeile der Zuordnungsmatrix wiederfinden lassen. Unabhängig von der gewählten Zuordnung sind wir jedoch stets im Stande, die Ziffernfolge einer reellen Zahl zu konstruieren, die nicht in der Matrix vorkommt. Diese können wir erzeugen, indem wir uns entlang der Hauptdiagonalen von links oben nach rechts unten bewegen und die vorgefundene Ziffer um eins erhöhen oder erniedrigen. Die konstruierte Ziffernfolge kommt nirgends in der Matrix vor, da sie sich von jener der  $i$ -ten Zeile per Konstruktion in der  $i$ -ten Ziffer unterscheidet. Die Überlegung zeigt, dass eine bijektive Zuordnung der Elemente aus  $\mathbb{R}$  zu den Elementen aus  $\mathbb{N}$  nicht möglich ist. Kurzum: Die Menge der reellen Zahlen ist nicht abzählbar.

lisierungsargument, eine genauso leistungsfähige wie intuitive Methode, um eine Menge als überabzählbar zu identifizieren. Cantor stellt die folgende Überlegung an: Angenommen, die beiden Mengen  $\mathbb{N}$  und  $\mathbb{R}$  sind gleichmächtig, so muss eine bijektive Abbildung  $f : \mathbb{N} \rightarrow \mathbb{R}$  existieren, die jedes Element  $x \in \mathbb{N}$  eindeutig auf ein Element  $f(x) \in \mathbb{R}$  abbildet. Listen wir die Funktionswerte  $f(1), f(2), f(3), \dots$  von oben nach unten auf, so entsteht eine zweidimensionale Matrix, wie sie in Abbildung 2.21 skizziert ist. Formal entspricht das Element in Spalte  $x$  und Zeile  $y$  der  $x$ -ten Ziffer der Dezimalbruchdarstellung von  $f(y)$ . Natürlich können wir nur einen winzigen Ausschnitt der entstehenden Matrix zeichnen, da die Funktion  $f$  für unendlich viele Werte  $y \in \mathbb{N}$  definiert ist und sich die Dezimalbruchdarstellung der reellen Zahlen  $f(y)$  über unendlich viele Ziffern erstreckt. Kurzum: Die aufgestellte Matrix besteht aus unendlich vielen Spalten und Zeilen.

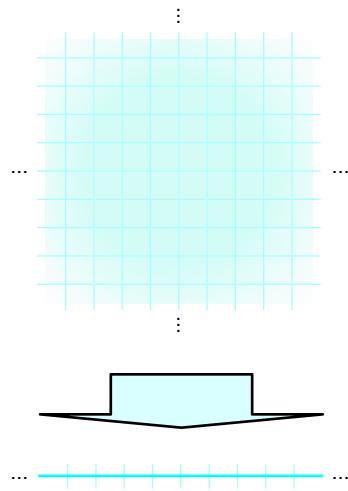
Mit Hilfe des Diagonalisierungsarguments können wir zeigen, dass die Matrix nie vollständig sein kann. Unabhängig von der konkreten Wahl von  $f$  existieren reelle Zahlen, die nicht in der Matrix enthalten sind und damit die Bijektivität von  $f$  ad absurdum führen. Wir konstruieren eine solche Zahl, indem wir uns entlang der Hauptdiagonalen von links oben nach rechts unten bewegen und die vorgefundenen Ziffern jeweils um



**Abbildung 2.22:** Im Reißverschlussverfahren lassen sich zwei reelle Zahlen zu einer einzigen reellen Zahl verschmelzen. Die Zuordnung ist eine bijektive Abbildung von  $\mathbb{R}$  auf  $\mathbb{R}^2$  und beweist die Gleichmächtigkeit beider Mengen.

eins erhöhen oder erniedrigen. Die entstehende Ziffernfolge interpretieren wir als die Nachkommaziffern einer reellen Zahl  $r$ . Wäre  $f$  eine bijektive Abbildung von  $\mathbb{N}$  auf  $\mathbb{R}$ , so müsste auch die Zahl  $r$  in irgendeiner Zeile vorkommen. Aufgrund des gewählten Konstruktionsschemas ist jedoch sichergestellt, dass sich die reelle Zahl der  $i$ -ten Zeile in der  $i$ -ten Ziffer von  $r$  unterscheidet. Die Annahme, eine bijektive Zuordnung zwischen  $\mathbb{N}$  zu  $\mathbb{R}$  könnte existieren, führt zu einem unmittelbaren Widerspruch. Folgerichtig ist jeder Versuch, die reellen Zahlen nacheinander durchzumerken, zum Scheitern verurteilt. Kurzum: Die Mengen  $\mathbb{N}$  und  $\mathbb{R}$  stehen stellvertretend für zwei verschiedene Unendlichkeiten.

Trotzdem gelten einige der Eigenschaften, die wir für die Menge  $\mathbb{N}$  herausgearbeitet haben, auch in der Menge der reellen Zahlen. So sind wir auch hier in der Lage, ein Tupel  $(x, y) \in \mathbb{R}$  bijektiv auf die Menge  $\mathbb{R}$  abzubilden. Abbildung 2.22 skizziert die zugrunde liegende Konstruktionsidee. Die beiden reellen Zahlen  $x \in \mathbb{R}$  und  $y \in \mathbb{R}$  werden zu einer gemeinsamen reellen Zahl  $\pi_{\mathbb{R}}(x, y) \in \mathbb{R}$  verschmolzen, indem die Vor- und Nachkommaziffern reißverschlussartig miteinander verschränkt werden.



**Abbildung 2.23:** Obwohl die dargestellte Fläche mehr Druckfarbe verbraucht als das Liniensegment, besitzen die zweidimensionale Ebene und die eindimensionale Gerade die gleiche „Anzahl“ reeller Punkte. Jeder Punkt des einen geometrischen Objekts lässt sich eindeutig auf einen Punkt des anderen abbilden.

Erneut hat uns der Cantor'sche Zugang zur Unendlichkeit eine verblüffende Eigenschaft von Zahlenmengen offenbart. Die Gleichmächtigkeit von  $\mathbb{R}$  und  $\mathbb{R}^2$  bedeutet, dass eine Gerade in der Ebene gleich viele Punkte besitzt wie die Ebene selbst. Wir sind damit in der Lage, die Punkte der Ebene verlustfrei auf die Punkte einer Geraden abzubilden. Ebenso ist es möglich, die Ebene lückenlos mit den Punkten einer Geraden zu belegen (vgl. Abbildung 2.23).

Kombinieren wir die Aufrufe von  $\pi_{\mathbb{R}}$  wieder rekursiv miteinander, so entsteht für jede natürliche Zahl  $n \in \mathbb{N}$  eine Abbildung  $\pi_{\mathbb{R}}^n$ , die den  $n$ -dimensionalen Zahlenraum  $\mathbb{R}^n$  bijektiv auf  $\mathbb{R}$  reduziert. Formal ist die Abbildung  $\pi_{\mathbb{R}}^n$ , in Analogie zu den Gleichungen (2.78) und (2.79), wie folgt definiert:

$$\pi_{\mathbb{R}}^1(x_1) := x_1 \quad (2.80)$$

$$\pi_{\mathbb{R}}^{n+1}(x_1, \dots, x_n, x_{n+1}) := \pi_{\mathbb{R}}(\pi_{\mathbb{R}}^n(x_1, \dots, x_n), x_{n+1}) \quad (2.81)$$

Am Beispiel der reellen Zahlen haben wir gesehen, dass eine Unendlichkeit existiert, die mächtiger ist als jene der natürlichen Zahlen. Das Ergebnis wirft die Frage auf, ob es eine weitere Unendlichkeit gibt, die wiederum mächtiger ist als jene der reellen Zahlen. Der folgende Satz von Cantor liefert uns eine positive Antwort auf diese Frage.



### Satz 2.1 (Satz von Cantor)

Für jede beliebige Menge  $M$  ist die Potenzmenge  $2^M$  mächtiger als  $M$  selbst.

Wir können diese Aussage beweisen, indem wir ein ähnliches Diagonalisierungsargument verwenden, mit dem wir bereits die Überabzählbarkeit der reellen Zahlen zeigen konnten. Auch hier gehen wir zunächst wieder von der Existenz einer bijektiven Abbildung  $f : M \rightarrow 2^M$  aus und führen die Annahme anschließend zu einem Widerspruch.

Sei nun  $f$  eine solche Funktion, die  $M$  bijektiv auf die Menge  $2^M$  abbildet. Für jedes Element  $m \in M$  können wir zwei Fälle unterscheiden: Entweder ist  $m$  im Bildelement  $f(m)$  enthalten ( $m \in f(m)$ ) oder nicht ( $m \notin f(m)$ ). Alle Elemente, auf die Letzteres zutrifft, wollen wir in der Menge  $T$  zusammenfassen:

$$T = \{m \in M : m \notin f(m)\} \quad (2.82)$$

Da  $f$  bijektiv und damit insbesondere auch surjektiv ist, muss ein Urbild  $m_T$  existieren mit  $f(m_T) = T$ . Wie für alle Elemente aus  $M$  gilt auch für das Element  $m_T$  entweder die Eigenschaft  $m_T \in T$  oder  $m_T \notin T$ . Beide Fälle führen jedoch unmittelbar zu einem Widerspruch:

$$m_T \in T \Rightarrow m_T \notin f(m_T) \Rightarrow m_T \notin T \quad (2.83)$$

$$m_T \notin T \Rightarrow m_T \in f(m_T) \Rightarrow m_T \in T \quad (2.84)$$

Damit haben wir gezeigt, dass es eine bijektive Funktion  $f : M \rightarrow 2^M$  nicht geben kann. Aus dem Cantor'schen Satz ergeben sich zwei wichtige Konsequenzen. Zum einen zeigt er, dass es keine *maximale Unendlichkeit* gibt, d. h., wir sind nicht in der Lage, eine Universalmenge zu konstruieren, die mächtiger ist als alle anderen Mengen. Es scheint, als ob es die Unendlichkeit abermals schafft, sich jeglichen Grenzen zu entziehen. Zum anderen bringt der Satz eine hierarchische Ordnung in die unendliche Menge der verschiedenen Unendlichkeiten:

$$|\mathbb{N}| < |2^{\mathbb{N}}| < |2^{2^{\mathbb{N}}}| < |2^{2^{2^{\mathbb{N}}}}| < |2^{2^{2^{2^{\mathbb{N}}}}}| < \dots \quad (2.85)$$

Cantor verwendete den hebräischen Buchstaben Aleph ( $\aleph$ ), um die Mächtigkeit einer unendlichen Menge zu beschreiben. Die kleinste Unendlichkeit wird mit der *Kardinalzahl*  $\aleph_0$  bezeichnet; sie entspricht der Kardinalität der natürlichen Zahlen. Eine kleinere Unendlichkeit als  $|\mathbb{N}|$  kann es nicht geben, da sich alle unendlichen Teilmengen von  $\mathbb{N}$  bijektiv auf  $\mathbb{N}$  abbilden lassen. Die nächstgrößere Unendlichkeit wird durch die Kardinalzahl  $\aleph_1$  beschrieben und so fort.

Mit Hilfe des Diagonalisierungsarguments konnte Cantor beweisen, dass die Menge der reellen Zahlen – das *Kontinuum* – eine größere Mächtigkeit besitzt als die Menge der natürlichen Zahlen. Zugleich hatte Cantor die Vermutung, dass es keine unendliche Menge gibt, die bez. ihrer Kardinalität zwischen  $\mathbb{N}$  und  $\mathbb{R}$  liegt. So sehr sich Cantor auch bemühte, blieb es ihm verwehrt, zu Lebzeiten einen Beweis für seine *Kontinuumshypothese* zu finden.

Der deutsche Mathematiker David Hilbert war von der Wichtigkeit der Cantor'schen Vermutung überzeugt. Auf der Liste der 23 wichtigsten mathematischen Probleme, die er im Jahre 1900 auf dem internationalen Mathematikerkongress in Paris vortrug, avancierte die Klärung der Kontinuumshypothese an erster Stelle.

Nach vielen erfolglosen Versuchen gelang Kurt Gödel im Jahre 1937 ein entscheidender Durchbruch. Wie im Fall des Auswahlaxioms konnte er zeigen, dass die Kontinuumshypothese mit den anderen Axiomen der Zermelo-Fraenkel-Mengenlehre vereinbar ist. Wird die Hypothese den ZF-Axiomen oder den ZFC-Axiomen hinzugefügt, so bleibt die Widerspruchsfreiheit erhalten, sofern diese innerhalb der restlichen Axiome gegeben ist. Einen Beweis der Kontinuumshypothese konnte Gödel nicht liefern und nährte gleichermaßen die Vermutung, dass ein solcher überhaupt nicht existiert.

Die endgültige Gewissheit ließ bis zum Jahre 1963 auf sich warten, als der amerikanische Mathematiker Paul Cohen zeigen konnte, dass auch die Negation der Kontinuumshypothese nicht im Widerspruch zur Zermelo-Fraenkel'schen Mengenlehre steht. Damit war das Rätsel um die Cantor'sche Vermutung geklärt. Die Kontinuumshypothese ist innerhalb des klassischen Axiomensystems weder beweisbar noch widerlegbar und kann als zusätzliches Axiom widerspruchsfrei hinzugefügt werden.

■ Rekursives Definitionsschema

$$n! = \begin{cases} 1 & \text{für } n = 0 \\ n \cdot (n-1)! & \text{für } n > 0 \end{cases}$$

■ Rekursive Implementierung

```
fakultaet.c
int fakultaet( int n )
{
    if ( n == 0 )
        return 1;
    else
        return
            n * fakultaet( n - 1 );
}
```

**Abbildung 2.24:** Rekursive Implementierung der Fakultätsfunktion

## 2.4 Rekursion und induktive Beweise

Immer dann, wenn ein Problem, eine Funktion oder ein Verfahren durch sich selbst beschrieben wird, sprechen wir von einer *rekursiven Definition*. In der Regel ist die Rekursion so konstruiert, dass sich das gesuchte Ergebnis aus einem oder mehreren Teilergebnissen *kleinerer Ordnung* berechnen lässt. Meist ist die Ordnung nach unten beschränkt, d. h., es existieren nicht weiter zerlegbare Basisfälle, die direkt berechnet werden können. Eine rekursive Definition besteht damit immer aus zwei Teilen. Im ersten Teil werden die Basisfälle definiert und im zweiten Teil die Rekursionsregeln festgelegt.

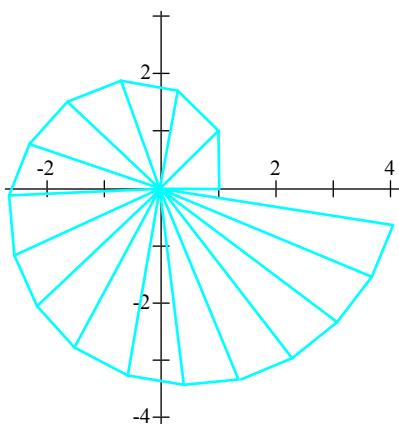
Abbildung 2.24 demonstriert das Rekursionsprinzip am Beispiel der Fakultätsfunktion. Da nahezu alle Programmiersprachen Selbstauffufe auf Funktionsebene unterstützen, lassen sich rekursive Definitionen eins zu eins in ein Programm umsetzen. In einer rekursiv programmierter Funktion werden die Basisfälle explizit ausprogrammiert und alle anderen Funktionswerte durch eine Reihe von Selbstauffufen ermittelt.

Von Programmieranfängern wird das Rekursionsprinzip gerne gemieden. Zu Unrecht, wie sich an etlichen Beispielen belegen lässt. Mit ein wenig Übung lassen sich viele Algorithmen deutlich übersichtlicher implementieren, als es die streng iterative Programmierung erlaubt.

Auch wenn das Rekursionsprinzip im Bereich der Informatik einen prominenten Platz einnimmt, ist es keine Erfindung des Informationszeitalters. In der Mathematik ist das Prinzip seit Langem verankert, wie das *Rad des Theodorus* belegt. Diese geometrische Figur wird aus mehreren aneinandergereihten Dreiecken  $T_1, \dots, T_n$  gebildet, die dem nachstehenden rekursiven Konstruktionsschema folgen:

- $T_1$  ist ein rechtwinkliges Dreieck mit der Seitenlänge 1.
- Die Hypotenuse von  $T_n$  ist ein Schenkel von  $T_{n+1}$ . Der andere Schenkel besitzt die Länge 1.

Werden die Dreiecke aneinandergereiht, so entsteht die in Abbildung 2.25 dargestellte Wurzelschnecke.



**Abbildung 2.25:** Das Rad des Theodorus (Wurzelschnecke) ist ein Beispiel einer rekursiv definierten geometrischen Struktur. Dem griechischen Gelehrten Theodorus (ca. 465 v. Chr.) gelang es mit Hilfe dieser Figur, die Zahlen  $\sqrt{3}, \sqrt{5}, \sqrt{7}, \dots, \sqrt{17}$  als irrational zu identifizieren.

Im nächsten Abschnitt werden wir mit der vollständigen Induktion ein wichtiges Beweisprinzip vorstellen, das sich die rekursive Struktur der natürlichen Zahlen zunutze macht. Anschließend werden wir die Methode in Abschnitt 2.4.2 verallgemeinern und mit der strukturellen Induktion ein Hilfsmittel an die Hand bekommen, mit dem sich Aussagen über rekursiv definierte Datenstrukturen formal beweisen lassen.

## 2.4.1 Vollständige Induktion

Die *vollständige Induktion* ist neben dem direkten Deduktionsbeweis und dem indirekten Widerspruchsbeweis die dritte grundlegende Beweistechnik der Mathematik. Ihre Berechtigung bezieht sie aus den in Abschnitt 2.3 eingeführten Peano-Axiomen. Das fünfte Peano-Axiom lautete wie folgt:

- P5) Enthält eine Teilmenge  $M \subseteq \mathbb{N}$  die Zahl 1 und zu jedem Element  $n$  auch ihren Nachfolger  $\text{succ}(n)$ , so gilt  $M = \mathbb{N}$ .

Aus den elementaren Eigenschaften der natürlichen Zahlen lässt sich die folgende Verallgemeinerung herleiten:

- P5') Enthält eine Teilmenge  $M \subseteq \mathbb{N}$  die Zahl  $n_0$  und zu jedem Element  $n \geq n_0$  auch ihren Nachfolger  $\text{succ}(n)$ , so gilt  $M = \{n \mid n \geq n_0\}$ .

Hieraus ergibt sich das Prinzip der vollständigen Induktion wie folgt:



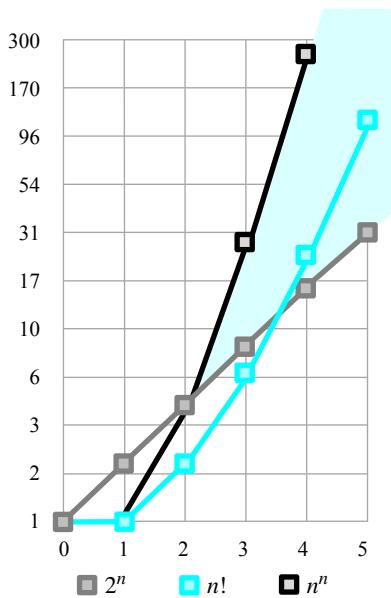
### Satz 2.2 (Vollständige Induktion)

Sei  $n_0 \in \mathbb{N}$  und  $A(n)$  eine parametrisierte Aussage über den natürlichen Zahlen. Wenn die folgenden beiden Aussagen gelten, so ist  $A(n)$  für alle  $n$  mit  $n \geq n_0$  wahr.

- $A(n_0)$  ist wahr.
- Für alle  $k$  mit  $k \geq n_0$  gilt: Aus  $A(k)$  folgt die Aussage  $A(k + 1)$ .

Anwenden lässt sich die vollständige Induktion auf alle Aussagen, die von einem Parameter  $n \in \mathbb{N}$  abhängen, wobei die Aussage *für alle*  $n$  ab einem gewissen Startwert  $n_0$  bewiesen werden soll. Ein vollständiger Beweis setzt sich aus insgesamt drei Schritten zusammen:

- Induktionsanfang: Für den Startwert  $n_0$  wird die Behauptung  $A(n_0)$  bewiesen.
- Induktionsannahme: Für einen beliebigen Wert  $n$  mit  $n \geq n_0$  wird die Aussage  $A(n)$  als wahr angenommen.
- Induktionsschritt: Unter der Induktionsannahme wird der Beweis geführt, dass die Aussage  $A(n + 1)$  ebenfalls wahr ist.



**Abbildung 2.26:** Die Funktionen  $2^n$ ,  $n!$  und  $n^n$  im Vergleich. Ab  $n = 4$  bilden  $2^n$  und  $n^n$  einen Korridor, den die Fakultätsfunktion  $n!$  nicht mehr verlässt. Mit der Technik der vollständigen Induktion lässt sich die Eigenschaft in wenigen Schritten beweisen.

Der Induktionsanfang, die Induktionsvoraussetzung und der Induktionsschritt stellen zusammen sicher, dass die Aussage *für alle  $n$  Gültigkeit* besitzt. Der Induktionsanfang beweist die Aussage für den Fall  $n = n_0$ . Die Gültigkeit für  $n_0 + 1$  folgt durch Anwendung des Induktionsschritts auf den Fall  $n_0$ , die Gültigkeit für  $n_0 + 2$  durch Anwendung des Induktionsschritts auf den Fall  $n_0 + 1$  und so fort.

Beachten Sie, dass wir die Induktionsannahme verstärken können, ohne die Gültigkeit des Beweisprinzips zu gefährden. Anstatt die Aussage  $A(n)$  nur für ein einzelnes  $n$  als wahr anzunehmen, können wir die Gültigkeit von  $A(k)$  für alle  $k$  mit  $n_0 \leq k < n$  ebenfalls als wahr annehmen.

Um nicht im Nebel der Theorie zu versinken, wollen wir die folgende Aussage mit dem Mittel der vollständigen Induktion beweisen:

### Satz 2.3

Ab einem gewissen Wert  $n_0 \in \mathbb{N}$  gilt für alle  $n \geq n_0$  die Abschätzung:

$$2^n < n! < n^n$$

#### Beweis

##### ■ Induktionsanfang

Für  $0 \leq n \leq 3$  ist die Abschätzung nicht erfüllt. Wir wählen  $n_0 = 4$ . Jetzt gilt  $(2^4 = 16) < (4! = 24) < (4^4 = 256)$ .

##### ■ Induktionsvoraussetzung

Für ein gewisses  $n \geq 4$  gelte die Abschätzung  $2^n < n! < n^n$ .

##### ■ Induktionsschritt

Wir müssen zeigen, dass die Abschätzung

$$2^{n+1} < (n+1)! < (n+1)^{n+1}$$

erfüllt ist. Diese können wir mit Hilfe der Induktionsvoraussetzung und den elementaren Rechenregeln wie folgt herleiten:

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n < (n+1) \cdot 2^n < (n+1) \cdot n! \\ &= (n+1)! \end{aligned}$$

$$\begin{aligned} (n+1)! &= (n+1) \cdot n! < (n+1)n^n < (n+1)(n+1)^n \\ &= (n+1)^{n+1} \end{aligned}$$

Damit ist die die Abschätzung für alle  $n \geq 4$  erfüllt und die Behauptung bewiesen.  $\square$

## 2.4.2 Strukturelle Induktion

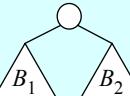
Die strukturelle Induktion ist ein mathematisches Beweisschema, das uns erlaubt, Induktionsbeweise über beliebige rekursiv definierte Strukturen zu führen. Genau wie im Fall der vollständigen Induktion beweisen wir in einem strukturellen Induktionsbeweis die Behauptung zunächst für einen oder mehrere Basisfälle. Anschließend zeigen wir im Induktionsschritt, dass sich die Gültigkeit der Behauptung auf das nächstkomplexere Objekt übertragen lässt. Konkret umfassen in einem strukturellen Induktionsbeweis die Basisfälle alle nicht zusammengesetzten Elemente. Setzt sich ein Element aus mehreren Teilobjekten zusammen, so wird die Behauptung unter der Annahme bewiesen, dass sie für alle Teilobjekte bereits gezeigt wurde.

In der Informatik spielt die strukturelle Induktion die gleiche Rolle wie die vollständige Induktion in der Mathematik. Insbesondere im Bereich der Software-Technik lässt sich das Beweisprinzip gewinnbringend einsetzen, da viele Datenstrukturen einem rekursiven Konstruktionsschema folgen. Was wir unter einer solchen Definition konkret zu verstehen haben, wollen wir am Beispiel des *Binärbaums* herausarbeiten.



### Definition 2.13 (Binärbaum)

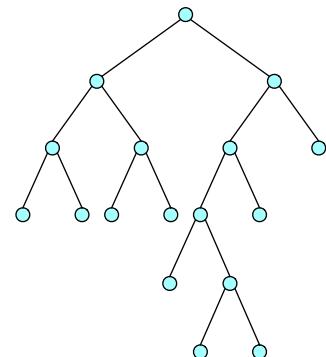
Ein *Binärbaum* (*binary tree*) über einer *Blättermenge*  $L$  ist wie folgt definiert:

- Jedes Blatt  $l \in L$  ist ein Binärbaum.
- Sind  $B_1$  und  $B_2$  Binäräume, dann ist auch  ein Binärbaum.

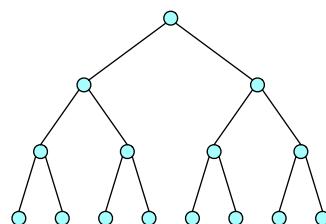
Binäräume sind damit nichts anderes als spezielle Bäume mit der Eigenschaft, dass jeder Knoten entweder 0 oder 2 Söhne hat. Die Anzahl der Knoten eines Baums bezeichnen wir mit  $|B|$ . Die maximale Anzahl von Kanten, die wir von dem Knoten bis zu einem Blatt ablaufen können, heißt die *Tiefe* des Baums. Ein Binärbaum heißt *balanciert*, wenn alle Pfade von der Wurzel zu den Blättern die gleiche Länge besitzen. Beachten Sie, dass die Produktionsregel in Abbildung 2.13 nicht zwangsläufig einen balancierten Baum entstehen lässt (vgl. Abbildung 2.27).

Mit Hilfe der strukturellen Induktion können wir viele Eigenschaften von Binäräumen beweisen. Als Beispiel wollen wir die Gültigkeit des

■ Binärbaum

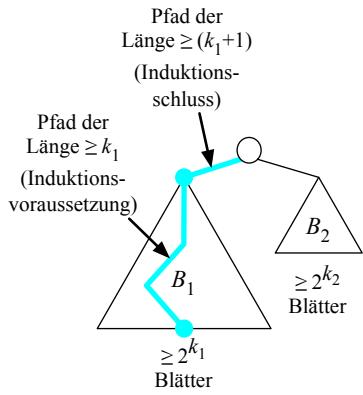


■ Balancierter Binärbaum

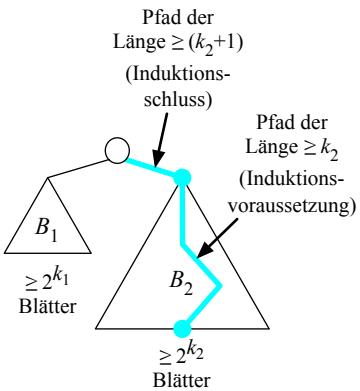


**Abbildung 2.27:** Balancierte Binäräume zeichnen sich dadurch aus, dass alle Pfade von der Wurzel zu den Blättern die gleiche Länge besitzen.

- Fall 1:  $|B_1| \geq |B_2|$



- Fall 2:  $|B_2| \geq |B_1|$



**Abbildung 2.28:** Grafische Veranschaulichung des Induktionsschritts

folgenden Satzes zeigen, der uns in Abschnitt 4.4.3 im Zusammenhang mit dem Pumping-Lemma für kontextfreie Sprachen erneut begegnen wird.



### Satz 2.4

Seien  $k \in \mathbb{N}$  eine natürliche Zahl und  $B$  ein Binärbaum mit  $|B| \geq 2^k$ . Dann existiert in  $B$  mindestens ein Pfad der Länge  $\geq k$ .

#### Beweis

- Induktionsanfang

Besteht ein Binärbaum  $B$  aus einem einzigen Blatt, so gilt

$$|B| = 1 = 2^0.$$

Der Baum besitzt trivialerweise einen Pfad der Länge 0.

- Induktionsvoraussetzung

$B_1$  und  $B_2$  seien zwei Binäräume mit  $|B_1| \geq 2^{k_1}$  und  $|B_2| \geq 2^{k_2}$ . Wir nehmen an,  $B_1$  und  $B_2$  erfüllen die zu beweisenden Eigenschaft, d. h., es gib einen Pfad  $P_1$  in  $B_1$  der Länge  $\geq k_1$  und einen Pfad  $P_2$  in  $B_2$  der Länge  $\geq k_2$ .

- Induktionsschritt

Wir kombinieren  $B_1$  und  $B_2$  zu einem Binärbaum  $B$  und zeigen, dass auch  $B$  die postulierte Eigenschaft erfüllt. Zwei Fälle sind zu unterscheiden (vgl. Abbildung 2.28):

- Fall 1:  $B_1$  enthält mindestens so viele Blätter wie  $B_2$   
 $B$  hat dann maximal  $2 \cdot 2^{k_1} = 2^{k_1+1}$  Knoten. Da in  $B_1$  nach Induktionsvoraussetzung ein Pfad der Länge  $k_1$  existiert, besitzt  $B$  einen Pfad der Länge  $k_1 + 1$ .
- Fall 2:  $B_2$  enthält mindestens so viele Blätter wie  $B_1$   
 $B$  hat dann maximal  $2 \cdot 2^{k_2} = 2^{k_2+1}$  Knoten. Da in  $B_2$  nach Induktionsvoraussetzung ein Pfad der Länge  $k_2$  existiert, besitzt  $B$  einen Pfad der Länge  $k_2 + 1$ .

Damit ist die Behauptung für alle Binäräume bewiesen. □

Der vollzogene Induktionsbeweis ist nicht der einzige mögliche. Anstatt die Behauptung induktiv über den strukturellen Aufbau der Binäräume zu beweisen, kann die Aussage auch durch vollständige Induktion gezeigt werden. In diesem Fall wird die natürliche Zahl  $k$  als Induktionsvariable verwendet.

## 2.5 Übungsaufgaben

Die Mengen  $M'$ ,  $M''$  und  $M_k$  ( $k \in \mathbb{N}$ ) seien wie folgt definiert:

$$M' := \{1, 3, 5, 7\}, \quad M'' := \{2, 3, 7, 11\}, \quad M_k := \{-k, -k+1, \dots, 0, \dots, k-1, k\}$$

**Aufgabe 2.1**



**Webcode 2859**

Bestimmen Sie die Menge  $M$  mit

- |                      |                           |                  |                                     |
|----------------------|---------------------------|------------------|-------------------------------------|
| a) $M = M' \cup M''$ | c) $M = M' \setminus M''$ | e) $M = 2^{M_1}$ | g) $M = \bigcup_{k=1}^{\infty} M_k$ |
| b) $M = M' \cap M''$ | d) $M = M'' \setminus M'$ | f) $M = 2^{M_2}$ | h) $M = \bigcap_{k=1}^{\infty} M_k$ |

$R_1$  und  $R_2$  seien wie folgt definiert:

$$R_1 := \{(2, 1), (3, 1), (4, 1), \dots, (3, 2), (4, 2), (5, 2), \dots, (4, 3), (5, 3), (6, 3), \dots\}$$

$$R_2 := \{(1, 2), (1, 3), (1, 4), \dots, (2, 3), (2, 4), (2, 5), \dots, (3, 4), (3, 5), (3, 6), \dots\}$$

**Aufgabe 2.2**



**Webcode 2339**

Welche bekannten Relationen verbergen sich hinter

- |          |          |                   |                              |
|----------|----------|-------------------|------------------------------|
| a) $R_1$ | b) $R_2$ | c) $R_1 \cup R_2$ | d) $\overline{R_1 \cup R_2}$ |
|----------|----------|-------------------|------------------------------|

Mengen sind von Natur aus ungeordnet und können ein und dasselbe Elemente immer nur einmal enthalten.

- a) Wie lassen sich trotzdem geordnete Folgen von Elementen darstellen, in denen Elemente doppelt vorkommen dürfen?
- b) Codieren Sie die Folge  $<1, 1, 2, 3, 4, 4>$  nach dem entwickelten Schema.

**Aufgabe 2.3**



**Webcode 2688**

Die Menge der *komplexen Zahlen*  $\mathbb{C}$  ist eine Erweiterung der Menge der reellen Zahlen  $\mathbb{R}$ . Eine komplexe Zahl  $c \in \mathbb{C}$  besteht aus einem *Realanteil*  $x \in \mathbb{R}$  und einem *Imaginäranteil*  $y \in \mathbb{R}$  und wird in der Form  $c = x + y \cdot i$  notiert.  $i$  heißt die *imaginäre Einheit* und erfüllt die Eigenschaft  $i^2 = -1$ . In der Menge der komplexen Zahlen lässt sich gewohnt rechnen:

$$(3 + 2i) + (5 + 7i) = (3 + 5) + (2 + 7)i = 8 + 9i$$

$$(3 + 2i) \cdot (5 + 7i) = 15 + 21i + 10i + 14 \cdot i^2 = 1 + 31i$$

**Aufgabe 2.4**

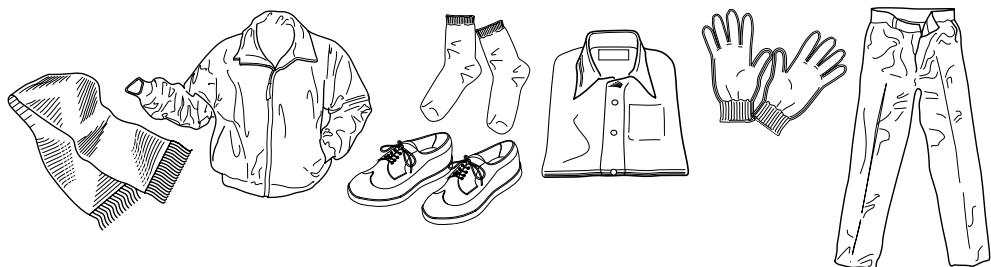


**Webcode 2195**

Zeigen oder widerlegen Sie, dass  $\mathbb{R}$  und  $\mathbb{C}$  die gleiche Kardinalität besitzen.

**Aufgabe 2.5****Webcode  
2904**

Bilden Sie über der folgenden Menge von Gegenständen eine Ordnungsrelation  $R$ . Diese soll ausdrücken, in welcher Reihenfolge Sie die Kleidungsstücke anlegen müssen, um ordentlich angezogen das Haus zu verlassen:



Ist die von Ihnen erzeugte „Kleiderordnung“ partiell oder total?

**Aufgabe 2.6****Webcode  
2909**

Sei  $M$  eine endliche Menge mit  $n$  Elementen. Die Anzahl der Möglichkeiten,  $M$  in  $k$  Äquivalenzklassen zu unterteilen, wird durch die *Stirling-Zahl*  $S(n, k)$  beschrieben. Sie ist nach dem schottischen Mathematiker James Stirling benannt.

- Wie viele Möglichkeiten existieren, um 2-elementige, 3-elementige und 4-elementige Mengen in 2 Klassen einzuteilen? Mit anderen Worten: Bestimmen Sie die Stirling-Zahlen  $S(n, 2)$  für  $2 \leq n \leq 4$ .
- Für beliebige Werte  $n, k \in \mathbb{N}$  mit  $n \geq k$  lässt sich die Stirling-Zahl mit Hilfe der folgenden Formel berechnen:

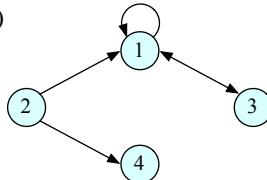
$$S(n, k) = \frac{1}{k!} \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} i^n \quad (2.86)$$

Werten Sie die Formel für alle  $n, k$  mit  $1 \leq k \leq 4$  und  $k \leq n \leq 8$  aus und tragen Sie die Funktionswerte in die folgende Tabelle ein. Verwenden Sie die ausgefüllte Tabelle, um Ihre Ergebnisse aus Teilaufgabe a) zu verifizieren.

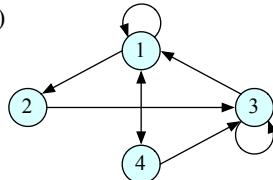
	$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$k = 1$								
$k = 2$								
$k = 3$								
$k = 4$								

Gegeben seien die folgenden Relationen:

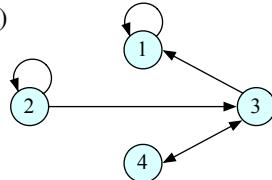
1)



2)



3)

**Aufgabe 2.7****Webcode  
2184**

a) Ordnen Sie jedem Relationengraphen eine der folgenden Adjazenzmatrizen zu:

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

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

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

b) Berechnen Sie für jede Relation die reflexiv transitive Hülle.

Die Kreiszahl  $\pi$  und die Euler'sche Konstante  $e$  sind irrational, d. h., wir können ihren Wert in Dezimalbruchschreibweise nur annähern. Um sie exakt niederzuschreiben, müsste dieses Buch unendlich viele Seiten besitzen. Aus pragmatischen Gründen wollen wir uns deshalb mit der Angabe der ersten 8 Nachkommastellen begnügen:

$$\pi = 3,14159265\dots$$

$$e = 2,71828182\dots$$

Bis heute ist nicht bekannt, ob die Summe  $\pi + e$  bzw. die Differenz  $\pi - e$  ebenfalls irrational ist. Zeigen Sie, dass zumindest eine der beiden Zahlen irrational sein muss.

Werten Sie die folgenden beiden Ausdrücke aus:

$$3^{(3^3)} =$$

$$(3^3)^3 =$$

**Aufgabe 2.9****Webcode  
2390**

Welcher Wert entspricht dem Ausdruck  $3 \uparrow^2 3$ ?

**Aufgabe 2.10****Webcode  
2955**

Gegeben seien die folgenden Mengen:

- |                     |                       |                       |                        |
|---------------------|-----------------------|-----------------------|------------------------|
| 1) $\mathbb{N}$     | 4) $2^{\mathbb{N}^2}$ | 7) $2^{\mathbb{Q}}$   | 10) $\mathbb{R}^2$     |
| 2) $\mathbb{N}^2$   | 5) $\mathbb{Q}$       | 8) $2^{\mathbb{Q}^2}$ | 11) $2^{\mathbb{R}}$   |
| 3) $2^{\mathbb{N}}$ | 6) $\mathbb{Q}^2$     | 9) $\mathbb{R}$       | 12) $2^{\mathbb{R}^2}$ |

- a) Welche der genannten Mengen sind gleichmächtig?  
 b) Ordnen Sie die Mengen entsprechend ihrer Kardinalität hierarchisch an.

**Aufgabe 2.11****Webcode  
2786**

Mit der *Cantor'schen Paarungsfunktion*  $\pi_{\mathbb{N}}$  haben Sie eine bijektive Abbildung  $\mathbb{N} \rightarrow \mathbb{N}^2$  kennengelernt und damit die Gleichmächtigkeit beider Mengen bewiesen. Dass die angegebene Definition von  $\pi_{\mathbb{N}}$  nicht die einzige Möglichkeit ist,  $\mathbb{N}$  bijektiv auf  $\mathbb{N}^2$  abzubilden, zeigt die folgende Zuordnungsvorschrift.

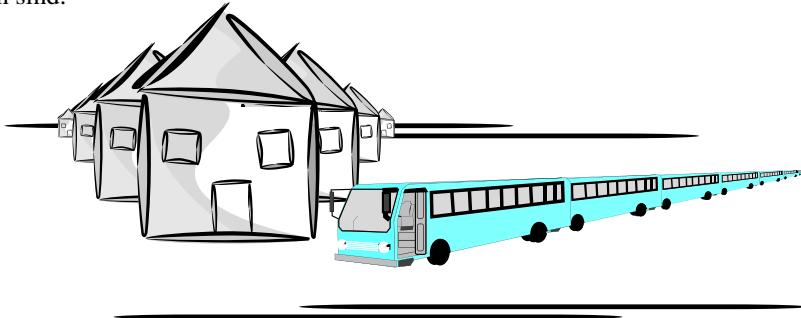
	1	2	3	4	5	6	7	8	9	...
1	1	3	5	7	9	11	13	15	17	...
2	2	6	10	14	18	22	26	30		...
3	4	12	20	28	36	44	52			...
4	8	24	40	56	72	88				...
5	16	48	80	112	144					...
6	32	96	160	224						...
7	64	192	320							...
8	128	384								...
9	256									...
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Finden Sie eine geschlossene mathematische Formel für die dargestellte Funktion.

Stellen Sie sich vor, Sie sind der neue Pächter von Hilberts Hotel. Wie immer sind alle der unendlich vielen Zimmer restlos ausgebucht. Eines Tages hält *Hilberts Bus* vor Ihrem Hotel. Dieser verfügt über unendlich viele Sitzplätze, die alle mit einer eindeutigen Nummer  $i \in \mathbb{N}$  versehen sind.

**Aufgabe 2.12**

**Webcode**  
**2532**

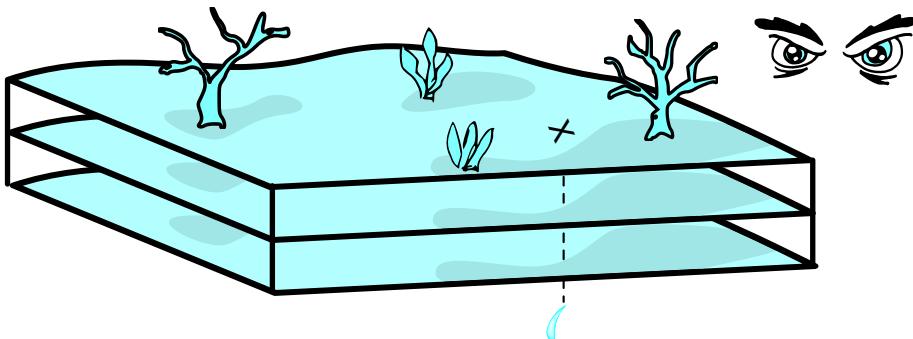


- Zu Ihrem Schrecken stellen Sie fest, dass der Bus vollständig besetzt ist. Beweisen Sie Ihr großes Organisationstalent und bringen Sie trotzdem alle neu angereisten Gäste in Ihrem Hotel unter. Welches Zimmer darf der Passagier auf dem  $i$ -ten Sitzplatz beziehen?
- Die Güte Ihres Hotels spricht sich schnell herum und so dauert es nicht lange, bis eines Tages unendlich viele Hilbert-Busse gleichzeitig ihre Gäste vor Ihrem Haus abliefern. Auch hier trägt jeder Bus eine eindeutige Nummer  $j \in \mathbb{N}$ . Können Sie den großen Andrang immer noch bewältigen und alle Gäste aufnehmen?

Sie stehen inmitten der fiktiven *Hilbert-Wüste*, die sich in alle Richtungen unendlich weit ausbreitet. Sie wissen um die Existenz eines  $1 \text{ km} \times 1 \text{ km}$  großen Ölfelds, das sich an einer unbekannten Stelle in unbekannter Tiefe unter dem Wüstenboden verbirgt.

**Aufgabe 2.13**

**Webcode**  
**2839**



Geben Sie eine Methode an, mit der Sie das Ölfeld in endlicher Zeit finden werden!

**Aufgabe 2.14****Webcode  
2422**

Vorsicht bei Induktionsbeweisen! Die vollständige Induktion verfolgt ein einfaches Grundprinzip, ihre Anwendung sollte jedoch stets mit Bedacht geschehen. So lässt sich die Aussage

*„Wenn sich unter  $n$  Pferden ein Schimmel befindet, dann sind alle Pferde Schimmel.“*

augenscheinlich mit Hilfe der vollständigen Induktion beweisen. Im Induktionsanfang zeigen wir die Aussage für  $n = 1$ . Besteht eine Gruppe aus einem einzigen Pferd und ist darin ein Schimmel enthalten, so sind offensichtlich alle Pferde dieser Gruppe Schimmel. Kurzum: Die Aussage ist für  $n = 1$  richtig.

Jetzt nehmen wir als Induktionsvoraussetzung an, die Aussage sei für eine Gruppe von  $n$  Pferden richtig und zeigen im Induktionsschritt, dass die Aussage dann auch für Gruppen von  $n + 1$  Pferden gilt. Zunächst wissen wir, dass sich in der Gruppe von  $n + 1$  Pferden (mindestens) ein Schimmel befindet. Wir stellen nun alle Pferde derart in einer Reihe auf, dass ein Schimmel ganz vorne steht:



Jetzt betrachten wir die Gruppe der ersten  $n$  Pferde. Da unsere Aussage für  $n$  per Induktionsannahme richtig ist und ein Schimmel in dieser Gruppe ist, so müssen alle anderen Pferde dieser Gruppe ebenfalls Schimmel sein und wir erhalten das folgende Zwischenergebnis:



Jetzt können wir die Induktionsvoraussetzung auch auf die letzten  $n$  Pferde anwenden, da sich unter diesen auf jeden Fall auch mindestens ein Schimmel befindet:



Voilà: Alle Pferde sind Schimmel!

Selbstverständlich ist die bewiesene Aussage nicht richtig – Induktion hin oder her. Analysieren Sie die vorgebrachten Argumente und finden Sie den Fehler in der Beweiskette.

Wir wollen in dieser Aufgabe das Hofstadter'sche MIU-System aus dem Übungsteil des ersten Kapitels wieder aufgreifen. Zur Erinnerung: Das MIU-System war durch ein einzelnes Axiom und vier Schlussregeln bestimmt:

**Aufgabe 2.15**
**Webcode  
2657**

## ■ Axiome

1. **MI** ist ein Satz

## ■ Schlussregeln

1. Mit **xI** ist auch **xIU** ein Satz
2. Mit **Mx** ist auch **Mxx** ein Satz
3. In jedem Satz darf **III** durch **U** ersetzt werden
4. In jedem Satz darf **UU** entfernt werden

Die rekursive Definition des MIU-Systems ermöglicht uns, Aussagen über alle ableitbaren Sätze mit dem Prinzip der strukturellen Induktion zu beweisen.

- a) Zeigen Sie durch strukturelle Induktion, dass alle ableitbaren Wörter die Eigenschaft erfüllen, dass die Anzahl der **I**'s nicht durch drei teilbar ist.
- b) Falls Sie die Übungsaufgabe des ersten Einführungskapitels nicht vollständig lösen konnten, versuchen Sie es erneut. Verwenden Sie die in Teilaufgabe a) gewonnene Erkenntnis.

In der praktischen Informatik spielen fast ausschließlich diejenigen Rekursionsvorschriften eine Rolle, die nach endlich vielen Schritten terminieren. Ob eine rekursiv definierte Funktion diese Eigenschaft besitzt, ist nicht immer so einfach zu erkennen wie in den bisher diskutierten Beispielen. Um das Gesagte zu verdeutlichen, betrachten wir die *Collatz-Funktion*  $c : \mathbb{N} \rightarrow \mathbb{N}_0$ , die folgendermaßen definiert ist:

$$c(n) = \begin{cases} 0 & \text{falls } n = 1 \\ 1 + c\left(\frac{n}{2}\right) & \text{falls } n > 0, n \text{ gerade} \\ 1 + c(3 \cdot n + 1) & \text{falls } n > 0, n \text{ ungerade} \end{cases}$$

- a) Berechnen Sie die Funktionswerte  $c(3)$ ,  $c(7)$  und  $c(27)$ .
- b) Terminiert die Rekursion Ihrer Meinung nach für alle  $n \in \mathbb{N}$ ?

**Aufgabe 2.16**
**Webcode  
2249**

**Aufgabe 2.17**

Der *Binomialkoeffizient* ist wie folgt definiert:



**Webcode  
2886**

$$\binom{n}{k} := \frac{n!}{k! \cdot (n-k)!} \quad (2.87)$$

a) Beweisen Sie das folgende Additionstheorem:

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \quad (2.88)$$

b) Der *binomische Lehrsatz* lautet wie folgt:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k, \quad a, b \in \mathbb{R}, n \in \mathbb{N} \quad (2.89)$$

Beweisen Sie den Lehrsatz durch vollständige Induktion.

**Aufgabe 2.18**

Im Jahre 1843 veröffentlichte der französische Mathematiker Jacques Philippe Marie Binet die folgende Formel:



**Webcode  
2963**

$$f_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right] \quad (2.90)$$

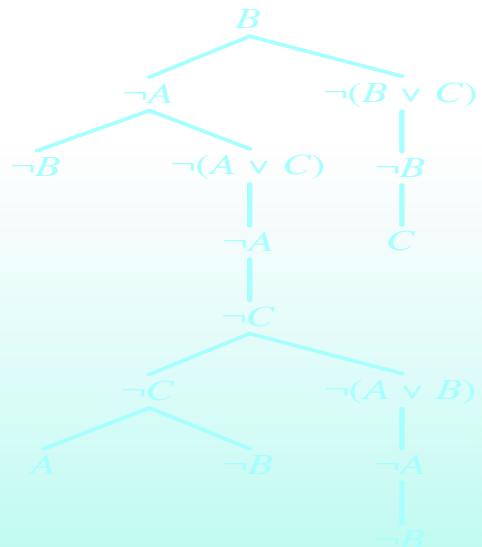
Zeigen Sie, dass die Binet-Funktion  $f_n$  für alle  $n \in \mathbb{N}$  die nachstehende Rekursionsgleichung erfüllt:

$$f_{n+2} = f_{n+1} + f_n \quad (2.91)$$

### 3 Logik und Deduktion

In diesem Kapitel werden Sie ...

- mit der Aussagenlogik die Grundlagen des logischen Schließens erlernen,
- formale Beweise im Hilbert-Kalkül führen,
- mit dem Resolutions- und dem Tableaukalkül zwei Widerspruchskalküle kennen lernen,
- die Aussagenlogik zur Prädikatenlogik erster Stufe erweitern,
- die Grundprinzipien der logischen Programmierung verstehen,
- einen Einblick in Logiken höherer Stufe erlangen.



■ Frühere Schreibweise

Formel	Schreibweise
$\neg A$	$\sim A$
$A \wedge B$	$A . B$
$A \vee B$	$A \vee B$
$A \rightarrow B$	$A \supset B$

■ Punkt-Strich-Notation

Formel	Schreibweise
$\neg A$	$\neg A, \bar{A}$
$A \wedge B$	$A \cdot B, AB$
$A \vee B$	$A + B$
$A \rightarrow B$	$A \rightarrow B$

**Abbildung 3.1:** Alternative Schreibweisen aussagenlogischer Formeln

■ Drei Formeln der Principia...

- \*203.  $\vdash p \supset \neg q . \neg q \supset \neg p$
- \*215.  $\vdash : \neg p \supset q . \neg q \supset p$
- \*216.  $\vdash : p \supset q . \neg q \supset \neg p$
- \*217.  $\vdash : \neg q \supset \neg p . \neg p \supset q$

■ ...und deren moderne Schreibweise

- (2.03)  $\vdash (p \rightarrow \neg q) \rightarrow (\neg q \rightarrow \neg p)$
- (2.15)  $\vdash (\neg p \rightarrow q) \rightarrow (\neg q \rightarrow p)$
- (2.16)  $\vdash (p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$
- (2.17)  $\vdash (\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$

**Abbildung 3.2:** In der Notation der Principia besitzt der Punkt eine Doppelbedeutung. In Abhängigkeit von seiner Position wird er für die konjunktive Verknüpfung oder zum Klammern von Teilausdrücken verwendet. Die Abbildung zeigt drei Formeln aus der Originalausgabe der Principia Mathematica sowie deren Übersetzung in die heute übliche Schreibweise.

## 3.1 Aussagenlogik

Die Aussagenlogik (PL0) ist die einfachste Spielart des logischen Schließens. Gegenstand der Aussagenlogik sind *atomare Aussagen* („Es regnet“, „Die Straße ist nass“) und die Beziehungen, die zwischen solchen Aussagen bestehen („Wenn es regnet, dann ist die Straße nass“). Sie besticht durch eine einfachen Aufbau und eine klare Struktur, kommt jedoch nicht an die Ausdrucksstärke der anderen hier vorgestellten Logiken heran. Trotzdem ist die Bedeutung der Aussagenlogik beträchtlich. Zum einen ist sie die theoretische Grundlage des Hardware-Entwurfs, da sich das Verhalten einer kombinatorischen Hardware-Schaltung auf der Logikebene eins zu eins auf eine aussagenlogische Formel abbilden lässt. Zum anderen ist sie als Teilmenge in allen anderen Logiken enthalten und damit der kleinste gemeinsame Nenner, über den alle Logiken miteinander verbunden sind.

### 3.1.1 Syntax und Semantik

Wir nähern uns der Aussagenlogik in zwei Schritten. Zunächst fixieren wir die *Syntax*, d. h., wir definieren, nach welchen Regeln aussagenlogische Ausdrücke (Formeln) aufgebaut sind. Eine Formel ist in diesem Stadium nichts weiter als eine Folge von bedeutungsleeren Symbolen, die in einer festgelegten Art und Weise miteinander kombiniert werden dürfen. Erst die *Semantik* versieht die Ausdrücke mit einer Bedeutung; sie legt fest, wie wir die unterschiedlichen Zeichen und Symbolen einer Logikformel zu interpretieren haben.



#### Definition 3.1 (Syntax der Aussagenlogik)

Die Menge der *aussagenlogischen Formeln* über dem Variablenvorrat  $V = \{A_1, A_2, \dots\}$  ist rekursiv definiert:

- Die booleschen Wahrheitswerte 0 und 1 sind Formeln.
- Jede Variable  $A_i \in V$  ist eine Formel.
- Sind  $F$  und  $G$  Formeln, dann sind es auch

$$(\neg F), (F \wedge G), (F \vee G), (F \rightarrow G), (F \leftrightarrow G), (F \Leftrightarrow G)$$

Der Operator  $\neg$  ist die *Negation*,  $\wedge$  die *Konjunktion (UND-Operator)*,  $\vee$  die *Disjunktion (ODER-Operator)* und  $\rightarrow$  die *Implikation*. Ferner be-

zeichnen wir  $\leftrightarrow$  als *Äquivalenz*- und  $\leftrightarrow$  als *Antivalenzoperator (XOR-Operator)*. Auch wenn die Namen bereits deutliche Hinweise geben, mit welcher Semantik wir die einzelnen Operatoren später belegen werden, sollten Sie versuchen, eine Formel zunächst als eine Aneinanderreihung von Symbolen zu betrachten, die noch keine konkrete Bedeutung besitzt.

Eine Formel  $F$ , die nicht weiter zerlegt werden kann, nennen wir *atomar*. In der Aussagenlogik ist die Menge der atomaren Formeln mit der Menge  $V \cup \{0, 1\}$  identisch. Ist  $F$  eine zusammengesetzte Formel, so bezeichnen wir seine Bestandteile als *Teiformeln*. Wir verwenden die etwas informelle Notation  $F \in G$ , um auszudrücken, dass  $F$  eine Teilformel von  $G$  ist; andernfalls schreiben wir  $F \notin G$ . Variablen werden wir im Folgenden durchweg mit Großbuchstaben bezeichnen, allerdings von Fall zu Fall den Symbolvorrat anpassen (z. B.  $X, Y, Z$  anstelle von  $A_1, A_2, A_3$ ).

Für die eingeführten Operatoren existiert keine einheitliche Notation. Zum einen wurde die Schreibweise in der Vergangenheit mehrfach geändert, zum anderen ist sie auch heute noch regional verschieden. Im oberen Teil von Abbildung 3.1 sind die Symbole zusammengefasst, wie sie zu Beginn des zwanzigsten Jahrhunderts üblich waren und zum Verständnis alter Forschungsbeiträge notwendig sind (vgl. Abbildung 3.2). Der untere Teil enthält die Symbole, wie sie insbesondere im US-amerikanischen Sprachraum verwendet werden. Die Notation  $\bar{A}$  für  $\neg A$  hat sich auch im deutschen Sprachraum etabliert, da sie für viele Ausdrücke zu einer übersichtlicheren Darstellung führt.

Um die Lesbarkeit zu verbessern, werden wir auf die Angabe mancher Klammerpaare verzichten. Mehrdeutigkeiten werden, wie in Abbildung 3.3 gezeigt, über eine Reihe von Bindungs- und Kettenregeln beseitigt. Bindungsregeln teilen die Operatoren in schwächer bindende und stärker bindende Operatoren ein, Kettenregeln bestimmen den Umgang mit Ausdrücken, in denen der gleiche Operator mehrmals hintereinander vorkommt. Wir legen die übliche Konvention zugrunde, dass die Negation ( $\neg$ ) stärker bindet als die Konjunktion ( $\wedge$ ). Diese bindet wiederum stärker als die Disjunktion ( $\vee$ ). Die Operatoren  $\rightarrow$ ,  $\leftrightarrow$  und  $\leftrightarrow$  binden am schwächsten. Kommen sie in einem Ausdruck gemischt vor, erfolgt die Klammerung linksassoziativ. Werden Teilterme mit demselben Operator verknüpft, betrachten wir die entstehende Kette ebenfalls als linksassoziativ geklammert. Die einzige Ausnahme bildet der (einstellige) Negationsoperator, den wir rechtsassoziativ gruppieren.

Die zweistelligen Operatoren  $\wedge$  und  $\vee$  lassen sich auf natürliche Weise zu mehrstelligen Operatoren verallgemeinern. Hierzu vereinbaren wir

### Bindungsregeln

Ausdruck	Bedeutung
$\neg A \wedge B$	$((\neg A) \wedge B)$
$A \vee B \wedge C$	$(A \vee (B \wedge C))$
$A \vee B \rightarrow C$	$((A \vee B) \rightarrow C)$
$A \rightarrow B \leftrightarrow C$	$((A \rightarrow B) \leftrightarrow C)$
$A \leftrightarrow B \rightarrow C$	$((A \leftrightarrow B) \rightarrow C)$

### Kettenregeln

Ausdruck	Bedeutung
$\neg\neg\neg A$	$\neg(\neg(\neg A))$
$A \wedge B \wedge C$	$(A \wedge B) \wedge C$
$A \vee B \vee C$	$(A \vee B) \vee C$
$A \rightarrow B \rightarrow C$	$(A \rightarrow B) \rightarrow C$
$A \leftrightarrow B \leftrightarrow C$	$(A \leftrightarrow B) \leftrightarrow C$
$A \leftrightarrow B \leftrightarrow C$	$(A \leftrightarrow B) \leftrightarrow C$

**Abbildung 3.3:** Zur Vereinfachung der Schreibweise dürfen Klammerpaare weggelassen werden. Zweideutigkeiten werden mit Hilfe von Bindungs- und Kettenregeln beseitigt. Erstere teilen die Operatoren in schwächer bindende und stärker bindende Operatoren ein, Letztere regeln den Umgang mit Ausdrücken, in denen der gleiche Operator mehrmals hintereinander vorkommt.

■ Erste Interpretation

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

$$\begin{array}{l} A \rightarrow 0 \\ B \rightarrow 0 \end{array}$$

$$(\neg 0 \rightarrow \neg 0) \wedge ((0 \rightarrow 0) \vee (0 \rightarrow 0))$$

■ Zweite Interpretation

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

$$\begin{array}{l} A \rightarrow 1 \\ B \rightarrow 0 \end{array}$$

$$(\neg 1 \rightarrow \neg 0) \wedge ((0 \rightarrow 1) \vee (1 \rightarrow 0))$$

■ Dritte Interpretation

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

$$\begin{array}{l} A \rightarrow 0 \\ B \rightarrow 1 \end{array}$$

$$(\neg 0 \rightarrow \neg 1) \wedge ((1 \rightarrow 0) \vee (0 \rightarrow 1))$$

■ Vierte Interpretation

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

$$\begin{array}{l} A \rightarrow 1 \\ B \rightarrow 1 \end{array}$$

$$(\neg 1 \rightarrow \neg 1) \wedge ((1 \rightarrow 1) \vee (1 \rightarrow 1))$$

**Abbildung 3.4:** Eine Interpretation  $I$  ordnet jeder aussagenlogischen Variablen einen der beiden Wahrheitswerte 0 (*falsch*) oder 1 (*wahr*) zu. Die Anzahl möglicher Interpretationen ist für jede aussagenlogische Formel endlich. Bezeichnet  $n$  die Anzahl der Variablen, so existieren  $2^n$  verschiedene Möglichkeiten, diese mit den Wahrheitswerten 0 und 1 zu belegen.

für die endlich vielen Formeln  $F_1, \dots, F_n$  die folgende Schreibweise:

$$\left( \bigwedge_{i=1}^n F_i \right) := F_1 \wedge \dots \wedge F_n \quad \left( \bigvee_{i=1}^n F_i \right) := F_1 \vee \dots \vee F_n \quad (3.1)$$

Die Semantik einer aussagenlogischen Formel wird über die *Modellrelation*  $\models$  festgelegt. Um diese formal definieren zu können, müssen wir vorab klären, was wir unter dem Begriff der *Interpretation* zu verstehen haben:



### Definition 3.2 (Interpretation)

Sei  $F$  eine aussagenlogische Formel.  $A_1, \dots, A_n$  bezeichnen die in  $F$  vorkommenden Variablen. Jede Abbildung

$$I : \{A_1, \dots, A_n\} \rightarrow \{0, 1\}$$

heißt eine *Interpretation* von  $F$ .

Eine Interpretation ordnet jeder Variablen einer aussagenlogischen Formel  $F$  einen der beiden Wahrheitswerte 0 oder 1 zu und wird aufgrund dieser Eigenschaft auch als *Belegung* bezeichnet (vgl. Abbildung 3.4). Mit dem Begriff der Interpretation haben wir die Grundlage geschaffen, um die Semantik der Aussagenlogik formal zu definieren:



### Definition 3.3 (Semantik der Aussagenlogik)

$F$  und  $G$  seien aussagenlogische Formeln und  $I$  eine Interpretation. Die Semantik der Aussagenlogik ist durch die *Modellrelation*  $\models$  gegeben, die induktiv über den Formelaufbau definiert ist:

$$\begin{aligned} I \models 1 \\ I \not\models 0 \\ I \models A_i :\Leftrightarrow I(A_i) = 1 \\ I \models (\neg F) :\Leftrightarrow I \not\models F \\ I \models (F \wedge G) :\Leftrightarrow I \models F \text{ und } I \models G \\ I \models (F \vee G) :\Leftrightarrow I \models F \text{ oder } I \models G \\ I \models (F \rightarrow G) :\Leftrightarrow I \not\models F \text{ oder } I \models G \\ I \models (F \leftrightarrow G) :\Leftrightarrow I \models F \text{ genau dann, wenn } I \models G \\ I \models (F \Leftrightarrow G) :\Leftrightarrow I \not\models (F \leftrightarrow G) \end{aligned}$$

Eine Interpretation  $I$  mit  $I \models F$  heißt *Modell* für  $F$ .

Wir können jede aussagenlogische Formel  $F$  mit  $n$  Variablen als *boolesche Funktion*  $f^F : \{0, 1\}^n \rightarrow \{0, 1\}$  auffassen, die für eine Belegung  $I$  genau dann zu 1 evaluiert, wenn  $I$  ein Modell für  $F$  ist. Mit anderen Worten: Weist  $I$  den Variablen  $A_1, \dots, A_n$  die Wahrheitswerte  $b_1, \dots, b_n$  zu, dann ist der Funktionswert  $f^M(b_1, \dots, b_n)$  durch die folgende Formel bestimmt:

$$f^F(b_1, \dots, b_n) = \begin{cases} 1 & \text{falls } I \models F \\ 0 & \text{falls } I \not\models F \end{cases} \quad (3.2)$$

Aufgrund des diskreten Definitionsbereichs lässt sich eine  $n$ -stellige boolesche Funktion in Form einer *Wahrheitstabelle* darstellen, indem alle möglichen Kombinationen der Eingangsvariablen  $A_1, \dots, A_n$  zusammen mit dem zugeordneten Funktionswert zeilenweise aufgelistet werden. Als Beispiele zeigt Abbildung 3.5 die Wahrheitstabellen der eingeführten aussagenlogischen Operatoren. Die Funktionswerte erschließen sich unmittelbar aus Definition 3.3. Wahrheitstabellen werden in der Literatur auch als *Wahrheitstafeln* oder *Funktions(wert)tabellen* bezeichnet; alle diese Begriffe bezeichnen die tabellarische Beschreibungsweise einer booleschen Funktion.

Abbildung 3.6 zeigt, wie sich Wahrheitstabellen für zusammengesetzte Ausdrücke erzeugen lassen. Ausgehend von den Basistermen werden zunächst die Teilformeln und anschließend der Gesamtausdruck ausgewertet. Die drei Beispiele wurden bewusst gewählt. Die Formel  $F_1$  ist so beschaffen, dass sie genau zwei Modelle besitzt; sie evaluiert genau dann zu 1, wenn die Variablen  $A, B, C$  mit dem gleichen Wahrheitswert belegt werden. In der Terminologie der Aussagenlogik wird die Funktion als *erfüllbar* bezeichnet.  $F_2$  ist ebenfalls erfüllbar, besitzt aber im Gegensatz zu  $F_1$  die Eigenschaft, dass ausnahmslos alle Variablenbelegungen ein Modell sind. Solche Formeln heißen *allgemeingültig*. In entsprechender Weise bezeichnen wir  $F_3$  als *unerfüllbare* Formel, da sie kein einziges Modell besitzt. Formal halten wir das Gesagte in der folgenden Definition fest:



#### Definition 3.4 (Erfüllbarkeit, Allgemeingültigkeit)

Eine aussagenlogische Formel  $F$  heißt

- *erfüllbar*, falls  $F$  mindestens ein Modell besitzt,
- *unerfüllbar*, falls  $F$  kein Modell besitzt,
- *allgemeingültig*, falls  $\neg F$  unerfüllbar ist.

Eine allgemeingültige Formel bezeichnen wir auch als *Tautologie*.

#### Negation

	$A$	$\neg A$
0	0	1
1	1	0

#### Konjunktion

	$A$	$B$	$A \wedge B$
0	0	0	0
1	0	1	0
2	1	0	0
3	1	1	1

#### Disjunktion

	$A$	$B$	$A \vee B$
0	0	0	0
1	0	1	1
2	1	0	1
3	1	1	1

#### Implikation

	$A$	$B$	$A \rightarrow B$
0	0	0	1
1	0	1	1
2	1	0	0
3	1	1	1

#### Äquivalenz

	$A$	$B$	$A \leftrightarrow B$
0	0	0	1
1	0	1	0
2	1	0	0
3	1	1	1

#### Antivalenz

	$A$	$B$	$A \leftrightarrow B$
0	0	0	0
1	0	1	1
2	1	0	1
3	1	1	0

Abbildung 3.5: Wahrheitstabellen der aussagenlogischen Basisoperatoren

■ Beispiel 1:  $F_1 = \underbrace{(\overline{A} \vee B)}_{G_1} \wedge \underbrace{(\overline{B} \vee C)}_{G_2} \wedge \underbrace{(\overline{C} \vee A)}_{G_3}$

$$\underbrace{\quad\quad\quad}_{G_4}$$

A	B	C	$G_1$	$G_2$	$G_3$	$G_4$	$F_1$
0	0	0	1	1	1	1	1
0	0	1	1	1	0	1	0
0	1	0	1	0	1	0	0
0	1	1	1	1	0	1	0
1	0	0	0	1	1	0	0
1	0	1	0	1	1	0	0
1	1	0	1	0	1	0	0
1	1	1	1	1	1	1	1

■ Beispiel 2:  $F_2 = \underbrace{((A \rightarrow B) \wedge (B \rightarrow C))}_{G_1} \rightarrow \underbrace{(A \rightarrow C)}_{G_3}$

$$\underbrace{\quad\quad\quad}_{G_4}$$

A	B	C	$G_1$	$G_2$	$G_3$	$G_4$	$F_2$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	1	0	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	1	0	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

■ Beispiel 3:  $F_3 = \underbrace{(A \leftrightarrow B)}_{G_1} \wedge \underbrace{(A \leftrightarrow C)}_{G_2} \wedge \underbrace{(B \leftrightarrow C)}_{G_3}$

$$\underbrace{\quad\quad\quad}_{G_4}$$

A	B	C	$G_1$	$G_2$	$G_3$	$G_4$	$F_3$
0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0
0	1	0	1	0	1	0	0
0	1	1	1	1	0	1	0
1	0	0	1	1	0	1	0
1	0	1	1	0	1	0	0
1	1	0	0	1	1	0	0
1	1	1	0	0	0	0	0

Abbildung 3.6: Wahrheitstabellen zusammengesetzter Funktionen

Abbildung 3.7 demonstriert den Zusammenhang zwischen den eingeführten Begriffen. Alle drei lassen sich in naheliegender Weise auf Mengen von aussagenlogischen Formeln erweitern. Die Formelmenge  $M = \{F_1, \dots, F_n\}$  heißt erfüllbar, wenn eine Interpretation  $I$  existiert, die für alle  $F_i \in M$  ein Modell ist. Beachten Sie, dass das Modell für alle Formeln das gleiche sein muss; es reicht also nicht aus, dass jede Formel

für sich erfüllbar ist. Die Unerfüllbarkeit und Allgemeingültigkeit von Formelmengen definieren wir analog.  $M$  ist unerfüllbar, wenn  $F_1, \dots, F_n$  kein gemeinsames Modell besitzen. Ist dagegen jede Interpretation ein Modell für die Elemente von  $M$ , so nennen wir  $M$  allgemeingültig.

Mit Hilfe der Modellrelation können wir den Begriff der *logischen Folgerung* formal definieren:



### Definition 3.5 (Logische Folgerung)

$M := \{F_1, \dots, F_n\}$  sei eine Menge aussagenlogischer Formeln. Wir schreiben

$$M \models G \quad (\text{„aus } M \text{ folgt } G“}),$$

wenn jedes Modell von  $M$  auch ein Modell der aussagenlogischen Formel  $G$  ist. Ferner vereinbaren wir die Kurzschreibweise  $\models G$  für  $\emptyset \models G$  und  $F \models G$  für  $\{F\} \models G$ .

Offensichtlich gelten die folgenden Zusammenhänge:

- $\models G$  gilt genau dann, wenn  $G$  allgemeingültig ist.
- $F \models G$  gilt genau dann, wenn  $F \rightarrow G$  allgemeingültig ist.
- $\{F_1, F_2, \dots, F_n\} \models G$  ist äquivalent zu  $\{F_2, \dots, F_n\} \models F_1 \rightarrow G$ .

In den kommenden Betrachtungen wird der Begriff der *Äquivalenz* immer wieder auftauchen:



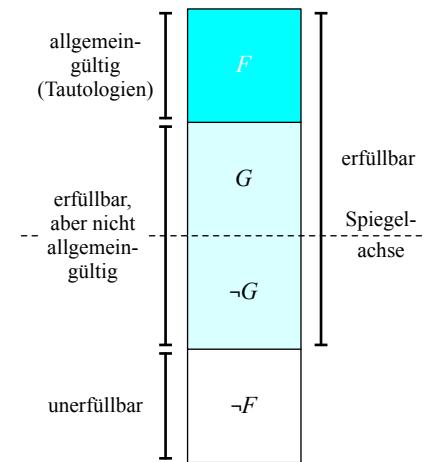
### Definition 3.6 (Äquivalenz)

Seien  $F$  und  $G$  zwei aussagenlogische Formeln. Die Relation  $\equiv$  ist wie folgt definiert:

$$F \equiv G \quad :\Leftrightarrow \quad F \models G \text{ und } G \models F$$

Zwei Formeln  $F$  und  $G$  mit  $F \equiv G$  heißen *äquivalent*.

Damit sind zwei Formeln  $F$  und  $G$  genau dann äquivalent, geschrieben als  $F \equiv G$ , falls sie exakt dieselben Modelle besitzen. Im mathematischen Sinne ist  $\equiv$  eine Äquivalenzrelation auf der Menge der aussagenlogischen Formeln und besitzt die Eigenschaften der Reflexivität, Symmetrie und Transitivität:



**Abbildung 3.7:** Das Spiegelungsprinzip visualisiert, wie sich die Eigenschaften der Formeln  $F$  und  $\neg F$  gegenseitig beeinflussen. Ist  $F$  allgemeingültig, so ist  $\neg F$  unerfüllbar. Ist  $F$  nicht allgemeingültig, aber dennoch erfüllbar, so gilt das Gleiche für  $\neg F$ . Damit ist die Allgemeingültigkeit eine exklusive Eigenschaft, die nur eine der beiden Formeln  $F$  oder  $\neg F$  erfüllen kann. Im Gegensatz hierzu können sowohl  $F$  als auch  $\neg F$  erfüllbar sein.

Idempotenz	De Morgan'sche Regeln
$F \wedge F \equiv F$ $F \vee F \equiv F$	$\neg(F \wedge G) \equiv \neg F \vee \neg G$ $\neg(F \vee G) \equiv \neg F \wedge \neg G$
Kommutativität	Neutralität
$F \wedge G \equiv G \wedge F$ $F \vee G \equiv G \vee F$	$F \wedge 1 \equiv F$ $F \vee 0 \equiv F$
Absorption	Elimination
$F \wedge (F \vee G) \equiv F$ $F \vee (F \wedge G) \equiv F$	$F \wedge 0 \equiv 0$ $F \vee 1 \equiv 1$
Distributivität	Doppelnegation
$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$	$\neg\neg F \equiv F$

**Tabelle 3.1:** Wichtige Äquivalenzen aussagenlogischer Ausdrücke

- Reflexivität: Für alle Formeln  $F$  gilt  $F \equiv F$ .
- Symmetrie: Aus  $F \equiv G$  folgt  $G \equiv F$ .
- Transitivität: Aus  $F \equiv G$  und  $G \equiv H$  folgt  $F \equiv H$ .

Die folgenden Zusammenhänge sind ebenfalls offensichtlich:

- $F$  ist genau dann allgemeingültig, wenn  $F \equiv 1$ .
- $F$  ist genau dann unerfüllbar, wenn  $F \equiv 0$ .

In Tabelle 3.1 sind wichtige Äquivalenzen zusammengefasst, die sich durch das Aufstellen von Wahrheitstafeln leicht verifizieren lassen. Die Bedeutung dieser Äquivalenzen ist zweigeteilt. Zum einen gestatten sie eine Einblick in die elementaren Zusammenhänge zwischen den eingeführten booleschen Operatoren, zum anderen dienen sie als wichtige Umformungsregeln für aussagenlogische Ausdrücke. Grundlage hierfür

ist das *Substitutionstheorem*, das uns gestattet, Teilformeln durch äquivalente Ausdrücke zu ersetzen, ohne die Modelle der Gesamtformel zu beeinflussen.



### Satz 3.1 (Substitutionstheorem)

Seien  $F, G, G'$  aussagenlogische Formeln mit  $G \in F$  und  $G \equiv G'$ .

$$F[G \leftarrow G']$$

bezeichnet diejenige Formel, die aus  $F$  entsteht, indem die Teilformel  $G$  durch  $G'$  ersetzt wird. Dann gilt:

$$F \equiv F[G \leftarrow G']$$

Mit dem Mittel der strukturellen Induktion aus Abschnitt 2.4.2 lässt sich das Substitutionstheorem induktiv über den Aufbau aussagenlogischer Formeln beweisen.

Vielleicht haben Sie sich gewundert, dass Tabelle 3.1 ausschließlich Rechenregeln für die aussagenlogischen *Elementaroperatoren*  $\neg$ ,  $\wedge$  und  $\vee$  enthält. Hierbei handelt es sich um keine Einschränkung im eigentlichen Sinne, da sich alle anderen Operatoren auf diese drei zurückführen lassen (vgl. Tabelle 3.2). Die Menge  $\{\neg, \wedge, \vee\}$  ist zudem ein *vollständiges Operatorensystem*, d. h., sie besitzt die Eigenschaft, dass sich jede boolesche Funktion durch einen aussagenlogischen Ausdruck beschreiben lässt, in dem ausschließlich Operatoren aus dieser Menge vorkommen. Ein Beweis der Vollständigkeit wird uns im nächsten Abschnitt ohne Zutun in die Hände fallen. Dort werden wir zeigen, wie sich eine entsprechende aussagenlogische Formel systematisch aus der Wahrheitstabelle einer booleschen Funktion erzeugen lässt.

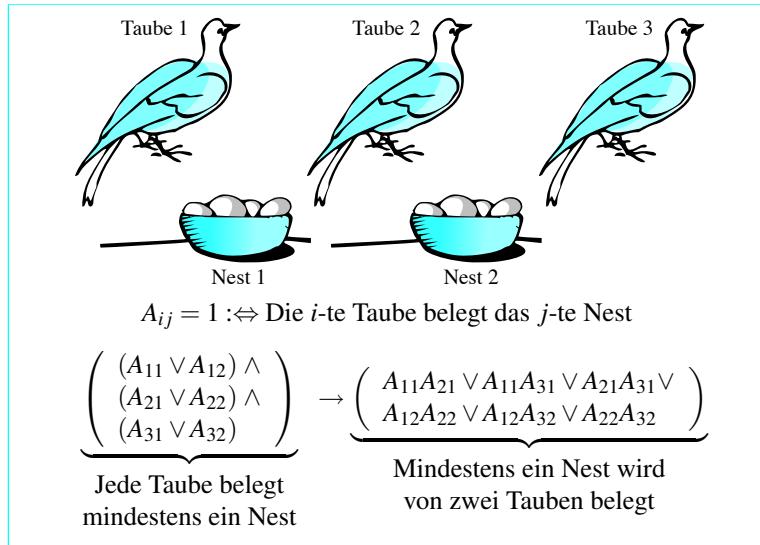
Neben der Menge der Elementaroperatoren existieren weitere vollständige Operatorensysteme, wie z. B. die Menge  $\{\neg, \rightarrow\}$ . Um die Vollständigkeit zu beweisen, nutzen wir unser Wissen, dass die drei Elementaroperatoren  $\wedge$ ,  $\vee$  und  $\neg$  zusammen ein vollständiges Operatorensystem bilden. Können wir zeigen, dass alle drei durch  $\neg$  und  $\rightarrow$  darstellbar sind, so lässt sich jede boolesche Funktion mit einem aussagenlogischen Ausdruck beschreiben, der ausschließlich die Operatoren  $\neg$  und  $\rightarrow$  enthält. Kurzum:  $\{\neg, \rightarrow\}$  bildet dann ebenfalls ein vollständiges Operatorensystem. Tabelle 3.3 zeigt, wie die notwendigen Reduktionen durchgeführt werden können.

Mit Hilfe der Aussagenlogik lassen sich viele der kombinatorischen Zusammenhänge beschreiben, die wir im Bereich des mathematischen

Implikation
$x \rightarrow y \equiv \neg x \vee y$
Äquivalenz
$x \leftrightarrow y \equiv (\neg x \wedge \neg y) \vee (x \wedge y)$ $\equiv (\neg x \vee y) \wedge (x \vee \neg y)$
Antivalenz
$x \leftrightarrow y \equiv (\neg x \wedge y) \vee (x \wedge \neg y)$ $\equiv (\neg x \vee \neg y) \wedge (x \vee y)$
Reduktion von $\neg$ auf $\{\rightarrow, \neg\}$
$\neg x \equiv x \rightarrow \neg x$
Reduktion von $\wedge$ auf $\{\rightarrow, \neg\}$
$x \wedge y \equiv \neg(\neg x \vee \neg y)$ $\equiv \neg(x \rightarrow \neg y)$
Reduktion von $\vee$ auf $\{\rightarrow, \neg\}$
$x \vee y = \neg \neg x \vee y$ $= \neg x \rightarrow y$

Tabelle 3.3: Reduktion der Elementaroperatoren auf die Operatorenmengen  $\{\rightarrow, \neg\}$

**Abbildung 3.8:** Das *Dirichlet'sche Schubfachprinzip* ist im angelsächsischen Raum unter dem Namen *pigeonhole principle (Taubenschlagprinzip)* bekannt. Verteilen sich, wie in diesem Beispiel, 3 Tauben auf 2 Nester, so muss mindestens ein Nest doppelt belegt werden. Mit Hilfe der Aussagenlogik lässt sich das Prinzip formalisieren und beweisen.



Schließens tagtäglich anwenden. Als Beispiel zeigt Abbildung 3.8 eine Formalisierung des *Dirichlet'schen Schubfachprinzips*. Dieses besagt, dass eine endliche Menge  $M$  nicht injektiv auf eine Menge  $N$  abgebildet werden kann, wenn  $N$  weniger Elemente enthält als  $M$ . Das Prinzip ist nach dem deutschen Mathematiker Johann Dirichlet (Abbildung 3.9) benannt und ein häufig angewandtes Beweisargument in der diskreten Mathematik. Jedem von uns ist das Schubfachprinzip aus dem Alltag geläufig. Verteilen wir  $m$  Gegenstände auf  $n$  Schubfächer und gilt  $m > n$ , so muss mindestens ein Schubfach mehrere Gegenstände enthalten. Im angelsächsischen Raum wird das *Dirichlet'sche Schubfachprinzip* als *pigeonhole principle (Taubenschlagprinzip)* bezeichnet. Auch hier ist die angestellte Überlegung die gleiche: Verteilen sich  $m$  Tauben auf  $n$  Nester und gilt  $m > n$ , so ist mindestens ein Nest mehrfach besetzt.

Mit Hilfe der Aussagenlogik können wir das Schubfachprinzip formalisieren und beweisen. Hierzu führen wir für jede mögliche Kombination von Gegenständen und Schubfächern eine aussagenlogische Variable  $A_{ij}$  ein, die genau dann den Wert 1 annimmt, wenn sich der  $i$ -te Gegenstand im  $j$ -ten Schubfach befindet. Um das Schubfachprinzip für  $n$  Gegenstände und  $n - 1$  Schubfächer zu formalisieren, benötigen wir  $n \cdot (n - 1)$  Variablen. Wir werden nun Schritt für Schritt herausarbeiten, wie sich das Schubfachprinzip mit Hilfe der booleschen Operatoren  $\neg$ ,  $\wedge$ ,  $\vee$  und  $\rightarrow$  formal nachbilden lässt:

- „Das  $i$ -te Element befindet sich in einem der Schubfächer“

$$\bigvee_{j=1}^{n-1} A_{ij} \quad (3.3)$$

- „Jedes Element befindet sich in einem der Schubfächer“

$$\bigwedge_{i=1}^n \bigvee_{j=1}^{n-1} A_{ij} \quad (3.4)$$

- „In Schubfach  $j$  befinden sich das  $i$ -te und  $k$ -te Element gleichzeitig“

$$A_{ij} \wedge A_{kj} \quad (3.5)$$

- „In Schubfach  $j$  befinden sich mindestens zwei Elemente“

$$\bigvee_{i=1}^{n-1} \bigvee_{k=i+1}^n (A_{ij} \wedge A_{kj}) \quad (3.6)$$

- „In einem Schubfach befinden sich mindestens zwei Elemente“

$$\bigvee_{j=1}^{n-1} \bigvee_{i=1}^{n-1} \bigvee_{k=i+1}^n (A_{ij} \wedge A_{kj}) \quad (3.7)$$

Verbinden wir die Formeln (3.4) und (3.7) mit dem Implikationsoperator, so erhalten wir die Aussage des Schubfachprinzips: Befinden sich  $n$  Elemente in  $n - 1$  Schubfächern, so enthält eines der Schubfächer mindestens zwei Elemente:

$$\bigwedge_{i=1}^n \bigvee_{j=1}^{n-1} A_{ij} \rightarrow \bigvee_{j=1}^{n-1} \bigvee_{i=1}^{n-1} \bigvee_{k=i+1}^n (A_{ij} \wedge A_{kj}) \quad (3.8)$$

Die in Abbildung 3.8 dargestellte Formel erhalten wir aus Formel (3.8) für den Spezialfall  $n = 3$ .

### 3.1.2 Normalformen

Weiter oben haben wir herausgearbeitet, dass wir eine aussagenlogische Formel  $F$  als boolesche Funktion interpretieren können, indem wir jede Interpretation  $I$  als Eingabebelegung auffassen und die Funktion genau dann zu 1 evaluieren lassen, wenn  $I$  ein Modell für  $F$  ist. Die enge Beziehung, die zwischen aussagenlogischen Formeln auf der einen Seite



Johann Peter Gustav Lejeune Dirichlet  
(1805 – 1859)

**Abbildung 3.9:** Das Schubfachprinzip erhielt seinen Namen durch Johann Peter Gustav Lejeune Dirichlet. Der deutsche Mathematiker wurde im nordrhein-westfälischen Düren geboren, damals Teil des Napoleonischen Kaiserreiches. 1822 nahm er das Studium der Mathematik in Paris auf. Bereits drei Jahre später demonstrierte er der Wissenschaftsgemeinde das erste Mal sein Talent, als er die Gültigkeit der Fermat'schen Vermutung für den Fall  $n = 5$  bewies. Im Jahre 1826 kehrte er nach Deutschland zurück und graduierte 1827 an der Universität Bonn. Seine akademische Karriere führte ihn über Breslau und Berlin nach Göttingen, wo er im Jahre 1855 den Lehrstuhl von Carl-Friedrich Gauß übernahm. Dort sollte ihm das Schicksal nur eine kurze Schaffenszeit gewähren. Am 5. Mai 1859, nur fünf Monate nach seiner Frau Rebecca Mendelssohn Bartholdy, verstarb er im Alter von 54 Jahren. Dirichlet zählt zu den großen Mathematikern des neunzehnten Jahrhunderts und machte sich vor allem in den Gebieten der partiellen Differentialgleichungen und der algebraischen Zahlentheorie verdient. Zu seinen bedeutendsten Hinterlassenschaften gehört der Dirichlet'sche Einheitsatz, die Dirichlet-Funktion und die Dirichlet'sche Eta-Funktion.

■ Beispiel 1

$$F := (A \wedge B) \vee A$$

$$G := A$$

	A	B	F	G
0	0	0	0	0
1	0	1	0	0
2	1	0	1	1
3	1	1	1	1

■ Beispiel 2

$$F := (A \leftrightarrow B) \vee (A \leftrightarrow B)$$

$$G := 1$$

	A	B	F	G
0	0	0	1	1
1	0	1	1	1
2	1	0	1	1
3	1	1	1	1

**Abbildung 3.10:** Zwei aussagenlogische Formeln können selbst dann äquivalent sein, wenn sie unterschiedliche Variablen enthalten. Wie die Wahrheitstafeln belegen, besitzen F und G jeweils die gleichen Modelle.

und booleschen Funktionen auf der anderen besteht, ist nicht eindeutig. So repräsentieren die Formeln

$$\begin{aligned} F_1 &= A \\ F_2 &= A \wedge A \\ F_3 &= A \wedge A \wedge A \\ &\dots \\ F_n &= A \wedge A \wedge \dots \wedge A \end{aligned}$$

allesamt die gleiche boolesche Funktion  $f : A \mapsto A$ . Die äußere Form lässt also keinerlei Rückschluss zu, ob zwei boolesche Formeln äquivalent zueinander sind oder nicht. Wie die Beispiele in Abbildung 3.10 zeigen, können zwei Formeln können sogar dann äquivalent sein, wenn sie unterschiedliche Variablen enthalten.

Um diesem Problem zu begegnen, wurden in der Vergangenheit mehrere *Normalformen* entwickelt, die eine Eins-zu-eins-Beziehung zwischen aussagenlogischen Formeln und booleschen Funktionen herstellen. Wichtige Normalformen sind die *konjunktive* und die *disjunktive Normalform*. Um diese formal zu definieren, benötigen wir die folgenden Hilfsbegriffe:



### Definition 3.7 (Literal, Minterm, Maxterm)

Sei  $F$  eine aussagenlogische Formel mit den Variablen  $A_1, \dots, A_n$ .

- Jedes Vorkommen einer Variablen  $A_i$  oder ihrer Negation  $\neg A_i$  bezeichnen wir als *Literal*, geschrieben als  $(\neg)A_i$  oder  $L_i$ .
- Jeder Ausdruck der Form  $(\neg)A_1 \wedge \dots \wedge (\neg)A_n$  heißt *Minterm*.
- Jeder Ausdruck der Form  $(\neg)A_1 \vee \dots \vee (\neg)A_n$  heißt *Maxterm*.

Hat ein Literal  $L$  die Form  $\neg A$ , so sprechen wir von einem *negativen*, andernfalls von einem *positiven Literal*. Minterme und Maxterme besitzen die Eigenschaft, dass sämtliche Variablen einer Funktion konjunktiv bzw. disjunktiv miteinander verknüpft werden. Hieraus ergeben sich die folgenden beiden Eigenschaften:

- Ein Minterm evaluiert für genau eine Variablenbelegung zu 1.
- Ein Maxterm evaluiert für genau eine Variablenbelegung zu 0.

Mit Hilfe der eingeführten Begriffe definieren wir die disjunktive und konjunktive Normalform wie folgt:

	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>F</i>	
$A \vee B \vee C \vee D$	0	0	0	0	0	
	0	0	0	1	1	$\bar{A} \wedge \bar{B} \wedge \bar{C} \wedge D$
	0	0	1	0	1	$\bar{A} \wedge \bar{B} \wedge C \wedge \bar{D}$
	0	0	1	1	1	$\bar{A} \wedge \bar{B} \wedge C \wedge D$
$A \vee \bar{B} \vee C \vee D$	0	1	0	0	0	
	0	1	0	1	1	$\bar{A} \wedge B \wedge \bar{C} \wedge D$
$A \vee \bar{B} \vee \bar{C} \vee D$	0	1	1	0	0	
$A \vee \bar{B} \vee \bar{C} \vee \bar{D}$	0	1	1	1	0	
$\bar{A} \vee B \vee C \vee D$	1	0	0	0	0	
$\bar{A} \vee B \vee C \vee \bar{D}$	1	0	0	1	0	
	1	0	1	0	1	$A \wedge \bar{B} \wedge C \wedge \bar{D}$
$\bar{A} \vee B \vee \bar{C} \vee \bar{D}$	1	0	1	1	0	
	1	1	0	0	1	$A \wedge B \wedge \bar{C} \wedge \bar{D}$
	1	1	0	1	1	$A \wedge B \wedge \bar{C} \wedge D$
	1	1	1	0	1	$A \wedge B \wedge C \wedge \bar{D}$
$\bar{A} \vee \bar{B} \vee \bar{C} \vee \bar{D}$	1	1	1	1	0	

**Tabelle 3.4:** Konstruktionsschema der konjunktiven und der disjunktiven Normalform. Die konjunktive Normalform wird erzeugt, indem zunächst für jede Belegung  $I$  mit  $I \neq F$  ein Maxterm erzeugt wird. Die Variable  $A$  wird unverändert in den Maxterm aufgenommen, wenn  $A$  in der entsprechenden Variablenbelegung gleich 0 ist, und negiert aufgenommen, falls  $A$  mit 1 belegt ist. Anschließend werden alle Maxterme miteinander konjunktiv verknüpft. Die Konstruktion der disjunktiven Normalform verläuft analog, indem zunächst für jede Belegung  $I$  mit  $I \models F$  ein Minterm erzeugt wird. Jetzt wird die Variable  $A$  unverändert in den Minterm aufgenommen, wenn  $A$  in der entsprechenden Variablenbelegung gleich 1 ist, und negiert aufgenommen, falls  $A$  mit 0 belegt ist. Anschließend werden alle Minterme miteinander disjunktiv verknüpft.



### Definition 3.8 (Disjunktive und konjunktive Normalform)

Sei  $F$  eine aussagenlogische Formel mit den Variablen  $A_1, \dots, A_n$ .

- Die Formel  $F$  liegt in *konjunktiver Normalform* (KNF) vor, wenn sie die Form

$$F = \bigwedge_{i=1}^m ((\neg)A_1 \vee \dots \vee (\neg)A_n)$$

besitzt und alle Maxterme paarweise verschieden sind.

- Die Formel  $F$  liegt in *disjunktiver Normalform* (DNF) vor, wenn sie die Form

$$F = \bigvee_{i=1}^m ((\neg)A_1 \wedge \dots \wedge (\neg)A_n)$$

besitzt und alle Minterme paarweise verschieden sind.

Die konjunktive Normalform entspricht einer Kette UND-verknüpfter Maxterme und die disjunktive Normalform einer Kette ODER-

■ Konjunktive Normalform

$$\begin{aligned} & (A \vee B \vee C \vee D) \wedge \\ & (A \vee \neg B \vee C \vee D) \wedge \\ & (A \vee \neg B \vee \neg C \vee D) \wedge \\ & (A \vee \neg B \vee \neg C \vee \neg D) \wedge \\ & (\neg A \vee B \vee C \vee D) \wedge \\ & (\neg A \vee B \vee C \vee \neg D) \wedge \\ & (\neg A \vee B \vee \neg C \vee \neg D) \wedge \\ & (\neg A \vee \neg B \vee \neg C \vee \neg D) \end{aligned}$$

■ Disjunktive Normalform

$$\begin{aligned} & (\neg A \wedge \neg B \wedge \neg C \wedge D) \vee \\ & (\neg A \wedge \neg B \wedge C \wedge \neg D) \vee \\ & (\neg A \wedge \neg B \wedge C \wedge D) \vee \\ & (\neg A \wedge B \wedge \neg C \wedge D) \vee \\ & (A \wedge \neg B \wedge C \wedge \neg D) \vee \\ & (A \wedge B \wedge \neg C \wedge \neg D) \vee \\ & (A \wedge B \wedge \neg C \wedge D) \vee \\ & (A \wedge B \wedge C \wedge \neg D) \end{aligned}$$

**Abbildung 3.11:** Konjunktive und disjunktive Normalform für die Beispielfunktion aus Tabelle 3.4

verknüpfter Minterme. Aus der Wahrheitstabelle einer aussagenlogischen Formel  $F$  lassen sich die konjunktive und die disjunktive Normalform auf einfache Weise ableiten. Für die konjunktive Normalform wird für jede Belegung  $I$  mit  $I \not\models F$  ein Maxterm erzeugt. Anschließend werden diese konjunktiv miteinander verknüpft (vgl. Tabelle 3.4 links). Die disjunktive Normalform entsteht analog, indem für jede Belegung  $I$  mit  $I \models F$  ein Minterm erzeugt und diese anschließend disjunktiv miteinander verknüpft werden (vgl. Tabelle 3.4 rechts). Für das gezeigte Beispiel erhalten wir die in Abbildung 3.11 dargestellten Ergebnisse.

Das Konstruktionsschema besitzt zwei wesentliche Eigenschaften. Zum einen können wir es auf beliebige Wahrheitstabellen anwenden und somit zu jeder booleschen Funktion  $f$  eine äquivalente aussagenlogische Formel  $F$  in konjunktiver oder disjunktiver Normalform konstruieren. Da in  $F$  ausschließlich die drei Elementaroperatoren  $\neg$ ,  $\wedge$  und  $\vee$  vorkommen, haben wir nebenbei bewiesen, dass die Menge  $\{\neg, \wedge, \vee\}$  ein vollständiges Operatorenensemble bildet. Zum anderen ist das Konstruktionsschema deterministisch, d. h., wir hatten zu keiner Zeit eine Möglichkeit, die Konstruktion der Min- oder Maxterme in irgendeiner Weise zu beeinflussen. Da jede boolesche Funktion eine eindeutige Wahrheitstafeldarstellung besitzt, ist auch die erzeugte konjunktive bzw. disjunktive Formeldarstellung eindeutig.

In den folgenden Betrachtungen ist die Eigenschaft der Eindeutigkeit nicht von Bedeutung. Aus diesem Grund werden wir auf eine kompaktere Darstellung zurückgreifen, die die zweistufige Grundstruktur der disjunktiven bzw. der konjunktiven Normalform nicht zerstört. Die neue Darstellung basiert auf der Beobachtung, dass wir zwei Min- bzw. Maxterme immer dann zu einem gemeinsamen Term verschmelzen können, wenn sich diese im Vorzeichen eines einzigen Literals unterscheiden. Für unsere Beispielfunktion sind unter anderem die folgenden Vereinfachungen möglich:

$$\begin{aligned} & (A \wedge B \wedge \neg C \wedge \neg D) \vee (A \wedge B \wedge \neg C \wedge D) \\ & \equiv (A \wedge B \wedge \neg C) \wedge (\neg D \vee D) \\ & \equiv (A \wedge B \wedge \neg C) \end{aligned}$$

Wenden wir das Vereinfachungsschema durchgängig an, so können wir die 8 Teilausdrücke der disjunktiven und der konjunktiven Normalform auf jeweils 4 Teilausdrücke reduzieren. Beachten Sie, dass wir die Normalformeigenschaft durch die Reduktion verlieren. Wie in Abbildung 3.12 gezeigt, existieren zwei verschiedene Möglichkeiten, die ursprüngliche Funktion kompakt darzustellen. Folgerichtig sprechen wir nicht mehr länger von einer Normalform, sondern nur noch von einer konjunktiven bzw. disjunktiven *Form*. Eine konjunktive bzw. disjunk-

tive *Minimalform* liegt vor, wenn die Funktion mit der kleinstmöglichen Anzahl von Literalen dargestellt wird, d.h., wenn keine andere konjunktive bzw. disjunktive Form existiert, die mit weniger Literalen auskommt.



### Definition 3.9 (Konjunktive und disjunktive Minimalform)

Sei  $F$  eine aussagenlogische Formel mit den Variablen  $A_1, \dots, A_n$ .

- $F$  ist in *konjunktiver Form* (KF), wenn sie eine Konjunktion von Disjunktionen von Literalen ist.
- Eine konjunktive Form heißt *minimal*, wenn es keine äquivalente konjunktive Form gibt, die mit weniger Literalen auskommt.
- $F$  ist in *disjunktiver Form* (DF), wenn sie eine Disjunktion von Konjunktionen von Literalen ist.
- Eine disjunktive Form heißt *minimal*, wenn es keine äquivalente disjunktive Form gibt, die mit weniger Literalen auskommt.

Die Erzeugung einer konjunktiven oder einer disjunktiven Minimalform ist ein gut untersuchtes Teilgebiet der technischen Informatik. Unter dem Begriff der *zweistelligen Logikminimierung* wurde eine Vielzahl von Verfahren entwickelt, mit deren Hilfe sich die Minimalform effizient erzeugen bzw. annähern lässt [48]. Unter anderem kann mit diesen Verfahren gezeigt werden, dass es sich bei den Formeln aus Abbildung 3.12 tatsächlich um Minimalformen handelt.

Für die konjunktive Form einer aussagenlogischen Formel  $F$  existiert mit der *Klauseldarstellung* eine eigene Notation, von der wir in Abschnitt 3.1.3.2 im Zusammenhang mit dem Resolutionskalkül umfassend Gebrauch machen werden.



### Definition 3.10 (Klauseldarstellung)

Eine *Klausel* ist eine Menge von Literalen. Die Menge

$$\{(\neg)A_1, \dots, (\neg)A_i\}, \dots, \{(\neg)B_1, \dots, (\neg)B_j\}$$

steht stellvertretend für die Formel

$$((\neg)A_1 \vee \dots \vee (\neg)A_i) \wedge \dots \wedge ((\neg)B_1 \vee \dots \vee (\neg)B_j).$$

Die *leere Klausel*  $\square$  repräsentiert den Wahrheitswert 0.

### ■ Reduzierte konjunktive Formen

$$\begin{aligned} F = & (B \vee C \vee D) \wedge \\ & (A \vee \neg B \vee D) \wedge \\ & (\neg B \vee \neg C \vee \neg D) \wedge \\ & (\neg A \vee B \vee \neg D) \end{aligned}$$

$$\begin{aligned} F = & (A \vee C \vee D) \wedge \\ & (A \vee \neg B \vee \neg C) \wedge \\ & (\neg A \vee \neg C \vee \neg D) \wedge \\ & (\neg A \vee B \vee C) \end{aligned}$$

### ■ Reduzierte disjunktive Formen

$$\begin{aligned} F = & (\neg B \wedge C \wedge \neg D) \vee \\ & (A \wedge B \wedge \neg D) \vee \\ & (B \wedge \neg C \wedge D) \vee \\ & (\neg A \wedge \neg B \wedge D) \end{aligned}$$

$$\begin{aligned} F = & (\neg A \wedge \neg C \wedge D) \vee \\ & (\neg A \wedge \neg B \wedge C) \vee \\ & (A \wedge C \wedge \neg D) \vee \\ & (A \wedge B \wedge \neg C) \end{aligned}$$

**Abbildung 3.12:** Die betrachtete Beispielfunktion ist so strukturiert, dass sich je zwei Min- bzw. Maxterme zu einem gemeinsamen Term verschmelzen lassen. Die reduzierte Darstellung ist nicht mehr eindeutig, so dass wir die entstehenden Formeln nur noch als konjunktive bzw. disjunktive Form und nicht mehr als Normalform bezeichnen.

■ Kommutativität

$$\begin{array}{ccc} A \vee \neg B & & \neg B \vee A \\ \downarrow & & \downarrow \\ \{A, \neg B\} & & \{A, \neg B\} \end{array}$$

■ Assoziativität

$$\begin{array}{ccc} A \vee (\neg B \vee C) & & (A \vee \neg B) \vee C \\ \downarrow & & \downarrow \\ \{A, \neg B, C\} & & \{A, \neg B, C\} \end{array}$$

■ Idempotenz

$$\begin{array}{ccc} A \vee A & & A \vee A \vee A \\ \downarrow & & \downarrow \\ \{A\} & & \{A\} \end{array}$$

**Abbildung 3.13:** Zwischen Klauseln und Formeln besteht keine Eins-zu-eins-Beziehung. Jede Formel lässt sich eindeutig einer Klausel zuordnen, aber nicht umgekehrt. In der Klauseldarstellung sind die Eigenschaften der Kommutativität, Assoziativität und Idempotenz implizit vorhanden.

Auch wenn wir Klauseln fast immer wie Formeln behandeln werden, sollten Sie stets daran denken, dass zwischen beiden Darstellungsformen keine Eins-zu-eins-Beziehung besteht. Jede aussagenlogische Formel lässt sich eindeutig in eine Klausel verwandeln, aber nicht umgekehrt (vgl. Abbildung 3.13). Schuld daran ist die Mengendarstellung, in der zum einen die Information über die Reihenfolge der Elemente verloren geht und zum anderen jeder Term nur einmal aufgenommen werden kann. In einigen Anwendungsfällen ist dies gewollt. So ist die Klauseldarstellung der Formeldarstellung immer dann überlegen, wenn die Kommutativität ( $A \vee B \equiv B \vee A$ ), die Assoziativität ( $A \vee (B \vee C) \equiv (A \vee B) \vee C$ ) und die Idempotenz ( $A \vee A \equiv A$ ) keine Rolle spielen.

### 3.1.3 Beweistheorie

In Abschnitt 3.1.1 haben wir die Semantik der Aussagenlogik über die Modellrelation  $\models$  festgelegt, uns aber nicht weiter mit der Frage befasst, wie wir die Allgemeingültigkeit einer Formel beweisen können. Genau dies wollen wir in diesem Abschnitt nachholen und eine Reihe von Beweissystemen einführen, mit deren Hilfe sich die Gültigkeit einer Formel systematisch herleiten lässt. Auch wenn die verschiedenen Verfahren äußerlich betrachtet sehr unterschiedlich wirken, folgen sie alle dem gleichen Ansatz: Die Gültigkeit wird mit einem Regelsystem bewiesen, das auf der symbolischen Manipulation der zu beweisenden Formeln beruht. Da ein Beweis vollständig auf der syntaktischen Ebene durchgeführt wird, benötigen wir keinerlei Meta-Wissen über Interpretationen oder die Modellrelation. Ein solches Regelsystem bezeichnen wir als *aussagenlogisches Beweiskalkül*.

Jedes Kalkül definiert eine *Ableitungsrelation*  $\vdash$ , die über die folgenden Beziehungen mit der Modellrelation  $\models$  verbunden ist:



#### Definition 3.11 (Korrektheit, Vollständigkeit)

Sei  $K$  ein aussagenlogischer Beweiskalkül. Ist eine Formel  $F$  innerhalb des Kalküls ableitbar, so schreiben wir  $\vdash_K F$ .

- $K$  heißt *korrekt*, wenn aus  $\vdash_K F$  stets  $\models F$  folgt.
- $K$  heißt *vollständig*, wenn aus  $\models F$  stets  $\vdash_K F$  folgt.

Ein korrekter Kalkül besitzt demnach die Eigenschaft, dass ausschließlich wahre Aussagen ableitbar sind. Vollständig ist ein Kalkül genau

dann, wenn sich *alle* wahren Aussagen innerhalb des Kalküls als solche beweisen lassen. Geht aus dem Kontext hervor, auf welchen Kalkül wir uns beziehen, so schreiben wir nur noch  $\vdash F$  anstelle von  $\vdash_K F$ .

Neben den geschilderten Kalkülen existieren sogenannte *Widerspruchskalküle*, in denen eine Behauptung  $F$  nicht konstruktiv gezeigt wird. Stattdessen wird die Erfüllbarkeit der negierten Aussage  $\neg F$  unterstellt und die Annahme zu einem Widerspruch geführt ( $\neg F \models \square$ ). Aus der Unerfüllbarkeit von  $\neg F$  ergibt sich dann sofort die Allgemeingültigkeit von  $F$ .

Die Abkehr von der konstruktiven Beweisführung macht es erforderlich, die weiter oben eingeführten Begriffe der Korrektheit und Vollständigkeit für Widerspruchskalküle geringfügig umzuformulieren:



### Definition 3.12 (Korrektheit, Vollständigkeit)

Sei  $K$  ein Widerspruchskalkül. Lässt sich aus einer Formel  $F$  ein Widerspruch herleiten, so schreiben wir  $F \vdash_K \square$ .

- $K$  heißt *korrekt*, wenn aus  $\neg F \vdash_K \square$  stets  $\models F$  folgt.
- $K$  heißt *vollständig*, wenn aus  $\models F$  stets  $\neg F \vdash_K \square$  folgt.

Ein Widerspruchskalkül ist demnach korrekt, wenn ein Widerspruch nur aus unerfüllbaren Formeln abgeleitet werden kann. Er ist vollständig, wenn sich aus der Negation einer wahren Aussage immer ein Widerspruch ableiten lässt. Auch hier schreiben wir  $\vdash$  anstelle von  $\vdash_K$ , wenn aus dem Kontext hervorgeht, auf welchen Kalkül wir uns beziehen.

In den nächsten Abschnitten werden Sie drei Kalküle kennen lernen, die sich in ihrer äußereren Form und der Art der Beweisführung erheblich voneinander unterscheiden. Der erste fällt in die Klasse der *Hilbert-Kalküle*. Diese Kalküle bilden weitgehend das Prinzip des mathematischen Schließens nach und bestechen vor allem durch ihre Einfachheit und Klarheit. Auf der negativen Seite machen sie es vergleichsweise schwer, Beweise zu finden. In der Praxis wird aus diesem Grund meist auf *Resolutionskalküle* oder *Tableaukalküle* zurückgegriffen, die wir in den Abschnitten 3.1.3.2 und 3.2.3.2 im Detail besprechen werden.

#### 3.1.3.1 Hilbert-Kalkül

Hilbert-Kalküle zeichnen sich dadurch aus, dass wahre Aussagen aus einer Menge von Axiomen durch die sukzessive Anwendung fest defi-

Vorsicht mit dem Begriff der Normalform! In vielen Büchern über theoretische Informatik wird der Begriff der konjunktiven Normalform für sämtliche Formeln verwendet, die in konjunktiver Form vorliegen. Die Sprechweise ist widersprüchlich, da sie eine eindeutige Darstellung suggeriert, die in Wirklichkeit nicht gegeben ist. Jede Formel lässt sich auf unendlich viele Weisen als Konjunktion von Disjunktionen darstellen und das hier erarbeitete Beispiel hat gezeigt, dass selbst die Minimalform nicht eindeutig ist. Aus diesem Grund werden die Begriffe der konjunktiven Form und der konjunktiven Normalform in diesem Buch klar voneinander getrennt. Das Gesagte gilt gleichermaßen für die Begriffe der disjunktiven Form und der disjunktiven Normalform. Im strengen Sinne sind auch die konjunktive und die disjunktive Normalform keine echten Normalformen. Verantwortlich hierfür ist eine fehlende Ordnung zwischen den Literalen eines Minterms und den Mintermen selbst. Ohne diese können wir aus einer konjunktiven oder disjunktiven Normalform eine weitere erzeugen, indem wir die Literale innerhalb eines Minterms umordnen. Ebenso können wir die Position der Minterme vertauschen, ohne die Normalform-eigenschaft zu verletzen. Mathematisch ausgedrückt handelt es sich bei der konjunktiven und der disjunktiven Normalform um eine Normalform modulo Kommutativität und Assoziativität.

Eine im mathematischen Sinne echte Normalform ließe sich erzeugen, indem wir die Literale und Minterme beispielsweise alphabetisch anordnen. Für die meisten Anwendungen ist der Normalformbegriff in der hier eingeführten Form aber völlig ausreichend.



■ Axiome

Abschwächung (A1)

$$\frac{\{\}}{A \rightarrow (B \rightarrow A)}$$

Distributivität (A2)

$$\frac{\{\}}{(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))}$$

Kontraposition (A3)

$$\frac{\{\}}{(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)}$$

■ Schlussregeln

Modus ponens (MP)

$$\frac{A, A \rightarrow B}{B}$$

**Tabelle 3.5:** Axiome und Schlussregeln des betrachteten Hilbert-Kalküls

nierter Schlussregeln abgeleitet werden. In diesen Systemen ist ein Beweis eine Folge von Tautologien, an deren Ende die zu zeigende Behauptung steht. Alle anderen Formeln in der Beweiskette sind entweder ein Axiom oder eine Tautologie, die mit einer der Schlussregeln aus den vorher erzeugten Formeln abgeleitet wurde.

Im Folgenden werden wir die Schlussregeln in der Notation

$$\frac{F_1, F_2, \dots, F_n}{G} \quad (3.9)$$

angeben. Die über dem Mittelstrich notierten Formeln bilden zusammen die *Prämissen* und beschreiben die Voraussetzungen, die vor der Anwendung der Regel erfüllt sein müssen. Die unter dem Mittelstrich notierte Formel ist die *Konklusion*, d. h. die Schlussfolgerung, die aufgrund der Semantik des Logikkalküls aus der Prämisse abgeleitet werden kann. Das Notationsschema ist stark genug, um auch Axiome darzustellen, schließlich können wir diese als spezielle Schlussregeln mit leerer Prämisse auffassen.

Im Folgenden betrachten wir den Hilbert-Kalkül, der durch die Axiome und Schlussregeln aus Tabelle 3.5 gegeben ist. Das erste Axiom wird als *Abschwächungsregel* bezeichnet und besagt, dass aus  $A$  stets auch  $B \rightarrow A$  folgt. Das zweite Axiom drückt die *Distributivitätseigenschaft* des Implikationsoperators aus. Das dritte und letzte Axiom ist die logische *Kontraposition* – ein Schlussprinzip, das wir täglich einsetzen. Es besagt, dass wir die logische Schlussrichtung umdrehen können, wenn wir die Argumente verneinen („Wenn es regnet, dann ist die Straße nass“ ist gleichbedeutend mit „Wenn die Straße nicht nass ist, dann regnet es nicht“). Innerhalb des Kalküls existiert mit dem *Modus ponens* eine einzige Schlussregel, mit der neue Sätze abgeleitet werden können. Diese Regel ist uns intuitiv vertraut und besagt, dass wir die Gültigkeit einer Aussage  $B$  folgern können, wenn wir wissen, dass  $A$  wahr ist und  $B$  aus  $A$  gefolgert werden kann.

Insgesamt wirkt der Kalkül aus zweierlei Gründen spartanisch. Zum einen mag es den einen oder anderen Leser verwundern, dass er mit nur drei Axiomen und einer einzigen Schlussregel auskommt. Zum anderen scheint er nur eine begrenzte Formelklasse zu beschreiben, da die Axiome und Schlussregeln vollständig ohne die Elementaroperatoren  $\wedge$  und  $\vee$  formuliert sind. Der Ausschluss dieser Verknüpfungen ist jedoch keine Beschränkung im eigentlichen Sinne, da wir in Abschnitt 3.1.1 gezeigt haben, dass die Menge  $\{\neg, \rightarrow\}$  ein vollständiges Operatoren-System bildet. Folgerichtig können wir jede aussagenlogische Formel so umformen, dass sie nur noch Negations- und Implikationsoperatoren enthält.

Beachten Sie bei der Betrachtung der Axiome und Regeln, dass die Variablen lediglich Platzhalter sind, die durch beliebige aussagenlogische Ausdrücke substituiert werden können. So lassen sich aus dem Distributivitätsaxiom unter anderem die folgenden *Instanzen* bilden:

- Substitution:  $[A \leftarrow B, B \leftarrow C, C \leftarrow A]$   
 $\vdash B \rightarrow (C \rightarrow A) \rightarrow ((B \rightarrow C) \rightarrow (B \rightarrow A))$
- Substitution:  $[A \leftarrow A, B \leftarrow A, C \leftarrow A]$   
 $\vdash A \rightarrow (A \rightarrow A) \rightarrow ((A \rightarrow A) \rightarrow (A \rightarrow A))$
- Substitution:  $[A \leftarrow A, B \leftarrow (A \rightarrow A), C \leftarrow A]$   
 $\vdash (A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$

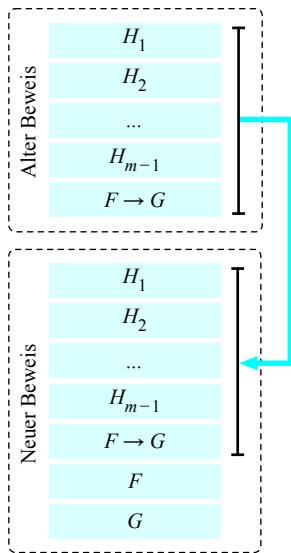
Das folgende Beispiel zeigt, wie die Tautologie  $A \rightarrow A$  innerhalb des Hilbert-Kalküls bewiesen werden kann:

- 1:  $\vdash (A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$  (A2)
- 2:  $\vdash (A \rightarrow ((A \rightarrow A) \rightarrow A))$  (A1)
- 3:  $\vdash (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$  (MP 1,2)
- 4:  $\vdash (A \rightarrow (A \rightarrow A))$  (A1)
- 5:  $\vdash (A \rightarrow A)$  (MP 3,4)

Das erste und zweite Glied der Beweiskette sind Instanzen des Distributivitätsaxioms und des Abschwächungsaxioms. Das dritte Glied entsteht durch die Anwendung der Schlussregel auf die vorher erzeugten Formeln. Das vierte Glied ist wiederum eine Instanz des Abschwächungsaxioms. Jetzt lässt sich  $F$  mit Hilfe der Schlussregel aus den Tautologien 3 und 4 direkt ableiten.

Nachdem wir die Formel  $A \rightarrow A$  als allgemeingültig identifiziert haben, können wir auf sie in allen zukünftigen Beweisen zurückgreifen. Der Hilbert-Kalkül ist bewusst so ausgelegt, dass einmal bewiesene Formeln nicht mehr erneut bewiesen werden müssen. Solche Formeln dürfen wir wie Axiome behandeln und an beliebigen Stellen in einer Beweiskette einfügen. Mit der Zeit entsteht eine sich kontinuierlich vergrößernende Bibliothek von Tautologien, der wir uns frei bedienen können. Der Hilbert-Kalkül spiegelt eins zu eins das Vorgehen der klassischen Mathematik wider. Auch hier beweisen wir eine Behauptung, indem wir auf den reichhaltigen Fundus bereits bekannter Sätze zurückgreifen.

Um den Hilbert-Kalkül gewinnbringend einsetzen zu können, wollen wir ihn noch um einen wichtigen Baustein ergänzen. Die Rede ist von



**Abbildung 3.14:** Beweisschema des Deduktionstheorems (Schlussrichtung von rechts nach links)

*Annahmen*, die in der klassischen Mathematik in den verschiedensten Formen gemacht werden und nicht notwendigerweise selbst wahr sein müssen. Um auch Aussagen der Form „Unter der Annahme, dass A gilt, folgt B“ mit Hilfe des Hilbert-Kalküls modellieren zu können, erlauben wir, einen Beweis um eine Menge von *Voraussetzungen* zu ergänzen. In diesem erweiterten Kalkül ist ein Beweis eine Kette von Formeln  $F_1, F_2, \dots, F_n$ , die nach den folgenden Konstruktionsregeln gebildet wird:

- $F_i$  ist eine Instanz eines Axioms oder
- $F_i$  ist eine Instanz einer Voraussetzung oder
- $F_i$  entsteht aus den vorangegangenen Gliedern der Beweiskette durch die Anwendung einer Schlussregel

Bezeichnet  $M$  die Menge der Voraussetzungen, so schreiben wir  $M \vdash F$ , falls sich die Formel  $F$  mit den beschriebenen Konstruktionsregeln ableiten lässt. Mit dieser Notation können wir den weiter oben eingeführten Ausdruck  $\vdash F$  als abkürzende Schreibweise für  $\emptyset \vdash F$  auffassen. Beachten Sie, dass für jede Formel  $F$  und eine beliebige Formelmenge  $M$  die Beziehung  $\{F\} \cup M \vdash F$  gilt; die Korrektheit folgt unmittelbar aus den oben genannten Konstruktionsregeln.

Die folgenden beiden Begriffe spielen in den nachstehenden Betrachtungen eine Rolle:



### Definition 3.13 (Konsistenz und Vollständigkeit)

Sei  $M$  eine Menge aussagenlogischer Formeln.  $M$  heißt

- *konsistent*, wenn für keine Formel  $F$  gilt:  $M \vdash F$  und  $M \vdash \neg F$ ,
- *vollständig*, wenn für jede Formel  $F$  gilt:  $M \vdash F$  oder  $M \vdash \neg F$ .

Achten Sie darauf, die Begriffe nicht zu verwechseln: Eine *vollständige Menge* ist etwas anderes als ein *vollständiger Kalkül* im Sinne von Definition 3.11. Die Begriffsüberschneidung ist denkbar unglücklich, hat sich im Sprachgebrauch jedoch so fest etabliert, dass wir uns nicht dagegen sträuben wollen.

Vielleicht haben Sie sich selbst die Frage gestellt, ob eine Erweiterung des Hilbert-Kalküls wirklich notwendig ist, schließlich sind wir in der

Lage, beliebige Wenn-dann-Beziehungen mit Hilfe des Implikationsoperators → zu formulieren. Der Unterschied zwischen beiden Konstrukten besteht darin, dass der Operator → innerhalb der Logik existiert, während die Folgerungsbeziehung  $M \vdash F$  eine Aussage über die Beweisbarkeit der Aussage  $F$  macht. Mit anderen Worten:  $M \vdash F$  ist eine Meta-Aussage, die außerhalb der Logik steht. Nichtsdestotrotz existiert zwischen beiden Konstrukten ein enger Zusammenhang, wie das nachstehende Theorem zum Ausdruck bringt:



### Satz 3.2 (Deduktionstheorem der Aussagenlogik)

Es seien  $F, F_1, \dots, F_n$  und  $G$  beliebige aussagenlogische Formeln. Dann gilt:

$$\{F_1, \dots, F_n\} \cup \{F\} \vdash G \Leftrightarrow \{F_1, \dots, F_n\} \vdash F \rightarrow G$$

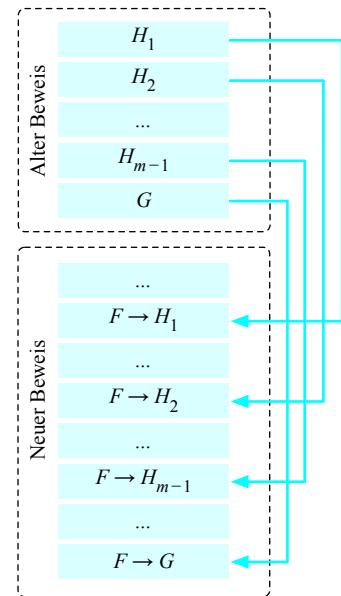
Das Deduktionstheorem ist in seiner Bedeutung nicht zu unterschätzen. Zum einen erlaubt es uns, zwischen der Logik- und der Meta-Ebene nach Belieben hin- und herzuspringen. Zum anderen wird es uns in die Lage versetzen, Beweise deutlich einfacher zu finden als bisher. Doch bevor wir das Deduktionstheorem produktiv einsetzen können, wollen wir uns zunächst von seiner Richtigkeit überzeugen.

Die Richtung von rechts nach links ist nahezu trivial. Gilt

$$\{F_1, \dots, F_n\} \vdash F \rightarrow G, \quad (3.10)$$

so existiert ein formaler Beweis, der  $F \rightarrow G$  aus  $\{F_1, \dots, F_n\}$  ableitet. Die Schlusskette können wir zu einem Beweis verlängern, der  $G$  aus  $\{F_1, \dots, F_n, F\}$  ableitet. Hierzu setzen wir  $F$  zunächst als Instanz ein und leiten  $G$  anschließend durch die Modus-Ponens-Schlussregel aus  $F \rightarrow G$  und  $F$  ab (vgl. Abbildung 3.14).

Die Schlussrichtung von links nach rechts erfordert etwas mehr Aufwand, folgt aber dem gleichen Schema. Ausgehend von einem Beweis für  $G$  aus  $\{F_1, \dots, F_n\} \cup \{F\}$  werden wir einen Beweis für  $F \rightarrow G$  aus  $\{F_1, \dots, F_n\}$  konstruieren. Das Grundschema des neuen Beweises ist in Abbildung 3.15 skizziert. Aus der vorhandenen Beweiskette  $H_1, \dots, H_{m-1}, G$  erzeugen wir eine neue, in der nacheinander die Formeln  $F \rightarrow H_i$  abgeleitet werden und am Ende die zu beweisende Behauptung  $F \rightarrow G$  steht. Beachten Sie, dass die Abbildung lediglich die Grobstruktur der Beweiskette festgelegt, da zwischen den Formeln Leerräume gelassen wurden. Die folgenden Ableitungssequenzen zeigen, wie diese genau zu füllen sind. Wir unterscheiden drei Fälle:



**Abbildung 3.15:** Beweisschema des Deduktionstheorems (Schlussrichtung von links nach rechts)

Theorem T1
$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$
Theorem T2
$A \rightarrow ((A \rightarrow B) \rightarrow B)$
Theorem T3
$\neg\neg A \rightarrow A$
Theorem T4
$A \rightarrow \neg\neg A$
Theorem T5
$(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$
Theorem T6
$A \rightarrow (\neg B \rightarrow \neg(A \rightarrow B))$
Theorem T7
$\neg A \rightarrow (A \rightarrow B)$
Theorem T8
$\neg(A \rightarrow B) \rightarrow A$
Theorem T9
$\neg(A \rightarrow B) \rightarrow \neg B$

**Tabelle 3.6:** Übersicht über die in Abbildung 3.16 bewiesenen Theoreme

- $H_i$  ist ein Axiom oder eine Voraussetzung  
 $\vdash H_i$   
 $\vdash H_i \rightarrow (F \rightarrow H_i)$  (A1)  
 $\vdash (F \rightarrow H_i)$  (MP)

- $H_i$  ist die Formel  $F$   
 $\vdash (F \rightarrow ((F \rightarrow F) \rightarrow F))$  (A1)  
 $\vdash (F \rightarrow ((F \rightarrow F) \rightarrow F)) \rightarrow ((F \rightarrow (F \rightarrow F)) \rightarrow (F \rightarrow F))$  (A2)  
 $\vdash (F \rightarrow (F \rightarrow F)) \rightarrow (F \rightarrow F)$  (MP)  
 $\vdash (F \rightarrow (F \rightarrow F))$  (A1)  
 $\vdash (F \rightarrow F)$  (MP)

- $H_i$  wurde durch die Regel (MP) aus  $H_j$  und  $H_j \rightarrow H_i$  erzeugt.

In diesem Fall wissen wir, dass die Formeln

$$(F \rightarrow H_j), \\ (F \rightarrow (H_j \rightarrow H_i))$$

bereits abgeleitet sind. Wir können den Beweis damit wie folgt ergänzen:

- $\vdash (F \rightarrow (H_j \rightarrow H_i)) \rightarrow ((F \rightarrow H_j) \rightarrow (F \rightarrow H_i))$  (A2)
- $\vdash (F \rightarrow H_j) \rightarrow (F \rightarrow H_i)$  (MP)
- $\vdash (F \rightarrow H_i)$  (MP)

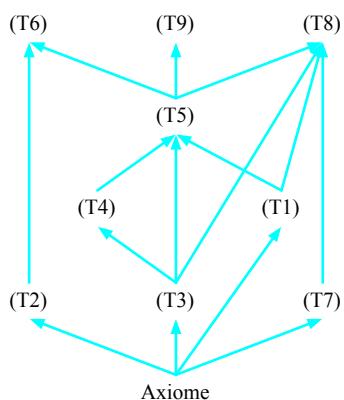
Damit ist das Deduktionstheorem bewiesen.

Die in Tabelle 3.6 zusammengefassten Formeln stammen aus [68] und sollen uns als Beispiele dienen, wie sich mit Hilfe des Deduktionstheorems Beweise führen lassen. Die einzelnen Ableitungssequenzen sind in Abbildung 3.16 zusammengefasst. Eine Analyse der Beweisketten zeigt, dass die Theoreme aufeinander aufbauen, d. h., es wird so oft wie möglich auf bereit bewiesene Ergebnisse zurückgegriffen. Welche Abhängigkeiten zwischen den Theoremen im Einzelnen bestehen, wird in Abbildung 3.17 grafisch verdeutlicht.

Beachten Sie, dass die entwickelten Ableitungssequenzen keine echten Beweise im Sinne des ursprünglichen Hilbert-Kalküls sind. Verantwortlich hierfür ist die Eigenschaft des Deduktionstheorems, eine Meta-Schlussregel zu sein, die Aussagen über Beweise macht und nicht innerhalb des Kalküls existiert. Mit jeder Anwendung des Deduktionstheorems treten wir gewissermaßen aus dem Kalkül heraus. Dass wir

$\blacksquare (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$	(T1)	$\{A \rightarrow B\} \vdash \neg\neg A \rightarrow A$	(T3)
$\{A \rightarrow B, B \rightarrow C, A\} \vdash A$	(trivial)	$\{A \rightarrow B\} \vdash (A \rightarrow B) \rightarrow (\neg\neg A \rightarrow B)$	(T1+MP)
$\{A \rightarrow B, B \rightarrow C, A\} \vdash A \rightarrow B$	(trivial)	$\{A \rightarrow B\} \vdash A \rightarrow B$	(trivial)
$\{A \rightarrow B, B \rightarrow C, A\} \vdash B$	(MP)	$\{A \rightarrow B\} \vdash \neg\neg A \rightarrow B$	(MP)
$\{A \rightarrow B, B \rightarrow C, A\} \vdash B \rightarrow C$	(trivial)	$\{A \rightarrow B\} \vdash B \rightarrow \neg\neg B$	(T4)
$\{A \rightarrow B, B \rightarrow C, A\} \vdash C$	(MP)	$\{A \rightarrow B\} \vdash (B \rightarrow \neg\neg B) \rightarrow (\neg\neg A \rightarrow \neg\neg B)$	(T1+MP)
$\{A \rightarrow B, B \rightarrow C\} \vdash A \rightarrow C$	(DT)	$\{A \rightarrow B\} \vdash \neg\neg A \rightarrow \neg\neg B$	(MP)
$\{A \rightarrow B\} \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)$	(DT)	$\{A \rightarrow B\} \vdash \neg B \rightarrow \neg A$	(MP)
$\vdash (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$	(DT)	$\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$	(DT)
<hr/>			
$\blacksquare A \rightarrow ((A \rightarrow B) \rightarrow B)$	(T2)	$\blacksquare A \rightarrow (\neg B \rightarrow \neg(A \rightarrow B))$	(T6)
$\{A, A \rightarrow B\} \vdash A$	(trivial)	$\{A\} \vdash (A \rightarrow B) \rightarrow B$	(T2+DT)
$\{A, A \rightarrow B\} \vdash A \rightarrow B$	(trivial)	$\{A\} \vdash (A \rightarrow B) \rightarrow B \rightarrow (\neg B \rightarrow \neg(A \rightarrow B))$	(T5)
$\{A, A \rightarrow B\} \vdash B$	(MP)	$\{A\} \vdash \neg B \rightarrow \neg(A \rightarrow B)$	(MP)
$\{A\} \vdash (A \rightarrow B) \rightarrow B$	(DT)	$\{A\} \vdash A \rightarrow (\neg B \rightarrow \neg(A \rightarrow B))$	(DT)
$\vdash A \rightarrow ((A \rightarrow B) \rightarrow B)$	(DT)	<hr/>	
<hr/>			
$\blacksquare \neg\neg A \rightarrow A$	(T3)	$\blacksquare \neg A \rightarrow (A \rightarrow B)$	(T7)
$\vdash \neg\neg A \rightarrow (\neg\neg\neg A \rightarrow \neg\neg A)$	(A1)	$\{\neg A\} \vdash \neg B \rightarrow \neg A$	(A1+DT)
$\{\neg\neg A\} \vdash \neg\neg\neg A \rightarrow \neg\neg A$	(DT)	$\{\neg A\} \vdash (\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$	(A3)
$\{\neg\neg A\} \vdash (\neg\neg\neg A \rightarrow \neg\neg A) \rightarrow (\neg A \rightarrow \neg\neg\neg A)$	(A3)	$\{\neg A\} \vdash (A \rightarrow B)$	(MP)
$\{\neg\neg A\} \vdash \neg A \rightarrow \neg\neg\neg A$	(MP)	$\vdash \neg A \rightarrow (A \rightarrow B)$	(DT)
$\{\neg\neg A\} \vdash (\neg A \rightarrow \neg\neg\neg A) \rightarrow (\neg\neg A \rightarrow A)$	(A3)	<hr/>	
$\{\neg\neg A\} \vdash \neg\neg A \rightarrow A$	(MP)	$\blacksquare \neg(A \rightarrow B) \rightarrow A$	(T8)
$\{\neg\neg A\} \vdash A$	(DT)	$\vdash \neg A \rightarrow (A \rightarrow B)$	(T7)
$\vdash \neg\neg A \rightarrow A$	(DT)	$\vdash (\neg A \rightarrow (A \rightarrow B)) \rightarrow (\neg(A \rightarrow B) \rightarrow \neg\neg A)$	(T5)
<hr/>			
$\blacksquare A \rightarrow \neg\neg A$	(T4)	$\vdash \neg(A \rightarrow B) \rightarrow \neg\neg A$	(MP)
$\vdash \neg\neg A \rightarrow \neg A$	(T3)	$\vdash \neg\neg A \rightarrow A$	(T3)
$\vdash (\neg\neg A \rightarrow \neg A) \rightarrow (A \rightarrow \neg\neg A)$	(A3)	$\vdash ((\neg\neg A \rightarrow A) \rightarrow (\neg(A \rightarrow B) \rightarrow A))$	(T1+MP)
$\vdash A \rightarrow \neg\neg A$	(MP)	$\vdash \neg(A \rightarrow B) \rightarrow A$	(MP)
<hr/>			
$\blacksquare (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$	(T5)	$\blacksquare \neg(A \rightarrow B) \rightarrow \neg B$	(T9)
$\{A \rightarrow B\} \vdash (\neg\neg A \rightarrow \neg\neg B) \rightarrow (\neg B \rightarrow \neg A)$	(A3)	$\vdash B \rightarrow (A \rightarrow B)$	(A1)
		$(B \rightarrow (A \rightarrow B)) \rightarrow (\neg(A \rightarrow B) \rightarrow \neg B)$	(T5)
		$\vdash \neg(A \rightarrow B) \rightarrow \neg B$	(MP)

Abbildung 3.16: Beweisführung im Hilbert-Kalkül



**Abbildung 3.17:** Die Beweise der Theoreme T1 bis T9 sind so angelegt, dass so oft wie möglich auf bereits bewiesene Ergebnisse zurückgegriffen wird. Der dargestellte Graph macht deutlich, welche Abhängigkeiten zwischen den Einzelbeweisen bestehen.

die Ableitungssequenzen trotzdem als Beweis ansehen dürfen, verdanken wir unserer geleisteten Vorarbeit. Weiter oben haben wir gezeigt, wie sich jede mit (DT) markierte Ableitung durch eine äquivalente Ableitungssequenz ersetzen lässt, die ohne das Deduktionstheorem auskommt. In diesem Sinne können wir die gezeigten Ableitungssequenzen als Bauplan verstehen, aus dem sich systematisch eine *echte* Beweiskette erzeugen lässt.

Abschließend wollen wir uns mit der Frage beschäftigen, wie es um die Korrektheit und Vollständigkeit des Hilbert-Kalküls in der hier vorgestellten Form steht. Wie wir in Definition 3.11 formal fixiert haben, ist ein Kalkül genau dann korrekt, wenn sich ausschließlich wahre Aussagen beweisen lassen (aus  $\vdash F$  folgt  $\models F$ ). Vollständig ist er genau dann, wenn alle wahren Aussagen innerhalb des Kalküls abgeleitet werden können (aus  $\models F$  folgt  $\vdash F$ ).

Die Korrektheit des Hilbert-Kalküls liegt auf der Hand. Zunächst lässt sich zeigen, dass alle Axiome allgemeingültig sind. Im Übungsteil auf Seite 147 dürfen Sie sich durch das Aufstellen der Wahrheitstabellen selbst davon überzeugen. Ferner ist leicht nachzuvollziehen, dass die einzige Schlussregel des Kalküls – der Modus ponens – die Tautologie-eigenschaft erhält. Mit anderen Worten: Sind die Prämissen allgemeingültig, so ist es auch die Konklusion. Damit sind alle ableitbaren Formeln Tautologien und der Hilbert-Kalkül im Sinne von Definition 3.11 korrekt.

Die Vollständigkeit des Hilbert-Kalküls ist weit weniger offensichtlich. Sie erfordert einen komplizierten Beweis, den wir hier nur grob in seiner Struktur skizzieren wollen. Er besteht aus zwei Teilen, in denen die folgenden Teilaussagen nacheinander gezeigt werden:

- Teilaussage 1: „Aus  $M \not\models F$  folgt:  $M \cup \{\neg F\}$  ist konsistent.“  
Wie in Definition 3.13 vereinbart, heißt eine Formelmenge  $M$  konsistent, wenn für keine Formel  $F$  sowohl  $F$  als auch  $\neg F$  gleichzeitig aus  $M$  abgeleitet werden kann.
- Teilaussage 2: „Jede konsistente Menge hat ein Modell“  
Die Aussage kann konstruktiv bewiesen werden, indem die Formelmenge iterativ um weitere Elemente angereichert wird. Sobald der Konstruktionsprozess endet, lässt sich aus der Ergebnismenge ein Modell extrahieren.

Zusammen führen beide Teilaussagen zu folgender Überlegung: Aus  $M \not\models F$  folgt, dass  $M \cup \{\neg F\}$  ein Modell besitzt. Dann gilt aber  $M \not\models F$  und im Umkehrschluss schließlich  $M \models F \Rightarrow M \vdash F$ .

### 3.1.3.2 Resolutionskalkül

Der Hilbert-Kalkül besticht zum einen durch seine einfache Struktur und zum anderen durch seine Vorgehensweise, die sich eng an jene der klassischen Mathematik anlehnt. Für die praktische Anwendung ist er jedoch nur eingeschränkt geeignet, da Beweise oft nur mit Mühe gefunden werden können. Die Suche wird insbesondere dadurch erschwert, dass in vielen Beweisen Instanzen der Axiome nach einem Schema erzeugt werden müssen, das auf den ersten Blick kaum ersichtlich ist.

In diesem Abschnitt werden wir mit dem *Resolutionskalkül* eine deutlich praktikablere Methode kennen lernen. Der Kalkül fällt in die Klasse der Widerspruchskalküle und setzt eine Formel in Klauseldarstellung voraus. Ein Resolutionsbeweis wird geführt, indem die Klauselmenge so lange erweitert wird, bis keine neuen Elemente mehr gebildet werden können oder die leere Klausel  $\square$  erzeugt wurde.

Für die Bildung neuer Klauseln steht die in Abbildung 3.18 dargestellte *Resolutionsregel* zur Verfügung. Sie lässt sich auf jedes Klauselpaar anwenden, das eine gemeinsame Variable  $A$  mit unterschiedlichen Vorzeichen enthält. Die neu erzeugte Klausel heißt *Resolvente* und wird gebildet, indem die Ausgangsklauseln vereinigt und alle Vorkommen von  $A$  und  $\neg A$  entfernt werden.

Das Ziel eines Resolutionsbeweises ist es, die leere Klausel  $\square$  abzuleiten. Hierzu sind im Allgemeinen mehrere Resolutionsschritte notwendig, die sich übersichtlich in einem *Resolutionsbaum* darstellen lassen (vgl. Abbildung 3.19). Beachten Sie, dass der Kalkül ausschließlich auf Formeln in Klauseldarstellung arbeitet und die Eingabe im Rahmen einer Vorverarbeitung zunächst in eine konjunktive Form gebracht werden muss.

Alles in allem setzt sich ein vollständiger Resolutionsbeweis aus drei Schritten zusammen, die nacheinander durchlaufen werden müssen:

- Die zu beweisende Formel  $F$  wird negiert und in eine konjunktive Form gebracht.
- $\neg F$  wird in die Klauseldarstellung überführt.
- Durch die kontinuierliche Bildung neuer Resolventen wird die leere Klausel  $\square$  erzeugt.

Als Beispiel werden wir versuchen, die Allgemeingültigkeit der Formel

$$(A \leftrightarrow B) \vee (A \leftrightarrow C) \vee (B \leftrightarrow C) \quad (3.11)$$

#### ■ Resolutionsregel

$$\frac{\{A\} \cup M_1 \quad \{\neg A\} \cup M_2}{M_1 \cup M_2}$$

#### ■ Beispiel 1

$$\frac{\{A, B\} \quad \{\neg A, \neg C\}}{\{B, \neg C\}}$$

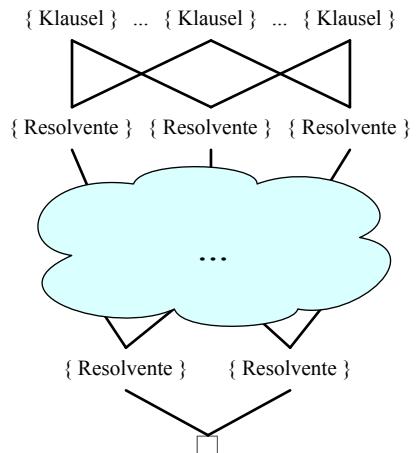
#### ■ Beispiel 2

$$\frac{\{B, \neg C\} \quad \{\neg B, \neg C\}}{\{\neg C\}}$$

#### ■ Beispiel 3

$$\frac{\{C\} \quad \{\neg C\}}{\square}$$

**Abbildung 3.18:** Aussagenlogische Resolventenbildung



**Abbildung 3.19:** Allgemeines Schema eines Resolutionsbeweises

$$\{A, B\} \quad \{\neg A, \neg C\} \quad \{\neg A, \neg B\} \quad \{B, C\}$$

$$\{\neg B, \neg C\} \quad \{A, C\}$$



$$\begin{array}{cccc} \{A, B\} & \{\neg A, \neg C\} & \{\neg A, \neg B\} & \{B, C\} \\ \diagdown & \diagup & \diagup & \diagdown \\ \{B, \neg C\} & \{\neg B, \neg C\} & \{A, C\} & \{\neg A, C\} \end{array}$$



$$\begin{array}{cccc} \{A, B\} & \{\neg A, \neg C\} & \{\neg A, \neg B\} & \{B, C\} \\ \diagdown & \diagup & \diagup & \diagdown \\ \{B, \neg C\} & \{\neg B, \neg C\} & \{A, C\} & \{\neg A, C\} \\ \diagdown & \diagup & \diagdown & \diagup \\ \{\neg C\} & & \{C\} & \end{array}$$



$$\begin{array}{cccc} \{A, B\} & \{\neg A, \neg C\} & \{\neg A, \neg B\} & \{B, C\} \\ \diagdown & \diagup & \diagup & \diagdown \\ \{B, \neg C\} & \{\neg B, \neg C\} & \{A, C\} & \{\neg A, C\} \\ \diagdown & \diagup & \diagdown & \diagup \\ \{\neg C\} & & \{C\} & \\ \diagdown & \diagup & & \\ \square & & & \end{array}$$

**Abbildung 3.20:** Schrittweise Konstruktion des Resolutionsbaums

mit Hilfe des Resolutionskalküls zu beweisen. Im ersten Schritt wird die Formel negiert und in eine konjunktive Form gebracht:

$$\begin{aligned} & \neg((A \leftrightarrow B) \vee (A \leftrightarrow C) \vee (B \leftrightarrow C)) \\ & \equiv \neg(A \leftrightarrow B) \wedge \neg(A \leftrightarrow C) \wedge \neg(B \leftrightarrow C) \\ & \equiv (A \leftrightarrow B) \wedge (A \leftrightarrow C) \wedge (B \leftrightarrow C) \\ & \equiv (A \vee B) \wedge (\neg A \vee \neg B) \wedge (A \vee C) \\ & \quad (\neg A \vee \neg C) \wedge (B \vee C) \wedge (\neg B \vee \neg C) \end{aligned}$$

In Klauselform ausgedrückt erhalten wir die folgende Darstellung:

$$\{A, B\}, \{\neg A, \neg B\}, \{A, C\}, \{\neg A, \neg C\}, \{B, C\}, \{\neg B, \neg C\}$$

Abbildung 3.20 zeigt schrittweise, wie sich der Resolutionsbaum aus der ursprünglichen Klauselmenge aufbauen lässt. Nach 5 Regelanwendungen ist die leere Klausel  $\square$  erzeugt und damit die Unerfüllbarkeit der Klauselmenge bewiesen.

Als Nächstes wollen wir das in Abschnitt 3.1.1 eingeführte Schubfachprinzip mit Hilfe der aussagenlogischen Resolution beweisen. Ausgangspunkt ist die in Abbildung 3.8 eingeführte Formel für 3 Gegenstände und 2 Schubfächer:

$$F = \left( \begin{array}{l} (A_{11} \vee A_{12}) \wedge \\ (A_{21} \vee A_{22}) \wedge \\ (A_{31} \vee A_{32}) \end{array} \right) \rightarrow \left( \begin{array}{l} A_{11}A_{21} \vee A_{11}A_{31} \vee A_{21}A_{31} \vee \\ A_{12}A_{22} \vee A_{12}A_{32} \vee A_{22}A_{32} \end{array} \right)$$

Im ersten Schritt transformieren wir die negierte Formel  $\neg F$  in eine konjunktive Form. Wir erhalten das nachstehende Ergebnis:

$$\begin{aligned} \neg F \equiv & (A_{11} \vee A_{12}) \wedge (A_{21} \vee A_{22}) \wedge (A_{31} \vee A_{32}) \wedge \\ & (\neg A_{11} \vee \neg A_{21}) \wedge (\neg A_{11} \vee \neg A_{31}) \wedge (\neg A_{21} \vee \neg A_{31}) \wedge \\ & (\neg A_{12} \vee \neg A_{22}) \wedge (\neg A_{12} \vee \neg A_{32}) \wedge (\neg A_{22} \vee \neg A_{32}) \end{aligned}$$

In Klauseldarstellung liest sich die Formel wie folgt:

$$\begin{array}{lll} \{A_{11}, A_{12}\}, & \{A_{21}, A_{22}\}, & \{A_{31}, A_{32}\} \\ \{\neg A_{11}, \neg A_{21}\}, & \{\neg A_{11}, \neg A_{31}\}, & \{\neg A_{21}, \neg A_{31}\} \\ \{\neg A_{12}, \neg A_{22}\}, & \{\neg A_{12}, \neg A_{32}\}, & \{\neg A_{22}, \neg A_{32}\} \end{array} \quad (3.12)$$

Abbildung 3.21 zeigt, dass sich aus der konstruierten Menge die leere Klausel  $\square$  ableiten lässt. Damit ist die Gültigkeit des Dirichlet'schen Schubfachprinzips formal bewiesen.

Die beiden Beispiele geben einen ersten Eindruck, wie sich die Allgemeingültigkeit von aussagenlogischen Formeln im Resolutionskalkül

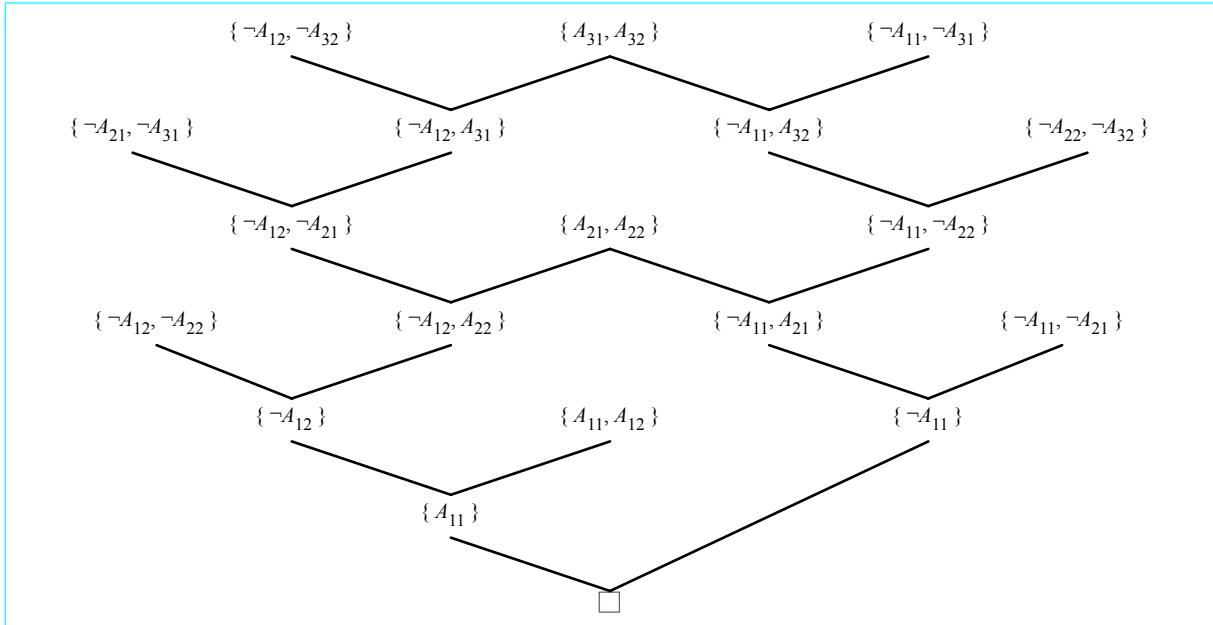


Abbildung 3.21: Formaler Beweis des Schubfachprinzips

beweisen lässt. Damit ist es an der Zeit, dass wir uns über die Korrektheit und Vollständigkeit des Kalküls Gedanken machen. Die Korrektheit der Resolutionsmethode ist offensichtlich. Ist  $M$  eine Klauselmenge und  $F$  eine ableitbare Resolvente, so besitzen  $M$  und  $M \cup \{F\}$  die gleichen Modelle. Ist es möglich,  $M$  um die leere Klausel  $\square$  zu ergänzen, so kann  $M$  kein Modell besitzen, da jedes Modell für  $F$  auch ein Modell für  $M \cup \{\square\}$  und damit auch ein Modell für  $\square$  sein müsste. Die leere Klausel  $\square$  steht jedoch stellvertretend für den Wahrheitswert 0 und damit für eine unerfüllbare Formel. Genau wie im Falle des Hilbert-Kalküls lässt sich zeigen, dass der Resolutionskalkül vollständig ist, d. h., für jede unerfüllbare Menge sind wir in der Lage, die leere Klausel  $\square$  auch wirklich abzuleiten.

Der Resolutionskalkül besticht vor allem durch seine einfache Anwendbarkeit, schließlich ist eine einzige Regel ausreichend, um den kompletten Beweis zu führen. Ferner müssen keine Formelinstanzen aus dem Nichts generiert werden, wie es im Hilbert-Kalkül der Fall ist. Die Achillesferse des Resolutionskalküls ist die Vorverarbeitung. Liegt eine Formel nicht in konjunktiver Form vor, so muss diese vorab erzeugt werden. Eine entsprechende Umformung ist zwar immer möglich, allerdings nimmt die Anzahl der resultierenden Klauseln für viele aussagen-

$P_n$	Klauseldarstellung		
$n = 2$	$\{\neg A_1, \neg A_2\}$		$\{A_1, A_2\}$
$n = 3$	$\{\neg A_1, \neg A_2, \neg A_3\}$ $\{A_1, A_2, \neg A_3\}$	$\{\neg A_1, A_2, A_3\}$	$\{A_1, \neg A_2, A_3\}$
$n = 4$	$\{\neg A_1, \neg A_2, \neg A_3, \neg A_4\}$ $\{\neg A_1, A_2, A_3, \neg A_4\}$ $\{A_1, A_2, \neg A_3, \neg A_4\}$	$\{\neg A_1, \neg A_2, A_3, A_4\}$ $\{A_1, \neg A_2, \neg A_3, A_4\}$ $\{A_1, A_2, A_3, A_4\}$	$\{\neg A_1, A_2, \neg A_3, A_4\}$ $\{A_1, \neg A_2, A_3, \neg A_4\}$
$n = 5$	$\{\neg A_1, \neg A_2, \neg A_3, \neg A_4, \neg A_5\}$ $\{\neg A_1, \neg A_2, A_3, A_4, \neg A_5\}$ $\{\neg A_1, A_2, A_3, \neg A_4, \neg A_5\}$ $\{A_1, \neg A_2, \neg A_3, A_4, \neg A_5\}$ $\{A_1, A_2, \neg A_3, \neg A_4, \neg A_5\}$ $\{A_1, A_2, A_3, A_4, \neg A_5\}$	$\{\neg A_1, \neg A_2, \neg A_3, A_4, A_5\}$ $\{\neg A_1, A_2, \neg A_3, \neg A_4, A_5\}$ $\{\neg A_1, A_2, A_3, A_4, A_5\}$ $\{A_1, \neg A_2, A_3, \neg A_4, \neg A_5\}$ $\{A_1, A_2, \neg A_3, A_4, A_5\}$	$\{\neg A_1, \neg A_2, A_3, \neg A_4, A_5\}$ $\{\neg A_1, A_2, \neg A_3, A_4, \neg A_5\}$ $\{A_1, \neg A_2, \neg A_3, \neg A_4, A_5\}$ $\{A_1, \neg A_2, A_3, A_4, A_5\}$ $\{A_1, A_2, A_3, \neg A_4, A_5\}$
$n = 6$	$\{\neg A_1, \neg A_2, \neg A_3, \neg A_4, \neg A_5, \neg A_6\}$ $\{\neg A_1, \neg A_2, \neg A_3, A_4, A_5, \neg A_6\}$ $\{\neg A_1, \neg A_2, A_3, A_4, \neg A_5, \neg A_6\}$ $\{\neg A_1, A_2, \neg A_3, \neg A_4, A_5, \neg A_6\}$ $\{\neg A_1, A_2, A_3, \neg A_4, \neg A_5, \neg A_6\}$ $\{\neg A_1, A_2, A_3, A_4, A_5, \neg A_6\}$ $\{A_1, \neg A_2, \neg A_3, A_4, \neg A_5, \neg A_6\}$ $\{A_1, \neg A_2, A_3, \neg A_4, A_5, A_6\}$ $\{A_1, A_2, \neg A_3, \neg A_4, \neg A_5, \neg A_6\}$ $\{A_1, A_2, \neg A_3, A_4, A_5, \neg A_6\}$ $\{A_1, A_2, A_3, A_4, \neg A_5, \neg A_6\}$	$\{\neg A_1, \neg A_2, \neg A_3, \neg A_4, A_5, A_6\}$ $\{\neg A_1, \neg A_2, A_3, \neg A_4, \neg A_5, A_6\}$ $\{\neg A_1, \neg A_2, A_3, A_4, A_5, A_6\}$ $\{\neg A_1, A_2, \neg A_3, A_4, \neg A_5, \neg A_6\}$ $\{\neg A_1, A_2, A_3, \neg A_4, A_5, A_6\}$ $\{A_1, \neg A_2, \neg A_3, \neg A_4, \neg A_5, A_6\}$ $\{A_1, \neg A_2, \neg A_3, A_4, A_5, A_6\}$ $\{A_1, \neg A_2, A_3, A_4, \neg A_5, A_6\}$ $\{A_1, A_2, \neg A_3, \neg A_4, A_5, A_6\}$ $\{A_1, A_2, \neg A_3, A_4, A_5, \neg A_6\}$	$\{\neg A_1, \neg A_2, \neg A_3, A_4, \neg A_5, A_6\}$ $\{\neg A_1, \neg A_2, A_3, \neg A_4, A_5, \neg A_6\}$ $\{\neg A_1, A_2, \neg A_3, \neg A_4, \neg A_5, A_6\}$ $\{\neg A_1, A_2, \neg A_3, A_4, A_5, A_6\}$ $\{\neg A_1, A_2, A_3, \neg A_4, A_5, A_6\}$ $\{A_1, \neg A_2, \neg A_3, \neg A_4, A_5, \neg A_6\}$ $\{A_1, \neg A_2, \neg A_3, A_4, A_5, \neg A_6\}$ $\{A_1, \neg A_2, A_3, A_4, A_5, \neg A_6\}$ $\{A_1, A_2, \neg A_3, \neg A_4, A_5, A_6\}$ $\{A_1, A_2, \neg A_3, A_4, A_5, \neg A_6\}$

**Tabelle 3.7:** Im Allgemeinen wächst die Klauseldarstellung exponentiell mit der Formelgröße an, hier demonstriert am Beispiel der Paritätsfunktion  $P_n = A_1 \leftrightarrow A_2 \leftrightarrow \dots \leftrightarrow A_n$ .

logische Ausdrücke exponentiell mit der Formellänge zu. Eindrucksvoll lässt sich das Phänomen am Beispiel der  $n$ -stelligen Paritätsfunktion

$$P_n := A_1 \leftrightarrow A_2 \leftrightarrow \dots \leftrightarrow A_n$$

demonstrieren (vgl. Tabelle 3.7). Für die Praxis bedeutet dieses Ergebnis, dass die konjunktive Form vieler realer Formeln nicht mehr darstellbar ist. An den Einsatz des Resolutionskalküls ist in diesen Fällen nicht zu denken, da der Beweis bereits an der Vorverarbeitung scheitert. Trotzdem gibt es keinen Grund, vorschnell die Waffen zu strecken. Im nächsten Abschnitt werden wir mit dem semantischen Tableau einen Kalkül kennen lernen, der die geschilderte Limitierung beseitigt und auf jegliche Vorverarbeitungen der zu beweisenden Formel verzichtet.

### 3.1.3.3 Tableaukalkül

#### Tableau

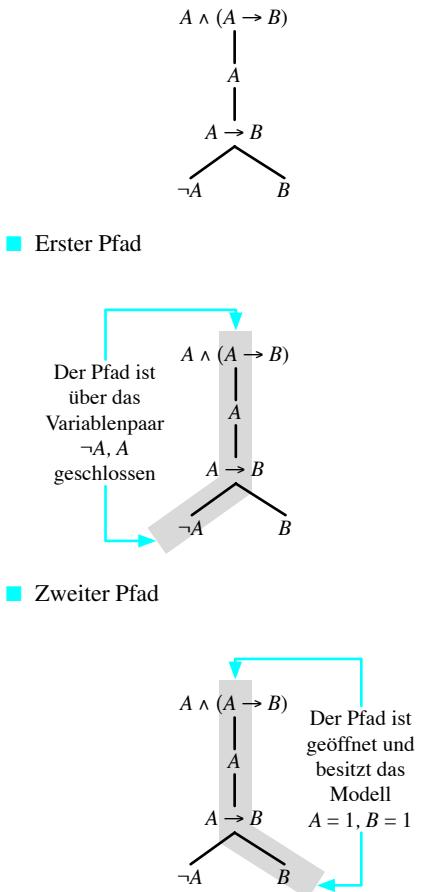
Der Tableaukalkül gehört wie der Resolutionskalkül zur Gruppe der Widerspruchskalküle, d. h., die Allgemeingültigkeit einer Formel  $F$  wird über die Unerfüllbarkeit der negierten Formel  $\neg F$  bewiesen. Trotz dieser Gemeinsamkeit ist die Art der Beweisführung eine völlig andere. Im Tableaukalkül wird eine Formel schrittweise in eine Baumstruktur – das sogenannte *Tableau* – transformiert, aus dem sich die zu beweisenden Formeleigenschaften ablesen lassen. Das Verfahren besticht durch zwei wesentliche Merkmale. Zum einen lässt sich das Tableau einer Formel  $F$  direkt aus den Teilformeln von  $F$  erzeugen, so dass eine Vorverarbeitung, wie sie im Resolutionskalkül notwendig ist, vollständig entfällt. Zum anderen lässt sich der Kalkül einsetzen, um Modelle für erfüllbare Formeln zu erzeugen. Schlägt ein Beweis fehl, so kann aus dem konstruierten Tableau eine erfüllende Variablenbelegung für  $F$  abgelesen werden. Jede solche Variablenbelegung spielt die Rolle eines *Gegenbeispiels*, das die Unerfüllbarkeit von  $F$  widerlegt.

Ein aussagenlogisches Tableau für eine Formel  $F$  ist durch zwei Eigenschaften charakterisiert:

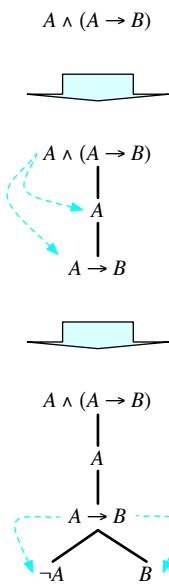
- Jeder Knoten ist mit einer Teilformel oder einer negierten Teilformel von  $F$  beschriftet.
- Für jedes Modell  $I$  von  $F$  existiert ein Pfad, so dass  $I$  ein gemeinsames Modell für alle Formeln dieses Pfads ist.

Als Beispiel ist in Abbildung 3.22 ein Tableau für die aussagenlogische Formel  $F := A \wedge (A \rightarrow B)$  dargestellt. Innerhalb des Tableaus existieren zwei Pfade, die potenzielle Modelle von  $F$  repräsentieren. Der linke Pfad enthält mit  $A$  und  $\neg A$  zwei Formeln, die kein gemeinsames Modell besitzen. Ein Pfad mit dieser Eigenschaft heißt *geschlossen* oder *widersprüchlich*. Der rechte Pfad enthält kein widersprüchliches Variablenpaar und lässt sich zur Konstruktion eines Modells verwenden. Setzen wir  $A = 1$  und  $B = 1$ , so sind alle Formeln des rechten Pfads und auch  $F$  selbst erfüllt. Ein Pfad mit dieser Eigenschaft heißt *offen* oder *widerspruchsfrei*.

Verallgemeinert gilt: Ist ein aussagenlogisches Tableau einer Formel  $F$  vorhanden, so können wir die Modelle von  $F$  an den offenen Pfaden ablesen. Kommt eine Variable auf dem Pfad positiv vor ( $A$ ), so wird sie mit dem Wahrheitswert 1 belegt. Kommt sie dagegen negativ vor ( $\neg A$ ), so wird ihr der Wahrheitswert 0 zugewiesen. Alle anderen Variablen dürfen beliebige Werte besitzen, so dass ein offener Pfad im Allgemeinen mehrere Modelle gleichzeitig repräsentiert.



**Abbildung 3.22:** Aussagenlogisches Tableau für die Formel  $A \wedge (A \rightarrow B)$



**Abbildung 3.23:** Schrittweise Konstruktion des aussagenlogischen Tableaus für die Formel  $A \wedge (A \rightarrow B)$

Es bleibt zu klären, wie wir für eine aussagenlogische Formel  $F$  ein entsprechendes Tableau systematisch konstruieren können. Für unsere Beispieldfunktion  $F$  lässt es sich ganz einfach über die folgende Überlegung herleiten:

- Im ersten Schritt wird ein Tableau erzeugt, das über einen einzigen, mit der Formel  $A \wedge (A \rightarrow B)$  beschrifteten Knoten verfügt (vgl. Abbildung 3.23 oben).
- Auf der obersten Ebene besitzt  $F$  die Form einer Konjunktion, so dass alle Modelle von  $F$  auch Modelle der beiden Teilausdrücke  $A$  und  $A \rightarrow B$  sein müssen. Damit können wir den initialen Pfad unseres Tableaus um die Formeln  $A$  und  $A \rightarrow B$  erweitern, ohne die oben formulierte Modelleigenschaft zu verletzen: Für jedes Modell  $I$  von  $F$  existiert weiterhin ein Pfad, so dass  $I$  ein gemeinsames Modell für alle Formeln dieses Pfads ist (vgl. Abbildung 3.23 Mitte).
- Das expandierte Tableau enthält mit  $A \rightarrow B$  eine neue Teilformel, die weiter zerlegt werden kann. Entsprechend der Semantik des Implikationsoperators ist  $A \rightarrow B$  genau dann wahr, wenn  $\neg A$  wahr oder  $B$  wahr ist. Die versteckte Disjunktion zwingt uns zu einer Fallunterscheidung, die innerhalb des Tableaus durch eine Verzweigung dargestellt wird (vgl. Abbildung 3.23 unten). Der linke Zweig entspricht dem Fall  $A = 0$  ( $\neg A$  ist wahr), der rechte Zweig dem Fall  $B = 1$  ( $B$  ist wahr).

Die Beispielkonstruktion verdeutlicht die Grundprinzipien, nach denen Tableaus für beliebige Formeln erzeugt werden können. Ausgehend von der initialen Formel wird diese sukzessive in ihre Bestandteile zerlegt und das Tableau schrittweise expandiert. Ein Zweig, auf dem ein komplementäres Variablenpaar entsteht, ist geschlossen und bedarf keiner weiteren Bearbeitung. Offene Pfade werden dagegen so lange erweitert, bis sämtliche Teilformeln zerlegt wurden. Ein solcher Pfad heißt *vollständig*.

Bisher haben wir stets von geschlossenen, offenen und vollständigen *Pfaden* gesprochen. Die Begriffe lassen sich in intuitiver Weise auf vollständige Tableaus übertragen. Wir nennen ein Tableau *geschlossen*, wenn alle seine Pfade geschlossen sind. Folgerichtig ist ein Tableau *offen* bzw. *widerspruchsfrei*, wenn mindestens ein offener Pfad existiert. Ein Tableau heißt *vollständig*, wenn alle offenen Pfade vollständig sind.

Damit lässt sich die Beweisführung im Tableaukalkül wie folgt zusammenfassen: Um die Allgemeingültigkeit einer Formel  $F$  zu zeigen, konstruieren wir ein *vollständiges* Tableau für  $\neg F$ . Ist es geschlossen, so

besitzt  $\neg F$  kein Modell und die Formel  $F$  ist als Tautologie identifiziert. Ist das Tableau offen, so existiert mindestens ein offener Pfad. Diesen können wir verwenden, um eine erfüllbare Belegung für  $\neg F$  abzulesen. Die Variablenbelegung ist ein Gegenbeispiel, das die Allgemeingültigkeit von  $F$  widerlegt.

In Abbildung 3.24 sind die Konstruktionsregeln für alle aussagenlogischen Operatoren zusammengefasst. Da sie in direkter Weise die Operatorensemantik nachbilden, können sie mit denselben Überlegungen hergeleitet werden, die wir für die Konstruktion unseres Beispieltableaus angestellt haben.

Betrachten wir die Regeln von einem abstrakteren Standpunkt, so lassen sich diese in zwei Gruppen einteilen. Die Vertreter der ersten Gruppe ( $\alpha$ -Regeln) besitzen einen konjunktiven Charakter und bewirken die Verlängerung eines Pfads. Die Vertreter der zweiten Gruppe ( $\beta$ -Regeln) besitzen einen disjunktiven Charakter und führen zu einer Verzweigung. In Abhängigkeit des angewandten Regeltyps sprechen wir folgerichtig von einer  $\alpha$ - oder einer  $\beta$ -Expansion eines Tableaus.

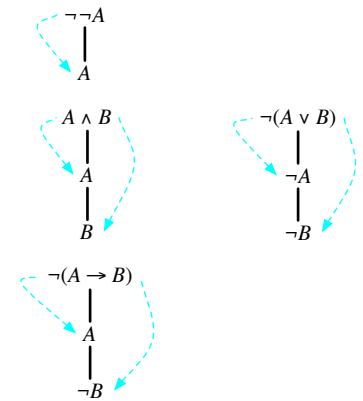
Plakativ ausgedrückt sind  $\alpha$ -Expansionen gutmütiger als  $\beta$ -Expansionen, da sie die Anzahl der Pfade innerhalb des Tableaus nicht vergrößern. Welche Konsequenzen sich hieraus ergeben, machen die beiden in Abbildung 3.25 dargestellten Tableaus für die Formel

$$\neg((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)))$$

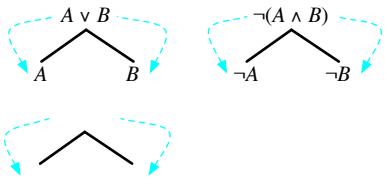
deutlich. Während das linke Tableau 6 Pfade besitzt, kommt die rechte Variante mit 4 Pfaden aus. Ein Blick auf die Reihenfolge der expandierten Formeln bringt den Grund für die unterschiedliche Größenentwicklung zum Vorschein. Im linken Tableau wurden zuerst die  $\beta$ -Expansionen und anschließend die  $\alpha$ -Expansionen ausgeführt. Hierdurch entstehen frühzeitige Verzweigungen, die das Tableau merklich anwachsen lassen. Im rechten Tableau wurde stattdessen mit den  $\alpha$ -Regeln begonnen. Hierdurch wird die Verzweigung verzögert und ein insgesamt kleineres Tableau erzeugt. Für die praktische Beweisführung ist es immer sinnvoll, die  $\alpha$ -Regeln vor den  $\beta$ -Regeln anzuwenden.

In Abbildung 3.26 ist als weiteres Beispiel der formale Beweis des Dirichlet'schen Schubfachprinzips dargestellt. Das entstehende Tableau enthält insgesamt 12 Pfade, die allesamt geschlossen sind. Damit ist auch das Tableau selbst geschlossen und das Schubfachprinzip formal bewiesen. Im Gegensatz zum Resolutionsbeweis aus Abbildung 3.21 bedarf die ursprüngliche Formel keinerlei Vorverarbeitung.

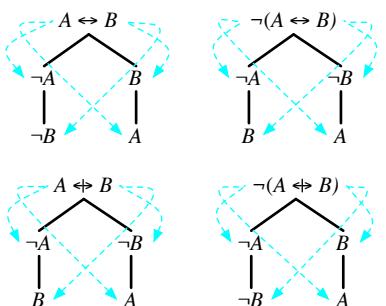
#### ■ $\alpha$ -Expansionen



#### ■ $\beta$ -Expansionen



#### ■ Kombinierte $\alpha/\beta$ -Expansionen



**Abbildung 3.24:** Expansionsregeln des aussagenlogischen Tableaukalküls

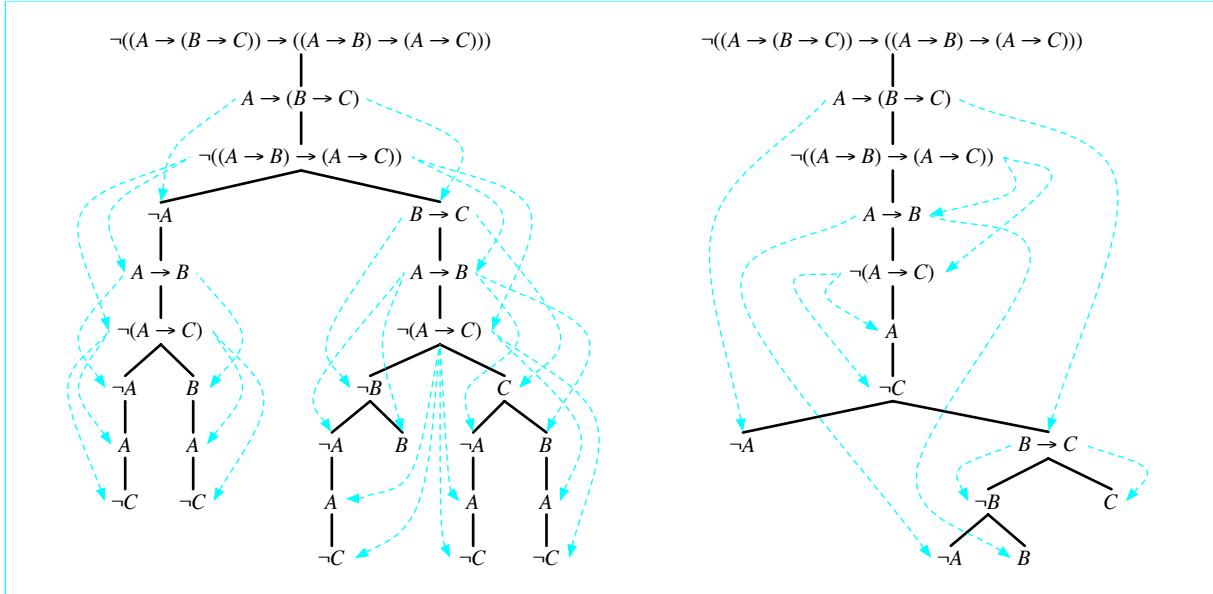


Abbildung 3.25: Die Reihenfolge, in der  $\alpha$ - und  $\beta$ -Regeln angewendet werden, beeinflusst die Größe eines Tableaus.

### 3.1.4 Anwendung: Hardware-Entwurf

Weiter oben haben wir gleich an mehreren Stellen die Bedeutung der Aussagenlogik für den digitalen Schaltungsentwurf angesprochen. In diesem Abschnitt wollen wir den Zusammenhang zwischen aussagenlogischen Formeln auf der einen Seite und Hardware-Schaltungen auf der anderen Seite genauer beleuchten. Konkret werden wir zeigen, wie sich Hardware-Schaltungen mit den Mitteln der Aussagenlogik systematisch entwerfen lassen.

Als Beispiel betrachten wir die in Abbildung 3.27 dargestellte Addition zweier Binärzahlen. Wie die Beispielrechnung zeigt, werden Zahlen im Binärsystem nach dem gleichen Schema addiert, das wir aus dem vertrauten Dezimalsystem kennen. Wir müssen lediglich darauf achten, einen Übertrag zu generieren, sobald die Summe zweier Ziffern größer als 1 ist. Im unteren Teil von Abbildung 3.27 ist das allgemeine Additionsschema dargestellt. Um die Addition zweier Binärzahlen mit Hilfe von Logikformeln abbilden zu können, codieren wir das  $i$ -te Bit der beiden Summanden mit den aussagenlogischen Variablen  $A_i$  und  $B_i$ . Die Variable  $Z_i$  beschreibt das  $i$ -te Summenbit und die Variable  $C_i$  den potenziellen Übertrag, der an der  $i$ -ten Bitstelle entsteht.

#### ■ Beispiel: $92 + 106$

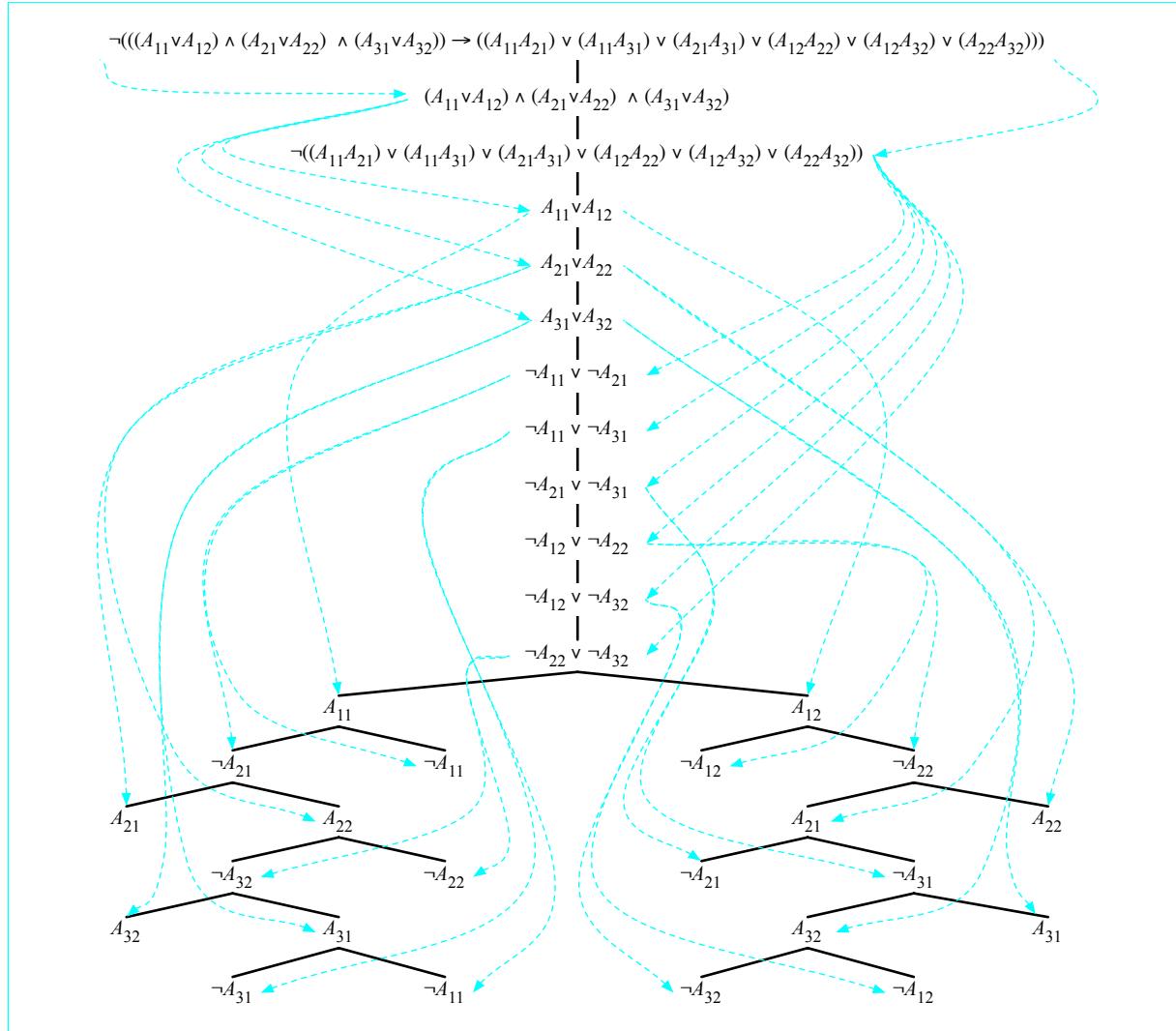
$$\begin{array}{r}
 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
 + & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
 \hline
 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0
 \end{array}$$

$$\begin{array}{r}
 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0
 \end{array}$$

#### ■ Allgemeines Additionsschema

$$\begin{array}{ccccccc}
 & A_n & \dots & A_3 & A_2 & A_1 & A_0 \\
 + & B_n & \dots & B_3 & B_2 & B_1 & B_0 \\
 & C_n & \dots & C_3 & C_2 & C_1 & \\
 \hline
 C_{n+1} & Z_n & \dots & Z_3 & Z_2 & Z_1 & Z_0
 \end{array}$$

Abbildung 3.27: Addition mehrstelliger Binärzahlen



**Abbildung 3.26:** Formaler Beweis des Schubfachprinzips im aussagenlogischen Tableaukalkül

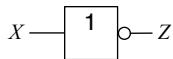
Aus dem Additionsschema können wir sofort die folgenden Beziehungen ableiten:

$$Z_i \equiv A_i \leftrightarrow B_i \leftrightarrow C_i \quad (3.13)$$

$$C_{i+1} \equiv A_i B_i \vee A_i C_i \vee B_i C_i \quad (3.14)$$

$$\equiv A_i B_i \vee C_i (A_i \leftrightarrow B_i) \quad (3.15)$$

■ NOT-Gatter



X	Z
0	1
1	0

$$Z \equiv \neg X$$

Der letzte Umformungsschritt ist nicht unmittelbar einsichtig und wird im Übungsteil auf Seite 144 bewiesen.

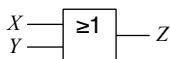
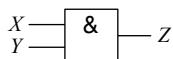
Um die weiter unten entwickelten Gleichungen übersichtlich zu halten, vereinbaren wir die folgenden Abkürzungen:

$$P_i := A_i \leftrightarrow B_i \quad (3.16)$$

$$G_i := A_i B_i \quad (3.17)$$

Jetzt lesen sich die Formeln (3.13) und (3.15) wie folgt:

■ AND-Gatter, OR-Gatter



X	Y	Z
0	0	0
0	1	0
1	0	0
1	1	1

$$Z \equiv X \wedge Y$$

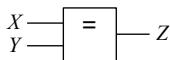
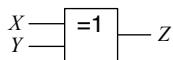
X	Y	Z
0	0	0
0	1	1
1	0	1
1	1	1

$$Z \equiv X \vee Y$$

Aus den beiden Gleichungen können wir ohne Umwege die Hardware-Implementierung eines Addierwerks ableiten. Hierzu identifizieren wir jede Variable mit einem Leitungssegment und erzeugen für jeden aussagenlogischen Operator ein physikalisches Logikgatter. In Abbildung 3.28 sind die Symbole sowie die berechneten Funktionen der wichtigsten Gatter in einer Übersicht zusammengefasst.

Beschränken wir uns auf die Verarbeitung von Zahlen der Bitbreite 4, so erhalten wir die in Abbildung 3.29 dargestellte Hardware-Schaltung. Auf den ersten Blick mögen die durcheinanderlaufenden Leitungen für mehr Verwirrung als Klärung sorgen. Nehmen Sie sich deshalb ein wenig Zeit und versuchen Sie, die Signalwege von den Ausgängen ( $Z_0, \dots, Z_3, C_4$ ) bis zu den Eingängen ( $A_0, \dots, A_3, B_0, \dots, B_3$ ) zurückzuverfolgen. Sie werden erkennen, dass die Formeln (3.18) und (3.19) eins zu eins durch die Hardware-Schaltung nachgebildet werden.

■ XOR-Gatter, NOXOR-Gatter



X	Y	Z
0	0	0
0	1	1
1	0	1
1	1	0

$$Z \equiv X \leftrightarrow Y$$

X	Y	Z
0	0	1
0	1	0
1	0	0
1	1	1

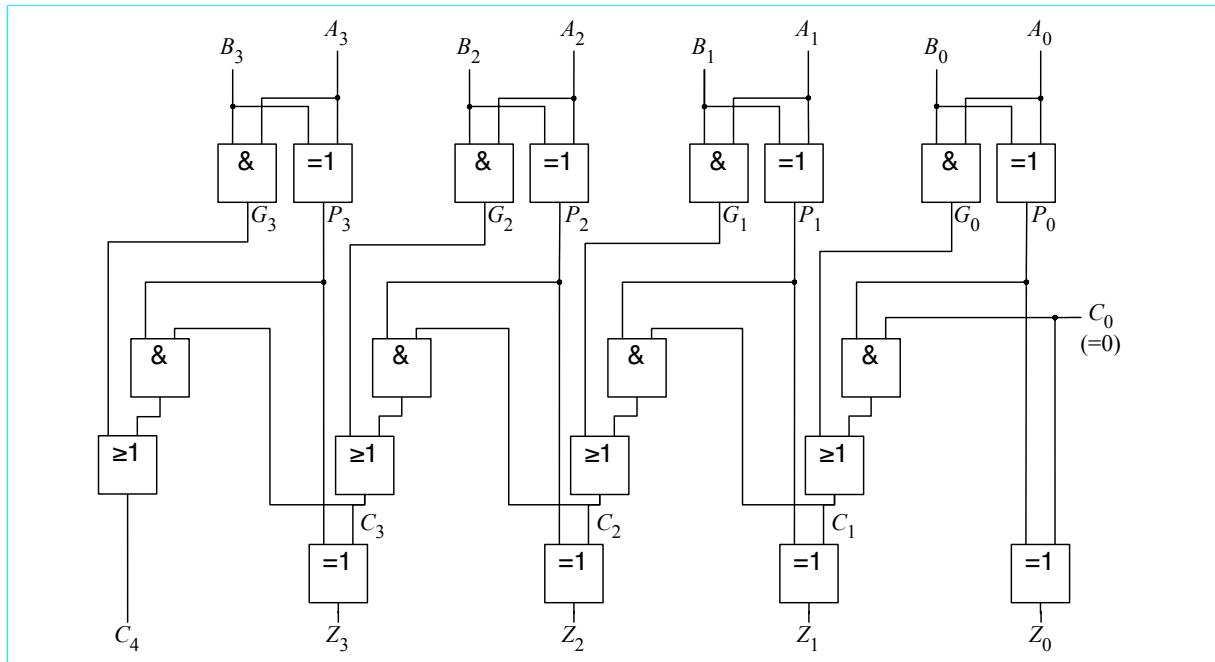
$$Z \equiv X \leftrightarrow Y$$

Die erzeugte Schaltung reicht das Übertragsbit (*carry bit*) von rechts nach links durch die gesamte Schaltung hindurch und wird aufgrund dieser Besonderheit als *Carry-ripple-Addierer* bezeichnet. Für große Bitbreiten wird das Addierwerk durch dieses Verhalten deutlich verlangsamt, da das  $i$ -te Summenbit erst berechnet werden kann, wenn das vorangegangene Übertragsbit vorliegt. Dieses kann wiederum erst dann berechnet werden, wenn das seinerseits vorangegangene Übertragsbit vorliegt und so fort. Der Carry-ripple-Addierer ist damit ausschließlich für Anwendungen geeignet, in denen die Kompaktheit der Schaltung wichtiger ist als die Geschwindigkeit.

Glücklicherweise sind wir mit Hilfe der Aussagenlogik in der Lage, die Hardware-Schaltung zu optimieren. Hierzu rollen wir die rekursiv definierte Formel

$$C_{i+1} \equiv G_i \vee C_i P_i \quad (3.20)$$

Abbildung 3.28: Logikgatter



**Abbildung 3.29:** Vollständig aufgebauter 4-Bit-Carry-ripple-Addierer

so lange aus, bis sämtliche Vorkommen von  $C_i$  mit  $i \neq 0$  aus der Formel verschwinden. Wir erhalten das folgende Ergebnis:

$$C_1 \equiv G_0 \vee C_0 P_0 \quad (3.21)$$

$$\begin{aligned} C_2 &\equiv G_1 \vee C_1 P_1 \\ &\equiv G_1 \vee (G_0 \vee C_0 P_0) P_1 \\ &\equiv G_1 \vee G_0 P_1 \vee C_0 P_0 P_1 \end{aligned} \quad (3.22)$$

$$\begin{aligned} C_3 &\equiv G_2 \vee C_2 P_2 \\ &\equiv G_2 \vee (G_1 \vee G_0 P_1 \vee C_0 P_0 P_1) P_2 \\ &\equiv G_2 \vee G_1 P_2 \vee G_0 P_1 P_2 \vee C_0 P_0 P_1 P_2 \end{aligned} \quad (3.23)$$

$$\begin{aligned} C_4 &\equiv G_3 \vee C_3 P_3 \\ &\equiv G_3 \vee (G_2 \vee G_1 P_2 \vee G_0 P_1 P_2 \vee C_0 P_0 P_1 P_2) P_3 \\ &\equiv G_3 \vee G_2 P_3 \vee G_1 P_2 P_3 \vee G_0 P_1 P_2 P_3 \vee C_0 P_0 P_1 P_2 P_3 \end{aligned} \quad (3.24)$$

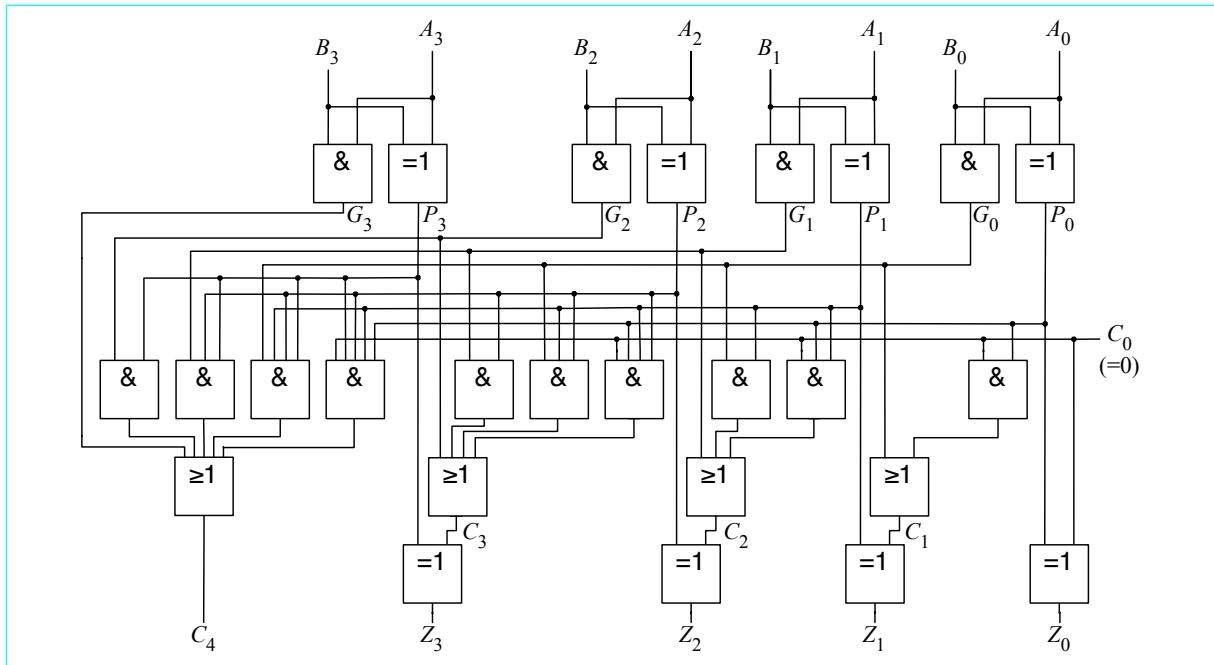


Abbildung 3.30: Vollständig aufgebauter 4-Bit-Carry-look-ahead-Addierer

Setzen wir die Formeln (3.21) bis (3.24) in eine Hardware-Schaltung um, so entsteht das in Abbildung 3.30 dargestellte Schaltnetz. Durch die getätigten Umformungen ist die *Tiefe* der Schaltung jetzt konstant, d.h., unabhängig von der Bitbreite durchläuft ein Signal von den Eingängen zu den Ausgängen eine konstante Anzahl an Logikgattern. Im Gegensatz zum Carry-ripple-Addierer werden die Übertragsbits jetzt direkt aus den Eingabebits erzeugt und damit in gewissem Sinne vorberechnet. Dieser Eigenschaft verdankt die Schaltung ihren Namen; sie wird in der Literatur als *Carry-look-ahead-Addierer* bezeichnet.

Vergleichen wir die Strukturbilder beider Addierer, so wird der Nachteil der geschwindigkeitsoptimierten Variante unmittelbar deutlich. Die Anzahl der Gatter, die für die Vorausberechnung eines Übertragsbits benötigt wird, vergrößert sich mit jeder Bitstelle. Hierdurch steigt der Flächenbedarf der Schaltung stark an. Wie stark die Größenzunahme wirklich ausfällt, werden wir im Detail klären, sobald in Kapitel 7 die formalen Grundlagen der Komplexitätstheorie gelegt wurden. Dort kommen wir im Übungsteil auf Seite 374 auf die spezielle Struktur des Carry-look-ahead-Addierers zurück.

## 3.2 Prädikatenlogik

In den vorhergehenden Abschnitten haben Sie gelernt, wie sich elementare Aussagen durch aussagenlogische Variablen repräsentieren lassen und diese zu komplexen Gebilden verknüpft werden können. Auch wenn sich viele Sachverhalte auf diese Weise beschreiben lassen, sind die Ausdrucksmöglichkeiten bei weitem nicht stark genug, um alle gängigen Aspekte des logischen Schließens abzubilden. Die Limitierungen, mit denen wir an dieser Stelle zu kämpfen haben, werden durch das folgende, in der Literatur häufig bemühte Beispiel deutlich:

1. Sokrates ist ein Mensch
2. Alle Menschen sind sterblich
3. Dann ist auch Sokrates sterblich

Die Eigenschaft, ein Mensch zu sein, ist eine parametrisierte Aussage der Form  $\text{Mensch}(x)$ , die in Abhängigkeit des Arguments wahr oder falsch wird. Für das Individuum  $x = \text{Sokrates}$  ist die Aussage wahr, für andere Werte von  $x$  sicherlich falsch. Eine atomare Aussage, deren Wahrheitswert durch ein oder mehrere eingesetzte Individuen bestimmt wird, bezeichnen wir als *Prädikat*. Die zweite Aussage macht eine quantitative Aussage über Individuen. Sie besagt, dass *alle* Menschen sterblich sind. Im Jargon der Logiker lässt sich die Aussage wie folgt ausdrücken: Für alle  $x$  gilt: Ist  $\text{Mensch}(x)$  eine wahre Aussage, dann ist auch  $\text{Sterblich}(x)$  eine wahre Aussage.

Erweitern wir die Aussagenlogik um mehrstellige Prädikate sowie um die Möglichkeit, quantifizierende Aussagen zu formulieren, so gelangen wir auf direktem Wege zur *Prädikatenlogik erster Stufe*. In ihr lässt sich das diskutierte Beispiel wie folgt formalisieren:

1.  $\text{Mensch}(\text{Sokrates})$
2.  $\forall x (\text{Mensch}(x) \rightarrow \text{Sterblich}(x))$
3.  $\models \text{Sterblich}(\text{Sokrates})$

Genau wie im Falle der Aussagenlogik werden wir Beweissysteme entwickeln, mit denen sich die Allgemeingültigkeit der soeben formulierten Aussage beweisen lässt. Um die Details solcher Kalküle richtig verstehen zu können, sind aber noch einige Vorarbeiten zu leisten. Zunächst wollen wir formal klären, was wir unter einem prädikatenlogischen Ausdruck genau zu verstehen haben.



The illustration shows a pair of stylized eyes with blue pupils looking upwards towards a thought bubble. The thought bubble contains the text: "aussagenlogische Variable = prädikatenlogische Variable?"

Die Aussagenlogik besitzt große Parallelen zur Prädikatenlogik und ist sogar vollständig als Teilmenge in ihr enthalten. Gerade deshalb ist Vorsicht angebracht, um gewisse Termini nicht zu verwechseln. Insbesondere der Begriff der Variablen erweist sich für viele Anfänger immer wieder als Fallstrick, da er in beiden Logiken mit einer unterschiedlichen Bedeutung belegt ist. In der Prädikatenlogik ist eine Variable ein Platzhalter für ein beliebiges Element einer festgelegten Grundmenge. Beispielsweise kann die Variable  $x$  in der Formel  $\text{Mensch}(x)$  stellvertretend für das Individuum *Sokrates* oder ein anderes Element der Grundmenge stehen. Erst die konkrete Wahl der Variablen  $x$  macht die Formel  $\text{Mensch}(x)$  zu einer wahren oder einer falschen Aussage. In der Aussagenlogik stehen Variablen dagegen für atomare Aussagen, die wahr oder falsch sein können. Damit sind sie in Wirklichkeit 0-stellige Prädikate und haben mit den prädikatenlogischen Variablen nur den Namen gemeinsam.

■ Signatur  $\Sigma$

$$\Sigma = (V_\Sigma, F_\Sigma, P_\Sigma) \text{ mit}$$

$$V_\Sigma = \{x, y\}$$

$$F_\Sigma = \{f \text{ (2-stellig)}\}$$

$$P_\Sigma = \{P \text{ (2-stellig)}\}$$

### 3.2.1 Syntax und Semantik

Die Syntaxdefinition der Prädikatenlogik erfolgt in drei Schritten. Zunächst führen wir den Begriff der *prädikatenlogischen Signatur* ein. Darauf aufbauend definieren wir den Begriff des *prädikatenlogischen Terms* und erweitern diesen anschließend zum Begriff der *prädikatenlogischen Formel*.

■ Terme über  $\Sigma$

$$\begin{aligned} &x \\ &y \\ &f(x, x) \\ &f(x, y) \\ &f(f(x, y), x) \\ &f(x, f(x, y)) \\ &f(f(x, x), f(x, y)) \\ &\dots \end{aligned}$$



#### Definition 3.14 (Prädikatenlogische Signatur)

Eine prädikatenlogische Signatur  $\Sigma$  ist ein Tripel  $(V_\Sigma, F_\Sigma, P_\Sigma)$ . Sie besteht aus

- einer Menge  $V_\Sigma = \{x_1, x_2, \dots\}$  von *Variablen*,
- einer Menge  $F_\Sigma = \{f_1, f_2, \dots\}$  von *Funktionssymbolen*,
- einer Menge  $P_\Sigma = \{P_1, P_2, \dots\}$  von *Prädikaten*.

Jede Funktion und jedes Prädikat besitzt eine feste Stelligkeit  $\geq 0$ .

■ Atomare Formeln über  $\Sigma$

$$\begin{aligned} &P(x, x) \\ &P(x, y) \\ &P(f(x, y), x) \\ &P(x, f(x, y)) \\ &P(x, f(f(x, y), x)) \\ &P(f(f(x, y), x), y) \\ &\dots \end{aligned}$$

Grob gesprochen definiert eine prädikatenlogische Signatur den Vorrat an elementaren Symbolen, aus denen eine Formel aufgebaut ist. Genau wie in der Aussagenlogik werden wir auch hier den Symbolvorrat von Fall zu Fall anpassen und z. B.  $x, y, z$  für  $x_1, x_2, x_3$ ,  $f, g, h$  für  $f_1, f_2, f_3$  und  $P, Q, R$  für  $P_1, P_2, P_3$  schreiben.



#### Definition 3.15 (Prädikatenlogischer Term)

Sei  $\Sigma = (V_\Sigma, F_\Sigma, P_\Sigma)$  eine prädikatenlogische Signatur. Die Menge der *prädikatenlogischen Terme* ist induktiv definiert:

- Jede Variable  $x \in V_\Sigma$  ist ein Term.
- Jedes 0-stellige Funktionssymbol  $f \in F_\Sigma$  ist ein Term.
- Sind  $f_1, \dots, f_n$  Terme und ist  $f \in F_\Sigma$  ein  $n$ -stelliges Funktionssymbol, so ist  $f(f_1, \dots, f_n)$  ein Term.

...

**Abbildung 3.31:** Schrittweise Konstruktion prädikatenlogischer Ausdrücke

Wie in Abbildung 3.31 (oben) demonstriert, lassen sich aus dem Symbolvorrat einer prädikatenlogischen Signatur im Allgemeinen unendlich viele Terme erzeugen. Eine besondere Bedeutung fällt dabei den 0-stelligen Funktionssymbolen zu. Diese besitzen keine Parameter und

spielen die Rolle von *Konstanten*. In unserem Eingangsbeispiel haben wir mit der Konstanten *Sokrates* bereits ein solches Funktionssymbol verwendet.

Mit den eingeführten Begriffen sind wir in der Lage, die Menge der *prädikatenlogischen Formeln* präzise zu definieren:



### Definition 3.16 (Syntax der Prädikatenlogik)

Sei  $\Sigma$  eine prädikatenlogische Signatur. Die Menge der *atomaren prädikatenlogischen Formeln* definieren wir wie folgt:

- Sind  $f_1, \dots, f_n$  Terme und  $P$  ein  $n$ -stelliges Prädikat, so ist  $P(f_1, \dots, f_n)$  eine atomare Formel.

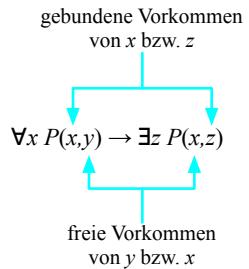
Die *prädikatenlogischen Formeln* sind induktiv definiert:

- Jede atomare Formel ist eine Formel.
- Ist  $x \in V_\Sigma$  und sind  $F$  und  $G$  Formeln, dann sind es auch  $0, 1, (\neg F), (F \wedge G), (F \vee G), (F \rightarrow G), (F \leftrightarrow G), (F \Leftrightarrow G), \forall x F, \exists x F$ .

Abbildung 3.31 (unten) zeigt eine kleine Auswahl erzeugbarer Formeln. Beachten Sie, dass nicht alle Variablen zwangsläufig im Wirkungsbereich eines Quantors stehen müssen. So kommt die Variable  $x$  in der Formel  $P(x, x)$  *frei* bzw. *ungebunden*, in der Formel  $\forall x P(x)$  dagegen *gebunden* vor. Das Beispiel in Abbildung 3.32 demonstriert, dass eine Variable in der gleichen Formel sowohl frei als auch gebunden vorkommen kann. Im Folgenden werden wir fast ausschließlich Formeln betrachten, in denen alle Variablenvorkommen durch Quantoren gebunden sind. Solche Formeln heißen *geschlossen*.

Der Umgang mit prädikatenlogischen Ausdrücken wird erheblich erleichtert, wenn die Variablen in zwei voneinander unabhängigen Teilausdrücken unterschiedlich benannt werden. Sind die quantifizierten Variablen einer *geschlossenen* Formel  $F$  paarweise verschieden, so sprechen wir von einer *bereinigten* Formel. Abbildung 3.33 zeigt, wie eine Formel  $F$  durch die Umbenennung mehrfach verwendeter Variablen in eine bereinigte Form gebracht werden kann.

Genau wie in der Aussagenlogik wird auch in der Prädikatenlogik die Semantik über eine *Modellrelation*  $\models$  festgelegt. Um diese zu definieren, müssen wir zunächst den Begriff Interpretation auf prädikatenlogische Formeln erweitern:



**Abbildung 3.32:** Steht eine Variable im Wirkungsbereich eines Quantors, so sprechen wir von einem *gebundenen* Vorkommen, ansonsten von einem *freien* Vorkommen. Formeln, in denen alle Variablenvorkommen gebunden sind, heißen *geschlossen*.

#### ■ Beispiel 1

$$\exists y \forall x P(x, y) \rightarrow \forall x \exists y P(x, y)$$

$$\exists y \forall x P(x, y) \rightarrow \forall v \exists w P(v, w)$$

#### ■ Beispiel 2

$$\exists x (P(x) \wedge \forall x Q(x))$$

$$\exists x (P(x) \wedge \forall y Q(y))$$

**Abbildung 3.33:** Eine geschlossene Formel wird *bereinigt*, indem mehrfach quantifizierte Variablen umbenannt werden. In der bereinigten Formel sind die quantifizierten Variablen paarweise verschieden.

■ Formel

$$F := \forall x \exists y P(f(x, y))$$

■ Signatur

$$V_\Sigma = \{x, y\}$$

$$F_\Sigma = \{f\}$$

$$P_\Sigma = \{P\}$$

■ Erste Interpretation

$$U := \mathbb{Z}$$

$$I(f) := (x, y) \mapsto x + y$$

$$I(P) := \{0\}$$

■ Zweite Interpretation

$$U := \mathbb{N}_0$$

$$I(f) := (x, y) \mapsto x + y$$

$$I(P) := \{0\}$$

**Abbildung 3.34:** Zwei Interpretationen für die Formel  $F := \forall x \exists y P(f(x, y))$



**Definition 3.17 (Prädikatenlogische Interpretation)**

Sei  $\Sigma = (V_\Sigma, F_\Sigma, P_\Sigma)$  eine prädikatenlogische Signatur. Eine *Interpretation*  $(U, I)$  über  $\Sigma$  besteht aus einer beliebigen nichtleeren Menge  $U$  und einer Abbildung  $I$ , die

- jedem  $n$ -stelligen Funktionssymbol  $f \in F_\Sigma$  eine Funktion

$$I(f) : U^n \rightarrow U \quad \text{und}$$

- jedem  $n$ -stelligen Prädikatsymbol  $P \in P_\Sigma$  eine Relation

$$I(P) \subseteq U^n \quad \text{zuordnet.}$$

Die Menge  $U$  wird in der Literatur als *Universum*, *Individuenbereich* oder *Grundmenge* bezeichnet. Beachten Sie, dass die getätigte Festlegung auch 0-stellige Funktions- und Prädikatsymbole mit einschließt. Einem 0-stelligen Funktionssymbol wird dann formal eine Funktion  $U^0 \rightarrow U$  zugeordnet, hinter der sich ein einzelnes Element aus dem Individuenbereich und damit eine Konstante verbirgt. 0-stellige Prädikatsymbole werden einer Relation  $U^0$  zugeordnet. Sie sind atomare Aussagen, die entweder wahr oder falsch sein können, und entsprechen damit eins zu eins den altbekannten aussagenlogischen Variablen.

Die Abbildung  $I$ , die jedem Funktionssymbol  $f$  eine Funktion  $I(f)$  zuordnet, lässt sich in naheliegender Weise auf variablenfreie Terme übertragen. Hierzu erweitern wir  $I$  nach dem folgenden induktiven Schema:

$$I(f(g_1, \dots, g_n)) := I(f)(I(g_1), \dots, I(g_n)) \tag{3.25}$$

Abbildung 3.34 demonstriert den Interpretationsbegriff anhand zweier Beispiele. Beide assoziieren das Funktionszeichen  $f$  mit der gewöhnlichen Addition und das Prädikatsymbol  $P$  mit der Nullmenge, d. h.,  $P(x)$  ist genau dann wahr, wenn  $x = 0$  ist. Unterschiedlich gewählt sind die zugrunde liegenden Individuenmengen. Die erste Interpretation schöpft aus dem Bereich der ganzen Zahlen, während die zweite Interpretation nur nichtnegative Zahlen in Betracht zieht. Unter diesen Voraussetzungen liest sich die Beispielformel  $F := \forall x \exists y P(f(x, y))$  wie folgt:

„Für alle  $x$  existiert ein  $y$  mit  $x + y = 0$ .“

Für die Menge der ganzen Zahlen ist die Aussage offensichtlich erfüllt, für die Teilmenge der nichtnegativen Zahlen dagegen nicht. Jetzt ist es an der Zeit, die informellen Überlegungen zu präzisieren und die Modellrelation  $\models$  formal einzuführen.



### Definition 3.18 (Semantik der Prädikatenlogik)

$F$  und  $G$  seien geschlossene prädikatenlogische Formeln und  $(U, I)$  eine Interpretation. Die Semantik der Prädikatenlogik ist durch die *Modellrelation*  $\models$  gegeben, die induktiv über dem Formelaufbau definiert ist:

- $(U, I) \models 1$
- $(U, I) \not\models 0$
- $(U, I) \models P(t_1, \dots, t_n) :\Leftrightarrow (I(t_1), \dots, I(t_n)) \in I(P)$
- $(U, I) \models (\neg F) :\Leftrightarrow (U, I) \not\models F$
- $(U, I) \models (F \wedge G) :\Leftrightarrow (U, I) \models F \text{ und } (U, I) \models G$
- $(U, I) \models (F \vee G) :\Leftrightarrow (U, I) \models F \text{ oder } (U, I) \models G$
- $(U, I) \models (F \rightarrow G) :\Leftrightarrow (U, I) \not\models F \text{ oder } (U, I) \models G$
- $(U, I) \models (F \leftrightarrow G) :\Leftrightarrow (U, I) \models F \text{ genau dann, wenn } (U, I) \models G$
- $(U, I) \models (F \Leftrightarrow G) :\Leftrightarrow (U, I) \not\models (F \leftrightarrow G)$
- $(U, I) \models \forall x F :\Leftrightarrow \text{Für alle } u \in U \text{ gilt } (U, I) \models F[x \leftarrow u]$
- $(U, I) \models \exists x F :\Leftrightarrow \text{Es gibt ein } u \in U \text{ mit } (U, I) \models F[x \leftarrow u]$

Eine Interpretation  $(U, I)$  mit  $(U, I) \models F$  heißt *Modell* für  $F$ .

In Definition 3.18 wird erstmals der Ausdruck  $F[x \leftarrow u]$  verwendet. Dieser entsteht aus  $F$ , indem die Vorkommen der Variablen  $x$  durch die Individualkonstante  $u$  ersetzt werden. Falls  $F$  Teilterme der Form  $\exists x F'$  oder  $\forall x F'$  besitzt, so bleiben diese unangetastet. Mit anderen Worten: Die Substitution ist so auszuführen, dass ausschließlich ungebundene Vorkommen von  $x$  ersetzt werden.

Der Begriff der *Substitution* wird uns an verschiedenen Stellen erneut begegnen. Allgemein formuliert handelt es sich dabei stets um eine Abbildung  $\sigma$ , die Variablen durch prädikatenlogische Terme ersetzt. Enthalten die eingesetzten Terme selbst keine Variablen, so sprechen wir von einer *Grundsubstitution* (vgl. Abbildung 3.35).

Genau wie im Falle der Aussagenlogik bezeichnen wir eine Formel  $F$  in der Prädikatenlogik als *erfüllbar*, wenn sie (mindestens) ein Modell besitzt. Ist jedes Modell einer Formelmenge  $M$  auch Modell einer Formel  $F$ , so schreiben wir  $M \models F$  („Aus  $M$  folgt  $F$ “). Ist ausnahmslos jede Interpretation ein Modell von  $F$ , gilt also  $\emptyset \models F$ , so ist  $F$  *allgemeingültig*. Wie gewohnt bezeichnen wir  $F$  in diesem Fall als *Tautologie* und verwenden die gekürzte Schreibweise  $\models F$ .

#### ■ Grundsubstitutionen

$$\begin{aligned}\sigma_1 &= [x \leftarrow a] \\ \sigma_2 &= [y \leftarrow b] \\ \sigma_3 &= [x \leftarrow a, y \leftarrow b]\end{aligned}$$

#### ■ Substitutionen

$$\begin{aligned}\sigma_4 &= [x \leftarrow y] \\ \sigma_5 &= [y \leftarrow f(y)] \\ \sigma_6 &= [x \leftarrow y, y \leftarrow f(y)]\end{aligned}$$

#### ■ Beispiele (ohne Quantoren)

$$\begin{aligned}\sigma_1 P(x, y) &= P(a, y) \\ \sigma_2 P(x, y) &= P(x, b) \\ \sigma_3 P(x, y) &= P(a, b) \\ \sigma_4 P(x, y) &= P(y, y) \\ \sigma_5 P(x, y) &= P(x, f(y)) \\ \sigma_6 P(x, y) &= P(y, f(y))\end{aligned}$$

#### ■ Beispiele (mit Quantoren)

$$\begin{aligned}\sigma_6 (\forall x P(x, y)) &= (\forall x P(x, f(y))) \\ \sigma_6 (\forall y P(x, y)) &= (\forall y P(y, y)) \\ \sigma_6 (\forall x \forall y P(x, y)) &= (\forall x \forall y P(x, y))\end{aligned}$$

**Abbildung 3.35:** Eine Variablensubstitution der Form  $[x \leftarrow t]$  ersetzt alle freien Vorkommen von  $x$  durch  $t$ . Alle gebundenen Vorkommen bleiben dagegen unangetastet.

■ Negationsnormalform

$$\begin{aligned}\neg\neg A &\equiv A \\ \neg(A \wedge B) &\equiv \neg A \vee \neg B \\ \neg(A \vee B) &\equiv \neg A \wedge \neg B \\ \neg(A \rightarrow B) &\equiv A \wedge \neg B \\ \neg(A \leftrightarrow B) &\equiv A \leftrightarrow B \\ \neg(A \leftrightarrow B) &\equiv A \leftrightarrow B \\ \neg\forall x F &\equiv \exists x \neg F \\ \neg\exists x F &\equiv \forall x \neg F\end{aligned}$$

■ Pränex-Form

$$\begin{aligned}F \wedge (\exists x G) &\equiv \exists x (F \wedge G), \quad x \notin F \\ (\exists x F) \wedge G &\equiv \exists x (F \wedge G), \quad x \notin G \\ F \wedge (\forall x G) &\equiv \forall x (F \wedge G), \quad x \notin F \\ (\forall x F) \wedge G &\equiv \forall x (F \wedge G), \quad x \notin G \\ F \vee (\exists x G) &\equiv \exists x (F \vee G), \quad x \notin F \\ (\exists x F) \vee G &\equiv \exists x (F \vee G), \quad x \notin G \\ F \vee (\forall x G) &\equiv \forall x (F \vee G), \quad x \notin F \\ (\forall x F) \vee G &\equiv \forall x (F \vee G), \quad x \notin G \\ F \rightarrow (\exists x G) &\equiv \exists x (F \rightarrow G), \quad x \notin F \\ (\exists x F) \rightarrow G &\equiv \exists x (F \rightarrow G), \quad x \notin G \\ F \rightarrow (\forall x G) &\equiv \forall x (F \rightarrow G), \quad x \notin F \\ (\forall x F) \rightarrow G &\equiv \forall x (F \rightarrow G), \quad x \notin G \\ F \leftrightarrow (\exists x G) &\equiv \exists x (F \leftrightarrow G), \quad x \notin F \\ (\exists x F) \leftrightarrow G &\equiv \exists x (F \leftrightarrow G), \quad x \notin G \\ F \leftrightarrow (\forall x G) &\equiv \forall x (F \leftrightarrow G), \quad x \notin F \\ (\forall x F) \leftrightarrow G &\equiv \forall x (F \leftrightarrow G), \quad x \notin G \\ F \leftrightarrow (\exists x G) &\equiv \exists x (F \leftrightarrow G), \quad x \notin F \\ (\exists x F) \leftrightarrow G &\equiv \exists x (F \leftrightarrow G), \quad x \notin G \\ F \leftrightarrow (\forall x G) &\equiv \forall x (F \leftrightarrow G), \quad x \notin F \\ (\forall x F) \leftrightarrow G &\equiv \forall x (F \leftrightarrow G), \quad x \notin G\end{aligned}$$

**Abbildung 3.36:** Umformungsregeln für die Erzeugung der Negationsnormalform (oben) und der Pränex-Form (unten)

### 3.2.2 Normalformen

Weiter oben haben wir herausgearbeitet, dass bestimmte Beweisverfahren der Aussagenlogik eine Vorverarbeitung der zu prüfenden Formeln benötigen. Das Gleiche gilt in der Prädikatenlogik. In diesem Abschnitt werden wir die wichtigsten Darstellungsformen für prädikatenlogische Formeln einführen und damit eine notwendige Vorarbeit für die in Abschnitt 3.2.3 diskutierten Beweisverfahren leisten.

Wir beginnen mit der einfachsten Normalform für prädikatenlogische Ausdrücke:



#### Definition 3.19 (Negationsnormalform)

Eine prädikatenlogische Formel  $F$  liegt in *Negationsnormalform* vor, wenn jedes Negationszeichen  $\neg$  vor einer atomaren Teilformel steht.

Die Negationsnormalform einer Formel  $F$  ist vergleichsweise einfach zu erzeugen. Die Grundlage hierfür bilden die in Abbildung 3.36 (oben) dargestellten Umformungsregeln.

Als Nächstes betrachten wir die *Pränex-Form*. Diese verfolgt die Idee, Quantoren aus tiefer liegenden Teiltermen in die oberste Formelebene zu verschieben.



#### Definition 3.20 (Pränex-Form)

Seien  $Q_i \in \{\forall, \exists\}$  prädikatenlogische Quantoren. Eine Formel  $F$  liegt in *Pränex-Form* vor, wenn sie die Form

$$Q_1 x_1 Q_2 x_2 \dots Q_n x_n F^*$$

besitzt und die Teilformel  $F^*$  keine weiteren Quantoren mehr enthält.  $F^*$  heißt die *Matrix* von  $F$ .

Die Pränex-Form lässt sich aus der Negationsnormalform erzeugen. Im ersten Schritte wird die Formel durch die Umbenennung mehrfach verwendeter Variablen bereinigt. Anschließend wird der Wirkungsbereich der Quantoren durch die Anwendung elementarer Umformungsregeln schrittweise vergrößert (vgl. Abbildung 3.36 unten). Ist keine Umformungsregel mehr anwendbar, so stehen die Quantoren bereits alle auf der linken Seite und die (bereinigte) Pränex-Form ist hergestellt.

Im nächsten Schritt wollen wir versuchen, die Existenzquantoren aus einer Formel zu eliminieren. Wir beginnen mit dem einfachsten Fall und betrachten eine Formel der Bauart  $\exists x F$ . Informell ausgedrückt ist die Formel genau dann wahr, wenn eine Belegung für  $x$  existiert, die  $F$  wahr werden lässt. Der Wert von  $x$  ist nicht davon abhängig, wie wir die anderen in  $F$  vorkommenden Variablen belegen. Daher können wir  $x$  ruhigen Gewissens durch ein neues Konstantensymbol  $u \notin F$  ersetzen und erhalten mit  $F[x \leftarrow u]$  eine Formel, die genau dann erfüllbar ist, wenn die ursprüngliche Formel  $\exists x F$  erfüllbar ist. Mit diesem Trick ist es uns gelungen, die ursprüngliche Formel in eine *erfüllbarkeitsäquivalente* Formel zu übersetzen, die keinen Existenzquantor mehr besitzt.

In einem anderen Licht stellt sich die Situation für Formeln der Bauart  $\forall x_1 \dots \forall x_n \exists x F$  dar. Informell ist eine solche Formel genau dann wahr, wenn für alle Wertekombinationen von  $x_1, \dots, x_n$  eine Belegung für  $x$  existiert, die  $F$  wahr werden lässt. Anders als im ersten Beispiel können wir  $x$  nicht einfach durch ein neues Konstantensymbol ersetzen, da die Belegung für  $x$  von der konkreten Belegung von  $x_1, \dots, x_n$  abhängt. Wenn aber für jede Wertekombination von  $x_1, \dots, x_n$  eine Belegung für  $x$  existiert, dann lässt sich der Wert von  $x$  durch eine  $n$ -stellige Funktion  $g$  berechnen. Folgerichtig können wir eine erfüllbarkeitsäquivalente Formel erzeugen, indem wir den Existenzquantor eliminieren und die Vorkommen von  $x$  durch den prädikatenlogischen Term  $g(x_1, \dots, x_n)$  mit  $g \notin F$  ersetzen. Die Stelligkeit des neuen Funktionssymbols  $g$  entspricht der Anzahl der Allquantoren, die links des eliminierten Existenzquantors stehen.

Damit haben wir alle Bausteine zusammengestellt, um sämtliche Existenzquantoren einer Formel  $F$  zu eliminieren. Über die Negationsnormalform erzeugen wir die bereinigte Pränex-Form und eliminieren dann sämtliche Existenzquantoren nach dem gezeigten Schema. Die entstehende Formel heißt die *Skolem-Form* von  $F$ .



### Definition 3.21 (Skolem-Form)

Eine prädikatenlogische Formel  $F$  liegt in *Skolem-Form* vor, wenn sie die Form

$$\forall x_1 \forall x_2 \dots \forall x_n F^*$$

besitzt und die Teilformel  $F^*$  keine weiteren Quantoren enthält.

$$\neg((\exists x \forall y P(f(x), y)) \vee (\exists x \forall y \neg Q(y, x)))$$

(Ausgangsformel)



$$\begin{aligned} &\neg((\exists x \forall y P(f(x), y)) \vee (\exists x \forall y \neg Q(y, x))) \\ &\equiv \neg(\exists x \forall y P(f(x), y)) \wedge \neg(\exists x \forall y \neg Q(y, x)) \\ &\equiv (\forall x \neg \forall y P(f(x), y)) \wedge (\forall x \neg \forall y \neg Q(y, x)) \\ &\equiv (\forall x \exists y \neg P(f(x), y)) \wedge (\forall x \exists y \neg \neg Q(y, x)) \\ &\equiv (\forall x \exists y \neg P(f(x), y)) \wedge (\forall x \exists y Q(y, x)) \end{aligned}$$

(Negationsnormalform)



$$\begin{aligned} &(\forall x \exists y \neg P(f(x), y)) \wedge (\forall x \exists y Q(y, x)) \\ &\equiv (\forall x \exists y \neg P(f(x), y)) \wedge (\forall z \exists w Q(w, z)) \\ &\quad (\text{Bereinigte Negationsnormalform}) \end{aligned}$$



$$\begin{aligned} &(\forall x \exists y \neg P(f(x), y)) \wedge (\forall z \exists w Q(w, z)) \\ &\equiv \forall x \exists y \forall z \exists w (\neg P(f(x), y) \wedge Q(w, z)) \\ &\quad (\text{Pränex-Form}) \end{aligned}$$



$$\begin{aligned} &\forall x \exists y \forall z \exists w (\neg P(f(x), y) \wedge Q(w, z)) \\ &\equiv_E \forall x \forall z \exists w (\neg P(f(x), g(x)) \wedge Q(w, z)) \\ &\equiv_E \forall x \forall z (\neg P(f(x), g(x)) \wedge Q(h(x, z), z)) \\ &\quad (\text{Skolem-Form}) \end{aligned}$$

**Abbildung 3.37:** Schrittweise Erzeugung der Skolem-Normalform

Abbildung 3.37 demonstriert die vollständige Umformungskette anhand eines konkreten Beispiels. Beachten Sie, dass die erzeugte Pränex-

$$(\forall x \exists y \neg P(f(x), y)) \wedge (\forall z \exists w Q(w, z))$$

(Bereinigte Negationsnormalform)



$$(\forall x \exists y \neg P(f(x), y)) \wedge (\forall z \exists w Q(w, z))$$

$$\equiv \forall z \exists w ((\forall x \exists y \neg P(f(x), y)) \wedge Q(w, z))$$

$$\equiv \forall z \exists w \forall x \exists y (\neg P(f(x), y) \wedge Q(w, z))$$

(Pränex-Form)



$$\forall z \exists w \forall x \exists y (\neg P(f(x), y) \wedge Q(w, z))$$

$$\equiv_E \forall z \forall x \exists y (\neg P(f(x), y) \wedge Q(h(z), z))$$

$$\equiv_E \forall z \forall x (\neg P(f(x), g(x, z)) \wedge Q(h(z), z))$$

(Skolem-Form)



**Abbildung 3.38:** Alternative Umformung.  
Im Allgemeinen sind die Pränex- und die Skolem-Form nicht eindeutig.

Form immer noch äquivalent zur ursprünglichen Formel ist, d. h. beide die gleichen Modelle besitzen. Im Gegensatz hierzu ist die Skolem-Form von  $F$  lediglich *erfüllbarkeitsäquivalent* zu  $F$ , geschrieben als  $F \equiv_E \text{Skolem}(F)$ . Mit anderen Worten: Aus der Erfüllbarkeit von  $F$  folgt die Erfüllbarkeit ihrer Skolem-Form und umgekehrt; trotzdem besitzen beide unterschiedliche Modelle. Obgleich die Erfüllbarkeitsäquivalenz eine schwächere Eigenschaft als die Äquivalenz ist, reicht sie aus, um z. B. die Allgemeingültigkeit einer Formel  $F$  zu beweisen. Können wir zeigen, dass die Skolem-Form von  $\neg F$  unerfüllbar ist, so ist auch  $\neg F$  unerfüllbar und  $F$  im Umkehrschluss als Tautologie identifiziert. In Abschnitt 3.2.3.1 werden wir die Skolem-Form im Zusammenhang mit der prädikatenlogischen Resolution wieder aufgreifen.

In der Literatur wird sowohl die Pränex-Form als auch die Skolem-Form häufig als Normalform bezeichnet. Im strengen Sinne ist dieser Begriff nicht korrekt, da beide Darstellungen nicht eindeutig sind. Abbildung 3.38 demonstriert, dass sich durch eine geänderte Abfolge der Regenanwendungen eine zweite Pränex-Form erzeugen lässt, in der die Quantoren anders angeordnet sind. Die geänderte Reihenfolge schlägt sich direkt auf die neu hinzugefügten Terme in der Skolem-Form nieder.

### 3.2.3 Beweistheorie

In diesem Abschnitt beschäftigen wir uns mit der Frage, wie die Allgemeingültigkeit einer prädikatenlogischen Formel systematisch bewiesen werden kann. Genau wie im Fall der Aussagenlogik werden wir verschiedene Kalküle definieren, die eine formale Ableitbarkeit wahrer Aussagen erlauben.

Um eine prädikatenlogische Formel  $F$  als Tautologie zu identifizieren, müssen wir zeigen, dass *jede* Interpretation ein Modell von  $F$  ist. Auf den ersten Blick mag es aussichtslos erscheinen, die Allgemeingültigkeit mit Hilfe eines mechanisch arbeitenden Kalküls zu beweisen. Schuld daran ist der in Definition 3.17 eingeführte Interpretationsbegriff, der uns mit einer wahren Flut an potenziellen Modellen überschüttet. Die große Anzahl kommt dadurch zustande, dass die Individuenmenge  $U$  einer Interpretation beliebig gewählt werden darf. Beispielsweise kann  $U$  die Menge der natürlichen Zahlen sein, alle Einwohner von Paris umfassen oder der Menge aller gleichschenkligen Dreiecke entsprechen. So unterschiedlich diese Interpretationen auch sind: Für ausnahmslos jede müssen wir zeigen, dass sie ein Modell von  $F$  ist.

In Wirklichkeit ist die Situation weniger aussichtslos, als sie an dieser Stelle wirken mag. Der französische Mathematiker Jacques Herbrand

(Abbildung 3.39) konnte zeigen, dass es gar nicht nötig ist, sämtliche in Frage kommenden Interpretationen zu untersuchen. Um eine Formel als Tautologie zu entlarven, ist es völlig ausreichend, die Suche auf die Klasse der *Herbrand-Interpretationen* zu beschränken. Um zu verstehen, wie eine solche Interpretation aufgebaut ist, führen wir zunächst den Begriff des *Herbrand-Universums* ein.



### Definition 3.22 (Herbrand-Universum)

Sei  $F$  eine prädikatenlogische Formel über der Signatur  $\Sigma$ . Das *Herbrand-Universum*  $HU(F)$  ist die Menge aller variablenfreien Terme, die mit Funktionssymbolen aus  $\Sigma$  gebildet werden können.

Aus der Signatur  $\Sigma = (V_\Sigma, F_\Sigma, P_\Sigma)$  einer prädikatenlogischen Formel  $F$  lässt sich das Herbrand-Universum rekursiv erzeugen:

- Alle Konstanten aus  $F_\Sigma$  gehören zu  $HU(F)$ .
- Ist  $f \in F_\Sigma$  ein  $n$ -stelliges Funktionszeichen und gehören  $t_1, \dots, t_n$  zu  $HU(F)$ , so gehört auch der Term  $f(t_1, \dots, t_n)$  zu  $HU(F)$ .

Nicht selten führt der Begriff des Herbrand-Universums zu Verständnisproblemen, da in gewissem Sinne eine Vermischung zwischen der syntaktischen und der semantischen Ebene stattfindet. Da die Grundmenge aus den Elementen von  $\Sigma$  erzeugt wird, beeinflusst die Syntax von  $F$  in direkter Weise den Individuenbereich, über dem die einzelnen Formelbestandteile interpretiert werden. Auch wenn die Konstruktion trickreich ist, spricht nichts gegen sie, da wir die Individuenmenge völlig frei wählen dürfen.

Die folgenden beiden Beispiele demonstrieren die Konstruktion des Herbrand-Universums:

- Beispiel 1:  $F = \forall x P(f(c, g(x)))$   
 $HU(F) = \{c, g(c), f(c, c), g(f(c, c)), f(g(c), c), f(g(c), g(c)), \dots\}$
- Beispiel 2:  $F = \exists x P(f(x))$   
 $HU(F) = \{a, f(a), f(f(a)), f(f(f(a))), f(f(f(f(a)))), \dots\}$

Das zweite Beispiel macht auf eine Besonderheit aufmerksam, die wir nicht vorschnell übergehen dürfen. Enthält  $\Sigma$  keine 0-stelligen Funktionssymbole, so lassen sich zunächst keine variablenfreien Terme bilden



Jacques Herbrand  
(1908 – 1931)

**Abbildung 3.39:** Jacques Herbrand wurde am 12. Februar 1908 in Paris geboren und bereits in seiner frühen Jugend erkannten die Eltern sein mathematisches Talent. Im Alter von 17 Jahren meisterte er mit Bravour die Aufnahmeprüfung der École Normale und begann sehr früh, ein ausgeprägtes Interesse für die Grundlagen der Mathematik zu entwickeln. 1929 promovierte Herbrand in mathematischer Logik und absolvierte anschließend seinen Militärdienst. Im Jahre 1931 eröffnete ihm ein Rockefeller-Stipendium die Möglichkeit, verschiedene Universitäten im Ausland zu besuchen. Unter anderen führte ihn seine Reise nach Berlin und Göttingen, wo er mit John von Neumann und Emmy Noether zusammentraf. Das Bild zeigt Jacques Herbrand in jungen Jahren. Später existieren nicht, da sein Leben im Alter von 23 Jahren ein frühes Ende fand. Vor seiner Rückkehr von Göttingen nach Frankreich kam er bei einem Wanderunfall in den Alpen zu Tode. Trotz seines frühen Ablebens ist Herbrands wissenschaftliches Vermächtnis immens. Seine Arbeiten auf dem Gebiet der mathematischen Logik bilden das theoretische Grundgerüst, auf dem die gesamte Beweistheorie der Prädikatenlogik beruht.

■ Formel

$$F := \forall x \exists y P(f(x, y))$$

■ Herbrand-Universum

$$\begin{aligned} HU(F) = & \{a, \\ & f(a, a), \\ & f(a, f(a, a)), \\ & f(f(a, a), f(a, a)), \\ & \dots \\ & \} \end{aligned}$$

■ Beispielinterpretation 1

$$\begin{aligned} U &= HU(F) \\ I(P) &= \emptyset \end{aligned}$$

■ Beispielinterpretation 2

$$\begin{aligned} U &= HU(F) \\ I(P) &= \{f(t, a) \mid t \in HU(F)\} \end{aligned}$$

■ Beispielinterpretation 3

$$\begin{aligned} U &= HU(F) \\ I(P) &= HU(F) \end{aligned}$$

**Abbildung 3.40:** Verschiedene Herbrand-Interpretationen für die prädikatenlogische Formel  $\forall x \exists y P(f(x, y))$

und das Herbrand-Universum würde zur leeren Menge degradieren. In diesem Fall lösen wir das Problem, indem wir der Menge  $F_\Sigma$  schlicht ein neues Konstantensymbol  $a$  hinzufügen. Die Änderung der Signatur hat keinen Einfluss auf die weiter unten erarbeiteten Ergebnisse.

Aufbauend auf dem Begriff des Herbrand-Universums führen wir den Begriff der *Herbrand-Interpretation* ein:



**Definition 3.23 (Herbrand-Interpretation)**

Sei  $F$  eine prädikatenlogische Formel über der Signatur  $\Sigma$ . Eine Interpretation  $(U, I)$  von  $F$  heißt *Herbrand-Interpretation*, falls

- $U = HU(F)$  und
- $I(t) = t$  für alle variablenfreien Terme  $t$ .

Eine Herbrand-Interpretation einer Formel  $F$  erfüllt demnach zwei charakteristische Eigenschaften. Zum einen entspricht die Grundmenge dem Herbrand-Universum  $HU(F)$ , d.h., der Individuenbereich ist die Menge der variablenfreien Terme, die aus den Funktionssymbolen von  $F$  gebildet werden können. Zum anderen ist die Zuordnung  $I$  so gestaltet, dass jeder variablenfreie Term  $t$  durch sich selbst interpretiert wird. Die Selbstinterpretation ist möglich, da als Grundmenge das Herbrand-Universum gewählt wurde und dieses alle variablenfreien Terme umfasst. In der Konsequenz unterscheiden sich Herbrand-Interpretationen ausschließlich im Umgang mit den Prädikatsymbolen (vgl. Abbildung 3.40).

Herbrand konnte zeigen, dass eine Formel  $F$  genau dann erfüllbar ist, wenn sie ein *Herbrand-Modell* besitzt. Hieraus folgt, dass  $F$  genau dann eine Tautologie ist, wenn die negierte Formel  $\neg F$  kein Herbrand-Modell besitzt. Der Zusammenhang hat weitreichende Konsequenzen für die Beweisführung, da wir die Suche nach Modellen auf die spezielle Menge der Herbrand-Interpretationen eingrenzen können. Mit einem Schlag gerät die automatisierte Beweisführung in greifbare Nähe. Den Durchbruch erzielte Herbrand mit dem folgenden Satz, den wir an dieser Stelle ohne Beweis akzeptieren wollen [42]:



**Satz 3.3 (Satz von Herbrand)**

Eine Formel  $F$  in Skolem-Form besitzt genau dann ein Herbrand-Modell, wenn alle endlichen Teilmengen der *Grundinstanzen* von  $F$  im aussagenlogischen Sinne erfüllbar sind.

Im Umkehrschluss besagt der Satz, dass eine Formel  $F$  in Skolem-Form genau dann unerfüllbar ist, wenn eine endliche Teilmenge der Grundinstanzen existiert, die im aussagenlogischen Sinne widersprüchlich ist. Die Menge der Grundinstanzen von  $F$  wird dabei erzeugt, indem alle Variablen durch Terme aus  $HU(F)$  und somit durch variablenfreie Terme ersetzt werden. Formal ist die Menge wie folgt definiert:



### Definition 3.24 (Grundinstanzen)

Sei  $\Sigma$  eine prädikatenlogische Signatur und  $F$  eine zu  $\Sigma$  passende Formel in Skolem-Form, d. h., es gilt:

$$F = \forall x_1 \dots \forall x_n F^*$$

Die Menge der *Grundinstanzen* von  $F$ , kurz  $G(F)$ , ist wie folgt definiert:

$$G(F) := \{F^*[x_1 \leftarrow t_1, \dots, x_n \leftarrow t_n] \mid t_1, \dots, t_n \in HU(F)\}$$

Für die praktische Beweisführung bedeutet der Satz von Herbrand das Folgende: Um die Allgemeingültigkeit einer Formel  $F$  zu beweisen, bilden wir zunächst die Negation  $\neg F$  und wählen eine passende Menge von Grundinstanzen aus. Jede atomare Formel behandeln wir als eigenständige aussagenlogische Variable. Können wir mit dem Instrumentarium der Aussagenlogik die Unerfüllbarkeit der konstruierten Menge nachweisen, so ist gezeigt, dass  $\neg F$  kein Herbrand-Modell besitzt. Damit besitzt  $\neg F$  überhaupt keine Modelle und  $F$  ist als Tautologie identifiziert. Als Beispiel betrachten wir die prädikatenlogische Formel

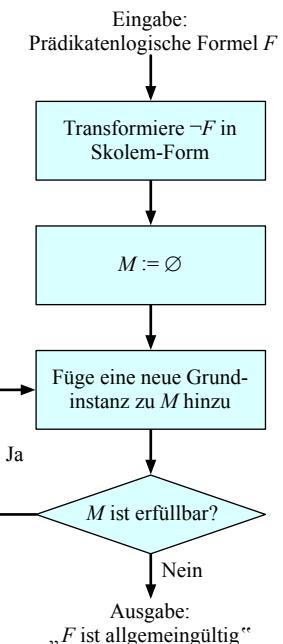
$$F := \exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$$

Um die Allgemeingültigkeit von  $F$  zu zeigen, bilden wir zunächst die Skolem-Form von  $\neg F$ :

$$\begin{aligned} \neg F &\equiv \neg(\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)) \\ &\equiv (\exists x \forall y P(x, y)) \wedge \neg(\forall y \exists x P(x, y)) \\ &\equiv (\exists x \forall y P(x, y)) \wedge (\exists y \forall x \neg P(x, y)) \\ &\equiv_E \forall y P(a, y) \wedge \forall x \neg P(x, b) \\ &\equiv \forall y \forall x (P(a, y) \wedge \neg P(x, b)) \end{aligned}$$

Aus der Skolem-Form können wir die folgenden Grundinstanzen von  $F$  ableiten:

$$\begin{aligned} G(F) &:= \{P(a, a) \wedge \neg P(a, b), P(a, a) \wedge \neg P(b, b), \\ &\quad P(a, b) \wedge \neg P(a, b), P(a, b) \wedge \neg P(b, b)\} \end{aligned}$$



**Abbildung 3.41:** Algorithmus von Gilmore

$$F = \exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$$



$$\neg F \equiv \exists x \forall y P(x, y) \wedge \exists y \forall x \neg P(x, y)$$



$$\text{Skolem}(F) = \forall y \forall x P(a, y) \wedge \neg P(x, b)$$

i	Grundinstanzen	Erfüllbar?
0	$\emptyset$	Ja
1	$P(a, a) \wedge \neg P(a, b)$	Ja
2	$P(a, a) \wedge \neg P(a, b), P(a, a) \wedge \neg P(b, b)$	Ja
3	$P(a, a) \wedge \neg P(a, b), P(a, a) \wedge \neg P(b, b), P(a, b) \wedge \neg P(a, b)$	Nein
Algorithmus terminiert		

$$\begin{aligned} \neg F &\text{ ist unerfüllbar} \\ \Rightarrow F &\text{ ist allgemeingültig} \end{aligned}$$

**Abbildung 3.42:** Algorithmus von Gilmore, hier angewendet auf die Formel  $\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$

### Die Teilmenge

$$\{P(a, b) \wedge \neg P(a, b)\}$$

ist offensichtlich unerfüllbar und damit die Allgemeingültigkeit von  $F$  bewiesen.

Aus den angestellten Überlegungen lässt sich der *Algorithmus von Gilmore* ableiten. Hierbei handelt es sich um ein konstruktives Verfahren, mit dem die Allgemeingültigkeit einer prädikatenlogischen Formel  $F$  systematisch bewiesen werden kann. Im Rahmen der Vorverarbeitung wird  $F$  negiert und in Skolem-Form überführt. Anschließend werden alle endlichen Teilmengen von  $G(F)$  gebildet. Dies kann in einem iterativen Prozess geschehen, der von der leeren Menge ausgeht und diese sukzessive um neue Formeln aus  $G(F)$  erweitert. Am Ende jedes Schritts wird die Menge mit Hilfe eines beliebigen aussagenlogischen Verfahrens auf Erfüllbarkeit geprüft. Ist die Menge unerfüllbar, so folgt aus dem Satz von Herbrand, dass die Formel  $\neg F$  kein Modell besitzt und  $F$  im Umkehrschluss eine allgemeingültige Formel sein muss. Abbildung 3.41 fasst die Arbeitsweise des Algorithmus von Gilmore grafisch zusammen.

In Abbildung 3.42 sind die Iterationsschritte dargestellt, die der Algorithmus von Gilmore für die diskutierte Beispielformel durchläuft. Ausgehend von der leeren Menge wird in jedem Schritt eine neue Grundinstanz hinzugefügt und die entstandene Menge auf Erfüllbarkeit geprüft. Nach 3 Iterationen ist eine unerfüllbare Teilmenge gefunden und die Ausgangsformel als Tautologie identifiziert.

Beachten Sie, dass der Algorithmus für unser Beispiel nach 4 Iterationen ebenfalls terminiert hätte, da  $G(F)$  in diesem speziellen Fall endlich ist. Die Endlichkeit von  $G(F)$  geht auf die Eigenschaft von  $F$  zurück, keine mehrstelligen Funktionssymbole zu enthalten. Kommt in einer Formel  $F$  mindestens ein  $n$ -stelliges Funktionssymbol mit  $n \geq 1$  vor, so lassen sich unendlich viele Grundinstanzen bilden und der Algorithmus terminiert nur dann, wenn eine unerfüllbare Teilmenge gefunden wird. Ist die bearbeitete Formel  $F$  keine Tautologie, so sind alle generierten Teilmengen erfüllbar und es entsteht eine Endlosschleife.

Anhand der folgenden Formel wollen wir dieses Verhalten genauer untersuchen:

$$F := \forall y \exists x P(x, y) \rightarrow \exists x \forall y P(x, y) \quad (3.26)$$

Die Formel unterscheidet sich von unserem ersten Beispiel lediglich in der Schlussrichtung der logischen Implikation.

Wie gewohnt bilden wir die Skolem-Form von  $\neg F$ :

$$\begin{aligned}\neg F &\equiv \neg(\forall y \exists x P(x, y) \rightarrow \exists x \forall y P(x, y)) \\ &\equiv (\forall y \exists x P(x, y)) \wedge \neg(\exists x \forall y P(x, y)) \\ &\equiv (\forall y \exists x P(x, y)) \wedge (\forall x \exists y \neg P(x, y)) \\ &\equiv_E \forall y P(f(y), y) \wedge \forall x \neg P(x, g(x)) \\ &\equiv \forall y \forall x (P(f(y), y) \wedge \neg P(x, g(x)))\end{aligned}$$

Die Grundinstanzen berechnen sich wie folgt:

$$\begin{aligned}G(F) := \{ &P(f(a), a) \wedge \neg P(a, g(a)), \\ &P(f(f(a)), f(a)) \wedge \neg P(a, g(a)), \\ &P(f(a), a) \wedge \neg P(f(a), g(f(a))), \dots \}\end{aligned}$$

Wie in Abbildung 3.43 angedeutet, lassen sich für diese Formel immer wieder neue Grundinstanzen bilden, so dass der Algorithmus von Gilmore nicht terminiert.

Die Eigenschaft des Algorithmus, für gewisse Formeln  $F$  in eine Endlosschleife zu geraten, ist kein Schönheitsfehler. Sie ist der Tatsache geschuldet, dass das Erfüllbarkeitsproblem der Prädikatenlogik in die Klasse der *unentscheidbaren Probleme* fällt. Anders als in der Aussagenlogik sind wir in der Prädikatenlogik nicht in der Lage, für jede prädikatenlogische Formel zweifelsfrei zu bestimmen, ob es sich um eine Tautologie handelt oder nicht. Konkret hat dies zur Folge, dass wir lediglich die Allgemeingültigkeit einer Formel  $F$  bestätigen können. Ist  $F$  keine Tautologie, so können wir zu keinem Zeitpunkt entscheiden, ob der Algorithmus unendlich lange läuft oder nicht doch im nächsten Schritt terminieren wird. Da der Entscheidungsprozess jetzt nur noch in eine Richtung funktioniert, sprechen wir in diesem Zusammenhang auch von einem *Semi-Entscheidungsverfahren*. Für den Moment wollen wir uns mit der etwas informellen Darstellung des Sachverhalts zufriedengeben. In Abschnitt 6.4 werden wir die Begriffe der *Entscheidbarkeit* und der *Semi-Entscheidbarkeit* erneut aufgreifen und in aller Ausführlichkeit behandeln.

In den nächsten beiden Abschnitten werden wir zeigen, wie sich die aussagenlogischen Resolutions- und Tableaukalküle zu prädikatenlogischen Beweisverfahren ausbauen lassen. Prädikatenlogische Hilbert-Kalküle existieren ebenfalls, haben jedoch so gut wie keine Praxisbedeutung. Wie schon im aussagenlogischen Fall müssen geeignete Formelinstanzen geraten werden. Da die Anzahl möglicher Kandidaten jedoch ungleich größer ist, wird die Beweisführung zusätzlich erschwert. Für eine ausführliche Darstellung prädikatenlogischer Hilbert-Kalküle sei der interessierte Leser auf [68] verwiesen.

$$F = \forall y \exists x P(x, y) \rightarrow \exists x \forall y P(x, y)$$

Negieren

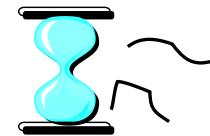
$$\neg F \equiv \forall y \exists x P(x, y) \wedge \forall x \exists y \neg P(x, y)$$

Skolemisieren

$$\begin{aligned}Skolem(F) = \\ \forall y \forall x (P(f(y), y) \wedge \neg P(x, g(x)))\end{aligned}$$

$i$	Grundinstanzen	Erfüllbar?
0	$\emptyset$	Ja
1	$P(f(a), a) \wedge \neg P(a, g(a))$	Ja
2	$P(f(a), a) \wedge \neg P(a, g(a)), P(f(f(a)), f(a)) \wedge \neg P(a, g(a))$	Ja
3	$P(f(a), a) \wedge \neg P(a, g(a)), P(f(f(a)), f(a)) \wedge \neg P(a, g(a)), P(f(a), a) \wedge \neg P(f(a), g(f(a)))$	Ja

...



**Abbildung 3.43:** Algorithmus von Gilmore, hier angewendet auf die Formel  $\forall y \exists x P(x, y) \rightarrow \exists x \forall y P(x, y)$

■ Beispiel 1

$$F_1 := P(f(y), y)$$

$$F_2 := P(x, g(x))$$



$F_1$  und  $F_2$  sind nicht unifizierbar. Es müsste gleichzeitig gelten:

$$[x \leftarrow f(y)] \text{ und } [y \leftarrow g(x)]$$

■ Beispiel 2

$$F_1 := P(x, f(y))$$

$$F_2 := P(f(y), x)$$



Unifikatoren:

$$\sigma_1 = [x \leftarrow f(y)]$$

$$\sigma_2 = [x \leftarrow f(f(z)), y \leftarrow f(z)]$$

$$\sigma_3 = [x \leftarrow f(f(f(z))), y \leftarrow f(f(z))]$$

...

**Abbildung 3.44:** Beispiele zur Verdeutlichung des Unifikationsbegriffs

### 3.2.3.1 Resolutionskalkül

Um den prädikatenlogischen Resolutionskalkül zu verstehen, werfen wir einen erneuten Blick auf Abbildung 3.42. Für die gezeigte Beispielformel  $\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$  bricht der Algorithmus von Gilmore ab, sobald die widersprüchliche Grundinstanz  $P(a, b) \wedge \neg P(a, b)$  gefunden wurde. In der Klauseldarstellung schreiben wir diese Formel als  $\{P(a, b)\}, \{\neg P(a, b)\}$ .

Betrachten wir die Skolem-Form von  $\neg F$  in Klauseldarstellung, so erhalten wir ein sehr ähnlich aussehendes Ergebnis:

$$\{P(a, y)\}, \{\neg P(x, b)\}$$

Die widersprüchliche Grundinstanz  $\{P(a, b)\}, \{\neg P(a, b)\}$  können wir sofort erhalten, indem wir eine Substitution  $\sigma$  konstruieren, die das Literal  $P(a, y)$  mit dem (unnegierten) Literal  $P(x, b)$  in Übereinstimmung bringt. Konkret können wir die Gleichheit herstellen, indem wir  $x$  durch  $a$  und  $y$  durch  $b$  ersetzen. In der Terminologie der Logik werden  $P(a, y)$  und  $P(x, b)$  durch die Substitution  $\sigma$  *unifiziert* und der gesamte Konstruktionsvorgang als *Unifikation* bezeichnet.



#### Definition 3.25 (Unifikation)

Zwei prädikatenlogische Formeln  $F$  und  $G$  sind *unifizierbar*, falls eine Substitution  $\sigma$  existiert mit

$$\sigma F = \sigma G.$$

Eine Substitution  $\sigma$  mit dieser Eigenschaft heißt *Unifikator*.

Der Unifikationsbegriff lässt sich intuitiv auf Formelmengen mit einer beliebigen Anzahl an Elementen erweitern. Die Menge  $\{F_1, \dots, F_n\}$  wird durch die Substitution  $\sigma$  unifiziert, falls  $\sigma F_1 = \dots = \sigma F_n$  gilt.

Auch wenn die angegebene Substitution in unserem Beispiel die einzige Möglichkeit ist, beide Literale zu unifizieren, ist die Situation im Allgemeinen ein wenig komplizierter. Wie das obere Beispiel in Abbildung 3.44 zeigt, sind nicht alle Formelpaare unifizierbar. Gäbe es einen Unifikator  $\sigma$  für die Formeln  $P(f(y), y)$  und  $P(x, g(x))$ , so müsste dieser  $x$  durch  $f(y)$  und gleichzeitig  $y$  durch  $g(x)$  ersetzen. Eine solche Substitution kann aufgrund des entstehenden Selbstbezugs nicht existieren. Wie das untere Beispiel in Abbildung 3.44 zeigt, existieren für andere Formelpaare mehrere, ja sogar unendlich viele Möglichkeiten, um

die Gleichheit herzustellen.  $\sigma_1$  spielt in diesem Beispiel eine besondere Rolle, da wir alle anderen Unifikatoren durch die Anwendung einer weiteren Substitution aus  $\sigma_1$  erzeugen können. Eine Substitution mit dieser Eigenschaft bezeichnen wir als *allgemeinsten Unifikator*.

Wir wollen uns nun mit der Frage beschäftigen, wie sich der allgemeinsten Unifikator systematisch erzeugen lässt. Die Antwort liefert uns der in Abbildung 3.45 skizzierte *Algorithmus von Robinson*. Intern arbeitet dieser auf der Menge  $M$  und einer Substitution  $\sigma$ . Zu Beginn wird  $M$  mit der zu unifizierenden Formelmenge und  $\sigma$  mit der identischen Abbildung  $\text{id} : x \mapsto x$  initialisiert. Anschließend prüft der Algorithmus, ob  $M$  nur ein einziges Element enthält. In diesem Fall unifiziert  $\sigma$  die Eingabemenge und wird ausgegeben. Enthält  $M$  zwei oder mehr Elemente, so werden die Formeln Zeichen für Zeichen von links nach rechts miteinander verglichen. An der ersten Position, an der sich mindestens zwei Formeln unterscheiden, überprüft der Algorithmus, ob die Gleichheit durch Substitution hergestellt werden kann. Dies ist immer dann der Fall, wenn eine Menge von Variablen  $x_1, \dots, x_m$  und ein Term  $t$  mit  $x_1, \dots, x_m \notin t$  vorgefunden werden, nicht aber zwei oder mehr unterschiedliche Terme aufeinandertreffen. Im ersten Fall wird  $\sigma$  mit der Substitution  $\mu = [x_1 \leftarrow t, \dots, x_m \leftarrow t]$  verkettet und der Vorgang auf der Menge  $\mu M$  wiederholt. Andernfalls terminiert der Algorithmus mit der Ausgabe „nicht unifizierbar“. Tabelle 3.8 fasst die schrittweise Berechnung eines allgemeinsten Unifikators für das Formelpaar

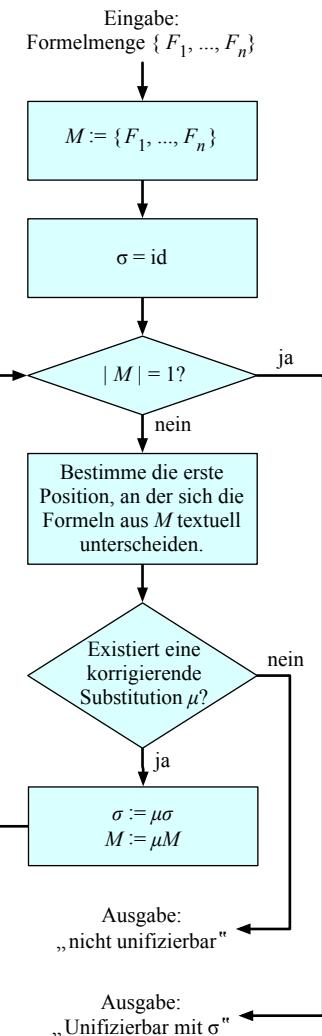
$$\begin{aligned} F_1 &:= P(f(g(x_2, x_3)), g(x_1, g(a, b))) \\ F_2 &:= P(f(x_4), g(h(a, x_5), g(x_2, x_3))) \end{aligned}$$

zusammen.

Nachdem wir Unifikatoren jetzt systematisch berechnen können, ist es an der Zeit, uns der prädikatenlogischen Resolutionsregel zuzuwenden. Sie lautet wie folgt:

$$\frac{M_1 \cup \{L_1\} \quad M_2 \cup \{\neg L_2\}}{\sigma(M_1 \cup M_2)} \quad \sigma L_1 = \sigma L_2 \quad (3.27)$$

Die Substitution  $\sigma$  bezeichnet den *allgemeinsten Unifikator* von  $L_1$  und  $L_2$ . In Worte liest sich die Resolutionsregel wie folgt: Zwei Klauseln lassen sich genau dann zu einer Resolvente verschmelzen, wenn diese ein komplementäres Formelpaar aufweisen, das mit einer Substitution  $\sigma$  unifiziert werden kann. Um die Resolvente zu bilden, wird der Unifikator  $\sigma$  auf  $M_1$  und  $M_2$  angewendet, das komplementäre Formelpaar entfernt und die restlichen Formeln zu einer gemeinsamen Klausel vereint.



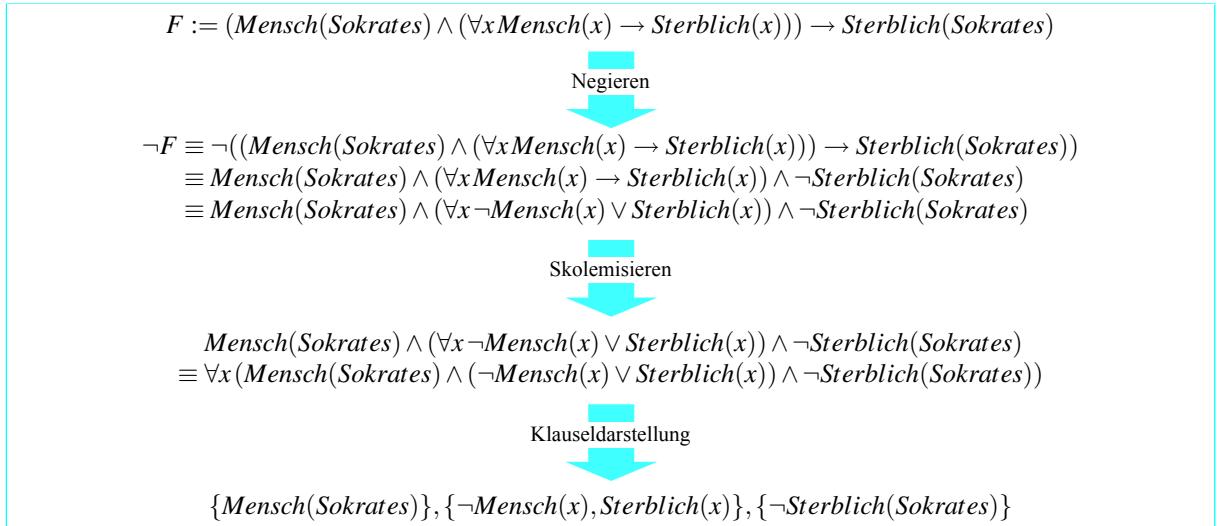
**Abbildung 3.45:** Unifikationsalgorithmus von Robinson

$M$	$\mu$	$\sigma$
$\downarrow$ $P(f(g(x_2, x_3)), g(x_1, g(a, b)))$ $P(f(x_4), g(h(a, x_5), g(x_2, x_3)))$ $\uparrow$		$\emptyset$
$P(f(\begin{array}{c} \downarrow \\ g \\ x_4 \end{array}, (x_2, x_3)), g(x_1, g(a, b)))$ $P(f(\begin{array}{c} \uparrow \\ x_4 \end{array}, ), g(h(a, x_5), g(x_2, x_3)))$	$x_4 \leftarrow g(x_2, x_3)$	$x_4 \leftarrow g(x_2, x_3)$
$P(f(g(x_2, x_3)), g(\begin{array}{c} \downarrow \\ x_1 \\ h \end{array}, , g(a, b)))$ $P(f(g(x_2, x_3)), g(\begin{array}{c} \uparrow \\ a \\ x_5 \end{array}, , g(x_2, x_3)))$	$x_1 \leftarrow h(a, x_5)$	$x_4 \leftarrow g(x_2, x_3),$ $x_1 \leftarrow h(a, x_5)$
$P(f(g(x_2, x_3)), g(h(a, x_5), g(\begin{array}{c} \downarrow \\ a \\ x_2 \end{array}, , b)))$ $P(f(g(x_2, x_3)), g(h(a, x_5), g(\begin{array}{c} \uparrow \\ x_2 \end{array}, , x_3)))$	$x_2 \leftarrow a$	$x_4 \leftarrow g(a, x_3),$ $x_1 \leftarrow h(a, x_5),$ $x_2 \leftarrow a$
$P(f(g(a, x_3)), g(h(a, x_5), g(a, \begin{array}{c} \downarrow \\ b \\ x_3 \end{array}, )))$ $P(f(g(a, x_3)), g(h(a, x_5), g(a, \begin{array}{c} \uparrow \\ x_3 \end{array}, )))$	$x_3 \leftarrow b$	$x_4 \leftarrow g(a, b),$ $x_1 \leftarrow h(a, x_5),$ $x_2 \leftarrow a,$ $x_3 \leftarrow b$
$P(f(g(a, b)), g(h(a, x_5), g(a, b)))$ $P(f(g(a, b)), g(h(a, x_5), g(a, b)))$ $\uparrow$		$x_4 \leftarrow g(a, b),$ $x_1 \leftarrow h(a, x_5),$ $x_2 \leftarrow a,$ $x_3 \leftarrow b$

**Tabelle 3.8:** Schrittweise Abarbeitung des Algorithmus von Robinson

Um Namenskollisionen zu vermeiden, darf die Resolutionsregel nur dann angewendet werden, wenn die beiden Prämissen keine gemeinsamen Variablen aufweisen. Dies ist keine Einschränkung im eigentlichen Sinne, da wir die Variablen einer Klausel vor der Resolventenbildung nach Belieben umbenennen können, ohne die Korrektheit des Verfahrens zu gefährden.

Erinnern Sie sich noch an das Eingangsbeispiel, in dem wir Sokrates als Mensch und die Sterblichkeit als universelle Eigenschaft eines je-



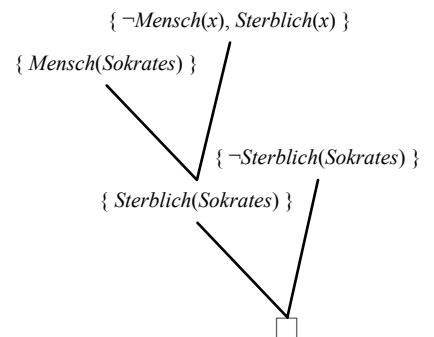
**Abbildung 3.46:** Um die Sterblichkeit von Sokrates im Resolutionskalkül zu beweisen, muss die Ausgangsformel zunächst in Klauseldarstellung überführt werden.

den Menschen beschrieben haben? Mit Hilfe der prädikatenlogischen Resolution sind wir jetzt in der Lage, die Sterblichkeit von Sokrates formal zu beweisen. Hierzu gilt es, die Allgemeingültigkeit der folgenden Aussage zu zeigen:

$$(\text{Mensch}(\text{Sokrates}) \wedge (\forall x \text{Mensch}(x) \rightarrow \text{Sterblich}(x))) \rightarrow \text{Sterblich}(\text{Sokrates}) \quad (3.28)$$

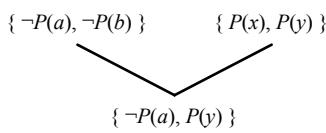
Um die Behauptung im Resolutionskalkül zu beweisen, müssen wir die negierte Formel zunächst in die Skolem-Form und anschließend in die Klauseldarstellung transformieren. Führen wir die in Abbildung 3.46 zusammengefassten Umformungsschritte durch, so erhalten wir als Ergebnis drei Klauseln, auf die wir den Resolutionskalkül direkt anwenden können. Der eigentliche Resolutionsbeweis erweist sich nach der geleisteten Voraarbeit als denkbar einfach. Wie in Abbildung 3.47 gezeigt, lässt sich die leere Klausel in nur zwei Schritten ableiten.

Wir wollen die prädikatenlogische Resolution jetzt von einem abstrakteren Standpunkt betrachten und der Frage nachgehen, ob wir ein korrektes und vollständiges Kalkül vor uns haben. Die Korrektheit der prädikatenlogischen Resolutionsregel ist leicht einzusehen. Sie folgt aus der Korrektheit der aussagenlogischen Regel sowie der Tatsache, dass der angewendete Unifikator die Aussagen der Prämissen unverändert lässt oder einschränkt, jedoch in keinem Fall verallgemeinert.

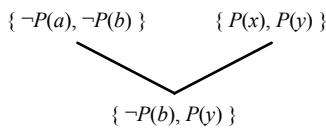


**Abbildung 3.47:** Sokrates ist sterblich! Formal bewiesen im Resolutionskalkül.

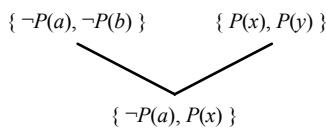
■ Erste Resolvente



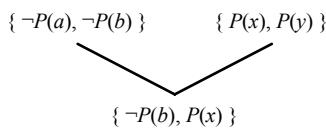
■ Zweite Resolvente



■ Dritte Resolvente



■ Vierte Resolvente



**Abbildung 3.48:** Obwohl die Ausgangsmenge unerfüllbar ist, lässt sich die leere Klausel  $\square$  nicht ableiten.

Dagegen ist der Kalkül in der vorgestellten Form nicht mehr vollständig. Warum diese Eigenschaft verloren geht, wollen wir am Beispiel der folgenden Klauselmenge herausarbeiten:

$$\{P(x), P(y)\}, \{\neg P(a), \neg P(b)\} \quad (3.29)$$

Die erste Klausel besagt, dass die Eigenschaft  $P$  für alle Elemente der Individuenmenge erfüllt ist, die zweite, dass  $P$  für die Elemente  $a$  und  $b$  nicht gilt. Obwohl die Menge offensichtlich unerfüllbar ist, kann die leere Klausel nicht mit der eingeführten Resolutionsregel abgeleitet werden. Warum dies so ist, macht Abbildung 3.48 deutlich: Es lassen sich ausschließlich Resolventen bilden, die wiederum 2 Elemente besitzen. Der Verursacher des Problems ist die Klausel  $\{P(x), P(y)\}$ . Sie entspricht dem folgenden Ausdruck:

$$\forall x \forall y (P(x) \vee P(y)) \quad (3.30)$$

Die Formel lässt sich zu

$$\forall x P(x) \vee \forall y P(y) \quad (3.31)$$

umformen und ist logisch äquivalent zu

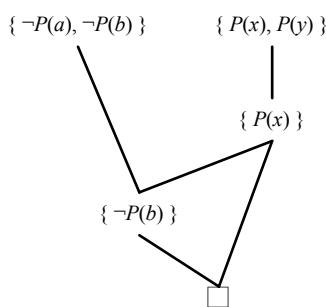
$$\forall x P(x). \quad (3.32)$$

Wären wir in der Lage, aus der Klausel  $\{P(x), P(y)\}$  die Klausel  $\{P(x)\}$  innerhalb des Kalküls zu erzeugen, so ließe sich auch die leere Klausel ableiten. Genau dies leistet die *Faktorisierungsregel*, die wir im prädikatenlogischen Fall als zusätzliche Schlussregel in den Kalkül integrieren müssen:

$$\frac{\{L_1, \dots, L_{n-1}, L_n\}}{\{\sigma L_1, \dots, \sigma L_{n-1}\}} \quad \sigma L_{n-1} = \sigma L_n \quad (3.33)$$

Abbildung 3.49 zeigt, wie sich die Unerfüllbarkeit der Klauselmenge unter Einbeziehung der Faktorisierungsregel beweisen lässt. Zunächst wird aus  $\{P(x), P(y)\}$  die Klausel  $\{P(x)\}$  erzeugt und anschließend die leere Klausel durch zweifache Resolventenbildung hergeleitet.

Zusammen mit der Faktorisierungsregel wird der Resolutionskalkül tatsächlich vollständig, d. h., wir können jede allgemeingültige prädikatenlogische Formel innerhalb des Kalküls als solche beweisen. Der formale Beweis ist kompliziert und soll an dieser Stelle nicht geführt werden. Der interessierte Leser sei auf [81] oder [68] verwiesen. Beachten Sie, dass dieses Ergebnis nicht im Widerspruch zur Semi-Entscheidbarkeit steht, die wir im Zusammenhang mit dem Algorithmus von Gilmore herausgearbeitet haben. Ist eine Formel  $F$  nicht allgemeingültig, so lassen sich im Allgemeinen unendlich viele Resolventen bilden und wir wissen zu keinem Zeitpunkt, ob die leere Klausel irgendwann darunter sein wird oder nicht.



**Abbildung 3.49:** Durch die Hinzunahme der Faktorisierungsregel wird der Resolutionskalkül vollständig. Auch die Unerfüllbarkeit unserer Beispieldarstellung lässt sich jetzt beweisen.

### 3.2.3.2 Tableaukalkül

Weiter oben haben wir herausgearbeitet, wie die aussagenlogische Resolution mit Hilfe der Unifikation zu einem prädikatenlogischen Kalkül ausgebaut werden kann. Mit dem gleichen Ansatz können wir auch den Tableaukalkül auf die Prädikatenlogik ausdehnen. Die grundlegende Vorgehensweise bleibt dabei unverändert: Um die Allgemeingültigkeit einer Formel  $F$  zu zeigen, gehen wir von der negierten Formel  $\neg F$  aus und versuchen, diese zu einem geschlossenen Tableau zu erweitern.

Um prädikatenlogische Formeln mit dem Tableaukalkül verarbeiten zu können, müssen wir zwei Erweiterungen vornehmen: Zum einen benötigen wir Schlussregeln für die beiden Quantoren  $\forall$  und  $\exists$ , zum anderen eine angepasste Regel, um Pfade zu schließen. Der Umgang mit den prädikatenlogischen Quantoren wird möglich, indem die bereits vorhandenen  $\alpha$ - und  $\beta$ -Regeln durch zwei neue, in Abbildung 3.50 zusammengefasste Regelgruppen ergänzt werden. Die neu hinzugekommenen  $\gamma$ -Regeln gestatten uns, einen Allquantor ( $\forall x F$ ) bzw. einen negierten Existenzquantor ( $\neg \exists x F$ ) zu eliminieren, indem  $x$  durch eine neue Variable  $y$  substituiert wird. Die Ersetzung muss *kollisionsfrei* erfolgen, d. h.,  $y$  darf nicht an anderer Stelle des Tableaus als freie Variable auftauchen. Die  $\delta$ -Regeln legen den Umgang mit Existenzaussagen ( $\exists x F$ ,  $\neg \forall x F$ ) fest. In diesem Fall wird die Variable  $x$  skolemisiert, indem sie durch einen Term der Form  $f(x_1, \dots, x_n)$  ersetzt wird. Hierbei ist  $f$  ein neues Funktionssymbol und  $x_1, \dots, x_n$  sind die freien Variablen von  $F$ .

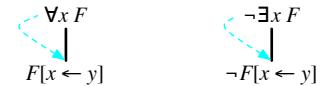
Auch das Schließen eines Pfades erfordert mehr Sorgfalt als bisher. Mussten wir im aussagenlogischen Fall lediglich darauf warten, dass im Rahmen der Expansion irgendwann ein komplementäres Formelpaar  $F, \neg F$  erzeugt wird, so müssen wir ein solches Paar im prädikatenlogischen Fall fast immer aktiv erzeugen. Hierzu werden auf dem betrachteten Pfad zwei Formeln  $F_1$  und  $\neg F_2$  gewählt und  $F_1$  und  $F_2$  miteinander unifiziert. Gelingt die Unifikation, so kann der Pfad geschlossen werden, indem der allgemeinste Unifikator von  $F_1$  und  $F_2$  auf sämtliche Tableauformeln angewendet wird.

Damit haben wir alle Bausteine zusammen, um ein prädikatenlogisches Tableau zu erzeugen. In jedem Konstruktionsschritt können wir zwischen zwei möglichen Aktionen wählen:

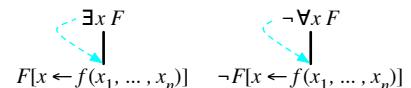
#### ■ Erweitern des Tableaus

Das Tableau wird durch die Anwendung einer  $\alpha$ -,  $\beta$ -,  $\gamma$ - oder  $\delta$ -Regel erweitert. Genau wie im aussagenlogischen Fall wirkt sich die

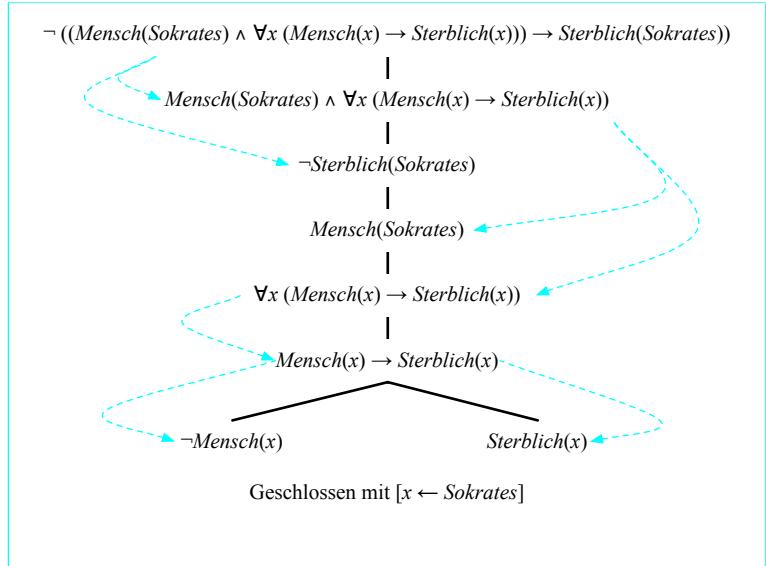
#### ■ $\gamma$ -Expansionen



#### ■ $\delta$ -Expansionen



**Abbildung 3.50:** Zusätzliche Expansionsregeln des prädikatenlogischen Tableaukalküls. Die  $\gamma$ -Regeln führen eine neue Variable  $y$  ein, die an keiner anderen Stelle im Tableau als freie Variable vorkommen darf. Die  $\delta$ -Regeln ersetzen die quantifizierte Variable durch einen Term der Form  $f(x_1, \dots, x_n)$ .  $f$  ist ein neues Funktionssymbol und  $x_1, \dots, x_n$  sind die freien Variablen der Formel  $F$ .

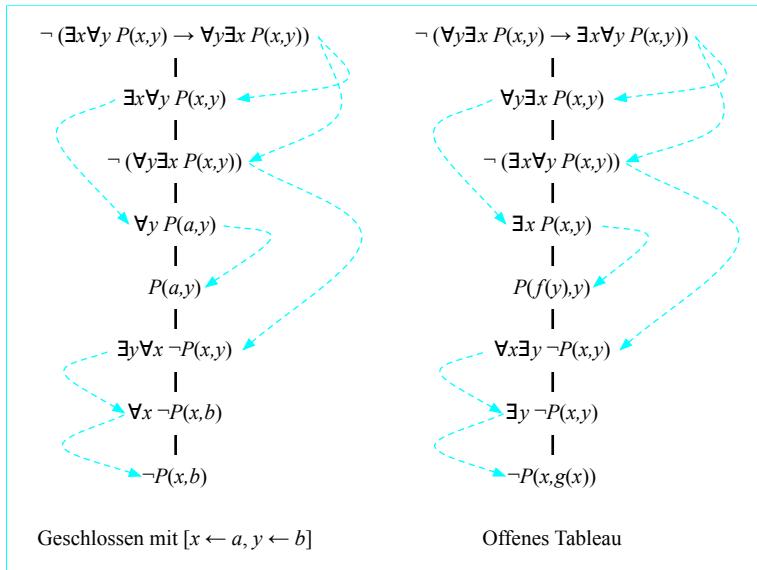


**Abbildung 3.51:** Sokrates ist sterblich!  
Diesmal bewiesen im Tableaukalkül.

Reihenfolge der Regelanwendungen auf die Größe des entstehenden Tableaus aus. Um die Anzahl der Verzweigungen so gering wie möglich zu halten, sind  $\alpha$ -Regeln immer vor  $\beta$ -Regeln anzuwenden. Ferner ist es unnötig, die gleiche Formel mehrmals mit einer  $\alpha$ -,  $\beta$ - oder  $\delta$ -Regel zu bearbeiten. Zusätzliche Expansionen vergrößern das Tableau, generieren aber niemals neue Abschlussmöglichkeiten. Anders verhält es sich mit den  $\gamma$ -Regeln, da ein prädikatenlogisches Tableau in vielen Fällen nur dann geschlossen werden kann, wenn Formeln des  $\gamma$ -Typs mehrmals expandiert wurden. Wie häufig die  $\gamma$ -Regeln angewendet werden müssen, bevor sich ein Tableau schließen lässt, kann nicht vorhergesagt werden. Hierdurch wird der Tableaukalkül zu einem Semi-Entscheidungsverfahren, das uns nur für allgemeingültige Formeln eine sichere Aussage erlaubt.

### ■ Schließen eines Pfads

Ein Pfad kann geschlossen werden, wenn er zwei Formeln  $F_1$  und  $\neg F_2$  enthält und  $F_1$  und  $F_2$  unifizierbar sind. Um den Abschluss durchzuführen, berechnen wir zunächst den allgemeinsten Unifikator  $\sigma$  von  $F_1$  und  $F_2$  und wenden diesen anschließend auf alle bisher erzeugten Formeln an. Danach kann das Tableau weiter expandiert oder ein anderer Pfad geschlossen werden. Beachten Sie, dass der Unifikator  $\sigma$  auf das gesamte Tableau angewendet wird und nicht nur auf die Formeln des aktuell zu schließenden Pfads.



**Abbildung 3.52:** Zwei prädikatenlogische Tableaus. Das linke Tableau ist geschlossen und die Ausgangsformel als unerfüllbar identifiziert. Um das rechte Tableau zu schließen, müssten wir  $x$  mit  $f(y)$  und gleichzeitig  $y$  mit  $g(x)$  ersetzen. Eine solche Substitution existiert nicht und das Tableau kann nicht geschlossen werden.

Abbildung 3.51 demonstriert, wie die Sterblichkeit von Sokrates mit Hilfe des Tableaukalküls formal bewiesen werden kann. Zunächst wird die Eingabeformel mit den beiden  $\alpha$ -Regeln in ihre konjunktiven Bestandteile zerlegt. Anschließend wird der Allquantor mit Hilfe der  $\gamma$ -Regel eliminiert und der verbleibende Implikationsoperator mit der  $\beta$ -Regel aufgelöst. Als Ergebnis entsteht ein Tableau, das mit der Substitution  $\sigma = [x \leftarrow \text{Sokrates}]$  geschlossen werden kann.

Die Anwendung des Tableaukalküls wollen wir an zwei weiteren Beispielen demonstrieren. Dabei greifen wir auf die folgenden beiden Formeln zurück, die uns bereits in der Diskussion über den Resolutionskalkül als fruchtbare Anschauungsobjekte dienten:

$$F_1 := \exists x \forall y P(x,y) \rightarrow \forall y \exists x P(x,y)$$

$$F_2 := \forall y \exists x P(x,y) \rightarrow \exists x \forall y P(x,y)$$

Die Formel  $F_1$  ist eine Tautologie und konnte bereits erfolgreich als solche bewiesen werden.  $F_2$  ist nicht allgemeingültig, da auf der linken Seite der Implikation eine stärkere Aussage steht als auf der rechten. Abbildung 3.52 zeigt die expandierten Tableaus für die Formeln  $F_1$  und  $F_2$ . Das linke Tableau kann mit der Substitution  $\sigma = [x \leftarrow a, y \leftarrow b]$  geschlossen werden. Wenden wir  $\sigma$  auf das Tableau an, so entsteht auf dem einzigen vorhandenen Pfad das komplementäre Formelpaar  $P(a,b), \neg P(a,b)$ . Im Gegensatz hierzu lässt sich das Tableau für die Formel  $F_2$  nicht schließen, da mit  $P(f(y),y)$  und  $P(x,g(x))$  genau die-

jenigen Terme entstehen, die wir in Abbildung 3.44 als nicht unifizierbar erkannt haben. Weitere  $\gamma$ -Regelanwendungen können die Situation nicht ändern, da wir das Tableau lediglich mit weiteren Instanzen der gleichen Form anreichern und keine neuen Abschlussmöglichkeiten erzeugen würden.

### 3.2.4 Anwendung: Logische Programmierung

War die Prädikatenlogik ursprünglich ein Teilbereich der reinen Mathematik, so erhielt sie im Zuge der aufkeimenden Computertechnik eine ganz praktische Bedeutung: Sie ist die theoretische Grundlage der Programmiersprache Prolog (*PRO*gramming in *LOG*ic). Prolog wurde Anfang der Siebzigerjahre entwickelt und ist der bekannteste Vertreter des *deklarativen Programmierparadigmas* [61]. Deklarative Programmiersprachen stellen die Problemformulierung und nicht die Lösungsstrategie in den Vordergrund; sie sind von der Idee getrieben, der Computer möge die Lösung aus der Beschreibung selbstständig deduzieren. Die Vorgehensweise unterscheidet sich damit fundamental von jener der imperativen oder der objektorientierten Programmiersprachen. Dort wird der Lösungsweg detailliert durch den Entwickler vorgegeben.

Ein Prolog-Programm ist aus *Fakten* und *Regeln* aufgebaut. Was sich hinter diesen Begriffen genau verbirgt, wollen wir am Beispiel des Stammbaums aus Abbildung 3.53 herausarbeiten. Dargestellt sind die Verwandtschaftsverhältnisse einiger Charaktere aus J. R. R. Tolkiens Fantasy-Epos *Herr der Ringe*.

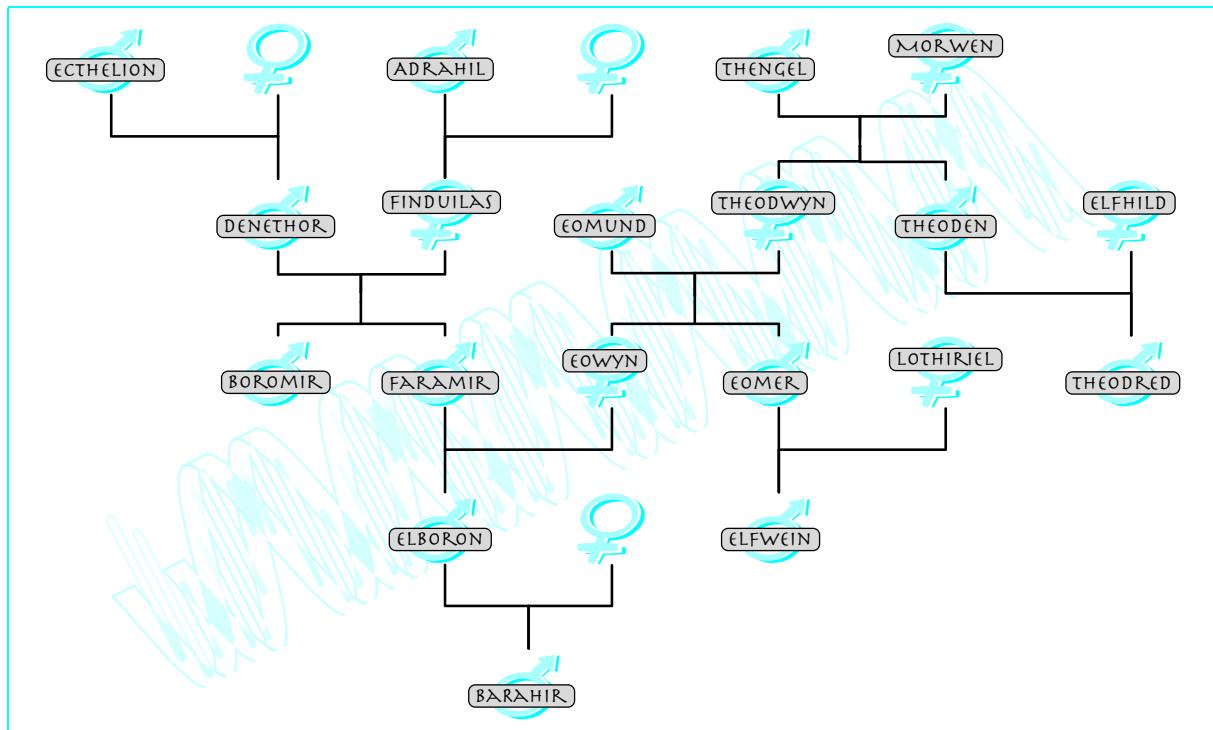
Ein Blick auf den Stammbaum reicht aus, um beispielsweise die folgenden Verwandtschaftsbeziehungen zu erkennen:

- „Elboron ist Eowyns Sohn“
- „Eowyn ist Eomunds Tochter“

Beide Sachverhalte werden innerhalb eines Prolog-Programms mit Hilfe zweier Fakten formuliert:

- `sohn(elboron,eowyn).`
- `tochter(eowyn,eomund).`

Die Prolog-Syntax deutet unmissverständlich an: Mit Fakten werden Prädikate beschrieben. Konkret legen die beiden Anweisungen fest,



**Abbildung 3.53:** Kleiner Ausschnitt aus dem Stammbaum der Charaktere der Fantasy-Trilogie *Herr der Ringe*

dass das Prädikat `sohn` für die Kombination (`elboron,eowyn`) und das Prädikat `tochter` für die Kombination (`eowyn, eomund`) wahr ist.

Regeln werden in Prolog eingesetzt, um Prädikate miteinander in Beziehung zu setzen. So können wir die Eigenschaft, ein Kind zu sein, in direkter Weise auf die Sohn-Tochter-Beziehung zurückführen:  $X$  ist ein Kind von  $Y$ , falls  $X$  ein Sohn von  $Y$  ist oder  $X$  eine Tochter von  $Y$  ist. In Prolog können wir die Beziehung wie folgt beschreiben:

- `kind(X,Y) :- sohn(X,Y).`
- `kind(X,Y) :- tochter(X,Y).`

Beachten Sie die Groß- und Kleinschreibung! Prädikate und Individuen beginnen in Prolog immer mit einem Kleinbuchstaben, Variablen mit einem Großbuchstaben. Aufweichungen dieser Regel existieren nicht, da Prolog über keine andere Möglichkeit verfügt, Variablen von Konstanten zu unterscheiden.

### stammbaum.pl

```

sohn(denethor,ecthelion).
sohn(boromir,denethor).
sohn(boromir,finduilas).
sohn(faramir,denethor).
sohn(faramir,finduilas).
sohn(elboron,faramir).
sohn(elboron,eowyn).
sohn(barahir,elboron).
sohn(eomer,eomund).
sohn(eomer,theodwyn).
sohn(elfwein,eomer).
sohn(elfwein,lothiriel).
sohn(theoden,thengel).
sohn(theoden,morwen).
sohn(theodred,theoden).
sohn(theodred,elfhild).
tochter(finduilas,adrahil).
tochter(eowyn,eomund).
tochter(eowyn,theodwyn).
tochter(theodwyn,thengel).
tochter(theodwyn,morwen).

kind(X,Y) :- sohn(X,Y).
kind(X,Y) :- tochter(X,Y).

nachfahre(X,Y) :- kind(X,Y).
nachfahre(X,Y) :- kind(X,Z),
                 nachfahre(Z,Y).

```

Die Kindbeziehung können wir nutzen, um weitere Prädikate zu definieren. Beispielsweise lässt sich die Eigenschaft, ein Nachfahre einer anderen Person zu sein, wie folgt charakterisieren:  $X$  ist ein Nachfahre einer Person  $Y$ , wenn  $X$  das Kind von  $Y$  oder das Kind einer anderen Person ist, die ihrerseits ein Nachfahre von  $Y$  ist. In Prolog drücken wir diesen Zusammenhang folgendermaßen aus:

```

7   nachfahre(X,Y) :- kind(X,Y).
8
9   nachfahre(X,Y) :- kind(X,Z), nachfahre(Z,Y).
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

```

Prolog-Programme lassen sich mit einem gewöhnlichen Texteditor erstellen. Anschließend wird der Interpreter gestartet und das Programm mit dem vordefinierten Befehl `consult('...')` eingelesen. Die folgenden Versuche wurden mit dem freien Interpreter GNU Prolog durchgeführt:

```

GNU Prolog 1.3.0
By Daniel Diaz
Copyright (C) 1999–2007 Daniel Diaz
| ?- consult('stammbaum.pl').
compiling stammbaum.pl for byte code...
stammbaum.pl compiled,
28 lines read – 2938 bytes written, 11 ms
yes
| ?-

```

Der Interpreter übersetzt die eingelesenen Fakten und Regeln zunächst in Byte-Code und fügt sie anschließend in die Wissensbasis ein. Der Quelltext des eingelesenen Programms ist in Abbildung 3.54 dargestellt und enthält eine komplette Beschreibung des Beispielstammbaums aus Abbildung 3.53 in Prolog-codierter Form.

Nachdem das Programm erfolgreich eingelesen wurde, ist der Interpreter bereit, Anfragen entgegenzunehmen. Beispielsweise können wir die Frage stellen, ob Elboron ein Nachfahre von Denethor ist.

```

:- nachfahre(elboron,denethor).
yes

```

Wie zu erwarten, wird die Anfrage bejaht. Anders verhält sich der Interpreter in dem folgenden Fall:

```

:- nachfahre(eowyn, ecthelion).
no

```

Dass die Anfrage verneint wird, überrascht nicht, schließlich ist Eowyn kein Nachfahre von Ecthelion.

Die Fähigkeiten von Prolog gehen weit über die Generierung von Ja-nein-Antworten hinaus. Indem wir Anfragen mit Variablen versehen, können wir Prolog dazu bewegen, mit konkreten Instanzen zu antworten. Beispielsweise können wir mit der nachstehenden Anfrage alle Nachfahren von Denethor berechnen:

```
:– nachfahre(X,denethor).
```

Der Prolog-Interpreter erzeugt die folgende Antwort:

```
X = boromir ?
```

In der Tat ist Boromir ein Nachfahre von Denethor; aber sind Faramir, Elboron und Barahir nicht ebenfalls Nachfahren? Die Antwortet lautet „Ja“ und Prolog ist imstande, diese ebenfalls auszugeben. Wir müssen den Interpreter lediglich anweisen, *alle* Lösungen zu berechnen. Hierzu genügt es, nach dem Fragezeichen den Buchstaben ’a‘ einzugeben. Prolog reagiert darauf mit der folgenden Ausgabe:

```
X = faramir
X = elboron
X = barahir
(1 ms) no
```

Das Wort „no“ in der letzten Zeile deutet an, dass keine weiteren Lösungen existieren.

Die Beispiele in Abbildung 3.55 zeigen, dass wir die Anfrage auch umgekehrt stellen können, indem die Variable *X* an die zweite Position gerückt wird. In diesem Fall berechnet der Prolog-Interpreter alle *Vorfahren* der im ersten Argument spezifizierten Person.

Wir können sogar noch einen Schritt weiter gehen und den Interpreter mit der Anfrage *nachfahre(X,Y)* aktivieren. In diesem Fall werden alle Personenpaare (*X,Y*) erzeugt, in denen *X* ein Nachfahre von *Y* ist (vgl. Abbildung 3.56). Anfragen lassen sich darüber hinaus kombinieren, wie das Beispiel in Abbildung 3.57 demonstriert. Durch die zusätzliche Angabe des Prädikats *tochter(X,\_)* wird die Ergebnisliste auf alle weiblichen Nachfahren eingeschränkt. Der spezielle Bezeichner ‘\_’ steht für eine willkürliche Variable, für deren Wert wir uns nicht interessieren.

### ■ Beispiel 1

Prolog-Console	
1	?– nachfahre(boromir,X).
2	
3	X = denethor
4	X = finduilas
5	X = ecthelion
6	X = adrahil
7	(1 ms) no
8	
9	

### ■ Beispiel 2

Prolog-Console	
1	?– nachfahre(elfwein,X).
2	
3	X = eomer
4	X = lothiriel
5	X = eomund
6	X = theodwyn
7	X = thengel
8	X = morwen
9	(1 ms) no

### ■ Beispiel 3

Prolog-Console	
1	?– nachfahre(elfhild,X).
2	
3	no
4	
5	
6	
7	
8	
9	

**Abbildung 3.55:** Weitere Anfragen an den Prolog-Interpreter

**Prolog-Console**

```
?- nachfahre(X,Y).
X = denethor
Y = ecthelion

X = boromir
Y = denethor

X = boromir
Y = finduilas

X = faramir
Y = denethor

X = faramir
Y = finduilas

X = elboron
Y = faramir

X = elboron
Y = eowyn

X = barahir
Y = elboron

X = eomer
Y = eomund

X = eomer
Y = theodwyn

X = elfwein
Y = eomer

X = elfwein
Y = lothiriel

...
41
```

### Interne Arbeitsweise von Prolog

Nachdem wir einen ersten Eindruck über die Leistungsfähigkeit von Prolog erhalten haben, wollen wir der internen Arbeitsweise dieser Sprache etwas genauer auf den Grund gehen.

Intern behandelt der Prolog-Interpreter Fakten und Regeln als prädikatenlogische Formeln, die gemeinsam die Wissensbasis bilden. Die wahre Gestalt dieser Formeln wird sofort ersichtlich, wenn wir die Prolog-Notation für den Moment beiseitelassen und auf die vertrauten Logiksymbole zurückgreifen. Die weiter oben definierten Logikformeln lesen sich dann wie folgt:

```

sohn(elboron,eowyn)
tochter(eowyn,eomund)
...
∀X ∀Y (sohn(X,Y) → kind(X,Y))
∀X ∀Y (tochter(X,Y) → kind(X,Y))
∀X ∀Y (kind(X,Y) → nachfahre(X,Y))
∀X ∀Y (kind(X,Z) ∧ nachfahre(Z,Y) → nachfahre(X,Y))

Auf den ersten Blick wirken die Ausdrücke wie ganz normale Formeln; auf den zweiten Blick wird deutlich, dass sie über eine spezielle Struktur verfügen. Um diese sichtbar zu machen, transformieren wir die Formeln zunächst in Klauseldarstellung. In wenigen Umformungsschritten können wir die folgende Darstellung erzeugen:

{sohn(elboron,eowyn)}
{tochter(eowyn,eomund)}
...
{¬sohn(X,Y),kind(X,Y)}
{¬tochter(X,Y),kind(X,Y)}
{¬kind(X,Y),nachfahre(X,Y)}
{¬kind(X,Z),¬nachfahre(Z,Y),nachfahre(X,Y)}
```

**Abbildung 3.56:** Auf die gestellte Anfrage antwortet der Prolog-Interpreter mit allen Personenpaaren, in denen  $X$  ein Nachfahre von  $Y$  ist.

Ein Blick auf die generierte Menge macht deutlich, dass keine Klausel mehr als ein positives Literal besitzt. Formeln mit dieser Eigenschaft wurden Anfang der Fünfzigerjahre durch den US-amerikanischen Logiker Alfred Horn ausführlich untersucht und tragen heute seinen Namen.



### Definition 3.26 (Horn-Formel, Horn-Klausel)

Eine aussagenlogische oder prädikatenlogische Formel  $F$  ist eine *Horn-Formel*, wenn sie die folgende Klauseldarstellung besitzt:

$$\{(\neg)L_1, \neg L_2, \neg L_3, \dots, \neg L_n\} \quad (3.34)$$

Die Menge der Horn-Klauseln besitzt mehrere interessante Eigenschaften. Zum einen ist sie bezüglich Resolventenbildung abgeschlossen, d. h., die Resolvente zweier Horn-Klauseln ist wiederum eine Horn-Klausel. Darüber hinaus lassen sich Resolutionsbeweise besonders einfach finden, da sich der Ableitungsgraph in Form einer linearen Kette entwickeln lässt.

Am Beispiel der Anfrage

```
:– nachfahre(elboron,denethor)
```

wollen wir die Arbeitsweise des Interpreters demonstrieren. Bezeichnen wir die Wissensbasis mit  $M$ , so versucht Prolog, die Allgemeingültigkeit der Formel

$$M \rightarrow \text{nachfahre}(elboron, denethor) \quad (3.35)$$

mit Hilfe der prädikatenlogischen Resolution zu beweisen. Hierzu erzeugt der Interpreter zunächst die negierte Formel

$$\neg(M \rightarrow \text{nachfahre}(elboron, denethor)) \quad (3.36)$$

$$\equiv M \wedge \neg \text{nachfahre}(elboron, denethor) \quad (3.37)$$

und übersetzt diese anschließend in Klauselform:

$$M \cup \{\neg \text{nachfahre}(elboron, denethor)\} \quad (3.38)$$

Auf dieser Menge führt Prolog einen prädikatenlogischen Resolutionsbeweis durch. Die Anfrage war erfolgreich, wenn es dem Interpreter gelingt, die leere Klausel abzuleiten. In diesem Fall antwortet das System mit yes und gibt die im Rahmen der Resolventenbildungen angewendeten Variablenubstitutionen aus. Kann die leere Klausel nicht abgeleitet werden, so antwortet der Interpreter mit no.

Abbildung 3.58 zeigt den entstehenden Resolutionsgraphen für unsere Beispieldanfrage. Die erste Resolvente wird immer mit der Anfrageklausel gebildet und das Ergebnis anschließend so lange weiter resolviert, bis die leere Klausel abgeleitet werden konnte oder die Ableitung in

### Prolog-Console

```
?– nachfahre(X,Y),
   tochter(X,_).

X = finduilas
Y = adrahil

X = eowyn
Y = eomund

X = eowyn
Y = eomund

X = eowyn
Y = theodwyn

X = eowyn
Y = theodwyn

X = theodwyn
Y = thengel

X = theodwyn
Y = thengel

X = theodwyn
Y = morwen

X = theodwyn
Y = morwen

X = eowyn
Y = thengel

X = eowyn
Y = thengel

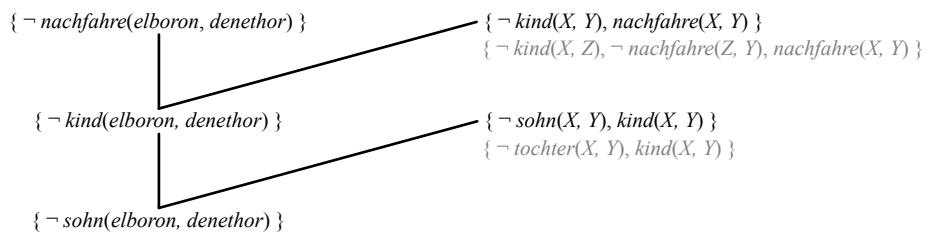
X = eowyn
Y = morwen

X = eowyn
Y = morwen
```

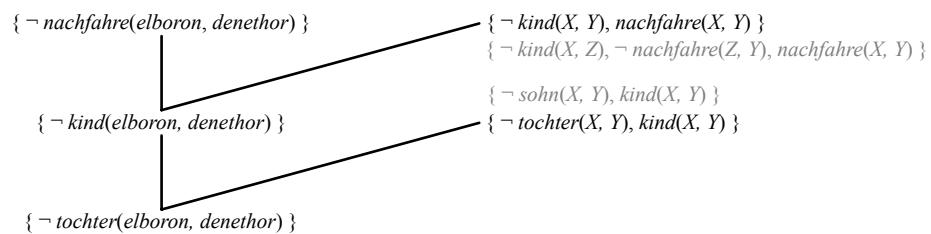
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41

**Abbildung 3.57:** Auf die gestellte Anfrage antwortet der Prolog-Interpreter mit allen Personenpaaren, in denen  $X$  ein weiblicher Nachfahre von  $Y$  ist.

## ■ Pfad 1



## ■ Pfad 2



## ■ Pfad 3

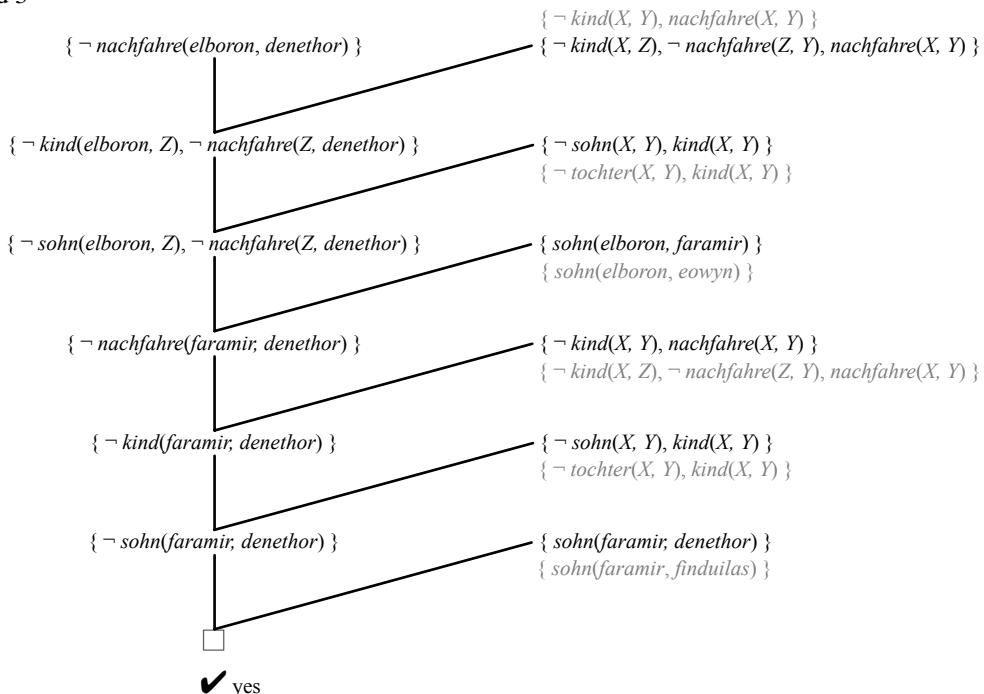


Abbildung 3.58: Intern führt der Prolog-Interpreter einen Resolutionsbeweis durch.

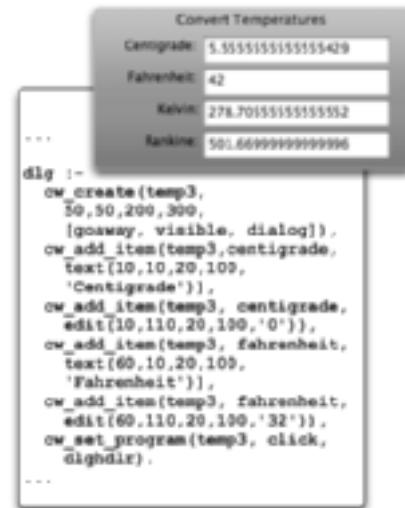
eine Sackgasse gerät. Während der Ableitung existieren an verschiedenen Stellen Entscheidungspunkte, an denen die Resolventenbildung ohne weitere Vorgaben indeterministisch wäre. Zum einen muss der Interpreter entscheiden, welches Literal als Nächstes zu eliminierten ist; zum anderen, mit welcher Klausel der Wissensbasis die neue Resolvente gebildet werden soll. Prolog legt die Vorgehensweise wie folgt fest: Zum einen wird immer das am weitesten links stehende Literal in der Anfrage bzw. in den resolvierten Nachfolgern eliminiert. Zum anderen werden die Regeln der Wissensbasis in derselben Reihenfolge berücksichtigt, wie sie im Programmtext angeordnet sind.

Mit diesen Vorgaben wird die Resolventenbildung zu einem deterministischen Prozess, der für die Anfrage `nachfare(elboron,denethor)` zunächst den in Abbildung 3.58 (oben) gezeigten Resolutionsbaum her vorbringt. Nach zwei Schritten gerät die Ableitung in eine Sackgasse, da sich die Klausel `{¬sohn(elboron,denethor)}` nicht weiter resolvieren lässt. In diesem Fall kehrt Prolog an den letzten Entscheidungspunkt zurück und revidiert die getroffene Auswahl. In der Terminologie der logischen Programmierung wird dieser Vorgang als *Backtracking* bezeichnet. In unserem Beispiel bildet der Interpreter die zweite Resolvente jetzt mit der Klausel `{¬tochter(X,Y), kind(X,Y)}` (vgl. Abbildung 3.58 Mitte), gerät jedoch wiederum in eine Sackgasse. Nach zweimaligem Backtracking wird der Beweis im dritten Anlauf schließlich gefunden. Der Interpreter kann die leere Klausel in 6 Resolutionsschritten erfolgreich ableiten und beantwortet die Anfrage mit 'yes' (vgl. Abbildung 3.58 unten).

### 3.3 Logiken höherer Stufe

Logiken höherer Stufe sind eine Erweiterung der Prädikatenlogik erster Stufe, die auf dem typisierten Lambda-Kalkül basieren [20]. Von der in Abschnitt 3.2 eingeführten Prädikatenlogik unterscheiden sie sich in den folgenden Punkten:

- Die strikte Unterscheidung zwischen Termen und Prädikaten wird aufgehoben. In Logiken höherer Stufe existieren ausschließlich Terme, die nach gewissen Regeln zu komplexeren Termen kombiniert werden können. Die Verschmelzung beider Begriffe führt dazu, dass jedes Prädikat als Argument von Funktionen und anderer Prädikate verwendet werden darf.
- Aufgrund der eingebauten Typisierung lassen sich in Logiken höherer Stufe viele Sachverhalte auf natürlichere Art und Weise formu-



**Abbildung 3.59:** GUI-Programmierung mit Prolog

Die Leistungsfähigkeit von Prolog geht weit über die hier vorgestellten Möglichkeiten hinaus. Heute existieren professionelle Entwicklungsumgebungen, die ein komfortables Arbeiten ermöglichen und den Programmierer durch eine Vielzahl vorgefertigte Bibliotheken unterstützen. Wie in Abbildung 3.59 gezeigt, lassen sich mit wenigen Zeilen Code grafische Applikationen entwickeln, deren Herkunft von außen nicht mehr sichtbar ist. Trotzdem ist der logischen Programmierung der große Durchbruch verwehrt geblieben. Wurde Prolog in den Achtzigerjahren noch als zukunftsweisende Programmiersprache der „fünften Generation“ bezeichnet, ist der damalige Enthusiasmus heute weitgehend abgeebbt. In der Praxis funktioniert die Idee, das Problem und den nicht den Lösungsweg zu beschreiben, weniger gut als in der Theorie erhofft. Trotzdem konnte Prolog in einigen Disziplinen wie z. B. der künstlichen Intelligenz seinen Platz behaupten. In diesem Bereich wird die Sprache seit vielen Jahren mit Erfolg eingesetzt.

Dass die Prädikatenlogik erster Stufe nicht ausreicht, um die natürlichen Zahlen zu charakterisieren, ist ein wichtiges Meta-Resultat über ihre Ausdrucksstärke. Aber auch in anderer Hinsicht erweist sich die Prädikatenlogik als überraschend ausdrucksschwach.

So lässt sich die mathematische Gleichheitsrelation = ebenfalls nicht innerhalb der Logik modellieren, d. h., es ist unmöglich, eine Formel zu konstruieren, die genau dann wahr ist, wenn ein bestimmtes Prädikat  $P(x,y)$  durch die Gleichheitsrelation interpretiert wird.

In der Vergangenheit wurde die Prädikatenlogik in verschiedene Richtungen erweitert, um die geschilderten Limitierungen zu umgehen. In der sogenannten *Prädikatenlogik mit Gleichheit* wird der Symbolvorrat um ein dediziertes Prädikat  $\doteq$  erweitert, das genau dann wahr ist, wenn auf der linken und der rechten Seite dasselbe Element der Individuenmenge steht. Die Konsequenzen dieser Erweiterung wurden in der Vergangenheit ausführlich untersucht und angepasste Varianten des Hilbert-, des Resolutions- und des Tableaukalküls entwickelt. In Bezug auf die Ausdrucksstärke steht die Prädikatenlogik mit Gleichheit zwischen der Prädikatenlogik erster Stufe und den Logiken höherer Stufe.

Ein weiteres Problem ist die Beschreibung von Kausalität, wie sie für die Verifikation zeitlicher Zusammenhänge benötigt wird. Für die Modellierung zeitbehafteter Systeme wird heute zumeist auf spezielle aussagenlogische und prädikatenlogische Temporallogiken zurückgegriffen. Zu den wichtigsten Vertretern gehören die *Linear Time Logic*, kurz LTL, und die *Computation Tree Logic*, kurz CTL. Diese entstehen aus der Aussagenlogik bzw. der Prädikatenlogik, indem der Symbolvorrat unter anderem um die temporalen Operatoren  $\circ$  („im nächsten Zeitpunkt“),  $\square$  („immer in der Zukunft“) und  $\diamond$  („irgendwann in der Zukunft“) erweitert wird.

lieren, als es in der Prädikatenlogik erster Stufe möglich ist. Trotzdem dienen die neu hinzugefügten Datentypen nicht ausschließlich der Bequemlichkeit. Sie verhindert die Niederschrift widersprüchlicher Aussagen, wie wir sie beispielsweise in Form der Russell'schen Antinomie in Abschnitt 1.2 kennen gelernt haben.

Durch die fehlende Trennung zwischen Termen und Prädikaten werden in Logiken höherer Stufe die Geltungsbereiche der Quantoren  $\forall$  und  $\exists$  erweitert. Im Gegensatz zur Prädikatenlogik, in der Quantoren ausschließlich auf Variablen angewendet werden dürfen, erlauben Logiken höherer Stufe die Quantifizierung über Prädikate hinweg. Hierdurch lassen sich Aussagen der Form

„Für alle Eigenschaften  $P$  gilt ...“ und

„Es existiert eine Eigenschaft  $P$ , so dass ...“

formulieren, die sich der Prädikatenlogik erster Stufe aufgrund ihrer eingeschränkten Beschreibungsmöglichkeiten entziehen.

Erst die Logiken höherer Stufe verfügen über die nötige Ausdrucksstärke, um z. B. die natürlichen Zahlen zu charakterisieren. Schuld daran ist das fünfte Peano-Axiom, das die vollständige Induktion auf den natürlichen Zahlen begründet.

In Abschnitt 2.4.1 haben wir die vollständige Induktion neben dem direkten Deduktionsbeweis und dem indirekten Widerspruchsbeweis als dritte grundlegende Beweistechnik der Mathematik kennen gelernt. Dort haben wir herausgearbeitet, dass sich die Induktionstechnik auf alle Aussagen anwenden lässt, die von einem natürlichezähligen Parameter  $n$  abhängen und *für alle  $n$*  gezeigt werden sollen. Um eine solche Aussage zu beweisen, sind wir in drei Schritten vorgegangen. Im Induktionsanfang haben wir die Behauptung zunächst für den Fall  $n = 0$  überprüft. Anschließend nahmen wir an, dass die Aussage für einen beliebigen Wert  $n \in \mathbb{N}_0$  gilt, und versuchten zu zeigen, dass sich die Gültigkeit der Behauptung auf den Fall  $n + 1$  überträgt. Gelingt dieser Beweis, so garantiert uns das fünfte Peano-Axiom, dass die Aussage für ausnahmslos alle natürlichen Zahlen erfüllt ist. In Logiken höherer Stufe lässt sich das Axiom auf natürliche Weise wie folgt beschreiben:

$$\forall P ((P(0) \wedge \forall n (P(n) \rightarrow P(\text{succ}(n)))) \rightarrow \forall n P(n))$$

Da der erste Quantor auf ein Prädikat angewendet wird, lässt sich die Formel nicht mit den Mitteln der traditionellen Prädikatenlogik formulieren.

is_prime.c	is_prime.ml
<pre> int is_prime(unsigned int nr) {     int i;      for (i=2; i&lt;nr; i++) {         if (nr % i == 0) {             return 0;         }     }      return 1; } </pre>	<pre> 1   val divides = Define 2     'divides a b = 3       ?x. b = a * x'; 4   val prime = Define 5     'prime p = 6       ~(p=1) /\  7         !x. x divides p ==&gt; 8           (x=1) \/ (x=p)'; 9 10    (!x. 11      (prime(x) ==&gt; (is_prime(x)=1) \/ 12        !prime(x) ==&gt; (is_prime(x)=0))) </pre>

**Abbildung 3.60:** Formale Spezifikation eines C-Programms mit Hilfe einer Logik höherer Stufe. Auf der linken Seite ist die Implementierung, auf der rechten die formale Spezifikation in der Sprache des Theorembeweisers HOL zu sehen.

Logiken höherer Stufe werden insbesondere im Bereich der Software-Verifikation eingesetzt. Hierbei wird das verlockende Ziel verfolgt, die *Korrektheit*, d. h. die Erfüllung der Spezifikation durch die Implementierung, mit Hilfe mathematischer Ableitungsregeln formal zu beweisen. Um die praktische Verwendung einer solchen Logik zu verdeutlichen, ist in Abbildung 3.60 exemplarisch eine einfache C-Funktion zusammen mit ihrer formalen Spezifikation dargestellt. Das Quellprogramm definiert eine Funktion `is_prime`, die für den Integer-Wert `nr` entscheidet, ob er eine Primzahl enthält oder nicht. Rechts daneben ist die Spezifikation dargestellt, formuliert in der Syntax des Theorembeweisers HOL [37]. Die Spezifikation definiert zunächst zwei Hilfsprädikate `divides` und `prime`, die zum einen die Teilbarkeitseigenschaft und zum anderen die Prim-Eigenschaft einer Zahl beschreiben. Das Verhalten der C-Funktion wird in Form eines mathematischen Theorems spezifiziert, das den Ergebniswert der Funktion `is_prime` mit dem Prädikat `prime` verknüpft.

Die hohe Ausdrucksstärke von Logiken höherer Stufe fordert ihren Tribut in Form einer komplexen Beweisführung. Die heute zur Verfügung stehenden Beweiskalküle verfügen nur über ein geringes Automatisierungspotenzial, so dass große Teile eines Korrektheitsbeweises manuell durchgeführt werden müssen. Die Berechenbarkeitstheorie setzt ebenfalls klare Grenzen. Aus dem Gödel'schen Unvollständigkeitssatz folgt sofort, dass Logiken höherer Stufe aufgrund ihrer Ausdrucksstärke die Eigenschaft der Semi-Entscheidbarkeit verlieren müssen (vgl. Abbildung 3.61).

Entscheidbar	Semi-Entscheidbar	Natürliche Zahlen	Gleichheit
+	+	-	-
-	+	-	-
-	-	+	+
Naturliche Grenze bez. der Berechenbarkeit			Aussagenlogik
Naturliche Grenze bez. der Ausdrucksstärke			Prädikatenlogik
Logik höherer Stufe			

**Abbildung 3.61:** Berechenbarkeitseigenschaften und Ausdrucksstärke der vorgestellten Logiken

## 3.4 Übungsaufgaben

### Aufgabe 3.1

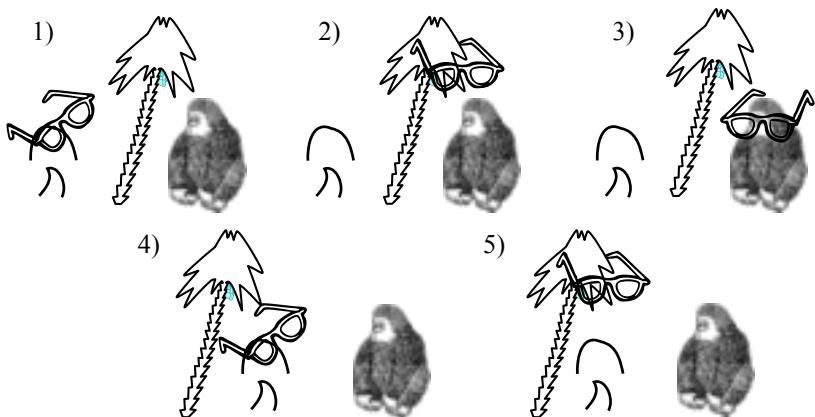


**Webcode  
3835**

Klammern sind ein Hilfsmittel, um eine Logikformel auf der syntaktischen Ebene in der gewünschten Art und Weise zu gruppieren. Die Probleme, die durch das Weglassen von Klammern entstehen, sind dieselben, mit denen wir uns auch in der deutschen Sprache tagtäglich konfrontiert sehen. Als Beispiel dient der folgende Satz:

„Ich sehe den Gorilla unter der Palme mit der Sonnenbrille“

- a) Wie müsste der Satz jeweils geklammert werden, damit er die folgenden Situationen korrekt beschreibt:



- b) Klammern sind bekanntlich kein offizieller Bestandteil der deutschen Sprache. Wie gehen wir stattdessen mit solchen Mehrdeutigkeiten um?

---

### Aufgabe 3.2



**Webcode  
3378**

Gegeben seien die folgenden beiden aussagenlogischen Formeln:

$$F := AB \vee AC \vee BC \quad \text{und} \tag{3.39}$$

$$G := AB \vee C(A \leftrightarrow B), \tag{3.40}$$

Zeigen Sie, dass  $F$  und  $G$  äquivalent sind, indem Sie

- a) für beide Formeln eine Wahrheitstabelle aufstellen.
- b)  $G$  durch die Anwendung der aussagenlogischen Umformungsregeln in  $F$  überführen.

Gegeben sei die folgende aussagenlogische Formel:

$$F := \left( \bigvee_{i=1}^n A_i \right) \wedge \left( \bigwedge_{i=1}^{n-1} \bigwedge_{j=i+1}^n \overline{A_i \wedge A_j} \right) \quad (3.41)$$

**Aufgabe 3.3****Webcode  
3561**

Vervollständigen Sie die nachstehende Wahrheitstabelle für den Fall  $n = 4$ :

$A_4$	$A_3$	$A_2$	$A_1$	$F$	$A_4$	$A_3$	$A_2$	$A_1$	$F$
0	0	0	0		8	1	0	0	0
1	0	0	1		9	1	0	0	1
2	0	1	0		10	1	0	1	0
3	0	1	1		11	1	0	1	1
4	0	1	0		12	1	1	0	0
5	0	1	0		13	1	1	0	1
6	0	1	1		14	1	1	1	0
7	0	1	1		15	1	1	1	1

Beschreiben Sie in Worten, welche Eigenschaft eine Variablenbelegung  $A_1, \dots, A_n$  erfüllen muss, damit  $F$  wahr wird.

Die aussagenlogischen Existenz- und Allquantoren  $\exists$  und  $\forall$  seien wie folgt definiert:

$$(\exists A F) \equiv 1 \Leftrightarrow F \equiv 1 \text{ für mindestens eine Belegung der Variablen } A$$

$$(\forall A F) \equiv 1 \Leftrightarrow F \equiv 1 \text{ für alle Belegungen der Variablen } A$$

**Aufgabe 3.4****Webcode  
3093**

Ferner vereinbaren wir die folgende Schreibweise:

$$\exists A_1, A_2, \dots, A_n F := \exists A_1 (\exists A_2, \dots, A_n F)$$

$$\forall A_1, A_2, \dots, A_n F := \forall A_1 (\forall A_2, \dots, A_n F)$$

Beachten Sie, dass die Quantoren auf aussagenlogische Variablen und damit streng genommen auf (nullstellige) Prädikate angewendet werden. Sie unterscheiden sich damit grundsätzlich von ihren prädikatenlogischen Pendants.

- Lassen sich die Quantoren durch die Elementaroperatoren  $\neg$ ,  $\wedge$  und  $\vee$  ausdrücken?
- Seien  $F$  und  $G$  aussagenlogische Formeln, in denen die Variablen  $A_1, \dots, A_n$  vorkommen. Welche bekannten Eigenschaften erfüllen  $F$  und  $G$ , wenn die Beziehungen  $\exists A_1, \dots, A_n G \equiv 1$  bzw.  $\forall A_1, \dots, A_n F \equiv 1$  gelten?

**Aufgabe 3.5****Webcode  
3798**

Mit  $F$  sei eine variablenfreie aussagenlogische Formel gegeben, die neben den beiden Wahrheitswerten 0 und 1 ausschließlich den Äquivalenzoperator  $\leftrightarrow$  enthält.

- Ist die Formel  $(1 \leftrightarrow 0) \leftrightarrow ((1 \leftrightarrow 0) \leftrightarrow (0 \leftrightarrow 1))$  eine Tautologie?
- Ist die Formel  $(1 \leftrightarrow 0) \leftrightarrow ((0 \leftrightarrow 0) \leftrightarrow (1 \leftrightarrow 0))$  eine Tautologie?
- Zeigen oder widerlegen Sie die folgende Behauptung:  $F$  ist genau dann eine Tautologie, wenn der Wahrheitswert 0 geradzahlig oft in  $F$  vorkommt.

**Aufgabe 3.6****Webcode  
3234**

Die Funktionen  $F_1$  und  $F_2$  seien wie folgt definiert:

$$F_1 = (L_1 \vee L_2 \vee L_3 \vee L_4) \quad (3.42)$$

$$F_2 = (L_1 \vee L_2 \vee L') \wedge (\neg L' \vee L_3 \vee L_4) \quad (3.43)$$

Zeigen Sie, dass die Formeln  $F_1$  und  $F_2$  erfüllbarkeitsäquivalent sind, d. h.,  $F_1$  ist genau dann erfüllbar, wenn  $F_2$  erfüllbar ist.

**Aufgabe 3.7****Webcode  
3192**

Die nachstehenden Wahrheitstabellen definieren die booleschen Operatoren  $\overline{\wedge}$  (NAND) und  $\overline{\vee}$  (NOR):

	$A$	$B$	$A \overline{\wedge} B$		$A$	$B$	$A \overline{\vee} B$
0	0	0	1	0	0	0	1
1	0	1	1	1	0	1	0
2	1	0	1	2	1	0	0
3	1	1	0	3	1	1	0

- Drücken Sie  $\overline{\wedge}$  und  $\overline{\vee}$  mit Hilfe der Elementaroperatoren  $\neg$ ,  $\wedge$  und  $\vee$  aus.
- Zeigen Sie, dass die Mengen  $\{\overline{\wedge}\}$  und  $\{\overline{\vee}\}$  vollständige Operatorensysteme sind.

**Aufgabe 3.8****Webcode  
3659**

In diesem Kapitel haben Sie gelernt, aussagenlogische Formeln mit Hilfe des Hilbert-Kalküls zu beweisen. Vervollständigen Sie die folgende Ableitungssequenz, indem Sie für jedes Element der Beweiskette angeben, wie dieses entstanden ist. Beachten Sie, dass der Beweis neben den Axiomen auch auf die bereits bewiesenen Theoreme auf Seite 99 zurückgreift.

- $\vdash A \rightarrow (\neg\neg A \rightarrow \neg(A \rightarrow \neg A))$  ( )
- $\{A\} \vdash \neg\neg A \rightarrow \neg(A \rightarrow \neg A)$  ( )
- $\{A\} \vdash A \rightarrow \neg\neg A$  ( )
- $\{A\} \vdash \neg\neg A$  ( )
- $\{A\} \vdash \neg(A \rightarrow \neg A)$  ( )
- $\vdash A \rightarrow \neg(A \rightarrow \neg A)$  ( )
- $\vdash (A \rightarrow \neg(A \rightarrow \neg A)) \rightarrow (\neg\neg(A \rightarrow \neg A) \rightarrow \neg A)$  ( )
- $\vdash \neg\neg(A \rightarrow \neg A) \rightarrow \neg A$  ( )
- $\vdash (A \rightarrow \neg A) \rightarrow \neg\neg(A \rightarrow \neg A)$  ( )
- $\vdash ((A \rightarrow \neg A) \rightarrow \neg\neg(A \rightarrow \neg A)) \rightarrow ((\neg\neg(A \rightarrow \neg A) \rightarrow \neg A) \rightarrow ((A \rightarrow \neg A) \rightarrow \neg A))$  ( )
- $\vdash (\neg\neg(A \rightarrow \neg A) \rightarrow \neg A) \rightarrow ((A \rightarrow \neg A) \rightarrow \neg A)$  ( )
- $\vdash (A \rightarrow \neg A) \rightarrow \neg A$  ( )

In Abschnitt 3.1.3.1 wurde argumentiert, dass der Hilbert-Kalkül korrekt ist. Um den Beweis abzuschließen, muss die Allgemeingültigkeit der Axiome

**Aufgabe 3.9**

**Webcode**
**3850**

- (A1) :  $A \rightarrow (B \rightarrow A)$
- (A2) :  $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
- (A3) :  $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

gezeigt werden. Führen Sie den Beweis durch die Vervollständigung der nachstehenden Wahrheitstabellen zu Ende:

	A	B	(A1)
0	0	0	
1	0	1	
2	1	0	
3	1	1	

	A	B	C	(A2)
0	0	0	0	
1	0	0	1	
2	0	1	0	
3	0	1	1	
4	1	0	0	
5	1	0	1	
6	1	1	0	
7	1	1	1	

	A	B	(A3)
0	0	0	
1	0	1	
2	1	0	
3	1	1	

**Aufgabe 3.10****Webcode****3235**

Beweisen oder widerlegen Sie die Unerfüllbarkeit der folgenden Klauselmenge mit Hilfe der aussagenlogischen Resolution:

$$\begin{array}{lcl} \{ A, B, C \} & \{ \neg A, \neg B \} & \{ \neg A, \neg C \} \\ \{ \neg B, \neg A \} & \{ \neg B, \neg C \} & \{ \neg C, \neg A \} \\ \{ \neg C, \neg B \} & \{ A, \neg B \} & \{ B, \neg C \} \end{array}$$

**Aufgabe 3.11****Webcode****3021**

In diesem Kapitel haben Sie gelernt, wie aussagenlogische Formeln im Resolutionskalkül bewiesen werden können. Da die entstehenden Beweise oft von beträchtlicher Länge sind, entsteht der Wunsch, mehrere Resolutionsschritte auf einmal durchzuführen. Hierzu wollen wir den bestehenden Kalkül um die folgende Resolutionsregel erweitern:

$$\frac{M_1 \cup \{F, G\}, M_2 \cup \{\neg F, \neg G\}}{M_1 \cup M_2}$$

Ist der resultierende Kalkül immer noch korrekt? Begründen Sie Ihre Antwort.

**Aufgabe 3.12****Webcode****3888**

Unifizieren Sie die folgenden Formelpaare mit dem Algorithmus von Robinson:

- |                                |                                      |
|--------------------------------|--------------------------------------|
| a) $f(g(x), y), f(g(z), g(a))$ | d) $f(x, g(y)), f(g(y), x)$          |
| b) $f(x), f(f(f(y)))$          | e) $f(x, g(y)), f(y, g(x))$          |
| c) $f(x), f(f(x))$             | f) $f(f(x), y, g(g(z))), f(x, y, z)$ |

**Aufgabe 3.13****Webcode****3045**

Sei  $K$  ein beliebiger Kalkül und  $M$  eine Formelmenge. Vervollständigen Sie die folgenden Definitionen:

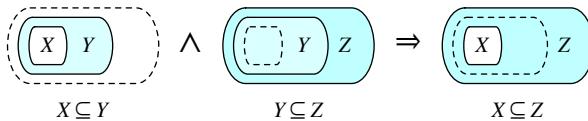
- |  |  |
|--|--|
| a) $K$ ist korrekt : $\Leftrightarrow$     |  |
| b) $K$ ist vollständig : $\Leftrightarrow$ |  |
| c) $M$ ist konsistent : $\Leftrightarrow$  |  |
| d) $M$ ist vollständig : $\Leftrightarrow$ |  |

Aus der elementaren Mengenlehre wissen Sie, dass die Inklusionsbeziehung transitiv ist:  
Sind  $X$ ,  $Y$  und  $Z$  Mengen, so folgt aus  $X \subseteq Y$  und  $Y \subseteq Z$  die Beziehung  $X \subseteq Z$ .

**Aufgabe 3.14**



**Webcode  
3971**



In mathematischer Notation lässt sich die Transitivität wie folgt charakterisieren:

$$\forall x \forall y \forall z (x \subseteq y \wedge y \subseteq z \rightarrow x \subseteq z) \quad (3.44)$$

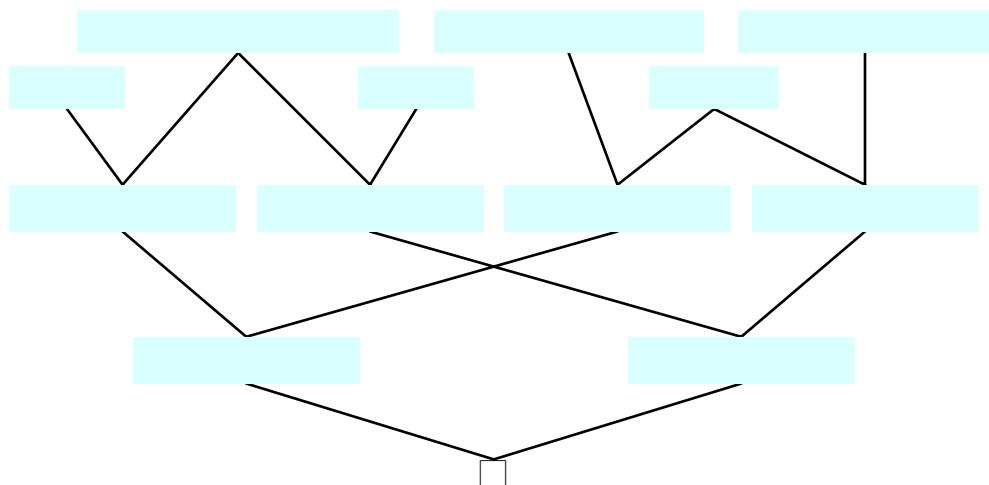
Beschreiben wir die Teilmengenbeziehung über die Formel

$$\forall x \forall y (x \subseteq y \leftrightarrow \forall z (z \in x \rightarrow z \in y)), \quad (3.45)$$

so lässt sich die Transitivität mit Hilfe der Prädikatenlogik formal beweisen. Hierzu führen wir zunächst die beiden Prädikate  $M$  (*member*) und  $C$  (*contains*) ein, um die Mengenzugehörigkeit  $\in$  und die Inklusionseigenschaft  $\subseteq$  zu beschreiben. Die Formeln (3.44) und (3.45) lassen sich dann wie folgt zusammenfassen:

$$\forall x \forall y (C(x, y) \leftrightarrow \forall z (M(z, x) \rightarrow M(z, y))) \rightarrow \forall x \forall y \forall z (C(x, y) \wedge C(y, z) \rightarrow C(x, z)) \quad (3.46)$$

Ihre Aufgabe ist es, die Transitivität mit Hilfe des Resolutionskalküls zu beweisen. Transformieren Sie die Formel (3.46) hierzu zunächst in Skolem-Form und vervollständigen Sie anschließend den folgenden Resolutionsgraphen:

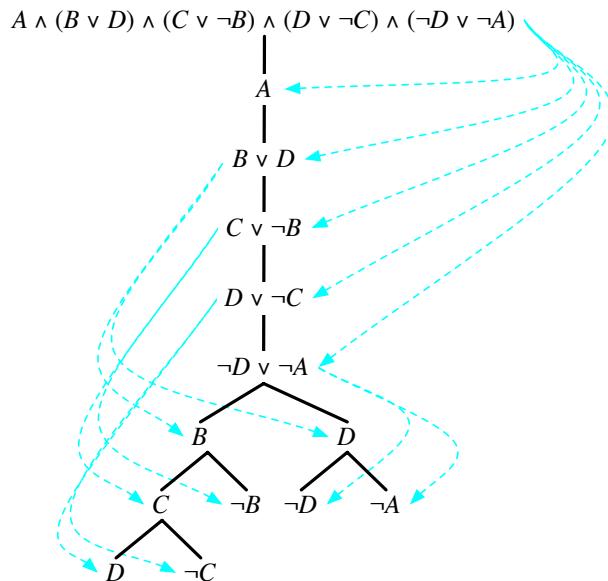


**Aufgabe 3.15**

**Webcode**  
**3369**

Gegeben sei das folgende Tableau für die Formel

$$F := A \wedge (B \vee D) \wedge (C \vee \neg B) \wedge (D \vee \neg C) \wedge (\neg D \vee \neg A). \quad (3.47)$$



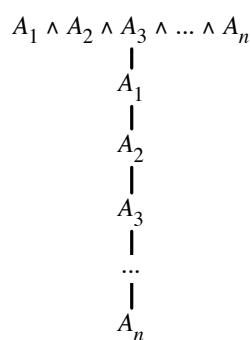
Der linke Pfad ist widerspruchsfrei, so dass die Belegung  $A = B = C = D = 1$  ein Modell für  $F$  sein muss. Verifizieren Sie diese Behauptung anhand einer Wahrheitstabelle und klären Sie den entstehenden Widerspruch auf.

**Aufgabe 3.16**

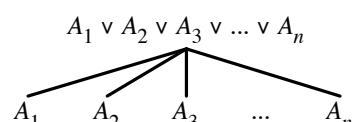
**Webcode**  
**3177**

Welche der folgenden aussagenlogischen Tableauregeln sind korrekt?

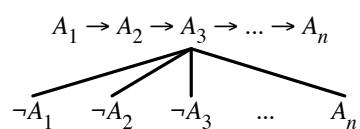
1) Erweiterte Konjunktionsregel



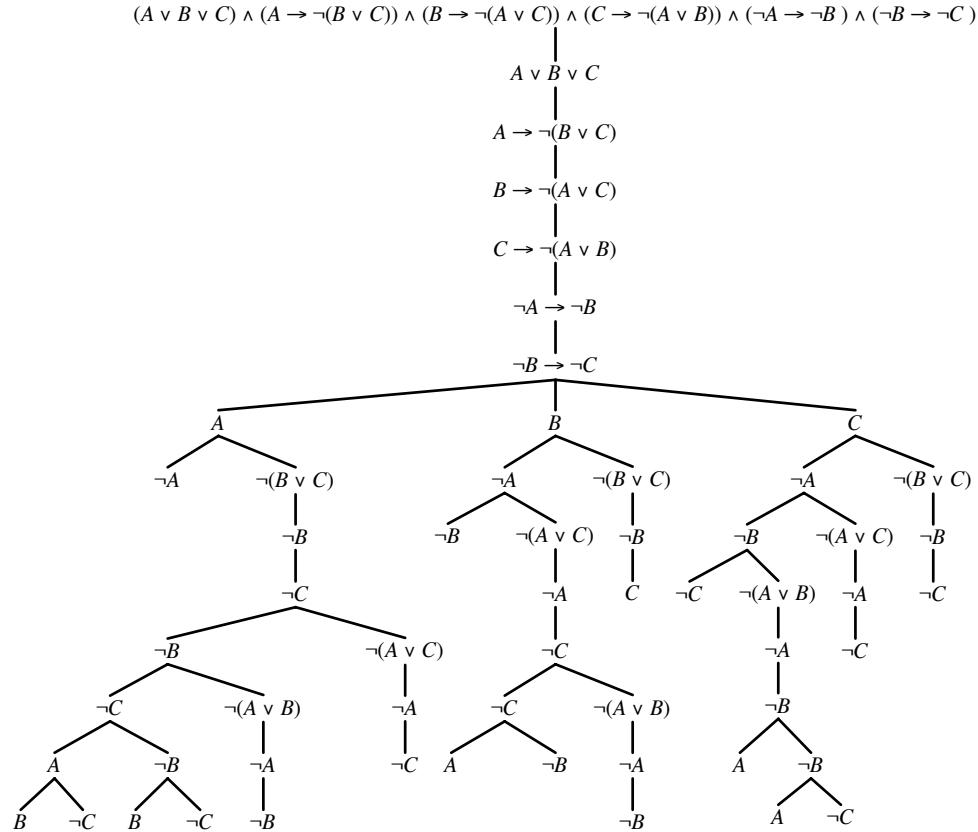
2) Erweiterte Disjunktionsregel



3) Erweiterte Implikationsregel



Gegeben sei das folgende aussagenlogische Tableau:



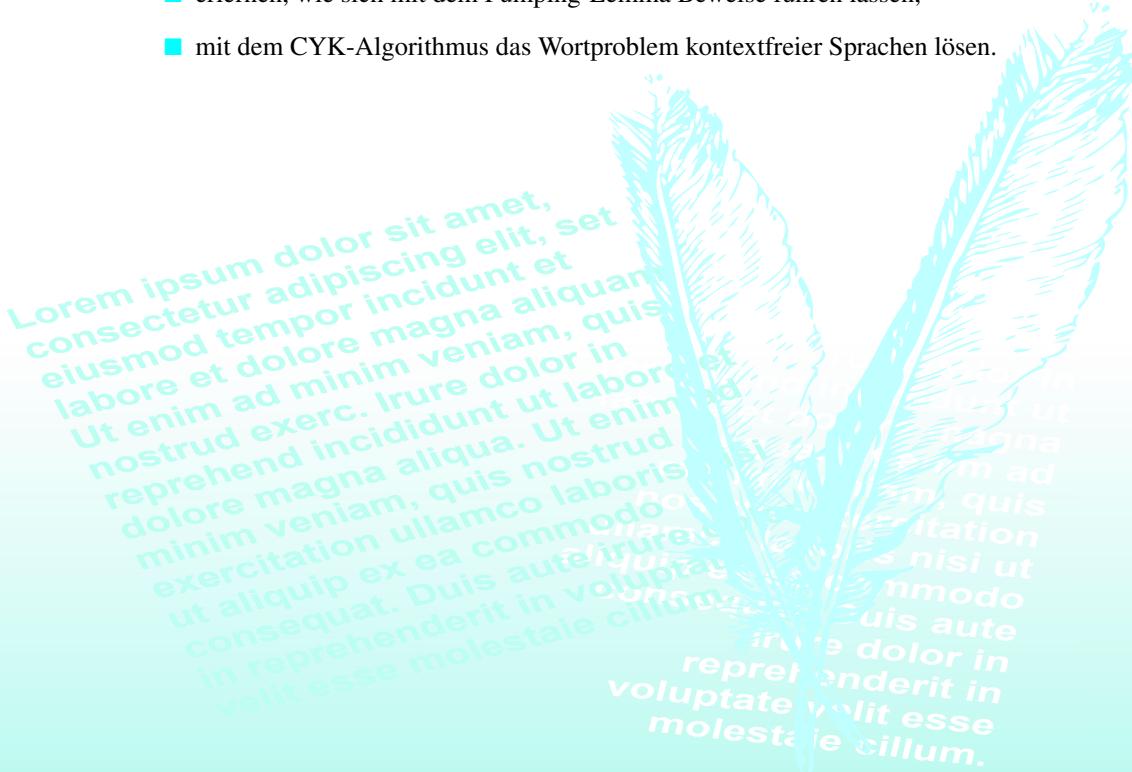
- a) Geben Sie für jeden widersprüchlichen Pfad an, durch welches Variablenpaar der Abschluss entsteht.
- b) Extrahieren Sie für jeden widerspruchsfreien Pfad ein Modell, falls solche Pfade überhaupt existieren.
- c) Ist das Tableau vollständig?
- d) Ist das Tableau geschlossen?
- e) Ist die Ausgangsformel eine Tautologie?



## 4 Formale Sprachen

In diesem Kapitel werden Sie ...

- formale Sprachen mit Hilfe von Grammatiken erzeugen,
- die Chomsky-Hierarchie verstehen,
- die Besonderheiten regulärer, kontextfreier und kontextsensitiver Grammatiken ergründen,
- die wichtigsten Entscheidungsprobleme im Bereich der formalen Sprachen kennen lernen,
- die Abschlusseigenschaften verschiedener Sprachtypen untersuchen,
- erlernen, wie sich mit dem Pumping-Lemma Beweise führen lassen,
- mit dem CYK-Algorithmus das Wortproblem kontextfreier Sprachen lösen.



■ Definition

$$\Sigma^0 := \{\epsilon\}$$

$$\Sigma^1 := \Sigma$$

$$\Sigma^{n+1} := \{xy \mid x \in \Sigma, y \in \Sigma^n\}$$

$$\Sigma^+ := \bigcup_{i=1}^{\infty} \Sigma^i$$

$$\Sigma^* := \bigcup_{i=0}^{\infty} \Sigma^i$$

■ Beispiel:  $\Sigma := \{a, b\}$

$$\Sigma^0 = \{\epsilon\}$$

$$\Sigma^1 = \{a, b\}$$

$$\Sigma^2 = \{aa, ab, ba, bb\}$$

...

$$\Sigma^+ = \{a, b, aa, ab, ba, bb, \dots\}$$

$$\Sigma^* = \{\epsilon, a, b, aa, ab, ba, bb, \dots\}$$

## 4.1 Sprache und Grammatik

Die Theorie der formalen Sprachen beschäftigt sich mit der systematischen Analyse, der Klassifikation und der Konstruktion von Wortmengen, die über einem endlichen *Alphabet* gebildet werden. Bevor wir uns im Detail mit den Eigenschaften formaler Sprachen beschäftigen, wollen wir mit der folgenden Definition die elementaren Begriffe einführen, die uns durch das gesamte Kapitel hinweg auf Schritt und Tritt begleiten werden.



### Definition 4.1 (Alphabet, Zeichen, Wort, Sprache)

- Ein *Alphabet*  $\Sigma$  ist eine endliche Menge von Symbolen.
- Jedes Element  $\sigma \in \Sigma$  ist ein *Zeichen* des Alphabets.
- Jedes Element  $\omega \in \Sigma^*$  wird als *Wort* über  $\Sigma$  bezeichnet.
- Jede Teilmenge  $L \subseteq \Sigma^*$  ist eine *formale Sprache* über  $\Sigma$ .

**Abbildung 4.1:** Formale Charakterisierung der Wortmengen  $\Sigma^i$ ,  $\Sigma^*$  und  $\Sigma^+$

■ Beispiel:  $L := \{ab, ba\}$

$$L^0 = \{\epsilon\}$$

$$L^1 = \{ab, ba\}$$

$$L^2 = \{abab, abba, baab, baba\}$$

...

$$L^+ = \{ab, ba, abab, abba, baab, baba, \dots\}$$

$$L^* = \{\epsilon, ab, ba, abab, abba, baab, baba, \dots\}$$

Die Definition fordert ausdrücklich, dass der Zeichenvorrat  $\Sigma$  einer Sprache nur aus endlich vielen Elementen besteht. Die Menge  $\Sigma^*$  wird als *Kleene'sche Hülle* bezeichnet und fasst alle endlichen Symbolsequenzen zusammen, die mit Zeichen aus dem Alphabet  $\Sigma$  aufgebaut werden können. Wie in den Abbildungen 4.1 und 4.2 in mathematischer Notation beschrieben, unterscheidet sie sich von der Menge  $\Sigma^+$  lediglich dadurch, dass  $\Sigma^*$  auch das leere Wort  $\epsilon$  enthält. Anders als die Wörter einer Sprache, die stets eine endliche Länge aufweisen, kann eine Sprache  $L$  aus unendlich vielen Wörtern bestehen. Die Beispiele in Abbildung 4.3 verdeutlichen den Sprachbegriff.

Im Bereich der formalen Sprachen sind die folgenden Fragestellungen von Interesse:

■ Wortproblem

Gilt für ein Wort  $\omega \in \Sigma^*$  und eine Sprache  $L$  die Beziehung  $\omega \in L$ ?

■ Leerheitsproblem

Enthält eine Sprache  $L$  mindestens ein Wort, gilt also  $L \neq \emptyset$ ?

■ Endlichkeitsproblem

Besitzt eine Sprache  $L$  nur endlich viele Elemente?

**Abbildung 4.2:** Nicht nur Alphabete, sondern beliebige Sprachen lassen sich mit den eingeführten Mengenoperatoren miteinander kombinieren.

### ■ Äquivalenzproblem

Gilt für zwei Sprachen  $L_1$  und  $L_2$  die Beziehung  $L_1 = L_2$ ?

### ■ Spracherzeugung

Gibt es für eine Sprache  $L$  eine Beschreibung, aus der sich alle Wörter systematisch ableiten lassen?

Die ersten vier Fragestellungen adressieren die *analytischen* Aspekte einer Sprache, auf die wir später im Detail zu sprechen kommen werden. Für den Moment wollen wir unser Augenmerk auf die letzte Fragestellung richten, die sich mit dem *generativen* Aspekt einer Sprache beschäftigt.

Folgt der Aufbau strukturierten Regeln, so lassen sich die Wörter einer Sprache mit Hilfe einer *Grammatik* erzeugen. Für unsere natürliche Sprache sind wir mit diesem Vorgehen wohlvertraut. Anstatt alle korrekt geformten Sätze nacheinander aufzulisten, wird eine Reihe von Regeln vereinbart, mit denen sich elementare Sprachkonstrukte systematisch zu komplexen Gebilden zusammensetzen lassen. Als Beispiel betrachten wir die folgende Grammatik, die einen kleinen Auszug aus dem deutschen Sprachschatz erzeugt:

$\langle \text{Satz} \rangle$	$\rightarrow$	$\langle \text{Subjekt} \rangle \langle \text{Prädikat} \rangle \langle \text{Objekt} \rangle$
$\langle \text{Subjekt} \rangle$	$\rightarrow$	$\langle \text{Artikel} \rangle \langle \text{Adjektiv} \rangle \langle \text{Substantiv} \rangle$
$\langle \text{Artikel} \rangle$	$\rightarrow$	Der   Die   Das
$\langle \text{Adjektiv} \rangle$	$\rightarrow$	kleine   süße   flinke
$\langle \text{Substantiv} \rangle$	$\rightarrow$	Eisbär   Elch   Kröte   Maus   Nilpferd
$\langle \text{Prädikat} \rangle$	$\rightarrow$	mag   fängt   isst
$\langle \text{Objekt} \rangle$	$\rightarrow$	Kekse   Schokolade   Käsepizza

In der Terminologie der formalen Sprachen werden die in spitze Klammern gesetzten Platzhalter als *Nonterminale* oder *Nichtterminale* und die nicht weiter ersetzbaren Sprachbestandteile als *Terminale* bezeichnet. Für unsere Beispielgrammatik erhalten wir die nachstehende Einteilung:

### ■ Nonterminale

$\langle \text{Satz} \rangle$ ,  $\langle \text{Subjekt} \rangle$ ,  $\langle \text{Artikel} \rangle$ ,  $\langle \text{Adjektiv} \rangle$ ,  $\langle \text{Substantiv} \rangle$ ,  $\langle \text{Prädikat} \rangle$ ,  $\langle \text{Objekt} \rangle$ ,

### ■ Terminale

Der, Die, Das, kleine, süße, flinke, Eisbär, Elch, Kröte, Maus, Nilpferd, mag, fängt, isst, Kekse, Schokolade, Käsepizza

### ■ Beispiel 1

Dyck-Sprache $D_2$	
$\Sigma$	$\{(,),[],\}$
$L$	Menge der korrekt geklammerten Ausdrücke
$\in L$	$((), [()]), ()[()()], \dots$
$\notin L$	$(, [()]), (x), \dots$

### ■ Beispiel 2

Primzahlen	
$\Sigma$	$\{0, 1, 2, \dots, 9\}$
$L$	Menge der Ziffernfolgen, die einer Primzahl entsprechen
$\in L$	$2, 3, 5, 7, 11, 13, \dots$
$\notin L$	$1, 4, 6, 8, 9, 10, 12, \dots$

### ■ Beispiel 3

ABC-Sprache	
$\Sigma$	$\{a, b, c\}$
$L$	Menge aller geordneten Folgen aus $a$ 's, $b$ 's und $c$ 's
$\in L$	$abc, aabbc, aaaabbcc, \dots$
$\notin L$	$cba, ababc, abcba, \dots$

### ■ Beispiel 4

Palindromsprache	
$\Sigma$	$\{a, b, c, \dots, z\}$
$L$	Menge aller spiegelbildlich angeordneten Zeichenketten
$\in L$	$aabaa, reittier, anna, otto$
$\notin L$	$abab, aaba, abcab$

**Abbildung 4.3:** Beispiele formaler Sprachen

Beispiel 1	Beispiel 2
<p>&lt;Satz&gt;</p> <p>→ &lt;Subjekt&gt;&lt;Prädikat&gt;&lt;Objekt&gt;</p> <p>→ &lt;Subjekt&gt; fängt &lt;Objekt&gt;</p> <p>→ &lt;Subjekt&gt; fängt Kekse</p> <p>→ &lt;Artikel&gt;&lt;Adjektiv&gt;&lt;Substantiv&gt; fängt Kekse</p> <p>→ Das &lt;Adjektiv&gt;&lt;Substantiv&gt; fängt Kekse</p> <p>→ Das flinke &lt;Substantiv&gt; fängt Kekse</p> <p>→ Das flinke Nilpferd fängt Kekse</p>	<p>&lt;Satz&gt;</p> <p>→ &lt;Subjekt&gt;&lt;Prädikat&gt;&lt;Objekt&gt;</p> <p>→ &lt;Subjekt&gt; isst &lt;Objekt&gt;</p> <p>→ &lt;Subjekt&gt; isst Käsepizza</p> <p>→ &lt;Artikel&gt;&lt;Adjektiv&gt;&lt;Substantiv&gt; isst Käsepizza</p> <p>→ Die &lt;Adjektiv&gt;&lt;Substantiv&gt; isst Käsepizza</p> <p>→ Die kleine &lt;Substantiv&gt; isst Käsepizza</p> <p>→ Die kleine Maus isst Käsepizza</p>

**Tabelle 4.1:** Durch die sukzessive Anwendung der Produktionen einer Grammatik  $G$  lassen sich alle Wörter der Sprache  $\mathcal{L}(G)$  aus dem Startsymbol ableiten.

Dem Nonterminal <Satz> kommt in unserem Beispiel eine besondere Bedeutung zu. Es ist immer das erste Symbol, mit dem eine Ableitung beginnt, und wird folgerichtig als *Startsymbol* bezeichnet. Die Beispiele in Tabelle 4.1 zeigen, wie sich aus dem Startsymbol einige mehr oder weniger sinnvolle Sätze der deutschen Sprache ableiten lassen.

Mit der geleisteten Vorarbeit sind wir in der Lage, den Begriff der Grammatik formal zu definieren:



### Definition 4.2 (Grammatik)

Eine *Grammatik*  $G$  ist ein Viertupel  $(V, \Sigma, P, S)$ . Sie besteht aus

- der endlichen *Variablenmenge*  $V$  (*Nonterminale*),
- dem endlichen *Terminalalphabet*  $\Sigma$  mit  $V \cap \Sigma = \emptyset$ ,
- der endlichen Menge  $P$  von *Produktionen* (*Regeln*) und
- der *Startvariablen*  $S$  mit  $S \in V$ .

Jede Produktion aus  $P$  hat die Form  $l \rightarrow r$  mit  $l \in (V \cup \Sigma)^+$  und  $r \in (V \cup \Sigma)^*$ .

Durch die Menge der Produktionen definiert jede Grammatik eine Ableitungsrelation  $\Rightarrow$  auf der Menge  $(V \cup \Sigma)^*$ . Haben zwei Wörter  $x, y \in$

$(V \cup \Sigma)^*$  die Form  $x = lur$  und  $y = lvr$  mit  $l, r \in (V \cup \Sigma)^*$ , so gilt  $x \Rightarrow y$  genau dann, wenn die Grammatik eine Produktionsregel der Form  $u \rightarrow v$  enthält. Mit  $\Rightarrow^*$  bezeichnen wir die reflexiv transitive Hülle der Ableitungsrelation. Verbal ausgedrückt gilt  $x \Rightarrow^* y$  genau dann, wenn das Wort  $y$  dem Wort  $x$  entspricht oder sich in endlich vielen Schritten aus  $x$  ableiten lässt.

Jede Grammatik  $G$  erzeugt eine Sprache  $\mathcal{L}(G)$ . Diese definieren wir als die Menge der Wörter über dem Terminalalphabet  $\Sigma$ , die sich aus dem Startsymbol  $S$  ableiten lassen:

$$\mathcal{L}(G) := \{y \in \Sigma^* \mid S \Rightarrow^* y\} \quad (4.1)$$

Ein gezielter Blick auf Gleichung (4.1) zeigt, dass die Wörter der Sprache  $\mathcal{L}(G)$  ausschließlich aus Terminalsymbolen bestehen. Nonterminale spielen lediglich die Rolle von Platzhaltern, die nach und nach durch Symbole des Terminalalphabets oder durch weitere Nonterminale ersetzt werden. Erst wenn alle Nonterminale verschwunden sind, haben wir ein Wort der Sprache  $\mathcal{L}(G)$  erzeugt.

Als Beispiel betrachten wir die in Abbildung 4.4 dargestellte Grammatik zur Erzeugung der *Dyck-Sprache*  $D_2$ . Allgemein ist die Dyck-Sprache  $D_n$  als die Menge der wohlgeformten Wörter definiert, die aus  $n$  unterschiedlichen Klammerpaaren aufgebaut sind.

Ein Blick auf die Grammatik zeigt, dass die Menge der Nonterminale  $V = \{S\}$ , die Menge der Terminalzeichen  $\Sigma = \{(,), [, ]\}$  und das Startsymbol  $S$  unmittelbar aus den Ableitungsregeln hervorgehen. In Fällen wie diesem können wir uns daher ruhigen Gewissens auf die Angabe der Produktionen beschränken. Ferner vereinbaren wir eine abkürzende Schreibweise, die mehrere Produktionen mit der gleichen linken Seite zu einer einzigen Regel zusammenfasst. Im oberen Teil von Abbildung 4.5 ist das allgemeine Schema der Schreibweisenverkürzung abgebildet; der untere Teil zeigt, wie sich die Produktionen unserer Beispielgrammatik jetzt wesentlich kompakter formulieren lassen.

Am Beispiel des Dyck-Worts  $()()()$  wollen wir die Grammatik in Aktion erleben. Hierzu sind in Tabelle 4.2 drei Möglichkeiten dargestellt, wie sich das Wort aus dem Startsymbol  $S$  ableiten lässt.

- Die erste Ableitungssequenz (Tabelle 4.2 links) besitzt die Eigenschaft, dass in jedem Schritt das am weitesten links stehende Nonterminal ersetzt wurde. Eine solche Sequenz heißt *Linksableitung*.
- Die zweite Ableitungssequenz (Tabelle 4.2 Mitte) wurde so konstruiert, dass in jedem Schritt das am weitesten rechts stehende Nonterminal ersetzt wurde. Eine solche Sequenz heißt *Rechtsableitung*. In

■ Signatur

$$G = (\{S\}, \{(,), [, ]\}, P, S)$$

■ Produktionsmenge  $P$

$$\begin{aligned} S &\rightarrow \epsilon \\ S &\rightarrow SS \\ S &\rightarrow [S] \\ S &\rightarrow (S) \end{aligned}$$

**Abbildung 4.4:** Grammatik zur Erzeugung der Dyck-Sprache  $D_2$

■ Verkürzte Schreibweise

$$\begin{aligned} l &\rightarrow r_1 \\ &\dots \\ l &\rightarrow r_n \end{aligned}$$



$$l \rightarrow r_1 | \dots | r_n$$

■ Beispiel

$$\begin{aligned} S &\rightarrow \epsilon \\ S &\rightarrow SS \\ S &\rightarrow [S] \\ S &\rightarrow (S) \end{aligned}$$

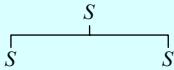
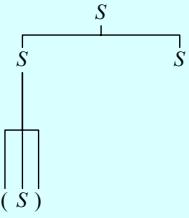
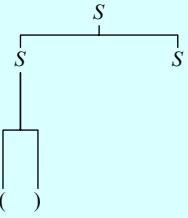
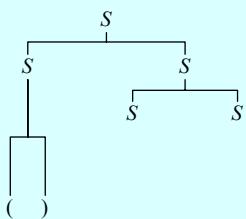
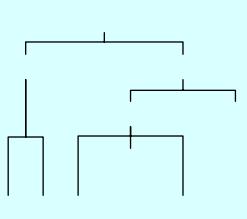
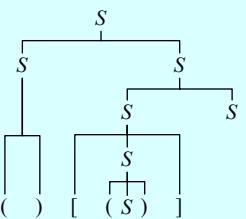
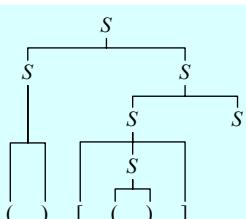
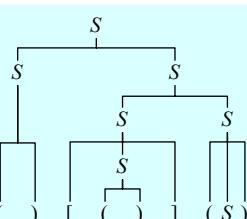
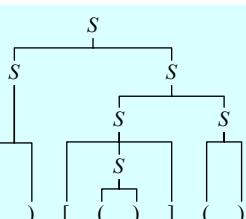


$$S \rightarrow \epsilon | SS | [S] | (S)$$

**Abbildung 4.5:** Zur Verkürzung der Schreibweise dürfen Produktionen mit gleicher linker Seite zu einer einzigen Regel zusammengefasst werden.

Ableitungssequenz 1	Ableitungssequenz 2	Ableitungssequenz 3
$\textcolor{teal}{S} \rightarrow \textcolor{teal}{SS}$ $\rightarrow (\textcolor{teal}{S})S$ $\rightarrow ()\textcolor{teal}{S}$ $\rightarrow ()\textcolor{teal}{SS}$ $\rightarrow ()[\textcolor{teal}{S}]S$ $\rightarrow ()[()\textcolor{teal}{S}]S$ $\rightarrow ()[()]\textcolor{teal}{S}$ $\rightarrow ()[()](\textcolor{teal}{S})$ $\rightarrow ()[()]( )$	$S \rightarrow S\textcolor{teal}{S}$ $\rightarrow S(\textcolor{teal}{S})$ $\rightarrow \textcolor{teal}{S}()$ $\rightarrow S[\textcolor{teal}{S}]()$ $\rightarrow S[()]\textcolor{teal}{S}$ $\rightarrow \textcolor{teal}{S}[()]( )$ $\rightarrow (\textcolor{teal}{S})[()]( )$ $\rightarrow ()[()\textcolor{teal}{S}]( )$ $\rightarrow ()[()](\textcolor{teal}{S})( )$ $\rightarrow ()[()]( )()$	$S \rightarrow \textcolor{teal}{SS}$ $\rightarrow \textcolor{teal}{S}SS$ $\rightarrow (\textcolor{teal}{S})SS$ $\rightarrow ()\textcolor{teal}{SS}$ $\rightarrow ()[S]S$ $\rightarrow ()[()]\textcolor{teal}{S}$ $\rightarrow ()[()](\textcolor{teal}{S})$ $\rightarrow ()[()]( )()$

**Tabelle 4.2:** Drei Ableitungssequenzen für das Wort  $()[()]( )$ 

$S \rightarrow SS$	$\rightarrow (S)S$	$\rightarrow ()S$
		
$\rightarrow ()SS$	$\rightarrow ()[S]S$	$\rightarrow ()[(S)]S$
		
$\rightarrow ()[()]S$	$\rightarrow ()[()](S)$	$\rightarrow ()[()]( )$
		

**Tabelle 4.3:** Schrittweise Konstruktion eines Syntaxbaums für das Dyck-Wort  $()[()]( )$

diesem Beispiel führt sowohl die Links- als auch die Rechtsableitung zu dem gleichen Wort  $()[()()$ . Andere Grammatiken erfüllen diese Eigenschaft nicht; dort führen die Links- und die Rechtsableitung zu unterschiedlichen Wörtern.

- Die dritte Ableitungssequenz (Tabelle 4.2 rechts) ist ebenfalls eine Linksableitung, da genau wie im ersten Beispiel in jedem Schritt das am weitesten links stehende Nonterminal ersetzt wird. Der Unterschied zwischen beiden Sequenzen besteht alleine in der Wahl der Produktionen, die auf das entsprechende Nonterminal angewendet werden. Das Beispiel unterstreicht, dass die Links- und die Rechtsableitung im Allgemeinen nicht eindeutig sind.

Jede Ableitungssequenz lässt sich in einen *Syntaxbaum* übersetzen. Dieser ist so angelegt, dass jeder innere Knoten einem Nonterminal aus der Ableitungssequenz entspricht und die Blätter aneinandergereiht das abgeleitete Wort ergeben. Für die Konstruktion des Syntaxbaums wird zunächst die Wurzel mit dem Startsymbol markiert. Anschließend werden die Blätter entsprechend den angewendeten Produktionen expandiert oder im Falle einer Regel der Form  $S \rightarrow \varepsilon$  aus dem Baum entfernt. Tabelle 4.3 zeigt die schrittweise Konstruktion des Syntaxbaums für die erste Ableitungssequenz aus Tabelle 4.2.

Erzeugen wir für jede der eingeführten Ableitungssequenzen einen Syntaxbaum, so erhalten wir die in Tabelle 4.4 dargestellten Ergebnisse. Ein Vergleich der beiden unteren Bäume zeigt, dass zwei verschiedene Ableitungen die gleiche Baumdarstellung ergeben können. Hierfür verantwortlich ist die Eigenschaft von Syntaxbäumen, von der Reihenfolge der angewendeten Regeln zu abstrahieren. Da aber umgekehrt jede Ableitungssequenz zu einem eindeutigen Syntaxbaum führt, müssen zwei strukturell unterschiedliche Syntaxbäume stets aus zwei verschiedenen Ableitungssequenzen entstanden sein.

Eine Grammatik  $G$  heißt *eindeutig*, wenn alle Ableitungen eines Worts  $\omega \in \mathcal{L}(G)$  immer zu demselben Syntaxbaum führen. Andernfalls bezeichnen wir  $G$  als *mehrdeutig*. Beachten Sie, dass die Mehrdeutigkeit die Eigenschaft einer Grammatik und nicht die Eigenschaft einer Sprache ist, da sich eine mehrdeutige Grammatik  $G$  häufig in eine eindeutige Grammatik  $G'$  mit  $\mathcal{L}(G) = \mathcal{L}(G')$  überführen lässt. Nichtsdestotrotz existieren Sprachen, die ausschließlich durch mehrdeutige Grammatiken erzeugt werden. Eine solche Sprache bezeichnen wir als *inhärent mehrdeutig*. Beachten Sie ferner, dass auch in eindeutigen Grammatiken mehrere verschiedene Ableitungen für ein Wort  $\omega$  existieren können. Das Kriterium der Eindeutigkeit stellt lediglich sicher, dass alle Ableitungen zu ein und demselben Syntaxbaum führen.

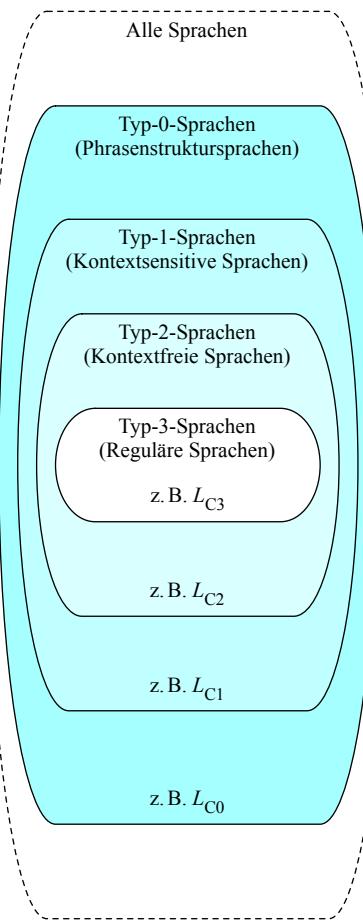
Ableitungssequenz 1
$S \rightarrow S\textcolor{red}{S}$
$\rightarrow S(\textcolor{red}{S})$
...

Ableitungssequenz 2
$S \rightarrow S\textcolor{red}{S}$
$\rightarrow S(\textcolor{red}{S})$
...

Ableitungssequenz 3
$S \rightarrow S\textcolor{red}{S}$
$\rightarrow SSS$
...

**Tabelle 4.4:** Syntaxbäume der drei Ableitungssequenzen aus Tabelle 4.2

## 4.2 Chomsky-Hierarchie



**Abbildung 4.6:** Die Chomsky-Hierarchie teilt die Menge der formalen Sprachen in vier verschiedene Typklassen ein. Eine Sprache  $L$  ist eine Typ- $n$ -Sprache, wenn eine Typ- $n$ -Grammatik existiert, die  $L$  erzeugt. Zwischen den vier Sprachklassen besteht eine echte Inklusionsbeziehung, d. h., für alle  $n$  mit  $0 \leq n < 3$  gilt  $\mathcal{L}_n \supset \mathcal{L}_{n+1}$  und  $\mathcal{L}_n \neq \mathcal{L}_{n+1}$ .

Formale Grammatiken sind ein mächtiges Werkzeug für die Erzeugung der unterschiedlichsten Sprachen. Die Spanne reicht von einelementigen Wortmengen bis hin zu komplexen Sprachgebilden, die in ihrer Natur dem gesprochenen Wort gleichen. Die Struktur der Produktionen einer Grammatik  $G$  hat dabei einen maßgeblichen Einfluss auf die Eigenschaften der erzeugten Sprache  $\mathcal{L}(G)$ . Im Jahre 1957 postulierte der amerikanische Sprachwissenschaftler Noam Chomsky ein Regelwerk, mit dessen Hilfe sich formale Grammatiken in vier Klassen einteilen lassen [17]:

### ■ Phrasenstrukturgrammatiken (Typ-0-Grammatiken)

Jede Grammatik ist per Definition immer auch eine Typ-0-Grammatik. Insbesondere unterliegt die Struktur der Produktionen keinen weiteren als den in Definition 4.2 vereinbarten Einschränkungen.

### ■ Kontextsensitive Grammatiken (Typ-1-Grammatiken)

Eine Grammatik heißt *kontextsensitiv*, falls für alle Produktionsregeln  $l \rightarrow r$  die Beziehung  $|r| \geq |l|$  gilt. In der Konsequenz kann die Anwendung einer Produktion niemals zu einer Verkürzung der abgeleiteten Zeichenkette führen.

### ■ Kontextfreie Grammatiken (Typ-2-Grammatiken)

Typ-2-Grammatiken sind dadurch charakterisiert, dass die linke Seite einer Produktionsregel ausschließlich aus einer einzigen Variablen besteht. Für alle Produktionen  $l \rightarrow r$  gilt also  $l \in V$ .

### ■ Reguläre Grammatiken (Typ-3-Grammatiken)

Reguläre Grammatiken sind kontextfrei und besitzen die zusätzliche Eigenschaft, dass die rechte Seite einer Produktion entweder aus dem leeren Wort  $\epsilon$  oder einem Terminalsymbol, gefolgt von einem Nonterminal, besteht. Formal gesprochen besitzt jede Produktion die Form  $l \rightarrow r$  mit  $l \in V$  und  $r \in \{\epsilon\} \cup \Sigma V$ .

Eine Sprache  $L$  bezeichnen wir als Typ- $n$ -Sprache, wenn eine Typ- $n$ -Grammatik  $G$  existiert, die  $L$  erzeugt. Die Menge aller Typ- $n$ -Sprachen notieren wir mit dem Symbol  $\mathcal{L}_n$ .

Zwischen den verschiedenen Sprachklassen besteht die folgende Inklusionsbeziehung:

$$\mathcal{L}_0 \supset \mathcal{L}_1 \supset \mathcal{L}_2 \supset \mathcal{L}_3 \quad (4.2)$$

Die Inklusionsbeziehung ist eine echte, d. h., es gibt zu jeder Klasse  $\mathcal{L}_n$  mit  $0 \leq n < 3$  eine Sprache  $L$ , die in  $\mathcal{L}_n$ , jedoch nicht in  $\mathcal{L}_{n+1}$  enthalten ist (vgl. Abbildung 4.6). Die folgenden Beispiele geben einen Eindruck über die vier Sprachklassen:

- $L_{C3} := \{(ab)^n \mid n \in \mathbb{N}\}$   
ist eine Typ-3-Sprache.
- $L_{C2} := \{a^n b^n \mid n \in \mathbb{N}\}$   
ist eine Typ-2-Sprache, aber keine Typ-3-Sprache.
- $L_{C1} := \{a^n b^n c^n \mid n \in \mathbb{N}\}$   
ist eine Typ-1-Sprache, aber keine Typ-2-Sprache.
- $L_{C0} := \{a^n \mid n \in \mathbb{N}\}$   
ist eine Typ-0-Sprache, aber keine Typ-1-Sprache.

Bei der Untersuchung der verschiedenen Sprachklassen spielen insbesondere die Abschlusseigenschaften eine wichtige Rolle. Hierunter verbirgt sich die Frage, ob die Verknüpfung zweier  $\mathcal{L}_n$ -Sprachen zu einer Sprache führt, die wiederum in der Sprachklasse  $\mathcal{L}_n$  liegt oder aus dieser herausfällt. Die folgenden Verknüpfungen sind in diesem Zusammenhang von Bedeutung:

- Vereinigung  
Ist mit  $L_1, L_2 \in \mathcal{L}_n$  auch die Sprache  $L_1 \cup L_2 \in \mathcal{L}_n$ ?
- Durchschnitt  
Ist mit  $L_1, L_2 \in \mathcal{L}_n$  auch die Sprache  $L_1 \cap L_2 \in \mathcal{L}_n$ ?
- Komplement  
Ist mit  $L \in \mathcal{L}_n$  auch die Sprache  $\Sigma^* \setminus L \in \mathcal{L}_n$ ?
- Konkatenation  
Ist mit  $L_1, L_2 \in \mathcal{L}_n$  auch die Sprache  $L_1 L_2 \in \mathcal{L}_n$ ?
- Kleene'sche Hülle  
Ist mit  $L \in \mathcal{L}_n$  auch die Sprache  $L^* \in \mathcal{L}_n$ ?

In den nächsten Abschnitten werden wir die charakteristischen Eigenschaften der eingeführten Sprachklassen im Detail herausarbeiten. Unter anderem werden wir im Rahmen unserer Untersuchungen aufzeigen, dass die Beispielsprachen  $L_{C0}$  bis  $L_{C3}$  tatsächlich in die angegebenen Sprachklassen fallen.

Chomskys Typ-0-Grammatiken sind eng mit den *Semi-Thue-Systemen* verwandt, die der norwegische Mathematiker Axel Thue im Jahre 1914 zur Untersuchung von Ableitungskalkülen ersann [89]. Formal ist ein Semi-Thue-System über einem Alphabet  $\Sigma$  nichts weiter als eine Relation  $S \subseteq \Sigma^* \times \Sigma^*$ . Die Elemente von  $S$  entsprechen den Produktionen einer Grammatik und werden genau wie diese in der Form  $u \rightarrow v$  notiert. Damit entpuppen sich Semi-Thue-Systeme als eine primitive Beschreibungsform für Grammatiken, die auf die nötigsten Bestandteile reduziert wurde.

Semi-Thue-Systeme und Grammatiken definieren eine Ableitungsrelation nach dem exakt gleichen Schema. Eine Zeichenkette der Form  $lur$  lässt sich in  $lvr$  umformen (geschrieben als  $lur \Rightarrow lvr$ ), wenn eine Produktion der Form  $u \rightarrow v$  existiert. Eine von Grammatiken bekannte Unterteilung in Terminale und Nonterminale existiert in Semi-Thue-Systemen nicht. Ebenfalls wird auf die Definition eines dedizierten Startsymbols verzichtet. Eine spezielle Variante sind Semi-Thue-Systeme mit einer symmetrischen Ableitungsrelation. Ist mit  $u \rightarrow v$  immer auch die Produktion  $v \rightarrow u$  enthalten, so sprechen wir von einem *Thue-System*.



Axel Thue  
(1863 – 1922)

■ Grammatik

$$G = (\{S\}, \{a, b\}, P, S)$$

■ Produktionsmenge  $P$

$$\begin{array}{lcl} S & \rightarrow & aB \\ B & \rightarrow & bC \\ C & \rightarrow & \epsilon \mid aB \end{array}$$

■ Sprache

$$\begin{aligned} \mathcal{L}(G) = \{ & ab \\ & abab \\ & ababab \\ & abababab, \dots \} \end{aligned}$$

**Abbildung 4.7:** Mit Hilfe einer regulären Grammatik lässt sich die formale Sprache  $L_{C3} = \{(ab)^n \mid n \geq 1\}$  erzeugen.

## 4.3 Reguläre Sprachen

Die Menge der regulären Sprachen (Typ-3-Sprachen) ist die kleinste Sprachklasse in der Chomsky-Hierarchie. Obwohl sie über eine vergleichsweise einfache Struktur verfügen, nehmen die Sprachen einen prominenten Platz in der Informatik ein. So sind viele Datenformate regulär und die Suchmuster, die uns z. B. auf der Shell-Ebene das Auffinden von Dateien erlauben, sind ebenfalls nichts anderes als reguläre Ausdrücke.

### 4.3.1 Definition und Eigenschaften

Wie in Abschnitt 4.2 dargelegt, unterliegen die Produktionen einer regulären Grammatik erheblichen Einschränkungen. Nur solche Regeln sind erlaubt, deren linke Seite aus einem Nonterminal und deren rechte Seite entweder aus dem leeren Wort  $\epsilon$  oder einem Terminalzeichen, gefolgt von einem Nonterminal, besteht.

Unter Beachtung dieser Einschränkungen lässt sich die Sprache

$$L_{C3} = \{(ab)^n \mid n \geq 1\} \quad (4.3)$$

mit der in Abbildung 4.7 dargestellten Grammatik erzeugen. Abbildung 4.8 demonstriert, wie sich die Wörter  $abab$  und  $ababab$  aus dem Startsymbol ableiten lassen. Ein Blick auf die Ableitungssequenzen entlarvt die Rolle des Nonterminals  $B$ . Es tritt immer dann auf, wenn zuletzt ein  $a$  erzeugt wurde, und stellt sicher, dass die Zeichenkette mit einem  $b$  fortgesetzt wird.

Die einfache Struktur der Produktionen einer regulären Grammatik wirkt sich unmittelbar auf das Erscheinungsbild der entstehenden Syntaxbäume aus. Da die rechte Seite einer Produktion aus maximal zwei Zeichen besteht und das erste immer aus der Menge der Terminalzeichen stammt, weisen die entstehenden Syntaxbäume die Struktur einer linearen Kette auf. Aufgrund dieser Eigenschaft werden reguläre Grammatiken auch als *rechtslineare Grammatiken* bezeichnet.

Die Linearitätseigenschaft sorgt dafür, dass Wörter in regulären Grammatiken immer nach dem gleichen Prinzip erzeugt werden. Ausgehend von dem leeren Wort in Form des Startsymbols fügt jede Produktion der Form  $A \rightarrow \sigma B$  das Zeichen  $\sigma$  an und ersetzt das aktuell vorhandene Nonterminal  $A$  durch das neue Symbol  $B$ . Hierdurch wird die erzeugte Zeichenkette mit jedem Ableitungsschritt um ein einzelnes Zeichen verlängert und nach rechts durch ein wechselndes Nonterminal begrenzt.

Dieses fungiert als Zustandsmerker und reglementiert die Anzahl der im nächsten Schritt anwendbaren Produktionen. Die Epsilon-Regeln der Form  $A \rightarrow \epsilon$  spielen ebenfalls eine entscheidende Rolle. Wird eine von ihnen angewendet, so verschwindet das Nonterminal aus der erzeugten Zeichenkette und der Produktionsprozess kommt zum Erliegen.

Für einige Anwendungsfälle ist es wünschenswert, möglichst viele Regeln der Form  $l \rightarrow \epsilon$  aus der Menge der Produktionen zu entfernen. In der Tat können wir auf die meisten Epsilon-Regeln verzichten, indem wir auch Produktionen zulassen, deren rechte Seiten aus einem einzigen Terminalzeichen bestehen.

In unserem Beispiel lässt sich die Epsilon-Regel  $C \rightarrow \epsilon$  eliminieren, indem die Grammatik durch die zusätzliche Regel  $B \rightarrow b$  erweitert wird. Wir erhalten das folgende Ergebnis:

$$\begin{array}{l} S \rightarrow aB \\ B \rightarrow b \\ B \rightarrow bC \\ C \rightarrow aB \end{array}$$

In der entstandenen Form besteht die rechte Seite einer Produktion nur noch aus einem isolierten Terminalzeichen oder einem Terminalzeichen, gefolgt von einem Nonterminal. Würden wir auf der rechten Seite mehr als ein Terminalzeichen zulassen, so ließe sich unsere Beispielgrammatik sogar noch weiter vereinfachen:

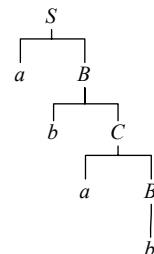
$$\begin{array}{l} S \rightarrow aB \\ B \rightarrow b \\ B \rightarrow baB \end{array}$$

Wir können die gezeigte Umformung auf beliebige Grammatiken anwenden und auf diese Weise fast alle Epsilon-Regeln nach und nach eliminieren. Die einzige Ausnahme bildet die Regel  $S \rightarrow \epsilon$ . Würden wir diese – falls vorhanden – aus der Menge der Produktionen entfernen, so ließe sich das leere Wort  $\epsilon$  nicht mehr ableiten.

In Abschnitt 4.1 haben wir mit dem Wortproblem, dem Leerheitsproblem, dem Endlichkeitsproblem und dem Äquivalenzproblem vier wichtige Fragestellungen für die Untersuchung formaler Sprachen eingeführt. Alle vier sind für reguläre Sprachen *entscheidbar*, d. h., es existiert ein Verfahren, das für alle Eingaben in feststellt, ob die betreffende Eigenschaft zutrifft oder nicht (vgl. Abbildung 4.9). Die Entscheidbarkeitseigenschaften wollen wir für den Moment ohne Beweis akzeptieren. In Abschnitt 5.4 wird uns deren Gültigkeit im Rahmen der Betrachtungen über endliche Automaten fast von selbst in den Schoß fallen.

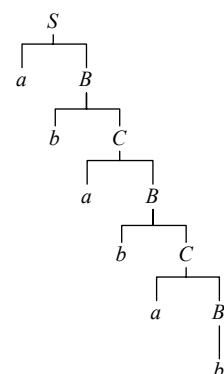
#### ■ Ableitung von $abab$

$$\begin{array}{l} S \rightarrow aB \\ \quad\quad\quad \rightarrow abC \\ \quad\quad\quad \rightarrow abaB \\ \quad\quad\quad \rightarrow ababC \\ \quad\quad\quad \rightarrow abab \end{array}$$



#### ■ Ableitung von $ababab$

$$\begin{array}{l} S \rightarrow aB \\ \quad\quad\quad \rightarrow abC \\ \quad\quad\quad \rightarrow abaB \\ \quad\quad\quad \rightarrow ababC \\ \quad\quad\quad \rightarrow ababaB \\ \quad\quad\quad \rightarrow abababC \\ \quad\quad\quad \rightarrow ababab \end{array}$$



**Abbildung 4.8:** Von regulären Grammatiken erzeugte Syntaxbäume besitzen die Struktur einer nach rechts unten geneigten linearen Kette.

■ Entscheidungsprobleme regulärer Sprachen

Problem	Eingabe	Fragestellung	Entscheidbar?
Wortproblem	Sprache $L$ , Wort $\omega \in \Sigma^*$	Ist $\omega \in L$ ?	✓ Ja
Leerheitsproblem	Sprache $L$	Ist $L = \emptyset$ ?	✓ Ja
Endlichkeitsproblem	Sprache $L$	Ist $ L  < \infty$ ?	✓ Ja
Äquivalenzproblem	Sprachen $L_1$ und $L_2$	Ist $L_1 = L_2$ ?	✓ Ja

■ Abschlusseigenschaften regulärer Sprachen

Operation	Eingabe	Fragestellung	Erfüllt?
Vereinigung	Sprache $L_1, L_2 \in \mathcal{L}_3$	Ist $L_1 \cup L_2 \in \mathcal{L}_3$ ?	✓ Ja
Schnitt	Sprache $L_1, L_2 \in \mathcal{L}_3$	Ist $L_1 \cap L_2 \in \mathcal{L}_3$ ?	✓ Ja
Komplement	Sprache $L \in \mathcal{L}_3$	Ist $\Sigma^* \setminus L \in \mathcal{L}_3$ ?	✓ Ja
Produkt	Sprache $L_1, L_2 \in \mathcal{L}_3$	Ist $L_1 L_2 \in \mathcal{L}_3$ ?	✓ Ja
Stern	Sprache $L \in \mathcal{L}_3$	Ist $L^* \in \mathcal{L}_3$ ?	✓ Ja

Abbildung 4.9: Eigenschaften regulärer Sprachen in der Übersicht

### 4.3.2 Pumping-Lemma für reguläre Sprachen

Wir wollen uns an dieser Stelle ein wenig näher an die Grenzen herantasten, die uns die eingeschränkte Struktur der Produktionen einer regulären Grammatik auferlegt. Weiter oben haben wir dargelegt, wie Wörter in regulären Grammatiken erzeugt werden. Sehen wir von der letzten Regelanwendung ab, so wird in jedem Ableitungsschritt ein Terminalzeichen und ein neues Nonterminal erzeugt. Das Nonterminal steht immer an letzter Stelle und begrenzt die Auswahl der im nächsten Schritt anwendbaren Regeln. In diesem Sinne wirkt es wie ein Zustandsspeicher, der einen Rückschluss auf die bisher erzeugten Zeichen erlaubt. Da die Menge der Nonterminale endlich ist, lassen sich während der Erzeugung eines Wortes nur endlich viele Zustände unterscheiden. Genau hierin liegt eine der grundlegenden Limitierungen regulärer Sprachen verborgen, die wir im Folgenden genauer untersuchen wollen.

Betrachten wir eine Ableitungssequenz, die mehr Ableitungsschritte enthält als Nonterminale zur Verfügung stehen, so muss mindestens ein

Nonterminal mehrfach auftauchen. Bezeichnen wir dieses Nonterminalzeichen mit  $A$ , so besitzt die Ableitungssequenz die folgende Form:

$$\begin{aligned} & \dots \\ \rightarrow & \underbrace{\sigma_1 \sigma_2 \dots \sigma_i}_{u} A \\ \rightarrow & \underbrace{\sigma_1 \sigma_2 \dots \sigma_i}_{u} \underbrace{\sigma_{i+1} \sigma_{i+2} \dots \sigma_j}_{v} A \\ \rightarrow & \underbrace{\sigma_1 \sigma_2 \dots \sigma_i}_{u} \underbrace{\sigma_{i+1} \sigma_{i+2} \dots \sigma_j}_{v} \underbrace{\sigma_{j+1} \sigma_{j+2} \dots \sigma_k}_{w} A \end{aligned}$$

Die Ableitungssequenz zeigt, dass es möglich ist, aus dem Nonterminal  $A$  die Zeichenkette

$$vA = \sigma_{i+1} \sigma_{i+2} \dots \sigma_j A \quad (4.4)$$

abzuleiten, die mindestens ein Terminalzeichen enthält ( $|v| \geq 1$ ). Da die erzeugte Sequenz erneut mit dem Nonterminal  $A$  endet, lassen sich zusätzlich die Sequenzen

$$v^2A = \sigma_{i+1} \sigma_{i+2} \dots \sigma_j \sigma_{i+1} \sigma_{i+2} \dots \sigma_j A \quad (4.5)$$

$$v^3A = \sigma_{i+1} \sigma_{i+2} \dots \sigma_j \sigma_{i+1} \sigma_{i+2} \dots \sigma_j \sigma_{i+1} \sigma_{i+2} \dots \sigma_j A \quad (4.6)$$

$\dots = \dots$

ableiten (vgl. Abbildung 4.10). Die angestellte Überlegung zeigt zwei-erlei: Zum einen lässt sich jedes hinreichend lange Wort einer regulären Sprache in der Form  $uvw$  ausdrücken. Zum anderen müssen neben dem Wort  $uvw$  auch die Wörter  $uv^i w$  für alle  $i \in \mathbb{N}_0$  in der Sprache enthalten sein. Genau dies ist die Kernaussage des *Pumping-Lemmas* für reguläre Sprachen.



### Satz 4.1 (Pumping-Lemma für reguläre Sprachen)

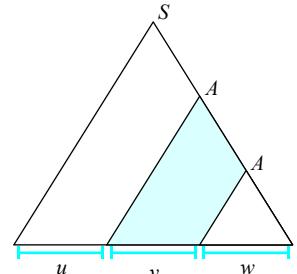
Für jede reguläre Sprache  $L$  existiert ein  $j \in \mathbb{N}$ , so dass sich alle Wörter  $\omega \in L$  mit  $|\omega| \geq j$  in der folgenden Form darstellen lassen:

$$\omega = uvw \quad \text{mit } |v| \geq 1 \text{ und } |uv| \leq j$$

Dann ist mit  $\omega$  auch das Wort  $uv^i w$  für alle  $i \in \mathbb{N}_0$  in  $L$  enthalten.

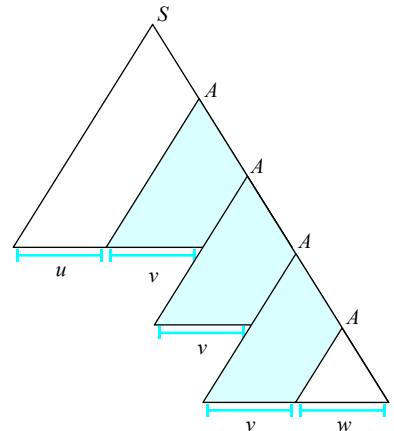
Das Pumping-Lemma gibt uns ein leistungsfähiges Instrument an die Hand, um eine Sprachen als nicht regulär zu entlarven. Die Beweisführung folgt dabei immer dem gleichen Muster. Zunächst wird für die

### Wortstruktur regulärer Sprachen



Überschreitet die Anzahl der Ableitungsschritte eines Worts eine gewisse Grenze  $j$ , so muss aufgrund der endlichen Anzahl der Nonterminale mindestens eines davon mehrfach im Syntaxbaum auftauchen (hier das Nonterminal  $A$ ). Folgerichtig lässt sich jedes hinreichend lange Wort in der Form  $uvw$  darstellen mit  $|v| \geq 1$  und  $|uv| \leq j$ .

### „Aufpumpen“ des Mittelstücks



Die Ableitung des Mittelstücks lässt sich beliebig oft wiederholen. Damit sind neben  $uvw$  immer auch die Wörter  $uv^i w$  für alle  $i \in \mathbb{N}_0$  in der Sprache enthalten.

**Abbildung 4.10:** Veranschaulichung des Pumping-Lemmas anhand der Syntaxbäume regulärer Grammatiken

Vergleichen wir die Sprache

$$L_{C2} := \{a^n b^n \mid n \in \mathbb{N}\}$$

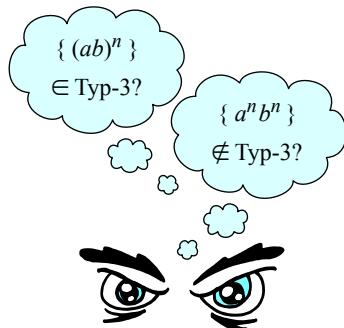
mit der weiter oben diskutierten Sprache

$$L_{C3} := \{(ab)^n \mid n \in \mathbb{N}\},$$

so erscheint der Unterschied auf den ersten Blick nur marginal zu sein. Trotzdem lässt sich  $L_{C2}$ , anders als  $L_{C3}$ , nicht mit Hilfe einer regulären Grammatik erzeugen.

Schuld daran ist die Anordnung der Symbole  $a$  und  $b$ . Erzeugen wir die einzelnen Zeichen eines Worts, wie in regulären Grammatiken gefordert, von links nach rechts, so müssen wir uns für alle Wörter der Form  $a^n b^n$  zunächst die Anzahl der produzierten  $a$ 's merken, um anschließend die richtige Anzahl von  $b$ 's hervorbringen zu können. Da der Wert von  $n$  nach oben unbeschränkt ist, wären zu diesem Zweck unendlich viele Zustände notwendig. Aufgrund der endlichen Anzahl an Nonterminalen – unseren Zustandsmerkern – ist dies ein unmögliches Unterfangen.

Um die Wörter der Sprache  $L_{C2}$  zu erzeugen, ist deutlich weniger logistische Arbeit erforderlich. Hier müssen wir uns lediglich merken, ob ein Terminalsymbol  $a$  erzeugt wurde oder nicht. Im ersten Fall müssen wir zunächst ein  $b$  produzieren, um ein gültiges Wort zu erhalten. Im zweiten Fall haben wir bereits ein korrektes Wort der Sprache vor uns.



untersuchte Sprache  $L$  gezeigt, dass sich ein Wort  $\omega \in L$  in der Form  $uvw$  darstellen lässt. Dem Pumping-Lemma folgend muss dann auch das Wort  $uv^i w$  in der Sprache enthalten sein. Ist dies nicht der Fall, so kann  $L$  keine reguläre Sprache sein.

Mit Hilfe des Pumping-Lemmas können wir z. B. beweisen, dass die in Abschnitt 4.2 eingeführte Sprache

$$L_{C2} := \{a^n b^n \mid n \in \mathbb{N}\} \quad (4.7)$$

nicht regulär ist. Wäre  $L_{C2}$  eine reguläre Sprache, so würde nach dem Pumping-Lemma ein  $j \in \mathbb{N}$  existieren, so dass sich jedes Wort  $\omega$  mit  $|\omega| \geq j$  in der Form  $uvw$  darstellen lässt mit  $|v| \geq 1$  und  $|uv| \leq j$ . Für das Wort  $a^j b^j$  folgt hieraus, dass der (nichtleere) Mittelteil  $v$  nur aus  $a$ 's bestehen kann. Mit  $uvw$  wäre dann aber auch das Wort

$$uv^2w = a^j a^{|v|} b^j = a^j \underbrace{a \dots a}_{\geq 1} b^j \quad (4.8)$$

in  $L$  enthalten, im Widerspruch zum Aufbau von  $L_{C2}$ .

Beachten Sie an dieser Stelle, dass uns das Pumping-Lemma ein Hilfsmittel an die Hand gibt, um nachzuweisen, dass eine Sprache  $L$  *nicht* regulär ist. Insbesondere darf die Schlussrichtung von Satz 4.1 nicht umgekehrt werden. Auch wenn die Wörter einer Sprache alle Eigenschaften des Pumping-Lemmas erfüllen, ist diese nicht notwendigerweise regulär.

### 4.3.3 Reguläre Ausdrücke

Reguläre Sprachen lassen sich elegant mit Hilfe *regulärer Ausdrücke* beschreiben. Formal sind diese wie folgt definiert:



#### Definition 4.3 (Syntax regulärer Ausdrücke)

Mit  $\Sigma$  sei ein beliebiges Alphabet gegeben.  $Reg_\Sigma$ , die Menge der *regulären Ausdrücke* über  $\Sigma$ , wird induktiv durch die folgenden Regeln gebildet:

- $\emptyset, \epsilon \in Reg_\Sigma$
- $\Sigma \subset Reg_\Sigma$
- Mit  $r \in Reg_\Sigma$  und  $s \in Reg_\Sigma$  sind auch  $rs$  und  $(r \mid s) \in Reg_\Sigma$
- Mit  $r \in Reg_\Sigma$  sind auch  $(r)$  und  $r^* \in Reg_\Sigma$



#### Definition 4.4 (Semantik regulärer Ausdrücke)

Sei  $r$  ein regulärer Ausdruck über dem Alphabet  $\Sigma$ . Die von  $r$  erzeugte Sprache  $\mathcal{L}(r)$  ist induktiv definiert:

$$\begin{aligned}\mathcal{L}(\emptyset) &= \emptyset \\ \mathcal{L}(\varepsilon) &= \{\varepsilon\} \\ \mathcal{L}(a \in \Sigma) &= \{a\} \\ \mathcal{L}(rs) &= \mathcal{L}(r)\mathcal{L}(s) \\ \mathcal{L}((r \mid s)) &= \mathcal{L}(r) \cup \mathcal{L}(s) \\ \mathcal{L}((r)) &= \mathcal{L}(r) \\ \mathcal{L}(r^*) &= \mathcal{L}(r)^*\end{aligned}$$

Für reguläre Ausdrücke gelten die in Tabelle 4.5 zusammengefassten Rechenregeln.

Die Beispiele in Abbildung 4.11 demonstrieren, wie sich Sprachen mit Hilfe von regulären Ausdrücken beschreiben lassen. Dass wir zu jeder der angegebenen Grammatiken einen regulären Ausdruck finden konnten, der die gleiche Sprache erzeugt, ist bei weitem kein Zufall. In der Tat lässt sich zeigen, dass zu jeder Grammatik ein äquivalenter regulärer Ausdruck existiert und umgekehrt. Zwischen regulären Grammatiken und regulären Ausdrücken besteht somit nur ein äußerlicher Unterschied; beide erzeugen dieselbe Sprachklasse  $\mathcal{L}_3$ . In Kapitel 5 wird dieser elementare Zusammenhang in ein helleres Licht gerückt werden. Dort werden wir den Begriff des endlichen Automaten einführen und zeigen, wie sich reguläre Grammatiken und reguläre Ausdrücke eins zu eins auf den Automatenbegriff reduzieren lassen.

Reguläre Ausdrücke besitzen eine große Bedeutung in der praktischen Informatik. Sie werden von vielen Kommandozeilenwerkzeugen z. B. für die Spezifikation von Suchmustern verwendet und sind damit insbesondere den Benutzern UNIX-ähnlicher Betriebssysteme wohlvertraut. Tabelle 4.6 gibt eine Übersicht über die Syntax, in der reguläre Ausdrücke von typischen UNIX-Werkzeugen wie Grep oder Sed verstanden werden [56]. Die Syntax orientiert sich im Kern an jener aus Definition 4.3, – insbesondere sind die Konkatenation ( $ab$ ), die Auswahl ( $a|b$ ) und der Kleene-Stern ( $^*$ ) nahezu unverändert vorhanden. Darüber hinaus werden weitere Konstrukte unterstützt, die zu keiner Erweiterung der beschreibbaren Sprachen führen. Die zusätzlichen Syntaxelemente dienen lediglich zur Verkürzung der Schreibweise und lassen sich auf die Kernkonstrukte zurückführen.

Kommutativgesetz
$r \mid s = s \mid r$
Idempotenzgesetz
$r \mid r = r$
Distributivgesetze
$r(s \mid t) = rs \mid rt$ $(s \mid t)r = sr \mid tr$
Neutrale Elemente
$r \mid \emptyset = \emptyset \mid r = r$ $r\varepsilon = \varepsilon r = r$

**Tabelle 4.5:** Rechenregeln für reguläre Ausdrücke

■  $L_1 := \{(ab)^n \mid n \in \mathbb{N}\}$

$$\begin{array}{lcl} S & \rightarrow & aB \\ B & \rightarrow & bC \\ C & \rightarrow & \varepsilon \mid ab \end{array}$$



$$ab(ab)^*$$

■  $L_2 := \{a^i b^j d^k \mid i, j, k \in \mathbb{N}\}$

$$\begin{array}{lcl} S & \rightarrow & aS \mid aB \\ B & \rightarrow & bB \mid bC \\ C & \rightarrow & cC \mid c \end{array}$$



$$aa^*bb^*cc^*$$

**Abbildung 4.11:** Reguläre Grammatiken und reguläre Ausdrücke erzeugen die gleiche Sprachklasse  $\mathcal{L}_3$ .

Zeichen	
.	Beliebiges Zeichen außer dem Zeilenumbruch
[...]	Positivliste (jedes Zeichen innerhalb der spezifizierten Liste)
[^...]	Negativliste (jedes Zeichen außerhalb der spezifizierten Liste)
[w]	Klein- oder Großbuchstabe, Unterstrich
[W]	Ziffer, Sonderzeichen, Leerraum
[s]	Leerraum (Whitespace, Tabulator, Carriage return)
[S]	Beliebiges Zeichen außer dem Leerraum
Positionen	
^	Beginn einer Zeile
\$	Ende einer Zeile
<	Beginn eines Worts
>	Ende eines Worts
Kombinationen	
+	Der vorangegangene Ausdruck kommt mindestens einmal vor
?	Der vorangegangene Ausdruck kommt höchstens einmal vor
*	Der vorangegangene Ausdruck kommt gar nicht oder beliebig oft vor
{n,}	Der vorangegangene Ausdruck kommt mindestens $n$ -mal vor
{n,m}	Der vorangegangene Ausdruck kommt mindestens $n$ -mal, aber höchstens $m$ -mal vor
{,m}	Der vorangegangene Ausdruck kommt höchstens $m$ -mal vor
	Alternative (entweder der linke oder der rechte Ausdruck)
()	Gruppierung
Häufig benötigte Zeichen- und Symbolmengen	
[:blank:]	Leerzeichen oder Tabulator
[:space:]	Leerzeichen, Tabulator, newline, form feed, carriage return
[:cntrl:]	Steuerzeichen
[:lower:]	Kleinbuchstabe
[:upper:]	Großbuchstabe
[:alpha:]	Buchstabe ([:lower:] oder [:upper:])
[:digit:]	Ziffer
[:xdigit:]	Hexadezimalziffer
[:alnum:]	Alphanumerisches Zeichen ([:alpha:] oder [:digit:])
[:punct:]	Punktierungszeichen
[:graph:]	Grafisches Zeichen ([:alpha:] oder [:punct:])
[:print:]	Darstellbares Zeichen ([:alnum:] oder [:punct:])

**Tabelle 4.6:** Kommandozeilenwerkzeuge wie Grep oder Sed verwenden reguläre Ausdrücke für die Angabe von Suchmustern.

## 4.4 Kontextfreie Sprachen

### 4.4.1 Definition und Eigenschaften

*Kontextfreie Grammatiken* sind eine Erweiterung der regulären Grammatiken. In beiden sind die Produktionen so gestaltet, dass auf der linken Seite nur ein einzelnes Nonterminal stehen darf. Im Gegensatz zu regulären Grammatiken, die auch die Form der rechten Seite restriktieren, kann diese in kontextfreien Grammatiken aus einer beliebigen Sequenz von Terminal- und Nonterminalzeichen bestehen. Mit anderen Worten: Eine Grammatik ist genau dann kontextfrei, wenn jede Produktion die Form  $l \rightarrow r$  mit  $l \in V$  und  $r \in (\Sigma \cup V)^*$  besitzt.

In Abschnitt 4.3 haben wir mit dem Pumping-Lemma gezeigt, dass die Sprache  $\{a^n b^n \mid n \in \mathbb{N}\}$  nicht regulär ist und damit von keiner regulären Grammatik erzeugt werden kann. Kontextfreie Sprachen sind hingegen ausdrucksstark genug, um die Sprache zu beschreiben. Abbildung 4.12 fasst die entsprechenden Produktionsregeln zusammen.

Als weiteres Beispiel zeigt Abbildung 4.13 eine Grammatik zur Erzeugung der Sprache  $\{a^i b^j a^k \mid i \in \mathbb{N}, j, k \in \mathbb{N}_0\}$ . Auch diese ist kontextfrei, da die linken Seiten der Produktionen nur aus Variablen bestehen.

### 4.4.2 Normalformen

Die Produktionen kontextfreier Grammatiken lassen sich durch geschickte Umformung stark vereinfachen. Was wir hierunter genau zu verstehen haben, werden die nächsten beiden Abschnitte zeigen. Zunächst werden wir in Abschnitt 4.4.2.1 den Begriff der *Chomsky-Normalform* einführen und darlegen, wie sich eine kontextfreie Grammatik äquivalenterhaltend in eine solche überführen lässt. Anschließend werden wir in Abschnitt 4.4.2.2 zeigen, wie sich kontextfreie Grammatiken mit Hilfe der *Backus-Naur-Form* beschreiben lassen.

#### 4.4.2.1 Chomsky-Normalform



##### Definition 4.5 (Chomsky-Normalform)

Eine Grammatik  $G$  liegt in *Chomsky-Normalform* vor, wenn alle Produktionen die Form  $A \rightarrow \sigma$  oder  $A \rightarrow BC$  besitzen mit  $A, B, C \in V$  und  $\sigma \in \Sigma$ .

#### ■ Grammatik

$$G := (\{S\}, \{a, b\}, P, S)$$

#### ■ Produktionsmenge $P$

$$S \rightarrow aSb \mid ab$$

#### ■ Ableitung des Worts $aaaabbbb$

$$\begin{aligned} S &\rightarrow aSb \\ &\rightarrow aaSbb \\ &\rightarrow aaaSbbb \\ &\rightarrow aaaabbbb \end{aligned}$$

Abbildung 4.12: Grammatik zur Erzeugung der Sprache  $\{a^n b^n \mid n \in \mathbb{N}\}$

#### ■ Grammatik

$$G := (\{S, A, B\}, \{a, b\}, P, S)$$

#### ■ Produktionsmenge $P$

$$\begin{aligned} S &\rightarrow AB \mid ABA \\ A &\rightarrow aA \mid a \\ B &\rightarrow Bb \mid \epsilon \end{aligned}$$

#### ■ Ableitung des Worts $aabbaa$

$$\begin{aligned} S &\rightarrow ABA \\ &\rightarrow aABA \\ &\rightarrow aaBA \\ &\rightarrow aaBbA \\ &\rightarrow aaBbbA \\ &\rightarrow aabbA \\ &\rightarrow aabbaA \\ &\rightarrow aabbaaa \end{aligned}$$

Abbildung 4.13: Grammatik zur Erzeugung der Sprache  $\{a^i b^j a^k \mid i \in \mathbb{N}, j, k \in \mathbb{N}_0\}$

Ausgangspunkt	Schritt 1	Schritt 2	Schritt 3	Schritt 4
$S \rightarrow AB$	$S \rightarrow AB$	$S \rightarrow AB$	$S \rightarrow AB$	$S \rightarrow AB$
$S \rightarrow ABA$	$S \rightarrow A$	$S \rightarrow aA$	$S \rightarrow V_a A$	$S \rightarrow V_a A$
$A \rightarrow aA$	$S \rightarrow ABA$	$S \rightarrow a$	$S \rightarrow a$	$S \rightarrow a$
$A \rightarrow a$	$S \rightarrow AA$	$S \rightarrow ABA$	$S \rightarrow ABA$	$S \rightarrow S_2 A$
$B \rightarrow Bb$	$A \rightarrow aA$	$S \rightarrow AA$	$S \rightarrow AA$	$S_2 \rightarrow AB$
$B \rightarrow \epsilon$	$A \rightarrow a$	$A \rightarrow aA$	$A \rightarrow V_a A$	$S \rightarrow AA$
	$B \rightarrow Bb$	$A \rightarrow a$	$A \rightarrow a$	$A \rightarrow V_a A$
	$B \rightarrow b$	$B \rightarrow Bb$	$B \rightarrow BV_b$	$A \rightarrow a$
		$B \rightarrow b$	$B \rightarrow b$	$B \rightarrow BV_b$
			$V_a \rightarrow a$	$B \rightarrow b$
			$V_b \rightarrow b$	$V_a \rightarrow a$
				$V_b \rightarrow b$

Tabelle 4.7: Schrittweise Erzeugung der Chomsky-Normalform

Um eine kontextfreie Grammatik  $G$  mit  $\epsilon \notin \mathcal{L}(G)$  in die Chomsky-Normalform zu überführen, sind vier Schritte zu absolvieren. In Tabelle 4.7 werden diese für das Beispiel aus Abbildung 4.13 durchlaufen.

#### ■ Schritt 1: Elimination der $\epsilon$ -Regeln

Alle Regeln der Form  $A \rightarrow \epsilon$  werden eliminiert, indem die Ersetzung von  $A$  durch  $\epsilon$  in allen anderen Regel vorweggenommen wird. Da  $\epsilon \notin \mathcal{L}(G)$  ist, wird das leere Wort hierdurch vollständig aus den Produktionen entfernt.

#### ■ Schritt 2: Elimination von Kettenregeln

Jede Produktion der Form  $A \rightarrow B$  mit  $A, B \in V$  wird als *Kettenregel* bezeichnet. Diese tragen nicht zur Produktion von Terminalzeichen bei und lassen sich ebenfalls eliminieren. Hierzu gehen wir wie in Schritt 1 vor und nehmen die Ersetzung der rechten Seite vorweg.

#### ■ Schritt 3: Separation von Terminalzeichen

Jedes Terminalzeichen  $\sigma$ , das in Kombination mit anderen Symbolen auftaucht, wird durch ein neues Nonterminal  $V_\sigma$  ersetzt und die Menge der Produktionen durch die Regel  $V_\sigma \rightarrow \sigma$  ergänzt.

#### ■ Schritt 4: Elimination von mehrelementigen Nonterminalketten

Alle Produktionen der Form  $A \rightarrow B_1 B_2 \dots B_n$  werden in die Produktionen  $A \rightarrow A_{n-1} B_n, A_{n-1} \rightarrow A_{n-2} B_{n-1}, \dots, A_2 \rightarrow B_1 B_2$  zerteilt. Nach der Ersetzung sind alle längeren Nonterminalketten vollständig heruntergebrochen und die Chomsky-Normalform erreicht.

Die spezielle Struktur einer Grammatik in Chomsky-Normalform wirkt sich unmittelbar auf das Erscheinungsbild der entstehenden Syntaxbäume aus. Da jedes Nonterminal entweder durch ein Terminalzeichen oder durch zwei weitere Nonterminale ersetzt wird, entsteht im Innern die Struktur eines Binärbaums. Wie wir in Abschnitt 2.4.2 herausgearbeitet haben, besteht in diesen Bäumen ein enger Zusammenhang zwischen ihrer Tiefe und der Anzahl der Blätter. Ist ein Binärbaum  $B$  *vollständig*, d. h., besitzen alle Blätter die gleiche Tiefe  $h$ , so besitzt der Baum exakt  $2^h$  Blätter. Ist der Binärbaum nicht vollständig, so gilt offensichtlich die Beziehung  $|B| < 2^h$ .

Abbildung 4.14 stellt die entstehenden Syntaxbäume gegenüber, die für das Wort *aabbaa* aus der Originalgrammatik (Tabelle 4.7 links) und der generierten Chomsky-Normalform (Tabelle 4.7 rechts) entstehen.

#### 4.4.2.2 Backus-Naur-Form

Kontextfreie Sprachen sind ausdrucksstark genug, um die Syntax der meisten Programmiersprachen zu beschreiben. Bereits Anfang der Sechzigerjahre verwendete der amerikanische Computerpionier John Backus eine kontextfreie Grammatik, um die Syntax der Programmiersprache Algol60 formal zu spezifizieren. Die von Backus eingeführte Notation wird heute als *Backus-Naur-Form* bezeichnet und hat sich zum De-facto-Standard für die Beschreibung von Programmiersprachen entwickelt.

Auf den ersten Blick unterscheidet sich die Backus-Naur-Form von der Produktionssyntax dieses Buches vor allem in der Verwendung des Ableitungssymbols  $::=$  anstelle von  $\rightarrow$ . Darüber hinaus führte Backus einige Spezialkonstrukte ein, mit denen sich die Produktionen kontextfreier Grammatiken übersichtlich beschreiben lassen. Hierzu gehört unter anderem die weiter oben eingeführte Strichnotation, um Produktionen mit gleicher linker Seite zu einer einzigen Regel zusammenzufassen.

In der *erweiterten Backus-Naur-Form* können Wortfragmente zusätzlich in eckige und geschweifte Klammerpaare eingeschlossen werden. So besagt der Ausdruck

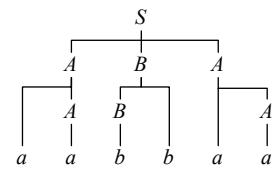
$$A ::= r_1[r_2]r_3, \quad (4.9)$$

dass zwischen  $r_1$  und  $r_3$  optional das Wort  $r_2$  eingefügt werden darf. Der Ausdruck

$$A ::= r_1\{r_2\}r_3 \quad (4.10)$$

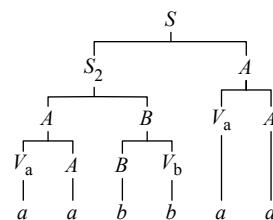
#### ■ Originalgrammatik

$$\begin{aligned} S &\rightarrow ABA \\ &\rightarrow aABA \\ &\rightarrow aaBA \\ &\rightarrow aaBbA \\ &\rightarrow aaBbbA \\ &\rightarrow aabbA \\ &\rightarrow aabbaA \\ &\rightarrow aabbaa \end{aligned}$$



#### ■ Chomsky-Normalform

$$\begin{aligned} S &\rightarrow S_2 A \\ &\rightarrow ABA \\ &\rightarrow V_a ABA \\ &\rightarrow aABA \\ &\rightarrow aaBA \\ &\rightarrow aaBV_b A \\ &\rightarrow aabV_b A \\ &\rightarrow aabbA \\ &\rightarrow aabbV_a A \\ &\rightarrow aabbaA \\ &\rightarrow aabbaa \end{aligned}$$



**Abbildung 4.14:** Die Syntaxbäume von Grammatiken in Chomsky-Normalform haben die Form von Binärbäumen.

■ Auswahl

$$A ::= r_1 \mid \dots \mid r_n$$



$$A \rightarrow r_1$$

...

$$A \rightarrow r_n$$

bedeutet hingegen, dass sich das optionale Wortfragment  $r_2$  beliebig oft wiederholen kann. Keines der Konstrukte führt zu einer Erweiterung der Ausdrucksstärke; beide lassen sich, wie in Abbildung 4.15 gezeigt, auf eine gewöhnliche Produktionenmenge zurückführen. Insgesamt handelt es sich bei der Backus-Naur-Form um eine alternative Beschreibungsform für kontextfreie Grammatiken, die sich lediglich im Aussehen, nicht aber in der Ausdrucksstärke von der bisher verwendeten Notation unterscheidet.

■ Optionales Argument

$$A ::= r_1 [r_2] r_3$$



$$A \rightarrow r_1 r_3$$

$$A \rightarrow r_1 r_2 r_3$$

■ Wiederholung

$$A ::= r_1 \{ r_2 \} r_3$$



$$A \rightarrow r_1 B r_3$$

$$B \rightarrow Br_2$$

$$B \rightarrow \epsilon$$

**Abbildung 4.15:** Reduktion der Backus-Naur-Form auf gewöhnliche Produktionen.

### 4.4.3 Pumping-Lemma für kontextfreie Sprachen

Für die Klasse der regulären Sprachen haben wir mit dem Pumping-Lemma ein wertvolles Instrument erhalten, um die Nichtregularität vieler Sprachen zu zeigen. Ein ähnliches Lemma lässt sich auch für die Klasse der kontextfreien Sprachen herleiten.

Für die folgenden Betrachtungen nehmen wir an, dass eine beliebige Grammatik  $G = (V, \Sigma, P, S)$  in Chomsky-Normalform gegeben ist. Wir setzen  $j := 2^{|V|}$  und wählen ein beliebiges Wort  $\omega \in \mathcal{L}(G)$  mit  $|\omega| \geq j$ . Da  $G$  in Chomsky-Normalform gegeben ist, besitzt der zugehörige Syntaxbaum im Innern die Form eines Binärbaums mit mindestens  $2^{|V|}$  Blättern. Für diesen Baum garantiert uns der auf Seite 68 bewiesene Satz 2.4, dass wir einen Pfad auswählen können, der mindestens die Länge  $|V|$  besitzt. Zusammen mit dem Startsymbol finden wir auf dem gewählten Pfad mindestens  $|V| + 1$  Nonterminale wieder, so dass eines davon mehrfach auftauchen muss. Bezeichnen wir dieses Nonterminal mit  $A$ , so lässt sich der Syntaxbaum in einer Form darstellen, wie sie im oberen Teil von Abbildung 4.17 skizziert ist. Insgesamt erhalten wir eine Zerlegung des abgeleiteten Wortes in fünf Segmente.

Da  $G$  in Chomsky-Normalform vorliegt, kann aus  $A$  nur dann ein weiteres  $A$  erzeugt werden, wenn mindestens ein Ableitungsschritt der Form  $A \rightarrow BC$  durchlaufen wurde. Damit muss mindestens eines der Segmente  $v$  oder  $x$  ein Zeichen enthalten, d. h., es gilt die Beziehung:  $|vx| \geq 1$ .

Über die Mindestlänge der Segmente  $u$  und  $y$  können wir keine Aussage machen; beide können zum leeren Wort degenerieren. Dafür sind wir in der Lage, die Länge der Sequenz  $vwx$  nach oben abzuschätzen. Hierzu nehmen wir ohne Beschränkung der Allgemeinheit an, dass die zwei

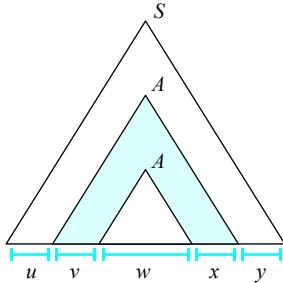
Algol-Grammatik (Auszug)	
<program>	::= <block>   <compound statement>
<block>	::= <unlabelled block>   <label>: <block>
<unlabelled block>	::= <block head> ; <compound tail>
<block head>	::= 'BEGIN' <declaration>   <block head> ; <declaration>
<compound statement>	::= <unlabelled compound>   <label>: <compound statement>
<unlabelled compound>	::= 'BEGIN' <compound tail>
<compound tail>	::= <statement> 'END'   <statement> ; <compound tail>
<declaration>	::= <type declaration>   <array declaration>   <switch declaration>   <procedure declaration>
<type declaration>	::= <local or own type> <type list>
<local or own type>	::= <type>   'OWN' <type>
<type>	::= 'REAL'   'INTEGER'   'BOOLEAN'
<type list>	::= <simple variable>   <simple variable> , <type list>
<array declaration>	::= 'ARRAY' <array list>   <local or own type> 'ARRAY' <array list>
<array list>	::= <array segment>   <array list> , <array segment>
<array segment>	::= <array identifier> [ <bound pair list> ]   <array identifier> , <array segment>
<array identifier>	::= <identifier>
<bound pair list>	::= <bound pair>   <bound pair list> , <bound pair>
<bound pair>	::= <lower bound> : <upper bound>
<upper bound>	::= <arithmetic expression>
<lower bound>	::= <arithmetic expression>

**Abbildung 4.16:** Auszug aus der Algol60-Syntax, niedergeschrieben in Backus-Naur-Form

Vorkommen der Nonterminale  $A$  in Abbildung 4.17 (oben) so gewählt wurden, dass alle weiteren Vorkommen von  $A$ , falls diese überhaupt existieren, näher an der Wurzel liegen und alle anderen Nonterminale, die näher an den Blättern liegen, paarweise verschieden sind. Hierdurch ist das obere ausgewählte  $A$  maximal  $|V|$  Schritte von den Blättern entfernt und der aufgespannte Syntaxbaum kann höchstens  $2^{|V|} = j$  Blätter enthalten. Damit gilt die Beziehung  $|vwx| \leq j$ .

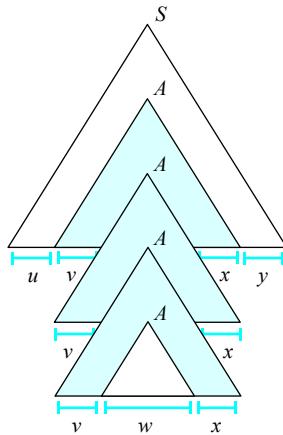
Genau wie im Falle des Pumping-Lemmas für reguläre Sprachen erlaubt uns das Doppelvorkommen von  $A$ , das ableitbare Wort „aufzupumpen“, indem wir die Ableitungssequenz von  $A$  nach  $A$  wiederholen. Hierdurch können wir die Worte  $uv^2wx^2y$ ,  $uv^3wx^3y$ , ... produzieren und eine entsprechende Überlegung zeigt, dass auch das Wort  $uv^0wx^0y$  ableitbar ist (vgl. Abbildung 4.17 unten). Fassen wir die erarbeiteten Ergebnisse zusammen, so erhalten wir in direkter Weise das Pumping-Lemma für kontextfreie Sprachen:

■ Wortstruktur kontextfreier Sprachen



Überschreitet die Anzahl der Ableitungsschritte eines Worts eine gewisse Grenze  $j$ , so muss aufgrund der endlichen Anzahl der Nonterminale mindestens eines davon mehrfach im Syntaxbaum auftauchen (hier das Nonterminal  $A$ ). Hierdurch lässt sich jedes hinreichend lange Wort in der Form  $uvwxy$  darstellen mit  $|vx| \geq 1$  und  $|vwx| \leq j$ .

■ „Aufpumpen“ des Mittelstücks



Die Ableitung des Mittelstücks lässt sich beliebig oft wiederholen. Neben  $uvwxy$  sind somit auch die Wörter  $uv^iwx^i y$  für alle  $i \in \mathbb{N}_0$  in der Sprache enthalten.

**Abbildung 4.17:** Veranschaulichung des Pumping-Lemmas anhand der Syntaxbäume kontextfreier Grammatiken.



**Satz 4.2 (Pumping-Lemma für kontextfreie Sprachen)**

Für jede kontextfreie Sprache  $L$  existiert ein  $j \in \mathbb{N}$ , so dass sich alle Wörter  $\omega \in L$  mit  $|\omega| \geq j$  in der folgenden Form darstellen lassen:

$$\omega = uvwxy \quad \text{mit } |vx| \geq 1 \text{ und } |vwx| \leq j$$

Ferner ist mit  $\omega$  auch das Wort  $uv^iwx^i y$  für alle  $i \in \mathbb{N}_0$  in  $L$  enthalten.

Das Pumping-Lemma versetzt uns in die Lage, die Sprache  $L_{C1} = \{a^n b^n c^n \mid n \in \mathbb{N}\}$  als nicht kontextfrei zu entlarven. Für den Beweis nehmen wir an,  $L_{C1}$  sei kontextfrei. Dann garantiert uns das Pumping-Lemma, dass ein  $j \in \mathbb{N}$  existiert, so dass sich jedes Wort  $\omega = a^i b^i c^i$  mit  $|\omega| \geq j$  in der Form  $uvwxy$  darstellen lässt mit  $|vx| \geq 1$  und  $|vwx| \leq j$ . Wählen wir  $i = j$ , so kann das Segment  $vwx$  aufgrund seiner Längenbeschränkung nicht gleichzeitig  $a$ 's und  $c$ 's enthalten. Entfernen wir die Segmente  $v$  und  $x$  aus  $\omega$ , so entsteht mit  $uwy$  ein Wort, das eine ungleiche Anzahl von  $a$ 's,  $b$ 's und  $c$ 's enthält. Nach dem Pumping-Lemma muss das Wort  $uwy = uv^0wx^0y$  jedoch in  $L_{C1}$  enthalten sein, im Widerspruch zur Definition dieser Sprache.

Das Pumping-Lemma hat sich soeben als wertvolles Hilfsmittel erwiesen, um die Sprache  $L_{C1}$  als nicht kontextfrei zu entlarven. Dass es sich um keine Universalwaffe handelt, wollen wir anhand der folgenden Beispielsprache herausarbeiten:

$$L_{\text{fool}} := \{b^k c^l d^m \mid k, l, m \in \mathbb{N}\} \cup \{a^m b^n c^n d^n \mid m, n \in \mathbb{N}\}$$

Obwohl  $L_{\text{fool}}$  nicht kontextfrei ist, erfüllt die Sprache alle innerhalb des Pumping-Lemmas getroffenen Aussagen. Hierzu setzen wir  $j = 4$  und wählen für alle Wörter  $\omega \in L_{\text{fool}}$  mit  $|\omega| \geq j$  die nachstehende Zerlegung:

$$\omega = \begin{cases} \underbrace{u}_{b^+} \underbrace{b^+ c^+ d^+}_{u} \underbrace{v}_{b^+} \underbrace{w}_{c^+} \underbrace{x}_{d^+} \underbrace{y}_{c^+ d^+} & \text{falls } a \notin \omega, bb \in \omega \\ \underbrace{b^+}_{u} \underbrace{c^+}_{v} \underbrace{d^+}_{w} \underbrace{y}_{c^+ d^+} & \text{falls } a \notin \omega, cc \in \omega \\ \underbrace{b^+ c^+ d^+}_{u} \underbrace{v}_{b^+} \underbrace{w}_{c^+} \underbrace{x}_{d^+} \underbrace{y}_{c^+ d^+} & \text{falls } a \notin \omega, dd \in \omega \\ \underbrace{u}_{a} \underbrace{v}_{b^*} \underbrace{w}_{b^n} \underbrace{x}_{c^n} \underbrace{y}_{d^n} & \text{falls } a \in \omega \end{cases}$$

Mit der getroffenen Wahl von  $u, v, w, x$  und  $y$  gelten die folgenden Beziehungen:

- $|vx| \geq 1$
- $|vwx| \leq j$
- $uv^iwx^i y \in L$  für alle  $i \in \mathbb{N}_0$

Damit ist es unmöglich, die Sprache  $L_{\text{fool}}$  mit Hilfe des Pumping-Lemmas von den kontextfreien Sprachen zu unterscheiden. Der Grund für das Versagen geht auf die Eigenschaft des Pumping-Lemmas zurück, keine Aussage über die Startposition der Teilwörter  $u, v, w, x$  und  $y$  zu machen. Hierdurch war es uns möglich, den kritischen Teilabschnitt  $vwx$  in Wörtern der Form  $a^m b^n c^m d^n$  komplett mit  $a$ 's zu füllen und damit zu vermeiden, dass die Struktur des nicht kontextfreien Teilworts  $b^m c^m d^n$  durch das Aufpumpen von  $v$  und  $x$  zerstört wird.

Um die Sprache dennoch als nicht kontextfrei zu identifizieren, müssen wir zu stärkeren Waffen greifen. Eine solche gibt uns *Ogdens Lemma* an die Hand – eine Verallgemeinerung des Pumping-Lemmas, das uns „pumpbaren“ Symbole freier wählt:



#### Definition 4.6 (Ogdens Lemma für kontextfreie Sprachen)

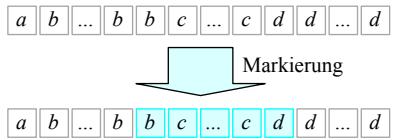
Für jede kontextfreie Sprache  $L$  existiert ein  $j \in \mathbb{N}$ , so dass alle Wörter  $\omega \in L$  mit  $|\omega| \geq j$  die folgende Eigenschaft erfüllen: Markieren wir mindestens  $j$  Zeichen in  $\omega$ , so lässt sich das Wort in der Form  $\omega = uvwxy$  schreiben, so dass

- mindestens ein Zeichen in  $vx$  markiert ist,
- höchstens  $j$  Zeichen in  $vwx$  markiert sind,
- und für alle  $i \in \mathbb{N}_0$  gilt:  $uv^iwx^i y \in L$

Wir wollen das Lemma an dieser Stelle ohne Beweis übernehmen. Eine detaillierte Herleitung findet sich z. B. in [50].

Mit Hilfe von Ogdens Lemma können wir zeigen, dass  $L_{\text{fool}}$  keine kontextfreie Sprache sein kann. Hierzu betrachten wir das Wort  $\omega = ab^j c^j d^j$ , wobei  $j$  die Konstante aus Ogdens Lemma ist. Markieren wir die Symbolsequenz  $bc^j d$ , so muss es für  $\omega$  eine Zerlegung  $uvwxy$  geben, so dass  $vx$  mindestens einen und  $vwx$  höchstens  $j$  der markierten Buchstaben enthält. Damit kann die Sequenz  $vwx$  und damit auch die Sequenz  $vx$  maximal zwei verschiedene Buchstaben aus der Menge  $\{b, c, d\}$  enthalten (vgl. Abbildung 4.18). Im Wort  $uwy$  kommt die

Das Pumping-Lemma besitzt viele Namen! Um der zunehmenden Verbreitung von Anglizismen entgegenzuwirken, wurden von einigen deutschsprachigen Autoren die Begriffe *Schleifensatz* oder *Iterationslemma* vorgeschlagen [78]. Trotz einiger Bemühungen konnten sich die Begriffe bisher nicht flächendeckend durchsetzen. Andere Autoren bezeichnen das Pumping-Lemma für reguläre Sprachen schlicht als *uvw*-Theorem und die kontextfreie Variante als *uvwxy*-Theorem. Vereinzelt wird es in Ahnlehnung an einen seiner geistigen Väter als *Bar-Hillel-Theorem* bezeichnet, benannt nach dem israelischen Mathematiker Yehoshua Bar-Hillel. Der großen Namensvielfalt zum Trotz halten wir in diesem Buch an dem ursprünglichen Begriff *Pumping-Lemma* fest, da er immer noch am unmissverständlichsten andeutet, um welches Theorem es sich hier handelt.



Nach Ogdens Lemma lässt sich das Ausgangswort in der Form  $uvwxy$  schreiben, so dass in  $vx$  mindestens ein Zeichen und in  $vwx$  höchstens  $j$  Zeichen markiert sind. Damit ergeben sich für die Sequenz  $vwx$  drei Möglichkeiten:

- Möglichkeit 1:  $vwx = bc \dots c < j$
- Möglichkeit 2:  $vwx = c \dots c \leq j$
- Möglichkeit 3:  $vwx = c \dots cd < j$

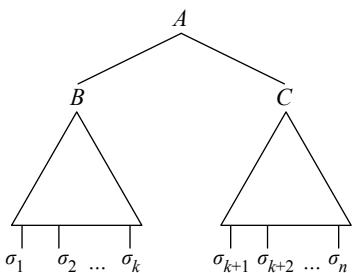
**Abbildung 4.18:** Ogdens Lemma, angewendet auf das Wort  $ab^j c^j d^j$

- Fall 1:  $|\omega| = 1$



Besteht ein ableitbares Wort aus einem einzelnen Terminalzeichen  $\sigma_1$ , so kann es aus einem Nonterminal  $A$  nur durch die Anwendung der Regel  $A \rightarrow \sigma_1$  entstanden sein.

- Fall 2:  $|\omega| > 1$



Besteht ein ableitbares Wort aus mehreren Terminalzeichen  $\sigma_1, \dots, \sigma_n$ , so kann es aus einem Nonterminal  $A$  nur durch die vorangegangene Anwendung einer Regel  $A \rightarrow BC$  entstanden sein.

**Abbildung 4.19:** Der CYK-Algorithmus arbeitet nach dem Prinzip der dynamischen Programmierung. Er macht sich die spezielle Struktur von Syntaxbäumen zu Nutze, die von Grammatik in Chomsky-Normalform erzeugt werden.

Anzahl an  $b$ 's,  $c$ 's und  $d$ 's hierdurch aus dem Gleichgewicht, so dass es kein Element von  $L$  sein kann. Nach Ogdens Lemma müsste  $uwv$  aber in  $L$  enthalten sein, falls  $L$  tatsächlich kontextfrei wäre.

#### 4.4.4 Entscheidungsprobleme

Das Wortproblem für kontextfreie Sprachen ist entscheidbar und lässt sich mit dem Mittel der *dynamischen Programmierung* effizient lösen. Anwenden lässt sich die dynamische Programmierung immer dann, wenn sich ein Problem in kleinere Teile zerlegen lässt und die optimale Lösung des Gesamtproblems aus den optimalen Lösungen der Teilprobleme berechnet werden kann. Von der klassischen Rekursion unterscheidet sich die dynamische Programmierung durch den Einsatz einer Tabelle, in der sämtliche Zwischenergebnisse gespeichert werden. Durch das Vorhalten der bereits berechneten Zwischenlösungen konsumieren die Algorithmen mehr Speicherplatz als ihre rein rekursiv programmierten Pendants, so dass sich die dynamische Programmierung immer dann anbietet, wenn die Laufzeit und nicht der Speicherbedarf eines Algorithmus im Vordergrund steht.

Prominente Algorithmen, die nach dem Prinzip der dynamischen Programmierung arbeiten, sind der *Viterbi-Algorithmus* [95] und der *Floyd-Warshall-Algorithmus* [30, 96]. Auch das bekannte *Rucksackproblem* (vgl. Abschnitt 7.1) lässt sich auf diese Weise effizient lösen [54].

Die Wissenschaftler John Cocke, Daniel Younger und Tadao Kasami erkannten Ende der Sechzigerjahre unabhängig voneinander, dass sich das Wortproblem kontextfreier Sprachen mit dem Mittel der dynamischen Programmierung lösen lässt [22, 53, 101]. Ausgangspunkt für den nach den Anfangsbuchstaben seiner Entdecker benannten *CYK-Algorithmus* ist eine Grammatik  $G$  in Chomsky-Normalform. Im Kern basiert der CYK-Algorithmus auf der folgenden Beobachtung:

- Lässt sich aus einem Nonterminal  $A$  ein Wort  $\omega$  ableiten, das aus einem einzelnen Terminalzeichen  $\sigma$  besteht, so muss die Regel  $A \rightarrow \sigma$  existieren. Andernfalls würden die Produktionen mindestens ein weiteres Nonterminal und damit auch ein weiteres Terminalzeichen produzieren. Für den Fall  $|\omega| = 1$  lässt sich das Wortproblem somit ohne Mühe entscheiden (vgl. Abbildung 4.19 oben).
- Besteht das Wort  $\omega$  aus mehreren Terminalzeichen  $\sigma_1, \dots, \sigma_n$  mit  $n \geq 2$ , so kann es aus einem Nonterminal  $A$  nur durch eine vorangegangene Anwendung einer Regel  $A \rightarrow BC$  entstanden sein. Können wir nachweisen, dass ein gewisses  $k$  mit  $1 \leq k \leq n$  existiert, so

## CYK-Algorithmus

```

// Eingabe: Grammatik  $G = (V, \Sigma, P, S)$ 
//           Wort  $\omega = \sigma_1, \dots, \sigma_n$ 
// Ausgabe: true , wenn  $\omega \in \mathcal{L}(G)$ , false wenn  $\omega \notin \mathcal{L}(G)$ 

boolean cyk(G, ω)
{
    // Berechne die erste Zeile ...
    for (i = 1; i ≤ n; i++) {
        cyk[i][1] = {A | (A → σ_i) ∈ P};
    }

    // Berechne alle restlichen Zeilen ...
    for (j = 2; j ≤ n; j++) {
        for (i = 1; i ≤ n+1-j; i++) {
            cyk[i][j] = ∅;
            for (k = 1; k < j; k++) {
                cyk[i][j] = cyk[i][j] ∪ {A | (A → BC) ∈ P, B ∈ cyk[i][k], C ∈ cyk[i+k][j-k]};
            }
        }
    }
    return S ∈ cyk[1][n];
}

```

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

Abbildung 4.20: Der CYK-Algorithmus (Pseudo-Code)

dass sich die Anfangssequenz  $\sigma_1 \dots \sigma_k$  aus  $B$  und die Endesequenz  $\sigma_{k+1} \dots \sigma_n$  aus  $C$  ableiten lässt, dann lässt sich das Gesamtwort  $\omega$  aus  $A$  ableiten (vgl. Abbildung 4.19 unten).

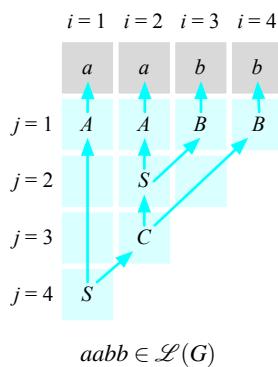
Damit ist es uns gelungen, das Problem für Wörter  $\omega$  der Länge  $n$  auf die Lösung für Wörter der Länge  $k$  bzw.  $n - k$  zurückzuführen. Auch wenn wir den Wert von  $k$  nicht kennen und alle Möglichkeiten in Betracht ziehen müssen, ist sichergestellt, dass die Teilwörter eine kleinere Länge besitzen als  $\omega$  selbst. Damit sind alle Voraussetzungen für die Anwendbarkeit der dynamischen Programmierung erfüllt.

Um das Wortproblem für  $\omega = \sigma_1, \dots, \sigma_n$  zu entscheiden, verwaltet der CYK-Algorithmus intern ein zweidimensionales Array  $cyk$  der Größe  $n \times n$ . Sobald der Algorithmus terminiert, enthält das Feld  $cyk[i][j]$  alle Nonterminale, aus denen sich das Teilwort  $\sigma_i, \dots, \sigma_{i+j-1}$  ableiten lässt. Offensichtlich gelten die folgenden Eigenschaften:

■ Grammatik

$$\begin{array}{l} S \rightarrow AB \mid AC \\ C \rightarrow SB \\ A \rightarrow a \\ B \rightarrow b \end{array}$$

■  $\omega_1 = aabb$



■  $\omega_2 = abbb$

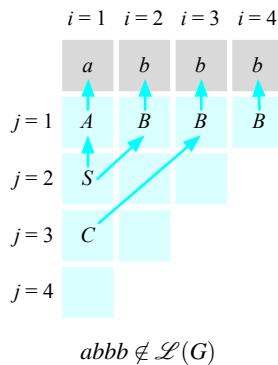


Abbildung 4.21: Der CYK-Algorithmus in Aktion

- Für  $i + j > n + 1$  kann  $\text{cyk}[i][j]$  niemals Nonterminale enthalten. Effektiv benötigt der CYK-Algorithmus damit nur etwas mehr als die Hälfte der Array-Felder. Alle anderen Felder brauchen nicht berücksichtigt zu werden.
- Das Wort  $\omega$  lässt sich genau dann ableiten, wenn das Feld  $\text{cyk}[1][n]$  das Startsymbol  $S$  enthält. Damit reduziert sich das Wortproblem auf einen simplen Inklusionstest, sobald das Array  $\text{cyk}$  komplett aufgebaut ist.

Die Hauptarbeit des CYK-Algorithmus besteht im Ausfüllen der Array-Felder  $\text{cyk}[i][j]$  (vgl. Abbildung 4.20). In zwei verschachtelten Schleifen iteriert der Algorithmus hierzu in gewöhnlicher Leserichtung von links nach rechts und von oben nach unten über die Array-Felder  $\text{cyk}[i][j]$ . Für jedes Feld wird geprüft, ob eine Regel  $A \rightarrow BC$  und ein  $k$  existieren, so dass sich das Teilwort  $\sigma_i, \dots, \sigma_{i+k-1}$  aus  $B$  und das Teilwort  $\sigma_{i+k}, \dots, \sigma_{i+j-1}$  aus  $C$  erzeugen lässt. Dies ist genau dann der Fall, wenn das Nonterminal  $B$  in  $\text{cyk}[i,k]$  und das Nonterminal  $C$  in  $\text{cyk}[i+k,j-k]$  enthalten ist. Fällt der Test erfolgreich aus, so wird dem Element  $\text{cyk}[i][j]$  das Nonterminal  $A$  hinzugefügt.

Im Kern verbirgt sich hinter dieser Implementierung nichts anderes als ein rekursiver Algorithmus. Der Effizienzgewinn resultiert aus der Eigenschaft, die Zwischenergebnisse tabellarisch zu speichern und den rekursiven Aufruf durch einen simplen Tabellenzugriff zu ersetzen. Während der rein rekursiv arbeitende Algorithmus eine exponentielle Laufzeit benötigen würde, macht es die dynamische Programmierung an dieser Stelle möglich, das Wortproblem in kubischer Laufzeit zu entscheiden. Erkauft wird der Effizienzgewinn durch einen erhöhten Logistikbedarf, der den benötigten Speicherplatz des CYK-Algorithmus quadratisch mit der Länge des Eingabeworts wachsen lässt.

Abbildung 4.21 demonstriert die Anwendung des CYK-Algorithmus anhand zweier Beispiele. Für die erste Zeichensequenz wird das Wortproblem positiv entschieden. Da das Feld  $\text{cyk}[1][4]$  das Startsymbol  $S$  enthält, ist sichergestellt, dass sich das Wort  $aabb$  aus dem Startsymbol ableiten lässt. Für das zweite Beispiel endet der Test negativ. Die Sequenz  $abbb$  lässt sich aus keinem Nonterminal und damit erst recht nicht aus dem Startsymbol ableiten.

#### 4.4.5 Abschlusseigenschaften

Für die folgenden Betrachtungen seien mit  $G_1 = \{V_1, \Sigma, P_1, S_1\}$  und  $G_2 = \{V_2, \Sigma, P_2, S_2\}$  zwei kontextfreie Grammatiken über dem Alpha-

bet  $\Sigma$  gegeben. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass die Variablenmengen  $V_1$  und  $V_2$  keine gemeinsamen Elemente enthalten. Aus  $G_1$  und  $G_2$  lässt sich auf direktem Weg eine Grammatik  $G_{1\cup 2}$  definieren, die  $\mathcal{L}(G_1) \cup \mathcal{L}(G_2)$  erzeugt. Hierzu fassen wir die Variablenmengen  $V_1$  und  $V_2$  sowie die Produktionenmengen  $P_1$  und  $P_2$  zu einer neuen Variablen- bzw. Produktionenmenge zusammen. Ferner führen wir ein neues Startsymbol  $S$  ein, aus dem sich durch eine neu hinzugefügte Produktion sowohl das Startsymbol von  $G_1$  als auch das Startsymbol von  $G_2$  erzeugen lässt. Insgesamt erhalten wir mit

$$G_{1\cup 2} := \{V_1 \cup V_2, \Sigma, P_1 \cup P_2 \cup \{S \rightarrow S_1 \mid S_2\}, S\}$$

eine Grammatik, die alle Wörter aus  $\mathcal{L}(G_1)$  und  $\mathcal{L}(G_2)$  erzeugt. Damit ist der Abschluss kontextfreier Sprachen bez. der Vereinigungsoperation gezeigt.

Auf ganz ähnliche Weise können wir eine Grammatik  $G_{1\cdot 2}$  erzeugen, die alle Wörter aus der Produktmenge  $\mathcal{L}(G_1)\mathcal{L}(G_2)$  erzeugt. Auch hier führen wir beide Variablen- und Produktionenmengen zusammen und ersetzen die Startsymbole  $S_1$  und  $S_2$  durch ein frisches Nonterminal  $S$ . Der einzige Unterschied betrifft die neu hinzugefügte Ableitungsregel, die  $S$  durch  $S_1S_2$  ersetzt:

$$G_{1\cdot 2} := \{V_1 \cup V_2, \Sigma, P_1 \cup P_2 \cup \{S \rightarrow S_1S_2\}, S\}$$

Die Grammatik erzeugt die Wortmenge  $\mathcal{L}(G_1)\mathcal{L}(G_2)$  und beweist den Abschluss kontextfreier Sprachen bez. Produktbildung.

Die Konstruktion der Produktgrammatik weist den Weg für die Konstruktion einer Grammatik, die alle Wörter der Kleene'schen Hülle  $\mathcal{L}(G_1)^*$  erzeugt. Hierzu reichern wir die Menge der Produktionen mit neuen Ableitungsregeln an, die aus dem neuen Startsymbol  $S$  eine beliebige Anzahl des ursprünglichen Startsymbols  $S_1$  entstehen lassen. Als Ergebnis erhalten wir die folgende Grammatik:

$$G_1^* := \{V_1, \Sigma, P_1 \cup \{S \rightarrow \epsilon \mid SS_1\}, S\}$$

Abbildung 4.22 demonstriert die drei eingeführten Konstruktionen am Beispiel der Grammatiken  $G_1 := (V_1, \Sigma, P_1, S_1)$  und  $G_2 := (V_2, \Sigma, P_2, S_2)$  mit  $\Sigma := \{a, b, c\}$ ,  $V_1 := \{S_1, A_1, B_1\}$ ,  $V_2 := \{S_2, A_2, B_2\}$  und

$$\begin{aligned} P_1 &:= \{S_1 \rightarrow A_1B_1, A_1 \rightarrow ab \mid aA_1b, B_1 \rightarrow c \mid cB_1\} \\ P_2 &:= \{S_2 \rightarrow A_2B_2, A_2 \rightarrow a \mid aA_2, B_2 \rightarrow bc \mid bB_2c\} \end{aligned}$$

Es bleibt die Untersuchung der Schnitt- und der Komplementoperation. Anhand der eingeführten Beispielgrammatiken  $G_1$  und  $G_2$  können wir

#### Grammatik $G_1$

$$\begin{aligned} S_1 &\rightarrow A_1B_1 \\ A_1 &\rightarrow ab \mid aA_1b \\ B_1 &\rightarrow c \mid cB_1 \end{aligned}$$

#### Grammatik $G_2$

$$\begin{aligned} S_2 &\rightarrow A_2B_2 \\ A_2 &\rightarrow a \mid aA_2 \\ B_2 &\rightarrow bc \mid bB_2c \end{aligned}$$

#### Vereinigung

$$\begin{aligned} S &\rightarrow S_1 \mid S_2 \\ S_1 &\rightarrow A_1B_1 \\ A_1 &\rightarrow ab \mid aA_1b \\ B_1 &\rightarrow c \mid cB_1 \\ S_2 &\rightarrow A_2B_2 \\ A_2 &\rightarrow a \mid aA_2 \\ B_2 &\rightarrow bc \mid bB_2c \end{aligned}$$

#### Produktbildung

$$\begin{aligned} S &\rightarrow S_1S_2 \\ S_1 &\rightarrow A_1B_1 \\ A_1 &\rightarrow ab \mid aA_1b \\ B_1 &\rightarrow c \mid cB_1 \\ S_2 &\rightarrow A_2B_2 \\ A_2 &\rightarrow a \mid aA_2 \\ B_2 &\rightarrow bc \mid bB_2c \end{aligned}$$

#### Kleene'sche Hülle

$$\begin{aligned} S &\rightarrow \epsilon \mid SS_1 \\ S_1 &\rightarrow A_1B_1 \\ A_1 &\rightarrow ab \mid aA_1b \\ B_1 &\rightarrow c \mid cB_1 \end{aligned}$$

**Abbildung 4.22:** Kontextfreie Grammatiken sind bez. Vereinigung, Produktbildung und Hüllensbildung abgeschlossen.

■ Entscheidungsprobleme kontextfreier Sprachen

Problem	Eingabe	Fragestellung	Entscheidbar?
Wortproblem	Sprache $L$ , Wort $\omega \in \Sigma^*$	Ist $\omega \in L$ ?	✓ Ja
Leerheitsproblem	Sprache $L$	Ist $L = \emptyset$ ?	✓ Ja
Endlichkeitsproblem	Sprache $L$	Ist $ L  < \infty$ ?	✓ Ja
Äquivalenzproblem	Sprachen $L_1$ und $L_2$	Ist $L_1 = L_2$ ?	✗ Nein

■ Abschlusseigenschaften kontextfreier Sprachen

Operation	Eingabe	Fragestellung	Erfüllt?
Vereinigung	Sprache $L_1, L_2 \in \mathcal{L}_2$	Ist $L_1 \cup L_2 \in \mathcal{L}_2$ ?	✓ Ja
Schnitt	Sprache $L_1, L_2 \in \mathcal{L}_2$	Ist $L_1 \cap L_2 \in \mathcal{L}_2$ ?	✗ Nein
Komplement	Sprache $L \in \mathcal{L}_2$	Ist $\Sigma^* \setminus L \in \mathcal{L}_2$ ?	✗ Nein
Produkt	Sprache $L_1, L_2 \in \mathcal{L}_2$	Ist $L_1 L_2 \in \mathcal{L}_2$ ?	✓ Ja
Stern	Sprache $L \in \mathcal{L}_2$	Ist $L^* \in \mathcal{L}_2$ ?	✓ Ja

Abbildung 4.23: Eigenschaften kontextfreier Sprachen in der Übersicht

zeigen, dass die Menge der kontextfreien Sprachen bez. der Schnittoperation nicht abgeschlossen ist. Es gilt:

$$\mathcal{L}(G_1) = \{a^i b^j c^j \mid i, j \in \mathbb{N}\} \quad (4.11)$$

$$\mathcal{L}(G_2) = \{a^j b^i c^i \mid i, j \in \mathbb{N}\} \quad (4.12)$$

Als Schnitt von  $\mathcal{L}(G_1)$  und  $\mathcal{L}(G_2)$  erhalten wir die Sprache

$$\mathcal{L}(G_1) \cap \mathcal{L}(G_2) = \{a^i b^i c^i\}, \quad (4.13)$$

die wir bereits weiter oben als nicht kontextfrei identifiziert haben. Aus dem bisher Bewiesenen folgt unmittelbar, dass die kontextfreien Sprachen auch bez. der Komplementbildung nicht abgeschlossen sein können. Aufgrund der De Morgan'schen Regel gilt die folgende Beziehung:

$$\mathcal{L}(G_1) \cap \mathcal{L}(G_2) = \overline{\mathcal{L}(G_1)} \cup \overline{\mathcal{L}(G_2)} \quad (4.14)$$

Wären die kontextfreien Sprachen bez. Komplementbildung abgeschlossen, so würde die Abgeschlossenheit der Schnittoperation folgen, im Widerspruch zu den bewiesenen Resultaten. Abbildung 4.23 fasst die herausgearbeiteten Ergebnisse tabellarisch zusammen.

## 4.5 Kontextsensitive Sprachen

### 4.5.1 Definition und Eigenschaften

Kontextsensitive Grammatiken sind eine Erweiterung der kontextfreien Grammatiken. Sie zeichnen sich dadurch aus, dass auf der linken Seite einer Produktion eine beliebige Kombination aus Terminal- und Nonterminalzeichen stehen darf. Erst hierdurch wird es möglich, die Ersetzbarkeit eines Nonterminals an die Beschaffenheit seiner Umgebung – den *Kontext* – zu binden. Die einzige Einschränkung, der die Produktionen kontextsensitiver Grammatiken unterliegen, betrifft die Länge der linken und rechten Seiten: Für jede Produktion der Form  $l \rightarrow r$  muss die Beziehung  $|l| \leq |r|$  gewahrt sein. In kontextsensitiven Grammatiken ist damit sichergestellt, dass die produzierte Zeichensequenz in einem Ableitungsschritt niemals verkürzt wird.

Mit Hilfe kontextsensitiver Grammatiken sind wir in der Lage, die Sprache

$$L_{C1} = \{a^i b^i c^i \mid i \in \mathbb{N}\}$$

zu erzeugen. Für die Konstruktion einer entsprechenden Grammatik gehen wir in drei Schritten vor:

- Neben dem Startsymbol  $S$  führen wir drei Nonterminale  $A$ ,  $B$  und  $C$  ein, die stellvertretend für jeweils eines der Terminalzeichen  $a$ ,  $b$  und  $c$  stehen. Ferner stellen wir durch entsprechende Produktionen sicher, dass wir die Nonterminale  $A$ ,  $B$  und  $C$  beliebig oft, aber stets in gleicher Anzahl erzeugen können (obere Regelgruppe in Abbildung 4.24).
- Die bisher eingeführten Produktionen erlauben uns, die benötigte Anzahl  $A$ 's,  $B$ 's und  $C$ 's zu erzeugen. Diese sind jedoch noch ungeordnet und müssen vor der weiteren Bearbeitung zunächst in die richtige Reihenfolge gebracht werden. Um die notwendige Sortierung zu gewährleisten, reichern wir die Grammatik um drei weitere Produktionen an (mittlere Regelgruppe in Abbildung 4.24).
- Zum Schluss benötigen wir Produktionen, die aus den Nonterminalen  $A$ ,  $B$  und  $C$  die Terminalzeichen  $a$ ,  $b$  und  $c$  erzeugen. Die Ersetzung darf nicht beliebig erfolgen, sondern ausschließlich dann, wenn die Nonterminale in der richtigen Reihenfolge angeordnet sind. Um dies zu erreichen, nutzen wir aus, dass Terminalzeichen in kontextsensitiven Grammatiken auch auf der linken Seite einer Produktion auftauchen dürfen (untere Regelgruppe in Abbildung 4.24).

### ■ Grammatik

$$S \rightarrow ABC$$

$$S \rightarrow SABC$$

$$BA \rightarrow AB$$

$$CB \rightarrow BC$$

$$CA \rightarrow AC$$

$$AB \rightarrow ab$$

$$BC \rightarrow bc$$

$$Aa \rightarrow aa$$

$$bB \rightarrow bb$$

$$cC \rightarrow cc$$

### ■ Ableitung des Worts $aaabbbccc$

$$S \rightarrow SABC$$

$$\rightarrow SABCABC$$

$$\rightarrow ABCABCABC$$

$$\rightarrow AABCBCABC$$

$$\rightarrow AABCCABC$$

$$\rightarrow ABBCCABC$$

$$\rightarrow AABBCACBC$$

$$\rightarrow AABBAACCBC$$

$$\rightarrow AAABAACCBC$$

$$\rightarrow AAABCCBC$$

$$\rightarrow AAABCBCCC$$

$$\rightarrow AAABBCCCCC$$

$$\rightarrow AAabBBCCC$$

$$\rightarrow AAbBbcCC$$

$$\rightarrow AaabBbcCC$$

$$\rightarrow aaabBbcCC$$

$$\rightarrow aaabbccC$$

$$\rightarrow aaabbccC$$

$$\rightarrow aaabbccc$$

**Abbildung 4.24:** Erzeugung der Sprache  $L_{C1} = \{a^n b^n c^n \mid n \in \mathbb{N}\}$  mit Hilfe einer kontextsensitiven Grammatik

■ Entscheidungsprobleme kontextsensitiver Sprachen

Problem	Eingabe	Fragestellung	Entscheidbar?
Wortproblem	Sprache $L$ , Wort $\omega \in \Sigma^*$	Ist $\omega \in L$ ?	✓ Ja
Leerheitsproblem	Sprache $L$	Ist $L = \emptyset$ ?	✗ Nein
Endlichkeitsproblem	Sprache $L$	Ist $ L  < \infty$ ?	✗ Nein
Äquivalenzproblem	Sprachen $L_1$ und $L_2$	Ist $L_1 = L_2$ ?	✗ Nein

■ Abschlusseigenschaften kontextsensitiver Sprachen

Operation	Eingabe	Fragestellung	Erfüllt?
Vereinigung	Sprache $L_1, L_2 \in \mathcal{L}_1$	Ist $L_1 \cup L_2 \in \mathcal{L}_1$ ?	✓ Ja
Schnitt	Sprache $L_1, L_2 \in \mathcal{L}_1$	Ist $L_1 \cap L_2 \in \mathcal{L}_1$ ?	✓ Ja
Komplement	Sprache $L \in \mathcal{L}_1$	Ist $\Sigma^* \setminus L \in \mathcal{L}_1$ ?	✓ Ja
Produkt	Sprache $L_1, L_2 \in \mathcal{L}_1$	Ist $L_1 L_2 \in \mathcal{L}_1$ ?	✓ Ja
Stern	Sprache $L \in \mathcal{L}_1$	Ist $L^* \in \mathcal{L}_1$ ?	✓ Ja

Abbildung 4.25: Eigenschaften kontextsensitiver Sprachen in der Übersicht

### 4.5.2 Entscheidungsprobleme

Sämtliche Produktionen  $l \rightarrow r$  kontextsensitiver Grammatiken müssen die Beziehung  $|l| \leq |r|$  erfüllen. Auf den ersten Blick erscheint die Forderung als willkürlich. Auf den zweiten Blick erweist sie sich als der Schlüssel für die Entscheidbarkeit des Wortproblems, da ein Wort in einem Ableitungsschritt niemals kürzer werden kann. Hat eine Ableitungssequenz als Zwischenergebnis eine Kette mit mehr als  $n$  Symbolen hervorgebracht, so kann sie niemals ein Wort der Länge  $n$  erzeugen. Aufgrund dieser Eigenschaft ist die Menge der Ableitungssequenzen, die ein Wort der Länge  $n$  generieren, endlich und wir können das Wortproblem für  $\omega$  mit  $|\omega| = n$  entscheiden, indem wir nacheinander alle in Frage kommenden Ableitungssequenzen durchsuchen.

Im Gegensatz zum Wortproblem sind das Leerheitsproblem, das Endlichkeitsproblem und das Äquivalenzproblem für kontextfreie Sprachen unentscheidbar, d. h., es gibt kein Verfahren, das eine beliebige Grammatik entgegennimmt und die Fragestellung immer korrekt beantwortet.

### 4.5.3 Abschlusseigenschaften

Die Menge der kontextsensitiven Sprachen ist bez. Vereinigung, Schnitt, Komplement, Produkt und Kleene'scher Hülle abgeschlossen. Um diese Eigenschaften zu zeigen, führen wir zwei kontextsensitive Grammatiken  $G_1$  und  $G_2$  wie folgt zu einer gemeinsamen Grammatik zusammen:

#### ■ Vereinigung

$\mathcal{L}(G_1) \cup \mathcal{L}(G_2)$  wird durch die nachstehende Grammatik erzeugt:

$$G_{1 \cup 2} := \{V_1 \cup V_2, \Sigma, P_1 \cup P_2 \cup \{S \rightarrow S_1 | S_2\}, S\}$$

#### ■ Produkt

$\mathcal{L}(G_1)\mathcal{L}(G_2)$  wird durch die nachstehende Grammatik erzeugt:

$$G_{1 \cdot 2} := \{V_1 \cup V_2, \Sigma, P_1 \cup P_2 \cup \{S \rightarrow S_1 S_2\}, S\}$$

#### ■ Kleene'sche Hülle

$\mathcal{L}(G_1)^*$  wird durch die nachstehende Grammatik erzeugt:

$$G_1^* := \{V_1, \Sigma, P_1 \cup \{S \rightarrow \epsilon | SS_1\}, S\}$$

Den Beweis der Abgeschlossenheit bez. Durchschnitt und Komplement wollen wir an dieser Stelle nicht führen. Die Eigenschaften lassen sich am einfachsten mit Hilfe linear beschränkter Turing-Maschinen zeigen, die wir in Abschnitt 6.3 als äquivalente Beschreibungsform für kontextsensitive Sprachen kennen lernen werden. Abbildung 4.25 fasst die Entscheidbarkeits- und Abschlusseigenschaften für kontextsensitive Sprachen in einer Übersicht zusammen.

## 4.6 Rekursiv aufzählbare Sprachen

Jede Sprache, die sich durch eine Grammatik im Sinne von Definition 4.2 erzeugen lässt, heißt rekursiv aufzählbar. Im Gegensatz zu allen anderen Sprachklassen unterliegen die linke und die rechte Seite einer Produktion  $l \rightarrow r$  keinen Restriktionen; beide dürfen aus einer beliebigen Sequenz von Terminal- und Nonterminalzeichen bestehen (vgl. Abbildung 4.26).

Typ-0-Grammatiken sind ausdrucksstärker, als es der erste Blick vermuten lässt. In Kapitel 6 werden wir zeigen, dass Typ-0-Sprachen und

#### ■ Grammatik

$$S \rightarrow SD$$

$$S \rightarrow La$$

$$aD \rightarrow Daa$$

$$LD \rightarrow L$$

$$L \rightarrow \epsilon$$

#### ■ Ableitung des Worts $a^4$

$$S \rightarrow SD$$

$$\rightarrow SDD$$

$$\rightarrow SDDD$$

$$\rightarrow SDDDD$$

$$\rightarrow LaDDDD$$

$$\rightarrow LDaaDDD$$

$$\rightarrow LaaDDD$$

$$\rightarrow LaDaDD$$

$$\rightarrow LDaaaaDD$$

$$\rightarrow LaaaaDD$$

$$\rightarrow LaaDaaD$$

$$\rightarrow LaaDaaaA$$

$$\rightarrow LaDaaaaaaaaD$$

$$\rightarrow LDaaaaaaaaaaD$$

$$\rightarrow LaaaaaaaaaaD$$

$$\rightarrow LaaaaaaaDaa$$

$$\rightarrow LaaaaaaDaaaa$$

$$\rightarrow LaaaaaDaaaaaaaa$$

$$\rightarrow LaaaDaaaaaaaaaaaa$$

$$\rightarrow LaaDaaaaaaaaaaaaaa$$

$$\rightarrow LaDaaaaaaaaaaaaaaaa$$

$$\rightarrow LDaaaaaaaaaaaaaaaaaa$$

$$\rightarrow aaaaaaaaaaaaaaaaaaa$$

**Abbildung 4.26:** Erzeugung der Sprache  $L_{C0} = \{a^{2^n} \mid n \in \mathbb{N}\}$  mit Hilfe einer Typ-0-Grammatik

■ Entscheidungsprobleme rekursiv aufzählbarer Sprachen

Problem	Eingabe	Fragestellung	Entscheidbar?
Wortproblem	Sprache $L$ , Wort $\omega \in \Sigma^*$	Ist $\omega \in L$ ?	✗ Nein
Leerheitsproblem	Sprache $L$	Ist $L = \emptyset$ ?	✗ Nein
Endlichkeitsproblem	Sprache $L$	Ist $ L  < \infty$ ?	✗ Nein
Äquivalenzproblem	Sprachen $L_1$ und $L_2$	Ist $L_1 = L_2$ ?	✗ Nein

■ Abschlusseigenschaften rekursiv aufzählbarer Sprachen

Operation	Eingabe	Fragestellung	Erfüllt?
Vereinigung	Sprache $L_1, L_2 \in \mathcal{L}_0$	Ist $L_1 \cup L_2 \in \mathcal{L}_0$ ?	✓ Ja
Schnitt	Sprache $L_1, L_2 \in \mathcal{L}_0$	Ist $L_1 \cap L_2 \in \mathcal{L}_0$ ?	✓ Ja
Komplement	Sprache $L \in \mathcal{L}_0$	Ist $\Sigma^* \setminus L \in \mathcal{L}_0$ ?	✗ Nein
Produkt	Sprache $L_1, L_2 \in \mathcal{L}_0$	Ist $L_1 L_2 \in \mathcal{L}_0$ ?	✓ Ja
Stern	Sprache $L \in \mathcal{L}_0$	Ist $L^* \in \mathcal{L}_0$ ?	✓ Ja

**Abbildung 4.27:** Eigenschaften rekursiv aufzählbarer Sprachen in der Übersicht

Turing-Maschinen die gleiche Berechnungsstärke besitzen. Damit lassen sich mit Typ-0-Grammatiken alle Sprachen erzeugen, die in irgend einer Weise algorithmisch berechenbar sind. Dass darüber hinaus Sprachen existieren, die nicht berechenbar sind und damit auch nicht durch eine Typ-0-Grammatik erzeugt werden können, ist ein wichtiges Resultat, das wir in Kapitel 6 ausführlich herausarbeiten werden.

Die große Ausdrucksstärke von Typ-0-Grammatiken führt dazu, dass wir nur noch begrenzte Aussagen über die erzeugten Sprachen machen können. Insbesondere sind das Wortproblem, das Leerheitsproblem, das Endlichkeitsproblem und das Äquivalenzproblem unentscheidbar.

Dagegen sind Typ-0-Sprachen bez. Vereinigung, Durchschnitt, Konkatenation und Hülle abgeschlossen, d. h., zwei Grammatiken  $G_1$  und  $G_2$  lassen sich zu einer einzigen Grammatik verschmelzen, die  $\mathcal{L}(G_1) \cup \mathcal{L}(G_2)$ ,  $\mathcal{L}(G_1) \cap \mathcal{L}(G_2)$ ,  $\mathcal{L}(G_1)\mathcal{L}(G_2)$  oder  $\mathcal{L}(G_1)^*$  erzeugt. Einzig die Komplementbildung verletzt die Abschlusseigenschaften, da nicht zu jeder Grammatik  $G$  eine Grammatik existiert, die  $\mathcal{L}(G)$  erzeugt.

## 4.7 Übungsaufgaben

Gegeben seien die folgenden Alphabete:

$$\Sigma_1 := \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\Sigma_2 := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\Sigma_3 := \{A, B, C, D, E, F\}$$

$$\Sigma_4 := \{8, 9\}$$

**Aufgabe 4.1**



**Webcode  
4658**

Finden Sie umgangssprachliche Beschreibungen für die nachstehenden Sprachen:

- a)  $\Sigma_2 \mid \Sigma_1 \Sigma_2^*$
- c)  $(\Sigma_2 \setminus \Sigma_4) \mid (\Sigma_1 \setminus \Sigma_4)(\Sigma_2 \setminus \Sigma_4)^*$
- b)  $(\Sigma_2 \cup \Sigma_3) \mid (\Sigma_1 \cup \Sigma_3)(\Sigma_2 \cup \Sigma_3)^*$

Gegeben seien die folgenden Mengen:

$$L_1 := \{aa, bb\}$$

$$L_2 := \{a\}^+$$

$$L_3 := \{b\}^+$$

**Aufgabe 4.2**



**Webcode  
4194**

Erzeugen Sie die nachstehenden Sprachen:

- a)  $L_1 \cup L_2$
- b)  $L_1 \cup L_3$
- c)  $L_1^* \cap L_2$
- d)  $L_1^* \cap L_3$

Als Beispiel einer Grammatik haben Sie in diesem Kapitel die folgenden Produktionsregeln für eine Teilmenge der deutschen Sprache kennengelernt:

- <Satz> → <Subjekt> <Prädikat> <Objekt>
- <Subjekt> → <Artikel><Adjektiv><Substantiv>
- <Artikel> → Der | Die | Das
- <Adjektiv> → kleine | süße | flinke
- <Substantiv> → Eisbär | Elch | Kröte | Maus | Nilpferd
- <Prädikat> → mag | fängt | isst
- <Objekt> → Kekse | Schokolade | Käsepizza

**Aufgabe 4.3**



**Webcode  
4893**

Nicht alle Sätze, die sich aus diesen Produktionen ableiten lassen, sind grammatisch korrekt. Wie das folgende Beispiel zeigt, lassen sich Wortsequenzen ableiten, in denen die Satzteile nicht zusammenpassen: „Das kleine Maus mag Käsepizza“. Schreiben Sie die Grammatik so um, dass nur solche Sätze ableitbar sind, in denen Artikel und Substantiv sprachlich korrekt kombiniert werden.

**Aufgabe 4.4****Webcode****4400**

Mit  $L_1$ ,  $L_2$  und  $L_3$  seien zwei beliebige Sprachen gegeben. Welche der folgenden Aussagen sind richtig?

- |   |                                    |
|---|------------------------------------|
| a) $(L_1 \cup L_2)L_3 = L_1L_3 \cup L_2L_3$ | e) $(L_1^*)^* = L_1^*$             |
| b) $(L_1 \cap L_2)L_3 = L_1L_3 \cap L_2L_3$ | f) $(L_1^+)^+ = L_1^+$             |
| c) $(L_1 \cup L_2)^* = L_1^* \cup L_2^*$    | g) $(L_1L_2)^*L_1 = L_1(L_2L_1)^*$ |
| d) $(L_1 \cap L_2)^* = L_1^* \cap L_2^*$    | h) $(L_1L_2)^+L_1 = L_1(L_2L_1)^+$ |

**Aufgabe 4.5****Webcode****4634**

In der Programmiersprache C werden Variablennamen nach der folgenden Regel gebildet:

*„Namen bestehen aus Buchstaben und Ziffern; dabei muss das erste Zeichen ein Buchstabe sein. Der Unterstrich ‘\_’ zählt als Buchstabe.“ [55]*

Formalisieren Sie die verbale Beschreibung mit einem Ausdruck in Backus-Naur-Form.

**Aufgabe 4.6****Webcode****4955**

Die *Palindromsprache*  $\mathcal{P}(\Sigma)$  über einem Alphabet  $\Sigma$  ist die Menge der Wörter aus  $\Sigma^*$ , die von links und rechts gelesen die gleiche Zeichensequenz ergeben. Beispielsweise gelten für die Palindromsprache  $\mathcal{P}(\{a,b,c\})$  die folgenden Beziehungen:

$$\begin{array}{ll} aba \in \mathcal{P}(\{a,b,c\}) & ab \notin \mathcal{P}(\{a,b,c\}) \\ abccba \in \mathcal{P}(\{a,b,c\}) & abcabc \notin \mathcal{P}(\{a,b,c\}) \\ aabbcbbaa \in \mathcal{P}(\{a,b,c\}) & aabbccbaa \notin \mathcal{P}(\{a,b,c\}) \end{array}$$

- Geben Sie eine kontextfreie Grammatik  $G$  an, die  $\mathcal{P}(\{a,b,c\})$  erzeugt.
- Zeigen Sie, dass die Palindromsprache  $\mathcal{P}(\{a,b,c\})$  nicht regulär ist.

**Aufgabe 4.7****Webcode****4832**

In Abschnitt 4.1 haben Sie die folgende Grammatik zur Erzeugung der Dyck-Sprache  $D_2$  kennen gelernt:  $S \rightarrow \epsilon \mid SS \mid [S] \mid (S)$

- Modifizieren Sie die Grammatik so, dass sich das leere Wort nicht mehr ableiten lässt.
- Übersetzen Sie die modifizierte Grammatik in Chomsky-Normalform.

Die Verallgemeinerung der Bildungsregeln regulärer Grammatiken führt uns auf direktem Weg zur *Greibach-Normalform*. Formal liegt eine Grammatik  $G$  in Greibach-Normalform vor, wenn alle Produktionen die Form

$$A \rightarrow \sigma \quad \text{oder} \quad A \rightarrow \sigma B_1 \dots B_n$$

besitzen mit  $n \in \mathbb{N}$ ,  $A, B_1, \dots, B_n \in V$  und  $\sigma \in \Sigma$ . Reguläre Grammatiken erhalten wir als Spezialfall für  $n = 1$ . Es lässt sich zeigen, dass sämtliche von Greibach-Grammatiken erzeugte Sprachen kontextfrei sind. Umgekehrt existiert zu jeder kontextfreien Sprache  $L$  mit  $\varepsilon \notin L$  eine Grammatik in Greibach-Normalform, die  $L$  erzeugt (siehe hierzu [50]).

Erzeugen Sie die Greibach-Normalform für die folgenden Grammatiken:

a) $S \rightarrow AB$	$A \rightarrow a$	b) $S \rightarrow ()$
$S \rightarrow ABA$	$B \rightarrow Bb$	$S \rightarrow SS$
$A \rightarrow aA$	$B \rightarrow \varepsilon$	$S \rightarrow (S)$

**Aufgabe 4.8**

**Webcode  
4932**

Die Grammatiken

$$G_1 := (\{S, E, Z\}, \{a, \dots, j\}, P_1, S) \quad \text{und} \quad G_2 := (\{S, E, Z\}, \{a, \dots, j\}, P_2, S)$$

seien durch die folgenden Produktionen definiert:

**Aufgabe 4.9**

**Webcode  
4476**

■ Produktionenmenge  $P_1$

$$\begin{aligned} S &\rightarrow a \mid d \mid g \mid j \mid SS \mid EZ \mid ZE \\ E &\rightarrow b \mid e \mid h \mid ES \mid ZZ \mid SE \\ Z &\rightarrow c \mid f \mid i \mid EE \mid ZS \mid SZ \end{aligned}$$

■ Produktionenmenge  $P_2$

$$\begin{aligned} S &\rightarrow a \mid d \mid g \mid j \mid bZ \mid cE \mid dS \mid eZ \mid fE \mid gS \mid hZ \mid iE \mid jS \\ E &\rightarrow b \mid e \mid h \mid bS \mid cZ \mid dE \mid eS \mid fZ \mid gE \mid hS \mid iZ \mid jE \\ Z &\rightarrow c \mid f \mid i \mid bE \mid cS \mid dZ \mid eE \mid fS \mid gZ \mid hE \mid iS \mid jZ \end{aligned}$$

- Welcher Zusammenhang besteht zwischen  $G_1$  und  $G_2$ ?
- Welchem Chomsky-Typ entsprechen  $\mathcal{L}(G_1)$  und  $\mathcal{L}(G_2)$ ?
- Für welche Werte  $n \in \mathbb{N}$  ist das Wort  $b(abcdefghijkl)^n$  in  $G_1$  oder  $G_2$  ableitbar?

**Aufgabe 4.10**

Die Grammatiken

**Webcode  
4878** $G_1 := (\{S, A\}, \{0, \dots, 9\}, P_1, S)$  und  $G_2 := (\{S, E, Z\}, \{0, \dots, 9\}, P_2, S)$ 

seien durch die folgenden Produktionen definiert:

■ Produktionenmenge  $P_1$ 

$$\begin{aligned} S &\rightarrow A0 \mid A2 \mid A4 \mid A6 \mid A8 \\ A &\rightarrow \varepsilon \mid A0 \mid A1 \mid A2 \mid A3 \mid A4 \mid A5 \mid A6 \mid A7 \mid A8 \mid A9 \end{aligned}$$

■ Produktionenmenge  $P_2$ 

$$\begin{aligned} S &\rightarrow 0 \mid 3 \mid 6 \mid 9 \mid 1Z \mid 2E \mid 3S \mid 4Z \mid 5E \mid 6S \mid 7Z \mid 8E \mid 9S \\ E &\rightarrow 1 \mid 4 \mid 7 \mid 1S \mid 2Z \mid 3E \mid 4S \mid 5Z \mid 6E \mid 7S \mid 8Z \mid 9E \\ Z &\rightarrow 2 \mid 5 \mid 8 \mid 1E \mid 2S \mid 3Z \mid 4E \mid 5S \mid 6Z \mid 7E \mid 8S \mid 9Z \end{aligned}$$

Welche numerischen Eigenschaften erfüllen die erzeugbaren Ziffernfolgen?

**Aufgabe 4.11**Definieren Sie drei Grammatiken  $G_1$ ,  $G_2$  und  $G_3$  mit den folgenden Eigenschaften:**Webcode  
4298**

- a)  $G_1$  erzeugt alle Ziffernfolgen, deren Dezimalwert durch 4 teilbar ist.
- b)  $G_2$  erzeugt alle Ziffernfolgen, deren Dezimalwert durch 5 teilbar ist.
- c)  $G_3$  erzeugt alle Ziffernfolgen, deren Dezimalwert durch 6 teilbar ist.

**Aufgabe 4.12**

In diesem Kapitel haben Sie mit

**Webcode  
4114**

$$L_{\text{fool}} := \{b^k c^l d^m \mid k, l, m \in \mathbb{N}\} \cup \{a^m b^n c^n d^n \mid m, n \in \mathbb{N}\}$$

eine Sprache kennengelernt, die nicht kontextfrei ist, aber dennoch alle innerhalb des Pumping-Lemmas getroffenen Aussagen erfüllt. War es wirklich notwendig, die Sprache so kompliziert zu wählen oder hätten wir die gleiche Betrachtung an einer der folgenden Wortmengen durchführen können?

a)  $L'_{\text{fool}} := \{a^m b^n c^n d^n \mid m, n \in \mathbb{N}\}$

b)  $L''_{\text{fool}} := \{a^m b^n c^n d^n \mid m \in \mathbb{N}_0, n \in \mathbb{N}\}$

Für diese Aufgabe ist die Grammatik  $G = (\{S, A, B\}, \{0, 1\}, P, S)$  gegeben. Die Menge der Produktionen  $P$  lautet wie folgt:

$$\begin{array}{l} S \rightarrow AB \mid BAB \mid B0 \\ A \rightarrow BA \mid 0 \\ B \rightarrow 00 \mid 0AB \mid AB0 \mid ABAB \mid 1 \end{array}$$

- a) Lässt sich in  $G$  das leere Wort ableiten?
- b) Formen Sie die Grammatik in Chomsky-Normalform um.
- c) Prüfen Sie mit Hilfe des CYK-Algorithmus nach, ob das Wort 110100 in  $\mathcal{L}(G)$  enthalten ist. Füllen Sie hierzu die nachstehende Tabelle aus:

	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
$j = 1$	1	1	0	1	0	0
$j = 2$						
$j = 3$						
$j = 4$						
$j = 5$						
$j = 6$						

In diesem Kapitel haben wir herausgearbeitet, dass die Sprache

$$L_{C1} = \{a^n b^n c^n \mid n \in \mathbb{N}\}$$

durch die folgende kontextsensitive Grammatik erzeugt wird:

$$\begin{array}{lll} S \rightarrow ABC & CB \rightarrow BC & Aa \rightarrow aa \\ S \rightarrow SABC & CA \rightarrow AC & bB \rightarrow bb \\ BA \rightarrow AB & AB \rightarrow ab & cC \rightarrow cc \end{array}$$

Erzeugen Sie eine reduzierte Grammatik, die nur 3 Nonterminale besitzt und die gleiche Sprache erzeugt.

### Aufgabe 4.13



Webcode

4411

### Aufgabe 4.14



Webcode

4102



## 5 Endliche Automaten

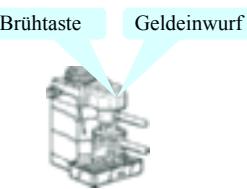
---

In diesem Kapitel werden Sie ...

- den zentralen Begriff des endlichen Automaten kennen lernen,
- den Unterschied zwischen Akzeptoren und Transduktoren verstehen,
- deterministische Automaten um nichtdeterministische Zustandsübergänge anreichern,
- das klassische Automatenmodell zu einer Kellermaschine erweitern,
- den Zusammenhang zwischen Automaten und formalen Sprachen herstellen,
- in Petri-Netzen und zellulären Automaten zwei alternative Automatenmodelle erkennen.

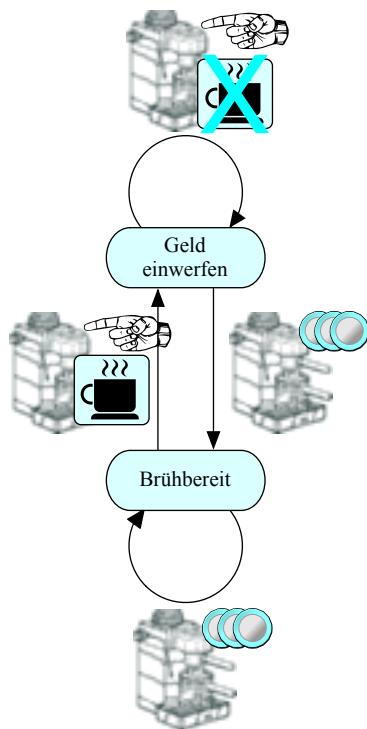


■ Aufbau



Bevor Kaffee gebrüht werden kann, muss zunächst eine Münze in den Geldschlitz geworfen werden. Anschließend kann die Maschine mit einem Druck auf die Brühtaste gestartet werden.

■ Zustandsdiagramm



**Abbildung 5.1:** Aufbau und Funktionsweise einer primitiven Kaffeemaschine

## 5.1 Begriffsbestimmung

Viele technische Systeme arbeiten ereignisbasiert; sie warten auf das Eintreten eines äußeren Ereignisses (*Ursache*) und reagieren darauf mit einer fest definierten Aktion (*Wirkung*). Wie die Reaktion im Einzelnen aussieht, wird zum einen durch das Ereignis selbst und zum anderen durch den *Zustand* bestimmt, in dem sich das System aktuell befindet. Der Zustand ist das Gedächtnis des Systems und macht es möglich, die Ereignishistorie in der Reaktionsberechnung zu berücksichtigen. Insgesamt hat ein Ereignis damit zwei Auswirkungen: Zum einen veranlasst es das System zu einer nach außen sichtbaren Reaktion, zum anderen kann es zu einem nach außen unsichtbaren Wechsel des internen Zustands führen.

Die Komplexität der entstehenden Interaktionsmuster nimmt mit der wachsenden Anzahl der internen Zustände stark zu und verlangt nach einer adäquaten Beschreibungsform. Eine weit verbreitete Darstellungsmöglichkeit, um das Ein- und Ausgabeverhalten eines Systems übersichtlich zu beschreiben, sind *Zustandsdiagramme*.

Das in Abbildung 5.1 exemplarisch abgebildete Zustandsdiagramm modelliert das Verhalten eines primitiven Kaffeautomaten, der über einen Münzeinwurfschlitz und einen Knopf zum Starten der Brüheinheit verfügt. Wie der Automat auf das Drücken des Brühknopfes reagiert, hängt davon ab, in welchem von zwei Zuständen er sich gegenwärtig befindet. Im Zustand „Geld einwerfen“ wird der Knopfdruck ignoriert, während im Zustand „Brühbereit“ die Brüheinheit gestartet wird. Der Zustandswechsel erfolgt ebenfalls ereignisgesteuert. Der Zustand „Brühbereit“ wird erst nach dem Einwurf einer Münze eingenommen und nach Betätigung der Brühtaste wieder verlassen.

Das beschriebene Beispiel ist eines von vielen und lässt sich nahezu beliebig ersetzen. Abstrahieren wir von der konkreten Funktion des modellierten Systems, so finden wir in allen Beispielen stets die gleiche Vorgehensweise wieder: Das Systemverhalten wird durch ein Zustandsmodell beschrieben, das zu jeder Zeit bestimmt, mit welcher Aktion auf ein Ereignis reagiert wird.

Mit den *endlichen Automaten* gibt uns die theoretische Informatik ein Instrument an die Hand, um (endliche) Zustandsmodelle wie dieses formal zu erfassen und systematisch zu analysieren. Die Modellierung technischer Systeme ist dabei eine wichtige, aber nicht die einzige Anwendung. Wie wir später sehen werden, lassen sich auch viele sprachtheoretische Fragestellungen auf diesen Beschreibungsformalismus abbilden.

Endliche Automaten kommen in verschiedenen Spielarten vor, von denen wir eine ganze Reihe in den nächsten Abschnitten detailliert untersuchen werden. Bevor wir damit beginnen, wollen wir versuchen, vorab ein wenig Ordnung in das drohende Chaos zu bringen. Grundsätzlich lassen sich zwei Automatentypen voneinander unterscheiden:

### ■ Akzeptoren

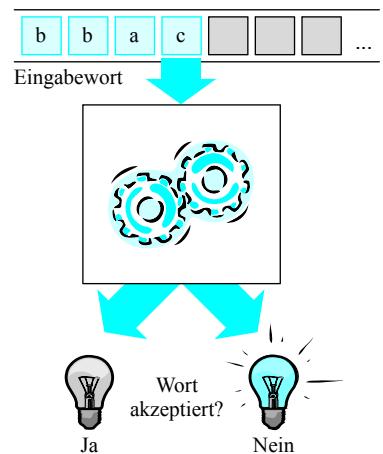
Endliche Automaten dieses Typs nehmen eine Zeichenfolge  $\omega$  entgegen und entscheiden im Zuge einer Ja-Nein-Entscheidung, ob  $\omega$  ein gültiges Eingabewort ist (vgl. Abbildung 5.2 oben). Unabhängig von der Länge der Eingabe produzieren Akzeptoren immer eine binäre Antwort; insbesondere wird im Gegensatz zu Transduktoren kein Ausgabewort erzeugt. Die Menge aller Wörter, die von einem endlichen Automaten  $A$  mit der Antwort „Ja“ quittiert werden, bildet die von  $A$  akzeptierte Sprache  $\mathcal{L}(A)$ . Wie die nachfolgenden Untersuchungen zeigen werden, sind die von endlichen Automaten akzeptierten Sprachen eng mit den in Kapitel 4 eingeführten Sprachklassen verbunden.

### ■ Transduktoren

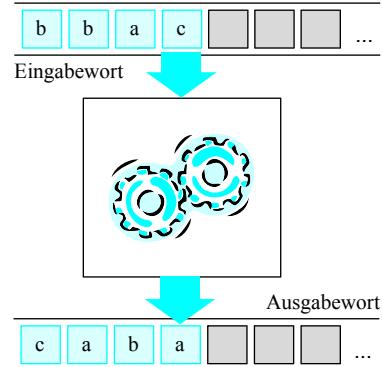
Ein Transduktor ist eine abstrakte Maschine, die eine Zeichenfolge  $\omega$  von einem Eingabeband liest und daraus eine Folge von Ausgabezeichen generiert. In Abhängigkeit der verwendeten Zustandsübergangsbedingungen werden *Mealy-Automaten* und *Moore-Automaten* unterschieden. Von außen betrachtet folgt ihre Arbeitsweise dem gleichen sequenziellen Schema: Für jedes in einem Berechnungsschritt eingelesene Zeichen wird ein einzelnes Zeichen auf das Ausgabeband geschrieben. Beide sind damit nichts anderes als Übersetzer, die eine Eingabesequenz in eine Ausgabesequenz gleicher Länge transformieren (vgl. Abbildung 5.2 unten). Transduktoren spielen eine gewichtige Rolle im Hardware-Entwurf, da sich jede synchron getaktete Schaltung durch einen Mealy- oder einen Moore-Automaten beschreiben lässt.

Im direkten Vergleich zeigen Akzeptoren einen einfacheren Aufbau als Transduktoren und werden aus diesem Grund in den nachfolgenden Abschnitten zuerst behandelt. In Abschnitt 5.2 werden wir das Konzept des Akzeptors zunächst in seiner Reinform einführen und anschließend in den Abschnitten 5.3 bis 5.5 um nichtdeterministisches Verhalten und einen Kellerspeicher ergänzen. In Abschnitt 5.6 werden wir mit dem Mealy- und dem Moore-Automaten die beiden wichtigsten Transduktorentypen im Detail vorstellen und an einem konkreten Beispiel herausarbeiten, wie sich Automaten auf systematische Weise in digitale Hardware-Schaltungen übersetzen lassen.

### ■ Akzeptor



### ■ Transduktor



**Abbildung 5.2:** Transduktoren und Akzeptoren im Vergleich

■ Automat

$$S := \{s_0, s_1, s_2\}$$

$$\Sigma := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

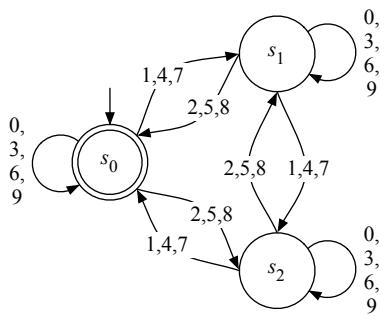
$$\delta(s_0, \sigma) := \begin{cases} s_0 & \text{für } \sigma \in \{0, 3, 6, 9\} \\ s_1 & \text{für } \sigma \in \{1, 4, 7\} \\ s_2 & \text{für } \sigma \in \{2, 5, 8\} \end{cases}$$

$$\delta(s_1, \sigma) := \begin{cases} s_1 & \text{für } \sigma \in \{0, 3, 6, 9\} \\ s_2 & \text{für } \sigma \in \{1, 4, 7\} \\ s_0 & \text{für } \sigma \in \{2, 5, 8\} \end{cases}$$

$$\delta(s_2, \sigma) := \begin{cases} s_2 & \text{für } \sigma \in \{0, 3, 6, 9\} \\ s_0 & \text{für } \sigma \in \{1, 4, 7\} \\ s_1 & \text{für } \sigma \in \{2, 5, 8\} \end{cases}$$

$$E := \{s_0\}$$

■ Zustandsdiagramm



■ Legende



Startzustand



Endzustand

**Abbildung 5.3:** Deterministischer endlicher Automat mit drei Zuständen. Die eingelesene Ziffernfolge wird genau dann akzeptiert, wenn sie einer durch 3 teilbaren Dezimalzahl entspricht.

## 5.2 Deterministische Automaten

### 5.2.1 Definition und Eigenschaften

Wir beginnen mit der Definition des *deterministischen endlichen Akzeptors*, kurz *DEA*.



#### Definition 5.1 (Deterministischer endlicher Akzeptor)

Ein deterministischer endlicher Akzeptor (*deterministic finite state machine*), kurz *DEA*, ist ein 5-Tupel  $(S, \Sigma, \delta, E, s_0)$ . Er besteht aus

- der endlichen *Zustandsmenge*  $S$ ,
- dem endlichen *Eingabealphabet*  $\Sigma$ ,
- der *Zustandsübergangsfunktion*  $\delta : S \times \Sigma \rightarrow S$ ,
- der Menge der *Endzustände* (*Finalzustände*)  $E \subseteq S$  und
- dem *Startzustand*  $s_0 \in S$ .

Zu Beginn befindet sich jeder Automat in seinem Startzustand  $s_0$ . Wird ein Akzeptor mit dem Eingabewort

$$\omega = \sigma_0 \sigma_1 \sigma_2 \dots \sigma_n \quad (5.1)$$

stimuliert, so durchläuft er nacheinander die folgenden Zustände:

$$s_0, s_1, s_2, \dots, s_{n+1} \quad \text{mit } s_{i+1} = \delta(s_i, \sigma_i) \quad (5.2)$$

Nachdem das letzte Zeichen  $\sigma_n$  verarbeitet wurde, hält der Automat im Zustand  $s_{n+1}$  an. Das Wort  $\omega$  gilt genau dann als akzeptiert, wenn der zuletzt eingenommene Zustand in der Menge  $E$  der Endzustände enthalten ist. Die von einem *DEA*  $A$  akzeptierte Sprache  $\mathcal{L}(A)$  lässt sich damit wie folgt beschreiben:

$$\mathcal{L}(A) = \{\sigma_0 \sigma_1 \dots \sigma_n \in \Sigma^* \mid \delta(\dots \delta(\delta(s_0, \sigma_0), \sigma_1), \dots, \sigma_n) \in E\} \quad (5.3)$$

Ob die Sprache  $L$  das leere Wort  $\epsilon$  enthält, lässt sich direkt an der Menge der Endzustände ablesen.  $\epsilon$  wird genau dann akzeptiert, wenn der Startzustand selbst ein Endzustand ist.

Als Beispiel betrachten wir den endlichen Automaten in Abbildung 5.3. Er besteht aus insgesamt drei Zuständen und kann als Eingabe eine

beliebige Folge von Dezimalziffern verarbeiten. Der Automat ist so konstruiert, dass er sich genau dann im Endzustand  $s_0$  befindet, wenn die eingelesene Ziffernfolge einer durch drei teilbaren Dezimalzahl entspricht. Die Funktionsweise basiert auf der zahlentheoretischen Erkenntnis, dass eine Dezimalzahl genau dann durch 3 teilbar ist, wenn es ihre Quersumme ist. Jetzt wird auf einen Schlag die Bedeutung der Zustände  $s_0$ ,  $s_1$  und  $s_2$  klar. Der Zustand  $s_0$  wird genau dann eingenommen, wenn die bisher eingelesene Ziffernfolge ohne Rest durch 3 teilbar ist. In den Zuständen  $s_1$  und  $s_2$  befindet sich der Akzeptor genau dann, wenn die Division durch 3 den ganzzahligen Rest 1 bzw. 2 ergibt. Die eingelesene Ziffernfolge entspricht damit genau dann einer durch 3 teilbaren Dezimalzahl, wenn sich der Automat am Ende wieder im Startzustand befindet.

Für die später angestellten Untersuchungen ist es ratsam, das Automatenverhalten ein wenig formaler zu charakterisieren, als wir es mit den Gleichungen (5.1) bis (5.3) bereits getan haben. Den Schlüssel hierzu bilden der Begriff der *Konfiguration* und die darauf definierte Übergangsrelation  $\rightarrow_A$ :



### Definition 5.2 (Konfiguration (DEA))

Mit  $A = (S, \Sigma, \delta, E, s_0)$  sei ein deterministischer endlicher Automat gegeben. Jedes Tupel  $(s, \omega)$  mit  $s \in S$  und  $\omega \in \Sigma^*$  heißt *Konfiguration* von  $A$ . Die Übergangsrelation  $\rightarrow_A$  definieren wir wie folgt:

$$(s_0, \sigma_0 \sigma_1 \dots \sigma_n) \rightarrow_A (s_1, \sigma_1 \dots \sigma_n) : \Leftrightarrow s_1 = \delta(s_0, \sigma_0)$$

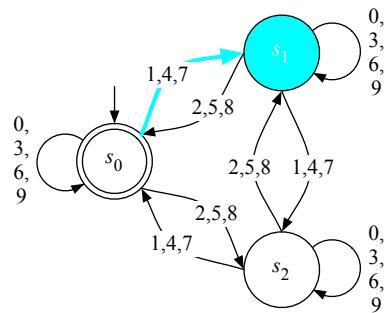
Geht aus dem Kontext hervor, um welchen Automaten es sich handelt, so schreiben wir verkürzend  $\rightarrow$  anstelle von  $\rightarrow_A$ .

Grob gesagt entspricht eine Konfiguration dem aktuellen Verarbeitungszustand des Automaten, der durch den aktuell eingenommenen Zustand und das einzulesende Restwort vollständig beschrieben wird. Mit Hilfe des Konfigurationsbegriffs lässt sich die von einem Automaten  $A$  akzeptierte Sprache  $\mathcal{L}(A)$  wie folgt charakterisieren:

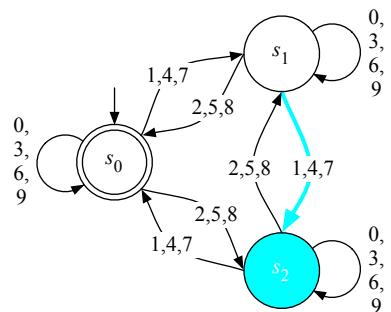
$$\mathcal{L}(A) := \{\omega \in \Sigma^* \mid \text{Für ein } s_e \in E \text{ gilt } (s_0, \omega) \rightarrow (s_e, \varepsilon)\} \quad (5.4)$$

Abbildung 5.4 demonstriert, wie sich die Konfiguration unseres Beispielautomaten während der Verarbeitung des Eingabeworts 147 ändert. Da wir einen deterministischen Automaten vor uns haben, ist der im nächsten Schritt einzunehmende Folgezustand jederzeit eindeutig definiert und der in Gleichung (5.4) vorkommende Endzustand  $s_e$  damit ebenfalls eindeutig festgelegt.

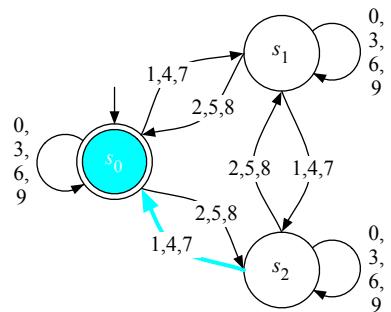
■  $(s_0, 147) \rightarrow (s_1, 47)$



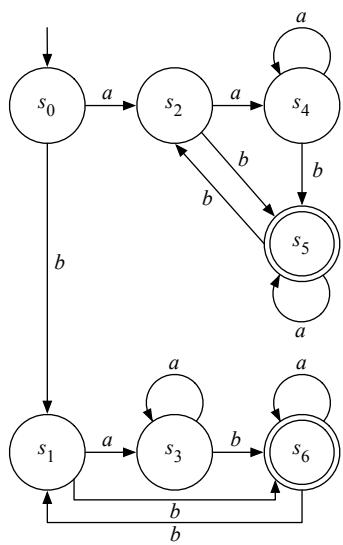
■  $(s_1, 47) \rightarrow (s_2, 7)$



■  $(s_2, 7) \rightarrow (s_0, \varepsilon)$



**Abbildung 5.4:** Konfigurationsübergänge für das Beispielwort 147



**Abbildung 5.5:** Ausgangsbeispiel für die Automatenminimierung

## 5.2.2 Automatenminimierung

Endliche Automaten sind keine kanonische Beschreibungsform für formale Sprachen, d. h., zu jedem Automaten  $A$  existieren weitere, die dieselbe Sprache akzeptieren. Zwei Automaten  $A_1$  und  $A_2$  mit  $\mathcal{L}(A_1) = \mathcal{L}(A_2)$  bezeichnen wir als *äquivalent*. Äquivalente Automaten können große strukturelle Unterschiede aufweisen und sich insbesondere in der Anzahl der Zustände erheblich unterscheiden. Ein Automat heißt *reduziert*, wenn kein anderer Automat existiert, der die gleiche Sprache akzeptiert und mit weniger Zuständen auskommt. Aufgrund ihrer Minimalität sind reduzierte Automaten von besonderem Interesse und entsprechend groß ist das Verlangen nach einem Verfahren, das einen gegebenen Automaten in eine reduzierte Form überführt.

Die Grundidee der Automatenreduktion besteht darin, *äquivalente Zustände* zu bestimmen. Grob gesprochen sind zwei Zustände  $s_1$  und  $s_2$  genau dann äquivalent, wenn sie von außen nicht unterschieden werden können. Dies ist genau dann der Fall, wenn die Antwort („akzeptiert“ oder „nicht akzeptiert“) für ein Wort  $\omega$  stets die gleiche ist, egal ob wir in  $s_1$  oder in  $s_2$  starten. Die Zustandsäquivalenz lässt sich auf den Begriff der *k-Äquivalenz* zurückführen, die das oben Gesagte auf Wörter  $\omega$  mit  $|\omega| \leq k$  beschränkt. Formal definieren wir die umrissenen Äquivalenzbegriffe wie folgt:



### Definition 5.3 (Zustandsäquivalenz, Bisimulation)

Sei  $A = (S, \Sigma, \delta, E, s_0)$  ein endlicher deterministischer Akzeptor. Die *k-Äquivalenz* zwischen zwei Zuständen  $s_1$  und  $s_2$ , geschrieben als  $s_1 \sim_k s_2$ , definieren wir wie folgt:

$$s_1 \sim_0 s_2 : \Leftrightarrow s_1, s_2 \text{ sind beide in } E \text{ oder beide nicht in } E$$

$$s_1 \sim_{k+1} s_2 : \Leftrightarrow \text{Für alle } \sigma \in \Sigma \text{ gilt } \delta(s_1, \sigma) \sim_k \delta(s_2, \sigma)$$

Gilt  $s_1 \sim_k s_2$  für alle  $k \in \mathbb{N}_0$ , so heißen  $s_1$  und  $s_2$  *äquivalent*, in Zeichen  $s_1 \sim s_2$ . Die Relation  $\sim$  heißt *Bisimulation*.

Der rekursive Charakter von Definition 5.3 zeigt den Weg auf, wie wir alle bisimulativen Zustände eines gegebenen Automaten berechnen können. Ausgehend von der initialen Zustandsmenge bestimmen wir im ersten Schritt alle 0-äquivalenten Zustände. Als Ergebnis erhalten wir zwei Äquivalenzklassen. In der ersten finden wir alle Finalzustände, in der zweiten die restlichen Zustände wieder. Jetzt werden die Klassen in einem iterativen Prozess weiter unterteilt. Hierzu bestimmen wir

■ Übergangstabelle

	$s_0$	$s_1$	$s_2$	$s_3$	$s_4$	$s_5$	$s_6$
$a$	$s_1$	$s_3$	$s_4$	$s_3$	$s_4$	$s_5$	$s_6$
$b$	$s_2$	$s_5$	$s_6$	$s_5$	$s_6$	$s_1$	$s_2$

■ Erste Partition

	$s_0$	$s_1$	$s_2$	$s_3$	$s_4$	$s_5$	$s_6$
	$P_1$				$P_2$		
$a$	$s_1, P_1$	$s_3, P_1$	$s_4, P_1$	$s_3, P_1$	$s_4, P_1$	$s_5, P_2$	$s_6, P_2$
$b$	$s_2, P_1$	$s_5, P_2$	$s_6, P_2$	$s_5, P_2$	$s_6, P_2$	$s_1, P_1$	$s_2, P_1$

■ Zweite Partition

	$s_0$	$s_1$	$s_2$	$s_3$	$s_4$	$s_5$	$s_6$
	$P_1$	$P_2$			$P_3$		
$a$	$s_1, P_2$	$s_3, P_2$	$s_4, P_2$	$s_3, P_2$	$s_4, P_2$	$s_5, P_3$	$s_6, P_3$
$b$	$s_2, P_2$	$s_5, P_3$	$s_6, P_3$	$s_5, P_3$	$s_6, P_3$	$s_1, P_2$	$s_2, P_2$

**Abbildung 5.6:** Schrittweise Reduktion des endlichen Automaten aus Abbildung 5.5. Im ersten Schritt werden die Zustände in zwei Äquivalenzklassen aufgeteilt, so dass sich alle Finalzustände in der einen und die restlichen Zustände in der anderen wiederfinden. Nach diesem Schritt sind alle 0-äquivalenten Zustände bestimmt. Anschließend werden die Äquivalenzklassen in einem iterativen Prozess weiter aufgeteilt. Nach der ersten Iteration sind alle in einer Klasse verbleibenden Zustände paarweise 1-äquivalent, nach der zweiten Iteration paarweise 2-äquivalent und so fort. Machen wir mit der Aufteilung so lange weiter, bis ein Fixpunkt erreicht ist, so sind die Zustände in den verbleibenden Äquivalenzklassen zueinander äquivalent. Den reduzierten Automaten können wir jetzt sofort konstruieren, indem wir für jede Äquivalenzklasse einen separaten Zustand erzeugen.

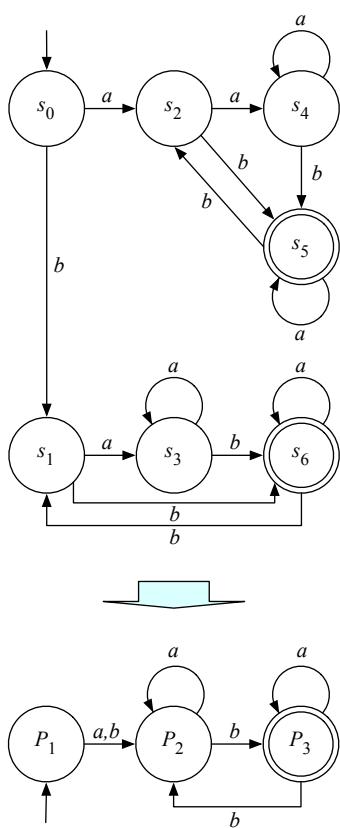
für jeden Zustand zunächst die Äquivalenzklassen seiner Folgezustände. Zwei Zustände belassen wir nur dann in derselben Äquivalenzklasse, wenn die Äquivalenzklassen ihrer Folgezustände identisch sind. Auf diese Weise haben wir nach der ersten Iteration alle 1-äquivalenten Zustände, nach der zweiten Iteration alle 2-äquivalenten Zustände isoliert und so fort. Nach spätestens  $|S|$  Verfeinerungsschritten lassen sich keine neuen Äquivalenzklassen mehr bilden. Jetzt lässt sich aus der berechneten Partition der reduzierte Automat konstruieren, indem wir für jede Äquivalenzklasse einen eigenen Zustand erzeugen und entsprechend der berechnenden Übergangstabelle miteinander verbinden.

Wir wollen das Gesagte für den Automaten aus Abbildung 5.5 in die Tat umsetzen. Um den reduzierten Automaten zu konstruieren, stellen wir zunächst die Übergangstabelle auf (vgl. Abbildung 5.6 obere Tabelle). Anschließend separieren wir die Finalzustände und erhalten im ersten Verfeinerungsschritt die folgenden beiden Äquivalenzklassen:

$$P_1 = \{s_0, s_1, s_2, s_3, s_4\} \quad (5.5)$$

$$P_2 = \{s_5, s_6\} \quad (5.6)$$

Die mittlere Tabelle in Abbildung 5.6 macht die gebildeten Äquivalenzklassen sichtbar. Neben den Zuständen sind in der Tabelle zusätzlich



**Abbildung 5.7:** Minimierter Akzeptor. Die Anzahl der Zustände konnte von 7 auf 3 reduziert werden, ohne die akzeptierte Sprache zu verändern.

die Nummern der Äquivalenzklassen notiert, in die der Automat bei der Verarbeitung eines neuen Eingabezeichens wechselt. An den abgebildeten Nummern lässt sich sofort erkennen, welche Partitionen im nächsten Verfeinerungsschritt gebildet werden müssen. So werden in unserem Beispiel die Zustände in  $P_1$  in zwei weitere Äquivalenzklassen unterteilt, während die Äquivalenzklasse  $P_2$  unverändert bestehen bleibt. Damit erhalten wir die folgende Verfeinerung:

$$P_1 = \{s_0\} \quad (5.7)$$

$$P_2 = \{s_1, s_2, s_3, s_4\} \quad (5.8)$$

$$P_3 = \{s_5, s_6\} \quad (5.9)$$

An dieser Stelle haben wir einen *Fixpunkt* erreicht, da weitere Verfeinerungsschritte keine neuen Äquivalenzklassen hervorbringen. Zusammengefasst kommen wir zu folgendem Ergebnis:

- $s_0$  ist zu keinem anderen Zustand äquivalent und kann nicht zusammengefasst werden.
- $s_1, \dots, s_4$  sind paarweise bisimulativ und lassen sich zu einem einzigen Zustand verschmelzen.
- $s_5, s_6$  sind bisimulativ und werden ebenfalls zu einen einzigen Zustand zusammengefasst.

Wie in Abbildung 5.7 gezeigt, ist es uns mit Hilfe des vorgestellten Minimierungsverfahrens gelungen, die 7 Zustände des ursprünglichen Automaten auf nur noch 3 zu reduzieren.

## 5.3 Nichtdeterministische Automaten

### 5.3.1 Definition und Eigenschaften

Alle bisher betrachteten Automaten waren *deterministisch*, d.h., der Folgezustand war durch das gelesene Eingabezeichen und den jeweils eingenommenen Zustand immer eindeutig bestimmt. Für einige Anwendungsfälle ist es wünschenswert, sich von der Idee des deterministischen Zustandsübergangs zu verabschieden (vgl. Abbildung 5.8). Dies können wir erreichen, indem wir die Übergangsfunktion  $\delta$  durch eine Berechnungsvorschrift ersetzen, die aus dem gelesenen Eingabezeichen

und dem aktuellen Zustand eine Menge potenzieller Nachfolger berechnet. Formal setzt sich ein solcher *nichtdeterministischer endlicher Akzeptor*, kurz NEA, aus den folgenden Komponenten zusammen:



#### Definition 5.4 (Nichtdeterministischer endlicher Akzeptor)

Ein nichtdeterministischer endlicher Automat (*nondeterministic finite state machine*), kurz NEA, ist ein 5-Tupel  $(S, \Sigma, \delta, E, s_0)$ . Er besteht aus

- der endlichen Zustandsmenge  $S$ ,
- dem endlichen Eingabealphabet  $\Sigma$ ,
- der Zustandsübergangsfunktion  $\delta : S \times \Sigma \rightarrow 2^S$ ,
- der Menge der Endzustände (Finalzustände)  $E \subseteq S$  und
- dem Startzustand  $s_0 \in S$ .

Genau wie im deterministischen Fall startet der Akzeptor im Zustand  $s_0$  und liest das Eingabewort zeichenweise ein. Mit jedem gelesenen Zeichen  $\sigma$  wechselt er aus dem aktuellen Zustand  $s_i$  in einen Folgezustand  $s_{i+1}$  aus der Menge  $\delta(s_i, \sigma)$ . Somit existieren für jede Eingabesequenz

$$\omega = \sigma_0, \sigma_1, \sigma_2, \dots, \sigma_n \quad (5.10)$$

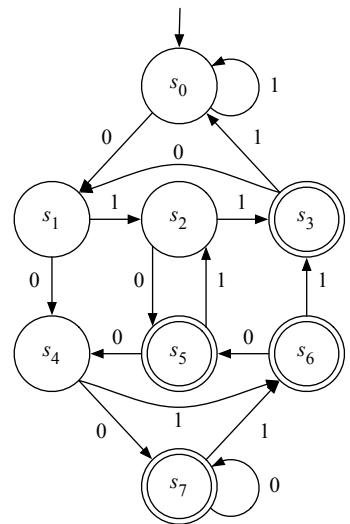
potenziell mehrere Zustandsfolgen

$$s_0, s_1, s_2, \dots, s_{n+1} \quad \text{mit} \quad s_{i+1} \in \delta(s_i, \sigma_i), \quad (5.11)$$

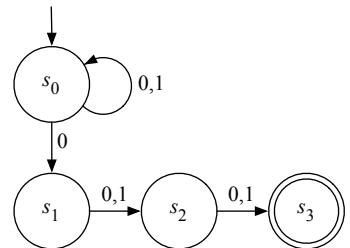
die der Automat durchlaufen kann. Wir vereinbaren, dass ein Wort  $\omega$  genau dann akzeptiert wird, wenn mindestens eine Zustandsfolge in einem Finalzustand endet. Hinter dieser Festlegung verbirgt sich die Modellvorstellung, dass der Automat eine erfolgreiche Zustandsfolge gewissermaßen erraten kann, d. h., er wählt an jedem Entscheidungspunkt einen Pfad aus, der in einen Finalzustand führt. In der Literatur wird zur Veranschaulichung dieser Idee gerne die Metapher des *Orakels* bemüht, das den Automaten an allen Entscheidungspunkten den richtigen Weg weist.

Bachten Sie, dass ein NEA unter Umständen überhaupt keine Sequenz der Form (5.11) hervorbringt. Verantwortlich hierfür ist die Menge  $\delta(s, \sigma)$ , die ausdrücklich auch die leere Menge sein darf. Ist  $\delta(s, \sigma) = \emptyset$ , so gerät die Abarbeitung im Zustand  $s$  ins Stocken, da für das aktuell

■ DEA

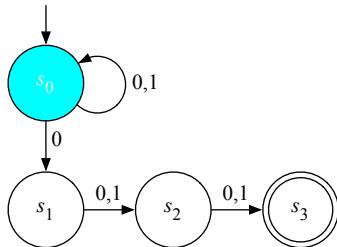


■ NEA

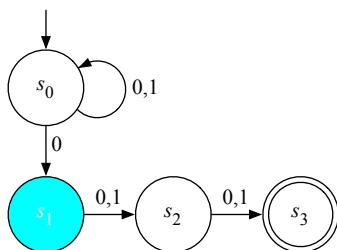


**Abbildung 5.8:** Einige Sprachen lassen sich mit NEAs erheblich einfacher beschreiben als mit DEAs, hier demonstriert am Beispiel der Sprache aller Bitvektoren, deren drittletzte Ziffer gleich 0 ist. Während der deterministische Automat hierzu 8 Zustände benötigt, kommt die nichtdeterministische Variante mit nur 4 Zuständen aus.

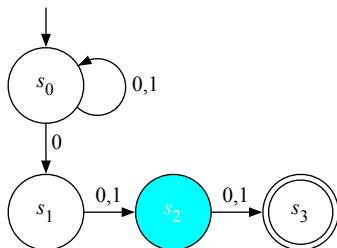
- Möglichkeit 1:  $s_0 \rightarrow s_0 \rightarrow s_0 \rightarrow s_0$



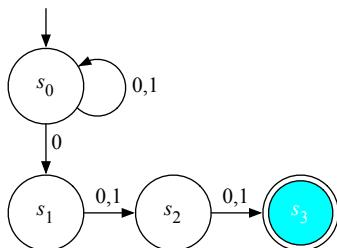
- Möglichkeit 2:  $s_0 \rightarrow s_0 \rightarrow s_0 \rightarrow s_1$



- Möglichkeit 3:  $s_0 \rightarrow s_0 \rightarrow s_1 \rightarrow s_2$



- Möglichkeit 4:  $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3$



**Abbildung 5.9:** Die vier möglichen Konfigurationsübergänge für das Eingabewort 000

eingelesene Zeichen  $\sigma$  keine Folgezustände existieren. In diesem Fall gilt das betrachtete Wort per Definition als nicht akzeptiert, unabhängig davon, ob der Zustand  $s$  selbst ein Endzustand ist oder nicht.

Um die von nichtdeterministischen Automaten akzeptierten Sprachen formal zu beschreiben, greifen wir, wie schon im Fall der deterministischen Automaten, auf den Begriff der *Konfiguration* zurück.



### Definition 5.5 (Konfiguration (NEA))

Mit  $A = (S, \Sigma, \delta, E, s_0)$  sei ein nichtdeterministischer endlicher Automat gegeben. Jedes Tupel  $(s, \omega)$  mit  $s \in S$  und  $\omega \in \Sigma^*$  heißt eine *Konfiguration* von  $A$ . Die Übergangsrelation  $\rightarrow_A$  definieren wir wie folgt:

$$(s_1, \sigma_0, \sigma_1, \dots, \sigma_n) \rightarrow (s_2, \sigma_1, \dots, \sigma_n) : \Leftrightarrow s_2 \in \delta(s_1, \sigma_0)$$

Die Definition dieses Begriffs ist für beide Automatentypen nahezu identisch. Ein direkter Vergleich mit Definition 5.2 zeigt, dass sich einzige die Definition der Übergangsrelation  $\rightarrow$  geringfügig unterscheidet. Anstelle des Gleichheitssymbols taucht in der NEA-Definition das Elementsymbol  $\in$  auf.

Mit Hilfe des Konfigurationsbegriffs lässt sich die von einem nichtdeterministischen Automaten  $A$  akzeptierte Sprache  $\mathcal{L}(A)$  wie folgt charakterisieren:

$$\mathcal{L}(A) := \{\omega \in \Sigma^* \mid \text{Für ein } s_e \in E \text{ gilt } (s_0, \omega) \rightarrow (s_e, \varepsilon)\} \quad (5.12)$$

Obwohl die beiden Gleichungen (5.12) und (5.4) im Wortlaut identisch sind, ist der Zustand  $s_e$  im Falle von NEAs nicht mehr eindeutig bestimmt. Die Ursache ist in der Definition der Übergangsrelation  $\rightarrow$  verborgen, die ein nichtdeterministisches Übergangsverhalten beschreibt.

Als Beispiel sind in Abbildung 5.9 die vier möglichen Konfigurationsübergänge zusammengefasst, die der weiter oben eingeführte Beispielautomat für das Eingabewort 000 durchlaufen kann. Da der vierte Übergang in einem Finalzustand endet, wird das Eingabewort durch den Automaten akzeptiert.

### 5.3.2 Satz von Rabin, Scott

In Abschnitt 5.3.1 haben wir anhand einer konkreten Sprache herausgearbeitet, dass sich ein akzeptierender Automat deutlich einfacher be-

schreiben lässt, wenn wir nichtdeterministische Zustandsübergänge erlauben. Die angestellten Überlegungen werfen die Frage auf, ob die Menge der akzeptierbaren Sprachen durch den hinzugefügten Nichtdeterminismus vergrößert wird. Mit anderen Worten: Gibt es eine Sprache  $L$ , die von einem nichtdeterministischen Automaten akzeptiert werden kann, nicht jedoch von einem deterministischen?

Die Antwort auf diese Frage gibt der folgende Satz, der von Michael Oser Rabin und Dana Scott im Jahre 1959 in ihrer berühmten Arbeit „*Finite Automata and Their Decision Problems*“ bewiesen wurde [76].



### Satz 5.1 (Satz von Rabin und Scott)

Zu jedem nichtdeterministischen endlichen Automaten gibt es einen deterministischen endlichen Automaten, der die gleiche Sprache akzeptiert. Es gilt also:

$$\mathcal{L}(\text{NEA}) = \mathcal{L}(\text{DEA})$$

Um den Satz zu beweisen, werden wir darlegen, dass sich der Nichtdeterminismus eines NEAs beseitigen lässt, ohne die akzeptierte Sprache zu verändern. Konkret werden wir zeigen, wie sich aus einem nichtdeterministischen Akzeptor

$$A_{\text{NEA}} = (S, \Sigma, \delta, E, s_0) \quad (5.13)$$

ein deterministischer Akzeptor

$$A_{\text{DEA}} = (S', \Sigma, \delta', E', s'_0) \quad (5.14)$$

konstruieren lässt, der die gleiche Sprache akzeptiert.

Die Konstruktion basiert auf der Idee, die möglichen Zustände des NEAs gewissermaßen gleichzeitig zu besuchen. Hierzu definieren wir  $A_{\text{DEA}}$  so, dass seine Zustandsmenge gleich der Potenzmenge der NEA-Zustandsmenge ist. Befindet sich  $A_{\text{DEA}}$  beispielsweise im Zustand  $\{s_4, s_7\}$ , so bedeutet dies, dass sich  $A_{\text{NEA}}$  entweder im Zustand  $s_4$  oder im Zustand  $s_7$  aufhalten kann. Machen wir einen Zustand  $\{s_1, \dots, s_n\}$  des DEA genau dann zu einem Endzustand, wenn einer der Zustände  $s_1, \dots, s_n$  ein Endzustand des NEA ist, so akzeptieren beide die gleiche Sprache. Zusammengefasst führen die angestellten Überlegungen

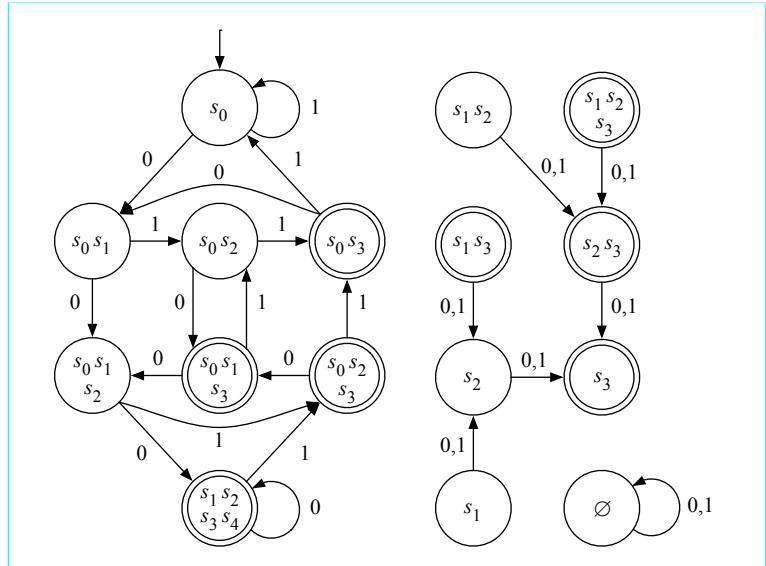
Michael O. Rabin wurde 1931 in Breslau geboren. Nach dem Studium an der Hebrew University in Jerusalem wechselte er 1953 an die Princeton University, die ihm 1956 den Doktorgrad verlieh. Seine akademische Karriere setzte er am neu gegründeten Thomas J. Watson Research Center fort. Im Jahre 1957 arbeitete er zusammen mit Dana Stewart Scott die Arbeit „*Finite Automata and Their Decision Problems*“ aus. Der ein Jahr jüngere Scott war ein Schüler von Alonzo Church und zu dieser Zeit noch mit seiner Promotion beschäftigt.

Rabin und Scott hatten als Erste die Idee, das Konzept des endlichen Automaten um nichtdeterministische Zustandsübergänge zu erweitern. In ihrer Originalarbeit aus dem Jahre 1959 charakterisieren sie den Begriff wie folgt:

*„A nondeterministic automaton is not a probabilistic machine but rather a machine with many choices in its moves. At each stage of its motion across a tape it will be at liberty to choose one of several new internal states. Of course, some sequence of choices will lead either to impossible situations from which no moves are possible or to final states not in the designated class F. We disregard all such failures, however, and agree to let the machine accept a tape if there is at least one winning combination of choices of states leading to a designated final state.“ [76]*

Mit ihrer Arbeit gelang Rabin und Scott der große Wurf. Zum einen erwies sich das eingeführte Begriffsgerüst in der Folgezeit als ein leistungsfähiges Instrument für die Beschreibung und die Analyse von Automaten und Sprachen. Zum anderen brachten sie mit dem Indeterminismus eine neuartige Denkrichtung ein, die heute weite Teile der theoretischen Informatik prägt. Im Jahre 1976 wurden Rabin und Scott für ihre richtungsweisende Arbeit mit dem Turing-Award geehrt.

**Abbildung 5.10:** Jeder NEA lässt sich in einen DEA übersetzen, der die gleiche Sprache akzeptiert. Der Kernidee der Transformation besteht darin, dem DEA eine Zustandsmenge zuzuweisen, die der Potenzmenge der NEA-Zustandsmenge entspricht. Die Zustandsübergangsfunktion definieren wir so, dass sich der aktuell eingenommene DEA-Zustand  $\{s_1, \dots, s_n\}$  aus allen Zuständen  $s_1, \dots, s_n$  zusammensetzt, die der NEA aufgrund des Nichtdeterminismus potentiell einnehmen kann. Machen wir  $\{s_1, \dots, s_n\}$  genau dann zu einem Endzustand, wenn einer der Zustände  $s_1, \dots, s_n$  ein Endzustand des NEA ist, so akzeptieren beide Automaten die gleiche Sprache. Angewendet auf den Beispiel-NEA aus Abbildung 5.8 ergibt sich der hier abgebildete Akzeptor.



zu dem folgendem Ergebnis:

$$S' := 2^S \quad (5.15)$$

$$\delta'(\{s_1, \dots, s_n\}, \sigma) := \bigcup_{i=1}^n \delta(s_i, \sigma) \quad (5.16)$$

$$E' := \{s \in S' \mid s \cap E \neq \emptyset\} \quad (5.17)$$

$$s'_0 := \{s_0\} \quad (5.18)$$

Abbildung 5.10 demonstriert die Automatenkonstruktion am Beispiel des weiter oben eingeführten NEAs. Genau wie der nichtdeterministische Originalautomat akzeptiert der erzeugte DFA alle Bitsequenzen, die an der drittletzten Stelle eine 0 enthalten.

Der Zustandsübergangsgraph macht deutlich, dass die Potenzmengenkonstruktion zu einer Reihe von Zuständen führt, die von dem Startzustand nicht erreichbar sind. Entfernen wir diese aus der Zustandsmenge, so verfügt der konstruierte DFA nur noch über 8 Zustände, ist aber immer noch deutlich größer als die ursprüngliche nichtdeterministische Variante. Ein vergleichender Blick zeigt überdies, dass der konstruierte Automat strukturell dem weiter oben eingeführten DFA aus Abbildung 5.8 entspricht. Zwei Automaten, die sich wie in unserem Beispiel ausschließlich in der Benennung ihrer Zustände unterscheiden, heißen *isomorph*. Offenbar sind zwei isomorphe Automaten immer auch äquivalent, aber nicht umgekehrt.

### 5.3.3 Epsilon-Übergänge

In Abschnitt 5.3.1 haben wir eine Sprache kennen gelernt, die sich mit Hilfe deterministischer Automaten nur sehr umständlich beschreiben lässt. Die Einführung nichtdeterministischer Zustandsübergänge hat es uns ermöglicht, dieselbe Sprache auf deutlich elegantere Weise zu charakterisieren. In diesem Abschnitt werden wir das Konzept des nichtdeterministischen Automaten um  $\varepsilon$ -Übergänge anreichern und so zu einer noch handlicheren Beschreibungsform gelangen. Auch hier wird sich zeigen, dass die Erweiterung keinen Einfluss auf die Ausdrucksstärke hat, da sich jeder  $\varepsilon$ -Automat auf einen äquivalenten NEA oder DEA reduzieren lässt.



#### Definition 5.6 (Nichtdeterministischer endlicher $\varepsilon$ -Akzeptor)

Ein nichtdeterministischer endlicher  $\varepsilon$ -Akzeptor, kurz  $\varepsilon$ -NEA, ist ein 5-Tupel  $(S, \Sigma, \delta, E, s_0)$ . Er besteht aus

- der endlichen Zustandsmenge  $S$ ,
- dem endlichen Eingabealphabet  $\Sigma$  mit  $\varepsilon \notin \Sigma$ ,
- der Zustandsübergangsfunktion  $\delta : S \times (\Sigma \cup \{\varepsilon\}) \rightarrow 2^S$ ,
- der Menge der Endzustände (Finalzustände)  $E \subseteq S$  und
- dem Startzustand  $s_0$ .

Die zusätzlich hinzugefügten  $\varepsilon$ -Übergänge beschreiben eine besondere Art des Zustandsübergangs. Dieser kann spontan erfolgen, d.h., ohne ein neues Eingabezeichen zu konsumieren. Was wir hierunter genau zu verstehen haben, fixieren wir in der folgenden Definition:



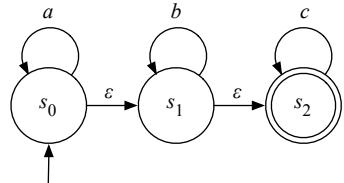
#### Definition 5.7 (Konfiguration ( $\varepsilon$ -NEA))

Mit  $A = (S, \Sigma, \delta, E, s_0)$  sei ein nichtdeterministischer endlicher  $\varepsilon$ -Akzeptor gegeben. Jedes Tupel  $(s, \omega)$  mit  $s \in S$  und  $\omega \in \Sigma^*$  heißt eine Konfiguration von  $A$ . Die Übergangsrelation  $\rightarrow$  definieren wir wie folgt:

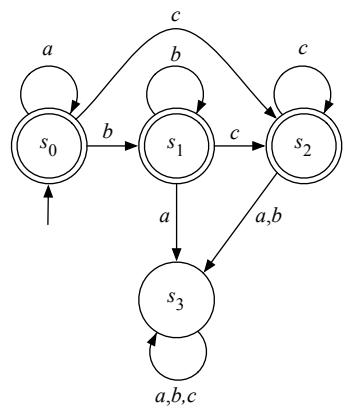
$$(s_1, \omega) \rightarrow (s_2, \omega) \Leftrightarrow s_2 \in \delta(s_1, \varepsilon)$$

$$(s_1, \sigma\omega) \rightarrow (s_2, \omega) \Leftrightarrow s_2 \in \delta(s_1, \sigma)$$

#### Nichtdeterministischer $\varepsilon$ -Akzeptor

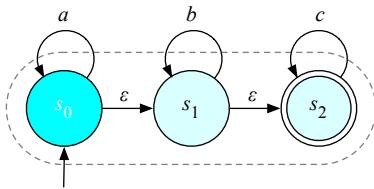


#### Deterministischer Akzeptor

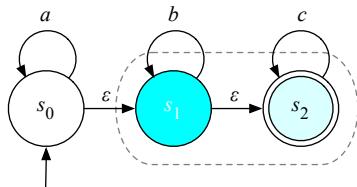


**Abbildung 5.11:** Viele Sprachen lassen sich mit  $\varepsilon$ -Automaten kompakter beschreiben als mit deterministischen Akzeptoren. Die dargestellten Automaten demonstrieren diese Eigenschaft am Beispiel der Sprache  $L = \{a^i b^j c^k \mid i, j, k \in \mathbb{N}_0\}$ .

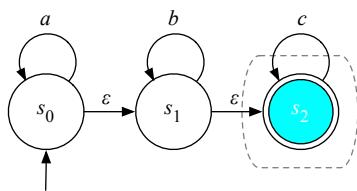
■  $\|s_0\|_\epsilon = \{s_0, s_1, s_2\}$



■  $\|s_1\|_\epsilon = \{s_1, s_2\}$



■  $\|s_2\|_\epsilon = \{s_2\}$



**Abbildung 5.12:**  $\epsilon$ -Hüllen unseres Beispielautomats

Die von einem  $\epsilon$ -Automaten  $A$  akzeptierte Sprache  $\mathcal{L}(A)$  ist wie folgt definiert:

$$\mathcal{L}(A) := \{\omega \in \Sigma^* \mid \text{Für ein } s_\epsilon \in E \text{ gilt } (s_0, \omega) \xrightarrow{\epsilon} (s_\epsilon, \epsilon)\} \quad (5.19)$$

Abbildung 5.11 (oben) demonstriert die Stärke des  $\epsilon$ -Prinzips am Beispiel der folgenden Sprache:

$$L = \{a^i b^j c^k \mid i, j, k \in \mathbb{N}_0\} \quad (5.20)$$

Akzeptiert wird auch das leere Wort, obwohl der Startzustand  $s_0$  selbst kein Endzustand ist. Die liebgewonnene Eigenschaft der anderen Automatentypen, dass das leere Wort  $\epsilon$  genau dann akzeptiert wird, wenn der Startzustand ein Finalzustand ist, wird von  $\epsilon$ -Automaten somit nicht mehr erfüllt.

Insgesamt erweisen sich  $\epsilon$ -Übergänge als überaus leistungsfähig, da wir mit ihrer Hilfe Auswahlen modellieren können, die kein Eingabezeichen konsumieren. Trotzdem lassen sich  $\epsilon$ -Übergänge, wie der DEA in Abbildung 5.11 (unten) bereits vermuten lässt, durch das Hinzufügen neuer Zustände eliminieren. In unserem Beispiel reicht ein weiterer Zustand aus, um die gleiche Sprache mit einem deterministischen Akzeptor ohne  $\epsilon$ -Übergänge zu akzeptieren.

Im Folgenden wollen wir ein Konstruktionsschema entwickeln, das aus jedem  $\epsilon$ -NEA systematisch einen DEA erzeugt, der die gleiche Sprache akzeptiert. Das Verfahren ist eine Erweiterung der Teilmengenkonstruktion aus Abschnitt 5.3.2, die  $\epsilon$ -Übergänge mitberücksichtigt. Eine wichtige Rolle wird der Begriff der  $\epsilon$ -Hülle eines Zustands  $s$  spielen, die wir kurz mit  $\|s\|_\epsilon$  bezeichnen:

$$\|s\|_\epsilon := \{s' \mid s \xrightarrow{\epsilon} s'\} \quad \text{mit} \quad s \xrightarrow{\epsilon} s' : \Leftrightarrow s' \in \delta(s, \epsilon) \quad (5.21)$$

Die eingeführte Relation  $\xrightarrow{\epsilon}$  stellt alle Zustände in Beziehung, die über einen  $\epsilon$ -Übergang direkt miteinander verbunden sind. Die  $\epsilon$ -Hülle entspricht der reflexiv transitiven Hülle dieser Relation und enthält damit neben  $s$  alle Elemente, die über eine beliebige Anzahl von  $\epsilon$ -Kanten von  $s$  aus erreichbar sind. Die  $\epsilon$ -Hüllen unseres Beispielautomaten sind in Abbildung 5.12 zusammengefasst. Beachten Sie an dieser Stelle, dass die  $\epsilon$ -Hüllen keine Äquivalenzrelation ist und damit nicht zu einer Partition der Zustandsmenge führt. Um dies zu erreichen, müsste  $\xrightarrow{\epsilon}$  zusätzlich die Eigenschaft der Symmetrie erfüllen.

Der Begriff der  $\epsilon$ -Hülle wird in Gleichung (5.21) für einzelne Zustände definiert. Wir wollen ihn in naheliegender Weise auf beliebige Zustandsmengen ausweiten und treffen die folgende Vereinbarung:

$$\|\{s_1, \dots, s_n\}\|_\epsilon := \bigcup_{i=1}^n \|s_i\|_\epsilon \quad (5.22)$$

Mit der geleisteten Vorarbeit sind wir in der Lage, die in Abschnitt 5.3.2 eingeführte Potenzmengenkonstruktion fast unverändert auf die Klasse der  $\varepsilon$ -Automaten zu übertragen. Für einen beliebigen  $\varepsilon$ -Akzeptor

$$A_{\varepsilon\text{-NEA}} = (S, \Sigma, \delta, E, s_0) \quad (5.23)$$

konstruieren wir einen äquivalenten DEA

$$A_{\text{DEA}} = (S', \Sigma, \delta', E', s'_0) \quad (5.24)$$

wie folgt:

$$S' := 2^S \quad (5.25)$$

$$\delta'(\{s_1, \dots, s_n\}, \sigma) := \|\cup_{i=1}^n \delta(s_i, \sigma)\|_\varepsilon \quad (5.26)$$

$$E' := \{s \in S' \mid s \cap E \neq \emptyset\} \quad (5.27)$$

$$s'_0 := \{\|s_0\|_\varepsilon\} \quad (5.28)$$

Das Konstruktionsverfahren unterscheidet sich lediglich an zwei Stellen von jenem aus Abschnitt 5.3.2. Zum einen werden bei der Berechnung der Folgezustände nicht nur die direkt erreichbaren, sondern auch diejenigen Zustände hinzugenommen, die über einen oder mehrere  $\varepsilon$ -Übergänge erreichbar sind. Zum anderen definieren wir den neuen Startzustand als die  $\varepsilon$ -Hülle des ursprünglichen Startzustands  $s_0$ .

In Abbildung 5.13 ist die DEA-Konstruktion für den oben eingeführten  $\varepsilon$ -Akzeptor dargestellt. Eliminieren wir alle unerreichbaren Teilgraphen, so verbleibt ein DEA mit 4 Zuständen (vgl. Abbildung 5.14). Ein vergleichender Blick auf Abbildung 5.11 zeigt, dass der dort dargestellte DEA und der soeben konstruierte Automat isomorph sind.

Mit Hilfe des skizzierten Konstruktionsschemas sind wir in der Lage, jeden beliebigen  $\varepsilon$ -Automaten auf einen äquivalenten DEA abzubilden. Damit haben wir einen konstruktiven Beweis für den folgenden Satz gefunden:

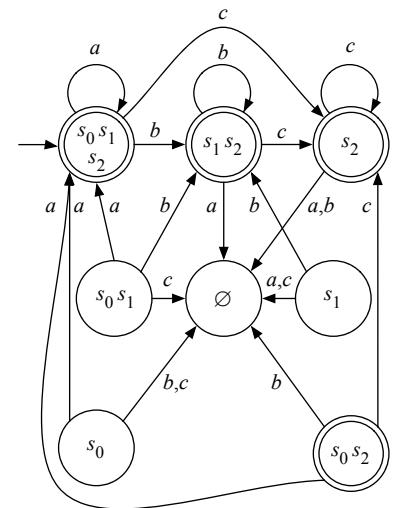


### Satz 5.2 ( $\varepsilon$ -Reduktionstheorem)

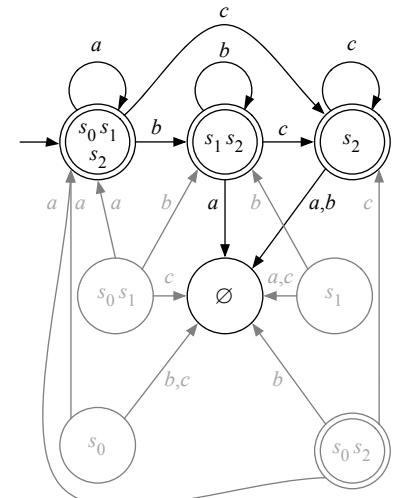
Zu jedem nichtdeterministischen endlichen  $\varepsilon$ -Akzeptor gibt es einen deterministischen endlichen Akzeptor, der die gleiche Sprache akzeptiert. Es gilt also:

$$\mathcal{L}(\varepsilon\text{-NEA}) = \mathcal{L}(\text{DEA})$$

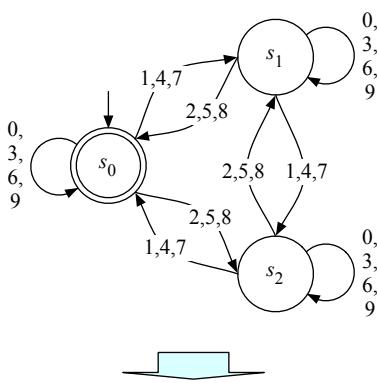
Damit haben wir gezeigt, dass die Hinzunahme von  $\varepsilon$ -Übergängen zu keiner Erweiterung der Ausdrucksstärke führt. Kurzum: Die (nichtdeterministischen)  $\varepsilon$ -Akzeptoren begründen exakt dieselbe Sprachklasse wie die weiter oben eingeführten DEAs und NEAs.



**Abbildung 5.13:** Übersetzung des  $\varepsilon$ -Automaten aus Abbildung 5.11 (oben) in einen äquivalenten DEA

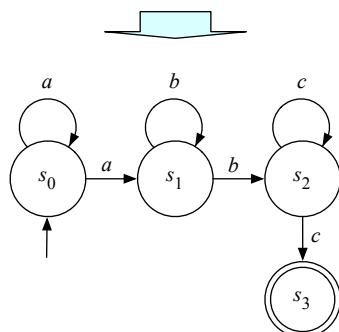


**Abbildung 5.14:** Eliminieren wir alle nicht erreichbaren Zustände, so verbleibt ein DEA mit 4 Zuständen. Der entstandene Automat ist isomorph zu unserem Eingangsbeispiel aus Abbildung 5.11 (unten).



**Abbildung 5.15:** Übersetzung eines DEA in eine reguläre Grammatik

$$\begin{array}{lcl} A_0 & \rightarrow & aA_0 \mid aA_1 \\ A_1 & \rightarrow & bA_1 \mid bA_2 \\ A_2 & \rightarrow & cA_2 \mid cA_3 \\ A_3 & \rightarrow & \epsilon \end{array}$$



**Abbildung 5.16:** Übersetzung einer regulären Grammatik in einen NEA

## 5.4 Automaten und reguläre Sprachen

Zwischen endlichen Automaten und den regulären Sprachen aus Abschnitt 4.3 besteht ein enger Zusammenhang, den wir an dieser Stelle genauer beleuchten wollen. Wir werden zum einen zeigen, dass jede von einem Automaten  $A$  akzeptierte Sprache regulär ist und zum anderen, dass für jede reguläre Sprache ein endlicher Automat konstruiert werden kann, der sie akzeptiert. Mit anderen Worten: Wir werden zeigen, dass endliche Automaten und reguläre Ausdrücke zwei Beschreibungsformen der gleichen Sprachklasse sind. Dabei spielt es keine Rolle, ob wir das Konzept des DEAs, des NEAs oder des  $\epsilon$ -NEAs zugrunde legen, schließlich haben wir in den vorherigen Abschnitten herausgearbeitet, wie sich diese äquivalenzerhaltend ineinander überführen lassen.

Für die folgenden Betrachtungen sei mit

$$A := \{S, \Sigma, \delta, E, s_0\} \quad (5.29)$$

ein beliebiger DEA gegeben. Wir werden zeigen, dass die Sprache  $\mathcal{L}(A)$  regulär ist, indem wir eine reguläre Grammatik

$$G := (V, \Sigma, P, S) \quad (5.30)$$

formulieren mit  $\mathcal{L}(G) = \mathcal{L}(A)$ . Hierbei verfolgen wir die Grundidee, die Zustände des Automaten als Nonterminale aufzufassen, d.h., für jeden Zustand  $s_i \in S$  existiert ein  $A_i \in V$  und umgekehrt. Hierdurch lässt sich jeder Zustandsübergang von  $s_i$  nach  $s_j$  mit  $s_j = \delta(s_i, \sigma)$  in direkter Weise in eine Ableitungsregel der Form

$$A_i \rightarrow \sigma A_j \quad (5.31)$$

übersetzen. Komplettiert wird die Menge der Produktionen, indem wir für jeden Endzustand  $s_e \in E$  eine Produktion der Form

$$A_e \rightarrow \epsilon \quad (5.32)$$

hinzufügen. Hierdurch kann die Wörterzeugung dann und nur dann abbrechen, wenn sich der zugehörige Automat in einem Endzustand befindet. Verwenden wir dasjenige Nonterminal  $A_0$  als Startsymbol, das dem Startzustand  $s_0$  zugeordnet ist, so erzeugt die konstruierte Grammatik  $G$  die Sprache  $\mathcal{L}(A)$ . Konstruktionsbedingt ist die Grammatik  $G$  regulär und damit auch die von  $A$  akzeptierte Sprache. Abbildung 5.15 demonstriert das Gesagte anhand unseres Einführungsbeispiels aus Abbildung 5.3.

Wir wollen nun umgekehrt vorgehen und zeigen, dass sich jede reguläre Grammatik  $G$  in einen endlichen Automaten  $A$  übersetzen lässt.

Mit Hilfe nichtdeterministischer Akzeptoren gelingt uns die Transformation auf besonders einfache Weise. Zunächst erzeugen wir für jedes Nonterminal  $A_i$  einen separaten Automatzustand  $s_i$ . Anschließend übersetzen wir jede Produktion der Form  $A_i \rightarrow \sigma A_j$  in einen Zustandsübergang von  $s_i$  nach  $s_j$  und markieren die verbindende Kante mit den Eingabezeichen  $\sigma$ . Die Produktionen der Form  $A_k \rightarrow \epsilon$  definieren die Endzustände des konstruierten Automaten, d. h., wir setzen  $E := \{s_k \mid (A_k \rightarrow \epsilon) \in P\}$ . Ein nichtdeterministischer Automat entsteht immer dann, wenn die Grammatik für ein Nonterminal  $A_i$  und ein Eingabezeichen  $\sigma$  zwei oder mehr Produktionen der Form  $A_i \rightarrow \sigma A_j$  enthält. Abbildung 5.16 erklärt die Übersetzung anhand eines konkreten Beispiels.

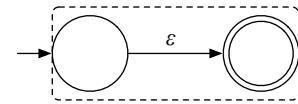
In Abschnitt 4.3.3 haben wir mit den *regulären Ausdrücken* eine alternative Beschreibungsform für reguläre Sprachen eingeführt. Einen Beweis, dass beide wirklich die gleiche Sprachklasse beschreiben, sind wir aber bisher schuldig geblieben. Mit Hilfe der nichtdeterministischen  $\epsilon$ -Automaten können wir eine der beiden Schlussrichtungen mit Leichtigkeit beweisen. Hierzu sind in Abbildung 5.17 sechs Konstruktionsmuster abgebildet, die zeigen, wie sich ein regulärer Ausdruck  $R$  rekursiv in einen  $\epsilon$ -Automaten transformieren lässt, der  $\mathcal{L}(R)$  akzeptiert. Da sich jeder  $\epsilon$ -NEA in einen DEA und dieser wiederum in eine reguläre Grammatik übersetzen lässt, haben wir gezeigt, dass jede Sprache, die durch einen regulären Ausdruck beschrieben wird, eine Typ-3-Sprache ist.

Die Reduktion eines regulären Ausdrucks auf einen akzeptierenden Automaten ist von hoher praktischer Relevanz. Um z. B. große Datenbestände effizient nach bestimmten Zeichenmustern zu durchsuchen, erzeugen viele Werkzeuge, die reguläre Ausdrücke als Suchmuster verwenden, intern einen endlichen Automaten. Ist dieser konstruiert, so lässt sich in linearer Zeit berechnen, ob eine entsprechende Zeichenkette vorhanden ist bzw. an welcher Stelle sie vorkommt.

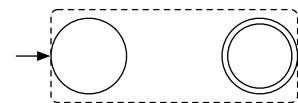
Die bewiesene Schlussrichtung lässt sich umkehren, d. h., für jeden endlichen Automaten  $A$  existiert ein regulärer Ausdruck, der  $\mathcal{L}(A)$  erzeugt. Für die Praxis ist diese Richtung der Äquivalenz die unbedeutendere und wir wollen den vergleichsweise komplizierten Beweis an dieser Stelle nicht führen. Eine ausführliche Betrachtung dieser Schlussrichtung findet sich z. B. in [50].

Insgesamt erhalten wir den in Abbildung 5.18 skizzierten Zusammenhang zwischen den verschiedenen Beschreibungsformen formaler Sprachen. Wie das Diagramm zeigt, beschreiben nichtdeterministische Akzeptoren, deterministische Akzeptoren, reguläre Grammatiken und reguläre Ausdrücke allesamt die gleiche Sprachklasse.

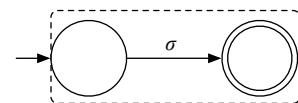
■ Leeres Wort:  $\epsilon$



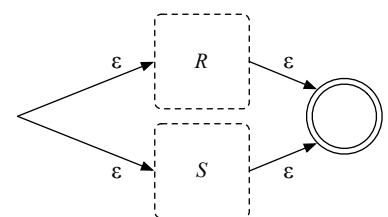
■ Leere Menge:  $\emptyset$



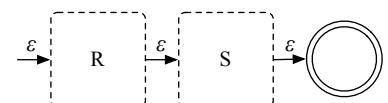
■ Einzelnes Zeichen:  $\sigma$



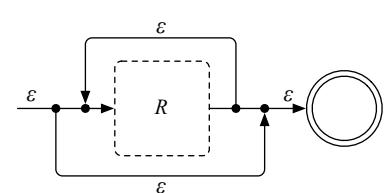
■ Auswahl:  $R \mid S$



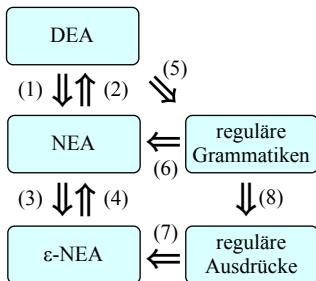
■ Komposition:  $RS$



■ Kleene'sche Hülle:  $R^*$



**Abbildung 5.17:** Jeder reguläre Ausdruck lässt sich rekursiv in einen äquivalenten nichtdeterministischen  $\epsilon$ -Automaten transformieren.



- (1) jeder DFA ist ein NFA
- (2) Abschnitt 5.3.2
- (3) jeder NFA ist ein  $\epsilon$ -NFA
- (4) Abschnitt 5.3.3
- (5) Abschnitt 5.4
- (6) Abschnitt 5.4
- (7) Abschnitt 5.4
- (8) siehe z. B. [50]

**Abbildung 5.18:** Zusammenfassung der herausgearbeiteten Äquivalenzbeziehungen

### 5.4.1 Abschlusseigenschaften

In Abschnitt 4.3 haben wir informell dargelegt, dass die Menge der regulären Sprachen bez. Vereinigung, Schnitt, Komplement, Produkt und Hüllenbildung abgeschlossen ist. Auch hier ebnet unser erworbenes Wissen über die Äquivalenz von regulären Grammatiken und endlichen Automaten den Weg, um die Behauptungen jetzt nachträglich zu beweisen.

Wir beginnen mit der einfachsten Abschlusseigenschaft: dem Komplement. Um zu zeigen, dass für jede reguläre Sprache  $L$  auch das Komplement  $\bar{L} = \Sigma^* \setminus L$  regulär ist, gehen wir in zwei Schritten vor: Im ersten Schritt konstruieren wir einen endlichen Automaten  $A$  mit  $\mathcal{L}(A) = L$ . Dass ein solcher Automat für jede reguläre Sprache existieren muss, haben wir im vorherigen Abschnitt herausgearbeitet. Im zweiten Schritt konstruieren wir aus  $A$  den *Komplementärautomaten*  $\bar{A}$ , der die Sprache  $\mathcal{L}(A)$  erzeugt.



#### Definition 5.8 (Komplementärautomat)

Sei  $A = (S, \Sigma, \delta, E, s_0)$  ein deterministischer endlicher Akzeptor.

$$\bar{A} := (S, \Sigma, \delta, S \setminus E, s_0) \quad (5.33)$$

heißt der *Komplementärautomat* von  $A$ .

Dass der Komplementärautomat die Sprache  $\overline{\mathcal{L}(A)}$  erzeugt, ist leicht einzusehen. Da wir die Menge der Endzustände invertiert haben, wird ein Wort  $\omega$  genau dann von  $\bar{A}$  akzeptiert, wenn es von  $A$  zurückgewiesen wird. Mit  $L$  wird damit immer auch  $\bar{L}$  von einem Automaten akzeptiert, so dass die Menge der regulären Sprachen in Bezug auf das Komplement abgeschlossen ist.

Den Abschluss bez. Schnitt beweisen wir nach dem gleichen Schema. Wir werden zeigen, dass zwei Automaten  $A = (S, \Sigma, \delta, E, s_0)$  und  $A' = (S', \Sigma, \delta', E', s'_0)$  so miteinander verschmolzen werden können, dass am Ende die Sprache  $\mathcal{L}(A) \cap \mathcal{L}(A')$  akzeptiert wird. Der gesuchten Akzeptor heißt *Produktautomat* und basiert auf der Idee,  $A$  und  $A'$  gewissermaßen parallel auszuführen. Um dies zu erreichen, definieren wir die neue Zustandsmenge als das kartesische Produkt von  $S$  und  $S'$ . Hierdurch entspricht jeder Zustand des Produktautomaten einem Tupel  $(s, s')$ , in das wir die aktuell eingenommenen Zustände von  $A$  und  $A'$  gleichzeitig hineincodieren können. Ferner legen wir die Zustandsübergangsfunktion so fest, dass der Produktautomat von einem Zustand

$(s_1, s'_1)$  unter Eingabe von  $\sigma$  genau dann in den Zustand  $(s_2, s'_2)$  übergeht, wenn  $A$  von  $s_1$  nach  $s_2$  und  $A'$  von  $s'_1$  nach  $s'_2$  wechselt.



### Definition 5.9 (Produktautomat)

Mit  $A = (S, \Sigma, \delta, E, s_0)$  und  $A' = (S', \Sigma, \delta', E', s'_0)$  seien zwei deterministische endliche Akzeptoren gegeben. Der Automat

$$A \times A' := (S'', \Sigma, \delta'', E'', s''_0) \quad \text{mit}$$

$$S'' := S \times S'$$

$$\delta''((s, s'), \sigma) := (\delta(s, \sigma), \delta'(s', \sigma))$$

$$E'' := \{(s, s') \mid s \in E \text{ und } s' \in E'\}$$

$$s''_0 := \{(s_0, s'_0)\}$$

heißt der *Produktautomat* von  $A$  und  $A'$ .

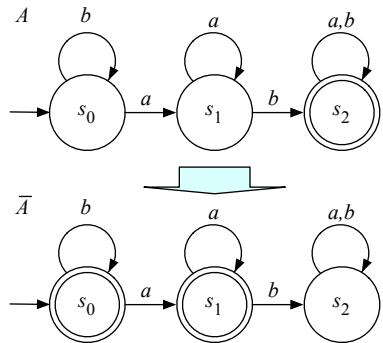


Abbildung 5.19: Der konstruierte Komplementärautomat akzeptiert die Sprache  $\overline{\mathcal{L}(A)}$ .

Beachten Sie, dass wir die Menge  $E$  so gewählt haben, dass der Produktautomat nur dann einen Finalzustand einnimmt, wenn sich sowohl  $A$  als auch  $A'$  in Finalzuständen befinden. Hierdurch akzeptiert  $A \times A'$  ein Wort genau dann, wenn es von  $A$  und  $A'$  akzeptiert wird. Mit anderen Worten: Der Produktautomat akzeptiert die Sprache  $\mathcal{L}(A) \cap \mathcal{L}(A')$ .

Ändern wir die Definition von  $E''$  in

$$E'' := \{(s, s') \mid s \in E \text{ oder } s' \in E'\} \quad (5.34)$$

ab, so erhalten wir einen Akzeptor für die Sprache  $\mathcal{L}(A) \cup \mathcal{L}(A')$ . In den Abbildungen 5.19 und 5.20 wird die Bildung des Komplementär- und des Produktautomaten anhand konkreter Beispiele demonstriert.

Zwei Automaten  $A$  und  $A'$  lassen sich auch so zusammenführen, dass die Produktsprache  $\mathcal{L}(A)\mathcal{L}(A')$  bzw. die Kleene'sche Hülle  $\mathcal{L}(A)^*$  akzeptiert wird. Abbildung 5.21 skizziert die Grundidee für die Konstruktion eines Akzeptors für die Sprache  $\mathcal{L}(A)\mathcal{L}(A')$ . Die Automaten  $A$  und  $A'$  werden sequenziell zusammengeschaltet, indem jeder Endzustand von  $A$  über eine  $\epsilon$ -Kante mit dem Startzustand von  $A'$  verbunden wird. Setzen wir die Finalzustände des neuen Automaten mit den Finalzuständen von  $A'$  gleich, so erhalten wir den gesuchten Akzeptor. Ebenso einfach lässt sich ein Automat  $A$  so modifizieren, dass er die Kleene'sche Hülle  $\mathcal{L}(A)^*$  akzeptiert. Hierzu erzeugen wir einen neuen Startzustand, der gleichzeitig als Endzustand fungiert, und führen von jedem der alten Endzustände eine zusätzliche  $\epsilon$ -Kante auf den neuen Startzustand zurück (vgl. Abbildung 5.22).

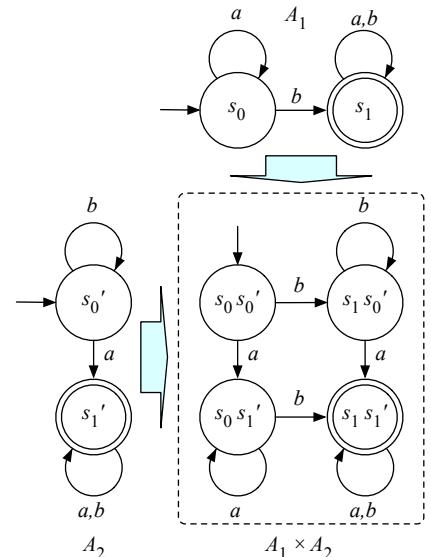
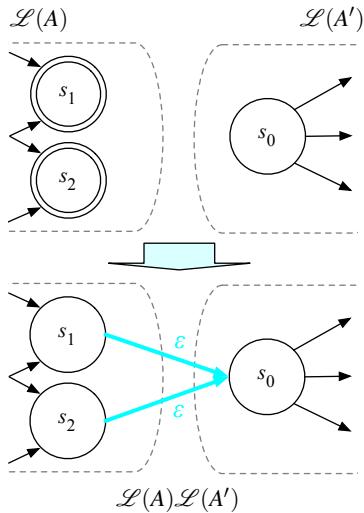
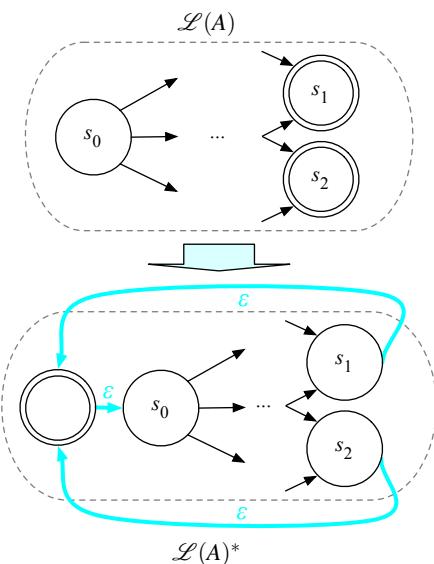


Abbildung 5.20: Der konstruierte Produktautomat akzeptiert die Sprache  $\mathcal{L}(A_1) \cap \mathcal{L}(A_2)$ .



**Abbildung 5.21:** Zwei Akzeptoren  $A$  und  $A'$  können zu einem gemeinsamen Automaten verschmolzen werden, der die Sprache  $\mathcal{L}(A)\mathcal{L}(A')$  erzeugt.



**Abbildung 5.22:** Jeder Akzeptor  $A$  lässt sich zu einem Automaten erweitern, der die Kleene'sche Hülle  $\mathcal{L}(A)^*$  akzeptiert.

## 5.4.2 Entscheidungsprobleme

Im Folgenden wollen wir herausarbeiten, wie sich das Wortproblem, das Leerheitsproblem, das Endlichkeitsproblem und das Äquivalenzproblem für reguläre Sprachen entscheiden lassen. Erneut bezeichne  $G$  eine reguläre Grammatik und  $A$  einen DEA mit  $\mathcal{L}(A) = \mathcal{L}(G)$ .

- Das Wortproblem ist entschieden, wenn wir für alle  $\omega \in \Sigma^*$  feststellen können, ob  $\omega$  in  $\mathcal{L}(G)$  enthalten ist oder nicht. Mit Hilfe des Akzeptors  $A$  können wir das Wortproblem für  $G$  lösen, indem wir  $A$  mit dem fraglichen Wort  $\omega$  schlicht „ausführen“.  $\omega$  gehört genau dann zu  $\mathcal{L}(G)$ , wenn sich  $A$  nach der Verarbeitung des letzten Eingabezeichens in einem Finalzustand befindet.
- Das Leerheitsproblem lässt sich mit Hilfe von Graphen-Algorithmen entscheiden.  $\mathcal{L}(G)$  entspricht genau dann der leeren Menge, wenn im Zustandsdiagramm von  $A$  kein Pfad vom Startzustand zu einem der Finalzustände führt.
- Genau wie das Leerheitsproblem lässt sich auch das Endlichkeitsproblem mit Hilfe von Graphen-Algorithmen entscheiden.  $\mathcal{L}(G)$  ist genau dann endlich, wenn kein Pfad existiert, der den Startzustand mit einem Finalzustand verbindet und eine Schleife enthält.
- Hinter dem Äquivalenzproblem verbirgt sich die Frage, ob zwei reguläre Grammatiken  $G_1$  und  $G_2$  die gleiche Sprache erzeugen. Um das Problem zu entscheiden, bestimmen wir zunächst zwei Akzeptoren  $A_1$  und  $A_2$  mit  $\mathcal{L}(A_1) = \mathcal{L}(G_1)$  und  $\mathcal{L}(A_2) = \mathcal{L}(G_2)$ . Jetzt nutzen wir aus, dass reguläre Sprachen bez. Schnitt und Komplement abgeschlossen sind und das Leerheitsproblem entscheidbar ist. Es gilt die folgende Reduktion:

$$\begin{aligned}\mathcal{L}(G_1) = \mathcal{L}(G_2) &\Leftrightarrow \mathcal{L}(G_1) \subseteq \mathcal{L}(G_2) \wedge \mathcal{L}(G_2) \subseteq \mathcal{L}(G_1) \\ \mathcal{L}(G_1) \subseteq \mathcal{L}(G_2) &\Leftrightarrow \mathcal{L}(A_1) \cap \overline{\mathcal{L}(A_2)} = \emptyset \\ \mathcal{L}(G_2) \subseteq \mathcal{L}(G_1) &\Leftrightarrow \mathcal{L}(A_2) \cap \overline{\mathcal{L}(A_1)} = \emptyset\end{aligned}$$

Die Automatenminimierung eröffnet uns eine zweite Möglichkeit, um das Äquivalenzproblem zu entscheiden. Es lässt sich zeigen, dass der Minimierungsalgorithmus Automaten erzeugt, die bis auf Isomorphie eindeutig bestimmt sind. Damit können wir die Äquivalenz überprüfen, indem wir zunächst  $A_1$  und  $A_2$  in eine minimierte Darstellung überführen und die entstandenen Zustandsgraphen anschließend einem Isomorphietest unterziehen. Auch dies können wir erleben, indem wir auf Standardalgorithmen aus der Graphentheorie zurückgreifen.

## 5.5 Kellerautomaten

### 5.5.1 Definition und Eigenschaften

In Abschnitt 5.4 haben wir herausgearbeitet, dass alle Sprachen, die von endlichen Automaten akzeptiert werden, regulär sind. Das bedeutet, dass für die nichtreguläre Sprache

$$L_{C2} = \{a^n b^n \mid n \in \mathbb{N}\} \quad (5.35)$$

kein endlicher Automat existiert, der  $L$  akzeptiert. Warum es einen solchen nicht geben kann, demonstrieren die vier Akzeptoren in Abbildung 5.23. Ein Blick auf die Zustandsübergänge zeigt, dass der Automat  $A_n$  mit

$$\mathcal{L}(A_n) = \{a^i b^i \mid i \leq n\} \quad (5.36)$$

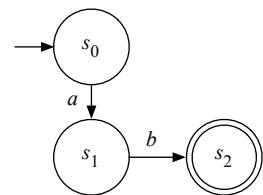
eine endliche Teilmenge von  $L_{C2}$  akzeptiert, die sich mit steigendem  $n$  kontinuierlich vergrößert. Die Sprache  $L_{C2}$  erhalten wir als Approximation der Sprachenfolge  $\mathcal{L}(A_n)$  für  $n \rightarrow \infty$ :

$$L_{C2} = \bigcup_{n=1}^{\infty} \mathcal{L}(A_n) \quad (5.37)$$

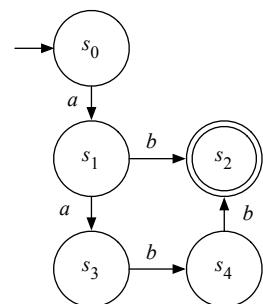
Die Anzahl der Zustände, die wir für den Aufbau des Automaten  $A_n$  benötigen, wächst linear mit dem Parameter  $n$ . Die Zunahme ist unvermeidbar, da sich der Akzeptor zunächst die Anzahl der gelesenen  $a$ 's merken muss, bevor er die darauf folgenden  $b$ 's verarbeiten kann. Da endliche Automaten per Definition über keine weiter gehenden Möglichkeiten zur Informationsspeicherung verfügen, bleibt uns als einzige Option übrig, den aktuellen Zählerstand in die Zustandsmenge hineinzucodieren. Folgerichtig muss der Automat  $A_n$  mindestens  $n$  Zustände besitzen, um  $n$  verschiedene Zählerstände zu unterscheiden. Da die Anzahl der  $a$ 's und  $b$ 's in den Wörtern von  $L_{C2}$  nach oben unbeschränkt ist, müsste ein entsprechender Akzeptor unendlich viele Zustände besitzen, im Widerspruch zu seiner Endlichkeit.

Aus dem Gesagten erwächst die folgende Vermutung: Gelingt es, einen endlichen Automaten um einen unendlich großen Gedächtnisspeicher anzureichern, so müssten Sprachen der Form (5.35) problemlos zu erkennen sein. Diese Überlegung führt uns in direktem Wege zum Begriff des *Kellerautomaten*.

■ Automat  $A_1$



■ Automat  $A_2$



■ Automat  $A_n$

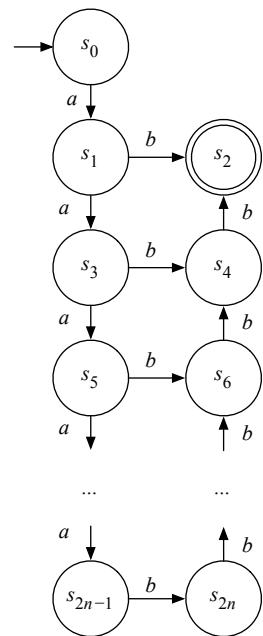


Abbildung 5.23: Endliche Akzeptoren für die Sprachen  $L_n = \{a^i b^i \mid 1 \leq i \leq n\}$

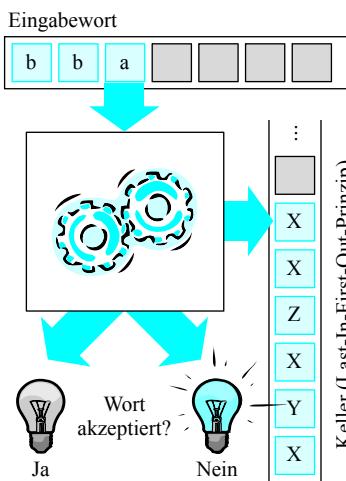


Abbildung 5.24: Kellerautomat



### Definition 5.10 (Kellerautomat)

Ein Kellerautomat (*pushdown automaton*), kurz PDA, ist ein 5-Tupel  $(S, \Sigma, \Gamma, \delta, s_0)$ . Er besteht aus

- der endlichen *Zustandsmenge*  $S$ ,
- dem endlichen *Eingabealphabet*  $\Sigma$  mit  $\epsilon \notin \Sigma$ ,
- dem endlichen *Kelleralphabet*  $\Gamma$  mit  $\perp \in \Gamma$ ,
- der *Zustandsübergangsfunktion*  $\delta : S \times (\Sigma \cup \{\epsilon\}) \times \Gamma \rightarrow 2^{S \times \Gamma^*}$ ,
- dem *Startzustand*  $s_0$ .

Im Wesentlichen entspricht ein Kellerautomat einem nichtdeterministischen  $\epsilon$ -Akzeptor, der um einen separaten Kellerspeicher mit unendlich großer Kapazität erweitert wurde (vgl. Abbildung 5.24). Der Kellerspeicher ist als *Stapel* (*stack*) organisiert und erlaubt daher nur einen eingeschränkten Zugriff auf die Elemente. Die Funktionsweise ist ähnlich derer eines konventionellen Bücherstapels; hier können wir ein neues Buch entweder oben auf den Stapel packen (*Push-Operation*) oder das oberste Buch wegnehmen (*Pop-Operation*). In einem Stack dürfen Elemente weder von unten noch aus der Mitte entnommen werden, d. h., das zuletzt hinzugefügte Element wird immer als erstes wieder entfernt (*LIFO-Prinzip, Last-In-First-Out*).

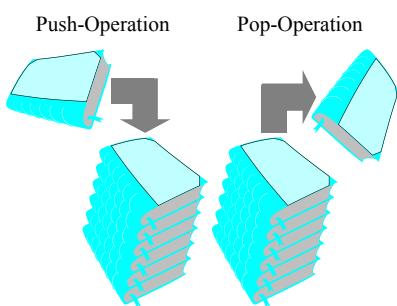


Abbildung 5.25: Stacks (Stapel) arbeiten nach dem Last-In-First-Out-Prinzip. Ähnlich einem gewöhnlichen Bücherstapel werden neue Elemente stets auf die Stapeloberseite gelegt (PUSH-Operation) und von dort entnommen (POP-Operation). Das zuletzt hinzugefügte Element wird also stets als erstes wieder entfernt.

Im Gegensatz zu den bisher betrachteten Akzeptoren besitzen Kellerautomaten zwei verschiedene Alphabete  $\Sigma$  und  $\Gamma$ . Das Eingabealphabet  $\Sigma$  enthält die Zeichen, aus denen sich die Eingabewörter zusammensetzen, und das Kelleralphabet  $\Gamma$  alle Symbole, die in den Kellerspeicher geschrieben werden dürfen. Damit beide Alphabete einfacher unterschieden werden können, halten wir uns an die gängige Konvention, Eingabezeichen mit Kleinbuchstaben und Kellerzeichen mit Großbuchstaben darzustellen.

In gewohnter Weise wird das Eingabewort in einem Kellerautomaten zeichenweise bearbeitet. In jedem Verarbeitungsschritt liest der PDA ein Eingabezeichen  $\sigma$  ein und entfernt das oberste Kellerzeichen  $\gamma$ . In Abhängigkeit von  $\sigma$ ,  $\gamma$  und des aktuellen Zustands  $s$  geht der Kellerautomat in einen Folgezustand  $s'$  über und schreibt mit Hilfe mehrerer PUSH-Operationen eine Zeichenkette  $\gamma'_0 \dots \gamma'_i \in \Gamma^*$  in den Kellerspeicher. Damit im ersten Verarbeitungsschritt überhaupt ein Kellerzeichen entfernt werden kann, befüllen wir den Speicher vorab mit dem dedizierten Element  $\perp \in \Gamma$ .

Die Zustandsübergänge eines Kellerautomaten entsprechen denen des  $\varepsilon$ -NEAs aus Abschnitt 5.3.3, so dass es Verarbeitungsschritte geben kann, die kein Eingabezeichen konsumieren ( $\varepsilon$ -Übergang). Nichtsdestotrotz wird auch in diesem Fall das oberste Kellerzeichen entfernt. Beachten Sie, dass in jedem Schritt mehr als ein Zeichen in den Kellerspeicher zurückgeschrieben werden darf. Hierdurch ist es möglich, die Entfernung des obersten Zeichens rückgängig zu machen, indem wir es als zusätzliches Symbol wieder in den Kellerspeicher legen. Es ist ebenfalls erlaubt, überhaupt kein Zeichen in den Kellerspeicher zurückzuschreiben. In diesem Fall wird die Anzahl der im Keller gespeicherten Elemente um 1 reduziert.

Formal lässt sich das Verhalten eines Kellerautomaten mit dem Begriff der Konfiguration erfassen, den wir in den Abschnitten 5.2 und 5.3 in ähnlicher Form für die Beschreibung von DEAs und NEAs erfolgreich eingesetzt haben.



### Definition 5.11 (Konfiguration (PDA))

Mit  $K = (S, \Sigma, \Gamma, \delta, s_0)$  sei ein beliebiger Kellerautomat gegeben. Jedes Tripel  $(s, \omega, \kappa)$  mit  $s \in S$ ,  $\omega \in \Sigma^*$  und  $\kappa \in \Gamma^*$  heißt eine *Konfiguration* von  $K$ . Die Übergangsrelation  $\rightarrow$  definieren wir wie folgt:

$$(s_1, \omega, \gamma\kappa) \rightarrow (s_2, \omega, \kappa'\kappa) : \Leftrightarrow (s_2, \kappa') \in \delta(s_1, \varepsilon, \gamma)$$

$$(s_1, \sigma\omega, \gamma\kappa) \rightarrow (s_2, \omega, \kappa'\kappa) : \Leftrightarrow (s_2, \kappa') \in \delta(s_1, \sigma, \gamma)$$

Vereinbarungsgemäß akzeptiert ein Kellerautomat  $K = (S, \Sigma, \Gamma, \delta, s_0)$  die folgende Sprache:

$$\mathcal{L}(K) := \{\omega \mid (s_0, \omega, \perp) \xrightarrow{*} (s_i, \varepsilon, \varepsilon)\} \quad (5.38)$$

Wir haben die akzeptierte Sprache in einer Form festgelegt, die gänzlich ohne Endzustände auskommt. Ob das Wort  $\omega$  akzeptiert wird, hängt ausschließlich von der Beschaffenheit des Kellers ab. Konkret wird ein Wort  $\omega$  genau dann akzeptiert, wenn es eine Möglichkeit gibt, die Verarbeitung mit einem leeren Keller abzuschließen. Beachten Sie, dass der Kellerautomat nichtdeterministisch arbeitet. Hierdurch ist ein Wort  $\omega$  bereits dann in der Sprache enthalten, wenn mindestens eine Möglichkeit existiert, die Bearbeitung mit einem leeren Keller zu beenden. Daneben können andere Berechnungspfade existieren, die zu einem nichtleeren Keller führen.

Die angestellten Überlegungen versetzen uns in die Lage, einen Kellerautomaten zu konstruieren, der die nichtreguläre Sprache  $L_{C2}$  akzeptiert. Wie in Abbildung 5.26 gezeigt, kommt ein solcher Automat mit

■ Kellerautomat  $K = (S, \Sigma, \Gamma, \delta, s_0)$

$$S := \{s_0, s_1\}$$

$$\Sigma := \{a, b\}$$

$$\Gamma := \{A, \perp\}$$

$$\delta(s_0, a, \perp) :=_{(1)} \{(s_0, A\perp)\}$$

$$\delta(s_0, a, A) :=_{(2)} \{(s_0, AA)\}$$

$$\delta(s_0, b, A) :=_{(3)} \{(s_1, \varepsilon)\}$$

$$\delta(s_1, b, A) :=_{(4)} \{(s_1, \varepsilon)\}$$

$$\delta(s_1, \varepsilon, \perp) :=_{(5)} \{(s_1, \varepsilon)\}$$

■ Beispiel 1:  $\omega = aabb$

Zustand	$\omega$	Keller
$s_0$	aabb	$\perp$
(1) $s_0$	abb	$A\perp$
(2) $s_0$	bb	$AA\perp$
(3) $s_1$	b	$A\perp$
(4) $s_1$	$\varepsilon$	$\perp$
(5) $s_1$	$\varepsilon$	$\varepsilon$

✓ akzeptiert

■ Beispiel 2:  $\omega = aaabb$

Zustand	$\omega$	Keller
$s_0$	aaabb	$\perp$
(1) $s_0$	aabb	$A\perp$
(2) $s_0$	abb	$AA\perp$
(2) $s_0$	bb	$AAA\perp$
(3) $s_1$	b	$AA\perp$
(4) $s_1$	$\varepsilon$	$A\perp$

✗ nicht akzeptiert

**Abbildung 5.26:** Die nichtreguläre Sprache  $L_{C2} = \{a^n b^n \mid n \in \mathbb{N}\}$  lässt sich mit Hilfe des dargestellten Kellerautomaten akzeptieren.

■ Kellerautomat

$$\begin{aligned}
 S &:= \{s_0, s_1\} \\
 \Sigma &:= \{a, b\} \\
 \Gamma &:= \{A, B\} \\
 \delta(s_0, a, \gamma) &:= (1) \{(s_0, A\gamma)\} \\
 \delta(s_0, b, \gamma) &:= (2) \{(s_0, B\gamma)\} \\
 \delta(s_0, \epsilon, \gamma) &:= (3) \{(s_1, \gamma)\} \\
 \delta(s_1, a, A) &:= (4) \{(s_1, \epsilon)\} \\
 \delta(s_1, b, B) &:= (5) \{(s_1, \epsilon)\} \\
 \delta(s_1, \epsilon, \perp) &:= (6) \{(s_1, \epsilon)\}
 \end{aligned}$$

■ Beispiel:  $\omega = abbaabba$

	Zustand	$\omega$	Keller
(1)	$s_0$	abbaabba	$\perp$
	$s_0$	bbaabba	$A\perp$
	$s_0$	baabba	$BA\perp$
	$s_0$	aabba	$BBA\perp$
	$s_0$	abba	$ABBA\perp$
	$s_1$	abba	$ABBA\perp$
(4)	$s_1$	bba	$BBA\perp$
(5)	$s_1$	ba	$BA\perp$
(5)	$s_1$	a	$A\perp$
(4)	$s_1$	$\epsilon$	$\perp$
(6)	$s_1$	$\epsilon$	$\epsilon$

✓ akzeptiert

Abbildung 5.27: Kellerautomat zum Erkennen der Palindromsprache  $L_{\text{Pal}}$

zwei Zuständen  $s_0$  und  $s_1$  aus. Das Kelleralphabet  $\Gamma$  besteht aus einem einzigen Symbol  $A$ , das wir als Merker für die Anzahl der bereits gelesenen  $a$ 's einsetzen. Jedes Mal, wenn ein  $a$  eingelesen wird, legt der Automat ein  $A$  im Keller ab. Sobald das erste  $b$  gelesen wird, wechselt der Automat in den Zustand  $s_1$  und beginnt, den Keller mit jedem gelesenen Symbol zu leeren. Genau dann, wenn die Anzahl der gelesenen  $a$ 's gleich der Anzahl der gelesenen  $b$ 's ist, kann der Keller vollständig geleert werden und das Eingabewort wird akzeptiert.

In dem diskutierten Beispiel haben wir die volle Leistungsfähigkeit des Kellerautomaten noch gar nicht ausgeschöpft. Dies wollen wir jetzt nachholen und zeigen, wie die *Palindromsprache*

$$L_{\text{Pal}} := \{\epsilon\} \cup \{\sigma_1 \dots \sigma_n \sigma_n \dots \sigma_1 \mid n \in \mathbb{N}, \sigma_i \in \{a, b\}\} \quad (5.39)$$

mit einem Kellerautomaten erkannt werden kann. Die Grundidee des Automaten ist simpel: Zunächst werden die Eingabesymbole  $\sigma_1, \dots, \sigma_n$  der Reihe nach eingelesen und in den Kellerspeicher geschrieben. Anschließend werden die nächsten  $n$  Symbole verarbeitet und Zeichen für Zeichen mit dem Kellerinhalt abgeglichen. Der Kellerautomat fährt mit der Bearbeitung nur dann fort, wenn das aktuell verarbeitete Zeichen mit dem obersten Zeichen des Kellerspeichers übereinstimmt (vgl. Abbildung 5.27).

So weit so gut. Aber wie kann der Automat wissen, wann mit dem Rückbau des Kellerspeichers begonnen werden muss? Da die Länge des Eingabeworts zu Beginn der Verarbeitung nicht bekannt ist, ist es unmöglich, den Wert von  $n$  vorab auf deterministischem Weg zu bestimmen. Dass wir die Palindromsprache trotzdem mit Hilfe eines Kellerautomaten erkennen können, haben wir seinen nichtdeterministischen Eigenschaften zu verdanken. Im Gegensatz zu seinen deterministischen Pendanten kann ein nichtdeterministischer Automat die Wortmitte schlicht erraten.

## 5.5.2 Kellerautomaten und kontextfreie Sprachen

Kellerautomaten sind alles andere als eine willkürliche Erweiterung der endlichen Automaten aus Abschnitt 5.2. Die Architektur ist so angelegt, dass die Menge der von Kellerautomaten akzeptierten Sprachen und die Menge der kontextfreien Sprachen aus Abschnitt 4.4 identisch sind. In diesem Abschnitt werden wir untersuchen, wie dieser Zusammenhang zustande kommt.

Als Erstes wollen wir uns mit der Frage beschäftigen, wie sich eine kontextfreie Grammatik

$$G = \{V, \Sigma, P, S\} \quad (5.40)$$

in einen Kellerautomaten

$$K_G = (\{s_0\}, \Sigma, \Gamma, \delta, s_0) \quad (5.41)$$

übersetzen lässt, der exakt die Wörter aus  $\mathcal{L}(G)$  akzeptiert. Die Lösung des Problems besteht in der Konstruktion eines Automaten, der die Ableitung eines Worts  $\omega$  im Kellerspeicher nachvollzieht. Wie Gleichung (5.41) bereits andeutet, kommt der konstruierte Automat mit nur einem Zustand  $s_0$  aus, d.h., die gesamte Intelligenz ist in den Regeln zur Manipulation des Kellerspeichers verborgen.

Das Kelleralphabet setzen wir wie folgt fest:

$$\Gamma := \Sigma \cup V \quad (5.42)$$

Die Menge der Produktionen  $P$  kann eins zu eins in die Zustandsübergangsfunktion  $\delta$  hineincodiert werden. Für jedes Nonterminal  $A \in V$  übersetzen wir die Menge der Produktionen

$$A \rightarrow \omega_1, \dots, A \rightarrow \omega_n \quad (5.43)$$

in die folgende Regel:

$$\delta(s_0, \epsilon, A) := \{(s_0, \omega_1), \dots, (s_0, \omega_n)\} \quad (5.44)$$

Zusätzlich definieren wir Regeln für den Umgang mit Terminalzeichen. Wird aktuell das Terminalzeichen  $\sigma$  eingelesen, so soll der Kellerautomat nur dann mit der Verarbeitung fortfahren, wenn  $\sigma$  gleichzeitig das oberste Kellerzeichen ist. Um das gewünschte Verhalten zu erzielen, definieren wir für jedes Zeichen  $\sigma \in \Sigma$  den folgenden Zustandsübergang:

$$\delta(s_0, \sigma, \sigma) := \{(s_0, \epsilon)\} \quad (5.45)$$

Zu guter Letzt ergänzen wir den Kellerautomaten um eine Regel, die das Symbol  $\perp$  durch das Startsymbol  $S$  ersetzt und auf diese Weise einen geregelten Start der Worterkennung ermöglicht:

$$\delta(s_0, \epsilon, \perp) := \{(s_0, S)\} \quad (5.46)$$

Abbildung 5.28 demonstriert die skizzierte Automatenkonstruktion für die in Abschnitt 4.1 eingeführte Dyck-Sprache  $D_2$ . Im unteren Teil der Abbildung ist eine Folge von Zustandsübergängen für das Dyck-Wort

■ Grammatik

$$S \rightarrow \epsilon | SS | [S] | (S)$$

■ Kellerautomat  $K$

$$\begin{aligned} \delta(s_0, \epsilon, S) &:=_{(1)} \{(s_0, \epsilon)\} \\ \delta(s_0, \epsilon, S) &:=_{(2)} \{(s_0, SS)\} \\ \delta(s_0, \epsilon, S) &:=_{(3)} \{(s_0, [S])\} \\ \delta(s_0, \epsilon, S) &:=_{(4)} \{(s_0, (S))\} \\ \delta(s_0, \sigma, \sigma) &:=_{(5)} \{(s_0, \epsilon)\} \\ \delta(s_0, \epsilon, \perp) &:=_{(6)} \{(s_0, S)\} \end{aligned}$$

■ Beispiel:  $\omega = ()[()]( )$

	Zustand	$\omega$	Keller
(6)	$s_0$	$()[()()$	$\perp$
(2)	$s_0$	$()[()()$	$SS$
(4)	$s_0$	$()[()()$	$(S)S$
(5)	$s_0$	$)[()()$	$S)S$
(1)	$s_0$	$)[()()$	$)S$
(5)	$s_0$	$[()()$	$S$
(2)	$s_0$	$[()()$	$SS$
(3)	$s_0$	$[()()$	$[S]S$
(5)	$s_0$	$]()$	$S]S$
(4)	$s_0$	$]()$	$(S)]S$
(5)	$s_0$	$]()$	$S]S$
(1)	$s_0$	$]()$	$)]S$
(5)	$s_0$	$]()$	$]S$
(5)	$s_0$	$($	$S$
(4)	$s_0$	$($	$(S)$
(5)	$s_0$	$)$	$S)$
(1)	$s_0$	$)$	$)$
(5)	$s_0$	$\epsilon$	$\epsilon$

✓ akzeptiert

**Abbildung 5.28:** Jede kontextfreie Grammatik  $G$  lässt sich in einen Kellerautomaten  $K$  übersetzen, der  $\mathcal{L}(G)$  akzeptiert. Der in diesem Beispiel konstruierte Automat akzeptiert die Dyck-Sprache  $D_2$ .

■ Kellerautomat

$$\begin{aligned} S &:= \{s_0, s_1\} \\ \Sigma &:= \{a, b, \$\} \\ \Gamma &:= \{A, B\} \\ \delta(s_0, a, \gamma) &:=_{(1)} \{(s_0, A\gamma)\} \\ \delta(s_0, b, \gamma) &:=_{(2)} \{(s_0, B\gamma)\} \\ \delta(s_0, \$, \gamma) &:=_{(3)} \{(s_1, \gamma)\} \\ \delta(s_1, a, A) &:=_{(4)} \{(s_1, \varepsilon)\} \\ \delta(s_1, b, B) &:=_{(5)} \{(s_1, \varepsilon)\} \\ \delta(s_1, \varepsilon, \perp) &:=_{(6)} \{(s_1, \varepsilon)\} \end{aligned}$$

■ Beispiel:  $\omega = abba\$abba$

	Zustand	$\omega$	Keller
(1)	$s_0$	$abba\$abba$	$\perp$
(2)	$s_0$	$bba\$abba$	$A\perp$
(2)	$s_0$	$ba\$abba$	$BA\perp$
(1)	$s_0$	$a\$abba$	$BBA\perp$
(1)	$s_0$	$\$abba$	$ABBA\perp$
(3)	$s_1$	$abba$	$ABBA\perp$
(4)	$s_1$	$bba$	$BBA\perp$
(5)	$s_1$	$ba$	$BA\perp$
(5)	$s_1$	$a$	$A\perp$
(4)	$s_1$	$\varepsilon$	$\perp$
(6)	$s_1$	$\varepsilon$	$\varepsilon$

✓ akzeptiert

**Abbildung 5.29:** Deterministischer Kellerautomat zur Erkennung der Palindromsprache  $L_{\text{Pal\$}}$

$()[()]( )$  dargestellt, die mit einem leeren Keller endet. An diesem Beispiel lässt sich gut erkennen, wie die einzelnen Ableitungsschritte im Kellerspeicher repliziert werden.

Wir haben in diesem Abschnitt herausgearbeitet, wie sich jede kontextfreie Grammatik in einen äquivalenten Kellerautomaten überführen lässt. In der Tat lässt sich auch die Umkehrung beweisen: Jede von einem Kellerautomaten  $K$  akzeptierte Sprache  $\mathcal{L}(K)$  lässt sich durch eine kontextfreie Grammatik  $G$  erzeugen. Den nicht ganz einfachen Beweis wollen wir an dieser Stelle nicht führen; er ist ausführlich in [50] beschrieben. Insgesamt gilt der folgende Satz:



### Satz 5.3 (Äquivalenztheorem für Kellerautomaten)

Die Klasse der von Kellerautomaten akzeptierten Sprachen ist mit der Klasse der kontextfreien Sprachen identisch.

Beachten Sie, dass unser Konstruktionsschema einen Kellerautomaten produziert, der genau einen Zustand  $s_0$  besitzt. Damit zeigt Satz 5.3 zugleich, dass sich jeder Kellerautomat auf einen äquivalenten Automaten mit einem einzigen Zustand reduzieren lässt. Einen solchen können wir erzeugen, indem wir aus dem ursprünglichen Automaten zunächst eine kontextfreie Grammatik erzeugen und diese anschließend in einen Kellerautomaten mit nur einem Zustand zurückübersetzen.

Das Ergebnis gibt einen wichtigen Hinweis darauf, woher die Ausdrucksstärke von Kellerautomaten herführt. Sie wird ausschließlich durch den (unendlich großen) Kellerspeicher geschaffen und durch die Kombination mit einer endlichen Zustandsmenge nicht erweitert. Trotzdem sind die Zustände nicht sinnlos. Für viele Sprachen lassen sich akzeptierende Kellerautomaten deutlich kompakter und übersichtlicher formulieren, wenn mehr als ein Zustand verwendet wird.

### 5.5.3 Deterministische Kellerautomaten

Sehen wir von der speziellen Behandlung des Kellerspeichers ab, so arbeitet ein Kellerautomat genau nach dem gleichen Prinzip wie ein nichtdeterministischer  $\varepsilon$ -Automat. In diesem Abschnitt wollen wir eine spezielle Variante des Kellerautomaten einführen, die die nichtdeterministischen Zustandsübergänge beseitigt.



### Definition 5.12 (Deterministischer Kellerautomat)

Ein Kellerautomat  $(S, \Sigma, \Gamma, \delta, s_0)$  heißt *deterministisch*, wenn für alle Zustände  $s \in S$ , Eingabezeichen  $\sigma \in \Sigma$  und Kellersymbole  $\kappa \in \Gamma$  die folgende Beziehung gilt:  $|\delta(s, \sigma, \kappa) \cup \delta(s, \varepsilon, \kappa)| \leq 1$

Demnach existiert in einem deterministischen Kellerautomaten für jedes Eingabezeichen  $\omega$  und jedes oberste Kellerzeichen  $\kappa$  maximal ein Zustandsübergang. Genau wie bisher wird ein Wort  $\omega$  akzeptiert, wenn der Automat nach der Verarbeitung des letzten Eingabezeichens einen leeren Keller aufweist. Verbleiben dagegen Symbole im Kellerspeicher oder bleibt der Automat vor der Verarbeitung des letzten Zeichens aufgrund einer fehlenden Übergangsregel stehen, so wird  $\omega$  abgelehnt. Ganz im Gegensatz zur Architektur des klassischen DEAs aus Abschnitt 5.2 wollen wir die Vereinbarung treffen, dass auch ein deterministischer Kellerautomat nicht in jedem Schritt zwingend ein Eingabezeichen konsumieren muss.  $\varepsilon$ -Übergänge sollen jedoch nur dann zulässig sein, wenn keine andere Übergangsregel anwendbar ist.

Als Beispiel ist in Abbildung 5.29 ein deterministischer Kellerautomat definiert, der die Sprache

$$L_{\text{Pal\$}} := \{\$\} \cup \{\sigma_1 \dots \sigma_n \$ \sigma_n \dots \sigma_1 \mid n \in \mathbb{N}, \sigma_i \in \Sigma \setminus \{\$\}\} \quad (5.47)$$

akzeptiert. Die Sprache  $L_{\text{Pal\$}}$  unterscheidet sich von der Palindromsprache  $L_{\text{Pal}}$  durch ein zusätzliches Terminalzeichen  $\$$ , das die Mitte des Eingabeworts markiert. Die Verwendung eines zusätzlichen Mittelzeichens ist an dieser Stelle essentiell, da uns anders als im nichtdeterministischen Fall kein Orakel mehr zur Verfügung steht, das die Mitte des Worts für uns errät. Verzichten wir auf das Mittelzeichen, so kann die Sprache von keinem deterministischen Kellerautomaten akzeptiert werden.

Tatsächlich stehen wir hier vor einer gänzlich anderen Situation als im Falle des klassischen endlichen Automaten. Dort konnten wir zeigen, dass sich jeder  $\varepsilon$ -NEA in einen äquivalenten deterministischen Akzeptor überführen lässt. Für Kellerautomaten ist eine solche Reduktion nicht möglich. In der Konsequenz ergibt sich der folgende Satz, den wir an dieser Stelle ohne formalen Beweis akzeptieren wollen:



### Satz 5.4

Die Sprachklasse der von deterministischen Kellerautomaten akzeptierten Sprachen ist eine echte Teilmenge der von nichtdeterministischen Kellerautomaten akzeptierten Sprachen.

In der Literatur ist der Begriff des Kellerautomaten nicht eindeutig definiert. In diesem Buch wird ein Kellerautomat als 5-Tupel  $(S, \Sigma, \Gamma, \delta, s_0)$  beschrieben, in anderen dagegen als 6-Tupel  $(S, \Sigma, \Gamma, \delta, E, s_0)$ . Die zusätzlich hinzugefügte Komponente  $E$  ist die Menge der Endzustände.

Dass wir vollständig auf Endzustände verzichten konnten, haben wir der gewählten Akzeptanzbedingung zu verdanken. Ein Automat unserer Bauart akzeptiert ein Eingabewort  $\omega$  genau dann, wenn der Kellerspeicher nach der Verarbeitung des letzten Eingabezeichens leer ist. Dabei ist es unerheblich, in welchem Zustand er sich am Ende befindet.

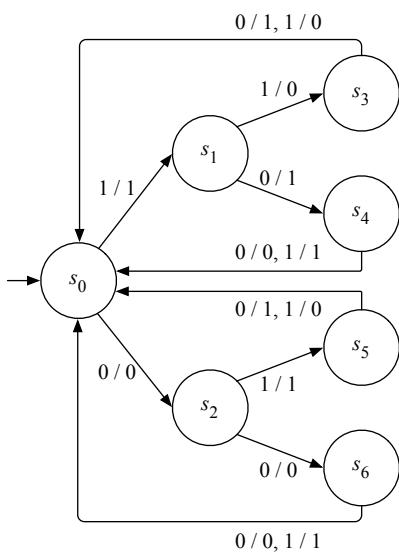
Automaten mit Endzuständen verwenden eine andere Akzeptanzbedingung. Ähnlich dem klassischen DEA wird ein Wort  $\omega$  genau dann akzeptiert, wenn nach der Verarbeitung des letzten Eingabezeichens ein Endzustand eingenommen wird. In diesem Fall spielt es keine Rolle, ob der Kellerspeicher zu diesem Zeitpunkt leer ist oder noch Symbole enthält.

Die beiden Akzeptanzbedingungen sind gleichwertig, d. h., für jeden Kellerautomaten  $K$ , der eine Sprache  $L$  mit leerem Keller akzeptiert, existiert ein Kellerautomat  $K'$ , der  $L$  per Endzustand akzeptiert, und umgekehrt. Beachten Sie, dass diese Beziehung für deterministische Kellerautomaten nicht gilt! Hier wird die Menge der akzeptierbaren Sprachen durch den Wechsel der Akzeptanzbedingung in der Tat verändert.

Ein Kellerautomat ist  
ein 5-Tupel ...



Ein Kellerautomat ist  
ein 6-Tupel ...



**Abbildung 5.30:** Seriell arbeitender Binär-Gray-Code-Wandler

## 5.6 Transduktoren

### 5.6.1 Definition und Eigenschaften

Alle der bisher betrachteten Automatentypen arbeiten als Akzeptoren. Ein Eingabewort wird Zeichen für Zeichen eingelesen und am Ende entschieden, ob die eingelesene Sequenz akzeptiert oder abgelehnt wird. Im Gegensatz hierzu arbeiten *Transduktoren* als Übersetzer. Anstelle einer Ja-Nein-Ausgabe produzieren diese eine Menge von Ausgabezeichen, die nacheinander auf ein separates Ausgabeband geschrieben werden. Formal definieren wir den Begriff des Transduktors wie folgt:



#### Definition 5.13 (Endlicher Transdukt)

Ein deterministischer endlicher Transduktor (*deterministic finite state transducer*), kurz DET, ist ein 6-Tupel  $(S, \Sigma, \Pi, \delta, \lambda, s_0)$ . Er besteht aus

- der endlichen Zustandsmenge  $S$ ,
- dem endlichen Eingabealphabet  $\Sigma$ ,
- dem endlichen Ausgabealphabet  $\Pi$ ,
- der Zustandsübergangsfunktion  $\delta : S \times \Sigma \rightarrow S$ ,
- der Ausgabefunktion  $\lambda : S \times \Sigma \rightarrow \Pi$  und
- dem Startzustand  $s_0$ .

Zu Beginn befindet sich ein Transdukt in seinem Startzustand  $s_0$ . Wird er mit dem Eingabewort

$$\omega = \sigma_0, \sigma_1, \sigma_2, \dots, \sigma_n \quad (5.48)$$

stimuliert, so durchläuft er nacheinander die Zustände

$$s_0, s_1, s_2, \dots, s_n \quad \text{mit } s_{i+1} = \delta(s_i, \sigma_i) \quad (5.49)$$

und produziert die Ausgabe

$$\pi_0, \pi_1, \pi_2, \dots, \pi_n \quad \text{mit } \pi_i = \lambda(s_i, \sigma_i). \quad (5.50)$$

Transduktoren besitzen per Definition keine Endzustände. Es interessiert einzig das produzierte Ausgabewort.

Um den Begriff mit Leben zu füllen, betrachten wir das Beispiel in Abbildung 5.30. Der dargestellte Transduktor implementiert einen seriellen Code-Wandler, der einen binären Eingabestrom entgegennimmt ( $\Sigma = \{0, 1\}$ ) und in einen ebenfalls binären Ausgabestrom übersetzt ( $\Pi = \{0, 1\}$ ). Die Bitmuster des Gray-Codes sind in Abbildung 5.31 zusammengefasst. Der Automat startet im Zustand  $s_0$  und interpretiert jeweils drei kontinuierliche Eingabeziffern als eine zusammengehörige Binärzahl. Diese wird durch die Automatenlogik in den Gray-Code umgesetzt und das resultierende Bitmuster auf das Ausgabeband geschrieben. In jedem Verarbeitungsschritt liest und schreibt der Transduktor genau eine Ziffer.

Beachten Sie die erweiterten Kantenmarkierungen des Transduktors. In der Markierung  $\sigma/\pi$  steht  $\sigma$  für ein Symbol des Eingabealphabets  $\Sigma$  und  $\pi$  für ein Symbol des Ausgabealphabets  $\Pi$ .

## 5.6.2 Automatenminimierung

In Abschnitt 5.2 haben wir den Äquivalenzbegriff für endliche Akzeptoren eingeführt. Abstrakt betrachtet sind zwei Automaten genau dann äquivalent, wenn sie nach außen das gleiche Verhalten zeigen. Im Falle von Akzeptoren bedeutet dies nichts anderes, als dass beide die gleiche Sprache akzeptieren. Für übersetzende Automaten können wir den Begriff ganz ähnlich definieren und bezeichnen zwei Transduktoren als äquivalent, wenn jede Eingabesequenz die gleiche Ausgabesequenz erzeugt. Genau wie im Falle des Akzeptors lässt sich die Automatenäquivalenz mit dem Begriff der Bisimulation formal erfassen.



### Definition 5.14 (Zustandsäquivalenz, Bisimulation)

Sei  $A = (S, \Sigma, \Pi, \delta, \lambda, s_0)$  ein endlicher Transduktor. Die  $k$ -Äquivalenz zwischen zwei Zuständen  $s_1$  und  $s_2$ , geschrieben als  $s_1 \sim_k s_2$ , definieren wir wie folgt:

$s_1 \sim_0 s_2 \Leftrightarrow$  Für alle  $\sigma \in \Sigma$  gilt  $\lambda(s_1, \sigma) = \lambda(s_2, \sigma)$

$s_1 \sim_{k+1} s_2 \Leftrightarrow s_1 \sim_0 s_2$  und

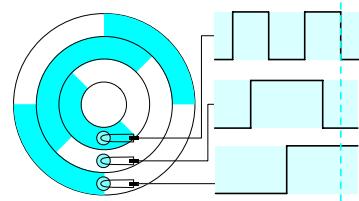
für alle  $\sigma \in \Sigma$  gilt  $\delta(s_1, \sigma) \sim_k \delta(s_2, \sigma)$

Gilt  $s_1 \sim_k s_2$  für alle  $k \in \mathbb{N}_0$ , so heißen  $s_1$  und  $s_2$  äquivalent, in Zeichen  $s_1 \sim s_2$ . Die Relation  $\sim$  wird als *Bisimulation* bezeichnet.

### Code-Tabelle

Dezimal	Binär	Gray-Code
0	000	000
1	001	001
2	010	011
3	011	010
4	100	110
5	101	111
6	110	101
7	111	100

### Anwendung



**Abbildung 5.31:** Der Gray-Code besitzt die Eigenschaft, dass sich die Bitmuster zweier benachbarter Ziffern in genau einem Bit unterscheiden [38]. Codes mit dieser Eigenschaft heißen *einschrittig*. Im Bereich der Automatisierungstechnik wird der Gray-Code unter anderem zur Codierung von Messwerten verwendet, die über mechanische oder optoelektronische Sensoren erfasst werden. Aufgrund der Einschrittigkeit ist er weit weniger anfällig für Messfehler als der konventionelle Binärcode.

**Abbildung 5.32:** Schrittweise Reduktion des endlichen Transduktors aus Abbildung 5.30. Im ersten Schritt wird die Zustandsmenge so aufgeteilt, dass genau diejenigen Zustände in einer Äquivalenzklasse zusammengefasst sind, die für alle Eingabezeichen  $\sigma$  das gleiche Ausgabezeichen erzeugen. Nach diesem Schritt sind alle 0-äquivalenten Zustände bestimmt. Anschließend werden die Äquivalenzklassen in einem iterativen Prozess weiter aufgeteilt. Nach der ersten Iteration sind alle in einer Klasse verbleibenden Zustände paarweise 1-äquivalent, nach der zweiten Iteration paarweise 2-äquivalent und so fort. Machen wir mit der Aufteilung so lange weiter, bis ein Fixpunkt erreicht ist, so sind die Zustände in den verbleibenden Äquivalenzklassen zueinander äquivalent. Genau wie im Fall der Akzeptorenminimierung können wir den reduzierten Transduktor konstruieren, indem wir für jede Äquivalenzklasse einen separaten Zustand erzeugen.

#### Übergangstabelle

	$s_0$	$s_1$	$s_2$	$s_3$	$s_4$	$s_5$	$s_6$
0	$s_2, 0$	$s_4, 1$	$s_6, 0$	$s_0, 1$	$s_0, 0$	$s_0, 1$	$s_0, 0$
1	$s_1, 1$	$s_3, 0$	$s_5, 1$	$s_0, 0$	$s_0, 1$	$s_0, 0$	$s_0, 1$

#### Erste Partition

	$s_0$	$s_2$	$s_4$	$s_6$	$s_1$	$s_3$	$s_5$
	$P_1$				$P_2$		
0	$s_2, P_1$	$s_6, P_1$	$s_0, P_1$	$s_0, P_1$	$s_4, P_1$	$s_0, P_1$	$s_0, P_1$
1	$s_1, P_2$	$s_5, P_2$	$s_0, P_1$	$s_0, P_1$	$s_3, P_2$	$s_0, P_1$	$s_0, P_1$

#### Zweite Partition

	$s_0$	$s_2$	$s_4$	$s_6$	$s_1$	$s_3$	$s_5$
	$P_1$		$P_2$		$P_3$	$P_4$	
0	$s_2, P_1$	$s_6, P_2$	$s_0, P_1$	$s_0, P_1$	$s_4, P_2$	$s_0, P_1$	$s_0, P_1$
1	$s_1, P_3$	$s_5, P_4$	$s_0, P_1$	$s_0, P_1$	$s_3, P_4$	$s_0, P_1$	$s_0, P_1$

#### Dritte Partition

	$s_0$	$s_2$	$s_4$	$s_6$	$s_1$	$s_3$	$s_5$
	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$		
0	$s_2, P_2$	$s_6, P_3$	$s_0, P_1$	$s_0, P_1$	$s_4, P_3$	$s_0, P_1$	$s_0, P_1$
1	$s_1, P_4$	$s_5, P_5$	$s_0, P_1$	$s_0, P_1$	$s_3, P_5$	$s_0, P_1$	$s_0, P_1$

Die Äquivalenz zweier Transduktoren ist genau dann gegeben, wenn ihre Startzustände zueinander bisimulativ sind. Für die Konstruktion eines reduzierten Automaten gehen wir wie im Fall des endlichen Akzeptors vor. Im ersten Schritt stellen wir die Übergangstabelle auf und teilen die Zustände anschließend in verschiedene Äquivalenzklassen ein. Zunächst fassen wir diejenigen Zustände zusammen, die für alle Eingabezeichen  $\sigma$  das gleiche Ausgabezeichen erzeugen. Auf diese Weise erhalten wir alle 0-äquivalenten Zustände. Anschließend werden die Äquivalenzklassen so verfeinert, dass im  $k$ -ten Iterationsschritt alle Zustände einer Äquivalenzklasse zueinander  $k$ -äquivalent sind. Wiederholen wir den Prozess, bis keine neuen Partitionen entstehen, so sind alle äquivalenten Zustände bestimmt. Auch hier konstruieren wir am Ende den reduzierten Automaten, indem wir aus jeder Äquivalenzklasse einen beliebigen Repräsentanten entnehmen und die Zustände gemäß den berechneten Übergängen miteinander verbinden.

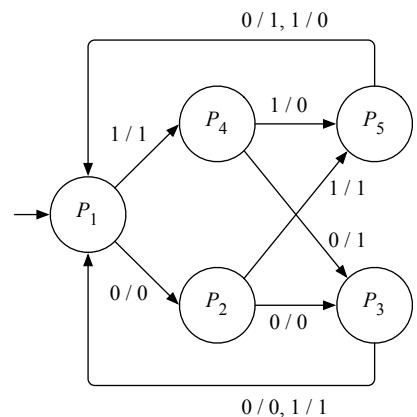
Abbildung 5.32 demonstriert die Reduktion am Beispiel des seriellen Gray-Code-Wandlers aus Abbildung 5.30. Nach der dritten Iteration ist ein Fixpunkt erreicht und mit den fünf gefundenen Äquivalenzklassen die finale Partition der Zustandsmenge bestimmt. Das Ergebnis zeigt, dass die Zustände  $s_4$  und  $s_6$  sowie die Zustände  $s_3$  und  $s_5$  zueinander bisimulativ sind und miteinander verschmolzen werden können. Insgesamt ist es uns damit gelungen, die Anzahl der Zustände von 7 auf 5 zu verringern (Abbildung 5.33).

### 5.6.3 Automatensynthese

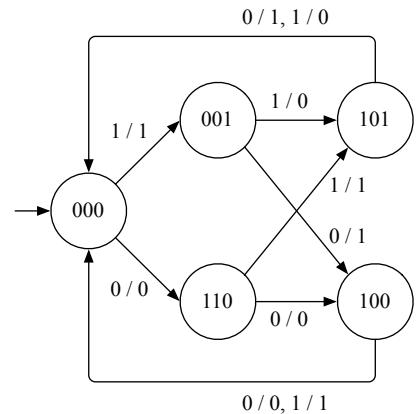
Transduktoren sind von großer praktischer Bedeutung, da sie eins zu eins in eine Hardware-Schaltung – ein sogenanntes *Schaltwerk* – übersetzt werden können. Hierzu bestimmen wir zunächst eine binäre Codierung der Zustände, d.h., wir ordnen jedem Zustand  $s_i \in S$  einen Bitvektor der Länge  $k$  zu, der  $s_i$  eindeutig charakterisiert. Da wir mit Bitvektoren der Länge  $k$  genau  $2^k$  Zustände unterscheiden können, gilt im Umkehrschluss die Beziehung  $k = \lceil \log_2 |S| \rceil$ . Mit anderen Worten: Die Anzahl der Bits, die wir für die Codierung benötigen, wächst logarithmisch mit der Anzahl der Zustände des Transduktors.

Exemplarisch ist in Abbildung 5.34 eine der vielen Möglichkeiten dargestellt, um die Zustände des minimierten Binär-Gray-Code-Wandlers zu codieren. Auch wenn die Zuordnung der Bitvektoren zu den einzelnen Zuständen im Prinzip willkürlich erfolgen kann, hat sie in der Praxis einen erheblichen Einfluss auf die Eigenschaften der entstehenden Hardware-Schaltung. Genau wie die geschickte Wahl der Zustandscodierung zu einer sehr kompakten Schaltung führen kann, lässt eine ungeschickte Wahl in vielen Fällen eine unnötig komplexe Schaltung entstehen. Das Auffinden einer geeigneten Zustandscodierung ist ein wichtiger Arbeitsschritt im computergestützten Schaltungsentwurf, der in der Praxis mit Hilfe spezieller Software-Werkzeuge durchgeführt wird.

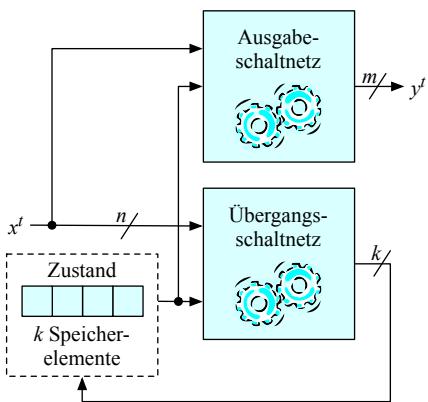
Ist eine binäre Zustandscodierung bestimmt, werden die Automatenzustände auf die reale Hardware-Schaltung abgebildet. Hierzu wird für jedes Bit der Zustandscodierung ein binäres Speicherelement (*Flipflop* oder *Latch*) in die Schaltung eingesetzt und die Übergangsfunktion  $\delta$  und die Ausgabefunktion  $\lambda$  werden in zwei konventionelle *Schaltnetze* übersetzt. Das *Übergangsschaltnetz* berechnet aus dem aktuellen Zustand und der aktuellen Eingabe die Steuersignale, mit denen wir die Speicherbausteine beschalten müssen, um sie im nächsten Takt in den korrekten Folgezustand zu bringen. Das *Ausgetriebeneschaltnetz* berechnet die aktuelle Ausgabe des Schaltwerks. Die Ein- und Ausgabe der



**Abbildung 5.33:** Serieller Binär-Gray-Code-Wandler. Ergebnis nach der Automatenminimierung.



**Abbildung 5.34:** Zustandscodierter Automat des seriellen Gray-Code-Wandlers.



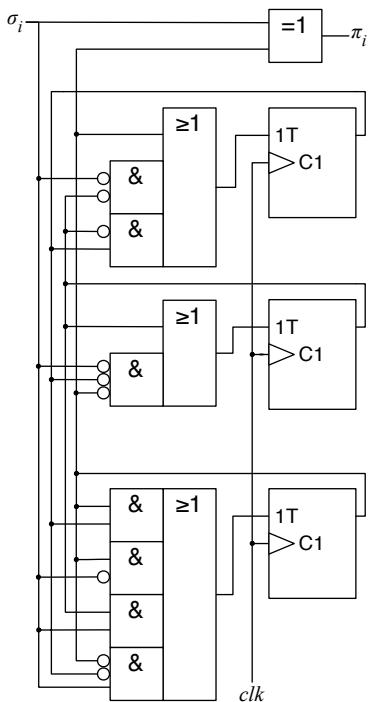
**Abbildung 5.35:** Jeder Transduktor lässt sich eins zu eins in ein Schaltwerk in Huffman-Normalform übersetzen.

Hardware-Schaltung wird durch Bitvektoren der Länge  $n$  bzw.  $m$  gebildet. Zwischen einem Schaltwerk mit  $n$  Eingangsleitungen und  $m$  Ausgangsleitungen und dem binär codierten Automaten besteht damit der folgende Zusammenhang:

$$\Sigma = \{0, 1\}^n, \quad \Pi = \{0, 1\}^m \quad (5.51)$$

Führen wir die Ausgänge des Ausgabeschaltnetzes aus der Schaltung heraus und die Ausgänge des Übergangsschaltnetzes zurück auf die Eingänge der Speicherelemente, so entsteht ein Schaltwerk in *Huffman-Normalform*. In Abbildung 5.35 ist dessen Grobstruktur grafisch zusammengefasst.

Abbildung 5.36 zeigt die resultierende Hardware-Schaltung des seriellen Gray-Code-Wandlers in Huffman-Normalform. Eine detaillierte Beschreibung, wie sich das Übergangss- und das Ausgabeschaltnetz aus der codierten Automatenbeschreibung ableiten lässt, wird in [48] gegeben.



**Abbildung 5.36:** Implementierung des seriellen Gray-Code-Wandlers in Huffman-Normalform

## 5.6.4 Mealy- und Moore-Automaten

In Definition 5.13 haben wir festgelegt, dass sowohl der eingenommene Zustand als auch das gelesene Eingabezeichen in die Berechnung des aktuellen Ausgabezeichens  $\lambda(s_i, \sigma_i)$  mit einbezogen wird. Einige Automaten nutzen diese Flexibilität nur unvollständig aus und berechnen die aktuelle Ausgabe ausschließlich aus dem gegenwärtig eingenommenen Zustand. Automaten mit dieser Eigenschaft sind in der Praxis von so großer Bedeutung, dass sie in der Informatik einen eigenen Namen erhalten haben.



### Definition 5.15 (Mealy- und Moore-Automat)

Gegeben sei ein beliebiger endlicher Automat  $(S, \Sigma, \Pi, \delta, \lambda, s_0)$ . Geht in die Berechnung des Ausgabezeichens sowohl der aktuelle Zustand als auch das aktuelle Eingabezeichen ein, gilt also

$$\pi_i = \lambda(s_i, \sigma_i), \quad (5.52)$$

so sprechen wir von einem *Mealy-Automaten*. Ist die Ausgabefunktion stattdessen nur vom aktuellen Zustand abhängig, gilt also

$$\pi_i = \lambda(s_i), \quad (5.53)$$

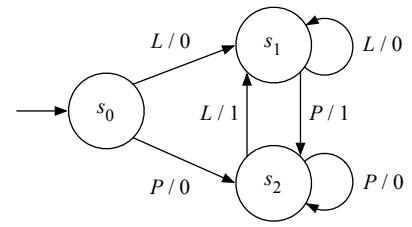
so sprechen wir von einem *Moore-Automaten*.

Abbildung 5.37 demonstriert den Unterschied zwischen Mealy- und Moore-Automaten anhand zweier Beispiele. Die Übergangstabelle des Mealy-Automaten zeigt, dass die Ausgabe in  $s_1$  und  $s_2$  sowohl von dem eingenommenen Zustand als auch von dem aktuell gelesenen Eingabezeichen abhängt. Im Falle des Moore-Automaten spielt das aktuell gelesene Eingabezeichen dagegen keine Rolle; hier wird die Ausgabe ausschließlich durch den eingenommenen Zustand bestimmt. Wegen dieser Eigenschaft werden Moore-Automaten typischerweise in einer Notation angegeben, die das Ausgabezeichen nicht mehr länger den Kanten, sondern den Zuständen zuordnet. Abbildung 5.37 zeigt den Moore-Automaten in beiden Darstellungen. Beachten Sie, dass der Automatentyp nicht zweifelsfrei aus der verwendeten Notation abgeleitet werden kann. Ein Moore-Automat liegt vor, wenn die Ausgabefunktion nur von dem eingenommenen Zustand abhängt, unabhängig davon, ob die Ausgabezeichen in Mealy-typischer Notation an den Kanten oder in Moore-typischer Notation an den Zuständen vermerkt sind.

Liegt ein Schaltwerk in Huffman-Normalform vor, so lässt sich mit einem einzigen Blick erkennen, ob es aus einem Mealy- oder einem Moore-Automaten synthetisiert wurde. Per Definition berechnet sich die Ausgabe eines Mealy-Automaten aus dem aktuellen Zustand und der aktuellen Eingabe des Schaltwerks. In der Huffman-Normalform führen damit neben den Ausgängen der Speicherelemente auch eine oder mehrere Eingangsleitungen in das Schaltnetz zur Ausgabeberechnung (vgl. Abbildung 5.38 links). Im Gegensatz hierzu hängt die Ausgabe bei Moore-Automaten ausschließlich vom aktuellen Zustand des Schaltwerks ab. In der Huffman-Normalform drückt sich die Moore-Eigenschaft dadurch aus, dass keine direkte Verbindung zwischen den Eingangssignalen und den Eingängen des Ausgabeschaltnetzes mehr existiert (vgl. Abbildung 5.38 rechts).

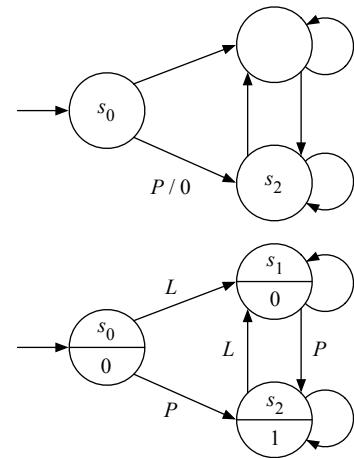
An dieser Stelle drängt sich die Frage auf, ob Mealy- und Moore-Transduktoren ein voneinander verschiedenes Automatenmodell beschreiben oder doch vielleicht zueinander äquivalent sind. Ein kurzer Blick auf die Definitionen 5.13 und 5.15 zeigt, dass wir jeden Moore-Automaten als einen speziellen Mealy-Automaten auffassen können. Die weitaus interessantere Frage ist die, ob wir jeden Mealy-Automaten in einen äquivalenten Moore-Automaten umformen können. In der hier definierten Form ist eine solche Reduktion nicht ohne weiteres möglich, da die Ausgabe eines Mealy-Automaten zum Zeitpunkt  $i$  sowohl von dem eingenommenen Zustand  $s_i$  als auch der aktuellen Eingabe  $\sigma_i$  abhängt. Ein Moore-Automat kann zur Ausgabeberechnung nur den Zustand  $\sigma_i$  auswerten und hat zum Zeitpunkt  $i$  noch kein Wissen von der aktuellen Eingabe  $\sigma_i$ .

Mealy-Automat



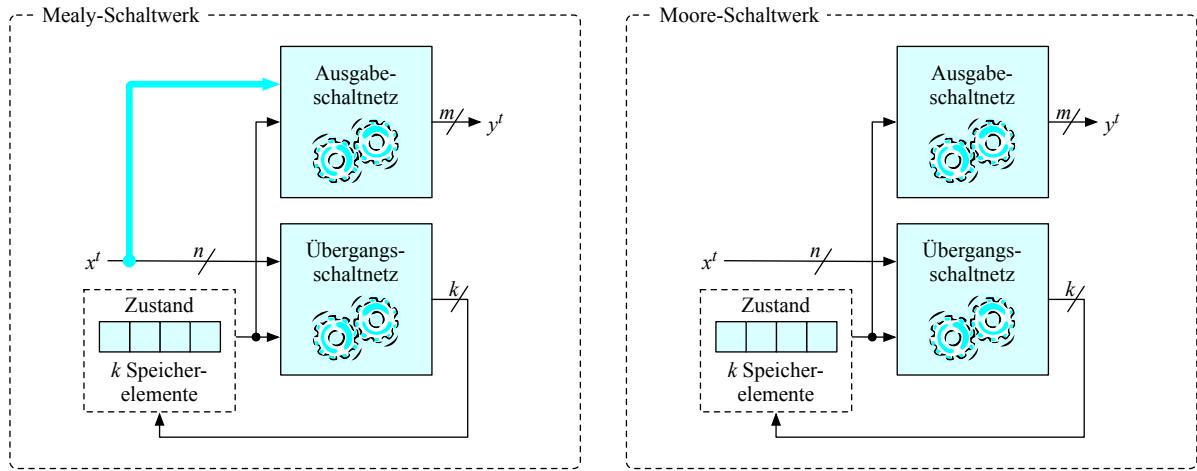
$s$	$s_0$	$s_1$	$s_2$
$\delta(s, L)$	$s_1$	$s_1$	$s_1$
$\delta(s, P)$	$s_2$	$s_2$	$s_2$
$\lambda(s, L)$	0	0	1
$\lambda(s, P)$	0	1	0

Moore-Automat



$s$	$s_0$	$s_1$	$s_2$
$\delta(s, L)$	$s_1$	$s_1$	$s_1$
$\delta(s, P)$	$s_2$	$s_2$	$s_2$
$\lambda(s)$	0	0	1

Abbildung 5.37: Mealy- und Moore-Automaten im Vergleich



**Abbildung 5.38:** An der Huffman-Normalform eines Schaltwerks lässt sich besonders einfach erkennen, ob ein Mealy- oder ein Moore-Automat implementiert wird. Während das Ausgabeschaltnetz in Mealy-Schaltwerken zusätzliche Verbindungen zu den Eingangsleitungen aufweist, wird es in Moore-Schaltwerken ausschließlich durch die Leitungen des Speicherblocks gespeist.

Nichtsdestotrotz ist es möglich, für jeden Mealy-Automaten einen Moore-Automaten zu konstruieren, wenn wir das eingeführte Automatenmodell geringfügig ändern. Die Grundidee besteht darin, die produzierte Zeichensequenz um einen Schritt verzögert auf das Ausgabeband zu schreiben. Ein Transduktor beginnt auch in unserem modifizierten Modell wie gehabt im Startzustand  $s_0$ . Wird er mit dem Eingabewort

$$\omega = \sigma_0, \sigma_1, \sigma_2, \dots, \sigma_n \quad (5.54)$$

stimuliert, so durchläuft er die Zustände

$$s_0, s_1, s_2, \dots, s_n \quad \text{mit } s_{i+1} = \delta(s_i, \sigma_i) \quad (5.55)$$

und produziert die Ausgabe

$$\pi_1, \pi_2, \dots, \pi_{n+1} \quad \text{mit } \pi_i = \lambda(s_i, \sigma_{i-1}). \quad (5.56)$$

Das modifizierte Automatenmodell unterscheidet sich in zwei wesentlichen Punkten von dem bisherigen. Zum einen produziert der Transduktor zum Zeitpunkt 0 keine Ausgabe; das erste Zeichen wird zum Zeitpunkt 1 auf das Ausgabeband geschrieben, das letzte zum Zeitpunkt  $n + 1$ . Zum anderen berechnet sich die Ausgabe aus dem eingenommenen Zustand und dem *zuvor* gelesenen Eingabezeichen. Durch diese Verschiebung wird es möglich, das Eingabezeichen in den eingenommenen Zustand hineinzucodieren und die Ausgabefunktion von der Mealy-Form in die Moore-Form zu überführen.

Wie in Abbildung 5.39 gezeigt, gehen wir hierzu in zwei Schritten vor. Zunächst werden die Ausgabezeichen aus der Kantenmarkierung herausgelöst und dem Folgezustand zugeordnet (vgl. Abbildung 5.39 Mitte). Probleme bereiten uns diejenigen Zustände, die über zwei oder mehr eingehende Kanten verfügen, die mit einem unterschiedlichen Ausgabezeichen markiert sind. Hier lässt sich der Konflikt auflösen, indem wir die Zustände aufspalten und die Kanten auf denjenigen Zustand mit der passenden Ausgabe umleiten (vgl. Abbildung 5.39 unten). Die Umwandlung zeigt, dass die vereinfachte Ausgabeberechnung ihren Preis in einer Erhöhung der Zustandsanzahl fordert. Besitzt das Ausgabealphabet  $n$  Zeichen, so kann der konstruierte Moore-Automat bis zu  $n$  mal mehr Zustände besitzen als der Mealy-Automat.

Unsere Betrachtungen werfen die Frage auf, welches der vorgestellten Automatenmodelle dem anderen überlegen ist. Wie so oft hängt auch hier die Antwort vom Standpunkt des Betrachters ab. Legen wir eine praktische Sicht zugrunde, so scheint das ursprünglich eingeführte Automatenmodell das natürlichere zu sein. In diesem Fall entspricht das Ein- und Ausgabeverhalten eines Mealy- bzw. eines Moore-Automaten exakt dem einer Hardware-Schaltung, so dass wir den Begriff des Transduktors ohne Übertreibung als das theoretische Fundament der digitalen Schaltungstechnik ansehen können. Legen wir stattdessen eine theoretische Sicht zugrunde, so wirkt das modifizierte Ausgabeverhalten nach Gleichung (5.56) als das verführerische. Es besitzt den Vorteil, dass sich Mealy- und Moore-Automaten als äquivalent erweisen, was in der praxisorientierten Variante nicht der Fall ist.

In der Literatur wird der Mealy- und der Moore-Begriff aus den geschilderten Gründen unterschiedlich eingeführt und in vielen Fällen – bewusst oder unbewusst – von der ursprünglichen Definition von George H. Mealy [67] und Edward F. Moore [70] abgewichen. Auch die hier getroffene Definition des Moore-Automaten unterscheidet sich von jener aus der Originalarbeit. Wir folgen hier bewusst der praxisorientierten Variante, die eine direkte Entsprechung im Hardware-Entwurf findet.

Aus dem Gesagten wird eines ganz klar: Die Interpretation der Begriffe Mealy und Moore muss stets mit Bedacht befolgen und kann zu ganz unterschiedlichen Ergebnissen führen. Allen in der Literatur angekommenen Definitionen ist lediglich gemein, dass der Begriff Mealy ein Automatenmodell beschreibt, das die Ausgabe aus Zustand und Eingabe berechnet, während der Begriff Moore ein Automatenmodell meint, das für die Ausgabeberechnung ausschließlich den Zustand in Betracht zieht.

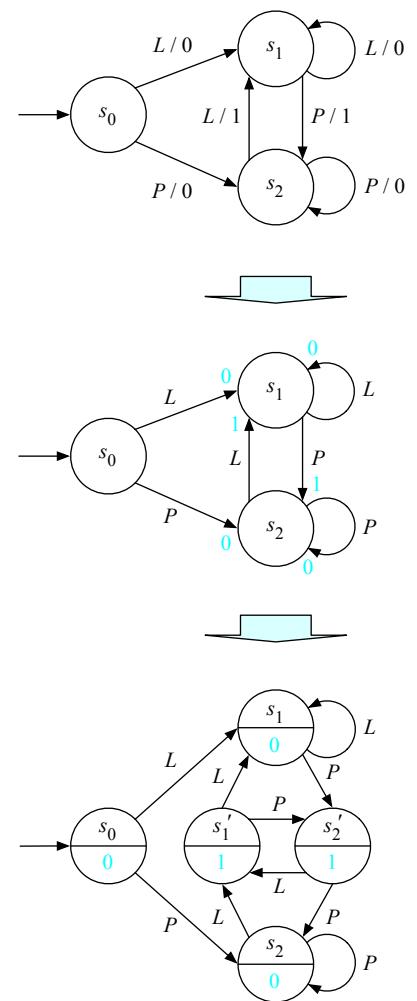
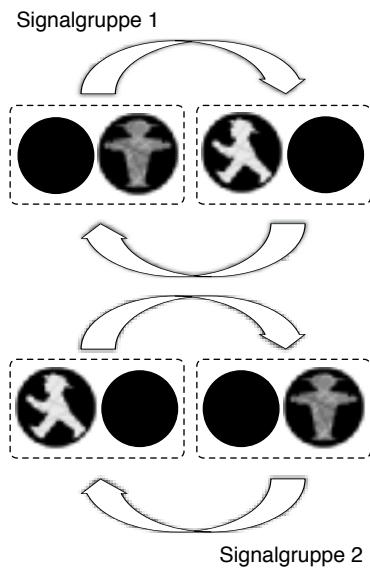
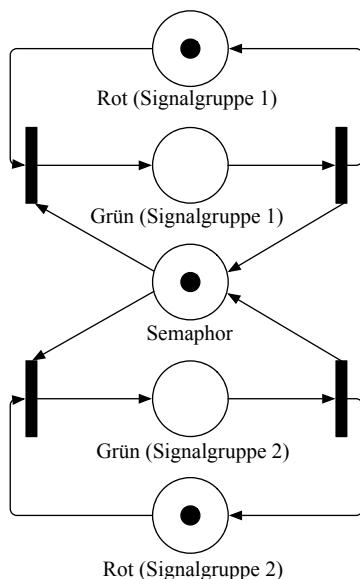


Abbildung 5.39: Moore-Konversion



„Zu keinem Zeitpunkt dürfen beide Signalgruppen ein grünes Licht zeigen.“



**Abbildung 5.40:** Modellierung einer Ampelsteuerung mit Hilfe eines Petri-Netzes

## 5.7 Petri-Netze

In den vorangegangenen Abschnitten haben wir mit dem endlichen Automaten ein mächtiges Werkzeug zur Modellierung zustandsbasierter Systeme kennen gelernt. Nichtsdestotrotz existieren Anwendungen, die mit den eingeführten Formalismen nur schwer zu erfassen sind. Beispiele sind die Beschreibung kausaler Zusammenhänge sowie die Modellierung von Nebenläufigkeit. Die entstehende Lücke wird durch *Petri-Netze* geschlossen, die genau wie endliche Automaten zustandsbasiert arbeiten, jedoch über deutlich komplexere Übergangsmechanismen verfügen. Der Name Petri-Netz geht auf den deutschen Mathematiker Carl Adam Petri zurück, der diesen Automatentypus Anfang der Sechzigerjahre ausführlich untersuchte [74].

Petri-Netze unterscheiden zwischen *Bedingungen* und *Ereignissen*. Erstere werden durch *Stellen*, letztere durch *Transitionen* beschrieben. Abbildung 5.40 zeigt ein Beispielnetz, verdeutlicht in der für Petri-Netze typischen Graphendarstellung. In dieser werden Stellen durch Kreise und Transitionen durch einen Balken, in manchen Fällen auch durch ein ungefülltes Rechteck, repräsentiert. Die Abhängigkeiten, die zwischen Stellen und Transitionen bestehen, werden durch Kanten modelliert. Jede Kante verbindet dabei eine Stelle mit einer Transition oder eine Transition mit einer Stelle, nie jedoch eine Kante mit einer Kante oder eine Stelle mit einer Stelle. Zudem sind alle Kanten eines Petri-Netzes gerichtet, so dass jeder Transition eindeutig eine Eingabe- und eine Ausgabestelle zugeordnet werden kann.

In einem Petri-Netz wird der aktuelle Zustand eines Systems durch *Marken* modelliert. Diese werden den Stellen zugeordnet und in der Graphdarstellung durch Punkte repräsentiert. Die Marken sind gewissermaßen das Elixier, das ein Petri-Netz zum Leben erweckt. Ihre Verteilung bestimmt, ob sich eine Transition in einem *aktivierten*, d.h. schaltbereiten Zustand befindet. Konkret ist eine Transition immer dann aktiviert, wenn alle Eingabestellen mindestens eine Marke enthalten. Beachten Sie, dass eine aktivierte Transition einen Schaltvorgang auslösen *kann*, aber nicht *muss*. Schaltet eine Transition, so wird eine Marke aus jeder Eingabestelle entfernt und jeder Ausgangsstelle eine zusätzliche Marke hinzugefügt. Da die Anzahl der Eingabestellen einer Transition von der Anzahl der Ausgangsstellen abweichen kann, können durch den Schaltvorgang neue Marken entstehen oder bestehende vernichtet werden.

Abbildung 5.40 demonstriert das Gesagte am Beispiel einer primitiven Ampelsteuerung. Das gezeigte Petri-Netz modelliert zwei Signalgrup-

pen, die nacheinander eine Rot- und eine Grünphase durchlaufen. Die Umschaltvorgänge der Signalgruppen können asynchron erfolgen, müssen aber jederzeit die Bedingung erfüllen, dass niemals beide Ampeln gleichzeitig Grün zeigen. Im Petri-Netz wird die Abhängigkeit durch einen Semaphor in Form einer separaten Stelle modelliert. Eine Signalgruppe kann nur dann in die Grünphase wechseln, wenn der Semaphor eine Marke enthält. Durch den Schaltvorgang wird sie entfernt und erst beim erneuten Eintreten in die Rotphase zurückgeschrieben. Durch die temporäre Wegnahme ist sichergestellt, dass die zweite Signalgruppe erst dann in die Grünphase eintreten kann, wenn sich die erste wieder in der Rotphase befindet.

Das Petri-Netz zur Ampelsteuerung verwendet typische Grundmuster zur Modellierung des Systemverhaltens. Zum einen wird der periodische Wechsel zwischen der Rot- und der Grünphase durch in Kette geschaltete Stellen realisiert. Zum anderen verwendet das Netz eine zusätzliche Stelle als Semaphor, der die unabhängig voneinander arbeitenden Signalgruppen synchronisiert. Die wichtigsten Grundmuster sind in Abbildung 5.41 in einer Übersicht zusammengefasst.

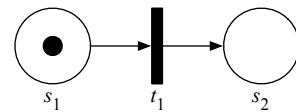
## Konfigurationen

Die Anzahl und die Verteilung der Marken eines Petri-Netzes definieren eine *Konfiguration*. Für ein Netz mit  $n$  Stellen können wir diese formal als Vektor  $\kappa \in \mathbb{N}_0^n$  auffassen, dessen  $i$ -te Komponente angibt, wie viele Marken in der  $i$ -ten Stelle vorhanden sind.

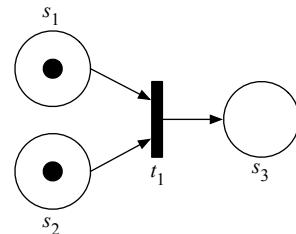
Die Vektordarstellung versetzt uns in die Lage, Petri-Netze mit den Mitteln der linearen Algebra zu modellieren und zu analysieren. Zu diesem Zweck trennen wir uns vorübergehend von der Graphendarstellung und übersetzen die Struktur eines Petri-Netzes in eine sogenannte *Inzidenzmatrix I*. Diese enthält für jede Stelle  $s_i$  eine separate Zeile und für jede Transition  $t_j$  eine separate Spalte. Der Wert des Elements  $(i, j)$  beschreibt, wie sich die Anzahl der Marken in der Stelle  $s_i$  ändert, wenn die Transition  $t_j$  schaltet. Positive Werte bedeuten, dass Marken hinzugefügt, negative Werte, dass Marken entfernt werden. Bleibt die Anzahl der Marken in einer Stelle unverändert, so enthält die Inzidenzmatrix an der entsprechenden Stelle den Wert 0.

Jede Sequenz von nacheinander schaltenden Transitionen lässt sich ebenfalls in eine Vektordarstellung übersetzen. Hierzu ordnen wir die  $i$ -te Vektorzeile der  $i$ -ten Transition zu und notieren, wie oft diese in der betrachteten Sequenz schaltet. Der entstehende Vektor wird als *Parikh-Vektor*  $\Psi$  bezeichnet. Beachten Sie, dass die Reihenfolge, in der die ein-

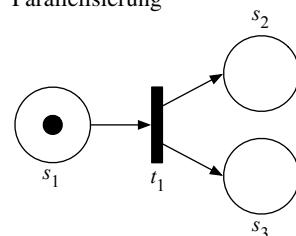
### Kettenbildung



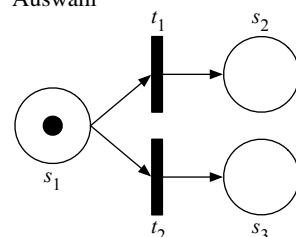
### Synchronisation



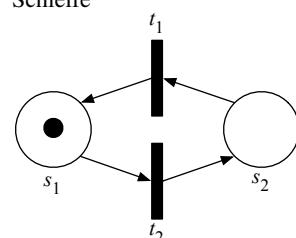
### Parallelisierung



### Auswahl



### Schleife



**Abbildung 5.41:** Petri-Netz-Topologien in der Übersicht

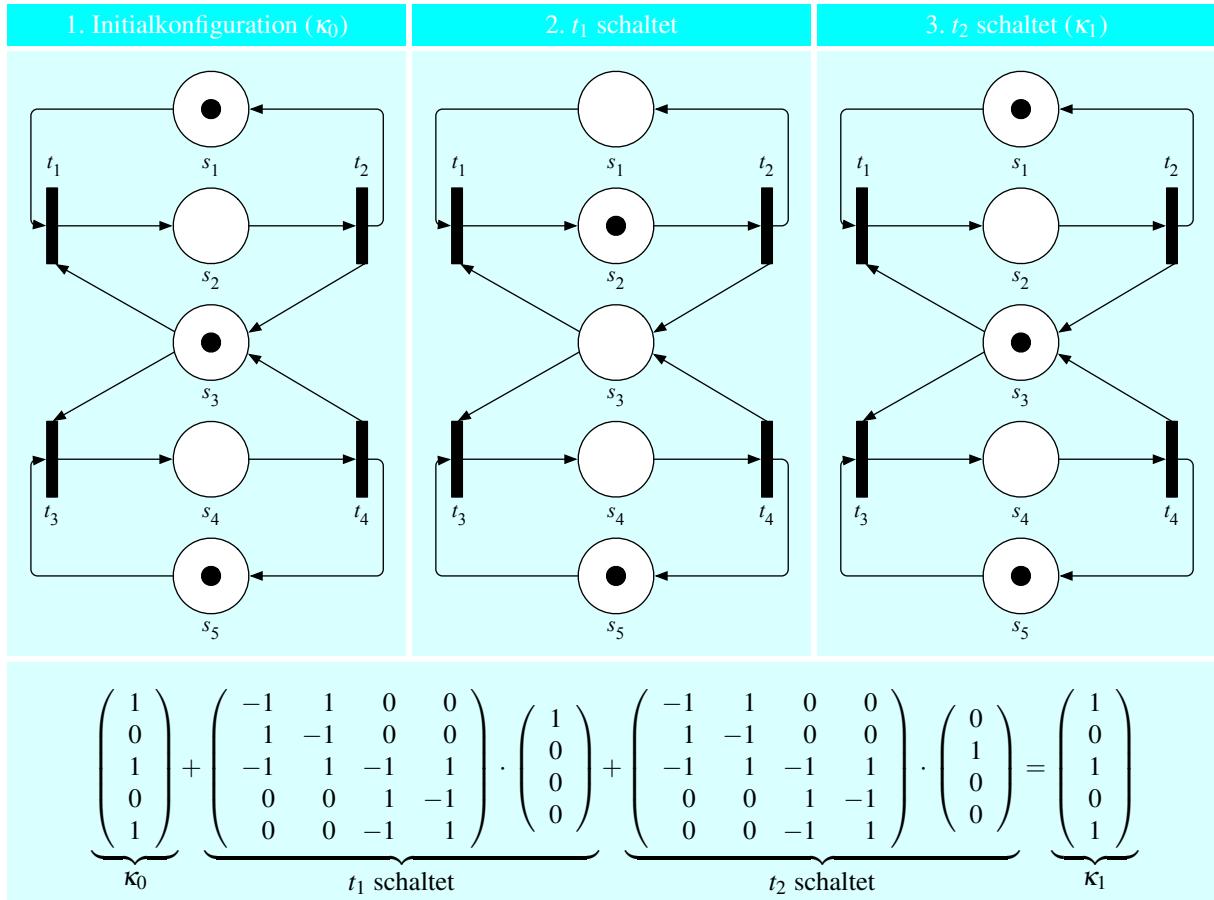


Tabelle 5.1: Vollständiger Umschaltzyklus der ersten Signalgruppe

zellen Transitionen schalten, nicht aus der Vektordarstellung abgeleitet werden kann; sie gibt ausschließlich darüber Auskunft, *wie oft* eine Transition schaltet. Nichtsdestotrotz ist der Parikh-Vektor von großem Nutzen, da wir durch die Multiplikation mit der Inzidenzmatrix die Folgekonfiguration eines Petri-Netzes berechnen können. Bezeichnen wir die aktuelle Konfiguration mit  $\kappa$  und die Folgekonfiguration mit  $\kappa'$ , so gilt die folgende Beziehung:

$$\kappa' = \kappa + I \cdot \Psi \quad (5.57)$$

Tabelle 5.1 demonstriert das Gesagte am Beispiel der weiter oben eingeführten Ampelsteuerung. Dargestellt ist ein kompletter Umschaltzyklus für die erste Signalgruppe. Ausgehend von der Initialkonfiguration

schaltet zuerst die Transition  $t_1$ . Hierbei werden die Marken in den Stellen  $s_1$  und  $s_3$  gelöscht und eine neue Marke in  $s_2$  erzeugt. Anschließend schaltet die Transition  $t_2$  und versetzt das Petri-Netz zurück in die Anfangskonfiguration.

Gleichung (5.57) lässt sich in direkter Weise für die *Erreichbarkeitsanalyse* eines Petri-Netzes einsetzen. Wir nennen eine Konfiguration  $\kappa_1$  erreichbar, wenn eine Sequenz von schaltenden Transitionen existiert, mit der die Anfangskonfiguration  $\kappa_0$  in  $\kappa_1$  überführt wird. Falls eine solche Sequenz existiert, besitzt die *Markierungsgleichung*

$$I \cdot \Psi = \kappa_1 - \kappa_0 \quad (5.58)$$

eine Lösung in den natürlichen Zahlen. Beachten Sie, dass die Umkehrung dieser Aussage nicht gilt, d. h., nicht jede natürlichezahlige Lösung lässt sich auch wirklich in eine entsprechende Transitionssequenz umsetzen. Als Beispiel betrachten wir das Petri-Netz in Abbildung 5.42. Die Lösbarkeit der Markierungsgleichung suggeriert, dass sich eine Konfiguration erreichen lässt, in der ausschließlich die Stelle  $s_3$  mit einer Marke befüllt ist. In Wirklichkeit lässt sich diese Konfiguration nicht herstellen. Die unmarkierte Stelle  $s_2$  sorgt dafür, dass die Transition  $t_1$  niemals schalten kann.

Erreichbarkeitsuntersuchungen gehören zu den wichtigsten Fragestellungen, die mit Hilfe von Petri-Netzen beantwortet werden können. Neben diesen werden Petri-Netze zur Analyse der folgenden Systemeigenschaften genutzt:

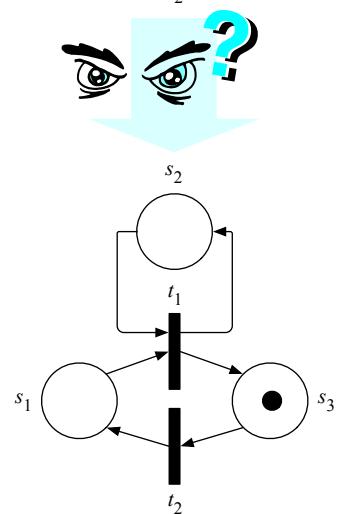
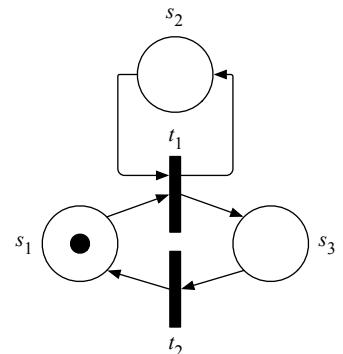
### Lebendigkeit

Ein Petri-Netz heißt *lebendig*, wenn es für jede Transition  $t$  die Eigenschaft erfüllt, dass sich aus jeder erreichbaren Konfiguration eine andere Konfiguration erzeugen lässt, in der  $t$  aktiviert ist. Tabelle 5.2 (links) zeigt ein Petri-Netz, das die Lebendigkeitseigenschaft nicht erfüllt. Die Transition  $t_3$  ist bereits aus der Startkonfiguration nicht aktivierbar, da die Stellen  $s_1$  und  $s_2$  nur wechselweise eine Marke enthalten. Damit  $t_3$  schalten kann, müssten jedoch beide Stellen zur selben Zeit eine Marke enthalten.

### Sicherheit

Ein Petri-Netz heißt *sicher*, wenn die Anzahl der Markierungen in jeder Stelle  $s$  einen gewissen Wert  $C(s)$  nicht übersteigt.  $C(s)$  heißt die *Kapazität* von  $s$ . Das mittlere der drei in Tabelle 5.2 dargestellten Petri-Netze ist unsicher. In diesem Beispiel werden die Transitionen  $t_1$  und  $t_2$  abwechselnd aktiviert und immer dann, wenn  $t_2$  schaltet,

### Konfigurationsübergang



### Markierungsgleichung

$$\begin{pmatrix} -1 & 1 \\ 0 & 0 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

**Abbildung 5.42:** Die Lösbarkeit der Markierungsgleichung ist ein notwendiges, aber kein hinreichendes Kriterium für die Erreichbarkeit einer Konfiguration. Obwohl die Markierungsgleichung in diesem Beispiel eine Lösung in den natürlichen Zahlen besitzt, ist der dargestellte Konfigurationsübergang nicht möglich.

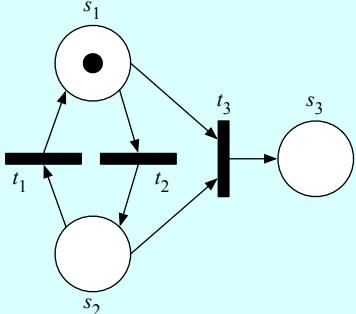
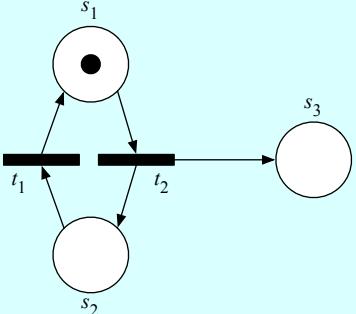
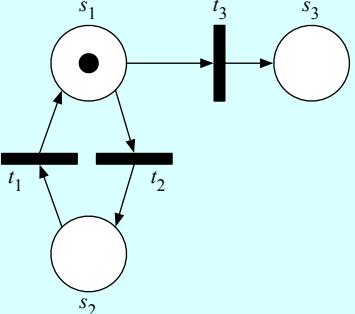
Beispiel 1	Beispiel 2	Beispiel 3
		
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> nicht lebendig</li> <li><input checked="" type="checkbox"/> sicher</li> <li><input checked="" type="checkbox"/> verklemmungsfrei</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> lebendig</li> <li><input checked="" type="checkbox"/> nicht sicher</li> <li><input checked="" type="checkbox"/> verklemmungsfrei</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> nicht lebendig</li> <li><input checked="" type="checkbox"/> sicher</li> <li><input checked="" type="checkbox"/> nicht verklemmungsfrei</li> </ul>

Tabelle 5.2: Petri-Netz-Eigenschaften

eine zusätzliche Marke in der Stelle  $s_3$  erzeugt. Die Anzahl der Marken nimmt hierdurch kontinuierlich zu und ist damit nach oben unbeschränkt.

#### ■ Verklemmungsfreiheit

Ein Petri-Netz ist *verklemmungsfrei*, wenn zu jeder Zeit mindestens eine Transition aktiviert ist. Ist ein Petri-Netz nicht verklemmungsfrei, so lässt sich aus der Startmarkierung eine Konfiguration erzeugen, in der keine aktiven Transitionen existieren. Es entsteht ein Systemstillstand (*Deadlock*). Innerhalb des rechten Petri-Netzes in Tabelle 5.2 lässt sich eine solche Situation leicht herbeiführen. Sobald die Transition  $t_3$  schaltet, lässt sich weder  $t_1$ ,  $t_2$  noch  $t_3$  erneut aktivieren.

Die Lebendigkeit und die Verklemmungsfreiheit sind keine vollständig unabhängigen Systemeigenschaften. So ist jedes lebendige Petri-Netz immer auch verklemmungsfrei. Die Umkehrung dieser Schlussfolgerung gilt nicht, wie wir am Beispiel des linken Petri-Netzes in Abbildung 5.2 demonstriert haben. Obwohl das Netz die Lebendigkeiteigenschaft nicht erfüllt, kommt es zu keinem Deadlock, da zu jedem Zeitpunkt eine aktivierte Transition existiert.

## 5.8 Zelluläre Automaten

■ Hexagon-Nachbarschaft

In diesem Abschnitt wollen wir einen einführenden Blick auf ein Automatenmodell werfen, das sich grundlegend von den bisher betrachteten unterscheidet. Die Rede ist von *zellulären Automaten*, deren Ursprünge bis in die Vierzigerjahre des letzten Jahrhunderts zurückreichen, in der wissenschaftlichen Literatur aber erst Jahre später aufgearbeitet wurden [71]. Eingesetzt wird das Modell vor allem zur Beschreibung dynamischer, selbstorganisierender Systeme.



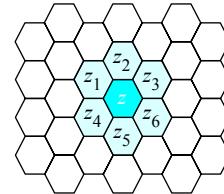
### Definition 5.16 (Zellulärer Automat)

Ein zellulärer Automat (*cellular automaton*), kurz ZA, ist ein 4-Tupel  $(Z, S, v, \delta)$ . Er besteht aus

- der *Zellmenge*  $Z$ ,
- der endlichen *Zustandsmenge*  $S$ ,
- der *Nachbarschaftsfunktion*  $v : Z \rightarrow Z^n$ ,
- der *Zustandsübergangsfunktion*  $\delta : S \times S^n \rightarrow S$

Grob gesprochen setzt sich ein zellulärer Automat aus einer großen Menge  $Z$  von Elementarautomaten zusammen, die wir im Folgenden als *Zellen* bezeichnen. Genau wie im Falle des klassischen Automaten befindet sich eine Zelle zu jedem Zeitpunkt in einem von endlich vielen Zuständen. Die Menge der erlaubten Zustände bezeichnen wir mit  $S$ . In den folgenden Beispielen werden wir die Zustände allesamt durch verschiedene Farben darstellen, so dass  $S$  in diesen Fällen dem verfügbaren Farvvorrat entspricht.

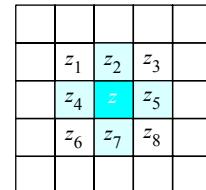
In einem zellulären Automaten agieren die einzelnen Zellen nicht unabhängig voneinander. Ganz im Gegenteil: Sie stehen in ständiger Interaktion. Wie sich eine Zelle verhält, wird zum einen durch ihren eigenen, aktuell eingenommenen Zustand und zum anderen durch den Zustand ihrer Nachbarzellen bestimmt. Die Nachbarschaftsbeziehung eines zellulären Automaten wird durch die Funktion  $v$  bestimmt.  $v$  bildet eine Zelle  $z$  auf einen  $n$ -elementigen Vektor ab, der alle Nachbarn von  $z$  enthält. Abbildung 5.43 zeigt, dass mit  $v$  beliebige Topologien von Nachbarschaftsbeziehungen modelliert werden können; hier demonstriert am Beispiel einer hexagonalen Anordnung, in der jede Zelle von jeweils 6 Nachbarzellen umgeben wird. Am häufigsten werden jedoch die folgenden beiden Nachbarschaftsbeziehungen eingesetzt:



$$v(z) = \{z_1, z_2, z_3, z_4, z_5, z_6\}$$

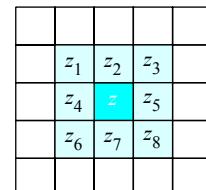
**Abbildung 5.43:** Mit Hilfe der Nachbarschaftsfunktion lassen sich beliebige Topologien modellieren.

■ Von-Neumann-Nachbarschaft



$$v(z) = \{z_2, z_4, z_5, z_7\}$$

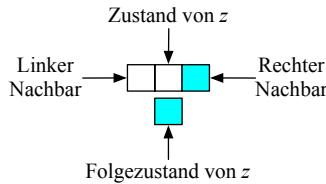
■ Moore-Nachbarschaft



$$v(z) = \{z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8\}$$

**Abbildung 5.44:** Die Von-Neumann- und die Moore-Nachbarschaft im Vergleich

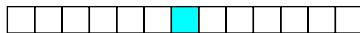
■ Regelschema



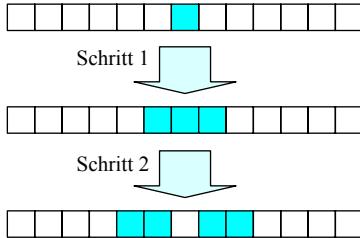
■ Vollständiger Regelsatz

Regel 1	Regel 2	Regel 3	Regel 4
██████	█████C	████C█	████CC
Regel 5	Regel 6	Regel 7	Regel 8
C█████	CC█C	CC█C	CC

■ Initiale Konfiguration



■ Automat in Aktion



**Abbildung 5.45:** Lineare zelluläre Automaten basieren auf einer eindimensionalen Zell-Topologie. Der dargestellte Regelsatz definiert einen zweifarbigen Automaten. Welche Farbe eine Zelle im nächsten Rechenschritt annimmt, wird zum einen durch ihre momentane Einfärbung und zum anderen durch die Einfärbungen der beiden Nachbarzellen bestimmt.

■ Von-Neumann-Nachbarschaft

Sind die Zellen in Form von Quadranten auf einer zweidimensionalen Fläche angeordnet, so besteht eine *Von-Neumann-Nachbarschaft* genau dann, wenn sich die betrachteten Zellen eine Kante teilen. Wir sprechen in diesem Zusammenhang auch von einer *4er-Nachbarschaft* (vgl. Abbildung 5.44 oben).

■ Moore-Nachbarschaft

Eine *Moore-Nachbarschaft* wird auch als *8er-Nachbarschaft* bezeichnet. Sie besteht bereits dann, wenn sich die betrachteten Zellen eine Ecke teilen (vgl. Abbildung 5.44 unten). Die Von-Neumann-Nachbarschaft ist vollständig in der Moore-Eigenschaft erhalten.

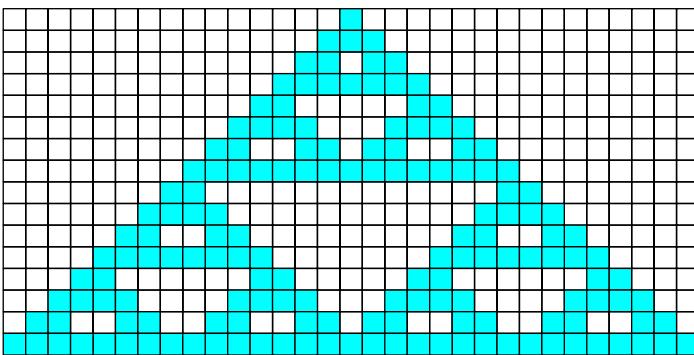
Nachdem wir den grundsätzlichen Aufbau eines zellulären Automaten erarbeitet haben, ist es an der Zeit, das genaue Schaltverhalten zu untersuchen. Befinden sich die Nachbarzellen  $z_1, \dots, z_n$  von  $z$  in den Zuständen  $s_{z_1}, \dots, s_{z_n}$ , so lässt sich der Nachfolgezustand von  $z$  wie folgt berechnen:

$$s'_z = \delta(s_z, s_{z_1}, \dots, s_{z_n}) \quad (5.59)$$

Jede Auswertung von  $\delta$  entspricht der Änderung des Zustands einer einzelnen Zelle.

Den aktuellen Zustand einer Zelle  $z$  bezeichnen wir als *lokale Konfiguration*. Die Gesamtheit aller lokalen Konfigurationen heißt *globale Konfiguration*; sie definiert den Zustand, in dem sich der zelluläre Automat gegenwärtig befindet. Im Gegensatz zu den konventionellen endlichen Automaten werden für die Berechnung des Konfigurationsübergangs keine Eingabezeichen ausgewertet, so dass das zukünftige Verhalten bereits vollständig durch den gegenwärtig eingenommenen Zustand und die Zustände der Nachbarzellen festgelegt ist. In der Einbeziehung der Nachbarzellen liegt die Stärke zellulärer Automaten. Die permanente Rückkopplung macht es möglich, durch die Angabe einiger weniger, einfach aufgebauter Regeln ein komplexes, selbstorganisierendes Verhalten zu erzeugen.

Im Folgenden wollen wir mit den *linearen Automaten* eine Untergruppe der zellulären Automaten genauer untersuchen, die durch die detaillierteren Forschungsarbeiten des britischen Mathematikers Stephen Wolfram einen hohen Bekanntheitsgrad erlangen konnte [99]. Hierbei handelt es sich um zelluläre Automaten mit einer eindimensionalen Topologie, in der wir uns alle Zellen wie auf einer Schnur aufgereiht vorstellen können. Zwei Zellen gelten als benachbart, wenn diese unmittelbar aneinanderliegen. In linearen Automaten liegt sowohl eine Von-Neumann-



**Abbildung 5.46:** Das Sierpinski-Dreieck, erzeugt durch einen zellulären Automaten. Im Bereich der fraktalen Geometrie wird das Sierpinski-Dreieck häufig verwendet, um das Prinzip der Selbstähnlichkeit zu demonstrieren. Grob gesprochen ist ein Objekt genau dann selbstähnlich, wenn es als Ganzes die gleiche Struktur aufweist wie seine Teile. Am Beispiel des Sierpinski-Dreiecks lässt sich die Eigenschaft gut erkennen. Trennen wir eines der drei Teildreiecke heraus, so erhalten wir erneut ein Sierpinski-Dreieck, das in seiner Struktur dem ursprünglichen gleicht.

als auch eine Moore-Nachbarschaft vor; beide Konzepte sind im eindimensionalen Raum identisch.

Abbildung 5.45 zeigt einen linearen Automaten mit zwei Zuständen. Wie oben angedeutet, codieren wir die Zustände durch das Einfärben der Zellen und bezeichnen einen Automaten dieser Bauart auch als *zweifarbig*.  $\delta(s_z, s_{z_l}, s_{z_r})$  ist die Folgefärbung des Zustands  $z$  und berechnet sich aus der aktuellen Farbe  $s_z$  von  $z$  sowie den Farben  $s_{z_l}$  und  $s_{z_r}$  seiner beiden Nachbarzellen  $z_l$  und  $z_r$ .

Wie sich der Automat in Aktion verhält, lässt sich in der unteren Hälfte von Abbildung 5.45 beobachten. Zunächst legen wir die *Startkonfiguration* fest. In unserem Beispiel sieht diese so aus, dass alle Zellen bis auf eine weiß eingefärbt sind. Auf der initialen Konfiguration startend, führt der zelluläre Automat jetzt sukzessiv eine Folge von Arbeitsschritten aus. In jedem Schritt gehen alle Zellen synchron in ihren Folgezustand über, so dass an allen Positionen ein potenzieller Farbwechsel stattfindet. Tragen wir die nacheinander berechneten Konfigurationen untereinander auf, so entsteht ein zweidimensionales Bild, in dem die vertikale Achse die Zeitachse bildet und jeder horizontale Schnitt einer einzelnen Konfiguration entspricht.

Abbildung 5.46 klärt auf, welches Bild der weiter oben definierte Beispielautomat erzeugt. Die gewählten Produktionsregeln lassen das sogenannte *Sierpinski-Dreieck* entstehen – eine heute gut untersuchte Struktur aus dem Bereich der fraktalen Geometrie [65, 84].

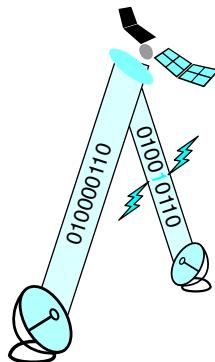
In Kapitel 6 werden wir den zellulären Automaten erneut begegnen. Dort werden wir zeigen, dass dieser Automatentypus stark genug ist, um mit wenigen Modifikationen eine Turing-Maschine zu simulieren.

## 5.9 Übungsaufgaben

**Aufgabe 5.1**

**Webcode  
5237**

Im Bereich der fehlererkennenden Datenübertragung spielt der *Paritätscode* eine wichtige Rolle. Die Codierung verfolgt die Idee, ausschließlich Datenpakete zu versenden, die eine gerade Anzahl Einsen aufweisen. Hierzu werden die Datenpakete vor dem Versenden um ein *Paritätsbit* ergänzt, das die Gesamtzahl der Einsen gerade werden lässt. Die folgende Tabelle listet exemplarisch alle Codewörter des 5-Bit-Paritätscodes auf.  $x_0, \dots, x_3$  entsprechen den Datenbits und  $p$  dem künstlich hinzugefügten Paritätsbit.



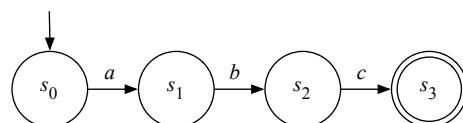
$x_3$	$x_2$	$x_1$	$x_0$	$p$
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	0
0	1	0	0	1
0	1	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	0

- Erzeugen Sie einen DEA, der die Integrität eines empfangenen Datenpakets überprüft und alle korrekt übertragenen Wörter akzeptiert. Wurde ein einzelnes Bit des Datenpakets während der Übertragung verfälscht, so soll der Automat das Eingabewort zurückweisen.
- Wie verhält sich der von Ihnen konstruierte Automat, falls zwei Bits während der Datenübertragung verfälscht wurden?

**Aufgabe 5.2**

**Webcode  
5866**

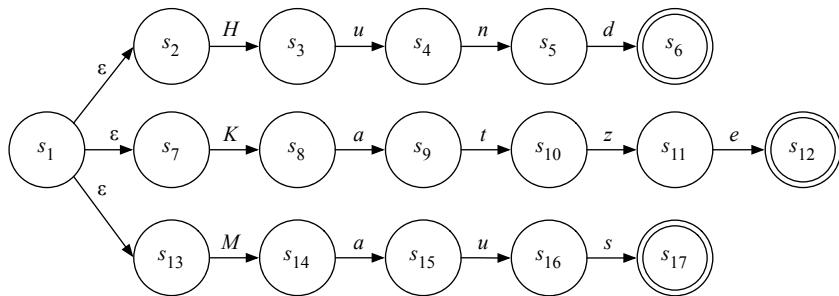
Der endliche Automat  $A = (\{s_0, s_1, s_2, s_3\}, \{a, b, c\}, \delta, s_0)$  sei durch das folgende Zustandsübergangsdiagramm gegeben:



A akzeptiert die Sprache  $L = \{abc\}$ . Handelt es sich hier um einen DEA oder um einen NEA? Begründen Sie Ihre Antwort.

Gegeben sei der folgende nichtdeterministische  $\varepsilon$ -Akzeptor, der auf die Erkennung bestimmter Worte ausgelegt ist.

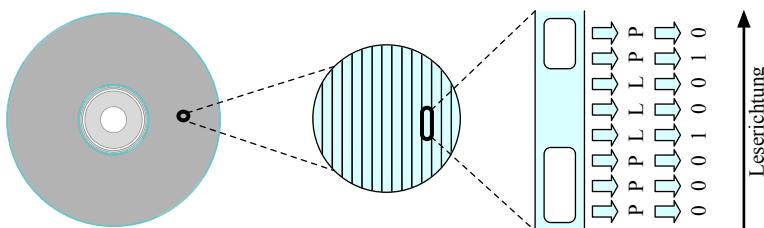
**Aufgabe 5.3**

**Webcode  
5892**


- Formen Sie den Automaten so um, dass er nur einen einzigen Endzustand besitzt.
- Lässt sich die angewendete Umformung auf einen beliebigen  $\varepsilon$ -NEA übertragen?
- Lässt sich jeder *DEA* so umformen, dass er genau einen Endzustand besitzt?

Auf der physikalischen Ebene arbeiten CDs, DVDs und Blu-ray discs alle nach dem gleichen Grundprinzip. Die gespeicherten Daten werden als Folge mikroskopisch kleiner *Pits* (P) und *Lands* (L) auf das Trägermaterial aufgebracht. Pits besitzen die Eigenschaft, den einfallenden Laserstrahl zu streuen, und entsprechen bei nichtbeschreibbaren Medien kleinen Einkerbungen im Trägermaterial. Beim Lesen eines optischen Datenträgers wird der P-L-Datenstrom zunächst in einen binären Datenstrom aus Nullen und Einsen übersetzt. Jeder Übergang von P nach L oder von L nach P entspricht einer Eins, ansonsten wird eine Null codiert.

**Aufgabe 5.4**

**Webcode  
5295**


Konstruieren Sie einen Transduktor, der eine gegebene P-L-Sequenz in den zugehörigen 0-1-Datenstrom zurückübersetzt.

**Aufgabe 5.5****Webcode  
5876**

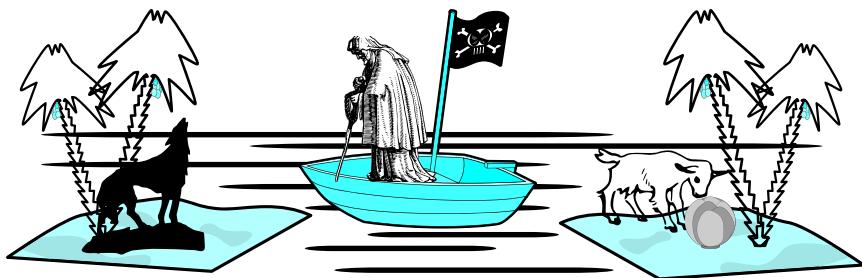
Im *BCD-Code* wird eine Dezimalzahl codiert, indem jede Ziffer in ein 4 Bit breites Datenpaket übersetzt wird:

Dezimalziffer	BCD-Codewort	Dezimalziffer	BCD-Codewort
0	0000	5	0101
1	0001	6	0110
2	0010	7	0111
3	0011	8	1000
4	0100	9	1001

Konstruieren Sie einen seriellen BCD-Dezimal-Wandler, der einen BCD-codierten Datenstrom einliest und in die ursprüngliche Dezimaldarstellung zurückübersetzt.

**Aufgabe 5.6****Webcode  
5922**

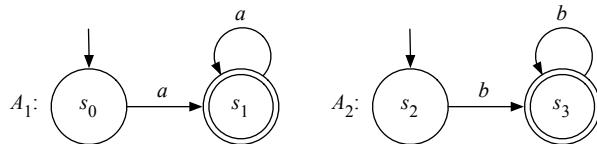
Das Wolf-Ziege-Kohlkopf-Problem, kurz WZK-Problem, ist ein bekanntes Denkspiel. Ein Bauer ist mit der Aufgabe betraut, einen Wolf, eine Ziege und einen Kohlkopf auf die andere Uferseite zu bringen. Ihm steht nur ein kleines Boot zur Verfügung, so dass er jeweils nur einen der drei transportieren kann. Lässt er dabei die beiden Tiere alleine, so wird der Wolf die Ziege reißen. Die Ziege ist nicht weniger unschuldig und wird den Kohlkopf fressen, sobald sie der Bauer alleine lässt.



Modellieren Sie das WZK-Problem mit Hilfe eines endlichen Automaten. Dieser soll so konstruiert werden, dass jeder Zustand eindeutig eine bestimmte Position der Beteiligten codiert. Beschriften Sie die Transition mit einem Buchstaben aus der Menge  $\{BW, BZ, BK\}$ , je nachdem ob der Bauer den Wolf, die Ziege oder den Kohlkopf an das andere Ufer bringt.

- Wie muss der Bauer die Überfahrt durchführen, damit alle Beteiligten wohlbehalten an das andere Ufer gelangen?
- Lassen sich die Lösungen des WZK-Problems direkt aus der Menge der akzeptierten Eingabewörter des von Ihnen konstruierten Automaten ableiten?

Die Akzeptoren  $A_1$  und  $A_2$  seien wie folgt gegeben:


**Aufgabe 5.7**

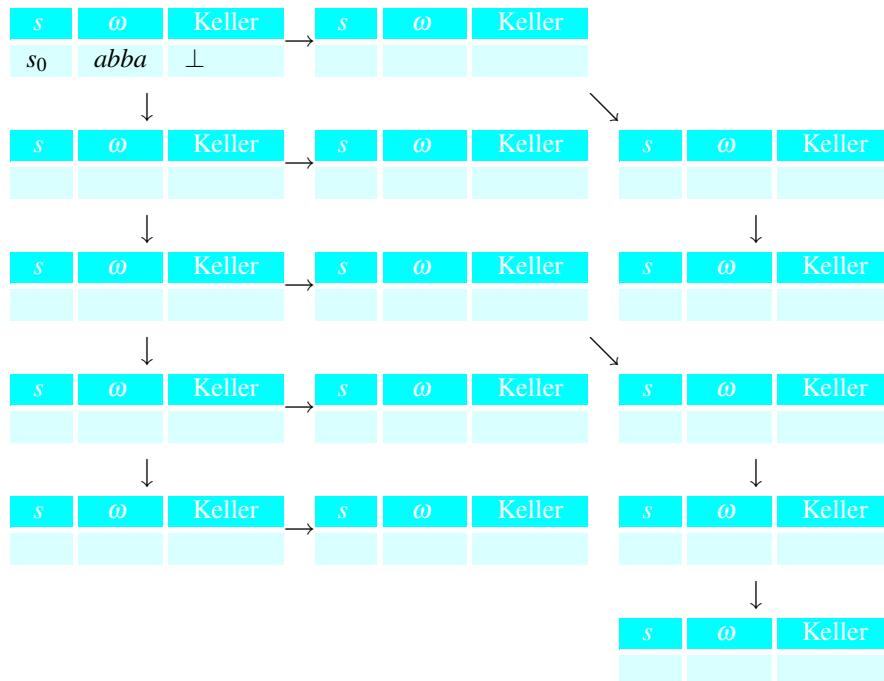
**Webcode  
5983**

- Welche Sprache akzeptieren  $A_1$  und  $A_2$ ?
- Erzeugen Sie aus  $A_1$  und  $A_2$  einen Automaten  $A$  mit  $\mathcal{L}(A) = \mathcal{L}(A_1) \cup \mathcal{L}(A_2)$ .
- Erzeugen Sie aus  $A_1$  und  $A_2$  einen Automaten  $A$  mit  $\mathcal{L}(A) = \mathcal{L}(A_1) \cap \mathcal{L}(A_2)$ .

In diesem Kapitel haben Sie einen Kellerautomaten kennengelernt, der die Palindromsprache

$$L_{\text{Pal}} := \{\varepsilon\} \cup \{\sigma_1 \dots \sigma_n \sigma_n \dots \sigma_1 \mid n \in \mathbb{N}, \sigma_i \in \{a, b\}\} \quad (5.60)$$

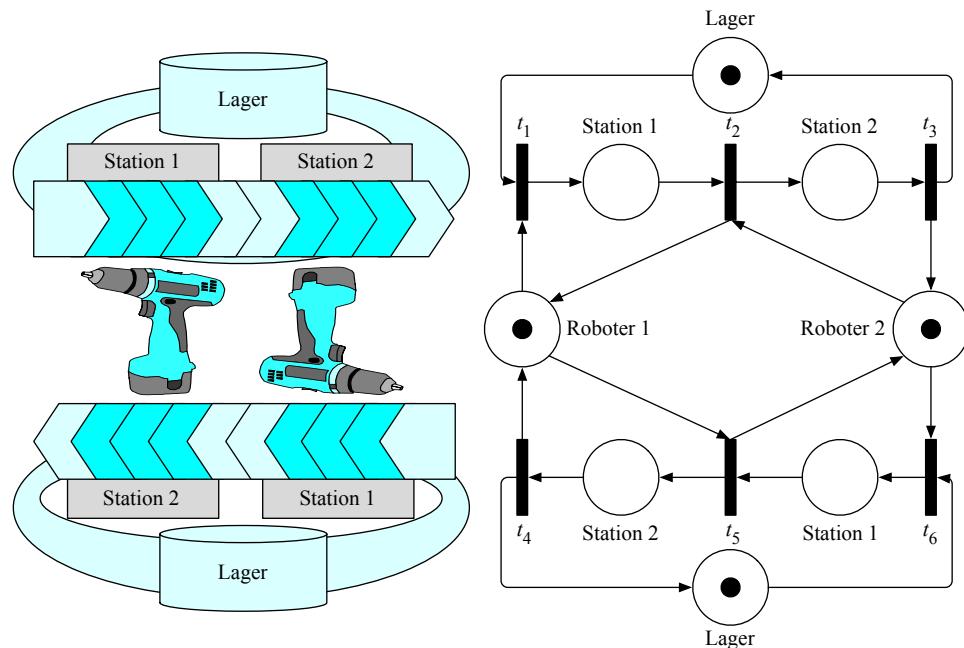
akzeptiert. Die formale Definition des Automaten ist in Abbildung 5.27 dargestellt. Vervollständigen Sie das folgende Diagramm, das alle Konfigurationsübergänge für das Eingabewort  $abba$  zusammenfasst:


**Aufgabe 5.8**

**Webcode  
5929**

**Aufgabe 5.9****Webcode  
5482**

In diesem Kapitel haben Sie gelernt, wie sich dynamische Systemeigenschaften mit Hilfe von Petri-Netzen beschreiben lassen. In der vorliegenden Übungsaufgabe wird ein Petri-Netz verwendet, um die Abläufe einer industriellen Produktionsanlage zu modellieren. Unsere fiktive Produktionsstraße besteht aus zwei Arbeitsstationen, an denen fest montierte Industrieroboter ihre Arbeit verrichten. An den Robotern werden zwei in entgegengesetzte Richtungen laufende Förderbänder vorbeigeführt. Entsprechend den eingestellten Laufrichtungen wird ein Werkstück im oberen Kreislauf zuerst durch den linken und anschließend durch den rechten Roboter bearbeitet. Im unteren Kreislauf ist die Reihenfolge genau andersherum.

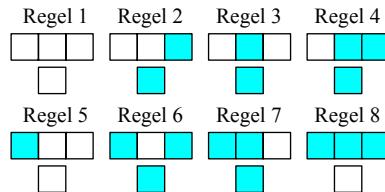


Ein Werkstück wird zunächst aus dem Lager entnommen, danach durch beide Arbeitsstationen geführt und anschließend in das Lager zurückbefördert. Erst danach kann die Arbeit mit dem nächsten Werkstück beginnen. Die Roboter können Werkstücke auf beiden Förderbändern bearbeiten, aber nicht gleichzeitig beide Bänder bedienen.

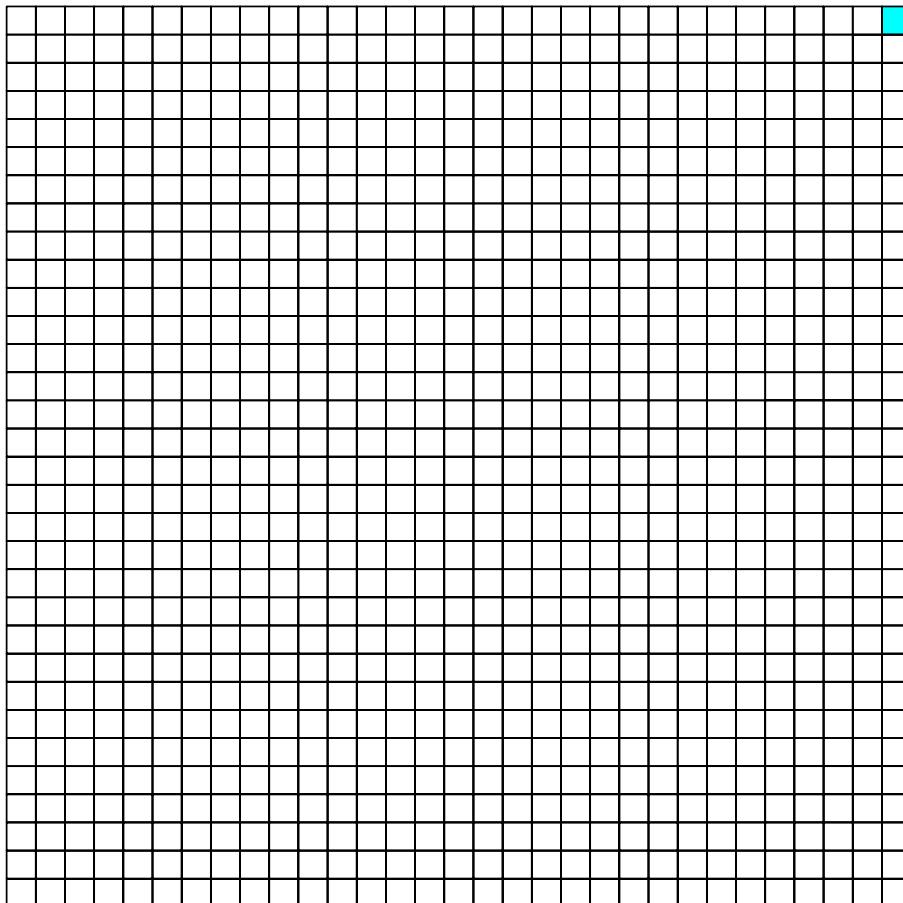
Rechts ist das Petri-Netz-Modell der Produktionsstraße abgebildet. Lager, Roboter und Arbeitsstationen werden durch separate Stellen modelliert. Per Definition ist eine Arbeitsstation genau dann belegt, wenn sich eine Marke in der entsprechenden Stelle befindet.

- Analysieren Sie das Petri-Netz. Zeigen Sie, dass ein Systemstillstand eintreten kann.
- Modifizieren Sie das Modell so, dass ein verklemmungsfreies Petri-Netz entsteht.

In Abschnitt 5.8 haben Sie einen zellulären Automaten zur Erzeugung des Sierpinski-Dreiecks kennen gelernt. In dieser Übungsaufgabe wollen wir die Entstehungsregeln minimal modifizieren:

**Aufgabe 5.10****Webcode****5599**

Stellen Sie fest, wie sich das Verhalten des Automaten geändert hat. Vervollständigen Sie hierzu das folgende Diagramm:





## 6 Berechenbarkeitstheorie

---

In diesem Kapitel werden Sie ...

- den abstrakten Begriff der Berechenbarkeit durchdringen,
- einfache Programme in der Loop-, While- und Goto-Sprache verfassen,
- den Aufbau primitiv-rekursiver Funktionen verstehen,
- die Funktionsweise und die Ausdrucksfähigkeit von Turing-Maschinen erforschen,
- einen Einblick in Registermaschinen und das Lambda-Kalkül erhalten,
- die Kernaussage der Church'schen These nachvollziehen,
- die theoretischen Grenzen der Berechenbarkeit erfahren,
- eine Reihe von unentscheidbaren Problemen kennen lernen.



■ Beispiel 1

**add.loop**

```

1  x0 := x1 ;
2  loop x2 do
3      x0 := succ(x0)
4  end

```

■ Beispiel 2

**triple.loop**

```

1  x0 := x1;
2  loop x1 do
3      x0 := succ(x0)
4  end;
5  loop x1 do
6      x0 := succ(x0)
7  end

```

**Abbildung 6.1:** Zwei Programme der Loop-Sprache. Das erste Programm implementiert die Addition zweier natürlicher Zahlen ( $x_0 := x_1 + x_2$ ), das zweite verdreifacht den Eingabewert ( $x_0 := 3 \cdot x_1$ ).

## 6.1 Berechnungsmodelle

Jeder von uns besitzt eine intuitive Vorstellung davon, was es bedeutet, etwas zu *berechnen*. Bei genauerer Betrachtung entpuppen sich unsere Gedankenmodelle jedoch schnell als zu vage, um daraus handfeste Schlussfolgerungen abzuleiten. Insbesondere reichen unsere informellen Vorstellungen nicht aus, um belastbare Aussagen über die Unberechenbarkeit bestimmter Funktionen zu treffen oder den schon mehrmals recht lax verwendeten Begriff der Entscheidbarkeit auf seine eigenen Füße zu stellen. Kurzum: Wir kommen nicht umhin, den Begriff der *Berechenbarkeit* formal zu präzisieren. Zu diesem Zweck wurde die Berechenbarkeitstheorie geschaffen, die uns die benötigte Grundlage in Form von formalen Berechnungsmodellen zur Verfügung stellt.

In den folgenden Abschnitten werden wir die aus heutiger Sicht wichtigsten Berechnungsmodelle genauer untersuchen. Lassen Sie sich nicht von der großen Anzahl an Modellen abschrecken, auch wenn die Stoffmenge erdrückend erscheint! In Abschnitt 6.2 werden wir im Zusammenhang mit der *Church'schen These* zeigen, dass sich die meisten Modelle nur äußerlich unterscheiden und denselben Berechenbarkeitsbegriff begründen. In diesem Sinne wird sich die Berechenbarkeit als eine tiefgründige Eigenschaft erweisen, die unabhängig von ihrer Form existiert und sich durch diese in keiner Weise beeinflussen lässt.

### 6.1.1 Loop-Programme

Wir beginnen mit der Diskussion der *Loop-Sprache*, dem einfachsten Berechnungsmodell dieses Kapitels.



#### Definition 6.1 (Loop-Programme)

Ein Loop-Programm besteht aus den folgenden Komponenten:

- der *Konstanten* 0,
- den *Variablen*  $x_0, x_1, x_2, \dots$ ,
- den *Operatoren* succ und pred,
- dem *Zuweisungsoperator* ':=',
- dem *Kompositionssymbol* ';' ,
- dem *Schleifenkonstrukt* loop do end

Abbildung 6.1 zeigt, wie sich die einzelnen Sprachkonstrukte zu komplexeren Programmen zusammensetzen lassen. Die Syntax folgt den Konstruktionsprinzipien moderner Programmiersprachen, so dass wir auf eine ausschweifende Definition an dieser Stelle verzichten wollen. Über die Semantik der Loop-Sprache wollen wir dagegen nicht so schnell hinweggehen.

Im Zentrum der Loop-Semantik steht der *Speichervektor*

$$\mathbf{v} = (x_0, x_1, \dots, x_n, x_{n+1}, \dots, x_m), \quad (6.1)$$

der den Zustand aller Programmvariablen zu einem bestimmten Zeitpunkt beschreibt. Per Definition werden die Eingabewerte in den Variablen  $x_1, \dots, x_n$  bereitgestellt und das berechnete Ergebnis in  $x_0$  abgelegt. Die restlichen Variablen dienen der internen Speicherung von Zwischenergebnissen. Im Folgenden bezeichnen wir mit  $\mathbf{v}[x_i \leftarrow y]$  den Vektor  $\mathbf{v}$ , in dem die  $i$ -te Komponente durch den Wert  $y$  ersetzt wurde.

Die *Übergangsfunktion*  $\delta(\mathbf{v}, P)$  nimmt einen Speichervektor  $\mathbf{v}$  sowie ein Loop-Programm  $P$  entgegen und berechnet daraus den Speichervektor, der aus  $\mathbf{v}$  nach der Ausführung von  $P$  entsteht. Wir definieren  $\delta$  induktiv über die Programmstruktur:

#### ■ Wertzuweisung

$$\delta(\mathbf{v}, x_i := 0) := \mathbf{v}[x_i \leftarrow 0] \quad (6.2)$$

$$\delta(\mathbf{v}, x_i := \text{succ}(x_j)) := \mathbf{v}[x_i \leftarrow x_j + 1] \quad (6.3)$$

$$\delta(\mathbf{v}, x_i := \text{pred}(x_j)) := \begin{cases} \mathbf{v}[x_i \leftarrow x_j - 1] & \text{für } x_j > 0 \\ \mathbf{v} & \text{für } x_j = 0 \end{cases} \quad (6.4)$$

#### ■ Komposition

$$\delta(\mathbf{v}, P_1; P_2) := \delta(\delta(\mathbf{v}, P_1), P_2) \quad (6.5)$$

#### ■ Loop-Schleife

$$\delta(\mathbf{v}, \text{loop } x_i \text{ do } P) := \delta(\mathbf{v}, \underbrace{P; P; \dots; P}_{x_i \text{ Kopien}}) \quad (6.6)$$

Abbildung 6.2 zeigt, wie sich das oben eingeführte Loop-Programm add.loop mit Hilfe der Übergangsfunktion schrittweise simulieren lässt. Sind die Register  $x_1$  und  $x_2$ , wie in unserem Beispiel, mit den Werten 3 und 4 vorinitialisiert, so finden wir in Register  $x_0$  am Ende den erwarteten Ergebniswert 7 vor.

Die Übergangsfunktion  $\delta$  setzen wir nun ein, um den Begriff der Loop-Berechenbarkeit formal zu definieren:

$$\begin{aligned} & \delta((0, 3, 4), \\ & \quad x_0 := x_2; \\ & \quad \text{loop } x_1 \text{ do } x_0 := \text{succ}(x_0) ) \\ &= \delta(\delta((0, 3, 4), x_0 := x_2), \\ & \quad \text{loop } x_1 \text{ do } x_0 := \text{succ}(x_0) ) \\ &= \delta((4, 3, 4), \\ & \quad \text{loop } x_1 \text{ do } x_0 := \text{succ}(x_0) ) \\ &= \delta((4, 3, 4), \\ & \quad x_0 := \text{succ}(x_0); \\ & \quad x_0 := \text{succ}(x_0); \\ & \quad x_0 := \text{succ}(x_0) ) \\ &= \delta(\delta((4, 3, 4), x_0 := \text{succ}(x_0)), \\ & \quad x_0 := \text{succ}(x_0); \\ & \quad x_0 := \text{succ}(x_0) ) \\ &= \delta((5, 3, 4), \\ & \quad x_0 := \text{succ}(x_0); \\ & \quad x_0 := \text{succ}(x_0) ) \\ &= \delta(\delta((5, 3, 4), x_0 := \text{succ}(x_0)), \\ & \quad x_0 := \text{succ}(x_0) ) \\ &= \delta((6, 3, 4), \\ & \quad x_0 := \text{succ}(x_0) ) \\ &= (7, 3, 4) \end{aligned}$$

**Abbildung 6.2:** Wie hier am Beispiel des Programms add.loop demonstriert, wird die Ausführung eines Loop-Programms durch die schrittweise Auswertung der Übergangsfunktion simuliert. Zu Beginn befinden sich in den Variablen  $x_1$  und  $x_2$  die Eingabewerte 3 und 4. Am Ende enthält die Ergebnisvariable  $x_0$  erwartungsgemäß die Summe  $3 + 4 = 7$ .

Berechnungsmodelle haben nichts mit gutem Programmierstil zu tun! Im Folgenden werden Sie viele Programme kennen lernen, die aus der Sicht der modernen Software-Technik weit von einer empfehlenswerten Lösung entfernt sind.

Behalten Sie stets im Auge, dass es in diesem Kapitel um den abstrakten Begriff der Berechenbarkeit und nicht um die Erstellung effizienter, wartbarer und verständlicher Programme geht. Niemand wird freiwillig einen Algorithmus in der hier entwickelten Loop-, While- oder Goto-Sprache verfassen wollen und soll es auch nicht! Das Einzige, was an dieser Stelle zählt, ist der formale Beweis, dass eine Implementierung aus theoretischer Sicht möglich wäre.



### Definition 6.2 (Loop-Berechenbarkeit)

Sei  $f : \mathbb{N}^n \rightarrow \mathbb{N}$  eine beliebige Funktion über den natürlichen Zahlen.  $f$  heißt *Loop-berechenbar*, falls ein Loop-Programm  $P$  mit der folgenden Eigenschaft existiert:

$$\delta((0, x_1, \dots, x_n, 0, \dots), P) = (f(x_1, \dots, x_n), \dots)$$

Mit dieser Definition haben wir implizit festgelegt, dass  $x_0$  sowie alle für die interne Verwendung vorgesehenen Variablen zu Beginn mit dem Wert 0 belegt sind. Das ist der Grund, weshalb wir diese Variablen in unseren Loop-Programmen ohne manuelle Initialisierung bedenkenlos verwenden dürfen.

Auf den ersten Blick erscheinen Loop-Programme schon fast als trivial und wir werden weiter unten in der Tat herausarbeiten, dass nicht jede berechenbare Funktion auch tatsächlich Loop-berechenbar ist. Nichtsdestotrotz ist das Schleifenkonstrukt stark genug, um wichtige Kontrollflussoperatoren zu simulieren. Beispielsweise können wir die Loop-Sprache durch ein If-Konstrukt ergänzen, ohne sie im Kern erweitern zu müssen. Hierzu fassen wir den Befehl

`if ( $x_i = 0$ ) then  $P$  end`

ganz einfach als Makro für das folgende Schleifenkonstrukt auf:

`$x_j := 1$ ;  
loop  $x_i$  do  $x_j := 0$  end;  
loop  $x_j$  do  $P$  end`

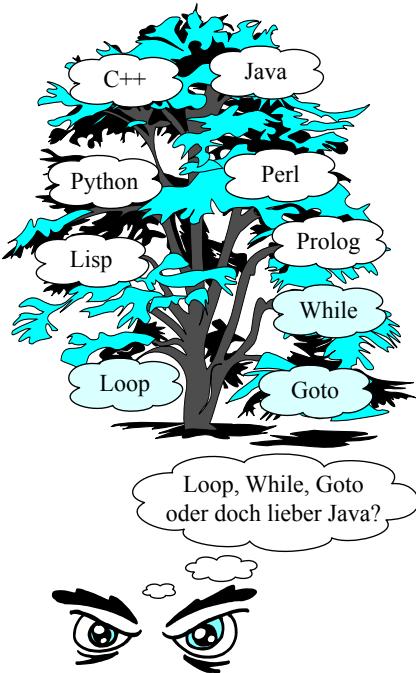
Auch im Hinblick auf den Konstantenvorrat sowie die zur Verfügung gestellten Arithmetikoperationen erweist sich die Loop-Sprache als äußerst spartanisch. Zum Glück sind wir hier ebenfalls in der Lage, durch die Definition einiger nützlicher Makros Linderung zu schaffen. So können wir z. B. alle natürlichen Zahlen bedenkenlos als Konstanten verwenden, indem wir diese als Abkürzungen für die folgenden Ausdrücke betrachten:

$$1 := \text{succ}(0), \tag{6.7}$$

$$2 := \text{succ}(\text{succ}(0)), \tag{6.8}$$

$$3 := \text{succ}(\text{succ}(\text{succ}(0))), \dots \tag{6.9}$$

Darüber hinaus ist die Loop-Sprache aussagekräftig genug, um alle elementaren Arithmetikoperatoren zu erzeugen. Abbildung 6.3 zeigt, wie



sich z. B. die Addition ( $x_1 + x_2$ ), die Multiplikation ( $x_1 \cdot x_2$ ), die Potenz ( $x_1^{x_2}$ ) sowie die Hyperpotenz  $x_1 \uparrow^2 x_2$  durch Loop-Programme berechnen lassen. Um unnötige Schreibarbeit zu ersparen, benutzen die Implementierungen die bereits definierten Funktionen in Form von *Makros*. Lösen wir alle Makros entsprechend ihrer Definition auf, so erhalten wir ein „echtes“ Loop-Programm, das ausschließlich die in Definition 6.1 eingeführten Operatoren verwendet. Beachten Sie, dass es hierzu nicht ausreicht, die Makro-Definition nur textuell zu ersetzen, da die Verwendung der gleichen Variablennamen unweigerlich zu Namenskonflikten führt. Probleme dieser Art lassen sich beheben, indem die Makro-Variablen umbenannt und die Aufrufparameter vor und hinter dem expandierten Makro-Code umkopiert werden.

Die gewählten Beispiele bringen zwei zentrale Eigenschaften von Loop-Programmen zum Vorschein. Zum einen zeigen sie, dass sich durch die verschachtelte Verwendung des Schleifenoperators auch arithmetische Operationen höherer Grade implementieren lassen. Selbst der ungewöhnliche Up-Arrow-Operator, den wir ausführlich in Abschnitt 2.3.2 besprochen haben, lässt sich problemlos berechnen. Zum anderen wird deutlich, dass ein enger Zusammenhang zwischen der Anzahl der benötigten Schleifenkonstrukte und dem Grad der realisierten Arithmetikoperation besteht. Kommt die Addition mit einer einzigen Schleife aus, so benötigen wir für die Multiplikation zwei und für die Potenzierung bereits drei ineinander geschachtelte Schleifen. Verallgemeinert gilt der folgende Satz:



### Satz 6.1

Jedes Loop-Programm zur Berechnung der Funktion  $x \uparrow^n y$  benötigt mindestens  $n + 2$  Schleifen.

Wir wollen die aus der Beobachtung gewonnene Eigenschaft an dieser Stelle ohne Beweis akzeptieren. Mit dem Mittel der strukturellen Induktion lässt sie sich über dem rekursiven Aufbau von Loop-Programmen formal belegen (siehe z.B. [82]).

Satz 6.1 hat weitreichende Konsequenzen für die Ausdrucksstärke der Loop-Sprache. So folgt aus ihm unmittelbar, dass die Ackermann-Funktion  $\text{ack}(n, m)$  nicht Loop-berechenbar ist. Warum dies so ist, geht aus der folgenden Beziehung hervor, die wir in Abschnitt 2.3.2 im Detail herausgearbeitet haben:

$$\text{ack}(n, m) = 2 \uparrow^{n-2} (m+3) - 3 \quad (6.10)$$

■  $x_0 := \text{add}(x_1, x_2)$

#### add.loop

```
// Berechnet x0 := x1 + x2
1
2
3
4
5
6
```

 $x_0 := x_1;$ 
 $\text{loop } x_2 \text{ do}$ 
 $x_0 := \text{succ}(x_0)$ 
 $\text{end}$ 

■  $x_0 := \text{mult}(x_1, x_2)$

#### mult.loop

```
// Berechnet x0 := x1 · x2
1
2
3
4
5
6
```

 $x_0 := 0;$ 
 $\text{loop } x_2 \text{ do}$ 
 $x_0 := \text{add}(x_1, x_0)$ 
 $\text{end}$ 

■  $x_0 := \text{power}(x_1, x_2)$

#### power.loop

```
// Berechnet x0 := x1^{x2}
1
2
3
4
5
6
```

 $x_0 := 1;$ 
 $\text{loop } x_2 \text{ do}$ 
 $x_0 := \text{mult}(x_1, x_0)$ 
 $\text{end}$ 

■  $x_0 := \text{hyper}(x_1, x_2)$

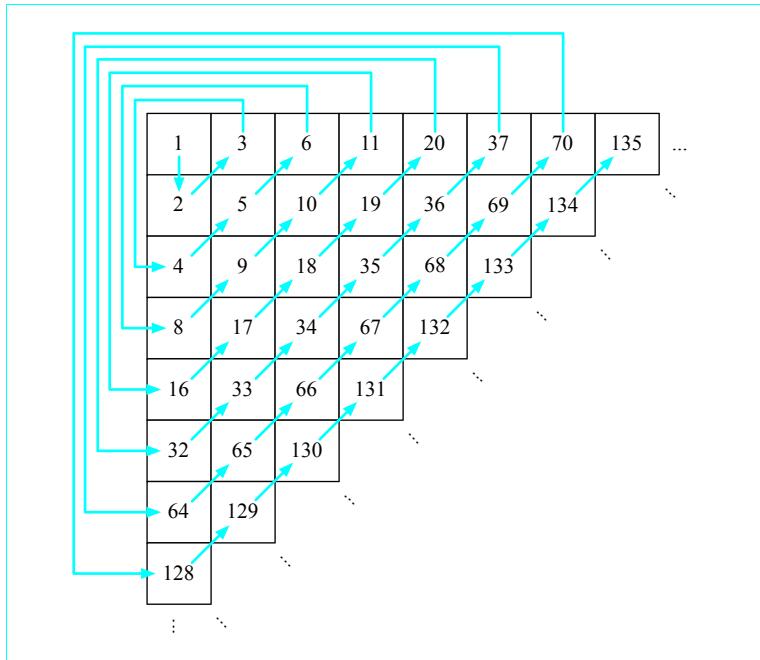
#### hyper.loop

```
// Berechnet x0 := x1 \uparrow^2 x2
1
2
3
4
5
6
```

 $x_0 := 1;$ 
 $\text{loop } x_2 \text{ do}$ 
 $x_0 := \text{power}(x_1, x_0)$ 
 $\text{end}$ 

**Abbildung 6.3:** Alle gängigen Arithmetikoperationen lassen sich mit Hilfe von Loop-Programmen simulieren.

**Abbildung 6.4:** Die abgebildete Paarungsfunktion ordnet jedem Tupel  $(p, q) \in \mathbb{N}_0^2$  eine Zahl  $\pi(p, q) \in \mathbb{N}$  zu. Ein vergleichender Blick auf Abbildung 2.20 zeigt, dass es sich hierbei um eine Abwandlung der Cantor'schen Paarungsfunktion aus Kapitel 2 handelt. Die gewählte Funktion ist im Gegensatz zum Original nicht mehr bijektiv, erfüllt aber dennoch ihren Zweck: Sie gestattet uns, ein beliebiges Zahlenpaar aus der Menge  $\mathbb{N}_0^2$  in eine einzige Zahl aus  $\mathbb{N}$  hineinzucodieren. Die gewählte Variante besitzt den Vorteil, eine vergleichsweise einfache Berechnungsformel zu besitzen. Hierdurch erfordert die Codierung weniger Rechenschritte als das Original.



Gäbe es ein Loop-Programm, das  $\text{ack}(n, m)$  tatsächlich für beliebige Werte von  $n$  berechnet, so müsste dieses aufgrund von Satz 6.1 – im Widerspruch zum endlichen Aufbau eines Loop-Programms – unendlich viele Schleifenkonstrukte enthalten.

### Korollar 6.1

Die Ackermann-Funktion  $\text{ack}(n, m)$  ist nicht Loop-berechenbar.

Neben der Ackermann-Funktion existiert eine wichtige Klasse von Funktionen, die ebenfalls nicht Loop-berechenbar sind. Die Rede ist von *partiellen Funktionen*, die in Abschnitt 2.2 eingeführt wurden und in der theoretischen Informatik eine wichtige Rolle spielen. Partielle Funktionen sind für uns die formale Grundlage, um Programme zu beschreiben, die nicht für alle Eingabekombinationen terminieren.

Ein Blick auf die Gleichungen (6.2) bis (6.6) klärt unmittelbar auf, warum diese Limitierung besteht. Loop-Programme terminieren für jede beliebige Eingabe und können damit im Gegensatz zu Programmiersprachen, die in der realen Software-Entwicklung verwendet werden, keine Endlosschleifen hervorbringen.

**Satz 6.2**

Alle Loop-berechenbaren Funktionen  $f : \mathbb{N}^n \rightarrow \mathbb{N}$  sind total.

Zum Schluss wollen wir uns ein wenig genauer mit den Möglichkeiten beschäftigen, die uns innerhalb eines Loop-Programms für die Speicherung interner Zwischenergebnisse bereitgestellt werden.

Zunächst sieht die Sprachdefinition vor, dass uns beliebig viele Variablen zur Verfügung stehen, die wir nach Belieben beschreiben und auslesen können. Viele Programme ließen sich jedoch einfacher schreiben, wenn wir Zwischenergebnisse auf einem Stapel (*stack*) ablegen könnten. Wie ein Stapel funktioniert, haben wir detailliert in der Diskussion über Kellerautomaten besprochen (vgl. Abschnitt 5.5). Wir werden nun zeigen, dass die Loop-Sprache, so primitiv sie auf den ersten Blick auch wirkt, stark genug ist, um einen Kellerspeicher zu simulieren.

Hierbei verfolgen wir den Ansatz, alle Stapelemente in eine einzige Variable hineinzucodieren. Den Schlüssel hierzu bildet die Cantor'sche Paarungsfunktion aus Abschnitt 2.3.3, die eine eineindeutige Abbildung zwischen der Menge  $\mathbb{N}^2$  und  $\mathbb{N}$  herstellt. Für unseren Zweck verwenden wir eine abgewandelte Variante, die wie folgt definiert ist:

$$\pi(x, y) = 2^{x+y} + x \quad (6.11)$$

Abbildung 6.4 zeigt einen Auszug aus der zweidimensionalen Wertetabelle. Die Funktion  $\pi$  sowie deren Umkehrfunktion  $\pi^{-1}$  sind Loop-berechenbar, so dass wir Zahlentupel und einzelne Zahlen beliebig hincodieren können. Die Implementierungen sind in Abbildung 6.5 dargestellt. Beide machen ausgiebig von den weiter oben eingeführten Makro-Konstrukten Gebrauch.

Nachdem wir nun in der Lage sind, ein beliebiges Zahlenpaar in eine einzige Zahl hineinzucodieren, ist unser Ziel schon so gut wie erreicht. Wir können einen Stapel mit  $k$  Elementen  $n_1, \dots, n_k$  repräsentieren, indem wir die Paarungsfunktion  $\pi$  rekursiv anwenden:

$$n = \pi(n_k, \pi(n_{k-1}, \dots, \pi(n_1, 0) \dots)) \quad (6.12)$$

Mit  $n$  erhalten wir eine einzige natürliche Zahl, die stellvertretend für den gesamten Kellerspeicher steht. Das Element 0 nimmt eine Sonderstellung ein. Es repräsentiert einen leeren Stapel und kann dazu verwendet werden, die Anzahl der Stapelemente zu ermitteln.

Die geleistete Arbeit hat sich gelohnt. Abbildung 6.6 zeigt, wie wir die elementaren Stapeloperationen in der Loop-Sprache implementieren können. new erzeugt einen leeren Stapel, push fügt dem Stapel ein

■  $x_0 := \text{cantor}(x_1, x_2)$

**cantor.loop**

```

1   x0 := x1 + x2 ;
2   x0 := 2x0 ;
3   x0 := x0 + x1
4
5

```

■  $(x_1, x_2) := \text{cantor}^{-1}(x_0)$

**cantor\_invers.loop**

```

1   loop x0
2     if (2 · 2x3 ≤ x0)
3       x3 := succ(x3)
4     end;
5
6   // An dieser Stelle gilt:
7   // x3 = max{n | 2n ≤ x0}
8
9   x1 := x0 - 2x3;
10  x2 := x3 - x1
11
12

```

**Abbildung 6.5:** Die Cantor'sche Paarungsfunktion ist Loop-berechenbar.

■  $x_j := \text{new}()$

**new.loop**

```
1   xj := 0;
```

2  
3

Element hinzu und pop entfernt das oberste Element. Ab sofort dürfen wir alle vier Makrobefehle in unseren Loop-Programmen frei verwenden.

■  $\text{push}(x_i, x_j)$

**push.loop**

```
1   xj := cantor(xi, xj);
```

2  
3

Abbildung 6.6 zeigt ferner, wie sich die Size-Operation in Form eines Loop-Programms berechnen lässt.  $\text{size}(x)$  liefert die Anzahl der Stack-Elemente zurück und ist für den praktischen Umgang mit dieser Datenstruktur unumgänglich. Die Implementierung basiert auf der Tatsache, dass die Anzahl der Elemente eines mit  $x$  codierten Stapels stets kleiner ist als der Wert  $x$  selbst. Entsprechend lässt sich die Anzahl der Elemente bestimmen, indem wir die Stack-Inhalte der Reihe nach decodieren und einen dedizierten Zähler so lange erhöhen, bis das Stack-Ende erreicht ist.

■  $x_i := \text{pop}(x_j)$

**pop.loop**

```
1   (xi, xj) := cantor-1(xj)
```

2  
3

■  $x_i := \text{size}(x_j)$

**size.loop**

```
1   xi := 0;
2   loop xj do
3     if (xj ≠ 0) then
4       xi := succ(xi);
5       pop(xj)
6     end
7   end
```

1  
2  
3  
4  
5  
6  
7  
8  
9

## 6.1.2 While-Programme

Die Diskussion über die Loop-Sprache hat gezeigt, dass das eingeführte Schleifenkonstrukt nicht ausdrucksstark genug ist, um alle Funktionen zu berechnen, die auch im intuitiven Sinne berechenbar sind. Die Ackermann-Funktion hat uns die Limitierungen deutlich vor Augen geführt. In diesem Abschnitt wollen wir die Loop-Schleife um ein komplexeres Konstrukt ergänzen, das zu einer echten Erweiterung der Ausdrucksstärke führen wird. Die Rede ist von der *While-Schleife*.



### Definition 6.3 (While-Programme)

Ein While-Programm besteht aus den folgenden Komponenten:

- der *Konstanten* 0,
- den *Variablen*  $x_0, x_1, x_2, \dots$ ,
- den *Operatoren* succ und pred,
- dem *Zuweisungsoperator* ':=',
- dem *Kompositionsoperator* ';' ,
- dem *Schleifenkonstrukt* loop do end,
- dem *Schleifenkonstrukt* while do end

**Abbildung 6.6:** Die Loop-Sprache ist ausdrucksstark genug, um einen Stapel zu simulieren. Die Programme zeigen, wie sich die vier elementaren Stapeloperationen implementieren lassen.

Alle Konstrukte der Loop-Sprache finden sich auch in der While-Sprache wieder und wir übernehmen deren Semantik eins zu eins.

Die While-Sprache wird hierdurch zu einer echten Erweiterung der Loop-Sprache, so dass wir nicht nur jedes Loop-Programm als While-Programm betrachten können, sondern darüber hinaus auf sämtliche der weiter oben definierten Makros zurückgreifen dürfen.

Um die Semantik der While-Sprache vollständig zu definieren, müssen wir nur noch die Bedeutung der While-Schleife festlegen. Zu diesem Zweck definieren wir zuerst die *Terminierungsmenge*  $T_i$ :

$$T_i := \{k \in \mathbb{N}_0 \mid \delta(v, P^k) = (\dots, x_{i-1}, 0, x_{i+1}, \dots)\} \quad (6.13)$$

Ausgehend von einem gegebenen Speichervektor  $v$  enthält die Terminierungsmenge alle Zahlen  $k \in \mathbb{N}_0$  mit der Eigenschaft, dass  $x_i$  nach der  $k$ -ten Wiederholung von  $P$  den Wert 0 annimmt. Besonders wichtig wird für uns das Minimum der Menge  $T$  sein. Dieses beschreibt die minimale Anzahl von Iterationen, die wir  $P$  ausführen müssen, um die Bedingung  $x_i > 0$  falsch werden zu lassen. Ein Sonderfall liegt vor, falls  $T$  zur leeren Menge degeneriert. In diesem Fall ist die Bedingung  $x_i > 0$  immer erfüllt und wir können in  $T$  kein Minimum bestimmen.

Basierend auf dem Begriff der Terminierungsmenge legen wir die Semantik des While-Konstrukt wie folgt fest:

$$\delta(v, \text{while } x_i \text{ do } P) = \begin{cases} \perp & \text{falls } T_i = \emptyset \\ \delta(v, P^{\min T_i}) & \text{falls } T_i \neq \emptyset \end{cases} \quad (6.14)$$

Für den programmübergreifenden Umgang mit undefinierten Funktionswerten vereinbaren wir die folgende Beziehung:

$$\delta(\perp, P) = \perp \quad (6.15)$$

Hierdurch wird nachgebildet, dass eine einzige nichtterminierende While-Schleife dazu führt, dass das gesamte Programm niemals anhält.

Wir sind nun in der Lage, den Begriff der While-Berechenbarkeit formal zu definieren.

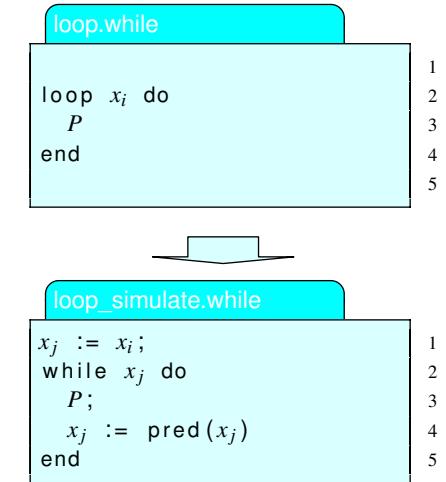


#### Definition 6.4 (While-Berechenbarkeit)

Mit  $f : \mathbb{N}^n \rightarrow \mathbb{N}$  sei eine partielle Funktion über den natürlichen Zahlen gegeben.  $f$  heißt *While-berechenbar*, falls ein While-Programm  $P$  mit den folgenden Eigenschaften existiert:

$$\delta((0, x_1, \dots, x_n, 0, \dots), P) = \begin{cases} \perp & \text{falls } f(x_1, \dots, x_n) = \perp \\ (f(x_1, \dots, x_n), \dots) & \text{falls } f(x_1, \dots, x_n) \neq \perp \end{cases}$$

Vielleicht ist Ihnen in der Definition der While-Sprache aufgefallen, dass wir die Loop-Schleife nicht aus dem Sprachschatz entfernt haben. In der Tat hätten wir auf die Aufnahme des Loop-Konstrukts problemlos verzichten können. Die While-Schleife ist so ausdrucksstark, dass wir jede Loop-Schleife, wie in Abbildung 6.7 gezeigt, simulieren können. Dass wir an der Loop-Schleife dennoch festhalten, hat trifftige Gründe, die am Ende dieses Abschnitts ersichtlich werden. Der interessierte Leser möge bereits jetzt einen Blick auf Satz 6.3 werfen. Dieser würde falsch werden, wenn wir das Loop-Konstrukt aus der While-Sprache verbannen.



**Abbildung 6.7:** Der While-Befehl ist ausdrucksstark genug, um den Loop-Befehl zu simulieren.

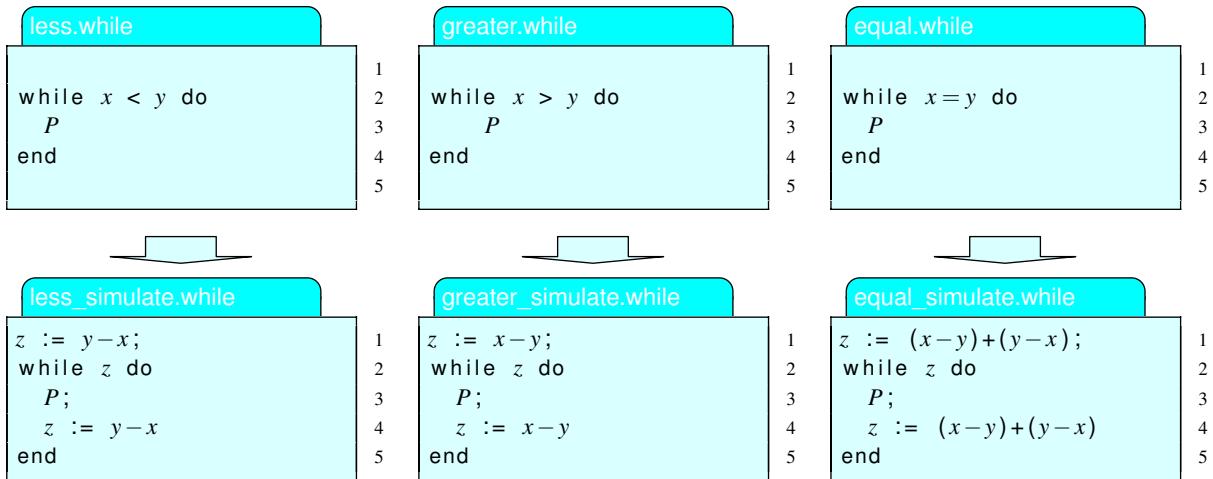


Abbildung 6.8: Alle gängigen Arithmetikoperationen lassen sich mit Hilfe von While-Programmen simulieren.

Abbildung 6.8 zeigt, dass sich auch die Form der erlaubten Schleifenbedingungen weiter verallgemeinern lässt. Neben  $<$ ,  $>$  und  $=$  lassen sich in analoger Weise die Relationen  $\leq$ ,  $\geq$  sowie Vergleiche mit numerischen Konstanten modellieren.

Im Folgenden wollen wir herausarbeiten, wie flexibel die While-Schleife wirklich ist. Kombinieren wir das Schleifenkonstrukt mit den in Abschnitt 6.1.1 eingeführten Push- und Pop-Operationen, so sind wir in der Lage, rekursive Funktionsaufrufe in gewissen Grenzen zu simulieren. Insbesondere dann, wenn der rekursive Aufruf ganz am Ende des Funktionsrumpfes steht, gelingt die Simulation ohne Probleme. In diesem Fall reicht es aus, die Funktionsparameter auf den Stack zu legen und den Funktionsrumpf innerhalb einer While-Schleife auszuführen. Ein rekursiver Aufruf wird simuliert, indem die Aufrufparameter auf den Stack geschoben und im Zuge des Rücksprungs wieder entfernt werden. Die While-Schleife wird verlassen, sobald der Stack keine Elemente mehr enthält.

Beachten Sie, dass rekursive Aufrufe, die in der Mitte des Funktionsrumpfs stehen, nicht auf diese Weise simuliert werden können. Im Gegensatz zu realen Programmiersprachen sieht die While-Sprache keine Möglichkeit vor, eine Rücksprungadresse auf dem Stapel abzulegen.

Abbildung 6.9 demonstriert das Transformationsprinzip am Beispiel der Ackermann-Funktion. Die linke Seite enthält eine konventionelle C-Implementierung, die den Funktionswert  $\text{ack}(n, m)$  mit Hilfe einer

<b>ackermann.c</b> <pre> int ack( int n, int m) {     if (n == 0) {         return m+1;     }      if (m == 0) {         return ack(n-1, 1);     }      return ack(n-1, ack(n,m-1)); } </pre>	<b>ackermann.while</b> <pre> 1 push(n, stack); 2 push(m, stack); 3 4 while size(stack) &gt; 1 do 5 6     y := pop(stack); 7     x := pop(stack); 8 9     if (x == 0) then 10        push(y+1, stack) 11    end 12    else if (y == 0) then 13        push(x-1, stack); 14        push(1, stack); 15    end 16    else 17        push(x-1, stack); 18        push(x, stack); 19        push(y-1, stack) 20    end 21 end 22 23 x0 := pop(stack); </pre>
--	---

**Abbildung 6.9:** Die Ackermann-Funktion ist While-berechenbar. Das linke Programm zeigt eine C-Implementierung, die den Funktionswert  $\text{ack}(n, m)$  rekursiv berechnet. Mit Hilfe der Push- und Pop-Makros lässt sich die Rekursion simulieren und das C-Programm in ein äquivalentes While-Programm überführen.

While-Schleife und mehreren rekursiven Aufrufen berechnet. Die rechte Seite zeigt, wie sich die Rekursion unter Verwendung der Push- und Pop-Operationen simulieren lässt. Mit dem konstruierten Programm haben wir ein wichtiges Ergebnis der Berechenbarkeitstheorie gezeigt. Zusammen mit Korollar 6.1 beweist dessen Existenz, dass die While-Sprache eine größere Ausdrucksstärke als die Loop-Sprache besitzt.

Zum Schluss wollen wir uns mit der Frage beschäftigen, wie viele While-Schleifen für die Berechnung einer Funktion mindestens benötigt werden. Für Loop-Programme haben wir in Abschnitt 6.1.1 beobachtet, dass die Anzahl der Schleifenkonstrukte, die für die Berechnung der Funktion  $x \uparrow^n y$  benötigt werden, linear mit dem Parameter  $n$  wächst. Diese Erkenntnis wirft unweigerlich die Frage auf, ob ein ähnliches Ergebnis auch für While-Programme gilt. Der folgende Satz beantwortet diese Frage negativ:

■ add(3,4)

```
add.goto
M1 : x0 := x2;
M2 : if x1 goto M4;
M3 : halt;
M4 : x0 := succ(x0);
M5 : x1 := pred(x1);
M6 : if x0 goto M2
```



### Satz 6.3 (Satz von Kleene)

Jede While-berechenbare Funktion lässt sich durch ein While-Programm mit nur einer While-Schleife berechnen.

**Abbildung 6.10:** Das dargestellte Goto-Programm berechnet die Summe zweier natürlicher Zahlen ( $x_0 = x_1 + x_2$ ).

■ add(3,4)

```
((0,3,4,0,...), 1)
→ ((4,3,4,0,...), 2)
→ ((4,3,4,0,...), 4)
→ ((5,3,4,0,...), 5)
→ ((5,2,4,0,...), 6)
→ ((5,2,4,0,...), 2)
→ ((5,2,4,0,...), 4)
→ ((6,2,4,0,...), 5)
→ ((6,1,4,0,...), 6)
→ ((6,1,4,0,...), 2)
→ ((6,1,4,0,...), 4)
→ ((7,1,4,0,...), 5)
→ ((7,0,4,0,...), 6)
→ ((7,0,4,0,...), 2)
→ ((7,0,4,0,...), 3)
→ ((7,0,4,0,...), 0)
```

### 6.1.3 Goto-Programme

Goto-Programme sind ähnlich einfach aufgebaut wie die weiter oben eingeführten Loop- und While-Programme und kommen gänzlich ohne die konventionellen Schleifenkonstrukte aus. An die Stelle der Loop- und der While-Schleife tritt der bedingte Sprung (If-Goto-Konstrukt).



### Definition 6.5 (Goto-Programme)

Ein *Goto-Programm* ist eine Sequenz markierter Anweisungen:

$M_1 : A_1; M_2 : A_2; \dots; M_n : A_n$

Die Anweisungen  $A_i$  bestehen aus den folgenden Komponenten:

- der *Konstanten* 0,
- den *Variablen*  $x_0, x_1, x_2, \dots$ ,
- den *Operatoren* succ und pred,
- dem *Zuweisungsoperator* ':=',
- dem *bedingten Sprungbefehl* if  $x_i$  goto  $M_j$ ,
- dem *Stoppbefehl* halt

**Abbildung 6.11:** Schrittweise Ausführung des Goto-Programms aus Abbildung 6.10. Das Programm wird mit den Initialwerten  $x_1 = 3$  und  $x_2 = 4$  gestartet. Nach Ausführungsende enthält die Ergebnisvariable  $x_0$  erwartungsgemäß den Wert 7.

Die Semantik von Loop- und While-Programmen konnten wir induktiv über den Programmaufbau definieren, da die Schleifenkonstrukte keine Möglichkeit vorsehen, um an beliebige Stellen im Quellcode zu springen. Goto-Programme hingegen bieten diese Möglichkeit. Aus diesem Grund wählen wir einen zustandsbasierten Ansatz, wie er uns bereits im Rahmen der Diskussion über endliche Automaten begegnet ist. Im

Kern steht der Begriff der *Konfiguration*, der uns erlaubt, den augenblicklichen Zustand der Programmausführung im Sinne einer Momentaufnahme zu beschreiben.

Konkret wird die Konfiguration eines Goto-Programms durch einen Speichervektor  $v$  und einen *Markenindex*  $k$  gebildet. Die Übergangsrelation  $\rightarrow$  beschreibt, wie sich eine gegebene Konfiguration im Zuge der Programmausführung verändert. Die Folgekonfiguration wird durch den Befehl  $A_k$  bestimmt, wobei  $k$  dem Markierungsindex der aktuellen Konfiguration  $(v, k)$  entspricht. In Abhängigkeit von  $A_k$  definieren wir  $\rightarrow$  wie folgt:

- Zuweisung ( $M_k : x_i := 0$ ,  $M_k : x_i := \text{succ}(x_j)$ ,  $M_k : x_i := \text{pred}(x_j)$ )

$$(v, k) \rightarrow (\delta(v, A_k), k + 1) \quad (6.16)$$

Die Definition von  $\delta$  übernehmen wir unverändert aus der Loop-Sprache.

- Bedingter Sprung ( $M_k : \text{if } x_i \text{ goto } M_l$ )

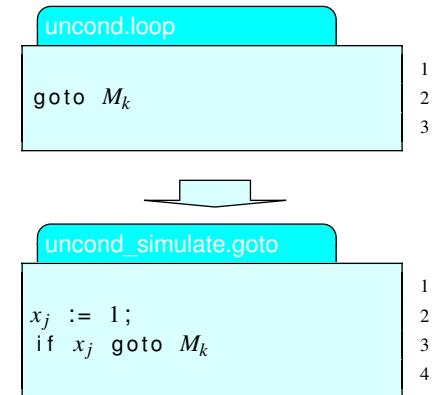
$$(v, k) \rightarrow \begin{cases} (v, k + 1) & \text{falls } x_i = 0 \\ (v, l) & \text{falls } x_i \neq 0 \end{cases} \quad (6.17)$$

- Stoppbefehl ( $M_k : \text{stop}$ )

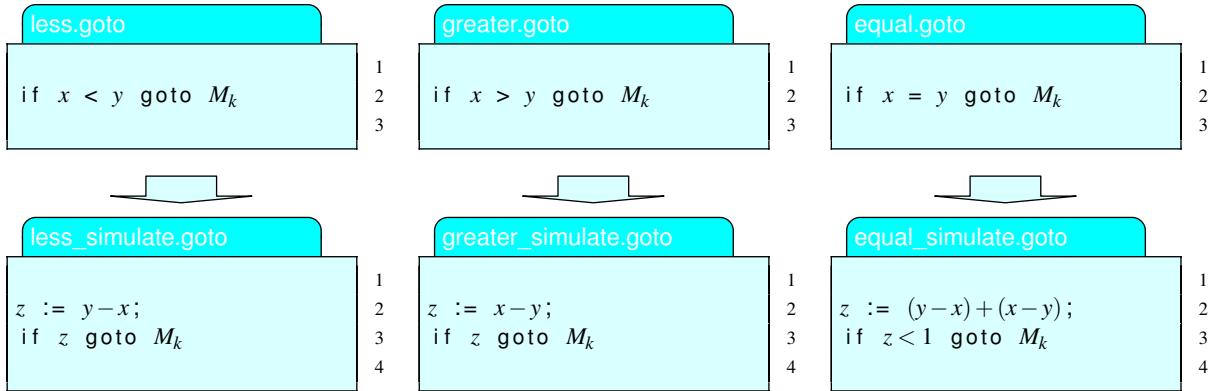
$$(v, k) \rightarrow (v, 0) \quad (6.18)$$

Die Abbildungen 6.10 und 6.11 zeigen, wie die Addition zweier Zahlen  $x_1$  und  $x_2$  mit Hilfe eines Goto-Programms implementiert werden kann. Ersetzen wir den Operator  $\text{succ}$  durch den Operator  $\text{pred}$ , so entsteht ein Programm, das die (gesättigte) Subtraktion zweier Zahlen realisiert.

Im Folgenden wollen wir eine Reihe weiterer Vereinbarungen treffen, die den Umgang mit Goto-Programmen deutlich vereinfachen werden. Zum einen lassen wir zu, dass neben dem bedingten Sprung (If-Goto-Konstrukt) ein unbedingter Sprung (Goto-Konstrukt) eingesetzt werden darf. Die Verwendung ist legitim, da wir das Konstrukt, wie in Abbildung 6.12 gezeigt, auf den bedingten Sprung reduzieren können. Zum anderen erlauben wir, dass die If-Bedingungen auch Vergleiche der Form  $x_i < x_j$ ,  $x_i > x_j$  oder  $x_i = x_j$  enthalten dürfen, wobei  $x_j$  entweder für eine andere Variable oder eine Konstante steht. Abbildung 6.13 demonstriert, wie sich die entsprechenden Anweisungen durch native Goto-Programme simulieren lassen.



**Abbildung 6.12:** Der unbedingte Sprung lässt sich auf den bedingten Sprung reduzieren. Für  $x_j$  darf eine beliebige Variable substituiert werden, die nicht bereits an anderer Stelle verwendet wird.



**Abbildung 6.13:** Die Goto-Sprache ist ausdrucksstark genug, um komplexe If-Bedingungen zu simulieren.

Mit den getroffenen Vereinbarungen können wir viele Programme übersichtlicher formulieren. Eine entsprechende Reimplementierung des Beispielprogramms add.loop ist in Abbildung 6.14 dargestellt.

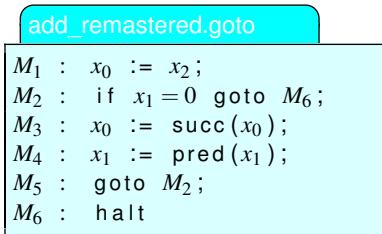
Mit Hilfe der Übergangsrelation → sind wir in der Lage, den Begriff der Goto-Berechenbarkeit exakt festzulegen:



### Definition 6.6 (Goto-Berechenbarkeit)

Mit  $f : \mathbb{N}^n \rightarrow \mathbb{N}$  sei eine partielle Funktion über den natürlichen Zahlen gegeben.  $f$  heißt *Goto-berechenbar*, falls ein Goto-Programm  $P$  mit den folgenden Eigenschaften existiert:

$$\begin{aligned} ((0, x_1, \dots, x_n, 0, \dots), 1) \not\rightarrow^* ((\dots), 0) &\text{ falls } f(x_1, \dots, x_n) = \perp \\ ((0, x_1, \dots, x_n, 0, \dots), 1) \rightarrow^* ((f(x_1, \dots, x_n), \dots), 0) &\text{ sonst} \end{aligned}$$



**Abbildung 6.14:** Das dargestellte Goto-Programm berechnet die Summe zweier natürlicher Zahlen ( $x_0 = x_1 + x_2$ ). Es handelt es sich um eine Umformulierung des Originalprogramms aus Abbildung 6.10.

Berechnet ein Goto-Programm  $P$  die Funktion  $f(x_1, \dots, x_n)$ , so können wir einen konkreten Funktionswert bestimmen, indem wir die EingabevARIABLEN  $x_1, \dots, x_n$  auf die gewünschten Werte setzen und das Programm, wie oben gezeigt, ausführen. Für alle  $x_1, \dots, x_n$  mit  $f(x_1, \dots, x_n) \neq \perp$  terminiert die Programmausführung irgendwann in einer Konfiguration, die den Markierungsindex 0 enthält, und wir können den gesuchten Funktionswert aus der Variablen  $x_0$  auslesen. Gilt  $f(x_1, \dots, x_n) = \perp$ , so wird der Markierungsindex 0 nicht erreicht.

Auch wenn sich Goto-Programme auf den ersten Blick erheblich von den While-Programmen aus Abschnitt 6.1.2 unterscheiden, sind die

Differenzen rein äußerlicher Natur. Um den Zusammenhang zwischen beiden Sprachen offenzulegen, zeigen wir zunächst, wie sich ein While-Programm durch ein äquivalentes Goto-Programm ersetzen lässt, und anschließend, wie aus einem Goto-Programm ein äquivalentes While-Programm erzeugt werden kann.

Für die folgenden Betrachtungen sei ein beliebiges While-Programm gegeben, das sich aus einer Kette von  $n$  Anweisungen  $A_1$  bis  $A_n$  zusammensetzt. In einem ersten Schritt übersetzen wir die Sequenz in eine markierte Anweisungskette und schließen diese am Ende mit einem halt-Befehl ab:

$$M_1 : A_1; M_2 : A_2; \dots; M_n : A_n; M_{n+1} : \text{halt} \quad (6.19)$$

Im zweiten Schritt ersetzen wir jeden While-Befehl der Form

$$M_i : \text{while } x_i \text{ do } P \text{ end}$$

durch das folgende Goto-Konstrukt:

$$\begin{aligned} M_i &: \text{if } x_i = 0 \text{ goto } M_{i+1}; \\ &\quad P; \\ &\quad \text{goto } M_i; \\ M_{i+1} &: \dots \end{aligned}$$

Die Konstruktion stellt sicher, dass das erzeugte Goto-Programm die gleiche (partielle) Funktion berechnet wie das ursprüngliche While-Programm.

Die umgekehrte Schlussrichtung können wir ebenfalls zeigen, müssen hierzu aber ein wenig trickreicher agieren. Um ein Goto-Programm der Form

$$M_1 : A_1; M_2 : A_2; \dots; M_n : A_n \quad (6.20)$$

in ein äquivalentes While-Programm zu übersetzen, kommen wir nicht umhin, Sprünge zu beliebigen Programmstellen zu simulieren. Hierbei verfolgend wir die Grundidee, den Markenindex eines Goto-Programms in eine dedizierte Variable  $y$  hineinzucodieren, die im ursprünglichen Programm nicht verwendet wird. Betteln wir die Variable, wie in Abbildung 6.15 gezeigt, in eine Reihe von If-Anweisungen ein, so können wir eine vollständige Fallunterscheidung über alle Markenindizes durchführen. Jeder If-Zweig entspricht der Ausführung eines Befehls des Goto-Programms. Um eine kontinuierliche Programmausführung zu simulieren, umhüllen wir das Programmgerüst mit einer While-Schleife, die genau dann verlassen wird, wenn der Markenindex den Wert 0 annimmt.

### Programmgerüst.while

```

y := 1;
1
2
while y ≠ 0 do
3
4
    if y = 1 then
5
        ... // A1
6
    end;
7
    if y = 2 then
8
        ... // A2
9
    end;
10
    ...
11
    if y = n then
12
        ... // An
13
    end
14
end
15
16

```

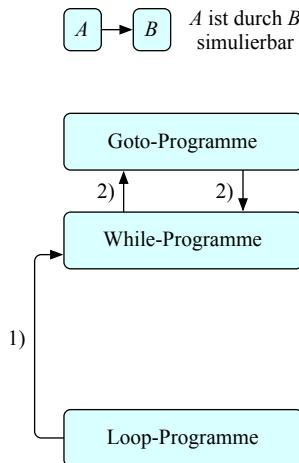
**Abbildung 6.15:** Das abgebildete Programmgerüst erlaubt, Goto-Programme mit Hilfe der While-Sprache zu simulieren. Die Variable  $y$  übernimmt die Rolle des Markenindexes.

Goto-Anweisung	While-Anweisung
$M_k : x_i := 0$	$x_i := 0; y := k + 1$
$M_k : x_i := \text{succ}(x_j)$	$x_i := \text{succ}(x_j); y := k + 1$
$M_k : x_i := \text{pred}(x_j)$	$x_i := \text{pred}(x_j); y := k + 1$
$M_k : \text{goto } M_l$	$y := l$
$M_k : \text{if } x_i \text{ goto } M_l$	$y := k+1; \text{if } x_i \text{ then } y := l$
$M_k : \text{halt}$	$y := 0$

**Tabelle 6.1:** Transformation von Goto-Anweisungen in die While-Sprache. Sprünge werden durch die Modifikation der Indexvariablen  $y$  simuliert.

Innerhalb des Goto-Programms wird dieser Markenindex genau dann erreicht, wenn der halt-Befehl ausgeführt wurde und das Programm terminiert.

Damit sind wir fast am Ziel. Wir müssen nur noch die Einzelanweisungen  $A_1$  bis  $A_n$  übersetzen und in das konstruierte Programmgerüst einfügen. Die entsprechenden Transformationen sind in Tabelle 6.1 zusammengefasst. Eine besondere Rolle spielt auch hier wieder die Indexvariable  $y$ . Diese wird durch die vorhandenen Arithmetikoperationen so manipuliert, dass im nächsten Iterationsschritt immer der korrekte Folgebefehl ausgeführt wird. Insgesamt liefern die Transformationen einen konstruktiven Beweis für den folgenden Satz:



#### Satz 6.4

Die Klasse der While-berechenbaren Funktionen stimmt mit der Klasse der Goto-berechenbaren Funktionen überein.

Abbildung 6.16 fasst die bisher erarbeiteten Ergebnisse in einer Gesamtübersicht zusammen.

Der oben konstruierte Beweis hält eine weitere Überraschung für uns bereit. Führen wir beide Transformationen für ein beliebiges While-Programm nacheinander durch, so erhalten wir aufgrund des Konstruktionsschemas aus Abbildung 6.15 ein Programm, das aus einer einzigen While-Schleife besteht. Wir haben damit einen Beweis für den Satz von Kleene gefunden, den wir in Abschnitt 6.1.2 ohne Begründung eingeführt haben. Jetzt wird auch der Name klar, mit dem Programme in der speziellen Form aus Abbildung 6.15 häufig bezeichnet werden: Sie liegen in *Kleene'scher Normalform* vor.

**Abbildung 6.16:** While-Programme besitzen eine größere Ausdrucksstärke als Loop-Programme. Zwischen While- und Goto-Programmen besteht hingegen kein Unterschied. Die Programme beider Sprachen lassen sich ineinander überführen, ohne die berechnete Funktion zu verändern.

### 6.1.4 Primitiv-rekursive Funktionen

Alle bisher betrachteten Ansätze verfolgen die Idee, den Berechenbarkeitsbegriff auf der Ebene von Programmiersprachen zu erfassen. Aus der Sicht des Informatikers macht diese Vorgehensweise durchaus Sinn, da sich hinter der Loop-, While- und Goto-Sprache die gleichen Konzepte verborgen, die wir aus realen Programmiersprachen kennen. Die Theorie der rekursiven Funktionen verfolgt einen anderen Ansatz und macht den Berechenbarkeitsbegriff auf rein mathematischem Weg zugänglich.

Auf den folgenden Seiten werden wir uns der Thematik schrittweise nähern, da die auftretenden Begriffe erfahrungsgemäß schwieriger zu verinnerlichen sind als jene der anderen Berechnungsmodelle. Wir beginnen mit dem Prinzip der *primitiven Rekursion* und führen erst im Anschluss daran die Menge der *primitiv-rekursiven Funktionen* ein.



#### Definition 6.7 (Primitive Rekursion)

Mit  $g : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  und  $h : \mathbb{N}_0 \rightarrow \mathbb{N}_0^3$  seien zwei Funktionen über  $\mathbb{N}_0$  gegeben. Eine Funktion  $f : \mathbb{N}_0^2 \rightarrow \mathbb{N}_0$  ist nach dem Schema der *primitiven Rekursion* aufgebaut, wenn sie die folgende Form besitzt:

$$f(m, n) = \begin{cases} g(n) & \text{falls } m = 0 \\ h(f(m-1, n), m-1, n) & \text{falls } m > 0 \end{cases}$$

Ein genauer Blick auf das Rekursionsschema zeigt, dass der Funktionswert  $f$  in einer Schleife berechnet wird, in der  $m$  die Rolle der Schleifenvariablen spielt. Ist  $m = 0$ , so wird der Funktionswert über die Funktion  $g(n)$  bestimmt. Ist  $m > 0$ , so wird der Funktionswert ermittelt, indem die Funktion  $h$  auf den berechneten Funktionswert  $f(m-1, n)$  sowie die Parameter  $m-1$  und  $n$  angewendet wird. Auf den ersten Blick mag die Definition willkürlich erscheinen, auf den zweiten Blick wird jedoch schnell deutlich, dass die Formel den Aufbau einer rekursiv implementierten Schleife widerspiegelt. Der Zusammenhang wird sichtbar, wenn die Formelfragmente, wie in Abbildung 6.17 getan, in eine programmähnliche Form gebracht werden.

Das Schema der primitiven Rekursion ist stark genug, um alle üblichen Arithmetikoperationen auszudrücken. Am einfachsten gelingt die Umsetzung in eine primitiv-rekursive Darstellung, wenn wir in zwei Schritten vorgehen. Zunächst implementieren wir die Operationen mit einem

primrek.c

```

1 int f(m,n)
2 {
3     if (m == 0) {
4         // stuff
5         return g(n)
6     } else {
7         // recursive call
8         tmp = f(m-1,n);
9
10        // stuff
11        return h(tmp,m-1,n);
12    }
13 }
```

**Abbildung 6.17:** Viele rekursiv programmierte Funktionen sind nach dem Prinzip der primitiven Rekursion aufgebaut.

## add.c

```

int add(m,n)
{
    if (m == 0) {
        return n;
    } else {
        return
            succ(add(m-1,n));
    }
}

```

## mult.c

```

int mult(m,n)
{
    if (m == 0) {
        return 0;
    } else {
        return
            add(mult(m-1,n),n);
    }
}

```

## pow.c

```

int pow(m,n)
{
    if (m == 0) {
        return 1;
    } else {
        return
            mult(pow(m-1,n),n);
    }
}

```

Programm, das die Form aus Abbildung 6.17 besitzt. Anschließend extrahieren wir die Formelanteile  $g$  und  $h$  und konstruieren daraus die gesuchte Darstellung.

Basierend auf den Implementierungen aus Abbildung 6.18 erhalten wir für die Addition, die Multiplikation und die Potenzierung die folgenden Ergebnisse:

$$\text{add}(m,n) = \begin{cases} n & \text{falls } m = 0 \\ \text{succ}(\text{add}(m-1,n)) & \text{falls } m > 0 \end{cases} \quad (6.21)$$

$$\text{mult}(m,n) = \begin{cases} 0 & \text{falls } m = 0 \\ \text{add}(\text{mult}(m-1,n),n) & \text{falls } m > 0 \end{cases} \quad (6.22)$$

$$\text{pow}(m,n) = \begin{cases} 1 & \text{falls } m = 0 \\ \text{mult}(\text{pow}(m-1,n),n) & \text{falls } m > 0 \end{cases} \quad (6.23)$$

Nachdem das Grundschema der primitiven Rekursion eingeführt ist, können wir die *primitiv-rekursiven Funktionen* formal erklären:



### Definition 6.8 (Primitiv-rekursive Funktionen)

- Die Nullfunktion  $f(n) := 0$  ist primitiv-rekursiv.
- Die Nachfolgerfunktion  $\text{succ}(n) := n + 1$  ist primitiv-rekursiv.
- Die Projektion  $p_i^n(x_1, \dots, x_n) := x_i$  ist primitiv-rekursiv.
- Sind  $h : \mathbb{N}_0^k \rightarrow \mathbb{N}_0$  und  $g_1, \dots, g_k : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$  primitiv-rekursiv, dann ist es auch  $h(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n))$ .
- Sind  $g : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$  und  $h : \mathbb{N}_0^{n+2} \rightarrow \mathbb{N}_0$  primitiv-rekursiv, dann ist es auch  $f(m, x_1, \dots, x_n)$  mit

$$f(0, x_1, \dots, x_n) = g(x_1, \dots, x_n), \\ f(m+1, x_1, \dots, x_n) = h(f(m, x_1, \dots, x_n), m, x_1, \dots, x_n).$$

**Abbildung 6.18:** Aus der gewählten Programmstruktur lässt sich die primitiv-rekursive Definition der implementierten arithmetischen Operationen sofort ableiten.

Die Definition folgt dem induktiven Schema aus Abschnitt 2.4. Die ersten drei Regeln legen die elementaren primitiven Funktionen fest; natürlich sind dies die Nullfunktion, die Nachfolgerfunktion und die Projektion. Die letzten beiden Regeln geben an, wie sich aus bereits bekannten primitiv-rekursiven Funktionen weitere konstruieren lassen. Die erste Regel erlaubt uns, primitiv-rekursive Funktionen als Parameter einzusetzen (*Komposition*), die zweite besagt, dass die Menge bez. primitiver Rekursion abgeschlossen ist. Das zum Einsatz kommende

## ■ Lineare Rekursion

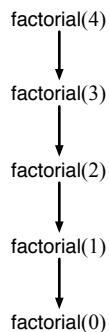
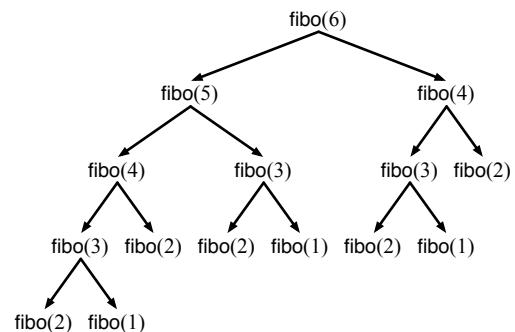
**factorial.java**

```
public static factorial(int n) {
    if (n == 0) {
        return 1;
    } else {
        return n * factorial(n-1);
    }
}
```

## ■ Verzweigende Rekursion

**fibonacci.java**

```
public static fibo(int n) {
    if (n <= 2) {
        return 1;
    } else {
        return fibo(n-1) + fibo(n-2);
    }
}
```

■ Berechnungsbaum für  $n = 4$ ■ Berechnungsbaum für  $n = 6$ **Abbildung 6.19:** Lineare Rekursion und verzweigende Rekursion im Vergleich

Bildungsschema ist eine verallgemeinerte Variante der primitiven Rekursion aus Definition 6.7.

Legen wir die eingeführten Bildungsregeln streng aus, so entsprechen die Funktionen (6.21) bis (6.23) nicht der in Definition 6.8 festgelegten Struktur. Durch den geschickten Einsatz der Projektionsfunktion können wir diese jedoch leicht in eine entsprechende Form bringen:

$$\begin{aligned}
 \text{add}(0, n) &= p_1^1(n), \\
 \text{add}(m+1, n) &= \text{succ}(p_1^3(\text{add}(m, n), m, n)) \\
 \text{mult}(0, n) &= 0, \\
 \text{mult}(m+1, n) &= \text{add}(p_1^3(\text{mult}(m, n), m, n), p_3^3(\text{mult}(m, n), m, n)) \\
 \text{pow}(0, n) &= \text{succ}(0), \\
 \text{pow}(m+1, n) &= \text{mult}(p_1^3(\text{pow}(m, n), m, n), p_3^3(\text{pow}(m, n), m, n))
 \end{aligned}$$

Die primitive Rekursion ist nur ein Rekursionsschema von vielen. Sie gehört in die größere Gruppe der *linearen Rekursionen*, in der sich z. B. auch die *Kopfrekursion (head recursion)* und die *Endrekursion (tail recursion)* befinden. Von einer linearen Rekursion sprechen wir immer dann, wenn in jeder Rekursionsebene höchstens ein weiterer rekursiver Aufruf initiiert wird. Eine Kopf- bzw. eine Endrekursion liegt vor, wenn der Selbstauftrag die erste bzw. die letzte Aktion nach dem Basisfalltest ist. Hinter dem primitiven Rekursionsschema verbirgt sich somit eine spezielle Kopfrekursion, die den Wert des ersten Parameters in jedem neuen Aufruf um eins verringert.

Die lineare Rekursion verdankt ihren Namen der Eigenschaft, dass jeder Aufruf zu einem Berechnungsbau in Form einer linearen Kette führt (vgl. Abbildung 6.19 links). Lassen wir dagegen mehrere, nacheinander ausgeführte Aufrufe zu, so entsteht eine Baumstruktur und wir reden von einer *verzweigenden Rekursion* (vgl. Abbildung 6.19 rechts). Sind die rekursiven Aufrufe derart miteinander verknüpft, dass das Ergebnis eines rekursiven Aufrufs als Parameter für den nächsten Aufruf dient, so sprechen wir von einer *verschachtelten Rekursion*. Eine *wechselseitige Rekursion* liegt vor, wenn sich mehrere Funktionen gegenseitig aufrufen.

David Hilbert äußerte im Jahre 1926 die Vermutung, dass alle berechenbaren Funktionen primitiv-rekursiv sind [46]. In diesem Sinne müssten sich alle Rekursionstypen auf die primitive Rekursion reduzieren lassen. Hilberts Annahme wurde durch die Arbeit von Wilhelm Ackermann widerlegt [1]. Mit der Ackermann-Funktion präsentierte er eine Funktion, die nicht primitiv-rekursiv ist, aber mit Hilfe verschachtelter Rekursionsaufrufe berechnet werden kann. Die Ackermann-Funktion ist uns in diesem Buch bereits mehrfach begegnet, wenn auch nicht in der im Jahre 1928 publizierten Form.

Die Projektionsfunktion  $p_i^j$  ist ein wertvolles Hilfsmittel, um primitiv-rekursive Funktionen flexibel umzuformen; wir können sie einsetzen, um Variablen gezielt auszuwählen oder zu vertauschen. Ist die Funktion  $f(x_1, x_2, x_3, x_4)$  primitiv-rekursiv, dann ist es beispielsweise auch  $g(x_1, x_2) = f(x_2, x_1, x_1, 0)$ . Mit Hilfe der Projektionsfunktion können wir  $g$  ohne Umwege aus  $f$  konstruieren:

$$g(x_1, x_2) = f(p_2^2(x_1, x_2), p_1^2(x_1, x_2), p_1^2(x_1, x_2), 0)$$

Primitiv-rekursive Funktionen besitzen eine Eigenschaft, die an die Diskussion der Loop-Sprache erinnert: Sie sind allesamt total. Mit einem einfachen induktiven Argument ist die Gültigkeit dieser Aussage leicht einzusehen. Zunächst sind die elementaren primitiv-rekursiven Funktionen offensichtlich total. Des Weiteren lassen die beiden Bildungsregeln (Komposition und primitive Rekursion) erneut totale Funktionen entstehen.

Wie Sie vielleicht schon vermuten, gehen die Gemeinsamkeiten zwischen primitiv-rekursiven Funktionen und Loop-berechenbaren Funktionen noch deutlich weiter. In der Tat lässt sich durch eine geeignete Transformation jede Loop-berechenbare Funktion primitiv-rekursiv formulieren und umgekehrt jede primitiv-rekursive Funktion mit Hilfe eines Loop-Programms berechnen. Kurzum: Beide Berechnungsmodelle sind äquivalent.

Wir wollen nun genauer betrachten, wie die entsprechenden Transformationen aussehen müssen. Im Folgenden sei  $P$  ein Loop-Programm, in dem die Variablen  $x_1, \dots, x_n$  vorkommen. Mit  $a_1, \dots, a_n$  bezeichnen wir eine beliebige Anfangsbelegung von  $x_1, \dots, x_n$  und mit  $b_1, \dots, b_n$  die Endbelegung, die sich nach der Ausführung von  $P$  einstellt. Wir werden nun herausarbeiten, wie sich  $P$  in eine primitiv-rekursive Funktion

$$f_P : \mathbb{N}_0 \rightarrow \mathbb{N}_0 \tag{6.24}$$

mit der folgenden Eigenschaft transformieren lässt:

$$f_P(\pi(a_0, \dots, a_n)) = \pi(b_0, \dots, b_n) \tag{6.25}$$

$\pi$  ist eine beliebige Funktion, die  $\mathbb{N}_0^n$  bijektiv auf  $\mathbb{N}_0$  abbildet, und dient dazu, den Inhalt des kompletten Variablenatzes  $x_1, \dots, x_n$  eindeutig in eine einzige natürliche Zahl hineinzucodieren. Eines ähnlichen Kunstgriffs haben wir uns bereits in Abschnitt 6.1.1 im Zusammenhang mit der Loop-Implementierung eines Stapelspeichers bedient.

Da  $\pi$  eine bijektive Abbildung ist, lässt sich die Zuordnung umkehren. Ausgehend von  $\pi^{-1}$  definieren wir  $n$  Umkehrfunktionen

$$\pi_1^{-1} : \mathbb{N}_0 \rightarrow \mathbb{N}_0, \dots, \pi_n^{-1} : \mathbb{N}_0 \rightarrow \mathbb{N}_0 \tag{6.26}$$

mit der Eigenschaft

$$\pi_i^{-1}(\pi(x_1, \dots, x_n)) = x_i \quad (6.27)$$

Über die Funktion  $\pi_i^{-1}$  lässt sich der Wert von  $x_i$  aus der Codierung  $\pi(x_1, \dots, x_n)$  zurückberechnen (vgl. Abbildungen 6.20 und 6.21). Dass die Funktionen  $\pi, \pi_i^{-1}$  existieren, ist nach den bisher in diesem Buch errungenen Erkenntnissen selbstverständlich. Dass sie sich primitiv-rekursiv berechnen lassen, dagegen nicht. Im Übungsteil auf Seite 322 werden wir herausarbeiten, dass tatsächlich primitiv-rekursive Funktionen  $\pi$  und  $\pi_i^{-1}$  mit der gesuchten Eigenschaft existieren.

Die gesuchte Funktion  $f_P$  lässt sich induktiv aus dem Aufbau eines Loop-Programms  $P$  ableiten. Wir unterscheiden 5 Fälle:

- Fall 1:  $P$  ist von der Form  $x_i := 0$

Wir setzen

$$f_P(\pi(a_0, \dots, a_n)) := \pi(a_0, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \quad (6.28)$$

- Fall 2:  $P$  ist von der Form  $x_i := x_j$

Wir setzen

$$f_P(\pi(a_0, \dots, a_n)) := \pi(a_0, \dots, a_{i-1}, a_j, a_{i+1}, \dots, a_n) \quad (6.29)$$

- Fall 3:  $P$  ist von der Form  $x_i := \text{succ}(x_j)$  oder  $x_i := \text{pred}(x_j)$

Wir setzen

$$f_P(\pi(a_0, \dots, a_n)) := \pi(a_0, \dots, a_{i-1}, a_j \pm 1, a_{i+1}, \dots, a_n) \quad (6.30)$$

- Fall 4:  $P$  ist von der Form  $P' ; P''$

Für die Teilausdrücke  $P'$  und  $P''$  existieren primitiv-rekursive Funktionen  $f_{P'}$  und  $f_{P''}$ . Wir setzen

$$f_P(\pi(a_0, \dots, a_n)) := f_{P''}(f_{P'}(\pi(a_0, \dots, a_n))) \quad (6.31)$$

- Fall 5:  $P$  ist von der Form  $\text{loop } x_i \text{ do } P' \text{ end}$

Für den Teilausdruck  $P'$  ist eine primitiv-rekursive Funktion  $f_{P'}$  bereits bekannt. Wir setzen

$$f_P(\pi(a_0, \dots, a_n)) = f_{\text{loop}}(a_i, \pi(a_0, \dots, a_n)) \quad (6.32)$$

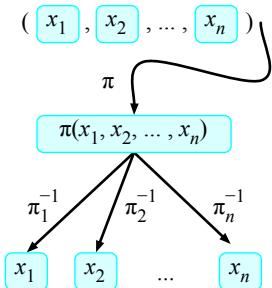
mit

$$f_{\text{loop}}(0, x) = x \quad (6.33)$$

$$f_{\text{loop}}(n+1, x) = f_{P'}(f_{\text{loop}}(n, x), x) \quad (6.34)$$

Die Hilfsfunktion  $f_{\text{loop}}$  ist offenbar primitiv-rekursiv und damit auch die konstruierte Funktion  $f_P$ .

### ■ Codierungsschema

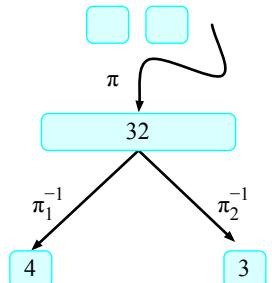


**Abbildung 6.20:** Mit Hilfe der Funktion  $\pi$  kann der komplette Variablensatz  $x_1, \dots, x_n$  eines Loop-Programms in eine einzige natürliche Zahl hineincodiert werden.

### ■ Wertetabelle von $\pi$

	$x = 2$	$x = 3$	$x = 4$
$y = 1$	8	13	19
$y = 2$	12	18	25
$y = 3$	17	24	32
	⋮	⋮	⋮

### ■ Codierung



**Abbildung 6.21:** Demonstration des Codierungsschemas am Beispiel des Zahlenpaares (4,3)

■ Komposition

**composition.loop**

```

1   y1 := g1(x1, ..., xn);
2   y2 := g2(x1, ..., xn);
3   ...
4   yk := gk(x1, ..., xn);
5   x0 := h(y1, y2, ..., yk)
6
7
8

```

■ Primitive Rekursion

**primrek.loop**

```

1   y := 0;
2   x0 := g(x1, ..., xn);
3
4   loop m do
5     y := succ(y);
6     x0 := h(x0, y, x1, ..., xn);
7   end
8
9

```

**Abbildung 6.22:** Der rekursive Aufbau primitiv-rekursiver Funktionen wird durch zwei Bildungsschemata bestimmt: Komposition und primitive Rekursion. Beide lassen sich innerhalb der Loop-Sprache formulieren.

Auch die umgekehrte Transformation ist möglich, d. h., wir können jede primitiv-rekursive Funktion  $f$  mit Hilfe eines Loop-Programms berechnen. Zunächst halten wir fest, dass die drei primitiv-rekursiven Elementarfunktionen (Nullfunktion, Nachfolgerfunktion, Projektion) offensichtlich Loop-berechenbar sind. Damit verbleibt die Aufgabe, die Loop-Berechenbarkeit für zwei weitere Fälle zu zeigen:

■ Fall 1:  $f$  ist von der Form

$$f(x_1, \dots, x_n) = h(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n))$$

Abbildung 6.22 (oben) zeigt, wie sich  $f$  berechnen lässt.

■ Fall 2:  $f$  ist von der Form

$$f(0, x_1, \dots, x_n) = g(x_1, \dots, x_n),$$

$$f(m+1, x_1, \dots, x_n) = h(f(m, x_1, \dots, x_n), m, x_1, \dots, x_n)$$

Abbildung 6.22 (unten) zeigt, wie sich  $f$  berechnen lässt.

Der folgende Satz trägt die Früchte unserer Arbeit zusammen:



**Satz 6.5**

Die Klasse der primitiv-rekursiven Funktionen stimmt mit der Klasse der Loop-berechenbaren Funktionen überein.

## $\mu$ -Rekursion

Die in Satz 6.5 manifestierte Äquivalenz hat zur Folge, dass sich sämtliche Limitierungen der Loop-Sprache mit einem Schlag auf die Klasse der primitiv-rekursiven Funktionen übertragen. Zum einen ist es unmöglich, partielle primitiv-rekursive Funktionen zu definieren, zum anderen existieren totale Funktionen wie die Ackermann-Funktion, die sich nicht primitiv-rekursiv formulieren lassen.

Abhilfe schafft eine Erweiterung des Rekursionsschemas, die als  $\mu$ -Rekursion bezeichnet wird. Ausgangspunkt ist eine  $n+1$ -stellige Funktion  $f : \mathbb{N}_0^{n+1} \rightarrow \mathbb{N}_0$ , die durch die Anwendung des  $\mu$ -Operators wie folgt auf eine  $n$ -stellige Funktion reduziert wird:

$$(\mu f)(x_1, \dots, x_n) := \min \left\{ m \mid \begin{array}{l} f(m, x_1, \dots, x_n) = 0 \\ \text{und für alle } k < m \text{ ist} \\ f(k, x_1, \dots, x_n) \neq \perp \end{array} \right\} \quad (6.35)$$

Beachten Sie, dass die rechte Seite von Gleichung (6.35) zur leeren Menge degradieren kann. In diesem Fall ist kein minimales Element vorhanden und der Funktionswert  $(\mu f)(x_1, \dots, x_n)$  per Definition gleich  $\perp$ . Wir verwenden den  $\mu$ -Operator als Grundlage, um die Klasse der  $\mu$ -rekursiven Funktionen zu definieren:

### **Definition 6.9 ( $\mu$ -rekursive Funktionen)**

Die Klasse der  $\mu$ -rekursiven Funktionen ist die kleinste Klasse von Funktionen, die alle primitiv-rekursiven Funktionen enthält und außerdem unter der Anwendung des  $\mu$ -Operators abgeschlossen ist.

Für die Klasse der  $\mu$ -rekursiven Funktionen existiert eine Analogie zu Satz 6.5. Wir werden zeigen, dass jede While-berechenbare Funktion  $\mu$ -rekursiv ist und umgekehrt.

Hierzu sei mit  $P$  ein beliebiges While-Programm gegeben. Genau wie oben konstruieren wir hieraus eine Funktion  $f_P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  mit der Eigenschaft

$$f_P(\pi(a_0, \dots, a_n)) = \pi(b_0, \dots, b_n) \quad (6.36)$$

Die Variablenmengen  $a_1, \dots, a_n$  und  $b_1, \dots, b_n$  bezeichnen erneut die Anfangs- und die Endbelegung der Programmvariablen. Die Funktion  $f_P$  lässt sich wieder induktiv aus der Programmstruktur von  $P$  ableiten und wird  $\mu$ -rekursiv sein.

Für alle Elemente der While-Sprache, die auch in der Loop-Sprache enthalten sind, können wir die weiter oben durchgeföhrten Beweisschritte eins zu eins übernehmen. Es bleibt, den Beweis für Programme  $P$  der Form `while  $x_i$  do  $P'$  end` zu föhren. In diesem Fall wird das Teillprogramm  $P'$  so lange ausgeführt, bis  $x_i$  den Wert 0 annimmt und  $P'$  in allen vorangegangenen Iterationen terminiert. Definieren wir die ( $\mu$ -rekursive) Hilfsfunktion  $h(m, x)$  als

$$h(m, x) := \underbrace{f_{P'}(f_{P'}(\dots(f_{P'}(x) \dots)))}_{m-\text{mal}}, \quad (6.37)$$

so lässt sich die Anzahl der Iterationen einer (terminierenden) While-Schleife über die Formel

$$\min\{m \mid \pi_i^{-1}(h(m, x)) = 0\} \quad (6.38)$$

berechnen. Mit Hilfe des  $\mu$ -Operators können wir die Formel (6.38) in

$$(\mu(\pi_i^{-1} \circ h))(x) \quad (6.39)$$

**$\mu$ -recursion.while**

```

1   y := f(0,x1,...,xn);
2   while y ≠ 0 do
3       x0 := succ(x0);
4       y := f(x0,x1,...,xn);
5   end

```

**Abbildung 6.23:** Die While-Schleife ist ausdrucksstark genug, um den  $\mu$ -Operator zu simulieren.

umformulieren und erhalten mit

$$f_P(x) = h((\mu(\pi_i^{-1} \circ h))(x), x) \quad (6.40)$$

die von uns gesuchte Funktion.

Damit entpuppt sich die  $\mu$ -Rekursion als mächtig genug, um das While-Konstrukt in allen seinen Facetten zu simulieren.

Umgekehrt lässt sich jede  $\mu$ -rekursive Funktion mit Hilfe eines While-Programms berechnen. Auch hier können wir sämtliche Beweisschritte übernehmen, die sich auf primitiv-rekursive Formeln beziehen, und müssen nur noch zeigen, dass sich der  $\mu$ -Operator auf ein äquivalentes While-Konstrukt abbilden lässt.

Hierzu sei mit  $f(m, x_1, \dots, x_n)$  eine beliebige  $\mu$ -rekursive Funktion gegeben. Unter der Induktionsannahme, dass  $f(m, x_1, \dots, x_n)$  While-berechenbar ist, können wir die Funktion

$$(\mu f)(x_1, \dots, x_n) := \min \left\{ m \mid \begin{array}{l} f(m, x_1, \dots, x_n) = 0 \\ \text{und für alle } k < m \text{ ist} \\ f(k, x_1, \dots, x_n) \neq \perp \end{array} \right\} \quad (6.41)$$

wie in Abbildung 6.23 gezeigt, berechnen. Damit sind wir am Ziel und haben den folgenden Satz bewiesen:

 **Satz 6.6**

Die Klasse der  $\mu$ -rekursiven Funktionen stimmt mit der Klasse der While-berechenbaren Funktionen überein.

Erneut können wir mit einem Schlag auf die Erkenntnisse zurückgreifen, die wir in der Diskussion über die While-Sprache gewonnen haben. Erinnern Sie sich noch an Satz 6.3 – den Satz von Kleene? Dieser besagte, dass sich jede While-berechenbare Funktion durch ein Programm mit nur einer While-Schleife berechnen lässt. Drücken wir die gewonnene Erkenntnis in der Nomenklatur der  $\mu$ -rekursiven Funktionen aus, so erhalten wir auf direktem Weg das folgende Ergebnis:

 **Korollar 6.2**

Jede  $n$ -stellige  $\mu$ -rekursive Funktion  $f : \mathbb{N}_0^n \rightarrow \mathbb{N}$  lässt sich in der Form

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_n, (\mu h)(x_1, \dots, x_n))$$

berechnen, wobei  $h$  und  $g$  primitiv-rekursiv sind.

### 6.1.5 Turing-Maschinen

Die Turing-Maschine ist das älteste und gleichzeitig am häufigsten bemühte Modell, um den Berechenbarkeitsbegriff formal zu erfassen. Mit seinem im Jahre 1936 vorgestellten Begriffsgerüst gelingt Turing eine bemerkenswerte Gratwanderung. Zum einen erfüllt die Turing-Maschine in jeder Hinsicht die Anforderungen eines formalen Modells, so dass sie mathematisch präzise Aussagen über den Berechenbarkeitsbegriff erlaubt. Zum anderen ist sie von einer inneren Einfachheit und Klarheit geprägt, die einen überraschend intuitiven Zugang zu dieser komplexen Materie eröffnet. Im Gegensatz zu rein mathematischen Ansätzen, zu denen z. B. das zeitgleich von Alonzo Church entwickelte *Lambda-Kalkül* [18, 19] und die in Abschnitt 6.1.4 vorgestellte Theorie der primitiv-rekursiven Funktionen gehören, erscheint die Turing-Maschine zum Anfassen nah.

#### 6.1.5.1 Einband-Turing-Maschinen

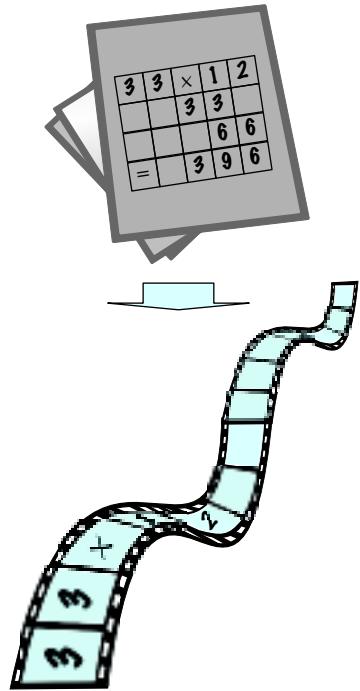
In seiner Originalarbeit motivierte Turing die Konzeption seines Maschinenmodells wie folgt:

*„Computing is normally done by writing certain symbols on paper. We may suppose this paper is divided into squares like a child's arithmetic book.“*

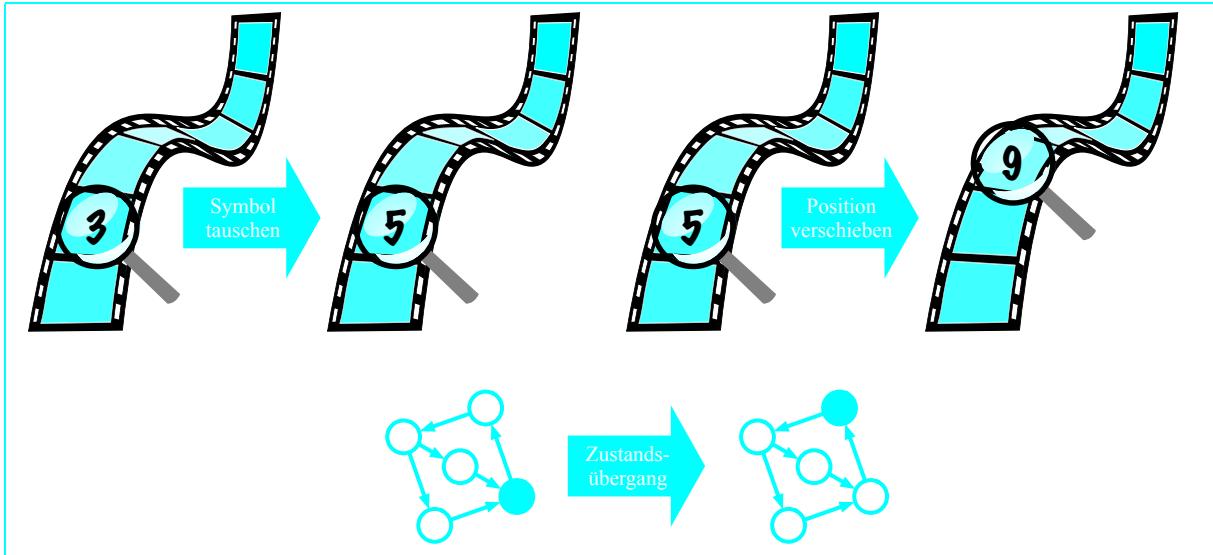
Das Zitat zeigt die Unbefangenheit, die sich durch Turings gesamte Arbeit zieht. Er startete seine Überlegungen über die Berechenbarkeit mit dem, was er seit seiner Kindheit zum Rechnen verwendete: einem leeren Stück karierten Papier. Unmittelbar danach nahm Turing dann doch eine erste Abstraktion vor. Er sah, dass die zweidimensionale Gestalt des Rechenpapiers im Grunde genommen keine Rolle spielt. Alle Berechnungen, die wir per Hand auf Papier durchführen können, sind auch auf einem eindimensionalen Band möglich – wenngleich nicht immer mit der gleichen Eleganz (vgl. Abbildung 6.24).

*„[...] I think that it is agreed that the two-dimensional character of paper is no essential of computation. I assume then that the computation is carried out on one-dimensional paper, i.e. on tape divided into squares.“*

Turing lässt weitere Annahmen folgen. Zunächst geht er davon aus, dass es nur endlich viele Symbole gibt, mit denen die Felder seines Bandes gefüllt werden können. Er ging außerdem davon aus, dass sich das



**Abbildung 6.24:** Der britische Mathematiker Alan Turing machte ein unendlich langes Band zur Grundlage seines Rechenmodells. Aus mathematischer Sicht ist ein solches ausreichend, da sich alle Rechenoperationen, die auf einem zweidimensionalen Blatt durchgeführt werden können, auf einem eindimensionalen Band nachvollziehen lassen.



**Abbildung 6.25:** Turing definierte wenige primitive Elementaroperationen, aus denen komplexe Berechnungen erwachsen. In jedem Bearbeitungsschritt kann eine Turing-Maschine das aktuell betrachtete Symbol durch ein anderes ersetzen und das Betrachtungsfenster (*observed square*) verschieben. Die ausgeführten Aktionen gehen mit einem potenziellen Wechsel des inneren Zustands (*state of mind*) einher.

menschliche Gehirn im Zuge einer Berechnung zu jedem Zeitpunkt in einem von endlich vielen Zuständen befindet.

*„We may suppose that there is a bound  $B$  to the number of symbols or squares which the computer can observe at one moment. [...] We will also suppose that the number of states of mind which will be taken into account is finite.“*

Anschließend definiert Turing eine Menge von Elementaroperationen, aus denen sich komplexe Berechnungen zusammensetzen. Diese erlauben, das Symbol des aktuell betrachteten Felds auszutauschen und die Aufmerksamkeit auf eines der Nachbarfelder zu lenken:

*„The simple operations must therefore include: (a) Changes of the symbol on one of the observed squares. (b) Changes of one of the squares observed to another square within  $L$  squares of one of the previously observed squares.“*

Beide Aktionen werden durch einen möglichen Wechsel des internen Zustands begleitet:

*„It may be that some of these changes necessarily involve a change of state of mind. The most general single operation must therefore be taken to be one of the following: (A) A possible change (a) of symbol together with a possible change of state of mind. (B) A possible change (b) of observed squares, together with a possible change of state of mind.“*

Abbildung 6.25 fasst die von Turing eingeführten Elementaroperationen bildlich zusammen.

Damit ist es an der Zeit, den Begriff der Turing-Maschine formal zu präzisieren. Wir orientieren uns dabei an der Nomenklatur, die wir für die Beschreibung endlicher Automaten in Kapitel 5 erfolgreich eingesetzt haben.



### Definition 6.10 (Turing-Maschine)

Eine (deterministische) Turing-Maschine, kurz TM, ist ein 7-Tupel  $(S, \Sigma, \Pi, \delta, s_0, \square, E)$ . Sie besteht aus

- der endlichen *Zustandsmenge*  $S$ ,
- dem endlichen *Eingabealphabet*  $\Sigma$ ,
- dem *Bandalphabet*  $\Pi$  mit  $\Pi \supset \Sigma$ ,
- der *Zustandsübergangsfunktion*  $\delta : S \times \Pi \rightarrow S \times \Pi \times \{\leftarrow, \rightarrow\}$ ,
- dem *Startzustand*  $s_0$ ,
- dem *Blank-Symbol*  $\square \in \Pi \setminus \Sigma$ ,
- der Menge der *Endzustände (Finalzustände)*  $E \subseteq S$ .

Zu Beginn befindet sich jede Turing-Maschine in ihrem Startzustand  $s_0$ . Das zu verarbeitende Eingabewort  $\omega \in \Sigma^*$  steht bereits auf dem Band und der virtuelle Schreib-Lese-Kopf ist über dem ersten Eingabezeichen positioniert. Beachten Sie, dass die Maschine über ein Band verfügt, dass sich in beide Richtungen unendlich weit ausbreitet. Um die noch freien Felder von dem Eingabewort unterscheiden zu können, vereinbaren wir, dass alle Felder links und rechts der Eingabesequenz mit dem Blank-Symbol  $\square$  beschrieben sind.

Ausgehend von dieser Initialkonfiguration führt eine Turing-Maschine die folgenden Aktionen durch (vgl. Abbildung 6.26):

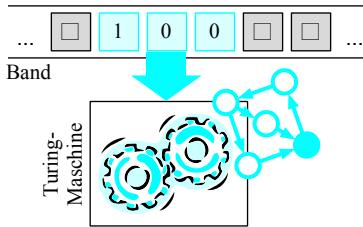


Alan Mathison Turing (1912 – 1954)

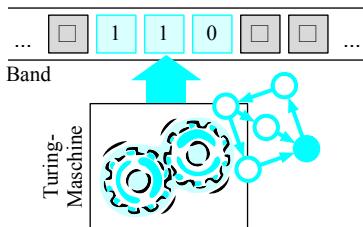
Alan Turing wurde am 23. Juni 1912 in London-Paddington geboren. Bereits in seiner frühen Jugend wurde seine außerordentliche mathematische Begabung sichtbar, genauso wie sein Unvermögen, sich gesellschaftlichen Normen und staatlichen Autoritäten zu beugen. Turings wissenschaftliches Vermächtnis ist beachtlich. Neben seinen grundlegenden Beiträgen zur Theorie der Berechenbarkeit lieferte er während des zweiten Weltkriegs wertvolle Erkenntnisse im Bereich der Kryptoanalyse. Im Jahre 1950 schlug er mit dem *Turing-Test* ein Verfahren vor, mit dem sich der Intelligenzbegriff auf Maschinen übertragen lässt [92].

Im Jahr 1952 sollte Turings Karriere ein abruptes Ende finden. Als die Polizei sein Haus nach einem Einbruch untersuchte, gestand er eine homosexuelle Beziehung ein. Das prüde England der Sechzigerjahre reagierte erbarmungslos und sprach Turing in einem Strafverfahren der sexuellen Perversion schuldig. Die angeordnete Zwangsterapien machten aus ihm einen gebrochenen Mann. Zwei Jahre später, am 7. Juni 1954, wurde Alan Turing im Alter von 42 Jahren neben den Resten eines vergifteten Apfels tot aufgefunden.

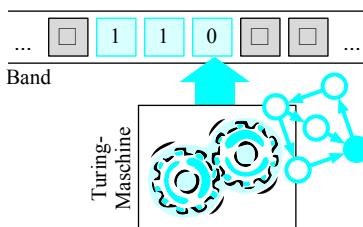
■ Zeichen lesen



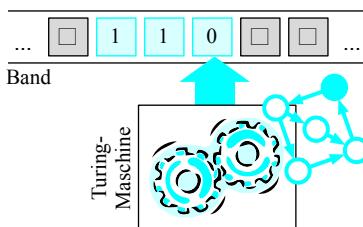
■ Zeichen schreiben



■ Kopf bewegen



■ Zustand wechseln



- Der Schreib-Lese-Kopf liest das aktuelle Bandzeichen  $\sigma$  ein

- Der Funktionswert  $(s', \sigma', r) = \delta(s, \sigma)$  wird berechnet

- Das Bandzeichen wird durch  $\sigma'$  ersetzt

- Der Kopf wird nach links ( $r = ' \leftarrow '$ ) oder rechts ( $r = ' \rightarrow '$ ) bewegt

- Der Folgezustand  $s'$  wird eingenommen

Hierin bezeichnet  $s$  den Zustand, in dem sich die Turing-Maschine aktuell befindet. Die Übergangsfunktion  $\delta$  ist eine partielle Funktion und muss deshalb nicht für alle Eingabekombinationen aus der Menge  $S \times \Sigma$  definiert sein. In der Konsequenz kann die Turing-Maschine (gewolltermaßen) in einen Zustand geraten, der keine weitere Aktion mehr zulässt. In diesem Fall bleibt die Maschine stehen und die Berechnung ist beendet.

Nachdem wir die Funktionsweise einer Turing-Maschine informell festgelegt haben, wollen wir das Gesagte in eine mathematisch präzise Form überführen. Wie schon im Falle des endlichen Automaten und seiner diversen Varianten spielen der Begriff der Konfiguration und die darauf definierte Übergangsrelation → die zentrale Rolle.



### Definition 6.11 (Konfiguration (TM))

Sei  $T = (S, \Sigma, \Pi, \delta, s_0, \square, E)$  eine beliebige Turing-Maschine. Jedes Tripel  $(v, s, \omega)$  mit  $v, \omega \in \Pi^+$  und  $s \in S$  heißt eine *Konfiguration* von  $T$ . Die Übergangsrelation → <sub>$T$</sub>  definieren wir wie folgt:

- Rechtsbewegung:  $\delta(s, \sigma) = (s', \sigma', \rightarrow), \rho, \sigma \in \Pi$

$$(v\rho, s, \sigma\omega) \rightarrow_T \begin{cases} (v\rho\sigma', s', \omega) & \text{falls } \omega \neq \varepsilon \\ (v\rho\sigma', s', \square) & \text{falls } \omega = \varepsilon \end{cases}$$

- Linksbewegung:  $\delta(s, \sigma) = (s', \sigma', \leftarrow), \rho, \sigma \in \Pi$

$$(v\rho, s, \sigma\omega) \rightarrow_T \begin{cases} (v, s', \rho\sigma'\omega) & \text{falls } v \neq \varepsilon \\ (\square, s', \rho\sigma'\omega) & \text{falls } v = \varepsilon \end{cases}$$

Informell gesprochen besitzen die drei Konfigurationsbestandteile die folgende Bedeutung:  $v$  und  $\omega$  bilden zusammen den Bandinhalt, wobei sich der Schreib-Lese-Kopf aktuell über dem ersten Zeichen von  $\omega$  befindet.  $s$  ist der aktuelle Zustand der Turing-Maschine. In der Festlegung der Übergangsrelation müssen wir berücksichtigen, dass sich der

Abbildung 6.26: Die Turing-Maschine in Aktion

Schreib-Lese-Kopf beliebig nach links und rechts und damit insbesondere über die Grenzen des Eingabewortes hinweg bewegen darf. Unsere Definition trägt diesem Verhalten Rechnung, indem der Bandinhalt beim Überschreiten der Wortgrenze um ein Blank-Symbol verlängert wird.

Abbildung 6.27 demonstriert die Konfigurationsübergänge anhand eines konkreten Beispiels. Die Zustandsübergangsfunktion  $\delta$  ist aus Gründen der Übersichtlichkeit in Form einer Tabelle definiert. Im unteren Teil der Abbildung sind die Konfigurationsübergänge dargestellt, die während der Bearbeitung des Eingabeworts  $\omega = 111111$  entstehen. Die Übergangsfunktion  $\delta$  ist so definiert, dass sich die Turing-Maschine im Startzustand  $s_0$  zunächst nach rechts über alle vorgefundenen Einsen hinwegbewegt und das erste vorgefundene Blank-Symbol durch eine 1 ersetzt. Zeitgleich wechselt sie in den Zustand  $s_1$  und beginnt, den Schreib-Lese-Kopf nach links zurückzubewegen. Sobald sich dieser links über das erste Eingabezeichen hinausschiebt, kehrt die Maschine mit einer Rechtsbewegung auf das erste Eingabezeichen zurück und stoppt im Terminalzustand  $s_2$ . Insgesamt haben wir mit diesem ersten Beispiel eine Maschine kennen gelernt, die das Eingabewort  $\omega = 1^n$  in das Ausgabewort  $f(\omega) = 1^{n+1}$  überführt.

Analog zu den Begriffen der Loop-, While- und Goto-Berechenbarkeit sind wir jetzt in der Lage, den Begriff der *Turing-Berechenbarkeit* formal zu definieren:



### Definition 6.12 (Turing-Berechenbarkeit)

Mit  $f : \Sigma^* \rightarrow \Sigma^*$  sei eine beliebige partielle Funktion über Wörtern des Eingabealphabets  $\Sigma$  gegeben.  $f$  heißt *Turing-berechenbar*, falls eine Turing-Maschine  $T = (S, \Sigma, \Pi, \delta, s_0, \square, E)$  mit den folgenden Eigenschaften existiert:

- $T$  terminiert unter Eingabe von  $\omega$  genau dann in einem Endzustand  $s_e \in E$ , wenn  $f(\omega) \neq \perp$
- In diesem Fall gilt:  $(\square, s_0, \omega) \xrightarrow{*} (\square^*, s_e, f(\omega)\square^*)$

Informell stellt sich der Begriff der Turing-Berechenbarkeit wie folgt dar: Um den Funktionswert  $f(\omega)$  zu berechnen, wird zunächst die Zeichenfolge  $\omega$  an einer beliebigen Stelle auf das Band geschrieben und der Schreib-Lese-Kopf auf das erste Zeichen positioniert. Anschließend wird die Maschine gestartet und die weiter oben im Detail beschriebenen Berechnungsschritte durchgeführt. Terminiert die Maschine in einem Endzustand, so können wir den Funktionswert  $f(\omega)$  vom Band

### Turing-Maschine

$$\begin{aligned} S &= \{s_0, s_1, s_2\} \\ \Sigma &= \{1\} \\ \Pi &= \{\square\} \\ E &= \{s_2\} \end{aligned}$$

### Übergangstabelle

	1	$\square$
$s_0$	$(s_0, 1, \rightarrow)$	$(s_1, 1, \leftarrow)$
$s_1$	$(s_1, 1, \leftarrow)$	$(s_2, \square, \rightarrow)$
$s_2$	—	—

### Konfigurationsübergänge

$\rightarrow$	$(\square, s_0, 111111)$
$\rightarrow$	$(\square 1, s_0, 111111)$
$\rightarrow$	$(\square 11, s_0, 111111)$
$\rightarrow$	$(\square 111, s_0, 111111)$
$\rightarrow$	$(\square 1111, s_0, 111111)$
$\rightarrow$	$(\square 11111, s_0, 111111)$
$\rightarrow$	$(\square 111111, s_0, 111111)$
$\rightarrow$	$(\square 111111, s_1, 111111)$
$\rightarrow$	$(\square 1111, s_1, 111111)$
$\rightarrow$	$(\square 111, s_1, 111111)$
$\rightarrow$	$(\square 11, s_1, 111111)$
$\rightarrow$	$(\square 1, s_1, 111111)$
$\rightarrow$	$(\square, s_1, 111111)$
$\rightarrow$	$(\square, s_1, \square 1111111)$
$\rightarrow$	$(\square\square, s_2, 1111111)$

**Abbildung 6.27:** Konfigurationsübergänge für das Eingabewort  $\omega = 111111$ . Die Bandposition, auf der sich der Schreib-Lese-Kopf aktuell befindet, ist farblich hervorgehoben.

### ■ Turing-Maschine

$$S = \{s_0, s_1\}$$

$$\Sigma = \{1\}$$

$$\Pi = \{1, \square\}$$

$$E = \{s_0, s_1\}$$

### ■ Übergangstabelle

	1	$\square$
$s_0$	$(s_1, 1, \rightarrow)$	$(s_1, \square, \rightarrow)$
$s_1$	$(s_0, 1, \leftarrow)$	$(s_0, \square, \leftarrow)$

### ■ Konfigurationsübergänge

$(\square, s_0, 11111)$   
 $\rightarrow (\square 1, s_1, 11111)$   
 $\rightarrow (\square, s_0, 11111)$   
 $\rightarrow (\square 1, s_1, 11111)$   
 $\rightarrow (\square, s_0, 11111)$   
 $\rightarrow (\square 1, s_1, 11111)$   
 $\rightarrow (\square, s_0, 11111)$   
 $\rightarrow (\square 1, s_1, 11111)$   
 $\rightarrow (\square, s_0, 11111)$   
 $\rightarrow (\square 1, s_1, 11111)$   
 $\rightarrow (\square, s_0, 11111)$   
 $\rightarrow (\square 1, s_1, 11111)$   
 $\rightarrow (\square, s_0, 11111)$   
 $\dots$

**Abbildung 6.28:** Die konstruierte Turing-Maschine terminiert für keine Eingabe. Sie berechnet mit  $f(\omega) = \perp$  die an allen Stellen undefinierte Funktion. Der untere Teil der Abbildung zeigt die Konfigurationsübergänge für das Beispielwort  $\omega = 11111$ .

lesen. Der Schreib-Lese-Kopf steht in diesem Fall über dem ersten Zeichen von  $f(\omega)$ . Da in einem Konfigurationsübergang neue Blank-Symbole entstehen können, wird das Ergebnis in der Finalkonfiguration links und rechts von beliebig vielen Blank-Symbolen ( $\square^*$ ) eingerahmt.

Zwei Fällen müssen wir unsere besondere Beachtung schenken. Zum einen ist es möglich, dass die Turing-Maschine zwar terminiert, aber keinen Endzustand erreicht. Zum anderen besteht die Möglichkeit, dass die Maschine in eine Endlosschleife gerät und niemals anhält (vgl. Abbildung 6.28). In beiden Fällen betrachten wir die Berechnung als gescheitert und weisen ihr den Funktionswert  $\perp$  zu. Turing-Maschinen sind damit auf natürliche Weise in der Lage, partielle Funktionen zu berechnen.

Vergleichen wir den Berechenbarkeitsbegriff mit jenen der Abschnitte 6.1.1 bis 6.1.2, so unterscheidet er sich in einem wesentlichen Punkt: Er ist für Funktionen über der Wortmenge  $\Sigma^*$  definiert und nicht, wie bisher, über der Menge der natürlichen Zahlen. Um den Berechenbarkeitsbegriff für unsere Zwecke nutzbar zu machen, müssen wir eine geeignete Codierung finden, die Zahlenwerte auf Wörter der Menge  $\Sigma^*$  abbildet. Zwei Codierungen sind in diesem Zusammenhang von besonderer Bedeutung:

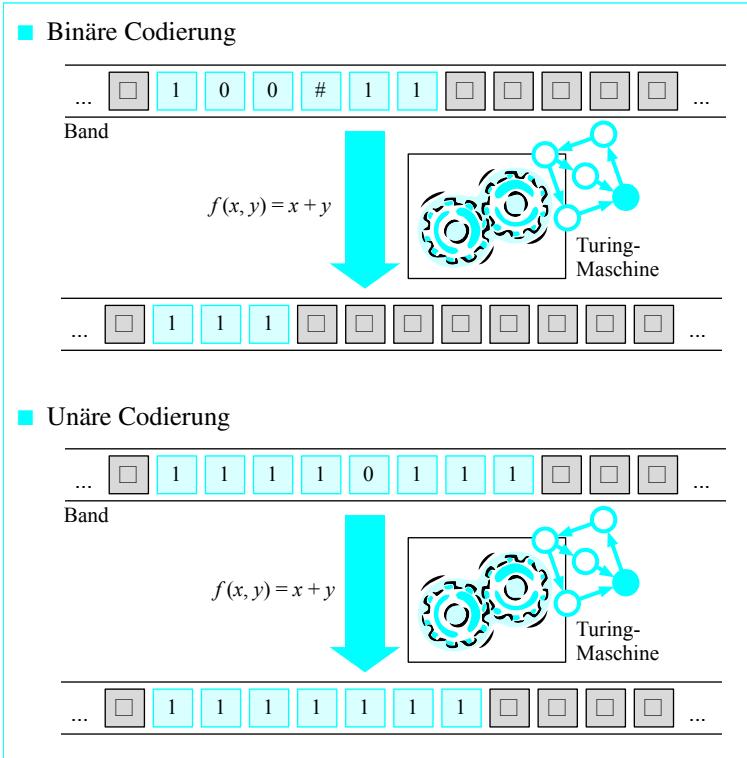
### ■ Binäre Codierung

Die Ein- und Ausgabewerte werden im Binärformat auf das Band geschrieben (vgl. Abbildung 6.29 oben). Die Codierung entspricht jener, die in aktuellen Computersystemen zum Einsatz kommt. Interessant ist sie vor allem im Zusammenhang mit Komplexitätsuntersuchungen, da sich viele Ergebnisse direkt auf reale Rechnerarchitekturen übertragen lassen.

### ■ Unäre Codierung

Die Ein- und Ausgabewerte werden durch Einserfolgen entsprechender Länge repräsentiert (vgl. Abbildung 6.29 unten). Die unäre Codierung besitzt den Vorteil, dass sich viele Algorithmen besonders einfach in eine entsprechende Turing-Maschine übersetzen lassen. Für Komplexitätsbetrachtungen ist sie nicht geeignet, da bereits das Schreiben einer Zahl  $n$  einen linear steigenden Aufwand verursacht.

Um die folgenden Betrachtungen nicht unnötig zu verkomplizieren, werden wir auf die einfachere und für unsere Zwecke völlig ausreichende unäre Codierung zurückgreifen.



**Abbildung 6.29:** Die binäre und die unäre Codierung im Vergleich. Bei der binären Codierung werden die Eingabewerte als eine Folge von Nullen und Einsen auf das Eingabeband geschrieben und liegen damit in dem gleichen Zahlenformat vor, das auch in realen Rechnersystemen zum Einsatz kommt. Da sich mit  $m$  Bits  $2^m$  verschiedene Binärmuster unterscheiden lassen, werden im Umkehrschluss  $\lceil \log_2 n \rceil$  Bandstellen benötigt, um die Zahl  $n$  binär codiert auf das Eingabeband zu schreiben. Die unäre Codierung ist die weitaus primitivere Variante; sie stellt eine Zahl  $n$  dar, indem eine Folge von  $n$  Einsen hintereinander auf das Eingabeband geschrieben wird. Die Null kann dazu verwendet werden, um zwei Codierungsmuster voneinander zu trennen. Die unäre Codierung bietet den Vorteil, dass sich viele Algorithmen besonders einfach in entsprechende Turing-Maschinen übersetzen lassen. Aus diesem Grund werden wir im Folgenden häufig auf sie zurückgreifen, auch wenn sie unbestritten die geringere Praxisbedeutung besitzt.

Auf dieser Grundlage können wir die Funktionsweise der in Abbildung 6.27 eingeführten Turing-Maschine auch numerisch interpretieren: Sie berechnet die Nachfolgerfunktion  $f(x) = \text{succ}(x)$ . Weiter oben haben wir bereits angedeutet, wie die Maschine arbeitet. Über der ersten Eins startend bewegt die Maschine den Schreib-Lese-Kopf so weit nach rechts, bis das erste Blank-Symbol erscheint. Dieses wird durch eine Eins ersetzt und der unär codierte Eingabewert hierdurch um eins erhöht. Anschließend spult die Maschine das Band zurück, indem sie den Schreib-Lese-Kopf in die Ausgangsposition zurückbewegt.

Abbildung 6.30 zeigt die Konstruktion einer Turing-Maschine zur Berechnung der Vorgängerfunktion  $f(x) = \text{pred}(x)$ . Genau wie die erste Maschine bewegt sie den Schreib-Lese-Kopf an das Ende der Eingabesequenz. Sobald ein Blank-Symbol erscheint, erfolgt eine Linksbewegung und die vorgefundene Eins wird mit einem Blank-Symbol überschrieben. Jetzt steht der gesuchte Wert  $x - 1$  auf dem Band und die Maschine bewegt den Schreib-Lese-Kopf auf seine ursprüngliche Position zurück.

### ■ Turing-Maschine

$$\begin{aligned} S &= \{s_0, s_1, s_2, s_3\} \\ \Sigma &= \{1\} \\ \Pi &= \{1, \square\} \\ E &= \{s_3\} \end{aligned}$$

### ■ Übergangstabelle

	1	$\square$
$s_0$	$(s_0, 1, \rightarrow)$	$(s_1, \square, \leftarrow)$
$s_1$	$(s_2, \square, \leftarrow)$	$(s_3, \square, \rightarrow)$
$s_2$	$(s_2, 1, \leftarrow)$	$(s_3, \square, \rightarrow)$
$s_3$	—	—

### ■ Konfigurationsübergänge

	$(\square, s_0,$	$111111)$
$\rightarrow$	$(\square 1, s_0,$	$11111)$
$\rightarrow$	$(\square 11, s_0,$	$1111)$
$\rightarrow$	$(\square 111, s_0,$	$111)$
$\rightarrow$	$(\square 1111, s_0,$	$11)$
$\rightarrow$	$(\square 11111, s_0,$	$1)$
$\rightarrow$	$(\square 111111, s_0,$	$\square)$
$\rightarrow$	$(\square 11111, s_1,$	$1\square)$
$\rightarrow$	$(\square 1111, s_2,$	$1\square\square)$
$\rightarrow$	$(\square 111, s_2,$	$1\square\square\square)$
$\rightarrow$	$(\square 11, s_2,$	$11\square\square\square)$
$\rightarrow$	$(\square 1, s_2,$	$111\square\square\square)$
$\rightarrow$	$(\square, s_2,$	$1111\square\square\square)$
$\rightarrow$	$(\square, s_2,$	$11111\square\square\square)$
$\rightarrow$	$(\square\square, s_3,$	$11111\square\square)$

**Abbildung 6.30:** Die dargestellte Turing-Maschine berechnet die Funktion  $f(x) = \text{pred}(x)$ .

Komplexere Operationen lassen sich nach demselben Schema realisieren. Als Beispiel zeigt Abbildung 6.31 eine Turing-Maschine zur Addition zweier Zahlen  $x$  und  $y$ . Zu Beginn werden beide Operanden unär codiert und zusammen mit einer separierenden Null auf das Band geschrieben. Um die Zahlen zu addieren, geht die Maschine in drei Schritten vor: Zunächst wird temporär der Wert  $x + y + 1$  erzeugt, indem ausgehend von der Startposition die trennende Null gesucht und durch eine Eins ersetzt wird. Anschließend wird der Schreib-Lese-Kopf, genau wie im Falle der Berechnung von  $\text{pred}(x)$ , an das Ende bewegt und die letzte Eins gelöscht. Jetzt steht das gesuchte Ergebnis  $x + y$  auf dem Band und die Maschine muss nur noch zurückgespult werden.

In Abbildung 6.32 wird eine weitere Turing-Maschine definiert, die in den nachfolgenden Betrachtungen noch eine wichtige Rolle spielen wird. Die Rede ist von der Move-Maschine, die das komplette Eingabewort um eine Stelle nach rechts verschiebt. Hierzu wird in jedem Schritt das aktuelle Bandzeichen eingelesen, mit dem Vorgängersymbol überschrieben und der Schreib-Lese-Kopf anschließend eine Stelle nach rechts bewegt. Der Vorgang wird so lange wiederholt, bis das Blank-Symbol eingelesen wird. In diesem Fall ist das gesamte Wort verschoben und die Maschine terminiert nach dem Rückspulen des Bands im Endzustand  $s_e$ . Beachten Sie, dass die Zustandsmenge der Move-Maschine maßgeblich durch die Anzahl der Elemente des Bandalphabets  $\Pi$  bestimmt wird. Damit sich die Maschine an das gelesene Vorgängersymbol „erinnern“ kann, müssen wir für jedes Element des Bandalphabets einen dedizierten Zustand definieren.

Die Move-Maschine macht sich eine häufig verwendete Erweiterung des Basismodells zu Nutze, die wir nicht unbeachtet übergehen wollen. Der Übergang  $\delta(s_0, \square) = (s_2, \square, \circlearrowright)$  drückt aus, dass der Schreib-Lese-Kopf an seiner aktuellen Position verharren soll. Ein solches Verhalten ist im Basismodell nicht vorgesehen; hier wird der Kopf in jedem Schritt entweder nach links, oder nach rechts bewegt. Trotzdem handelt es sich um keine Erweiterung im eigentlichen Sinne, da wir das Verhalten sehr einfach im Basismodell simulieren können. Anstatt direkt in den Zustand  $s_2$  überzugehen, lassen wir die Maschine zunächst in einen Zwischenzustand  $s'$  wechseln. Hierbei bewegen wir den Kopf nach links, ohne den Bandinhalt zu verändern. Anschließend erfolgt der Übergang nach  $s_2$ , gekoppelt mit einer Rechtsbewegung. Über einen solchen ZwischenSchritt lässt sich simulieren, dass sich der Schreib-Lese-Kopf während eines Zustandsübergangs scheinbar nicht bewegt. Damit können wir das neu hinzugekommene Symbol  $\circlearrowright$  bedenkenlos verwenden; es handelt sich lediglich um eine Schreiberleichterung und erfordert keine Anpassung des zugrunde liegenden Berechnungsmodells.

Im Folgenden wollen wir mehrere Erweiterungen der ursprünglichen Turing-Maschine diskutieren, mit denen sich viele Berechnungen deutlich bequemer durchführen lassen. Dabei werden wir die erstaunliche Beobachtung machen, dass keine zu einer echten Steigerung der Ausdrucksfähigkeit führen wird. Sämtliche Erweiterungen lassen sich im Basismodell simulieren.

### 6.1.5.2 Einseitig und linear beschränkte Turing-Maschinen

*Einseitig beschränkte Turing-Maschinen* verwenden ein Band, das sich nur in eine Richtung unendlich weit ausbreitet. Ohne Beschränkung der Allgemeinheit wollen wir von einem nach links beschränkten Band ausgehen und die Felder mit den natürlichen Zahlen nummerieren. Der Bandanfang besitzt den Index 1 und speichert das erste Zeichen der Eingabesequenz. Der Schreib-Lese-Kopf einer einseitig beschränkten Turing-Maschine kann sich nicht über das Bandende hinausbewegen. Eine angeforderte Linksbewegung wird ignoriert und der Schreib-Lese-Kopf verharrt in seiner Position.

Einseitig beschränkte Turing-Maschinen lassen sich durch das Basismodell simulieren, indem das Bandende durch ein dediziertes Symbol  $\diamond$  markiert und die Übergangsfunktion für jeden Zustand  $s \in S$  um die Regel

$$\delta(s, \diamond) = (s, \diamond, \rightarrow) \quad (6.42)$$

ergänzt wird. Hierdurch wird der Schreib-Lese-Kopf auf die Startposition zurückbewegt, sobald der Bandanfang verlassen wird.

Die Umkehrung gilt ebenfalls, d. h., wir können jede Turing-Maschine durch eine einseitig beschränkte Turing-Maschine simulieren. Wir beginnen, indem wir den Bandanfang erneut mit dem dedizierten Symbol  $\diamond$  markieren. Anschließend bewegen wir den Schreib-Lese-Kopf nach rechts auf das erste Zeichen der Eingabe und starten die Maschine. Solange sich der Kopf rechts des ersten Eingabezeichens befindet, verläuft die Berechnung wie gehabt. Bewegt die Maschine den Schreib-Lese-Kopf jedoch über die linke Grenze hinaus, treffen wir also auf das vorher eingefügte Symbol  $\diamond$ , so müssen wir ein wenig Sonderarbeit leisten. Wir schaffen zunächst Platz für ein neues Zeichen, indem wir den gesamten Bandinhalt, analog zur Arbeitsweise der Move-Maschine aus Abbildung 6.32, um eine Stelle nach rechts verschieben. Anschließend führen wir die Berechnung in gewohnter Weise fort. Damit erweist sich die einseitige Beschränkung des Bandes als harmloser, als es der erste Blick vermuten lässt. Sie führt zu einem Automatenmodell, dessen Berechnungsstärke mit jener des Basismodells übereinstimmt.

#### Turing-Maschine

$$\begin{aligned} S &= \{s_0, s_1, s_2, s_3, s_4\} \\ \Sigma &= \{1, 0\} \\ \Pi &= \{1, 0, \square\} \\ E &= \{s_4\} \end{aligned}$$

#### Übergangstabelle

	1	0	$\square$
$s_0$	$(s_0, 1, \rightarrow)$	$(s_1, 1, \rightarrow)$	—
$s_1$	$(s_1, 1, \rightarrow)$	—	$(s_2, \square, \leftarrow)$
$s_2$	$(s_3, \square, \leftarrow)$	—	$(s_4, \square, \rightarrow)$
$s_3$	$(s_3, 1, \leftarrow)$	—	$(s_4, \square, \rightarrow)$
$s_4$	—	—	—

**Abbildung 6.31:** Die Add-Maschine berechnet die Summe zweier unär codierter Operanden  $x$  und  $y$ .

#### Turing-Maschine

$$\begin{aligned} S &= \{s_\sigma \mid \sigma \in \Sigma\} \cup \{s_0, s_1, s_2\} \\ \Pi &= \Sigma \cup \{\square\} \\ E &= \{s_2\} \end{aligned}$$

#### Übergangstabelle

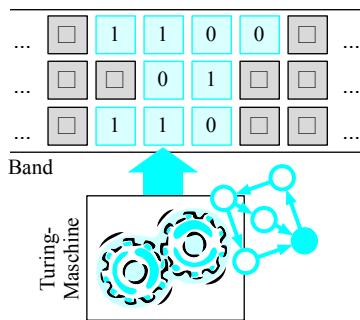
	$\sigma'$	$\square$
$s_0$	$(s_{\sigma'}, \square, \rightarrow)$	$(s_2, \square, \circlearrowleft)$
$s_\sigma$	$(s_{\sigma'}, \sigma, \rightarrow)$	$(s_1, \sigma, \leftarrow)$
$s_1$	$(s_1, \sigma', \leftarrow)$	$(s_2, \square, \rightarrow)$
$s_2$	—	—

**Abbildung 6.32:** Die Move-Maschine verschiebt den Bandinhalt um eine Stelle nach rechts.

■ Mehrspur-Turing-Maschine

$$\Sigma = \{1, 0\}$$

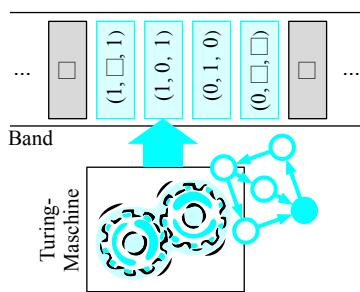
$$\Pi = \{1, 0, \square\}$$



■ Simulation im Basismodell

$$\Sigma = \{1, 0\}^3$$

$$\Pi = \{1, 0, \square\}^3$$



**Abbildung 6.33:** Eine Mehrspur-Turing-Maschine lässt sich durch die Erweiterung des Eingabe- und des Bandalphabets im Basismodell simulieren.

Anders stellt sich die Situation für *linear beschränkte Turing-Maschinen* dar. Einer solchen Maschine stehen für die Berechnung nur diejenigen Felder zur Verfügung, die zur Codierung der Eingabesequenz benötigt wurden. Mit anderen Worten: Es ist nicht erlaubt, den Schreib-Lese-Kopf nach links oder rechts über die Eingabesequenz hinauszubewegen. Dass diese Einschränkung die Berechnungsstärke massiv beeinflusst, liegt auf der Hand. So ist es unmöglich, eine Ausgabe zu produzieren, die länger ist als die Eingabe selbst. In Abschnitt 6.3 werden wir dieses Automatenmodell erneut aufgreifen und zeigen, dass es trotz seiner offensichtlichen Limitierungen dennoch eine große Rolle in der theoretischen Informatik spielt.

### 6.1.5.3 Mehrspur-Turing-Maschinen

Eine *k-Spur-Turing-Maschine* besteht aus einem Band, das in  $k$  separate Spuren unterteilt ist. Die einzelnen Spuren werden von fest aneinandergekoppelten Schreib-Lese-Köpfen angesprochen (vgl. Abbildung 6.33 oben). Ähnlich dem Prinzip, das konventionellen Festplattenlaufwerken zugrunde liegt, können sich die Köpfe alle gleichzeitig nach links oder rechts, jedoch nicht unabhängig voneinander bewegen.

Bei genauerer Betrachtung entpuppt sich das Konzept der Mehrspur-Turing-Maschine als eine eher marginale Erweiterung des Basismodells. Eine *k*-Spur-Turing-Maschine mit dem Eingabealphabet  $\Sigma$  und dem Bandalphabet  $\Pi$  lässt sich mit einer konventionellen Turing-Maschine simulieren, indem die Zeichen der  $k$  Spuren in ein Einzelzeichen hineincodiert werden. Um dies zu erreichen, ersetzen wir  $\Sigma$  ganz einfach durch  $\Sigma^k$  und  $\Pi$  durch  $\Pi^k$ . Abbildung 6.33 (unten) demonstriert die Transformation auf grafische Weise.

### 6.1.5.4 Mehrband-Turing-Maschinen

Eine in vielerlei Hinsicht wertvolle Weiterentwicklung ist die *Mehrband-Turing-Maschine*. Im Gegensatz zur Mehrspur-Turing-Maschine gestattet sie, dass alle Schreib-Lese-Köpfe unabhängig voneinander bewegt werden dürfen. Um das Verhalten einer solchen Maschine vollständig zu erfassen, müssen wir die Übergangsfunktion  $\delta$  geringfügig anpassen. Für eine  $k$ -Band-Maschine besitzt sie die folgende Form:

$$\delta(s, \sigma_1, \dots, \sigma_k) = (s', \sigma'_1, \dots, \sigma'_k, r_1, \dots, r_k) \quad (6.43)$$

Die Funktionsdefinition ist wie folgt zu lesen: Befindet sich die Turing-Maschine im Zustand  $s$  und steht der  $i$ -te Schreib-Lese-Kopf über dem Symbol  $\sigma_i$ , so geht die Maschine in den Zustand  $s'$  über und ersetzt das Zeichen  $\sigma_i$  auf dem  $i$ -ten Band durch das Zeichen  $\sigma'_i$ . Zusätzlich werden die Schreib-Lese-Köpfe entsprechend den Richtungsangaben  $r_i$  bewegt. Ist  $r_i = ' \leftarrow '$ , so fährt der  $i$ -te Kopf eine Stelle nach links. Im Fall  $r_i = ' \rightarrow '$  findet eine Rechtsbewegung statt.

Obwohl die Mehrband-Turing-Maschine weit mächtiger erscheint als die ursprüngliche Einband-Maschine, lässt sie sich ebenfalls auf das Basismodell zurückführen (vgl. Abbildung 6.34). Die Grundidee besteht darin, die  $k$ -Band-Turing-Maschine auf eine Mehrspur-Turing-Maschine zu reduzieren und die unterschiedlichen Positionen der Schreib-Lese-Köpfe in symbolischer Form auf dem Band zu speichern. Hierzu verwenden wir eine Mehrspur-Turing-Maschine mit  $2k$  Spuren. Jedem Band der zu simulierenden  $k$ -Band-Turing-Maschine ordnen wir 2 separate Spuren zu. Während die *Datenspur* eine symbolweise Bandkopie enthält, verwendet die *Positionsspur* ausschließlich die Zeichen  $\square$  und  $\uparrow$ . Das Symbol  $\uparrow$  markiert die Position, an der sich der simulierte Schreib-Lese-Kopf aktuell befindet.

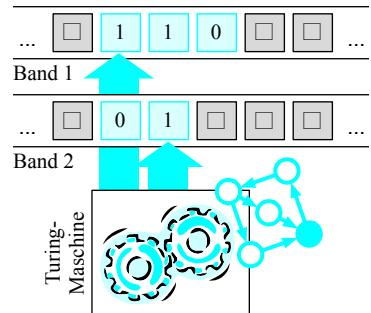
Um den Zustandsübergang einer  $k$ -Band-Maschine nachzuempfinden, muss die Mehrspurmaschine zunächst die Positionen der simulierten Schreib-Lese-Köpfe bestimmen. Hierzu wird das Band zurückgespult, bis auf allen Spuren ein Blank-Symbol erscheint. Danach wird der Kopf sukzessive nach rechts bewegt. Sobald eine Pfeilmarkierung auf einer der Positionsspuren erscheint, merkt sich die Maschine das auf der Datenspur vorgefundene Zeichen durch den Übergang in einen speziell hierfür vorgesehenen Zustand. Da wir die Symbolinformation hierdurch vollständig in die Zustandsmenge hineincodieren, wächst diese selbst für kleine Mehrband-Turing-Maschinen enorm an. Nichtsdestotrotz bleibt die Anzahl der Zustände in jedem Fall endlich.

Nachdem die letzte Pfeilmarkierung gefunden wurde, steht eindeutig fest, in welche Folgekonfiguration die Maschine übergeht. Die für jedes Band auszuführenden Aktionen werden jetzt nacheinander simuliert. Hierzu wird auf der aktuell bearbeiteten Positionsspur erneut die Pfeilmarkierung gesucht und das zugehörige Zeichen auf der Datenspur ersetzt. Danach wird eine Kopfbewegung nach links oder rechts simuliert, indem die Pfeilmarkierung auf der Positionsspur in die jeweilige Richtung verschoben wird.

#### ■ Mehrband-Turing-Maschine

$$\Sigma = \{1, 0\}$$

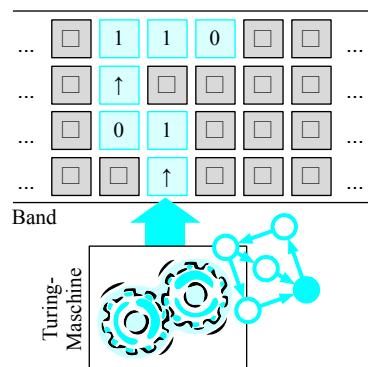
$$\Pi = \{1, 0, \square\}$$



#### ■ Simulation im Mehrspurmodell

$$\Sigma = \{1, 0, \uparrow\}$$

$$\Pi = \{1, 0, \uparrow, \square\}$$



**Abbildung 6.34:** Eine Mehrband-Turing-Maschine mit  $k$  unabhängigen Bändern lässt sich auf eine Mehrspur-Turing-Maschine mit  $2k$  Bändern abbilden. Jedes Band wird durch zwei Spuren repräsentiert. Die Datenspur ist eine Kopie des Bandinhalts. Auf der Positionsspur ist die Lage des simulierten Schreib-Lese-Kopfes verzeichnet.

■ Replace-Maschine

$$S = \{s_0, s_1\}$$

$$\Sigma = \{1, 0\}$$

$$\Pi = \{1, 0, \square\}$$

$$E = \{s_1\}$$

	1	0	$\square$
$s_0$	$(s_0, 1, \rightarrow)$	$(s_1, 1, \rightarrow)$	—
$s_1$	—	—	—

■ Erase-Maschine

$$S = \{s_2, s_3, s_4\}$$

$$\Sigma = \{1, 0\}$$

$$\Pi = \{1, 0, \square\}$$

$$E = \{s_4\}$$

	1	0	$\square$
$s_2$	$(s_2, 1, \rightarrow)$	—	$(s_3, \square, \leftarrow)$
$s_3$	$(s_4, \square, \leftarrow)$	—	—
$s_4$	—	—	—

■ Rewind-Maschine

$$S = \{s_5, s_6\}$$

$$\Sigma = \{1, 0\}$$

$$\Pi = \{1, 0, \square\}$$

$$E = \{s_6\}$$

	1	0	$\square$
$s_5$	$(s_5, 1, \leftarrow)$	—	$(s_6, \square, \rightarrow)$
$s_6$	—	—	—

**Abbildung 6.35:** Die Funktionsweise der Add-Maschine aus Abbildung 6.31 setzt sich aus drei Arbeitsschritten zusammen. Jeder Einzelschritt lässt sich mit Hilfe einer separaten Turing-Maschine beschreiben.

### 6.1.5.5 Maschinenkomposition

Betrachten wir die bisher konstruierten Turing-Maschinen genauer, so zeigen diese auf der obersten Ebene fast alle eine sequenzielle Struktur. Am Beispiel der in Abbildung 6.31 eingeführten Maschine zur Addition zweier Zahlen  $x$  und  $y$  wird die Struktur besonders deutlich; die Berechnung der Summe erfolgt hier in drei nacheinander ausgeführten Schritten. Im ersten Schritt wird die trennende Null durch eine Eins ersetzt und damit das Zwischenergebnis  $x + y + 1$  hergestellt. Im zweiten Schritt wird die letzte Eins gelöscht und die Maschine im dritten Schritt zurückgespult. Insgesamt entpuppt sich die Additions-Maschine als die Komposition

- der Maschine Replace zum Ersetzen der Null,
- der Maschine Erase zum Löschen der letzten Eins und
- der Maschine Rewind zum Zurückspulen des Bands.

Alle drei Einzelmaschinen sind in Abbildung 6.35 zusammengefasst.

Im Umkehrschluss gibt uns diese Beobachtung eine einfache Möglichkeit an die Hand, um komplexe Funktionen durch die Komposition mehrerer einfach aufgebauter Maschinen zu realisieren. Zu diesem Zweck seien  $n$  beliebige Turing-Maschinen gegeben:

$$T_1 = (S_1, \Sigma_1, \Pi_1, \delta_1, s_{10}, \square, \{e_{10}, \dots, e_{1m_1}\}) \quad (6.44)$$

$$T_2 = (S_2, \Sigma_2, \Pi_2, \delta_2, s_{20}, \square, \{e_{20}, \dots, e_{2m_2}\}) \quad (6.45)$$

...

$$T_n = (S_n, \Sigma_n, \Pi_n, \delta_n, s_{n0}, \square, \{e_{n0}, \dots, e_{nm_n}\}) \quad (6.46)$$

Um die Betrachtungen einfach zu halten, treffen wir die folgenden Vereinbarungen:

- Ohne Beschränkung der Allgemeinheit wollen wir annehmen, dass die Zustandsmengen  $S_1, \dots, S_n$  paarweise disjunkt sind. Zustandsmengen, die keine gemeinsamen Elemente enthalten, lassen sich herstellen, indem die Maschinenzustände vor der Komposition entsprechend umbenannt werden.
- Nur solche Zustände sind als Endzustände zugelassen, die keine weiteren Übergänge mehr erlauben. Auch diese Forderung lässt sich durch eine geringfügige Modifikation der Zustandsmenge und der Übergangsfunktion erfüllen.

Unter den beschriebenen Voraussetzungen lassen sich  $T_1, \dots, T_n$  zu einer Kompositionsmaschine vereinigen, indem wir sie an  $k$  Nahtstellen

$$(e_1, s_1), (e_2, s_2), \dots, (e_k, s_k) \quad (6.47)$$

miteinander verbinden. Hierin bezeichnet  $e_i$  einen Endzustand einer Turing-Maschine und  $s_i$  den Startzustand einer anderen. Den Übergang von  $s_i$  nach  $e_i$  gestalten wir so, dass der Schreib-Lese-Kopf an der aktuellen Position verharrt und der Bandinhalt nicht verändert wird. Hierzu fügen wir für jede Nahtstelle die folgende Regel hinzu:

$$\delta(e_i, \sigma) = (s_i, \sigma, \circlearrowright) \quad (6.48)$$

Insgesamt hat die Kompositionsmaschine damit die Form

$$T' = (S', \Sigma', \Pi', \delta', s', \square, E') \quad (6.49)$$

mit

$$S' := S_1 \cup \dots \cup S_n \quad (6.50)$$

$$\Sigma' := \Sigma_1 \cup \dots \cup \Sigma_n \quad (6.51)$$

$$\Pi' := \Pi_1 \cup \dots \cup \Pi_n \quad (6.52)$$

$$\delta' := \delta_1 \cup \dots \cup \delta_n \cup \{(e_i, \sigma) \mapsto (s_i, \sigma, \circlearrowright) \mid 1 \leq i \leq k\} \quad (6.53)$$

$$s' := s_{10} \quad (6.54)$$

$$E' := E_1 \cup \dots \cup E_n \quad (6.55)$$

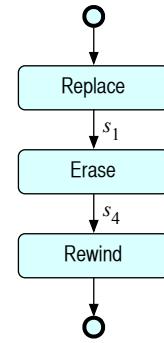
Die Festlegung der Endzustände ist nicht die einzige mögliche. Alternative Definitionen nehmen diejenigen Zustände aus der Menge  $E'$  heraus, die eine Nahtstelle zu einer anderen Maschine besitzen. In diesem Fall würde das Ergebnis der Berechnung  $\perp$  lauten, falls die Turing-Maschine an einer Nahtstelle  $(e_i, s_i)$  stehen bleibt.

Mit Hilfe von Graphen lässt sich die Komposition von Turing-Maschinen sehr übersichtlich veranschaulichen. In dieser Darstellung wird jede Nahtstelle, die eine Turing-Maschine  $T_1$  mit einer Turing-Maschine  $T_2$  verbindet, durch einen Pfeil dargestellt, dessen Kante mit dem Endzustand von  $T_1$  beschriftet ist. Auf die Angabe des Startzustands von  $T_2$  kann verzichtet werden, da dieser eindeutig bestimmt ist. Abbildung 6.36 demonstriert das Gesagte am Beispiel der Additionsmaschine.

### 6.1.5.6 Universelle Turing-Maschinen

In den vorangegangenen Abschnitten haben wir untersucht, wie sich grundlegende arithmetische Operationen mit Hilfe von Turing-Maschinen berechnen lassen. In diesem Abschnitt werden wir herausarbeiten, dass Turing-Maschinen sogar in der Lage sind, sich selbst zu

#### Kompositionsmaschine

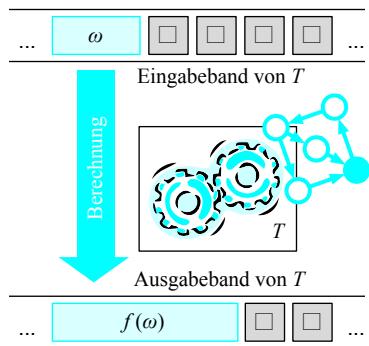


#### Übergangstabelle

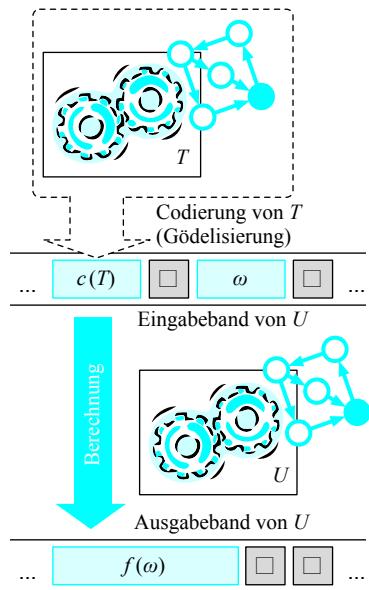
	1	0	$\square$
$s_0$	$(s_0, 1, \rightarrow)$	$(s_1, 1, \rightarrow)$	—
$s_1$	$(s_2, 1, \circlearrowright)$	$(s_2, 0, \circlearrowright)$	$(s_2, \square, \circlearrowright)$
$s_2$	$(s_2, 1, \rightarrow)$	—	$(s_3, \square, \leftarrow)$
$s_3$	$(s_4, \square, \leftarrow)$	—	—
$s_4$	$(s_5, 1, \circlearrowright)$	$(s_5, 0, \circlearrowright)$	$(s_5, \square, \circlearrowright)$
$s_5$	$(s_5, 1, \leftarrow)$	—	$(s_6, \square, \rightarrow)$
$s_6$	—	—	—

**Abbildung 6.36:** Mit dem Mittel der Komposition lassen sich Turing-Maschinen zu komplexeren Maschinen zusammenschalten.

■ Turing-Maschine  $T$



■ Universelle Turing-Maschine  $U$



**Abbildung 6.37:** Prinzip der universellen Turing-Maschine. Neben dem Eingabewort  $\omega$  wird die Gödelnummer einer anderen Turing-Maschine  $T$  auf das Eingabeband geschrieben. Die universelle Turing-Maschine  $U$  simuliert das Verhalten von  $T$  und produziert dieselbe Ausgabe, die  $T$  für das Eingabewort  $\omega$  produzieren würde.

simulieren. Eine Turing-Maschine  $U$ , die eine beliebige andere Maschine  $T$  simulieren kann, heißt *universell*. Abbildung 6.37 veranschaulicht die grundsätzliche Arbeitsweise einer solchen Maschine:

- Als Eingabe nimmt  $U$  die Beschreibung einer anderen Turing-Maschine  $T$  in codierter Form sowie ein Eingabewort  $\omega$  entgegen.
- Als Ausgabe schreibt  $U$  dieselbe Sequenz auf das Band, die auch die Originalmaschine  $T$  für die Eingabe  $\omega$  produzieren würde.

Im Gegensatz zu allen anderen vorgestellten Maschinen ist die Funktion der universellen Turing-Maschine nicht auf eine Spezialaufgabe beschränkt. In ihrer Funktionsweise ist sie dem modernen Computer sehr ähnlich; sie agiert als Interpreter, der das Verhalten von  $T$  Schritt für Schritt auf dem Eingabewort simuliert. Die codierte Form von  $T$  entspricht dem Programm, das die universelle Maschine in die Lage versetzt, beliebige Berechnungen durchzuführen.

So weit die Theorie. Aber wie können wir eine Turing-Maschine dazu bewegen, eine andere Maschine zu simulieren? Wir wollen uns der Antwort schrittweise nähern und zunächst ein Verfahren ersinnen, mit dessen Hilfe eine Turing-Maschine codiert werden kann. Die Codierung ist notwendig, um die Turing-Maschine  $T$  zusammen mit dem Eingabewort  $\omega$  auf dem Band der universellen Maschine zu speichern.

Für unsere Betrachtungen gehen wir von einer Maschine der Form

$$T = (\{s_1, s_2, \dots, s_n\}, \{0, 1\}, \{0, 1, \square\}, \delta, s_1, \square, \{s_2\}) \quad (6.56)$$

aus. Neben den Symbolen 0, 1 und  $\square$  sind keine weiteren Zeichen auf dem Band zugelassen.  $s_1$  bezeichnet den Startzustand und  $s_2$  den (einzigsten) Endzustand. Die Beschränkung besitzt den Vorteil, dass das Eingabe- und das Bandalphabet sowie der Start- und Endzustand eindeutig festgelegt sind und sich zwei Turing-Maschinen nur noch in der Übergangsfunktion  $\delta$  unterscheiden können. Hierdurch ist es ausreichend, eine Codierung der Übergangsfunktion  $\delta$  auf das Band zu schreiben, um eine Turing-Maschine eindeutig zu charakterisieren.

Abbildung 6.38 zeigt eine mögliche Codierung der weiter oben eingeführten Erase-Maschine. Die Umsetzung in eine Binärzahl erfolgt in zwei Schritten. Zunächst wird für jeden Eintrag der Übergangstabelle eine Binärzahl erzeugt, indem die fünf Komponenten (Startzustand, Eingabesymbol, Folgesymbol, Ausgabesymbol und Richtung) in Form von Einserketten unär codiert und mit der Null als Trennzeichen zusammengefügt werden. Anschließend werden die erstellten Bitsequenzen

nach dem gleichen Schema zu einer großen Binärzahl verschmolzen. Die erzeugte Zahl heißt die *Gödelnummer* der Turing-Maschine  $T$  und die Codierung wird als *Gödelisierung* bezeichnet.

Beachten Sie, dass es eine Vielzahl von Möglichkeiten gibt, um Turing-Maschinen zu codieren, und die hier gewählte nur eine unter vielen ist. Wir wollen deshalb klären, welche Minimalanforderungen eine Codierung erfüllen muss, damit sie für die Gödelisierung einer Turing-Maschine eingesetzt werden kann.

- Offensichtlich muss die Gödelisierung gewährleisten, dass die Übergangstabelle durch die erzeugte Gödelnummer eindeutig festgelegt ist. Diese Eigenschaft ist genau dann erfüllt, wenn die Menge der Turing-Maschinen *injektiv* in die Menge der natürlichen Zahlen abgebildet wird. In der hier gewählten Codierung ist die Injektivität gewährleistet, da wir die unär codierten Symbole eindeutig durch die Null als Trennzeichen voneinander unterscheiden können.
- Die Gödelisierung stellt im Allgemeinen keine Eins-zu-eins-Beziehung zwischen der Menge der Turing-Maschinen und der Menge der Binärzahlen her. Es können also immer Binärzahlen existieren, die keiner Turing-Maschine entsprechen. Wir wollen nur solche Codierungen zulassen, für die wir entscheiden können, ob eine gültige oder eine ungültige Gödelnummer vorliegt.
- Die Injektivität einer Gödelisierung gewährleistet, dass die Übergangstabelle einer Turing-Maschine eindeutig durch ihre Gödelnummer bestimmt ist. Damit wir die Codierung für unsere Zwecke einsetzen können, müssen wir zusätzlich fordern, dass sie *berechenbar* ist. Das heißt, dass eine Turing-Maschine existieren muss, die aus einer beliebigen Übergangstabelle eine Gödelnummer berechnet und aus einer beliebigen Gödelnummer die Übergangstabelle extrahiert.

Verallgemeinert lesen sich die aufgestellten Eigenschaften wie folgt:



### Definition 6.13 (Gödelisierung)

Die Funktion  $c : M \rightarrow \mathbb{N}$  heißt *Gödelisierung*, wenn sie die folgenden Eigenschaften erfüllt:

- $c$  ist injektiv
- Die Bildmenge  $c(M)$  ist entscheidbar
- $c : M \rightarrow \mathbb{N}$  und  $c^{-1} : c(M) \rightarrow M$  sind berechenbar

#### Erase-Maschine

	1	0	$\square$
$s_1$	$(s_3, 1, \rightarrow)$	—	$(s_2, \square, \leftarrow)$
$s_3$	$(s_2, \square, \leftarrow)$	—	—
$s_2$	—	—	—



$$\delta(s_1, 1) = (s_3, 1, \rightarrow)$$

$$\delta(s_1, \square) = (s_2, \square, \leftarrow)$$

$$\delta(s_3, 1) = (s_2, \square, \leftarrow)$$

#### Codierung

Symbol	Code	Symbol	Code
$s_1$	1	$\leftarrow$	1
$s_2$	11	$\rightarrow$	11
$s_3$	111	(	0
0	1	,	0
1	11	)	0
$\square$	111	=	0

$$\delta(s_1, 1) = (s_3, 1, \rightarrow)$$



010110001110110110110

$$\delta(s_1, \square) = (s_2, \square, \leftarrow)$$



010111000110111010

$$\delta(s_3, 1) = (s_2, \square, \leftarrow)$$

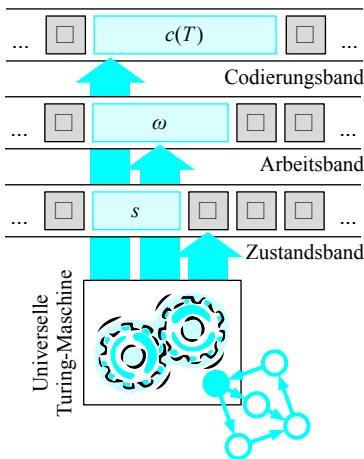


0111011000110111010

#### Gödelnummer

0101100011101101100101110...  
...001101110100111011000110111010

**Abbildung 6.38:** Gödelisierung der Erase-Maschine



**Abbildung 6.39:** 3-Band-Implementierung der universellen Turing-Maschine. Das *Codierungsband* speichert die Gödelnummer  $c(T)$  der zu simulierenden Maschine. Auf dem *Arbeitsband* wird die Arbeitsweise von  $T$  nachvollzogen und auf dem *Zustandsband* der simulierte Zustand von  $T$  abgelegt.

Die Implementierung einer universellen Turing-Maschine kann ebenfalls auf unterschiedliche Weise erfolgen. Eine einfache Möglichkeit besteht in der Verwendung einer 3-Band-Maschine (vgl. Abbildung 6.39). Auf dem ersten Band – dem *Codierungsband* – nimmt sie die Gödelnummer der zu simulierenden Turing-Maschine sowie das Eingabewort  $\omega$  entgegen. Im ersten Schritt wird  $\omega$  auf das zweite Band – das *Arbeitsband* – verschoben. Die Gödelnummer von  $T$  verbleibt auf dem Codierungsband und dient während der gesamten Berechnung als Merkhilfe für die auszuführenden Aktionen. Das dritte Band ist das *Zustandsband*. In codierter Form speichert es zu jedem Zeitpunkt den Zustand, in dem sich die simulierte Turing-Maschine  $T$  während der Abarbeitung von  $\omega$  befinden würde. Da die Maschine, wie oben vereinbart, im Zustand  $s_1$  startet, wird der Inhalt des Zustandsbands vorab mit der Sequenz  $\dots \square 1 \square \dots$  initialisiert.

Ein Berechnungsschritt von  $T$  wird durch die folgenden Aktionen simuliert: Zunächst liest die Maschine die Unärcodierung des aktuellen Zustands von Band 3 und das nächste zu verarbeitende Zeichen von Band 2. Anschließend wird auf Band 1 nach dem auszuführenden Übergang gesucht. Befindet sich die simulierte Maschine beispielsweise im Zustand  $s_3$  (111) und wird das Eingabezeichen 1 (11) eingelesen, so wird nach dem Bitmuster 111011000 gesucht. Die Gödelnummer von  $T$  ist so konstruiert, dass diese Bitsequenz niemals mehrfach auftreten kann. Wurde das Bitmuster gefunden, so liest die Maschine die nachfolgenden Bits der Form  $1^i 0 1^j 0 1^k$  ein. Die Sequenzen  $1^i$ ,  $1^j$  und  $1^k$  entsprechen der unären Codierung des Folgezustands, des zu schreibenden Zeichens sowie der auszuführenden Kopfbewegung. Die Information wird durch die universelle Turing-Maschine ausgewertet und in entsprechende Aktionen umgesetzt. Das Folgezeichen wird auf das Arbeitsband geschrieben und die Kopfbewegung ausgeführt. Der neu einzunehmende Zustand wird auf das Zustandsband geschrieben.

Die universelle Turing-Maschine bricht die skizzierte Bearbeitungssequenz ab, sobald kein passendes Bitmuster auf Band 1 gefunden wurde. In diesem Fall ist für den aktuellen Zustand und das gefundene Eingabezeichen kein Übergang definiert und die simulierte Maschine würde die Bearbeitung stoppen. Jetzt entscheidet der Inhalt auf Band 3 über den Ausgang der Berechnung. Befindet sich die simulierte Maschine in einem Endzustand, so kopiert die universelle Maschine den Inhalt des zweiten auf das erste Band und geht ihrerseits in einen Endzustand über. Befindet sich auf Band 3 eine abweichende Sequenz, so stoppt die universelle Maschine, ohne in einen Endzustand überzugehen.

Die vergleichsweise grobe Beschreibung des Arbeitsprinzips soll uns an dieser Stelle genügen. Würden wir das genaue Verhalten der univer-

sellten Turing-Maschine auf der Zustandsebene vollständig auscodieren, so würde die Übergangstabelle den Umfang dieses Buchs sprengen.

Auf den ersten Blick mag die Universalität als eine Eigenschaft erscheinen, die nur sehr großen Turing-Maschinen vorbehalten ist. Dass dieser Eindruck täuscht, wird der nächste Abschnitt zeigen. Dort werden wir zunächst eine alternative Notation einführen und anschließend die kleinstmögliche universelle Turing-Maschine kennen lernen.

### 6.1.5.7 Zelluläre Turing-Maschinen

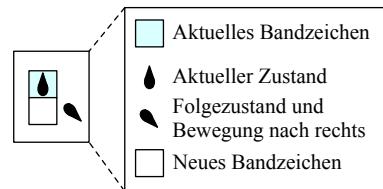
Die bisherige Darstellung der Turing-Maschine orientierte sich im Kern an Turings Originalarbeit; wir stellten uns eine mechanische Einheit vor, die einen Schreib-Lese-Kopf frei über einem unendlich langem Band hin- und herbewegt. In diesem Abschnitt wollen wir eine andere Darstellungsvariante diskutieren, die sich an jener des linearen Automaten aus Abschnitt 5.8 orientiert.

Linearen Automaten liegt eine eindimensionale Zelltopologie zugrunde. Die Zellen sind nebeneinander angeordnet und erstrecken sich in beide Richtungen in das Unendliche. Sie bilden exakt das unendliche Band nach, das wir für die Modellierung der Turing-Maschine benötigen. Der Bandinhalt wird durch die Färbungen der Zellen dargestellt, so dass wir die zur Verfügung stehende Farbmenge in direkter Weise als das Bandalphabet einer Turing-Maschine interpretieren können.

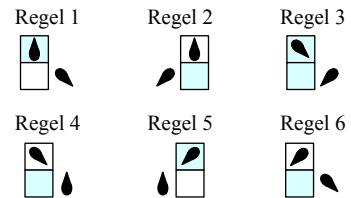
Die geschilderten Gemeinsamkeiten zwischen linearen Automaten und Turing-Maschinen dürfen nicht darüber hinwegtäuschen, dass sich beide Modelle in einem wesentlichen Punkt unterscheiden. Während die Berechnung in einem linearen Automaten verteilt erfolgt und alle Zellen parallel eine Zustandsänderung durchführen, arbeitet eine Turing-Maschine mit einem dedizierten Schreib-Lese-Kopf, der sich zu jeder Zeit an einer wohldefinierten Position befindet.

Um das Verhalten einer Turing-Maschine trotzdem adäquat zu beschreiben, bedarf es einer geringfügigen Modifikation des linearen Automaten. Wir erweitern das Modell, indem wir eine *Kopfzelle* (*head cell*) definieren, die als Schreib-Lese-Kopf fungiert. Das Schaltverhalten des erweiterten linearen Automaten legen wir analog zur Funktionsweise der Turing-Maschine fest. In jedem Berechnungsschritt wird die Kopfzelle umgefärbt und anschließend um eine Position nach links oder rechts geschoben. Außerdem reichern wir die Kopfzelle um einen zusätzlichen Zustand an, der mit dem Zustand der modellierten Turing-Maschine identisch ist.

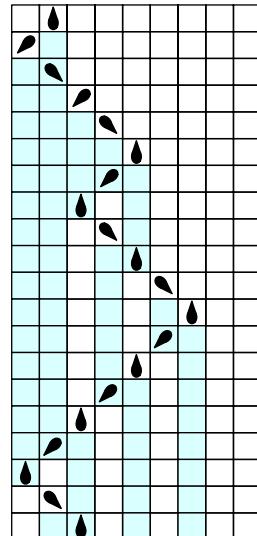
#### Regelschema



#### Vollständiger Regelsatz

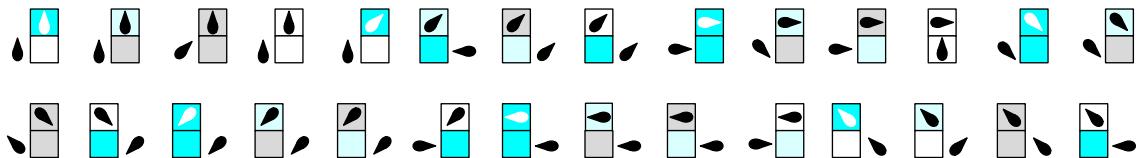


#### Automat in Aktion



**Abbildung 6.40:** Durch eine Modifikation des Grundmodells lassen sich lineare zelluläre Automaten für die Simulation von Turing-Maschinen einsetzen.

- Marvin Minskys universelle Turing-Maschine aus dem Jahre 1962 [69]



- Stephen Wolframs universelle 2,5-Turing-Maschine aus dem Jahre 2002 [99]



- Die kleinstmögliche universelle Turing-Maschine: Wolframs 2,3-Maschine aus dem Jahre 2002 [99]



**Abbildung 6.41:** Die Jagd nach der kleinstmöglichen universellen Turing-Maschine fand im Jahre 2007 ihr erfolgreiches Ende. In diesem Jahr bewies der Brite Alex Smith die Universalität von Wolframs 2,3-Maschine.

Abbildung 6.40 zeigt, wie sich eine Turing-Maschine in der Notation des modifizierten linearen Automaten beschreiben lässt. Die dargestellte Maschine besitzt vier Zustände, die durch den Drehwinkel des verwendeten Keilsymbols unterschieden werden. Die Zellen können eine von zwei Farben annehmen, so dass der zelluläre Automat einer Turing-Maschine mit einem zweielementigen Bandalphabet entspricht. Das Verhalten wird durch insgesamt 6 Regeln bestimmt. Jede Regel wird durch zwei Farbfelder und zwei Keilsymbole beschrieben. Das obere Farbfeld beschreibt das aktuelle und das untere das neu zu schreibende Bandzeichen. Die Richtung des oberen Keils gibt an, in welchem Zustand sich die Maschine befinden muss, damit die entsprechende Regel angewendet werden kann. Der untere Keil definiert den Folgezustand und die auszuführende Kopfbewegung. Ist das Keilsymbol links des Folgezustands eingezeichnet, bewegt sich der Schreib-Lese-Kopf nach links, ist es rechts eingezeichnet, bewegt er sich nach rechts. In unserem Beispiel führen die Regeln 1, 3, 4 und 6 eine Kopfbewegung nach rechts und die Regeln 2 und 5 eine Kopfbewegung nach links aus.

Abbildung 6.41 zeigt drei historisch bedeutsame Turing-Maschinen, dargestellt in der Notation der zellulären Automaten. Alle drei Maschinen sind universell, d. h., sie sind in der Lage, jede andere Turing-Maschine zu simulieren. Die erste wurde im Jahre 1962 von dem amerikanischen Computerwissenschaftler Marvin Minsky vorgestellt. Seine universelle Maschine unterscheidet 7 Zustände und 4 Farben. In der von Stephen Wolfram verwendeten Nomenklatur wird die Maschine als 7,4-Maschine bezeichnet. Im Vergleich zur Originalarbeit von Turing war Minsky ein großer Wurf gelungen. Dort erstreckt sich die Beschreibung einer universellen Maschine noch über vier ganze Seiten [90].

Im Jahre 2002 stellte der britische Mathematiker Stephen Wolfram eine weiterentwickelte Maschine vor, die ebenfalls universell ist, aber mit weniger Zuständen auskommt. Während Minskys Modell 7 Zustände benötigt, kommt die neue 2,5-Maschine mit nur 2 Zuständen aus. Die Anzahl der Farben musste Wolfram allerdings von 4 auf 5 erhöhen. Bedeutender sollte jedoch seine zeitgleich veröffentlichte 2,3-Maschine werden (Abbildung 6.41 unten). Wolfram schlug die Maschine als einen potenziellen Kandidaten für die kleinstmögliche Turing-Maschine vor, die die Eigenschaft der Universalität erfüllt [99]. Auch wenn es Wolfram nicht gelang, seine Vermutung selbst zu belegen, konnte er ein wichtiges Zwischenresultat erzielen: Er bewies, dass 2 Farben und 2 Zustände *nicht* ausreichen, um die Eigenschaft der Universalität zu erreichen. Wäre die 2,3-Maschine also tatsächlich universell, so wäre es gleichzeitig die kleinste universelle Maschine, die überhaupt existiert.

Wolframs Vermutung wurde im Jahre 2007 zur Gewissheit. In diesem Jahr gelang dem 20-jährigen Briten Alex Smith der Nachweis, dass die 2,3-Maschine die Eigenschaft der Universalität erfüllt. Das Rätsel um die kleinstmögliche universelle Turing-Maschine hat damit ein erfolgreiches Ende gefunden.

### 6.1.6 Alternative Berechnungsmodelle

Neben den bisher vorgestellten Berechnungsmodellen wurden in der Vergangenheit weitere entwickelt. Bekannte Vertreter sind

- die Registermaschine,
- der Lambda-Kalkül von Church und Kleene,
- die Post'sche Tag-Maschine und
- die dynamische Logik.

Besitzt Wolframs 2,3-Maschine eine praktische Anwendung? Es scheint gute Gründe zu geben, die Frage mit Nein zu beantworten, schließlich lehrt uns die Erfahrung, dass die Programmierung einer Maschine schwieriger wird, je einfacher sie aufgebaut ist. Die 2,3-Maschine scheint diese empirisch gewonnene Vermutung auf eindringliche Weise zu bestätigen. Deutliche Hinweise liefert der Compiler, den Smith im Rahmen seines Universitätsbeweises konstruierte. Der Compiler hat die Aufgabe, eine beliebige Turing-Maschine  $T$  in ein Eingabewort zu übersetzen, das die 2,3-Maschine dazu veranlasst,  $T$  zu simulieren. Wolfram äußert sich hierüber wie folgt:

*„But his ‘compiler’ doesn’t make terribly compact or efficient code. In fact, for anything but the simplest cases, the code tends to be astronomically large and horrendously inefficient.“* [100]

Lösen wir uns dagegen von den klassischen Denkmustern, die uns die aktuelle Computertechnik auferlegt, so fällt die Antwort weniger eindeutig aus. Für Wolfram ist z. B. eine völlig andere Art des Computers denkbar:

*„Perhaps one day there’ll even be practical molecular computers built from this very 2,3 Turing machine. With tapes a bit like RNA strands, and heads moving up and down like ribosomes. When we think of nanoscale computers, we usually imagine carefully engineering them to mimic the architecture of the computers we know today. But one of the lessons [...] is that there’s a completely different way to operate.“* [100]

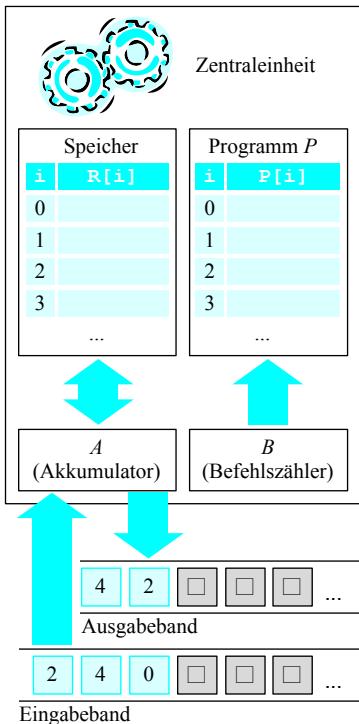
Erst die Zukunft kann zeigen, ob und wenn ja, in welcher Form die 2,3-Maschine den Sprung in die praktische Anwendung schaffen wird. Unabhängig davon ist die Maschine der Beweis dafür, dass die Universalität keine Eigenschaft ist, die einer komplexen Maschinerie bedarf. Bereits wenige, einfache Regeln reichen aus, um sie zu erreichen.

Die beiden Erstgenannten werden wir in ihren Grundzügen kurz vorstellen, aber nicht in der gleichen Tiefe diskutieren wie die weiter oben eingeführten Modelle. Informationen zu den Post'schen Tag-Maschinen gibt [75]. Dynamische Logiken werden ausführlich in [40] besprochen.

### 6.1.6.1 Registermaschinen

Die *Registermaschine* verkörpert ein Berechnungsmodell, das der Architektur realer Computersysteme sehr nahe kommt. Die Frage, was wir im Detail unter diesem Begriff zu verstehen haben, wird in der Literatur jedoch unterschiedlich beantwortet. Es existiert eine Vielzahl von Maschinentypen, die sich sowohl in der Anzahl und der Beschaffenheit der Register als auch im Befehlssatz unterscheiden. Das hier vorgestellte Modell wird in der Literatur meist als *verallgemeinerte Registermaschine* oder als *Random Access Machine*, kurz RAM, bezeichnet.

Abbildung 6.42 skizziert den Aufbau einer verallgemeinerten Registermaschine. Auf der obersten Ebene verfügt sie über ein *Eingabeband*, ein *Ausgabeband* und eine *Zentraleinheit*. Die Zentraleinheit untergliedert sich in den *Akkumulator A*, den *Befehlszähler B*, das *Programm P* und den *Speicher*, der durch abzählbar viele Register  $R[1], R[2], \dots$  gebildet wird. Jedes Register kann über eine eindeutig vergebene Adresse direkt angesprochen und mit einer natürlichen Zahl beliebiger Größe beschrieben werden. Das Programm besteht aus einer endlichen Anweisungsfolge  $P[1], \dots, P[m]$ , die über den Befehlszähler  $B$  adressiert wird. Die vorhandenen Bänder dienen der Ein- und Ausgabe von Daten und werden über einen Lese- und einen Schreibkopf angesteuert. Der Lesekopf steht über der  $i$ -ten Zelle  $z_i$  des Eingabebands und der Schreibkopf über der  $j$ -ten Zelle  $z'_j$  des Ausgabebands. Initial seien  $i$  und  $j$  gleich 0,  $B$  gleich 1 und der Inhalt aller Register gleich 0. Nachdem die Registermaschine gestartet wurde, führt sie so lange den Befehl  $P[B]$  aus, bis der Befehlszähler den Wert 0 erreicht.



**Abbildung 6.42:** Allgemeiner Aufbau der verallgemeinerten Registermaschine

Der Befehlssatz der Registermaschine ist in Tabelle 6.2 zusammengefasst. Mit Hilfe der Befehle `INP` oder `OUT` wird ein Zeichen vom Eingabeband eingelesen oder auf das Ausgabeband geschrieben. Der Lese- und der Schreibkopf bewegen sich ausschließlich von links nach rechts, so dass alle Zeichen nur einmal, in unveränderbarer Reihenfolge eingelesen bzw. ausgegeben werden können. Die Befehle `LDA` und `STA` dienen dem Datentransfer zwischen Akkumulator und Speicher. Insgesamt unterstützt die Registermaschine drei Adressierungsarten: die *unmittelbare Adressierung* (`LDA #n`), die *absolute Adressierung* (`LDA n, STA n`) und die *indirekte Adressierung* (`LDA (n), STA (n)`). Des Weiteren verfügt

Befehl	Beschreibung	Aktion
INP	Überträgt den nächsten Wert vom Eingabeband in den Akkumulator	$A := z_i$ $B := B + 1, i := i + 1$
OUT	Schreibt den Akkumatorinhalt auf das Ausgabeband	$z'_j := A$ $B := B + 1, j := j + 1$
LDA $\#n$	Lädt den Akkumulator mit dem Wert $n$	$A := n$ $B := B + 1$
LDA $n$	Lädt den Akkumulator mit dem Inhalt von Register $n$	$A := R[n]$ $B := B + 1$
LDA $(n)$	Lädt den Akkumulator über ein indirekt adressiertes Register	$A := R[R[n]]$ $B := B + 1$
STA $n$	Überträgt den Akkumatorinhalt in das Register $n$	$R[n] := A$ $B := B + 1$
STA $(n)$	Überträgt den Akkumatorinhalt in ein indirekt adressiertes Register	$R[R[n]] := A$ $B := B + 1$
ADD $\#n$	Erhöht den Akkumatorinhalt um einen konstanten Wert	$A := A + n$ $B := B + 1$
SUB $\#n$	Verringert den Akkumatorinhalt um einen konstanten Wert	$A := \max\{0, A - n\}$ $B := B + 1$
JMP $n$	Direkter Sprung zur $n$ -ten Programmanweisung	$B := n$
BEQ $i, n$	Indirekter Sprung in Abhängigkeit des Akkumatorinhalts	$B := n$ falls $A = i$ $B := B + 1$ falls $A \neq i$

**Tabelle 6.2:** Vollständiger Befehlssatz der verallgemeinerten Registermaschine

die Registermaschine über primitive Arithmetikfähigkeiten in Form der Befehle ADD und SUB. Die Subtraktion wird auch hier gesättigt durchgeführt, da die Register per Definition keine negativen Zahlen aufnehmen können. Die Befehle JMP und BEQ dienen zur Steuerung des Kontrollflusses. JMP beschreibt  $B$  mit einem konstanten Wert und verursacht hierdurch einen Sprung an eine beliebige Programmstelle. BEQ implementiert einen bedingten Sprung, der nur dann ausgelöst wird, wenn der Akkumulator einen bestimmten Wert enthält.

```
mirror.asm
START: LDA #1
        STA 1
READ:  LDA 1
        ADD #1
        STA 1
        INP
        BEQ 0, WRITE
        STA (1)
        JMP READ
WRITE: LDA 1
        SUB #1
        STA 1
        BEQ 1, HALT
        LDA (1)
        OUT
        JMP WRITE
HALT:  JMP 0
```

**Abbildung 6.43:** Das dargestellte Beispielprogramm veranlasst die Registermaschine, den Inhalt des Eingabebands in umgekehrter Reihenfolge auf dem Ausgabeband wiederzugeben. Um die Programmstruktur zu verdeutlichen, wurden die absoluten Sprungadressen durch symbolische Bezeichner ersetzt.

Abbildung 6.43 demonstriert die Funktionsweise der Registermaschine anhand eines konkreten Beispiels. Das dargestellte Programm liest eine Folge von Zahlen vom Eingabeband und gibt diese in umgekehrter Reihenfolge auf dem Ausgabeband aus. Die Ziffer 0 markiert das Ende der Eingabefolge und wird nicht auf das Ausgabeband geschrieben.

Um die gewünschte Funktionalität zu erreichen, werden die Register  $R[2], R[3], \dots$  als Kellerspeicher eingesetzt, der zunächst in aufsteigender Richtung beschrieben und danach in absteigender Richtung wieder ausgelesen wird. Das Register  $R[1]$  wird als Indexzeiger verwendet, der zu jedem Zeitpunkt auf das Kopfelement des Kellerspeichers verweist. Tabelle 6.3 zeigt im Detail, wie die Eingabesequenz 2,4,0 verarbeitet wird. Nach 41 Berechnungsschritten terminiert die Maschine und hinterlässt wie erwartet die Ziffernfolge 4,2 auf dem Ausgabeband.

Die verallgemeinerte Registermaschine ist in der Lage, eine beliebige Turing-Maschine zu simulieren. Eine einfache Möglichkeit besteht darin, mit den Registern  $R[2], R[3], \dots$  ein einseitig beschränktes Band nachzubilden und die Position des Schreib-Lese-Kopfes in Register  $R[1]$  zu speichern. Das Verhalten der Turing-Maschine wird in drei Einzelschritten simuliert. Zuerst wird der Inhalt des Eingabebands auf das virtuelle Arbeitsband kopiert. Anschließend wird das Verhalten der Turing-Maschine schrittweise nachvollzogen und am Ende der finale Inhalt des virtuellen Arbeitsbands auf das Ausgabeband kopiert.

Umgekehrt lässt sich jede Registermaschine mit Hilfe einer Turing-Maschine simulieren. Um die Transformation zu verstehen, halten wir zunächst fest, dass wir jedes Programm so modifizieren können, dass nur endlich viele Register verwendet werden. Die Transformation ist möglich, da der Wertebereich eines Registers – im Gegensatz zu realen Computerarchitekturen – unbeschränkt ist. Über die Cantor'sche Paarungsfunktion können wir damit den Inhalt des gesamten Registersatzes eindeutig in ein einziges Register packen.

Eine Registermaschine mit  $n$  Registern lässt sich mit einer einseitig beschränkten Turing-Maschine mit  $n+3$  Bändern simulieren. Auf den ersten  $n$  Bändern wird der Inhalt des Registersatzes gespeichert, auf den verbleibenden 3 Bändern wird das Eingabeband, das Ausgabeband und der Akkumulator nachgebildet. Für das Befehlsregister wird kein zusätzliches Band benötigt. Da jedes Programm nur endlich viele Anweisungen besitzt, können wir den Wert von  $B$  in die Zustandsfolge hineincodieren, die von der Turing-Maschine nacheinander durchlaufen wird. Wenngleich die angestellten Überlegungen sehr informeller Natur sind, erklären sie im Kern, warum die Registermaschine die gleiche Berechnungsstärke wie die Turing-Maschine besitzt.

Zyklus	B	Befehl	Eingabeband	Ausgabeband	A	R[1]	R[2]	R[3]	R[3]
01	1	LDA #1	2, 4, 0	–	1	0	0	0	0
02	2	STA 1	2, 4, 0	–	1	1	0	0	0
03	3	LDA 1	2, 4, 0	–	1	1	0	0	0
04	4	ADD #1	2, 4, 0	–	2	1	0	0	0
05	5	STA 1	2, 4, 0	–	2	2	0	0	0
06	6	INP	4, 0	–	2	2	0	0	0
07	7	BEQ 0, WRITE	4, 0	–	2	2	0	0	0
08	8	STA (1)	4, 0	–	2	2	2	0	0
09	9	JMP READ	4, 0	–	2	2	2	0	0
10	3	LDA 1	4, 0	–	2	2	2	0	0
11	4	ADD #1	4, 0	–	3	2	2	0	0
12	5	STA 1	4, 0	–	3	3	2	0	0
13	6	INP	0	–	4	3	2	0	0
14	7	BEQ 0, WRITE	0	–	4	3	2	0	0
15	8	STA (1)	0	–	4	3	2	4	0
16	9	JMP READ	0	–	4	3	2	4	0
17	3	LDA 1	0	–	3	3	2	4	0
18	4	ADD #1	0	–	4	3	2	4	0
19	5	STA 1	0	–	4	4	2	4	0
20	6	INP	–	–	0	4	2	4	0
21	7	BEQ 0, WRITE	–	–	0	4	2	4	0
22	10	LDA 1	–	–	4	4	2	4	0
23	11	SUB #1	–	–	3	4	2	4	0
24	12	STA 1	–	–	3	3	2	4	0
25	13	BEQ 1, HALT	–	–	3	3	2	4	0
26	14	LDA (1)	–	–	4	3	2	4	0
27	15	OUT	–	4	4	3	2	4	0
28	16	JMP WRITE	–	4	4	3	2	4	0
29	10	LDA 1	–	4	3	3	2	4	0
30	11	SUB #1	–	4	2	3	2	4	0
31	12	STA 1	–	4	2	2	2	4	0
32	13	BEQ 1, HALT	–	4	2	2	2	4	0
33	14	LDA (1)	–	4	2	2	2	4	0
34	15	OUT	–	4,2	2	2	2	4	0
35	16	JMP WRITE	–	4,2	2	2	2	4	0
36	10	LDA 1	–	4,2	2	2	2	4	0
37	11	SUB #1	–	4,2	1	2	2	4	0
38	12	STA 1	–	4,2	1	1	2	4	0
39	13	BEQ 1, HALT	–	4,2	1	1	2	4	0
40	17	JMP 0	–	4,2	1	1	2	4	0
41	0	–	–	4,2	1	1	2	4	0

**Tabelle 6.3:** Ablaufprotokoll für die Eingabesequenz 2,4,0

Der Lambda-Kalkül ist das mathematische Fundament aller funktionalen Programmiersprachen. Der älteste Vertreter dieser Gruppe ist Lisp. Die Sprache wurde im Jahre 1958 von John McCarthy ins Leben gerufen und ist nach Fortran die zweitälteste Computersprache überhaupt. Genau wie Prolog wird Lisp vor allem für Anwendungen aus dem Bereich der künstlichen Intelligenz eingesetzt. Lisp-Programme besitzen einen einfachen Aufbau, da lediglich zwei Grundelemente unterschieden werden: Atome und Listen. Letztere dürfen sich selbst als Element enthalten und ermöglichen so die Konstruktion komplexer Datenstrukturen. Sowohl die interne Arbeitsweise als auch die Notation von Lisp orientieren sich an jenen des Lambda-Kalküls:

Parameter	Argument
(( lambda ( x ) (* x x ) ) 3 )	↔ ↔ ↔ ↔ ↔ ↔
$\lambda$	Definition

Lisp erreicht seine große Flexibilität aufgrund der Eigenschaft, nicht zwischen Daten und Anweisungen zu unterscheiden. Jedes Lisp-Programm ist eine Liste und wie jedes andere Objekt zur Laufzeit manipulierbar. Umgekehrt kann jede Liste als Programm interpretiert und durch den Interpreter ausgeführt werden.

Lisp ist die älteste, aber nicht die einzige Programmiersprache, die sich an der Arbeitsweise des Lambda-Kalküls orientiert. Das funktionale Programmierparadigma wurde in der Vergangenheit in verschiedene Richtungen weiterentwickelt und um zusätzliche Konzepte angereichert. Im Zuge dieser Entwicklungen sind unter anderem die Sprachen Haskell, ML, Miranda und Scheme entstanden. Obwohl sich das Aussehen der Quelltexte teilweise erheblich unterscheidet, basieren sie alle auf dem gleichen operativen Kern: dem Lambda-Kalkül von Alonzo Church und Stephen Kleene.

### 6.1.6.2 Lambda-Kalkül

Der Lambda-Kalkül (kurz  $\lambda$ -Kalkül) wurde in den Dreißigerjahren von Alonzo Church und Stephen Kleene entwickelt. Er wurde mit dem Ziel entworfen, komplexe mathematische Funktionen durch die Kombination allgemein gehaltener Rechenvorschriften zu definieren. Die grundlegende Operation des Lambda-Kalküls ist die Anwendung einer Funktion  $f$  auf ein Argument  $x$ , geschrieben als  $(f x)$ . Ist z. B. add eine Funktion zur Addition zweier Zahlen, so berechnet  $((\text{add } x) y)$  die Summe  $x + y$ . Indem wir eine Variable mit Hilfe des  $\lambda$ -Operators binden, lassen sich aus bestehenden Funktionen neue erzeugen. So bezeichnet  $(\lambda x. ((\text{add } x) x))$  eine von  $x$  abhängige Funktion, deren Ergebniswert durch  $((\text{add } x) x) = 2 \cdot x$  festgelegt ist. Die Anwendung des  $\lambda$ -Operators wird als *Abstraktion* bezeichnet.

Damit haben wir bereits alle Grundbausteine des Lambda-Kalküls kennen gelernt. Formal definieren wir die Menge der *Lambda-Terme* (kurz  $\lambda$ -Terme) wie folgt:



#### Definition 6.14 ( $\lambda$ -Terme)

Sei  $V = \{x_1, x_2, \dots\}$  eine Menge von Variablen. Dann gilt:

- Jede Variable  $x_i \in V$  ist ein  $\lambda$ -Term.
- Sind  $f$  und  $g$   $\lambda$ -Terme, dann ist  $(fg)$  ein  $\lambda$ -Term.
- Ist  $f$  ein  $\lambda$ -Term und  $x_i \in V$ , dann ist  $(\lambda x_i.f)$  ein  $\lambda$ -Term.

$\lambda$ -Ausdrücke lassen sich nach dieser Definition freizügig kombinieren. Eine Funktion kann beliebige Lambda-Terme als Argumente erhalten und somit auch auf Funktionen angewendet werden. Wie das folgende Beispiel zeigt, kann sich eine Funktion sogar selbst als Argument entgegennehmen:

$$((\lambda x.x)(\lambda x.x))$$

Mit Hilfe von *Konversionsregeln* lässt sich ein  $\lambda$ -Term in einen äquivalenten Term überführen, der die gleiche Funktion beschreibt. Auf diese Weise werden die  $\lambda$ -Terme in Äquivalenzklassen aufgeteilt und wir schreiben  $f = g$ , falls  $f$  und  $g$  der gleichen Klasse angehören. Im Einzelnen handelt es sich um die folgenden drei Regeln:

- $\alpha$ -Konversion

$$(\lambda x.f) = (\lambda y.f[x \leftarrow y]) \quad (6.57)$$

Die Konversion erlaubt die Umbenennung von Variablen, ist jedoch nur unter gewissen Einschränkungen anwendbar. Zum einen muss die Variable  $y$  so gewählt werden, dass durch die Substitution keine neuen Bindungen innerhalb von  $f$  entstehen. Zum anderen werden nur diejenigen Vorkommen von  $x$  ersetzt, die in  $f$  ungebunden vorkommen.

### ■ $\beta$ -Konversion

$$((\lambda x.f) g) = f[x \leftarrow g] \quad (6.58)$$

Diese Regel entspricht dem Einsetzen des Parameters  $g$  in die Funktion  $f$ . Der Funktionswert wird berechnet, indem alle Vorkommen der Variablen  $x$  durch  $g$  ersetzt werden. Auch hier dürfen nur jene Vorkommen von  $x$  ersetzt werden, die in  $f$  nicht durch einen weiteren  $\lambda$ -Operator gebunden sind.

### ■ $\eta$ -Konversion

$$(\lambda x.fx) = f \quad (6.59)$$

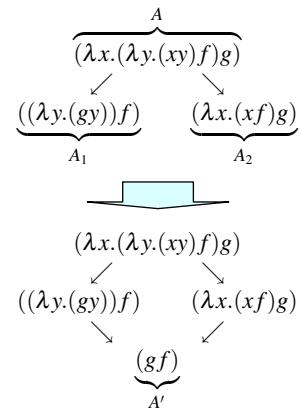
Die Konversion besagt, dass zwei Funktionen genau dann gleich sind, wenn sie für alle Belegungen der Eingangsgröße den gleichen Funktionswert berechnen. Die  $\eta$ -Konversion ist optional und kann aus dem Kalkül entfernt werden, ohne seine grundlegenden Eigenschaften zu verändern.

Ein  $\lambda$ -Term liegt in *Normalform* vor, wenn keine  $\beta$ -Konversion mehr anwendbar ist. Der Kalkül erfüllt die nach Alonzo Church und J. Barkley Rosser benannte *Church-Rosser-Eigenschaft*, aus der unter anderem folgt, dass die Reihenfolge, in der  $\alpha$ - und  $\beta$ -Konversionen angewendet werden, keine Rolle spielt (vgl. Abbildung 6.44).

Beachten Sie, dass sich nicht jeder  $\lambda$ -Ausdruck in endlich vielen Schritten in eine Normalform überführen lässt. Wie das Beispiel in Abbildung 6.45 zeigt, können unendlich lange Ableitungssequenzen entstehen. Der abgebildete  $\lambda$ -Ausdruck  $Y$  wird aufgrund seiner speziellen Eigenschaft als *Fixpunktoperator* bezeichnet. Er spielt innerhalb des  $\lambda$ -Kalküls eine prominente Rolle und kann dazu verwendet werden, beliebige rekursive Funktionen zu definieren.

Im direkten Vergleich mit den meisten anderen Berechnungsmodellen wirkt der  $\lambda$ -Kalkül minimalistisch, schließlich beschränkt er sich auf die Definition weniger fundamentaler Konversionsregeln, die eine rein syntaktische Manipulationen von Ausdrücken erlauben. Trotzdem ist der  $\lambda$ -Kalkül genauso ausdrucksstark wie die in Abschnitt 6.1.5 ausführlich beschriebene Turing-Maschine. Entsprechende Resultate wurden von Kleene und Turing in den Dreißigerjahren bewiesen [57, 91].

### ■ Beispiel



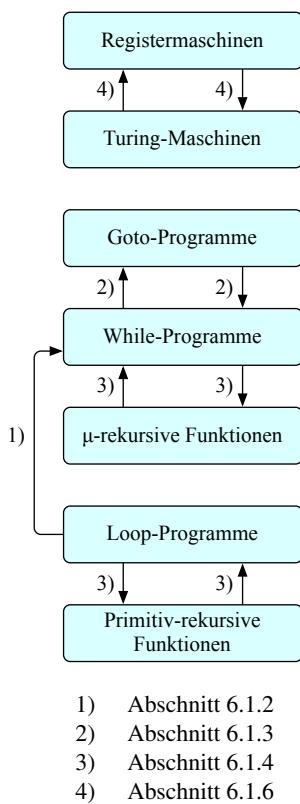
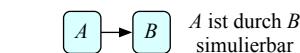
**Abbildung 6.44:** Der Lambda-Kalkül erfüllt die Church-Rosser-Eigenschaft. Lässt sich ein Ausdruck  $A$  in die Ausdrücke  $A_1$  und  $A_2$  umformen, so lassen sich diese durch weitere Umformungen immer wieder zu einem gemeinsamen Ausdruck  $A'$  zusammenführen.

$$Y := (\lambda f.((\lambda x.(f(xx)))(\lambda x.(f(xx)))))$$



$$\begin{aligned} & (Yg) \\ &= ((\lambda f.((\lambda x.(f(xx)))(\lambda x.(f(xx))))))g \\ &= ((\lambda x.(g(xx)))(\lambda x.(g(xx)))) \\ &= (g((\lambda x.(g(xx)))(\lambda x.(g(xx)))))) \\ &= (g(Yg)) \\ &= (g(Y(Yg))) \\ &= (g(Y(Y(Yg))))) \\ &= (g(Y(Y(Y(Yg)))))) \\ &= \dots \end{aligned}$$

**Abbildung 6.45:** Für beliebige  $\lambda$ -Terme  $f$  erfüllt der Fixpunktoperator  $Y$  die Eigenschaft  $f(Yf) = f$ . Angewendet auf  $g$  entsteht eine unendlich lange Ableitungssequenz.



**Abbildung 6.46:** Ausdrucksstärke der verschiedenen Berechnungsmodelle

## 6.2 Church'sche These

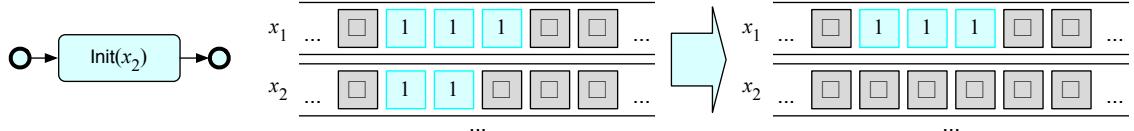
In den vorangegangenen Abschnitten haben wir verschiedene Berechnungsmodelle eingeführt, die den Begriff der *Berechenbarkeit* mathematisch präzise beschreiben. Im Rahmen unserer Betrachtungen konnten wir bereits einige wichtige Teilergebnisse erringen (vgl. Abbildung 6.46). So haben wir in Abschnitt 6.1.2 am Beispiel der Ackermann-Funktion herausgearbeitet, dass die Loop-Sprache berechnungsschwächer als die While-Sprache ist und in Abschnitt 6.1.3 die Äquivalenz von While- und Goto-Programmen bewiesen. Anschließend haben wir in Abschnitt 6.1.4 gezeigt, dass die Menge der primitiv-rekursiven Funktionen mit der Menge der Loop-berechenbaren Funktionen und die Menge der  $\mu$ -rekursiven Funktionen mit der Menge der While-berechenbaren Funktionen übereinstimmt. Abschließend haben wir in Abschnitt 6.1.6 die Äquivalenz zwischen Turing-Maschinen und Registermaschinen skizziert.

Ein wichtiger Beweis steht bisher noch aus, bevor wir den Kreis endgültig schließen können. Die Rede ist von der Äquivalenz zwischen While-Programmen und Turing-Maschinen. Dass sich beide tatsächlich als gleich ausdrucksstark erweisen werden, ist ein beeindruckendes Ergebnis der Berechenbarkeitstheorie, schließlich könnten beide Modelle in ihrem Aufbau und ihrer Struktur kaum unterschiedlicher sein. Die While-Sprache folgt dem Ansatz, den wir aus der klassischen Software-Technik kennen. Im Kern ist sie der Prototyp des imperativen Programmierparadigmas und entsprechend einfach lassen sich While-Programme in reale Sprachen übersetzen. Im Gegensatz hierzu erinnern Turing-Maschinen in ihrem Aufbau an die klassische Hardware-Technik. Interpretieren wir das Band als Speicher und den Zustandsautomat als Prozessor, so lässt sich die Funktionsweise einer Turing-Maschine nahezu eins zu eins mit der eines modernen Computers gleichsetzen. Auch dort werden Daten permanent vom Speicher in den Prozessor geladen, verändert und in den Speicher zurückgeschrieben.

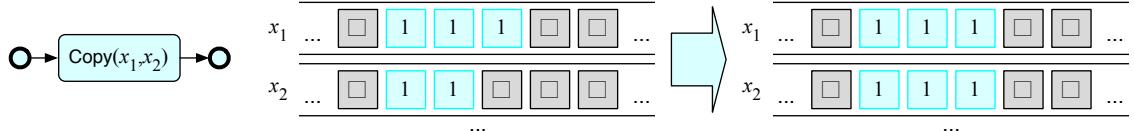
Um die Äquivalenz beider Berechnungsmodelle zu beweisen, werden wir in zwei Schritten vorgehen. Zuerst werden wir demonstrieren, dass sich jedes While-Programm mit Hilfe einer Turing-Maschine simulieren lässt. Anschließend zeigen wir die Umkehrung.

Die Simulation eines While-Programms  $P$  gelingt am einfachsten mit einer Turing-Maschine mit  $k$  Bändern, wobei wir den Parameter  $k$  so wählen, dass jede in  $P$  vorkommende Variable  $x_i$  auf einem separaten Band Platz findet. Um die einzelnen Operationen eines While-Programms auf der Turing-Maschine zu simulieren, definieren wir die

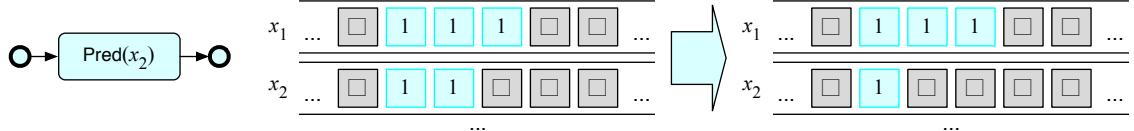
- Init-Maschine: initialisiert ein ausgewähltes Band mit dem Wert 0



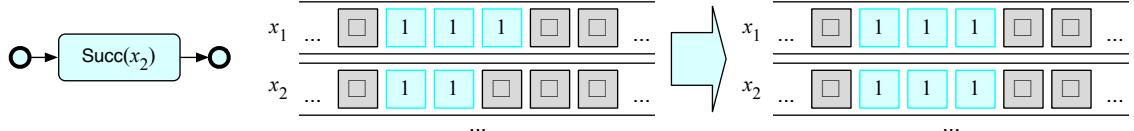
- Copy-Maschine: kopiert den Inhalt eines Bands auf ein anderes



- Pred-Maschine: berechnet den Vorgänger einer unär codierten Zahl



- Succ-Maschine: berechnet den Nachfolger einer unär codierten Zahl

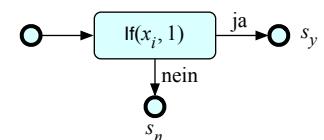


**Abbildung 6.47:** Elementarmaschinen zur Simulation der While-Sprache

vier in Abbildung 6.47 dargestellten Elementarmaschinen. Mit ihnen sind wir in der Lage, alle Zuweisungs- und Arithmetikoperationen der While-Sprache abzubilden.

Außerdem definieren wir für alle  $k \in \mathbb{N}_0$  eine Maschine  $\text{If}(x_i, k)$ , die den Inhalt des  $i$ -ten Bands mit dem Wert  $k$  vergleicht. Abbildung 6.49 zeigt exemplarisch die Definition der Maschine  $\text{If}(x_i, 1)$ . Anders als die weiter oben vorgestellten Elementarmaschinen besitzt die If-Maschine zwei Endzustände. Ist der Inhalt des  $i$ -ten Bands gleich  $k$ , so wird der Zustand  $s_y$  und in allen anderen Fällen der Zustand  $s_n$  eingenommen.

Damit haben wir alle Bausteine in unserem Repertoire, um ein beliebiges While-Programm durch die Komposition der Elementarmaschinen in eine äquivalente Turing-Maschine zu übersetzen. Das Konstruktions-



	0	1	$\square$
$s_0$	$(s_n, 0, \circlearrowleft)$	$(s_1, 1, \rightarrow)$	$(s_n, \square, \circlearrowleft)$
$s_1$	$(s_n, 0, \leftarrow)$	$(s_n, 1, \leftarrow)$	$(s_y, \square, \leftarrow)$
$s_n$	—	—	—
$s_y$	—	—	—

**Abbildung 6.49:** Die If-Maschine

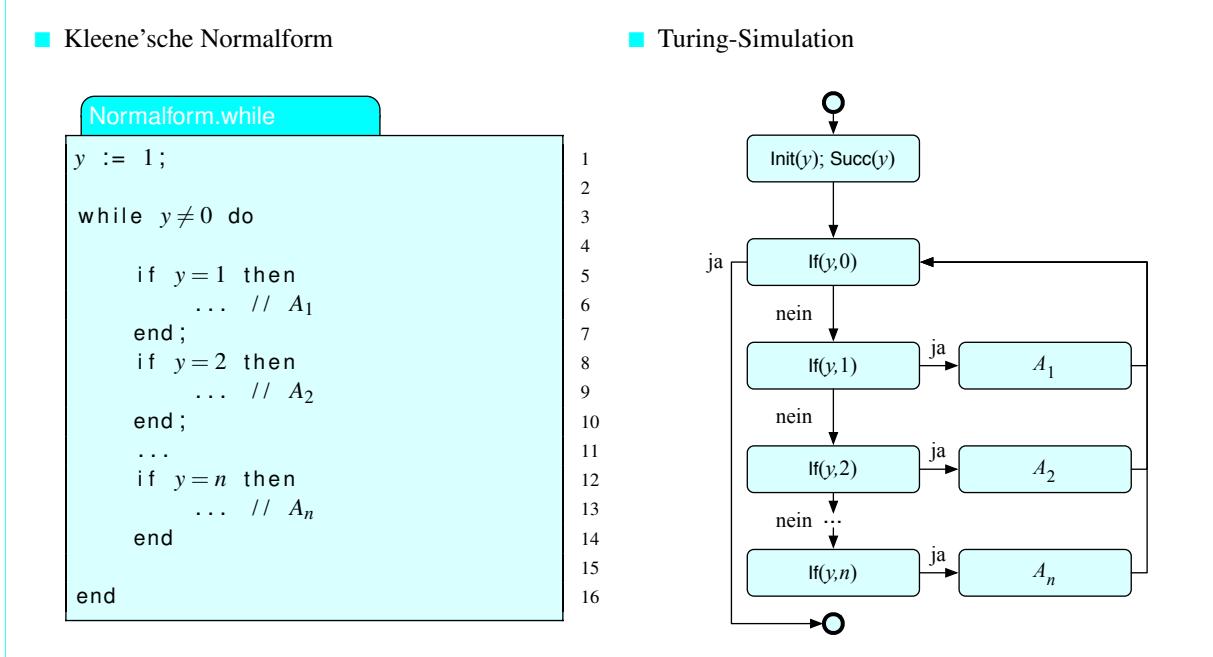


Abbildung 6.48: Simulation von While-Programmen mit Hilfe von Turing-Maschinen

schema in Abbildung 6.48 zeigt, wie sich ein While-Programm in Kleene'scher Normalform in eine Turing-Maschine überführen lässt. Den Kern der Konstruktion bildet die Simulation der While-Schleife. Diese wird durch eine If-Maschine realisiert, die in jedem Schleifendurchlauf den Wert des Bandes  $y$  überprüft. Ist  $y = 0$ , so geht die Turing-Maschine in den Endzustand über und terminiert. Ist  $y \neq 0$ , so wird mit Hilfe weiterer If-Maschinen eine Fallunterscheidung durchgeführt, die eins zu eins der Struktur des While-Programms entspricht. Trifft die  $i$ -te If-Bedingung zu, so wird die While-Anweisung  $A_i$  simuliert. Diese besteht aus einer Reihe arithmetischer Manipulationen, die mit Hilfe der Elementarmaschinen aus Abbildung 6.47 nachempfunden werden können.

Da sich jedes While-Programm in ein äquivalentes Programm in Kleene'scher Normalform übersetzen lässt, ist gezeigt, dass jedes While-Programm durch eine Turing-Maschine simuliert werden kann. Damit sind wir unserem Ziel, die Äquivalenz zwischen Turing-Maschinen und While-Programmen zu zeigen, einen großen Schritt näher gekommen:


**Satz 6.7**

Jede While-berechenbare Funktion ist Turing-berechenbar.

Wir wenden uns nun der umgekehrten Richtung zu: der Simulation von Turing-Maschinen mit While-Programmen. Wir werden den Beweis indirekt führen, indem wir auf eines unserer erzielten Zwischenergebnisse aus Abschnitt 6.1.3 zurückgreifen. Dort haben wir gezeigt, dass jede While-berechenbare Funktion auch Goto-berechenbar ist und umgekehrt. Wir nutzen dieses Resultat aus und zeigen, dass sich jede Turing-Maschine durch ein Goto-Programm simulieren lässt. Aus diesem Ergebnis folgt dann unmittelbar die Äquivalenz zwischen Turing-Maschinen und While-Programmen.

Für die folgende Betrachtung sei eine beliebige Turing-Maschine

$$T = (S, \Sigma, \Pi, \delta, s_0, \square, E) \quad (6.60)$$

gegeben. Das Bandalphabet  $\Pi$  betrachten wir als geordnete Menge, d.h., jedes Element  $\pi \in \Pi$  besitzt eine eindeutige Position, die wir mit  $\langle \pi \rangle$  ( $1 \leq \langle \pi \rangle \leq |\Pi|$ ) bezeichnen.

Wir wollen nun versuchen, eine Konfiguration der Turing-Maschine  $T$  innerhalb eines Goto-Programms darzustellen. Wie in Abschnitt 6.1.5 eingeführt, ist eine Konfiguration ein Tripel  $(v, s, \omega)$  mit

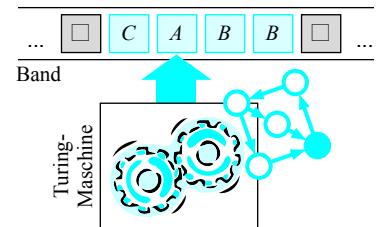
$$v = \{\rho_m, \dots, \rho_1\}, \quad s \in S, \quad \omega = \{\sigma_1, \dots, \sigma_n\}. \quad (6.61)$$

Die Variable  $s$  repräsentiert den aktuellen Zustand der Maschine und die Zeichenfolgen  $\rho_m, \dots, \rho_1$  und  $\sigma_1, \dots, \sigma_n$  entsprechen den Bandsymbolen links und rechts des Lesekopfes. Der Kopf selbst befindet sich über dem Zeichen  $\sigma_1$ . Beachten Sie, dass die Indizes der Zeichen in  $v$  aufsteigend und in  $\omega$  absteigend notiert sind. Die Reihenfolge wurde bewusst so gewählt; sie stellt sicher, dass sich das Zeichen mit dem kleinsten Index in unmittelbarer Kopfnähe befindet. Wie wir gleich sehen werden, ist es hierdurch möglich, eine Konfigurationsänderung ohne große Umwege auf die Multiplikation, die Division und die Modulo-Berechnung abzubilden.

Um eine Konfiguration zu repräsentieren, konstruieren wir ein Goto-Programm mit drei Variablen  $x_v$ ,  $x_s$  und  $x_\omega$  (vgl. Abbildung 6.50). Der aktuelle Zustand der Turing-Maschine wird in der Variablen  $x_s$  gespeichert.  $x_v$  und  $x_\omega$  codieren den Inhalt von  $v$  und  $\omega$  in Form einer  $b$ -adischen Zahlendarstellung:

$$x_v := \sum_{i=1}^m \langle \rho_i \rangle \cdot b^i \quad (6.62)$$

$$x_\omega := \sum_{i=1}^n \langle \sigma_i \rangle \cdot b^i \quad (6.63)$$



■ Bandalphabet

$$\Pi = \{A, B, C, \square\}$$

$$\langle A \rangle = 1$$

$$\langle B \rangle = 2$$

$$\langle C \rangle = 3$$

■ Bandcodierung ( $b = 5$ )

$$v = C$$

$$\begin{aligned} x_v &= \langle C \rangle \cdot 5^1 \\ &= 15 \end{aligned}$$

$$\omega = ABB$$

$$\begin{aligned} x_\omega &= \langle A \rangle \cdot 5^1 + \langle B \rangle \cdot 5^2 + \langle B \rangle \cdot 5^3 \\ &= 1 \cdot 5 + 2 \cdot 25 + 2 \cdot 125 \\ &= 305 \end{aligned}$$

**Abbildung 6.50:** Simulation von Turing-Maschinen mit Goto-Programmen. Die aktuelle Konfiguration der simulierten Maschine wird durch den Inhalt der drei Variablen  $x_v$ ,  $x_\omega$  und  $x_s$  nachgebildet.

■ Linksbewegung

$$\delta(s_i, \sigma) = (s_j, \sigma', \leftarrow)$$



simleft.goto

```

 $x_\omega := x_\omega \text{ div } b;$ 
 $x_\omega := \langle \sigma' \rangle + b \cdot x_\omega;$ 
 $x_\omega := (x_v \bmod b) + b \cdot x_\omega;$ 
 $x_v := x_v \text{ div } b;$ 
 $x_s := j$ 

```

Die Zahl  $b$  ist die *Basis* der Zahlendarstellung und wird so gewählt, dass sie die Anzahl der Symbole des Bandalphabets  $\Pi$  übersteigt. Hierdurch erreichen wir eine eindeutige Abbildung von  $\Pi^*$  in die Menge der natürlichen Zahlen. Vielleicht ist Ihnen aufgefallen, dass die Gleichungen (6.62) und (6.63) für den Fall  $b = 10$  nichts weiter als eine mathematische Beschreibung der uns vertrauten Dezimalzahlen sind. Jeder Wert  $\langle p_i \rangle$  bzw.  $\langle \sigma_i \rangle$  entspricht in diesem Fall einer einzelnen Ziffer. Die Ziffer 0 wird in unserer Darstellung bewusst vermieden, da die Folgen 0, 00 und 000 allesamt einen unterschiedlichen Bandinhalt repräsentieren, numerisch aber nicht voneinander unterschieden werden können.

1  
2  
3  
4  
5

Abbildung 6.51 zeigt, wie sich ein Konfigurationsübergang mit Hilfe arithmetischer Operationen simulieren lässt. Zunächst wird das Zeichen  $\sigma_1$  durch das Folgezeichen  $\sigma'$  ersetzt. Dies geschieht in zwei Schritten. Im ersten Schritt wird das Zeichen  $\sigma_1$  aus  $\omega$  entfernt, indem der Wert  $x_\omega$  durch die Basis  $b$  ganzzahlig dividiert wird. Im zweiten Schritt wird  $x_\omega$  mit  $b$  multipliziert und der Wert  $\langle \sigma' \rangle$  addiert. Hierdurch wird das Zeichen  $\sigma'$  an das linke Ende von  $\omega$  angehängt.

■ Rechtsbewegung

$$\delta(s_i, \sigma) = (s_j, \sigma', \rightarrow)$$



simright.goto

```

 $x_\omega := x_\omega \text{ div } b;$ 
 $x_\omega := \langle \sigma' \rangle + b \cdot x_\omega;$ 
 $x_v := b \cdot x_v + (x_\omega \bmod b);$ 
 $x_\omega := x_\omega \text{ div } b;$ 
 $x_s := j$ 

```

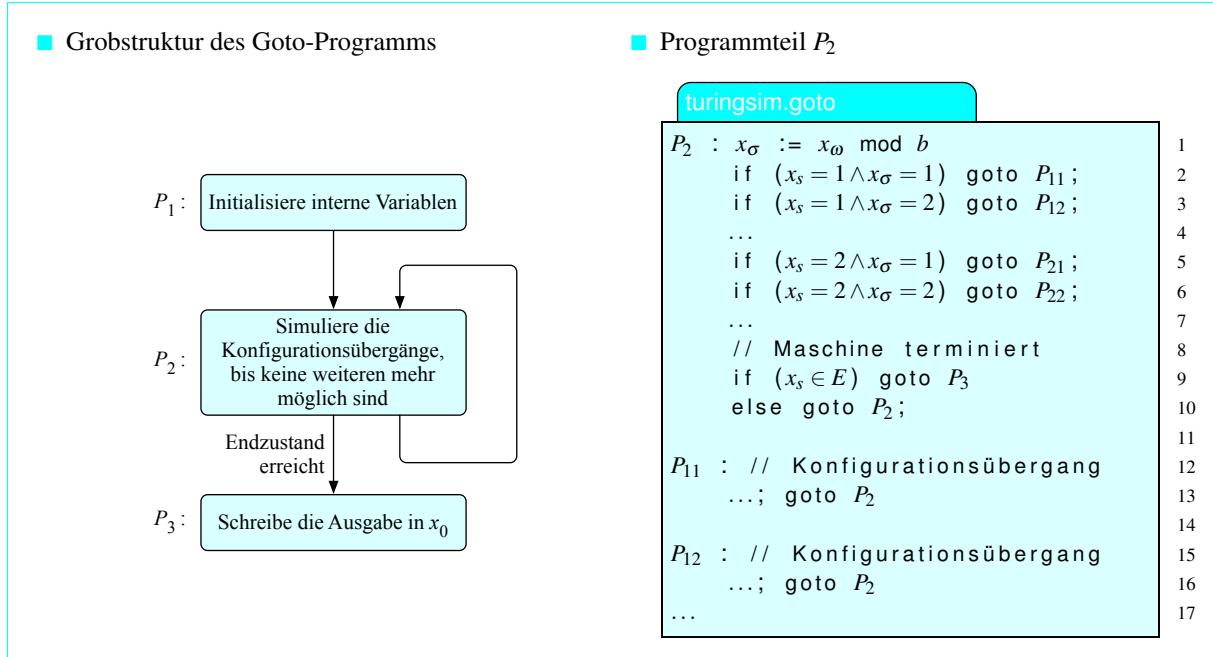
1  
2  
3  
4  
5

Anschließend wird die Bewegung des Schreib-Lese-Kopfes simuliert. Im Falle einer Linksbewegung wird das Zeichen  $\rho_1$  mit Hilfe der Modulo-Operation bestimmt und der Zeichenkette  $\omega$  von links hinzugefügt. Die anschließende Division von  $x_v$  durch  $b$  führt dazu, dass das Zeichen  $\rho_1$  aus  $v$  verschwindet. Die Rechtsbewegung erfolgt analog. Jetzt wird das Zeichen  $\sigma_1$  bestimmt und von rechts an die Zeichenkette  $v$  angehängt. Danach wird  $\sigma_1$  durch die Divisionsanweisung aus der Zeichenkette  $\omega$  entfernt. Beschreiben wir die Variable  $x_s$  am Ende noch mit dem Index des Folgezustands, so ist der Konfigurationsübergang vollständig ausgeführt.

**Abbildung 6.51:** Der Konfigurationsübergang einer Turing-Maschine lässt sich innerhalb eines Goto-Programms durch eine Folge arithmetischer Operationen nachbilden.

Fügen wir die Puzzle-Stücke in der richtigen Art und Weise zusammen, so können wir jede Turing-Maschine mit Hilfe eines Goto-Programms simulieren. Wie in Abbildung 6.52 (links) skizziert, besteht das Programm auf der obersten Ebene aus drei sequenziell durchlaufenden Teilen. In  $P_1$  werden die intern verwendeten Variablen  $x_v$ ,  $x_\omega$  und  $x_s$  initialisiert. In  $P_3$  wird der Inhalt der Variablen analysiert und das berechnete Ergebnis in die AusgabevARIABLE  $x_0$  geschrieben. Beide Programmteile sind offensichtlich Goto-berechenbar, da sie lediglich eine Reihe von Umcodierungen vornehmen.

Die eigentliche Arbeit wird in Programmabschnitt  $P_2$  verrichtet (vgl. Abbildung 6.52 rechts). Zu Beginn wird mit Hilfe der Modulo-Operation der Index des Zeichens  $\sigma_1$  ermittelt und in der Variablen  $x_\sigma$  gespeichert. In Abhängigkeit von  $x_\sigma$  und dem Inhalt der Zustandsvariablen  $x_s$  springt das Programm eine bestimmte Marke an. Konkret im-



**Abbildung 6.52:** Jede Turing-Maschine lässt sich mit einem Goto-Programm simulieren.

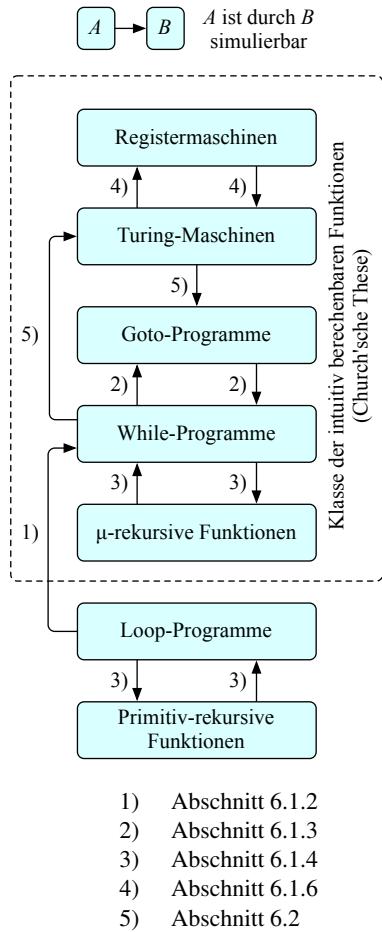
implementiert der Programmtext ab Marke  $M_{i(\sigma)}$  den Zustandsübergang  $\delta(s_i, \sigma)$  nach dem in Abbildung 6.51 entwickelten Schema.

Damit haben wir gezeigt, dass sich jede Turing-Maschine durch ein Goto-Programm simulieren lässt, und Satz 6.4 stellt sicher, dass auch die Übersetzung in ein While-Programm gelingt. Damit sind wir am Ziel unserer Überlegungen angekommen und dürfen den folgenden Satz in unseren Wissensfundus aufnehmen:

### Satz 6.8

Jede Turing-berechenbare Funktion ist While-berechenbar.

Zusammen beweisen die Sätze 6.7 und 6.8 die Äquivalenz zwischen While-Programmen und Turing-Maschinen. Beziehen wir die bisher erarbeiteten Äquivalenzen ebenfalls in die Betrachtung mit ein, so entsteht das in Abbildung 6.53 dargestellte Gesamtbild. Zwei Aspekte sind an dieser Stelle von besonderer Bedeutung:



**Abbildung 6.53:** Nahezu alle Berechnungsmodelle besitzen ihren äußerlichen Unterschieden zum Trotz exakt die gleiche Ausdrucksstärke. Diese empirische Beobachtung veranlasste Alonzo Church zur Formulierung seiner berühmten These.

So verschieden die Ansätze auch sind – nahezu alle Berechnungsmodelle besitzen die gleiche Ausdrucksstärke. Der Berechenbarkeitsbegriff bleibt damit stets derselbe, egal ob wir ihn über die While-Sprache, die Goto-Sprache, das Konzept der Turing-Maschine oder eines der anderen vorgestellten Modelle definieren. Eine Ausnahme bildet die Loop-Sprache. In Abschnitt 6.1.1 haben wir am Beispiel der Ackermann-Funktion gezeigt, dass diese ausdrucksschwächer ist als die While-Sprache.

In der Vergangenheit wurde mehrmals versucht, die Menge der berechenbaren Funktionen durch die Angabe eines ausdrucksstärkeren Berechnungsmodells zu vergrößern. Allen Anstrengungen zum Trotz wurde ein ausdrucksstärkeres Berechnungsmodell bis heute nicht gefunden. Selbst so ausgefallene Konzepte wie der *Quantenrechner* [72] oder das *DNA computing* [4] konnten die Grenze des maschinell Berechenbaren nicht verschieben.

Der amerikanische Mathematiker Alonzo Church sah darin eine empirische Bestätigung, dass der intuitive Berechenbarkeitsbegriff mit dem Begriff der Turing-Berechenbarkeit zusammenfällt. Genau dies ist der Inhalt der berühmten *Church'schen These*:

### Satz 6.9 (Church'sche These)

Die Klasse der Turing-berechenbaren Funktionen stimmt mit der Klasse der intuitiv berechenbaren Funktionen überein.

Der Begriff der *intuitiv berechenbaren Funktion* bedarf an dieser Stelle besonderer Aufmerksamkeit. Er bezeichnet eine Funktion, die von einem Menschen – in welcher Form auch immer – ausgerechnet werden kann. Damit besagt die Church'sche These nichts anderes, als dass jede Funktion, die überhaupt in irgendeiner Weise berechenbar ist, auch durch eine Turing-Maschine berechnet werden kann.

Die Church'sche These ist kein Satz im mathematisch präzisen Sinne, da der Begriff der intuitiv berechenbaren Funktion keine formale Definition besitzt. Gäbe es diese, so hätten wir uns – bewusst oder unbewusst – bereits auf ein konkretes Berechnungsmodell festgelegt und die eigentliche Bedeutung dieses Begriffs ad absurdum geführt. Folgerichtig wird es niemals möglich sein, die Church'sche These zu beweisen. Wir können lediglich Indizien für ihre Gültigkeit sammeln und genau dies ist Forschern in der Vergangenheit vielfach gelungen.

## 6.3 Akzeptierende Turing-Maschinen

In den bisherigen Betrachtungen haben wir die Turing-Maschine ausschließlich zur Berechnung von Funktionen eingesetzt. Durch die Interpretation als universeller Rechner sind wir dem Gedankengang gefolgt, den Alan Turing bei der Erschaffung seines Berechnungsmodells im Sinn hatte.

Betrachten wir ausschließlich die Arbeitsweise und nicht die Berechnungsstärke der Turing-Maschine, so entspricht sie in vielen Punkten dem *Transduktor* aus Abschnitt 5.6. In diesem Abschnitt wollen wir zeigen, wie wir Turing-Maschinen im Sinne von *Akzeptoren* verwenden können, die in der Diskussion über formale Sprachen eine dominierende Rolle spielten. Wir beginnen mit einer formalen Definition der von Turing-Maschinen akzeptierten Sprachen (vgl. Abbildung 6.54):



### Satz 6.10 (Turing-Akzeptanz)

Eine Turing-Maschine  $T = (S, \Sigma, \Pi, \delta, s_0, \square, E)$  akzeptiert das Eingabewort  $\omega \in \Sigma^*$ , falls sie unter Eingabe von  $\omega$  in einem Endzustand  $s_e \in E$  terminiert.

Die von  $T$  akzeptierte Sprache  $\mathcal{L}(T)$  ist wie folgt definiert:

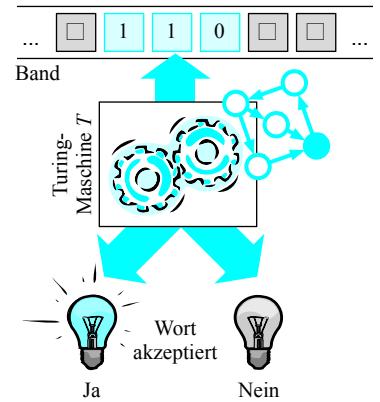
$$\mathcal{L}(T) := \{\omega \in \Sigma^* \mid T \text{ akzeptiert } \omega\}$$

Eine Sprache  $L$  heißt

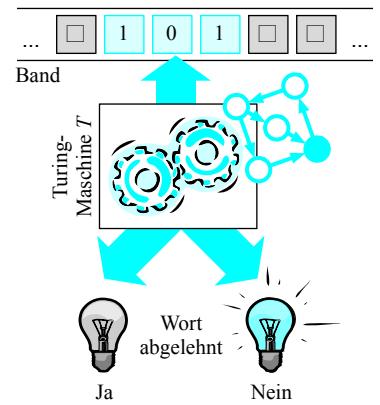
- *rekursiv aufzählbar*, falls eine Turing-Maschine  $T$  existiert, die  $L$  akzeptiert.
- *rekursiv*, falls eine Turing-Maschine  $T$  existiert, die  $L$  akzeptiert und zusätzlich für jede Eingabe terminiert.

Um zu testen, ob ein Wort  $\omega$  von einer Turing-Maschine  $T$  akzeptiert wird, müssen wir lediglich das Band mit  $\omega$  befüllen und  $T$  starten. Hält die Maschine nach endlich vielen Schritten in einem Endzustand an, so gilt  $\omega$  als akzeptiert. Terminiert  $T$  in einen Zustand  $s \notin E$ , so wird das Eingabewort  $\omega$  abgelehnt. Das Gleiche gilt für den Fall, dass  $T$  in einer Endlosschleife gerät und überhaupt nicht terminiert. Abbildung 6.55 fasst alle drei Fälle grafisch zusammen. Beachten Sie, dass die Akzeptanz eines Wortes  $\omega$  nur davon abhängt, ob der final eingenommene Zustand ein Endzustand ist. Der generierte Bandinhalt ist für die Akzeptanz von  $\omega$  bedeutungslos.

- Fall 1:  $\omega$  wird akzeptiert ( $\omega \in \mathcal{L}(T)$ )

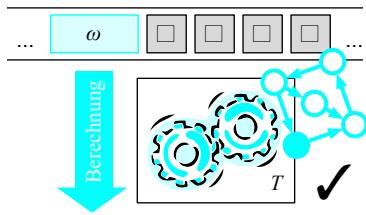


- Fall 2:  $\omega$  wird abgelehnt ( $\omega \notin \mathcal{L}(T)$ )



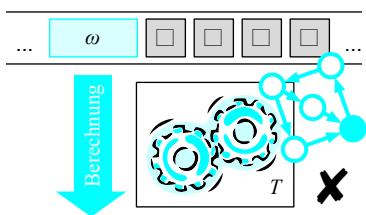
**Abbildung 6.54:** Die Turing-Maschine als Akzeptor

■ Fall 1



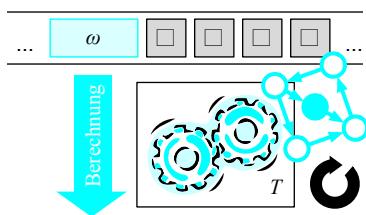
Die Turing-Maschine terminiert  
in einem Endzustand  $s \in E$   
 $\Rightarrow \omega \in \mathcal{L}(T)$

■ Fall 2



Die Turing-Maschine terminiert  
in einem Zustand  $s \notin E$   
 $\Rightarrow \omega \notin \mathcal{L}(T)$

■ Fall 3



Die Turing-Maschine gerät in  
eine Endlosschleife  
 $\Rightarrow \omega \notin \mathcal{L}(T)$

**Abbildung 6.55:** Arbeitsweise akzeptierender Turing-Maschinen

Bevor wir mit unseren Betrachtungen über Turing-akzeptierbare Sprachen fortfahren, wollen wir die bisher verwendete Definition der Übergangsfunktion  $\delta$  geringfügig auflockern. Genau wie im Falle des endlichen Automaten werden wir auch hier nichtdeterministische Zustandsübergänge zulassen und  $\delta$  zukünftig als *Übergangsrelation* bezeichnen. Die Turing-Maschine wird hierdurch um Entscheidungspunkte angereichert, die in Abhängigkeit der getätigten Auswahl zu unterschiedlichen Berechnungssequenzen führen. Analog zum Konzept des nichtdeterministischen endlichen Automaten wollen wir ein Wort  $\omega$  als akzeptiert ansehen, wenn mindestens eine Berechnungssequenz in einem Finalzustand endet.

Der Übergang von einer Übergangsfunktion zu einer Übergangsrelation  $\delta$  wirft die Frage auf, ob der hinzugefügte Nichtdeterminismus das Modell der akzeptierenden Turing-Maschine erweitert oder nur der Schreiberleichterung dient. Im Falle des endlichen Automaten haben wir herausgearbeitet, dass sich jeder nichtdeterministische Automat auf ein deterministisches Pendant reduzieren lässt. Wir werden nun zeigen, dass eine entsprechende Reduktion auch für Turing-Maschinen möglich ist – wenn auch nicht mit derselben Eleganz.

Der Kern der Reduktion basiert auf der Tatsache, dass der eingeschlagene Berechnungspfad an einem Entscheidungspunkt in nur endlich viele unterschiedliche Richtungen gelenkt werden kann. Die Endlichkeit hat zur Folge, dass wir jede terminierende Berechnungssequenz durch eine Zahlenfolge

$$e_1, \dots, e_n \text{ mit } 1 \leq e_i \leq w \quad (6.64)$$

repräsentieren können, in der  $n$  die Anzahl der getroffenen Entscheidungen und  $w$  die maximale Anzahl der Wahlmöglichkeiten bezeichnet. Obwohl unendlich viele Sequenzen der Form (6.64) existieren, lassen sie sich auf einfache Weise nacheinander berechnen. Für  $w = 2$  können wir die Sequenzen beispielsweise wie folgt aufzählen:

$$\{(1), (2), (1, 1), (1, 2), (2, 1), (2, 2), (1, 1, 1), (1, 1, 2), \dots\} \quad (6.65)$$

Wir werden nun eine deterministische Turing-Maschine konstruieren, die alle möglichen Berechnungspfade der Reihe nach simuliert. Hierzu erzeugt die Maschine alle endlichen Berechnungsfolgen der Form (6.64) und arbeitet diese anschließend nacheinander ab. Um die Konstruktion übersichtlich zu gestalten, verwenden wir eine 3-Band-Maschine (vgl. Abbildung 6.56). Band 1 – das Eingabeband – enthält eine Kopie des Eingabeworts  $\omega$  und bleibt während der gesamten Berechnung unverändert. Die anderen beiden Bänder werden benötigt, um

die möglichen Berechnungsfolgen der nichtdeterministischen Turing-Maschine nacheinander zu simulieren. In jeder Einzelsimulation werden drei Schritte durchlaufen:

- Im ersten Schritt wird die zu simulierende Berechnungsfolge auf Band 2 – dem Auswahlband – erzeugt. Hierzu generiert die Maschine nacheinander die in (6.64) beschriebenen Folgen.
- Im zweiten Schritt wird die Master-Kopie vom Eingabeband auf Band 3 – das Arbeitsband – kopiert.
- Jetzt wird auf dem Arbeitsband das Verhalten der nichtdeterministischen Maschine simuliert. In jedem Schritt entscheidet die Zahlenfolge auf Band 2 über den einzuschlagenden Berechnungspfad.

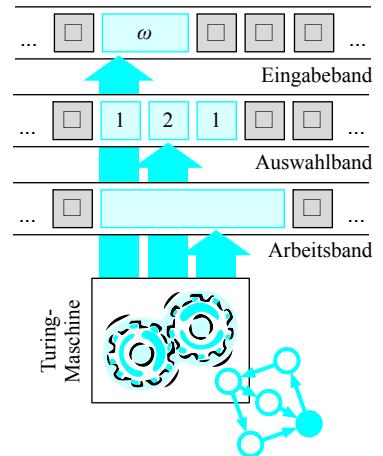
Terminiert die Maschine in einem Endzustand, so haben wir einen akzeptierenden Berechnungspfad gefunden und das Eingabewort ist ein Element der Sprache  $\mathcal{L}(T)$ . Enthält das Auswahlband eine Folge der Länge  $n$  und konnte nach  $n$  Schritten noch kein Endzustand erreicht werden, so wird die Simulation abgebrochen und der Vorgang mit der nächsten Berechnungsfolge wiederholt.

Auf diese Weise wird das Verhalten der nichtdeterministischen Maschine vollständig nachgeahmt. Akzeptiert diese das Wort  $\omega$ , so existiert ein akzeptierender Berechnungspfad. Dieser wird von der konstruierten deterministischen Maschine irgendwann simuliert und das Wort  $\omega$  ebenfalls akzeptiert. Wird  $\omega$  durch die nichtdeterministische Maschine nicht akzeptiert, so wird das deterministische Pendant eine Sequenz nach der anderen simulieren und stets scheitern. Die Maschine terminiert nicht und  $\omega$  ist kein Element der akzeptierten Sprachen. Damit haben wir den folgenden Satz bewiesen:

### Satz 6.11

Jede nichtdeterministische Turing-Maschine kann durch eine deterministische Turing-Maschine simuliert werden.

Wir werden die nichtdeterministische Turing-Maschine nun zum Erkennen von Sprachen einsetzen. Dabei wird sich das Maschinenmodell als leistungsfähiger erweisen, als es der erste Blick vermuten lässt. In der Tat werden wir zeigen, dass jede Typ-0-Sprache, d. h. jede Sprache, die sich generativ mit Hilfe einer Grammatik erzeugen lässt, durch eine Turing-Maschine akzeptiert werden kann.



**Abbildung 6.56:** Simulation einer nichtdeterministischen Turing-Maschine mit Hilfe einer deterministischen 3-Band-Maschine. Das Eingabeband enthält eine Master-Kopie des Eingabeworts  $\omega$  und wird nicht verändert. Auf dem Auswahlband werden nacheinander die Berechnungspfade erzeugt, die von der nichtdeterministischen Turing-Maschine durchlaufen werden können. Für jeden Pfad simuliert die Maschine das jeweilige Verhalten auf dem Arbeitsband und geht im Erfolgsfall in einen Endzustand über.

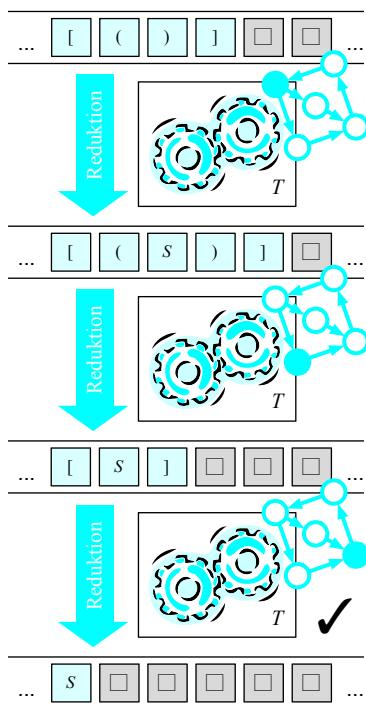
■ Grammatik  $G$

$$\begin{aligned} S &\rightarrow \epsilon \\ S &\rightarrow SS \\ S &\rightarrow [S] \\ S &\rightarrow (S) \end{aligned}$$

■ Wortproblem

Gilt  $[() \in \mathcal{L}(G)$ ?

■ Simulation



**Abbildung 6.57:** Für jede Typ-0-Sprache  $L$  existiert eine Turing-Maschine  $T$ , die  $L$  akzeptiert.

Für die nachstehenden Betrachtungen sei mit  $G = (V, \Sigma, P, S)$  eine beliebige Typ-0-Grammatik gegeben. Wie in Abschnitt 4.1 dargelegt, besteht die Sprache  $\mathcal{L}(G)$  aus allen Wörtern  $\omega \in \Sigma^*$ , die aus dem Startsymbol  $S$  ableitbar sind. Mit anderen Worten: Für jedes Wort  $\omega \in \mathcal{L}(G)$  existiert eine Ableitungssequenz der Form

$$S \rightarrow \omega_1 \rightarrow \omega_2 \rightarrow \dots \rightarrow \omega \quad (6.66)$$

mit  $\omega_i \in (\Sigma \cup V)^*$ . Um eine akzeptierende Turing-Maschine für  $\mathcal{L}(G)$  zu konstruieren, müssen wir die in (6.66) dargestellte Ableitungsrichtung umkehren: Genau dann, wenn es der Maschine gelingt, das Eingabewort  $\omega$  auf dem Band in das Startsymbol  $S$  zurückzuführen, wird es akzeptiert.

Die Rückführung wird durch die Tatsache erschwert, dass im Allgemeinen mehrere anwendbare Regeln zur Auswahl stehen. Durch die geleistete Vorarbeit können wir das Problem jedoch einfach lösen, indem wir die Turing-Maschine nichtdeterministisch konstruieren. Wir nutzen an dieser Stelle unser Wissen aus, dass zwischen nichtdeterministischen und deterministischen Maschinen kein prinzipieller Unterschied besteht.

Das Arbeitsprinzip der konstruierten Maschine folgt dem in Abbildung 6.57 skizzierten Schema. Initial wird das Eingabewort  $\omega$  auf das Band geschrieben und die Turing-Maschine gestartet. Diese wählt zunächst eine Produktion der Form  $v_1 \rightarrow v_2$  aus und sucht anschließend die Zeichenfolge  $v_2$  auf dem Eingabeband. Sowohl die Auswahl als auch die Suche geschehen nichtdeterministisch. Ist die Zeichenkette  $v_2$  nicht vorhanden, so terminiert die Turing-Maschine in einem Zustand außerhalb der Finalmenge, andernfalls wird  $v_2$  durch  $v_1$  ersetzt. Der Austausch muss mit Bedacht erfolgen, da  $v_2$  und  $v_1$  im Allgemeinen aus unterschiedlich vielen Symbolen bestehen. Folgerichtig muss ein Teil des Bandinhalts vor der Ersetzung um eine entsprechende Anzahl von Symbolen nach links oder rechts verschoben werden. Die Maschine geht in einen Endzustand über, sobald das Startsymbol  $S$  auf dem Eingabeband steht. Ist der Bandinhalt von  $S$  verschieden, so wird der gesamte Vorgang wiederholt. Durch die nichtdeterministische Konstruktion ist sichergestellt, dass  $S$  genau dann erzeugt werden kann, wenn eine Ableitungssequenz der Form (6.66) existiert. Damit ist die Gültigkeit des folgenden Satzes bewiesen:



**Satz 6.12**

Zu jeder Typ-0-Sprache  $L$  existiert eine Turing-Maschine, die  $L$  akzeptiert.

Handelt es sich bei  $G$  um eine kontextsensitive Grammatik, so gilt für alle Produktionen  $l \rightarrow r$  die Beziehung  $|l| \leq |r|$ . Da die simulierende Turing-Maschine  $T$  die Ersetzung in umgekehrter Richtung nachvollzieht, bewegt sich der Schreib-Lese-Kopf niemals über die Grenzen des Eingabeworts hinaus. Mit anderen Worten:  $T$  ist linear beschränkt. Damit haben wir ein weiteres wichtiges Resultat der Berechenbarkeitstheorie erzielt:



### Satz 6.13

Zu jeder Typ-1-Sprache  $L$  existiert eine nichtdeterministische, linear beschränkte Turing-Maschine, die  $L$  akzeptiert.

Anders als in Satz 6.12 dürfen wir auf den Zusatz „nichtdeterministisch“ nicht verzichten. Zwar haben wir gezeigt, dass sich jede nichtdeterministische Turing-Maschine durch eine deterministische simulieren lässt, allerdings ändert die von uns gezeigte Reduktion den benötigten Bandplatz. Die konstruierte Maschine ist damit nicht mehr linear beschränkt.

Die Umkehrung der Sätze 6.12 und 6.13 gilt ebenfalls, d.h., die von allgemeinen bzw. linear beschränkten Turing-Maschinen akzeptierten Sprachen gehen nicht über die Typ-0- bzw. die Typ-1-Sprachen hinaus.

Wir wollen nun grob skizzieren, wie sich ein Turing-Akzeptor  $T$  in eine äquivalente Grammatik  $G$  übersetzen lässt. Die Konstruktion basiert auf der Grundidee, die Konfigurationen von  $T$  vollständig in die Wortmenge von  $G$  hineinzucodieren. Ist  $T = (S, \Sigma, \Pi, \delta, s_0, \square, E)$  die zu simulierende Turing-Maschine und  $G = (V, \Sigma_G, P, S)$  die zu konstruierende Grammatik, dann wählen wir die Mengen  $V$  und  $\Sigma_G$  wie folgt:

$$V := (S \times \Pi), \quad \Sigma_G := \Pi. \quad (6.67)$$

Die Wahl ermöglicht uns, jede Konfiguration

$$((\rho_m \dots \rho_1), s, (\sigma_1 \dots \sigma_n)) \quad (6.68)$$

von  $T$  in das Wort

$$\rho_m \dots \rho_1(s, \sigma_1) \sigma_2 \dots \sigma_n \in (V \cup \Sigma_G)^* \quad (6.69)$$

zu übersetzen. Ferner zeigt Abbildung 6.58, wie die Übergangsrelation  $\delta$  in direkter Weise auf die Produktionenmenge  $P$  abgebildet werden kann. Die erzeugten Regeln sind so gestaltet, dass alle Berechnungsschritte von  $T$  eins zu eins nachgeahmt werden können. Fügen wir die Einzelteile in der richtigen Art und Weise zusammen, so entsteht eine Grammatik, die  $\mathcal{L}(T)$  nach dem folgenden Arbeitsprinzip erkennt:

#### ■ Reduktionsziel

Turing-Maschine  
 $T = (S, \Sigma, \Pi, \delta, s_0, \square, E)$



Grammatik  
 $G = (V, \Sigma_G, P, S)$

#### ■ Simulation der Linksbewegung

$$\delta(s, \sigma) = (s', \sigma', \leftarrow)$$



$$\rho(s, \sigma) \rightarrow (s', \rho) \sigma'$$

#### ■ Simulation der Rechtsbewegung

$$\delta(s, \sigma) = (s', \sigma', \rightarrow)$$



$$(s, \sigma) \rho \rightarrow \sigma' (s', \rho)$$

**Abbildung 6.58:** Um eine Turing-Maschine  $T$  in eine Grammatik  $G$  mit  $\mathcal{L}(T) = \mathcal{L}(G)$  zu übersetzen, wird die Übergangsrelation  $\delta$  eins zu eins auf die Produktionenmenge von  $G$  abgebildet.

In diesem Abschnitt haben wir herausgearbeitet, dass zwischen Typ-0- und Typ-1-Sprachen auf der einen Seite und den akzeptierenden Turing-Maschinen auf der anderen Seite ein enger Zusammenhang besteht. Insbesondere attestierte uns Satz 6.15, dass die Typ-1-Sprachen genau diejenigen sind, die sich von nichtdeterministischen, linear beschränkten Turing-Maschinen akzeptieren lassen. Auf das Wort „nichtdeterministisch“ können wir nicht ohne Weiteres verzichten, da die Methode, mit der wir einen nichtdeterministischen in einen deterministischen Turing-Akzeptor übersetzen haben, die Eigenschaft der linearen Beschränktheit zerstört. Natürlich wäre es trotzdem denkbar, dass eine Reduktion existiert, die einen nichtdeterministischen linear beschränkten Akzeptor (LBA) in einen deterministischen Akzeptor übersetzt und die Eigenschaft der linearen Beschränktheit bewahrt. Diese Fragestellung wird als *erstes LBA-Problem* bezeichnet.

Bis heute wartet das erste LBA-Problem auf seine Lösung. Würde es eine positive Antwort erfahren, so könnten wir das Wort „nichtdeterministisch“ in Satz 6.15 streichen. In diesem Fall wären die Klasse der Typ-1-Sprachen und die Klasse der linear beschränkten (deterministischen) Turing-Maschinen identisch.

Das erste LBA-Problem ist nicht zu verwechseln mit dem *zweiten LBA-Problem*. Hinter diesem verbirgt sich die Frage nach der Komplement-Abgeschlossenheit linear beschränkter Turing-Maschinen. Diese Eigenschaft bedeutet, dass mit jeder Sprache  $L \subseteq \Sigma^*$ , die von einer linear beschränkten Turing-Maschine akzeptiert wird, auch das Komplement  $\bar{L}$  von einem LBA akzeptiert wird. Seit seiner Formulierung in den Sechzigerjahren rechnete man fast 30 Jahre mit einer negativen Antwort. Erst im Jahre 1987 wurde das Rätsel um das zweite LBA-Problem gelüftet – zur Überraschung vieler mit einer positiven Antwort [51, 88].

- Im ersten Schritt wird die Startkonfiguration für ein beliebiges Wort  $\omega \in \Sigma_G^*$  abgeleitet. Hierzu wird die Produktionenmenge von  $P$  mit entsprechenden Regeln versehen.
- Ausgehend von den erzeugten Startkonfigurationen wird das Verhalten der Turing-Maschine simuliert. Die Grundlage hierfür bilden die in Abbildung 6.58 dargestellten Produktionen.
- Terminiert die simulierte Turing-Maschine in einem Finalzustand  $s \in E$ , so wird das Eingabewort  $\omega$  aus dem Konfigurationswort wiederhergestellt. Das entstehende Wort ist am Ende frei von Nonterminalzeichen und damit Bestandteil von  $\mathcal{L}(G)$ . Terminiert die Maschine in einem Zustand  $s \notin E$ , so unterbleibt die Rekonstruktion. Damit ist  $\omega$  nicht aus dem Startsymbol ableitbar und folglich kein Bestandteil von  $\mathcal{L}(G)$ . Gerät die Turing-Maschine in eine Endlosschleife, so produziert die Grammatik eine unendliche Ableitungssequenz. Dies ist ebenfalls gleichbedeutend mit  $\omega \notin \mathcal{L}(G)$ .

Jede von einer Turing-Maschine  $T$  akzeptierte Sprache  $L$  lässt sich somit von einer Typ-0-Grammatik erzeugen. In Kombination mit Satz 6.12 erhalten wir das folgende Ergebnis:



#### Satz 6.14 (Turing-Maschinen und Typ-0-Sprachen)

Die Klasse der Typ-0-Sprachen ist mit der Klasse der von Turing-Maschinen akzeptierten Sprachen identisch.

Der Zusammenhang zwischen der simulierten Turing-Maschine  $T$  und der erzeugten Grammatik  $G$  geht noch weiter. Ist  $T$  linear beschränkt, d. h., bewegt sich der Schreib-Lese-Kopf von  $T$  niemals über die Grenzen des Eingabeworts hinaus, so lässt sich die Grammatik so formulieren, dass alle Produktionen  $l \rightarrow r$  die Beziehung  $|l| \leq |r|$  erfüllen. Mit anderen Worten:  $G$  ist eine Typ-1-Grammatik. Beziehen wir die Aussage von Satz 6.13 mit ein, so ergibt sich der folgende Zusammenhang:



#### Satz 6.15 (Turing-Maschinen und Typ-1-Sprachen)

Die Klasse der Typ-1-Sprachen ist mit der Klasse der Sprachen identisch, die von nichtdeterministischen, linear beschränkten Turing-Maschinen akzeptiert werden.

Damit entpuppen sich die verschiedenen Varianten von Turing-Akzeptoren und Grammatiken als alternative Beschreibungsformen für exakt dieselben Sprachklassen.

## 6.4 Entscheidbarkeit

Nachdem wir in den vorangegangenen Abschnitten den Berechenbarkeitsbegriff formal erfasst haben, sind wir nun in der Lage, den bereits mehrfach gefallenen Begriff der *Entscheidbarkeit* ebenfalls auf ein stabiles Fundament zu stellen.



### Definition 6.15 (Entscheidbarkeit, Semi-Entscheidbarkeit)

Eine Menge  $M \subseteq T$  heißt *entscheidbar*, falls die *charakteristische Funktion*  $\chi_M : T \rightarrow \{0, 1\}$  mit

$$\chi_M(\omega) = \begin{cases} 1 & \text{falls } \omega \in M \\ 0 & \text{falls } \omega \notin M \end{cases}$$

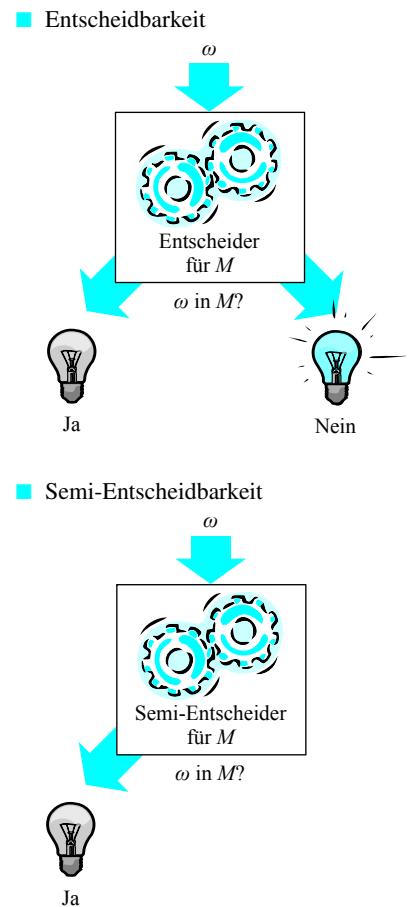
berechenbar ist.  $M$  heißt *semi-entscheidbar*, falls die *partielle charakteristische Funktion*  $\chi'_M : T \rightarrow \{1\}$  mit

$$\chi'_M(\omega) = \begin{cases} 1 & \text{falls } \omega \in M \\ \perp & \text{falls } \omega \notin M \end{cases}$$

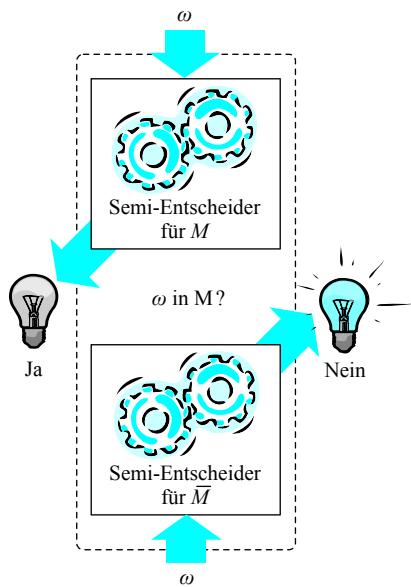
berechenbar ist.

Im Kern dieser Definition steht der Begriff der *charakteristischen Funktion*. Sie ist das formale Bindeglied zwischen dem auf Funktionen ausgelegten Berechenbarkeitsbegriff und dem für Mengen formulierten Entscheidbarkeitskriterium. Die Trägermenge  $T$  unterliegt keinen Einschränkungen und kann beliebig gewählt werden. Für die folgenden Betrachtungen werden wir zumeist eine Wortmenge ( $T = \Sigma^*$ ) oder die Menge der natürlichen Zahlen ( $T = \mathbb{N}$ ) zugrunde legen.

Abbildung 6.59 demonstriert, wie sich die beiden Entscheidbarkeitsbegriffe bildlich erfassen lassen. Für entscheidbare Mengen  $M$  existiert eine algorithmisch arbeitende Maschine, die ein Element  $\omega \in M$  entgegennimmt und die Frage beantwortet, ob  $\omega$  zu  $M$  gehört oder nicht. In der bildlichen Darstellung werden die beiden möglichen Antworten durch eine separate Glühlampe symbolisiert, von denen genau eine nach endlicher Zeit zu leuchten beginnt. Wann unsere gestellte Frage „Ist  $\omega \in M$ ?“ durch eine glühende Lampe beantwortet wird, steht in den Sternen. Nichtsdestotrotz ist sichergestellt, dass wir sowohl für den Fall  $\omega \in M$  als auch für den Fall  $\omega \notin M$  irgendwann eine Antwort erhalten werden. Wir müssen uns also lediglich ein wenig in Geduld üben und lange genug warten.



**Abbildung 6.59:** Bildliche Darstellung der Entscheidungsbegriffe



**Abbildung 6.60:** Sind sowohl  $M$  als auch das Komplement  $\bar{M}$  semi-entscheidbar, so lässt sich die Menge  $M$  entscheiden.

Im Gegensatz zu einem Entscheider besitzt ein *Semi-Entscheider* nur eine einzige Glühlampe. Wird er mit einem Element  $\omega \in M$  gestartet, so beginnt die Lampe nach endlicher Zeit zu leuchten. Für  $\omega \notin M$  lässt sich keine Aussage treffen, da wir nicht wissen können, ob sich die Maschine innerhalb einer Endlosschleife befindet oder zu einem späteren Zeitpunkt vielleicht doch noch eine positive Antwort liefern wird. Damit ist die Semi-Entscheidbarkeit gleichbedeutend mit einer Halbaussage. Die gestellte Frage „Ist  $\omega \in M$ ?“ wird nur im positiven Fall nach endlicher Zeit beantwortet. Fällt die Antwort negativ aus, so zeigt die Maschine keinerlei Reaktion.

In manchen Fällen reicht die Eigenschaft der Semi-Entscheidbarkeit trotzdem aus, um eine Menge  $M$  zu entscheiden. Dies ist immer dann der Fall, wenn neben  $M$  auch das Komplement  $\bar{M}$  semi-entscheidbar ist. Abbildung 6.60 zeigt auf grafische Weise, wie sich die Semi-Entscheider für  $M$  und  $\bar{M}$  zu einem Entscheider für  $M$  kombinieren lassen. Beide Semi-Entscheider werden mit dem Eingabewort  $\omega$  versorgt und parallel gestartet. Liegt  $\omega$  in  $M$ , so reagiert der erste Semi-Entscheider nach einer endlichen Zeitspanne. Ist  $\omega$  nicht in  $M$  enthalten, so wird dies durch den zweiten Semi-Entscheider irgendwann angezeigt. Damit haben wir einen konstruktiven Beweis für den folgenden Satz gefunden:

### Satz 6.16

Eine Menge  $M$  ist genau dann entscheidbar, wenn sowohl  $M$  als auch  $\bar{M}$  semi-entscheidbar sind.

Die eingeführten Entscheidbarkeitsbegriffe sind eng mit den Begriffen der *Abzählbarkeit* und der *Aufzählbarkeit* verwandt. Auch diese wollen wir formal einführen:



### Definition 6.16 (Abzählbarkeit, Aufzählbarkeit)

Eine Menge  $M$  heißt

- *abzählbar*, falls eine bijektive Abbildung  $f : \mathbb{N} \rightarrow M$  existiert.
- *aufzählbar*, falls  $M$  endlich ist oder eine berechenbare bijektive Abbildung  $f : \mathbb{N} \rightarrow M$  existiert.

Die Begriffe „*abzählbar*“ und „*aufzählbar*“ sind in der Literatur nicht einheitlich belegt. Schuld daran ist – zumindest teilweise – die englische Sprache, in der keine entsprechenden Bedeutungsabstufungen vorhanden sind. Dort werden abzählbare Mengen als *enumerable sets* und aufzählbare Mengen als *recursively enumerable sets* bezeichnet. In Anlehnung an die englischen Originalbegriffe wird der Zusatz *rekursiv* auch in deutschen Werken häufig übernommen und dann durchgängig von rekursiv aufzählbaren Mengen gesprochen.



Dem Begriff der Abzählbarkeit sind wir bereits in Kapitel 2 im Rahmen der Mächtigkeitsbetrachtungen verschiedener Mengen begegnet. Schon

dort haben wir eine Menge genau dann als abzählbar bezeichnet, wenn es möglich ist, die natürlichen Zahlen und die Elemente von  $M$  paarweise einander zuzuordnen. Die bijektive Abbildung  $f$  beschreibt, wie sich die Elemente gruppieren lassen, und liefert uns gleichzeitig eine auflistende Darstellung für  $M$ :

$$M = \{f(1), f(2), f(3), \dots\} \quad (6.70)$$

Beachten Sie, dass die Funktion  $f$  lediglich existieren, aber nicht zwangsläufig berechenbar sein muss. Ist Letzteres dennoch der Fall, so sprechen wir von einer *aufzählbaren* oder einer *rekursiv aufzählbaren* Menge. Plakativ gesprochen sind solche Mengen dadurch charakterisiert, dass wir deren Elemente der Reihe nach *aufsagen* können (vgl. Abbildung 6.61). Dies ist möglich, da  $f$  berechenbar ist und wir die Funktionswerte  $f(i)$  für  $i = 1, 2, 3, \dots$  daher nacheinander ausrechnen können.

Beachten Sie ferner, dass eine endliche Menge ebenfalls aufzählbar ist, eine abzählbare Menge aber stets unendlich viele Elemente besitzt. Streng genommen ist damit nicht jede aufzählbare Menge auch abzählbar. Beschränken wir uns jedoch auf die Betrachtung unendlicher Mengen, so gilt eine entsprechende Inklusionsbeziehung: Jede aufzählbare Menge mit unendlich vielen Elementen ist immer auch abzählbar.

Zwischen der Aufzählbarkeit und der Semi-Entscheidbarkeit einer Menge besteht eine Verwandtschaft, die sehr viel enger ist, als es der erste Blick vermuten lässt. Zunächst ist jede aufzählbare Menge  $M$  auch semi-entscheidbar, schließlich können wir alle Elemente der Reihe nach aufsagen und genau dann stoppen, wenn wir das gesuchte Element  $\omega$  gefunden haben. Ist  $\omega \in M$ , so werden wir das Element nach endlich vielen Schritten antreffen. Ist  $\omega \notin M$ , so fahren wir für immer fort.

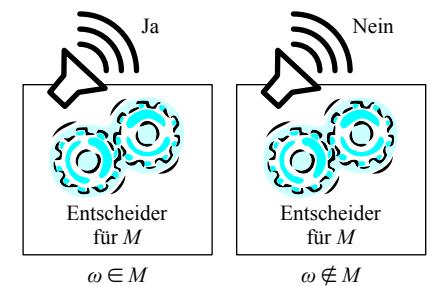
Interessanterweise gilt auch die umgekehrte Schlussrichtung: Jede semi-entscheidbare Menge  $M$  ist aufzählbar. Auf den ersten Blick erscheint unser Vorhaben gewaltig: Wir müssen einen Semi-Entscheider so ansteuern, dass er nacheinander die Elemente von  $M$  identifiziert, und gleichzeitig darauf achten, dass er niemals in eine Endlosschleife gerät. In den folgenden Ausführungen beschränken wir uns auf Mengen  $M$  mit  $M \subseteq \mathbb{N}$ ; die Ergebnisse lassen sich jedoch ohne große Änderungen auf beliebige abzählbare Mengen übertragen.

Zum Erfolg verhilft uns erneut die Cantor'sche Paarungsfunktion

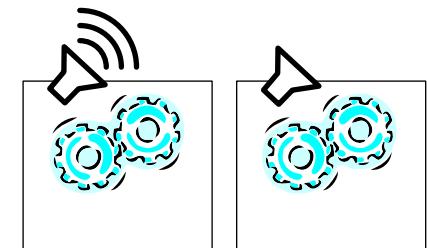
$$\pi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \quad (6.71)$$

aus Abschnitt 2.3.3.  $\pi$  stellt eine Zuordnung zwischen der Menge aller Tupel  $(i, j) \in \mathbb{N}^2$  und der Menge der natürlichen Zahlen her. Um eine semi-entscheidbare Menge  $M$  aufzuzählen, gehen wir wie folgt vor:

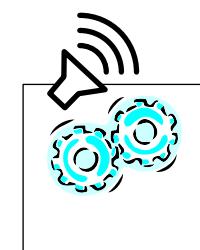
#### ■ Entscheidbarkeit



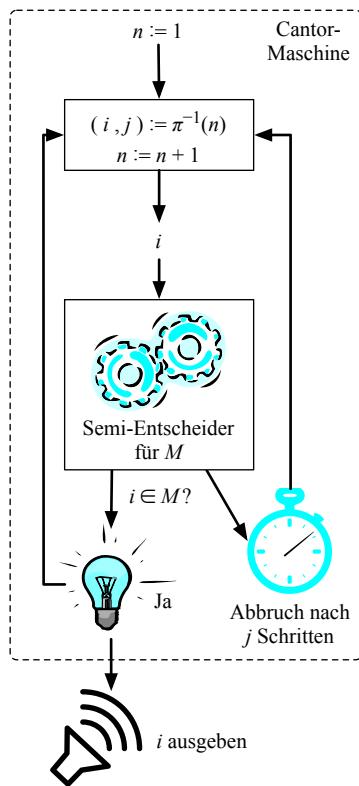
#### ■ Semi-Entscheidbarkeit



#### ■ Aufzählbarkeit



**Abbildung 6.61:** Entscheidbarkeit, Semi-Entscheidbarkeit und Aufzählbarkeit im Vergleich



**Abbildung 6.62:** Mit einigen Tricks und Kniffen ist es möglich, eine *Cantor-Maschine* zu konstruieren, die alle Elemente einer semi-entscheidbaren Menge nacheinander aufzählt.

- In einer unendlichen Schleife berechnen wir nacheinander die Elemente

$$\pi^{-1}(1), \pi^{-1}(2), \pi^{-1}(3), \dots \quad (6.72)$$

Als Ergebnis erhalten wir eine Folge, in der jedes Tupel  $(i, j) \in \mathbb{N}^2$  irgendwann auftaucht (vgl. Abbildung 6.62).

- Für jedes Tupel  $(i, j)$  starten wir den Semi-Entscheider mit der Eingabe  $i$ . Stellt dieser die Mengenzugehörigkeit innerhalb von  $j$  Schritten fest, so geben wir  $i$  aus und ignorieren alle weiteren Tupel, deren erste Komponente gleich  $i$  ist. Ist der Semi-Entscheider nach  $j$  Schritten noch zu keinem Ergebnis gekommen, brechen wir die Berechnung ab und fahren mit dem nächsten Tupel fort. Da für jede Zahl  $i \in M$  ein  $j \in \mathbb{N}$  mit der Eigenschaft existiert, dass der Semi-Entscheider die Mengenzugehörigkeit in  $j$  Schritten positiv beantwortet, werden nacheinander alle Elemente von  $M$  erzeugt.

Damit ist es uns gelungen, den folgenden Satz zu beweisen:

### Satz 6.17 (Aufzählbarkeit und Semi-Entscheidbarkeit)

Eine Menge  $M$  ist genau dann aufzählbar, wenn sie semi-entscheidbar ist.

Kombinieren wir die Aussagen der Sätze 6.16 und 6.17, so erhalten wir ohne weiteres Zutun das folgende Ergebnis:

### Korollar 6.3

Eine Menge  $M$  ist genau dann entscheidbar, wenn  $M$  und  $\overline{M}$  aufzählbar sind.

Beachten Sie, dass wir den Entscheidbarkeitsbegriff für Mengen formuliert haben, wir aber an vielen Stellen von entscheidbaren oder unentscheidbaren *Problemen* reden. Der Zusammenhang lässt sich einfach herstellen, indem wir für eine frei wählbare Trägermenge  $T$  und eine beliebige Eigenschaft  $E$  zunächst die folgende Menge definieren:

$$M_E := \{e \in T \mid e \text{ erfüllt die Eigenschaft } E\} \quad (6.73)$$

Das Problem „Erfüllt  $e$  die Eigenschaft  $E$ ?“ bezeichnen wir als entscheidbar, wenn die zugehörige Menge  $M_E$  entscheidbar ist. Über die gleiche Reduktion lässt sich der Begriff der Semi-Entscheidbarkeit übertragen.

## 6.5 Unentscheidbare Probleme

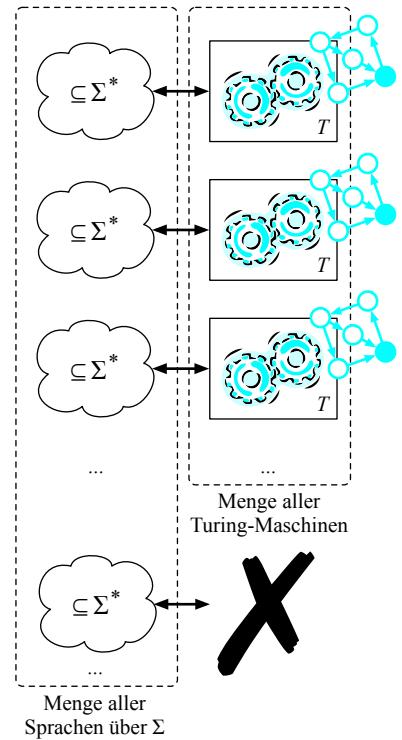
In diesem Abschnitt wollen wir uns einem der wichtigsten Erkenntnisse der Berechenbarkeitstheorie zuwenden. Die Rede ist von der Existenz unentscheidbarer Mengen oder gleichbedeutend: der Existenz unentscheidbarer Probleme. Für viele Software- und Hardware-Entwickler mag die Beschäftigung mit dieser Materie als wenig praxisrelevant erscheinen, schließlich können sich die wenigsten wissenschaftlich daran erinnern, mit einem unentscheidbaren Problem jemals konfrontiert gewesen zu sein.

Dass es unentscheidbare Probleme geben muss, ist nach den geleisteten Vorbereitungen aber leicht einzusehen. Ist eine Menge  $M \subseteq \Sigma^*$  entscheidbar, so existiert eine Turing-Maschine  $T_M$  zur Berechnung der charakteristischen Funktion  $\chi_M$ . Da nur abzählbar viele Turing-Maschinen existieren, können demzufolge auch nur abzählbar viele entscheidbare Mengen existieren. In Abschnitt 2.1.2 haben wir jedoch herausgearbeitet, dass die Menge  $2^\Sigma$  überabzählbar viele Elemente enthält. Plakativ gesprochen besagt dieses Ergebnis, dass nicht genug Turing-Maschinen zur Verfügung stehen, um alle Mengen  $M \subseteq \Sigma^*$  zu entscheiden (vgl. Abbildung 6.63). Damit ist die Existenz unentscheidbarer Mengen unausweichlich.

Die getätigte Überlegung wirft die Frage auf, warum wir in der Praxis dennoch selten auf unentscheidbare Probleme stoßen. Hauptverantwortlich ist die Tatsache, dass wir die Probleme, mit denen wir uns hauptsächlich beschäftigen, nicht zufällig wählen. Die meisten aus unserer Sicht *interessanten* Fragestellungen weisen eine vergleichsweise reguläre Struktur auf und sind aus diesem Grund sehr häufig entscheidbar. Nichtsdestotrotz werden die Beispiele in diesem Abschnitt die weitverbreitete Ansicht widerlegen, dass unentscheidbare Probleme ausschließlich pathologischer Natur sind. In der Tat reihen sich in diese Problemklasse viele Fragestellungen ein, die in der Praxis von handfestem Interesse sind. Die Konsequenzen der Berechenbarkeitstheorie sind damit weit mehr als mathematische Spielereien; sie zeigen uns unverrückbare Grenzen auf, die tief in die Praxis der modernen Soft- und Hardware-Entwicklung hineinreichen.

### 6.5.1 Halteproblem

Wir beginnen unsere Untersuchungen mit verschiedenen Varianten des *Halteproblems* für Turing-Maschinen. Anschließend werden wir mit den gewonnenen Ergebnissen den Satz von Rice beweisen. Dieser Satz



**Abbildung 6.63:** Es existieren überabzählbar viele Teilmengen von  $\Sigma^*$ , aber nur abzählbar viele Turing-Maschinen. Damit ist die Existenz unentscheidbarer Mengen unausweichlich.

**Tabelle 6.4:** Ein einfaches Diagonalisierungsargument zeigt die Unentscheidbarkeit des Halteproblems. In der dargestellten Tabelle sind horizontal alle Wörter  $\omega \in \Sigma^*$  und vertikal alle Turing-Maschinen aufgelistet. Der Tabelleneintrag  $(i, j)$  gibt Antwort auf die Frage, ob die Turing-Maschine  $T_i$  unter Eingabe von  $\omega_j$  hält. Wäre das Halteproblem entscheidbar, so ließe sich eine Turing-Maschine  $H'$  konstruieren, die den Diagonaleintrag  $(i, i)$  bestimmt und genau dann terminiert, wenn die gefundene Antwort „nein“ lautet.  $H'$  taucht aber nicht in der Liste auf, im Widerspruch zur Tabellenkonstruktion.

	$\omega_1$	$\omega_2$	$\omega_3$	$\omega_4$	$\omega_5$	$\omega_6$	$\omega_7$
$T_1$	ja	ja	nein	ja	nein	ja	nein
$T_2$	nein	ja	nein	ja	ja	nein	ja
$T_3$	ja	ja	nein	nein	nein	ja	ja
$T_4$	ja	nein	nein	ja	ja	ja	nein
$T_5$	ja	ja	nein	ja	nein	nein	nein
$T_6$	nein	nein	ja	ja	ja	nein	ja
$T_7$	nein	nein	ja	ja	ja	nein	nein

wird von so allgemeiner Natur sein, dass sich hieraus viele Aussagen der Berechenbarkeitstheorie fast von selbst ergeben.



### Definition 6.17 (Allgemeines Halteproblem)

Das *allgemeine Halteproblem* lautet wie folgt:

- Gegeben: Turing-Maschine  $T$  und Eingabewort  $\omega$
- Gefragt: Terminiert  $T$  unter Eingabe von  $\omega$ ?

Mit seiner wegbereitenden Arbeit aus dem Jahre 1936 zerschlug Turing alle Hoffnungen, das Halteproblem zu lösen.



### Satz 6.18 (Turing, 1936)

Das allgemeine Halteproblem ist unentscheidbar.

Die Aussage dieses Satzes ist weitreichend. Er besagt, dass kein systematisches Verfahren existieren kann, das für alle Turing-Maschinen  $T$  und alle Wörter  $\omega$  immer korrekt entscheidet, ob  $T$ , angewendet auf  $\omega$ , nach endlich vielen Schritten terminiert.

Für den Beweis der Unentscheidbarkeit nehmen wir an, dass ein Entscheidungsverfahren für das Halteproblem existiert, und führen die Annahme anschließend zu einem Widerspruch. Diesen werden wir

durch ein Diagonalisierungsargument herbeiführen, das jenem aus Abschnitt 2.3.3 sehr ähnlich ist. Dort haben wir das Prinzip der Diagonalisierung verwendet, um die Überabzählbarkeit der reellen Zahlen zu zeigen.

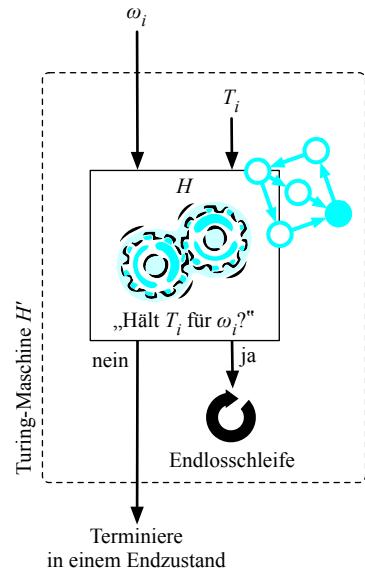
Damit wir das Diagonalisierungsargument anwenden können, konstruieren wir zunächst eine Matrix, wie sie in Tabelle 6.4 ausschnittsweise dargestellt ist. Auf der vertikalen Achse listen wir alle Turing-Maschinen auf. Wählen wir die Reihenfolge so, dass alle Maschinen anhand ihrer Gödelnummer in aufsteigender Reihenfolge angeordnet sind, so ist sichergestellt, dass sich jede Turing-Maschine eindeutig einer bestimmten Zeile zuordnen lässt und damit mit Sicherheit in der vorgenommenen Auflistung vorkommt. Auf der horizontalen Achse ordnen wir die Wortmenge  $\Sigma^*$  so an, dass jedes Element  $\omega \in \Sigma^*$  in einer bestimmten Spalte erscheint. Abschließend verzeichnen wir in der  $i$ -ten Zeile und der  $j$ -ten Spalte, ob die Turing-Maschine  $T_i$  unter Eingabe von  $\omega_j$  nach endlich vielen Schritten terminiert.

Wäre das Halteproblem entscheidbar, so würde eine Turing-Maschine  $H$  existieren, die neben einem Eingabewort  $\omega$  eine Turing-Maschine  $T$  in codierter Form entgegennimmt und stets korrekt bestimmt, ob  $T$  bei Eingabe von  $\omega$  terminiert. Die fiktive Turing-Maschine  $H$  ist nichts anderes als eine Maschine zur Berechnung der soeben konstruierten Matrix. Wie in Abbildung 6.64 skizziert, konstruieren wir aus  $H$  eine zweite Maschine  $H'$ . Diese berechnet für das Eingabewort  $\omega_i$  zunächst das Matrixelement  $(i, i)$  und verhält sich reziprok zu der erhaltenen Antwort. Hält die Maschine  $T_i$  bei Eingabe von  $\omega$  an  $((i, i) = „ja“)$ , so geht  $H'$  in eine Endlosschleife über. Rechnet  $T_i$  dagegen für immer weiter  $((i, i) = „nein“)$ , so terminiert  $H'$  in einem Finalzustand.

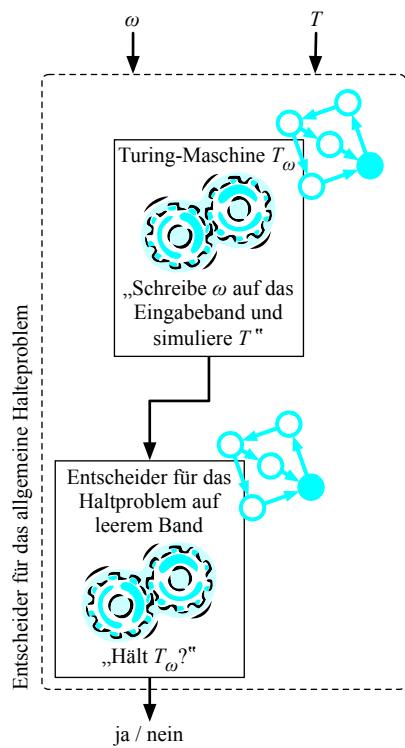
Da  $H'$  selbst eine Turing-Maschine ist, müssen wir sie in einer bestimmten Zeile unserer konstruierten Matrix vorfinden; der Aufbau der Matrix garantiert ja gerade, dass alle Maschinen der Reihe nach aufgezählt werden. Doch egal, in welcher Zeile wir auch nachschauen: Die Diagonalkonstruktion führt immer einen Widerspruch herbei. Für alle  $i \in \mathbb{N}$  gilt  $H' \neq T_i$ , da  $T_i$  die Eingabe  $\omega_i$  genau dann akzeptiert, wenn sie von  $H'$  abgelehnt wird. Der Widerspruch macht deutlich, dass wir die Annahme über die Existenz von  $H$  fallen lassen müssen und es keine Maschine geben kann, die das Halteproblem entscheidet.

## Halteproblem auf leerem Band

Neben dem allgemeinen Halteproblem existiert eine abgeschwächte Variante, die wie folgt definiert ist:



**Abbildung 6.64:** Gäbe es eine Turing-Maschine  $H$ , die das Halteproblem entscheidet, so könnten wir diese zu einer Maschine  $H'$  umbauen, die genau dann für das Eingabewort  $\omega_i$  terminiert, wenn die Turing-Maschine  $T_i$  bei Eingabe von  $\omega_i$  unendlich lange rechnet. Mit Hilfe des Diagonalisierungsarguments können wir die Konstruktion von  $H'$  als widersprüchlich entlarven und daraus schließen, dass die Maschine  $H$  nicht existieren kann.



**Abbildung 6.65:** Reduktion des allgemeinen Halteproblems auf das Halteproblem auf leerem Band. Wären wir in der Lage, das Halteproblem auf leerem Band zu lösen, so könnten wir einen Entscheider für das allgemeine Halteproblem konstruieren. Aus der Unentscheidbarkeit des allgemeinen Halteproblems folgt unmittelbar, dass auch das Halteproblem auf leerem Band nicht entschieden werden kann.



### Definition 6.18 (Halteproblem auf leerem Band)

Das *Halteproblem auf leerem Band* lautet wie folgt:

- Gegeben: Turing-Maschine  $T$
- Gefragt: Terminiert  $T$  mit der Eingabe  $\varepsilon$ ?

Während das allgemeine Halteproblem fordert, dass wir die Terminierungseigenschaft für beliebige Turing-Maschinen und beliebige Eingaben  $\omega$  entscheiden können, betrachtet das spezielle Halteproblem nur den Fall  $\omega = \varepsilon$ , d. h., ein entsprechender Algorithmus müsste das Verhalten einer Turing-Maschine nur für den Fall analysieren, dass sie mit einem leeren Band gestartet wird. Das spezielle Halteproblem ist damit augenscheinlich einfacher zu lösen als das allgemeine.

Nichtsdestotrotz reiht sich auch die abgeschwächte Variante in die Riege der unentscheidbaren Probleme ein. Dieses Ergebnis ist leicht einzusehen, da sich das allgemeine Halteproblem auf das Halteproblem auf leerem Band zurückführen lässt. Abbildung 6.65 zeigt, wie eine entsprechende Reduktion durchgeführt werden kann. Um zu entscheiden, ob eine Turing-Maschine für ein Eingabewort  $\omega \in \Sigma^*$  hält, konstruieren wir zunächst eine Turing-Maschine  $T_\omega$ , die alle Zeichen von  $\omega$  auf das Band schreibt und anschließend  $T$  simuliert.  $T_\omega$  wird mit einem leeren Band gestartet und terminiert genau dann, wenn die Originalmaschine  $T$  mit der Eingabe  $\omega$  terminiert. Gäbe es eine Turing-Maschine, die das Halteproblem auf leerem Band entscheidet, so wären wir demnach auch in der Lage, das allgemeine Halteproblem zu entscheiden. Aus Satz 6.18 folgt daher sofort, dass auch das spezielle Halteproblem unentscheidbar sein muss.



### Satz 6.19

Das Halteproblem auf leerem Band ist unentscheidbar.

## 6.5.2 Satz von Rice

Die Unentscheidbarkeit des Halteproblems hat uns gezeigt, dass Aussagen über Turing-Maschinen existieren, die sich einer maschinellen Beweisbarkeit entziehen. Kein algorithmisches Verfahren ist in der Lage, die Terminierungseigenschaft für alle Turing-Maschinen  $T_i$  und alle Eingabewörter  $\omega_j$  stets korrekt vorherzusagen. Durch eine geeignete

Reduktion waren wir darüber hinaus in der Lage, auch das Halteproblem auf leerem Band als unentscheidbar zu identifizieren. In diesem Abschnitt wollen wir uns mit der Frage beschäftigen, ob noch weitere Aussagen über Turing-Maschinen existieren, die nicht algorithmisch entschieden werden können. So viel vorweg: Wir werden eine verblüffende Antwort erhalten.

In den folgenden Betrachtungen bezeichnet  $E$  eine beliebige Eigenschaft, die eine Turing-Maschine besitzen kann oder nicht.  $E$  soll eine *nichttriviale* Eigenschaft sein, d. h., es gibt mindestens eine Maschine, die die untersuchte Eigenschaft besitzt, und mindestens eine Maschine, die sie nicht besitzt. Die folgende Aufzählung enthält eine exemplarische Auswahl möglicher Eigenschaften.

- $T$  berechnet eine konstante Funktion
- Alle Ausgaben von  $T$  sind mindestens  $n$  Zeichen lang
- $T$  berechnet eine totale Funktion
- $T$  generiert zweimal das gleiche Zeichen in Folge

Der Phantasie sind an dieser Stelle keine Grenzen gesetzt. Wir wollen nun ausloten, welche Konsequenzen sich aus der Existenz eines Entscheidungsverfahrens für  $E$  ergeben. Hierzu führen wir zunächst die Turing-Maschine  $T_{\perp}$  ein, die für keine Eingabe terminiert. Zugegebenermaßen ist  $T_{\perp}$  eine vergleichsweise langweilige Maschine, da sie die überall undefinierte Funktion berechnet. Für den Moment wollen wir annehmen, dass  $T_{\perp}$  die gewählte Eigenschaft  $E$  erfüllt. Da  $E$  nichttrivial ist, existiert mindestens eine weitere Maschine  $T_{\overline{E}}$ , die  $E$  nicht erfüllt. Wir fassen zusammen:

$$T_{\perp} \text{ erfüllt die Eigenschaft } E \quad (6.74)$$

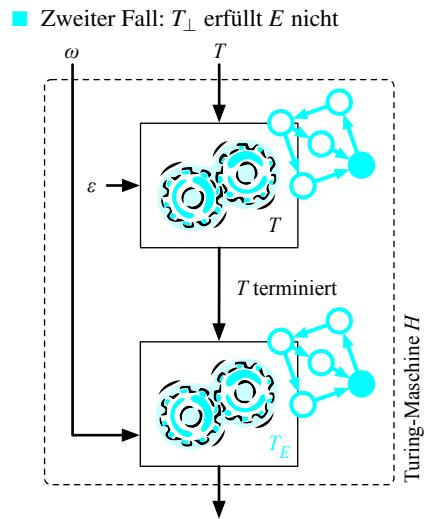
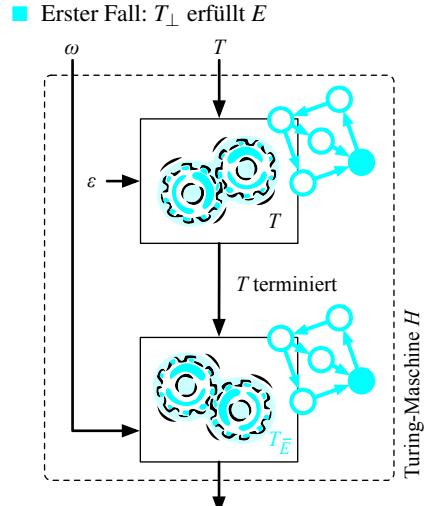
$$T_{\overline{E}} \text{ erfüllt die Eigenschaft } E \text{ nicht} \quad (6.75)$$

Wir konstruieren nun eine Maschine  $H$ , die eine Turing-Maschine  $T$  und ein Wort  $\omega$  als Eingabe entgegennimmt. Wie der obere Teil von Abbildung 6.66 zeigt, wird innerhalb von  $H$  zunächst die Maschine  $T$  mit dem leeren Eingabewort  $\varepsilon$  gestartet. Hält diese nach endlich vielen Schritten an, so wendet  $H$  die Maschine  $T_{\overline{E}}$  auf das Eingabewort  $\omega$  an.

Um das Verhalten von  $H$  zu verstehen, unterscheiden wir zwei Fälle:

- $T$  terminiert nicht

In diesem Fall ist  $H$  funktional identisch mit  $T_{\perp}$  und erfüllt die Eigenschaft  $E$ .



**Abbildung 6.66:** Kernstück des Beweises für den Satz von Rice. Über die dargestellte Zusammenschaltung wird ein direkter Zusammenhang zwischen der untersuchten Maschineneigenschaft  $E$  und der Terminierung von  $H$  hergestellt.

Der Satz von Rice macht alle Hoffnungen zunichte, nichttriviale Aussagen über Turing-Maschinen mit einem maschinell arbeitenden Verfahren beweisen zu können. Aufgrund der bewiesenen Äquivalenzen ist die Aussage nicht auf Turing-Maschinen beschränkt und lässt sich ohne Änderung auf die anderen Berechnungsmodelle übertragen. Die Grenzen, die uns der Satz von Rice auferlegt, reichen damit tief in die Praxis der realen Software-Entwicklung hinein. So folgt daraus unmittelbar, dass es keinen Algorithmus geben kann, der für ein beliebiges Programm maschinell verifiziert, ob es sich entsprechend seiner Spezifikation verhält. Selbst so einfache Probleme wie die Frage nach der Existenz von Endlosschleifen entziehen sich einer algorithmischen Lösung.

Im Bereich der Software-Verifikation wurden in der Vergangenheit zahlreiche Methoden und Verfahren entwickelt, die zum Ziel haben, gewisse Eigenschaften über Programme formal zu beweisen. Verliert die Software-Verifikation durch den Satz von Rice nicht auf einen Schlag ihre Berechtigung? Die Antwort ist Nein. Unbestritten folgt aus dem Satz von Rice, dass kein Verifikationswerkzeug existieren kann, das für *jedes* Programm die korrekte Antwort liefert. Er schließt jedoch nicht aus, dass Verfahren existieren, die für die *meisten* Programme oder vielleicht sogar für *alle praxisrelevanten* Programme korrekt arbeiten. In der Tat wurde in der Vergangenheit eine Vielzahl von Algorithmen entwickelt, die theoretisch betrachtet unvollständig sind, in der Praxis aber gut funktionieren.

Trotzdem lehrt uns die Berechenbarkeitstheorie, dass Programme existieren, für die jedes Verifikationswerkzeug versagen muss. Die Unvollständigkeit ist dabei kein Fehler in der Verifikations-Software; sie ist eine genauso fundamentale wie unvermeidliche Eigenschaft, die wir in der gleichen Weise akzeptieren müssen wie die Naturgesetze in der Physik.

#### ■ $T$ terminiert

In diesem Fall ist  $H$  funktional identisch mit  $T_{\overline{E}}$  und erfüllt die Eigenschaft  $E$  nicht.

Voilá. Mit der vorgenommenen Konstruktion ist es uns gelungen, einen direkten Zusammenhang zwischen der Eigenschaft  $E$  und der Terminierung von  $H$  herzustellen. Würde ein Verfahren existieren, das  $E$  entscheidet, so könnten wir  $H$  nach dem gezeigten Schema konstruieren und das Halteproblem für beliebige Turing-Maschine lösen.

Beachten Sie, dass die obige Überlegung stets unter der Annahme stand, dass die gewählte Eigenschaft  $E$  auf  $T_{\perp}$  zutrifft. Sollte dies nicht der Fall sein, so modifizieren wir die Maschine  $H$  wie in der unteren Hälfte von Abbildung 6.66 gezeigt. Anstelle von  $T_{\overline{E}}$  starten wir eine beliebige Maschine  $T_E$ , die  $E$  erfüllt. Die Fallunterscheidung liest sich jetzt wie folgt:

#### ■ $T$ terminiert nicht

In diesem Fall ist  $H$  funktional identisch mit  $T_{\perp}$  und erfüllt die Eigenschaft  $E$  nicht.

#### ■ $T$ terminiert

In diesem Fall ist  $H$  funktional identisch mit  $T_E$  und erfüllt die Eigenschaft  $E$ .

Wiederum ist es uns gelungen, einen Eins-zu-eins-Zusammenhang zwischen  $E$  und der Terminierung von  $T$  herzustellen. Gäbe es ein Entscheidungsverfahren für die Eigenschaft  $E$ , so könnten wir das Halteproblem ebenfalls lösen. Die bereits bewiesene Unentscheidbarkeit des Halteproblems führt damit unweigerlich zu der Erkenntnis, dass ein Entscheidungsverfahren für  $E$  nicht existieren kann. Genau dies ist die Aussage des berühmten Satzes von Henry Gordon Rice aus dem Jahre 1953.



### Satz 6.20 (Satz von Rice)

Mit  $E$  sei eine beliebige, nichttriviale Eigenschaft von Turing-Maschinen gegeben. Dann ist das folgende Problem unentscheidbar:

#### ■ Gegeben: Turing-Maschine $T$

#### ■ Gefragt: Besitzt $T$ die Eigenschaft $E$ ?

Die Tragweite des Satzes von Rice ist enorm. In einem Rundumschlag macht er die Hoffnung zunichte, irgendeine nichttriviale Eigenschaft über Turing-Maschinen algorithmisch entscheiden zu können. Seine Allgemeinheit macht diesen Satz zu einer der wertvollsten Aussagen der theoretischen Informatik – wenngleich wir uns alle sicher eine positivere Lösung der Berechenbarkeitsfrage gewünscht hätten.

### 6.5.3 Reduktionsbeweise

Erinnern Sie sich noch an den Unentscheidbarkeitsbeweis des Halteproblems auf leerem Band? Die Unentscheidbarkeit hatten wir nicht direkt bewiesen. Stattdessen zeigten wir, dass das Halteproblem auf leerem Band stark genug ist, um das allgemeine Halteproblem zu lösen. Mit anderen Worten: Wir hatten das allgemeine Halteproblem auf das Halteproblem auf leerem Band *reduziert*. Aus unserem Wissen über die Unentscheidbarkeit des allgemeinen Halteproblems konnten wir dann sofort schließen, dass auch das Halteproblem auf leerem Band unentscheidbar sein muss.

Die Reduktionstechnik ist in der Berechenbarkeitstheorie von so großer Bedeutung, dass wir sie in diesem Abschnitt in eine allgemein verwendbare Form bringen wollen. Wir beginnen mit der formalen Definition des bisher nur informell verwendeten Reduktionsbegriffs.

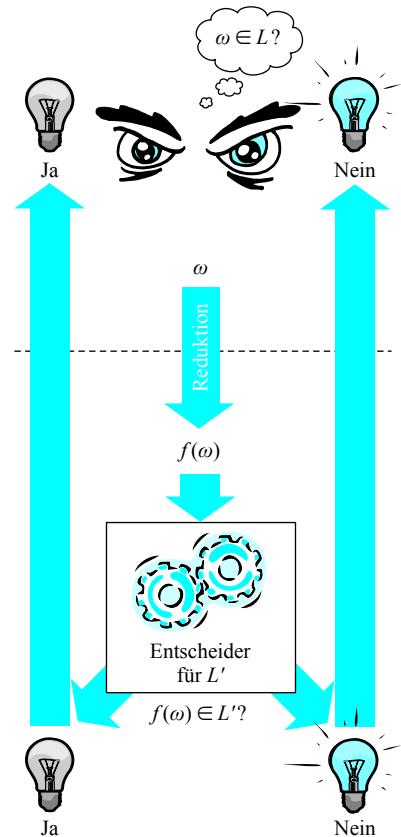


#### Definition 6.19 (Reduzierbarkeit)

Mit  $L \subseteq \Sigma^*$  und  $L' \subseteq \Gamma^*$  seien zwei Sprachen gegeben.  $L$  ist genau dann auf  $L'$  reduzierbar, geschrieben als  $L \leq L'$ , falls eine totale Funktion  $f : \Sigma^* \rightarrow \Gamma^*$  mit den folgenden Eigenschaften existiert:

- $f$  ist berechenbar
- $\omega \in L \Leftrightarrow f(\omega) \in L'$

Ist eine Sprache  $L$  auf eine andere Sprache  $L'$  reduzierbar, so sind wir in der Lage, die Frage  $\omega \in L$  durch eine äquivalente Frage über  $L'$  zu beantworten. Wie in Abbildung 6.67 gezeigt, berechnen wir hierzu zunächst das Element  $f(\omega)$ . Mit Hilfe dieses Elements können wir die Mengenzugehörigkeit durch ein Entscheidungsverfahren für  $L'$  beantworten. Vor allem aber erlaubt die Reduktionstechnik, die bewiesene Unentscheidbarkeit einer Sprache bzw. eines Problems  $L$  auf eine andre Sprache bzw. ein anderes Problem  $L'$  zu übertragen. Unsere Überlegungen offenbaren den folgenden Zusammenhang:



**Abbildung 6.67:** Die Reduktionstechnik in Aktion. Um die Mengenzugehörigkeit  $\omega \in L$  zu entscheiden, wird zunächst das Element  $f(\omega)$  berechnet und anschließend die Frage  $f(\omega) \in L'$  beantwortet.

■ Alphabet

$$\Sigma := \{0, 1\}$$

■ Wortpaare

$$\begin{array}{l} (01 \quad , \quad 1) \\ (0 \quad , \quad 000) \\ (01000 \quad , \quad 01) \end{array}$$

■ Lösung

$$01000 \boxed{0} \boxed{0} \boxed{01}$$

$$\boxed{01} \boxed{000} \boxed{000} \boxed{1}$$

**Abbildung 6.68:** Das Post'sche Korrespondenzproblem besitzt für die dargestellte Instanz eine Lösung.



**Satz 6.21**

Ist  $L$  eine unentscheidbare Sprache, so ist jede Sprache  $L'$  mit  $L \leq L'$  ebenfalls unentscheidbar.

Haben wir also erst einmal eine Reihe von unentscheidbaren Sprachen oder Problemen gefunden, so können wir diese mit Hilfe der Reduktionstechnik um weitere ergänzen. Achten Sie stets darauf, die Richtung der Reduktion nicht zu verwechseln. Die Unentscheidbarkeit einer Sprache  $L'$  wird bewiesen, indem eine unentscheidbare Sprache  $L$  auf  $L'$  reduziert wird und nicht umgekehrt. In unserem obigen Beweis haben wir exakt diese Reihenfolge eingehalten: Wir haben das allgemeine Halteproblem auf das Halteproblem auf leerem Band reduziert.

### 6.5.4 Das Post'sche Korrespondenzproblem

In diesem Abschnitt wenden wir uns dem *Post'schen Korrespondenzproblem* zu. Es wurde im Jahre 1946 von dem polnisch-US-amerikanischen Mathematiker Emil Leon Post formuliert und gehört heute zu den wichtigsten unentscheidbaren Problemen. Seine Bedeutung beruht weniger auf seiner inhaltlichen Aussage, sondern in erster Linie auf der Eigenschaft, dass es sich vergleichsweise einfach auf andere Probleme reduzieren lässt. In dieser Funktion gehört das Post'sche Korrespondenzproblem zu den wichtigsten Instrumenten für das Führen von Unentscheidbarkeitsbeweisen.

■ Alphabet

$$\Sigma := \{0, 1\}$$

■ Wortpaare

$$\begin{array}{l} (011 \quad , \quad 100) \\ (11 \quad , \quad 110) \\ (010 \quad , \quad 011) \end{array}$$

■ Lösung müsste wie folgt beginnen

$$\boxed{11} \boxed{?} \boxed{?} \dots$$

$$\boxed{110} \boxed{?} \boxed{?} \dots$$

**Abbildung 6.69:** Das Post'sche Korrespondenzproblem besitzt für die dargestellte Instanz eine negative Lösung.



**Definition 6.20 (Post'sches Korrespondenzproblem)**

Das *Post'sche Korrespondenzproblem* (*Post's Correspondence Problem*, kurz PCP) lautet wie folgt:

- Gegeben: Wortpaare  $(x_1, y_1), \dots, (x_n, y_n)$  mit  $x_i, y_i \in \Sigma^+$
- Gefragt: Gibt es eine Folge  $i_1, \dots, i_k$  mit der Eigenschaft

$$x_{i_1} x_{i_2} \dots x_{i_k} = y_{i_1} y_{i_2} \dots y_{i_k}?$$

Abbildung 6.68 veranschaulicht das Post'sche Korrespondenzproblem anhand einer Tupelfolge mit drei Wortpaaren. Unsere Aufgabe ist es herauszufinden, ob wir die linken und rechten Komponenten im Sinne

■ Wortpaare

$(001, 0), (01, 011), (01, 101), (10, 001)$

■ Erste Sequenz

01	10	01	10	10	01	001	01	10	01	10	01	10	01	10	01	10	01	10	01	001	10	10
01	001	01	10	001	001	01	10	10	10	01	001	01	001	001	001	001	001	01	10	01	10	
001	01	001	10	10	01	001	10	001	001	01	10	001	001	01	001	001	001	01	001	001	01	001
01	001	10	001	001	01																	

■ Zweite Sequenz

011	001	101	001	001	011	0	011	001	101	001	101	001	001	101	001	101	001	001	101	001	001
011	0	001	001	011	0	101	001	0	0	101	001	001	001	001	011	0	011	0	0	0	0
101	001	101	001	0	011	0	001	001	011	0	001	0	0	101	001	0	0	101	0	0	0
101	0	011	0	001	0	0	101														

**Abbildung 6.70:** Auch diese Instanz des Post'schen Korrespondenzproblems besitzt eine Lösung.

von Definition 6.20 zu zwei gleichen Wortketten zusammenfügen können. Wie in der Abbildung gezeigt, besitzt die abgebildete Instanz des Korrespondenzproblems in der Tat eine Lösung.

In Abbildung 6.69 ist eine zweite Probleminstanz dargestellt, die keine Lösung besitzt. Verglichen mit dem ersten Beispiel müssen wir allerdings ein wenig tiefgründiger argumentieren, schließlich gilt es zu zeigen, dass sich alle bildbaren Wortketten voneinander unterscheiden. Auf den ersten Blick ist dies kein leichtes Unterfangen, da die Längen der erzeugbaren Symbolketten nicht nach oben beschränkt sind. Auf den zweiten Blick wird trotzdem deutlich, warum die abgebildete Probleminstanz keine Lösung besitzt. Gäbe es eine Lösung, so müsste die erste Kette mit 11 und die zweite Kette mit 110 beginnen; alle anderen Kombinationen führen unmittelbar zu verschiedenen Symbolsequenzen. Da jetzt die erste Kette die Kürzere ist, muss die zweite Kette das fehlende Zeichen irgendwann wieder aufholen. Dies ist jedoch unmöglich, da die rechte Seite in allen Wortpaaren genauso viele oder mehr Zeichen enthält als die linke.

Dass sich das Post'sche Korrespondenzproblem selbst für harmlos anmutende Wortpaare oft nur schwer lösen lässt, verdeutlicht das Beispiel

■ MPCP-Instanz

Alphabet:

$$\Sigma := \{0, 1\}$$

Tupelfolge:

$$\begin{array}{ll} (011 & , \quad 100) \\ (11 & , \quad 110) \\ (010 & , \quad 011) \end{array}$$



■ PCP-Instanz

Alphabet:

$$\Sigma := \{0, 1\} \cup \{\sqsubset, \sqsupset\}$$

Tupelfolge:

$$\begin{array}{ll} (\sqsubset 0 \sqsubset 1 \sqsubset 1 \sqsubset & , \quad \sqsubset 1 \sqsubset 0 \sqsubset 0) \\ (1 \sqsubset 1 \sqsubset & , \quad \sqsubset 1 \sqsubset 1 \sqsubset 0) \\ (0 \sqsubset 1 \sqsubset 0 \sqsubset & , \quad \sqsubset 0 \sqsubset 1 \sqsubset 1) \\ (\sqsupset & , \quad \sqsupset \sqsupset) \end{array}$$

**Abbildung 6.71:** Transformation einer MPKP-Instanz in eine äquivalente PKP-Instanz. Die neu hinzugefügten Symbole  $\sqsubset$  und  $\sqsupset$  sorgen dafür, dass die konstruierten Ketten immer mit dem ersten Wortpaar beginnen müssen.

in Abbildung 6.70. Es stammt aus [82] und ist so konstruiert, dass erst nach 66 Zusammenfügungen zwei identische Zeichenketten entstehen.

Bevor wir die Unentscheidbarkeit des Post'schen Korrespondenzproblems beweisen, führen wir noch eine leicht modifizierte Variante ein.



### Definition 6.21 (Modifiziertes Korrespondenzproblem)

Das *modifizierte Korrespondenzproblem (Modified Post's Correspondence Problem, kurz MPCP)* lautet wie folgt:

- Gegeben: Wortpaare  $(x_1, y_1), \dots, (x_n, y_n)$  mit  $x_i, y_i \in \Sigma^+$
- Gefragt: Gibt es eine Folge  $i_2, \dots, i_k$  mit der Eigenschaft

$$x_1 x_{i_2} \dots x_{i_k} = y_1 y_{i_2} \dots y_{i_k}?$$

Das modifizierte Korrespondenzproblem unterscheidet sich in einem nahezu unscheinbaren Punkt. Während die zu bildenden Ketten in der allgemeinen Variante mit einem beliebigen Wortpaar  $(x_{i_1}, y_{i_1})$  gestartet werden können, müssen sie in der modifizierten Variante immer mit dem Wortpaar  $(x_1, y_1)$  beginnen.

Wie Sie vielleicht schon vermuten, gilt  $\text{MPCP} \leq \text{PCP}$ , d. h., wir sind in der Lage, das modifizierte Korrespondenzproblem mit Hilfe der allgemeinen Variante zu lösen. Bevor wir eine entsprechende Reduktion konstruieren, wollen wir die Ausgangssituation nochmals rekapitulieren. Wir unterscheiden zwei Fälle:

- PCP besitzt für  $(x_1, y_1), \dots, (x_n, y_n)$  keine Lösung. In diesem Fall können die  $x$ - und  $y$ -Komponenten der gegebenen Worttupel nicht zu einer gleichlautenden Zeichensequenz kombiniert werden. Damit existiert erst recht keine Kombination, die  $x_1$  und  $y_1$  als Erstes verwendet. Folgerichtig besitzt auch MPCP für die gegebene Tupelfolge keine Lösung.
- PCP besitzt für  $(x_1, y_1), \dots, (x_n, y_n)$  eine Lösung. In diesem Fall existiert mindestens eine Indexfolge  $i_1, \dots, i_k$  mit  $x_{i_1}, \dots, x_{i_k} = y_{i_1}, \dots, y_{i_k}$ . Gilt für alle Indexfolgen die Beziehung  $i \neq 1$ , so besitzt zwar das PCP-Problem eine Lösung, nicht jedoch das MPCP-Problem.

Die Reduktion von MPCP auf PCP muss so erfolgen, dass jede PCP-Lösung zwangsläufig mit dem Paar  $(x_1, y_1)$  beginnen muss. In der Tat

sind wir mit einem kleinen Trick in der Lage, dies zu erreichen. Hierzu ergänzen wir das Alphabet  $\Sigma$  um zwei neue Symbole und modifizieren die Wortpaare  $(x_i, y_i)$  so, dass sich  $x_i$  und  $y_i$  für  $i \neq 1$  im ersten Symbol unterscheiden (vgl. Abbildung 6.71). Beachten Sie, dass die Lösbarkeit des Korrespondenzproblems durch die Modifikation nicht beeinflusst wird: Das MPCP-Problem ist für eine Wortfolge  $W$  genau dann lösbar, wenn es für die modifizierte Folge  $W'$  lösbar ist. Da jetzt jede PCP-Lösung von  $W'$  zwangsläufig mit dem Paar  $(x_1, y_1)$  beginnen muss, erhalten wir den folgenden Zusammenhang:

- Das MPCP-Problem besitzt für  $W$  eine Lösung
- $\Leftrightarrow$  Das MPCP-Problem besitzt für  $W'$  eine Lösung
- $\Leftrightarrow$  Das PCP-Problem besitzt für  $W'$  eine Lösung

Damit sind wir unserem Ziel, die Unentscheidbarkeit von PCP zu beweisen, einen großen Schritt näher gekommen. Nach Satz 6.21 reicht es aus, die Unentscheidbarkeit des einfacheren MPCP-Problems zu zeigen. Die konstruierte Reduktion sorgt dafür, dass sich das Ergebnis in direkter Weise auf das allgemeine Korrespondenzproblem überträgt.

Die Unentscheidbarkeit von MPCP lässt sich durch die Reduktion des Halteproblems auf leerem Band beweisen. Hierzu sei mit  $T = (S, \Sigma, \Pi, \delta, s_0, \square, E)$  eine beliebige Turing-Maschine gegeben. Wir werden zeigen, dass wir das Halteproblem lösen können, wenn es einen Entscheider für MPCP gäbe. Die Grundidee ist dabei bestechend einfach: Wir werden für die Maschine  $T$  eine MPCP-Instanz konstruieren, die ihr Verhalten nachahmt. Die Tupelfolge  $(x_1, y_1), \dots, (x_k, y_k)$  setzt sich aus den folgenden Wortpaaren zusammen:

- Startpaar  
 $((\varepsilon), (\varepsilon)\langle \kappa_0 \rangle)$
- Übergangspaare  
 $((\kappa_i), (\kappa_j))$  für alle Konfigurationsübergänge  $\kappa_i \rightarrow \kappa_j$
- Abschlusspaare  
 $((\kappa_e)\langle \varepsilon \rangle, \langle \varepsilon \rangle)$  für alle Endkonfigurationen  $\kappa_e$

Um die Idee dieser Konstruktion zu verstehen, nehmen wir an, die Turing-Maschine  $T$  durchläuft nacheinander die Konfigurationen  $\kappa_0, \kappa_1, \kappa_2, \kappa_3$ . Abbildung 6.72 zeigt, wie die Konfigurationsübergänge innerhalb der MPCP-Instanz nachgebildet werden und sich die gebildeten Wortketten in jedem Schritt verlängern. Von entscheidender Bedeutung ist die Eigenschaft, dass die obere Kette der unteren um eine Konfiguration hinterherhinkt. Terminiert  $T$  nicht, so geht die Konstruktion

- Initialkonfiguration:  $\kappa_0$

$x : \langle \varepsilon \rangle$

$y : \langle \varepsilon \rangle \langle \kappa_0 \rangle$

- Übergang von  $\kappa_0$  auf  $\kappa_1$

$x : \langle \varepsilon \rangle \langle \kappa_0 \rangle$

$y : \langle \varepsilon \rangle \langle \kappa_0 \rangle \langle \kappa_1 \rangle$

- Übergang von  $\kappa_1$  auf  $\kappa_2$

$x : \langle \varepsilon \rangle \langle \kappa_0 \rangle \langle \kappa_1 \rangle$

$y : \langle \varepsilon \rangle \langle \kappa_0 \rangle \langle \kappa_1 \rangle \langle \kappa_2 \rangle$

- Übergang von  $\kappa_2$  auf  $\kappa_3$

$x : \langle \varepsilon \rangle \langle \kappa_0 \rangle \langle \kappa_1 \rangle \langle \kappa_2 \rangle$

$y : \langle \varepsilon \rangle \langle \kappa_0 \rangle \langle \kappa_1 \rangle \langle \kappa_2 \rangle \langle \kappa_3 \rangle$

- Abschluss, falls  $\kappa_3$  Endzustand ist

$x : \langle \varepsilon \rangle \langle \kappa_0 \rangle \langle \kappa_1 \rangle \langle \kappa_2 \rangle \langle \kappa_3 \rangle \langle \varepsilon \rangle$

$y : \langle \varepsilon \rangle \langle \kappa_0 \rangle \langle \kappa_1 \rangle \langle \kappa_2 \rangle \langle \kappa_3 \rangle \langle \varepsilon \rangle$

**Abbildung 6.72:** Das Verhalten einer Turing-Maschine lässt sich mit Hilfe von Wortsequenzen nachbilden. Die Abschlussregeln werden dabei so gewählt, dass die untere Sequenz die obere genau dann einholen kann, wenn die simulierte Turing-Maschine terminiert.

■ PCP-Instanz

$$(x_1, y_1), \dots, (x_n, y_n), \quad x_i, y_i \in \Sigma^+$$



■ Grammatik  $G_1$

$$G_1 := (S_{G_1}, \Sigma_{G_1}, P_{G_1}, s_{G_1})$$

$$S_{G_1} := \{S_1\}$$

$$s_{G_1} := S_1$$

$$\Sigma_{G_1} := \Sigma \cup \{i_1, \dots, i_n\}$$

■ Produktionenmenge  $P_{G_1}$

$$S_1 \rightarrow i_1 x_1 \mid \dots \mid i_n x_n$$

$$S_1 \rightarrow i_1 S_1 x_1 \mid \dots \mid i_n S_1 x_n$$

■ Grammatik  $G_2$

$$G_2 := (S_{G_2}, \Sigma_{G_2}, P_{G_2}, s_{G_2})$$

$$S_{G_2} := \{S_2\}$$

$$s_{G_2} := S_2$$

$$\Sigma_{G_2} := \Sigma \cup \{i_1, \dots, i_n\}$$

■ Produktionenmenge  $P_{G_2}$

$$S_2 \rightarrow i_1 y_1 \mid \dots \mid i_n y_n$$

$$S_2 \rightarrow i_1 S_2 y_1 \mid \dots \mid i_n S_2 y_n$$

**Abbildung 6.73:** Reduktion von PCP auf das Schnittproblem kontextfreier Sprachen

beliebig weiter und die erste Kette wird ständig eine Konfiguration voraus sein. Kurzum: Die MPCP-Instanz besitzt keine Lösung. Terminiert  $T$ , so kommen die Abschlussregeln ins Spiel. Diese sind so konstruiert, dass die obere Kette den fehlenden Konfigurationsübergang aufholt. Mit anderen Worten: Nach der Anwendung einer Abschlussregel sind die gebildeten Ketten identisch und die MPCP-Instanz lösbar. Insgesamt haben wir damit einen direkten Zusammenhang zwischen der Lösbarkeit von MPCP und der Terminierung von Turing-Maschinen hergestellt. Wäre MPCP entscheidbar, so könnten wir auch das Halteproblem entscheiden – im Widerspruch zu unseren bisherigen Erkenntnissen.

Die Beweisskizze bringt die Kernidee der Reduktion gut zum Vorschein, wenngleich in sehr informeller Weise. Um den Beweis in mathematischer Präzision zu führen, müssen wir zusätzlich zeigen, wie sich die Konfigurationen  $\kappa_i$  textuell beschreiben lassen. In der obigen Beweisskizze sind wir einfach stillschweigend davon ausgegangen, dass eine entsprechende Codierung existiert. Die Abstraktion wurde an dieser Stelle bewusst vorgenommen, um die Kernidee des Beweises klar herauszuschälen. Eine mathematisch präzise Ausführung der umrissenen Beweisidee findet sich z. B. in [50].

## 6.5.5 Weitere unentscheidbare Probleme

In diesem Abschnitt werden wir unser Wissen über das Post'sche Korrespondenzproblem nutzen, um weitere Probleme als unentscheidbar zu identifizieren. Konkret handelt es sich um Probleme aus dem Bereich der formalen Sprachen, die wir in Kapitel 4 ausführlich diskutiert haben. Im Einzelnen werden wir die Unentscheidbarkeit der folgenden Probleme beweisen:

■ Schnittproblem für kontextfreie Grammatiken

Gegeben: Kontextfreie Grammatiken  $G_1$  und  $G_2$

Gefragt:  $\mathcal{L}(G_1) \cap \mathcal{L}(G_2) \neq \emptyset$ ?

■ Mehrdeutigkeitsproblem für kontextfreie Grammatiken

Gegeben: Kontextfreie Grammatik  $G$

Gefragt: Besitzt jedes Wort  $\omega \in \mathcal{L}(G)$  eine eindeutige Ableitung?

■ Leerheitsproblem für kontextsensitive Grammatiken

Gegeben: Kontextsensitive Grammatik  $G$

Gefragt:  $\mathcal{L}(G) \neq \emptyset$ ?

Als Erstes werden wir die Unentscheidbarkeit des Schnittproblems kontextfreier Sprachen durch die Reduktion des Post'schen Korrespondenzproblems beweisen. Hierzu bilden wir die Tupelfolge  $(x_1, y_1), \dots, (x_n, y_n)$  einer gegebenen Instanz des Korrespondenzproblems so auf zwei Grammatiken  $G_1$  und  $G_2$  ab, dass die folgende Beziehung gewährleistet ist:

$$\text{PCP-Instanz hat eine Lösung} \Leftrightarrow \mathcal{L}(G_1) \cap \mathcal{L}(G_2) \neq \emptyset \quad (6.76)$$

Abbildung 6.73 legt die Konstruktion von  $G_1$  und  $G_2$  offen. Die Grammatik  $G_1$  ist so konstruiert, dass diejenigen Sequenzen abgeleitet werden können, deren Suffixe aus den bildbaren Wortsequenzen der PCP-Instanz bestehen. Die Definition von  $G_2$  erfolgt analog für die Komponenten  $y_1, \dots, y_n$ . Die Präfixe der abgeleiteten Wörter werden aus den Symbolen  $i_1, \dots, i_n$  gebildet. Sie sind eine textuelle Repräsentation der Auswahlindizes des PCP und dürfen auf keinen Fall fehlen. Deren Existenz stellt sicher, dass wir ein Wort  $\omega$  nur dann sowohl mit  $G_1$  als auch mit  $G_2$  ableiten können, wenn beide Ableitungen die gleiche Regelielenfolge einhalten. Diese Eigenschaft ist der Schlüssel zum Erfolg. Ein Wort liegt jetzt genau dann in der Schnittmenge  $\mathcal{L}(G_1) \cap \mathcal{L}(G_2)$ , wenn die betrachtete PCP-Instanz eine Lösung besitzt. Könnten wir das Schnittproblem für kontextfreie Sprachen entscheiden, so könnten wir durch die konstruierte Reduktion auch das Post'sche Korrespondenzproblem entscheiden. Aus dem Widerspruch ergibt sich unmittelbar das folgende Ergebnis:



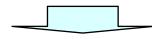
### Satz 6.22

Das Schnittproblem ist für kontextfreie Grammatiken unentscheidbar.

Als Nächstes wenden wir uns dem Mehrdeutigkeitsproblem kontextfreier Sprachen zu. Hinter diesem verbirgt sich die Frage, ob für eine gegebene Typ-2-Grammatik  $G$  ein Wort  $\omega$  existiert, das auf unterschiedliche Weise aus dem Startsymbol abgeleitet werden kann. Auch hier können wir die Unentscheidbarkeit durch eine Reduktion des Post'schen Korrespondenzproblems erhalten. Wie in Abbildung 6.74 gezeigt, folgt die Grammatik  $G$  weitgehend dem Konstruktionsprinzip, das uns weiter oben die Unentscheidbarkeit des Schnittproblems zeigen ließ. Die Produktionenmenge ist so aufgebaut, dass das Startsymbol  $S$  zunächst in eines der beiden Nonterminale  $S_1$  oder  $S_2$  überführt wird. Die weiteren Ableitungen sind mit jenen von  $G_1$  und  $G_2$  aus Abbildung 6.73 identisch. Existieren in  $G$  zwei verschiedene Ableitungssequenzen, die das

#### ■ PCP-Instanz

$$(x_1, y_1), \dots, (x_n, y_n)$$



#### ■ Grammatik $G$

$$G_1 := (S_G, \Sigma_G, P_G, s_G)$$

$$S_G := \{S, S_1, S_2\}$$

$$s_G := S$$

$$\Sigma_G := \Sigma \cup \{i_1, \dots, i_n\}$$

#### ■ Produktionenmenge $P_G$

$$S \rightarrow S_1 \mid S_2$$

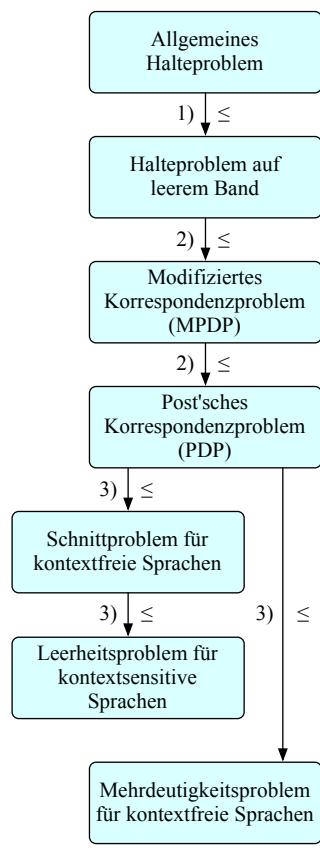
$$S_1 \rightarrow i_1 x_1 \mid \dots \mid i_n x_n$$

$$S_1 \rightarrow i_1 S_1 x_1 \mid \dots \mid i_n S_1 x_n$$

$$S_2 \rightarrow i_1 y_1 \mid \dots \mid i_n y_n$$

$$S_2 \rightarrow i_1 S_2 y_1 \mid \dots \mid i_n S_2 y_n$$

**Abbildung 6.74:** Reduktion von PCP auf das Mehrdeutigkeitsproblem



- 1) Abschnitt 6.5.1
- 2) Abschnitt 6.5.4
- 3) Abschnitt 6.5.5

**Abbildung 6.75:** Durch die Reduktion des Post'schen Korrespondenzproblems lässt sich eine Reihe weiterer Probleme als unentscheidbar entlarven.

gleiche Wort  $\omega$  entstehen lassen, so muss eine Sequenz das Nonterminal  $S_1$  und die andere das Nonterminal  $S_2$  enthalten. In diesem Fall ist dann auch die PCP-Instanz lösbar. Die Umkehrung gilt ebenfalls. Ist die PCP-Instanz unlösbar, so kann es in  $G$  keine zwei Ableitungssequenzen geben, die das gleiche Wort  $\omega$  erzeugen. Damit haben wir das Post'sche Korrespondenzproblem erfolgreich auf das Mehrdeutigkeitsproblem reduziert und dessen Unentscheidbarkeit bewiesen.

### Satz 6.23

Das Mehrdeutigkeitsproblem ist für kontextfreie Grammatiken unentscheidbar.

Als Drittes wenden wir uns dem Leerheitsproblem für kontextsensitiven Sprachen zu. Anders als in den ersten beiden Beispielen werden wir das Post'sche Korrespondenzproblem nicht direkt reduzieren. Stattdessen machen wir von unserem Wissen über die Unentscheidbarkeit des Schnittproblems kontextfreier Sprachen Gebrauch. Wir zeigen, dass das Schnittproblem kontextfreier Sprachen entscheidbar wäre, wenn wir das Leerheitsproblem kontextsensitiver Sprachen entscheiden könnten.

$L_1$  und  $L_2$  bezeichnen zwei beliebige kontextfreie Sprachen, für die wir das Schnittproblem entscheiden wollen. Für die folgende Betrachtung nutzen wir zwei elementare Eigenschaften kontextsensitiver Sprachen aus. Zum einen ist die Menge der Typ-1-Sprachen eine Obermenge der Typ-2-Sprachen. Damit sind sowohl  $L_1$  als auch  $L_2$  gleichzeitig Typ-1-Sprachen. Zum anderen ist die Menge der Typ-1-Sprachen bez. der Schnittoperation abgeschlossen, d. h., die Schnittmenge  $L_1 \cap L_2$  ist eine kontextsensitive Sprache. Könnten wir das Leerheitsproblem für kontextsensitive Sprachen entscheiden, so hätten wir einen Weg gefunden, das Schnittproblem kontextfreier Sprachen ebenfalls zu lösen. Damit ist es uns abermals gelungen, mit der Reduktionstechnik ein wichtiges Unberechenbarkeitsresultat zu erzielen.

### Satz 6.24

Das Leerheitsproblem ist für kontextsensitive Sprachen unentscheidbar.

Insgesamt entsteht der in Abbildung 6.75 dargestellte Zusammenhang. Allein die Unentscheidbarkeit des allgemeinen Halteproblems reichte aus, um alle anderen Probleme mit Hilfe der Reduktionstechnik ebenfalls als unentscheidbar zu identifizieren.

## 6.6 Übungsaufgaben

In diesem Kapitel haben Sie gelernt, wie sich die While-Sprache durch die Definition von Makros erweitern lässt, ohne ihre Ausdrucksstärke zu verändern. Unter anderem wurde gezeigt, wie komplexe Schleifenbedingungen der Form  $x < y$ ,  $x > y$  und  $x = y$  auf die Standardkonstrukte reduziert werden können. Zeigen Sie, dass eine ähnliche Reduktion auch für die booleschen Konnektive  $\wedge$  und  $\vee$  möglich ist. Tragen Sie Ihre Lösung in das jeweils rechtsstehende Listing ein:

**Aufgabe 6.1**



**Webcode**

**6237**

and.while

```
while x&y do
  P
end
```

and\_reduced.while

1	
2	
3	
4	
5	

or.while

```
while x∨y do
  P
end
```

or\_reduced.while

1	
2	
3	
4	
5	

Betrachten Sie die folgende Implementierung der Fakultätsfunktion:

**Aufgabe 6.2**



**Webcode**

**6104**

factorial.c

```
int factorial(m,n)
{
    if (m == 0) {
        return 1;
    }
    return mult(factorial(m-1, n),m);
}
```

1	
2	
3	
4	
5	
6	
7	
8	

Extrahieren Sie aus dem Programm die primitiv-rekursive Form der berechneten Funktion. Welche Bedeutung hat der Parameter  $n$ ?

**Aufgabe 6.3****Webcode  
6006**Gegeben sei die Funktion  $\pi : \mathbb{N}_0^2 \rightarrow \mathbb{N}_0$  mit

$$\pi(x, y) = \binom{x+y+1}{2} + x. \quad (6.77)$$

Analysieren Sie die Funktionswerte, indem Sie die folgende Tabelle vervollständigen:

	$x = 0$	$x = 1$	$x = 2$	$x = 3$	$x = 4$	$x = 5$
$y = 0$						
$y = 1$						
$y = 2$						
$y = 3$						
$y = 4$						
$y = 5$						

Offensichtlich ist  $\pi$  eine spezielle Variante der Cantor'schen Paarungsfunktion, die  $\mathbb{N}_0^2$  bijektiv auf  $\mathbb{N}_0$  abbildet.

- Zeigen Sie, dass  $\pi$  eine primitiv-rekursive Funktion ist.
- Zeigen Sie, dass auch die beiden Umkehrfunktionen  $\pi_1^{-1} : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  und  $\pi_2^{-1} : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  mit  $x = \pi_1^{-1}(\pi(x, y))$  und  $y = \pi_2^{-1}(\pi(x, y))$  primitiv-rekursiv sind.
- Zeigen Sie, dass sich die Mengen  $\mathbb{N}_0^k$  und  $\mathbb{N}_0$  mit Hilfe primitiv-rekursiver Funktionen bijektiv aufeinander abbilden lassen.

**Aufgabe 6.4****Webcode  
6150**

In diesem Kapitel haben Sie mit der verallgemeinerten Registermaschine ein bekanntes Berechnungsmodell kennen gelernt. Wir wollen unser Augenmerk auf den Registersatz lenken, der in der gewählten Darstellung aus unendlich vielen Registern besteht, die jedes für sich eine beliebige natürliche Zahl speichern können.

Ändert sich die Berechnungsstärke der Registermaschine, wenn wir...

- die Anzahl der Register auf endlich viele reduzieren?
- in einem Register nur noch Werte aus einem endlichen Intervall speichern dürfen?
- die Restriktionen aus a) und b) miteinander kombinieren?

Diese Aufgabe soll Ihnen ein Gefühl für die strukturelle Komplexität von Turing-Maschinen vermitteln. Um die Betrachtung nicht komplizierter als nötig zu gestalten, wollen wir ausschließlich Maschinen mit einem zweielementigen Bandalphabet  $\Pi$  und einem einzigen Endzustand betrachten. Wir nehmen weiter an, dass der Schreib-Lese-Kopf drei mögliche Bewegungen vollziehen kann (Linksschritt, Rechtsschritt, Position halten).  $T(n)$  bezeichne die Anzahl der Möglichkeiten, eine solche Turing-Maschine mit  $n$  Zuständen zu konstruieren.

Stellen Sie eine Formel für  $T(n)$  auf und vervollständigen Sie die nachstehende Tabelle:

$n$	$T(n)$	$n$	$T(n)$
1		6	
2		7	
3		8	
4		9	
5		10	

### Aufgabe 6.5



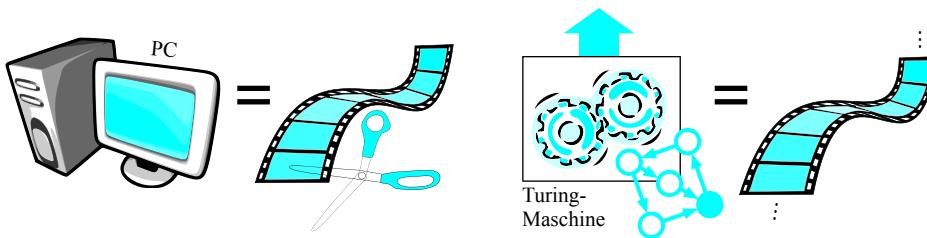
Webcode  
6968

Viele Experten sehen in der Turing-Maschine dasjenige Berechnungsmodell, das dem modernen Computer, wie wir ihn heute kennen, am nächsten kommt. Von einem formalen Standpunkt aus ist diese Sichtweise angreifbar, da alle gegenwärtig verfügbaren und zukünftig gebauten Computer nur über einen endlich großen Speicher verfügen. Turing-Maschinen besitzen hingegen ein unendliches langes Band.

### Aufgabe 6.6



Webcode  
6784



Die Endlichkeit des Speichers hat zur Konsequenz, dass reale Computer nur endlich viele Zustände einnehmen können. In Wirklichkeit sind sie damit nichts anderes als endliche Automaten und folglich berechnungsschwächer als Turing-Maschinen. Warum werden Turing-Maschinen von den meisten Experten dennoch als das adäquatere Modell zur Beschreibung realer Computer angesehen?

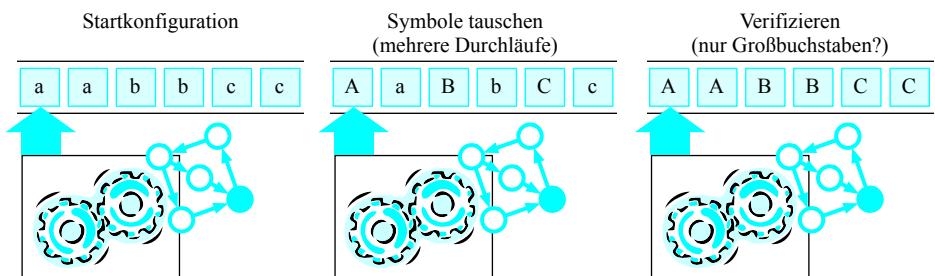
**Aufgabe 6.7****Webcode  
6355**In dieser Aufgabe betrachten wir eine Turing-Maschine  $T$  mit

$$\mathcal{L}(T) := \{a^n b^n c^n \mid n \in \mathbb{N}\} \quad (6.78)$$

Die Implementierung von  $T$  ist durch die folgende Übergangstabelle festgelegt:

	$a$	$A$	$b$	$B$	$c$	$C$	$\square$
$s_a$	$(s_b, A, \rightarrow)$	$(s_a, A, \rightarrow)$	—	—	—	—	—
$s_b$	$(s_b, a, \rightarrow)$	—	$(s_c, B, \rightarrow)$	$(s_b, B, \rightarrow)$	—	—	—
$s_c$	—	—	$(s_c, b, \rightarrow)$	—	$(s_t, C, \rightarrow)$	$(s_c, C, \rightarrow)$	—
$s_t$	—	—	—	—	$(s_r, c, \leftarrow)$	—	$(s_v, \square, \leftarrow)$
$s_r$	$(s_r, a, \leftarrow)$	$(s_a, A, \rightarrow)$	$(s_r, b, \leftarrow)$	$(s_r, B, \leftarrow)$	$(s_r, c, \leftarrow)$	$(s_r, C, \leftarrow)$	$(s_a, \square, \rightarrow)$
$s_v$	—	$(s_v, A, \leftarrow)$	—	$(s_v, B, \leftarrow)$	—	$(s_v, C, \leftarrow)$	$(s_e, \square, \rightarrow)$
$s_e$	—	—	—	—	—	—	—

Die Maschine arbeitet in mehreren Schritten. Zunächst bewegt sie den Schreib-Lese-Kopf von links nach rechts über das Eingabewort  $\omega$  und tauscht je ein  $a$ , ein  $b$  und ein  $c$  durch die Hilfssymbole  $A$ ,  $B$  und  $C$  aus. Dieser Vorgang wird durch die Zustände  $s_a$ ,  $s_b$  und  $s_c$  gesteuert. Anschließend wird in Zustand  $s_t$  geprüft, ob noch weitere  $c$ 's auf dem Band vorhanden sind. Falls ja, fährt der Schreib-Lese-Kopf an den Anfang zurück (Zustand  $s_r$ ) und wiederholt den geschilderten Ersetzungsprozess. Wurde das letzte  $c$  ersetzt, so geht die Maschine in die Verifikationsphase über (Zustand  $s_v$ ). In dieser bewegt die Maschine den Schreib-Lese-Kopf auf die erste Bandposition zurück und überprüft, ob sämtliche ursprünglich vorhandenen Symbole ersetzt wurden.

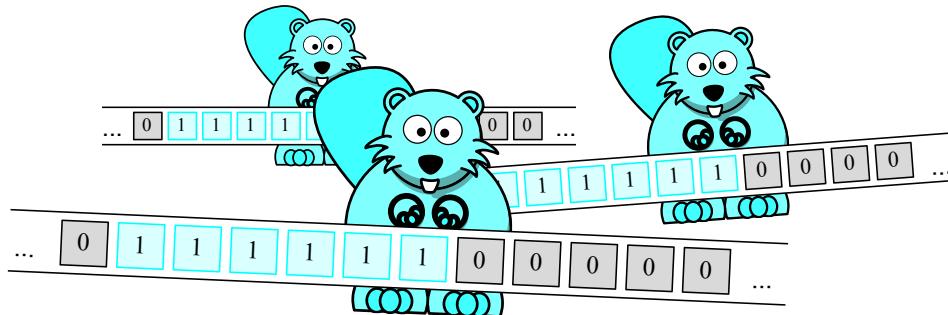


$T$  terminiert im Endzustand  $s_e$ , wenn der Überprüfungsprozess erfolgreich war. Dies ist genau dann der Fall, wenn das Eingabewort  $\omega$  die gleiche Anzahl  $a$ 's,  $b$ 's und  $c$ 's enthält.

- Simulieren Sie die Konfigurationsübergänge für das Eingabewort  $\omega = aabbcc$ .
- Ist  $T$  eine deterministische Turing-Maschine?

Im Jahre 1962 rief der ungarische Mathematiker Tibor Radó den Wettbewerb des *fleißigen Bibers* ins Leben. Fleißige Biber (*busy beaver*) der Größe  $n$  sind Turing-Maschinen mit  $n$  Zuständen, die möglichst viele Einsen auf ein mit Nullen vorinitialisiertes Band schreiben [11, 77]. Endlosschleifen sind dabei explizit verboten, d. h., die Turing-Maschine muss nach endlich vielen Schritten terminieren. Der Endzustand zählt nicht als Zustand.

**Aufgabe 6.8**

**Webcode  
6834**


Unser Interesse gilt der Frage, wie viele Einsen ein fleißiger Biber der Größe  $n$  höchstens erzeugen kann. Wir bezeichnen diesen Maximalwert mit  $B(n)$ . Da nur abzählbar viele Turing-Maschinen existieren, ist der Wert der *Biberfunktion*  $B$  für alle  $n$  wohldefiniert. Trotzdem sind die Funktionswerte nur bis  $n = 4$  exakt bekannt. Es gilt:

$$B(1) = 1 \tag{6.79}$$

$$B(2) = 4 \tag{6.80}$$

$$B(3) = 6 \tag{6.81}$$

$$B(4) = 13 \tag{6.82}$$

Die Bestimmung der Funktionswerte ist keinesfalls trivial. Für  $n = 4$  gibt es bereits mehr als eine halbe Billion Turing-Maschinen, die als fleißige Biber in Frage kommen. Damit verwundert es kaum, dass für  $B(5)$  nur noch Abschätzungen existieren. Im Jahre 1983 wurde ein fleißiger Biber gefunden, der 240 Einsen erzeugt. Ein Jahr später konnte der Wert durch einen anderen Biber zunächst auf 501 und dann auf 1915 erhöht werden. Im Jahre 1989 wurde schließlich ein Biber gefunden, der 4098 Einsen auf das Band schreibt. Ob diese Zahl dem Funktionswert  $B(5)$  entspricht, ist gegenwärtig ungewiss. Jeder ins Rennen geschickte Biber erlaubt uns lediglich, den Funktionswert  $B(n)$  nach unten abzuschätzen.

Es wächst der Wunsch nach einem Algorithmus, der die Biberfunktion  $B(n)$  für beliebige  $n$  ausrechnen kann. Machen Sie die Hoffnung über die Existenz eines solchen Algorithmus zunichte, indem Sie die Biberfunktion  $B$  als unberechenbar entlarven. Gehen Sie dabei ähnlich vor wie im Beweis der Unentscheidbarkeit des Halteproblems, indem Sie zunächst annehmen, dass  $B(n)$  mit Hilfe eines Programms  $P$  berechnet werden kann. Konstruieren Sie anschließend ein Programm  $P'$ , das  $P$  verwendet und die Annahme zu einem Widerspruch führt.

**Aufgabe 6.9****Webcode  
6926**

In dieser Aufgabe wollen wir uns mit den Eigenschaften der sogenannten *Diagonalsprache*  $L_D$  beschäftigen. Ähnlich wie in der Diskussion des Halteproblems listen wir zunächst alle Turing-Maschinen entlang der vertikalen Achse einer Matrix auf und versehen die horizontale Achse mit einer Aufzählung der Wörter aus  $\Sigma^*$ . Nun wird in der  $i$ -ten Zeile und der  $j$ -ten Spalte eingetragen, ob das Eingabewort  $\omega_j$  von der Maschine  $T_i$  akzeptiert wird oder nicht. Auf diese Weise erhalten wir mit der  $i$ -ten Zeile eine tabellarische Beschreibung der Sprache  $\mathcal{L}(T_i)$ .

	$\omega_1$	$\omega_2$	$\omega_3$	$\omega_4$	$\omega_5$	$\omega_6$
$T_1$	ja	ja	nein	ja	nein	ja
$T_2$	nein	ja	nein	ja	ja	nein
$T_3$	ja	ja	nein	nein	nein	ja
$T_4$	ja	nein	nein	ja	ja	ja
$T_5$	ja	ja	nein	ja	nein	nein
$T_6$	nein	nein	ja	ja	ja	nein

Aus der abgebildeten Matrix können wir die *Diagonalsprache*  $L_D$  wie folgt ableiten:

$$L_D := \{\omega_i \mid \omega_i \text{ wird von } T_i \text{ nicht akzeptiert}\} \quad (6.83)$$

Bildlich gesprochen erhalten wir  $L_D$ , indem wir die Hauptdiagonale der konstruierten Matrix herabsteigen und den Zelleninhalt für jedes Element invertieren.

Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort.

- a)  $L_D$  ist entscheidbar
- b)  $L_D$  ist aufzählbar
- c)  $\overline{L_D}$  ist aufzählbar

**Aufgabe 6.10****Webcode  
6475**

In dieser Aufgabe beschäftigen wir uns ausschließlich mit denjenigen Turing-Maschinen, die für alle Eingabewörter  $\omega$  terminieren. Genau wie in der vorherigen Aufgabe listen wir die Maschinen entlang der vertikalen Achse einer Matrix auf und versehen die horizontale Achse mit einer Aufzählung der Wörter aus  $\Sigma^*$ . Auch hier tragen wir in der  $i$ -ten Zeile und der  $j$ -ten Spalte ein, ob das Eingabewort  $\omega_j$  der Sprache  $\mathcal{L}(T_i)$  angehört oder nicht.

Die Diagonalsprache  $L_D$  definieren wir wie gehabt:

$$L_D := \{\omega_i \mid \omega_i \text{ wird von } T_i \text{ nicht akzeptiert}\} \quad (6.84)$$

Aus den Maschinen  $T_i$  konstruieren wir jetzt eine Cantor-Maschine  $C$ , die nach dem folgenden Prinzip arbeitet: Steht das Wort  $\omega_i$  auf dem Eingabeband, so startet  $C$  die Maschine  $T_i$  und antwortet mit „ja“, falls  $T_i$  mit „nein“ antwortet und umgekehrt. Offensichtlich akzeptiert  $C$  die Diagonalsprache  $L_D$ . Da die aufgerufenen Turing-Maschinen  $T_i$  für alle Eingaben terminieren, hält auch  $C$  für alle Eingaben nach endlich vielen Schritten an. Damit müsste die Cantor-Maschine ebenfalls in der oben konstruierten Matrix auftauchen, im Widerspruch zu der durchgeföhrten Diagonalkonstruktion. Lösen Sie den Widerspruch in diesem Gedankenangang auf.

In dieser Aufgabe beschäftigen wir uns mit einem prominenten Spezialfall des allgemeinen Halteproblems.

### Aufgabe 6.11



**Webcode**  
6132



#### Definition 6.22 (Spezielles Halteproblem)

Das spezielle Halteproblem lautet wie folgt:

- Gegeben: Turing-Maschine  $T$
  - Gefragt: Terminiert  $T$  mit der Eingabe  $\langle T \rangle$ ?
- $\langle T \rangle$  bezeichnet die Gödelnummer von  $T$ .

- Zeigen Sie, dass auch das spezielle Halteproblem unentscheidbar ist.
- Lässt sich die Unentscheidbarkeit aus dem Satz von Rice ableiten?

Welche der folgenden Aussagen sind äquivalent?

### Aufgabe 6.12



**Webcode**  
6833

- Die Sprache  $L$  ist aufzählbar
- Die Sprache  $L$  ist semi-entscheidbar
- $L$  ist eine Typ-0-Sprache
- Es existiert eine Turing-Maschine  $T$  mit  $\mathcal{L}(T) = L$

- e) Die charakteristische Funktion  $\chi_L$  ist berechenbar
- f) Die partielle charakteristische Funktion  $\chi'_L$  ist berechenbar

---

**Aufgabe 6.13**

Gegeben sei die nachstehende Folge von Wortpaaren aus der Menge  $\{\Diamond, \Box\}^+ \times \{\Diamond, \Box\}^+$ :

**Webcode**  
6839

$$(\Diamond\Box, \Box\Box), (\Diamond, \Diamond\Box\Diamond), (\Box\Diamond\Diamond, \Diamond\Diamond)$$

- a) Lösen Sie das Post'sche Korrespondenzproblem für die angegebene Instanz.
- b) Warum konnten Sie eine Lösung finden, obwohl das Problem unentscheidbar ist?

---

**Aufgabe 6.14**

**Webcode**  
6673

In diesem Kapitel haben Sie mit dem modifizierten Post'schen Korrespondenzproblem, kurz MPCP, eine spezielle Variante des PCP kennen gelernt.

- a) Besitzt MPCP für die Tupelfolge  $(01, 011), (110, 010), (001, 10)$  eine Lösung?
- b) Zeigen Sie  $\text{PCP} \leq \text{MPCP}$ , indem Sie eine Reduktion von PCP auf MPCP konstruieren.

---

**Aufgabe 6.15**

**Webcode**  
6754

Das Post'sche Korrespondenzproblem haben wir für Paare  $(x_i, y_i)$  von Wörtern über einem beliebigen Alphabet  $\Sigma$  definiert. Gilt  $\Sigma = \{0, 1\}$ , so sprechen wir von einem *binären Korrespondenzproblem*, kurz BPCP. Zeigen Sie  $\text{PCP} \leq \text{BPCP}$ , indem Sie eine Reduktion von PCP auf BPCP konstruieren.

## 7 Komplexitätstheorie

---

In diesem Kapitel werden Sie ...

- den abstrakten Begriff der algorithmischen Komplexität begreifen,
- das O-Kalkül zur Algorithmenbewertung einsetzen,
- eine Übersicht über die wichtigsten Komplexitätsklassen erhalten,
- an die Grenze der praktischen Berechenbarkeit vordringen,
- NP-harte und NP-vollständige Probleme zu unterscheiden lernen,
- das P-NP-Problem verstehen.

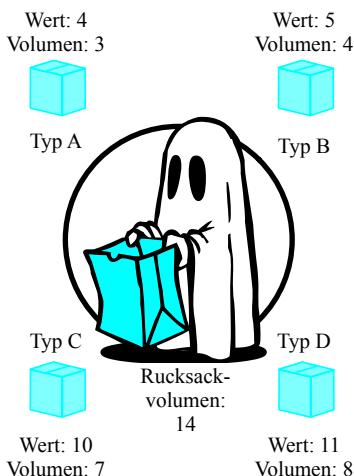


## 7.1 Algorithmische Komplexität

Während sich die Berechenbarkeitstheorie mit der prinzipiellen Lösbarkeit von Problemen beschäftigt, untersucht die Komplexitätstheorie die Effizienz der eingesetzten Algorithmen. Für die praktische Informatik ist die Komplexitätstheorie von unschätzbarem Wert, schließlich lässt sich ein Entscheidungsverfahren nur dann auf reale Probleme anwenden, wenn sich sein Ressourcenverbrauch in realistischen Grenzen bewegt. Die praktische Anwendbarkeit eines Verfahrens wird vor allem durch seine Laufzeit und seinen Speicherplatzverbrauch bestimmt; beide Ressourcen stehen uns heute wie auch in der Zukunft nur in begrenztem Maße zur Verfügung.

In Kapitel 1 haben Sie am Beispiel des Problems PRIME bereits einen Eindruck erhalten, wie schnell die theoretische Berechenbarkeit in der Praxis an ihre Grenze stößt. Lösen wir PRIME auf naive Weise, so nimmt die Anzahl der Divisionen exponentiell mit der Bitbreite der zu testenden Zahl zu. Geringe Bitbreiten reichen aus, um selbst modernste Computeranlagen Jahrzehnte zu beschäftigen.

Die in der theoretischen Informatik durchgeführten Komplexitätsberechnungen verfolgen das Ziel, die Laufzeit- und den Speicherplatzbedarf eines Algorithmus auf einer abstrakten Ebene zu bestimmen. Insbesondere sollen die gewonnenen Ergebnisse unabhängig von



**Abbildung 7.1:** Hinter dem Rucksackproblem verbirgt sich die Aufgabe, das Diebesgut so auszuwählen, dass der erzielte Gewinn maximal ist.

- der Programmiersprache,
- dem installierten Betriebssystem,
- der Prozessorleistung,
- der Speicherausstattung und
- der zugrunde liegenden Computerarchitektur

sein. Dies ist der Grund, warum wir im Folgenden stets mit einheitlosen Zahlen agieren werden.

Um einen tieferen Einblick in die Laufzeit- und Platzkomplexität realer Algorithmen zu erhalten, werden wir in diesem Abschnitt zwei Lösungsmöglichkeiten des *Rucksackproblems* diskutieren. Mit Begriffen des Alltags lässt sich das zu lösende Problem wie folgt veranschaulichen: Ein Ganove findet in einem Tresor verschiedene Gegenstände vor, die in Abhängigkeit ihres Typs ein bestimmtes Volumen besitzen

und auf dem Schwarzmarkt einen fixen Geldbetrag einbringen. Der Ganove sieht sich mit der Aufgabe konfrontiert, seinen Rucksack so mit Diebesgut zu füllen, dass der erbeutete Wert maximal wird. Dabei nehmen wir an, dass die Gegenstände jedes Typs in unbegrenzter Anzahl vorhanden sind und wir den Wert und das Volumen als ganzzahlige Größen beschreiben können. Abbildung 7.1 demonstriert das Dilemma des Ganoven anhand eines konkreten Beispiels.

Mathematisch gesehen verbirgt sich hinter dem Rucksackproblem die folgende Aufgabe:



### Definition 7.1 (Rucksackproblem)

Gegeben sei eine Zahl  $v \in \mathbb{N}$  sowie eine Menge von Wertepaaren

$$(c_1, v_1), \dots, (c_n, v_n) \text{ mit } c_i, v_i \in \mathbb{N}, 1 \leq i \leq n$$

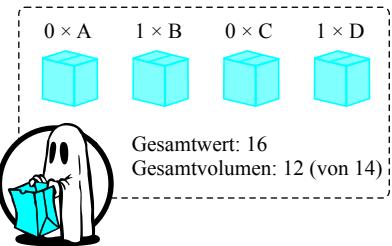
Gesucht ist eine Folge ganzzahliger Werte  $a_1, \dots, a_n \in \mathbb{N}_0$ , so dass

$$\sum_{i=1}^n a_i v_i \leq v \text{ und } \sum_{i=1}^n a_i c_i \text{ maximal ist.}$$

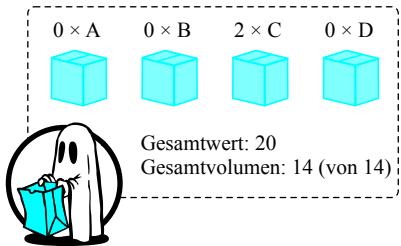
Obwohl das Problem auf den ersten Blick simpel erscheint, existiert selbst für kleine Rucksäcke eine Vielzahl an Auswahlmöglichkeiten. Für unser Eingangsbeispiel sind in Abbildung 7.2 zwei konkrete Wahlmöglichkeiten exemplarisch aufgeführt. Der erste Rucksack ist mit einem Typ-B-Gegenstand und einem Typ-D-Gegenstand bestückt und kommt auf einen Gesamtwert von  $5 + 11 = 16$ . Obwohl das Rucksackvolumen mit dieser Befüllung noch nicht komplett ausgeschöpft ist, lässt sich kein anderes Element mehr dazupacken, schließlich ist der kleinste Gegenstand (Typ A) größer als das Restvolumen. Wählt der Ganove stattdessen zwei Typ-C-Elemente, so wird das Rucksackvolumen komplett ausgeschöpft und ist mit einem Gesamtwert von 20 die bessere Wahl. Später werden wir zeigen, dass wir mit dieser Befüllung eine optimale Lösung vor uns haben, d.h., keine andere Wahl führt zu einem höheren Gesamtwert der entwendeten Ware.

Wir wollen uns der algorithmischen Lösung des Rucksackproblems nähern, indem wir zunächst eine abgeschwächte Variante untersuchen. Anstatt eine konkrete Auswahl an Gegenständen zu berechnen, versuchen wir zunächst den maximal erreichbaren Gewinn zu ermitteln. Anschließend machen wir uns Gedanken darüber, wie wir die erstellten Algorithmen so erweitern können, dass aus dem Ergebnis eine Liste der zu entwendenden Gegenstände extrahiert werden kann.

#### Erste Zusammenstellung



#### Zweite Zusammenstellung



**Abbildung 7.2:** Zwei konkrete Auswahlmöglichkeiten für das Rucksackproblem aus Abbildung 7.1.

knapsack_recursive.c	knapsack.c
<pre> int knapsack( int n ) {     int i, best, tmp;      best = 0;     for (i = 0; i &lt; m; i++) {         if (n - size[i] &gt;= 0) {             tmp = knapsack(n-size[i]);             tmp += gain[i];             if (tmp &gt; best) {                 best = tmp;             }         }     }     return best; } </pre>	<pre> 1   int knapsack( int n ) 2   { 3       int i , j , tmp ; 4 5       for ( i = 0 ; i &lt; m ; i ++ ) { 6           for ( j = 0 ; j &lt;= n ; j ++ ) { 7               if ( j - size [ i ] &gt;= 0 ) { 8                   tmp = best [ j - size [ i ] ]; 9                   tmp += gain [ i ]; 10                  if ( tmp &gt; best [ j ] ) 11                      best [ j ] = tmp ; 12 13               } 14           } 15       } 16       return best [ n ]; 17   } 18 </pre>

**Abbildung 7.3:** Rekursive und iterative Implementierung des Rucksackproblems

Das linke Listing in Abbildung 7.3 zeigt, wie das abgeschwächte Rucksackproblem rekursiv gelöst werden kann. Die Funktion knapsack nimmt die Größe eines Rucksacks als Parameter entgegen und berechnet für diesen den maximal erzielbaren Gewinn. Während der Ausführung greift die Funktion auf die globalen Arrays size und gain zurück. Für  $0 \leq i < m$  enthalten die Elemente size[i] und gain[i] das Volumen bzw. den Wert des  $i$ -ten Gegenstands und bleiben während der gesamten Berechnung unverändert. Wir nehmen für die Berechnung an, dass die Variable  $m$  mit der Anzahl der zur Verfügung stehenden Gegenstände initialisiert ist.

Intern arbeitet die Funktion nach einem einfachen Prinzip. In einer Schleife wird über alle zur Auswahl stehenden Elemente iteriert und in der  $i$ -ten Iteration hypothetisch das  $i$ -te Element ausgewählt. Anschließend wird über einen rekursiven Aufruf die optimale Befüllung für den dann verbleibenden Rucksackinhalt berechnet und die beste der bisher gefundenen Lösungen in der Variablen best gespeichert.

Angewendet auf unser Beispielszenario aus Abbildung 7.1 liefert der Funktionsaufruf knapsack(14) den Wert 20 zurück. Wie dieser Wert zu stande kommt, zeigt Abbildung 7.4 anhand des Rekursionsbaums, den der Algorithmus intern durchläuft.

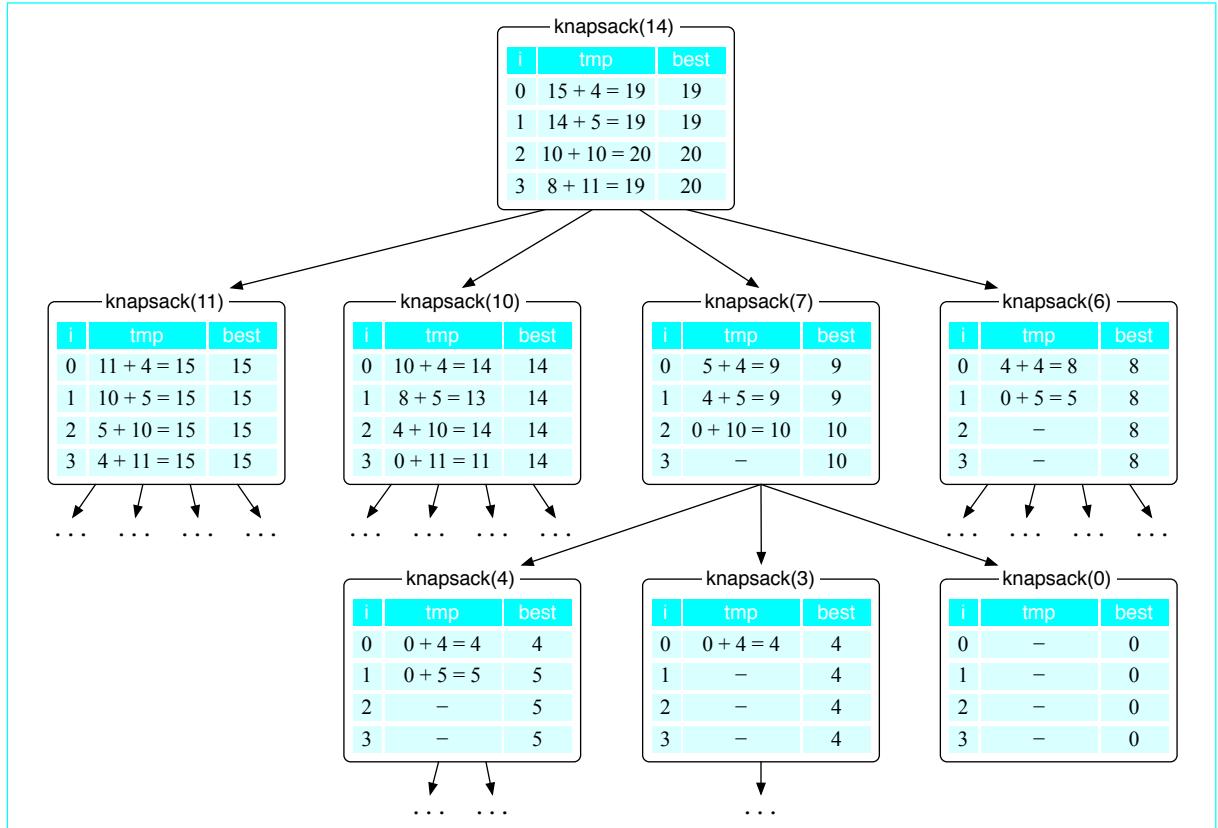


Abbildung 7.4: Auszug aus der internen Berechnungsfolge der rekursiven Implementierung

Der Rekursionsbaum gibt bereits wertvolle Hinweise auf die Laufzeitkomplexität des Algorithmus. In jedem Funktionsaufruf wird der Schleifenkörper  $m$ -mal durchlaufen und in jeder Iteration ein rekursiver Aufruf getätigt. Da der Aufrufparameter  $n$  hierbei um mindestens 1 verringert wird, besitzt der Rekursionsbaum eine maximale Tiefe von  $n$ . Damit enthält der vollständig expandierte Rekursionsbaum bis zu  $m^n$  Knoten, so dass sich die Laufzeit des Algorithmus nach oben durch die Funktion  $m^n$  abschätzen lässt. In der Nomenklatur der Komplexitätstheorie wird die Proportionalitätsbeziehung in der Form  $O(m^n)$  notiert. Was sich hinter dieser Notation formal verbirgt, werden wir im nächsten Abschnitt klären.

Für die Bestimmung des Speicherplatzbedarfs müssen wir beachten, dass ein realer Rechner in jedem rekursiven Aufruf einen neuen Stack-

Rahmen erzeugen muss, in dem alle lokalen Variablen der Funktion zwischengespeichert werden. Die maximale Anzahl der gleichzeitig gespeicherten Stack-Rahmen entspricht der maximalen Tiefe des Rekursionsbaums und ist damit gleich  $n$ . Mit anderen Worten: Der Speicherplatzbedarf steigt linear mit der Größe des Rucksacks und bleibt durch den zweiten Parameter  $m$  unbeeinflusst.

Die rekursive Implementierung von `knapsack(n)` besitzt die folgende Komplexität:



Laufzeit	Speicherplatz
$O(m^n)$	$O(n)$

Die Analyse offenbart, dass die rekursive Lösung des abgeschwächten Rucksackproblems in der Praxis kaum brauchbar ist. Verantwortlich ist die Laufzeit, die mit steigender Rucksackgröße exponentiell zunimmt.

## Dynamische Programmierung

$j$	$i = 1$	$i = 2$	$i = 3$	$i = 4$
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	4	4	4	4
4	4	5	5	5
5	4	5	5	5
6	8	8	8	8
7	8	9	10	10
8	8	10	10	11
9	12	12	12	12
10	12	13	14	14
11	12	14	15	15
12	16	16	16	16
13	16	17	18	18
14	16	18	20	20

**Tabelle 7.1:** Mit dem Mittel der dynamischen Programmierung lässt sich das Rucksackproblem bestechend einfach lösen.

Dennoch ist das Rucksackproblem effizient lösbar. Den Schlüssel hierzu liefert das Prinzip der dynamischen Programmierung, dem wir bereits in Abschnitt 4.4.4 im Rahmen der Diskussion über den CYK-Algorithmus begegnet sind. Folgt unser Ganove diesem Prinzip, so ersetzt er die Variable `best` durch eine Tabelle der Länge  $n$  und speichert in `best[j]` den maximal zu erbeutenden Wert für einen Rucksack mit dem Fassungsvermögen  $j$  (vgl. Abbildung 7.3 rechts).

Das Array dient als Arbeitsbereich und wird in einem iterativen Prozess permanent aktualisiert. Im ersten Iterationsschritt wird `best` so ausgefüllt, als hätten wir ausschließlich Typ-A-Gegenstände zur Verfügung. Im nächsten Iterationsschritt wird auch die Auswahl von B erwogen, im übernächsten die Auswahl von C und so fort. Der Ganove geht nun so vor, dass er in jeder Iteration die optimale Lösung für `best[i]` aus den bereits berechneten Werten ermittelt.

Angenommen, der Wert `best[14]` enthält am Ende der zweiten Iteration den Wert 18. Der Wert besagt, dass unser Ganove einen maximalen Gewinn von 18 erzielen kann, wenn er nur Typ-A- und Typ-B-Gegenstände stiebt. Basierend auf unserem Beispielszenario stellt er folgende Überlegung an: Stiebt er einen Typ-C-Gegenstand, so besitzt dieser den Wert

<pre>knapsack_final.c</pre> <pre> void knapsack(int n) {     int i, j, tmp;      for (i = 0; i &lt; m; i++) {         for (j = 0; j &lt;= n; j++) {             if (j - size[i] &gt;= 0) {                 tmp = best[j-size[i]];                 tmp += gain[i];                 if (tmp &gt; best[j]) {                     best[j] = tmp;                     item[j] = i;                 }             }         }     } } </pre>	<pre>main.c</pre> <pre> 1   int size[] = { 3, 4, 7, 8 }; 2   int gain[] = { 4, 5, 10, 11 }; 3   int best[15], item[15]; 4   int m = 4; 5 6   int main() 7   { 8       int j; 9 10      knapsack(14); 11 12      for (j=14; j&gt;=3; j-=size[item[j]]) 13          printf("%d ", item[j]); 14 15      return 0; 16 17 18 19 </pre>
--	---

**Abbildung 7.5:** Durch eine minimale Programmerweiterung lässt sich nicht nur der maximal zu erbeutende Gewinn, sondern auch die optimale Bepackung des Rucksacks berechnen. Die zu stehlenden Gegenstände lassen sich auf einfache Weise durch die Rückverfolgung der gespeicherten Tabelleneinträge bestimmen.

10 und es bleibt im Rucksack ein Restvolumen von 8 übrig. Die optimale Lösung, um das Restvolumen zu füllen, kennen wir aber bereits; sie entspricht dem Wert von `best[8]`. Ist die Summe aus `best[8]` und 10 größer als der bisher berechnete Wert 18, so lohnt es sich, einen Typ-C-Gegenstand zu entwenden. Andernfalls bleibt der Ganove bei Typ-A- und Typ-B-Gegenständen. Angewendet auf unser ursprüngliches Beispielszenario liefert der Algorithmus das in Tabelle 7.1 dargestellte Ergebnis. Den maximal zu erbeutenden Wert kann unser Ganove am Ende der Berechnung im Feld `best[14]` ablesen.

Um die Komplexität dieser Implementierungsvariante zu bestimmen, werfen wir erneut einen Blick auf das rechte Listing in Abbildung 7.3. Insgesamt durchläuft die Funktion `knapsack` zwei verschachtelte Schleifen. Während die äußere über alle Gegenstände iteriert und damit  $m$ -mal ausgeführt wird, erstreckt sich die innere Schleife über alle Rucksackvolumina von 0 bis  $n$ . Die Laufzeit des Algorithmus nimmt somit proportional mit dem Produkt  $m \cdot n$  zu.

Auch der Speicherplatzverbrauch fällt moderat aus. Neben dem neu hinzugefügten Array `best` benötigen wir keine weiteren Hilfsvariablen. Das

Array besitzt  $n$  Elemente, so dass der Speicherplatz linear mit dem Volumen der betrachteten Rucksäcke wächst. Dass sich der Speicherhunger der betrachteten Implementierung in Grenzen hält, haben wir einer besonderen Eigenschaft des Rucksackproblems zu verdanken. Da wir zur Bestimmung des Feldelements  $\text{best}[j]$  ausschließlich die Ergebnisse der vorangegangenen Iteration benötigen, können wir ältere Zwischenergebnisse verwerfen. Damit ist es vollkommen ausreichend, zu jedem Zeitpunkt nur eine einzige der in Tabelle 7.1 dargestellten Spalten im Speicher vorzuhalten. Anders als es z. B. im CYK-Algorithmus aus Abschnitt 4.4.4 der Fall war, können wir das Rucksackproblem hierdurch mit einem eindimensionalen Array lösen.

Mit dem Mittel der dynamischen Programmierung lässt sich das Rucksackproblem mit der folgenden Komplexität lösen:



	Laufzeit	Speicherplatz
	$O(m \cdot n)$	$O(n)$

$j$	$i = 1$	$i = 2$	$i = 3$	$i = 4$
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	4,A	4,A	4,A	4,A
4	4,A	5,B	5,B	5,B
5	4,A	5,B	5,B	5,B
6	8,A	8,A	8,A	8,A
7	8,A	9,B	10,C	10,C
8	8,A	10,B	10,B	11,D
9	12,A	12,A	12,A	12,A
10	12,A	13,B	14,C	14,C
11	12,A	14,B	15,C	15,C
12	16,A	16,A	16,A	16,A
13	16,A	17,B	18,C	18,C
14	16,A	18,B	20,C	20,C

**Tabelle 7.2:** Interne Berechnungsabfolge des finalen Algorithmus. Durch die Rückverfolgung der Einträge lässt sich die optimale Rucksackbepackung extrahieren.

Die bisher vorgestellten Implementierungsvarianten geben dem Ganoven zwar über den maximal zu erbeutenden Gewinn Auskunft, liefern ihm jedoch keinerlei Hinweis, welche Gegenstände er dafür auswählen muss. Genau dies ist aber die Aufgabe des ursprünglich in Definition 7.1 formulierten Rucksackproblems. Legen wir die zweite Implementierungsvariante zugrunde, so können wir dieses Problem mit einer minimalen Modifikation lösen. Hierzu ergänzen wir das Array  $\text{best}$  um ein zweites Array  $\text{item}$ , in dem wir den zuletzt hinzugefügten Gegenstandstyp speichern. Jedes Mal, wenn das Array-Element  $\text{best}[j]$  beschrieben wird, aktualisieren wir ebenfalls das Element  $\text{item}[j]$ . Die entsprechend modifizierte Implementierung ist in Abbildung 7.5 zusammengefasst.

Durch die Rückverfolgung der gespeicherten Einträge kann unser Ganove eine optimale Rucksackbepackung für unser Beispieldaten ablesen. Über den Typ des ersten Gegenstandes gibt der Inhalt von  $\text{item}[14]$  (= C) Auskunft (vgl. Tabelle 7.2). Um den zweiten Gegenstand zu bestimmen, berechnen wir das Volumen von C und subtrahieren das Ergebnis von 14. Es gilt  $\text{item}[14-7]$  (= C), so dass wir einen zweiten Typ-C-Gegenstand entwenden. Mit diesem Gegenstand ist der Rucksack restlos vollgepackt und die optimale Lösung gefunden. Gut, dass die meisten Ganoven noch nie etwas vom Prinzip der dynamischen Programmierung gehört haben...

### 7.1.1 O-Kalkül

Weiter oben haben wir zur Angabe der algorithmischen Komplexität bereits auf die *O-Notation* zurückgegriffen, ohne uns um eine genaue Beegriffsbestimmung zu kümmern. Dies wollen wir jetzt nachholen und die durchgeführten Laufzeit- und Speicherplatzbetrachtungen gleichzeitig auf eine abstraktere Ebene heben. Hierzu werden wir zunächst eine formale Definition der verschiedenen Notationsvarianten vornehmen und anschließend die Gültigkeit mehrerer Rechenregeln erarbeiten. Als Ergebnis werden wir mit dem *O-Kalkül* eine Beschreibungsform erhalten, die den Umgang mit Wachstumsfunktionen deutlich erleichtert.

Im Kern verfolgt die O-Notation die Idee, Wachstumsfunktionen anhand ihrer Wertentwicklungen in Äquivalenzklassen einzuteilen, die von den realen Funktionswerten abstrahieren. Formal definieren wir die Notation wie folgt:



#### Definition 7.2 (O-Notation)

Die Funktion  $f : \mathbb{N} \rightarrow \mathbb{R}^+$  fällt in die Komplexitätsklasse

$$O(g(n)),$$

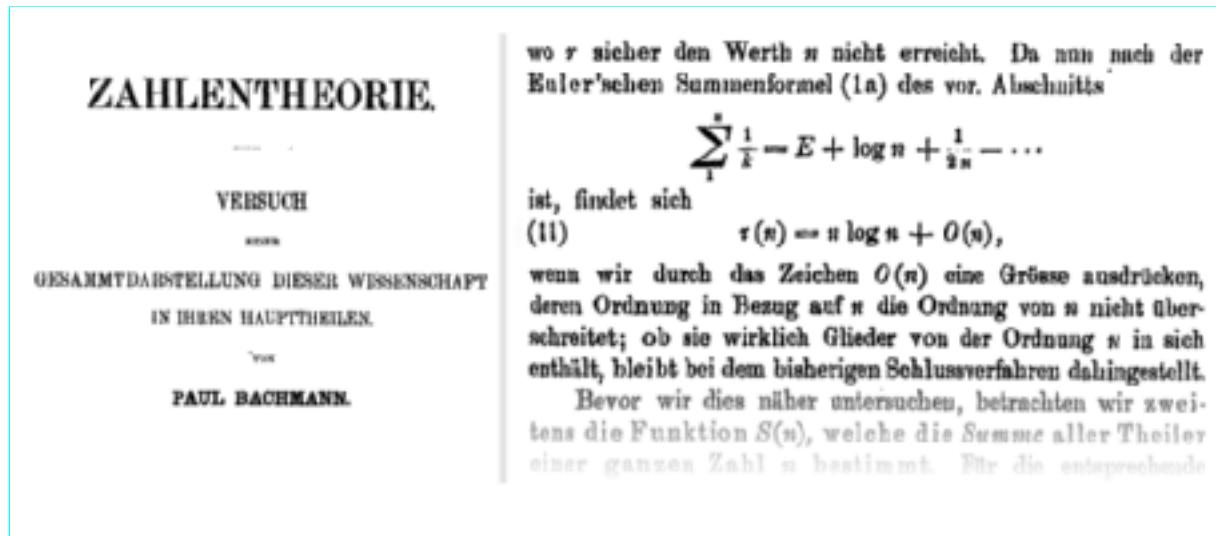
falls eine Konstante  $c \in \mathbb{R}^+$  und ein  $n_0 \in \mathbb{N}$  existieren, so dass

$$f(n) \leq c \cdot g(n)$$

für alle  $n \geq n_0$  gilt.

Das Notationszeichen O ist eines von mehreren *Landau-Symbolen*, benannt nach dem deutschen Mathematiker Edmund Georg Hermann Landau (vgl. Abbildung 7.6). Zwei Punkten wollen wir an dieser Stelle unsere besondere Aufmerksamkeit schenken.

- In Definition 7.2 wird lediglich gefordert, dass die Beziehung  $f(n) \leq c \cdot g(n)$  für alle  $n$  erfüllt sein muss, die *größer oder gleich* einer gewissen Konstanten  $n_0$  sind. Die getätigte Einschränkung legt einen Kerngedanken der Komplexitätsanalyse offen. Ziel ist es, das Laufzeitverhalten und den Platzbedarf eines Programms für sehr große Eingaben zu analysieren. Wie sich die ermittelten Wachstumsfunktionen auf einem endlichen Anfangsstück verhalten, spielt hierfür keine Rolle. Da wir den Größenparameter  $n$  gegen unendlich streben lassen, sprechen wir auch von der *asymptotischen Komplexität* eines Programms oder Algorithmus.



**Abbildung 7.6:** Die O-Notation hat sich heute als Standard für die Beschreibung von Komplexitätsklassen etabliert. Die verwendeten Symbole wurden vor allem durch die Arbeiten des deutschen Mathematikers Edmund Landau bekannt, ihr wahrer Ursprung reicht jedoch bis in das Jahr 1894 zurück. Dort taucht die O-Notation im zweiten Band von Paul Bachmanns Werk „Zahlentheorie: Versuch einer Gesamtdarstellung dieser Wissenschaft“ auf Seite 401 auf [5]. In [62] äußert sich Landau wie folgt über die Notation: „Das Zeichen  $O(g(x))$  habe ich zuerst bei Herrn Bachmann vorgefunden. Das hier hinzugefügte Zeichen  $o(g(x))$  entspricht dem, was ich in meinen Abhandlungen früher mit  $\{g(x)\}$  zu bezeichnen pflegte.“

- Die in Definition 7.2 vorkommende Konstante  $c$  dürfen wir beliebig wählen. Konkret hat dies zu Folge, dass die O-Notation von sämtlichen konstanten Faktoren abstrahiert. Fällt eine Funktion  $f(n)$  in die Komplexitätsklasse  $O(g(n))$ , so gehört auch die Funktion  $k \cdot f(n)$  zu dieser Klasse – unabhängig davon, wie groß wir die Konstante  $k$  auch wählen. Diese Eigenschaft ist gewollt, da wir sämtliche Komplexitätsbetrachtungen auf abstrakten Größen durchführen, die bewusst von einer konkreten Einheit abstrahieren. Kurzum: Die wichtige Information ist für uns die asymptotische Zunahme der Kenngröße und nicht deren realer Wert.

Behalten Sie stets im Gedächtnis, dass der Ausdruck  $O(g(n))$  eine *Menge von Funktionen* beschreibt und die Schreibweise  $f(n) \in O(g(n))$  ausdrückt, dass die Funktion  $f$  in die durch  $g$  definierte Komplexitätsklasse fällt. Obwohl dies die formal korrekte Schreibweise ist, hat sich in der Praxis die Notation  $f(n) = O(g(n))$  durchgesetzt. Aus mathematischer Sicht ist diese Schreibweise schlicht falsch. Trotzdem ist sie heute so weit verbreitet, dass wir uns an dieser Stelle nicht dagegen sträuben wollen.

Mit Hilfe der O-Notation sind wir in der Lage, das asymptotische Wachstum einer Funktion  $f(n)$  *nach oben* abzuschätzen. In analoger Weise drücken die Symbole  $\Omega$  und  $\Theta$  eine Abschätzung nach unten bzw. in beide Richtungen aus.



### Definition 7.3 ( $\Sigma$ -, $\Theta$ -Notation)

Die Funktion  $f : \mathbb{N} \rightarrow \mathbb{R}^+$  fällt in die Komplexitätsklasse

$$\Omega(g(n)), \quad (7.1)$$

falls eine Konstante  $c \in \mathbb{R}^+$  und ein  $n_0 \in \mathbb{N}$  existieren, so dass

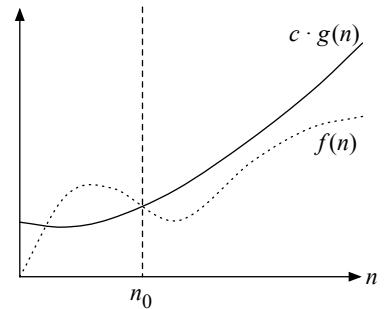
$$f(n) \geq c \cdot g(n) \quad (7.2)$$

für alle  $n \geq n_0$  gilt.  $f$  fällt in die Komplexitätsklasse

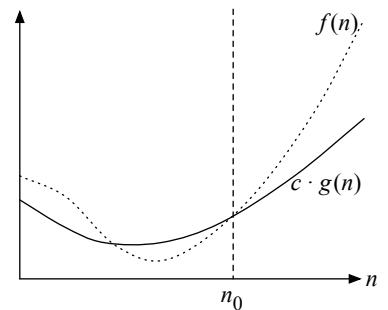
$$\Theta(g(n)), \quad (7.3)$$

falls  $f$  sowohl in  $O(g(n))$  als auch in  $\Omega(g(n))$  liegt.

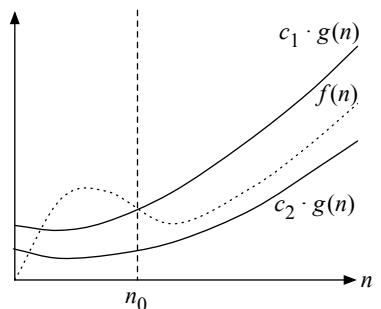
■  $O(n)$



■  $\Omega(n)$



■  $\Theta(n)$



**Abbildung 7.7:** Die Landau-Symbole  $O$ ,  $\Omega$  und  $\Theta$  im Vergleich



### Definition 7.4 ( $o$ -, $\omega$ -Notation)

Die Funktion  $f : \mathbb{N} \rightarrow \mathbb{R}^+$  fällt in die Komplexitätsklasse

$$o(g(n)) \quad \text{bzw.} \quad \omega(g(n)), \quad (7.4)$$

falls für alle Konstanten  $c \in \mathbb{R}^+$  ein  $n_0 \in \mathbb{N}$  existiert, so dass

$$c \cdot f(n) \leq g(n) \quad \text{bzw.} \quad c \cdot f(n) \geq g(n) \quad (7.5)$$

für alle  $n \geq n_0$  gilt.

Die Mengen  $o(g(n))$  bzw.  $\omega(g(n))$  lassen sich aus den verwandten Mengen  $O(g(n))$  und  $\Omega(g(n))$  konstruieren, indem diejenigen Funktio-

In den meisten Informatikbüchern wird die Komplexität von Algorithmen in der O-Notation angegeben. Tatsächlich scheint aber die  $\Theta$ -Komplexität das adäquatere Messinstrument zu sein, da die Laufzeit oder der Speicherplatzbedarf durch die O-Notation lediglich nach oben abgeschätzt wird. Des Weiteren werden Ausdrücke der Form  $O(g(n))$  in der Praxis häufig missinterpretiert. So suggeriert der Ausdruck  $O(2^n)$ , dass sich Probleme aus dieser Klasse ausschließlich durch Algorithmen lösen lassen, deren Laufzeit oder Speicherbedarf exponentiell mit der Eingangsgröße  $n$  zunimmt. Da die O-Notation aber nur eine Abschätzung nach oben vornimmt, liegen z. B. auch alle Algorithmen mit linearem Ressourcenverbrauch in der Komplexitätsklasse  $O(2^n)$ . Die Angabe der  $\Theta$ -Komplexität würde Missverständnisse dieser Art vorab vermeiden.

In der Praxis wird schlicht und einfach deshalb auf die O-Notation zurückgegriffen, weil sich die  $\Theta$ -Komplexität für viele Probleme nur schwer berechnen lässt. Um zu zeigen, dass ein Problem in  $\Theta(g(n))$  liegt, müssen wir nachweisen, dass  $g(n)$  sowohl eine asymptotische obere Schranke ( $O(g(n))$ ) als auch eine asymptotische untere Schranke ( $\Omega(g(n))$ ) ist. Erstes kann wie gewohnt dadurch geschehen, dass ein konkreter Algorithmus mit der entsprechenden Komplexität angegeben wird. Der Nachweis einer unteren Schranke gestaltet sich in den meisten Fällen ungleich schwieriger. Hier müssen wir nachweisen, dass *alle* Algorithmen, die das untersuchte Problem lösen, mindestens die durch  $g(n)$  definierte Komplexität besitzen. In der Tat existieren nur wenige Probleme, für die der formale Nachweis einer exakten unteren Komplexitätsschranke bisher gelungen ist. Dies ist der Grund, warum wir in der Praxis fast immer auf die O-Notation angewiesen sind und auf die aussagekräftigere  $\Theta$ -Notation verzichten müssen.

nen herausgenommen werden, die in der gleichen Komplexitätsklasse wie  $g(n)$  liegen. Es gelten die folgenden Zusammenhänge:

$$o(g(n)) = O(g(n)) - \Theta(g(n)) \quad (7.6)$$

$$\omega(g(n)) = \Omega(g(n)) - \Theta(g(n)) \quad (7.7)$$

So ähnlich die Notationen auf den ersten Blick erscheinen mögen, so unterschiedlich ist ihr Einsatzzweck. O,  $\Omega$  und  $\Theta$  dienen in erster Linie zur Bestimmung der Komplexität eines Algorithmus. In diesem Fall wird das Ziel verfolgt, die wahre Komplexitätsklasse so genau wie möglich zu treffen. o und  $\omega$  dienen stattdessen der Abgrenzung von Komplexitätsklassen. Können wir z. B. die Beziehung  $\log n = o(\sqrt{n})$  zeigen, so ist der Beweis erbracht, dass beide Funktionen unterschiedlichen Komplexitätsklassen angehören, die Logarithmus-Funktion also asymptotisch langsamer wächst als Wurzel- $n$ . Dagegen besitzt die Beziehung  $\log n = O(\sqrt{n})$  eine deutlich geringere Aussagekraft. Sie wäre auch dann erfüllt, wenn beide Funktionen asymptotisch gleich schnell wachsen würden.

Bisher haben wir die O-Notation dazu verwendet, um die asymptotische Komplexität einzelner Algorithmen zu beschreiben. Im Folgenden werden wir den Begriff weiter fassen und auch von der asymptotischen Komplexität von *Problemen* reden.



### Definition 7.5 (Problemkomplexität)

$P$  sei ein beliebiges Ja-Nein-Problem.  $A$  sei die Menge aller Algorithmen, die  $P$  entscheiden. Wir schreiben

- $P = O(g(n))$ , falls für ein  $a \in A$  gilt:  $f_a = O(g(n))$
- $P = \Omega(g(n))$ , falls für alle  $a \in A$  gilt:  $f_a = \Omega(g(n))$
- $P = \Theta(g(n))$ , falls  $P \in O(g(n))$  und  $P \in \Omega(g(n))$

Die Wachstumsfunktion  $f_a : \mathbb{N} \rightarrow \mathbb{R}^+$  beschreibt den Ressourcenverbrauch von  $A$  für eine Eingabe der Länge  $n$ .

## 7.1.2 Rechnen im O-Kalkül

In diesem Abschnitt werden wir zunächst eine alternative Definition der Laundau-Symbole ins Spiel bringen und anschließend mehrere Rechenregeln einführen, die uns einen algebraischen Umgang mit den Komplexitätsklassen ermöglichen.

Sicher erinnern Sie sich, dass wir die Bedeutung der Landau-Symbole  $O$  und  $\Omega$  mit Hilfe von Ungleichungen der Form  $f(n) \leq c \cdot g(n)$  bzw.  $f(n) \geq c \cdot g(n)$  definiert haben. Diese Art der Darstellung entspricht zwar weitgehend der intuitiven Vorstellung eines asymptotischen Wachstums, ist für den Beweis von Komplexitätsaussagen aber nur bedingt geeignet.

Abhilfe schafft eine alternative Charakterisierung des asymptotischen Wachstums, die auf der Grenzwertbetrachtung des Quotienten  $\frac{f(n)}{g(n)}$  beruht. Divergiert der Quotient gegen  $\infty$  bzw. konvergiert er gegen 0, so können wir daraus schließen, dass die Funktion  $f$  asymptotisch schneller bzw. asymptotisch langsamer wächst als  $g$ . Konvergiert der Quotient gegen einen konstanten Wert größer null, so zeigen  $f$  und  $g$  das gleiche asymptotische Wachstum. Insgesamt erhalten wir die folgende Grenzwertregel:



### Satz 7.1 (Grenzwertregel)

Für die Funktionen  $f, g : \mathbb{N} \rightarrow \mathbb{R}^+$  gilt der folgende Zusammenhang:

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} < \infty \Rightarrow f(n) = O(g(n))$$

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} > 0 \Rightarrow f(n) = \Omega(g(n))$$

Neben  $O$  und  $\Omega$  lassen sich auch die anderen Landau-Symbole  $\Theta$ ,  $o$  und  $\omega$  über eine entsprechende Grenzwertbetrachtung charakterisieren. Tabelle 7.3 fasst die Ergebnisse in einer Übersicht zusammen.

Den praktischen Nutzen der Grenzwertregel wollen wir am Beispiel des asymptotischen Wachstums von Polynomen der Form

$$p(n) = a_k n^k + a_{k-1} n^{k-1} + \dots + a_1 n + a_0 \quad (7.8)$$

erproben. Fordern wir die Eigenschaft  $a_k > 0$ , so entspricht  $k$  dem *Grad* des Polynoms  $p$  und es gilt die folgende Beziehung:

$$\lim_{n \rightarrow \infty} \frac{p(n)}{n^k} = \lim_{n \rightarrow \infty} \left( a_k + \frac{a_{k-1}}{n} + \dots + \frac{a_1}{n^{k-1}} + \frac{a_0}{n^k} \right) = a_k \quad (7.9)$$

Wegen  $a_k > 0$  folgt aus der Grenzwertregel unmittelbar der folgende Satz:

Obere asymptotische Schranke ( $f$ wächst höchstens so schnell wie $g$ )		
$f(n) = O(g(n))$	$\exists c \in \mathbb{R}^+ \ \exists n_0 \in \mathbb{N} \ \forall n \geq n_0 : f(n) \leq c \cdot g(n)$	$0 \leq \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} < \infty$
Untere asymptotische Schranke ( $f$ wächst mindestens so schnell wie $g$ )		
$f(n) = \Omega(g(n))$	$\exists c \in \mathbb{R}^+ \ \exists n_0 \in \mathbb{N} \ \forall n \geq n_0 : f(n) \geq c \cdot g(n)$	$0 < \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} \leq \infty$
Exakte asymptotische Schranke ( $f$ wächst genauso schnell wie $g$ )		
$f(n) = \Theta(g(n))$	$\exists c_1, c_2 \in \mathbb{R}^+ \ \exists n_0 \in \mathbb{N} \ \forall n \geq n_0 : c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$	$0 < \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} < \infty$
Starke obere asymptotische Schranke ( $f$ wächst langsamer als $g$ )		
$f(n) = o(g(n))$	$\forall c \in \mathbb{R}^+ \ \exists n_0 \in \mathbb{N} \ \forall n \geq n_0 : c \cdot f(n) \leq g(n)$	$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$
Starke untere asymptotische Schranke ( $f$ wächst schneller als $g$ )		
$f(n) = \omega(g(n))$	$\forall c \in \mathbb{R}^+ \ \exists n_0 \in \mathbb{N} \ \forall n \geq n_0 : c \cdot f(n) \geq g(n)$	$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \infty$

**Tabelle 7.3:** Landau-Symbole in der Übersicht**Satz 7.2 (Asymptotisches Wachstum von Polynomen)**

Sei  $p(n)$  ein Polynom vom Grad  $k$ . Dann gilt  $p(n) = \Theta(n^k)$

Betrachten wir den Aufbau des Polynoms (7.8) von einem abstrakten Standpunkt aus, so können wir  $p(n)$  als eine Summe von Teiltermen unterschiedlicher Komplexitätsklassen ansehen. Zwischen den Summanden des Polynoms besteht die folgende Hierarchiebeziehung:

$$a_k n^k = o(a_{k+1} n^{k+1}) \quad (7.10)$$

Ferner hat uns Satz 7.2 gezeigt, dass das asymptotische Wachstum eines Polynoms ausschließlich durch den Summanden  $a_k n^k$  und damit durch den Teilausdruck mit dem stärksten asymptotischen Wachstum bestimmt wird. Wir wollen dieses Ergebnis verallgemeinern und betrachten jetzt die Summe zweier Funktionen  $f$  und  $g$  mit  $f(n) = o(g(n))$ . Unter Verwendung der oben eingeführten Grenzwerte können wir diese Eigenschaft auch so formulieren:

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0 \quad (7.11)$$

Da sich der Quotient der Nulllinie immer weiter annähert, existiert ein  $n_0 \in \mathbb{N}$  mit

$$0 \leq \frac{f(n)}{g(n)} \leq 1 \quad \text{für alle } n \geq n_0. \quad (7.12)$$

Jetzt können wir die Summe  $f(n) + g(n)$  für  $n \geq n_0$  wie folgt abschätzen:

$$f(n) + g(n) \leq g(n) + g(n) \leq 2 \cdot g(n) \quad (7.13)$$

Voilá. Auch hier wird die Komplexitätsklasse ausschließlich durch den dominierenden Summanden  $g$  bestimmt und wir haben einen Beweis für den folgenden Satz gefunden:



### Satz 7.3 (Summation im O-Kalkül)

Seien  $f, g : \mathbb{N} \rightarrow \mathbb{R}^+$  zwei Funktionen mit  $f = o(g(n))$ . Dann gilt:

$$f(n) + g(n) = O(g(n)) \quad (7.14)$$

Der Satz hat weitreichende Konsequenzen für das Rechnen im O-Kalkül, schließlich wird die asymptotische Komplexität einer Summe ausschließlich durch denjenigen Summanden mit der höchsten Wachstumsordnung bestimmt. Haben wir diesen identifiziert, so können wir die Komplexitätsklasse durch das Weglassen aller anderen Terme sofort bestimmen.

Satz 7.3 ist zugleich die Begründung, warum wir niemals Ausdrücke wie z. B.  $O(3 \cdot n^3 + 7 \cdot n^2)$  angeben werden. Da die Komplexitätsklasse einzig und alleine durch den kubischen Term  $3 \cdot n^3$  bestimmt wird, verwenden wir die vereinfachte Schreibweise  $O(n^3)$ .

Dass wir den konstanten Faktor 3 ebenfalls streichen können, ist eine weitere zentrale Eigenschaft des O-Kalküls. Gilt nämlich  $f(n) = O(k \cdot g(n))$  für eine Konstante  $k \in \mathbb{R}^+$ , so existieren per Definition Konstanten  $c \in \mathbb{R}^+$  und  $n_0 \in \mathbb{N}$  mit  $f(n) \leq c \cdot (k \cdot g(n))$  für alle  $n \geq n_0$ . Aus  $c \cdot (k \cdot g(n)) = (c \cdot k) \cdot g(n)$  folgt sofort die Beziehung  $f(n) = O(g(n))$  und wir erhalten auf einen Schlag das nachstehende Ergebnis:



### Definition 7.6 (Multiplikation im O-Kalkül)

Für beliebige Funktionen  $g : \mathbb{N} \rightarrow \mathbb{R}^+$  und Konstanten  $k \in \mathbb{R}^+$  gilt:

$$O(k \cdot g(n)) = O(g(n)) \quad (7.15)$$

Aus Satz 7.6 können wir eine interessante Eigenschaft über das asymptotische Wachstum der Logarithmus-Funktion ableiten. Zunächst halten wir fest, dass der Logarithmus für beliebige Basen  $a$  und  $b$  die folgende Beziehung erfüllt:

$$\begin{aligned} \log_a x &= \log_a b^{\log_b x} \\ &= (\log_a b) \cdot \log_b x \end{aligned}$$

Die Umformung zeigt, dass sich die verschiedenen Logarithmus-Funktionen nur durch einen konstanten Faktor voneinander unterscheiden. Jetzt greift Satz 7.6 und garantiert uns für beliebige Basen  $a$  und  $b$  die Beziehung

$$O(\log_a n) = O(\log_b n)$$

Die asymptotische Komplexität der Logarithmusfunktion bleibt durch die konkrete Wahl der Basis gänzlich unbeeinflusst. Aus diesem Grund dürfen wir die Komplexitätsklasse ruhigen Gewissens in der basenunabhängigen Form

$$O(\log n)$$

angeben, ohne an Präzision zu verlieren. Beachten Sie, dass sich diese Eigenschaft nicht auf die Umkehrfunktion des Logarithmus – die Exponentialfunktion – überträgt. Hier gilt für  $a \neq b$  die Beziehung

$$O(a^n) \neq O(b^n),$$

d. h., jede Basis definiert hier in der Tat eine eigene Komplexitätsklasse.

$O(\log_a n) = O(\log_b n)$

$O(a^n) \neq O(b^n)$



Wachstumsfunktion	
$f_0(n)$	$= O(1)$
$f_1(n)$	$= O(\log \log \log n)$
$f_2(n)$	$= O(\log \log n)$
$f_3(n)$	$= O(\sqrt{\log n})$
$f_4(n)$	$= O(\log n)$
$f_5(n)$	$= O((\log n)^2)$
$f_6(n)$	$= O(\sqrt[3]{n})$
$f_7(n)$	$= O(n)$
$f_8(n)$	$= O(n \log n)$
$f_9(n)$	$= O(\sqrt{n^3})$
$f_{10}(n)$	$= O(n^2)$
$f_{11}(n)$	$= O(n^3)$
$f_{12}(n)$	$= O(n^{\log n})$
$f_{13}(n)$	$= O(2^{\sqrt{n}})$
$f_{14}(n)$	$= O(2^n)$
$f_{15}(n)$	$= O(e^n)$
$f_{16}(n)$	$= O(n!)$
$f_{17}(n)$	$= O(n^n)$
$f_{18}(n)$	$= O(2^{n^2})$
$f_{19}(n)$	$= O(2^{2^n})$

**Tabelle 7.4:** Hierarchie verschiedener Wachstumsfunktionen

## 7.2 Komplexitätsklassen

Mit Hilfe der verschiedenen Laudau-Notationen sind wir in der Lage, Wachstumsfunktionen in verschiedene Äquivalenzklassen einzuteilen. Diese bilden untereinander eine Hierarchie, die in Tabelle 7.4 auszugsweise zusammengefasst ist. Alle gelisteten Funktionen erfüllen die Beziehung

$$\lim_{n \rightarrow \infty} \frac{f_i}{f_{i+1}} = 0, \quad 0 \leq i \leq 18 \quad (7.16)$$

Gleichung (7.16) ist gleichbedeutend mit  $f_i(n) = o(f_{i+1})$ , so dass jede der abgebildeten Funktionen bewiesenermaßen eine eigenständige Komplexitätsklasse definiert.

In der Realität sind die vorgestellten Wachstumsfunktionen unterschiedlich oft anzutreffen. Von besonderer Bedeutung sind dort die folgenden Komplexitätsklassen:

### ■ $O(1)$ (Konstanter Ressourcenverbrauch)

Diese Komplexitätsklasse spielt nahezu ausschließlich in der Speicherplatzanalyse eine Rolle. Der Speicherplatzverbrauch eines solchen Algorithmus ist konstant und wird durch die Eingabegröße  $n$  nicht beeinflusst. Läge die Laufzeit in der Klasse  $O(1)$ , so könnte der Algorithmus immer nur eine konstante Anzahl an Eingabezeichen auswerten – unabhängig von der wahren Eingabelänge. Es erfordert eine gehörige Portion destruktiven Scharfsinns, um einen sinnvollen Algorithmus mit dieser Eigenschaft hervorzubringen.

### ■ $O(\log n)$ (Logarithmisches Wachstum)

Viele Algorithmen, die nach dem *Teile-und-herrsche-Prinzip (divide and conquer)* arbeiten, fallen in diese Kategorie. Ein logarithmischer Zeitaufwand entsteht z. B. dann, wenn ein Problem der Länge  $n$  in jedem Verarbeitungsschritt auf ein Problem der Länge  $\frac{n}{2}$  reduziert wird. Beispiele sind die Suche innerhalb eines Binärbaums oder das ordnungserhaltende Einfügen in eine sortierte Liste [83].

### ■ $O(n)$ (Lineares Wachstum)

Die Laufzeit bzw. der Speicherplatzverbrauch eines solchen Algorithmus nimmt proportional mit der Eingabegröße  $n$  zu. Algorithmen mit dieser Eigenschaft gibt es zuhauf. Bekannte Vertreter linearer Laufzeitalgorithmen sind z. B. die Suche eines Elements in einem unsortierten Array oder die Multiplikation zweier  $n$ -stelliger Vektoren.

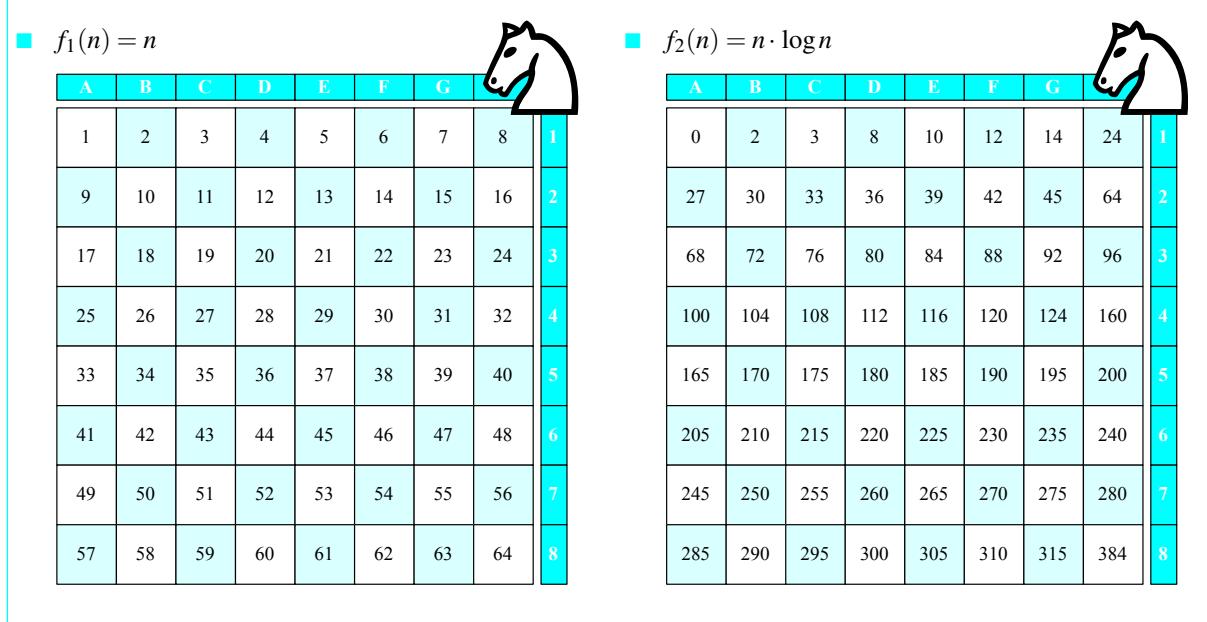


Abbildung 7.8: Die Wachstumsfunktionen  $n$  und  $n \cdot \log n$  im Vergleich

#### ■ $O(n \log n)$ (Linear-logarithmisches Wachstum)

In der Praxis kommen viele Algorithmen zum Einsatz, deren Laufzeit proportional mit dem Produkt  $n \cdot \log n$  zunimmt. Beispiele sind die Sortierung einer Liste (Heapsort [98], Mergesort [60]), die Berechnung der schnellen Fourier-Transformation (*Fast Fourier Transform*, kurz FFT) oder die Bestimmung der kürzesten Route für die Pkw-Navigation.

#### ■ $O(n^k)$ (Polynomielles Wachstum)

Die asymptotische Entwicklung der Laufzeit bzw. des Platzbedarfs wird in diesen Algorithmen durch ein Polynom begrenzt. Ein bekanntes Beispiel für einen polynomiellen Laufzeitalgorithmus ist die Multiplikation zweier  $n \times n$ -Matrizen. Auch das schon häufiger erwähnte PRIME-Problem lässt sich in Polynomialzeit lösen und fällt damit in diese Algorithmenklasse.

#### ■ $O(k^n)$ (Exponentielles Wachstum)

Die Laufzeit bzw. der Platzbedarf dieser Algorithmen nimmt exponentiell mit der Eingabelänge  $n$  zu und wächst damit stärker als jedes Polynom. Die enorme Wachstumsgeschwindigkeit der Exponentialfunktion schränkt den praktischen Nutzen dieser Algorithmen

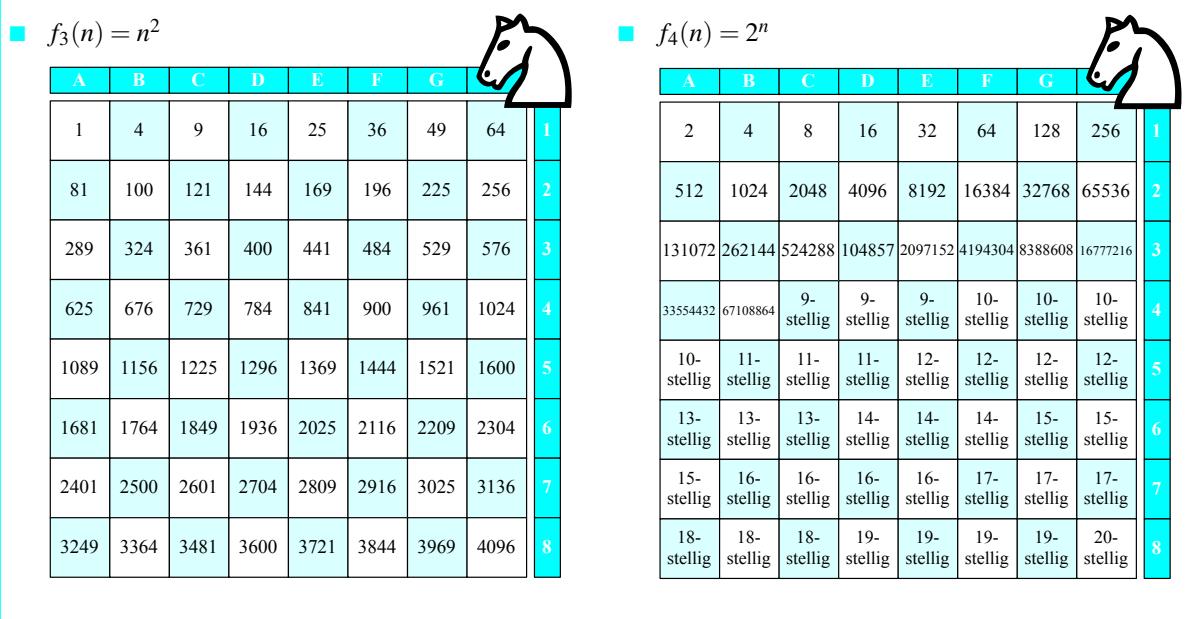


Abbildung 7.9: Die Wachstumsfunktionen  $n^2$  und  $2^n$  im Vergleich

drastisch ein; oft scheinen Algorithmen aus dieser Klasse schon für kleine Eingabegrößen augenscheinlich nicht mehr zu terminieren.

Wir wollen unser Augenmerk auf zwei Besonderheiten der aufgelisteten Wachstumsfunktionen richten. Die erste Beobachtung betrifft das linear-logarithmische Wachstum. Da die Laufzeit dieser Algorithmen überproportional mit der Eingabegröße  $n$  anwächst, scheint deren praktische Verwertbarkeit auf den ersten Blick fraglich zu sein. Bei genauerer Betrachtung stellt sich diese Wachstumsklasse jedoch als erstaunlich harmlos heraus – selbst große Eingaben lassen sich in der Praxis sehr effizient verarbeiten. Um Ihnen ein Gefühl für das Wachstumsverhalten zu vermitteln, ist in Abbildung 7.8 das linear-logarithmische Wachstum dem linearen Wachstum gegenübergestellt. Dass die überproportionale Zunahme so moderat ausfällt, verdanken wir der außerordentlich geringen Geschwindigkeit, mit der die Logarithmus-Funktion gegen unendlich strebt.

Ein weiteres erstaunliches Ergebnis offenbart Abbildung 7.9. Die Gegenüberstellung der beiden Komplexitätsklassen  $O(n^2)$  und  $O(2^n)$  zeigt, wie stark sich das polynomielle und das exponentielle Wachstum wirklich unterscheiden. Die Exponentialfunktion steigt so schnell

an, dass der genaue Funktionswert bereits für vergleichsweise kleine  $n$  nicht mehr exakt in die Felder eingetragen werden kann.

Die exponentielle Wachstumsgeschwindigkeit unterscheidet sich so eklatant von der polynomiellen Wachstumsgeschwindigkeit, dass die meisten theoretischen Informatiker hier die Trennlinie zwischen den praktisch lösbar und praktisch unlösbar Problemen ziehen. Grob gesprochen gilt ein Problem  $P$  als praktisch unlösbar, wenn alle Algorithmen für  $P$  ein exponentielles Laufzeitverhalten aufzeigen (vgl. Abbildung 7.10).

In der theoretischen Informatik ist der Unterschied zwischen den polynomiellen und den exponentiellen Wachstumsklassen von so großer Bedeutung, dass wir ihren Eigenschaften im nächsten Abschnitt noch etwas tiefer auf den Zahn fühlen wollen.

## 7.2.1 P und NP

Über die Laufzeit eines Algorithmus haben wir bereits viel gesprochen, bisher aber versäumt, eine präzise Definition für diesen Begriff bereitzustellen. Dies wollen wir an dieser Stelle nachholen und das formale Gedankengerüst der Turing-Maschine entsprechend erweitern.



### Definition 7.7 (Laufzeit von Turing-Maschinen)

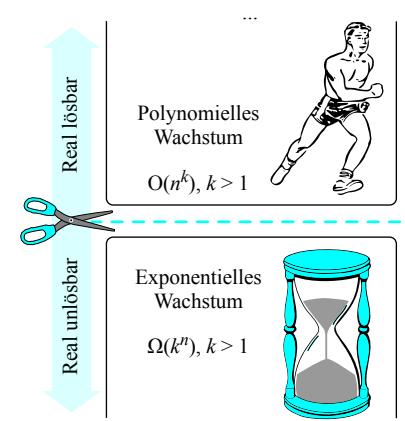
Mit  $T$  sei eine akzeptierende Mehrband-Turing-Maschine gegeben. Über die Hilfsmenge  $A$  (*Accept*) mit

$$A(\omega) := \{n \mid T \text{ terminiert nach } n \text{ Schritten in } z \in E\}$$

definieren wir die *Laufzeitfunktion*  $t_T : \Sigma^* \rightarrow \mathbb{N}$  wie folgt:

$$t_T(\omega) = \begin{cases} \min A(\omega) & \text{falls } A(\omega) \neq \emptyset \\ 0 & \text{falls } A(\omega) = \emptyset \end{cases}$$

Definition 7.7 enthält einige Besonderheiten, die eine nähere Betrachtung verdienen. Zunächst fällt auf, dass der Laufzeitbegriff für akzeptierende Turing-Maschinen formuliert ist. Dies stellt keine Einschränkung im eigentlichen Sinne dar, da wir gezeigt haben, dass zwischen der Entscheidbarkeit einer Sprache, der Berechenbarkeit einer Funktion und der Lösung eines Ja-Nein-Problems kein prinzipieller Unterschied



**Abbildung 7.10:** Der Übergang von polynomiellen zu exponentiellen Wachstumsfunktionen bildet in der theoretischen Informatik die Grenze zwischen real lösbar und real unlösbar Problemen.

Die Ergebnisse dieses Abschnitts haben uns dazu gebracht, polynomiale Probleme als praktisch lösbar und exponentielle Probleme als praktisch unlösbar anzusehen. Wir wollen diese Sichtweise auf den Prüfstand stellen und uns mit der Frage beschäftigen, ob die imaginär gezogene Trennlinie überhaupt existiert oder ob es vielleicht Wachstumsfunktionen gibt, die stärker als jedes Polynom, aber schwächer als jede Exponentialfunktion steigen. In der Tat haben wir in Tabelle 7.4 mit  $n^{\log_a n}$  eine solche Funktion bereits kennen gelernt. Da  $\log_a n$  mit wachsendem  $n$  gegen unendlich strebt, gilt

$$n^{\log_a n} = \omega(n^k)$$

für alle  $k \in \mathbb{N}$ . Andererseits gilt

$$n^{\log_a n} = a^{\log_a(n^{\log_a n})} = a^{(\log_a n)^2}$$

Die Funktion wächst langsamer als jede Exponentialfunktion der Form  $k^n$  und wir erhalten die Beziehung:

$$n^{\log_a n} = o(k^n)$$

Algorithmen mit solchen Komplexitäten sind in der Realität jedoch so selten anzutreffen, dass sie praktisch kaum eine Rolle spielen. Dies ist der Grund, warum wir die Trennlinie des praktisch Lösbareren auch weiterhin zwischen polynomiellem und exponentiellem Wachstumsraten ziehen dürfen.

Beachten Sie, dass nicht jedes Problem, für das ein polynomieller Algorithmus existiert, auch wirklich einfach lösbar ist. In der Praxis sind die zu verarbeitenden Eingaben oft so groß, dass bereits diejenigen Algorithmen an ihre Grenze stoßen, die aus theoretischer Sicht „nur“ ein quadratisches Laufzeitverhalten zeigen. Viele Praktiker sehen daher im Übergang von  $\Theta(n \log n)$  nach  $\Theta(n^2)$  die wahre kritische Grenze, die zwischen real anwendbaren und faktisch nutzlosen Algorithmen unterscheidet.

besteht. Alle erzielten Ergebnisse lassen sich in diese Richtung verallgemeinern und wir können mit demselben Begriffsinstrumentarium über die Zeitkomplexität von Problemen oder Funktionen sprechen.

Zudem fällt auf, dass wir mit  $T$  explizit eine Turing-Maschine mit mehreren Bändern zugrunde gelegt haben. Die vorgenommene Verallgemeinerung ist der Tatsache geschuldet, dass Rechenschritte, die auf modernen Computeranlagen als elementar angesehen werden können, in Turings Basismodell nur umständlich, d. h. mit einer anderen Laufzeitkomplexität, durchgeführt werden können. Aus dem Originalmodell abgeleitete Laufzeitergebnisse lassen sich hierdurch nur sehr eingeschränkt auf die Realität übertragen. Mehrband-Turing-Maschinen ähneln modernen Computerarchitekturen dagegen in vielerlei Hinsicht, so dass sich die theoretischen Ergebnisse nahezu eins zu eins auf die realen Gegebenheiten übertragen lassen.

Des Weiteren haben wir in Definition 7.7 die Beziehung  $t_T(\omega) = 0$  vereinbart, falls  $T$  das Eingabewort  $\omega$  zurückweist. Damit wird die Laufzeit alleine durch die Wörter  $\omega$  bestimmt, die von  $T$  akzeptiert werden.

Auf der Laufzeitfunktion  $t_T$  aufbauend definieren wir die Komplexitätsklasse TIME( $f(n)$ ):



### Definition 7.8 (Klasse TIME)

Eine Sprache  $L$  liegt in TIME( $f(n)$ ), falls eine *deterministische* Mehrband-Turing-Maschine  $T$  mit den folgenden Eigenschaften existiert:

- $\mathcal{L}(T) = L$
- Für alle Wörter  $\omega \in \Sigma^*$  gilt  $t_T(\omega) \leq f(|\omega|)$

Während  $t_T$  die Laufzeit einer Turing-Maschine für spezielle Wörter beschreibt, stellt Definition 7.8 einen Zusammenhang zwischen der Anzahl der Berechnungsschritte und der Länge der Eingabe her. Damit sind wir in der Lage, sämtliche Wachstumsberechnungen aus den vorherigen Abschnitten auf Turing-Maschinen zu übertragen.

Beachten Sie, dass in der Definition von TIME( $f(n)$ ) explizit gefordert wird, dass die zugrunde liegende Turing-Maschine deterministisch ist. Heben wir diese Beschränkung auf, so gelangen wir ohne Umwege zur nichtdeterministischen Komplexitätsklasse NTIME( $f(n)$ ):



### Definition 7.9 (Klasse NTIME)

Eine Sprache  $L$  liegt in  $\text{NTIME}(f(n))$ , falls eine *nichtdeterministische* Mehrband-Turing-Maschine  $T$  mit den folgenden Eigenschaften existiert:

- $\mathcal{L}(T) = L$
- Für alle Wörter  $\omega \in \Sigma^*$  gilt  $t_T(\omega) \leq f(|\omega|)$

Da jede deterministische Turing-Maschine im formalen Sinne auch nichtdeterministisch ist, folgt sofort die Inklusionsbeziehung

$$\text{TIME}(f(n)) \subseteq \text{NTIME}(f(n)) \quad (7.17)$$

Auf Basis von TIME und NTIME lassen sich weitere Komplexitätsklassen ableiten, indem wir  $f(n)$  durch konkrete Funktionen ersetzen. Von besonderem Interesse sind diejenigen Sprachen  $L$ , die von Turing-Maschinen in polynomieller Laufzeit akzeptiert werden:



### Definition 7.10 (P, NP)

Die polynomiellen Komplexitätsklassen P und NP sind wie folgt definiert:

$$P := \bigcup_{k \in \mathbb{N}} \text{TIME}(n^k)$$

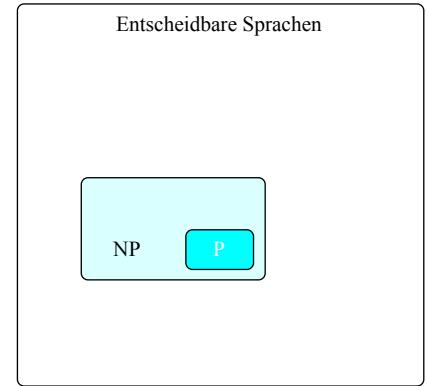
$$NP := \bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k)$$

Aus Gleichung (7.17) folgt unmittelbar die Inklusionsbeziehung

$$P \subseteq NP \quad (7.18)$$

Landläufig wird  $P$  auch als die Klasse der *effizient entscheidbaren Sprachen*, der *effizient berechenbaren Funktionen* oder der *effizient lösbaren Probleme* bezeichnet. Abbildung 7.11 stellt die Inklusionsbeziehungen der bisher eingeführten Komplexitätsklassen grafisch gegenüber.

Auch wenn der Unterschied zwischen den Klassen P und NP auf den ersten Blick unscheinbar wirkt, könnten seine Auswirkungen kaum größer sein. So existieren viele praktische Problemstellungen, die mit Hilfe nichtdeterministischer Algorithmen sehr einfach gelöst werden können,



**Abbildung 7.11:** Inklusionsbeziehungen der bisher eingeführten Komplexitätsklassen

■ Nichtdeterministische Lösung

**solveSAT.ndet**

```

1 // guess
2  $x_1 := 0 \text{ or } 1$ 
3 ...
4  $x_n := 0 \text{ or } 1$ 
5
6 // verify
7 if ( $F(x_1, \dots, x_n) \equiv 1$ )
8   return true;
9 else
10  return false;
11
12

```

■ Deterministische Lösung

**solveSAT.det**

```

1 // brute force attack
2 forall  $x_1$  in {0,1} {
3   ...
4     forall  $x_n$  in {0,1} {
5       if ( $F(x_1, \dots, x_n) \equiv 1$ )
6         return true;
7     }
8   ...
9 }
10 return false;
11
12

```

**Abbildung 7.12:** Nichtdeterministische und deterministische Implementierung zur Lösung des SAT-Problems

sich einer effizienten deterministischen Lösung aber vehement zu entziehen scheinen.

Abbildung 7.12 demonstriert das Gesagte am Beispiel des Problems SAT, dem wir bereits im Einführungskapitel in Abschnitt 1.2.4 begegnet sind. Hinter SAT verbirgt sich die Frage, ob für eine gegebene aussagenlogische Formel  $F$  eine erfüllende Belegung der Variablen existiert oder nicht. Nichtdeterministisch ist das Problem auf einfache Weise lösbar, indem wir zunächst die richtige Kombination von Wahrheitswerten erraten und anschließend zeigen, dass  $F$  für diese Belegung tatsächlich den Wahrheitswert 1 annimmt. Der Algorithmus ist nicht nur einfach, sondern auch effizient. Bezeichnet  $n$  die Länge der Formel  $F$ , so müssen wir für maximal  $n$  Variablen die Belegung erraten und  $F$  anschließend auswerten. Beide Schritte lassen sich mit linearem Zeitaufwand erledigen.

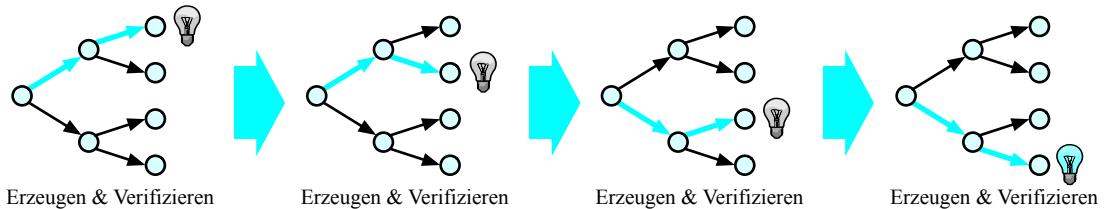
Natürlich sind wir auch in der Lage, einen Algorithmus zu formulieren, der das SAT-Problem deterministisch löst. Wie in Abbildung 7.12 (unten) gezeigt, schreiben wir hierzu ein Programm, das sämtliche Wahrheitswertkombinationen erzeugt und  $F$  jedes Mal aufs Neue auf Erfüllbarkeit prüft. Leider müssen wir für einen Ausdruck mit  $n$  Variablen  $2^n$  verschiedene Kombinationen in Betracht ziehen, so dass die Laufzeit unseres Algorithmus exponentiell zunimmt. In der Praxis werden wir mit dieser Methode nur für sehr kleine Ausdrücke in der Lage sein, das Erfüllbarkeitsproblem zu entscheiden.

Die Art und Weise, wie wir das SAT-Problem nichtdeterministisch gelöst haben, lässt sich für viele weitere Problemstellungen verallgemeinern. In Frage kommen alle Probleme, die über einen großen, meist exponentiell wachsenden Suchraum verfügen und zudem die Eigenschaft besitzen, dass sich eine gefundene Lösung mit geringem Aufwand als solche verifizieren lässt. Deterministischen Algorithmen bleibt in der Regel nichts anderes üblich, als den Suchraum systematisch zu durchkämmen (*Brute-Force-Methode*). Wächst dieser exponentiell mit der Eingabegröße an, so erhalten wir einen Algorithmus, der in der Praxis nur für sehr kleine Eingaben ein akzeptables Laufzeitverhalten zeigt.

Das im Jahre 1959 von Dana Scott und Michael Rabin eingeführte Konzept der nichtdeterministischen Berechnung überwindet dieses Problem. Wie in Abschnitt 6.3 ausführlich dargelegt, akzeptiert eine nichtdeterministische Turing-Maschine ein Wort genau dann, wenn mindestens eine Berechnungsfolge existiert, die in einem akzeptierenden Zustand endet. Die Definition erlaubt ganz bewusst, dass weitere Pfade existieren, die zu einer unendlichen Berechnungsfolge führen oder in einem nichtakzeptierenden Zustand enden. Aus algorithmischer Sicht

■ Deterministische Lösungsstrategie

Der Suchraum wird systematisch durchkämmt (Brute-Force-Methode).



■ Nichtdeterministische Lösungsstrategie

Der richtige Berechnungspfad wird geraten und die Lösung anschließend verifiziert (Orakelprinzip).

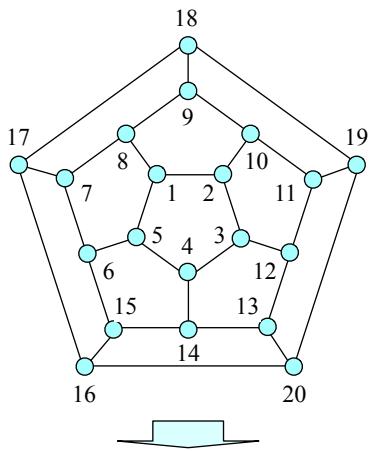


**Abbildung 7.13:** Deterministische und nichtdeterministische Lösungsstrategien im Vergleich

entspricht dieses Konzept einem Programm nach dem oben diskutierten Schema. Die potenzielle Lösung wird erraten und am Ende nur noch auf Gültigkeit überprüft. Abbildung 7.13 stellt die deterministische Lösungsstrategie der nichtdeterministischen nach Scott und Rabin grafisch gegenüber.

Wie nutzbringend die nichtdeterministische Berechnung ist, verdeutlicht auch das in Abschnitt 1.2.4 diskutierte Hamilton-Problem. Für einen gegebenen Graphen  $G$  galt es zu entscheiden, ob ein Rundweg existiert, der jeden Knoten exakt einmal passiert. Auch hier steht ein exponentieller Suchraum der Eigenschaft gegenüber, dass sich für einen gegebenen Pfad mit wenig Aufwand entscheiden lässt, ob er das Hamilton-Problem löst oder nicht. Folgerichtig können wir ein nichtdeterministisches Lösungsverfahren konstruieren, das im ersten Schritt einen geschlossenen Linienzug errät und anschließend die Hamilton-Eigenschaft überprüft. Abbildung 7.14 demonstriert die Lösungsstrategie anhand eines konkreten Beispiels.

■ Eingabe: Graph  $G$

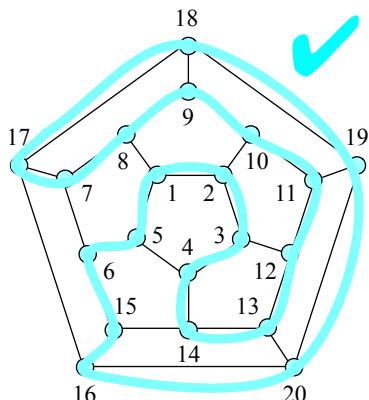


■ Raten

$1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 14 \rightarrow$   
 $13 \rightarrow 12 \rightarrow 11 \rightarrow 10 \rightarrow 9 \rightarrow$   
 $8 \rightarrow 7 \rightarrow 17 \rightarrow 18 \rightarrow 19 \rightarrow$   
 $20 \rightarrow 16 \rightarrow 15 \rightarrow 6 \rightarrow 5 \rightarrow 1$



■ Verifizieren



**Abbildung 7.14:** Nondeterministisch kann das Hamilton-Problem auf einfache Weise gelöst werden.

## 7.2.2 PSPACE und NPSPACE

Die Klassen P und NP haben wir über die Laufzeitkomplexität von Turing-Maschinen definiert. Der Bandplatz, den eine Maschine während einer Berechnung belegt, wurde bisher vollständig außen vor gelassen. Hierfür existieren mit PSPACE und NPSPACE eigene Komplexitätsklassen, die der gleichen Kernidee folgen. Bevor wir die Klassen formal definieren, wollen wir aber zunächst festlegen, was wir genau unter dem Platzbedarf einer (nichtdeterministischen) Turing-Maschine verstehen wollen.



### Definition 7.11 (Platzbedarf von Turing-Maschinen)

Mit  $T$  sei eine akzeptierende Mehrband-Turing-Maschine gegeben. Über die Hilfsmenge  $A$  (*Accept*) mit

$$A(\omega) := \{n \mid T \text{ benutzt } n \text{ Zellen und terminiert in } z \in E\}$$

definieren wir die *Bandplatzfunktion*  $s_T : \Sigma^* \rightarrow \mathbb{N}$  wie folgt:

$$s_T(\omega) = \begin{cases} \min A(\omega) & \text{falls } A(\omega) \neq \emptyset \\ 0 & \text{falls } A(\omega) = \emptyset \end{cases}$$

Die Bandplatzfunktion  $s_T$  ist der Schlüssel für die Definition der Platzklassen PSPACE und NPSPACE:



### Definition 7.12 (PSPACE und NPSPACE)

Eine Sprache  $L$  liegt in PSPACE, falls eine *deterministische* Mehrband-Turing-Maschine  $T$  und ein Polynom  $p(n) \in \mathbb{R}[n]$  mit den folgenden Eigenschaften existieren:

- $\mathcal{L}(T) = L$
- Für alle Wörter  $\omega \in \Sigma^*$  gilt  $s_T(\omega) \leq p(|\omega|)$

$L$  liegt in NPSPACE, wenn eine *nichtdeterministische* Mehrband-Turing-Maschine mit den genannten Eigenschaften existiert.

Obwohl die Platzklassen PSPACE und NPSPACE einen völlig anderen Aspekt als die Zeitklassen P und NP betrachten, lässt sich zwischen beiden eine Verbindung herstellen. Nimmt der Speicherplatzbedarf eines Algorithmus z. B. quadratisch mit der Eingabelänge  $n$  zu, so werden

zum Beschreiben des Speichers mindestens  $n^2$  Rechenschritte benötigt. Kurzum: Die Zeitkomplexität eines Algorithmus kann niemals kleiner sein als seine Platzkomplexität.

Ein anderes wichtiges Resultat bewies der US-amerikanische Computerwissenschaftler Walter Savitch im Jahre 1970. Er konnte zeigen, dass jede von einer nichtdeterministischen Turing-Maschine akzeptierte Sprache mit einer deterministischen Turing-Maschine akzeptiert werden kann, deren Platzbedarf nur quadratisch höher liegt [80]. Folgerichtig geht die Eigenschaft des polynomiellen Platzbedarfs durch die Übersetzung in eine deterministische Maschine nicht verloren und wir erhalten auf einen Schlag die Beziehung  $\text{PSPACE} = \text{NPSPACE}$ . Zusammengefasst ergibt sich die folgende Inklusionskette (vgl. Abbildung 7.15):



#### Satz 7.4 (Klassenhierarchie)

$$\text{P} \subseteq \text{NP} \subseteq \text{PSPACE} = \text{NPSPACE}$$

Ob zwischen den Klassen P und NP eine echte Inklusionsbeziehung besteht, ist gegenwärtig ungeklärt. In Abschnitt 7.3 werden wir uns näher damit beschäftigen, wie beide Klassen zusammenhängen.

### 7.2.3 EXP und NEXP

In Analogie zu den polynomiellen Komplexitätsklassen P und NP definieren wir die exponentiellen Komplexitätsklassen EXP und NEXP:



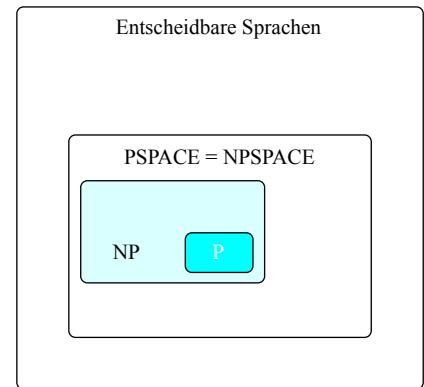
#### Definition 7.13 (EXP, NEXP)

Die exponentiellen Komplexitätsklassen EXP und NEXP sind wie folgt definiert:

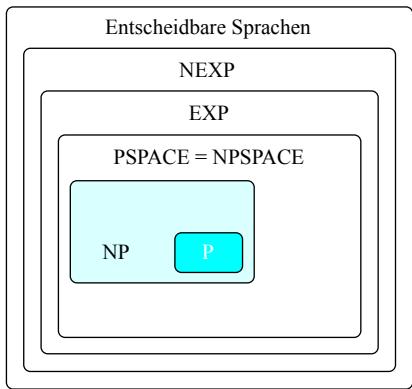
$$\text{EXP} := \bigcup_{c,k \in \mathbb{N}} \text{TIME}(c^{n^k})$$

$$\text{NEXP} := \bigcup_{c,k \in \mathbb{N}} \text{NTIME}(c^{n^k})$$

In den Klassen EXP und NEXP sind somit alle Sprachen enthalten, die in höchstens exponentieller Laufzeit durch eine deterministische bzw. eine nichtdeterministische Turing-Maschine entschieden werden



**Abbildung 7.15:** Inklusionsbeziehungen der bisher eingeführten Komplexitätsklassen



**Abbildung 7.16:** Inklusionsbeziehungen der bisher eingeführten Komplexitätsklassen

können. Offensichtlich gilt zwischen EXP und seiner nichtdeterministischen Variante NEXP die folgende Inklusionsbeziehung:

$$\text{EXP} \subseteq \text{NEXP} \quad (7.19)$$

Wir wollen nun versuchen, die Klassen EXP und NEXP in Bezug zu den bisher eingeführten Klassen zu stellen. Zunächst halten wir fest, dass Wachstumsraten existieren, die jenseits des Exponentiellen liegen. So haben wir in Tabelle 7.4 mit  $O(2^{2^n})$  bereits eine Funktion kennen gelernt, die stärker wächst als die in Definition 7.13 gewählten Exponentialfunktionen. Hieraus folgt, dass die Klassen EXP und NEXP echte Teilmengen der entscheidbaren Sprachen sind.

Weniger offensichtlich ist die Beziehung, die zwischen der Speicherplatzklasse PSPACE und der Laufzeitklasse EXP besteht. Um diese Beobachtung zu vertiefen, nehmen wir an,  $T$  sei eine Turing-Maschine, deren Platzverbrauch nur polynomiell mit der Größe der Eingabe  $\omega$  wächst. Da wir die Anzahl der belegten Bandzellen von  $T$  durch ein Polynom  $p(|\omega|)$  nach oben abschätzen können, gelingt uns gleichzeitig eine quantitative Aussage über die Konfigurationen, in denen sich  $T$  befinden kann. Da eine Konfiguration durch den aktuellen Zustand ( $|S|$  Möglichkeiten), die Kopfposition ( $p(|\omega|)$  Möglichkeiten) und den Bandinhalt ( $|\Pi|^{p(|\omega|)}$  Möglichkeiten) eindeutig bestimmt ist, können maximal

$$p(|\omega|) \cdot |S| \cdot |\Pi|^{p(|\omega|)} \quad (7.20)$$

verschiedene Konfigurationen existieren. Da die Turing-Maschine deterministisch arbeitet, kann sie nur terminieren, wenn sie niemals dieselbe Konfiguration zweimal einnimmt. Damit ist der Ausdruck (7.20) gleichermaßen eine Abschätzung für die Anzahl der Konfigurationsübergänge. Da sich (7.20) selbst durch einen Term der Form  $c^{n^k}$  abschätzen lässt, ist die Laufzeit von  $T$  exponentiell nach oben begrenzt. Mit anderen Worten: PSPACE liegt in EXP. In Kombination mit der Inklusionsbeziehung (7.19) erhalten wir das folgende Ergebnis:

### Satz 7.5

$$\text{PSPACE} \subseteq \text{EXP} \subseteq \text{NEXP}$$

Abbildung 7.16 fasst die bisher herausgearbeiteten Ergebnisse grafisch zusammen.

### 7.2.4 Komplementäre Komplexitätsklassen

Zu jeder Komplexitätsklasse  $C$  existiert eine komplementäre Komplexitätsklasse, die wir als  $\text{co}C$  bezeichnen. Formal definieren wir diese wie folgt:



#### Definition 7.14 (Komplementäre Komplexitätsklasse)

Mit  $C$  sei eine beliebige Komplexitätsklasse gegeben. Die Menge

$$\text{co}C := \{L \mid \bar{L} \in C\}$$

ist die *komplementäre Komplexitätsklasse* von  $C$ .

Eine Sprache  $L$  gehört demnach genau dann zur Klasse  $\text{co}C$ , wenn ihr Komplement  $\bar{L}$  zu  $C$  gehört.

Im Folgenden wollen wir die Eigenschaften der Komplementärklasse genauer untersuchen. Hierzu nehmen wir zunächst an, dass mit  $C$  eine deterministische Komplexitätsklasse gegeben ist. In diesem Fall existiert für jede Sprache  $L$  eine deterministische Turing-Maschine  $T$ , die für alle Eingaben  $\omega$  nach endlich vielen Berechnungsschritten terminiert. Ist  $\omega \in L$ , so liefert  $T$  die Antwort „ja“, ansonsten „nein“. Invertieren wir die Menge der Endzustände, so erhalten wir eine Maschine  $T'$ , die das Komplement  $\bar{L}$  entscheidet. Da sich das Laufzeitverhalten der Maschine nicht verändert hat, liegt  $T'$  in der gleichen Komplexitätsklasse wie  $T$ . Aus  $L \in C$  folgt damit stets die Beziehung  $\bar{L} \in C$ , so dass die Mengen  $\text{co}C$  und  $C$  exakt die gleichen Elemente enthalten müssen. Damit haben wir einen Beweis für den folgenden Satz erbracht:



#### Satz 7.6

Für jede *deterministische* Komplexitätsklasse  $C$  gilt  $C = \text{co}C$ .

Ersetzen wir  $C$  in Satz 7.6 durch die deterministischen Komplexitätsklassen P oder PSPACE, so erhalten wir das folgenden Ergebnis:

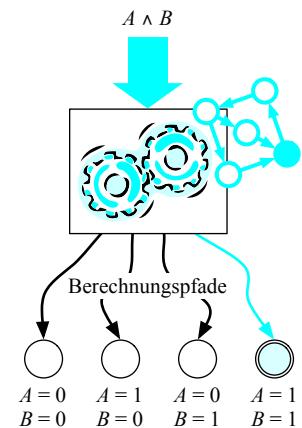


#### Korollar 7.1

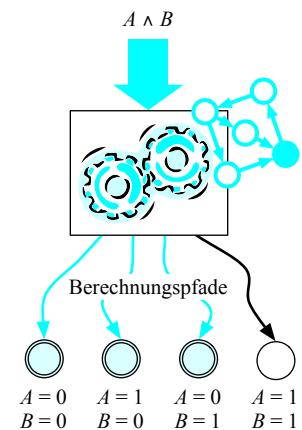
Für die Komplexitätsklassen P und PSPACE gilt:

$$P = \text{co}P \text{ und } \text{PSPACE} = \text{coPSPACE}$$

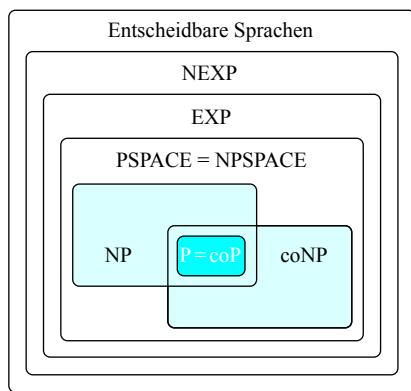
#### Turing-Maschine $T$



#### $T$ nach der Zustandsinvertierung



**Abbildung 7.17:** Vorsicht bei nichtdeterministischen Turing-Maschinen! Im Gegensatz zu deterministischen Maschinen reicht es nicht aus, die Menge der Endzustände zu invertieren, um einen Akzeptor für die Sprache  $\mathcal{L}(T)$  zu erhalten.



**Abbildung 7.18:** Inkluusionsbeziehungen der bisher eingeführten Komplexitätsklassen

Auf nichtdeterministische Komplexitätsklassen lassen sich die getätigten Überlegungen nicht übertragen. Invertieren wir die Menge der Endzustände einer nichtdeterministischen Turing-Maschine, so erhalten wir – anders als im deterministischen Fall – keinen Akzeptor für die Komplementsprache. Der Grund hierfür liegt in der Definition des Nichtdeterminismus verborgen. Um ein Wort zu akzeptieren, reicht es aus, dass ein einziger Berechnungspfad in einen Endzustand führt; andere Pfade dürfen dagegen in beliebigen Zuständen terminieren.

Abbildung 7.17 demonstriert das Problem am Beispiel einer nichtdeterministischen Turing-Maschine zur Lösung von SAT. Für die Eingabe  $A \wedge B$  ergeben sich vier verschiedene Berechnungspfade, die den vier verschiedenen Variablenkombinationen von  $A$  und  $B$  entsprechen. Die Formel  $A \wedge B$  wird als erfüllbar akzeptiert, da ein Berechnungspfad existiert, der in einem Endzustand terminiert. Dieser Pfad entspricht der Kombination  $A = B = 1$ . Invertieren wir alle Endzustände, so entstehen drei Berechnungspfade, die erneut in einem Endzustand terminieren. Folgerichtig wird die Formel  $A \wedge B$  weiterhin akzeptiert.

Beachten Sie, dass es genauso falsch wäre, aus den angestellten Überlegungen die Beziehung  $NP \neq coNP$  zu folgern. Wir haben lediglich gezeigt, dass wir ein nichtdeterministisches Entscheidungsverfahren für eine Sprache  $L$  – anders als im deterministischen Fall – nicht durch die simple Invertierung der Endzustände zu einem Entscheidungsverfahren für die Komplementmenge  $\bar{L}$  umbauen können. Obwohl es als unwahrscheinlich gilt, ist es nicht ausgeschlossen, dass ein solcher Umbau auf anderem Wege funktioniert. Die Frage, ob die Gleichung  $NP = coNP$  gilt oder nicht, ist bis heute ungeklärt und gehört zu den wichtigsten ungelösten Problemen der modernen theoretischen Informatik.

Ein interessantes Ergebnis erhalten wir, wenn wir die Klasse P mit der Klasse coNP in Bezug setzen. Hierzu sei  $L$  ein Element aus P. Dann ist  $\bar{L}$  per Definition ein Element von coP. Da nach Satz 7.6 die Beziehung  $\bar{L} \in P$  gilt, folgt aus der Inkluisionseigenschaft  $P \subseteq NP$  sofort  $\bar{L} \in NP$ . Damit ist  $\bar{L} \in coNP$ .  $\bar{L}$  ist aber nichts anderes als das Element  $L$  selbst, so dass wir effektiv die Inkluision  $P \subseteq coNP$  gezeigt haben. Zusammen mit der Beziehung  $P \subseteq NP$  erhalten wir den folgenden Satz:

### Satz 7.7

Es gilt die Inkluisionsbeziehung  $P \subseteq (NP \cap coNP)$

Abbildung 7.18 fasst die bisher herausgearbeiteten Inkluisionsbeziehungen grafisch zusammen.

## 7.3 NP-Vollständigkeit

### 7.3.1 Polynomielle Reduktion

Erinnern Sie sich noch an das Prinzip der *Problemreduktion*, mit dem wir in Kapitel 6 unter anderem die Unentscheidbarkeit des Post'schen Korrespondenzproblems zeigen konnten? Die Grundidee war verblüffend einfach: Wir hatten ein Problem  $L$  auf ein Problem  $L'$  reduziert, indem wir zeigten, dass mit einer Lösungsstrategie für  $L'$  auch  $L$  gelöst werden kann. War  $L$  ein bekanntmaßen unentscheidbares Problem, so folgte unmittelbar, dass auch  $L'$  unentscheidbar sein musste.

Auch im Bereich der Komplexitätstheorie lässt sich das Reduktionsprinzip gewinnbringend einsetzen. Hier wird es verwendet, um Komplexitätsaussagen einer Problemklasse an andere zu vererben. Den Schlüssel hierzu bildet der Begriff der *polynomiellen Reduzierbarkeit*, den wir an dieser Stelle formal einführen wollen:



#### Definition 7.15 (Polynomielle Reduzierbarkeit)

Mit  $L \subseteq \Sigma^*$  und  $L' \subseteq \Gamma^*$  seien zwei Sprachen gegeben.  $L$  ist genau dann auf  $L'$  polynomiell reduzierbar, geschrieben als  $L \leq_{poly} L'$ , falls eine totale Funktion  $f : \Sigma^* \rightarrow \Gamma^*$  mit den folgenden Eigenschaften existiert:

- $f$  ist in polynomieller Zeit berechenbar
- $\omega \in L \Leftrightarrow f(\omega) \in L'$

Wissen wir, dass eine Sprache  $L'$  in polynomieller Zeit entscheidbar ist, dann gilt diese Eigenschaft auch für jede Sprache  $L$  mit  $L \leq_{poly} L'$ . Wie in Abbildung 7.19 gezeigt, wird die Frage  $\omega \in L$  zunächst auf die äquivalente Frage  $\omega' \in L'$  abgebildet und erst dann entschieden. Beide Schritte weisen eine polynomielle Laufzeit von  $O(n^{k_1})$  bzw.  $O(n^{k_2})$  auf, so dass wir die ursprüngliche Frage  $\omega \in L$  mit der Komplexität

$$O(n^{k_1} + n^{k_2}) = O(n^{\max\{k_1, k_2\}}) \quad (7.21)$$

und damit ebenfalls in polynomieller Zeit beantworten können.

Im Folgenden werden wir nicht nur von polynomiell entscheidbaren Sprachen, sondern auch vermehrt von *polynomiell lösbar* Problemen reden. Die Redensart ist legitim, da wir bereits mehrfach festgestellt haben, dass zwischen der Entscheidbarkeit einer Sprache und der Lösung eines Ja-Nein-Problems kein prinzipieller Unterschied besteht.

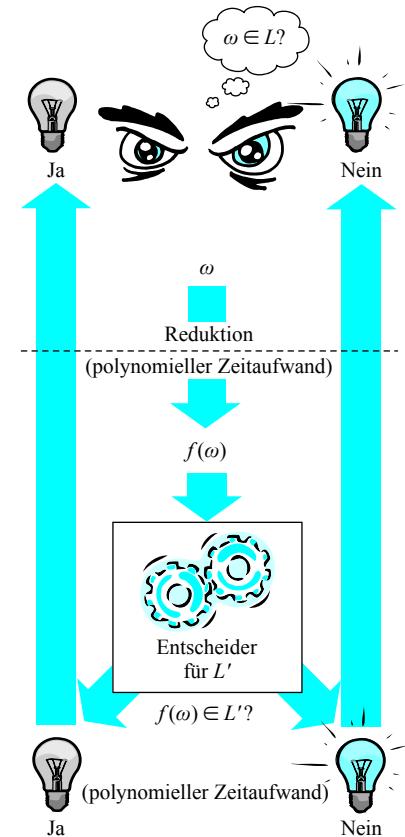
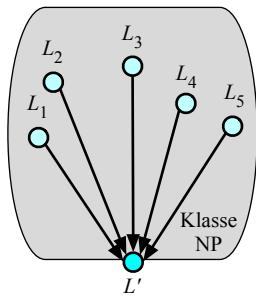
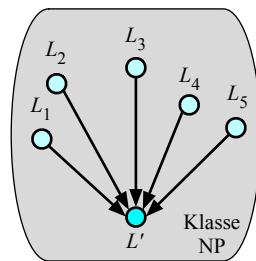


Abbildung 7.19: Prinzip der polynomiellen Reduzierbarkeit



Ein Problem  $L'$  ist *NP-hart*, wenn sich alle Probleme aus der Klasse NP darauf reduzieren lassen.  $L'$  kann selbst in NP liegen, muss es aber nicht.



Ein Problem  $L'$  ist *NP-vollständig*, wenn sich alle Probleme aus der Klasse NP darauf reduzieren lassen und  $L'$  selbst in NP liegt.

**Abbildung 7.20:** Zusammenhang zwischen NP-harten und NP-vollständigen Problemen

### 7.3.2 P-NP-Problem

Mit Hilfe der polynomiellen Reduzierbarkeit sind wir in der Lage, zwei prominente Problemklassen der Komplexitätstheorie zu definieren:



#### Definition 7.16 (NP-hart, NP-vollständig)

Eine Sprache  $L' \subseteq \Sigma^*$  heißt

- *NP-hart*, falls für alle  $L \in \text{NP}$  die Beziehung  $L \leq_{\text{poly}} L'$  gilt.
- *NP-vollständig*, falls  $L'$  NP-hart und ein Element von NP ist.

NPC bezeichnet die Klasse aller NP-vollständigen Probleme.

Wörtlich gesprochen ist ein Problem genau dann NP-hart, wenn sich alle nichtdeterministisch polynomiell lösbar Probleme darauf reduzieren lassen (vgl. Abbildung 7.20 oben). Ist es darüber hinaus selbst nichtdeterministisch polynomiell lösbar, so sprechen wir von einem NP-vollständigen Problem (vgl. Abbildung 7.20 unten). Abbildung 7.21 zeigt, wie sich die Komplexitätsklasse NPC in die bisher herausgearbeitete Klassenhierarchie einfügt.

Ein Beweis der NP-Vollständigkeit besteht immer aus zwei Teilen:

- Es ist zu zeigen, dass das untersuchte Problem in der Klasse NP liegt. Dies kann durch die Angabe eines nichtdeterministischen Algorithmus erfolgen, der zunächst eine Antwort rät und anschließend in polynomieller Zeit überprüft, ob wir eine Lösung vor uns haben.
- Es ist zu zeigen, dass sich alle Probleme aus der Klasse NP auf das untersuchte Problem reduzieren lassen (vgl. Abbildung 7.22). Dies kann durch die polynomielle Reduktion eines beliebigen anderen Problems aus der Klasse NPC geschehen.

NP-vollständige Probleme sind aus dem folgenden Grund von Interesse: Gelingt es uns, für ein einziges dieser Probleme zu zeigen, dass es *deterministisch* mit *polynomiell*em Aufwand gelöst werden kann, so wären auf einen Schlag alle anderen NP-vollständigen Probleme ebenfalls deterministisch polynomiell lösbar. Wir würden damit nichts weniger als die Beziehung  $P = NP$  beweisen und hätten das berühmte *P-NP-Problem* positiv beantwortet. Auf einen Schlag hätten wir einer Vielzahl von Problem ihren Schrecken genommen, die sich gegenwärtig einer effizienten Lösung entziehen.

Wenngleich das P-NP-Problem bis heute ungelöst ist, vermuten die meisten Experten, dass die Mengen P und NP verschieden sind. Ein Grund hierfür ist die große Anzahl an Problemen, die in der Vergangenheit als NP-vollständig identifiziert wurden. Wäre  $P = NP$ , so ließen sich all diese Probleme in polynomieller Zeit auf realen Computeranlagen lösen. So verlockend diese Möglichkeit auch klingt: Mit jedem neu entdeckten NP-vollständigen Problem scheint sie ein Stück weit unwahrscheinlicher zu werden. Trotzdem ist eine positive Lösung des P-NP-Problems keinesfalls ausgeschlossen und es wäre nicht das erste Mal, dass die mehrheitliche Expertenmeinung im Bereich der theoretischen Informatik widerlegt werden würde.

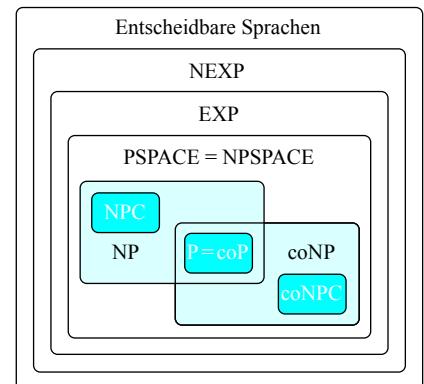


Abbildung 7.21: Inklusionsbeziehungen der eingeführten Komplexitätstypen

### 7.3.3 Satz von Cook

Dass überhaupt NP-harte oder NP-vollständige Probleme existieren, ist keinesfalls selbstverständlich. Halten wir uns an Definition 7.16, so können wir ein Problem  $L'$  als NP-hart identifizieren, indem wir ein anderes NP-hartes Problem darauf reduzieren. Damit wir die Reduktionstechnik anwenden können, muss also stets ein anderes Problem mit der gewünschten Eigenschaft existieren. Aus dieser Henne-Ei-Situation gibt es für uns nur einen Ausweg: Wir müssen die NP-Härte für irgend ein Problem direkt beweisen. Ist dieser Schritt gelungen, so lässt sich die Eigenschaft mit Hilfe der Reduktionstechnik auf weitere Probleme übertragen.

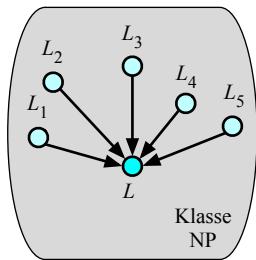
Im Jahre 1971 gelang es dem amerikanischen Computerwissenschaftler Stephen Cook, die NP-Vollständigkeit des SAT-Problems zu zeigen [24]. Weil sein Beweis auf die Reduktionstechnik verzichtet, kommt er ohne die Annahme aus, dass andere NP-vollständige Probleme existieren. Der Satz von Cook ist der Grundstein, auf dem alle anderen Vollständigkeitsbeweise aufbauen.



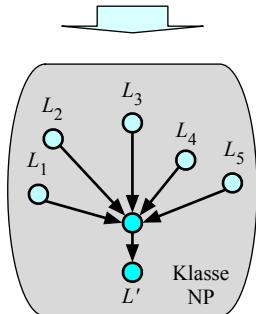
#### Satz 7.8 (Satz von Cook)

Das Erfüllbarkeitsproblem der Aussagenlogik (SAT) ist NP-vollständig.

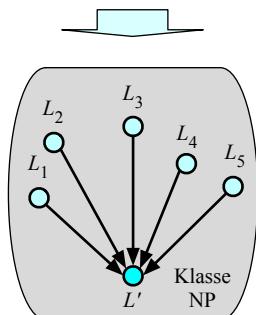
Der Vollständigkeitsbeweis besteht aus zwei Teilen. Zum einen müssen wir zeigen, dass SAT in NP liegt, und zum anderen, dass SAT ein NP-hartes Problem ist. Den ersten Teil haben wir in Abschnitt 7.2.1 erledigt. Dort haben wir herausgearbeitet, dass sich SAT nichtdeterministisch in linearer Zeit lösen lässt. Die eigentliche Schwierigkeit im Beweis des



Ist  $L$  NP-vollständig, so lassen sich alle Probleme aus NP auf  $L$  reduzieren.



Lässt sich  $L$  polynomiell auf  $L' \in$  NP reduzieren, so folgt aus der Transitivität, ...



... dass sich alle Probleme aus NP auch auf  $L'$  reduzieren lassen.  $L'$  ist damit ebenfalls NP-vollständig.

**Abbildung 7.22:** Die NP-Vollständigkeit eines Problems lässt sich durch die polynomielle Reduktion eines anderen NP-vollständigen Problems beweisen.

Satzes von Cook besteht im Nachweis der NP-Härte, schließlich müssen wir uns davon überzeugen, dass sich ausnahmslos alle Probleme der Klasse NP polynomiell auf SAT reduzieren lassen.

In den folgenden Betrachtungen bezeichnet  $L$  ein beliebiges Problem aus NP. Per Definition existiert eine nichtdeterministische Turing-Maschine  $T$ , die  $L$  in polynomieller Zeit entscheidet. Wir werden nun zeigen, dass wir für jedes Eingabewort  $\omega$  eine Formel  $F$  mit der nachstehenden Eigenschaft konstruieren können:

$$T(\omega) \text{ terminiert in einem Endzustand} \Leftrightarrow F(\omega) \text{ ist erfüllbar} \quad (7.22)$$

Gelingt es uns,  $F$  in polynomieller Zeit zu konstruieren, so sind wir am Ziel: Wir haben  $L$  polynomiell auf SAT reduziert.

Bevor wir die Struktur der Formel  $F$  im Detail diskutieren, führen wir zunächst die Variablen ein, die zu ihrer Konstruktion benötigt werden. Auf der obersten Ebene lassen sich diese in drei Kategorien einteilen:

- $B_{i,k,\sigma}$ : Variablen zur Codierung des Bandinhalts  
 $B_{i,k,\sigma} = 1 : \Leftrightarrow$  Nach  $i$  Schritten steht an Position  $k$  das Zeichen  $\sigma$
- $S_{i,s}$ : Variablen zur Codierung des aktuellen Zustands  
 $S_{i,s} = 1 : \Leftrightarrow T$  befindet sich nach  $i$  Schritten im Zustand  $s$
- $P_{i,k}$ : Variablen zur Codierung der aktuellen Kopfposition  
 $P_{i,k} = 1 : \Leftrightarrow T$  befindet sich nach  $i$  Schritten auf Bandposition  $k$

Beachten Sie, dass die Laufzeit der Turing-Maschine  $T$  polynomiell beschränkt ist. Ist  $n = |\omega|$  die Länge der Eingabe, so wird die Anzahl der Arbeitsschritte von  $T$  durch ein Polynom  $p(n)$  begrenzt. Auch wenn der exakte Wert von  $p(n)$  in unserer Betrachtung keine Rolle spielt, ist die Abschätzung wichtig. Sie besagt, dass die Indizes  $i, s$  im Intervall  $[0; p(n)]$  liegen müssen. Zudem kann sich der Schreib-Lese-Kopf maximal  $p(n)$  Positionen nach links bzw. rechts bewegen, d.h., wir müssen den Bandinhalt ausschließlich auf dem endlichen Teilstück  $-p(n), \dots, p(n)$  betrachten. Wie gewohnt gehen wir davon aus, dass der Schreib-Lese-Kopf initial über der Position 0 steht. Insgesamt zeigt die Betrachtung, dass  $F$  zwar eine große Menge an Variablen enthält, deren Anzahl aber nur polynomiell mit der Eingabelänge  $n$  wächst.

Um nicht im Nebel der Theorie zu versinken, wollen wir das Gesagte am Beispiel der Sprache

$$L := \{\#^n \mid n \in \mathbb{N}\} \quad (7.23)$$

genauer untersuchen. Die Sprache wurde bewusst ausgewählt, da sie durch eine bestechend einfache Turing-Maschine mit nur zwei Zuständen erkannt werden kann (vgl. Abbildung 7.23). Sie besteht aus dem Eingabealphabet  $\Sigma = \{\#\}$ , dem Bandalphabet  $\Pi = \{\#, \square\}$ , dem Startzustand  $s_0$  und dem (einzigsten) Endzustand  $s_1$ . Die Funktionsweise der Turing-Maschine ist äußerst simpel. Vom Startzustand geht sie direkt in den Endzustand über, falls das aktuelle Bandzeichen gleich  $\#$  ist; in diesem Fall gilt  $\omega \in L$ . Wird stattdessen das Blank-Symbol  $\square$  gelesen, terminiert die Maschine in  $s_0$ . Da die Berechnung immer nach einem Schritt beendet ist, ist die Laufzeit durch das Polynom  $p(n) = 1$  begrenzt. Wie die Auflistung in der unteren Hälfte von Abbildung 7.23 zeigt, werden trotzdem 22 Variablen benötigt, um die Turing-Maschine auf eine SAT-Instanz abzubilden.

Nachdem wir die verschiedenen Variablen zusammen mit ihrer Bedeutung eingeführt haben, können wir uns der eigentlichen Konstruktion von  $F$  zuwenden. Wie in Abbildung 7.24 im Detail dargestellt, gleicht die Formel auf der obersten Ebene einer viergliedrigen Konjunktion:

$$F = S \wedge R \wedge T \wedge A \quad (7.24)$$

Die Teilausdrücke besitzen die folgende Bedeutung:

#### ■ $S$ (Startbedingung)

Dieser Teilausdruck beschreibt die initiale Konfiguration der Turing-Maschine.  $T$  befindet sich im Startzustand  $s_0$ , alle Zellen des relevanten Bandabschnitts, die nicht mit Zeichen des Eingabeworts  $\omega$  belegt sind, enthalten ein Blank-Symbol und der Schreib-Lese-Kopf steht auf Position 0.

#### ■ $R$ (Randbedingungen)

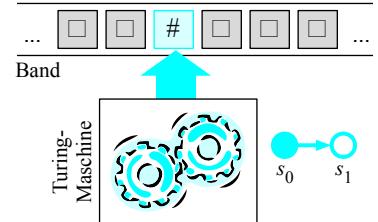
Dieser Teilausdruck beschreibt generelle Konsistenz-eigenschaften, die eine Turing-Maschine zu jedem Zeitpunkt erfüllen muss. Die Eigenschaften werden mit Hilfe dreier Teilausdrücke  $R_1, R_2, R_3$  formuliert, die im Einzelnen die folgende Bedeutung besitzen:

- $R_1$ : Eine Turing-Maschine befindet sich zu jedem Zeitpunkt in genau einem Zustand.
- $R_2$ : Zu jedem Zeitpunkt befindet sich der Schreib-Lese-Kopf an genau einer Position.
- $R_3$ : Zu jedem Zeitpunkt befindet sich genau ein Symbol an jeder Bandstelle.

Mehrere Formeln aus Abbildung 7.24 nutzen den Ausdruck

$$\text{Onehot}(A_1, A_2, \dots), \quad (7.25)$$

#### ■ Turing-Maschine



$$S = \{s_0, s_1\}$$

$$\Sigma = \{\#\}$$

$$\Pi = \{\#, \square\}$$

$$E = \{s_1\}$$

#### ■ Übergangstabelle

	#	$\square$
$s_0$	$(s_1, \#, \circlearrowleft)$	—
$s_1$	—	—

#### ■ Bandvariablen

$$\begin{array}{lll} B_{0,-1,\square} & B_{0,0,\square} & B_{0,1,\square} \\ B_{0,-1,\#} & B_{0,0,\#} & B_{0,1,\square} \\ B_{1,-1,\square} & B_{1,0,\square} & B_{1,1,\square} \\ B_{1,-1,\#} & B_{1,0,\#} & B_{1,1,\square} \end{array}$$

#### ■ Zustandsvariablen

$$\begin{array}{ll} S_{0,s_0} & S_{0,s_1} \\ S_{1,s_0} & S_{1,s_1} \end{array}$$

#### ■ Positionsvariablen

$$\begin{array}{lll} P_{0,-1} & P_{0,0} & P_{0,1} \\ P_{1,-1} & P_{1,0} & P_{1,1} \end{array}$$

**Abbildung 7.23:** Erster Schritt in der Konstruktion einer SAT-Instanz. Aus der Beschreibung der Turing-Maschine wird die Menge der Variablen ermittelt, die zur Codierung benötigt werden.

Der Begriff der NP-Vollständigkeit wurde im Jahre 1971 durch den Computerwissenschaftler Stephen Arthur Cook eingeführt. 1939 in Buffalo, New York, geboren, führte ihn seine akademische Laufbahn über Michigan, Harvard und Berkeley an die University of Toronto, wo er noch heute lehrt. In seiner berühmten Publikation „*The Complexity of Theorem Proving Procedures*“ zeigte er die NP-Vollständigkeit von SAT und der vereinfachten Variante 3SAT. 1982 wurde Cook für seine wegweisende Arbeit mit dem Turing-Award ausgezeichnet:

„For his advancement of our understanding of the complexity of computation in a significant and profound way. His seminal paper, *The Complexity of Theorem Proving Procedures*, presented at the 1971 ACM SIGACT Symposium on the Theory of Computing, laid the foundations for the theory of NP-Completeness. The ensuing exploration of the boundaries and nature of NP-complete class of problems has been one of the most active and important research activities in computer science for the last decade.“



Unabhängig von Cook entwickelte der im ukrainischen Dnipropetrowsk geborene und später in die USA emigrierte Mathematiker Leonid Levin einen zur NP-Vollständigkeit äquivalenten Begriff. In seiner 1973 publizierten Arbeit wies er die Eigenschaft für insgesamt 6 Probleme nach; darunter auch SAT [63]. Aus diesem Grund ist der Satz von Cook in der Literatur auch als Cook-Levin-Theorem bekannt.

um die geschilderten Eigenschaften zu beschreiben. Dieser steht stellvertretend für eine aussagenlogische Formel, die genau dann zu 1 auswertet, wenn eine und nur eine der Variablen  $A_1, A_2, \dots$  mit 1 belegt wird. In der Übungsaufgabe auf Seite 146 hatten Sie Gelegenheit herauszufinden, wie sich eine solche Funktion mit den Operatoren  $\wedge$ ,  $\vee$  und  $\neg$  konstruieren lässt.

#### ■ *T* (Transitionsbedingungen)

Die Teilformel *T* codiert die möglichen Konfigurationsübergänge und setzt sich wiederum aus der Konjunktion dreier Teilausdrücke  $T_1$ ,  $T_2$  und  $T_3$  zusammen. Die Bedeutung dieser Terme liest sich wie folgt:

- $T_1$ : Die Maschine geht in die Folgekonfiguration über.
- $T_2$ : Bereits terminierte Maschinen sind inaktiv.
- $T_3$ : Nur der Schreib-Lese-Kopf kann den Bandinhalt ändern.

#### ■ *A* (Akzeptanzbedingung)

Dieser Teilterm codiert die Bedingung, dass die Turing-Maschine das Eingabewort  $\omega$  genau dann akzeptiert, wenn sie in einem Endzustand anhält. Da die Laufzeit von *T* durch das Polynom  $p(n)$  beschränkt ist, muss der Endzustand in weniger als  $p(n)$  Berechnungsschritten erreicht werden. Da sich die Konfiguration einer terminierten Maschine nicht mehr ändert, erreicht *T* genau dann einen Endzustand, wenn sich die Maschine zum Zeitpunkt  $p(n)$  in einem solchen befindet.

Abbildung 7.25 demonstriert die Formelkonstruktion für die weiter oben eingeführte Beispiel-Turing-Maschine. Haben wir  $F_\omega$  nach dem dargelegten Schema für ein Eingabewort  $\omega$  aufgestellt, so lässt sich aus jeder Berechnungsfolge, die *T* unter Eingabe von  $\omega$  in einem Endzustand terminieren lässt, eine erfüllende Belegung für  $F_\omega$  ableiten. Umgekehrt gestattet die Konstruktion von  $F_\omega$ , dass wir aus jeder erfüllenden Belegung eine Berechnungsfolge ableiten können, die *T* in einen Endzustand führt. Kurzum: *T* akzeptiert das Eingabewort  $\omega$  genau dann, wenn für  $F_\omega$  eine erfüllende Belegung existiert.

Abbildung 7.27 zeigt den Zusammenhang zwischen der Akzeptanz eines Wortes  $\omega$  durch die Turing-Maschine *T* und der Erfüllbarkeit von  $F_\omega$  anhand zweier konkreter Berechnungssequenzen. Im linken Beispiel wird die Maschine mit dem Eingabewort  $\#$  gestartet. Die Maschine terminiert nach dem ersten Bearbeitungsschritt in einem Endzustand und die Formel  $F_\#$  wird durch die korrespondierende Variablenbelegung erfüllt. Im rechten Beispiel wird *T* auf das leere Wort angewendet. Hier

■ Finale SAT-Instanz

$$F = S \wedge R \wedge T \wedge A$$

■ Startbedingung

$$S = S_{0,s_0} \wedge P_{0,0} \bigwedge_{k=-p(n)}^{-1} B_{0,k,\square} \bigwedge_{k=0}^{n-1} B_{0,k,\omega_k} \bigwedge_{k=n}^{p(n)} B_{0,k,\square}$$

■ Randbedingungen:  $R = R_1 \wedge R_2 \wedge R_3$  mit

$$\begin{aligned} R_1 &= \bigwedge_{i=0}^{p(n)} \text{Onehot}(S_{i,s_0}, S_{i,s_1}, \dots) \\ R_2 &= \bigwedge_{i=0}^{p(n)} \text{Onehot}(P_{i,-p(n)}, \dots, P_{i,0}, \dots, P_{i,p(n)}) \\ R_3 &= \bigwedge_{i=0}^{p(n)} \bigwedge_{k=-p(n)}^{p(n)} \text{Onehot}(B_{i,k,\sigma_1}, B_{i,k,\sigma_2}, \dots) \end{aligned}$$

■ Transitionsbedingungen:  $T = T_1 \wedge T_2 \wedge T_3$  mit

$$\begin{aligned} T_1 &= \bigwedge_{\substack{i,k,s,\sigma \\ \delta(s,\sigma) \neq \emptyset}} (S_{i,s} \wedge P_{i,k} \wedge B_{i,k,\sigma}) \rightarrow \left[ \bigvee_{\substack{(s',\sigma',\leftarrow) \\ \in \delta(s,\sigma)}} (S_{i+1,s'} \wedge P_{i+1,k-1} \wedge B_{i+1,k,\sigma'}) \right. \\ &\quad \left. \bigvee_{\substack{(s',\sigma',\rightarrow) \\ \in \delta(s,\sigma)}} (S_{i+1,s'} \wedge P_{i+1,k+1} \wedge B_{i+1,k,\sigma'}) \bigvee_{\substack{(s',\sigma',\circlearrowleft) \\ \in \delta(s,\sigma)}} (S_{i+1,s'} \wedge P_{i+1,k} \wedge B_{i+1,k,\sigma'}) \right] \\ T_2 &= \bigwedge_{\substack{i,k,s,\sigma \\ \delta(s,\sigma) = \emptyset}} (S_{i,s} \wedge P_{i,k} \wedge B_{i,k,\sigma}) \rightarrow (S_{i+1,s} \wedge P_{i+1,k} \wedge B_{i+1,k,\sigma}) \\ T_3 &= \bigwedge_{i=0}^{p(n)} \bigwedge_{k=-p(n)}^{p(n)} \bigwedge_{\sigma \in \Pi} (\overline{P_{i,k}} \wedge B_{i,k,\sigma}) \rightarrow B_{i+1,k,\sigma} \end{aligned}$$

■ Akzeptanzbedingung

$$A = \bigvee_{z \in E} S_{p(n),z}$$

**Abbildung 7.24:** Codierung von Turing-Maschinen als SAT-Instanz

■ Finale SAT-Instanzen (für  $\omega = \#$  und  $\omega = \varepsilon$ )

$$F_{\#} = S_{\#} \wedge (R_1 \wedge R_2 \wedge R_3) \wedge (T_1 \wedge T_2 \wedge T_3) \wedge A$$

$$F_{\varepsilon} = S_{\varepsilon} \wedge (R_1 \wedge R_2 \wedge R_3) \wedge (T_1 \wedge T_2 \wedge T_3) \wedge A$$

■ Startbedingung

$$S_{\#} = S_{0,s_0} \wedge P_{0,0} \wedge B_{0,-1,\square} \wedge B_{0,0,\#} \wedge B_{0,1,\square}$$

$$S_{\varepsilon} = S_{0,s_0} \wedge P_{0,0} \wedge B_{0,-1,\square} \wedge B_{0,0,\square} \wedge B_{0,1,\square}$$

■ Randbedingungen

$$R_1 = (S_{0,s_0} \vee S_{0,s_1}) \wedge \overline{(S_{0,s_0} \wedge S_{0,s_1})} \wedge (S_{1,s_0} \vee S_{1,s_1}) \wedge \overline{(S_{1,s_0} \wedge S_{1,s_1})}$$

$$R_2 = (P_{0,-1} \vee P_{0,0} \vee P_{0,1}) \wedge \overline{(P_{0,-1} \wedge P_{0,0})} \wedge \overline{(P_{0,-1} \wedge P_{0,1})} \wedge \overline{(P_{0,0} \wedge P_{0,1})}$$

$$\wedge (P_{1,-1} \vee P_{1,0} \vee P_{1,1}) \wedge \overline{(P_{1,-1} \wedge P_{1,0})} \wedge \overline{(P_{1,-1} \wedge P_{1,1})} \wedge \overline{(P_{1,0} \wedge P_{1,1})}$$

$$R_3 = (B_{0,-1,\square} \vee B_{0,-1,\#}) \wedge \overline{(B_{0,-1,\square} \wedge B_{0,-1,\#})} \wedge (B_{0,0,\square} \vee B_{0,0,\#}) \wedge \overline{(B_{0,0,\square} \wedge B_{0,0,\#})} \wedge$$

$$(B_{0,1,\square} \vee B_{0,1,\#}) \wedge \overline{(B_{0,1,\square} \wedge B_{0,1,\#})} \wedge (B_{1,-1,\square} \vee B_{1,-1,\#}) \wedge \overline{(B_{1,-1,\square} \wedge B_{1,-1,\#})} \wedge$$

$$(B_{1,0,\square} \vee B_{1,0,\#}) \wedge \overline{(B_{1,0,\square} \wedge B_{1,0,\#})} \wedge (B_{1,1,\square} \vee B_{1,1,\#}) \wedge \overline{(B_{1,1,\square} \wedge B_{1,1,\#})}$$

■ Transitionsbedingungen

$$T_1 = ((S_{0,s_0} \wedge P_{0,-1} \wedge B_{0,-1,\#}) \rightarrow (S_{1,s_1} \wedge P_{1,-1} \wedge B_{1,-1,\#})) \wedge \\ ((S_{0,s_0} \wedge P_{0,0} \wedge B_{0,0,\#}) \rightarrow (S_{1,s_1} \wedge P_{1,0} \wedge B_{1,0,\#})) \wedge \\ ((S_{0,s_0} \wedge P_{0,1} \wedge B_{0,1,\#}) \rightarrow (S_{1,s_1} \wedge P_{1,1} \wedge B_{1,1,\#}))$$

$$T_2 = ((S_{0,s_0} \wedge P_{0,-1} \wedge B_{0,-1,\square}) \rightarrow (S_{1,s_0} \wedge P_{1,-1} \wedge B_{1,-1,\square})) \wedge$$

$$((S_{0,s_0} \wedge P_{0,0} \wedge B_{0,0,\square}) \rightarrow (S_{1,s_0} \wedge P_{1,0} \wedge B_{1,0,\square})) \wedge$$

$$((S_{0,s_0} \wedge P_{0,1} \wedge B_{0,1,\square}) \rightarrow (S_{1,s_0} \wedge P_{1,1} \wedge B_{1,1,\square})) \wedge$$

$$((S_{0,s_1} \wedge P_{0,-1} \wedge B_{0,-1,\#}) \rightarrow (S_{1,s_1} \wedge P_{1,-1} \wedge B_{1,-1,\#})) \wedge$$

$$((S_{0,s_1} \wedge P_{0,0} \wedge B_{0,0,\#}) \rightarrow (S_{1,s_1} \wedge P_{1,0} \wedge B_{1,0,\#})) \wedge$$

$$((S_{0,s_1} \wedge P_{0,1} \wedge B_{0,1,\#}) \rightarrow (S_{1,s_1} \wedge P_{1,1} \wedge B_{1,1,\#})) \wedge$$

$$((S_{0,s_1} \wedge P_{0,-1} \wedge B_{0,-1,\square}) \rightarrow (S_{1,s_1} \wedge P_{1,-1} \wedge B_{1,-1,\square})) \wedge$$

$$((S_{0,s_1} \wedge P_{0,0} \wedge B_{0,0,\square}) \rightarrow (S_{1,s_1} \wedge P_{1,0} \wedge B_{1,0,\square})) \wedge$$

$$((S_{0,s_1} \wedge P_{0,1} \wedge B_{0,1,\square}) \rightarrow (S_{1,s_1} \wedge P_{1,1} \wedge B_{1,1,\square})) \wedge$$

$$T_3 = ((\overline{P_{0,-1}} \wedge B_{0,-1,\square}) \rightarrow B_{1,-1,\square}) \wedge ((\overline{P_{0,-1}} \wedge B_{0,-1,\#}) \rightarrow B_{1,-1,\#}) \wedge$$

$$((\overline{P_{0,0}} \wedge B_{0,0,\square}) \rightarrow B_{1,0,\square}) \wedge ((\overline{P_{0,0}} \wedge B_{0,0,\#}) \rightarrow B_{1,0,\#}) \wedge$$

$$((\overline{P_{0,1}} \wedge B_{0,1,\square}) \rightarrow B_{1,1,\square}) \wedge ((\overline{P_{0,1}} \wedge B_{0,1,\#}) \rightarrow B_{1,1,\#})$$

■ Akzeptanzbedingung

$$A = S_{1,s_1}$$

**Abbildung 7.25:** Konstruktion zweier SAT-Instanzen  $F_{\omega}$  und  $F_{\varepsilon}$  für unsere Beispiel-Turing-Maschine

■ Finale SAT-Instanzen (für  $\omega = \#$  und  $\omega = \varepsilon$ )

$$F_{\#} = S_{\#} \wedge (R_1 \wedge R_2 \wedge R_3) \wedge (T_1 \wedge T_2 \wedge T_3) \wedge A$$

$$F_{\varepsilon} = S_{\varepsilon} \wedge (R_1 \wedge R_2 \wedge R_3) \wedge (T_1 \wedge T_2 \wedge T_3) \wedge A$$

■ Startbedingung

$$S_{\#} = S_{0,s_0} \wedge P_{0,0} \wedge B_{0,-1,\square} \wedge B_{0,0,\#} \wedge B_{0,1,\square}$$

$$S_{\varepsilon} = S_{0,s_0} \wedge P_{0,0} \wedge B_{0,-1,\square} \wedge B_{0,0,\square} \wedge B_{0,1,\square}$$

■ Randbedingungen

$$R_1 = (S_{0,s_0} \vee S_{0,s_1}) \wedge (\overline{S_{0,s_0}} \vee \overline{S_{0,s_1}}) \wedge (S_{1,s_0} \vee S_{1,s_1}) \wedge (\overline{S_{1,s_0}} \vee \overline{S_{1,s_1}})$$

$$R_2 = (P_{0,-1} \vee P_{0,0} \vee P_{0,1}) \wedge (\overline{P_{0,-1}} \vee \overline{P_{0,0}}) \wedge (\overline{P_{0,-1}} \vee \overline{P_{0,1}}) \wedge (\overline{P_{0,0}} \vee \overline{P_{0,1}}) \wedge$$

$$(P_{1,-1} \vee P_{1,0} \vee P_{1,1}) \wedge (\overline{P_{1,-1}} \vee \overline{P_{1,0}}) \wedge (\overline{P_{1,-1}} \vee \overline{P_{1,1}}) \wedge (\overline{P_{1,0}} \vee \overline{P_{1,1}})$$

$$R_3 = (B_{0,-1,\square} \vee B_{0,-1,\#}) \wedge (\overline{B_{0,-1,\square}} \vee \overline{B_{0,-1,\#}}) \wedge (B_{0,0,\square} \vee B_{0,0,\#}) \wedge (\overline{B_{0,0,\square}} \vee \overline{B_{0,0,\#}}) \wedge$$

$$(B_{0,1,\square} \vee B_{0,1,\#}) \wedge (\overline{B_{0,1,\square}} \vee \overline{B_{0,1,\#}}) \wedge (B_{1,-1,\square} \vee B_{1,-1,\#}) \wedge (\overline{B_{1,-1,\square}} \vee \overline{B_{1,-1,\#}}) \wedge$$

$$(B_{1,0,\square} \vee B_{1,0,\#}) \wedge (\overline{B_{1,0,\square}} \vee \overline{B_{1,0,\#}}) \wedge (B_{1,1,\square} \vee B_{1,1,\#}) \wedge (\overline{B_{1,1,\square}} \vee \overline{B_{1,1,\#}})$$

■ Transitionsbedingungen

$$T_1 = (\overline{S_{0,s_0}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\#}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\#}} \vee P_{1,-1}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\#}} \vee B_{1,-1,\#}) \wedge$$

$$(\overline{S_{0,s_0}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\#}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\#}} \vee P_{1,0}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\#}} \vee B_{1,0,\#}) \wedge$$

$$(\overline{S_{0,s_0}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\#}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\#}} \vee S_{1,s_1} \vee P_{1,1}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\#}} \vee S_{1,s_1} \vee B_{1,1,\#})$$

$$T_2 = (\overline{S_{0,s_0}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\square}} \vee S_{1,s_0}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\square}} \vee P_{1,-1}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\square}} \vee B_{1,-1,\square}) \wedge$$

$$(\overline{S_{0,s_0}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\square}} \vee S_{1,s_0}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\square}} \vee P_{1,0}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\square}} \vee B_{1,0,\square}) \wedge$$

$$(\overline{S_{0,s_0}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\square}} \vee S_{1,s_0}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\square}} \vee P_{1,1}) \wedge (\overline{S_{0,s_0}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\square}} \vee B_{1,1,\square}) \wedge$$

$$(\overline{S_{0,s_1}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\#}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\#}} \vee P_{1,-1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\#}} \vee B_{1,-1,\#}) \wedge$$

$$(\overline{S_{0,s_1}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\#}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\#}} \vee P_{1,0}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\#}} \vee B_{1,0,\#}) \wedge$$

$$(\overline{S_{0,s_1}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\#}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\#}} \vee P_{1,1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\#}} \vee B_{1,1,\#}) \wedge$$

$$(\overline{S_{0,s_1}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\square}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\square}} \vee P_{1,-1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,-1}} \vee \overline{B_{0,-1,\square}} \vee B_{1,-1,\square}) \wedge$$

$$(\overline{S_{0,s_1}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\square}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\square}} \vee P_{1,0}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,0}} \vee \overline{B_{0,0,\square}} \vee B_{1,0,\square}) \wedge$$

$$(\overline{S_{0,s_1}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\square}} \vee S_{1,s_1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\square}} \vee P_{1,1}) \wedge (\overline{S_{0,s_1}} \vee \overline{P_{0,1}} \vee \overline{B_{0,1,\square}} \vee B_{1,1,\square})$$

$$T_3 = (P_{0,-1} \vee \overline{B_{0,-1,\square}} \vee B_{1,-1,\square}) \wedge (P_{0,-1} \vee \overline{B_{0,-1,\#}} \vee B_{1,-1,\#}) \wedge$$

$$(P_{0,0} \vee \overline{B_{0,0,\square}} \vee B_{1,0,\square}) \wedge (P_{0,0} \vee \overline{B_{0,0,\#}} \vee B_{1,0,\#}) \wedge$$

$$(P_{0,1} \vee \overline{B_{0,1,\square}} \vee B_{1,1,\square}) \wedge (P_{0,1} \vee \overline{B_{0,1,\#}} \vee B_{1,1,\#})$$

■ Akzeptanzbedingung

$$A = S_{1,s_1}$$

**Abbildung 7.26:** Transformation der SAT-Instanzen  $F_{\omega}$  und  $F_{\varepsilon}$  in eine konjunktive Form

verhaart die Maschine im Startzustand  $s_0$  und  $F_e$  evaluiert mit der korrespondierenden Variablenbelegung zu 0.

Da uns das entwickelte Konstruktionsschema ermöglicht, jedes Problem der Klasse NP auf SAT zu reduzieren, sind wir einer fertigen Beweisskizze für den Satz von Cook bereits sehr nahe. Der fehlende Baustein ist der Nachweis, dass die Reduktion polynomiell erfolgt, d. h., dass die konstruierte Formel  $F$  nur polynomiell mit der Eingabelänge  $n$  wächst. Von dieser Eigenschaft können wir uns überzeugen, indem wir die Länge der vier Teilterme  $S$ ,  $R$ ,  $T$  und  $A$  genauer untersuchen. Es gelten die folgenden Beziehungen:

$$\begin{array}{ll} |S| = O(p(n)) & |R| = O(p(n)^3) \\ |T| = O(p(n)^2) & |A| = O(1) \end{array}$$

Die Gesamtformel  $F$  lässt sich mit dem Aufwand  $O(p(n)^3)$  konstruieren und wächst damit in der Tat nur polynomiell mit der Eingabelänge  $n$ . Damit sind wir am Ziel und haben SAT als NP-vollständiges Problem identifiziert, ohne auf die Reduktionstechnik zurückzugreifen.

### 7.3.4 Reduktionsbeweise

Die mühsame Arbeit des vorherigen Abschnitts war nicht umsonst, schließlich können wir unser erworbenes Wissen über SAT jetzt einsetzen, um weitere Probleme als NP-vollständig zu identifizieren. Hierzu werden wir auf die weiter oben skizzierte Reduktionstechnik zurückgreifen und zeigen, dass sich SAT in polynomieller Zeit auf die untersuchten Probleme reduzieren lässt.

Als erstes Beispiel betrachten wir mit 3SAT eine abgeschwächte Variante von SAT. Formal ist dieses Problem wie folgt definiert:

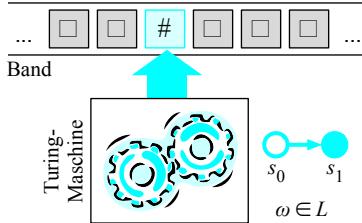


#### Definition 7.17 (3SAT)

Das Problem 3SAT lautet wie folgt:

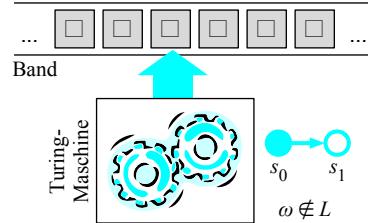
- Gegeben:  $n$  aussagenlogische Klauseln mit maximal 3 Literalen
- Gefragt: Gibt es eine erfüllende Belegung?

Genau wie SAT stellt 3SAT die Frage nach der Erfüllbarkeit einer aussagenlogischen Formel. Während SAT jedoch beliebige Eingaben zulässt,

■ Beispiel 1:  $\omega = \#$ 

Bandvariablen		
$B_{0,-1,\square} = 1$	$B_{0,0,\square} = 0$	$B_{0,1,\square} = 1$
$B_{0,-1,\#} = 0$	$B_{0,0,\#} = 1$	$B_{0,1,\#} = 0$
$B_{1,-1,\square} = 1$	$B_{1,0,\square} = 0$	$B_{1,1,\square} = 1$
$B_{1,-1,\#} = 0$	$B_{1,0,\#} = 1$	$B_{1,1,\#} = 0$
Zustandsvariablen		
$S_{0,s_0} = 1$	$S_{0,s_1} = 0$	
$S_{1,s_0} = 0$	$S_{1,s_1} = 1$	
Positionsvariablen		
$P_{0,-1} = 0$	$P_{0,0} = 1$	$P_{0,1} = 0$
$P_{1,-1} = 0$	$P_{1,0} = 1$	$P_{1,1} = 0$

# ∈ L,  $F_\#$  evaluiert zu 1

■ Beispiel 2:  $\omega = \epsilon$ 

Bandvariablen		
$B_{0,-1,\square} = 1$	$B_{0,0,\square} = 1$	$B_{0,1,\square} = 1$
$B_{0,-1,\#} = 0$	$B_{0,0,\#} = 0$	$B_{0,1,\#} = 0$
$B_{1,-1,\square} = 1$	$B_{1,0,\square} = 1$	$B_{1,1,\square} = 1$
$B_{1,-1,\#} = 0$	$B_{1,0,\#} = 0$	$B_{1,1,\#} = 0$
Zustandsvariablen		
$S_{0,s_0} = 1$	$S_{0,s_1} = 0$	
$S_{1,s_0} = 1$	$S_{1,s_1} = 0$	
Positionsvariablen		
$P_{0,-1} = 0$	$P_{0,0} = 1$	$P_{0,1} = 0$
$P_{1,-1} = 0$	$P_{1,0} = 1$	$P_{1,1} = 0$

$\epsilon \notin L$ ,  $F_\epsilon$  evaluiert zu 0

**Abbildung 7.27:** Zwei konkrete Beispiele, die den Zusammenhang zwischen T und  $F_\omega$  demonstrieren. Die Turing-Maschine T akzeptiert das Eingabewort  $\omega$  genau dann, wenn die Formel  $F_\omega$  erfüllbar ist.

muss die Formel für 3SAT in der speziellen konjunktiven Form

$$\{L_{11}, L_{12}, L_{13}\} \wedge \{L_{21}, L_{22}, L_{23}\} \wedge \dots \wedge \{L_{n1}, L_{n2}, L_{n3}\} \quad (7.26)$$

vorliegen. Beachten Sie, dass wir in Definition 7.17 nicht gefordert haben, dass eine Klausel genau 3 Literale besitzen muss. Hierdurch ist z. B. auch die Formel

$$\{A, \neg B\} \wedge \{\neg A\} \quad (7.27)$$

eine 3SAT-Instanz.

Bevor wir die Reduktion von SAT auf 3SAT vollziehen, wollen wir einen erneuten Blick auf den im vorherigen Abschnitt durchgeführten Beweis werfen. Wir haben gezeigt, wie sich eine nichtdeterministische

Der amerikanische Computerwissenschaftler Richard Manning Karp erkannte als einer der Ersten, wie bedeutend Cooks Entdeckung über die NP-Vollständigkeit von SAT wirklich war. In seiner 1972 publizierten Arbeit stellte er 20 weitere Probleme vor, die er mit Hilfe der Reduktionstechnik als NP-vollständig identifizierte. Zu diesen gehörte unter anderem auch das CLIQUE-Problem, das uns in diesem Abschnitt zur Demonstration der Reduktionstechnik dient. Für seine bedeutenden Arbeiten wurde Karp im Jahre 1985 mit dem Turing-Award ausgezeichnet:

*„For his continuing contributions to the theory of algorithms including the development of efficient algorithms for network flow and other combinatorial optimization problems, the identification of polynomial-time computability with the intuitive notion of algorithmic efficiency, and, most notably, contributions to the theory of NP-completeness. Karp introduced the now standard methodology for proving problems to be NP-complete which has led to the identification of many theoretical and practical problems as being computationally difficult.“*



Neben seinen Errungenschaften im Gebiet der theoretischen Informatik leistete Karp wichtige Beiträge im Gebiet der Algorithmentechnik. Zu den wichtigsten Arbeiten gehören der Edmonds-Karp-Algorithmus zur Berechnung des maximalen Flusses in Netzwerken und der Rabin-Karp-Algorithmus für die Hash-basierte Textsuche.

Turing-Maschine  $T$  polynomiell auf eine aussagenlogische Formel  $F$  reduzieren lässt, die genau dann erfüllbar ist, wenn  $T$  in einem Endzustand terminiert. Betrachten wir die Struktur der konstruierten Formel  $F$  genauer, so wird klar, dass wir in Wirklichkeit ein stärkeres Ergebnis bewiesen haben. Auf der obersten Ebene besitzt  $F$  eine konjunktive Struktur und auch die Teilterme sind diesbezüglich weitgehend regulär aufgebaut.

Ersetzen wir den Implikationsoperator  $A \rightarrow B$  durch den äquivalenten Ausdruck  $\overline{A} \vee B$ , schieben die Negationen mit Hilfe der De Morgan'schen Regeln in die Teilterme und wenden auf die verbleibenden Ausdrücke das Distributivgesetz an, so lässt sich  $F$  in eine Klausel-form überführen, die nur polynomiell länger wird als die ursprüngliche Formel  $F$ . Abbildung 7.26 zeigt die entstehende Klauselmenge für unsere weiter oben diskutierte Beispielmaschine. Damit ist die NP-Vollständigkeit von 3SAT bereits dann bewiesen, wenn wir es schaffen, eine Klauselmenge der Form

$$\{L_{11}, \dots, L_{1i_1}\}, \dots, \{L_{21}, \dots, L_{2i_2}\}, \dots, \{L_{n1}, \dots, L_{ni_n}\} \quad (7.28)$$

so auf eine äquivalente 3SAT-Instanz abzubilden, dass die Länge nur polynomiell zunimmt.

Um dies zu erreichen, bedienen wir uns eines Ergebnisses, das Sie im Übungsteil auf Seite 146 herausarbeiten durften. Dort sollten Sie zeigen, dass die Formel

$$(L_1 \vee L_2 \vee L_3 \vee L_4) \quad (7.29)$$

genau dann erfüllbar ist, wenn die Formel

$$(L_1 \vee L_2 \vee L') \wedge (\neg L' \vee L_3 \vee L_4) \quad (7.30)$$

erfüllbar ist. Wenden wir dieses Schema rekursiv an, so können wir die Menge (7.28) wie folgt in eine erfüllbarkeitsäquivalente Klauselmenge übertragen:

$$\{L_{11}, L_{12}, L'\}, \{\neg L', L_{13}, L''\}, \{\neg L'', L_{14}, L'''\}, \dots \quad (7.31)$$

Die erzeugte Menge ist eine Instanz von 3SAT, in der sich die Gesamtzahl der Literale nur linear erhöht hat. Mit der vorgenommenen Transformation ist es uns gelungen, die ursprüngliche Klauselmenge polynomiell auf eine Instanz von 3SAT zu reduzieren und hierdurch die Beziehung  $SAT \leq_{poly} 3SAT$  zu zeigen. Damit sind wir am Ziel und haben den folgenden Satz bewiesen:



### Satz 7.9 (Satz von Cook)

Das Problem 3SAT ist NP-vollständig.

Auch wenn 3SAT in der praktischen Informatik kaum eine Rolle spielt, ist seine Bedeutung für die theoretische Informatik umso größer. Genau wie SAT können wir 3SAT dazu verwenden, um andere Probleme als NP-vollständig zu identifizieren; aufgrund der einfachen Klauselstruktur lässt sich die Reduktion aber meist einfacher durchführen als im Falle von SAT. Am Beispiel des CLIQUE-Problems wollen wir eine entsprechende Reduktion demonstrieren.



### Definition 7.18 (CLIQUE)

Das Problem CLIQUE lautet wie folgt:

- Gegeben: Graph  $G$  mit Knotenmenge  $V$  und Kantenmenge  $E$ .
- Gefragt: Existieren  $n$  Knoten  $v_1, \dots, v_n$ , die paarweise durch eine Kante aus  $E$  verbunden sind?

Eine Menge  $C = \{v_1, \dots, v_n\}$  mit dieser Eigenschaft heißt Clique der Größe  $n$ .

Interpretieren wir die Knoten eines Graphen als Menschen und die Kanten als Verwandtschaftsbeziehungen, so entspricht eine Clique der Größe  $m$  einer Gruppe von  $m$  Menschen, in der jeder jeden kennt.

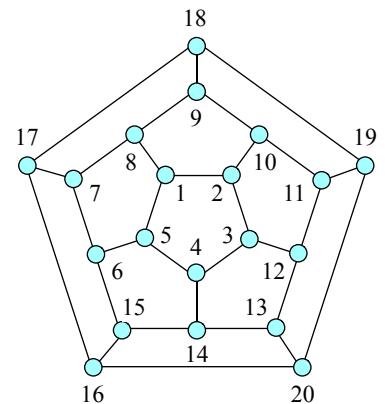
Abbildung 7.28 demonstriert die Beziehung anhand zweier Beispielgraphen. Während der erste Graph ausschließlich Cliques der Größe 2 enthält, sind im zweiten Graphen mit  $\{2,3,5\}$ ,  $\{3,4,6\}$ ,  $\{3,4,6\}$  und  $\{5,6,8\}$  vier verschiedene 3er-Cliques vorhanden.

Wir werden nun zeigen, dass wir mit CLIQUE ein weiteres NP-vollständiges Problem vor uns haben. Dass es in der Komplexitätsklasse NP liegt, ist offensichtlich: Um festzustellen, ob eine Clique der Größe  $n$  existiert, müssen wir lediglich eine geeignete Knotenmenge  $v_1, \dots, v_n$  raten und anschließend überprüfen, ob alle Knoten paarweise durch eine Kante verbunden sind. Die Überprüfung ist in polynomieller Zeit durchführbar, da der Aufwand lediglich quadratisch mit  $n$  zunimmt.

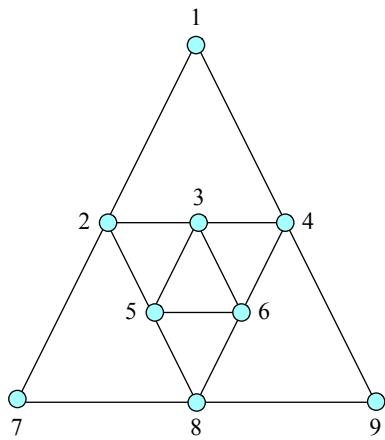
Den Rest des Beweises erledigen wir durch die Reduktion von 3SAT auf CLIQUE. Hierzu müssen wir eine  $n$ -elementige Klauselmenge

$$M := \{L_{11}, L_{12}, L_{13}\} \wedge \{L_{21}, L_{22}, L_{23}\} \wedge \dots \wedge \{L_{n1}, L_{n2}, L_{n3}\} \quad (7.32)$$

#### Beispiel 1



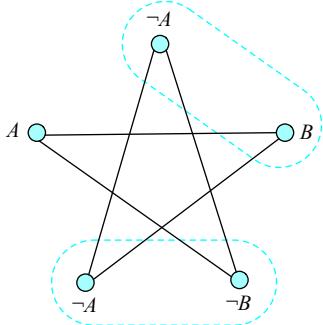
#### Beispiel 2



**Abbildung 7.28:** Eine Clique der Größe  $k$  ist eine Menge von  $k$  paarweise verbundenen Knoten. Während der obere Graph ausschließlich Cliques der Größe 2 enthält, besitzt der untere Graph 4 Cliques der Größe 3.

■ Beispiel 1

$$M := \{A\} \wedge \{\neg A, B\} \wedge \{\neg A, \neg B\}$$



Der Graph enthält keine Clique der Größe 3  $\Rightarrow M$  ist unerfüllbar

polynomiell auf einen Graphen  $G = (V, E)$  mit der folgenden Eigenschaft abbilden:

$$M \text{ ist erfüllbar} \Leftrightarrow G \text{ enthält eine Clique der Größe } n$$

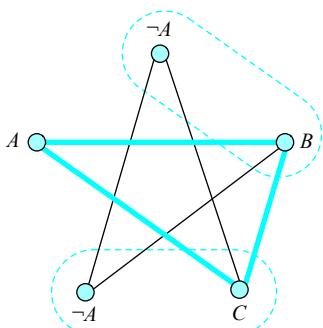
Abbildung 7.29 demonstriert anhand zweier Beispiele, wie wir einen Graphen mit dieser Eigenschaft erhalten können. Zunächst generieren wir für jedes Literal einen Knoten  $v$ . Anschließend verbinden wir zwei Knoten  $v_1$  und  $v_2$  genau dann mit einer Kante, falls

- $L_1$  und  $L_2$  nicht derselben Klausel angehören und
- $L_1$  und  $L_2$  gleichzeitig erfüllbar sind.

Zwei Literale  $L_1$  und  $L_2$  sind genau dann gleichzeitig erfüllbar, wenn sie nicht komplementär zueinander sind. Die zweite Bedingung ist damit äquivalent zu der Aussage  $L_1 \neq \neg L_2$ .

■ Beispiel 2

$$M := \{A\} \wedge \{\neg A, B\} \wedge \{\neg A, C\}$$



Der Graph enthält eine Clique der Größe 3  $\Rightarrow M$  ist erfüllbar

Erfüllende Belegung:  $A = B = C = 1$

**Abbildung 7.29:** Transformation einer  $n$ -elementigen Klauselmenge  $M$  in einen Graphen  $G$ .  $M$  ist genau dann erfüllbar, wenn  $G$  eine Clique der Größe  $n$  enthält.



**Satz 7.10**

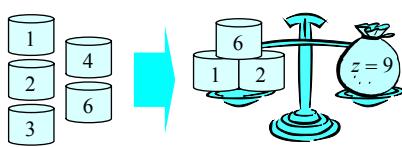


Das Problem CLIQUE ist NP-vollständig.

Abbildung 7.30 enthält eine Auswahl weitere Probleme, die sich mit Hilfe der Reduktionstechnik als NP-vollständig entlarven lassen. Eine ausführliche Darstellung, wie die Reduktionen im Einzelnen durchgeführt werden können, findet sich in [82].

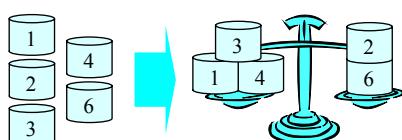
### ■ SELECT

Gegeben seien eine Folge natürlicher Zahlen  $x_1, \dots, x_n \in \mathbb{N}$  und eine weitere natürliche Zahl  $z \in \mathbb{N}$ . Existiert eine Auswahl von Elementen  $x_{i_1}, \dots, x_{i_k}$ , deren Summe  $z$  ergibt? Mit anderen Worten: Existiert eine Teilmenge  $S \subseteq \{1, \dots, n\}$  mit  $\sum_{i \in S} x_i = z$ ?



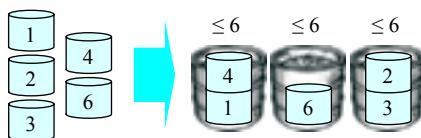
### ■ PARTITION

Gegeben sei eine Folge natürlicher Zahlen  $x_1, \dots, x_n$ . Lassen sich die Zahlen so aufteilen, dass die Summe beider Partitionen gleich ist? Mit anderen Worten: Existiert eine Teilmenge  $S \subseteq \{1, \dots, n\}$  mit  $\sum_{i \in S} x_i = \sum_{i \notin S} x_i$ ?



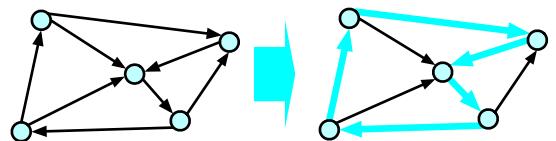
### ■ BIN PACKING

Gegeben seien  $k$  Container mit dem gleichen Fassungsvermögen  $V$ . Für  $n$  Zahlen  $x_1, \dots, x_n$  ist zu entscheiden, ob sich diese auf die Container verteilen lassen, ohne das Fassungsvermögen zu überschreiten. Mit anderen Worten: Existiert eine Zuordnung  $f : \{1, \dots, n\} \rightarrow \{1, \dots, k\}$  mit  $\sum_{f(i)=j} x_i < V$ ?



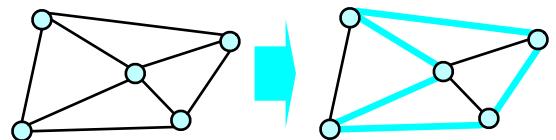
### ■ HAMILTON (gerichtet)

Gegeben sei ein *gerichteter* Graph  $G = (V, E)$ . Lassen sich die Knoten derart umsortieren, dass die neu geordnete Menge  $V' = (v_1, \dots, v_n)$  für  $1 \leq i < n$  die Beziehung  $(v_i, v_{i+1}) \in E$  und für  $i = n$  die Beziehung  $(v_i, v_1) \in E$  erfüllt?



### ■ HAMILTON (ungerichtet)

Gegeben sei ein *ungerichteter* Graph  $G = (V, E)$ . Lassen sich die Knoten derart umsortieren, dass die neu geordnete Menge  $V' = (v_1, \dots, v_n)$  für  $1 \leq i < n$  die Beziehung  $(v_i, v_{i+1}) \in E$  und für  $i = n$  die Beziehung  $(v_i, v_1) \in E$  erfüllt?



### ■ TRAVELING SALESMAN

Gegeben sei eine Menge von Städten  $\{S_1, \dots, S_n\}$  sowie eine Straßenkarte, auf der die Entfernungen zwischen  $S_i$  und  $S_j$  verzeichnet sind. Für eine gegebene Konstante  $k$  gilt es zu entscheiden, ob alle Städte auf einem Rundweg besucht werden können, der die Gesamtstrecke  $k$  nicht überschreitet.

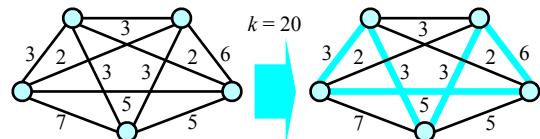


Abbildung 7.30: Auswahl weiterer NP-vollständiger Probleme

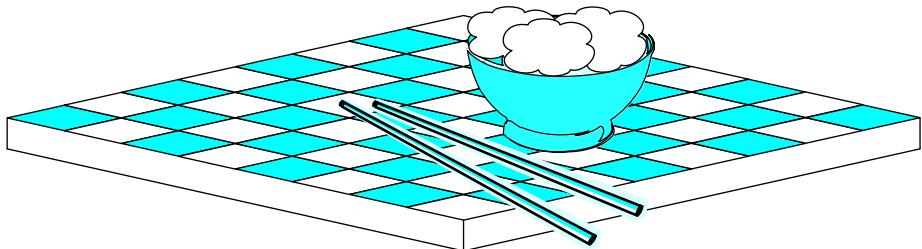
## 7.4 Übungsaufgaben

### Aufgabe 7.1



**Webcode  
7890**

großen Dienst erwies? Der Bauer nahm ein Schachbrett zur Hand und bat den Kaiser darum, auf das erste Feld ein Reiskorn zu legen und die Zahl der Reiskörner mit jedem Feld zu verdoppeln. Der Kaiser wollte ihm jeden Wunsch gewähren und willigte ein.



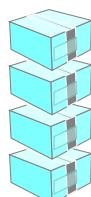
- Erklären Sie, warum der königliche Mathematiker das Bewusstsein verlor.
- Hätte der Kaiser einwilligen sollen, wenn sich der Bauer für eine polynomiale Zunahme der Reiskörner entschieden hätte?

### Aufgabe 7.2

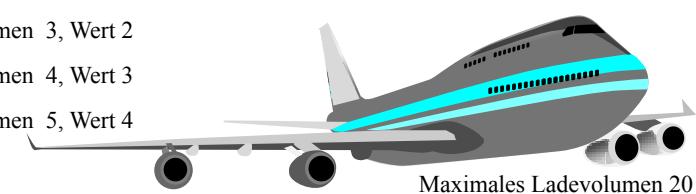


**Webcode  
7587**

Ihre Aufgabe ist es, die Beladung des abgebildeten Transportflugzeugs zu organisieren. Als Fracht stehen Ihnen vier verschiedene Containertypen zur Verfügung, die sich in Volumen und Wert voneinander unterscheiden.



- Volumen 3, Wert 2
- Volumen 4, Wert 3
- Volumen 5, Wert 4



Die abgebildeten Java-Funktionen durchsuchen ein absteigend sortiertes Integer-Array `a` nach dem Element `key`. Ist die Suche erfolgreich, so liefert die Funktion die Listenposition von `key` zurück. Ist `key` nicht in der Liste enthalten, so ist der Funktionswert gleich `-1`.

**Aufgabe 7.3****Webcode****7375****linSearch.java**

```
public static int
linSearch(int[] a, int key)
{
    int lo = 0;
    int hi = a.length;

    for (lo = 0; lo < hi; lo++) {
        int val = a[lo];

        if (val == key)
            return lo;
    }
    return -1;
}
```

**binSearch.java**

```
1  public static int
2  binSearch(int[] a, int key)
3  {
4      int lo = 0;
5      int hi = a.length;
6
7      while (lo < hi) {
8          int mid = (lo + hi) >> 1;
9          int val = a[mid];
10
11         if (val < key)
12             lo = mid + 1;
13         else if (val > key)
14             hi = mid;
15         else
16             return mid;
17     }
18     return -1;
19 }
```

Die linke Implementierung verwendet eine *lineare Suche* und vergleicht alle Array-Elemente von `a` nacheinander mit dem Element `key`. Sobald das Element gefunden wurde, terminiert der Algorithmus vorzeitig und liefert den aktuellen Stand der Schleifenvariablen `lo` zurück.

Die zweite Implementierung verwendet das Prinzip der *binären Suche*. Über die Variablen `lo` und `hi` wird ein Suchintervall definiert, in dem sich das Element `key` befinden muss. Zu Beginn erstreckt sich das Intervall über sämtliche Array-Elemente und wird anschließend iterativ verkleinert. Hierzu wird das Element in der Intervallmitte bestimmt (Position `mid`) und mit der Variablen `key` verglichen. Ist das Element kleiner als `key`, so muss sich das gesuchte Element in der rechten Hälfte befinden. Ist es dagegen größer, so kann es ausschließlich in der linken Hälfte liegen. Auf diese Weise wird das Suchintervall kontinuierlich halbiert, bis das Element `key` gefunden wird oder das Suchintervall zur leeren Menge degradiert.

- Welche Laufzeitkomplexitäten besitzt die lineare Suche?
- Welche Laufzeitkomplexitäten besitzt die binäre Suche?
- Ist die binäre Suche der linearen Suche in allen Fällen überlegen?

**Aufgabe 7.4****Webcode  
7761**

Auf Seite 112 ist das Strukturbild eines vollständig aufgebauten 4-Bit-Carry-look-ahead-Addierers dargestellt. Ihre Aufgabe ist es, die asymptotische Wachstumsrate des Flächenbedarfs eines  $n$ -Carry-look-ahead-Addierers zu bestimmen.

- Welche Flächenkomplexität besitzt der Addierer unter der Annahme, dass alle Logikgatter die gleiche Größe haben und der Flächenbedarf der Signalleitungen vernachlässigbar ist?
- Welche Flächenkomplexität besitzt der Addierer unter der Annahme, dass der Flächenbedarf eines Logikgatters proportional mit der Anzahl seiner Eingänge wächst?

Geben Sie Ihre Antworten in der Notation des O-Kalküls an.

**Aufgabe 7.5****Webcode  
7469**

Exponentielle Wachstumsraten sind der Feind eines jeden Programmierers und nur wenige Menschen sind in der Lage, sie präzise abzuschätzen. Wie schwer uns der Umgang mit dem Exponentiellen wirklich fällt, demonstriert das folgende, aus der Volkswirtschaftslehre entliehene Beispiel. Dargestellt ist eine vergleichende Hochrechnung des Wirtschaftswachstums der drei Länder Indien, Indonesien und Japan für die Jahre 1890 bis 1990:



In Indien wuchs das Bruttoinlandsprodukt (BIP) in diesem Zeitraum durchschnittlich ca. 0,65 % pro Jahr. In Indonesien betrug das Wachstum zur gleichen Zeit durchschnittlich ca. 1 % und in Japan ca. 3 % pro Jahr.

- Schätzen Sie ohne Rechnung, um welchen Faktor sich das Bruttoinlandsprodukt in den angesprochenen 100 Jahren in jedem Land verändert hat.
- Rechnen Sie die kumulierte Wachstumsrate exakt aus und vergleichen Sie das Ergebnis mit Ihrer Schätzung.

Mit der o-Notation haben Sie eine Möglichkeit kennen gelernt, starke obere asymptotische Schranken anzugeben. So drückt die Schreibweise  $f(n) = o(g(n))$  aus, dass  $f$  asymptotisch langsamer wächst als  $g$ . Formal haben wir die o-Notation wie folgt definiert:

$$\forall c \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 : c \cdot f(n) \leq g(n) \quad (7.33)$$

Können wir diese Definition durch die folgende Alternative ersetzen, ohne die definierten Komplexitätsklassen zu verändern?

a)  $\exists n_0 \in \mathbb{N} \forall c \in \mathbb{R}^+ \forall n \geq n_0 : c \cdot f(n) \leq g(n)$

Wie wirken sich die nachstehenden Veränderungen aus?

b)  $\forall c \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n > n_0 : c \cdot f(n) \leq g(n)$

c)  $\forall c \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n \geq n_0 : c \cdot f(n) < g(n)$

d)  $\forall c \in \mathbb{R}^+ \exists n_0 \in \mathbb{N} \forall n > n_0 : c \cdot f(n) < g(n)$

**Aufgabe 7.6**

**Webcode  
7049**

In Kapitel 3 haben Sie mit dem Tableaukalkül ein Semi-Entscheidungsverfahren für die Prädikatenlogik erster Stufe kennen gelernt. Wir sind in dieser Aufgabe an der Laufzeit des Tableau-Verfahrens interessiert. Um diese abschätzen zu können, definieren wir zunächst die Funktion  $t(F)$ :

$$t(F) = \begin{cases} n & : \text{Unter Eingabe von } F \text{ terminiert das Verfahren nach } n \text{ Schritten} \\ 0 & : \text{Unter Eingabe von } F \text{ terminiert das Verfahren nicht} \end{cases} \quad (7.34)$$

Um die Laufzeit in Relation zur Eingabelänge zu setzen, definieren wir die Wachstumsfunktion  $f(n)$  wie folgt:

$$f(n) = \max \{t(F) \mid |F| = n\} \quad (7.35)$$

$|F|$  bezeichnet die Länge der prädikatenlogischen Formel  $F$ . Damit entspricht der Funktionswert  $f(n)$  der maximalen Anzahl an Berechnungsschritten, die das Tableaux-Verfahren im Terminierungsfall für Eingaben der Länge  $n$  benötigt. Wir wollen die Frage klären, welcher Komplexitätsklasse wir  $f(n)$  zuordnen können.

- a) Versuchen Sie, das asymptotische Wachstum von  $f(n)$  nach oben abzuschätzen, indem Sie eine Funktion  $g(n)$  mit  $f(n) = O(g(n))$  angeben.
- b) Obwohl die gesuchte Funktion  $g(n)$  existieren muss, war Ihre Suche mit Sicherheit nicht erfolgreich. Erklären Sie, warum Sie keine Chance hatten, die Funktion  $g(n)$  zu finden.

**Aufgabe 7.7**

**Webcode  
7199**

**Aufgabe 7.8**

Vielleicht erinnern Sie sich an das Anagramm

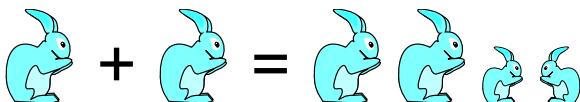


**Webcode**

7490

1 1 2 3 5 8 13 21 LEONARDO DA VINCI! THE MONA LISA!

aus dem packenden Thriller *Sakrileg*. Die Zahlen sind Teil der *Fibonacci-Folge*, die der italienische Mathematiker Leonardo da Pisa, gennant Fibonacci, in der ersten Hälfte des dreizehnten Jahrhunders aufstellte. Was die meisten Leser von Dan Brown's Roman nicht wissen: Die Folge ist das Ergebnis von Fibonaccis Untersuchungen über das Wachstum von Kaninchenpopulationn. Er ging dabei von folgenden Annahmen aus: Zu Beginn existiert ein einziges Paar geschlechtsreifer Kaninchen. Jedes neugeborene Paar wird im zweiten Monat geschlechtsreif und jedes geschlechtsreife Paar gebärt pro Monat ein weiteres Paar.



Offensichtlich lässt sich die Folge mit der nachstehenden Funktion berechnen:

fibonacci.c

```
int fibonacci(int n)
{
    if (n == 1 || n == 2) return 1;
    else return fibonacci(n-1) + fibonacci(n-2);
}
```

1  
2  
3  
4  
5

Die Laufzeit, die der Funktionsaufruf  $\text{fibonacci}(n)$  konsumiert, bezeichnen wir mit  $T(n)$ . Die rekursive Struktur erlaubt es uns, das asymptotische Wachstum von  $T(n)$  in Form einer *Rekurrenzgleichung* anzugeben:

$$T(1) = 1, \quad T(2) = 1, \quad T(n) = T(n-1) + T(n-2) \quad (7.36)$$

- a) Welcher Zusammenhang besteht zwischen  $T(n)$  und  $\text{fibonacci}(n)$ ?
- b) Versuchen Sie,  $T(n)$  mit einer geschlossenen Formel zu berechnen.
- c) Bestimmen Sie mit der ermittelten Formel die Laufzeitkomplexität des Algorithmus.
- d) Kann die dynamische Programmierung helfen, die Laufzeit zu verbessern?

In dieser Aufgabe geht es um die Berechnung des Produkts zweier quadratischer Matrizen  $X, Y \in \mathbb{R}^{n \times n}$ . Um die Betrachtungen nicht komplizierter als nötig zu gestalten, sei  $n$  eine Zweierpotenz. In diesem Fall lassen sich  $X$  und  $Y$  und die Produktmatrix  $Z$  in vier gleich große Fragmente zerlegen:

$$X := \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}, \quad Y := \begin{pmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{pmatrix}, \quad Z := \begin{pmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{pmatrix} \quad (7.37)$$

Basierend auf dieser Zerlegung können wir  $Z$  wie folgt ausrechnen:

$$Z_{11} := X_{11} \cdot Y_{11} + X_{12} \cdot Y_{21} \quad (7.38)$$

$$Z_{12} := X_{11} \cdot Y_{12} + X_{12} \cdot Y_{22} \quad (7.39)$$

$$Z_{21} := X_{21} \cdot Y_{11} + X_{22} \cdot Y_{21} \quad (7.40)$$

$$Z_{22} := X_{21} \cdot Y_{12} + X_{22} \cdot Y_{22} \quad (7.41)$$

Im Jahre 1969 konnte der deutsche Mathematiker Volker Strassen zeigen, dass sich die Berechnung optimieren lässt [87]. Der *Strassen-Algorithmus* beginnt mit der Vorberechnung mehrerer Hilfsmatrizen:

$$H_1 := (X_{11} + X_{22}) \cdot (Y_{11} + Y_{22}) \quad (7.42)$$

$$H_2 := (X_{21} + X_{22}) \cdot Y_{11} \quad (7.43)$$

$$H_3 := X_{11} \cdot (Y_{12} - Y_{22}) \quad (7.44)$$

$$H_4 := X_{22} \cdot (Y_{21} - Y_{11}) \quad (7.45)$$

$$H_5 := (X_{11} + X_{12}) \cdot Y_{22} \quad (7.46)$$

$$H_6 := (X_{21} - X_{11}) \cdot (Y_{11} + Y_{12}) \quad (7.47)$$

$$H_7 := (X_{12} - X_{22}) \cdot (Y_{21} + Y_{22}) \quad (7.48)$$

Anschließend werden die vier Komponenten der Produktmatrix wie folgt erzeugt:

$$Z_{11} := H_1 + H_4 - H_5 + H_7 \quad (7.49)$$

$$Z_{12} := H_3 + H_5 \quad (7.50)$$

$$Z_{21} := H_2 + H_4 \quad (7.51)$$

$$Z_{22} := H_1 - H_2 + H_3 + H_6 \quad (7.52)$$

- a) Zeigen Sie, dass der Strassen-Algorithmus tatsächlich das Produkt  $X \cdot Y$  berechnet.
- b) Bestimmen Sie die asymptotische Laufzeitkomplexität des Strassen-Algorithmus. Vergleichen Sie die von Ihnen ermittelte Komplexitätsklasse mit jener der rekursiven, aber unoptimierten Variante.
- c) Ist der Strassen-Algorithmus immer besser als die Standardmethode, die Sie aus dem Mathematikunterricht kennen? Sehen Sie eine Möglichkeit, beide Algorithmen zu kombinieren?

### Aufgabe 7.9



**Webcode  
7789**

**Aufgabe 7.10****Webcode  
7437**

In Abschnitt 2.4.1 haben wir bewiesen, dass für alle  $n$  mit  $n \geq 4$  die Abschätzung

$$2^n < n! < n^n$$

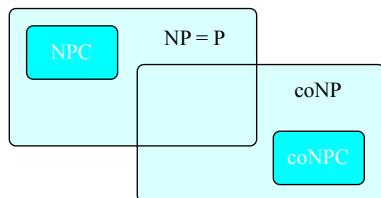
gilt. Welche der folgenden Beziehungen lassen sich aus diesem Ergebnis ableiten?

- a)  $2^n = O(n!)$
- b)  $2^n = \Omega(n^n)$
- c)  $2^n = o(n!)$
- d)  $2^n = \omega(n^n)$
- e)  $n! = O(2^n)$
- f)  $n! = \Omega(n^n)$
- g)  $n! = o(2^n)$
- h)  $n! = \omega(n^n)$
- i)  $n^n = O(2^n)$
- j)  $n^n = \Omega(n!)$
- k)  $n^n = o(2^n)$
- l)  $n^n = \omega(n!)$

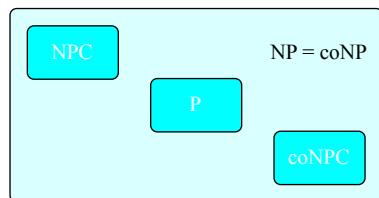
**Aufgabe 7.11****Webcode  
7189**

In diesem Kapitel haben Sie eine Reihe von Komplexitätsklassen zusammen mit ihren Inklusionsbeziehungen kennen gelernt. Wie die einzelnen Klassen genau in Beziehung stehen, ist heute noch nicht in allen Einzelheiten bekannt. Welche der abgebildeten Inklusionskonstellationen sind aus heutiger Sicht möglich?

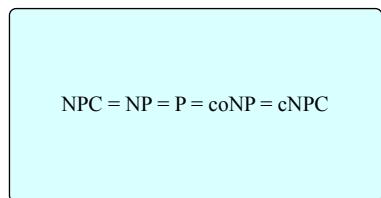
■ Konstellation 1



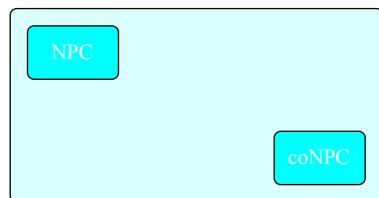
■ Konstellation 3



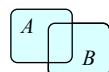
■ Konstellation 2



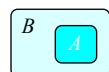
■ Konstellation 4



Interpretieren Sie die Venn-Diagramme nach dem folgenden Schema:



$A \setminus B \neq \emptyset, B \setminus A \neq \emptyset, A \cap B \neq \emptyset$



$A \subset B, B \setminus A \neq \emptyset$

In dieser Aufgabe wollen wir 3SAT auf Klauselmengen mit einer beliebigen, aber festen Anzahl von Literalen erweitern:

**Aufgabe 7.12**

**Webcode**  
7955

**Definition 7.19 ( $k$ -SAT)**

Das Problem  $k$ -SAT lautet wie folgt:

- Gegeben:  $n$  aussagenlogische Klauseln mit jeweils  $k$  Literalen.
- Gefragt: Gibt es eine erfüllende Belegung?

Beweisen Sie die folgenden Aussagen:

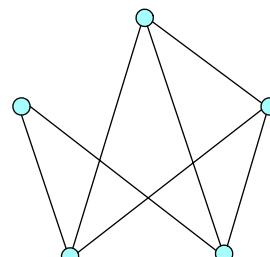
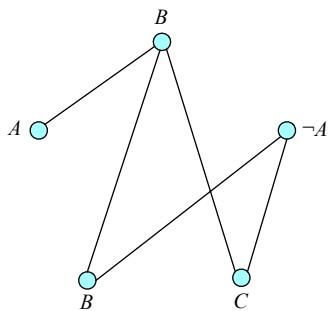
- a)  $k$ -SAT ist für  $k \geq 3$  NP-vollständig.
- b)  $k$ -SAT ist für  $k < 3$  polynomiell deterministisch lösbar.

In diesem Kapitel haben Sie gelernt, wie die NP-Vollständigkeit von CLIQUE durch die Reduktion von 3SAT bewiesen werden kann. Ausgehend von einer  $n$ -elementigen Klauselmenge  $M$  haben wir einen Graphen  $G$  konstruiert, der genau dann eine Clique der Größe  $n$  enthält, wenn  $M$  erfüllbar ist. Die resultierenden Graphen könnten z. B. wie folgt aussehen:

**Aufgabe 7.13**

**Webcode**  
7230

 ■  $G_1$ 

 ■  $G_2$ 


- a) Ihre Aufgabe ist es, den Konstruktionsprozess umzukehren. Geben Sie für  $G_1$  und  $G_2$  die Ausgangsmengen  $M_1$  und  $M_2$  an.
- b) Sind  $M_1$  und  $M_2$  für alle Graphen  $G_1$  und  $G_2$  immer eindeutig bestimmt?

**Aufgabe 7.14**

Welche der folgenden Aussagen sind richtig?



**Webcode  
7345**

- a)  $P = \bigcup_{k \in \mathbb{N}} \text{TIME}(n^k)$
- b)  $P = \bigcup_{a_i, k \in \mathbb{N}} \text{TIME}(a_k \cdot n^k + a_{k-1} \cdot n^{k-1} + \dots + a_1 \cdot n + a_0)$
- c)  $\text{EXP} = \bigcup_{c, k \in \mathbb{N}} \text{TIME}(c^{n^k})$
- d)  $\text{EXP} = \bigcup_{k \in \mathbb{N}} \text{TIME}(k^{n^k})$

# Anhang

---

**A Notationsverzeichnis**

**B Abkürzungsverzeichnis**

**C Glossar**

**Literaturverzeichnis**

**Namensverzeichnis**

**Sachwortverzeichnis**





# A Notationsverzeichnis

---

## Mathematik

$\emptyset$ oder $\{\}$	Leere Menge
$M, M_i, N, N_i \dots$	Menge
$\{a, b, c, \dots\}$	Menge mit den Elementen $a, b, c, \dots$
$a \in M$	$a$ ist enthalten in $M$
$a \notin M$	$a$ ist nicht enthalten in $M$
$\overline{M}$	Komplementärmenge
$M_1 \setminus M_2$	Differenzmenge
$M_1 \subseteq M_2$ oder $M_2 \supseteq M_1$	$M_1$ ist Teilmenge von $M_2$
$M_1 \subset M_2$ oder $M_2 \supset M_1$	$M_1$ ist Teilmenge von $M_2$ und $M_1 \neq M_2$
$M_1 \cup M_2$	Vereinigungsmenge von $M_1$ und $M_2$
$M_1 \cap M_2$	Schnittmenge von $M_1$ und $M_2$
$M_1 \times M_2$	Kartesisches Produkt (Kreuzprodukt) von $M_1$ und $M_2$
$M^n$	$M \times M \times \dots \times M$ ( $n$ -mal)
$ M $	Kardinalität von $M$
$2^M$	Potenzmenge (Menge aller Teilmengen von $M$ )
$\mathbb{N}$	Menge der positiven Zahlen $(1, 2, 3, \dots)$
$\mathbb{N}_0$	Menge der nichtnegativen Zahlen $(0, 1, 2, 3, \dots)$
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{Q}$	Menge der rationalen Zahlen (Brüche)
$\mathbb{R}$	Menge der reellen Zahlen
$x \bmod y$	Ganzzahliger Divisionsrest von $\frac{x}{y}$
$R, S, \dots$	Relation
$x \sim_R y$	$x$ und $y$ stehen in der Relation $R$ zueinander
$x \not\sim_R y$	$x$ und $y$ stehen nicht in der Relation $R$ zueinander
$R \cdot S$	Relationenprodukt
$R^{-1}$	Inverse Relation
$R^+$	Transitive Hülle von $R$
$R^*$	Reflexiv transitive Hülle von $R$
$[x]_\sim$	Äquivalenzklasse $(= \{y \mid x \sim y\})$
$f, g, h, \dots$	Funktion
$\text{succ}(x)$	Nachfolger der natürlichen Zahl $x$ ( $\text{succ}(x) = x + 1$ )
$a \uparrow^n b$	Up-Arrow-Notation zur Beschreibung großer Zahlen
$\text{ack}(n, m)$	Ackermann-Funktion
$\pi$	Kreiszahl oder (Cantor'sche) Paarungsfunktion

## Logik

$0$	Logisch falsch ( <i>false</i> )
$1$	Logisch wahr ( <i>true</i> )
$A_1, A_2, \dots, A, B, C, \dots, X, Y, Z$	Aussagenlogische Variable
$\neg A$ oder $\bar{A}$	Negation (nicht $A$ )
$(\neg)A$ oder $L$	Literal (entweder $A$ oder $\neg A$ )
$A \wedge B$	Konjunktion ( $A$ und $B$ )
$A \vee B$	Disjunktion ( $A$ oder $B$ )
$A \rightarrow B$	Implikation (aus $A$ folgt $B$ )
$A \leftrightarrow B$ oder $A \oplus B$	Antivalenz (entweder $A$ oder $B$ )
$A \leftrightarrow B$	Äquivalenz ( $A$ genau dann, wenn $B$ )
$F, G, H, \dots$	Formeln
$F = G$	Gleichheit ( $F$ und $G$ sind syntaktisch gleich)
$F \equiv G$	Äquivalenz ( $F$ und $G$ sind logisch äquivalent)
$F \equiv_E G$	Erfüllbarkeitsäquivalenz ( $F$ ist genau dann erfüllbar, wenn $G$ erfüllbar ist)
$I$	Interpretation oder Belegung
$I \models F$	Modellrelation ( $I$ ist ein Modell für $F$ )
$\vdash_K$ oder $\vdash$	Ableitungsrelation (im Kalkül $K$ )
$\{A, B, C\}$	Klausel (entspricht $A \vee B \vee C$ )
$\square$	Leere Klausel (entspricht 0)
$x, y, z, \dots$	Prädikatenlogische Variable
$f(x), g(x, f(y)), \dots$	Prädikatenlogischer Term
$P, Q, R, \dots$	Prädikat
$\forall, \exists$	Allquantor („für alle ...“), Existenzquantor („es gibt ein ...“)
$\Sigma = (U, I)$	Prädikatenlogische Signatur
$HU(F)$	$U$ = Grundmenge, Universum, Individuenbereich
$G(F)$	$I$ = Interpretation
	Herbrand-Universum der Formel $F$
	Grundinstanzen der Formel $F$

## Formale Sprachen

$G$	Grammatik
$V$	Variablenmenge (Menge aller Nonterminale)
$A, B, C, \dots$	Nonterminale
$\Sigma$	Terminalalphabet
$\sigma, \sigma_0, \sigma_1, \dots$	Terminale
$\epsilon$	Leeres Wort
$\Sigma^*$	Mit Symbolen aus $\Sigma$ bildbare Zeichenketten (Kleene'sche Hülle)
$\Sigma^+$	Entspricht $\Sigma^* \setminus \{\epsilon\}$
$\omega$	Wort ( $\omega \in \Sigma^*$ )

---

$ \omega $	Wortlänge (Anzahl der Symbole in $\omega$ )
$P$	Produktionenmenge
$L, L_1, L_2, \dots$	Sprache
$\mathcal{L}(G)$	Von $G$ erzeugte Sprache
$\Rightarrow_G$	Von $G$ induzierte Ableitungsrelation
$\mathcal{L}_n$	Menge der Typ- $n$ -Sprachen
$Reg_\Sigma$	Menge der regulären Ausdrücke

## Endliche Automaten

$A, A_1, A_2, \dots$	Automat
$S = \{s_0, s_1, \dots\}$	Zustandsmenge
$\Sigma$	Eingabealphabet
$\sigma, \sigma_0, \sigma_1, \dots$	Eingabezeichen
$\omega$	Eingabewort
$\delta$	Zustandsübergangsfunktion
$E$	Menge der Endzustände ( $E \subseteq S$ )
$\rightarrow_A$	Übergangsrelation
$\sim_k$	$k$ -Äquivalenz (zwischen Zuständen)
$\sim$	Bisimulation ( $\sim \subseteq S \times S$ )
$\varepsilon$	Leeres Wort bzw. $\varepsilon$ -Übergang
$\ s\ _\varepsilon$	$\varepsilon$ -Hülle des Zustands $s$
$K, K_1, K_2, \dots$	Kellerautomat
$\Gamma$	Kelleralphabet
$\gamma$	Kellerzeichen
$\perp$	Kellerbodensymbol
$T, T_1, T_2, \dots$	Transduktor
$\Pi$	Ausgabealphabet
$\pi, \pi_0, \pi_1, \dots$	Ausgabezeichen
$\lambda$	Ausgabefunktion
$P, P_1, P_2, \dots$	Petri-Netz
$\kappa$	Konfiguration
$I$	Inzidenzmatrix
$\Psi$	Parikh-Vektor
$Z$	Zellmenge (eines zellulären Automaten)
$v$	Nachbarschaftsfunktion

## Berechenbarkeitstheorie

$\text{succ}(x_i)$	Nachfolgerberechnung (+1)
$\text{pred}(x_i)$	(Gesättigte) Vorgängerberechnung ( $\max\{0, x_i - 1\}$ )

$\coloneqq$	Zuweisungsoperator
$;$	Kompositionsoperator
loop do end	Loop-Schleifenkonstrukt
while do end	While-Schleifenkonstrukt
if goto	Bedingter Sprung
halt	Stoppbefehl
$v$	Speichervektor
$\delta$	(Zustands)übergangsfunktion
$p_i^n(a_1, \dots, a_n)$	Projektion ( $p_i^n(a_1, \dots, a_n) := a_i$ )
$\mu$	Rekursionsoperator
$T, T_1, T_2, \dots$	Turing-Maschine
$S = \{s_0, s_1, \dots\}$	Zustandsmenge
$\Sigma$	Eingabealphabet
$\Pi$	Bandalphabet
$\omega, v$	Bandinhalt (als Wort)
$\sigma, \sigma_0, \sigma_1, \dots, \rho, \rho_0, \rho_1, \dots$	Bandinhalt (einzelne Zeichen)
$\square$	Blank-Symbol
$\leftarrow, \rightarrow, \circlearrowleft$	Kopfänderung einer Turing-Maschine (links, rechts, nicht bewegen)
$\pi$	Codierung, (Cantor'sche) Paarungsfunktion
$\langle T \rangle$	Gödelnummer der Turing-Maschine $T$
$\chi, \chi'$	Charakteristische Funktion, partielle charakteristische Funktion
$L \leq L'$	$L$ ist reduzierbar auf $L'$
$B(n)$	Biberfunktion
$L_D$	Diagonalsprache

## Komplexitätstheorie

$f(n) = O(g(n))$	$f$ wächst höchstens so schnell wie $g$
$f(n) = \Omega(g(n))$	$f$ wächst mindestens so schnell wie $g$
$f(n) = \Theta(g(n))$	$f$ wächst genauso schnell wie $g$
$f(n) = o(g(n))$	$f$ wächst langsamer als $g$
$f(n) = \omega(g(n))$	$f$ wächst schneller als $g$
$t_T$	Laufzeitfunktion
$s_T$	Bandplatzfunktion
P	Deterministisch in polynomieller Zeit entscheidbare Probleme
NP	Nichtdeterministisch in polynomieller Zeit entscheidbare Probleme
PSPACE	Deterministisch in polynomiellem Platzbedarf entscheidbare Probleme
NPSPACE	Nichtdeterministisch in polynomiellem Platzbedarf entscheidbare Probleme
EXP	Deterministisch in exponentieller Zeit entscheidbare Probleme
NEXP	Nichtdeterministisch in exponentieller Zeit entscheidbare Probleme
coP, coNP, ...	Komplementäre Komplexitätsklasse
$L \leq_{poly} L'$	$L$ ist polynomiell reduzierbar auf $L'$

## B

# Abkürzungsverzeichnis

---

ACM	Association for Computing Machinery
AKS	Agrawal-Kayal-Saxena(-Primzahltest)
BCD	Binary-Coded Decimal
BIP	Bruttoinlandsprodukt
BPCP	Binäres Post'sches Korrespondenzproblem
CMI	Clay Mathematics Institute
COBOL	COmmon Business-Oriented Language
CTL	Computation Tree Logic
CYK	Cocke-Younger-Kasami(-Algorithmus)
DEA	Deterministischer endlicher Automat
DET	Deterministischer endlicher Transduktor
DF	Disjunktive Form
DNF	Disjunktive Normalform
DNA, DNS	Desoxyribonukleinsäure
DT	Deduktionstheorem
DVD	Digital Versatile Disc
ENIAC	Electronic Numerical Integrator And Computer
EXP	(Deterministisch) exponentiell
FFT	Fast Fourier Transformation
FIFO	First In, First Out
GNU	GNU is not Unix
GUI	Graphical User Interface
HOL	Higher-Order Logic
HTML	HyperText Markup Language
HU	Herbrand-Universum
KF	Konjunktive Form
KNF	Konjunktive Normalform
LBA	Linear beschränkter Akzeptor
LIFO	Last In, First Out
LTL	Linear Temporal Logic
MP	Modus Ponens
MPCP	Modifiziertes Post'sches Korrespondenzproblem
NEA	Nichtdeterministischer endlicher Akzeptor
NEXP	Nichtdeterministisch exponentiell
NP	Nichtdeterministisch polynomiell
NPC	NP Complete (NP-vollständig)

NPSPACE	Nichtdeterministisch polynomieller Platzverbrauch
P	(Deterministisch) polynomiell
PCP	Post'sches Korrespondenzproblem
PDA	Pushdown Automaton (Kellerautomat)
PROLOG	PROGramming in LOGic
PSPACE	(Deterministisch) polynomieller Platzverbrauch
RAM	Random Access Machine oder Random Access Memory
ROM	Read-Only Memory
RNA, RNS	Ribonukleinsäure
RSA	Rivest-Shamir-Adleman(-Kryptosystem)
WZK	Wolf-Ziege-Kohlkopf(-Problem)
SAT	(Boolean) SATisfiability (problem)
SIGACT	Special Interest Group on Algorithms and Computation Theory
TM	Turing-Maschine
UC	University of California
ZA	Zellulärer Automat
ZF	Zermelo-Fraenkel(-Mengenlehre)
ZFC	Zermelo-Fraenkel(-Mengenlehre) mit Auswahlaxiom (axiom of Choice)

# C Glossar

---

Spezielle Variante des  $\text{\texttt{SAT}}$ -Problems. Für eine gegebene Menge von Klauseln mit je drei Literalen ist zu entscheiden, ob eine erfüllende Belegung existiert. Genau wie SAT gehört auch diese Fragestellung zu den  $\text{\texttt{NP-vollständigen}}$  Problemen. Aufgrund seiner Einfachheit wird 3SAT gerne dazu verwendet, um andere Probleme mit dem Mittel der  $\text{\texttt{polynomiellen Reduktion}}$  ebenfalls als NP-vollständig zu identifizieren.

**3SAT**

$\text{\texttt{Abschnitt 7.3.4}}$

Eine Menge  $M$  heißt abzählbar, wenn sie die gleiche  $\text{\texttt{Mächtigkeit}}$  wie die Menge der natürlichen Zahlen besitzt. Dies ist genau dann der Fall, wenn jedes Element von  $M$  eineindeutig einer natürlichen Zahl zugeordnet werden kann. Jede aufzählbare Menge mit unendlich vielen Elementen ist auch abzählbar, nicht jedoch umgekehrt.

**Abzählbarkeit**

$\text{\texttt{Abschnitt 2.3.3}}$

Beispiel einer Funktion, die  $\text{\texttt{While-berechenbar}}$ , aber nicht  $\text{\texttt{Loop-berechenbar}}$  ist. Ihre Existenz beweist, dass die  $\text{\texttt{Loop-Sprache}}$  nicht an die Stärke der meisten anderen in diesem Buch diskutierten  $\text{\texttt{Berechnungsmodelle}}$  herankommt.

**Ackermann-Funktion**

$\text{\texttt{Abschnitt 2.3.2}}$

Überbegriff für eine Reihe  $\text{\texttt{endlicher Automaten}}$ , die sich weiter in deterministische ( $\text{\texttt{DEA}}$ ) und nichtdeterministische ( $\text{\texttt{NEA}}$ ) Akzeptoren untergliedern lassen. In beiden Fällen bestehen die Automaten aus einer Menge von Zuständen, einem Eingabealphabet, einer Zustandsübergangsfunktion, einer Reihe von End- oder Finalzuständen sowie einem dedizierten Startzustand. In jedem Verarbeitungsschritt nimmt der Automat ein einzelnes Eingabzeichen entgegen und geht in einen neuen Zustand über. Die Eingabesequenz wird genau dann akzeptiert, wenn die Verarbeitung in einem Finalzustand endet.

**Akzeptor**

$\text{\texttt{Abschnitt 5.2}}$

Eine allgemeingültige Formel besitzt die Eigenschaft, dass jede  $\text{\texttt{Interpretation}}$  ein  $\text{\texttt{Modell}}$  ist. Eine solche Formel ist damit immer wahr, unabhängig davon, wie wir ihre Bestandteile interpretieren. Der Begriff wird synonym mit dem Begriff der  $\text{\texttt{Tautologie}}$  verwendet.

**Allgemeingültigkeit**

$\text{\texttt{Abschnitt 3.1.1}}$

**Allgemeiner Unifikator****☞ Abschnitt 3.2.3.1**

Spezieller **☞ Unifikator** mit der Eigenschaft, dass sich alle Unifikatoren durch die Anwendung einer weiteren Substitution erzeugen lassen.

**Antinomie****☞ Abschnitt 1.2.1**

Spezielle Art des logischen Widerspruchs, in der die Richtigkeit einer Aussage ihre eigene Falschheit zur Folge hat und umgekehrt. In formalen Systemen führen Antinomien zu Inkonsistenzen und damit zur völligen Unbrauchbarkeit der zugrunde liegenden Axiome und Schlussregeln. Zu den bekanntesten Vertretern gehören das **☞ Barbier-Paradoxon** sowie die **☞ Russell'sche Antinomie** der naiven Mengenlehre.

**Äquivalenzproblem****☞ Abschnitt 4.1**

Wichtige Problemstellung aus dem Bereich der **☞ formalen Sprachen**. Hinter dem Äquivalenzproblem verbirgt sich die Frage, ob zwei Sprachen  $L_1$  und  $L_2$  aus den gleichen Wörtern bestehen. Mit anderen Worten: Gilt  $L_1 = L_2$ ?

**Asymptotisches Wachstum****☞ Abschnitt 7.1.1**

Beschreibt den Werteverlauf einer Funktion  $f(n)$  für den Fall  $n \rightarrow \infty$ . Wie sich die Funktion  $f(n)$  auf einem beliebigen, aber endlichen Anfangsstück verhält, spielt für das asymptotische Wachstum keine Rolle. Von konstanten Faktoren wird ebenfalls abstrahiert, so dass die Wachstumsanalyse zu einer Einteilung von Funktionen in verschiedene **☞ Komplexitätsklassen** führt. Das asymptotische Wachstum ist die Grundlage, um das Laufzeitverhalten und den Speicherplatzverbrauch von Algorithmen auf einer abstrakten Ebene zu beschreiben.

**Aussagenlogik****☞ Abschnitt 3.1**

Die Aussagenlogik beschäftigt sich mit *atomaren Aussagen* („Es regnet“, „Die Straße ist nass“) und den Beziehungen, die zwischen solchen Aussagen bestehen („Wenn es regnet, dann ist die Straße nass“). Die Bedeutung der Aussagenlogik ist zweigeteilt. Zum einen ist sie als Teilmenge in nahezu allen anderen Logiken enthalten, unter anderem auch in der **☞ Prädikatenlogik** und den **☞ Logiken höherer Stufe**. Zum anderen spielt sie eine wichtige Rolle im Hardware-Entwurf, da sich jede kombinatorische Digitalschaltung mit Hilfe aussagenlogischer Formeln beschreiben lässt.

**Automatenminimierung****☞ Abschnitt 5.2.2**

Verfahren, um die Anzahl der Zustände eines **☞ endlichen Automaten** zu verringern, ohne die nach außen sichtbare Funktion zu verändern. Ein Automat heißt reduziert, wenn kein funktional äquivalenter Automat existiert, der weniger Zustände besitzt.

---

Bezeichnet die Umsetzung eines **endlichen Automaten** in ein Schaltungsmodell, das aus Speicherelementen und Logikgattern besteht. Die Automatensynthese ist ein wesentlicher Arbeitsschritt im Entwurfsprozess digitaler Hardware-Schaltungen.

**Automatensynthese**  
☞ Abschnitt 5.6.3

---

Zentraler Bestandteil eines **Hilbert-Kalküls**. Axiome bilden den Ausgangspunkt eines formalen Beweises und müssen per Definition nicht selbst abgeleitet werden. In einem formalen Beweis wird die zu zeigende Aussage durch die sukzessive Anwendung fest definierter **Schlussregeln** aus den Axiomen deduziert.

**Axiom**  
☞ Abschnitt 3.1.3.1

---

Spezielle Notation zur Beschreibung **kontextfreier Sprachen**. Die Backus-Naur-Form wurde erstmals zur Spezifikation der Sprache Algol60 eingesetzt und hat sich heute als De-facto-Standard für die Syntaxdefinition von Programmiersprachen etabliert.

**Backus-Naur-Form**  
☞ Abschnitt 4.4.2.2

---

Bildhafte **Antinomie**, die das Problem der Selbstbezüglichkeit anschaulich demonstriert. Der Barbier von Sevilla rasiert alle Männer von Sevilla, die sich nicht selbst rasieren. Die inuitive Annahme, dass der Barbier sich entweder selbst oder nicht selbst rasiert, wird durch einen Ringschluss stets zu Widerspruch geführt. Das Paradoxon entspricht im Kern der **Russell'schen Antinomie**, mit der die Mathematik zu Beginn des zwanzigsten Jahrhunderts in ihre bislang größte Krise gestürzt wurde.

**Barbier-Paradoxon**  
☞ Abschnitt 2.5

---

Eine Funktion  $f$  heißt berechenbar, falls ein systematisches Verfahren existiert, das für alle Eingaben  $x$  nach endlich vielen Schritten terminiert und den Funktionswert  $f(x)$  als Ausgabe liefert. Was wir unter einem systematischen Verfahren zu verstehen haben, wird durch die Definition eines **Berechnungsmodells** formal festgelegt. Der Begriff der berechenbaren Funktion ist eng mit dem Begriff der **Entscheidbarkeit** gekoppelt.

**Berechenbarkeit**  
☞ Abschnitt 6.1

---

Teilgebiet der theoretischen Informatik, das sich mit den formalen Grundlagen und den Grenzen der algorithmischen Methode befasst. Im Gegensatz zur **Komplexitätstheorie** steht die prinzipielle **Berechenbarkeit** einer Funktion im Vordergrund und nicht die Effizienz der Lösung. Eine zentrale Erkenntnis der Berechenbarkeitstheorie ist die Existenz unberechenbarer Funktionen (**Halteproblem**).

**Berechenbarkeitstheorie**  
☞ Kapitel 6

---

**Berechnungsmodell**

☞ Abschnitt 6.1

Formales Konstrukt, um den Begriff der ☞Berechenbarkeit mathematisch präzise zu erfassen. In der Vergangenheit wurden zahlreiche Berechnungsmodelle postuliert, die sich von außen betrachtet erheblich voneinander unterscheiden. Einige besitzen durch und durch mathematischen Charakter, während sich andere sehr nahe an der Hardware-Architektur realer Computersysteme orientieren. Die ☞primitiv-rekursiven Funktionen, die ☞ $\mu$ -rekursiven Funktionen und das Lambda-Kalkül gehören zur ersten Gruppe, die ☞Loop-, ☞Goto- und ☞While-Sprache sowie die ☞Turing-Maschine und die ☞Register-Maschine zur zweiten.

---

**Bisimulation**

☞ Abschnitt 5.2.2

Spezielle Äquivalenzrelation auf der Zustandsmenge eines ☞endlichen Automaten. Zwei Zustände  $s_1$  und  $s_2$  sind genau dann bisimulativ zueinander, wenn sich der Automat für alle zukünftigen Eingaben gleich verhält, unabhängig davon, ob er sich in  $s_1$  oder  $s_2$  befindet. Die Bestimmung bisimulativer Zustände ist eine Kernaufgabe in der ☞Automatenminimierung.

---

**Charakteristische Funktion**

☞ Abschnitt 6.4

Mathematisches Konstrukt, das den Zusammenhang zwischen der ☞Berechenbarkeit einer Funktion und der ☞Entscheidbarkeit einer Menge herstellt. Eine Menge  $M$  ist genau dann entscheidbar, wenn die charakteristische Funktion  $\chi_M$  berechenbar ist. Ein Spezialfall ist die partielle charakteristische Funktion, die direkt zum Begriff der ☞Semi-Entscheidbarkeit führt.

---

**Chomsky-Hierarchie**

☞ Abschnitt 4.2

Rangfolge von Klassen formaler ☞Grammatiken. Anhand der Struktur der Produktionsregeln wird eine Grammatik einer von vier Klassen zugeordnet. Typ-0-Grammatiken unterliegen keinerlei Einschränkung und definieren die Sprachklasse der rekursiv aufzählbaren Sprachen. Typ-1- und Typ-2-Grammatiken erzeugen die ☞kontextsensitiven und die ☞kontextfreien Sprachen. ☞Reguläre Sprachen werden von Typ-3-Grammatiken erzeugt. Zwischen den Sprachklassen besteht eine Inklusionsbeziehung, d.h., jede Typ-3-Sprache ist auch eine Typ-2-Sprache und so fort. Ferner existieren in jeder Klasse Sprachen, die in der eingebetteten Klasse nicht enthalten sind.

---

**Chomsky-Normalform**

☞ Abschnitt 4.4.2.1

Spezielle Darstellungsform für Typ-2-Grammatiken. Zu jeder ☞kontextfreien Sprache  $L$  existiert eine ☞Grammatik in Chomsky-Normalform, die  $L$  erzeugt. Die Chomsky-Normalform ist eng verwandt mit der ☞Greibach-Normalform.

---

**Church'sche These**  
☞ Abschnitt 6.2

Von Alonzo Church aufgestellte These über den Berechenbarkeitsbegriff. Sie besagt, dass die Klasse der Turing-berechenbaren Funktionen mit der Klasse der intuitiv berechenbaren Funktionen übereinstimmt. Mit anderen Worten: Jede Funktion, die überhaupt in irgendeiner Weise berechenbar ist, kann auch durch eine ☞Turing-Maschine berechnet werden. Die These wird durch die Beobachtung gestützt, dass alle hinreichend berechnungsstarken Modelle wie die ☞While-Sprache, die ☞Goto-Sprache, die ☞ $\mu$ -Rekursion oder die ☞Registermaschine exakt den gleichen Berechenbarkeitsbegriff definieren.

---

**Co-Komplexität**  
☞ Abschnitt 7.2.4

Zu jeder ☞Komplexitätsklasse  $C$  existiert die komplementäre Komplexitätsklasse  $\text{co}C$ . Eine Sprache  $L$  gehört genau dann zu  $\text{co}C$ , wenn das Komplement  $\bar{L}$  zu  $C$  gehört. Die co-Komplexität spielt nur im Bereich nichtdeterministischer Komplexitätsklassen eine Rolle. Für jede deterministische Komplexitätsklasse  $C$  gilt die Beziehung  $C = \text{co}C$ .

---

**CYK-Algorithmus**  
☞ Abschnitt 4.4.4

Nach John Cocke, Daniel Younger und Tadao Kasami benannter Algorithmus zur Lösung des ☞Wortproblems ☞kontextfreier Sprachen. Der Algorithmus basiert auf dem Verfahren der ☞dynamischen Programmierung. Ausgangspunkt ist eine ☞Grammatik  $G$  in ☞Chomsky-Normalform.

---

**DEA**  
☞ Abschnitt 5.2

Deterministischer endlicher ☞Akzeptor. Im Gegensatz zu seinem nichtdeterministischen Pendant (☞NEA) ist der auszuführende Zustandsübergang für jedes Eingabezeichen eindeutig definiert. Die von DEAs und NEAs akzeptierte Sprachklasse ist identisch und entspricht der Klasse der ☞regulären Sprachen.

---

**Diagonalisierung**  
☞ Abschnitt 2.3.3

Mathematisches Beweisverfahren, um Aussagen über die Mächtigkeit zweier Mengen zu verifizieren. Unter anderem kann mit der Methode die Gleichmächtigkeit von  $\mathbb{N}$  und  $\mathbb{Q}$  gezeigt (erstes Cantor'sche Diagonalargument) oder die Menge  $\mathbb{R}$  als überabzählbar entlarvt werden (zweites Cantor'sches Diagonalargument). In Kapitel 6 wurde die Diagonalisierung eingesetzt, um die ☞Unentscheidbarkeit des allgemeinen ☞Halteproblems zu beweisen.

---

**Dirichlet'sches Schubfachprinzip**  
☞ Abschnitt 3.1.1

Mathematische Schlussregel aus dem Bereich der diskreten Mathematik. Plakativ beschreibt sie den folgenden Sachverhalt: Werden  $n + 1$  Gegenstände auf  $n$  Fächer verteilt, so enthält mindestens ein Fach mehr

als einen Gegenstand. In der Literatur wird das Dirichlet'sche Schubfachprinzip auch als *Taubenschlagprinzip* bezeichnet, in Anlehnung an den englischen Begriff *pigeonhole principle*.

---

**Disjunktive Form**

☞ Abschnitt 3.1.2

Eine Logikformel liegt in disjunktiver Form vor, wenn sie als Disjunction von Konjunktionen aufgebaut ist.

---

**Disjunktive Normalform**

☞ Abschnitt 3.1.2

Eine Logikformel liegt in disjunktiver Normalform vor, wenn sie als Disjunction von ☞Mintermen aufgebaut ist und alle Minterme paarweise verschieden sind.

---

**Dynamische Programmierung**

☞ Abschnitt 4.4.4

Spezielles Konstruktionsprinzip für Algorithmen. Die dynamische Programmierung kann immer dann eingesetzt werden, wenn sich die optimale Lösung eines Problems aus den optimalen Lösungen seiner Teilprobleme zusammensetzen lässt. Ein bekannter Algorithmus, der nach diesem Prinzip arbeitet, ist der ☞CYK-Algorithmus zur Lösung des ☞Wortproblems ☞kontextfreier Sprachen. Auch das ☞Rucksackproblem lässt sich mit dem Prinzip der dynamischen Programmierung effizient lösen.

---

**Endlicher Automat**

☞ Kapitel 5

Mathematisches Modell zur Beschreibung zustandsbasierter Systeme. Entsprechend ihrer Funktionsweise werden endliche Automaten in ☞Akzeptoren und ☞Transduktoren eingeteilt. Akzeptoren sind ein wichtiges Hilfsmittel für die Analyse ☞formaler Sprachen. Transduktoren sind die theoretische Grundlage für die Modellierung jeglicher Computer-Hardware.

---

**Endlichkeitsproblem**

☞ Abschnitt 4.1

Wichtige Problemstellung aus dem Bereich der ☞formalen Sprachen. Hinter dem Endlichkeitsproblem verbirgt sich die Frage, ob eine Sprache  $L$  über einen endlichen Wortschatz verfügt. Mit anderen Worten: Gilt  $|L| < \infty$ ?

---

**Entscheidbarkeit**

☞ Abschnitt 6.4

Eine Menge  $M$  heißt entscheidbar, falls die ☞charakteristische Funktion ☞berechenbar ist. Für eine entscheidbare Menge  $M$  existiert ein systematisches Verfahren, das für alle Eingaben  $\omega$  nach endlicher Zeit beantwortet, ob  $\omega$  ein Element von  $M$  ist oder nicht. Heute wissen wir, dass zahllose ☞unentscheidbare Mengen existieren. Kurzum: Der algorithmischen Methode sind unüberwindbare Grenzen gesetzt.

---

**Epsilon-Übergang**  
☞ Abschnitt 5.3.3

Spontaner Zustandsübergang in einem ☞endlichen Automaten, der kein Eingabezeichen konsumiert. Epsilon-Übergänge (kurz  $\varepsilon$ -Übergänge) erleichtern die Konstruktion von ☞Akzeptoren für viele ☞reguläre Sprachen, führen aber zu keiner grundlegenden Veränderung des Automatenmodells. Jeder  $\varepsilon$ -Automat lässt sich in einen äquivalenten Automaten übersetzen, der keine  $\varepsilon$ -Übergänge mehr besitzt.

Eine erfüllbare Formel besitzt die Eigenschaft, dass mindestens eine ☞Interpretation auch ein ☞Modell ist. Eine wichtige Teilmenge der erfüllbaren Formeln sind die ☞Tautologien.

Zwei Formeln heißen erfüllbarkeitsäquivalent, wenn aus der ☞Erfüllbarkeit der einen die Erfüllbarkeit der anderen folgt. Zwei äquivalente Formeln sind immer auch erfüllbarkeitsäquivalent, aber nicht umgekehrt.

Die ☞Komplexitätsklasse EXP enthält alle Sprachen, die von deterministischen ☞Turing-Maschinen in exponentieller Zeit entschieden werden können.

Menge von Wörtern, die über einem endlichen Alphabet  $\Sigma$  gebildet werden. Formale Sprachen lassen sich mit Hilfe von ☞Grammatiken generativ erzeugen und anhand der ☞Chomsky-Hierarchie in verschiedene Klassen einteilen. Wichtige Fragestellungen in der Theorie der formalen Sprachen sind das ☞Wortproblem, das ☞Leerheitsproblem, das ☞Äquivalenzproblem und das ☞Endlichkeitsproblem.

In diesem Buch wird der Begriff des formalen Systems synonym mit dem Begriff des ☞Kalküls verwendet. Leider hat sich diese Terminologie in der Literatur nicht einheitlich durchgesetzt. So wird ein formales System in einigen Büchern nur dann als Kalkül bezeichnet, wenn es spezielle Eigenschaften wie z. B. die Forderung nach einer endlichen Anzahl von ☞Axiomen oder ☞Schlussregeln erfüllt.

Beweisverfahren für Formeln der ☞Prädikatenlogik. Der Gilmore-Algorithmus zeigt die ☞Allgemeingültigkeit einer Formel  $F$ , indem schrittweise die Menge der ☞Grundinstanzen von  $\neg F$  approximiert wird. Ist die erzeugte Teilmenge im aussagenlogischen Sinne ☞unbefüllbar, so ist nach dem ☞Satz von Herbrand auch die Formel

**Erfüllbarkeit**  
☞ Abschnitt 3.1.1

**Erfüllbarkeitsäquivalenz**  
☞ Abschnitt 3.2.2

**EXP**  
☞ Abschnitt 7.2.3

**Formale Sprache**  
☞ Abschnitt 4.1

**Formales System**  
☞ Abschnitt 3.1.3

**Gilmore-Algorithmus**  
☞ Abschnitt 3.2.3

$\neg F$  unerfüllbar. Aus der Unerfüllbarkeit von  $F$  folgt sofort die Allgemeingültigkeit von  $F$ .

### Gödelisierung

☞ Abschnitt 6.1.5.6

Eine injektive Funktion  $c : M \rightarrow \mathbb{N}$  heißt Gödelisierung, wenn die Bildmenge  $c(M)$  entscheidbar und neben  $c$  auch die Umkehrfunktion  $c^{-1}$  berechenbar ist.  $c(x)$  heißt die Gödelnummer des Elements  $x$ , geschrieben als  $\langle x \rangle$ . Die Gödelisierung erlaubt es, Aussagen über Objekte einer abzählbaren Menge  $M$  in Aussagen über die natürlichen Zahlen zu übersetzen.

### Goto-Programm

☞ Abschnitt 6.1.3

Programm, verfasst in der fiktiven Goto-Sprache. Der bedingte Sprungbefehl (If-Goto) ist die einzige Möglichkeit, den Kontrollfluss zu steuern. Nach der Church'schen These lässt sich jede intuitiv berechenbare Funktion mit Hilfe eines Goto-Programms berechnen.

### Goto-Sprache

☞ Abschnitt 6.1.3

Menge aller Goto-Programme. Nach der Church'schen These sind alle intuitiv berechenbaren Funktionen  $f$  Goto-berechenbar, d. h., es existiert ein Goto-Programm, das  $x$  als Eingabe entgegennimmt und  $f(x)$  als Ausgabe liefert. Die Goto-Sprache besitzt die gleiche Berechnungsstärke wie die While-Sprache, die Turing-Maschine, die Registermaschine und die  $\mu$ -rekursiven Funktionen.

### Grammatik

☞ Abschnitt 4.1

Instrumentarium zur generativen Beschreibung formaler Sprachen. Die Wörter einer Sprache werden aus einem Startsymbol durch die Anwendung verschiedener Produktionsregeln abgeleitet. Abhängig von der Struktur der einzelnen Produktionen werden Grammatiken in vier disjunkte Klassen eingeteilt. Es entsteht die sogenannte Chomsky-Hierarchie.

### Greibach-Normalform

☞ Abschnitt 4.7

Verallgemeinerung der Bildungsregeln regulärer Grammatiken. Es lässt sich zeigen, dass jede von einer Greibach-Grammatik erzeugte Sprache kontextfrei ist. Umgekehrt existiert zu jeder kontextfreien Sprache  $L$  mit  $\epsilon \notin L$  eine erzeugende Grammatik in Greibach-Normalform. Eine weitere wichtige Darstellungsvariante für Typ-2-Sprachen ist die Chomsky-Normalform.

### Grundinstanz

☞ Abschnitt 3.2.3

Sei  $F$  eine Formel der Prädikatenlogik. Eine Grundinstanz entsteht, indem alle Variablen durch Terme ersetzt werden, die ausschließlich Funktions- und Konstantensymbole aus  $F$  enthalten.

Synonym für die Frage, ob für jede  $\text{\texttt{Turing-Maschine}} T$  und jedes Eingabewort  $\omega$  algorithmisch entschieden werden kann, ob  $T$  unter Eingabe von  $\omega$  terminiert. Die  $\text{\texttt{Berechenbarkeitstheorie}}$  lehrt uns, dass das Halteproblem  $\text{\texttt{unentscheidbar}}$  ist und ein solches Entscheidungsverfahren aus fundamentalen Überlegungen heraus nicht existieren kann. Mit Hilfe der  $\text{\texttt{Reduktionstechnik}}$  lassen sich weitere  $\text{\texttt{unentscheidbare}}$  Probleme identifizieren. Hierzu gehören das  $\text{\texttt{Halteproblem auf leerem Band}}$ , das  $\text{\texttt{spezielle Halteproblem}}$  und das  $\text{\texttt{Post'sche Korrespondenzproblem}}$ . Die Verallgemeinerung des Halteproblems führt auf direkten Weg zum berühmten  $\text{\texttt{Satz von Rice}}$ .

**Halteproblem**  
 $\text{\texttt{Abschnitt 6.5}}$

Synonym für die Frage, ob für jede  $\text{\texttt{Turing-Maschine}} T$  algorithmisch entschieden werden kann, ob  $T$  unter Eingabe von  $\varepsilon$  terminiert. Das Halteproblem auf leerem Band ist  $\text{\texttt{unentscheidbar}}$ .

**Halteproblem auf leerem Band**  
 $\text{\texttt{Abschnitt 6.5}}$

Bekanntes Problem aus der Graphentheorie. Untersucht wird die Frage, ob in einem Graphen  $G$  ein geschlossener Weg existiert, der alle Knoten genau einmal besucht. Das Hamilton-Problem ist  $\text{\texttt{NP-vollständig}}$  und damit Teil einer großen Klasse schwer zu lösender Probleme. Für die  $\text{\texttt{Komplexitätstheorie}}$  ist es von Interesse, da eine geringfügige Änderung der Aufgabenstellung zu einem Problem führt, das in linearer Zeit gelöst werden kann ( $\text{\texttt{Königsberger Brückenproblem}}$ ).

**Hamilton-Problem**  
 $\text{\texttt{Abschnitt 1.2.4}}$

Spezielle  $\text{\texttt{Interpretation}}$  für Formeln der  $\text{\texttt{Prädikatenlogik}}$ , in der die Variablen- und Funktionssymbole durch Elemente des  $\text{\texttt{Herbrand-Universums}}$  interpretiert werden.

**Herbrand-Interpretation**  
 $\text{\texttt{Abschnitt 3.2.3}}$

Das Herbrand-Universum einer prädikatenlogischen Formel  $F$  ist die Menge aller variablenfreier Terme, die mit den Funktionssymbolen von  $F$  gebildet werden können.

**Herbrand-Universum**  
 $\text{\texttt{Abschnitt 3.2.3}}$

Ist eine  $\text{\texttt{Herbrand-Interpration}}$  ein  $\text{\texttt{Modell}}$  einer Formel  $F$ , so sprechen wir von einem Herbrand-Modell. Alle prädikatenlogischen Kalküle beruhen auf der Eigenschaft, dass eine Formel  $F$  genau dann erfüllbar ist, wenn sie ein Herbrand-Modell besitzt.

**Herbrand-Modell**  
 $\text{\texttt{Abschnitt 3.2.3}}$

Spezielle  $\text{\texttt{Kalküle}}$ , die sich an der traditionellen mathematischen Beweisführung orientieren. In einem Hilbert-Kalkül werden wahre

**Hilbert-Kalkül**  
 $\text{\texttt{Abschnitt 3.1.3}}$

Aussagen aus einer Menge von Axiomen durch die sukzessive Anwendung fest definierter Schlussregeln abgeleitet. Ein Beweis ist eine Folge von **Tautologien**, an deren Ende die Behauptung steht. Hilbert-Kalküle sind von hohem theoretischen Interesse, spielen in der Praxis dagegen kaum eine Rolle. Hier kommen fast ausschließlich **Widerspruchskalküle** zum Einsatz, in denen sich die **Allgemeingültigkeit** einer Formel mit weniger Aufwand beweisen lässt.

---

### Induktionsaxiom

**Abschnitt 2.3.1**

Name des fünften **Peano-Axioms**. Seine Aussage lautet wie folgt: Enthält eine Teilmenge  $M$  von  $\mathbb{N}$  die Zahl 1 und zu jedem Element  $n$  auch ihren Nachfolger  $n'$ , so gilt  $M = \mathbb{N}$ . Aus dem Induktionsaxiom erwächst das Beweisprinzip der **vollständigen Induktion**.

---

### Interpretation

**Abschnitt 3.1.1**

Spezielle Abbildung, die den Symbolen einer Logikformel eine Bedeutung zuordnet. Interpretationen sind das Bindeglied zwischen der **Syntax** und der **Semantik** einer **Logik**.

---

### Inzidenzmatrix

**Abschnitt 5.7**

Matrix der Größe  $m \times n$ , die das Schaltverhalten eines **Petri-Netzes** mit  $m$  Stellen und  $n$  Transitionen beschreibt. Für jede Stelle existiert eine eigene Zeile und für jede Transition eine eigene Spalte. Der Wert  $(i, j)$  besagt, wie sich die Anzahl der Marken in der Stelle  $S_i$  ändert, wenn die Transition  $T_j$  schaltet. Durch die Multiplikation mit dem **Parikh-Vektor** lässt sich die Folgekonfiguration berechnen.

---

### Kalkül

**Abschnitt 3.1.3**

Regelsystem, mit dem die Allgemeingültigkeit einer Logikformel auf **syntaktischer** Ebene bewiesen werden kann. Die Durchführung eines Beweises verläuft rein maschinell und kommt ohne Meta-Wissen über **Interpretationen** oder **Modelle** aus. In der **Aussagenlogik** und **Prädikatenlogik** spielen die **Hilbert-Kalküle**, der **Resolutionskalkül** und der **Tableaukalkül** eine hervorgehobene Rolle. Die beiden letztgenannten fallen in die Klasse der **Widerspruchskalküle**. In diesem Buch wird der Begriff des Kalküls synonym mit dem Begriff des **formalen Systems** verwendet.

---

### Kardinalzahl

**Abschnitt 2.3.3**

Maß für die **Mächtigkeit** einer Menge. Die Kardinalzahl einer endlichen Menge mit  $n$  Elementen entspricht  $n$ . Unendliche Mengen lassen sich bez. ihrer Mächtigkeit in Äquivalenzklassen einteilen, die durch die Kardinalzahlen  $\aleph_0, \aleph_1, \dots$  repräsentiert werden.  $\aleph$  (Aleph) ist der erste Buchstabe des hebräischen Alphabets.

---

Spezieller **endlicher Automat**, der neben einer endlichen Zustandsmenge einen **Kellerspeicher** besitzt. Durch den hinzugefügten Speicher gewinnen Kellerautomaten im Vergleich zu DEAs oder NEAs an Ausdrucksstärke hinzu. Die Klasse der von Kellerautomaten akzeptierten Sprachen entspricht der Klasse der **kontextfreien Sprachen**.

**Kellerautomat**  
☞ Abschnitt 5.5

---

Unendlich großer Speicher, der nach dem FIFO-Prinzip arbeitet. Die Abkürzung FIFO steht für *First In, First Out* und bedeutet, dass immer nur das oberste Kellerzeichen manipuliert werden kann.

**Kellerspeicher**  
☞ Abschnitt 5.5

---

Eine Klausel ist eine Menge von **Literalen**  $\{(\neg)A_1, \dots, (\neg)A_i\}$  und steht stellvertretend für die Formel  $(\neg)A_1 \vee \dots \vee (\neg)A_i$ . Die leere Klausel  $\square$  repräsentiert den Wahrheitswert 0.

**Klausel**  
☞ Abschnitt 3.1.2

---

Spezielle Darstellungsform für **While-Programme**, die mit einer einzigen While-Schleife auskommen. Nach dem **Satz von Kleene** existiert für jedes While-Programm ein äquivalentes Programm in Kleene'scher Normalform.

**Kleene'sche Normalform**  
☞ Abschnitt 6.1.3

---

In der **Komplexitätstheorie** werden Funktionen anhand ihres **asymptotischen Wachstums** in verschiedene Komplexitätsklassen eingeteilt. Für deren Beschreibung wird die **O-Notation** verwendet. Komplexitätsklassen werden eingesetzt, um die Laufzeit und den Platzverbrauch von Algorithmen zu kategorisieren. Von besonderer Bedeutung sind die Klassen **P**, **NP**, **EXP**, **NEXP**, **PSPACE** und **NPSPACE**. Zu jeder Komplexitätsklasse  $C$  existiert eine komplementäre Komplexitätsklasse  $\text{co}C$  (**Co-Komplexität**).

**Komplexitätsklasse**  
☞ Abschnitt 7.1.1

---

Teilgebiet der theoretischen Informatik, das sich mit der Frage beschäftigt, wie sich Algorithmen für sehr große Eingaben verhalten. Hierzu werden Algorithmen anhand ihres Speicherplatzbedarfs und Zeitverbrauchs in verschiedene Komplexitätsklassen eingeteilt, die Rückschlüsse auf das asymptotische Wachstum der untersuchten Parameter zulassen. Im Gegensatz zur **Berechenbarkeitstheorie**, die Fragen nach der puren Existenz von Berechnungsverfahren beantwortet, stellt die Komplexitätstheorie die praktische Verwertbarkeit von Algorithmen in den Vordergrund.

**Komplexitätstheorie**  
☞ Kapitel 7

---

**Konfiguration**

☞ Abschnitt 5.2

Momentaufnahme eines ☞*endlichen Automaten* oder einer ☞*Turing-Maschine*. Der Konfigurationsbegriff ist ein technisches Hilfsmittel, um Zustandsübergänge und die hieraus resultierende Ableitungsrelation in mathematisch präziser Form zu charakterisieren.

---

**Königsberger Brückenproblem**

☞ Abschnitt 1.2.4

Bekanntes Problem aus der Graphentheorie. Untersucht wird die Frage, ob in einem Graphen  $G$  ein geschlossener Weg existiert, der alle Kanten genau einmal besucht. Leonhard Euler konnte zeigen, dass das Problem in linearer Zeit gelöst werden kann. Für die ☞*Komplexitätstheorie* ist es von Interesse, da eine geringfügige Änderung der Aufgabenstellung ein ☞*NP-vollständiges* Problem entstehen lässt (☞*Hamilton-Problem*).

---

**Konjunktive Form**

☞ Abschnitt 3.1.2

Eine Logikformel liegt in konjunktiver Form vor, wenn sie als Konjunktion von Disjunktionen aufgebaut ist.

---

**Konjunktive Normalform**

☞ Abschnitt 3.1.2

Eine Logikformel liegt in konjunktiver Normalform vor, wenn sie als Konjunktion von ☞*Maxtermen* aufgebaut ist und alle Maxterme paarweise verschieden sind.

---

**Kontextfreie Grammatik**

☞ Abschnitt 4.2

Grammatik mit der Eigenschaft, dass die linke Seite einer Produktionsregel ausschließlich aus einer einzigen Variablen besteht. In der Nomenklatur der ☞*Chomsky-Hierarchie* werden kontextfreie Grammatiken als Typ-2-Grammatiken bezeichnet.

---

**Kontextfreie Sprache**

☞ Abschnitt 4.2

Eine Sprache  $L$  heißt kontextfrei, falls eine ☞*kontextfreie Grammatik* existiert, die  $L$  erzeugt. Die Menge der kontextfreien Sprachen entspricht der Menge der von ☞*Kellerautomaten* akzeptierten Sprachen.

---

**Kontextsensitive Grammatik**

☞ Abschnitt 4.2

Grammatik mit der Eigenschaft, dass die Anwendung einer Produktion niemals zu einer Verkürzung der abgeleiteten Zeichenkette führt. In der Nomenklatur der ☞*Chomsky-Hierarchie* werden kontextsensitiven Grammatiken als Typ-1-Grammatiken bezeichnet.

---

**Kontextsensitive Sprache**

☞ Abschnitt 4.2

Eine Sprache  $L$  heißt kontextsensitiv, falls eine ☞*kontextsensitive Grammatik* existiert, die  $L$  erzeugt. Die Menge der kontextsensitiven Sprachen entspricht der Menge der Sprachen, die von linear beschränkten ☞*Turing-Maschinen* akzeptiert werden.

Bezeichnung für die Symbolmenge  $\{O, \Omega, \Theta, o, \omega\}$ . Die Landau-Symbole werden in der  $\mathcal{O}$ -Notation verwendet, um das asymptotische Wachstum von Funktionen zu beschreiben.

**Landau-Symbole**  
☞ Abschnitt 7.1.1

Wichtige Problemstellung aus dem Bereich der formalen Sprachen. Hinter dem Leerheitsproblem verbirgt sich die Frage, ob eine gegebene Sprache  $L$  mindestens ein Wort enthält. Mit anderen Worten: Gilt  $L \neq \emptyset$ ?

**Leerheitsproblem**  
☞ Abschnitt 4.1

Ableitungssequenz mit der Eigenschaft, dass in jedem Schritt das am weitesten links stehende Nonterminal ersetzt wurde.

**Linksableitung**  
☞ Abschnitt 4.1

Bezeichnung für eine atomare Formel oder deren Negation. In der Aussagenlogik hat ein Literal damit die Form  $A$  oder  $\neg A$ , wobei  $A$  eine beliebige aussagenlogische Variable bezeichnet.

**Literal**  
☞ Abschnitt 3.1.2

Teilbereich der Mathematik, der sich mit grundlegenden Fragestellungen mathematischer Theorien beschäftigt. Ferner wird der Begriff für die Beschreibung von formalen Systemen verwendet, in denen die Syntax und die Semantik strikten Regeln folgen. In der Vergangenheit wurden verschiedene Logiken postuliert, die sich sowohl in ihrem Erscheinungsbild als auch in ihrer Ausdrucksstärke erheblich voneinander unterscheiden. Wichtige Vertreter sind die Aussagenlogik, die Prädikatenlogik sowie die Logiken höherer Stufe.

**Logik**  
☞ Kapitel 3

Erweiterung der Prädikatenlogik, die unter anderem stark genug ist, um die natürlichen Zahlen zu beschreiben. Im Gegensatz zur Prädikatenlogik dürfen in Logiken höherer Stufe auch Teilmengen des Grundbereichs, d. h. auch Prädikate quantifiziert werden. Erst hierdurch wird es möglich, das für die Formalisierung der natürlichen Zahlen unabdingbare Induktionsaxiom innerhalb der Logik auszudrücken. Logiken höherer Stufe werden in denjenigen Bereichen der formalen Hard- und Software-Verifikation eingesetzt, die eine hohe Ausdrucksstärke benötigen.

**Logik höherer Stufe**  
☞ Abschnitt 3.3

Programm, verfasst in der fiktiven Loop-Sprache. Die Loop-Schleife ist die einzige Möglichkeit, den Kontrollfluss zu steuern. Anders als in einem While-Programm steht die Anzahl der auszuführenden

**Loop-Programm**  
☞ Abschnitt 6.1.1

---

Iterationen vor dem Schleifeneintritt fest und kann danach nicht mehr verändert werden.

---

**Loop-Sprache**

☞ Abschnitt 6.1.1

Menge aller ☞Loop-Programme. Die Loop-Sprache ist berechnungsschwächer als die ☞While-Sprache oder die ☞Goto-Sprache. So lässt sich beispielsweise die ☞Ackermann-Funktion mit Hilfe eines ☞While-Programms oder eines ☞Goto-Programms berechnen, nicht jedoch mit einem Loop-Programm.

---

**Mächtigkeit**

☞ Abschnitt 2.3.3

Mathematisches Konstrukt, das quantitative Aussagen über die Anzahl der Elemente beliebig großer Mengen gestattet. Die Mächtigkeit endlicher Mengen wird mit der Anzahl ihrer Elemente gleichgesetzt. Unendliche Mengen werden bez. ihrer Eigenschaft untersucht, bijektiv auf andere Mengen mit bekannter Mächtigkeit abbildbar zu sein. Auf diese Weise entsteht eine Hierarchie verschiedener Unendlichkeiten, die sich mit Hilfe von ☞Kardinalzahlen eindeutig beschreiben lassen.

---

**Maxterm**

☞ Abschnitt 3.1.2

Aussagenlogische Formel, die für genau eine Variablenbelegung falsch wird. Ein Maxterm einer Funktion mit  $n$  Variablen besteht aus  $n$  disjunktiv verknüpften ☞Literalen.

---

**Mealy-Automat**

☞ Abschnitt 5.6.4

Spezieller ☞Transduktor, der die Ausgabe sowohl aus dem aktuellen Zustand als auch aus der aktuellen Eingabe berechnet. Mealy-Automaten werden aufgrund dieser Eigenschaft auch als Übergangautomaten bezeichnet.

---

**Mehrdeutigkeitsproblem**

☞ Abschnitt 4.1

Wichtige Problemstellung aus dem Bereich der ☞formalen Sprachen. Hinter dem Mehrdeutigkeitsproblem verbirgt sich die Frage, ob die Ableitungssequenzen einer Grammatik  $G$  stets eindeutig sind. In mehrdeutigen Grammatiken existiert mindestens ein Wort  $\omega$ , das sich durch unterschiedliche Regelanwendungen aus dem Startsymbol  $S$  ableiten lässt.

---

**Minterm**

☞ Abschnitt 3.1.2

Aussagenlogische Formel, die für genau eine Variablenbelegung wahr wird. Ein Minterm einer Funktion mit  $n$  Variablen besteht aus  $n$  konjunktiv verknüpften ☞Literalen.

---

**Modell**

☞ Abschnitt 3.1.1

Spezielle ☞Interpretation, die eine gegebene logische Formel wahr werden lässt.

---

Elementare Schlussregel der mathematischen Logik, die sich in Worten wie folgt umschreiben lässt: Wenn die Aussage  $A$  wahr ist und aus  $A$  die Aussage  $B$  folgt, so ist auch  $B$  wahr. Der Modus ponens ist die bevorzugte Schlussregel in den meisten  $\Rightarrow$ Hilbert-Kalkülen.

**Modus ponens**  
 $\Rightarrow$  Abschnitt 3.1.3

---

Spezieller  $\Rightarrow$ Transduktoren, der die aktuelle Ausgabe ausschließlich aus dem aktuellen Zustand berechnet. Moore-Automaten werden aufgrund dieser Eigenschaft auch als Zustandsautomaten bezeichnet.

**Moore-Automat**  
 $\Rightarrow$  Abschnitt 5.6.4

---

Kleinste Menge, die alle  $\Rightarrow$ primitiv-rekursiven Funktionen enthält und außerdem unter der Anwendung des  $\mu$ -Operators abgeschlossen ist. Die  $\mu$ -rekursiven Funktionen besitzen die gleiche Berechnungsstärke wie die  $\Rightarrow$ While-Sprache, die  $\Rightarrow$ Goto-Sprache, die  $\Rightarrow$ Turing-Maschine und die  $\Rightarrow$ Registermaschine. Nach der  $\Rightarrow$ Church'schen These ist jede intuitiv berechenbare Funktion auch  $\mu$ -rekursiv.

**$\mu$ -rekursive Funktion**  
 $\Rightarrow$  Abschnitt 6.1.4

---

Nichtdeterministischer endlicher  $\Rightarrow$ Akzeptor. Im Gegensatz zu seinem deterministischen Pendant ( $\Rightarrow$ DEA) können für die gleiche Eingabe mehrere mögliche Zustandsübergänge definiert sein und damit mehrere verschiedene Berechnungsfolgen für die gleiche Eingabe existieren. Mit dem  $\Rightarrow$ Potenzmengenautomaten existiert zu jedem NEA ein DEA, der die gleiche  $\Rightarrow$ formale Sprache akzeptiert. Die von DEAs und NEAs akzeptierten Sprachklassen sind identisch und entsprechen der Klasse der  $\Rightarrow$ regulären Sprachen.

**NEA**  
 $\Rightarrow$  Abschnitt 5.3

---

Eine Formel liegt in Negationsnormalform vor, wenn das Negationszeichen nur vor atomaren Formeln auftaucht. In der  $\Rightarrow$ Prädikatenlogik wird diese Darstellung als Zwischenschritt in der Erzeugung der  $\Rightarrow$ Pränex-Form verwendet.

**Negationsnormalform**  
 $\Rightarrow$  Abschnitt 3.2.2

---

Die  $\Rightarrow$ Komplexitätsklasse NEXP enthält alle Sprachen, die von nichtdeterministischen  $\Rightarrow$ Turing-Maschinen in exponentieller Zeit entschieden werden können.

**NEXP**  
 $\Rightarrow$  Abschnitt 7.2.3

---

Die  $\Rightarrow$ Komplexitätsklasse NP enthält alle Sprachen, die von nichtdeterministischen  $\Rightarrow$ Turing-Maschinen in polynomieller Zeit entschieden werden können. NP ist eine Obermenge von  $\Rightarrow$ P. Ob es sich dabei um eine echte Obermenge handelt ( $NP \setminus P \neq \emptyset$ ), ist Gegenstand des derzeit ungelösten  $\Rightarrow$ P-NP-Problems.

**NP**  
 $\Rightarrow$  Abschnitt 7.2.1

**NP-hart****Abschnitt 7.3.2**

Ein Problem ist NP-hart, wenn sich sämtliche Probleme der Komplexitätsklasse  $\text{\texttt{NP}}$  durch  $\text{\texttt{polynomiale Reduktion}}$  darauf abbilden lassen. Ein NP-hartes Problem kann, muss aber nicht selbst in der Klasse NP liegen.

**NPSPACE****Abschnitt 7.2.2**

Die  $\text{\texttt{Komplexitätsklasse}}$  NPSPACE enthält alle Sprachen, die von nichtdeterministischen  $\text{\texttt{Turing-Maschinen}}$  mit polynomiellem Bandplatzverbrauch entschieden werden können. Aus dem  $\text{\texttt{Satz von Savitch}}$  folgt, dass die Klasse NSPACE mit der Klasse  $\text{\texttt{PSPACE}}$  übereinstimmt.

**NP-vollständig****Abschnitt 7.3.2**

Ein Problem ist NP-vollständig, wenn es  $\text{\texttt{NP-hart}}$  ist und selbst in der Klasse  $\text{\texttt{NP}}$  liegt. NP-vollständige Probleme gelten als die schwierigsten Probleme innerhalb von NP, da sich alle anderen Probleme durch  $\text{\texttt{polynomiale Reduktion}}$  darauf abbilden lassen.

**O-Notation****Abschnitt 7.1.1**

Standardschreibweise für die Benennung von  $\text{\texttt{Komplexitätsklassen}}$ . Das große 'O' ist eines von fünf  $\text{\texttt{Landau-Symbolen}}$  und der Namensgeber dieser Notation.

**P****Abschnitt 7.2.1**

Die  $\text{\texttt{Komplexitätsklasse}}$  P enthält alle Sprachen, die von deterministischen  $\text{\texttt{Turing-Maschinen}}$  in polynomieller Zeit entschieden werden können. P ist eine Teilmenge von  $\text{\texttt{NP}}$ . Ob es sich dabei um eine echte Teilmenge handelt ( $\text{\texttt{NP}} \setminus \text{\texttt{P}} \neq \emptyset$ ), ist Gegenstand des derzeit ungelösten  $\text{\texttt{P-NP-Problems}}$ .

**Paarungsfunktion****Abschnitt 2.3.3**

Die Cantor'sche Paarungsfunktion bildet die Elemente der Menge  $\mathbb{N} \times \mathbb{N}$  bijektiv auf die Menge  $\mathbb{N}$  ab. Ihre Existenz beweist, dass die Menge  $\mathbb{N}^k$  für alle  $k \in \mathbb{N}$  die gleiche  $\text{\texttt{Mächtigkeit}}$  besitzt wie die natürlichen Zahlen selbst.

**Parikh-Vektor****Abschnitt 5.7**

Vektordarstellung einer Sequenz von nacheinander schaltenden Transitionen eines  $\text{\texttt{Petri-Netzes}}$ . Durch die Multiplikation mit der  $\text{\texttt{Inzidenzmatrix}}$  lässt sich die Folgekonfiguration eines Petri-Netzes berechnen.

**Partielle Funktion****Abschnitt 2.2**

Funktion, die nicht für alle Elemente ihres Definitionsbereichs einen definierten Funktionswert besitzt. In der klassischen Mathematik ist

dieser Begriff unbekannt – dort sind alle Funktionen per Definition **total**. In der theoretischen Informatik werden partielle Funktionen für die Beschreibung von Algorithmen eingesetzt, die für gewisse Eingabewerte nicht terminieren.

Formale Beschreibung der natürlichen Zahlen, die aus insgesamt fünf Axiomen besteht. Die Peano-Axiome dienen uns heute als Grundlage für den berechenbarkeitstheoretischen Umgang mit den natürlichen Zahlen. Unter anderem folgt aus Peanos fünftem Axiom, dem **Induktionsaxiom**, dass die **Prädikatenlogik** erster Stufe zu schwach ist, um die natürlichen Zahlen zu formalisieren.

**Peano-Axiome**  
☞ Abschnitt 2.3.1

Formales Modell zur Beschreibung nebenläufiger Systeme. Genau wie **endliche Automaten** arbeiten Petri-Netze zustandsbasiert, verfügen jedoch über deutlich komplexere Übergangsmechanismen. Streng unterschieden werden *Bedingungen* und *Ereignisse*. Erstere werden durch *Stellen*, letztere durch *Transitionen* beschrieben. In einem Petri-Netz wird der aktuelle Zustand eines Systems durch *Marken* modelliert. Schaltet eine Transition, so wird eine Marke aus jeder Eingabestelle entfernt und jeder Ausgangsstelle eine zusätzliche Marke hinzugefügt.

**Petri-Netz**  
☞ Abschnitt 5.7

Hinter diesem Problem verbirgt sich die Frage, ob jede Sprache, die durch eine nichtdeterministische Turing-Maschine in polynomieller Zeit entschieden werden kann, auch von einer deterministischen Turing-Maschine in polynomieller Zeit entschieden werden kann. Das P-NP-Problem gilt als das wichtigste der bis dato offenen Probleme der theoretischen Informatik, da seine Lösung weitreichende Konsequenzen für nahezu alle Teilbereiche der Informatik hat. Wäre  $P = NP$ , so ließen sich viele Algorithmen in polynomieller Zeit lösen, für die heute ausschließlich Algorithmen mit exponentiellem Zeitaufwand existieren. Unter anderem wären viele kryptografische Systeme auf einen Schlag angreifbar. In der großen Zahl der bisher entdeckten **NP-vollständigen** Probleme sehen viele Experten einen Hinweis darauf, dass P und NP voneinander verschieden sind. Einen formalen Beweis für diese Vermutung konnte jedoch noch niemand erbringen.

**P-NP-Problem**  
☞ Abschnitt 7.3.2

Wichtiges Beweisprinzip der **Komplexitätstheorie**. Im Rahmen eines Reduktionsbeweises wird gezeigt, dass sich ein Problem lösen lässt, indem die Fragestellung in polynomieller Zeit auf ein anderes Problem abgebildet wird, dessen (polynomiale) Lösung bereits bekannt ist. Durch den geschickten Einsatz dieser Technik lassen sich die Kom-

**Polynomielle Reduktion**  
☞ Abschnitt 7.3.1

plexitätseigenschaften vieler Probleme auf weitere Fragestellungen übertragen. Der Begriff ist eng verwandt mit der **Reduzierbarkeit** aus dem Bereich der **Berechenbarkeitstheorie**.

---

### Post'sches Korrespondenzproblem

**Abschnitt 6.5.4**

Für eine Folge von Wortpaaren  $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$  gilt es zu entscheiden, ob eine Indexsequenz  $i_1, \dots, i_k$  existiert, so dass die Konkatenation von  $x_{i_1}, \dots, x_{i_k}$  die gleiche Zeichenkette hervorbringt wie die Konkatenation von  $y_{i_1}, \dots, y_{i_k}$ . Genau wie das **Halteproblem** ist auch das **Post'sche Korrespondenzproblem unentscheidbar**. Die Eigenschaft, auf viele andere Problemstellungen **reduzierbar** zu sein, macht das Post'sche Korrespondenzproblem zu einem der wichtigsten Hilfsmittel im Bereich der **Berechenbarkeitstheorie**.

---

### Potenzmengenautomat

**Abschnitt 5.3.2**

Spezieller Automat, der die Potenzmenge der Zustände eines anderen Automaten als Zustandsraum verwendet. Der Potenzmengenautomat ist der Schlüssel, um die Äquivalenz von **DEAs** und **NEAs** zu beweisen. Die Konstruktion ermöglicht es, jeden **NEA** in einen **DEA** zu übersetzen, der die gleiche Sprache akzeptiert.

---

### Prädikatenlogik

**Abschnitt 3.2**

Die Prädikatenlogik erweitert die **Aussagenlogik** um mehrstellige Prädikate sowie um die Quantoren  $\forall$  („für alle“) und  $\exists$  („es existiert“). Viele Aspekte des logischen Schließens, die in der Aussagenlogik nicht ausgedrückt werden können, lassen sich mit Hilfe prädikatenlogischer Formeln formal beschreiben. Die Prädikatenlogik ist die Grundlage der Programmiersprache **Prolog**.

---

### Pränex-Form

**Abschnitt 3.2.2**

Eine Formel liegt in Pränex-Form vor, wenn alle Quantoren links von den anderen Formelbestandteilen stehen. Ausgehend von der **Negationsnormalform** lässt sich jede Formel der **Prädikatenlogik** in eine äquivalente Formel in Pränex-Form übersetzen.

---

### Primitive Rekursion

**Abschnitt 6.1.4**

Eine Funktion  $f : \mathbb{N}_0^2 \rightarrow \mathbb{N}_0$  ist nach dem Schema der **primitiven Rekursion** aufgebaut, wenn sie die folgende Form besitzt:

$$f(m, n) = \begin{cases} g(n) & \text{falls } m = 0 \\ h(f(m-1, n), m-1, n) & \text{falls } m > 0 \end{cases}$$

---

### Primitiv-rekursive Funktion

**Abschnitt 6.1.4**

Kleinste Menge von Funktionen, die die Nullfunktion, die Nachfolgerfunktion und die Projektion enthält und bez. Komposition und

---

☞ **primitiver Rekursion** abgeschlossen ist. Die Klasse der primitiv-rekursiven Funktionen besitzt die gleiche Berechnungsstärke wie die ☞ **Loop-Sprache**. Mit anderen Worten: Jede primitiv-rekursive Funktion lässt sich mit einem Loop-Programm berechnen und jede Loop-berechenbare Funktion ist ihrerseits primitiv-rekursiv. Die primitiv-rekursiven Funktionen sind vollständig in der Menge der ☞  **$\mu$ -rekursiven Funktionen** enthalten.

---

Logische Programmiersprache, die auf dem prädikatenlogischen ☞ **Resolutionskalkül** basiert. Prolog-Programme bestehen aus einer Problembeschreibung in Form von Logikformeln. Wird eine Anfrage gestellt, versucht der Prolog-Interpreter, die Antwort selbstständig aus der Problembeschreibung zu deduzieren.

### Prolog

☞ Abschnitt 3.2.4

---

Die ☞ **Komplexitätsklasse PSPACE** enthält alle Sprachen, die von deterministischen ☞ **Turing-Maschinen** mit polynomiellem Bandplatzverbrauch entschieden werden können. Aus dem ☞ **Satz von Savitch** folgt, dass die Klasse PSPACE mit der Klasse ☞ **NPSPACE** übereinstimmt.

### PSPACE

☞ Abschnitt 7.2.2

---

Hilfsmittel, um zu beweisen, dass eine Menge  $L \subseteq \Sigma^*$  keine ☞ **reguläre Sprache** oder keine ☞ **kontextfreie Sprache** ist. Das Pumping-Lemma nutzt die Eigenschaft dieser Sprachklassen aus, dass mit jedem hinreichend langen Wort  $\omega \in L$  auch diejenigen Wörter  $\omega_i$  in  $L$  enthalten sind, die durch das Duplizieren gewisser Teilsequenzen entstehen.

### Pumping-Lemma

☞ Abschnitt 4.3.2

---

Ableitungssequenz mit der Eigenschaft, dass in jedem Schritt das am weitesten rechts stehende Nonterminal ersetzt wurde.

### Rechtsableitung

☞ Abschnitt 4.1

---

Wichtiges Beweisprinzip der ☞ **Berechenbarkeitstheorie**. Im Rahmen eines Reduktionsbeweises wird gezeigt, dass sich ein Problem lösen lässt, indem die Fragestellung auf ein anderes Problem abgebildet wird, dessen Lösung bereits bekannt ist. Durch den geschickten Einsatz dieser Technik lassen sich die Berechenbarkeitseigenschaften vieler Probleme auf weitere Fragestellungen übertragen. Der Begriff ist eng verwandt mit der ☞ **polynomiellen Reduzierbarkeit** aus dem Bereich der ☞ **Komplexitätstheorie**.

### Reduktion

☞ Abschnitt 6.5

---

Spezielles ☞ **Berechnungsmodell**, das der Architektur realer Computer-systeme sehr nahe kommt. Eine Registermaschine setzt sich aus dem

### Registermaschine

☞ Abschnitt 6.1.6.1

Eingabeband, dem Ausgabeband und der Zentraleinheit zusammen. Letztere besteht aus dem Speicher, dem Programm und zwei Registern. Die Programmanweisungen werden über den Befehlszähler adressiert und sequentiell abgearbeitet. Arithmetische Berechnungen werden im Akkumulator durchgeführt. Die Registermaschine besitzt die gleiche Berechnungsstärke wie die  $\text{\texttt{While-Sprache}}$ , die  $\text{\texttt{Goto-Sprache}}$ , die  $\text{\texttt{Turing-Maschine}}$  und die  $\text{\texttt{\mu-rekursiven Funktionen}}$ . Nach der  $\text{\texttt{Church'schen These}}$  lässt sich jede intuitiv berechenbare Funktion mit Hilfe einer  $\text{\texttt{Registermaschine}}$  berechnen.

---

## Regulärer Ausdruck

$\Rightarrow$  Abschnitt 4.3.3

Alternative Beschreibungsform für  $\text{\texttt{reguläre Sprachen}}$ . Reguläre Ausdrücke sind der De-facto-Standard für die Spezifikation von Suchmustern.

---

## Reguläre Grammatik

$\Rightarrow$  Abschnitt 4.2

$\Rightarrow$  *Kontextfreie Grammatik* mit der zusätzlichen Eigenschaft, dass die rechte Seite einer Produktion entweder aus dem leeren Wort  $\epsilon$  oder einem Terminalsymbol, gefolgt von einem Nonterminal, besteht. In der Nomenklatur der  $\text{\texttt{Chomsky-Hierarchie}}$  werden kontextfreie Grammatiken als Typ-3-Grammatiken bezeichnet.

---

## Reguläre Sprache

$\Rightarrow$  Abschnitt 4.2

Eine Sprache  $L$  heißt regulär, falls eine  $\text{\texttt{reguläre Grammatik}}$  existiert, die  $L$  erzeugt. Die Menge der regulären Sprachen stimmt mit der Menge der von  $\text{\texttt{DEAs}}$  und  $\text{\texttt{NEAs}}$  akzeptierten Sprachen überein.

---

## Resolutionskalkül

$\Rightarrow$  Abschnitt 3.1.3

Spezielles  $\text{\texttt{Widerspruchskalkül}}$  der  $\text{\texttt{Aussagenlogik}}$  und  $\text{\texttt{Prädikatenlogik}}$ . Um die  $\text{\texttt{Allgemeingültigkeit}}$  einer Formel  $F$  zu zeigen, wird die negierte Formel  $\neg F$  in eine Menge von  $\text{\texttt{Klauseln}}$  übersetzt. Anschließend werden in einem iterativen Prozess neue Resolventen abgeleitet. Wird die leere Klausel  $\square$  deduziert, so terminiert das Verfahren. In diesem Fall ist gezeigt, dass  $\neg F$  kein  $\text{\texttt{Modell}}$  besitzt und  $F$  demnach eine  $\text{\texttt{Tautologie}}$  sein muss.

---

## Robinson-Algorithmus

$\Rightarrow$  Abschnitt 3.2.3.1

Systematisches Verfahren, um eine Menge prädikatenlogischer Formeln zu  $\text{\texttt{unifizieren}}$ . Der Algorithmus durchsucht die Formeln zeichenweise von links nach rechts. Abweichungen werden durch Substitutionen korrigiert. Sind die Eingabeformeln unifizierbar, so lässt sich der Unifikator durch die Verkettung der berechneten Substitutionen erzeugen. Der Algorithmus von Robinson berechnet den  $\text{\texttt{allgemeinsten Unifikator}}$  der Eingabemenge.

---

**Rucksackproblem**  
☞ Abschnitt 7.1

Ein Rucksack ist so mit Gegenständen zu bepacken, dass der erzielte Gesamtwert maximal wird, ohne das Fassungsvermögen zu überschreiten. In der hier vorgestellten Variante sind für jeden Gegenstandstyp beliebig viele Exemplare vorhanden und die Werte und Volumina ganzzahlig. Unter diesen Voraussetzungen lässt sich das Rucksackproblem effizient mit dem Mittel der ☞dynamischen Programmierung lösen. Eine leichte Abwandlung der Problemstellung lässt dagegen ein ☞NP-vollständiges Problem entstehen.

---

**Russell'sche Antinomie**  
☞ Abschnitt 1.2.1

Fundamentaler Widerspruch in der Cantor'schen Mengenlehre. Unter der Annahme, dass sich eine Menge  $M$  entweder selbst enthält oder nicht selbst enthält, definierte der britische Mathematiker Bertrand Russell die Menge aller Mengen, die sich nicht selbst als Element enthalten. Genau wie im Falle des ☞Barbier-Paradoxons führt diese Definition einen fundamentalen Widerspruch herbei. Erst der formale axiomatische Aufbau der Mengenlehre durch Ernst Zermelo und Abraham Fraenkel konnte die entdeckte Inkonsistenz im Cantor'schen Begriffsgerüst entgültig beheben.

---

**SAT**  
☞ Abschnitt 7.3.3

Frage nach der ☞Erfüllbarkeit einer Formel der ☞Aussagenlogik. Zu den Sternstunden der theoretischen Informatik gehört der Beweis, dass SAT ein ☞NP-vollständiges Problem ist (☞Satz von Cook).

---

**Satz von Cantor**  
☞ Abschnitt 2.3.3

Gleich mehrere zentrale Ergebnisse der Mathematik werden mit Georg Cantors Namen verbunden. Hierzu gehört der Nachweis, dass  $\mathbb{N}$  und  $\mathbb{N}^2$  die gleiche ☞Mächtigkeit besitzen (zu zeigen über das erste Cantor'sche Diagonalisierungsargument), wie auch der Satz über die ☞Überabzählbarkeit der reellen Zahlen (zu zeigen über das zweite Cantor'sche Diagonalisierungsargument).

---

**Satz von Cook**  
☞ Abschnitt 7.3.3

Im Jahre 1971 gelang es Stephen Cook, die ☞NP-Vollständigkeit von ☞SAT zu beweisen, ohne auf das Prinzip der ☞polynomiellen Reduktion zurückzugreifen. Der Satz ist in zweierlei Hinsicht von Bedeutung. Zum einen beweist er, dass NP-vollständige Probleme wirklich existieren. Zum anderen lassen sich durch polynomielle Reduktion andere Fragestellungen als NP-vollständig identifizieren. Hierzu gehören unter anderem das ☞Hamilton-Problem sowie die Probleme CLIQUE, SELECT, PARTITION, BIN PACKING und TRAVELING SALESMAN. Für die Durchführung der Reduktion wird zumeist auf die vereinfachte Variante ☞3SAT zurückgegriffen, die ebenfalls NP-vollständig ist.

---

**Satz von Herbrand**

☞ Abschnitt 3.2.3

Der Satz von Herbrand stellt einen wichtigen Zusammenhang zwischen der ☞*Prädikatenlogik* und der ☞*Aussagenlogik* her. Er besagt, dass eine Formel  $F$  in ☞*Skolem-Form* genau dann ein ☞*Herbrand-Modell* besitzt, wenn alle endlichen Teilmengen der ☞*Grundinstanzen* von  $F$  im aussagenlogischen Sinne erfüllbar sind.

---

**Satz von Kleene**

☞ Abschnitt 6.1.2

Besagt, dass sich jede While-berechenbare Funktion mit einem ☞*While-Programm* berechnen lässt, das eine einzige Schleife besitzt. Die Anzahl der Schleifen, die für die Umsetzung eines Algorithmus benötigt werden, ist somit unabhängig von dessen Komplexität.

---

**Satz von Rabin und Scott**

☞ Abschnitt 5.3.2

Besagt, dass zu jedem nichtdeterministischen endlichen Automaten ein deterministischer endlicher Automat existiert, der die gleiche Sprache akzeptiert.

---

**Satz von Rice**

☞ Abschnitt 6.5.2

Im Jahre 1953 gelang es Henry Gordon Rice, einen Zusammenhang zwischen dem ☞*Halteproblem* und einer beliebigen nichttrivialen Eigenschaft von Turing-Maschinen herzustellen. Aus dem Satz von Rice folgt unmittelbar, dass es unmöglich ist, irgendeine nichttriviale Eigenschaft von Turing-Maschinen algorithmisch zu überprüfen.

---

**Satz von Savitch**

☞ Abschnitt 7.2.2

Besagt, dass jedes von einer nichtdeterministischen ☞*Turing-Maschine* lösbar Problem mit einer deterministischen Turing-Maschine gelöst werden kann, deren Platzbedarf nur quadratisch höher liegt.

---

**Schlussregel**

☞ Abschnitt 3.1.3.1

Zentraler Bestandteil eines ☞*Hilbert-Kalküls*. Die Schlussregeln eines Kalküls definieren, wie sich aus bestehenden Aussagen neue Aussagen ableiten lassen. In einem formalen Beweis wird die zu zeigende Behauptung durch die sukzessive Anwendung der Schlussregeln aus den ☞*Axiomen* deduziert.

---

**Semantik**

☞ Abschnitt 3.1.1

Während die ☞*Syntax* den strukturellen Aufbau von Objekten beschreibt, befasst sich die Semantik mit deren Bedeutung. Im Bereich der natürlichen Sprache definiert die Semantik, welche Elemente der realen Welt sich hinter den gesprochenen Wörtern verbergen.

---

**Semi-Entscheidbarkeit**

☞ Abschnitt 6.4

Eine Menge  $M$  heißt semi-entscheidbar, falls die partielle ☞*charakteristische Funktion* ☞*berechenbar* ist. Für eine semi-entscheidbare

Menge  $M \subseteq \Sigma^*$  existiert ein systematisches Verfahren, das für alle Elemente  $\omega \in M$  nach endlicher Zeit die Mengenzugehörigkeit bestätigt. Ist  $\omega \notin M$ , so kommt die Berechnung zu keinem Ende.

Eine prädikatenlogische Formel liegt in Skolem-Form vor, wenn sie die Pränex-Form besitzt und keine Existenzquantoren mehr enthält. Jede Formel der Prädikatenlogik lässt sich in eine erfüllbarkeitsäquivalente Formel in Skolem-Form übersetzen.

Synonym für die Frage, ob für jede Turing-Maschine  $T$  algorithmisch entschieden werden kann, ob  $T$  unter Eingabe der eigenen Gödelnummer  $\langle T \rangle$  terminiert (Gödelisierung). Das spezielle Halteproblem ist unentscheidbar.

Variante der vollständigen Induktion, mit der sich Aussagen über rekursiv definierte Strukturen beweisen lassen. Hierzu wird die Aussage zunächst für alle Basisfälle explizit bewiesen und anschließend gezeigt, dass sich deren Gültigkeit auf zusammengesetzte Objekte vererbt.

Die Syntax befasst sich mit dem strukturellen Aufbau von Objekten. Im Bereich der natürlichen Sprache definiert die Syntax die Regeln, nach denen einzelne Wörter zu grammatisch korrekten Sätzen kombiniert werden können. Auf der syntaktischen Ebene werden Objekte als sinnleere Symbolketten verstanden. Erst die Semantik weißt den einzelnen Objekten eine Bedeutung zu.

Baumförmige Darstellung der Ableitungssequenzen einer Grammatik. Ein Syntaxbaum wird so konstruiert, dass alle inneren Knoten mit Nonterminalen und alle Blätter mit Terminalsymbolen markiert sind. In der Baumdarstellung geht die Information über die Reihenfolge der Produktionsanwendungen verloren, so dass verschiedene Ableitungssequenzen zu demselben Syntaxbaum führen können.

Spezielles Widerspruchskalkül der Aussagenlogik und Prädikatenlogik. Um die Allgemeingültigkeit einer Formel  $F$  zu zeigen, wird aus den Teilformeln von  $\neg F$  eine Baumstruktur – das sogenannte Tableau – erzeugt. Anhand spezieller Abschlussbedingungen lassen sich offene und geschlossene Zweige identifizieren. Sind alle Zweige geschlossen, so besitzt  $\neg F$  kein Modell und  $F$  ist als Tautologie identifiziert.

**Skolem-Form**  
☞ Abschnitt 3.2.2

**Spezielles Halteproblem**  
☞ Abschnitt 6.5

**Strukturelle Induktion**  
☞ Abschnitt 2.4.2

**Syntax**  
☞ Abschnitt 3.1.1

**Syntaxbaum**  
☞ Abschnitt 4.1

**Tableaukalkül**  
☞ Abschnitt 3.1.3.3

---

**Tautologie**

☞ Abschnitt 3.1.1

Bezeichnung für eine uneingeschränkt wahre Aussage. Der Begriff wird synonym mit dem Begriff der ☞Allgemeingültigkeit verwendet.

---

**Theoretische Informatik**

☞ Kapitel 1 – 7

Untersucht die mathematischen Methoden und Modelle, die sich hinter der Fassade der modernen Hardware- und Software-Technik verbergen. Wichtige Teilbereiche der theoretischen Informatik sind die ☞Logik, die Theorie der ☞formalen Sprachen, die Theorie der ☞endlichen Automaten sowie die ☞Berechenbarkeits- und die ☞Komplexitätstheorie.

---

**Totale Funktion**

☞ Abschnitt 2.2

Funktion, die für alle Elemente ihres Definitionsbereichs einen festgelegten Funktionswert besitzt. In der klassischen Mathematik sind alle Funktionen per Definition total und daher nicht explizit als solche gekennzeichnet. In der theoretischen Informatik existiert zusätzlich der Begriff der ☞partiellen Funktion.

---

**Transduktoren**

☞ Abschnitt 5.6

Neben den ☞Akzeptoren die zweite große Untergruppe ☞endlicher Automaten. Transduktoren bestehen aus einer Menge von Zuständen, einem Eingabe- und einem Ausgabealphabet, einer Zustandsübergangsfunktion sowie einem dedizierten Startzustand. In jedem Verarbeitungsschritt nimmt der Automat ein einzelnes Eingabezeichen entgegen und übersetzt dieses in ein Ausgabezeichen. Die Verarbeitung endet, wenn das letzte Eingabezeichen eingelesen wurde. Die Übersetzung von Transduktoren in digitale Hardware-Schaltungen ist Gegenstand der ☞Automatensynthese.

---

**Turing-Berechenbarkeit**

☞ Abschnitt 6.1.5

Eine Funktion  $f$  heißt Turing-berechenbar, falls eine ☞Turing-Maschine existiert, die  $f$  berechnet. Nach der ☞Church'schen These ist die Klasse der Turing-berechenbaren Funktionen mit der Klasse der intuitiv berechenbaren Funktionen identisch.

---

**Turing-Maschine**

☞ Abschnitt 6.1.5

Mathematisches Modell, um den Berechenbarkeitsbegriff formal zu erfassen. Grundlage ist ein eindimensionales Band, das sich aus unendlich vielen, nebeneinander angeordneten Zellen zusammensetzt. Die Maschine verfügt über einen Schreib-Lese-Kopf, der zu jeder Zeit über einer bestimmten Zelle positioniert ist. In jedem Bearbeitungsschritt kann eine Turing-Maschine das aktuell betrachtete Symbol durch ein anderes ersetzen und den Schreib-Lese-Kopf verschieben. Die ausgeführten Aktionen gehen mit einem potenziellen Wechsel des inneren Zustands einher. Anders als z. B. im Falle des ☞Transduktors

werden alle Lese- und alle Schreiboperationen auf dem gleichen Band ausgeführt. Turings Maschinenmodell besitzt die gleiche Berechnungsstärke wie die **While-Sprache**, die **Goto-Sprache**, die **Registermaschine** und die  **$\mu$ -rekursiven Funktionen**. Nach der **Church'schen These** lässt sich jede intuitiv berechenbare Funktion mit Hilfe einer Turing-Maschine berechnen.

Eine Menge  $M$  mit unendlich vielen Elementen heißt überabzählbar, wenn es nicht möglich ist,  $M$  bijektiv auf die Menge der natürlichen Zahlen abzubilden. Mit dem Mittel der **Diagonalisierung** kann unter anderem die Überabzählbarkeit der reellen Zahlen gezeigt werden. Der Begriff ist eng verwandt mit dem Begriff der **Abzählbarkeit**.

**Überabzählbarkeit**  
☞ Abschnitt 2.3.3

Eine Funktion  $f$  heißt unberechenbar, falls kein systematisches Verfahren existiert, das für alle Eingaben  $x$  nach endlich vielen Schritten terminiert und den Funktionswert  $f(x)$  als Ausgabe liefert. Was wir unter einem systematischen Verfahren zu verstehen haben, wird durch die Definition eines **Berechnungsmodells** formal festgelegt. Der Begriff der unberechenbaren Funktion ist eng mit dem Begriff der **Unentscheidbarkeit** gekoppelt.

**Ungerechenbarkeit**  
☞ Abschnitt 6.1

Eine Menge  $M$  heißt unentscheidbar, falls die **charakteristische Funktion** **unberechenbar** ist. Für eine unentscheidbare Menge  $M$  existiert kein systematisches Verfahren, das für alle Eingaben  $\omega$  nach endlicher Zeit beantwortet, ob  $\omega$  ein Element von  $M$  ist oder nicht. Viele praktische Fragestellungen, zu denen auch das **Halteproblem** und das **Post'sche Korrespondenzproblem** gehören, wurden in der Vergangenheit als unentscheidbar identifiziert.

**Unentscheidbarkeit**  
☞ Abschnitt 6.4

Eine unerfüllbare Formel besitzt die Eigenschaft, kein einziges **Modell** zu besitzen. Eine solche Formel ist damit immer falsch, unabhängig davon, wie wir ihre Bestandteile interpretieren.

**Unerfüllbarkeit**  
☞ Abschnitt 3.1.1

Methode, die für eine Menge prädikatenlogischer Formeln einen **Unifikator** berechnet. Ein bekannter Vertreter ist der **Robinson-Algorithmus** zur Berechnung des **allgemeinsten Unifikators**.

**Unifikation**  
☞ Abschnitt 3.2.3.1

Eine Menge prädikatenlogischer Formeln  $\{F_1, \dots, F_n\}$  heißt unifizierbar, falls eine Substitution  $\sigma$  existiert mit  $\sigma F_1 = \dots = \sigma F_n$ . Die Substitution  $\sigma$  wird als Unifikator bezeichnet.

**Unifikator**  
☞ Abschnitt 3.2.3.1

---

**Universelle Turing-Maschine**

☞ Abschnitt 6.1.5

Spezielle Turing-Maschine, die in der Lage ist, jede andere Turing-Maschine zu simulieren. Hierzu wird die zu simulierende Maschine **gödelisiert** und zusammen mit dem Eingabewort auf das Band geschrieben.

---

**Up-Arrow-Notation**

☞ Abschnitt 2.3.2

Von Donald E. Knuth eingeführte Schreibweise, mit der sich arithmetische Verknüpfungen in einem einheitlichen Schema darstellen lassen. Unter anderem ermöglicht die  $\uparrow$ -Notation, Operatoren wie die Hyperpotenz aufzuschreiben, für die in der klassischen Mathematik kein natives Symbol existiert.

---

**Vollständige Induktion**

☞ Abschnitt 2.4.1

Neben dem direkten und dem indirekten Beweis ist die vollständige Induktion die dritte klassische Beweistechnik der Mathematik. Sie ist immer dann anwendbar, wenn eine parametrisierte Aussage  $A(n)$  für alle natürlichen Zahlen  $n$  bewiesen werden soll. Ein Induktionsbeweis erfolgt in drei Schritten: Zunächst wird im Induktionsanfang die Aussage für einen oder mehrere Basisfälle bewiesen. Im nächsten Schritt erfolgt die Annahme, dass die Aussage für ein gewisses  $n$  und alle kleineren Werte bewiesen sei (Induktionsannahme). Gelingt im Anschluss der Beweis, dass aus der Gültigkeit von  $A(n)$  die Gültigkeit von  $A(n+1)$  folgt, so ist die Aussage für alle  $n$  bewiesen. Eine mit der vollständigen Induktion verwandte Beweistechnik ist die **strukturelle Induktion**.

---

**While-Programm**

☞ Abschnitt 6.1.2

Programm, verfasst in der fiktiven **While-Sprache**. Die While-Schleife ist die einzige Möglichkeit, den Kontrollfluss zu steuern. Nach der **Church'schen These** lässt sich jede intuitiv berechenbare Funktion mit Hilfe eines While-Programms berechnen.

---

**While-Sprache**

☞ Abschnitt 6.1.2

Menge aller **While-Programme**. Nach der **Church'schen These** sind alle intuitiv berechenbaren Funktionen  $f$  While-berechenbar, d. h., es existiert ein While-Programm, das  $x$  als Eingabe entgegennimmt und  $f(x)$  als Ausgabe liefert. Die While-Sprache besitzt die gleiche Berechnungsstärke, wie die **Goto-Sprache**, die **Turing-Maschine**, die **Registermaschine** und die  **$\mu$ -rekursiven Funktionen**.

---

**Widerspruchskalkül**

☞ Abschnitt 3.1.3

Spezieller **Kalkül**, der die **Allgemeingültigkeit** einer Formel über die **Unerfüllbarkeit** der negierten Aussage beweist. Bekannte Vertreter sind der **Resolutionskalkül** und der **Tableaukalkül**.

---

Wichtige Problemstellung aus dem Bereich der **formalen Sprachen**. Hinter dem Wortproblem verbirgt sich die Frage, ob ein bestimmtes Wort  $\omega$  in einer Sprache  $L$  enthalten ist. Mit anderen Worten: Gilt  $\omega \in L$ ?

**Wortproblem**  
☞ Abschnitt 4.1

---

Zustandsbasiertes System, das aus einer großen Anzahl simultan arbeitender Elementarautomaten, den sogenannten Zellen, besteht. Zu jedem Zeitpunkt befinden sich diese in einem von endlich vielen Zuständen. In jedem Schalschritt geht eine Zellen in eine Folgekonfiguration über, die sowohl durch ihren eigenen Zustand als auch durch die Zustände ihrer Nachbarn bestimmen wird. Hierdurch stehen die Zellen in ständiger Interaktion. Eingesetzt wird das Modell vor allem zur Beschreibung dynamischer, selbstorganisierender Systeme.

**Zellulärer Automat**  
☞ Abschnitt 5.8



# Literaturverzeichnis

---

- [1] Ackermann, W.: Zum Hilbertschen Aufbau der reellen Zahlen. In: *Mathematische Annalen* 99 (1928), S. 118–133
- [2] Agrawal, M.; Kayal, N.; Saxena, N.: PRIMES is in P. In: *Annals of Mathematics* 160 (2004), Nr. 2, S. 781–793
- [3] Aho, A. V.; Lam, M. S.; Sethi, R.; Ullman, J. D.: *Compilers. Principles, Techniques, and Tools*. Amsterdam: Addison-Wesley, 2006
- [4] Amos, M.: *Theoretical and Experimental DNA Computation*. Berlin, Heidelberg, New York: Springer-Verlag, 2005
- [5] Bachmann, P.: *Zahlentheorie. Versuch einer Gesamtdarstellung dieser Wissenschaft in ihren Haupttheilen. Zweiter Theil*. Leipzig: Teubner-Verlag, 1894
- [6] Bauer, F. L.: *Entziferte Geheimnisse, Methoden und Maximen der Kryptographie*. Berlin, Heidelberg, New York: Springer-Verlag, 2000
- [7] Biggs, N. L.; Lloyd, E. K.; Wilson, R. J.: *Graph Theory 1736 – 1936*. Oxford: Oxford University Press, 1986
- [8] Bois-Reymond, E. H. D.: *Über die Grenzen des Naturerkennens*. Saarbrücken: VDM Verlag Dr. Müller, 2006
- [9] Boole, G.: *An Investigation of the Laws of Thought*. London: Walton and Maberley, 1854. – Nachgedruckt in [10]
- [10] Boole, G.; Corcoran, J.: *The Laws of Thought (Reprint)*. New York: Prometheus Books, 2003
- [11] Kapitel The Busy Beaver Game and the Meaning of Life. In: Brady, A. H.: *The Universal Turing Machine: A Half Century Survey*. Oxford: Oxford University Press, 1991, S. 259 – 277
- [12] C. H. Edwards, Jr.: *The Historical Development of the Calculus*. Berlin, Heidelberg, New York: Springer-Verlag, 1994
- [13] Cantor, G.: Beiträge zur Begründung der transfiniten Mengenlehre. In: *Mathematische Annalen* 46 (1895), Nr. 4, S. 481–512
- [14] Cantor, G.; Zermelo, E. (Hrsg.): *Gesammelte Abhandlungen mathematischen und philosophischen Inhalts*. Hildesheim: Georg Olms Verlag, 1966

- [15] Casiro, F.: Das Hotel Hilbert. In: *Spektrum der Wissenschaft Spezial* 2 (2005), S. 76–80
- [16] Chomsky, N.: Three models for the description of language. In: *IEEE Transactions on Information Theory* 2 (1956), Nr. 3, S. 113–124
- [17] Chomsky, N.: *Syntactic Structures*. Berlin: Mouton de Gruyter, 2002
- [18] Church, A.: A Note on the Entscheidungsproblem. In: *The Journal of Symbolic Logic* 1 (1936), Nr. 1, S. 40–41
- [19] Church, A.: An Unsolvable Problem of Elementary Number Theory. In: *American Journal of Mathematics* 58 (1936), Nr. 2, S. 345–363
- [20] Church, A.: A Formulation of the Simple Theory of Types. In: *Journal of Symbolic Logic* 5 (1940), S. 56–68
- [21] Cobham, A.: The intrinsic computational difficulty of functions. In: Bar-Hillel, Y. (Hrsg.): *Proceedings of the 1964 International Congress for Logic, Methodology, and Philosophy of Science*. Amsterdam: North Holland, 1964, S. 24–30
- [22] Cocke, J.: *Programming languages and their compilers: Preliminary notes*. New York: Courant Institute of Mathematical Sciences, New York University, 1969
- [23] Cohen, P.: *Set Theory and the Continuum Hypothesis*. New York: Benjamin, 1963
- [24] Cook, S. A.: The Complexity of Theorem-Proving Procedures. In: *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing*. New York: ACM Press, 1971, S. 151–158
- [25] Dedekind, R.: *Stetigkeit und irrationale Zahlen*. Braunschweig, 1912
- [26] Dedekind, R.: *Was sind und was sollen Zahlen?* Braunschweig, 1918
- [27] Edmonds, J.: Paths, Trees, and Flowers. In: *Canadian Journal of Mathematics* 17 (1965), Nr. 3, S. 449–467
- [28] Euklid; Thaer, Clemens (Hrsg.): *Die Elemente. Buch I - XIII.* Frankfurt: Verlag Harri Deutsch, 2003 (Ostwalds Klassiker)
- [29] Euler, L.: Solutio problematis ad geometriam situs pertinentis. In: *Commentarii academiae scientiarum Petropolitanae* 8 (1741), S. 128 – 140
- [30] Floyd, R. W.: Algorithm 97: Shortest path. In: *Communications of the ACM* 5 (1962), June, Nr. 6, S. 345
- [31] Fraenkel, A.: Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre. In: *Mathematische Annalen* 86 (1922), S. 230–237
- [32] Frege, G.: *Grundgesetze der Arithmetik, Begriffsschriftlich abgeleitet*. Bd. 2. Jena: Verlag Hermann Pohle, 1903
- [33] Frege, G.: *Grundgesetze der Arithmetik, Begriffsschriftlich abgeleitet*. Bd. 2. Darmstadt: Wissenschaftliche Buchgesellschaft, 1962

- [34] Frege, G.: *Begriffsschrift und andere Aufsätze*. Hildesheim: Verlag Olms, 2007
- [35] Gödel, K.: *Über die Vollständigkeit des Logikkalküls*, Universität Wien, Diss., 1929
- [36] Gödel, K.: The consistency of the axiom of choice and of the generalized continuum-hypothesis. 24 (1938), S. 556–557
- [37] Gordon, M. J. C.; Melham, T. F.: *Introduction to HOL: A theorem proving environment for higher-order logic*. Cambridge: Cambridge University Press, 1993
- [38] Gray, F.: *U.S. Patent No. 2.632.058*. 1953
- [39] Hally, M.: *Electronic brains: Stories from the Dawn of the Computer Age*. Washington, D.C.: Joseph Henry Press, 2005
- [40] Harel, D.: *First-Order Dynamic Logic*. Berlin, Heidelberg, New York: Springer-Verlag, 1979 (Lecture Notes in Computer Science)
- [41] Hartmanis, J.; Stearns, R. E.: On the computational complexity of algorithms. In: *Transactions of the American Mathematical Society* 117 (1965), S. 285–306
- [42] Herbrand, J.: *Recherches sur la théorie de la démonstration*, University of Paris, Diss., 1930
- [43] Hermes, H.: *Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit*. Berlin, Heidelberg, New York: Springer-Verlag, 1961
- [44] Heuser, H.: *Lehrbuch der Analysis I*. Wiesbaden: Teubner-Verlag, 2006
- [45] Hilbert, D.: *Grundlagen der Geometrie*. Leipzig: Teubner Verlag, 1899. – Festschrift der Enthüllung des Gauß-Weber-Denkmales in Göttingen / hrsg. von dem Fest-Comitee
- [46] Hilbert, D.: Über das Unendliche. In: *Mathematische Annalen* 95 (1926), Nr. 1, S. 161–190
- [47] Hodges, A.: *Enigma*. Wien: Springer-Verlag, 1994
- [48] Hoffmann, D. W.: *Grundlagen der Technischen Informatik*. München: Hanser-Verlag, 2007
- [49] Hofstadter, D. R.: *Gödel, Escher, Bach: Ein endloses geflochtenes Band*. Stuttgart: Klett-Cotta, 2006
- [50] Hopcroft, J. E.; Ullman, J. D.; Motwani, R.: *Einführung in die Automatentheorie, Formale Sprachen und Komplexitätstheorie*. München: Pearson Studium, 2003
- [51] Immermann, N.: Nondeterministic space is closed under complementation. In: *SIAM Journal on Computing* 17 (1988), Nr. 5, S. 935–938
- [52] Kapitel Reducability Among Combinatorial Problems. In: Karp, R. M.: *Complexity of Computer Computations*. Plenum Press, 1972, S. 85 – 103
- [53] Kasami, T.: An efficient recognition and syntax analysis algorithm for context free languages. (1965), Nr. AF CRL-65-758

- [54] Kellerer, H.; Pferschy, U.; Pisinger, D.: *Knapsack Problems*. Berlin, Heidelberg, New York: Springer-Verlag, 2007
- [55] Kernighan, B. W.: *Programmieren in C*. München: Hanser Fachbuchverlag, 1990
- [56] Kernighan, B. W.; Pike, R. P.: *The UNIX Programming Environment*. Englewood Cliffs, NJ: Prentice Hall, 1984
- [57] Kleene, S. C.: Lambda-definability and recursiveness. In: *Duke Mathematical Journal* 2 (1936), S. 340–353
- [58] Kleene, S. C.: *Representation of events in nerve nets and finite automata. Project RAND Research Memorandum RM-704*. Santa Monica, CA: RAND Corporation, 1951
- [59] Knuth, D. E.: Mathematics and Computer Science: Coping with Finiteness. In: *Science Magazine* 194 (1976), Nr. 4271, S. 1235–1242
- [60] Knuth, D. E.: *The Art of Computer Programming, Volume 3: Sorting and Searching*. Redwood City, CA: Addison Wesley Longman Publishing Co., Inc., 1998
- [61] Kowalski, R. A.: The early years of logic programming. In: *Communications of the ACM* 31 (1988), Nr. 1, S. 38–43
- [62] Landau, E.: *Handbuch der Lehre von der Verteilung der Primzahlen*. Leipzig: Teubner-Verlag, 1909
- [63] Levin, L.: Universal Sequential Search Problems. In: *Problems of Information Transmission* 9 (1973), Nr. 3, S. 265–266
- [64] Levin, L.: Randomness Conservation Inequalities: Information and Independence in Mathematical Theories. In: *Information and Control* 61 (1984), April, Nr. 1, S. 15–37
- [65] Mandelbrot, B.: *Die Fraktale Geometrie der Natur*. Basel: Birkhäuser Verlag, 1987
- [66] McCulloch, W.; Pitts, W.: A Logical Calculus of the Ideas Immanent in Nervous Activity. In: *Bulletin of Mathematical Biophysics* 5/115 (1943)
- [67] Mealy, G. H.: A Method for Synthesizing Sequential Circuits. In: *Bell Systems Technical Journal* 34 (1955), September, S. 1045–1079
- [68] Menzel, W.; Schmitt, P. H.: *Formale Systeme. Vorlesungsskript Wintersemester 94/95*. Universität Karlsruhe, 1994
- [69] Minsky, M. L.: Size and Structure of Universal Turing Machines Using Tag Systems. In: *Recursive Function Theory: Proceedings, Symposium in Pure Mathematics* Bd. 5. Providence: American Mathematical Society, 1962, S. 229–238
- [70] Moore, E. F.: Gedanken-Experiments on Sequential Machines. In: Shannon, C. E. (Hrsg.); McCarthy, J. (Hrsg.): *Automata Studies*. Princeton, NJ: Princeton University Press, 1956, S. 129–153
- [71] Neumann, J. von; Burks, A. W. (Hrsg.): *Theory of self-reproducing automata*. Urbana: University of Illinois Press, 1966

- [72] Nielsen, M. A.; Chuang, I. L.: *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000 (Cambridge Series on Information & the Natural Sciences)
- [73] Peano, G.: *Arithmetices principia, nova methodo exposita*. Bocca: Augustae Taurinorum, 1889
- [74] Petri, C. A.: Kommunikation mit Automaten. In: *Schriften des Rheinisch-Westfälischen Institutes für instrumentelle Mathematik* (1962)
- [75] Post, E.: Formal reductions of the combinatorial decision problem. In: *American Journal of Mathematics* 65 (1943), Nr. 2, S. 197–215
- [76] Rabin, M.; Scott, D.: Finite automata and their decision problems. In: *IBM Journal of Research and Development* 3 (1959), S. 114–125
- [77] Rado, T.: On Non-Computable Functions. In: *The Bell System Technical Journal* 41 (1962), Nr. 3, S. 877–884
- [78] Rechenberg, P.: *Technisches Schreiben. (Nicht nur) für Informatiker*. München: Hanser-Verlag, 2006
- [79] Robinson, S.: New Method Said to Solve Key Problem in Math. (2002), August, 8
- [80] Savitch, W. J.: Relationships Between Nondeterministic and Deterministic Tape Complexities. In: *Journal of Computer and System Sciences* 4 (1970), Nr. 2, S. 177–192
- [81] Schöning, U.: *Logik für Informatiker*. Heidelberg: Spektrum Akademischer Verlag, 2000
- [82] Schöning, U.: *Theoretische Informatik – kurzgefasst*. Heidelberg: Spektrum Akademischer Verlag, 2001
- [83] Sedgewick, R.: *Algorithmen*. München: Pearson Studium, 2002
- [84] Sierpinski, W.: Sur une nouvelle courbe qui remplit toute une aire plaine. In: *Bull. Acad. Sci. Cracovie Serie A* (1912), S. 462–478
- [85] Solovay, R. M.; Strassen, V.: A fast Monte-Carlo test for primality. In: *SIAM Journal on Computing* 6 (1977), Nr. 1, S. 84–85
- [86] Stern, N.: Who Invented the First Electronic Digital Computer? In: *Annals of the History of Computing* 2 (1980), October, Nr. 4, S. 375–376
- [87] Strassen, V.: Gaussian Elimination is not Optimal. In: *Numerische Mathematik* 14 (1969), Nr. 3, S. 354–356
- [88] Szelepcsenyi, R.: The method of forced enumeration for nondeterministic automata. In: *Acta Informatica* 26 (1988), Nr. 3, S. 279–284
- [89] Thue, A.: Probleme über Veränderungen von Zeichenreihen nach gegebenen Regeln. In: *Skrifter utgit av Videnskapsselskapet i Kristiania* I.10 (1914)
- [90] Turing, A. M.: On computable numbers with an application to the Entscheidungsproblem. In: *Proceedings of the London Mathematical Society* 2 (1936), July – September, Nr. 42, S. 230–265

- [91] Turing, A. M.: Computability and Lambda-Definability. In: *Journal of Symbolic Logic* 2 (1937), Nr. 4, S. 153–163
- [92] Turing, A. M.: Computing Machinery and Intelligence. In: *Mind* 59 (1950), S. 433–460
- [93] Venn, J.: *Symbolic Logic*. London: MacMillan Publishing, 1881
- [94] Venn, J.: *Symbolic Logic (Reprint)*. Providence, RI: AMS Chelsea Publishing, American Mathematical Society, 2007
- [95] Viterbi, A. J.: Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. In: *IEEE Transactions on Information Theory* 13 (1967), Nr. 2, S. 260–269
- [96] Warshall, S.: A Theorem on Boolean Matrices. In: *Journal of the ACM* 9 (1962), January, Nr. 1, S. 11 – 12
- [97] Wermke, D. (Hrsg.); Kunkel-Razum, K. (Hrsg.); Scholze-Stubenrecht, W. (Hrsg.): *Duden, Die deutsche Rechtschreibung*. Mannheim: Dudenverlag, 2004
- [98] Williams, J. W. J.: Algorithm 232: Heapsort. In: *Communications of the ACM* 7 (1964), S. 347–348
- [99] Wolfram, S.: *A New Kind of Science*. Champaign, IL: Wolfram Media, Inc., 2002
- [100] Wolfram, S.: The Prize Is Won; The Simplest Universal Turing Machine is Proved. In: *Wolfram Blog*, <http://blog.wolfram.com> (2007), October
- [101] Younger, D. H.: Recognition and Parsing of Context-Free Languages in Time  $n^3$ . In: *Information and Control* 10 (1967), Nr. 2, S. 189–208
- [102] Zermelo, E.: Untersuchungen über die Grundlagen der Mengenlehre. In: *Mathematische Annalen* 64 (1908), S. 261–281
- [103] Zermelo, E.: Über Grenzzahlen und Mengenbereiche. In: *Fundamenta Mathematicae* 16 (1930), S. 29–47

# Namensverzeichnis

## A

Ackermann, Wilhelm F., 55  
Adleman, Leonard M., 27  
Agrawal, Manindra, 33  
Allen, Frances E., 27

## B

Bachman, Charles W., 27  
Backus, John W., 27, 171  
Bar-Hillel, Yehoshua, 175  
Binet, Jacques P. M., 76  
Blum, Manuel, 27  
Boole, George, 42, 43  
Brahmagupta, 52  
Brooks, Frederick P. Jr., 27  
Brown, Dan, 376

## C

Cantor, Georg F. L. P., 17, 38, 409  
Carbató, Fernando J., 27  
Cerf, Vinton G., 27  
Chomsky, A. Noam, 25, 160, 169  
Church, Alonzo, 265, 288, 289, 296, 393  
Clarke, Edmund M., 27  
Cocke, John, 27, 176, 393  
Codd, Edgar F., 27  
Cohen, Paul, 63  
Cohen, Paul J., 39  
Collatz, Lothar, 75  
Cook, Stephen A., 27, 32, 359, 362, 409

## D

da Pisa, Leonardo, 376  
Dahl, Ole-Johan, 27

De Morgan, Augustus, 43  
Dedekind, J. W. Richard, 53  
Descartes, René, 57  
Dijkstra, Edsger W., 27  
Dirichlet, Peter G. L., 87  
Du Bois-Reymond, Emil H., 19

## E

Eckert, J. Presper, 23  
Emerson, E. Allen, 27  
Engelbart, Douglas, 27  
Euklid von Alexandria, 14, 53  
Euler, Leonhard, 31, 71

## F

Feigenbaum, Edward, 27  
Fibonacci, 376  
Floyd, Robert W., 27  
Fraenkel, Abraham A. H., 17, 39, 409  
Frege, Gottlob, 16

## G

Garey, Michael, 32  
Gauß, J. Carl Friedrich, 57  
Gray, Jim, 27  
Gödel, Kurt, 143

## H

Hamilton, Sir William, 30  
Hamming, Richard, 27  
Hartmanis, Juris, 27  
Herbrand, Jacques, 120, 410  
Hermes, Hans, 56  
Hilbert, David, 15

Hoare, C. Antony R., 27  
Hofstadter, Douglas R., 35  
Hopcroft, John E., 27  
Horn, Alfred, 138

Iverson, Kenneth E., 27

## J

Johnson, David, 32

## K

Kahan, William, 27  
Kahn, Robert E., 27  
Karp, Richard M., 27, 32, 368  
Kasami, Tadao, 176, 393  
Kay, Alan, 27  
Kayal, Neeraj, 33  
Kleene, Stephen C., 26, 252, 256, 288, 289, 399, 410  
Knuth, Donald E., 27, 55, 414

## L

Lampson, Butler W., 27  
Landau, Edmund G. H., 338, 401  
Leibniz, Gottfried W., 52, 57  
Levin, Leonid, 32

## M

Mauchly, John W., 23  
McCarthy, John, 27, 288  
McCulloch, Warren S., 26  
Mealy, George H., 26

Milner, Robin, 27  
Minsky, Marvin L., 27, 282, 283  
Moore, Edward F., 26

## N

Naur, Peter, 27  
Newell, Allen, 27  
Newton, Sir Isaac, 52  
Nygaard, Kristen, 27

## P

Peano, Giuseppe, 51  
Perlis, Alan J., 27  
Petri, Carl A., 226  
Pitts, Walter, 26  
Pnueli, Amir, 27  
Post, Emil L., 314, 406

## R

Rabin, Michael O., 26, 27, 201, 350, 410  
Radó, Tibor, 325  
Reddy, Raj, 27

Rice, Henry G., 312, 410  
Ritchie, Dennis M., 27  
Rivest, Ronald L., 27  
Rosser, J. Barkley, 289  
Russell, Bertrand A. W., 17, 409

## S

Savitch, Walter, 353, 410  
Saxena, Nitin, 33  
Scott, Dana S., 26, 27, 201, 350, 410  
Shamir, Adi, 27  
Sifakis, Joseph, 27  
Simon, Herbert A., 27  
Smith, Alex, 283  
Solovay, Robert M., 32  
Stearns, Richard E., 27  
Stirling, James, 70  
Strassen, Volker, 32, 377  
Sutherland, Ivan, 27

## T

Tarjan, Robert E., 27  
Thompson, Kenneth L., 27  
Thue, Axel, 161

Tolkien, John R. R., 134  
Turing, Alan M., 20, 21, 265, 267, 289

## V

Venn, John, 40  
Viterbi, Andrew J., 176

## W

Whitehead, Alfred N., 17  
Wilkes, Maurice V., 27  
Wilkinson, J. H., 27  
Wirth, Niklaus E., 27  
Wolfram, Stephen, 232, 282, 283

## Y

Yao, Andrew Chi-Chih, 27  
Younger, Daniel H., 176, 393

## Z

Zermelo, Ernst F. F., 17, 39, 409  
Zuse, Konrad, 22

# Sachwortverzeichnis

## Symbolen

$\mu$ -Operator, 262  
 $\mu$ -Rekursion, 262  
 $\mu$ -rekursive Funktion, 263, 403  
3SAT, 366, 389  
4er-Nachbarschaft, 232  
8er-Nachbarschaft, 232

## A

Abbildung, 49  
Ableitungsrelation, 92  
Abschwächungsregel, 94  
Absolute Adressierung, 284  
Abstraktion, 288  
Abtrennungsregel, 17  
Abzählbarkeit, **58**, 304, 389  
Ackermann-Funktion, 55, 389  
Addierer  
  Carry-look-ahead-, 112  
  Carry-ripple-, 110  
Adressierung  
  absolute, 284  
  indirekte, 284  
  unmittelbare, 284  
Äquivalenz, 83  
Akkumulator, 284  
AKS-Algorithmus, 33  
Akzeptierende Turing-Maschine, 297  
Akzeptierender Automat, 193, 389  
Akzeptor, 193, 297, 389  
  Minimierung, 196  
  Turing-, 297  
Algorithmische Komplexität, 330  
Algorithmus  
  CYK-, 176, 393  
  effektiver, 27  
  effizienter, 27

Gilmore-, 124, 395  
Las-Vegas-, 32  
Monte-Carlo-, 32  
randomisierter, 32  
rekursiver, 259  
Robinson-, 127, 408  
Strassen-, 377  
Allgemeingültigkeit, 81, 389  
  prädikatenlogische, 117  
Allgemeinster Unifikator, 127, 390  
Alphabet, 154  
Antinomie, 390  
  Russell'sche, **17**, 39, 409  
Antivalenzoperator, 79  
Äquivalenz, 83  
  -klasse, 43  
  -operator, 79  
  -problem, 155, 390  
  -relation, 48  
Arbeitsband, 280  
Asymptotische Komplexität, 337  
Asymptotisches Wachstum, 390  
Atomare Aussage, 78, 390  
Atomare Formel, 79  
Aufzählbarkeit, 304  
Ausdruck  
  regulärer, 26, **166**, 207, 408  
Ausgabealphabet  
  von Transduktoren, 218  
Ausgabeband, 284  
Ausgabeschaltnetz, 221  
Aussage  
  atomare, 78, 390  
  Aussagenlogik, 23, **78**, 390  
  Normalformen, 87  
Auswahlaxiom, 39  
Automat  
  äquivalenter, 196  
  akzeptierender, 193, 389  
DEA, 194, 393  
deterministischer, 194  
endlicher, 25, **191**, 394  
Keller-, 211, 399  
linearer, 232  
Mealy-, 193, **222**, 402  
Moore-, 193, **222**, 403  
NEA, 199, 403  
nichtdeterministischer, 198  
Potenzmengen-, 201, 406  
Produkt-, 209  
reduzierter, 196  
übersetzender, 193, 218  
zellulärer, **231**, 239, 415  
Automatenminimierung, 390  
  von Akzeptoren, 196  
  von Transduktoren, 219  
Automatensynthese, 221, 391  
Automatentheorie, 25, 191  
Axiom, 35, 391

## B

Backtracking, 141  
Backus-Naur-Form, 171, 391  
  erweiterte, 171  
Bandalphabet  
  von Turing-Maschinen, 267  
Bandplatzfunktion, 352  
Bar-Hillel-Theorem, 175  
Barbier-Paradoxon, 34, 391  
Basis, 294  
BCD-Code, 236  
Befehlszähler, 284  
Belegung, 80  
Berechenbarkeit, **242**, 290, 391  
  Goto-, 254  
  Loop-, 244  
  Turing-, 269, 412

While-, 249  
 Berechenbarkeitstheorie, 241, 391  
 Berechnungsmodell, 242, 392  
 Beweis  
     direkter, 65  
     durch Widerspruch, 65  
     induktiver, 64  
 Beweistheorie  
     aussagenlogische, 92  
     prädikatenlogische, 120  
 Biberfunktion, 325  
 Bijektive Funktion, 50  
 Bild, 50  
 Binärbaum, 67  
     balancierter, 67  
 Binäre Codierung, 270  
 Binäre Suche, 373  
 Binomialkoeffizient, 76  
 Binomischer Lehrsatz, 76  
 Bisimulation, 196, 219, 392  
 Blättermenge, 67  
 Blank-Symbol, 267  
 Boolesche Algebra, 42  
 Boolesche Funktion, 81  
 Brute-Force-Methode, 350

**C**

Cantor'sche Paarungsfunktion, 60, 72  
 Cantor-Maschine, 306  
 Carry bit, 110  
 Carry-look-ahead-Addierer, 112  
 Carry-ripple-Addierer, 110  
 CD, 235  
 Charakteristische Funktion, 303, 392  
 Chomsky-Hierarchie, 25, 160, 392  
 Chomsky-Normalform, 169, 392  
 Church'sche These, 242, 290, 296, 393  
 Church-Rosser-Eigenschaft, 289  
 CLIQUE, 369  
 Co-Komplexität, 355, 393  
 COBOL, 24  
 Code  
     einschrittiger, 219  
 Codierung  
     binäre, 270  
     unäre, 270

Collatz-Funktion, 75  
 Colossus, 23  
 Computation Tree Logic, 142  
 Cook  
     Satz von, 359, 369  
 Cook, Satz von, 409  
 CYK-Algorithmus, 176, 393

**D**

Datenspur, 275  
 DEA, 194, 393  
 Deadlock, 230  
 Dedekind'scher Schnitt, 53  
 Deduktion, 77  
 Deduktionsbeweis, 65  
 Definition  
     rekursive, 64  
 Definitionsmenge, 49  
 Deklarative Programmierung, 134  
 Deterministischer Automat, 194  
 Diagonalisierung, 38, 393  
 Diagonalisierungsargument, 60  
 Diagonalsprache, 326  
 Differenzmenge, 41  
 Dirichlet'sches Schubfachprinzip, 86, 393  
 Disjunktion, 78  
 Disjunktive Form, 91, 394  
 Disjunktive Minimalform, 91  
 Disjunktive Normalform, 89, 394  
 Distributivgesetz, 41, 94  
 Divide and conquer, 344  
 DNA computing, 296  
 DVD, 235  
 Dyck-Sprache, 157, 215  
 Dynamische Logik, 283  
 Dynamische Programmierung, 176, 334, 394

**E**

Einband-Turing-Maschine, 265  
 Eingabealphabet  
     von  $\varepsilon$ -Automaten, 203  
     von DEAs, 194  
     von Kellerautomaten, 212

von NEAs, 199  
 von Transduktoren, 218  
 von Turing-Maschinen, 267

Eingabeband, 284  
 Einschrittiger Code, 219  
 Element, 38  
 Elementaroperatoren, 85  
 Endlicher Automat, 25, 191, 394  
 Endlichkeitsproblem, 154, 394  
 Endrekursion, 260  
 Endzustand  
     von  $\varepsilon$ -Automaten, 203  
     von DEAs, 194  
     von NEAs, 199  
     von Turing-Maschinen, 267

Enigma, 23  
 Entscheidbarkeit, 19, 303, 394  
     Semi-, 303, 410

Epsilon-Übergang, 203, 395

Erfüllbarkeit, 395  
     aussagenlogische, 81  
     prädikatenlogische, 117  
 Erfüllbarkeitsäquivalenz, 119, 395  
 Erreichbarkeitsanalyse, 229  
 Euklidische Axiome, 15  
 Euler-Kreis, 29  
 EXP, 353, 395

**F**

Faktorisierungsregel, 130  
 Faktum  
     in Prolog, 134  
 Ferritkernspeicher, 24  
 Fibonacci-Folge, 376  
 Finalzustand  
     von  $\varepsilon$ -Automaten, 203  
     von DEAs, 194  
     von NEAs, 199  
     von Turing-Maschinen, 267

Fixpunkt, 198  
     -operator, 289  
 Fleißiger Biber, 325  
 Flipflop, 221  
 Formale Sprache, 25, 154, 395  
 Formales System, 12, 35, 395  
 Formel

aussagenlogische, 78  
 bereinigte, 115  
 erfüllbarkeitsäquivalente, 119  
 geschlossene, 115  
 prädikatenlogische, 115

Formelmenge  
 konsistente, 96  
 vollständige, 96

Formulario-Projekt, 51

FORTRAN, 24

Funktion, 43, 49  
 $\mu$ -rekursive, 263, 403  
 Ackermann-, 55, 389  
 bijektive, 50  
 boolesche, 81  
 charakteristische, 303, 392  
 injektive, 50  
 partielle, 50, 246, 404  
 primitiv-rekursive, 257, 406  
 surjektive, 50  
 totale, 50, 412  
 unberechenbare, 307

Funktionstabelle, 81

Funktionswert, 50

**G**

Gegenbeispiel, 105  
 Generative Grammatik, 25  
 Gilmore-Algorithmus, 124, 395  
 Gleichheitsrelation, 46  
 Gödelisierung, 279, 396  
 Gödelnummer, 279, 309, 327, 396  
 Goto-Berechenbarkeit, 254  
 Goto-Programm, 252, 396  
 Goto-Sprache, 252, 396  
 Grad  
     von Polynomen, 341  
 Grammatik, 154–156, 396  
     eindeutige, 159  
     generative, 25  
     kontextfreie, 160, 169, 400  
     kontextsensitive, 160, 181, 400  
     mehrdeutige, 159  
     rechtslineare, 162  
     reguläre, 160, 162, 408  
 Greibach-Normalform, 187, 396

Grundinstanz, 123, 396  
 Grundlagenkrise, 14  
 Grundmenge, 116  
 Grundsubstitution, 117

**H**

Halteproblem, 21, 307, 397  
 allgemeines, 308  
 auf leerem Band, 310, 397  
 spezielles, 327, 411

Hamilton-Kreis, 30  
 Hamilton-Problem, 351, 397  
 Hardware-Entwurf, 108  
 Haskell, 288  
 Head recursion, 260  
 Herbrand  
     Satz von, 122, 410  
 Herbrand-Interpretation, 122, 397  
 Herbrand-Modell, 122, 397  
 Herbrand-Universum, 121, 397  
 Hilbert-Kalkül, 93, 397  
 Hilbert-Wüste, 73  
 Hilbertprogramm, 18  
 Hilberts Hotel, 60  
 Horn-Formel, 139  
 Hülle  
     Kleene'sche, 154  
     reflexiv transitive, 46, 47  
     transitive, 46

Huffman-Normalform, 222

**I**

Identität, 46  
 Ignorabimus, 19  
 Imaginäre Einheit, 69  
 Implikation, 78  
 Indirekte Adressierung, 284  
 Individuenbereich, 116  
 Induktion  
     strukturelle, 67, 411  
     vollständige, 43, 65, 414  
 Induktionsaxiom, 398  
 Induktiver Beweis, 64  
 Injektive Funktion, 50  
 Instanzen, 95

Interpretation, 80, 116, 398

Herbrand-, 122, 397

Inverses Element, 41

Inzidenzmatrix, 227, 398

Irrationale Zahl, 53

Isomorphie, 202

Iterationslemma, 175

**K**

Kalkül, 12, 35, 92, 398

Hilbert-, 93, 397

Lambda-, 288

Resolutions-, 101, 126, 408

Tableau-, 105, 131, 411

Widerspruchs-, 93, 414

Kapazität, 229

Kardinalität, 38, 57

Kardinalzahl, 63, 398

Kartesisches Produkt, 43

Kelleralphabet, 212

Kellerautomat, 211, 399

deterministischer, 216, 217

Kellerspeicher, 399

Kettenregel, 170

Klausel, 91, 399

leere, 91

Klauseldarstellung, 91

Kleene

Satz von, 252, 410

Kleene'sche Hülle, 154

Kleene'sche Normalform, 256, 292, 399

Königsberger Brückenproblem, 29, 400

Kollisionsfreiheit, 131

Kommutativgesetz, 41

Komplementärautomat, 208

Komplementärmenge, 41

Komplexe Zahl, 69

Komplexitätsklasse, 29, 344, 399

komplementäre, 355, 393

Komplexitätstheorie, 329, 399

Komposition, 258

Konfiguration, 400

globale, 232

lokale, 232

von  $\varepsilon$ -Automaten, 203

von DEAs, 195

von Kellerautomaten, 213  
von NEAs, 200  
von Petri-Netzen, 227  
von Turing-Maschinen, 268

Konjunktion, 78  
Konjunktive Form, 91, 400  
Konjunktive Minimalform, 91  
Konjunktive Normalform, 89, 400  
Konklusion, 94  
Konsistente Formelmenge, 96  
Kontextfreie Grammatik, 160, **169**, 400  
Kontextfreie Sprache, **169**, 214, 400  
Kontextsensitive Grammatik, 160, **181**, 400  
Kontextsensitive Sprache, 181, 400  
Kontinuum, 63  
Kontinuumshypothese, 63  
Kontraposition, 94  
Konversionsregel, 288  
Kopfrekursion, 260  
Kopfzelle, 281  
Korrekttheit, 92  
Korrespondenzproblem, 314, 406  
  binäres, 328  
  modifiziertes, 316

**L**  
Lambda-Kalkül, 288  
Lambda-Term, 288  
Landau-Symbole, 337, 401  
Las-Vegas-Algorithmus, 32  
Last-In-First-Out, 212  
Latch, 221  
Laufzeitfunktion, 347  
LBA-Problem  
  erstes, 302  
  zweites, 302  
Lebendigkeit  
  von Petri-Netzen, 229  
Leere Klausel, 91  
Leere Menge, 39  
Leerheitsproblem, 154, 401  
LIFO, 212  
Linear Time Logic, 142  
Lineare Rekursion, 260  
Lineare Suche, 373

Linearer Automat, 232  
Linksableitung, 157, 401  
Literal, 88, 401  
Logik, 77, 401  
  Aussagenlogik, 23, **78**, 390  
  dynamische, 283  
  höherer Stufe, 141, 401  
  Prädikatenlogik, 113, 406  
Logikminimierung, 91  
Logische Folgerung, 83  
Logische Programmierung, 134  
Logizismus, 16, 35  
Loop-Berechenbarkeit, 244  
Loop-Programm, 242, 401  
Loop-Sprache, 242, 402

## M

Mächtigkeit, 57, 402  
Makro, 245  
Marke, 226, 405  
Markenindex, 253  
Markierungsgleichung, 229  
Maschinenkomposition, 276  
Matrix, 118  
Maxterm, 88, 402  
Mealy-Automat, 193, **222**, 402  
Mehrband-Turing-Maschine, 274  
Mehrdeutigkeitsproblem, 402  
Mehrspur-Turing-Maschine, 274  
Menge, 38  
  disjunkte, 40  
  leere, 39  
  unentscheidbare, 307  
Mengenalgebra, 41  
Mengenlehre, 16  
  axiomatische, 39  
  Cantor'sche, 38  
  Fraenkel-, 39  
  Zermelo-Fraenkel-, 39  
Mengenoperation, 40  
Millenium-Probleme, 32  
Minimalform, 91  
  disjunktive, 91  
  konjunktive, 91  
Minimierung, 390  
Logik-, 91

von Akzeptoren, 196  
von Transduktoren, 219  
Minterm, 88, 402  
Miranda, 288  
ML, 288  
Modell, **80**, **117**, 402  
  Herbrand-, 122, 397  
Modellrelation, **80**, 115, 117  
Modus ponens, 17, **94**, 403  
Monte-Carlo-Algorithmus, 32  
Moore-Automat, 193, **222**, 403  
Moore-Nachbarschaft, 232

## N

Nachbarschaft  
  Moore-, 232  
  Von-Neumann-, 232  
Nachbarschaftsfunktion  
  von zellulären Automaten, 231  
Natürliche Zahl, 39, 51  
NEA, 199, 403  
Negation, 78  
Negationsnormalform, 118, 403  
Neutrales Element, 41  
NEXP, 353, 403  
Nichtdeterministischer Automat, 198  
Nichtterminal, 155  
Nonterminal, 155, 156  
Normalform, 88, 169  
  aussagenlogische, 87  
  Chomsky-, 169, 392  
  disjunktive, 89, 394  
  Greibach-, 187, 396  
  Huffman-, 222  
  Kleene'sche, **256**, 292, 399  
  konjunktive, 89, 400  
  Negations-, 118, 403  
  prädikatenlogische, 118  
NP, 347, 403  
NP-hart, 358, 404  
NP-vollständig, 31, **357**, 404  
NPSPACE, 352, 404

## O

O-Kalkül, 337

O-Notation, 337, 404

Obermenge, 40

ODER-Operator, 78

Ogdens Lemma, 175

Operator, 50, 54

Operatorenystem

vollständiges, 85

Orakel, 199, 351

Ordnung

lineare, 49

partielle, 49

totale, 49

Ordnungsrelation, 49

## P

P, 347, 404

P-NP-Problem, 358, 405

Paarungsfunktion, 60, 246, 404

Cantor'sche, 60, 72

Palindromsprache, 186, 214

Parikh-Vektor, 227, 404

Paritätsbit, 234

Paritätscode, 234

Partielle Funktion, 50, 246, 404

Partition, 43

Peano-Axiome, 51, 405

Petri-Netz, 226, 405

Pfad

geschlossener, 105

offener, 105

vollständiger, 106

widerspruchsfreier, 105

widersprüchlicher, 105

Phrasenstrukturgrammatik, 160

Pigeonhole principle, 86, 394

Polynom, 341

Polynomielle Reduktion, 357, 405

Pop-Operation, 212

Positionsspur, 275

Post'sche Tag-Maschine, 283

Post'sches Korrespondenzproblem, 314, 406

binäres, 328

modifiziertes, 316

Potenzmenge, 43

Potenzmengenautomat, 201, 406

Prädikat, 113

Prädikatenlogik, 113, 406

mit Gleichheit, 142

Normalformen, 118

Prämisse, 94

Pränex-Form, 118, 406

Primitiv-rekursive Funktion, 257, 406

Primitive Rekursion, 257, 406

Principia Mathematica, 17, 18

Problem

unentscheidbares, 307

Produktautomat, 209

Produktion, 156

Programm, 284

Goto-, 252, 396

Loop-, 242, 401

While-, 248, 414

Programmierung

deklarative, 134

dynamische, 176, 334, 394

logische, 134

Prolog, 407

PSPACE, 352, 407

Pumping-Lemma, 175, 407

für kontextfreie Sprachen, 172

für reguläre Sprachen, 164

Push-Operation, 212

## Q

Quantenrechner, 296

## R

Rabin und Scott

Satz von, 200, 410

Rad des Theodorus, 64

Random access machine, 284

Randomisierter Algorithmus, 32

Rationale Zahl, 52

Rechtsableitung, 157, 407

Rechtslineare Grammatik, 162

Reduktion, 407

polynomielle, 357, 405

Reduktionsbeweis, 313, 366

Reelle Zahl, 53

Regel, 35, 156

in Prolog, 134

Registermaschine, 284, 407

verallgemeinerte, 284

Reguläre Grammatik, 160, 162, 408

Reguläre Sprache, 162, 206, 408

Regulärer Ausdruck, 26, 166, 207, 408

Rekurrenzgleichung, 376

Rekursion, 64

$\mu$ -, 262

lineare, 260

primitive, 257, 406

verschachtelte, 260

verzweigende, 260

wechselseitige, 260

Rekursiv aufzählbar, 297

Rekursiv aufzählbare Sprache, 183, 297

Rekursive Definition, 64

Rekursive Sprache, 297

Relation, 43

Ableitungs-, 92

Äquivalenz-, 48

inverse, 46

Ordnungs-, 49

Relationenattribut, 44

Relationenprodukt, 46

Resolutionsbaum, 101

Resolutionskalkül, 408

aussagenlogisches, 101

prädikatenlogisches, 126

Resolutionsregel, 101

Resolvente, 101

Rice

Satz von, 310, 410

Robinson-Algorithmus, 127, 408

Rucksackproblem, 176, 330, 409

Russell'sche Antinomie, 17, 39, 409

## S

SAT, 409

Satz

von Cantor, 63, 409

von Cook, 359, 369, 409

von Herbrand, 122, 410

von Kleene, 252, 410

von Rabin und Scott, 200, 410

von Rice, 310, 410

- von Savitch, 353, 410  
**Savitch**  
 Satz von, 353, 410  
**Schaltnetz**, 221  
 Ausgabe-, 221  
 Übergangs-, 221  
**Schaltwerk**, 25, 221  
**Scheme**, 288  
**Schleife**  
 While-, 248  
**Schleifensatz**, 175  
**Schlussregel**, 410  
**Schnittmenge**, 40  
**Schubfachprinzip**, 86, 393  
**Selbstabbildung**, 50  
**Semantik**, 78, 410  
**Semi-Entscheidbarkeit**, 303, 410  
**Semi-Thue-System**, 161  
**Sicherheit**  
 von Petri-Netzen, 229  
**Sierpinski-Dreieck**, 233, 239  
**Skolem-Form**, 119, 411  
**Speicher**, 284  
**Speichervektor**, 243  
**Spezielles Halteproblem**, 327, 411  
**Sprache**  
 Diagonal-, 326  
 formale, 25, **154**, 395  
 Goto-, 252, 396  
 inhärent mehrdeutige, 159  
 kontextfreie, **169**, 214, 400  
 kontextsensitive, 181, 400  
 Loop-, 242, 402  
 Palindrom-, 186, 214  
 reguläre, **162**, 206, 408  
 rekursiv aufzählbare, 183, 297  
 rekursive, 297  
 unentscheidbare, 307  
 While-, 248, 414  
**Stack**, 212, 247  
**Stapel**, 212, 247  
**Startkonfiguration**, 233  
**Startsymbol**, 156  
**Startvariable**, 156  
**Startzustand**  
 von  $\epsilon$ -Automaten, 203  
 von DEAs, 194  
 von Kellerautomaten, 212  
 von NEAs, 199  
 von Transduktoren, 218  
 von Turing-Maschinen, 267  
**Stirling-Zahl**, 70  
**Strassen-Algorithmus**, 377  
**Strukturelle Induktion**, 67, 411  
**Substitution**, 117  
 Grund-, 117  
**Substitutionstheorem**, 85  
**Suche**  
 binäre, 373  
 lineare, 373  
**Surjektive Funktion**, 50  
**Syntax**, 78, 411  
**Syntaxbaum**, 159, 411  
**Synthese**  
 von Automaten, 221, 391, 410
- T**
- Tableau**  
 geschlossenes, 106  
 offenes, 106  
 vollständiges, 106  
 widerspruchsfreies, 106  
**Tableaukalkül**, 411  
 aussagenlogisches, 105  
 prädikatenlogisches, 131  
**Tag-Maschine**, 283  
**Tail recursion**, 260  
**Taubenschlagprinzip**, 86, 394  
**Tautologie**, 412  
 aussagenlogische, 81  
 prädikatenlogische, 117  
**Teile-und-herrsche-Prinzip**, 344  
**Teilformel**, 79  
**Teilmenge**, 40  
**Terminal**, 155  
**Terminalalphabet**, 156  
**Terminierungsmenge**, 249  
**Thue-System**, 161  
**Total Funktion**, 50, 412  
**Totalordnung**, 49  
**Trägermenge**, 40  
**Transduktor**, 193, **218**, 235, 297, 412  
 Minimierung, 219  
**Transistor**, 24
- Turing-Akzeptor**, 297  
**Turing-Berechenbarkeit**, 269, 412  
**Turing-Maschine**, 20, **265**, 412  
 akzeptierende, 297  
 Einband-, 265  
 einseitig beschränkte, 273  
 Komposition, 276  
 linear beschränkte, 273  
 Mehrband-, 274  
 Mehrspur-, 274  
 universelle, 277, 414  
 zelluläre, 281  
**Turing-Test**, 267
- U**
- Überabzählbarkeit**, 58, 413  
**Übergangsfunktion**, 243  
**Übergangsrelation**, 298  
**Übergangsschaltnetz**, 221  
**Übersetzender Automat**, 193, 218  
**Umkehrabbildung**, 50  
**Unäre Codierung**, 270  
**Unberechenbarkeit**, 307, 413  
**UND-Operator**, 78  
**Unendlichkeit**, 56  
**Unentscheidbarkeit**, 307, 413  
**Unerfüllbarkeit**, 81, 413  
**Unifikation**, 126, 413  
**Unifikator**, 126, 413  
 allgemeinster, 127, 390  
**Universalmenge**, 40  
**Universelle Turing-Maschine**, 277, 414  
**Universum**, 116  
 Herbrand-, 121, 397  
**Unmittelbare Adressierung**, 284  
**Untermenge**, 40  
**Up-Arrow-Notation**, 55, 414  
**Urbild**, 50
- V**
- Variable**, 78, 156  
**Venn-Diagramm**, 40, 41  
**Vereinigungsmenge**, 40  
**Verklemmungsfreiheit**  
 von Petri-Netzen, 230

Verschachtelte Rekursion, 260

Verzweigende Rekursion, 260

Vollständige Formelmenge, 96

Vollständige Induktion, 43, **65**, 414

Vollständiges Operatorensystem, 85

Vollständigkeit, 18, 92

Von-Neumann-Nachbarschaft, 232

## W

Wahrheitstabelle, 81

Wahrheitstafel, 81

Wechselseitige Rekursion, 260

While-Berechenbarkeit, 249

While-Programm, 248, 414

While-Schleife, 248

While-Sprache, 248, 414

Widerspruchsbeweis, 65

Widerspruchsfreiheit, 19

Widerspruchskalkül, 93, 414

Wort, 154

Wortproblem, 154, 415

Wurzelschnecke, 64

## X

XOR-Operator, 79

## Z

Z3, 22

Zahl

ganze, 39, 52

große, 54

irrationale, 53

natürliche, 39, 51

nichtnegative, 39

positive, 39

rationale, 52

reelle, 53

Zeichen, 154

Zelle, 231

Zellmenge, 231

Zelluläre Turing-Maschine, 281

Zellulärer Automat, **231**, 239, 415

Zentraleinheit, 284

Zermelo-Fraenkel-Mengenlehre, 39

Zermelo-Mengenlehre, 39

Zielmenge, 49

Zustand, 192

äquivalenter, 196

Zustandsband, 280

Zustandsmenge

von  $\varepsilon$ -Automaten, 203

von DEAs, 194

von Kellerautomaten, 212

von NEAs, 199

von Transduktoren, 218

von Turing-Maschinen, 267

von zellulären Automaten, 231

Zustandsübergangsdiagramm, 192

Zustandsübergangsfunktion

von  $\varepsilon$ -Automaten, 203

von DEAs, 194

von Kellerautomaten, 212

von NEAs, 199

von Transduktoren, 218

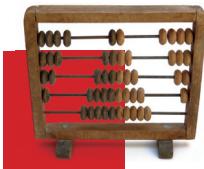
von Turing-Maschinen, 267

von zellulären Automaten, 231



#### DIE NEUE LEHRBUCHGENERATION //

- Für das Bachelor-Studium geeignet.
- Umfassende verständliche Einführung in die wichtigsten Teilgebiete.
- Grundlegende Konzepte, Methoden und Ergebnisse.
- Zahlreiche Beispiele und Übungsaufgaben.



**THEORETISCHE INFORMATIK //** Das Buch führt umfassend in das Gebiet der theoretischen Informatik ein und behandelt den Stoffumfang, der für das Bachelor-Studium an Universitäten und Fachhochschulen in den Fächern Informatik und Informationstechnik benötigt wird. Die Darstellung und das didaktische Konzept verfolgen das Ziel, einen durchweg praxisnahen Zugang zu den mitunter sehr theoretisch geprägten Themen zu schaffen. Theoretische Informatik muss nicht trocken sein. Sie kann Spaß machen und genau dies versucht das Buch zu vermitteln. Die verschiedenen Methoden und Verfahren werden anhand konkreter Beispiele eingeführt und durch zahlreiche Querverbindungen wird gezeigt, wie die fundamentalen Ergebnisse der theoretischen Informatik die moderne Informationstechnologie prägen.

Das Buch behandelt die Themengebiete: Logik und Deduktion, Automatentheorie, formale Sprachen, Entscheidbarkeitstheorie, Berechenbarkeitstheorie und Komplexitätstheorie. Die Lehrinhalte aller Kapitel werden durch zahlreiche Übungsaufgaben komplettiert, so dass sich die Lektüre neben der Verwendung als studienbegleitendes Lehrbuch auch bestens zum Selbststudium eignet.

**DAS EXTRA ZUM BUCH //** Die Lösungen zu den Übungsaufgaben, eine Linkssammlung sowie weiterführende Informationen bieten einen vielfältigen Zusatznutzen und stehen im Internet zur Verfügung: <http://www.dirkwhoffmann.de/TH>

**Prof. Dr. Dirk W. HOFFMANN** betreut die Lehrgebiete Technische Informatik, Embedded Software und Multimedia-Technik an der Fakultät für Informatik der Hochschule Karlsruhe.

HANSER

[www.hanser.de/computer](http://www.hanser.de/computer)

ISBN 978-3-446-41511-9

Studenten der Informatik  
und Informationstechnik

Systemvoraussetzungen für eBook-inside: Internet-Verbindung, Adobe Reader/Acrobat v6.0 oder höher für Windows (ab WIN98SE) oder MAC OS X. Am besten gleich online registrieren.