

René Krooß

ALGORITHMEN UND DATEN- STRUKTUREN

Praktische Übungen für die
Vorlesungen und Praktika



Quellcode zum Buch unter:
plus.hanser-fachbuch.de

HANSER



Ihr Plus – digitale Zusatzinhalte!

Auf unserem Download-Portal finden Sie zu diesem Titel kostenloses Zusatzmaterial.

Geben Sie auf **plus.hanser-fachbuch.de** einfach diesen Code ein:

plus-35ipn-en7sk



Bleiben Sie auf dem Laufenden!

Unser **Computerbuch-Newsletter** informiert Sie monatlich über neue Bücher und Termine. Profitieren Sie auch von Gewinnspielen und exklusiven Leseproben. Gleich anmelden unter:

www.hanser-fachbuch.de/newsletter



René Krooß

Algorithmen und Datenstrukturen

Praktische Übungen
für die Vorlesungen und Praktika

HANSER

Alle in diesem Buch enthaltenen Informationen, Verfahren und Darstellungen wurden nach bestem Wissen zusammengestellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund sind die im vorliegenden Buch enthaltenen Informationen mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor und Verlag übernehmen infolgedessen keine juristische Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieser Informationen – oder Teilen davon – entsteht.

Ebenso übernehmen Autor und Verlag keine Gewähr dafür, dass beschriebene Verfahren usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Buch berechtigt deshalb 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 – reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© 2022 Carl Hanser Verlag München, www.hanser-fachbuch.de

Lektorat: Brigitte Bauer-Schieweck

Copy editing: Petra Kienle, Früstenfeldbruck

Umschlagdesign: Marc Müller-Bremer, München, www.rebranding.de

Umschlagrealisation: Max Kostopoulos

Titelmotiv: © stock.adobe.com/AlexanderLimbach

Satz: Eberl & Koesel Studio, Altusried-Krugzell

Druck und Bindung: Eberl & Koesel GmbH, Altusried-Krugzell

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

Printed in Germany

Print-ISBN: 978-3-446-47222-8

E-Book-ISBN: 978-3-446-47241-9

E-Pub-ISBN: 978-3-446-47303-4

Inhalt

Vorwort	IX
Teil I: Grundlagen	1
1 Einführung	3
1.1 Berechenbarkeit von Algorithmen	4
1.2 Wie eine Turing-Maschine arbeitet	5
1.2.1 Beispiel 1: Addition zweier Zahlen mit einer Turing-Maschine	6
1.2.2 Beispiel 2: Suchen und ersetzen	8
1.2.3 Beispiel 3: Multiplikation zweier Zahlen mit einer erweiterten Turing-Maschine	10
1.2.4 Von der Turing-Maschine zum Prozessor	13
1.3 Laufzeitanalyse von Algorithmen	14
1.3.1 Das P-NP-Problem	16
1.4 Laufzeitabschätzungen von C-Programmen	17
1.5 Übungen	21
2 Basisalgorithmen	23
2.1 Der Ringtausch	24
2.2 Einfache Textsuche	28
2.3 Einfaches Suchen und Ersetzen	33
2.3.1 Entfernen eines Textes aus einer Zeichenkette	33
2.3.2 Einfügen von Freiräumen in den Text	34
2.3.3 Ein vollständiges Programm zum Suchen und Ersetzen	35
2.4 Einfaches Sortieren von Zahlen	38
2.4.1 Bubble Sort	39
2.4.2 Einfaches, sortiertes Einfügen	43
2.5 Primfaktorzerlegung	47
2.5.1 Wann ist eine Zahl eine Primzahl?	47
2.5.2 Die Primfaktorzerlegung – das Programm „Primteiler“	49
2.6 Berechnung des GGT (größter gemeinsamer Teiler)	53

2.7	Gezielte Suche nach Primzahlen	56
2.7.1	Das Sieb des Eratosthenes	56
2.8	Rechnen mit beliebig langen Zahlen	59
2.8.1	Addition beliebig langer Zahlen	59
2.8.2	Subtraktion beliebig langer Zahlen	64
2.8.3	Multiplikation beliebig langer Zahlen (Ägyptische Multiplikation) ...	68
2.8.4	Division beliebig langer Zahlen (Ägyptische Division)	71
2.9	Übungen	83
3	Rekursive Algorithmen	85
3.1	Der Prozessorstapel (Stack)	85
3.2	Was sind Rekursionen und wozu werden sie benötigt?	87
3.3	Beispielprogramme zur Rekursion	87
3.3.1	Berechnung der Fakultät	88
3.3.2	Berechnung von Fibonacci-Zahlen	90
3.3.3	Das Erstellen von Galois-Feldern	92
3.3.4	Die Türme von Hanoi	95
3.3.5	Ein Backtracking-Algorithmus	98
3.3.6	Ein einfacher Taschenrechner	104
3.4	Wann Rekursion und wann lieber nicht?	113
3.5	Übungen	114
	Teil II: Fortgeschrittene Themen	115
4	Verkettete Listen	117
4.1	Die Erstellung verketteter Listen	117
4.1.1	Einfach verkettete Listen	118
4.1.2	Doppelt verkettete Listen	127
4.2	Blockchains und Listen mit beliebigen Objekten	138
4.2.1	Blockchains	138
4.2.2	Listen mit beliebigen Objekttypen	151
4.3	Listen mit Java erstellen	166
4.3.1	Erstellen von Java-Listen mit LinkedList	167
4.3.2	Erstellen von Java-Listen mit Vector	171
4.3.3	Wann LinkedList und wann Vector?	172
4.4	Übungen	173
5	Bäume	175
5.1	Allgemeine Bäume	176
5.1.1	Einfach strukturierte allgemeine Bäume	176
5.1.2	Allgemeine Bäume mit beliebigen Objekten	188
5.2	Binärbäume	202
5.3	Bäume in Java	213
5.4	Übungen	218

6	Such- und Sortierverfahren	219
6.1	Wichtige effiziente Sortierverfahren	220
6.1.1	Min-Max-Sort	220
6.1.2	Mergesort	225
6.1.3	Quicksort	231
6.1.4	Treesort	238
6.1.5	Heapsort	241
6.2	Effiziente Suchalgorithmen	250
6.2.1	Der KMP-Algorithmus	250
6.2.2	Threadsearch	257
6.3	Übungen	264
Teil III: Weiterführende Themen		265
7	Signalverarbeitung	267
7.1	Was ist ein Signal?	267
7.1.1	Korrektes Messen von Signalen	268
7.2	Generierung digitaler Signale	272
7.2.1	Das Rechtecksignal	273
7.2.2	Das Sägezahnsignal	276
7.2.3	Das Dreiecksignal	278
7.2.4	Das weiße Rauschen	280
7.2.5	Das Sinussignal	283
7.2.6	Zeitveränderliche diskrete Signale	285
7.3	Filteralgorithmen	289
7.3.1	Der Pop-Klick-Filter	290
7.3.2	Der Distortion-Filter	293
7.3.3	Der EMA-Filter	295
7.3.4	Diskrete Fourier-Transformation (DFT)	299
7.4	Übungen	303
8	Grafische Bildverarbeitung	305
8.1	Der Medianfilter	305
8.2	Binärfilter	321
8.3	Lineares Filtern mit Filtermasken	324
8.4	Chroma Keying	329
8.5	Übungen	332
9	Simulation neuronaler Netze	333
9.1	Zeichenerkennung mit neuronalen Netzen	334
9.2	Spracherkennung	347

10	Kryptographische Algorithmen	357
10.1	Historische Chiffren	357
10.1.1	Die Caesar-Chiffre	358
10.1.2	Die Vigenère-Verschlüsselung	363
10.1.3	Die Enigma	366
10.2	Sichere Schlüsselübertragung	375
10.2.1	Verwenden der Modulo-Operation	375
10.2.2	Verwenden des RSA-Algorithmus	382
10.3	Blockchiffren	395
10.4	Hashing-Verfahren	412
10.4.1	Erweitertes XOR-Hashing	412
10.4.2	Der SHA-Algorithmus	422
10.5	Erzeugen sicherer Pseudo-Zufallszahlen	429
10.6	Übertragen von Nachrichten durch Quantenkryptographie	432
11	Graphen	435
11.1	Darstellung eines Graphen als Adjazenzmatrix	437
11.2	Darstellung eines Graphen als verallgemeinerte Baumstruktur	446
11.3	Eulerkreise	455
11.4	Petri-Netze	462
11.4.1	Prozess-Synchronisation	462
11.4.2	Das Erzeuger-Verbraucher-Problem	465
11.4.3	Das Philosophenproblem von Dijkstra	467
11.4.4	Simulation von Petri-Netzen mit Inzidenzmatrizen	481
11.5	Übungen	491
	Anhang: Lösung der Übungsaufgaben	493
	Anhang zu Kapitel 1 „Einführung“	493
	Anhang zu Kapitel 2 „Basialgorithmen“	498
	Anhang zu Kapitel 3 „Rekursive Algorithmen“	500
	Anhang zu Kapitel 4 „Verkettete Listen“	502
	Anhang zu Kapitel 5 „Bäume“	504
	Anhang zu Kapitel 6 „Such- und Sortierverfahren“	506
	Anhang zu Kapitel 7 „Signalverarbeitung“	507
	Anhang zu Kapitel 8 „Grafische Bildverarbeitung“	510
	Anhang zu Kapitel 11 „Graphen“	512
	Index	515

Vorwort

Bücher über Algorithmen gibt es mittlerweile viele und natürlich gibt es noch viel mehr Projekte, die komplexe Algorithmen verwenden. Warum muss es dann noch ein weiteres Buch über Algorithmen geben? Die Antwort ist, dass bei der Flut an Büchern, die es zum Thema Algorithmen mittlerweile gibt, das Thema Studium oft außen vor bleibt. In diesem Buch geht es deshalb um die Frage, welche Algorithmen speziell für das Studium wichtig sind und welche nicht. Eine zweite wichtige Frage ist natürlich auch die, ob Sie einen einfachen Einstieg in das komplexe Thema Algorithmen und Datenstrukturen finden können, der Ihnen im Studium weiterhilft. Die Antwort ist: Ja, auf jeden Fall, und das mit einem vertretbaren Aufwand. Die Frage, warum Sie sich gerade für dieses Buch entscheiden sollten, ist hiermit beantwortet: Bei den meisten Büchern über Algorithmen und Datenstrukturen, die zumindest ich selbst verwenden musste, steigt die Lernkurve oft schon am Anfang steil an. Auch wird oft Programmcode mit komplexen mathematischen Abhandlungen und Beweisen vermischt und dadurch kommt die Programmierpraxis zu kurz. Ich dagegen möchte den Schwerpunkt auf die Praxis legen und Ihnen Programmcode vorstellen, der sozusagen out of the box lauffähig ist. Dabei fange ich ganz einfach an und erkläre zunächst einmal, wie Sie zwei Werte miteinander vertauschen oder Zahlen sortiert in ein Array einfügen können. Ich möchte an dieser Stelle aber nicht an Bücher wie „Algorithmen und Datenstrukturen für Dummies“ anknüpfen, die die meisten Dinge im Comic- oder Pseudocode-Stil erklären. Ich möchte schon ein oder zwei Stufen höher ansetzen und Ihnen ausführbaren Quellcode zeigen. Von mir aus können Sie sogar „Algorithmen und Datenstrukturen für Dummies“ parallel zu diesem Buch lesen, oder – falls Sie dieses Buch schon gelesen haben – gleich mit diesem Buch weitermachen. Sie haben in diesem Fall quasi Level 1 und 2 schon geschafft und können sich nun Level 3 vornehmen. Ich denke, 10 000 Erfahrungspunkte könnte ich Ihnen als Dungeon-Master schon für die Dummies anschreiben.

Ich will mit dem letzten Absatz keinesfalls ausdrücken, dass all die Bücher, die Sie in Ihrem Studium durcharbeiten müssen, überflüssig sind. Wenn Sie aber vorher gelernt haben, wie Sie so einfache Dinge wie den größten gemeinsamen Teiler oder die Primfaktoren einer natürlichen Zahl berechnen können, dann können Sie später auch komplexe mathematische Verfahren in ein laufendes Programm umsetzen. Grundlegende Kenntnisse in der Programmierung möchte ich natürlich voraussetzen, Erfahrungen mit der Programmiersprache C oder Java sind an dieser Stelle von Vorteil. Dies heißt natürlich nicht, dass ich Sie mit allernhand unverständlichen, komplexen Klassendiagrammen aus der objektorientierten Ent-

wicklung bombardiere, die nur ein Profi verstehen kann. Obwohl ich dies durchaus könnte, möchte ich versuchen, die Programmierung und auch die Mathematik, die hinter vielen Algorithmen steckt, möglichst leicht verdaulich zu präsentieren.

Kommen wir nun zum Aufbau dieses Buchs. Die einzelnen Kapitel sind jeweils ähnlich gegliedert. Zuerst erfolgt eine kurze Einleitung, worum es geht, und dann schließt sich, falls erforderlich, eine Beschreibung der eventuell erforderlichen Programmier Techniken an. Wenn es mathematische Grundlagen gibt, werden die entsprechenden Funktionen erläutert und auch, welche Variablen diese Funktionen verwenden. Ich habe besonders darauf geachtet, dass Sie zu jedem Algorithmus mindestens ein Listing vorfinden, das anschließend ausführlich erklärt wird. In den Kapiteln selbst finden sich oft verschiedene Tipps und Hinweise, die auch durch spezielle Kästchen mit der Überschrift „Hinweis“ gekennzeichnet sind. Ich empfehle Ihnen, die Hinweise ernst zu nehmen, denn so erleichtern Sie sich das Leben.

Ich empfehle Ihnen auch, auf die in den Kapiteln angegebenen Webseiten oder weiterführenden Links zu gehen, denn auch dort erhalten Sie wertvolle Informationen. Online stehen Ihnen außerdem alle Quellcodes zum Buch zur Verfügung. Auf dieser Website des Hanser-Verlags

<https://plus.hanser-fachbuch.de/>

geben Sie folgenden Zugangscode ein:

`plus-35ipn-en7sk`

Kommen wir nun zur verwendeten Programmiersprache. Sämtliche Programme in diesem Buch sind in C, C++ oder Java geschrieben. Dies sind die Programmiersprachen, die auch im Studium verwendet werden. Natürlich können Sie diese Programme nicht auf e-Book-Readern wie z. B. dem Tolino ausführen, obwohl diese unter Umständen sogar angezeigt werden, wenn Sie auf den entsprechenden Link klicken. Bei Tablets mag sich die Sache anders verhalten, weil dort zumindest Java manchmal vorinstalliert ist. Am Ende jedes Kapitels befindet sich eine Rubrik mit Übungen, die Sie möglichst alle bearbeiten sollten. Dies hat den einfachen Grund, dass die Übungen an den Praktika und Klausuren orientiert sind, deshalb können ähnliche Aufgaben durchaus auch in den Prüfungen vorkommen.

Nun möchte ich noch ein paar Worte über die Gliederung dieses Buchs verlieren. In den ersten Kapiteln des Buchs lernen Sie alle Grundlagen in Bezug auf Algorithmen kennen. Sie lernen, was ein Algorithmus ist, wie und ob man entscheiden kann, ob ein bestimmtes mathematisches Problem überhaupt berechenbar ist, und welche grundlegenden (und einfachen) Algorithmen es gibt. An dieser Stelle lernen Sie z. B., wie Sie die Werte zweier Variablen vertauschen können, wie Sie den GGT zweier Zahlen berechnen, wie Sie eine Zahl in ihre Primfaktoren zerlegen oder wie Sie mit nur wenigen Programmzeilen ein einfaches Such- oder Sortierverfahren implementieren können. Auch der Umgang mit beliebig langen Zahlen wird hier erklärt. So erfahren Sie z. B., wie Sie mit Hilfe der ägyptischen Division beliebig lange Zahlen durcheinander dividieren können.

Im zweiten Teil (ab dem 4. Kapitel) werden die fortgeschrittenen Themen behandelt, die direkt auf dem ersten Teil aufbauen. Hier geht es um Dinge, die im Studium wichtig sind und die auch in den Vorlesungen und Praktika immer wieder vorkommen. Dies sind z. B. verkettete Listen, schnelle Sortierverfahren, effektive Mustersuche in Texten und Bäume.

Ab Kapitel 7 behandelt der dritte Teil spezielle Themen, die unter Umständen in Wahlpflichtfächern vorkommen und so nicht unbedingt in den zweiten Teil gehören. Dies umfasst z. B. die grafische Bildverarbeitung, die Signalverarbeitung oder spezielle Algorithmen für neuronale Netze. Viele Algorithmen im letzten Teil werden Sie wahrscheinlich niemals verwenden, denn vor allem die Wahlpflichtfächer sind oft eine Sache des Geschmacks und der eigenen Vorlieben. Ich habe versucht, möglichst viele wichtige Themenbereiche abzudecken, kann aber auch nicht ausschließen, dass die eine oder andere Sache fehlt. So gibt es z. B. über hundert Sortierverfahren und ebenso viele Suchalgorithmen. Auch über reguläre Ausdrücke, die in diesem Buch nicht enthalten sind, gibt es inzwischen mehrere gute Bücher, die ich einfach nicht nochmal schreiben möchte.

Nun wünsche ich Ihnen viel Spaß mit diesem Buch. Sollten während des Lesens Unklarheiten oder Fragen aufkommen, so scheuen Sie sich nicht, mir eine E-Mail zu schicken:

renekrooss@t-online.de

Ich freue mich über ein Feedback von Ihnen.

René Krooß



René Krooß ist Diplom-Informatiker, Programmierer und Experte für Computer-Hardware, Videoverarbeitung und 3D-Rendering. Seine Hobbys sind Elektronik, Modellbau und Retro-Computing.

Teil I: Grundlagen



- Kapitel 1: Einführung
- Kapitel 2: Basisalgorithmen
- Kapitel 3: Rekursive Algorithmen

1

Einführung

„Was genau ist ein Algorithmus?“ Auf diese Frage müssen wir zuerst eine Antwort finden, wenn wir uns weiter mit dem Thema beschäftigen wollen – sonst ist alles weitere Vorgehen sinnlos. Die Antwort ist aber eigentlich nicht so schwer zu finden, denn was ein Algorithmus ist, ist streng definiert. Die Definition lautet in etwa wie folgt:



Definition Algorithmus

Ein Algorithmus ist eine streng formale, ausführbare Rechenvorschrift, die in einer überschaubaren Zeit für eine bestimmte Ausgangsbedingung (z. B. in Form einer Zahl) ein reproduzierbares Ergebnis liefert. Hierbei ist es zulässig, dass einzelne Rechenschritte mehrmals wiederholt werden.

Ähnliche Definitionen gibt es zuhauf in zahlreichen Lehrbüchern, manchmal sind sie länger, manchmal kürzer. Ich habe eine möglichst kurze Fassung gewählt, weil es mir auf *die Essenz* ankommt. Außerdem möchte ich von Anfang an Missverständnissen vorbeugen, denn oft werden Algorithmen mit Dingen verglichen, die sie gewiss nicht sind. Einige Lehrbücher vergleichen z. B. Algorithmen mit Kochrezepten, bei deren strikter Einhaltung ein reproduzierbares Gericht herauskommt. Leider ist bei einem Kochrezept schon die Reproduzierbarkeit nicht gegeben, denn jeder Koch kocht anders. Bei dem einem Italiener ist z. B. die Tomatensauce sämiger, bei dem anderen Italiener ist sie schärfer. Außerdem enthalten Kochrezepte Anweisungen, wie „eine Prise Salz“ hinzuzugeben oder das Gericht „auf kleiner Stufe“ zu garen. Keine dieser Anweisungen ist exakt ausführbar. Aber selbst eine Anweisung wie „1,534 Gramm Salz hinzufügen“ oder „bei 102,885 Grad 582,35 Sekunden lang garen“ beachtet noch nicht, dass jeder Herd anders ist und dass Wasser bei hohem Luftdruck später kocht als bei niedrigem Luftdruck. Ein klassisches Kochrezept ist also weit davon entfernt, ein Algorithmus zu sein, weshalb Algorithmen auch eher im mathematischen Bereich angesiedelt sind. Dort und nur dort sind streng formale, ausführbare Vorschriften mit einer genau festgelegten Ausgangsbedingung und reproduzierbarem Ergebnis denkbar. Ein gutes erstes Beispiel für einen Algorithmus ist die schriftliche Division zweier Dezimalzahlen a und b . Wenn Sie für $a = 12$ und für $b = 5$ einsetzen, dann erhalten Sie als Ergebnis stets 2,4 – egal wie oft Sie (natürlich in korrekter Weise) nachrechnen.

Kommen wir nun zum letzten Punkt, nämlich zu der Aussage, dass ein Algorithmus „in einer überschaubaren Zeit“ ein Ergebnis liefern muss. Für die Division von 12 durch 5 tut

die schriftliche Division genau dies: Sie kommt in nur wenigen Schritten zu einem korrekten Ergebnis. Leider ändert sich die Sache schon dramatisch, wenn Sie z. B. 10 durch 3 teilen: Ab dem dritten Schritt wiederholen sich die Ziffern endlos und Sie bekommen 3,3333 ... heraus, ohne jemals den Rest 0 zu erhalten. Ihr Algorithmus endet also nicht in einer überschaubaren Zeit, wenn Sie keine zusätzliche Abbruchbedingung einfügen. Die Abbruchbedingung, die Sie wahrscheinlich schon aus der Schule kennen, ist die Perioden-Schreibweise. Sobald sich ein Rechenschritt wiederholt, wird der Algorithmus abgebrochen und man gibt eine Periode an.

■ 1.1 Berechenbarkeit von Algorithmen

Ein großes (und wahrscheinlich das größte) Problem von Algorithmen ist also zu entscheiden, ob diese berechenbar sind. „Berechenbar“ im mathematischen Sinne heißt, dass ein Algorithmus in einer endlichen Anzahl von Schritten anhält und dann auch ein korrektes Ergebnis liefert. Leider ist die Aussage, dass ein bestimmtes mathematisches Problem berechenbar ist, erst bewiesen, wenn es einen Algorithmus für dieses Problem gibt, der für jede mögliche Eingabe (z. B. in Form einer Zahl) stets in einer endlichen Anzahl von Schritten ein korrektes Ergebnis liefert. Genau dieser Beweis ist sehr schwierig und kann oft nur mit einem mathematischen Beweisverfahren wie der vollständigen Induktion erbracht werden. Man kann also innerhalb der Mathematik bestimmte Aussagen beweisen, aber eben nicht alle. So gibt es z. B. keinen perfekten Algorithmus, der mir innerhalb einiger Sekunden für eine beliebig lange Zahl sagt, ob diese eine Primzahl ist, und dieser Algorithmus kann wahrscheinlich auch überhaupt nicht gefunden werden. Weil die Sache mit der Berechenbarkeit in der Mathematik nicht so einfach ist, hat man sie in späteren Definitionen von Algorithmen abgeschwächt – sie ist nun für ein Berechnungsverfahren, das ein Algorithmus „sein möchte“, nicht mehr unbedingt nötig, sondern nur noch wünschenswert.

Trotzdem ist die Frage nach der Berechenbarkeit mathematischer Probleme an dieser Stelle immer noch nicht ganz beantwortet. Gibt es zumindest ernstzunehmende Versuche, um herauszufinden, wie wir feststellen können, ob eine bestimmte Fragestellung in einer endlichen bzw. vernünftigen Zeit beantwortbar ist? Leider ist es so, dass wir diese Frage bis jetzt nicht beantworten können. In der Vergangenheit, vor allem in den 20er-Jahren des letzten Jahrhunderts, gab es viele Ansätze und Vorschläge aus der Gruppentheorie, die aber spätestens aufgegeben wurden, als der Mathematiker Kurt Gödel seinen Unvollständigkeitssatz aufstellte. Der Unvollständigkeitssatz besagt Folgendes: In jedem mathematischen Axiomensystem (dies ist quasi eine Sammlung von Regeln, die für eine bestimmte Zahlengruppe wie z. B. die natürlichen Zahlen gilt) gibt es immer Annahmen, die weder beweisbar noch widerlegbar sind. D. h. natürlich auch, dass es immer Algorithmen gibt, von denen man nicht sagen kann, ob sie in einer endlichen Anzahl von Schritten ein Ergebnis liefern. Dennoch gibt es einige populäre Ansätze, um herauszufinden, ob ein bestimmter Algorithmus zumindest nachvollziehbare Ergebnisse liefert. Einer der populäreren Ansätze, den man auch immer im Studium kennenlernt, ist das verwenden einer Turing-Maschine. Auf den folgenden Seiten werden Sie nun an Beispielen erfahren, wie eine Turing-Maschine arbeitet.

■ 1.2 Wie eine Turing-Maschine arbeitet

In seinem berühmten Werk „On computable numbers“ (über berechenbare Zahlen) entwickelte Alan Turing ein Modell, mit dem man feststellen kann, ob ein mathematisches Problem berechenbar ist. Dieses Modell ist die später nach ihm benannte Turing-Maschine. Die Turing-Maschine ist so konstruiert, dass sie immer dann anhält, wenn ein mathematisches Problem berechenbar ist.

Eine Turing-Maschine wird oft in Form einer Eingabeeinheit dargestellt, in die ein unendlich langes Band hineinführt. Dieses Band, das Eingabeband, führt im einfachsten Fall auch direkt wieder aus der Maschine heraus und ist so auch gleichzeitig das Ausgabeband. Auf dem Band können nun – auch schon am Anfang – Symbole stehen. Diese Symbole sind beliebig wählbar, in den meisten Einführungsbeispielen in Bezug auf Turing-Maschinen sind dies aber fast immer Punkte und Striche, Nullen und Einsen oder Zahlen und Buchstaben. Wird die Turing-Maschine nun gestartet (dies kann z. B. durch einen Startknopf oder Hebel geschehen), liest sie zuerst das Symbol ein, über dem sich der Lesekopf zurzeit befindet. Je nachdem, welches Symbol sich nun gerade unter dem Lesekopf befindet, und je nachdem, in welchem Zustand sich die Maschine aktuell befindet, wird eine entsprechende Aktion ausgeführt. Diese Aktion ist meistens eine Ersetzung des Symbols, das sich unter dem Lesekopf befindet, durch ein anderes Symbol und ein anschließendes Verschieben des Bands nach rechts oder links. Natürlich kann der Ersetzungsschritt auch entfallen. Nach Ausführen einer Aktion wechselt die Maschine dann in einen anderen Zustand. Welcher Zustand dies ist, entnimmt die Maschine einer internen Tabelle. Gleichzeitig zu den Zustandswechseln können in der internen Tabelle auch noch zusätzliche Kommandos stehen, die z. B. das Band anhalten, wenn ein bestimmter Endzustand erreicht wird.

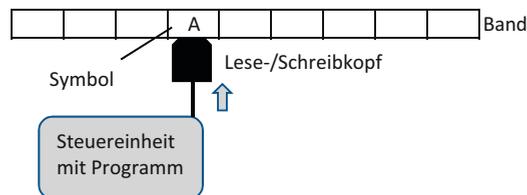


Bild 1.1 Arbeitsweise einer Turing-Maschine

Wie Sie in Bild 1.1 sehen können, hat das Eingabeband kein Ende und keinen Anfang. Ferner sind die Programme, die die Steuereinheit ausführt, fest verdrahtet. Weil die Turing-Maschine so ähnlich arbeitet wie ein sehr einfacher Computer, wird sie auch im Studium immer irgendwann besprochen. Meistens geschieht dies schon in den Vorlesungen zu den Grundlagen der Informatik, also in den ersten zwei Semestern. Deswegen habe auch ich die Turing-Maschine und die grundlegenden Überlegungen zur Berechenbarkeit mathematischer Probleme an den Anfang dieses Buchs gestellt. Die Betonung liegt hier auf „grundlegend“, ich werde also einige einfache Beispiele zu Turing-Maschinen anführen. Die ganzen komplexen mathematischen Formeln aus der Gruppentheorie, die Turing selbst verwendete, um sein Modell zu definieren, werde ich Ihnen natürlich ersparen.



Hinweise für Linux und den Raspberry Pi

Ich habe durchgehend dafür gesorgt, dass sämtliche Listings und Programme in diesem Buch sowohl unter Windows 10 als auch unter Linux ausführbar sind. Dies gilt auch für den inzwischen sehr populären Raspberry Pi – sämtliche Listings sind auf dem Pi übersetzbar, auch die Java-Beispiele. Wenn Sie auf dem Pi bestimmte Dinge beachten müssen, wird dies durch separate Kästchen mit dem Titel „Hinweise für den Raspberry Pi“ angezeigt.

1.2.1 Beispiel 1: Addition zweier Zahlen mit einer Turing-Maschine

Sie kennen wahrscheinlich die Binär-Schreibweise von Zahlen und wissen bereits, dass die Zahl 2 im Computer als „10“ abgebildet wird. Für die Addition von zwei Zahlen durch eine Turing-Maschine möchte ich aber eine noch einfachere Schreibweise mit Nullen und Einsen verwenden, nämlich die längencodierte Darstellung, die auch schon die ENIAC verwendete. Die ENIAC war der erste wirklich funktionierende Computer, den die Amerikaner entwickelt haben. Längencodierte Zahlendarstellung bedeutet nichts anderes, als eine Zahl in der entsprechenden Anzahl von Einsen darzustellen. Wenn Sie also in diesem Beispiel die Zahl 5 darstellen wollen, dann schreiben Sie „111110“. Dies sind fünf Einsen gefolgt von einer 0, die den Abschluss einer Zahl angibt. In diesem Beispiel müssen Sie also zwei Zahlen durch genau eine Null getrennt hintereinanderschreiben, die Trennung von Zahlen durch mehr als eine Null sei hier nicht erlaubt.

Kommen wir nun zu unserem ersten Beispiel, in dem die Zahlen 5 und 7 addiert werden sollen. Diese müssen Sie zuerst in folgender Form auf das Band schreiben:

11111011111110

In den folgenden Beispielen wird angenommen, dass ein Buchstabe im Text genau ein Symbol auf dem Band der Turingmaschine abbildet und dass sich der Lesekopf über dem ersten, linken Symbol im Text befindet. Nehmen wir nun an, dass die Turing-Maschine in diesem Beispiel einen Starthebel besitzt, den Sie zuerst umlegen müssen, um die Maschine in Gang zu setzen. Nehmen wir weiter an, dass Sie die Möglichkeit haben, das Band vorher korrekt einzulegen, und so den Lesekopf gezielt auf der ersten Eins (also ganz links) platzieren können. Ferner nehmen wir an, dass die Maschine immer zuerst Zustand Nr. 0 (den Initialisierungszustand) annimmt. Um zwei Zahlen zu addieren, müssen Sie nun folgende Regeln aufstellen:

- Wenn sich die Maschine in Zustand 0 befindet und das Symbol unter dem Lesekopf 1 ist, verschiebe das Band um eine Position nach links (dies ist quasi dasselbe, als ob der Lesekopf nach rechts wandert).
- Wenn sich die Maschine in Zustand 0 befindet und das Symbol unter dem Lesekopf 0 ist, so drucke das Symbol 1, verschiebe das Band um eine Position nach links und wechsele zu Zustand 1.
- Wenn sich die Maschine in Zustand 1 befindet und das Symbol unter dem Lesekopf 1 ist, verschiebe das Band um eine Position nach links.

- Wenn sich die Maschine in Zustand 1 befindet und das Symbol unter dem Lesekopf 0 ist, verschiebe das Band nach rechts (dies ist quasi dasselbe, als ob der Lesekopf nach links wandert), drucke das Symbol 0 und halte an.

Die Maschine startet in diesem Beispiel in Zustand 0 und liest so lange Einsen ein, bis sich die erste Null unter dem Lesekopf befindet. Diese Null wird dann durch eine Eins überschrieben und das Band wird danach um eine Position nach links gerückt. Die zu addierenden Zahlen werden dadurch zusammengefügt. Bevor die Maschine zu Zustand 1 wechselt, befinden sich nun die folgenden Zeichen auf dem Band (die eckigen Klammern geben die aktuelle Position des Lesekopfs an):

111111[1]1111110

Nun haben Sie aber die Zahlen noch nicht richtig addiert. Zählen Sie ruhig nach: Sie haben jetzt 13 Einsen auf dem Band stehen, $5+7$ ist aber 12. Um diesen Fehler zu korrigieren, benötigen Sie eben einen zusätzlichen Zustand, nämlich Zustand 1. Dieser Zustand funktioniert zunächst wie Zustand 0 und rückt das Band so lange um eine Position nach links, bis eine Null gefunden wird. Diese Null ist aber nun das Ende des Addiervorgangs, bei dem die letzte Eins entfernt und danach die Maschine angehalten wird. Das Entfernen von Symbolen läuft dabei so ab: Das Band wird um eine Position zurückgeschoben (also nach rechts) und an diese Stelle wird eine Null geschrieben. Jetzt ist das Ergebnis korrekt und auf dem Band steht:

111111111111[0]0

Wahrscheinlich werden Sie mit dem letzten Beispiel einige Probleme gehabt haben, bis Sie es richtig verstanden haben. Das erste Problem war vermutlich die Tatsache, dass die Regeln, nach denen die Maschine arbeitet, in einer relativ unübersichtlichen 4-Punkte-Liste zusammengestellt wurden. Das zweite Problem war wahrscheinlich die Verschiebung des Bands, die umgekehrt zur Verschiebung des Lesekopfs verlaufen musste. Deshalb werde ich ab jetzt annehmen, dass sich der Lesekopf und nicht das Band bewegt, denn dadurch verändere ich nicht die grundlegenden Eigenschaften der Turing-Maschine, sondern nur die Notation der Richtungsangaben (Mathematiker sagen in diesem Fall, ich führe eine eigenschaftserhaltende Transformation durch). Außerdem verwende ich ab jetzt Zustandstabellen, in der Art, wie auch Turing sie später vorschlug, um die Übersichtlichkeit der oft zahlreichen Regeln zu erhöhen. Zustandstabellen können Sie sehr gut in Excel erstellen. Für dieses Beispiel gilt Tabelle 1.1.

Tabelle 1.1 Zustandstabelle der Turing-Maschine aus Beispiel 1.2.1

Zustand	Symbol	Schreibe	Verschiebung	Nächster Zustand
0	1	–	1 rechts	0
0	0	1	1 rechts	1
1	1	–	1 rechts	1
1	0	–	1 links	2
2	–	0	–	Halt

Ein kleiner Nachteil der Zustandstabellen bleibt: Für das Entfernen der letzten Eins am Ende der Addition benötigen Sie einen zusätzlichen Zustand, weil die Tabelle immer nur

einen Zustandswechsel und eine Lesekopf-Verschiebung pro Schritt abbilden kann. Der Vorteil ist hier aber die gute Abbildbarkeit von Zustandstabellen z. B. auf ein C-Programm, mit dem Sie dann beliebige einfache Turing-Maschinen simulieren können. Hierbei sind die sogenannten einfachen Turing-Maschinen Turing-Maschinen, die nur ein Band und nur einen Lese-/Schreibkopf besitzen.

Kommen wir nun zu der Frage, ob Sie es in dem letzten Beispiel mit einem berechenbaren Problem zu tun haben. Bleibt die Turing-Maschine also für jede Eingabe stehen und liefert sie dann auch stets ein korrektes Ergebnis? Um diese Frage zu beantworten, wähle ich nun folgende fehlerhafte Eingabe aus:

111001110

Die Turing-Maschine startet hier wieder in Zustand 0 und liest so lange Einsen, bis sich die erste 0 unter dem Lesekopf befindet. Nach dem Überschreiben der ersten 0 mit einer 1 und dem Verrücken des Lesekopfs nach rechts wechselt die Maschine zu Zustand 1. Das Band sieht nun so aus:

1111[0]1110

Nun ist das Symbol unter dem Lesekopf „0“, und dies bedeutet, dass die Maschine die Eins vor der Null entfernt, und danach anhält. Das Band enthält nun folgende Ausgabe, die sich anschließend auch nicht mehr ändert:

111[0]01110

Dieses Ergebnis lässt sich entweder als die Zahl 3 oder als ungültige Ausgabe interpretieren. Auf jeden Fall ist das Ergebnis falsch, obwohl die Turing-Maschine für jede beliebige Eingabe einer endlichen Anzahl von Einsen stehen bleibt. Haben Sie es aber in diesem Beispiel wenigstens mit einem berechenbaren Problem zu tun? Die Antwort, die Turing hier geben würde, ist „nein“, denn ein Algorithmus sollte immer das korrekte Ergebnis liefern und dies tut der Algorithmus in diesem Beispiel für unkorrekte Eingaben nicht. Wenn Sie aber voraussetzen, dass sämtliche Eingaben stets im korrekten Format vorliegen, dann haben Sie es hier in der Tat mit einem berechenbaren Problem zu tun, sofern Sie eine endliche Anzahl an Einsen auf dem Band voraussetzen.

1.2.2 Beispiel 2: Suchen und ersetzen

Mit dem Wissen aus dem letzten Beispiel können Sie jetzt eine einfache Zeichenersetzung realisieren. Im nächsten Beispiel sollen alle Buchstaben durch Großbuchstaben ersetzt werden. Wenn das gelesene Symbol bereits ein Großbuchstabe ist, können Sie es einfach durch sich selbst ersetzen. Zahlen, Kommas, Bindestriche und Leerzeichen sollen ignoriert werden und ein Satz soll grundsätzlich durch einen Punkt beendet werden. Ein Punkt soll dann auch die Maschine stets zum Anhalten bringen. Der Ausgangstext soll wie folgt lauten:

1937 hat Turing seine Turing-Maschine erfunden.

Die Maschine startet nun wieder in Zustand 0 und findet die Zahl 1. Dieses Symbol wird ignoriert und der Lesekopf rückt um ein Feld nach rechts. Dieser Schritt wird nun für jede Zahl wiederholt und natürlich auch für das Leerzeichen. Das Zeichen „h“ wird dann durch das Zeichen „H“ ersetzt. Das Band enthält nun folgende Symbole:

1937 H[a]t Turing seine Turing-Maschine erfunden.

Auch das Zeichen „a“ wird durch das Zeichen „A“ ersetzt und der Lesekopf befindet sich anschließend auf dem Zeichen „t“. Anscheinend funktioniert unser Ersetzungsalgorithmus einwandfrei, wenn wir Tabelle 1.2 verwenden.

Tabelle 1.2 Zustandstabelle für die Turing-Maschine aus Beispiel 1.2.2

Zustand	Symbol	Schreibe	Verschiebung Lesekopf	Nächster Zustand
0	Leerzeichen	Leerzeichen	1 rechts	0
0	0	0	1 rechts	0
0	1	1	1 rechts	0
...
0	9	9	1 rechts	0
0	a	A	1 rechts	0
0	b	B	1 rechts	0
...
0	z	Z	1 rechts	0
0	.	.	–	Halt

Ich habe in der letzten Tabelle immer dort drei Punkte eingesetzt, wo Sie sich die entsprechenden Einträge dazu denken müssen. So muss ich nicht z.B. sämtliche Zustandsänderungen zwischen den Zahlen 1 und 9 auflisten, sondern Sie können die entsprechenden Ersetzungen zwischen den Zahlen 2 und 8 im Geist ergänzen. An dieser Stelle sehen Sie wahrscheinlich schon den größten Nachteil von Turing-Maschinen: Die Zustandstabellen können wahrlich umfangreich werden, denn Sie müssen dort jedes Symbol einzeln auflisten. Außerdem sind zumindest die einfachen Turing-Maschinen sehr unflexibel und Sie benötigen quasi für jeden Algorithmus eine separate Maschine. Turing führte später den Gedanken einer universellen Maschine ein, den er aber leider aus gesundheitlichen Gründen nicht mehr zu einer vollständigen Theorie ausbaute.

In diesem Buch geht es aber nicht um das wahrlich tragische Schicksal Alan Turings, sondern darum, wie seine Ideen später in der Informatik eingesetzt wurden. Deshalb ist die Frage nun, ob auch das Ersetzungsverfahren in diesem Beispiel ein Algorithmus ist, der auf jeden Fall anhält. Wenn Sie aber etwas nachdenken, kommen Sie schnell darauf, dass das Ersetzungsverfahren in diesem Beispiel z.B. niemals anhält, wenn der Punkt am Satzende fehlt oder wenn ein Zeichen im Text auftaucht, für das keine Ersetzungsregel existiert (in diesem Fall würde die Turing-Maschine einfach nichts tun und das für immer). Fügen wir nun die folgende implizite Regel ein: „Immer, wenn für ein Symbol keine Regel zutrifft oder das betreffende Feld leer ist, halte an.“ Nun hält unser Algorithmus zwar stets an, liefert aber nicht immer eine vollständige Ersetzung aller Buchstaben durch Großbuchstaben. Nehmen Sie z.B. folgenden Satz als Eingabe an:

Hallo Klaus! Es regnet, darum bleibe ich heute zuhause.

Da für das Zeichen „!“ keine Regel existiert, hält die Turing-Maschine dort an und das Band enthält in diesem Fall folgenden Text:

HALLO KLAUS[!] Es regnet, darum bleibe ich heute zuhause.

Ändern wir nun unsere implizite Regel wie folgt ab: „Immer, wenn für ein Symbol keine Regel zutrifft, ersetze das gelesene Symbol durch sich selbst und bewege den Lesekopf um einen Schritt nach rechts. Außerdem halte an, wenn der Lesekopf auf ein leeres Feld trifft.“ Nun können wir auch den Rest des Satzes in Großbuchstaben umwandeln und sogar den Punkt am Ende weglassen. Wenn wir voraussetzen, dass das Band nur eine endliche Anzahl nicht leerer Felder enthalten darf und dass ferner der Eingabetext nicht durch leere Felder unterbrochen werden darf, wird unser Beispiel aus Abschnitt 1.2.2 berechenbar und liefert auch stets korrekte Ergebnisse.

1.2.3 Beispiel 3: Multiplikation zweier Zahlen mit einer erweiterten Turing-Maschine

Wollen wir nun versuchen, zwei Zahlen nicht nur zusammenzufügen, sondern auch zu multiplizieren (die Multiplikation war übrigens lange Zeit das größte Problem bei der ENIAC). Wir wollen also statt $5+7$ $5*7$ berechnen. Die Ausgangsschreibweise der Zahlen soll wieder wie im allerersten Beispiel erfolgen, nämlich als:

11111011111110

Sie müssen nun versuchen, die Symbolfolge „11111110“ fünfmal hintereinanderzuhängen. Dies können Sie wie folgt realisieren: Sie ersetzen erst einmal die erste Eins durch eine Null und suchen danach die nächste Null. Dies ist die Null vor der Zahl, die hinter dem Produkt steht. Anschließend müssen Sie die Folge „1111111“ kopieren. Danach müssen Sie zum ersten Zeichen zurückfinden, das nicht 0 ist, und den Kopiervorgang der Folge „1111111“ so lange wiederholen, bis die erste Ziffernfolge vor dem Multiplikativen *aufgebraucht* ist. Ein großes Problem hierbei ist leider, dass Sie den Multiplikativen in dem Moment verändern, in dem Sie dort eine Zeichenkette anhängen. Das Problem der Multiplikation zweier Zahlen ist in der Tat mit einer Art einfacher Turing-Maschinen realisierbar, die sich *fleißige Biber* nennen, aber diese nun darzustellen, würde so manchen Leser schon jetzt *aussteigen* lassen. Ich will natürlich vermeiden, dass Sie schon jetzt aufgeben, Ihnen aber trotzdem ein Gefühl dafür geben, wo die Grenzen der ursprünglichen Turing-Maschinen liegen und was diesen fehlt. Dies wären folgende Dinge:

- Turing-Maschinen besitzen kein Gedächtnis in Form eines wie immer gearteten internen Speichers und können sich z. B. nicht daran erinnern, welches Symbol im letzten Schritt gelesen wurde.
- Turing-Maschinen können nicht an eine bestimmte Position direkt zurückspringen, sondern können den Lesekopf nur relativ zur aktuellen Position bewegen (man sagt auch, Turing-Maschinen können nur relative Sprünge ausführen).
- Bei Turing-Maschinen kann man das Programm, das ihnen einmal eingegeben wurde, nicht mehr ändern.
- Turing-Maschinen können nicht *lernen*, z. B. indem man ihnen später neue Regeln hinzufügt.

Kommen wir nun zurück zur Multiplikation zweier Zahlen. Dieses Problem können Sie nicht so einfach mit einer einfachen Turing-Maschine lösen, deshalb möchte ich die ursprüngliche Maschine durch einen Puffer erweitern. Ein Puffer ist ein Zwischenspeicher, der eine

bestimmte Anzahl an Symbolen aufnehmen kann, um diese später bei Bedarf weiterzuarbeiten. Ich will nun annehmen, dass ein zusätzlicher Puffer in einer erweiterten Turingmaschine bis zu 100 Symbole aufnehmen kann und dass ein spezielles Kommando den Pufferinhalt auf das Band schreiben kann, wobei der Lesekopf automatisch um die entsprechende Anzahl an Symbolen weiterbewegt wird. Durch einen Puffer können also Kopiervorgänge relativ einfach realisiert werden. Ferner will ich annehmen, dass es ein spezielles Kommando gibt, mit dem die Maschine sich die aktuelle Position des Lesekopfs merken kann, um später zu dieser Position zurückkehren zu können. Mit der erweiterten Turing-Maschine ist die Multiplikation zweier Zahlen nun relativ einfach realisierbar. Schauen Sie sich dazu das Ausgangsbeispiel noch einmal an. Am Anfang enthält das Band folgende Symbole:

11111011111110

Die Maschine befindet sich am Anfang in Zustand 0. In diesem Zustand liest sie zunächst das aktuelle Symbol unter dem Lesekopf, das am Anfang eine Eins ist. Wenn das Symbol unter dem Lesekopf eine Eins ist, wird diese durch eine Null ersetzt und der Lesekopf bewegt sich um eine Position nach rechts. Die Maschine merkt sich danach die aktuelle Position P und wechselt danach zu Zustand 1. In Zustand 1 wird der Lesekopf nun so lange nach rechts bewegt, wie sich unter diesem eine Eins befindet. Eine Null dagegen bewegt den Lesekopf um eine Position nach rechts, die Maschine leert den Zeichenpuffer und wechselt anschließend zu Zustand 2. In Zustand 2 liest die Maschine nun ebenfalls so lange Einsen vom Band, bis eine Null gefunden wurde, jedoch speichert sie nun jede Eins im Zeichenpuffer. Wurde in Zustand 2 eine Null gefunden, gibt die Maschine daraufhin den Zeichenpuffer aus, bewegt den Lesekopf zurück zu der Position, die sich die Maschine vorher gemerkt hat, und wechselt daraufhin wieder zu Zustand 0. Nun kann der Kopiervorgang erneut stattfinden, bis irgendwann alle Einsen am Anfang *aufgebraucht* sind und sich eine Null unter dem Lesekopf befindet. Dies ist die Null direkt vor dem Multiplikanden.

Wenn Sie jedoch aufgepasst haben, dann haben Sie gemerkt, dass die Maschine ein falsches Ergebnis liefert. Das liegt daran, dass wir ein Problem noch nicht gelöst haben: Immer, wenn an das Ende etwas angehängt wird, ändert sich automatisch der Multiplikand, wodurch beim nächsten Kopiervorgang die doppelte Anzahl Zeichen kopiert wird. Genau deshalb muss die ursprüngliche Zustandstabelle durch Kommandos erweitert werden, die z. B. explizit Zeichen in den Puffer kopieren oder diesen bei Bedarf leeren können. Ferner reichen die Symbole „0“ und „1“ nicht mehr aus, um z. B. die Eingabe von dem Ergebnis trennen zu können. Deshalb habe ich eine Zwei an der Position eingesetzt, ab der das Ergebnis stehen soll. Die Eingabe lautet also jetzt wie folgt:

11111011111112

Schauen wir, ob die Maschine nun korrekt arbeitet. In Zustand 0 liest die Maschine die Zahl 1 ein, ersetzt diese durch eine Null, bewegt den Lesekopf um eine Position nach rechts, merkt sich die aktuelle Position P und wechselt zu Zustand 1. In diesem Zustand werden jetzt so lange Einsen gelesen, bis unter dem Lesekopf eine Null steht. Ist dies der Fall, rückt der Lesekopf um eine Stelle nach rechts, der Zeichenpuffer wird geleert und die Maschine wechselt zu Zustand 2. In diesem Zustand werden nun so lange Einsen gelesen und im Zeichenpuffer gespeichert, bis eine Zwei gefunden wird. Wird eine Zwei gefunden, rückt der Lesekopf eine Position nach rechts und die Maschine wechselt zu Zustand 3. In diesem Zustand werden so lange Einsen gelesen, bis sich unter dem Lesekopf eine Null oder ein

leeres Feld befindet. Ist dies der Fall, wird der Zeichenpuffer ausgegeben. Nach dem ersten Kopiervorgang steht auf dem Band Folgendes:

01111011111112111111[leer]

Nachdem der Zeichenpuffer ausgegeben wurde, wechselt die Maschine zu Zustand 4. Zustand 4 ist nur dazu da, das Kommando „bewege den Lesekopf zurück zu der vorher gemerkten Position P“ auszuführen und anschließend zu Zustand 0 zu wechseln. Dies ist hier die zweite Position auf dem Band, das jetzt folgende Symbole enthält:

0[1]111011111112111111

Da sich unter dem Band eine Eins befindet, wird der Kopiervorgang wiederholt: Zuerst ersetzt die Maschine die 1 durch eine 0, anschließend sucht die Maschine die Zahl 0. Danach leert sie den Zeichenpuffer, liest sämtliche Einsen in den Puffer ein, bis sich die Zwei unter dem Lesekopf befindet, und sucht anschließend das erste leere Feld hinter der letzten Eins. Durch die Trennung von Eingabebereich und Ergebnisbereich werden die Einsen nun korrekt zusammengefügt. Am Ende enthält das Band folgende Ausgabe:

00000111111111111111111111111111111112

Leider kann auch die erweiterte Turing-Maschine unter Umständen unvorhergesehenes Verhalten zeigen, wie z. B. bei der folgenden Eingabe:

11111211111112

Für Zustand 0 wurde nicht definiert, wie bei dem Symbol „2“ verfahren werden soll, deshalb friert die Maschine an dieser Stelle ein. Wenn Sie sich wieder dafür entscheiden, vorher die implizite Annahme zu machen, dass die Maschine stehen bleiben soll, falls für ein Symbol keine Regel existiert, wird am Ende das Ergebnis falsch sein. Es folgt die erweiterte Zustandstabelle für das letzte Beispiel.

Tabelle 1.3 Zustandstabelle für die Turing-Maschine aus Beispiel 1.2.3

Zustand	Symbol	Schreibe	Verschiebung Lesekopf	Kommando	Nächster Zustand
0	1	0	1 rechts	Merke aktuelle Position P	1
0	0	–	–	–	Halt
1	1	–	1 rechts	–	1
1	0	–	1 rechts	Leere Zeichenpuffer	2
2	1	–	1 rechts	Übertrage Symbol in den Zeichenpuffer	2
2	2	–	1 rechts	–	3
3	1	–	1 rechts	–	3
3	leer	–	–	Ausgabe Zeichenpuffer	4
3	0	–	–	Ausgabe Zeichenpuffer	4
4	–	–	–	Zurück zu Position P	0

1.2.4 Von der Turing-Maschine zum Prozessor

Das letzte Beispiel funktioniert sehr gut für kleine Zahlen bis 100, danach ist entweder der Zeichenpuffer voll oder es dauert (bei einem beliebig erweiterbaren Puffer) sehr lange, um z.B. eine Zahl 1000-mal in den Ergebnisbereich zu übertragen. Kurz: Wir benötigen für komplexere Algorithmen eine alternative Lösung. Diese Lösung ist, die Zahlen anders darzustellen. Statt viele Einsen aneinanderzuhängen, wird mit den Nullen und Einsen ein Stellenwertsystem aufgebaut, das dem gewohnten Zahlensystem mit zehn Ziffern ähnelt. Anstatt jedoch nach der Zahl 9 eine neue Stelle zu benutzen und danach „10“ zu schreiben, muss in dem Binärsystem, das Computer benutzen, schon nach der Ziffer 1 (also für die Zahl 2) „10“ geschrieben werden. Der Vorteil des Binärsystems ist, dass dies sehr gut in elektronischen Schaltungen realisiert werden kann und die Ziffernfolgen so lang auch wieder nicht sind. Zumindest müssen die Zahlen im Binärsystem nicht so umständlich codiert werden wie die Zahlen in den letzten Beispielen. Eine weitere Überlegung der Ingenieure ab den 50er-Jahren war, mehrere binäre Symbole gleichzeitig zu verarbeiten und auf diese Weise zu Blöcken zusammenzufassen. Mit diesen Blöcken konnten dann auch (wieder durch entsprechende elektronische Schaltungen) grundlegende Operationen wie z.B. Addition, Subtraktion, Multiplikation und Division durchgeführt werden. Diese Blöcke von binären Zeichen (dies waren am Anfang oft vier oder acht Binärsymbole) nennt man Register, die auf diese Weise erweiterten Turing-Maschinen, die auch von sich aus grundlegende Rechenoperationen durchführen können, nennt man Prozessoren. Ein Prozessor ist der wichtigste Bestandteil moderner Computer und das elektronische Bauteil, das die Programme ausführt. Ein Prozessor ist quasi der real gewordene Traum Alan Turings, eine universelle Variante seiner Maschine zu bauen.

Eine zusätzliche Maßnahme bei Prozessoren ist, dass die auszuführenden Algorithmen nicht mehr in einer Tabelle fest verdrahtet sind. Was fest verdrahtet ist, sind grundlegende Operationen, wie z.B. einen separaten Speicher anzusprechen oder zwei Zahlen zu addieren. Jede Operation wird durch ein bestimmtes Muster von binären Symbolen bestimmt, die binären Symbole heißen seit den 50er-Jahren Bits (binary digits). Ich will im Folgenden annehmen, dass immer 8 Bits zu einer Einheit zusammengefasst werden (man spricht dann seit den 60er-Jahren von einem Byte) und dass auch ein Register 8 Bit breit ist. Auch die auszuführenden Operationen sollen 8 Bit breit sein und eine spezielle Nummer zwischen 0 (binär 00000000) und 255 (binär 11111111) zugeordnet bekommen. Der Prozessor liest nun erst einmal 8 Bits aus dem Speicher (es gibt also kein Band mehr), bestimmt die zugehörige Zahl, die dahintersteckt, und führt anhand einer internen Tabelle den dazugehörigen Befehl aus (gegebenenfalls werden dazu auch weitere Bytes eingelesen). Die Nummer, die zu einem bestimmten Befehl gehört, nennt man OP-Code.

An dieser Stelle ist Turings Traum einer universellen Rechenmaschine Wirklichkeit geworden, anstatt des Bands werden nun Speicherbausteine mit wahlfreiem Zugriff benutzt. An dieser Stelle taucht dann zum ersten Mal der Begriff *random access memory*, kurz RAM, auf. Der wahlfreie Zugriff auf das RAM macht einen Prozessor sehr leistungsfähig, weil die Zeit, die benötigt wird, um auf eine bestimmte Adresse zuzugreifen, kaum von der Größe des Speichers abhängt. Statt der Position eines Lesekopfs auf einem Band benutzt man also heute Speicheradressen. Manchmal wird die Abkürzung RAM in diesem Zusammenhang auch für *random access machine* (Maschine mit wahlfreiem Zugriff) benutzt. Diese Abkürzung ist schlicht falsch und Sie sollten diese überlesen, wenn sie z.B. in Internetforen auf-

taucht. Kommen wir aber zurück zu den Prozessoren. Moderne Prozessoren können nämlich noch viel mehr, sie können z. B. Speicheradressen direkt anspringen, um die Programmausführung an genau dieser Stelle fortzusetzen. Dies leisten spezielle Register, wie z. B. der Programmzähler PC (program counter). Das Zählregister PC zeigt immer auf die Speicheradresse des nächsten Befehls und wird auch stets automatisch aktualisiert, nachdem ein Befehl ausgeführt wurde.

Nehmen wir nun einen einfachen Prozessor, der zusätzlich zum Programmzähler ein Register besitzt, das 8 Bit breit ist. In dieses Register soll nun mit dem Befehl Nr. 1 eine 8-Bit-Zahl eingelesen werden. Schreiben wir ab jetzt Byte-Werte als Zahlen zwischen 0 und 255 und ersetzen die Bandposition durch eine Speicheradresse, die die Position des Bytes im Speicher angibt. Die Position 0 soll das erste Byte im Speicher darstellen. Nun müssen Sie für die Multiplikation von 5 mit 7 aus unserem letzten Beispiel zuerst die Zahl 5 in das Zahlenregister schreiben, das ich hier mit A abkürzen möchte. Dazu müssen Sie dem Prozessor folgende Bytes übergeben:

1,5 (Lade den Wert 5 in Register A)

Nun benötigen Sie noch zusätzliche Befehle für die Grundrechenarten. Seien die OP-Codes 2, 3, 4 und 5 für die Grundrechenarten +, -, * und / vorgesehen. Das Byte, das dem OP-Code folgt, sei der Operand des Befehls. Ein Operand ist der Teil einer mathematischen Operation, mit dem gerechnet wird, also der eigentliche Zahlenwert. Bei $5+7$ wären die Operanden 5 und 7. Unser Prozessor in diesem Beispiel speichert die Operanden in Register A. Um die Multiplikation aus Abschnitt 1.2.3 auszuführen, müssen Sie nun vorher die folgenden Bytes benutzen:

1,5 (Lade den Wert 5 in Register A)

5,7 (Multipliziere A mit 7 und speichere das Ergebnis wieder in Register A)

Sie sehen an dieser Stelle schon, dass moderne Prozessoren sehr viel effizienter arbeiten als die relativ langsamen Turing-Maschinen. Liefern aber die Algorithmen, die auf modernen Prozessoren laufen, nun endlich immer die richtigen Ergebnisse? Werden nun sämtliche mathematischen Probleme im Prinzip berechenbar? Die Antwort ist leider „nein“, denn die grundlegenden Probleme in Bezug auf die Berechenbarkeit werden auch durch moderne, schnelle Prozessoren nicht gelöst. Mehr noch: Im Prinzip kann ein moderner Prozessor durch eine einfache Turing-Maschine nachgebildet werden, wenn auch die Ausführungsgeschwindigkeit der Programme eher bescheiden ist. In dem nächsten Abschnitt werde ich nun eine Methode vorstellen, mit der Sie die Laufzeit von Algorithmen abschätzen können, die in C programmiert wurden. Auch dieses Thema ist Bestandteil der Vorlesungen in Allgemeiner Informatik.

■ 1.3 Laufzeitanalyse von Algorithmen

Die Grundlage der Komplexitäts- und Laufzeitanalyse von Algorithmen und Computerprogrammen im Allgemeinen ist das Entscheidungsproblem: Wie kann entschieden werden, ob eine bestimmte mathematisch-logische Aussage eindeutig wahr oder falsch ist und wie kann man in einer sinnvollen Zeit zu einem eindeutigen Ergebnis kommen? Und wenn z. B.

eine Berechnung mit einem plausiblen Ergebnis endet, was heißt dann in einer *sinnvollen Zeit*? Einen möglichen Ansatz haben Sie bereits kennengelernt, nämlich die Turing-Maschine. Beginnen wir nun wieder mit einem einfachen Beispiel für eine einfache Turing-Maschine. Es seien auf dem Band vor dem Start folgende Zeichen enthalten:

aaaaaaaaaaaaabbbbbbbbbbbbaaaaaaaaaaaaaa

Angenommen, es sollen alle „a“ durch „z“ ersetzt werden und die Maschine startet wieder in Zustand 0. Nun genügt im Endeffekt folgende Regel: Falls ein „a“ gelesen wurde, schreibe ein „z“ und rücke den Lesekopf um eine Position nach rechts. Das Programm verläuft nach diesen Überlegungen in folgender Schleife ab:

1. Falls ein „a“ gelesen wurde, schreibe ein „z“
2. Rücke den Lesekopf um eine Position nach rechts
3. Zurück zu Schritt 1

An dieser Stelle sehen Sie schon, dass der Algorithmus tut, was er soll – nur stoppt er nicht. Es wurde nämlich nicht definiert, was mit den anderen Zeichen geschehen soll. Da das Eingabeband unendlich lang ist, wird die Turing-Maschine bis in alle Ewigkeit um eine Position weiterrücken. Auch in diesem einfachen Beispiel wird die Turing-Maschine also erst stoppen, wenn ein Endzustand definiert wird. Dies kann z. B. die Regel sein, dass die Maschine immer dann anhält, wenn sich ein leeres Feld unter dem Lesekopf befindet. Der veränderte Algorithmus stoppt in diesem Fall, wenn das erste Leerfeld auftritt. Wenn das erste Eingabezeichen unter dem Lesekopf kein Leerfeld ist, stoppt der Algorithmus nun in einer endlichen Zeit, die sich einfach berechnen lässt:

Laufzeit=K*Anzahl der Zeichen bis zum ersten Leerfeld

Die Konstante K gibt hier an, wie lange die Turing-Maschine benötigt, um einen einzelnen Schritt inklusive möglicher Zustandswechsel auszuführen. Wenn es also einen definierten Startzustand und einen definierten erreichbaren Endzustand gibt, lässt sich die Laufzeit des Algorithmus relativ einfach berechnen. Ferner gilt: Jeder Algorithmus, der auf einer Turing-Maschine für sämtliche möglichen Eingaben zu einem Ende kommt, ist auch vollständig berechenbar. Leider liegt das grundlegende Problem genau hier, nämlich bei der Aussage „für sämtliche Eingaben“. Da das Eingabeband bei einer Turing-Maschine unendlich lang ist, bedeutet dies, dass für den im letzten Beispiel vorgestellten Algorithmus das Entscheidungsproblem nicht gelöst werden kann – man müsste bei beliebig langen Eingaben auch beliebig lang warten, um zu entscheiden, ob die Turing-Maschine jemals stoppt und ob sie dann eine logisch wahre, plausible und reproduzierbare Antwort liefert. Es gibt in der Mathematik viele Probleme, die sich nicht in einer *vernünftigen Zeit* berechnen lassen. Hier sind einige Beispiele:

- Das Produkt $a \cdot b$ sehr langer Primzahlen (ab etwa 100 Stellen) lässt sich nur sehr schwer faktorisieren, wenn man a und b nicht kennt.
- Die Entscheidung, ob eine zufällig gewählte Zahl eine Primzahl ist, wird mit wachsender Stellenanzahl schwieriger. Der Schwierigkeitsgrad wächst exponentiell mit der Stellenanzahl.
- Es gibt Funktionen, die Einwegfunktionen sind: Eine Berechnung in die eine Richtung ist sehr einfach, während die andere Richtung schwer bis unmöglich zu berechnen ist. Ein Beispiel ist das Produkt langer Primzahlen, ein anderes Beispiel ist z. B. der diskrete Logarithmus.

Sämtliche als „schwer bis unmöglich zu lösen“ deklarierten mathematischen Probleme haben die Eigenschaft, dass der Zeitaufwand der Berechnung exponentiell mit der Länge der Eingabe (z. B. der Stellen- oder Bitanzahl) wächst und Sie die Laufzeit nicht mehr durch ein wie immer geartetes Polynom der Art

$$f(x) = a_n x^n + a_{n-1} x_{n-1} + \dots + a_0 x^0$$

ausdrücken können. Stellen Sie sich an dieser Stelle z. B. eine dreifach verschachtelte Schleife vor, die die Variablen i , j und k als Zähler benutzt. Wenn i , j und k nun jeweils den Wert 10 haben, dann wird die äußerste Schleife zehnmal, und die innerste Schleife 1000-mal durchlaufen. Die Laufzeit ergibt sich hier also aus dem Produkt von i , j und k und lässt sich allgemein als Polynom der Form

$$f(x) = ax^3$$

darstellen. Solche Probleme, bei denen sich die Laufzeit durch ein wie immer geartetes Polynom darstellen lässt, sind mit einem modernen Computer noch in einer vernünftigen Zeit berechenbar. Mathematische Algorithmen jedoch, bei denen die Laufzeit wie folgt wächst, sind kaum noch in einer vernünftigen Zeit berechenbar:

$$f(x) = a \cdot e^{bx}$$

Was diese Aussage bedeutet, erfahren Sie in den nächsten Abschnitten.

1.3.1 Das P-NP-Problem

Bis jetzt gilt also folgende Aussage: Für mathematische Probleme, bei denen der Berechnungsaufwand exponentiell mit der Eingabelänge (gemessen in Ziffern bzw. Bits) wächst, gibt es zumindest in der nahen Zukunft trotz Einbeziehung moderner Technologien keine effiziente Lösung. Auf dieser Feststellung basieren einige wichtige Verschlüsselungsverfahren, wie z. B. RSA oder der sichere Schlüsselaustausch mit dem Diffie-Hellmann-Verfahren. In der Komplexitätstheorie gibt es drei für die Informatik wichtige Komplexitätsklassen. Diese nennt man P, EXP und NP. P umfasst dabei sämtliche Probleme, bei denen der Berechnungsaufwand polynomial mit der Länge der übergebenen Daten steigt. Der Aufwand lässt sich hier durch eine Funktion der Form

$$t(k) = n \cdot k^b$$

darstellen. $t(k)$ ist der Zeitaufwand in Abhängigkeit von der Eingabelänge k in Bit, b und n sind Konstanten. Bei den Problemen, die zur Komplexitätsklasse EXP gehören, wächst der Zeitaufwand exponentiell mit der Größe der zu berechnenden Zahlen. Der Aufwand lässt sich also hier durch eine Funktion der Form

$$t(k) = n \cdot b^k$$

darstellen. Auch hier sind n und b wieder Konstanten. Die Klasse NP (nicht polynomiale Algorithmen) liegt innerhalb von EXP und umfasst P. Die Klasse NP lässt im Gegensatz zu P und EXP zusätzlich zu den ursprünglichen Turing-Maschinen auch nicht-deterministische Turingmaschinen zu. Diese Art Turingmaschinen enthält an einigen Stellen Zufallselemente, die eine genaue Vorhersage unmöglich machen. Diese Eigenschaft nennt man nicht-deterministisch. Man könnte z. B. die zuletzt genannte Ersetzung von a durch z wie folgt abändern, um eine nicht-deterministische Turing-Maschine zu erzeugen: