Theoretische Informatik

Juraj Hromkovič

Theoretische Informatik

Formale Sprachen, Berechenbarkeit, Komplexitätstheorie, Algorithmik, Kommunikation und Kryptographie

5., überarbeitete Auflage

Springer Vieweg

Juraj Hromkovič
ETH Zürich
Zürich, Schweiz

ISBN 978-3-658-06432-7 ISBN 978-3-658-06433-4 (eBook)
DOI 10.1007/978-3-658-06433-4

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

Springer Vieweg
Die erste Auflage erschien unter dem Titel „Algorithmische Konzepte der Informatik".

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.springer-vieweg.de

Mit einer Weisheit,
die keine Träne kennt,
mit einer Philosophie,
die nicht zu lachen versteht,
und einer Größe,
die sich nicht vor Kindern verneigt,
will ich nichts zu tun haben.

Khalil Gibran

Meinen Eltern

Vorwort

Dieses Buch ist eine einfache Einführung in algorithmische Grundkonzepte der Theoretischen Informatik. Die Theoretische Informatik ist weltweit ein fester Bestandteil des Informatikstudiums. Im Unterschied zu den ingenieursmäßig geprägten Gebieten der Praktischen und der Technischen Informatik hebt die Theoretische Informatik mehr die naturwissenschaftlichen und mathematischen Aspekte der Informatik hervor. Gerade die mathematische Prägung ist oft ein Grund dafür, dass die Theoretische Informatik für zu schwer gehalten wird und dadurch ein nicht gerade beliebter Teil der Ausbildung ist. Der Schwierigkeitsgrad der Theoretischen Informatik ist aber meiner Meinung nach nicht der einzige Grund ihrer Unbeliebtheit, insbesondere wenn die Studierenden in ihrer Beurteilung außerdem noch das Prädikat „schwach motiviert“ oder sogar „langweilig“ verwenden. Das könnte auch damit zusammenhängen, dass sich die Einführung in die Theoretische Informatik im Grundstudium an vielen deutschen Hochschulen auf den klassischen Stoff der Berechenbarkeit, der Theorie der formalen Sprachen und der abstrakten Komplexitätstheorie beschränkt. Dass man dabei überwiegend nur die Konzepte und Ansichten, die vor dem Jahr 1970 entstanden sind, vermittelt, dürfte alleine nicht schlimm sein. Es führt aber oft dazu, dass man mit einer einzigen Motivation zu viele Vorlesungen der Art Definition – Satz – Beweis absolvieren muss und so halbiert sich die Wichtigkeit dieser Motivation in den Augen der Studierenden mit jeder weiteren Vorlesung, die anknüpft, ohne eine eigene Motivation zu bringen.

Um Abhilfe von diesem Zustand zu schaffen, muss man sich die Entwicklung der Theoretischen Informatik in den letzten 30 Jahren ansehen. Es geht dabei nicht nur darum, dass man in dieser Zeit tiefere Resultate und viele neue Konzepte entwickelt hat, sondern insbesondere darum, dass die Theorie immer mehr auf die Bedürfnisse der Praxis eingegangen ist. Dadurch sind die Anwendungen der Theorie direkter geworden und die Anschaulichkeit der Motivationen ist stark gestiegen. Die Theoretische Informatik liefert nicht-triviales Know-How, das in vielen Fällen faszinierende und überraschende Anwendungen ermöglicht. Es ist nicht möglich, in einem Einführungskurs alle derartigen spektakulären Erkenntnisse zu präsentieren, weil einige ein zu tiefes Verständnis der Materie fordern, als dass sie im Vordiplom als Ziel gestellt werden können. Aber es

gibt genügend Ideen, die in einer Einführung darstellbar sind, und die wesentlich die Denkweise eines Informatikers prägen können und sollten. Dieses Buch ist ein Versuch des Autors, zumindest teilweise seine Vision einer modernen Einführung in die algorithmischen Gebiete der Theoretischen Informatik zu realisieren. Dabei folgt er der Richtung, die in der englischsprachigen Literatur Mike Sipser und in der deutschsprachigen Literatur Ingo Wegener eingeschlagen haben, und die im Wesentlichen auf den oben präsentierten Gedanken basiert. Die klassischen Teile der Berechenbarkeit und Komplexitätstheorie sind hier reduziert und dafür einige wichtige Konzepte aus dem Bereich der Algorithmik, Randomisierung, Kommunikation und Kryptographie eingesetzt.

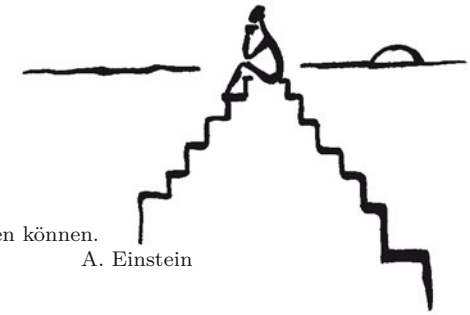
Die Strategien dieses Buches heißen „Einfachheit“ und „Weniger ist manchmal mehr“. Für uns ist die Prägung des intuitiven, informellen Verständnisses der Materie genau so wichtig wie präzise Formalisierung, detaillierte Beweisführungen und Begründungen. Didaktisch geht das Buch immer langsam vom Einfachen zum Komplizierten vor. Wir versuchen, die Anzahl der Begriffe und Definitionen zu minimieren, auch wenn wir dadurch auf die Präsentation einiger wichtiger Konzepte und Resultate verzichten müssen. Die Idee dahinter ist, dass es wichtiger ist, die unterschiedlichen konzeptuellen Denkweisen und Methoden zu präsentieren, als ein „vollständiges“ Bild einer abgeschlossenen mathematischen Theorie zu zeichnen. Da die Argumentation in diesem Buch nicht nur auf der formalen mathematischen Ebene geführt wird, sondern insbesondere auf das intuitive Verständnis der Materie baut, ist das Buch auch als Lehrmaterial für Fachhochschulen und Studierende, die Informatik nicht als Hauptfach studieren, gut geeignet.

Hilfreiche Unterstützung Anderer hat zu der Entstehung dieses Lehrbuches wesentlich beigetragen. Besonderer Dank gilt Dirk Bongartz, Hans-Joachim Böckenhauer und Alexander Ferrein für sorgfältiges Korrekturlesen und zahlreiche Verbesserungsvorschläge. Herzlicher Dank geht an Dietmar Berwanger, Volker Claus, Georg Schnitger, Erich Valkema und Peter Widmayer für Bemerkungen und anregende Diskussionen. Alexander Ferrein und Manuel Wahle danke ich für die sorgfältige Einbettung des Manuskripts in LaTeX. Mein tiefster Dank gilt Frau Stefanie Laux vom Teubner Verlag für die hervorragende und konstruktive Zusammenarbeit. Herzlichst danke ich Ingrid Zámečníková für die Illustrationen, den einzigen vollkommenen Teil des Buches, und Tanja für ihre Zitatensammlung.

Aachen, 2001 Juraj Hromkovič

Die Köpfe von Menschen soll man nicht
mit Fakten, Namen und Formeln füllen.
Um so etwas zu lernen,
braucht man nicht in die Schule zu gehen.
Der Zweck der Erziehung ist,
dem Menschen das Denken beizubringen,
und so eine Ausbildung, die keine Lehrbücher ersetzen können.

A. Einstein



Vorwort zur zweiten Auflage

Es freut mich sehr, dass diese alternative Einführung in die Theoretische Informatik so gut von Kollegen und Studenten angenommen wurde. Ich möchte hier zunächst allen denen herzlich danken, die Zeit gefunden haben, ihre Meinungen über das Buch sowie einige Verbesserungswünsche und Erweiterungsvorschläge zu äußern. Ich habe dieses Buch mit Sorgfalt geschrieben, weil ich wusste, dass der Inhalt des Buches den Rahmen der traditionellen Vorstellung der Grundlagen der Theoretischen Informatik sprengt. Deshalb habe ich befürchtet, dass es viele Kollegen als einen Verstoß gegen überwiegend akzeptierte Darstellungen der Informatikgrundlagen im Grundstudium bewerten würden. Außer den vielen positiven Kommentaren, die meine Sorgen schrumpfen ließen, fand ich am Erfreulichsten (als eine echte Bestätigung des Buchkonzeptes), dass die Leser sich überwiegend gerade die Erweiterung der nicht-klassischen Gebiete wie Randomisierung und Kommunikation gewünscht haben. Ich nahm diese Herausforderung mit Freude an und habe versucht, gleich die erste Möglichkeit zu nutzen, für die zweite Auflage das Buch sorgfältig zu überarbeiten und zu erweitern.

Das Kapitel Randomisierung wurde um einen neuen Abschnitt ergänzt, der die Methode der Fingerabdrücke zum Entwurf von zufallsgesteuerten Algorithmen als einen wichtigen Spezialfall der Anwendung der Methode der häufigen Zeugen präsentiert. Die Methode der Fingerabdrücke wurde an dem randomisierten Äquivalenztest für zwei Polynome illustriert.

Im Kapitel Kommunikation und Kryptographie kamen zwei neue Abschnitte dazu. Der Abschnitt Digitale Unterschriften zeigt eine sehr wichtige kommerzielle Anwendung des vorgestellten Konzeptes der Public-Key-Kryptosysteme. Dabei machen wir darauf aufmerksam, dass im Rahmen der klassischen Kryptographie keine Möglichkeit besteht, digitale Unterschriften ohne hohes Fälschungsrisiko zu leisten. Damit ist das kryptographische Konzept der öffentlichen Schlüssel eine Basis, ohne die man sich heute den sich dynamisch entwickelnden Bereich des E-Commerce gar nicht vorstellen kann. Der zweite neue Abschnitt zeigt einen Entwurf eines effizienten Telefonnetzes. Die Zielsetzung ist dabei, die Problemstellungen und geeignete Methoden zur Lösung der gestellten Probleme im Bereich der Kommunikation in Netzen am Beispiel eines eleganten Netzentwurfes zu

illustrieren.

Einige Kollegen haben sich gewünscht, in diesem Lehrmaterial auch den Beweis des Satzes von Cook zu lesen. Obwohl es sich um eines der grundlegendsten Resultate der Informatik handelt, vertrete ich weiter die Meinung, dass dieses Resultat einen zu schweren Beweis für das Grundstudium besitzt. Trotzdem habe ich mich entschieden, den Beweis einzufügen, um dem besonders interessierten Studierenden die Möglichkeit zu geben, diese grundsätzlich wichtige Beweistechnik kennenzulernen. Da ich diesen Beweis nun einbetten wollte, habe ich versucht, durch eine langsame Entwicklung der Beweisidee den Schwierigkeitsgrad des Beweises abzumildern. Deswegen entstanden drei Seiten über die Beschreibung von Texten und Spielkonfigurationen durch Boole'sche Formeln, die als eine Vorbereitung für den Beweis des Satzes von Cook dienen sollen. Nach dieser Einführung konzentriert sich der Beweis nur auf eines, und zwar wie man die Semantik der Berechnungen durch die Formeln effizient ausdrücken kann.

Außer den drei oben beschriebenen Erweiterungen wurden an vielen Stellen Korrekturen und Verbesserungen eingearbeitet, um die Anschaulichkeit und die Verständlichkeit der Beweise zu erhöhen. Nennenswert sind die neuen graphischen Darstellungen zu den Beweisen des Satzes von Rice und der Sätze über die Anwendung der Kolmogorov-Komplexität in der Theorie der Berechenbarkeit.

Aachen, im Oktober 2003 Juraj Hromkovič

Wenn du nicht auf das Unerwartete wartest,
findest du nichts Edles,
nichts, was schwer zu finden ist.

Heraklit

Vorwort zur dritten Auflage

Gleich am Anfang möchte ich mich bei den zahlreichen Kollegen bedanken, die sich Zeit für das Lesen und Kommentieren der zweiten Auflage genommen haben. Dabei war der am häufigsten geäußerte Wunsch, zusätzlich das Thema Grammatiken zu behandeln. Obwohl dieses Thema bereits sehr gut in mehreren Lehrbüchern behandelt wurde,[1] enthält die dritte Auflage nun ein neues Kapitel über Grammatiken und die Chomsky-Hierarchie. Somit bietet dieses Lehrbuch den Dozenten ein fast vollständiges Angebot an klassischen Themen, das durch einige neuere Konzepte bereichert wird. Auf diese Weise ist dieses Material sowohl für die Kollegen geeignet, die sich auf die klassischen Grundlagen der Informatik konzentrieren, als auch für diejenigen, die in der Einführungsveranstaltung über „Theoretische Informatik“ nicht-klassische Gebiete vorstellen wollen.

Das neue Kapitel stellt Grammatiken als Mechanismen zur Erzeugung von Wörtern vor, und somit als eine Alternative zur endlichen Darstellung von Sprachen. Die Schwerpunkte liegen auf dem Studium von kontextfreien Sprachen, die von zentralem Interesse für den Compilerbau sind, und auf der Äquivalenz zwischen Grammatiken und Turingmaschinen. Das Kapitel über Grammatiken steht ganz am Ende des Buches, aber dies bedeutet nicht, dass man dieses Thema am Ende der Veranstaltung präsentieren müsste. Die Teile über reguläre und kontextfreie Grammatiken können direkt im Anschluss an Kapitel 3 über endliche Automaten behandelt werden. Nach Kapitel 4 über Turingmaschinen hat man schon alle notwendigen Vorkenntnisse, um das ganze neue Kapitel zu meistern.

Wir sind der Meinung, dass es für eine erfolgreiche Vorbereitung auf eine Prüfung notwendig ist, beliebige Teile des Lerntextes inhaltlich korrekt wiedergeben zu können und leichte Abwandlungen der im Buch vorkommenden Aufgaben lösen zu können. Um die wichtigsten Grundkenntnisse hervorzuheben und dem Studierenden eine Selbstkontrolle zu ermöglichen, haben wir die Zusammenfassungen am Ende der Kapitel um eine Liste von Kontrollfragen erweitert. Wir empfehlen allen Dozenten zusätzlich, die genauen Anforderungen für das Studium gemäß ihrer eigenen Zielsetzungen schriftlich festzuhalten.

[1] Dies war auch der Hauptgrund, warum wir auf die Darstellung dieser Thematik in den ersten zwei Auflagen verzichtet haben.

Außer der oben beschriebenen Erweiterung wurden an einigen Stellen Korrekturen und verbesserte Erklärungen eingearbeitet. In diesem Zusammenhang möchte ich mich bei Christoph Zimmerli und Laurent Zimmerli für ausführliches Korrekturlesen der zweiten Auflage herzlich bedanken. Bester Dank geht an Hans-Joachim Böckenhauer und Julian Tschannen für sorgfältige Korrekturen des neuen Kapitels und an Martin Jaggi und Philipp Zumstein für einige Verbesserungsvorschläge. Bei Nicolas Born und Manuel Wahle bedanke ich mich für ihre Unterstützung bei der LaTeX-Bearbeitung der dritten Auflage. Besonderer Dank geht an Ulrich Sandten vom Teubner Verlag für eine sehr gute und konstruktive Zusammenarbeit, in der keine Tabus für neue Wege gegolten haben.

Mein herzlichster Dank geht an Karl Frey. Seine didaktischen Konzepte waren für mich die interessanteste fachdidaktische Auseinandersetzung und die größte didaktische Bereicherung in den letzten drei Jahren.

Zürich, im Juni 2007 Juraj Hromkovič

Die Kreativität
ist eine Abweichung von der Norm
bei einer vollständigen Beherrschung der Norm.

Juraj Popovňák

Vorwort zur vierten Auflage

Die vierte Auflage beinhaltet keine wesentlichen Änderungen im Vergleich zur dritten Auflage. Dafür wurden aber zahlreiche kleine Verbesserungen vorgenommen. Hier möchte ich meinen besten Dank an Bernhard Brodowsky, Martin Kaufmann, Noah Heusser, Enrico Kravina, Oli Frank, Simon Eugster, Ilya Vassilenko, Jan-Filip Zagalak und Philipp Zumstein für das aufmerksame Lesen und Kommentieren der verbesserungswürdigen Stellen richten.

Ein besonders herzlicher Dank geht an Emo Welzl für mehrere Jahre erfolgreicher Zusammenarbeit bei der gemeinsamen Durchführung der Vorlesung „Theoretische Informatik“ an der ETH und an Dennis Komm und Björn Steffen für die unaufhörliche Hilfe bei den ständigen Versuchen, die Lehrunterlagen und somit auch dieses Buch zu verbessern.

Zürich, im September 2010 Juraj Hromkovič

Die Vollkommenheit
besteht aus Kleinigkeiten,
doch die Vollkommenheit selbst
ist keine Kleinigkeit.

Michelangelo

Vorwort zur fünften Auflage

In dieser Auflage wurden viele kleinere Verbesserungen eingearbeitet, während sich der Inhalt des Buches im Wesentlichen nicht geändert hat. Ferner wurde die Darstellung vollständig überarbeitet. Was hinzugekommen ist, ist überwiegend kontextuelles Wissen, das es ermöglicht, die Informatik und die Mathematik als starke Forschungsinstrumente zur Wissensgenerierung mit ihren Möglichkeiten und Grenzen anzusehen. Die Darstellung der Informatik im Rahmen der Entwicklung der gesamten Wissenschaft ermöglicht es, die Einführung in die Informatikgrundlagen, die vorher von manchen als zu mathematisch-technisch und somit oftmals langweilig empfunden wurde, als eine faszinierende Entdeckungsreise zu gestalten.

Herzlich bedanken möchte ich mich bei Knut Baganz, Joël Bohnes, Jérôme Dohrau, Manuela Fischer, Manuel Kohler, Sacha Krug, Benjamin Richner, Hannes Rösti, Jasmin Smula, Björn Steffen, Emo Welzl, Jochen Zehnder und ganz besonders Daniel Schmitter für unzählige Verbesserungsvorschläge.

Mein besonderer Dank gilt Hans-Joachim Böckenhauer und Dennis Komm, die enorm viel Zeit und große Sorgfalt aufgewendet haben, um mir viele wertvolle Vorschläge für qualitative Verbesserungen vieler Erklärungen zu unterbreiten, und die bei ihrer Umsetzung mitgewirkt haben.

Zürich, im August 2014 Juraj Hromkovič

Inhaltsverzeichnis