

Juraj Hromkovič

Sieben Wunder der Informatik

Juraj Hromkovič

Sieben Wunder der Informatik

Eine Reise an die Grenze des Machbaren
mit Aufgaben und Lösungen

2., überarbeitete und erweiterte Auflage

Mit Zeichnungen von Ingrid Zámečnicková

STUDIUM



VIEWEG+
TEUBNER

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.

Prof. Dr. Juraj Hromkovič

Geboren 1958 in Bratislava, Slowakei. Studium der Mathematischen Informatik an der Komenský Universität, Bratislava. Promotion (1986) und Habilitation (1989) in Informatik an der Komenský Universität. 1990 – 1994 Gastprofessor an der Universität Paderborn, 1994 – 1997 Professor für Parallelität an der CAU Kiel. 1997 – 2003 Professor für Algorithmen und Komplexität an der RWTH Aachen. Seit 2001 Mitglied der Slowakischen Gesellschaft. Seit Januar 2004 Professor für Informatik an der ETH Zürich.

1. Auflage 2006
- 2., überarbeitete und erweiterte Auflage 2009

Alle Rechte vorbehalten

© Vieweg+Teubner | GWV Fachverlage GmbH, Wiesbaden 2009

Lektorat: Ulrich Sandten | Kerstin Hoffmann

Vieweg+Teubner ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

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.

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: STRAUSS GMBH, Mörlenbach
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8351-0172-2

Für

Urs Kirchgraber

Burkhard Monien

Adam Okrúhlica

Péťa und Peter Rossmanith

Georg Schnitger

Erich Valkema

Klaus und Peter Widmayer

und alle, die sich mit
der Forschung begeistern

lassen





Die Wissenschaft ist innerlich eine Einheit.
Die Aufteilung in einzelne Gebiete
ist nicht durch die Natur der Dinge bedingt,
sondern insbesondere durch die Schranken
der menschlichen Fähigkeiten in dem Erkenntnisprozess.

Max Planck

Vorwort

Dieses Buch ist eine Materialisierung der Vorlesungsreihe „Sieben Wunder der Informatik“, die im Wintersemester 2005/2006 an der ETH Zürich für jedermann angeboten wurde. Viele Menschen verbinden die Informatik nur mit dem Rechner und der Fähigkeit, mit ihm umzugehen. Textverarbeitung, Bildverarbeitung, Suche im Internet und andere Anwendungen gehören zu den Themen des Unterrichts für den Computerführerschein und irrtümlicherweise wird dies in vielen Bildungsbereichen mit dem Informatikunterricht verwechselt. Dabei hat die Nutzung unterschiedlicher Software ungefähr so viel mit der Informatik zu tun, wie das Autofahren mit dem Maschinenbau. Wenn wir also einen Autofahrer nicht automatisch für einen Maschinenbauingenieur halten, sollten wir auch einen Computeranwender nicht als Informatiker bezeichnen. Die erste und ursprüngliche Zielsetzung dieser Veranstaltung war es, die naive Vorstellung über Informatik durch das Bild einer Wissenschaftsdisziplin zu ersetzen, die einerseits ähnlich wie die Mathematik und die Naturwissenschaften die Gesetze entdeckt, nach denen diese Welt funktioniert und so zum allgemeinen Wissen beiträgt, und andererseits die errungenen Erkenntnisse mit Hilfe ingenieurwissenschaftlicher Techniken zur Herstellung unterschiedlicher Produkte nützt.

Obwohl diese Korrektur der Darstellung der Informatik in der Öffentlichkeit und in den Bildungssystemen für mich wichtig und erstrebenswert geblieben ist, verlagerte sich meine Aufmerksamkeit während der Vorbereitung der

„Sieben Wunder der Informatik“ immer mehr in Richtung anderer Prioritäten. Ich wollte das Entstehen der Informatik und ihre Entwicklung als eine spannende Geschichte erzählen. Und zwar nicht als Geschichte einer isolierten Wissenschaft, sondern einer Wissenschaft, die untrennbar mit anderen Wissenschaften verbunden ist, die aus Kenntnissen und Forschungsergebnissen anderer Gebiete schöpft und die andere Wissenschaften durch ihre Errungenschaften bereichert. Meine Idee war es, dass man auf diese Weise durch das Beispiel der Informatik zusätzlich mehr Verständnis für die Art und Weise gewinnen kann, wie allgemein Wissenschaften aufgebaut werden, und dass man so die Dynamik der Forschungsprozesse begreifen lernt. Es wurde mir wichtig zu vermitteln, dass nicht nur die in der Öffentlichkeit popularisierten Resultate und Entdeckungen den Erfolg der Forschung bestimmen, sondern dass die Entwicklung der Fachsprachen und die damit verbundene Begriffsbildung maßgebend für den wissenschaftlichen Fortschritt sind.

Während meiner Bemühungen, diese Ziele zu erreichen, bin ich zu der Überzeugung gelangt, dass die Anstrengung der typischen Ziele von Vorträgen für die Öffentlichkeit, wie beispielsweise das Verständnis der Bedeutung und der Wichtigkeit wissenschaftlicher Resultate zu fördern, für mich nicht zufriedenstellend ist. Ich entschloss mich, die Zuhörer auf die Entdeckungswege so mitzunehmen, dass sie danach fähig wären, selbstständig Teile dieser Wege zu beschreiten und somit die tiefe Begeisterung der Entdecker in einem tieferen Verständnis mitzuerleben. Dazu gehört nicht nur, einfache und anschauliche Darstellungen von komplexen Sachinhalten und Zusammenhängen zu finden, sondern auch die Zuhörer von ihrer passiven Rolle zu befreien. Deswegen beinhaltet dieses Buch viele Aufgabenstellungen, die an den Leser gerichtet sind. Die Aufgaben sind im Buch genau dort platziert, wo es am sinnvollsten ist, sie zu bearbeiten. Die Bemühungen, sie zu lösen, überprüfen und festigen das richtige Verständnis der vorangegangenen Erklärungen oder fordern den Teilnehmer auf, zu versuchen, die gewonnenen Kenntnisse zum selbstständigen Erreichen ursprünglicher Forschungsergebnisse anzuwenden.

Die ausgesuchten Themen gehören nicht nur zu den Meilensteinen der Informatikentwicklung. Sie sind auch wahre „Wunder“ in dem Sinne, dass der Forschungsweg zu ihnen voller unerwarteter Wendungen und spektakulärer Erkenntnisse war und dass sie auf den ersten Blick oft unglaublich erscheinen. Damit bieten diese Themen die Möglichkeit einer spannenden Präsentation, die die Zuhörer oder die Leser emotional in ihren Bann zieht. In welchem Maß dies dem Autor dieses Buches gelungen ist, bleibt Ihnen zu beurteilen.

Hilfreiche Unterstützung Anderer hat zur schnellen Entstehung dieser Materialisierung der Vorlesungsreihe „Sieben Wunder der Informatik“ beigetragen. Mein tiefster Dank gilt Hans-Joachim Böckenhauer und Joachim Kupke für die Mitwirkung bei der Durchführung der Vorlesungsreihe und für die Ausarbeitung der Musterlösungen zu den in den Vorträgen formulierten Aufgaben. Diese Musterlösungen befinden sich zusammen mit meinen Kurzfassungen der Vorträge auf

www.openclass.inf.ethz.ch/programm/archiv/WS2005/aufgaben

und stehen allen Lesern frei zur Verfügung. Wie bei den meisten meiner Bücher hat Hans-Joachim Böckenhauer sein scharfes Auge auf das ganze Manuskript geworfen und ich bin ihm für die vielen seiner Kommentare und Verbesserungsvorschläge sehr dankbar. Ein herzlicher Dank geht an Petra Hieber für die Erfindung des OpenClass-Konzeptes für die Vortragsreihen an der ETH und für ihre Bereitschaft, als Testperson das ganze Buch auf die Verständlichkeit für Nicht-Naturwissenschaftler zu prüfen.

Den mehr als 200 Teilnehmern von OpenClass „Sieben Wunder der Informatik“ danke ich herzlichst für die tolle Atmosphäre. Dank ihrer Begeisterung ist das Buchprojekt zu Stande gekommen. Nicolas Born, Yannick Born und Robin Künzler danke ich herzlich sowohl für die Einbettung des Manuskriptes in LaTeX und die damit verbundene Text- und Bildbearbeitung, als auch für sorgfältiges Korrekturlesen. Ein herzlicher Dank geht auch an das Team des Teubner Verlages für die hervorragende Zusammenarbeit, insbesondere an Ivonne Domnick und Ulrich Sandten, bei denen ich mich für den Zeitdruck entschuldigen muss, unter den ich sie während unserer Zusammenarbeit gesetzt habe. Mein tiefster Dank geht auch an Herbert Bruderer und Erich Valkema für die Diskussionen und für ihre Verbesserungsvorschläge zu den Themen der Manifeste, die am Ende des Buches als Nachworte präsentiert sind. Herzlichst danke ich Ingrid Zámečnicková für ihre originellen Illustrationen und Grzegorz Rozenberg und Arto Salomaa für die Erlaubnis, die Illustrationen aus ihren Büchern verwenden zu dürfen.

Ich wünsche Ihnen viel Spaß und aufregendes Lesevergnügen.

Zürich, August 2006.

Juraj Hromkovič

Vorwort zur zweiten Auflage

Inhaltlich unterscheidet sich die zweite Auflage kaum von der ersten. Es wurden jedoch viele kleine Verbesserungen vorgenommen, insbesondere was die Qualität der graphischen Darstellungen betrifft.

Für die Korrekturen und die Verbesserungsvorschläge möchte ich mich herzlich bei allen bedanken, die mir geschrieben haben. Besonders Aussagen aus Leserbriefen wie „Dieses Buch zu lesen ist spannender als ein Detektivroman.“ haben mir viel Freude bereitet. Mein besonderer Dank geht an Yannick Born und Björn Steffen für die Hilfe bei der Bearbeitung des Manuskripts und eigene Verbesserungsvorschläge, sowie an Jela Skerlak für das Zeichnen von neuen Abbildungen. Herzlichst bedanke ich mich auch bei Kerstin Hoffman und Ulrich Sandten von Vieweg+Teubner für die wie immer ausgezeichnete Zusammenarbeit mit einem nicht unbedingt einfachen Autor.

Den neuen Leserinnen und Lesern wünsche ich viel Vergnügen beim Lesen.

Zürich, September 2008.

Juraj Hromkovič

Inhaltsverzeichnis

| | |
|---|------------|
| 1 Eine kurze Geschichte der Informatik, oder: Warum Informatik nicht nur ein Führerschein zur Computerbenutzung ist. | 1 |
| 1.1 Was erfahren wir hier? | 1 |
| 1.2 Grundbausteine der Wissenschaften | 2 |
| 1.3 Das Ende einer Euphorie | 17 |
| 1.4 Geschichte der Informatik | 21 |
| 1.5 Zusammenfassung | 30 |
| 2 Algorithmik, oder: Was hat Programmieren mit Kuchenbacken gemeinsam? | 33 |
| 2.1 Was erfahren wir hier? | 33 |
| 2.2 Algorithmisches Kuchenbacken | 34 |
| 2.3 Und wie geht es mit einem Rechner? | 40 |
| 2.4 Unbeabsichtigt endloses Arbeiten | 56 |
| 2.5 Zusammenfassung | 62 |
| 3 Unendlich ist nicht gleich unendlich, oder: Warum die Unendlichkeit in der Informatik so unendlich wichtig ist | 67 |
| 3.1 Wozu brauchen wir die Unendlichkeit? | 67 |
| 3.2 Das Konzept von Cantor | 70 |
| 3.3 Unterschiedliche unendliche Größen | 99 |
| 3.4 Zusammenfassung | 105 |
| 4 Berechenbarkeit, oder: Warum gibt es Aufgaben, die ein durch Programme gesteuerter Rechner nie lösen kann? | 109 |
| 4.1 Zielsetzung | 109 |
| 4.2 Wie viele Programme gibt es? | 110 |
| 4.3 JA oder NEIN, das ist die Frage | 116 |
| 4.4 Die Methode der Reduktion | 123 |

| | | |
|----------|--|------------|
| 4.5 | Zusammenfassung | 143 |
| 5 | Komplexitätstheorie, oder: Was kann man tun, wenn die gesamte Energie des Universums zum Rechnen nicht ausreicht? | 149 |
| 5.1 | Einleitung in die Komplexitätstheorie | 149 |
| 5.2 | Wie misst man die Berechnungskomplexität? | 151 |
| 5.3 | Komplexität von Algorithmen | 156 |
| 5.4 | Die Grenzen der praktischen Lösbarkeit | 160 |
| 5.5 | Wie erkennt man ein schweres Problem? | 164 |
| 5.6 | Zu Hilfe, ich habe ein schweres Problem | 175 |
| 5.7 | Zusammenfassung | 179 |
| 6 | Der Zufall und seine Rolle in der Natur, oder: Zufall als Quelle der Effizienz in der Algorithmik | 185 |
| 6.1 | Zielsetzung | 185 |
| 6.2 | Gibt es echten Zufall? | 186 |
| 6.3 | Häufige Zeugen sind hilfreich | 191 |
| 6.4 | Hohe Sicherheitsmaßstäbe | 208 |
| 6.5 | Was haben wir hier entdeckt? | 212 |
| 7 | Kryptographie, oder: Wie man aus Schwächen Vorteile machen kann | 217 |
| 7.1 | Eine magische Wissenschaft der Gegenwart | 217 |
| 7.2 | Vorgeschichte der Kryptologie | 219 |
| 7.3 | Wann ist ein Kryptosystem sicher? | 223 |
| 7.4 | Symmetrische Kryptosysteme | 226 |
| 7.5 | Schlüsselvereinbarung | 230 |
| 7.6 | Kryptosysteme mit öffentlichen Schlüsseln | 237 |
| 7.7 | Meilensteine der Kryptographie | 246 |
| 8 | Rechnen mit DNA-Molekülen, oder: Eine Biocomputertechnologie am Horizont | 251 |
| 8.1 | Vorgeschichte | 251 |
| 8.2 | Wie man ein Labor in einen Biorechner umwandelt | 256 |
| 8.3 | Das Experiment von Adleman | 261 |
| 8.4 | Die Stärken und Schwächen der DNA-Rechner | 269 |
| 9 | Quantenrechner, oder: Das Rechnen in der Wunderwelt der Teilchen | 273 |
| 9.1 | Vorgeschichte und Zielsetzungen | 273 |

| | | |
|-----------|---|------------|
| 9.2 | Die Wunderwelt der Quantenmechanik | 275 |
| 9.3 | Wie rechnet man in der Welt der Teilchen? | 283 |
| 9.4 | Was bringt die Zukunft? | 292 |
| 10 | Wie man gute Entscheidungen für eine unbekannte Zukunft treffen kann, oder: Wie man einen gemeinen Gegner überlisten kann | 297 |
| 10.1 | Was wollen wir hier entdecken? | 297 |
| 10.2 | Qualitätsmessung von Online-Algorithmen | 299 |
| 10.3 | Eine zufallsgesteuerte Online-Strategie | 309 |
| 10.4 | Zusammenfassung | 326 |
| 11 | Physikalische Optimierung in der Informatik, Heilung als Informationsverarbeitung in der Medizin, oder: Wie könnten die homöopathischen Arzneimittel wirken? | 329 |
| 11.1 | Glaubwürdigkeit der Wissenschaftstheorien | 329 |
| 11.2 | Optimierung der Kristallstruktur | 332 |
| 11.3 | Optimierung in der Informatik | 335 |
| 11.4 | Heilung als algorithmische Optimierung | 339 |
| 1. | Nachwort | 345 |
| 2. | Nachwort | 353 |
| | Literaturverzeichnis | 357 |