当代科学前沿论丛

计算复杂性导论

堵丁柱　葛可一　王　洁

高等教育出版社

内容提要

计算复杂性理论是用数学方法研究使用数位计算机解决各种算法问题困难度的理论。本书对计算机科学中这一重要理论做了全面的介绍。其内容包含基本理论，如计算模型 *NP* - 完全性，以及较深入的课题，如线路复杂性、概率复杂性和交互证明系统等。此外，本书还包括了复杂性理论近年来两个较重大的突破，即概率可验证明及其在近似算法上的应用和平均 *NP* - 完全理论。本书中所有结果均有严格的数学证明，在每章后配有相关练习题。

本书可用作计算机专业、计算数学专业的计算机理论课程的教材，也是有关研究人员不可或缺的参考书。

图书在版编目（CIP）数据

计算复杂性导论 / 堵丁柱，葛可一，王洁. —北京：高等教育出版社，2002.8
ISBN 7-04-011307-4

Ⅰ.计… Ⅱ.①堵…②葛…③王… Ⅲ.计算复杂性－高等学校－教材 Ⅳ.TP301.5

中国版本图书馆 CIP 数据核字（2002）第 057095 号

计算复杂性导论
堵丁柱　葛可一　王　洁

出版发行	高等教育出版社	购书热线	010－64054588
社　　址	北京市东城区沙滩后街 55 号	免费咨询	800－810－0598
邮政编码	100009	网　　址	http://www.hep.edu.cn
传　　真	010－64014048		http://www.hep.com.cn
经　　销	新华书店北京发行所		
印　　刷	国防工业出版社印刷厂		
开　　本	787×960　1/16	版　　次	2002 年 8 月第 1 版
印　　张	25	印　　次	2002 年 8 月第 1 次印刷
字　　数	370 000	定　　价	52.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

《当代科学前沿论丛》专家委员会

(按姓氏笔画为序)

（国内部分）

王　夔　冯　端　师昌绪　曲钦岳　朱清时
孙　枢　李三立　李大潜　李国杰　杨芙清
吴建屏　邹承鲁　张尧庭　陈　竺　陈佳洱
陈希孺　陈宜瑜　周秀骥　姜伯驹　袁亚湘
钱　易　徐光宪　徐端夫　徐冠华　翟中和
戴立信　戴汝为

（海外部分）

王中林　文小刚　邓兴旺　田　刚　丛京生
刘　钧　汤　超　许　田　危　岩　严晓海
李　凯　李　明　邱子强　余振苏　范剑青
周午纵　郑元芳　宫　鹏　俞陆平　袁钧瑛
徐希平　程正迪　鄂维南

作者简介

堵丁柱

1948 年生。中国科学院应用数学所运筹学硕士 (1981)。美国加里福利亚大学圣巴巴拉分校数学博士 (1985)。美国伯克利数学科学研究所博士后 (1985-1986)。美国麻省理工学院助理教授 (1986-1987)。美国普林斯顿大学访问学者 (1990-1991)。现任美国明尼苏达大学计算机科学系教授，中国科学院应用数学所研究员。Journal of Combinatorial Optimization 主编，Book Series of Combinatorial Optimization 和 Book Series of Networks Theory and Applications 主编。主要研究方向为组合优化，计算复杂性，算法分析与设计，计算机和通讯网络。发表论文 130 篇，著书 7 本。1993 年获中国科学院自然科学一等奖。1995 年获中国自然科学二等奖。1998 年获美国运筹和管理学会 CSTC 奖（计算机与运筹学边缘科学奖）。

葛可一

1950 年生。台湾新竹清华大学数学学士 (1972)。美国俄亥俄州立大学数学硕士 (1974)，计算机科学博士 (1979)。现任美国纽约州立大学石溪分校计算机科学系教授。SIAM Journal on Computing 与 Journal of Complexity 编辑。曾主持多项美国自然科学基金会研究课题。主要研究方向为计算复杂性理论，数值计算复杂性和可计算性理论。发表论文 55 篇，著书 3 本。

王 洁

1961 年生。中山大学计算机科学系计算数学专业学士 (1982)，软件专业硕士 (1984)，美国波士顿大学计算机科学博士 (1990)。现任美国麻萨诸塞大学罗威尔分校计算机科学系教授，并任网络与系统安全实验室主任。主要研究方向为平均计算复杂性理论，网络与系统安全，应用算法。曾主持多项美国自然科学基金会的课题及美国英特尔 (Intel) 公司的课题。发表论文 70 篇及编书两本。1991 年获美国自然科学基金会科研启动奖，2002 年获英特尔公司大学项目 IXA 研究奖。

出版者的话

人类创造了科学技术，科学技术推动了人类的文明进程。两者的互动影响，今天已达到了前所未有的程度：人类的经济发展和社会进步的需要，为科学技术迅猛的创新，提供了强大的动力；科学技术的发展，在急剧地改变着人类的思维方式、学习方式、工作方式、生活方式、娱乐方式。科学技术已成为强大的社会生产力和巨大的社会资本。现在，每个国家，每个地区，甚至每个单位，都把科学技术创新、科学技术转化为生产力作为头等大事，抢占科学技术制高点，以此来提高自己的综合实力。

新中国成立 50 多年特别是改革开放 20 多年来，随着经济的蓬勃发展，科学技术得到了长足的进步，两弹一星、载人飞船、生物工程、信息技术等正在大步追赶国际先进水平。科学技术转化成的强大生产力，对国民经济发展和社会进步、对增强综合国力产生了重大的影响。

改革开放以来，在中国共产党的“科教兴国”方针的鼓舞下，举国上下，尊重科技，学习科技，普及科技，创新科技，应用科技，发展科技，已蔚然成风。科技结硕果、神州尽彩虹的绚丽画面，正在展示于世人面前。自 16 世纪中叶中国科学技术失去世界领先地位后所形成的中西科学技术的差距，现在正在缩小。重振中华科学技术雄风的序幕已经拉开。

为了能使我国的科学技术水平在不久的将来赶上并达到世界先进水平，我们不仅要自己进行科学技术创新，也要学习世界上一切国家的先进科学技术；不仅要靠国内的科技工作者发展我国的科学技术，还要借助海外学者特别是华人学者的力量。在这种思想的指导下，我们萌生了组织海外学者编写科技前沿丛书的想法。这一想法在海内外学者中引起了强烈的反响：在他们中，有的出谋献策，有的出资开会，有的撰搞，有的审稿，有的愿把稿酬作为基金，……海内外学者的诚言乐行，极大地感染着我们，鼓舞着我们；这一想法得到了教

育部陈至立部长和分管我社的周远清副部长的肯定和支持，这增加了我们开展此项工作的决心和信心。根据各方面意见，经过反复研究，最后将丛书定名为《当代科学前沿论丛》。《论丛》是我们献给祖国母亲的21世纪的圣礼，企盼我国能在21世纪夺回三四百年前失去的科学技术领先的地位。《论丛》如能在推动我国科学技术进步和“科教兴国”中有所作用，将是我们的最大欣慰。为了做好本《论丛》的出版工作，我们邀请了国内一些著名科学家和在海外工作的部分优秀学者组成《论丛》的专家委员会，帮助筹划、组织和评议《论丛》的出版。随着学科的发展，专家委员会的成员可能会有所变化。我们向一切关心和支持《论丛》出版工作的人士，表示衷心的感谢。由于缺乏经验，《论丛》出版后，编辑出版方面的不足，在所难免，诚望各方指正。

高等教育出版社

2000年6月

前 言

计算复杂性是计算机理论中极其重要的一个领域。它不但包含了一个完整独立而且内容丰富的理论，同时也对许多其它有关的计算机和应用数学领域产生了重大的影响。

计算复杂性理论发源于 20 世纪 60 年代，以有多项式时间上界的图灵机为基本计算模型而奠定了理论基础。在 70 年代初，这门学问由于 *NP*- 完全问题的发现而吸引了人们的注意。简单地说，如果一个问题无法在多项式时间内被确定型图灵机解决，我们称它为 *难解* 问题。 *NP*- 完全问题 就是一类直观上难解可是又找不出方法来证明它们的确难解的计算问题。从数学的角度来说，这和其它历史上有名的数学问题一样，给予人们一个智力上重大的挑战。而更重要的是，在无数与计算有关的学术领域里， *NP*- 完全问题以各种不同形式层出不穷。因此，这并不是一个纯粹的与世独立的智力游戏，而是对计算机科学有全面影响力的问题。

人们在 70 年代开始对 *NP*- 完全问题的研究主要是横向发展，也就是以许多不同的计算模型来分析难解问题的本质。这些新的计算模型包括了平行计算模型、概率计算模型、布尔线路、判断树、平均复杂性、交互证明系统以及程式长度复杂性等等。对这些新的计算模型的研究一方面使我们对难解问题有了更深一层的认识，一方面也产生了一些预想不到的应用。最显著的一个例子就是计算密码学的革命性突破：基于 *NP* 问题的公钥密码体系。另一个有名的例子是线性规划的多项式时间解的发现。

到了 80 年代中，对 *NP*- 完全问题的研究有了纵向的突破，在许多表面看来并不相关的计算模型之间发现了深刻的刻画关系。这些刻画关系不但解决了几个令人困扰多年的未解问题，同时也刺激了其它相关领域的发展。其中之一是对线路复杂性的研究发现了一些问题在某种有限制的线路模型中必有指数下界。这些结果使用了组合数学与概率方法等新的数学工具，并且解决了一个有

名的有关多项式分层的未解问题。另一个更重大的结果是以概率可验证明对 *NP* 类的刻画。由此得出了许多组合优化问题近似解的 *NP*- 完全性，从而刺激了算法界对近似算法研究的新热潮。这个结果来自于对交互证明系统这个概念的扩展，并且使用了线性代数与编码理论等数学证明技巧。

本书试图对这三十余年来计算复杂性的研究做一个总结。由于以上所介绍的这门学科的多样性，我们在有限的篇幅里对这些结果必须有所取舍。我们取舍的原则是以对 *NP*- 完全问题有深刻理解的结果为主，并且着重于它们最近的发展，以期能启发读者在这些方向上有新的发现，甚或发展出更有意义的新方向。我们对每一个结果都给出完整的数学证明。由于这些证明使用了许多不同的数学概念与证明技巧，这也是一个很好的数学训练。

本书的基本结构如下：我们在前四章介绍计算复杂性的基本概念与各种复杂性类。在后面八章里，我们分别介绍几个对 *NP*- 完全问题的研究方向。第五与第六章讨论 *NP*- 完全问题的线路复杂性和与此相关的 *NP* 类的内部结构。第七到第十章对概率计算复杂性做一个有系统的介绍，由较直观的概率计算模型逐步扩展到交互证明系统与概率可验证明，最后得到 *NP* 类的一个极为简单而漂亮的概率计算刻画。第十一章是这个刻画对 *NP*- 完全的优化问题的应用。在第十二章里，我们介绍一个比较新的、正在积极发展中的平均 *NP*- 完全性理论。这里的平均概念是基于问题实例的概率分布，与第七章的概率计算所使用的基于随机数码的概率分布不同，因而对 *NP*- 完全问题的研究方向也大相径庭。(另外一个与概率计算有深刻关系的量子计算模型与相关的复杂性理论，由于篇幅限制，我们不得不在此割舍。)

本书在编写期间得到美国国家科学基金会对第三位作者的资助 (CCR-982061
CCR-0296037)，在此特表感谢。

堵丁柱 (中国科学院应用数学研究所，美国明尼苏达大学)
葛可一 (美国纽约州立大学石溪分校)
王　洁 (美国麻萨诸塞大学罗威尔分校)

目　录

Contents

第一章　计算模型

算法和复杂性的概念必须建立在计算模型的基础上。在本章中，我们将介绍本书采用的计算模型：确定型图灵机和非确定型图灵机。

1.1　符号行，编码和布尔函数

本书最基本的数据结构是符号行。所有其它的数据结构可编码为符号行来处理。*符号行* 是 *符号* 的有限序列。例如，*complexity* 是个符号行，它是英文符号的有限序列；007 也是个符号行，它是数字符号的有限序列。符号是不能定义的。它们是预先给定的，总共只有有限个，其全体组成的集合称为 *字母表*。并非每个有限集合都能成为字母表。一个有限集合 S 可以成为字母表，当且仅当它满足如下性质：

性质 1.1. *两个由 S 中元素组成的有限序列等同，当且仅当两序列的元素个数相等并且对应元素相同。*

例如，$\{0,1\}$ 和 $\{00,01\}$ 都可以做字母表，但是 $\{1,11\}$ 不能做。对 $\{1,11\}$ 来说，11 是一个元素组成的序列，也是两个元素组成的序列。

设 Σ 是字母表。由 Σ 上符号行组成的集合称为 *语言*。由语言组成的族称为 *语言类*，或简称 *类*。

符号行 x 的 *长度* 是 x 中符号个数，记为 $|x|$。例如，$|complexity| = 10$，$|007| = 3$。为方便起见，我们允许一个符号行不含任何符号。这个符号行称为 *空符号行*，记为 λ。因此，$|\lambda| = 0$。（注意，如果 S 是个集合，那么我们用 $|S|$ 表示 S 的元素个数.）

符号行有个重要运算 ——*连接*。连接两个符号行 x 和 y 的结果是符号行 xy。连接满足结合律，亦即 $x(yz) = (xy)z$。此外，$\lambda x = x\lambda = x$。这样一来，所有 Σ