

新世纪计算机专业系列教材

# 计算机算法引论

## ——设计与分析技术

刘璟 编著

1.6

 科学出版社  
www.sciencep.com

新世纪计算机专业系列教材

# 计算机算法引论

——设计与分析技术

刘 璟 编著

科学出版社

北京

## 内 容 简 介

本书是一本面向计算机、软件工程和网络工程专业及相关专业的本科生(高年级)和研究生教材,根据国内外计算机技术的最新发展,讲述计算机算法的各种设计策略,包括分治技术、贪心技术、动态规划技术、回溯和分支限界技术等;介绍算法分析技术、算法的时间和空间复杂度分析方法,包括最坏情况和平均情况的分析等;讨论各类经典和应用问题的算法,包括排序算法、搜索算法、字符串匹配算法、图论算法、调度算法、组合优化算法、数论算法等。并在计算复杂性理论的基础上,引入近似算法、概率算法等最新内容。

### 图书在版编目(CIP)数据

计算机算法引论:设计与分析技术/刘璟编著. —北京:科学出版社,2003  
(新世纪计算机专业系列教材)

ISBN 7-03-011741-7

I. 计... II. 刘... III. 电子计算机—算法理论—高等学校—教材  
N. TP301.6

中国版本图书馆 CIP 数据核字(2003)第 054673 号

策划编辑:陈晓萍/责任编辑:丁 波  
责任印制:吕春珉/封面设计:王 浩

科学出版社 出版

北京东黄城根北街16号

邮政编码 100717

<http://www.sciencep.com>

双青印刷厂印刷

科学出版社发行:各地新华书店经销

2003年9月第 一 版 开本:787×1092 1/16

2003年9月第一次印刷 印张:17 3/4

印数:1—5 000 字数:397 000

定价:24.00元

(如有印装质量问题,我社负责调换<双青>)

# 新世纪计算机专业教材 编委会

## 顾问编委

施伯乐教授	复旦大学
白英彩教授	上海交通大学

## 主 任

左孝凌教授	上海交通大学
-------	--------

## 编 委

刘 璟教授	南开大学
宋方敏教授	南京大学
何炎祥教授	武汉大学
余雪丽教授	太原理工大学
阮家栋教授	上海工程技术大学
顾训穰教授	上海大学
徐汀荣教授	苏州大学
曾 明教授	西安交通大学
曹元大教授	北京理工大学
曹文君教授	复旦大学
陶树平教授	同济大学
缪淮扣教授	上海大学
谢康林教授	上海交通大学

## 总 序

20年来, 计算机学科的发展日新月异, 促使现代科学在各个领域突飞猛进。目前, 计算机科学技术已应用在实时控制、信息处理、通信传输、企事业管理等领域, 成为人们工作、学习、生活必不可少的工具。计算机技术的发展瞬息万变, 具有以下三方面特点:

(一) 传统的工、理、文、医、商、农在计算机的应用方面都有着各自专业的需要, 例如, 经济、艺术、法律、管理、医学等各种学科都需要依赖于计算机技术的应用。除了各自领域的专业实践外, 应用计算机已是各个专业提高效率、发挥潜能、促进发展的必不可少的手段。因此现在很难用传统的工、理、文、医、商、农等去界定学科的分类。

(二) 计算机网络改变了计算机通信的时空距离。计算机应用的发展是与计算机网络的发展紧密相连的。从最初的局域网(LAN)到广域网(WAN), 以至用一种新的方法将LAN和WAN互联起来, 即成为网际网(Internet)。这种网际网的实验原型Internet, 通常缩写为Internet。计算机网将计算机互连起来, 从而使计算机之间可以交换信息, 而且这种信息交换可以在几分钟内就影响到世界各地。计算机网络的发展, 带动了计算机学科在很多领域的拓展。

(三) 现代计算机学科向综合性发展。计算技术发展伊始, 每种学科均以软硬件分类, 泾渭分明。但自网络发展以来, Internet 软件中的两部分变得特别重要和特别具有开创性, 即网际协议(Internet Protocol, 简称IP)和传输控制协议(Transmission Control Protocol, 简称TCP)。这些协议是必不可少的软件系统。但是在网络系统中, 网络的互连必须依靠路由器、服务器、接口插座、调制解调器等硬件设施, 所以计算机网络很难归结为软件或硬件的单一体系。

随着计算机技术的发展, 计算机与通讯、视频、声音等密不可分; 随着多媒体的发展和应用, 计算机科学已经愈来愈成为与数字传输、视频、声、光、电等综合的学科。

尽管计算机技术的发展如此神速、新异, 但像一切新学科的发展一样, 计算机教育水平仍滞后于计算机技术的发展。为了适应计算机教学改革的需要, 我们国内部分重点院校的教授、学者, 在科学出版社的积极鼓励和支持下, 成立了新世纪计算机专业教材编委会。自2000年10月以来, 我们群策群力, 多次探讨了当前教育与技术进展之间的差距, 并且仔细研讨了美国ACM/IEEE-CS公布的*Computing Curricula 2001*的优点与不足, 结合我国计算机教育的实际情况, 提出了编著一套适用于计算机本科专业的励精图治的教材计划。这套教材的选题、定位乃至作者的遴选, 都得到了国内很多著名教授和学者的认同, 并且有很多选题都争取到了一些著名教授亲自参与编写。这套教材立意着重基础, 反映导向, 注重实践。

因此我们在基础课目方面, 首先列选了数据库原理、操作系统、编译程序原理、智能基础等基础教程。这些基础课教材都由一些国内著名学者执笔, 论述内容既注意打好扎实

基础，又注意要反映最新导向，高屋建瓴，使读者迅速接近最新领域。

同时，为了反映导向，我们抓住网络课程作为计算机专业学生的应用基础，编写了一本实用性极强的《计算机网络教程》。这本教材的编著思想是以基础—理论—应用为主线，通信是基础，协议是核心，互连是重点，应用是目标。

其次，为了拓展学生的网络应用本领，我们还安排了电子商务、多媒体应用以及 Web 数据库技术三门应用课程。电子商务和多媒体应用是计算机应用中最为热门的课程，也是拓展性极广的计算机应用领域，应用前景极为广阔。

Web 数据库技术是一种随着互联网技术发展起来的应用技术。它涉及网络、HTTP 协议、Script 语言、动态网页开发平台、远程数据访问技术等各种网络应用技术。目前国内外还无适合教材，因此，编写 Web 数据库技术的教材，可以说是填补了应用领域的一个空白。

在研究美国公布的“计算 2001-CS 教程”中，我们仔细探讨了数据结构这一课程的变化。在“计算 1991 教程”中，数据结构内容明确放在算法与数据结构之中，而“2001-CS 教程”却无数据结构的课程名称，代之以程序设计基础 (Programming Fundamentals)。文件中提到了基本数据结构和抽象数据类型以及面向对象的程序设计等内容。从这里可以看出，数据结构是以程序设计基础作为研究对象的。另外该教程把算法与复杂性作为一个单独课程列出，这一方面说明算法是一种问题求解的策略，另一方面也说明基本算法及复杂性的讨论对于程序设计是多么重要。

为此在这套丛书中我们安排了一个软件课程系列，即开设从语言、数据结构、算法到软件工程的课程。首先我们从面向对象的 C++ 语言入手，进一步讲解语言学概论。主要内容是分析语法结构，掌握语言构成规律，读懂语言文本。任何计算机语言均可触类旁通，这种从结构规律来学会应用的方法，就是以不变应万变，因为从根本上说，尽管计算机语言千变万化，但万变不离其宗。在搞通语言基础上，我们组编了数据结构，或者说是研究程序设计基础。然后是学习基本算法，也就是为了程序设计需要，而进行问题求解，即进行常用算法讨论。为了使开发软件遵循工程管理方法，软件工程的学习将是计算机专业学生规范软件开发的必不可少的训练课程。

我们筹组这套丛书时，希望每本教材都有创意，能引起共鸣，能被关注，能被采纳，能被推广。但是我们也注意到，由于各个学校情况不同，各人观点不同，理解角度也有所不同，所以对教材的选用和编著，不易一致认同。不过我们希望这套教材能够反映当前学校动向，在促进学以致用等方面有所促进、有所推动，更希望兄弟院校的教师、学者能够积极使用，参与讨论，以使本套丛书能够不断修改，日臻完善。

最后我要感谢科学出版社的领导对本套丛书的列选、报审、出版所给予的鼓励和支持。

左孝凌

2001 年 7 月 30 日

# 前 言

“计算机算法设计与分析”作为计算机学科的核心课程,源自 20 世纪 70 年代 D. Knuth 的巨著《计算机程序设计的艺术》(第一卷“基本算法”,第二卷“半数值算法”,第三卷“排序与搜索”)和 A. Aho、J. Hopcroft 与 J. Ullman 合著的《计算机算法的设计与分析》的发表,从那时候开始,“数据结构”、“算法分析”逐渐成为计算机专业本科和研究生的主要课程,有人统计,这两种书在其后发表的论文和专著中被引用次数最多,而 D. Knuth 还因此获得了 1974 年的图灵(Turing)奖,自 1965 年至今,在近四十届图灵奖的颁奖历史中,这是惟一的一次因写了一本影响巨大的书而获奖。现在,算法理论在计算学科领域中的核心地位已逐渐为人们所公认,三十年来,计算机科学技术的几乎每一项新的成就都与算法研究密切相关。

最近几年,我国计算机专业教育得到了前所未有的发展,除了在规模上扩大了几倍之外,在教学内容和课程设置方面,亦有诸多改进,现在人们对于借鉴国外经验尤为注重,例如,IEEE-Computer & ACM 发表的《计算教程 2001》(CC2001)对我国的计算机专业教育产生了很大的影响,它把“算法及其复杂性”列为计算学科的核心课程,这使得算法设计与分析技术的讲授更受重视。一方面在研究生培养计划中,算法及复杂性的知识成为主要必修内容,由于研究生的多数研究工作与算法相关,高水平的算法理论基础成了高质量计算机人才培养的必要条件。另一方面,有关算法的理论与技术的内容正在向本科教学中扩展,这种趋势在近几年越来越明显,过去在大多数计算机本科专业中,有关算法设计的初步知识是在“数据结构”课程中介绍的,目前,这种情况正在发生变化,一种做法是把传统的“数据结构”课程中算法及复杂性的内容充实加强,为了适应这一变化,一些“数据结构与算法”之类的教材已经在国内外出现;许多计算机科学技术专业则采取另一方案,即在“数据结构”课程之外,再开设一门本科生的算法课程,这是一种趋势。除此之外,许多新建的“软件工程”(包括示范性软件学院)、“网络工程”等专业的教学计划中,也多把算法课程放在重要地位。

为适应计算机教育的这种形势,本书的编写遵从下列宗旨。

## 1. 深度

算法的设计与分析技术包含着深入的理论内容,是为培养中高级计算机人才所必需的知识基础,本书不是一种算法查找手册,而是一本要深入浅出地讲授有效算法的设计与分析技术,引导读者了解国内外算法理论和应用的主流和最新发展,并通过对于大量的著名问题的优秀算法实例的讲解,使读者经过消化、理解,获得设计、分析和创新能力的书籍。

## 2. 结构

全书的安排(与目前国内外最好的教材一致)不拘泥于按问题或按设计技术分章分节,这有利于读者由浅入深逐步深入地学习全面的算法知识。第 1 章为绪论,介绍算法理

论的基本概念、基本思考方法、算法的评估标准,以及算法研究的目标和与解决实际问题的关系。第2章以读者比较熟悉的排序问题为例,全面介绍算法的分析技术,并以此为基础,指导读者在后面各章节中用分析的方法评价算法的优劣,从分析结果中得到设计更优算法的启示。第3、5、7、8章,介绍传统的算法设计技术,通过对于大量重要问题算法(包括图论问题、调度问题、选择问题和一些组合问题的算法)的设计,使读者掌握有效算法的主要设计策略。第2、4、6、11章则重点介绍排序、数据检索、字符串匹配和与数据加密相关的数论问题的算法设计问题。在针对具体问题讨论算法设计的同时,又逐步加深整个算法理论的学习,例如,讲排序问题重点结合算法分析技术,讨论检索问题时注意揭示算法与数据结构的密切相关性,数论问题算法的学习则引入了一种称为概率算法(随机算法)的全新技术。第9章概述NP-完全性理论,用较小的篇幅对计算复杂性理论的基本思想给出了一个清楚明晰的严谨描述。在第10和11章中对于近似算法和概率算法的讨论,为读者解决“计算机难解问题”开辟了新的思路和新的途径。

### 3. 层次

为了适应不同的教学需求(如不同的课时数、不同的读者程度等),也为了引导有兴趣的读者深入学习,我们把全部内容分为下面几个层次。

- (1)普通章节为必选的基本内容。
- (2)标“\*”的章节为可选的内容,教师可根据情况选择一部分讲授。
- (3)标“\*\*”的章节为比较深入的内容,可在研究生课程中介绍。
- (4)附录中的内容,可作为有兴趣的读者参考。

例如,我们把第8章“回溯与分枝限界技术”、第10章“近似算法”,第11章“数论算法及其应用”等都列为可选章节,是因为在有些算法教材中也可以不包括这些内容,主讲者可以根据情况有所取舍。有些标“\*\*”的内容,例如“Hash技术的新发展”、“随机二叉搜索树”等内容更适合研究生学习。在第9章,我们采用了一种新的方法引入“不确定算法”与NP类的概念,这有利于避免过多的理论叙述,而把图灵机(TM)和Cook定理的证明放在附录中,以便读者深入学习。

我能够把这本书奉献给读者,仰赖于多方面的帮助,特别应感谢四川大学李万学教授、上海交通大学左孝陵教授、复旦大学朱洪教授的鼓励和指点,感谢研究生王颖、江标为本书编选了各章的习题并完成了全书的图文编辑工作,感谢王刚博士阅读了本书并提出了有益的修改意见,感谢科学出版社陈晓萍编辑为本书的出版所付出的努力。

本书的编写吸收了国内外优秀教材的精华和作者二十年讲授算法设计与分析课程的教学实践经验,力图贡献出一本适应当前教育形势所需要的高质量教材,然而限于水平和精力,错误和不妥之处在所难免,恳请同行专家和阅读本书的老师和同学多多指正。

刘 璟

2003. 4



# 目 录

1 绪论 .....	1
1.1 交通信号灯问题 .....	1
1.1.1 问题 .....	1
1.1.2 实例 .....	1
1.1.3 图着色问题 .....	1
1.1.4 算法设计讨论 .....	3
1.1.5 讨论 .....	4
1.2 什么是算法 .....	5
1.2.1 算法 .....	5
1.2.2 算法与问题 .....	6
1.2.3 算法与程序 .....	6
1.3 算法的评估 .....	7
1.3.1 正确性 .....	7
1.3.2 时间代价 .....	8
1.3.3 空间代价 .....	8
1.3.4 最优性 .....	8
1.4 算法理论的基本概念 .....	9
1.4.1 基本操作 .....	9
1.4.2 问题实例长度 .....	10
1.4.3 复杂度的渐进性质 .....	10
1.4.4 最坏情形和最好情形 .....	11
1.4.5 平均情形和算法的期望复杂度 .....	12
1.4.6 复杂度函数的表示 .....	13
* 1.5 算法的研究与 Moore 定律 .....	15
* 1.6 MAXMIN 问题 .....	17
1.6.1 平凡算法 .....	17
1.6.2 改进一 .....	18
1.6.3 改进二 .....	18
1.6.4 改进三 .....	19
1.6.5 讨论 .....	20
习题 1 .....	22

<b>2 排序算法与算法的分析技术</b> .....	25
2.1 排序问题.....	25
2.2 $O(n^2)$ 阶的排序算法.....	26
2.2.1 选择排序.....	27
2.2.2 插入排序.....	28
2.2.3 起泡排序.....	29
* 2.3 基于相邻元比较的排序算法和希尔排序.....	30
2.3.1 插入排序的最优性.....	30
2.3.2 希尔排序.....	31
2.4 $O(n\log n)$ 阶的排序算法.....	33
2.4.1 快速排序算法.....	33
2.4.2 合并排序算法.....	39
* * 2.4.3 堆排序算法.....	42
2.5 比较排序算法的时间复杂度下界.....	52
2.5.1 判定树模型.....	52
2.5.2 最坏情形.....	53
2.5.3 平均情形.....	54
* 2.6 排序算法的有关研究.....	55
习题 2.....	57
<b>3 分治技术</b> .....	59
3.1 分治策略的思想.....	59
3.2 大整数乘法.....	60
3.3 矩阵相乘的 Strassen 算法.....	61
3.3.1 问题.....	61
3.3.2 分治.....	61
3.3.3 Strassen 的分治方法.....	62
3.3.4 Strassen 算法的描述.....	62
3.3.5 讨论.....	62
3.4 选择问题的线性算法.....	63
3.4.1 问题.....	63
3.4.2 简单算法.....	63
3.4.3 $O(n)$ 阶选择算法的思路.....	64
3.4.4 选择算法.....	64
3.4.5 选择算法 Select 的分析.....	65
* 3.4.6 讨论.....	66
习题 3.....	67
<b>4 数据集合上的搜索算法</b> .....	70
4.1 动态数据集与抽象数据类型.....	70

4.2	二叉搜索树	72
4.2.1	二叉搜索树	72
4.2.2	查询的实现	73
4.2.3	插入与删除操作	75
* * 4.3	随机二叉搜索树	77
4.4	红黑树	79
4.4.1	红黑树的性质	80
4.4.2	RB 树的插入与删除算法	81
* 4.4.3	关于 RB 树的几点讨论	84
4.5	2-3-4 树	85
4.5.1	2-3-4 树及其实例	85
4.5.2	2-3-4 树上的查询操作算法	86
* 4.5.3	2-3-4 树的构造过程	86
4.5.4	2-3-4 树的性能分析	87
* 4.5.5	有关 2-3-4 树的几点讨论	88
4.6	Hash 技术	89
4.6.1	Hash 算法的基本思想与一般模型	89
4.6.2	Hash 函数的设计	90
4.6.3	解决冲突的策略	91
* 4.6.4	Hash 算法的优劣分析	95
* * 4.6.5	Hash 技术的几种新发展	96
	习题 4	102
<b>5</b>	<b>贪心技术</b>	104
5.1	贪心策略的思想	104
5.1.1	付款问题	104
5.1.2	铺砖问题	105
5.1.3	贪心算法的基本思想	105
5.2	背包问题	108
5.3	Huffman 编码	110
* 5.4	多机调度问题的近似解法	115
5.5	单源最短路径的 Dijkstra 算法	117
	习题 5	122
<b>6</b>	<b>字符串匹配</b>	125
6.1	字符串匹配问题	125
6.2	KMP 算法	127
6.2.1	KMP 算法的思路	127
6.2.2	KMP 算法	127
6.2.3	KMP 算法的正确性	129
6.2.4	KMP 算法的分析	130

* 6.2.5	有关 KMP 算法的讨论 .....	130
6.3	BM 算法 .....	131
6.3.1	BM 算法的两种处理思路 .....	131
6.3.2	BM 算法的时间复杂度分析 .....	134
* * 6.3.3	对 BM 算法的进一步讨论 .....	135
6.4	RK 算法 .....	137
6.4.1	RK 算法的思路 .....	137
6.4.2	RK 算法的描述 .....	139
* 6.4.3	RK 算法的分析与讨论 .....	140
	习题 6 .....	141
<b>7</b>	<b>动态规划</b> .....	142
7.1	动态规划的基本原理 .....	142
7.1.1	Fibonacci 数的计算 .....	142
7.1.2	矩阵连乘的顺序问题 .....	143
7.1.3	动态规划算法的基本条件 .....	146
7.2	最优二分搜索树 .....	147
7.2.1	最优二分搜索树问题 .....	147
7.2.2	动态规划算法的思路 .....	149
7.2.3	OBST 算法 .....	150
7.2.4	OBST 算法的复杂度分析 .....	151
* 7.2.5	讨论 .....	151
* 7.3	近似串匹配问题 .....	152
7.3.1	近似串匹配问题的描述 .....	152
7.3.2	动态规划算法的思路 .....	153
7.3.3	动态规划算法 .....	154
7.3.4	算法的复杂度分析与实例 .....	155
7.3.5	讨论 .....	156
	习题 7 .....	157
<b>* 8</b>	<b>回溯与分枝限界技术</b> .....	158
8.1	回溯和分枝限界的基本思想 .....	159
8.1.1	八皇后问题 .....	159
8.1.2	子集合问题 .....	161
8.1.3	回溯与分枝限界算法的基本思路 .....	162
8.2	0-1 背包问题的回溯算法 .....	165
8.2.1	0-1 背包问题 .....	165
8.2.2	回溯策略的解题思路 .....	166
8.2.3	0-1 背包问题的回溯算法 .....	166
8.2.4	算法的复杂度分析 .....	169
8.2.5	一个运行实例 .....	169

8.3	无向图的团集问题 .....	170
8.3.1	团集问题 .....	170
8.3.2	解题思路 .....	171
8.3.3	团集问题的回溯算法 .....	171
8.3.4	算法 Max Clique()的分析与讨论 .....	173
8.4	旅行商问题的回溯算法 .....	173
8.4.1	旅行商问题 .....	173
8.4.2	旅行商问题的回溯算法 .....	174
8.5	分枝限界算法思路的特征 .....	175
8.5.1	0-1 背包问题的分枝限界策略 .....	175
8.5.2	分枝限界算法的优点和缺点 .....	177
8.5.3	用分枝限界算法解旅行商问题的一个实例 .....	178
	习题 8 .....	185
9	计算机难解问题与 $NP$ -完全性问题 .....	187
9.1	一些难解问题 .....	187
9.1.1	图着色问题 .....	188
9.1.2	0-1 背包问题 .....	188
9.1.3	子集合问题 .....	188
9.1.4	装箱问题 .....	188
9.1.5	作业调度问题 .....	189
9.1.6	可满足性问题 .....	189
9.1.7	图的团集问题 .....	189
9.1.8	Hamiltonian 回路问题与 Hamiltonian 路径问题 .....	190
9.1.9	旅行商问题 .....	190
9.2	多项式界与 P 类问题 .....	191
9.2.1	多项式(时间)界 .....	191
9.2.2	问题求解与判定问题 .....	193
9.2.3	P 类 .....	195
9.3	不确定算法与 $NP$ 类 .....	195
9.3.1	问题求解与验证 .....	195
9.3.2	非确定算法与 $NP$ 类 .....	196
9.4	问题的多项式归约和 NP-完全性 .....	199
9.4.1	多项式归约 .....	200
9.4.2	$NP$ -完全性 .....	201
9.4.3	Cook 定理 .....	201
9.5	与 NP-完全问题相关的理论问题与实际问题 .....	204
9.5.1	理论可计算性与实际可计算性 .....	204
9.5.2	"P=NP"问题 .....	206
9.5.3	NP-完全问题的计算处理 .....	207

习题 9 .....	208
<b>* 10 近似算法</b> .....	210
10.1 近似算法的思想与基本概念 .....	211
10.1.1 顶点覆盖问题的近似算法 .....	212
10.1.2 顶点覆盖问题的近似算法 aVertexCover() .....	213
10.1.3 近似算法 aVertexCover() 的复杂度分析 .....	214
10.1.4 算法 aVertexCover() 的近似度分析 .....	214
10.2 装箱问题的近似算法 .....	214
10.2.1 装箱问题 .....	214
10.2.2 装箱问题的近似策略的讨论 .....	214
10.2.3 装箱问题的 FF 策略近似算法 .....	217
10.2.4 bpFFD 算法的复杂度 .....	218
10.2.5 近似算法 bqFFD() 解的最优性分析 .....	218
10.2.6 讨论 .....	219
10.3 旅行商问题的近似算法 .....	220
10.3.1 最近邻点策略 .....	220
10.3.2 最短链接策略 .....	221
10.3.3 满足三角不等式的旅行商问题 .....	223
10.3.4 几点讨论 .....	225
习题 10 .....	225
<b>* 11 数论算法及其在计算机安全系统中的应用</b> .....	227
11.1 RSA 公钥密码系统 .....	227
11.1.1 数据加密的历史及现状 .....	227
11.1.2 公钥密码系统 .....	229
11.1.3 RSA 公钥密码系统 .....	229
11.1.4 公钥密码系统的数字签名功能 .....	230
11.1.5 公钥密码系统与计算机网络安全 .....	231
11.1.6 RSA 公钥密码系统的主要技术问题 .....	232
11.2 判素问题的概率算法 .....	232
11.2.1 判素问题 .....	232
11.2.2 输入长度和算术计算的时间代价 .....	233
11.2.3 基于数论的素数判别概率算法 .....	234
11.3 大素数的获得和 Miller-Rabin 算法的应用 .....	236
11.3.1 素数的稠密性 .....	236
11.3.2 Miller-Rabin 测试算法的时间代价 .....	237
11.3.3 Miller-Rabin 算法判定素数的正确性 .....	237
11.4 加密解密算法 .....	237
11.5 大整数分解与 RSA 系统的安全性 .....	239
11.5.1 整数的因子分解问题 .....	240

11.5.2 Pollard 的 rho 启发式算法 .....	240
习题 11 .....	242
附录 A 递归方程 (递归不等式) 的求解判定方法 .....	243
附录 B 实际性能最佳的排序算法的设计 .....	247
附录 C 计算模型 .....	252
附录 D Cook 定理 .....	256
附录 E 若干数论知识 .....	260
附录 F 算法索引 .....	266
主要参考文献 .....	268

# 1

## 绪 论

算法的理论处于计算机科学的核心地位,同时,它与计算机应用的许多实际问题有着直接的关系,例如,网络技术、多媒体技术、计算机安全技术等,其最关键的部分都是算法设计问题。因此,让我们从一个最常见的应用问题开始,体会算法理论是如何在实际问题中发挥作用的,以及人们如何是进行计算机算法的设计与分析的。

### 1.1 交通信号灯问题

#### 1.1.1 问题

城市中用交通信号灯来管理交叉路口的车辆的通行。现代城市的交通信号管理应达到如下两个目标。

- (1) 每一车辆通过路口时都不会与其他车辆发生冲突。
- (2) 车辆在路口等待通过的时间尽可能少。

一般信号灯的设置方法是确定几个固定相位,在同一相位下允许通过的路线不相交,同时,为了减少等待时间,应使相位数最少。

#### 1.1.2 实例

图 1.1 是一个五叉路口的实例,五条路 a,b,c,d,e 相交在一起,其中 c,e 为单行线,车辆通过该路口时共有 13 种不同路线:

ab,ac,ad,  
ba,bc,bd,  
da,db,dc,  
ea,eb,ec,ed。

各条线路可能相交,也不能不相交,例如,ab 与 dc 不相交,而 ac 与 eb 是相交的。

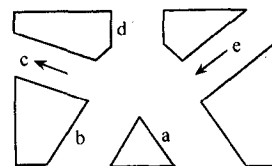


图 1.1 一个五叉路口

把信号灯设置为 13 个相位,每次只允许一条路线通行,当然不会产生冲突,但显然这样效率太低,车辆等待时间过长。把不相冲突的路线放在同一相位,允许同时通过是个好办法。那么,这 13 条路线最少可以分为几个不同相位呢? 故问题归结为,把所有路线分为尽可能少的组,组中的路线互不相交。当然,有的路线可同时出现在不同的组。熟悉算法知识的人会想到,这样的问题实际上是一个图着色问题。

#### 1.1.3 图着色问题

图着色(Graph Coloring)问题是一个经典的组合算法问题,它来源于地图着色问题。



在绘制地图时,总是要求相邻的国家着上不同的颜色以示区别。1852年一位美国大学生古德里(F. Guthrie)提出了一个猜测:为了给任意一个平面地图着色,并使任何有公共边界的区域颜色不同,至多需要四种颜色。这就是四色问题,又称四色猜想。古德里仅仅是提出了这个猜想,他和他的老师都未能证明。二十几年后的1878年,著名数学家凯莱(A. Kayley)发表了一篇“论地图着色”的文章,虽然仍没有解决这个问题,却掀起了四色猜想的研究热。经过一百年的探索,美国伊利诺大学的哈肯(W. Haken)与阿佩尔(K. Appel)通过改进算法,借助计算机(共用了1200个机时)终于在1976年完成了四色猜想的证明。当地的邮局在寄出的信上除了通常的邮戳外,还要加盖“四色是足够的”一句话以表示自豪。

当把地图(Map)上的一个国家与图(Graph)上的一个顶点对应,两个国家的相邻关系对应于无向图上的边,于是,上面关于地图的“四色问题”实际上是无向图的顶点着色问题的特例。

已知: $n$ 点无向图 $G=(V,E), |V|=n$ 。

求: $G$ 的最小色数 $k$ ,使得用 $k$ 种颜色对 $G$ 的顶点着色,可令任意两个相邻顶点着色不同。

着色问题是一个有名的NP-完全问题,我们将在第9章中指出,这类问题属于“计算机难解”问题,关于着色问题算法的研究,许多学者已有大量成果。

类似于地图着色问题,交通信号灯问题也可以归结为图的顶点着色问题。把路口的所有路线表示为无向图的顶点,两个顶点之间有一边连接(当且仅当对应的两条路线在路口相交),而把各个路线划分为尽可能少的互不相交的 $k$ 组,恰恰等价于求相应的无向图的最小色数 $k$ 。

具体的解决方案如下。

无向图顶点着色问题:顶点,边,最小色数 $k$ 。

地图着色问题:国家,相邻关系,最小色数 $k$ 。

交通信号灯问题:路线,交叉关系,最小相位(组)数 $k$ 。

图1.2给出的无向图对应于我们的五叉路口实例,该图有13个结点和20条边,其中 $ba, dc, ed$ 三个顶点是孤立点,说明这三条路线与其他所有路线不相交,就是所谓的“拐小弯”。

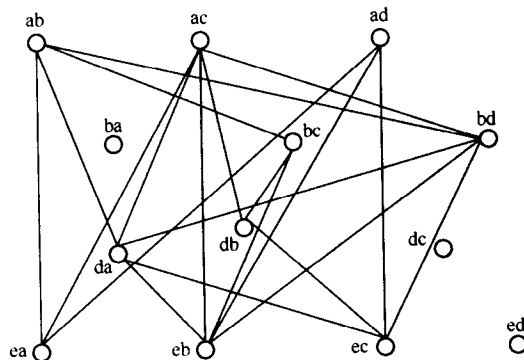


图 1.2 五叉路口信号灯问题对应的无向图