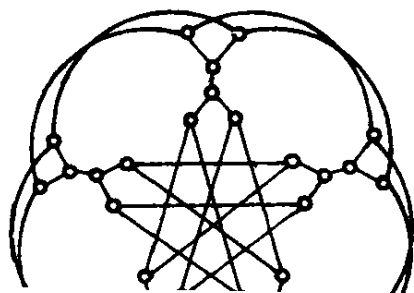


面向 21 世纪高等学校系列教材

离散数学引论

王树禾 著



中国科学技术大学出版社

2001·合肥

内 容 简 介

本书按硕士研究生教材定位写成,供数学、应用数学、计算机科学技术、信息等专业的研究生和需要较深离散数学的本科生选用。全书划分六篇,主要内容如下:

图论与算法图论、组合论、代数系统、数理逻辑、离散数学中的空间、矩阵和拟阵、Turing 机和计算复杂度理论,每篇配有难易适当的足够作业题。

全书概念与理论明晰严谨,注重算法与应用,文字洗练生动,立论深入浅出,可读与可教性强。

图书在版编目(CIP)数据

离散数学引论/王树禾著. —合肥:中国科学技术大学出版社, 2001.9

ISBN 7-312-01300-7

I . 离… II . 王… III . 离散数学-研究生-教材 IV . O158

中国版本图书馆 CIP 数据核字(2001)第 048454 号

中国科学技术大学出版社出版发行

(安徽省合肥市金寨路 96 号,230026)

中国科学技术大学印刷厂印刷

全国新华书店经销

开本:850×1168/32 印张:13.25 字数:340 千

2001 年 9 月第 1 版 2001 年 9 月第 1 次印刷

印数:1—3000 册

ISBN 7-312-01300-7/O·249 定价:18.00 元

序 言

此书是作者在中国科学技术大学数学系和计算机科学技术系多年主讲研究生和本科高年级离散数学课程的教学笔记整理编撰成册的。出书的目的,一是为研究生教学提供一部可读性和可教性都比较强的好用的教材,希望在严谨性、算法分析、实用与现代化诸方面与已发行的同类著作相比有些增广和新意;二是为从事离散数学研究和计算机科技工作的同志提供一部参考书。

计算机科学的掘起,正在从根本上改造着人类生产活动和智能活动的面貌。计算机是一种解决离散系统中的事理与计量的最强大的武器,被称为“计算机数学”的离散数学恰为计算机科学技术的基础。从数学科学的立场来讲,我们的许多基础数学分支,靠手和笔写证明的数学活动已经陷入“推理不变集”,很难做出重大突破,有不少数学家(例如中国的吴文俊、张景中、杨路等)已经开动计算机来搞数学证明,目前发展到了“可读(可视)证明”的新阶段。我们一直坚信微积分及其衍生的后代学科(例如微分方程)是人类科学思维和科学实践的最伟大的成就之一,从 20 世纪 80 年代起,离散数学越来越受到宠爱,有人戏称,微积分在科学中的皇位有朝一日会让给离散数学的。从应用的角度看,很多重大实用项目(例如信息技术、战争、经济等等)的理论模型正是离散数学模型,通过离散数学的理论推导、算法设计与分析、编程与软件制作,上机付诸实现。离散数学是一种高技术。

离散数学是数学领域当中数学思想最为活泼、最为深刻和充满矛盾的地方,对数学基础的奠定与巩固,离散数学有着不可替代

的作用。同时它富含的文化色彩和人文哲理则是人类现代文明的重要成分。离散数学是一种高文化。

可数集合里发生的事的数学方面都是离散数学的研究对象,囿于作者的见识和本书的定位,我们只选了六篇基础性的内容。

第一篇细讲了图论。背景是目前我国在本科生中开设图论课的大学尚不多,但是网络与信息产业的兴起,又要求高层次的科技人才必须多学点图论(亦称网络数学)。把它放在首篇,则是由于它援引其它知识极少,貌似平易近人,而且论证的技巧和结论生动活泼,足以诱发读者学习离散数学的兴趣。它的基本理论则是代数系统与算法分析理论中某些主要内容的预备知识。

第二篇安排的是与图论近缘的组合问题。和图论的遭遇相似,至今在大学里开设组合论者也不太多,所以本书对组合讲得比较细。

数学家并不都是聪明人,但搞图论与组合,不聪明可不行。反过来,通过图论与组合的学习,倒可以使得原本不太灵活者机敏起来,使人获得非平凡的智慧,并为解决离散数学的问题学会不少绝招。

第三篇是思想深刻、内容抽象的近世代数的某些内容。由于数学与应用数学专业的本科生已系统地学过近世代数,本书只对其主要概念进行简要地复习,但对置换群与 Pólya 计数理论,则进行了详细讲述。

第四篇讨论离散数学中的空间、矩阵和拟阵。它们是定量地解决离散数学问题的工具箱,使离散数学算术化,克服离散数学当中定性有余定量不足的缺点。同时用矩阵的观点解决区组设计和正交设计当中的理论问题与实用问题。

第五篇讲了不确定 Turing 机和计算复杂度理论。这是离散数学与计算机科学的核心问题、要害问题。

第六篇讲述数理逻辑。量时量力,只对命题逻辑与谓词逻辑的基本概念与规则进行了入门介绍,要点是讲推理的逻辑过程。

本书证明与解答的细节写得不可谓不细,使用此书做教材的老师们,可只拣要紧的内容讲授,即只须讲清楚思想、思路、关键技术和非一次性的证明方法,其余细节令同学课后阅读,如此可以用80学时完成教学,又可锻炼学生的独立思考能力。对于追求现代科学技术和现代理性的青年同志,劝君多学离散数学。

本书是中国科学技术大学研究生院资助项目,作者对中科大研究生院和中科大数学系给予本书出版的支持深表感谢;还应感谢我的学长陶懋颀教授,陶先生生前与作者有多年的离散数学方面的合作研究,本书的拟阵和图的群等内容就是参考我们旧日的合作工作写出的;感谢科大听我讲课的历届青年朋友们,正是他们的热烈选修和机智提问,促使我深入思考了许多有趣的问题,从而丰富了本书的内容;还应感谢我妻苏仲华,正因为她业余时间承担全部家务,保障了写作时间的足够投入。假若没有这些志同道合者的援助,仅凭我个人的绵薄之力,本书怕是不能问世的。

教材建设当然是为我国教育事业出力的善事,怎奈本书作者智钝才疏,奉献的这部拙作,想必错误不少,盼请各位同仁批评指正。

王树禾

2001年6月于中科大

目 录

序 言

第一篇 图及其算法	(1)
1.1 什么是图论	(1)
1.2 图的定义	(7)
1.3 Brouwer 不动点定理	(12)
1.4 Dijkstra 算法	(14)
习题一	(17)
1.5 树	(22)
1.6 生成树	(26)
1.6.1 生成树的个数	(26)
1.6.2 最优生成树的 Kruskal 算法	(28)
1.7 常用树	(30)
1.7.1 有序二元树	(30)
1.7.2 Huffman 树	(32)
习题二	(35)
1.8 平面图	(37)
1.8.1 平面图及其 Euler 公式	(37)
1.8.2 对偶图和极大平面图	(42)
1.8.3 Kuratowsky 定理	(44)
1.8.4 图的厚度	(46)
习题三	(47)
1.9 纵深搜索和平面嵌入算法	(49)
1.9.1 广度优先与深度优先搜索算法	(49)

1.9.2	求割顶和块的算法	(52)
1.9.3	有向图的 DFS 和极大强连通子图的算法	(54)
1.9.4	平面嵌入算法	(56)
习题四		(63)
1.10	匹配	(64)
1.10.1	匹配理论	(65)
1.10.2	二分图中最大匹配与最佳匹配的算法	(72)
习题五		(76)
1.11	图上遍历	(78)
1.11.1	Euler 图	(78)
1.11.2	求 Euler 回路的算法	(81)
1.11.3	中国邮路问题	(82)
1.11.4	Harmilton 图	(84)
习题六		(91)
1.12	色	(92)
1.12.1	边色数	(93)
1.12.2	顶色数与面色数	(96)
1.12.3	色多项式	(99)
习题七		(103)
1.13	支配集、独立集和 Ramsey 数	(105)
1.13.1	支配集和独立集	(105)
1.13.2	$\alpha(G), \beta(G), \gamma(G)$ 的计算	(106)
1.13.3	Ramsey 数	(110)
1.13.4	多元 Ramsey 数和 Schur 定理	(116)
习题八		(116)
1.14	有向图	(118)
1.14.1	有向图的连通性	(118)
1.14.2	有向轨与竞赛图	(119)

1.14.3	有向圈与竞赛图	(122)
1.14.4	有向 Euler 图	(125)
习题九		(129)
1.15	网络流	(130)
1.15.1	Ford - Fulkerson 最大流算法	(130)
1.15.2	Dinic 最大流算法	(133)
1.15.3	有上下界的网络中的流	(138)
1.15.4	有供需约束的流	(142)
1.15.5	PERT 问题	(143)
1.15.6	流与二分图	(146)
习题十		(148)
1.16	连通度	(153)
1.16.1	无向图的顶连通度	(153)
1.16.2	有向图的顶连通度	(156)
1.16.3	无向图的边连通度	(157)
1.16.4	有向图的边连通度和弱独立外向生成树	(158)
1.16.5	可靠通讯网络	(160)
习题十一		(162)
第二篇	组合基础	(166)
2.1	什么是组合论	(166)
2.2	鸽笼原理	(169)
2.3	+ × 原理与排列组合	(172)
2.3.1	无重复的排列组合	(173)
2.3.2	Catalan 数	(174)
2.3.3	可重复的排列组合	(178)
习题一		(182)
2.4	容斥原理	(184)
习题二		(192)

2.5	生成函数	(193)
2.5.1	生成函数概念	(193)
2.5.2	组合数的生成函数	(194)
2.5.3	拆分自然数	(196)
2.5.4	排列数的生成函数	(199)
	习题三	(202)
2.6	递归方程	(204)
2.6.1	递归方程的初值问题	(204)
2.6.2	线性常系数递归方程的生成函数解法	(205)
2.6.3	常系数线性齐次递归方程的特征值解法	(208)
2.6.4	常系数线性非齐次递归方程的解	(212)
2.6.5	递归方程的其它解法	(212)
2.6.6	Stirling 数	(215)
	习题四	(216)
	第三篇 代数与计数	(219)
3.1	代数系统及其性质	(219)
3.1.1	代数系统的定义	(219)
3.1.2	代数系统的同构与同态	(221)
3.2	群、环、域	(225)
3.2.1	群	(225)
3.2.2	环	(227)
3.2.3	域	(228)
	习题一	(230)
3.3	置换群和循环群	(233)
3.3.1	置换	(233)
3.3.2	置换群与循环群	(237)
3.4	Lagrange 定理和 Burnside 定理	(243)
3.5	Pólya 定理	(247)
	习题二	(252)

3.6 图的群	(253)
3.6.1 图的自同构群	(253)
3.6.2 有限群的 Cayley 图	(259)
习题三	(264)
第四篇 离散数学中的空间、矩阵和拟阵	(266)
4.1 圈空间和断集空间	(266)
4.1.1 圈空间	(266)
4.1.2 断集空间	(269)
4.2 关联矩阵和邻接矩阵	(272)
4.2.1 关联矩阵	(272)
4.2.2 邻接矩阵	(279)
4.3 圈矩阵和割集矩阵	(286)
4.4 开关网络分析	(292)
习题一	(299)
4.5 拟阵	(303)
4.5.1 拟阵的概念	(303)
4.5.2 拟阵理论	(308)
习题二	(312)
4.6 倒称矩阵与层次分析	(314)
4.7 正交拉丁方	(322)
4.8 区组设计与区组矩阵	(327)
4.8.1 BIBD 问题	(328)
4.8.2 区组关联矩阵	(328)
4.8.3 Hadamard 矩阵	(331)
4.8.4 区组设计的构作	(333)
4.9 魔矩阵密码	(336)
习题三	(342)
第五篇 不确定 Turing 机和计算的时间复杂度	(344)
5.1 好算法和坏算法	(344)

5.2	不确定 Turing 机和 NP 类问题	(346)
5.3	NPC 问题和 Cook 定理	(350)
5.4	NPC 中的组合问题	(356)
5.5	NPC 中的图论问题	(360)
	习题	(376)
第六篇	数理逻辑	(380)
6.1	命题逻辑	(381)
6.1.1	命题及其真假	(381)
6.1.2	联结词与命题公式	(381)
6.1.3	真值表	(382)
6.1.4	等价公式、代换定理与对偶定理	(385)
6.1.5	范式	(387)
6.2	命题逻辑中的推理	(390)
6.2.1	蕴含关系	(390)
6.2.2	真值表推理法	(391)
6.2.3	直接推理法	(392)
6.2.4	间接推理法	(393)
	习题一	(393)
6.3	谓词逻辑	(395)
6.3.1	命题的谓词表达形式	(395)
6.3.2	量词	(396)
6.3.3	谓词公式及其变元	(397)
6.3.4	谓词逻辑中的等价定律、代入规则	(399)
6.4	谓词逻辑中的推理	(403)
	习题二	(406)
	参考文献	(409)

第一篇 图及其算法

1.1 什么是图论

图论是离散数学的重要分支.图是指一个离散集 V 与其某些两元素子集的集合构成的一种数学结构,它的数学形象是,在纸上画几个(顶)点,再把其中一些点对用曲线段或直线段连接起来,如此形成的一维网络,其中点的位置与连线的曲直长短可以任意.图显示的是点与点之间的二元关系.

图论是在民间游戏当中孕育和诞生的,创生于 1736 年,欧拉是图论之父.其后的两百年间,这一学科的发展颇为迟缓,因为当时科学技术较为落后,对图论应用的要求甚寡,到 1936 年,匈牙利著名数学家寇尼希(König)发表名著《有限图与无限图理论》和 1930 年波兰数学家库拉托夫斯基(Kuratowsky)证明了平面图(即可以画在平面上,任两条连线不交叉的图)的充分必要条件之后,图论犹如拨亮了一盏明灯,在半个多世纪里,得到了长足的进展,因其在现代数学、计算机科学、工程技术、优化管理等领域和人类生产与社交活动中有大用而独树一帜,在数学营垒中异军突起,急剧发展.事实上,当今科学技术正在面临着新的突破,特别是计算机科学技术与网络化的崛起,要求每个数学家和科学家必须接受足够深入的图论教育,以便有能力去解决大量的网络优化和信息化社会当中离散事物的结构与关系问题.这正是图论日益受宠的背景.

下面用若干具体的图论问题显示图论的风貌.

1. 哥尼斯堡(Königsberg)七桥问题

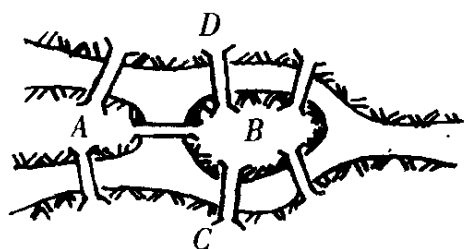


图 1.1

欧洲普瑞格尔河流过古城哥尼斯堡市,河中有岛两座,筑七座桥,如图 1.1. 节假日市民们老幼相携扶,上岛游览散步,不知何日何人提出如下问题:你能过每桥恰一次再返回出发点吗? 反复的奔走实验和总是不能

成功,使人们不知所以然地否定了成功的可能. 1736 年,年方 29 岁的瑞士著名数学家欧拉就此发表图论的首篇论文,严格证明了七桥问题无解. 1736 年遂被公认为图论元年.

2. 哈密顿(Hamilton)周游世界和货郎问题(Traveling salesman problem)对计算机科学的挑战

1857 年,英国数学家哈密顿发明了一种游戏:在正十二面体的 20 个顶点上分别标志上北京、东京、柏林、巴黎、纽约、旧金山、莫斯科、伦敦、罗马、里约热内卢、布拉格、新西伯利亚、墨尔本、耶路撒冷、爱丁堡、都柏林、布达佩斯、安亚伯、阿姆斯特丹、华沙等 20 个遍布全球的大都市,要求从某城出发,沿正十二面体的棱行进,每城恰过一次,再返回出发地. 这个游戏是可以成功的,哈氏当年以 25 枚金币的高价把此项专利出售给了一位玩具商.

哈密顿周游世界的游戏貌似欧拉解决的七桥问题,两者都要求遍历,但七桥问题一次性行遍所有的桥与哈密顿的一次性行遍所有的顶点在难度上一般而言不是同一个级别的问题,后者比前者困难得多! 走遍“桥”的问题已经彻底解决,而一次性行遍顶的问题却是当今数学之中悬而未决的难题,本书将把个中难处讲清楚.

把哈密顿周游世界的游戏推而广之,提出了一个在理论上和实用上皆价值连城的所谓货郎问题:

一位货郎到各村去卖货,再返回出发地,要求每村至少去一次,为其设计一种售货路线,使总耗时最短.

如果把村子进行全排列($abcd$ 与 $dcba$ 认为是一种排列),以

全排列为序分别求出相应的总路程,再从总路程中取用最小值对应的那条售货路线.由于村子个数有限,所以货郎问题的最优解是存在的(未必唯一),而且,如上所云,似乎求取有方.可惜 $\frac{1}{2} \times n!$ 种方案个数过多,即使处理一种排列方案算做一次运算,在每秒百亿次运算的巨型计算机上,对例如 128 个村子,要连续运算 10^{700} 个世纪以上!可见这种愚公移山式的解决方式是绝对应该否定的,应当设计有效的算法,但至今对此仍无本质进展,读完本书之后,就会明白,这类问题(代号为 NPC)也许永世不会有效解决了!

3. 四色问题

1852 年,伦敦的一位叫做高思利(Guthrie)的大学生提出如下猜想:

任给定的无色地图,把每国版图染上一种颜色,使得邻国异色,用四种颜色足矣.

1879 年,英国数学家肯普(Kempe)发表了极为巧妙的论证,宣称证明了四色猜想成立,不幸十年后被指出错误,1890 年,希伍德(Heawood)沿袭肯普的技巧证明了五色定理,即四色猜想中的 4 改成 5 确实成立.1976 年,美国数学家阿佩尔(Appel)和哈肯(Haken)宣布用计算机证实了四色猜想成立,他们用了一百亿个逻辑判断,耗用 1200 多个机时.但这种不可视的机器证明存在用肉眼看不出其真伪的缺点,至于手写的证明,怕是距成功的时日尚远.

粗看四色猜想,平易近人到如此程度,以致于可以向公路上和我们随机相遇的人用不了 3 分钟就能讲清楚题目的条件和要求,即使是文盲,也可以画出许多实例来验证四色猜想对一些特例可以成立,但它的严格证明,百余年间,不知耗尽了多么精干数学家的脑汁,皆不得其果!

4. 拉姆赛问题

1928 年,英国数学家、哲学家、经济学家拉姆赛(Ramsey)在伦敦数学会宣读了一篇数学奇文,提出了所谓拉姆赛数的计算与相

关理论,1930年他因腹部手术并发症不幸逝世,亡年仅仅26岁!但他的关于 Ramsey 数的遗产却永泽数学界,数学家们公认,如果要从离散数学当中选拔一个最精美的成就,那么我们将投拉姆赛理论的票.用图论的方式表述的拉姆赛问题如下:

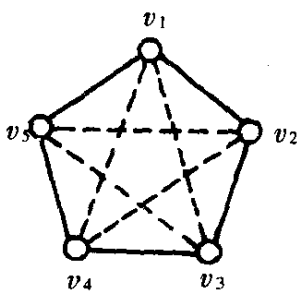


图 1.2

$\forall p, q \in \mathbb{N}$, 把一个画上全部对角线的正 n 边形上的直线段(以此 n 个点为两个端点者)用红与蓝两种颜色任意着色, 每条线段一种颜色, 其结果或者有一个红色 p 边形, 连同其全部对角线皆红色, 或者有一个蓝色 q 边形, 连同其全部对角线皆蓝色, 问 n 最小是多少才能保证出现上述结果?

把上述 n 的最小值记成 $r(p, q)$. 用社交的话来讲, $r(p, q)$ 是任给的人群中必有 p 人相识或有 q 人彼此不相识的人群人数之最小值. 例如 $r(3, 3) = 6$. 事实上, 设 v_1, v_2, \dots, v_6 是任取的 6 个人, 约定两人相识时, 在两人之间连一条红线, 否则, 在两人之间连一条蓝线; 于是与 v_1 相连的 5 条线中至少有三条同色, 不妨设其为红色, 且不妨设这三条红线的另一端为 v_2, v_3, v_4 , 若 v_2, v_3, v_4 三人之间有一条红线, 则与 v_1 一起出现三名彼此相识者, 不然, 即 v_2, v_3, v_4 之间无红线, 则他们三人彼此不相识, 故 $r(3, 3) \leq 6$. 而 5 个人 v_1, v_2, v_3, v_4, v_5 可能出现如图 1.2 所示的关系, 其上实线代表红线, 可见这时不再出现 3 人相识和 3 人不相识的现象, 故 $r(3, 3) = 6$.

$r(p, q)$ 称为拉姆赛数, 经过几代人的奋斗, 加上计算机的帮忙, 迄今只求得 9 个非平凡的 Ramsey 数:

$$\begin{aligned} r(3, 3) &= 6, r(3, 4) = 9, r(3, 5) = 14, \\ r(3, 6) &= 18, r(3, 7) = 23, r(3, 8) = 28, \\ r(3, 9) &= 36, r(4, 4) = 18, r(4, 5) = 25. \end{aligned}$$

著名匈牙利数学家厄尔多斯(Erdős)曾用下面的话比喻计算 Ramsey 数的艰巨性: 某年某月某日, 一伙外星强盗入侵地球, 威胁

道,若不能在一年内求出 $r(5,5)$,他们便灭绝人类!面对如此生死关头,人类应当召集全球所有的数学家和计算机专家,夜以继日地来计算 $r(5,5)$,以求人类免于灭顶之灾;如果外星人威胁说要求得 $r(6,6)$,那我们已别无选择,只能同仇敌忾,对这批入侵者进行先发制人的打击. 1993年,美国罗彻斯特理工学院的 S. P. Radziszowski 和澳大利亚国立大学的 B. D. McKay 用计算机求得 $r(4,5)=25$,相当一台标准电脑 11 年的工作量,是 1928 年以来 Ramsey 数研究当中最不平凡的成果. 我们似不应再有用笔和纸来计算 $r(5,5)$ 的奢望.

5. 伯努利(Bernoulli)一欧拉错放信笺问题

某人给 6 位朋友每人写了一封信,且准备了 6 个写有收信人地址姓名的信封,问有多少种装入信笺的可能,使得每份信笺与信封皆不相符? 把 6 改成 n 如何?

6. 妖怪问题

图 1.3 和 1.4 中的图称为妖怪(Snark graph),在这里妖怪已非社会用语,而是图论中的专业名词,妖怪是这样一类图:(1)每个顶点处关联着三条边;)2)删去三条边不会破裂成两个有边图;(3)最短圈的长(围长)不小于 5;(4)最少用 4 种颜色把它的边着色,使有公共顶点的边异色.

请再画出一个妖怪来!

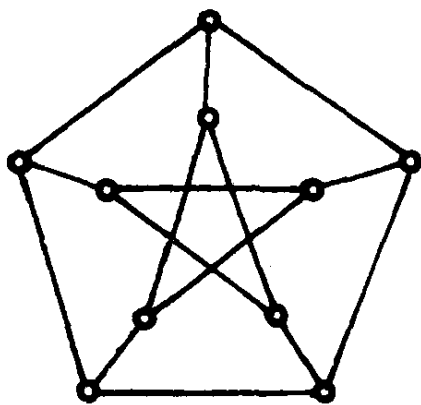


图 1.3

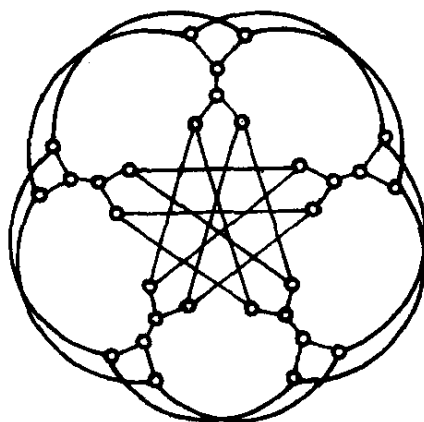


图 1.4

7. 中国邮路问题(Chinese postman problem)

1962年,中国数学家管梅谷提出如下的著名于世的中国邮路问题:

一位邮递员从邮局选好邮件去投递,然后返回邮局.当然他必须经过他所管辖的每条街道至少一次,请为他设计一种投递路线,使其耗时最少.

8. 追捕逃犯问题

1987年,王树禾提出如下追捕问题:

逃犯若干,在公路网上流窜,应至少派几名刑警,才能保证把这些罪犯捉拿归案?

9. 迷宫问题

希腊神话上有一故事:食人人面妖精米诺托担心被他残害的冤魂向他讨还血债,修筑了一座其结构不为外人所知的迷宫,希腊英雄忒修斯立志为民除害,欲沿每条走廊右侧通行,搜索且杀掉妖怪及其帮凶,再由入口退出.请为忒修斯设计一种搜索方法.(注意迷宫结构是未知的!)

10. $3x + 1$ 问题

1950年,卡拉兹(collatz)在麻萨诸塞坎布里奇市世界数学家大会上提出如下的“ $3x + 1$ ”猜想:对任取的自然数 x_0 ,

$$x_1 = \begin{cases} \frac{x_0}{2}, & x_0 \equiv 0 \pmod{2}; \\ \frac{3x_0 + 1}{2}, & x_0 \equiv 1 \pmod{2}, \end{cases}$$
$$x_{n+1} = \begin{cases} \frac{x_n}{2}, & x_n \equiv 0 \pmod{2}; \\ \frac{3x_n + 1}{2}, & x_n \equiv 1 \pmod{2} \end{cases} \quad n = 1, 2, \dots$$

则存在 $x_k = 1$.

厄尔多斯指出:“数学还没有发展到解决这个问题的水平.”

图论中如上述十个问题那样,在理论上、应用上和算法的复杂