第一篇　数 字

在古希腊，没有社会保险号码，没有电话号码，没有人口调查统计数字。没有选举后的投票数字，没有统计数据，也没有 1099 个表格要填。当时，世界还没有数字化，但数字在希腊知识分子的头脑中至关重要。确实，在公元前 6 世纪，萨摩斯的毕达哥拉斯通过研究数字创立了一种宗教，因为，他不仅把数字看成记数的工具，而且看成神圣、完善、友好、幸运及邪恶的符号。数学的一个分支称作数论，研究的是整数的性质，就是由古希腊人开创而且至今不衰的。

以下 3 章专谈数论。在这几章里，我强调指出，某些最古老并且听起来是最为基础的问题仍然悬而未决。虽说其原因尚不清楚，但至今悬而未决这一事实本身却赫然耸立，从而排除了认为数字不过是某种刻板活动的看法。数论曾被视为数学最纯的分支；似乎对现实世界毫无实用价值。然而近年来，数论已变成密码学的一个强有力的工具。不过，正如我在第四章“比尔密码之谜”中所探讨的，至今还存在着数学分析无法破译的传奇密码。

第一章　邪恶的数和友好的数

现为麻省理工学院大学生的米歇尔·弗里德曼，1985 年在布鲁克林高中毕业班就读时春风得意，获得了当年的威斯汀豪斯科学天才奖的第三名。为了他这一获奖项目，他不想用海虾、果蝇或扁虫来弄脏自己的手，也不想处理随便任何一个多年遗留下的理论上的问题。不，他只是挑选了堪称数学上最古老而未决的问题来对付。那是困扰着古希腊人和自那以后的每个人的一个问题：即存在奇数完全数吗？

毕达哥拉斯及其好友认为，整数的完满性，即完全数是任何其所有除数之和（该除数本身外）等于该数本身的整数。第一个完全数是 6。它可被 1、2 和 3 整除并且是 1、2 和 3 之和。第二个完全数是 28。它的除数是 1、2、4、7 和 14，这些数加起来为 28。希腊人所知道的就是这些，尽管他们做过尝试，但没有发现奇数完全数。

圣经评论家注意到，完全数 6 和 28 反映在宇宙的结构中：上帝在 6 天内创造了世界，月亮每 28 天绕地球一周。然而，使这些数字成为完全数的是其本身，而不是凭经验所了解的世界的任何联系。圣·奥古斯丁是这样表述的：“6 本身是一个完全数，并不是因为上帝在 6 天内创造了万物才如此；倒不如反过来说才对：因为 6 是完全数，所以上帝在 6 天内创造了万物。即使不存在 6 天工作一说，6 依然会是个完全数。”

“数学的整个领域都极其散漫，”坦普尔大学数学教授小彼得·哈及斯说，“我研究完全数是出于闲散的好奇心，因为它可能是最古老的未决问题。研究它也许意义不大，然而这一问题如此古老，没有人认为对之进行研究完全是浪费时间。如果这一问题是 5 年前第一次提出来的，那它是决不会令人感兴趣的。”

无论在哪一领域，达到完善总是很难的，偶数完全数也不例外。但是，人们至少知道它们是存在的。我们已发现了 30 个偶数完全数，最大的是一个由 13 万位阿拉伯数字组成的庞然大物：$2^{216,090}$（$2^{216,090}$-1）。也许第三十一个完全数不会出现了，因为早在 2300 多年前数学家就已知道有无穷多的素数（即只能被 1 和它本身整除的数），但在同一时期，他们却不能决定完全数是不是无限的。

要是在俄国茶室或“四季”咖啡馆里喝着可乐会见米歇尔·弗里德曼我会很高兴的，但他宁可让我们在斯替韦桑特中学他的校长办公室中见面，而该校是曼哈顿数学家和科学家的中心。传说，爱因斯坦不能做加减运算，但可在睡梦中研究高深的数学。米歇尔的情况也可以这么说。在选择我们会见时间这种简单的事情中就体现了出来，因为这位杰出的小伙子不适于将中学时间——“第三节”和“第五节”——转换成我们常人所遵照的小时和分钟。然而一旦我们真聚到了一起，这位腼腆的天才就口若悬河地谈论起来，一下成了使人兴趣盎然的人了。

米歇尔告诉我：“去年我为一位数学老师写一篇论文，我知道关于奇数完全数的问题。这问题使我感兴趣，因为它很简单，可还没人找到答案。”接着，米歇尔首先回顾了完全数的历史。

古人只知道 4 个完全数，它们是：6，28，496 和 8，128。欧几里得认识到——大概只有古希腊的神祗才晓得他是如何知道的

完全数	位数
1．21（22-1）=6	1
2．22（23-1）=28	2
3．24（25-1）=496	3
4．26（27-1）=8，128	4
5．212（213-1）=33，550，336	8
6．216（217-1）=8，589，869，056	10
7．218（219-1）=137，438，691，328	12
8．230（231-1）=	19
9．260（261-1）=	37
10．288（289-1）=	54
11.2106（2107-1）=	65
12. 2126（2127-1）=	77
13.2520（2521-1）=	314
14. 2606（2607-1）=	366
15.21，278（21，279-1）=	770
16.22，202（22，203-1）=	1，327
17.22，280（22．281-1）=	1，373
18. 23，216（22.317-1）=	1，937
19. 24，252（24，253-1）=	2，561
20.24，422（24，423-1）=	2，663
21.29，688（29，689-1）=	5，834
22. 29，940（29，941-1）=	5，985
23.211，212（211，213-1）=	6，751
24.219，936（219，937-1）=	12，003
25.221，700（221，701-1）=	13，066
26. 223，208（223，209-1）=	13，973
27.244，496（244，497-1）=	26，790
28. 286，242（286，243-1）=	51，924
29.2132.048（2132，049-1）=	79，502
30. 2216，090（2216，091-1）=	130，100

30 个完全数

这 4 个数是由公式 2^{n-1}（2^n-1）当 n=2，3，5 和 7 时推出来的。算式如下：

n＝2，2^1（2^2-1）=2（3）=6

n=3，2^2（2^3-1）＝4（7）＝28

n＝5，2^4（2^5-1）＝16（31）＝496

n＝7，2^6（2^7-1）＝64（127）＝8，128

欧几里得看出，在全部的 4 个算式中，2^n-1 是素数（3，7，31 和 127）。这种发现促使他证明一个重要的定理：当 2^n-1 为素数时，那么公式 2^{n-1}（2^n-1）则得出偶数完全数。

欧几里得的证明使得完全数理论有了一个兴旺的开端。但由于其他数

学家的短视，这一理论进展缓慢。许多思想精微的人自以为他们看出了数字模式，其实这些数字并不存在。如果他们看得更远一点，他们就会发现这种模式是虚幻的。

古人观察到，前 4 个完全数都是以 6 和 8 结尾的。进一步说，最后一个阿拉伯数字似乎是 6，8，6，8 地交替出现。所以有人推测，完全数最后一个阿拉伯数总会是 6 或 8，并且它们会继续交替出现。第五个完全数——古代人并不知道——的确是以 6 结尾的。但第六个完全数也是以 6 结尾的，这就打破了交替出现的模式。然而，关于最后一个阿拉伯数字总是 6 或 8 这一点，古人还是正确的。今天，数学家可以研究 30 个完全数——比古人多出 7 倍以上——但他们还必须找出尾数为 6 和 8 的模式。

古人还观察到，第一个完全数有一位数字，第二位完全数有 2 位数字，第三个有 3 位数，第四个有 4 位数。所以他们推测，第五个完全数会有 5 位数。在欧几里得故去 17 个世纪后发现了第五个完全数，它赫然具有 8 位数：33，550，336。并且位数继续迅速增多，以下 3 个完全数分别为 8，589，869，056；137，438，691，328；和 2，305，843，008，139，952，128。

欧几里得证明了一旦 2^{n-1} 是素数，那么 2^{n-1}（2^n-1）就会得出一个完全数，但他并没有说 n 的哪一个整数值会使 2^n-1 成为素数。由于使 2^n-1 为素数的前 4 个 n 值为前 4 个素数（2，3，5，7），可能有人推测：如 n 为素数，2^n-1 也会是素数。那么，让我们来试试看第五个素数：11。如 n=11，2^n-1 则为 2，047，而 2，047 并非素数（它是 23 和 89 的积）。真实情况是：要使 2^n-1 为素数，n 必须是素数，而 n 为素数并不就意味着 2^n-1 是素数。事实上，对于 n 的大多数素数值来说，2^n-1 并不是素数。

由 2^n-1 一式得出的数列现在称作默塞纳数列，马林·默塞纳是 17 世纪的巴黎僧侣，他在尽僧职之余抽空进行数论的研究。根据欧几里得的公式，每发现一个新的默塞纳素数，就会自动出现一个完全数。 1644 年，默塞纳自己说，2^{13}-1，2^{17}-1 和 2^{19}-1 这 3 个默塞纳数是素数（8，191；131，071 和 524，287）。这位僧侣还声称 2^{67}-1 这个巨大的默塞纳数会是位素数。在 250 多年的时间里，没有人对这一大胆的声言提出疑问。

1903 年，在美国数学协会的一次会议上，哥伦比亚大学教授弗兰克·纳尔逊·科尔提交了一篇慎重的论文，题为：论大数的分解因子。数学史家埃里克·坦普·贝尔记下这一时刻所发生的事：“一向沉默寡言的科尔走上台去，不言不语地开始在黑板上计算 2^{67}。然后小心地减去 1，得出 21 位的庞大数字：

147，573，952，589，676，412，927。

他仍一语不发地移到黑板上的空白处，一步步做起了乘法运算：

193，707，721×761，838，257，287

两次计算结果相同。默塞纳的猜想——假如确曾如此的话——就此消失在数学神话的废物堆里了。据记载，这是第一次也是惟一的一次，美国数学协会的一位听众在宣读论文之前向其作者热烈欢呼。科尔一声不吱在他座位上坐下。没人向他提任何问题。”

在欧几里得证明他的公式总是得出偶数完全数的大约 2，000 年之后，18 世纪的瑞士数学家伦纳德·尤勒证明，该公式将得出全部的偶数完全

数。这样，我们就可以用另一种方式提出奇数完全数问题：是否存在不是由欧几里得公式得出的完全数呢？

为弄清最近取得的进展，年轻的米歇尔·弗里德曼埋头翻阅过期杂志：《计算数学》、《数论杂志》、《数学学报》及一堆决不会在咖啡桌上看到的其他期刊。他甚至参阅理查德·盖伊的艰深的经典著作《数论中的未决问题》，该书不仅讨论完全数，而且还探讨十几个其他神秘专题：“近超完全数”、“友谊图表”、“优雅图”、“贪婪规则系统”、“纽环游戏”、“达文波特-施尼茨尔系列”、“半友善数”、“友善数”和“不可接触数”。

米歇尔知道，困于这一棘手问题的数论学家们验明：如果真有奇数完全数存在的话，所必须具备的各类特征有：它必须被至少 8 个不同的素数整除，其中最大的一定要大于 300，000，次大的也要大于 1，000。如果奇数完全数不能被 3 除，它至少应被 11 个不同的素数整除。此外，当一个奇数完全数除以 12 时，它应有余数 1；当它除以 36 时，它的余数应该是 9。

我们从这些验证中能得出什么结论呢？对奇数完全数的限制越多，奇数完全数存在的可能性就越小。1973 年，彼得·哈吉斯运用这样的限制条件并借助于计算机肯定地证明了 10^{50} 以下没有奇数完全数。米歇尔从盖伊的书中看到，自 1973 年以来，其他数论家“渐渐地把奇数完全数不可能存在的上限推到 10^{100}，尽管有人对后面这一证明表示怀疑”。

既然与盖伊一样有权威的人对这些证明提出质疑，米歇尔决定重新研究更低限问题。他运用 IBM PC 机及一组限制因素，包括一些文献中极少提到的来自印度的限制因素，证明在 10^{79} 之下不存在奇数完全数，10^{79} 有 8 个素数因数——这是一个奇数完全数所能有的最少的素数因数的数目。

米歇尔说：“我在论文中只是引用了盖伊的话：以前（关于奇数完全数低限很高）的证明是可疑的。当我参加威斯汀豪斯决赛时，我决定检查其他一些证明，但没有发现它们可疑的原因。因此，我给盖伊打了电话，他告诉我，数学家不喜欢由计算机做出的证明，因为你没法知道：编程序的人出继漏了吗？计算机出故障了吗？”

即使该计算机的计算错误（比如说在别的计算机上）被检查出来，但由于那些证明本身常常很长并且很复杂，因而除了原作者没人对它们一步步地仔细加以审查。只有哈吉斯的证明（整整长达 83 页！）曾由其他数学家全面地审查过，并宣布为有充分根据。

米歇尔哧哧地笑了，他不无骄傲地说：“我的证明也是可疑的。威斯汀豪斯的人们不是没有理解就是满不在乎。就我所知，没人真正审阅过我的论文。”

根据他的论文及其他辅助材料，米歇尔成了从多达 1，100 名参赛者中选出的 40 名威斯汀豪斯决赛选手之一。他们 40 人被召到华盛顿，在那儿决出 10 位优胜者。米歇尔解释说：“一旦你来到华盛顿，那几乎就不是根据你的论文来看了。一组科学家对你进行面试，他们会问：‘你如何测出太阳与地球间的距离？你如何测出华盛顿纪念碑的高度？’有一女孩说：‘用卷尺测量。’有位科学家领带上面附有半张元素周期表，他就元素周期表问题向每个人提问。有些人注意到了领带并径直读出答案。我不这样，因此我不得不记住氧的质子数及电子层数。”

米歇尔补充说：“向我们提问的还有一位精神病医生。”我吃了一惊。

“当我谈到精神病医生时，人们都感到吃惊。他向人们询问他们的家庭生活。威斯汀豪斯想发现未来的诺贝尔奖获得者。那才是他们的大事。他们希望在前 10 名中有未来的诺贝尔奖获得者。”米歇尔解释说，过去有 5 名威斯汀豪斯决赛选手（一年有 40 个，并且这种竞赛一直进行了 44 年）获得诺贝尔奖，但这 5 人之中，只有 1 人是前 10 名的。米歇尔耐心地向我解释，威斯汀豪斯这种做法还不如随意选择呢。（每年从 40 名中随意选择 10 名会在前 10 名中产生出 1.25 名诺贝尔奖金获得者。至于怎么会有 0.25 个科学家到斯德哥尔摩去领奖就只能留给数学家去想象了。）那些精神病专家显然是被请来从参赛者中发现获诺贝尔奖人物的苗子，以便提高他们的比例的。

米歇尔接着说：“我的指导人在我的申请中写道，我不会放过一个问题，我是非常固执的。因此，精神病专家就固执一事整整问了我 15 分钟，‘你怎么个固执法？你考虑过固执会给你今后的生活造成损害吗？你是否会就是因为你曾经反对过某些建议而根本拒绝接受呢？’”

既然米歇尔成功地进入了前 10 名，那也许可以说固执是荣获诺贝尔奖桂冠者的部分品性。对威斯汀豪斯（以及米歇尔）来说，不幸的是：没有数学或计算机科学方面的诺贝尔奖。如果他一心要获得这方面的诺贝尔奖，恐怕最终只好去摆弄海虾了。

其实，米歇尔如果放弃完全数会更有利于他的健康。其他研究完全数时间太长的人结果都不可避免地陷入到古人的数字神秘主义中去。文艺复兴时的数学家米歇尔·施蒂费尔和彼得·邦格斯没能解开完全数之谜；施蒂费尔错误地宣称，除 6 以外的所有完全数可被 4 整除，邦格斯也就尾数做出错误的判断。他们在摆弄过数字的完满性之后转向了相反的性质——罪恶，他们是在那个臭名昭著的凶数——666——上发现罪恶的。

华莱士·约翰·斯坦霍普——保罗·内森的科幻小说《牛顿的天赋》中的物理学家——为这一想法所困扰，即牛顿和往日其他科学巨子一定在乏味的数学计算上费了很多的时间。试想一下可怜的牛顿由于算术上的简单错误而无休止地拖延了重力的发现的情形吧！当斯坦霍普发明了一种背囊大小的时间机器时，他决定到 1666 年的英格兰去——当时牛顿正处在他的黄金年华，恰巧，那年还是那场世纪性瘟疫的最后一年——送给牛顿一个袖珍计算器。斯坦霍普的动机无疑是要把牛顿的非凡的大脑从乏味的计算中解脱出来。

可是，牛顿害怕这个计算器，尤其是它通红的数字显示：“上帝是我的救主，它是魔王的发明吗？它的眼睛闪耀着魔鬼王国的颜色呢。”

“你不能不相信你自己的眼睛，”斯坦霍普回答说，“让我演示给你看它是如何工作的。我只要按几个钮就可以给你除两个数。”斯坦霍普随便地按了几个数：81，918 除以 123。当得数亮出来时，牛顿立刻双膝跪倒在地并开始祈祷。然后，他站起来，猛地从火炉中抓起一把烫手的拨火铁棍向斯坦霍普掷去，斯坦霍普这才慌忙逃回到今日的时空坐标中来。

牛顿粗暴的反应可由斯坦霍普不幸选择的数来解释：81，918 除以 123 正巧是 666：凶数。信仰宗教的牛顿在可怕的红灯中惊恐地看到倒下的大天使在他面前悸动的指纹。据说，正是这次与魔鬼的遭遇才促使牛顿写神学著作。

虽然这个精妙的故事是虚构的，但它在精神上与牛顿迷恋于玄奥和超

自然是一致的。牛顿就宗教和神学问题写下了 130 多万字的著作。他写了多方面的文字来解释先知的语言，他无疑对《圣经》关于凶数 666 的预测很熟悉。由于其他研究科学和数学的人都陷于 666 的神秘性中，因此有必要探求一下该数是如何得此恶名的。

在中世纪，一群以希伯来神秘主义哲学家闻名的犹太学者就异教徒指出《圣经》中明显的矛盾、琐屑和谬误做出了睿智的回答。这些哲学家声称，《旧约》中的许多内容是用密码写成的。这是《圣经》显得紊乱的原因。然而，一旦破译出密码，一切都会豁然开朗，神的真谛也就被揭示出来了。破译的主要方法是隐语解法：通过对所有字母进行处理，将一个词或短语转换成数，以预定数值代替每个字母，并算出这些数字之和。他们认为该字母或短语与其他具有相等的和的词或短语有关。

例如，《创世纪》第十八章第二节：亚伯拉罕举目观看，“ 瞧！有 3 个人在对面站着 ”，但没有指明这 3 个人是谁。神秘主义哲学家们运用隐语解法发现这 3 个人是大天使米歇尔、加百列和拉斐尔。如果把希伯来原文的字母“ 瞧！3 个人 ”代之以相应的数，它们的和为 701，与“ 这些是米歇尔、加百列和拉斐尔 ”字母相应数之和相等。神秘主义哲学家们通过类似的数学破译密码法回答了《申命记》第三十章第十二节中提出的问题：“ 谁替我们上天去？ ’这些词的希伯来文所有字母合在一起得出的和与‘ 割礼和耶和华 ”和希伯来语所有字母之和相等，这意味着上帝认为割礼是去向天国的通行证。这种以数学解《圣经》的方法激发了犹太学者对数学的兴趣。

基督教神学家们很快采用了神秘主义哲学家们的神秘分析方法。《新约》本身实际上推动了在姓名与数字之间寻求对应关系的应用，正是在那儿第一次出现了 666 这个数。《启示录》第十三章第十一节警告邪恶力量：“ 我又看见另有一个兽从地中上来。有两个角如同羊羔，说话好像龙。 ”7 行后，我们知道了这只兽是与 666 这个数相关的一个人：“ 在这里有智慧，凡有理解力的人可以计算兽的数字：因为这是人的数字，他的数字是六百六十六。 ”但这人是谁呢？上文所述诱使我们对人名使用隐语解法来确认这头兽。

这头兽是敌基督或假基督。在《圣经》里所记的时代，假基督被认为是罗马皇帝。他通过创立一种异教而对上帝的统治进行挑战，这种异教崇拜皇帝并有自己的教士。《圣经》评论家怀疑这头兽是罗马皇帝尼禄，但要从他的名字中得出 666 来需要经过多次处理。如果把尼禄的名字用希腊语写成尼罗恩，再加上独裁者的称号，然后将独裁者尼禄合译为希伯来文，再将字母转为相应的数字，总数相加之和就是 666。

不管怎样，神奇地把该兽描绘成名数为 666 的人使得一代又一代的占数家绞尽脑汁。在 16 世纪，数学家们也参与其中。德国修道士米歇尔·施蒂费尔研究过代数和数论。他是首先使用加号+和减号-的人之一。他偷偷地把对该兽之数的奇特解释写入一本论代数的经典著作中去。施蒂费尔决心指摘教皇利奥十世的品性，他要对宗座之名进行曲解。

他把十拼成 DECIMUS（拉丁语“ 第十 ”），然后按罗马人的习惯把 U 改为 V 而得 DECIMVS。他从 LEO DECIMVS 中挑选出为罗马数字的字母——L，D，C，I，M 和 V，作为额外增添而从 LEOX 中加进 X。这样，施蒂费尔通过以数代替这些罗马数字而计算出该名字的数值：L（50）＋D（500）＋C（100）

+I（1）＋M（1，000）＋V（S）＋X（10）=1，666。

啊 !多了 1,000。施蒂费尔想,数值为 1,000 的 M 一定是代表 mysterium（神秘）。他从这组字母中除去神秘正好得出了 666。他做出这一发现后背弃了出家人的誓言而成为马丁·路德的追随者。

如果施蒂费尔把注意力集中到该教皇拉丁语尊号之一的罗马数字上，他就会更为令人信服地获得同样的结果，该尊号为 Vicar－ius Filii Dei，其计算结果为：V（5）＋I（1）＋C（100）＋I（1）＋U（5）+I（1）＋L（50）+I（1）＋I（1）＋D（500）＋I（1）=666。

尽管如此，施蒂费尔还是努力获得了他想要的东西。罗马天主教徒为这种叛逆的发现所激怒，威胁要杀死他。1522 年，他避难到路德自己的家中。路德很高兴有一个新的皈依者，但要他忘记占数那玩意儿。施蒂费尔没有理会这一劝告而开始从《圣经》中搜寻世界末日到来的线索。他深信世界末日是 1553 年 10 月 18 日，并到处传播这一消息，结果被捕。随着这一天的临近，他教区的教民倾其积蓄大肆吃喝。而当他们 10 月 19 日一早醒来看到世界依旧平静时，他们想杀死这个骗子，由于路德的干预，施蒂费尔才免于一死。对施蒂费尔来说，一生中面临两次死亡威胁已经够受的了，因此他放弃了预言而全身心地投入到数学中去。结果他成了 16 世纪德国一位杰出的代数学家。

我要补充的是，施蒂费尔对那头野兽的数字的解释并非没有引起争议。他的同时代人、长达 700 页《数的奥秘》一书的作者彼得·邦格斯试图悄悄把该数应用于路德本人。选取马丁·路德的名字 Martin Luther，姓用拉丁语则成 MARTINLUTERA。然后，让 A 至 I 的字母代表 1—9 的数字（I 和 J 按当时的习惯可以互换），K 到 S 的字母代表 10—90（均乘以 10），T 到 Z 代表 100 至 700 的数（均乘以 100）。邦格斯根据字母和数之间的这种联系看出 M（30）＋A（1）＋R（80）＋T（100）+I（9）＋N（40）＋L（20）＋U（200）＋T（100）＋E（5）＋R（80）＋A（1）=666。想想看嘛！

除 666 外，《圣经》为趣味数学提供了许多启示。如果《圣经》中运用的某个数不是像 100 或 1，000 这样的大整数，古人就认为该数有神秘的意义。一般来说，如果一个数被发现有某些别致而简单的算术特征——往往与一连串整数的和或积有关，那么这个特别的数则具有了神秘的意义。例如，在约翰福音的第二十一章第十一节中，耶稣和他的门徒在太巴列海成功地进行了一次捕鱼行动。当他们把那网鱼拖上来时发现有 153 条鱼：“西门·彼得就去把网拉到岸上，那网盛满了大鱼，共 153 条，鱼虽然很多，网却没有破。”153 在数学上有何特殊之处呢？想一想，然后我再透露实情。

首先，153=1＋2＋3＋4＋5＋6＋7＋8＋9＋10＋11＋12＋13＋14＋15＋16＋17。换句话说，它等于 1 至 17 间所有整数之和。

但 153 的魔力还不止这些。它可用另一种重要方式来表示：153=1＋（1×2）＋（1×2 ×3）＋（1×2× 3× 4）＋（1×2×3 ×4×5）。现代数学家会更简练地写出这一等式：153=1！+2！+3！+4！+5！如果一个数后面跟着一个感叹号，你就可以得到从 1 到该数本身所有整数的乘积。这种运算被称作求阶乘。

一位学者大致按照这种方法发现如果把 153 中各位数的 3 次方相加也可得出 153。可简单地表示为，$153=1^3+5^3+3^3$。据数学作家马丁·加德纳

说，1961 年，菲尔·科恩（以色列约纳姆人）告诉英国反传统周刊《新科学家》说，153 潜藏在每个含有因数 3 的数中。我要留给读者自己去推算科恩在《新科学家》中谈及的内容。不过这里有一个提示：选取 3 的任何倍数，计算出其各位数字 3 次方之和。再计算出得数的各位数字 3 次方之和。就这样不断地算下去。

我们再来看看《圣经》中的另一个数：220。《创世纪》第三十二章第十四节记载，雅各布给以扫 220 只山羊（母山羊 200，公山羊 20）以示友好。但为何是 220 呢？毕达哥拉斯的信徒们探求出作为“友好”的特别数字，而 220 则是这些数字中的第一个。友好数的概念是基于人的朋友是一种变相自我这一看法而来。毕达哥拉斯曾说：“一个朋友是另一个我，如同 220 与 284 一样。”这两个数在数学上有何特别突出之处呢？

原来，220 和 284 相互等于对方真除数之和（真除数是能被一个数整除的所有除数[包括 1，但不包括该数本身] 。）220 的真除数为 1，2，4，5，10，11，20，22，44，55 和 110。果然，1＋2+4＋5＋10＋11+20+22+44＋55＋110=284。而 284 的真除数为 1，2，4，71 和 142，它们之和为 220。

虽然古人对友好数很感兴趣，但第二对友好数（17，196 和 18，416）直到 1636 年才由皮埃尔·弗马特发现。到 19 世纪中期，许多有才能的数学家为发现一对对的友好数做了长期而艰苦的努力,结果发现了 60 对友好数。而直到 1866 年，才发现次最小的一对友好数：1，184 和 1，210，它是由一位 16 岁的男孩发现的。

现代数学家将友好数的概念从一组 2 个扩展到一组 3 个。在一组友好的 3 个数中，任何一个数的真除数之和都等于其他两个数之和。103，340，640；123，228，768 和 124，015，008 就是如此。另一组友好的三个数为 1，945，330，728，960；2，324，196，638，720 和 2，615，631，953，920。但对我来说，这种数看起来不像友好数。诚 18 然，如伟大的创造性数学家约瑟夫·马达奇所说，3 个一组的友好数并不易发现，在上面这一组数字中 3 个数分别有 959，959 和 479 个除数。

数学家们虽然注意到了“保障来自反复”这一古老谚语，他们可不是见好就收的人。有人想看看如果选一个数，算出其真除数之和，然后再算出该和的真除数之和，如此往复无穷，会出现什么样的情形。在大部分时间里，计算总是索然无味，但如果你一直这么做下去，就会难得地在某处回到了原来数上。以 12，496 为例，其真除数为 1，2，4，8，11，16，22，44，71，88，142，176，284，568，781，1，136，1，562，3，124 和 6，248。这些数相加，得 14，288。再把 14，288 的真除数相加，得数为 15，472（如果你不相信可以自己试一试！）。再做两次这样的运算，会先后得出 14，536 和 14，264。现在看 14，264 的真除数，它们分别为 1，2，4，8，1，783，3，566 和 7，132。将这 7 个除数相加，噢，你看，是 12，496。如果你不怕浪费时间的话，就从 14，316 这个数开始做同样的运算。你会在 28 轮后重新得出这个数！

第二章　阿基米德的报复

当那位伟大的印度数学家斯里尼瓦萨罗摩奴阇得了结核病住在伦敦医院时，他的同事 G．H．哈迪去看望他。这位哈迪从来就不善于激起谈兴，他对罗摩奴阇说：“我是乘坐出租车来的，车的牌号为 1729。对我来说，这个数字似乎很枯燥，我希望它不是个凶兆。”

“胡说，”罗摩奴阇回答说，“这个数字一点也不枯燥，相反它非常有趣。它是可以用两种不同方式表示的作为两个 3 次方之和的最小数。”（罗摩奴阇不知怎么立即就辨别出 $1729=1^3+12^3$ 和 9^3+10^3。）

罗摩奴阇死于 1920 年，年仅 32 岁。他是一位数论学家，是研究整数属性的数学奇才。数论是数学中最古老的领域之一，在一定程度上说也是最简单的领域。数当然是数学最普遍的基础材料，然而，关于它们仍然还有许多根本问题没有解答。

公元前 3 世纪，当波加的阿波罗尼奥斯天真地继续研究阿基米德的大数时，可能不知晓等待他以及数代数学家的将是什么。“我要让你们看一看谁懂得大数，”阿基米德想。据说，他出于报复之心而虚构出关于牧牛的计算问题，解决这一问题所需的数字是如此庞大，以致直到最近才得以解决。而且，解决这一问题的并不是人而是机器：世界上最快的电脑。

提出类似牧牛这类极其困难的问题只不过是阿基米德许多令人难以置信的功绩之一，这些功绩使他在他那个时代就成了一个传奇式人物。公元前 212 年，罗马将军马塞卢斯围困了西西里的叙拉古港，该城之王希伦请求王亲阿基米德驱逐 60 艘敌舰。阿基米德不久前发明了杠杆（他因此说了这句名言：“给我一个支点，我会搬动整个地球。”），他将杠杆和滑轮结合在一起制成巨大的吊车，这些吊车将那些入侵的战船吊出了港口。在战斗中，吊车还得到弩石弹射器和凸面镜的协助，凸面镜把阳光聚焦到船上使船着火。结果，罗马舰队遭到了毁灭。马塞卢斯说：“我们不要和这个几何怪物进行战斗了，他拿我们的船当杯子，从海中舀水。”

阿基米德使敌人 3 年不敢接近。后来，有一个晚上，当叙拉古人忙于宗教庆典时，罗马士兵攀上城墙并打开城门。当马塞卢斯的军队蜂拥而入时，他告诉部下说：“任何人都不得斗胆对阿基米德妄动一个手指头，这人是我们的座上宾。”

马塞卢斯的一个士兵在庭院中找到阿基米德，其时，阿基米德正在沙地上画几何图形，这位士兵违抗指令而拔出了剑。阿基米德请求说：“我的朋友，在你杀死我之前，请让我把我的圆画好。”这位士兵没有等待就把剑刺向阿基米德，阿基米德躺倒在地，喃喃地说：“他们夺走了我的躯体，但我将取走我的灵魂。”说完安然死去。

按照阿基米德的愿望，人们在他的墓碑上刻了一个圆柱体，柱体里面是一个球体——象征着他的骄傲的发现：球的体积是装下该球的最小的圆柱体体积的三分之二。

这个传说有多少是真的呢？阿基米德无疑是位机械天才。有充分证据表明他设计出能将 50 磅弩石抛出 300 英尺远的弩石弹射器。但近来对技术史的研究排除了他建造了能从海中吊起敌船的吊车的可能性。这种神话的根据可能是他发明过一种将他自己（不动的）的船吊到岸上来的吊车式的装置。

许多科学巨匠包括加利莱奥·伽利略和法国博物学家布丰伯爵，乔治-路易斯·莱克勒都对阿基米德用镜子焚烧敌船感兴趣，它与儿童用放大镜点燃纸片非常相似。理论上说这种镜子是可以制造的，但它要有一个保持太阳光线聚焦于移动目标上的可变焦距，普通镜子是做不到这一点的。（1747 年，布丰声称用一个复杂的镜子使 150 英尺远的木头着了火，并熔化了 140 英尺远的铅。）不管怎样，阿基米德不会费力去制造一个特别镜子的，因为那时已经出现了一种简单而高效的燃烧武器：将石脑油与一种同水接触即自动燃烧的化学物质相混合装入罐中，人们把这种罐子掷向敌船。

对阿基米德之死的生动描述可能相当真实，尽管人们会对他所说的话表示怀疑。公元前 75 年，伟大的罗马演说家西塞罗来到阿基米德的墓旁，发现墓碑上刻有外切一个球的圆柱体。

牛群的问题是怎么回事呢？它真是首先由阿基米德提出来的吗？别管阿基米德是否真是出于一时赌气而凭空想出这个问题的，人们知道他确曾推算过这个问题，因此至少有 2，200 年的历史了。

这个问题开始是这样的：“啊！朋友，如果你智慧过人，那就专心致志算出那天那群公牛的数目吧。它们曾在西西里岛的大平原上吃草，按毛色它们被分成 4 组：乳白牛、黑牛、黄牛和花斑牛。每组中的公牛数占大多数，它们之间的关系为：

1．白公牛＝黄公牛＋（$\frac{1}{2}+\frac{1}{3}$）黑公牛。

2．黑公牛＝黄公牛＋（$\frac{1}{4}+\frac{1}{5}$）花斑公牛。

3．花斑公牛＝黄公牛＋（$\frac{1}{6}+\frac{1}{7}$）白公牛。

4．白奶牛＝（$\frac{1}{3}+\frac{1}{4}$）黑牛。

5．黑奶牛＝（$\frac{1}{4}+\frac{1}{5}$）花斑牛。

6．花斑奶牛＝（$\frac{1}{5}+\frac{1}{6}$）黄牛。

7．黄奶牛＝（$\frac{1}{6}+\frac{1}{7}$）白牛。”

该问题继续说：“啊！朋友，如果你能算出每群中公牛和母牛的数目，你还是称不上无所不知或精通数字，也不能被列入智者之列。”于是该问题涉及到其数学的本质部分：解 7 个带有 8 个未知数的等式（4 组不同颜色的公牛和 4 组相应颜色的奶牛）。原来，这些等式并不难解。事实上，它们有无限多的答案，而牛群总头数的最小数值为 50，389，082，这些牛可以在西西里 6，358，400 公顷的大平原上自由自在地吃草。

然而，阿基米德并未就此停止。他对公牛数目另外又提出了两项限制条件，从而使这问题变得难多了：

8．白公牛＋黑公牛＝一个平方数。

9．花斑公牛＋黄公牛＝一个三角数。

问题最后说：“如果你已算出这群牛的总数，噢！朋友，你俨然就是

一个征服者了，不消说，你就是数字科学方面的专家了。”

阿基米德的牛群问题由于采用了三角数和平方数的概念而与华达哥拉斯的工作有关。公元前 6 世纪，毕达哥拉斯及其追随者用圆点布置成三角、四方或其他几何图形来表示数。如 3、6 和 10 这些数被称为三角数，因为它们可由构成三角的圆点来表示：

西门从海中拽出的鱼的数目 153 也是一个三角数。由于同样的原因，像 4，9 和 16 这些数被称为平方数，因为它们可以用圆点布置成正方形来表示：

不要以为古人为断定某个特定的数是否可以由特定的几何圆点图形表示而耗费长时间去胡写乱画，要知道，解决这一问题存在一种纯数的方法。所有三角数都可由连续的整数（从 1 开始）相加得出；如 3＝1＋2，6＝1＋2＋3，以及 10＝1＋2＋3＋4。所有的平方数都可由整数的平方得出：4＝2×2，9＝3×3，及 16＝4×4。

由于用三角数和平方数对公牛进行限制，牛问题变得非常棘手，两千年里没有取得真正的进展。1880 年，一位德国研究者在经过枯燥计算之后表明：符合所有 8 项条件的最小的牛头数为一个有 206，545 位数的数，该数是以 776 开头的。阿基米德可能是一个有魔力之人，但他决不是个现实主义者：西西里小岛上决不会容下这样一群牛。正如一位数理论家所说：“即使它们是最小的微生物——不，即使它们是电子，一个以从地球到银河的距离为半径的圆也只能包含这种动物的很小一部分。”

但没人认为缺乏现实感会妨碍数学研究。20 年后的 1899 年，伊利诺斯希尔斯伯勒的一位土木工程师和他的几位朋友组成希尔斯伯勒数学俱乐部，致力于发现余下的 206，542 位数。经过 4 年运算后，他们最后宣布，他们发现了 12 位最右边的数，又另外发现了 28 位最左边的数，但后来证明他们算的数都弄错了。60 年后，3 位加拿大人运用计算机首次发现了全部的答案，但他们从未予以公开发表。1981 年，当出自劳伦斯·利弗莫尔国家实验室的克雷 1 号巨型计算机的 47 页硬拷贝缩印在《趣味数学》杂志上时，全部的 206，545 位数才最终公布于世。

当时，克雷 1 号是世界上运算最快的计算机。克雷巨型计算机是昂贵的——最新型号值 2，000 万美元，实验室和公司不会买它来解决古老的数论问题。购买它是用于配制新的药物，勘探石油，破译苏联密码，在好莱坞电影中造成辉煌的特别效果以及模拟太空武器。

然而，人们常常让巨型计算机解决数论史上棘手的计算问题，以便证明它们是否运转正常。计算这种问题的好处是可以轻易地对其答案——即使以前不知道这些答案——进行检验：将它们还原到其等式中去。阿基米德的牛群问题正是在劳伦斯·利弗莫尔实验室检验克雷 1 号时得以解决的。这台巨型计算机仅用 10 分钟就发现了 206，545 位数的答案，并两次检验了这一问题的运算。

让我们以一个阿基米德曾处理过而我们也许能解决的问题来结束本节吧。希伦给金匠一定量的金子（设其重量为 W）制造皇冠。当希伦收到那顶皇冠时，他请阿基米德鉴定它是否含有全部的金子，或金匠是否偷走了一些而代之以较廉价的金属。公元前 1 世纪著名的罗马建筑师维特鲁威是

这样记载的：“ 阿基米德反复琢磨这一问题，一天他偶然来到洗澡间，在那儿，他注意到，当他坐进浴缸里，漫出浴缸的水的数量等于他浸在浴缸中的身体所排出的水量。这一点向他暗示了解决这一问题的方法，于是他立即欣喜地跳出浴缸，光着身子向家奔去，并大声喊着他已发现了他寻找的东西。因为当他跑的时候，他反复大声地用希腊语叫道，我找着啦！我找着啦！ ”

他找到了什么？阿基米德领悟到：既然金是密度最大的金属，那么，重量为 W 的纯金皇冠的体积会比同样重量搀假的金皇冠的体积要小些。他让一个容器装满水并投进重量为 W 的金子。然后他将溢出来的水收集起来，这些水的体积与该金子的体积相等。下一步他让另一个容器装满水，皇冠在监督之下被放入水中。果然，它排出的水体积较大，证明那位卑劣的金匠偷去了希伦国王的金子。

第三章　素数的滥用

原子说——相信事物不可分割——不仅指导着古希腊人研究物质而且指导着他们对数的研究。欧几里得及其同时代人认识到，某些整数如 2，3，5，7 及 11 是根本不能被除尽的。这些只能被它们自身和 1 整除的数被称为素数。那些不是素数的数——如 4，6，8，9，10 等等——有另外的除数。这些数被称作合成数（非素数），因为它们每个数都各自由某些素数“合成”。例如，4＝2×2，6＝2×3，8＝2×2×2，9＝3×3，及 10＝2×5。

1985 年 9 月，当休斯敦的谢夫隆地球科学公司对被称为克雷 X－MP 型的新式巨型计算机进行使用检验时，它在以每秒做 4 亿次运算的速度工作了 3 个多小时后发现了人（或机器）所知的最大素数。

大约在 2300 年前，欧几里得就证明存在无限多的素数。但迄今还没有人发现素数的模型或产生素数的有效公式。由于没有模型可参照，发现新的最大已知素数没有任何窍门，这一发现的新闻不仅迅速地传遍了数学界而且传遍了整个世界。美国哥伦比亚广播公司《晚间新闻》节目的主持人瓦尔特·克伦凯特专门在电视上插播了一个素数的轻松故事，而全国公共广播电台仍然有这样一个栏目。

谢夫隆计算机求得的创纪录的素数多达 65，050 位数。这个有 65，050 位数的庞大数字是一个梅森数，它等于 2 的 216，091 次幂减 1，要把这个数全部列出来要占去本书 30 页纸。“我们只是偶然地运算了足够的数而得出这一新素数的，”谢夫隆的一位副总裁告诉新闻界说，“让该机器开动并进行运转，证明它健全无损是我的职责，其结果是令人感兴趣的……但这些结果肯定无助于发现石油。”

寻找更大的素数并探求其性质与寻求奇数完全数一样都是数论的一部分。数论表面上简单。其主要定理可以表述得人人都可理解，但证明起来——如果是已知的话——却需要艰深而复杂的数学运算。例如 1742 年，生于普鲁士的数学家克里斯琴·哥德巴赫猜想每个比 2 大的偶数都是两个素数之和。根据这一分析，4＝2＋2，6＝3＋3，8＝3＋5，10＝5＋5 等等。数理论家借助于计算机将 1 亿以下的所有偶数都分成为两个素数之和，然而他们却没能证明哥德巴赫的简单猜想是普遍正确的。而这并不是因为缺乏尝试之故。过去两个半世纪以来，许多最有才能的数学家都曾思考过这一问题。

在数学的所有分支之中，数论传统上一直是最远离物理现实的。数学其他深奥领域的抽象结果似乎已有效地用于物理、化学和经济之中。而对数论中的多数结果来说却并非如此。如果哥德巴赫猜想明天得以证明，数学家会欣喜异常，而物理学家和化学家将不知道如何应用这一成果——如果它确有应用价值的话。因此，研究素数被认为是最纯的数学，与应用无关的数学。几个世纪前，数论的这种纯性为它赢得了“数学皇后”的美称。

然而在今天，这座宫殿里却出了问题。那最纯的论题——素数正在以国家安全的名义滥用自己。据报道我们政府所用的某些最好的密码是依靠素数创制的。在这些密码中，字母被转换成数字，其根据纯然是数学的：某些计算程序较易创制但极难破译。例如，计算机计算两个 100 位数的素数的积极其容易。但已知那个 200 位数的积去恢复那些素数除数却极其困难（当然，除非有人告诉你）。将这一点应用于密码使人茫无头绪。将电

文译成电码的人必不能破解密码。将电文译成电码，他只需知道 200 位数的积。但要破译这段电文他得知道两个素数除数；而只知道其积是远远不够的。

这种密码被称为公钥密码，因为它可以用一种很公开的方式来使用。如果我想收到秘密信件，我只需公布 200 位数的数字（并对如何用于编密进行解释）即可。然后，任何人只要他愿意就可以给我寄编成密码的信。因为只有我一人知道那两个素数除数，因此也只有我才能轻易地破译那些信件。然而，这种密码系统起作用的惟一原因是数论学家迄今依然不知如何将巨大的合成数化成构成它们的素数。

佐治亚大学著名的素数学家卡尔·波梅兰斯说：“这种密码系统是对无知的利用。由于这种密码，更多的人卷入了对数论的研究。而致力于研究分解因子问题（寻找素数除数）而未获成功的数学家愈多，这种密码就愈可靠。”因此，这种密码系统的成功又以另一种方式仰赖于数论：要确认那相乘的 100 位数的素数必须运用尖端的数学方法。

既然素数处于密码学的显要位置，我想考察一下关于素数何为已知的，以及何为未知的。很久以前，欧几里得就证明素数是无限多的。他 2，300 年前的证明依然是数学简明而别致的范例。

欧几里得说，我们假设素数是有限的，那么其中之一——我们称之为 P——就会是最大的。现设有一个比 P 大的数 Q，Q 等于 1 加上从 1 到 P 所有整数的积。换句话说，Q＝1＋1×2×3……×P。对于 Q 来说，很明显，从 2 到 P 的所有整数都不能整除它；每次除都会得出余数 1。如果 Q 不是素数，它就会被某个比 P 大的素数整除。相反，如果 Q 是素数的话，Q 本身就是一个比 P 大的素数。两种可能性都意味着比最大素数还要大的素数的存在。这当然就意味着，“最大的素数”这概念是虚设的。但如果没有这样一个怪数，素数就一定是无限的。

长期以来，数学家们一直梦想着发现一种公式，运用这个公式代入从 0 到无穷大的 n 的整数值就可以得出所有素数。18 世纪的大数学家列奥纳德·欧拉反复考虑用那个诱人的简单公式 n^2+n+41。如 n＝0，该公式则得出素数 41；如 n＝1，得素数 43；n＝2 得素数 47。的确，当 n 为 0 至 39 中连续的整数值时，欧拉公式得出的全是素数。但如 n＝40 时，这一公式突然不灵了。其得数 1，681 是 41 的平方。

n	n^2+n+41	结果	n	n^2+n+41	结果
0	41	素数	23	593	素数
1	43	素数	24	641	素数
2	47	素数	25	691	素数
3	53	素数	26	743	素数
4	61	素数	27	797	素数
5	71	素数	28	853	素数
6	83	素数	29	911	素数
7	97	素数	30	971	素数
8	113	素数	31	1033	素数
9	131	素数	32	1097	素数
10	151	素数	33	1163	素数
11	173	素数	34	1231	素数
12	197	素数	35	1301	素数
13	223	素数	36	1373	素数
l4	251	素数	37	1447	素数
15	281	素数	38	1523	素数
16	313	素数	39	1601	素数
17	347	素数	40	1681	复合数
18	383	素数	41	1763	复合数
19	121	素数	42	1847	素数
20	461	素数	43	1933	素数
21	503	素数	44	2021	复合数
22	547	素数	45	2111	素数

n	n^2+n+41	结果	n	n^2+n+41	结果
46	2203	素数	74	5591	素数
47	2297	素数	75	5741	素数
48	2393	素数	76	5893	复合数
49	2491	复合数	77	6047	素数
50	2591	素数	78	6203	素数
51	2693	素数	79	6361	素数
52	2797	素数	80	6521	素数
53	2903	素数	81	6683	复合数
54	3011	素数	82	6847	复合数
55	3121	素数	83	7013	素数
56	3233	复合数	84	7181	复合数
57	3347	素数	85	7351	素数
58	3463	素数	86	7523	素数
59	3581	素数	87	7697	复合数
60	3701	素数	88	7873	素数
61	3823	素数	89	8051	复合数
62	3947	素数	90	8231	素数
63	4073	素数	91	8413	复合数
64	4201	素数	92	8597	素数
65	4331	复合数	93	8783	素数
66	4463	素数	94	8971	素数
67	4507	素数	95	9161	素数
68	4733	素数	96	9353	复合数
69	4871	素数	97	9547	素数
70	5011	素数	98	9743	素数
71	5153	素数	99	9941	素数
72	5297	素数	100	10141	素数
73	5443	素数			

欧拉公式

1963 年，曾在洛斯阿拉莫斯从事早期原子弹研制性工作的卓越数学家斯坦尼斯劳·乌拉姆在一片纸上随意写出一串数字，它们是连续的整数，从 1 开始呈方形螺旋地向外扩展：

乌拉姆的小草笺

使他震惊的是，草笺中的素数——我已用线标了出来——都落在了对角纸上。乌拉姆受到这种偶然发现的鼓舞便与两个助手马克·韦尔斯和迈

伦·斯坦一起研究从除了 1 之外的整数开始的方形螺线。从 41 到 44 的整数也构成了一个螺线。同样，素数也常常落在对角线上。从 421 至 383 这条长对角线与由欧拉的 n^2+n+41 的公式所得出的素数是相对应的。

421	420	419	418	417	416	415	414	413	412	411	410	409	408	407	406	405	404	403	402
422	347	346	345	344	343	342	341	340	339	338	337	336	335	334	333	332	331	330	401
423	348	281	280	279	278	277	276	275	274	273	272	271	270	269	268	267	266	329	400
424	349	282	223	222	221	220	219	218	217	216	215	214	213	212	211	210	265	328	399
425	350	283	224	173	172	171	170	169	168	167	166	165	164	163	162	209	264	327	398
426	351	284	225	174	131	130	129	128	127	126	125	124	123	122	161	208	263	326	397
427	352	285	226	175	132	97	96	95	94	93	92	91	90	121	160	207	262	325	396
428	353	286	227	176	133	98	71	70	69	68	67	66	89	120	159	206	261	324	395
429	354	287	228	177	134	99	72	53	52	51	50	65	88	119	158	205	260	323	394
430	355	288	229	178	135	100	73	54	43	42	49	64	87	118	157	204	259	322	393
431	356	289	230	179	136	101	74	55	44	41	48	63	86	117	156	203	258	321	392
432	357	290	231	180	137	102	75	56	45	46	47	62	85	116	155	202	257	320	391
433	358	291	232	181	138	103	76	57	58	59	60	61	84	115	154	201	256	319	390
434	359	292	233	182	139	104	77	78	79	80	81	82	83	114	153	200	255	318	389
435	360	293	234	183	140	105	106	107	108	109	110	111	112	113	152	199	254	317	388
436	361	294	235	184	141	142	143	144	145	146	147	148	149	150	151	198	253	316	387
437	362	295	236	185	186	187	188	189	190	191	192	193	192	193	196	197	252	315	386
438	363	296	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	314	385
439	364	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	384
440	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383

乌拉姆的大草笺

1963 年，洛斯阿拉莫斯的马尼艾克二型主机储存了前 9，000 万个素数。“ 在洛斯阿拉莫斯我们也有一台第一流的图解计算设备， ”韦尔斯回忆说，“ 因此我们对用计算机绘出素数图式感到异常激动。 ”马尼艾克二型为 1，000 万以下的所有素数都绘出方形螺线图。果然，许多数都神奇地出现在对角线上。

欧拉公式 n^2+n+41 在 n 为大数值时证明有令人震惊之效。马尼艾克二型计算出，在 1，000 万以下的所有素数中，该公式可得出占总素数的 47．5%。而当 n 值较低时，该公式工作得更有成效。当 n 值小于 2，398 时，得素数的机会一半对一半。而当 n 值小于 100 时，该公式得出 86 个素数，合成数只有 14 个。

马尼艾克的图解

乌拉姆和助手们还发现了其他几乎与欧拉公式同样有效的生成素数的公式。公式 $4n^2+170n+1$，847 计算 1，000 万以下素数的成功率为 46．6%，并得出 760 个欧拉公式所不能推出的素数。公式 $4n^2+4^n+59$ 的成功率为 43．7%，同时得出大约 1，500 个不能由其他两个公式推出的素数。

最奇怪的是，虽然这些公式都有很高的成功率，虽然在方形螺线中存在明显的对角线规则，但数理论家已证明与欧拉公式相仿的公式无一能生

成全部的素数，或除素数外别无他物。但这一证明并未阻止浪漫主义者寻找素数的模式。

在 100 以内的数字中有 25 个素数：2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89 和 97。这些连续的素数（以及随后无限多的素数）之间的间隔并无明显的范式可循。由于 2 是惟一的偶数素数，2 与 3 也是惟一一对只相差 1 个的素数。

相差 2 的素数——被称为孪生素数——又如何呢？在前 25 个素数中有 8 对孪生素数：（3，5），（5，7），（11，13），（17，19），（29，31），（41，43），（59，61）和（71，73）。大约 150 年来，数字理论家就推测过，孪生素数就像素数本身一样是无限多的，但还没有人能证明这一点。在 1966 年，研究取得进展，那时，中国数学家陈景润证明：在只相隔两个的无穷对数字中：第一个数为素数，第二个数也是素数或是两个素数的积。（为两个素数之积的数被称为“ 殆素数 ”，这一叫法既表明了数学家们不可抑制的乐观主义，又证明了真正素数的发现之难。）

乐观主义的另一表现是：陈先生证明了哥德巴赫猜想的较无力那一面的说法：每个“ 充分大 ”的偶数是一个素数和一个殆素数之和。“ 充分大 ”是素数文献中对“ 我知道我的证明对比某数 Q 大的所有数都有效，但我不知道 Q 是多少 ”的婉语。虽然短语“ 充分大 ”一词模糊不清，数学家们仍然认为陈的证明是过去 30 年来对素数理论意义最为重大的发现。

人们对素数之间离得多开比素数如何相互靠近知道得更多一些。的确，很容易证明存在任意长的非素数的连续数列。让 n！表示 1 到 n 的所有整数的乘积。这样，n！就可以被从 2 到 n 的每个整数整除。试想一下 n!＋2，n！＋3，n！＋4……n！＋n 的连续数列。这时，数列中的第一项 n！＋2 则可被 2 整除；第二项 n！＋3 可被 3 整除；第三项 n！+4 可被 4 整除；等等。在这个数列中有 n—1 个数，没有一个是素数。通过任意选择 n 的大小，你可以得出你想要的无素数的连续整数数列。

但也有大量的长串素数数列。事实上，数理论家认为素数可以形成漫长的等差级数（由同样差分开的素数数列）。较短的等差级数是容易发现的。例如，素数 3，5 和 7 构成 3 项差额同为 2 的等差级数。（1944 年，有人证明有无限组等差级数的 3 个素数。）素数 199，409，619，829，1039，1249，1，459，1，669，1，879 和 2，089 构成一个 10 项共同差额为 210 的等差级数。至于更长的级数，由于初始的素数和共同差额急剧上升，因而难于发现它们。然而，1983 年，保罗·普里查德在康奈尔发现了 19 个呈等差级数的素数；初始素数为 8，297，644，387，共同差额为 4，180，566，390。

一些数学家甚至推测存在任意长连续素数的等差级数。例如，连续素数 1，741，1，747，1，753 和 1，759 构成 4 项差为 6 的等差级数。然而，现在还没人能证明这一猜想，更不必说素数不必是连续的等差级数这一根据相对不足的猜想了。

对于素数，我们知道什么又不知道什么？对此可写一篇长篇论文。再举一个简单例子就足已。有人已证明在比 1 大的任何数和其倍数之间至少有一个素数。（这个证明的一个令人震惊的后果是：在 n 位数中至少有 3 个素数——n 可为任何正整数。）但无人知道在任何比 1 大的数的平方和其相邻数平方之间是否有一个素数。

既然素数本身没有已知的模式可循，那么数学家在努力证明它们时明显显示出杂乱无章也许是惟一合适的做法。某些基本定理——如有无限多的素数，它们之间有任意长的间隔——已简单明了地得以证明。其他定理，如哥德巴赫猜想依然有待证明。虽然没有一个自重的数学家对其正确性表示怀疑。为取得进展，数理论家采用了证明关于“殆素数”和“足够大的数”的办法。这一领域需要出现另一个欧几里得或欧拉。在那之前，我们可能依然处于这种奇妙的状态：依赖于秘密通讯的政府和工业继续从数学家的无知中获利。

对数理论有兴趣的读者不妨对这些未被证明的猜想动动手和计算器。如果猜想是正确的，证明工作可能会采用技术数学的成果，这是门外汉所做不到的。但如果与所期望的相反，它们碰巧是错的，全部所需要的则是一个反例。据历史记载，那些最具数学头脑的人也会出错。欧拉声称，1个5次方的数决不会等于两个5次方的数、3个5次方的数或4个5次方的数之和。（换句话说，不存在满足等式 $x^5=y^5+z^5$ 条件的整数 x、y 和 z；不存在满足等式 $a^5=b^5+c^5+d^5$ 条件的整数 a，b，c 和 d；也没有满足等式 $m^5=n^5+o^5+p^5+q^5$ 条件的整数 m，n，o，p 和 q。）两个世纪后的1966年，这一断言受到驳斥，因为发现了一个反例：144的5次方正是另外4个5次方的数——即27，84，110和133——之和。

如果推断未获证明的猜想不是你的事，考虑考虑某些数也许是。但不要再犯哈迪的错误：早早地就把出租车号斥为无趣的。前不久我乘机远行。当我为一本小说所吸引住时，邻座那位坐卧不安的同伴笨嘴拙舌地试图激起谈兴：“我们乘坐的是407号飞机。对我来说，这个数似乎很枯燥，我希望它不是个凶兆。”

“胡说，”我从书中抬起头来答道，“这个数字一点也不枯燥，相反，它非常有趣。它是等于其各位数3次方之和的最大的3位数。”那人直盯着我，好像我是个疯子，但他拿出一张便条开始不停地草算起来。他做了一路的计算，而我却可以不受打扰地读完我的小说。

第四章　比尔密码之谜

密码学——编制和破译密码的科学——日益成为那些能够获得最新计算机技术的数学家所从事的量性学科。今天在军队和私人企业中所使用的密码与昨日的密码截然不同，总的来说是变得更为难以破译了。然而，尽管取得了这些进步，这种新型的数学密码在许多场合也不管用，而对一些古老的密码，最先进的破译技术仍然无法解开。

密码学一定有很长的历史，因为早在公元前 1 世纪，据说凯撒大帝就曾用过极简单的代换式密码，在这种密码中，每个字母都由其后的第三个字母（按字母顺序）所代替。当凯撒说：“ Hw we，Eu-xwh！ ”而不是“ Et tu，Brute！ ”（“ 你这畜生！ ”）时，他的心腹会懂得他的意思的。值得注意的是，大约 2，000 年后，联邦将军 A．S．约翰逊和皮埃尔·博雷加德在希洛战斗中再次使用过这种简易密码。

《旧约》中发现的一个密码与这同样简单。在《耶利米书》第二十五章第二十六节和第五十一章第四十一节中，先知为通天塔写了 Sheshach。希伯来文第二个字母（b）被倒数第二个字母（sh）所取代。第十二个字母（l）被倒数第十二个字母（ch）代替。（这些元音次序错乱，但在希伯来文中，元音不大重要。）这种密码被称为 Ath-bash——一个由希伯来文第一个字母（a）、最后一个字母（th）、第二个字母（b）和倒数第二个字母（sh）组成的单词。

最初代换式密码的缺点是可以通过分析每个符号出现的频率而轻易地被破译。在每种语言中，冗长的文章中的字母表现出一种可对之进行分辨的频率。例如，e 是英语中最常用的字母，其出现频率为八分之一。最好假定长长的密文中最常用的符号代表 e。如果密码分析者根据频率数能破译出 9 个最常用的字母 e，t，a，o，n，i，r，s 和 h，一般来说他就可破译 70%的密码。最现代的译密技术也是以古老的频率分析法为根据的。

频率分析法还可以用来对单词中的字母的位置及其组合进行分析。例如，全部英语单词中有一半以上是似 t，a，o，s 或 w 开头的。仅 10 个单词（the，of，and，to，a，in，that，it，is 和 I）就构成标准英语文章四分之一以上的篇幅。

编成密码的词汇量越大，用频率分析法译密就越容易。在激战方酣时，电文接连不断地从战场和司令部之间来回发送，其中少不了密电。第一次世界大战时，德国人每月用无线电播送 200 万编成密码的文字。在第二次世界大战时，盟军最高统帅部常常一天就播发 200 万字的编密文字。

在凯撒密码（即 Athbash）那种系统中，与明文相对应的密码符号都是按照某种模式编制的，而这些模式又不难发现，所以人们不用费多少气力就可以发现这种模式。例如，如果对凯撒密码文进行频率分析后表明：h 代表 e，w 代表 t 及 d 代表 a，那么，密码分析者就会怀疑，每个密码字母代表着按 a，b，c 字母顺序的前 3 个字母。然后他会核实他的怀疑是否正确。预感与猜测无疑是译密的关键，因为易于使用这些方法并检验它们是否有效。

如果不是因为使用了频率分析的话，苏格兰的玛丽皇后是不会掉脑袋的。她那时常常用简单的代换式密码写不忠实的信件，并以此卖弄自己比凯撒和耶利米更高明。她任意选用密码符号，并用毫无意义的符号写信。

a b c d e f g h ijk l m n o p q r s t u v w x y z

nulls

无意义的符号

然而，英国特工处的奠基人弗朗西斯·沃尔辛厄姆极力排除了那些无意义的符号，并计算剩下符号的频率。结果，他破译出玛丽阴谋暗杀伊丽莎白女王并继承她的皇位。正是根据这种密码分析法，玛丽被宣判犯了叛国罪而被处决。

如果玛丽知道 15 世纪意大利建筑师莱昂·巴蒂斯塔·阿尔贝蒂的做法的话，她也许会免遭杀头。阿尔贝蒂为破坏频率推算法而提出了一个他称之为“群王”的令人惊讶的方案。在这种方案中，明文中每一个字母都可由每个密码符号来表示。实质上，它是用一个以上的密码字母来对某个特定的密码单位进行编密。这种密码叫做多字母体系密码；阿尔贝蒂的思想是现代密码学的基础。

阿尔贝蒂系统采用了下列表格。表的上面是大写字母，即众所周知的密钥字母，它们是用于发现表中的密码字母的。表的左边是明文字母，也是大写的。

在发出信息之前，通讯各方必须就一种被称为密钥词的口令取得一致。要为某一段信息编密，就得在明文上面重复地写密钥词。例如，密钥词是 LOVE（爱），明文信息为 SEND MORE MON－EY（送更多的钱来）。发送信息者则写：

密钥：LOVE LOVE LOVEL

明文： SEND MORE MONEY

密钥字母 明文字母

密钥字母

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

在每个明文字母之上的密钥词字母指明表中那个密码字母应用来给那个特定的明文字母编密。SEND 中的 S 应由字母 L 代表（因为 LOVE 中的 L 正落在 SEND 中的 S 上面），于是在表中 S 横栏和 L 竖栏的相交处发现了密码文字母 d。

密钥字母　明文字母

密钥字母

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

同样，字母 O 则代表 SEND 中的 E，于是在 E 横栏和 O 竖栏的相交处发现了其密码文符号——S：

密钥字母　明文字母

密钥字母

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	r	g	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	b	c
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	b	c	d
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	r	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	r	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

运用这种方法对全段信息进行处理，我们发现 SENDMOREMONEY 相应的密码文为 DSIHXCMIXCIIJ：

密钥词：LOVE LOVE LOVEL

明文：SEND MORE MONEY

密码文：DSIH XCMIX CIIJ

译密的过程与此类似：在密码文上方反复地写上密钥词，明文就可从表中适当的字母中解出。这种系统的可爱之处在于即使偷听者得到这种表，但他如没有密钥词也不会知道很多。在战时，由于要特别保密，密钥词经常变换。

但粗心大意地使用，最保密的密码也会泄密，这使破译密码在实际中比在理论上要容易得多。外交和军事通讯通常都以特有的诙谐语（“ 敬礼 ”和“ 谨上 ”等）开头和结尾，它们是密码分析者的线索。某些特有的名称，

尤其是那些特别长的名称也会泄露天机。例如在第二次世界大战时，德国通讯设备就用密码说过 Wehrmacht-nachrich tenverbin dungen——德国国防军通讯情报处。

通过对敌人进行引诱常常可以获得信息。 1942 年 5 月，美国最高统帅部得知一支由 11 艘战列舰、5 艘航空母舰、16 艘巡洋舰和 49 艘驱逐舰组成的庞大日本舰队不久将要出击，但不知道出击地点。日本无线电播音员一次又一次地提到 AF。AF 是代表加利福尼亚、阿拉斯加、中途岛还是其他什么地方呢？为弄清这一问题，美国情报官员指示美国中途岛驻军用无线电向珍珠港播报淡水快用完的信息。中途岛驻军照办了。此后不久，美国人截获了日本人报告 AF 地区用水短缺的消息。当攻击来临时，美军已严阵以待了。美军在数量上处于劣势的情况下击退了日军，从而取得了中途岛大海战的胜利。

即使密码不会被泄露出去，它也会被破译出来，因为它有着内在的弱点，这些弱点常常为发送者所忽视而被足智多谋、进行窃听的密码分析家所利用。阿尔贝蒂的多字母体系密码在 300 年中一直被认为是无懈可击的，但是在 19 世纪 60 年代，一位昔日的普鲁士步兵弗里德里希·W．卡希斯卡发现了几个内在的弱点。例如，他发现，如果对一个不止一次出现的明码字母每次都用同样的密钥字母进行加密，那么就会出现同样的密码文。如在 SENDMORE MONEY 短句中，密钥字母 LO 两次把明文 MO 列加密成 XC：

密　钥：LOVE LOVE LOVEL

明　文： SEND　MORE　MONEY

密码文：DSIH XCMI XCIIJ

重复的密码文 XC 表明了密钥词的长度。一般来说，在重复文字中从一例到另一例之间的密码文字母数是密钥词字母的倍数。

如果密码文数位经常重复的话，密码分析家就能计算出密钥词的长度，并因此计算出所运用的密码字母表的数目。这样，要知哪个密码文字母来自哪个密码字母系列就只是一个分类问题了。而就每个密码字母系列来说，频率分析法将解出明文字母。

在阿尔贝蒂密码中，只要密钥保持秘密状态，即使加密法——密码字母系列表——为人所知也不会危及这种密码的保密性。而正在利用创新的数字方法的现代密码学者——如我们在上一章所见——把这一趋势推向极端：可以在加密方法和密钥都公开的情况下而不泄密。换句话说，给一段文字加密不像破译它那么困难。

在当今时代密码术日益电脑化之时，技术上的故障可以造成严重的后果。如果说曾有过某种形势，即需要运用一种现代数学提供的、而实际上又不可译解的密码的秘密通讯方式的话，那就是在 1985 年 10 月。某日凌晨，里根政府从情报人员处获悉：埃及总统霍斯尼·穆巴拉克谎称 4 名巴勒斯坦恐怖主义分子劫持了意大利阿基勒·劳罗号巡逻艇，并在轮椅上谋杀了 69 岁的莱昂·克林霍弗后不知去向。其实，与穆巴拉克公开声称的相反，劫艇者依然在埃及领土上，并准备偷偷地乘机离开这个国家。当美国情报人员极力想确定恐怖主义分子计划乘坐的飞机——一架停落在开罗附近航空基地的埃及航空公司波音 737 飞机时，五角大楼的反恐怖主义专家们迅速提出了一项计划：在侦察机和雷达干扰机的配合下，用 F－14 公猫

战斗机阻截这架民用的要出逃的飞机。

同时，里根总统和往常一样。当中央情报局和五角大楼采取紧急行动对，他在芝加哥外面的萨拉·李餐馆吃午饭，品尝烤制食品。一份来自华盛顿的火急（也是秘密的）电讯打断了他的饭后闲聊。总统的顾问向他简述了迫降埃及航空喷气机的大胆计划。里根对他听到的汇报表示赞成，但在点头签字之前，他要了解这将危及多少人的生命。几个小时后，里根登上了去华盛顿的“空中一号”，并同国防部长卡斯珀·温伯格通话，温伯格正乘军用飞机飞往他缅因州巴港的夏日之家。总统通过一条公开的无线电短波频道像通常一样说话，没用暗语，也没用高技术的玩意儿改变他的声音，他命令并不情愿的温伯格执行这一大胆的使命。一位业余无线电报员收听到总统鼓动性命令的每一个单词，这位偷听者的兄弟则不失时机地与哥伦比亚广播公司新闻部取得联系，但广播公司却没有报道总统的命令。哥伦比亚广播公司新闻部不是《纽约邮报》“第六版”，它想要第一手材料：或者是无线电报员本人（而不是他的兄弟），或者是偷听到的谈话录音带。几个小时后，埃及航空公司的飞机正按哥伦比亚新闻部所听说的那种方式迫降。

《纽约时报》后来引用白宫的一位官员的话说：“他们（里根和温伯格）乘坐的是两架不同的飞机，拥有两种不同的密码系统。本来他们可以通过另一种密码系统进行联系，但时间紧迫，于是他们决定不走密线。他们认为这种信息还没重大到需要保密的程度。”但你可以肯定，如果一位业余无线电报员偷听到他们的谈话，那么明显在监听“空中一号”所有无线电通话的苏联人也会偷听到。如果克里姆林宫不表现克制的话，那么，美国 F-14 战斗机遇到的可能是苏联空军中队的米格战斗机而不是无防御能力的民用客机了。

当时间急迫时，需要精密设备和复杂的数学方法的密码就不现实了。例如，在激战时，命令必须一接到就执行，没有很多时间去破译密码。如果里根和温伯格懂得一种相对不清的外语，他们也许会说这种语言的。布尔战争时，英国在各营地之间传递情报的通讯员说的就是拉丁语。这至少给偷听者们带来些障碍。

第一次世界大战时，在法国的美国远征军统帅担心德国人在监听每项通讯，他在军团的印第安人中发现了一种奇特的通讯方式，这些印第安人能说 26 种难懂的语言，其中只有 5 种语言有书写文字。当 8 个乔克塔印第安人用战地电话传布命令时，他们发出了第二营从丘弗里“巧妙撤退”的声音。在美国参加第二次世界大战之前，军方对许多土著美国语言进行研究并确定纳瓦荷语为理想的战场通讯语言。

在该部落之外只有 28 人知道这种语言，而该部落中无人同敌方有任何联系。纳瓦荷语像中文一样极为难学，因为其字义取决于发音中的微妙变化。而且，不存在纳瓦荷语教科书；只能从土著人那儿学到这种语言，五角大楼所幸的是，所有讲这种语言的土著人全在美国境内。既然纳瓦荷人有 5 万多，肯定有许多身强力壮的人被征召入伍。在二战临近结束时，420 名纳瓦荷人以其特别的方式帮助了美国海军从所罗门岛向冲绳岛推进，他们以一种特殊语言大声喊叫命令，这种语言使日本最高统帅部难以破译对方的情报，只得进行快速的部队调动。

虽然越来越多的数学家从事密码学研究，越来越多的巨型计算机被用

来编制和破译密码，但那些古老的密码依然使他们头痛并耗费着他们的时间。在一个半世纪前写成的著名的比尔密码——它明显在某个地方藏有1，700 万美元的地财——依然耗去了“ 美国最有能耐的密码分析家至少 10%的精力 ”，曾在斯佩里通用计算机公司干了 20 多年的主任计算机科学家、电脑密码统计性分析的先驱卡尔·哈默说，“ 决不应吝于做出这种收效甚微的努力 ”。哈默补充说：“ 这项工作——即使是那些走入了死胡同的工作——也为推动和改善计算机的研究做出了贡献。 ”

遗传下来的比尔密码源于 1820 年 1 月，当时，一位个头高高、皮肤黝黑、长着一双乌黑发亮的眼睛和一头乌黑发亮的头发、朴实而漂亮的陌生人骑马来到弗吉尼亚林奇堡的华盛顿旅馆。来人受到该旅馆老板罗伯特·莫里斯——富人知道他喜欢宴请宾客，穷人知道他慷慨大方——的欢迎，陌生人自我介绍说他叫托马斯·杰弗逊·比尔。他在巡视院子并检查为他和他的马准备的旅馆设备后告诉莫里斯说，他打算在那儿呆一个冬天。比尔精神饱满，谈锋极健，又是一位殷勤的客人，他的阳刚之美受到太太们的倾慕，遭到男人们的嫉妒。他以长长的故事来娱悦其他宾客，这些故事涉及每个可以想象得出的主题，但他对他的家庭、他的出身和他的住处却只字不提。那年的 3 月底，他一声不响地离开了这家旅馆，无人知道他的去向。

此后两年间，无人知道他的消息。后来，1822 年 1 月，他突然又出现在这个旅馆，他还像从前那么友善，只是比以前更为黝黑更为潇洒了，他那齐整而被晒黑了的躯体表明他曾经历过一次重大的户外探险。每个人，尤其是女人们欢迎他的归来。春天来到时，比尔又不见了。他留下了一个锁着的铁盒，莫里斯打算把它藏起来，等他回来再说。夏天，莫里斯收到比尔的一封来信，信头是圣路易，5 月 9 日。在信中，比尔描述了他遇到野牛和野蛮灰熊的情形。（那时，圣路易是一个小小的边境城市。）“ 我现在不能决定我会离开多久，”信继续说，“ 肯定不少于两年，也许更长。 ”

“ 我想谈一下关于那个我留下托你保管的盒子的事……它里边装着几份信件，它关系到我自己和许多其他同我做交易者的命运；万一我死去，其损失是无法挽回的，因此你会明白警惕而小心地保护它的必要性，以防巨大灾难的发生。盒内还装有几封写给你自己的信，它们会使你了解我们所从事的事业……如果我和我的同伴自这封信上的日期起 10 年内不来认领，你就打开它，只要把锁去掉就行。 ”

“ 你会发现，除了给你的信以外，其他信件如不借助于线索是难以理解的。这种线索我留给了这里的一位朋友，它是密封着的，它是寄给你本人的，上面签有‘ 1932 年 6 月前不予递送 ’的字样。凭借这把钥匙，你会全面理解要你做的一切事情……向你最美貌的夫人致以最真挚的祝愿，向诸位太太表示问候，向好奇的朋友——如果有的话——表示谢意，最后，郑重地向你本人致以最高的敬意，我同过去一样依然是你忠实的朋友，托·杰弗·比尔。 ”

不用说，莫里斯再也没有收到比尔的信。至于他是被印第安人所杀，或是为野兽所吞食，亦或曝尸于野还是饿殍而亡那就任凭读者去想象了。1832 年夏天到了，莫里斯却没收到允诺从圣路易寄来的线索。根据比尔的信，莫里斯本可以在那年砸开那只盒子，但由于忙于其他事务，他直到 1845 年才打开它。他在里面发现了两封写给他的信——一封很长而内涵丰富的

信和一封短而平淡的信——一些陈旧的收条和几张写满一连串数字的纸。

长信所注的日期为 1822 年 1 月 4 日，信是这样开始的：“ 当你熟读此信，发现你从未见过、你从未听到过姓名的伙伴对你的荣誉表示极大的信赖时，你一定会感到震惊。其原委是简单易说的。我们必须在这儿挑选一个人，在我们一旦身遭不测时实现我们的愿望，你为人诚实，名誉无可挑剔，又有商人般的精明，因此他们选中了你而没选中其他一些比你更有名，但也许没有像你那样可靠的人。正是怀着这种目的我两年前拜访了你的住所，这样，我可以通过亲身观察来看你是否与你名声相符。 ”

接下去这封信描述了比尔和一队 29 个快乐的“ 喜爱探险，尤其是那些带有危险的远征 ’的伙伴们如何于 1817 年 4 月开始到西边广袤的大平原进行两年的打猎冒险活动。1818 年春，大约在圣塔 · 菲以北 300 英里处，这个打猎队在恶劣的气候中拖着疲惫不堪的身体追赶着一大群野牛进了一个深深的峡谷。他们追赶累了，于是拴上马搭起了帐篷。当他们正准备晚饭时，他们中一位眼尖的瞭望者在岩石的缝中看到有金子。

信中说，在以后的 18 个月中，他们在友好的印第安人的帮助下挖出金子，还有银子。然后，比尔和他的几个好友把这些财宝拉到弗吉尼亚，他们打算把它们隐藏在那里的一个他们以前曾到过的洞中，这个洞 “ 在贝德福德县的布法德酒馆附近 ” 。然而到达该洞后，比尔认为它作贮藏库不合适，“ 附近的农民经常到洞里去，他们把它作为甘薯和其他蔬菜的贮藏所 ”。因此，他们选择了另一个隐蔽的地点。

然后，比尔又来华盛顿旅馆登记住宿。他对莫里斯像人们所称颂的那样可信感到满意，于是再次冒险西行加入他同伴之列。1822 年秋天，他将大量的金银带回弗吉尼亚，把这些贵重金属贮藏在那个隐蔽地点，并把锁着的盒子委托给莫里斯。

至于那 3 张难以理解的文件，上面写满了数字，信中写道，这些文件如用允诺给予的密钥破译出，就会揭示出隐藏处的确切地点、贮藏处具体所藏之物以及这 30 个冒险家的姓名和地址。该信指示莫里斯把这份财宝分成 31 等份，留一份给自己作为其服务的报酬，而将其余的各份分给 30 个债权人的亲属。 “ 最后，我亲爱的朋友， ” 比尔写道，“ 我请求你不要让虚假而无用的拘谨妨碍你接受并拿走指定给你本人的那份。它是一份礼物，不仅是我个人而且是我们队所有成员送给你的礼物，并且它并不微薄得与你给予我们所需要的帮助不成比例。 ”

盒子中的东西无疑勾起了莫里斯的好奇心。但驱使他的并不是贪婪之心，而是希望不辜负那个魅力超凡的猎艳者和他 29 个未知同伴的信赖，他们因喜爱大胆冒险而结合在一起。 “ 这些人生性莽撞好动，他们这种性格的魔力诱使他们越来越远离尘世，终于为之丧生 ” 。莫里斯在其一生余下的 19 年中致力于发现财宝，但由于没有那份神秘文件的密钥而不能有任何进展。在他临终前的 1863 年，他把那只盒子的事告诉了詹姆斯 · 沃德，沃德是一位酒馆侍者，有家有口，处事谨慎，他积了足够的钱以便能花时间寻找那些无法捉摸的财宝。

莫里斯认为，让沃德知道比尔的秘密是对他施以恩惠，可能还是一桩丰厚的惠赐。其实相反，它成了沃德的祸根。他开始沉溺于密码之中，他努力破译出第二页密码，揭示了所隐藏财宝的内容（2，921 磅金子，5，100 磅银子，按今天的标准就是价值约为 335 万美元的珠宝），但未发现

埋藏地点，他更不能自拔了。

“当碰巧揭示出第二页的内容时，我喜悦的心情简直无法形容”，沃德写他本人。然而，这次意外发现虽然使他一时欣喜异常，但却是他最大的不幸，为了那个今已证明是纯粹的子虚乌有之物，他放弃了家庭、朋友和一切正常的追求……当作者回想起为了这一希望他那焦虑的日日夜夜，他的深夜煎熬，他的代价，他的希望和他的失望时，他只能得出了这样的结论：莫里斯先生这一遗产，虽然他的本意是好的，却使沃德因福得祸。

再来看看那些密码本身：

第一页：1，700 万美元财宝贮藏地点：

71,194,38,1701,89,76,11,83,1629,48,94,63,132,16,111,
95,84,341,975,14,40,64,27,81,139,213,63,90,1120,8,
15,3,126,2018,40,74,758,485,604,230,436,664,582,150,
251,284,308,231,124,211,486,225,401,370,11,101,305,
139,189,17,33,88,208,193,145,1,94,73,416,918,263,28,
500,538,356,117,136,219,27,176,130,10,460,25,485,18,
436,65,84,200,283,118,320,138,36,416,280,15,71,224,
961,44,16,401,39,88,61,304,12,21,24,283,134,92,63,
246,486,682,7,219,184,360,780,18,64,463,474,131,160,
79,73,440,95,18,64,581,34,69,128,367,460,17,81,12,
103,820,62,116,97,103,862,70,60,1317,471,540,208,
121,890,346,36,150,59,568,614,13,120,63,219,812,
2160,1780,99,35,18,21,136,872,15,28,170,88,4,30,44,
112,18,147,436,195,320,37,122,113,6,140,8,120,305,
42,58,461,44,106,301,13,408,680,93,86,116,530,82,
568,9,102,38,416,89,71,216,728,965,818,2,38,121,195,
14,326,148,234,18,55,131,234,361,824,5,81,623,48,
961,19,26,33,10,1101,365,92,88,181,275,346,201,206,
86,36,219,320,829,840,68,326,19,48,122,85,216,284,
919,861,326,985,233,64,68,232,431,960,50,29,81,216,
321,603,14,612,81,360,36,51,62,194,78,60,200,314,
676,112,4,28,18,61,136,247,819,921,1060,464,895,10,
6,66,119,38,41,49,602,423,962,302,294,875,78,14,23,
111,109,62,31,501,823,216,280,34,24,150,1000,162,
286,19,21,17,340,19,242,31,86,234,140,607,115,33,
191,67,104,86,52,88,16,80,121,67,95,122,216,548,96,
11,201,77,364,218,65,667,890,236,154,211,10,98,34,
119,56,216,119,71,218,1164,1496,1817,51,39,210,36,3,
19,540,232,22,141,617,84,290,80,46,207,411,150,29,
38,46,172,85,194,36,261,543,897,624,18,212,416,127,
931,19,4,63,96,12,101,418,16,140,230,460,538,19,27,
88,612,1431,90,716,275,74,83,11,426,89,72,84,1300,
1706,814,221,132,40,102,34,858,975,1101,84,16,79,23,
16,81,122,324,403,912,227,936,447,55,86,34,43,212,
107,96,314,264,1065,323,328,601,203,124,95,216,814,

2906,654,820,2,301,112,176,213,71,87,96,202,35,10,2,
41,17,84,221,736,820,214,11,60,760。

第二页：财宝的具体内容：

115,73,24,818,37,52,49,17,31,62,657,22,7,15,140,47,
29,107,79,84,56,238,10,26,822,5,195,308,85,52,159,136,
59,210,36,9,46,316,543,122,106,95,53,58,2,42,7,
35,122,53,31,82,77,250,105,56,96,118,71,140,287,28,
353,37,994,65,147,818,24,3,8,12,47,43,59,818,45,316,
101,41,78,154,994,122,138,190,16,77,49,102,57,72,34,
73,85,35,371,59,195,81,92,190,106,273,60,394,629,
270,219,106,388,287,63,3,6,190,122,43,233,400,106,
290,314,47,48,81,96,26,115,92,157,190,110,77,85,196
46,10,113,140,353,48,120,106,2,616,61,420,822,29,
125,14,20,37,105,28,248,16,158,7,35,19,301,125,110,
496,287,98,117,520,62,51,219,37,37,113,140,818,138,
549,8,44,287,388,117,18,79,344,34,20,59,520,557,107
612,219,37,66,154,41,20,50,6,584,122,154,248,110,61
52,33,30,5,38,8,14,84,57,549,216,115,71,29,85,63,43
131,29,138,47,73,238,549,52,53,79,118,51,44,63,195,
12,238,112,3,49,79,353,105,56,371,566,210,515,125,
360,133,143,101,15,284,549,252,14,204,140,344,26,
822,138,115,48,73,34,204,316,616,63,219,7,52,150,44
52,16,40,37,157,818,37,121,12,95,10,15,35,12,131,62
115,102,818,49,53,135,138,30,31,62,67,41,85,63,10,
106,818,138,8,113,20,32,33,37,353,287,140,47,85,50,
37,49,47,64,6,71,33,4,43,47,63,1,27,609,207,229,
15,190,246,85,94,520,2,270,20,39,7,33,44,22,40,7,10,
3,822,106,44,496,229,353,210,199,31,10,38,140,297,
61,612,320,302,676,287,2,44,33,32,520,557,10,6,250,
566,246,53,37,52,83,47,320,38,33,818,7,44,30,31,250,
10,15,35,106,159,113,31,102,406,229,540,320,29,66,
33,101,818,138,301,316,353,320,219,37,52,28,549,320,
33,8,48,107,50,822,7,2,113,73,16,125,11,110,67,102,
818,33,59,81,157,38,43,590,138,19,85,400,38,43,77,
14,27,8,47,138,63,140,44,35,22,176,106,250,314,216,
2,10,7,994,4,20,25,44,48,7,26,46,110,229,818,190,34,
112,147,44,110,121,125,96,41,51,50,140,56,47,152,
549,63,818,28,42,250,138,591,98,653,32,107,140,112,
26,85,138,549,50,20,125,371,38,36,10,52,118,136,102,
420,150,112,71,14,20,7,24,18,12,818,37,67,110,62,33,
21,95,219,520,102,822,30,38,84,305,629,15,2,10,8,
219,106,353,105,106,60,242,72,8,50,204,184,112,125,
549,65,106,818,190,96,110,16,73,33,818,150,409,400,
50,154,285,96,106,316,270,204,101,822,400,8,44,37,

52,40,240,34,204,38,16,46,47,85,24,44,15,64,73,138,
818,85,78,110,33,420,515,53,37,38,22,31,10,110,106,
101,140,15,38,3,5,44,7,98,287,135,150,96,33,84,125,
818,190,96,520,118,459,370,653,466,106,41,107,612,
219,275,30,150,105,49,53,287,250,207,134,7,53,12,47,
85,63,138,110,21,112,140,495,496,515,14,73,85,584,
994,150,199,16,42,5,4,25,42,8,16,822,125,159,32,204,
612,818,81,95,405,41,609,136,14,20,28,26,353,302,
246,8,131,159,140,84,440,42,16,822,40,67,101,102,
193,138,204,51,63,240,549,122,8,10,63,140,47,48,140,288。

第三页：探险者亲属的姓名和地址：

317,8,92,73,112,89,67,318,28,96,107,41,631,78,146,
397,118,98,114,246,348,116,74,88,12,65,32,14,81,19,
76,121,216,85,33,66,15,108,68,77,43,24,122,96,117,
36,211,301,15,44,11,46,89,18,136,68,317,28,90,82,
304,71,43,221,198,176,310,319,81,99,264,380,56,37,
319,2,44,53,28,44,75,98,102,37,85,107,117,64,88,136,
48,151,99,175,89,315,326,78,96,214,218,311,43,89,51,
90,75,128,96,33,28,103,84,65,26,41,246,84,270,98,
116,32,59,74,66,69,240,15,8,121,20,77,89,31,11,106,
81,191,224,328,18,75,52,82,117,201,39,23,217,27,21,
84,35,54,109,128,49,77,88,1,81,217,64,55,83,116,251,
269,311,96,54,32,120,18,132,102,219,211,84,150,219,
275,312,64,10,106,87,75,47,21,29,37,81,44,18,126,
115,132,160,181,203,76,81,299,314,337,351,96,11,28,
97,318,238,106,24,93,3,19,17,26,60,73,88,14,126,138,
234,286,297,321,365,264,19,22,84,56,107,98,123,111,
214,136,7,33,45,40,13,28,46,42,107,196,227,344,198,
203,247,116,19,8,212,230,31,6,328,65,48,52,59,41,
122,33,117,11,18,25,71,36,45,83,76,89,92,31,65,70,
83,96,27,33,44,50,61,24,112,136,149,176,180,194,143,
171,205,296,87,12,44,51,89,98,34,41,208,173,66,9,35,
16,95,8,113,175,90,56,203,19,177,183,206,157,200,
218,260,291,305,618,951,320,18,124,78,65,19,32,121,
18,53,57,84,96,207,244,66,82,119,71,11,86,77,213,54,
82,316,245,303,86,97,106,212,18,37,15,81,89,16,7,81,
39,96,14,43,216,118,29,55,109,136,172,213,64,8,227,
304,611,221,364,819,375,128,296,11,18,53,76,10,15,
23,19,71,84,120,134,66,73,89,96,230,48,77,26,101,
127,936,218,439,178,171,61,226,313,215,102,18,167,
262,114,218,66,59,48,27,19,13,82,48,162,119,34,127,
139,34,128,129,74,63,120,11,54,61,73,92,180,66,75,
101,124,265,89,96,126,274,896,917,434,461,235,890,
312,413,328,381,96,105,217,66,118,22,77,64,12,12,7,

55,24,83,67,97,109,121,135,181,203,219,228,256,21,
34,77,319,374,382,675,684,717,864,203,4,18,92,16,63,
82,22,46,55,69,74,112,135,186,175,119,213,116,312,
343,264,119,186,218,343,417,845,951,124,209,49,617,
856,924,936,72,19,29,11,35,42,40,66,85,94,112,65,82,
115,119,236,244,186,172,112,85,6,56,38,44,85,72,32,
47,73,96,124,217,314,319,221,644,817,821,934,922,
416,975,10,22,18,46,137,181,101,39,86,103,116,138,
164,212,218,296,815,380,412,460,495,675,820,952。

沃德是如何设法破译出第二页的呢？密码文中数字的数目大大超过了 26 个（字母表中字母的数目），沃德想，既然如此，这些数字是不是有可能与比尔曾依次编号的文件中的单词相对应呢？考虑到这一点，沃德试着对许多著名文件中单词的字母进行编号并用那些字母代替密码文中的数字。“这全都是徒劳无益的，”沃德写道，“直到后来，《独立宣言》为其中一张纸的数字提供了线索而重新激发了我的希望。”沃德的做法是给《独立宣言》中每个单词的第一个字母进行编号。例如，他这样给前 9 个词进行编号：

1	2	3	4	5	6	7	8	9
WHEN,	IN	THE	COURSE	OF	HUMAN	EVENTS,	IT	BECOMES

他从这些单词中发现 1＝W，2＝1，3＝T，4＝C，5＝O，6＝H，7＝E，8＝1，9＝B。你已经可以看到比尔有两种办法给字母 I 加密：2 或 8。等到他给整个《独立宣言》编号之后，他对许多字母无疑就有了众多的选择。通过自由运用所有这些选择，他借助频率分析法破译难以译出的密码文。这样，由于沃德碰巧发现了适当的密钥——《独立宣言》——而破译了这段密码，他运用这一密钥而推断出下列一段文字：

“我在离布法德约 4 英里处的贝德福德县里的一个离地面 6 英尺深的洞穴或地窖中贮藏了下列物品，这些物品为各队员——他们的名字在后面第三张纸上——公有。第一窖藏有 1，014 磅金子，3，812 磅银子，藏于 1819 年 11 月。第二窖藏有 1，907 磅金子，1，288 磅银子，另有在圣路易为确保运输而换得的珠宝，价值 1．3 万美元，它们藏于 1821 年 12 月。以上物件稳稳地包在带有铁盖的铁罐之中。该窖穴用石头粗糙地砌成，那些铁罐就放在坚硬的石头之上并用其他石头覆盖。第一页描述了该窖穴的确切位置，因此，找到它并无困难。”

这段文字，尤其是最后一行激发起沃德的兴趣，他花了越来越多的精力去破译其余密码。然而，尽管他做了尝试，但却毫无进展。“随着时光的流逝，”沃德写道，“我从比较富裕降到赤贫的地步，并使那些我有责任保护的人遭受痛苦，这也是无视于他们的忠告的结果。终于，我注意到他们的状况，并决心立即并永远割断与这件事的一切联系，如果可能的话，尽力弥补我的过失。为做到这一点，并使我再也不会受到诱惑，我决定把这件事全部公开，卸下我对莫里斯承担的责任。”

于是，1894 年，他出版了一份比尔密码的报告书，这份报告是我们今

天了解该密码及或许由其所获得的大量财宝的惟一资料来源。我向你叙述的每一个有趣的细节——比尔高高的个头，黝黑的皮肤，莫里斯与富人和穷人都合得来，猛兽吸引着比尔及其猎队——全都出自沃德之口。然而却没有一项独立的证据：没有证明的信件，没有日记，没有遗嘱，也没有有关财宝的证明。而且，比尔想象中给莫里斯的盒子没有保存下来，声称在盒子里的信和加密的文件也是如此。如果沃德是一个喜欢恶作剧的人，那他一定精通此道：他赢得了一次历时最长也是代价最大的骗局。如果你想一想计算机为破译这些密码所花的全部时间就知道这一点。哈默说：“我们用计算机摆弄的那些数字需要100万人花10亿年时间才能用纸和笔重演一遍。”

20 世纪 60 年代，一些密码分析界最富智慧的人（和许多最拙劣者）组成了一个秘密协会——比尔密码协会——以便他们倾其知识和才智去发现那堆难以捉摸的财富。哈默就是该协会的一位著名成员，他对未经译解的比尔文件中的数字的分布做了大量统计、试验，并总结说，这些数字并不是随意写出的，它一定隐含着一段英文信息。多数密码学家同意哈默的分析，但存在一段文字并不意味着全部的东西就不是一场骗局。谁说这段文字就不是像“你是世上最大的笨蛋，大脑迟钝”这类的话呢？纽约密码协会主席路易斯·克鲁做了些另一种统计试验，目的是对沃德的写作风格与沃德报告书中所引用的比尔信件的风格进行比较。克鲁发现，这两种写作风格颇为相似，他深信比尔的信是沃德写的。例如，沃德句子平均长度是 28．82 个单词，而比尔信中句子平均长度为 28．75 个单词。然而，克鲁的分析使得几位比尔密码协会的成员关掉电脑而洗手不干了。

1981 年，弗吉尼亚技术学院的一位好幻想而又务实的低年级大学生沃伦·霍兰赋予比尔的这项遗物以新的生命。霍兰没能在建筑业上取得成就，因为他难以从顾客那里收到钱。他说：“在那个行业，人们忘记了诚实，忘记了做人，他们总是强人所难。”由于心情抑郁，存款日减，他开始性情内向，博览群书，包括比尔密码的报告书以及有关许多财宝寻求者——他们在约 160 年后仍然在弗吉尼亚的偏远山林中挖掘不已——的情报报告。虽然他也对这个故事感兴趣，但他不是那种要跑出去到野外挖掘的那种人——他在建筑业中干够了这些。后来，他有了！他通过神奇地投人所好而找到一条来钱的路子。他对自己写的一段话加密并拿到市场上去兜售，并为破译它的人颁奖。

他只花了几个小时就给他所喜欢的几首诗编好密码，这些诗的作者是卡明斯，书名为“诗人的忠告”，说的正是你自己在一个努力要使你泯如众人的世界中的美德。霍兰的做法与比尔一样。首先，他选择密钥：不是《独立宣言》，而是卡尔·萨根写的《宇宙》的第六章。然后，他依次对单词进行编号，从本章开始的一段引语的第一个字开始，每个数代表一个词的第一个字母。最后，他用这些数码代替“诗人的忠告”中的字母。他决定将密码文写在拼板玩具上，这样，他制造出谜中之谜。

这项工作容易，只花了一个下午的时间。难的是把这个谜推销到市场上去，这工作花去了两年时间。他想设立一个奖金为 10 万美元的破译奖，并打算以出售该谜来筹集这笔钱。但他想为该奖提供保险，怕万一卖得金额达不到 10 万美元。伦敦劳埃德保险公司拒绝为他作保，因为伦敦警察厅认为该密码可轻易被破译。最后他说服了一家美国保险公司，并找到了一

个销售商推销该谜。这个被称作“密码员”的谜，从它投入市场到 1985 年 3 月被破译为止的两年时间中，销售了约 25 万套。

1984 年冬，麻省理工学院 27 岁的计算机科学博士候选人阿兰·舍曼决定开设一门密码学小型课程，其目的就是要破译霍兰的“密码员”之谜。有 6 名学生，包括一名特别研究生罗伯特·鲍德温选了这门课。班上配备了一台当时最精密的个人用计算机——符号象征学 3600 型表格处理机，以及麻省理工学院计算机科学实验室所有其他设备，舍曼的办公室就设在实验室里。（他现为特福茨大学副教授，乘地铁上班有 4 站路。）

对于计算机科学实验室来说，未破译的密码并不陌生。那儿的许多教授对密码学做出过杰出的贡献，但一般来说，他们更关心的是学术性和理论上的问题而不是去赢得破译商用之谜的奖金。然而，贴在实验室墙上的纸表明此地也是风尘之地。贴得最显眼的是那张 1984 年 7 月 10 日《世界新闻周刊》的超级市场文摘的前页，该页在突出位置刊登着“嫉妒的电脑杀死一流科学家：老机器使主人触电身亡——在他买了更先进的型号后”的故事。墙上还钉有苏联各种城市奇怪的街区地图。中央情报局过去曾在这层楼办公。在他们搬出这幢楼之后，麻省理工学院学生从一个垃圾桶中翻出这些地图，还有一些诸如《如何在城市跟踪人》的小册子。

舍曼自己险些陷入诡计，这种诡计并不是中央情报局所干的间谍侦察，而是政府译密和编密总部国家安全局巧妙地运用计算机键盘所进行的窃听。这个政府组织中最秘密的部门甚至预算都保密，有人认为它的预算比中央情报局多一倍。其活动极为秘密，甚至它的雇员开玩笑说 NSA 不是 National Security Agency（国家安全局）的缩写，而是 Never Say Anything（守口如瓶）的缩写。安全局负责有争议的“数据加密标准”，其他政府机构和私人公司可能使用这种复杂密码来为有关私人的档案材料保密。批评家指责安全局在提倡这种密码，称之为实际上是不可译解的，因为该局在这种密码中设了一个秘密活动门，每当它想给机密档案加密时，它可以毫不费力地工作。舍曼不属这些批评家之列，但他费了许多精力来研究“数据加密标准”的数学属性以及那些特性与该密码可靠性的关系。他研究出该密码有一种奇怪的特性：存在着与其编码相同的文字！

一般来说，大家离开研究部门到安全局工作并不是因为受到突发的为国服务之心的驱使，而是因为该局对他们中的技术迷具有吸引力：国家安全局在马里兰的绝密设备明显比这个行星上任何其他地方都装备有更多的计算机。舍曼拒绝了该机构提供的工作，因为其严格的保密条例可能会使他无法再教授密码学或发表有关这个专题的论文。鉴于该局有名的保密命令，可以推测国家安全局一名雇员破译了比尔密码，但该局的条例禁止他报告其解法或正在黑幕的掩护下挖掘那些财宝。

当我 1985 年春遇见鲍德温时，他表示出对“密码学议定书”感兴趣，运用密码学是为达到“较高的目标”。我要是问他何为较低的目标就好了；而我所能想到的就是国家安全局对莫斯科豪华轿车间的无线电通话进行有记录的窃听，在这些轿车中，克里姆林宫的头面人物透露了当地男按摩师的特别服务。但鲍德温没有鼓动就详细谈论起“较高目标”来。他告诉我如何能使用密码签名，以便在你用键盘与一台计算机通信时，你知道它是你正在与之联系的那台计算机而不是某种正模拟这台机器的可恶而手段高明的破坏者。另一个较高目标是给私人支票和信用卡收据加密，这样，除

储户本人外无人知道他把钱花在什么上面。“支票应该是匿名的，”鲍德温说，“不应该让它对你的住址透露出一点痕迹，如果你给你情妇开支票那不关别人的事。”

鲍德温向我演示了他们用于破译“密码员”的计算机系统。他打开程序，屏幕上出现了下面一段文字：

注意：只有原始执行者才获准使用本系统，你是执行者吗？

“为了禁止越权使用，我们只用了这简单的一招，”鲍德温说，“它要求人们遵守道义。”

这种系统的思想是：使用者用备选的密钥文打字，计算机测出各种给该文编号的策略。一种策略是给每个单词的第一个字母进行编号，就像比尔给《独立宣言》编号一样。另一种方式是给每个字母编号。每种策略在文中各种标点处开始反复尝试。每种方式得出字母数字间的不同分配，然后计算机将之应用到密码文中去以图推断出一段英语文字来。

由于计算机不会读英文，鲍德温和舍曼不得不设计一种能辨出抽出的文字是毫无意义的，还是有意义的方法。他们通过让它做统计试验而做到了这一点。计算机计算抽出的文字中某些字母对的频率，并将这种频率与已知的英语频率进行比较。如果频率相近，计算机则将抽出的文字贮存起来以供比它更有文化的主人细读。

到目前为止，一切顺利。但该系统的成功有赖于鲍德温和舍曼用正确的密钥文打字。关于这一点，他们即使拥有现代密码学的一切手段也不会比沃德干得好多少。实际上，沃德本能更轻易地做到这一点，只因为在 1820 年时出版的文献较少，因而可供选择的候选密钥文也较少。不过，霍兰公布了几个秘密线索：“3.19”和“如果你知道它以 C 打头，它会有助于你吗？”这第一条线索想必是卡尔·萨根（Carl Sagan）姓名中的大写字母，因为 C 是字母表中的第三个字母而 S 是第十九个字母。第二条线索适用于《宇宙》一书，因为它是以 C 字母开头的。时间一日一日地过去，仍没人破译出“密码员”。于是霍兰不断地透露出有用的线索，供给并鼓励人们给出难题者打热线电话。

“1985 年 3 月初，”，鲍德温回忆说，“霍兰透露出一条线索：密钥是《宇宙》第六章一个首字母系列。我们推断出他说的是单词的首字母，因为没有足够的行或句来构成由那些行或句的首字母组成的密钥。我们雇了个人打印这一章，到 3 月中旬我们一直在进行这个项目，但我们一直未获得相对应的文字。我们试了试霍兰实际上所用的策略：从第一个单词的第一个字母开始，编号为 l，以此类推。到第二百五十六个单词时我们都很顺利，第二百五十六个单词是 c，它是 circa（大约）的缩略语。我们想，既然它代表着一个单词，霍兰一定会把这个 c.算上的。而实际上他把它省略了，这意味着我们编号的其余每个字母都差一个数，这一微小差别产生出毫无意义的文字。”

“还有其他一些特别的东西。萨根在某处写了 Jet PropulsionLaboratory（喷气推进试验室）的缩写 JPL。这个 JPL 是算 1 个词还是算 3 个词呢？霍兰却把它删去了。这个 c.，JPL 以及其他一些混杂的东西——首字母缩略词、脚注、图片说明、用连字号连接的词以及文中的数字——打破了我们的程序。当我们开始时，我们把密钥文想象成与《独立宣言》相类似的东西，《独立宣言》不同于《宇宙》那样的现代文

献，很少有那种混杂的文字。直到这种游戏的最后我们才感觉良好，看！我们的程序倍加小心地对数千个不同策略进行尝试——选择每个元音之后的字母或其他我们所能想出的不可思议之物，但它却不特别善于对该文进行处理，不善于确定什么是单词及什么不是单词。我们发现，处理首字母缩略语、脚注、用连结号连接的单词及其他混杂的词有大约 60 种不同的方法。我们没有指定这个程序做这些，我们也不打算用手将它们全部试一遍。”

3 月 27 日，舍曼和鲍德温设计出一种方法，能巧妙地识别信息部分与一部分密钥文的对应，这种方法避免了如何处理该文的特殊文字中出现的问题。他们注意到，在密码文中的许多地方，毗邻的密码符号号码数相近。比方说，在某处有这样一组号：867、877 和 860。其间最大差为 17。把没有混杂的密钥文中的 17 个连续词（从 860—877）集中起来，并依次将它们编上号，这样，他们就能推导出 867、877 和 860 的明文字母。他们实际上是在更为详尽的范围内这样做的，为的是可以推导出足够多的明文字母以便能对之进行统计数字分析。与以前一样，该程序是把推导出的文字中成对字母的频率与已知的一般英语的统计数字相比较。

3 月 29 日，计算机找出了一段显示出适当统计数字的文字摘要。鲍伯开始寻找对应文字，一直到写出卡明斯的诗句。“真有趣，”他说，“但从统计上说，全部英语文章的 99.8%都比诗更接近于普通英语。例如，该诗用了 15 次 no 和 you 两词。但与非英语相比，这诗与英语相近多了。我们所幸的是我们在这种统计中有足够的余地。”如果他们认为卡明斯很糟糕，他们应庆幸霍兰所爱的诗不是格特鲁德·斯泰因的诗。他们的程序拿什么处理“Rose is a rose isa rose”中字母的频率？

对舍曼和鲍德温来说，不幸的是“密码员”竞赛提交答案的最后日期不像他们所认为的是 3 月的最后一天，这天只是最后一个营业日。“难以想象我们竟没有认识到这一点，”鲍德温说，“我们认为我们是麻省理工学院的学生，因此我们不一定要细读其规则。”实际上他们略感慰藉的是，他们赢得了全部的 10 万美元，不然的话，他们不得不与其他 36 位及时提出解答的人平分。“此外，”那个从不会放过任何一个计算机会的鲍德温说，“我们许诺过把奖金的一半给这所大学作为财政援助。其余一半由阿兰、打字员和我分掉。你知道，打字员之所以占一定的比例是因为我们不能支付他钱。那样算，我的一份是 700 美元。天哪，我做两天的咨询工作就可挣这么多钱。”如果咨询业务停顿，鲍德温总可以通过整理他们有关比尔密码的计算机化译密系统来追寻比尔的宝藏。不过，查明比尔的密钥文是个恼人的问题，迄今为止，无论是先进的密码术还是电脑数字处理都无济于事，此外，比尔可不像霍兰那样在附近向你透露线索。

第二篇　形状

人类在发明车辆、使用金属、创造文字之前就具备初步的数学知识。史前的人工制品表明人类早期借助于计数棒上的刻痕进行计算。例如：在捷克斯洛伐克出土的一根 3 万年前的狼骨上面，刻有 55 道深深的刻痕，5 道刻痕为一组。早在埃及和美索不达米亚的古文化时期，人们就懂得几何学和算术，虽然现存的文物史料很不完备，不足以说明当时人们掌握这些知识的程度。亚里士多德认为，埃及僧侣们在闲暇时间里致力于研究，从而发展了几何学。但是希腊的历史学家希罗多德则认为，几何学能在埃及发展起来完全是出于需要。尼罗河每年泛滥的洪水淹没了沿河流域的大片农田，冲毁了农田地标。埃及人每年都要重新测量土地，需要掌握角度、方向和长度等方面的知识。无疑，建造埃及的大金字塔也需要几何学知识。

大多数古代文化和原始文化表明，当时人们似乎对几何图形有所了解。当然，可能人类天生就有完整的图形概念。甚至“把妻子错认为帽子的人”——一位患有精神病、不能辨认人和物的音乐家奥利弗·萨克斯——却能识别几何形状。几何学作为数学的一个学科，今天仍然保持其活力，几何学家们仍在最简单的几何图形中有所发现。

第五章　制作复活节大彩蛋

凯·麦肯齐是加拿大艾伯塔省韦格勒维尔镇的一位议员，当她谈论起计划在镇里的一片荒地上建造一个 3 层半楼高的复活节彩蛋时说：“这是我所想到的最好的主意。”该镇位于埃德蒙顿市以东 55 英里，是一个寂静的乡镇。荒地对面是一家私人疗养院，这里经常受到龙卷风的袭击。韦格勒维尔镇的 5，000 居民大部分是乌克兰人，但麦肯齐本人不是。他们仍然保持着油画《皮桑基》里的基督教复活节的 2，000 年老传统，用鲜艳的颜色给鸡蛋绘出复杂的图案。1974 年，为了庆祝加拿大皇家骑警队成立 100 周年，加拿大政府决定拨专款筹办庆祝活动。为什么不做一个巨大的彩蛋呢？麦肯齐想。鸡蛋象征骑警队为世代居住在韦格勒维尔镇的乌克兰人带来和平与安全。

起初，麦肯齐的镇公所的同事们认为这事很可笑，但她还是说服他们接受了做彩蛋这一建议。他们猜测，拨款委员会在审查无数项建议，如有马背上的骑警、仰首高歌的加拿大鹅和金黄色的枫叶等雕像之后，会接受这一独具匠心的提议的。事实上，提交的许多建议都极其普通，毫无希望。也有许多关于整修老建筑物的提议，就连挂在墙上颂扬骑警的徽章也是事后才提出的。最后，韦格勒维尔镇收到地方商会提供的 15，000 美元的专款，于是立即寻找制造彩蛋的人。

镇领导邀请一位受人尊敬的本地建筑师来制造世界上最大的装饰彩蛋，他也认为这事太可笑。几个月后，镇领导又请来这位建筑师检查其工作进展。他报告说，他认为是在哄骗他，所以他什么工作也没有做。镇领导又请了另一位建筑师，他觉得更可笑。在与 6 家设计公司商谈之后，镇领导与罗纳德·戴尔·雷施先生取得联系，他 35 岁，是美国犹他大学计算机学科副教授。雷施回忆说：

“起初，我也认为这事很可笑，但是，当他们最终交给我这项工作时，我有一年半的时间不再笑了。”

雷施所面临的问题是，有史以来，除了鸡能产蛋之外，还没有任何人制作过蛋形物，而且生物学家也不十分清楚鸡是如何制造蛋的。根据可以信赖的《大不列颠百科全书》收载，鸡每年大约产蛋 3，900 亿次。但家鸡，要生成一个完整的蛋大约需要 24 小时，开始时在鸡卵巢中形成蛋黄（卵细胞），初期的鸡蛋黄开始进行漫长旅行，走走停停、缓慢地通过输卵管。输卵管是一条从卵巢通到产道的管形通道。最初，鸡蛋停止不动 3 个小时，吸收从输卵管壁细胞中分泌出来的白蛋白（蛋白）。而后鸡蛋前进到输卵管的某一段，在那里停留 1 个小时，接受卵膜，成为蛋壳的内膜。最后，鸡蛋移向子宫，在那里停留 24 小时，积聚白垩质堆积物，这些堆积物硬化后成为蛋壳。至此，鸡蛋总是以较细的一端在前移动，但是在其产出之前半小时，它会急速翻转，所以在产蛋时，鸡蛋是粗端先产出来的。

最初，鸡蛋是液体结构。在没有外力作用时，它是圆球形的，这种形状与其他物体的接触面最少。设有一定量的液体，在所有可容纳此液体的形状中，球形的表面积最小。雕鸮与翠鸟所产的蛋实际上都是接近球形的，但是大多数鸟蛋都类似于鸡蛋，都是椭球形的，这是由于输卵管肌肉收缩挤压着把蛋向前推，从而改变了鸟蛋的球形形状。

事实上，所有形状本质上都具有某种功能，无疑，即使科学至今尚未

证实形状的具体功能是什么，而蛋的形状也不例外。也许，这与蛋类的滚动有关。如果鸡蛋都是球形的，那么它们容易滚走。某些海鸟，如栖居在北部海域的一种海雀——嘴又细又长的海鸠，所产的蛋比起鸡蛋来，更不像球形。海鸠蛋的形状很像一只陀螺，其动力学结构使之滚动时不会直线滚走，而是紧绕着环形滚动。与筑巢鸟相比，海鸠就像一个冒失鬼，它摈弃鸟巢，把陀螺形的鸟蛋直接产在海岸边光滑的悬崖边缘上，这是海鸠的幸运。

鸡蛋和许多其他鸟蛋都是一端比另一端粗些，这就是说蛋类能够在巢内紧密地堆放在一起，可比球形蛋堆放得要多。美国伯洛伊特学院鸟类学家乔尔·卡尔·韦尔蒂写道：“如果双胸斑沙》鸱（北美鸱科鸟一种小水鸟，以其悲哀、尖刺的叫声而闻名）的巢里 4 个鸟蛋排放混乱的话，母鸟就会将其细端朝内重新排列好蛋，非常像一块块薄馅饼，这不仅使亲鸟能更好地覆盖鸟蛋，而且由于其密集的排列使鸟蛋从鸟体上得到的热量散失得比较缓慢。

也许，蛋类的形状还有助于增加强度。它毕竟需要在■巢亲鸟的体重压力下不至于破裂。我们已经知道蛋的大小与蛋壳的厚薄度，鸡蛋的强度是蛋中比较强的，但它还不是非常强的，还不能像传说中所说的，能在大力士手中纵向紧握挤压下幸存下来。也许这位神话中的大力士能把一本电话号码簿撕成两半，（传说中的鸟蛋强度已被最新的广告用来招徕顾客，广告图片描绘了一个 C 形铁钳钳住的没有破裂的鸡蛋。）实际上，你也不会是一个只用单手打破鸡蛋的男子汉；而我在 6 岁时就曾用一只小脏手打破过鸡蛋。可见，科学是进步了，但厨房的地板却一塌糊涂。

雷施说道：“如果一位壮汉在鸡蛋表面上均匀施加压力，他将不能压破鸡蛋。这在理论上可能是正确的。然而实际上，没有一个人能够均匀地施加压力，总会在某点上大于另一点，因而鸡蛋就会破裂。在许多教科书中，人们总想说明，若在一大堆鸡蛋的上下铺些灰泥，大象站在上面，也不会压碎它们。这也只能说明任何一种结构的真实性：如果你能正确地施力，那么结构就能承受。而在现实世界中，却从来没有正确施力的。”

对此，雷施考虑，怎样工作才能使他从理论上和在实际中都成为一位理想的制作复活节彩蛋的人，他可以从图纸上的设计中看到那个高达 31 英尺、重达 2 吨半、像纪念碑一样庞大的复活节彩蛋。雷施的生活中有一句简单的座右铭“志在四方”。有时，他会离开美国几个月，到印度去思考，有时，他会在大学或研究中心附近开设商店，并从事他的几何图形艺术和计算机图形学研究工作。然而在大部分时间内，他都是到处走动，受聘于那些在几何设计方面需要帮助解决各种棘手问题的人，如他在韦格勒维尔镇的朋友们。由于雷施在数学或工程方面没有经过正式的培训，因此他所依靠的主要不是分析方法，而是靠他头脑中形成几何抽象概念的能力，然后用他自己的双手（目前则是用他的计算机打印机），把这种思维的抽象概念转化成为物理实体。

他曾为设在弗吉尼亚州的美国国家航空航天局的兰利研究中心设计过预制的航天飞机舱室组件。这些组件能够紧紧地装在运载它们进入太空的航天飞机载货架上，在太空展开后可以连接在一起，形成巨大的太空站结构。影片剧本《星际旅行》的制片人曾雇用他设计一种外星飞船的嘴；制片人告诉他，要把嘴设计成貌似器官而且具有高科技的特点，他终于设计

出这种神秘太空飞船的技术嘴，能够在其飞行途中吞没一切东西，包括星际飞船“企业号”在内。他也为荷兰的一家多国包装设计联合大型企业——范利尔皇家包装工业公司设计出一种高效的装箱方法，可把类似苹果和李子等球形水果更多地装入条板箱内。

找出一种最密集地堆积各种不同几何状物体的方法，是数学中一个古老的问题，它曾引起过许许多多的争论。例如 1694 年，伊萨克·牛顿就曾与牛津的天文学家戴维·格列高里进行过关于球形问题的争论，所有一样大小的球形，能够与任何一个同样大小的球形接触，其最多数目是多少，格列高里说是 13 个，而牛顿却认为是 12 个。这个问题的讨论持续了 180 年，最后证明牛顿是正确的。

在第十三个球形的周围放置 12 个球形,是已知的最密集堆积球形方法中的秘诀。设想在类似桌面般的平面上把一串球排成直线。接着，紧靠着第一行球放上另一行球，并使这行球落入另一行各球之间；于是任何一个球都会与另一行的两球接触。放上更多行球，直到整个桌面放满为止。增加第二行球，须使它们处于第一行各球之间的空隙处。然后在第二行球的空隙处放上球。使其形成第三行球。如果这种层层放球方式不受桌面限制，而是放满整个空间，那么球形会占该空间的 74%。换句话说，需要浪费 26%的空间。没有任何人知道是否还有更密集的堆积方法。

当雷施开始为范利尔皇家包装工业公司考虑苹果和李子的包装工作时，他假设球形水果要装在长方形的条板箱内装运，那么它们须按这两种已知的最密集排列方法中的一种装箱。他按该方法着手进行了几个月，直到他突然想到，已知的最密集的堆积方法是数学上假定整个宇宙都充满着球形。但是，在现实世界中，他所涉及的只是一个很小的有限体积，一个 3 英尺×4 英尺的条板箱。由于这种意识，他认为自己是能够解决这个问题的，但是他却得到了重要的经验教训：世界本身会给人以各种各样的约束，而这些约束是纸上谈兵式的推理所难以发现的。（雷施拒绝透露他的解决方法，因为尚未获得专利权。）

雷施喜欢说的一句话是设计就是“设计师与环境之间的一种来回反馈”——这也是对他自己的事业所做的描述。雷施是在美国密苏里州的独立城长大的，他回顾了关于他参加专业体育的情况。

在中学时，他曾是一位获得足球、篮球和田径运动 3 项荣誉证书的优秀运动员，但是当他在大学 3 年级时，体检时发现心脏有杂音，迫使他完全放弃了体育。“我的双手总是好的，”雷施说道。他不再把全部精力消耗在运动场上，而是把它引向艺术，特别是雕刻艺术，为此，他获得美国衣阿华大学的奖学金。

昔日在衣阿华大学时，他曾学习过工业设计，并一直在那里读书，直到 1966 年获得了大学主修课目的学位。但是，由于他在工程方面没有经过技术训练，因此不能在工业方面得到一份工作。雷施回忆说：“各类公司无不对我加以非难，因为我未修任何一门数学课程。当时，人们认定我一钱不值，而我也无可奈何。然而，今天我觉得我应该辩白。我能够制作东西，不像学校正在造就的那些聪明的傻瓜，他们身为工程师，能够理解所有抽象化概念，但却不能制作螺母和螺栓。使我感到高兴的是，现代的几何图形的设计，是在物理学、化学和计算机科学领域学科做出重大成就的关键。”

雷施的设计方法是采用一些基本的、最小的图形、同时探讨可以变换成为比较复杂结构的所有方法。“我已经从事一种职业，”雷施说道，“一种研究最简单的形式，即一张纸的职业。”并且探求以各种各样的方式弯曲和折叠一张纸时会出现什么样的形状。雷施接着说：“它不是折纸艺术，目的在于产生一种可以认识的形状。我所感兴趣的只足创造一种有规则的、积木式的形状。”而且，他已经这样做了——有些工作可以说是多余的。整整 20 多年，他已经把许多单片形式（纸张、铝箔和其他材料）变换成为可展示某种图案或规则结构的三维形式。他曾经在一些艺术陈列馆内展出许多较有意义的作品，而且他相信，沿着这条道路走下去，某些作品可以获得专利权，然而他不能证明，用单张纸折叠成为重复图案的所有可能的方法。

雷施还说道：“我承接了制作复活节彩蛋的工程项目，因为我认为它不难。当时，我刚好用纸折成了圆顶形结构的图样。这种结构看来很像鸡蛋的一端，因此我认为，我可以制作出两个这样的圆顶形结构，并在它们之间放置一个鼓起的圆桶，再把三者连接在一起。”那么，它就会立即成为一个复活节彩蛋。雷施已经开发出一种计算机程序，可对折叠纸的结构进行模拟，因此他认为，只要稍加修正，它就可以模拟鸡蛋。雷施回忆说：“当我承接这项工作时，我曾以为，在人类历史上，一定有人研究过理想鸡蛋的数学。”他指望，通过对鸡蛋数学与他的几何学模拟加以比较，能够分析判断出这项模拟令人满意的程度。

然而，雷施很快发现，在文献中没有关于鸡蛋的理想公式。对于许多已有名称的形状，文献中不仅含有代数式，而且还有作图的方法。以圆形为例，它很简单，是一平面上所有与该平面内某点等距离的各点集合。要作一个圆，可把一根细线的一端环绕系在一支铅笔上，另一端用图钉固定在一张纸上。绷紧细线，并使铅笔直立在纸上，环绕着图钉转动铅笔，结果就画出一圆形。在某一点上，扭转摆动甚至能使这个简单作图过程成为人们的笑料，在这个问题上，我曾从数学家马丁·加德纳那里听到：“妈妈，妈妈，为什么我总是绕着圆形走？”“闭嘴，孩子，不然我把你的另一只脚也钉死在地板上。”

从圆形到球形则是很容易的一步，想象把孩子的一只脚（或者细线的一端）钉死在三维空间中的一点上，然后沿四面八方转动小孩挺直的身体（或者绷紧的细线端上的铅笔），观察小孩头部（或者铅笔尖）所画出轨迹的形状，换句话说，你可以把球形看成是急速旋转圆形所扫过的形状。

当然，鸡蛋更接近于椭球形（它是急速旋转椭圆形所扫过的形状），而不是球形。即使是疯狂的数学家也不可能用快速旋转小孩的方法产生出一个椭圆形，但是，利用一支铅笔和一根用图钉固定其两端的松弛细线，就能很容易地画出椭圆形。

鸡蛋不同于椭圆形，其一端比另一端粗些，但是，这种不对称性并不意味着它不能用数学式表示。的确，这要回溯到 17 世纪，法国学者雷内·笛卡尔（“我思故我在”）就曾探索过卵形曲线的代数式。两个世纪以后苏格兰的数学物理学家詹姆斯·克拉克·麦克斯韦，继续进行笛卡尔的工作，扩大了他的研究成果，麦克斯韦曾以他的定量证明电与磁属于同一种现象而出名。当时，麦克斯韦只有 15 岁，他曾向苏格兰早期科学协会——爱丁堡皇家学会递交一篇关于卵形的论文。论文是被热情接受了，但是，令人

敬畏的学会却拒绝让这位小人物就这个论题向他们说教，从而错过了一个引人注目的场面，即用铅笔、细线、图钉并以小小的技巧就能画出卵形曲线图。

雷施的主要问题是，虽然你曾见过一个鸡蛋，可是你却未曾见过所有的鸡蛋。鸡蛋在形状上都略有不同，他有责任辨明鸡蛋的理想形式。经过一个时期的挫折之后，他同农业部联系，并收到了一本鸡蛋分级手册。“ 我认为，”雷施说道，“ 手册里肯定有鸡蛋的定义。然而我发现，它全部是标明 A、AA、B 和 BB 的图片。最后，我终于归结出一个可似称为理想鸡蛋的形象。于是，我给它拍成照片，然后在我的计算机程序中把它数字化。”雷施和两名研究生昼夜工作了 6 个多月，想把折叠纸结构转变成为一个蛋形物。可是，所得到的结果都被否定了。“ 我们不知道错在哪里，是计算机程序有误呢，还是几何图形不对，或是数学计算出了差错？”

类卵形的作图

将细长线的一端固定在 B 点上，然后两次环绕铅笔和一次环绕 A 点的图钉。最后把另一端系在铅笔上。绷紧细线，就可以画出卵形的上半部。而后倒转细线和铅笔组合，就可以画出卵形的下半部。

雷施抛开他的计算机程序,把曾经为他很好地服务了 20 多年的折叠纸技术搁置一边，再整个从头开始。他的方案是，把复活节彩蛋处理成好像一种三维的拼图玩具，由许多平面砖以微小的角度变化连接在一起，拼成彩蛋，从理论上讲，拼图的平面砖可以有各种不同的构型，而达到预期的目的，然而，雷施所需要的不仅是数学上的解法。雷施所用的平面砖必须进行加工，出于经济上的考虑，重要的是那么多的平面砖在形状和大小上应尽可能地一样；那样就可以出自同一模子了。

在二维中，用瓷砖拼成棋盘格子状，图形的平面完全由平面砖（直线形的）不重叠地覆盖着，这种图形历史悠久，而且丰富多采。早在 3 世纪时，亚历山德里亚的天文学家帕普斯就对蜂巢的几何结构感到惊奇，这种结构已被认为是蜜蜂在建造六角形（六边形）巢室时具有的“ 某种几何学上的深谋远虑 ”。在蜂巢中，由六角形镶嵌的平面可以节省蜂蜡，因为两个巢室可以共用一个巢壁。而且，帕普斯认为它的绝妙处还在于没有外来物质能够进入（蜂巢室）间隙中，从而不会弄脏（蜜蜂）酿出的蜜。帕普斯还观察到，除了正六角形之外，在正多边形中（所有边、角相等的直线图形），只有正方形和等边三角形可以角对角地贴面铺在平面上，然而，对于蜜蜂来说，六角形的优点，是因为它在一定的周长内能够包容最大的面积。换句话说，在这 3 种等边图形中，只有正六角形才能以最少的蜂蜡消耗装进最大数量的蜂蜜。

我们容易相信，帕普斯并没有忽略任何一种可以在平面上贴砖的正多边形。关键条件是这些多边形能够排满一个顶点周围的空隙。要做到这一点，分别需要有 6 块正三角形面砖、4 块正方形面砖和 3 块正六角形面砖。这 3 种多边形能够包围着一个顶点，是因为他们的内角（三角形为 60 °，正方形为 90 ° 和六角形为 120 °）能够除尽 360 °。其他的正多边形则不具有这种性质。例如正五边形，其内角为 108 °，所以在一个顶点周围铺贴 3 块正五角形面砖，平面上尚留有 36 ° 未能贴满。

六角形蜂房的优点

在所有二维图形中，给予一定的周长后，圆形含有最大的面积。但是它不适合于蜜蜂的巢室，因为在各个圆形之间，将有许多空隙浪费掉。六角形的另一种优点则来自它们的共用邻边。6 个外围的六角形可以产生一个“免费”的内六角形，因为内六角形的每边都是共用的，然而 6 个外围圆形却不能产生一个“免费”的内圆形，因为这些圆形没有共用的圆周，所以内圆形必须另行绘出。由 6 个外围六角形的共用邻边所形成的“节约”，则更为微妙。6 个外围六角形仅由 5 个六角形的周边长度构成。7 个圆形是的的确确的 7 个圆形,而 5 个六角形实际上可以形成 7 个六角形。

如果放宽要求，那么可以在贴砖中使用一种以上的正多边形面砖，但所有的顶点都应该一致（即在顺序方面，贴在任何一个顶点周围的正多边形面砖都要与任何其他顶点一样），因而还可能有另外的 8 种贴砖方式。无论你是喜欢用数学的分析方法，或是喜欢从经验上的判断，既可以通过纸上谈兵式的分析，也可以通过对浴室地板花样的综合调查，你会相信，不可能还有其他的贴砖方式。

到现在为止，我们所论述的贴砖方式全都是规律性的，它们都像壁纸那样，是重复的。每一种贴砖方式都含有一块“籽砖”，即贴砖中的最小单元，从总体上看，贴砖都是它的多次复制。如果你有一块籽砖的橡皮图章，那么你可以重复地使用它，只要上下或左右地移动，不需要转动它，就能做出整个贴面。在只由一种正多边形面砖（正三角形、正方形和正六角形）组成的 3 种贴砖方式中，籽砖显然是正多边形本身；蜂巢式的贴砖是由一个正六角形产生的。方形的贴砖是由一个正方形产生的，而三角形的贴砖则是由一个等边三角形产生的。荷兰艺术家 M.C.埃歇尔就是以他的规律性贴砖方式而著名，他的贴砖通常都不是正多边形，而是这类或那类的动物。

至于非规律性的贴砖方式，则不复杂。画出一张方形贴砖图。设想把每块方形面砖沿其对角线分为两个直角三角形。可以由你决定沿哪条对角线把每块方形面砖分开，但是所有方形面砖的分开方法则应使其直角三角形的整体贴砖方式形成非规律性的。这种非规律性的贴砖方式不能再简单了：它只由一种面砖——直角三角形面砖组成，而且，即使它不具有籽砖，从某种意义上讲，也仍然可以断定，三角形组成方形。

无须费力，就能把这种非规律性贴砖方式中的直角三角形重新排列成为周期性贴砖。要做到这一点，一种简单的方法，就是在每两块面砖组成的方形贴砖中，把对角线从左上角到右下角的那些方形移动 90 度。这样就可使所有的对角线方向一致，而籽砖就成了组成任何方形贴砖的两块直角三角形面砖了。

非规律性的贴砖方式也可以由任何数量的不同种类面砖贴成。这种数量上的不受限制，使得非规律性贴砖方式可供那些在几何图形上喜欢附庸风雅，希望浴室地板花样独特的人选用。要用两种面砖贴成非规律性贴砖，我们还得从方形面砖开始，然而，我们不是把它们沿对角线分开，而是在每块方形面砖的西北角或东南角刻出一条三角形刻痕。像前面一例的，我们选择的是没有图案的两角，而所有的刻痕则是同样尺寸的。其结果是非

规律性贴砖方式都由直角三角形与不规则的五角形组成。而且，这些面砖也可重新排列成为规律性式样，比方说，把每一块东南角有三角形刻痕的面砖取出，并把它们转动 180 度。

早在 60 年代初期，数学家们就认为，在至少以两种不同形状面砖为基础的任何非规律性贴砖方式中，必定存在一种用相同形状的面砖（或这两种不同形状面砖的子集）排列而成的规律性贴砖方式，然而他们还不能对此加以证明。1964 年，哈佛大学的一名研究生岁伯特·伯杰论证了这种看法是错误的。10 年以后，正当雷施研究复活节彩蛋时，牛津大学的理论物理学家、富有充分想象力的罗杰·彭罗斯提出了两种新面砖，它们称为风筝和飞镖，达到需要的目的。如图中所示，风筝和飞镖必须角与角连接在一起，但有些边则不能与其他面砖的边相接触。在面砖上做出凸起和凹口来限制它们，以免排列成不需要的形式。

令人惊奇的是，风筝与飞镖能够以无限多的方式在平面上贴砖，其中没有一种是规律性的，但其图案可具有高度的对称性，它们本身总是没有重复就终止了。

最值得注意的是，在这些贴砖方式中，任何一种贴砖方式中的有限范围往往是无穷尽地出现在该种特殊贴砖方式中的其他地方，也往往是无穷尽地以每隔一个贴砖的形式出现。马丁·加德纳在《科学美国人》的封面故事人物一文（1977 年 1 月）——彭罗斯面砖爱好者必读——中写道：“要知道这种情况是多么的奇妙，设想一下你生活在一个无限的平面上，它由彭罗斯的无穷无尽的贴砖方式中的一种来镶嵌成花纹状。你可以在不断扩大的面积内，一块一块地检验你所贴好的图案。不管你检查了多少块，总是不能确定你究竟是在哪一块贴砖上。不管你走得多远，或分区划片地检验也无济于事，因为所有这些范围都属于一个大的有限范围，里面所有拼图也都是准确地多次重复。当然，这对任何规律性的棋盘结构来说都是正确的，也是无关紧要的。然而彭罗斯的世界却不是规律性的，在无穷无尽的各种方式中，它们彼此各不相同，而且也只有在不能达到的界限处，才能把一个与另一个区别开来。”

如果这还不足以使你兴奋的话，接着加德纳又解释了另一个值得注意的特性，该特性由剑桥大学的数学家约翰·霍顿·康韦发现。假设你生活在某一城镇中，它是一个任意大小的圆形区域，该城镇是彭罗斯世界中的某处。你必须走多远才能发现一个完全相同的城镇？康韦证明了，远于你所在城镇的直径两倍处，你都不必去尝试！而且，如果你突然要迁往彭罗斯世界的无穷无尽的任何其他处，那么你也总是要迁往远离这座城至多直径两倍之处，那里就有与原住地相匹配的地方，而且很可能就在至多直径一倍之处。

彭罗斯的宇宙论的含义也是令人大吃一惊。只要用两种简单的基本组合，或者说原子，就能创造出数量无限的世界。所有的原子世界在任何可想象的有限范围内都显示出惊人的规律性，然而在宇宙范围内则显出独特的不规则性。

尽管雷施的设计工程近于幻想——一大群复活节女郎都搬不动如此巨大的复活节彩蛋，但是他所关心的事则很实际。他知道，在贴砖模式方面的大量数学与建筑学文献，仅仅适用于平面，而不适用于蛋形的曲面，面

对前景莫测的挑战，他绘制了一幅卵形图，图上画有纬度线。换句话说，他想象复活节彩蛋是由许多条形构成的，一条带叠在另一条带上，在每条带上分别贴砖。然而，对这种自然概念的计算机模拟表明，即使每条带都很细，而且面砖的数量又很多，人们的目光仍然会放在各条带上，而忽视整体的形状。

雷施放弃了带状结构，转向另一种最简单的图形结构，等边三角形结构。经过了 6 个月的思考和模拟之后，雷施认为，用 2，208 块同样大小的等边三角形面砖和 524 块三点星形面砖（等边但不是规则的六角形）就可贴成复活节彩蛋，三点星形面砖的宽度略有不同，它根据贴在彩蛋上的位置而定。面砖连接的角度都有变化，彩蛋中部隆起处小于 1 度，到末端处仅为 7 度。由于角度这么小，即使由平的面砖组成，彩蛋也呈平滑弯曲状，三角形面砖是用经过阳极化处理的铝片制成的，重量 2，000 磅，厚度为八分之一英寸；星形面砖的厚度则为其一半。用于固定的内部结构重 3，000 磅。彩蛋的长度 25.7 英尺，宽度 18.3 英寸。

雷施说道：“ 从未用这么大量的同样面砖贴成像彩蛋这样的三维表面。例如，航天飞机上的隔热砖都是形状各异的。如果航天飞机的设计师已经了解我的有关工作，或者我知道他们的问题，那么航天飞机就可以像贴彩蛋那样贴上隔热砖。这样，他们还可以携带备用的隔热砖进入太空。 ”可实际上由于航天飞机上的每块隔热砖都不同，所以它也无法携带备用隔热砖。航天飞机在高速通过大气层时，隔热砖往往会脱落，这时要贴上一块新砖就必须进行加工。

雷施还说道：“ 当韦格勒维尔镇雇用我时，协议是由我设计复活节彩蛋，由他们负责建造和油漆。然而，我很清楚，若不约请一家航天公司加工彩蛋面砖，韦格勒维尔镇将无法建造彩蛋。他们肯定担负不了这项工作。所以我告诉他们，还是由我来建造并油漆它。 ”

面砖的油漆，要在它们组装起来之前进行，此事牵扯到一些让步。该镇希望复活节彩蛋要用色彩鲜艳的红、蓝、绿、橘黄颜色粉饰，而且期望油漆的鲜亮色彩能够保持 100 年。雷施告诉他们，彩蛋使用这几种颜色油漆，每隔 3－5 年就要重新油漆一次。最终选用了 3 种颜色——金色、银色和青铜色，这几种颜色可以保持其光泽半个世纪。

在雷施开始建造彩蛋之前（要把这些面砖在内部连接在一起，而且不能看见其连接头，为此用了 6， 978 只螺母和螺栓以及 177 根连接到中心轴上的支杆），镇的管理条例要求有一位土木工程师或建筑师证明该设计在结构上肯定安全可靠。必须注意到，韦格勒维尔镇经常遭受每小时 100 英里风速的飓风袭击，当地的工程师或建筑师没有一位愿意证实，如此巨大的新奇形状在结构上具有完整性。“ 人们害怕，大风可能把它刮跑，”雷施回忆说，“ 我也承认有些担心。在建造彩蛋时，我成为指责的目标并受到了指责。 ”那时候，该工程已获得了势头，而且镇上也完全放弃了需要证明的规定，韦格勒维尔镇的许多居民都在打赌，所赌的不是彩蛋是否可能倒塌，而是如何倒塌（翻倒还是刮跑）以及何对倒塌（建造时还是建造后）。

雷施带领一队志愿人员组装复活节彩蛋，历时 6 星期。他们曾经历过一次侥幸脱险。当彩蛋的上端部分组装完毕并安装在中心轴的顶端上时，它看来很像一把巨伞。这时空中狂风暴雨肆虐，龙卷风席卷而下。雷施及

其伙伴花费整夜时间，把这个伞形结构转向顺风，使它不会被风刮走。

这座复活节彩蛋不仅要顶住自然力量，而且还要面对人们的愤怒。建造彩蛋劳累了一天以后，雷施会累得躺倒在当地一家旅馆中，他听到人们窃窃私语，计划要炸掉彩蛋。他也曾几次接到警告：中学的孩子们声称要炸毁彩蛋。雷施终于弄明白了，在他到达韦格勒维尔镇之前的一段时间内，报纸曾经传播谎言，说镇里把用于建造中学游泳池的经费挪去建造复活节彩蛋。“我只好四处游说，”雷施说道，“竭力向每个人解释彩蛋款项的实际来源，而且学校会有自己的游泳池的。没有人再想要炸掉彩蛋了，可是彩蛋确实遭受过几次来福枪射击。”

在复活节彩蛋完工后很长一段时间里，雷施使用计算机分析其结构的牢固性，并得出结论，它比所需的强 10 倍。雷施说道：“就是全体居民被大风吹倒，复活节彩蛋也不会。”

自从雷施离开韦格勒维尔镇，10 年过去了。当然，该镇依然存在，而这座独具匠心的纪念碑使韦格勒维尔镇出现在地图上（还被收载入女王伊丽莎白的加拿大旅游指南中）。该镇惟一的委屈是这个复活节彩蛋尚未被收入《吉尼斯世界纪录大全》之中。看来这是不公平的，加拿大艾伯塔省的另一个城镇卡尔加里镇就曾因用 20，117 个鸡蛋烹调出世界上最大的煎蛋饼而载入《吉尼斯世界纪录大全》。

第六章　麦比乌斯分子

数学家们吐露，
麦比乌斯带只有单面，
如果你要将它分成两半，
你将会感到十分可笑，
因为分开后还是一条带。

——无名氏

数学不仅可以在最宏大的规模上帮助进行形状设计，如 3 层半楼层高的复活节彩蛋，而且还可以在微小的范围内帮助设计。本章将叙述美国博尔德市科罗拉多大学的戴维·沃尔巴及其同事们如何在奇特的麦比乌斯带中合成分子的故事。

神秘的麦比乌斯带是数学家们的宠物。你可以用一条窄纸条制作麦比乌斯带，例如取一条加法器用纸带，半扭转，再把纸带两端连接，形成一闭合环，就成为麦比乌斯带。

麦比乌斯带只有单边，也只有单面。如果你用一把漆刷沿着纸带方向刷漆，那么你将发现，当漆刷回到起点时，它已漆满整个纸带的表面。如果你沿着纸带的一面做一种魔术记号，那么你也会立即相信，纸带只有一个边。

如果你沿着纸带方向把麦比乌斯带剪成两半，果然，就像五打油诗所说的，它仍然还是一条带子。

1858 年，法国巴黎的一家科学协会为数学方面的一篇最优秀论文颁了奖。在这次竞赛提交的论文中，德国莱比锡市的数学家奥古斯特·费迪南德·麦比乌斯“发现了”这种曲面，就是现在以他的名字命名的曲面。麦比乌斯仅用纯数学观点论述了他的发现，例如，没有讨论自然界中存在着麦比乌斯带分子的可能性。

的确麦比乌斯不会想到诸如麦比乌斯带分子存在的可能性，这是因为当时的有机化学科学还处于萌芽阶段，人们即使对最简单的分子形状也一无所知，更不用说对数学有意义的复杂分子了。在麦比乌斯发现的同时，德国波恩大学的奥古斯特·凯库勒宣布他的发现：碳原子可以连接形成长链，它将成为有机化学的基础。

4 年前，凯库勒在伦敦的公共马车上，首次在幻想中思考了碳链的问题。他回忆说：“那是一个晴朗的夏夜，我乘坐末班公共马车回家，和往常一样坐在‘车顶的’座位上，通过大城市中没有行人的街道，在平时，那是个充满活力的城市。我陷入幻想，并且好像看见许多原子在我眼前欢跳……我常常看到两个较小的原子如何联合形成偶原子，1 个较大的原子如何环抱着两个较小的原子；还有更大的原子如何抓住 3 个甚至 4 个较小的原子不放，同时，它们整体如何跳着眼晕的舞蹈快速旋转着。我也看到较大的原子如何形成链子……无论如何，我也要花些夜里的时间，把这些幻想中形成的形态轮廓写进论文中。”

11 年以后，1865 年，凯库勒认识到碳链子可以环绕着旋转，形成环。而梦幻又一次给他以灵感。“我坐着编写教科书，然而工作毫无进展，我

的思维开了小差。我把椅子转向取暖壁炉，并打起盹来。原子再次在我眼前欢跳。这时较小的原子谨慎地呆在基底上。我的心灵眼睛通过这种重复景象而更加敏锐，现在可以辨别出多种形体中较大的结构，长长地排列成行，有时还更紧密地拼接在一起；整行迂回曲折像蛇一样运动。瞧！那是什么？有一条蛇咬住了它自己的尾巴，嘲弄般地在我眼前快速旋转，仿佛一道闪电，把我惊醒了……当天晚上，我就推断出假设的结论。”

首先，凯库勒推导出苯的结构，它由 6 个碳原子和 6 个氢原子组成。凯库勒断定，6 个碳原子形成六角形，各带有一个氢原子与每个碳原子相连。

自从凯库勒辨明苯的形状以来，120 年内有机化学家们当然发现了更为复杂的分子的形状，诸如双螺旋的脱氧核糖核酸分子。但只是在近些年，化学家们才观察到形状呈麦比乌斯带的分子。

麦比乌斯分子不是在自然界中发现的，而是由戴维·沃尔巴及其同事们在实验室里合成的。开始时，他用形状像一架 3 级梯子的分子合成。（梯子的每级实际上是一个碳-碳的双键，这里可以忽略掉。）然后使梯子环绕着弯曲，再把两端连接，使其实际上形成一个环状物。

环形物中一半仅仅是一条环形带，而在另一半，当它两端连接时，将半截扭转，从而形成一条麦比乌斯带。

麦比乌斯带分子与麦比乌斯纸带一样，都具有许多神秘的性能。如果 3 个碳双健全部断开，那么分子仍然还是单个分子。碳双键的断开，相当于沿着纸带的中线环绕着把麦比乌斯带分成两半。对于分子和纸带两者来说，结果都是单带，只是其周长为原来的两倍。

化学家们很早就已知道，两种化合物可以有同样的分子式（即由同样化学成分严格地按同样比例组成的化合物），但却以性质不同的化学实体存在。如果同样的化学成分以不同的方式或以不同的角度相互键合时，这种现象就可能发生。然而，两种具有同样分子式的化合物，甚至具有同样的化学键，其在化学性质上也可能不同。怎么会有这种可能呢？

一门叫做拓扑学的数学分支学科可以解释这种现象。它是研究物体在不断发生变形时其性质仍然保持不变的数学学科。设想某物体是由柔性橡胶制成。拓扑学家想要知道，当物体受到推拉但不戳破或撕裂时，什么性质仍然保持不变。可用麦比乌斯带这个实例形象地说明这种抽象概念。假设你有一条橡胶的麦比乌斯带，你可以用一切可能的方法使它伸缩。不管你用多少种方法也都不能使它变形，最后得到的形状总是只有单面。因此，只有单面的性质就是拓扑学家们所关心的事。当一种形状能够连续变形成为另一种形状时，从拓扑学上看，两种形状被认为是等价的，所以，不管把麦比乌斯带伸缩成什么形状，从拓扑学的定义来说，它们也都是等价的。

现在考虑两条麦比乌斯带，一条用橡胶带朝某一方向扭转而成，另一条也用橡胶带但朝相反方向扭转制成。

从拓扑学上看，这两条麦比乌斯带是否等价？它们不等价。两者都不可能变形成为另一种形状。如果你从镜子里看这两条带子中的一条，那么

你会看到，其映像很像另一条带；两条带互成镜像。

这里我必须停下来发表一项否认声明，以避免数学家们来信恶意攻击。数学家们都是一群怪人，拓扑学家们都不把自己局限在三维空间之中。而在四维空间中，他们却能证明，镜子里的麦比乌斯带可以互相转变。然而我仍将坚持把我们的讨论限于三维之内，因为我们探究的主要对象分子的形状总是在三维中观察到的。因此，我要重申，在三维中，镜像的麦比乌斯带从拓扑学来看是截然不同的。

成分一样而且化学键相同的两种化学化合物为什么会有性质截然不同的实体，关键在于从拓扑学上看，可能存在着截然不同的镜像。

因为右手和左手都是众所周知的镜像，所以人们习惯地把与其镜像相反的物体称为左手的或右手的。在一对镜像物中，究竟哪一个叫做像，是一个习惯问题。这正如街道的右侧不存在绝对位置一样，它取决于你行走的方向。两种麦比乌斯带已被人们称为右旋和左旋的麦比乌斯带，但是不必担心何者右旋，何者左旋。分子也存在右旋和左旋形式，人们称它们为手性，它是从希腊词“手（Cheir）”借用来的。

右旋和左旋麦比乌斯带都是镜像形状的实例，从拓扑学来看，它们在性质上是截然不同的，但有着等价的镜像形状。现以一简单图形为例，一个圆形是它本身的镜像，显然，从拓扑学上看，圆形与它本身是等价的。

另一个例子是字母 R 及其镜像 Я。若用软橡胶制成图形 R，那么可以用拓扑学的变形方法把它变换成为它的镜像。

可是，分子不是软橡胶制成的，物理的约束力防止它们以任何方式发生变形。尽管如此，R 形分子还是能够转变成为它的镜像，无须弯曲变形——的确根本不需要弯曲。这次，如果把用硬塑料制成的字母图形 R 及其镜像 Я 放在桌子上，那么，只要把它拿起来翻转，就能使其中一个变成另一个。

这种变换由于物体始终保持其刚性，所以叫做刚性变换。

许多有机分子都是刚性的手性分子：它与它的镜像在刚性上是截然不同的。人体明显偏爱某种手征的手性分子。例如，大多数的蛋白质都是由左旋氨基酸和右旋糖组成的。当手性分子在人体内合成时，只能产生具有所需手征的手性分子。

但是，当诸如药物等手性分子在实验室内用非生物方法合成时，结果都是右旋与左旋形式分子的对半混合。当病人服药时，由于难于除掉不是所需形式的分子，所以服用的是混合物。一般说来，非所需形式的分子在生物学上是惰性的，而且只是经过身体，无任何作用。有时还是有害的。60 年代初期，就曾发生给妊娠妇女

服用撦里多米德药物事件。药物中的右旋分子具有所需的镇静药性，而左旋分子却能造成新生儿畸形。

英国伦敦皇家学院化学教授斯蒂芬·梅森在英国周刊《新科学家》发表的文章中，注意到收入标准药物手册中的 486 种合成生产的手性药物，只有 88 种是由所需的手征分子组成的。其余的 398 种全都是对半的混合物。梅森得出了结论：“它们都是在特定环境（人体）中使用，某种手征会得到特别的偏爱。可是，效果又会怎样呢？”

当一位有机化学家分析一种新分子时，首先要做的事是试图确定分子是否刚性的手性分子，即在刚性上与其镜像是否截然不同。这里可借助于拓扑学。从拓扑学上看，如果分子与其镜像性质不同，那么它们在刚性上也是不同的，因为刚性变换只能是许多通过拓扑学完成的变换中的一种。还以上面讨论过的 R 及其镜像 Я 作为例子。在从一个变形成为另一个时，可以得到一种中间的形状 Я，它具有对称性，其左半是其右半的镜像。

两级的麦比乌斯梯拓扑学家们知道，如果一种形状能够变形成为某种具有反射对称性的形状，那么该形状本身就能够变形成为其镜像。这就意味着，如果化学家能够让分子获得具有反射对称性的形状，那么，他就能消除分子的手性。

这种见解往往证明是有用的。沃尔巴已经从三级梯形分子中合成出分子的麦比乌斯带，他请我去直接观察从两级梯形分子中合成的类似方法。所得到的形状是手性吗？如下图所示，由于它能变换成为具有反射对称性的形状，所以不是手性的。

可惜，这种解释对于三级麦比乌斯分子似乎不起作用。经过许多思考实验之后，沃尔巴推测，好像它不可能变形成为具有反射对称性的形状。如果变形后已经显示出反射对称性，那么他就会断定，三级麦比乌斯形状可以变形成为它的镜像。可是，这样的逆叙正确吗？任何变形未能显示出反射对称性，是否意味着分子本身就不能变形成为其镜像？

毛病就出在答案太容易上。沃尔巴请我考虑两只橡胶手套，一只为右手的，另一只则是左手的。

两只手套

手套显然都是镜像的，可是从拓扑学来看，它们等价吗？当然，手套在刚性上是不等价的，因为如果我们像翻转字母 R 那样翻转两只手套中的一只来获得镜像，那是行不通的。然而，如果我们把任何一只手套从里往外翻转，那么就能使手套成为等价。

（拓扑学家因而发现它自己处在一个奇特的位置上，既不能认为手套是右手的，也不能认为是左手的。）在把手套从里往外翻转的过程中，手套在任何步骤都不具有反射对称性。

我们也许能够得出结论，手套是一个反例：某种形状在拓扑学上与其镜像等价，但在其变形过程中却不具备反射对称性。这种结论可能是错误的。只是我们没有让手套充分变形。如果我们使劲拽开手套，那么至少在理论上能够把手套变形成为一个圆盘的形状，这时手套就具有反射对称性（沿任何直径方向都有反射对称性）。

以上讨论的要点是，沃尔巴在化学方面的一些研究已向拓扑学家提出一个重要问题：如果某种形状在变形过程中不可能具备反射对称性，那么是否可以得出结论，从拓扑学上看，形状本身与其镜像不等价呢？这是一个基本问题，但在数学文献上，好像还没有人提出来过。

这个问题整个都牵扯到一个重要的哲学问题：物理科学上的新概念是否常常会启迪出数学上的新概念？或者反之？换句话说，何者在先，是物

理科学，还是数学？许多哲学家遇到过这个问题，这与众所周知的关于鸡和蛋何者在先的问题一样，答案看来是不会令人满意的。

在这两种情况下，人们所得出的结论，似乎不是一个不可置否的证据，而是一个目的性的试验。一些步柏拉图后尘的专横数学家断言，他们的学科是与物理学实际相脱离的。他们认为，即使没有可供计数的物体，数字也会存在。不大固执的数学家们则承认，科学与数学是紧密相连的，但他们坚持数学在先。他们提出群论作为证据，群论是数学的一门分支学科，在 19 世纪 30 年代诞生，它完全没有物理学上的用途，只是最近才被粒子物理学家应用，以便用于研究过去 20 年内发现的亚原子粒子集。

但是，物理学家们则相信他们的学科在先，而且认为历史是站在他们一边。例如伊萨克·牛顿创造了数学中著名的分支学科微积分，就是因为他当时需要一种数学工具，用来分析极小的空间与时间间隔。而我认为，数学与科学都相得益彰，才是惟一公正的结论，尽管这种判断既不鼓舞人心，也不增进知识。麦比乌斯带的故事就是数学与物理科学之间错综复杂相互促进关系的一个很好的实例。1858 年的论文竞赛中提出的麦比乌斯带仅仅创立了纯数学，现在它在化学中发展起来，而且已被化学家们熟练地运用，又为纯理论的数学家提出许多问题。

你可以感到欣慰的是，麦比乌斯带不仅可以服务于化学家，而且也可以服务于工业家。B．F．古德里奇公司已经获得麦比乌斯输送带的专利权。在普通输送带中，带的一侧会有较多的磨损与撕裂。而在麦比乌斯输送带中，应力可分布到“ 两侧 ”，从而可以延长其使用期一倍。

第七章　遗漏了的带一把手的三孔空心球形问题

在 40 年代和 50 年代期间，许多在数学上思维敏捷的人曾经热情地工作，研制出第一部电子计算机。当然，他们成功了，而且在过去 30 年内，数学家们在电子方面的脑力成果已使许多科学领域发生了巨大的变革，然而，可笑的是，数学本身却没有进展。美国斯坦福大学的数学家约瑟夫·凯勒说道：“看看我们这个系，我们拥有的计算机比学校其他系，包括法国文学系在内，都要少。”

“这是很可笑的事，”罗伯特·奥泽曼这样说，他是凯勒的同事，已在斯坦福大学工作了 30 年。“我们缺乏计算机显然是有几种原因，一是由于一些数学家的保守性——他们不愿意花时间去真正学习如何有效使用计算机——另外，他们认为使用计算机要花很多时间，这正是他们自己不愿努力思考的托词。”

然而这些日子，由于前斯坦福大学学生、现在美国阿默斯特市马萨诸塞州立大学工作的戴维·霍夫曼有了一项引人注意的新发现，使凯勒和霍夫曼对计算机在数学中应用的未来更有信心了，借助于改革了的计算机绘图系统，霍夫曼及其同行、美国赖斯大学几何学家威廉·米克斯第三发现了无穷无尽的优美曲面，这些曲面遵循某些严格的标准。而目前已知的只有 3 种曲面符合这些标准。这些奇异的曲面已使麦比乌斯带似乎显得世俗而又平凡。无疑，他们填补了数学上的一项空白，而且还证明了这些曲面像麦比乌斯带一样可以用于数学之外的一些学科，诸如胚胎学与牙科学等多种学科。

计算机对基础数学做出的最著名的贡献是一项“10 岁”的成果，它打乱了老规律。1976 年，美国伊利诺斯大学肯尼思·阿佩尔和沃尔夫冈·哈肯证明了著名的四色地图定理，该定理阐明了用这种方法至多只需 4 种颜色，就能把许多想象到的国家绘制在一张彩色平面地图内，而其中的任何两个邻国颜色不同。

当时，我还是美国哈佛大学的一名大学生，当该证明的消息传到坎布里奇市时，我的微分方程老师中断了讲课，打开香槟酒瓶，热烈庆贺。124 年来，四色地图定理（以简单的辞藻形容，就是多么的诱人）曾经搞乱了著名数学家与献身数学的业余爱好者的步伐，他们都曾徒劳地探索这项证明（或许可以预料地得到了反证）。我和穿着漂亮服装的同学都跟随着我们的老师，高举酒杯，为阿佩尔与哈肯已经攀登上数学的珠穆朗玛峰而干杯。

几天以后，我们知道了阿佩尔与哈肯使用的未曾有过的高速计算机取得的这项证明：1，200 小时的工作量仅用 3 小时就记录完。这项证明若用手工检验，简直是太长了。（好奇的读者可消磨 10 年的时间去研究《伊利诺斯数学杂志》第二十一卷中 460 多页的检验表。）

我还能回忆起当时我们的心绪是多么的烦恼。这项证明不符合那时保罗·厄尔多斯所赞同的数学观点，他是一位到处走动的古稀老人，世界上最多产的数学家之一。厄尔多斯认为，上帝有一本很薄的小册子，书中含有所有重要数学定理的简明的第一流的证明。毫无疑问，四色地图定理包含在该书内，而阿佩尔与哈肯的证明肯定不在其列。

我们的老师和我们都感到沮丧，有些人担心计算机会出差错，因而造

成微妙的误差。另一些人承认计算机有助于定理的证明，但还希望众所周知的聪明的中学生有朝一日会不用计算机就能做出简明漂亮的证明，一项像厄尔多斯心目中上帝所赋予的证明。还有一些人则想知道，那冗长乏味的证明是否就是论题的最后定论；不过，他们都曾猜想过，四色地图定理是整个令人感兴趣的定理中的代表，简单的证明不会存在，也不可能存在。

今天，10 多年过去了，对阿佩尔与哈肯的工作还是没有定论，当然也没有宣告计算机证明的时代的到来。计算机固然已经发现了新素数，而且解出了阿基米德的关于牛的问题，但这不是证明一个定理。事实上，自从四色地图定理以来，还没有一个著名的定理要由机器来证明，霍夫曼和米克斯曾用另一方式使用计算机，它可能是未来的出路。他们曾利用计算机的数字捣弄能力获得洞察力，使他们无须计算机的帮助就能不断取得进展，并证明了一项基本结果。

150 年来，许多数学家都曾研究肥皂膜的形状，而且霍夫曼和米克斯发现的许多曲面都是与这些形状有关的。如果把一铁丝圆环浸没在肥皂液中，然后取出，那么横跨在铁环上的肥皂膜形状是平圆盘状的。这种形状被认为是极小的曲面，因为在可能横跨铁环的所有曲面中，平圆盘形具有最小的面积。

平圆盘状肥皂膜

如果再用两个相距很短的铁丝圆环，一个放在另一个上方，再浸入肥皂液后取出，那么跨过两个铁环的肥皂膜形状叫做悬索曲面，它类似核电厂冷却塔的形状。

悬索平面状肥皂膜

这种形状也是一种极小曲面；因为连接两个铁环的所有曲面中，没有其他曲面具有更小的面积。自然界总是偏爱极小曲面，是因为它们在物理上稳定：最小的面积意味着贮存的能量最小。

可以把极小曲面的概念从肥皂膜的厨房物理学世界扩展到无限的超自然领域，我们把这个工作留给数学家们去做。无限小的曲面的说法似乎像是矛盾的，因为任何曲面要在一个方向或多个方向无限向外扩展，必须有一个无界的面积。如果一位数学家说一个无限的曲面是极小的，也就是说用制作肥皂膜的方法把该曲面充分缩小到有限范围内的最小面积，换句话说，如果你在该无限曲面上任何处做一魔术标记，并画一条非常小的闭合曲线，那么，在该曲线作为边界的前提下，曲线内的曲面将有最小的可能面积。

平面就是无限小曲面的最简单例子；平圆盘状肥皂膜正是一个平面。如果悬索曲面的两端永远扩展，结果也成为另一个无限极小曲面。平面和无限扩展的悬索曲面都是本身不会相交的曲面。它们也都不会自身形成双重曲面，也不会无限接近。

诸如平面和无界的悬索曲面等曲面都可变形，成为一个简单的有限物体：一个具有一些微孔和一些空心把手的空心球形。（不妨在皮箱上画出一个空心把手，它就可以使皮箱中的空气流过空心把手，再回到皮箱。从数学角度来说，每种空心把手都可以用来增加曲面的“连通度”，因为剪断空心把手将不会把曲面分成几块。）数学家们以他们丰富的想象力认为

曲面都是由超柔性的橡胶制成。如果用拉长、压缩、扭转或其他手段，但不包括撕开、穿孔或填孔等方法使这些曲面之一变形成为另一种曲面，那么这两种曲面被认为具有同样的拓扑学结构。

皮箱

例如空心球形就可以拉伸成为卵形曲面，因此这两种曲面具有同样的拓扑结构。

球形拉伸成为卵形

从拓扑学角度来看，平面与穿有单一微孔的球形相同，因为在这种奇特世界里，微孔可以无限地扯开，形成平面，这将使查尔斯·古德伊尔感到悲哀。

单孔球形扯开成为平面

悬索曲面与带有两个微孔的空心球形具有同样的拓扑结构；每个微孔都能拓宽并拉伸到无限大。（总的说来，多孔空心球形的每一个微孔都可以扩展成为无限大。）

双孔球形扩展成为悬索曲面

当霍夫曼和米克斯开始研究时，数学家们都知道，除了平面和无界的悬索曲面外，仅有另外一种无限极小曲面，它本身不会相交，在有孔的空心球形（带或不带把手）上，能用橡胶片的变形来模拟。这种曲面就是无界的螺旋面，它类似于扩展成无限大的螺旋。和平面一样，螺旋面与单孔空心球形具有同样的拓扑结构。

螺旋体

人们知晓的这 3 种极小曲面几乎存在 200 年了,而且过去 10 年的一系列成果也都说明，似乎不太可能有第四种存在。例如，1981 年，美国圣地亚哥市加利福尼亚大学的里克·舍恩就曾证明，带有两孔的空心球形仅能作为悬索曲面的模型，而不能作为无自身相交的其他无限小曲面的模型。同一年，巴西数学家卢奎西奥·豪尔赫则证明了，带有 3 孔、4 孔或 5 孔和不带把手的空心球形都不能成为适宜的模型。

霍夫曼说道：“ 由于在所有特殊情况下都已排除了新极小曲面的存在的可能性，许多人认为，而且试图证明没有新的例子能够存在。他们未能获得成功，但是大家却有一种共同的感觉，认为他们未能成功不是因为他们在无效地试图证明实际上是错误的东西，而是由于他们没有足够先进的数学工具。 ”

1983 年 11 月，霍夫曼获悉，一位名叫塞尔索·科斯塔的巴西研究生，在其博士论文中讨论了提及的曲面的疑难方程问题。科斯塔已能证明无限的、极小的曲面在拓扑学上可与带一把手的 3 孔空心球形相同。

但是，科斯塔和其他任何人都不知道提及的曲面看起来像是什么，因为定义曲面的方程似乎都是相当复杂。况且，也没有人知道曲面是否本身相交。如果该曲面要加入平面、无界悬索曲面和无界螺旋面的极小曲面的

神圣行列，那么它是不容许本身相交的。

自身相交的问题不是一个简单的问题。霍夫曼解释说：“ 当你有一组曲面方程时，你不能计算出某些量，说‘ 是，它自身相交 ’或‘ 不，它自身不相交 ’。而从本质上说，你只能证明曲面的某一块不能与另一块相交。”然而，对于一个无限曲面，这是远远不够的，因为你还必须与无数块曲面相比较。

霍夫曼计划使用计算机去计算曲面核心部分的坐标，然后绘制出曲面核心图。但是，常规的计算机制图学软件爱莫能助，因为它们所包括的主要是工程师们使用的立方形、球形和其他现有的形状，而不包括自身相交或扩展成无限大等奥秘的数学曲面。碰巧，他又获悉，美国马萨诸塞大学研究生詹姆斯·霍夫曼开发了一种计算机图形学的新软件。

另一种新曲面

戴维·霍夫曼说道：“ 我们的对策计划是使用计算机观察面。如果我们看到了它们自身相交，那么我们打算发表一篇有关这个实例的简短论文，排除该曲面可能是无限小曲面的看法。也许我们必须在一本低等的杂志上发表，因为在数学杂志上很难发表这类问题的否定结果。要是我们看不到它们自身相交，那么我们也不知道我们要做什么，只能说证明曲面本身不相交的工作实在太难了。 ”

然而，计算机生成的图形使他们的预料落空。它不仅显示出自身不相交，而且还显示出具有高度的对称性。它含有两条成直角相交的直线。霍夫曼在从不同角度“ 观看 ”曲面核心并经过长期艰苦的思考后，终于认识到曲面可以分解成为相同的 8 块。

在物理学中，眼见为实；而在数学中，就不够了。霍夫曼和米克斯看到了对称图形之后，把图形搁置一边，仅根据方程就证明了曲面本身不相交。出乎他们意料，竟然发现了第四种无限小曲面，这种曲面由两个悬索曲面和一个平面构成，整体像从“ 瑞士硬干酪心 ”中发出来似的。3 个月后，他们证实了存在着无限多的这种曲面，每一个曲面在拓扑学上都与带几个把手的 3 孔空心球形等价。

新球形模型

在霍夫曼和米克斯发表第一个新曲面核心的图片之后，英国剑桥大学的一位生物学家就和他们联系，他认为，发育中的胚胎可能呈现这种形状。最小面积曲面往往会自然地存在于有机与无机材料之间的界面中，因为这样的曲面可使表面张力降到最低程度。美国纽约市的一位牙外科医师打电话给霍夫曼，并且说明该图形看来正好像他们用于移植在假牙上固定假牙的骨质物，霍夫曼说，他认为“ 极小曲面的破坏性较小，因为它与骨质物的接触面较小。而且，还有许多‘ 把手 ’为骨质物履行使命 ”。

即使极小曲面在现实世界中未得到应用，而霍夫曼与米克斯的发现仍然是不朽的。不过它却暴露出有关无限小曲面的最新知识是多么的贫乏，而且它也证实了可以在纯数学研究中利用计算机。但对于将近 200 年来搞不清楚的问题，很难对其在计算机帮助下所取得的惊人进展提出异议。

第三篇　计算机

在发现巨大素数、解阿基米德牛群问题、破译密码、证明四色地图定理以及发现新图形等问题上，计算机证明对数学家是有用的。然而在计算机能做些什么问题上，却还有难以捉摸的限制。

自 20 世纪 30 年代起，数学就面临着一场革命，如同物理学的两次革命——广义相对论与量子力学——一样重要，这两次革命动摇了物理学的基础，并且推翻了关于空间、时间与因果律的经典理论。数学的前景展望也由于美国纽约大学的莫里斯·克林提出了“必然的损失”的说法而完全改观。一种崭新的工作已不再注重于数学计算的能力，而是注重于计算的限制。有意义的计算问题被规定为原理上不能解的，或在原理上能解而实际上无法解的问题。

一个从原理上不能解的有意义的典型问题就是“停机问题”，它是艾伦·马西森·图灵于 1936 年提出的。图灵想到了计算机程序是否迟早会提供结果和停机的问题。停机问题已不仅是纸上谈兵的理论家所关心的问题，而且是很容易在实践中出现的问题。

美国麻省理工学院计算机科学理论学家迈克尔·锡普塞说道：“你可以想象，当你把程序编入卡片，然后提交给计算机中心时，尤其是在这几天里，你是多么想知道答案。他们总是整夜地进行运算，第二天就送回给你。比方说，你有一笔 100 美元的钱存在机内。有时，计算机程序会有一个无限的循环，而且会耗掉许多钱。由于它会陷入无限的循环，因此你从程序上得不到任何东西。不论是你帐上的钱都已耗费完，还是计算机以何种方式注意到机器运行了很长时间，计算机自己停了机。

“那么，你一定会想，为什么事先不检验程序，如果其中有无限循环，就不应该用它运算”。然而令人惊奇的是，这种自然的概念不能够实现，因为图灵证明了，没有一种检验方法能够适用于所有程序。

除了图灵所证明的停机问题是不可解的之外，1936 年数学家向绝对数学知识的虚幻目标发动了另一次进攻。逻辑学家阿朗索·丘奇证明了所谓的判定问题也是不可解的：判定一个已知的语句是否表达一个算术的真值，决不可能有一般的过程。换句话说，能够输出所有算术真值的计算机是不存在的。至于你所给的每一种可能想到的算术语句，计算机也是不能确定其真值的。的确如此，要求找出算术的真值是没有诀窍的。

近几年来，数学界的注意力已从理论上不能解的问题转向理论上能够解而实际上不能解的问题上。在这些问题中，最著名的就是美国国际商业机器公司（IBM）的拉里·斯托克迈耶称之为“内在困难”的问题，即委婉法问题，如果这也算是一个问题的话。他请你构想一部想象中的最大功率的计算机。这部想象的计算机，可以大到充满整个宇宙（直径也许为 1，000 亿光年）。它将由质子大小（直径为 10^{-13} 厘米）的硬件构成，信号将以光速（每秒 3×10^{10} 厘米）在硬件中疾驰通过。它可以就某个问题工作 200 亿年，它超过了宇宙的估计年龄。这个难题具有一个令人不知所措的特点，即它在原则上能够解决，但即使用可想象出的最大功率的计算机，按宇宙年龄再工作上千百万年也无法解决。

这类问题之一是下棋问题，它在棋盘不是普通的 8×8，而是 n×n（这里 n 表示任意大的数目），而且还有不限数量的棋子（但每方只能有一个

王棋）。我们想有一种计算机程序，不论棋下到哪一步，不管我们是哪一方，比如说白子，它都可以用来确定是否能够赢。某种程序只在理论上可行而在实际中行不通，它需要考虑所有白方可能走的棋步，随后考虑所有黑方可能回应的棋步，还要考虑所有白方可能反回应的棋步，以此类推，考虑所有可能继续的棋步，直到结束时为止。

这种穷举搜索程序的缺点是速度太慢：有那么多可能继续的棋步，甚至理想的计算机也不可能在 200 亿年的时间内把所有棋步都考虑进去。1981 年，美国耶鲁大学的戴维·利希滕斯坦和以色列的数学家艾维兹里·弗伦克尔证明了对于足够大的棋盘也没有更快的程序。换句话说，耗时的穷举搜索程序没有简捷的方法。这种下棋问题，即使我们知道已有解法，也总是会使计算机的分析落空。

下面 4 章，我们将从理论和实践两个方面考虑计算机的能力与局限性。

第八章　图灵的通用计算机

艾伦·马西森·图灵是一位非凡的数学家、计算机科学的先驱者、破译纳粹的著名密码谜的关键人物。 1952 年 2 月，他以“粗野的下流言行，触犯了 1885 年刑事法修正条例第八条”的罪行，在英国曼彻斯特市被捕。在此之前不久，图灵的家被盗，盗窃犯是他的朋友阿诺德·默里，一位 19 岁的无业青年，图灵与他曾有过性关系。当图灵向警察报告盗窃案时，曾把他与默里的关系告诉了警察，他天真地认为，皇家委员会即将使同性恋合法化。两个月后，他因 6 次进行性骚扰受到审讯，并因总共 6 次的性骚扰被判有罪，将送往监狱。他接受定期服用两性化女性激素药物的方案，进行“有机疗法治疗”，因此给他一年缓刑。1954 年 6 月 7 日，41 岁的图灵吃了半个浸在氰化物溶液中的苹果自杀。[①]

在人工智能领域，图灵取得了基本概念方面的两项不朽成就：图灵检验法和图灵计算机。图灵检验法是他确定计算机能否思考

的方法。检验要求把计算机和任意选出的人与提问者分开，提问者

要通过中间物向他们提出数量不限的问题。图灵认为，如果提问者

未能区别两者之间是计算机还是人，那么就意味着计算机正在思考。换句话说，如果计算机被认为是有智能的，那么它就是智能型计算机。

要对图灵通用计算机的概念进行解释，需要一些基础概念。当图灵在英国剑桥大学时，1935 年他就是在那里成为英国皇家学院的一名研究员，他受到了物理学革命性发展的影响，该发展推翻了因果律和决定论的传统概念。按照牛顿的世界观，如果在自然体系方面掌握了足够的知识，那么整个未来都将是可以预测的。

1795 年，法国数学家、同时又是牛顿迷的皮埃尔-西蒙·拉普拉斯是这样论述智能的：“假如某一时刻有一种智能，这种智能可以包含所有的力量，并由此使自然界生气勃勃，而且使组成自然界的各种生命都有各自的位置——智能的强大足以使许许多多数据服从于分析——它可以使最大物体的运动与最轻原子的运动都包含在同一公式之内；对于智能来说，没有不能断定的事物，而且未来也和过去一样，都将出现在其眼前。”

然而，本世纪初，量子力学的提出，使未来完全根据现在和过去来决定的说法宣告结束。在 30 年代，由于量子力学，特别是由于观察者总是影响着观察结果的原理，使哲学界发生了大混乱，而英国剑桥大学正处在这种混乱的中心。图灵发现这种概念是不稳固的，而且他也被引向数学，因为看来它所涉及的是绝对的实体，与观察者无关。正如剑桥大学数论学家 G．H．哈迪所说的，317 是一个素数，不是因为我们想它是个素数，或者说我们的想法是以某种方式而不是另一种方式形成的，而是因为它就是一个素数，因为数学的实体性就是那样建立的。

图灵致力于解答某个疑难问题的工作，该问题切中了数学实体性的本质核心：是否有一机械方式确定数学中任何已知语句是正确的还是错误的？为了回答这个问题，他终于提出了“通用计算机”，即图灵计算机的概念，这种概念可以例行地回答数学的问题。图灵引入了能够运算数学的

[①] 关于图灵最后几年的悲剧性详情，在安德鲁·霍金斯著的同情性传记文学曾做报道，《艾伦·图灵：谜》（西蒙-舒斯特出版社，纽约， 1983）。

计算机概念，目的在于强化数学作为与人类事物无关的学科的地位。然而可笑的是，图灵发现，数学的某些问题是不能由计算机或人用机械的方法来解题的，例如，涉及非重复小数的数产生问题。

图灵计算机是一个非凡的概念。不过从其一系列性能的观点来看，它却是非常有限的。即使你对计算机的程序设计一无所知（或许整个主题会使你吃惊），但图灵计算机的如此有限性能，也会使你很快地理解它的“内部”工作情况，从而高兴地为它编写程序。然而，从计算的观点看，它是能够进行任何运算的，换句话说，数学家能够进行的任何运算，想象的最大功率计算机也能够进行运算。如果说，这种说法不是相当惊人的话，那么让我再隐晦地补充一句：图灵计算机，不管它叫什么名字，不一定是一部计算机。它可以是一个人或一组人。

那么，这种图灵计算机的基本原件是什么？首先，它有一条长带，设想它是一条窄窄的纸带，纸带上划有许多竖线，把它分成许多方形单元。

如果已知某单元不是空白的，那么它就含有有限字母符号中的某一种符号。图灵计算机，能够一次扫描纸带的一个单元，通常都是从含有符号的最左边单元开始。如果所扫描的单元是空白的，那么计算机就会让单元的空白留下，或者在单元中打印一个符号。如果所扫描的单元含有符号，那么计算机就可以让单元的符号留下不变，擦掉该符号并在该符号的位置上打印另一个符号，或者擦掉该符号并让单元留下空白。然后计算机停机，或者立即扫描到左边或右边的单元。

计算机对所扫描的单元要做些什么，下一个要扫描的是两个相邻单元的哪一个，这取决于计算机的状态或内部构形，状态数与符号数一样，必须是有限的。计算机的状态像一种思维状态，即计算机在“思维”些什么。要了解图灵计算机的运算，用不着对其状态的本质进行精确的、形而上的思考（或更抽象定义）。计算机的“程序表”规定了计算机对于符号与状态的每一种可能组合将要做出的反应。

举两数相加一例，将会非常清楚地阐明这些抽象概念。假定我们以“一元”的记号写出一些数字，其中整数 n 用一串 n 个*号来表示，在 n 个相连的单元内每单元一个*号。据此，**号表示 2，*****表示 5。一元记号的优点是只有一种符号*号，不需要 10 个不同的数字来表示任何已知的正整数。若要 2 加 5，只要把**号和*****号打印在纸带上，它们之间有一个空白单元，这样两串*号就可以区别开。

带有图解的程序表说明了计算机如何进行两数相加的运算。但在讨论程序表的特点之前，先要概括地描述加法的过程。聪明的计算机先找到两个数之间的空白单元，在空白单元打印一个* 号（那么在纸带上留有一串的 8 个* 号），而后继续下去，找到一串* 号的结束单元，并擦除掉最后一个* 号。这样，在纸带上就留有*******号，按一元记号，它就是 7，即 2 加 5 的和。

现在让我们再来看程序表。计算机的状态通常列在最左边的一栏内。在这个程序表内，共有 3 个状态，编号分别为 0、1 和 2。符号（和表示空白单元的词“空白”）通常横列在程序表的上方。在这个表内只有一个符号*号。

计算机在 0 状态中开始，按照惯例，扫描纸带上最左边的符号（换句话说，扫描**号中的第一个*号）。程序表描述了计算机如何运算状态 0

与符号*号的组合。计算机让符号留下不变，扫描到右边的下一个单元，并停留在状态 0 中，那么，计算机如何运算这个单元？由于计算机仍然处在状态 0 中，而且单元中的符号还是一个*号，计算机仍按前面所述进行运算：只让符号*号留下，扫描到右边的下一个单元，并停留在状态 0 中。

符号 / 状态	★	空白
0	右边状态 0	打印★号右边状态 1
1	右边状态 1	左边状态 2
2	擦除停机	

现在换到空白单元。程序表中状态 0 与空白符号的组合说明了计算机是如何进行运算的。它打印了一个*号，再扫描到右边的下一个单元，即进入状态 1。这时，这个单元中还是一个*号，而状态 1 和符号*号的组合就描述出计算机的行为：扫描到右边的下一个单元，并停留在状态 1 中。这个步骤要重复 4 次，因为每次都是一个*号继续出现。当计算机扫描到一串 5 个*号结束处的空白单元时，它会回到左边的一个单元，并进入状态 2。这个单元中有一个*号，计算机会擦掉它。然后计算机停机，处于一种完成状态。这种方法的作用是：相同的程序表都可以生成任何两数的和，无论数的大小如何，只要以一元的记号写出，两数间有一个空白单元，就能算出。在状态 0，计算机只是扫描第一个数的每个单元，一直扫描到空白单元，再在其上打印一个*号。在状态 1，它则是扫描第二个数的每个单元，直到空白单元，再回扫，并停留在最后一个*号的单元上。在状态 2，它只是擦掉这个*号。于是，纸带上就立即有了答案。

这种加法是众所周知的有限数法，因为程序表包括数量有限的状态和数量有限的符号。然而这种有限数法却可以生成范围无限的数。图灵计算机要运算可以想象的任何数之和，纸带的长度就必须是无限的，也就是说，如果纸带仅有 1，000 个单元长，而它就不能运算大于 1，000 的数。

在图灵计算机用这种方法完成两数相加的运算时，纸带将只有答案，而没有原来的两个数。如果有人试图编写一个带有原来两数的程序表，那么他一开始就应该想到，图灵计算机需要“ 计算 ”在两串*号中的 8 个*号。然而令人感到意外，图灵计算机不能进行这种计算。设想它扫描第一个*号时，就会跳入状态 1。每当它扫描另一个*号时，就会跳入下一个状态。这样下去，在它扫描第五个*号后，计算机就已处在状态 5 中，扫描第二十三个*号之后，就处在状态 23 中。看来用这种方法，图灵计算机似乎能够计算任何*号的数；即当它扫描完所有*号时，它的状态数就相应于它的*号数。但是，这种方法是行不通的。你知道这是为什么吗？

问题就在于这个方法不是有限数法。这种方法需要数目无限的状态。比方说，如果计算机仅有 5 个状态，那么它就不能计算多于 5 个的*号，因此它将被限制在和为 5 或小于 5 的数之内。如果它有 50，000 个状态，它也不能计算多于 50，000 个的*号。换句话说，对于有限数状态 n，它不能计算多于 n 的*号。这种方法行不通，是因为我们所要寻找的是在任何情况下都可用于任何加法的方法。

如果允许数字状态是无限的（或者符号数是无限的），那么程序表就编写不出来。而要求编写出有限数字的程序表，按照惯例，需要用机械的方式。

现在需要探讨一个令人感兴趣的说法，即图灵计算机不必是一部机器，而是程序表（如果你愿意的话，可以叫它软件），那就是图灵计算机的定义。任何一个实体，它可以是一部计算机、一个人、一条美人鱼、一个游魂、或是克里姆林宫，只要它能够按照程序表进行运算，就是一部图灵计算机。如果你能够按照加法图表中的程序表在纸带上进行两数的加法运算，那么你就是一部图灵计算机。在一篇卓越的论文中，图灵在理论上和实践中已经能够证明；图灵计算机无法做到的，数学家和计算机都无法做到。一部超级计算机能够非常迅速地解出的问题，动作迟缓的图灵计算机也同样能够做出解答。

掌握图灵计算机的实质和具备有限数法的解题能力，最佳的方法是自己编写程序表。我想提出一个建议，请你编写一种程序表，使它可以用于图灵计算机的一元记号的减法运算。但要提醒你，在编写程序表时，应让计算机以某种方式知道它已完成计算，并把该方式写入程序表中。否则，由于纸带的长度可以任意长，常常可能使计算机一直连续扫描许多空白单元。下图显示出了减法用的程序表。当然，其他程序表也可以进行运算。

符号 / 状态	★	空白
0	右边 状态 0	右边 状态 1
1	右边 状态 2	右边 状态 1
2	左边 状态 3	左边 状态 5
3	擦除 左边 状态 4	停止
4	擦除 右边 状态 1	左边 状态 4
5	擦除 左边 状态 6	
6	擦除 停止	左边 状态 6

第二个问题是为计算机编写一种程序表，可用于检验编写在纸带上的符号 P 和 Q 顺序是否是回文式的，即正读与反读的顺序都一样。一种方法

就是使计算机能够对第一个符号与最后一个符号进行比较，第二个符号与倒数第二个符号进行比较，以此类推。但要记住，这种方法必须是有限数字。如果顺序是回文式的，可以让计算机打印一个 Y，如果不是，则打印一个 N。这种方法是安德鲁·霍奇斯在为英国《新科学家》周刊撰写的一篇文章中采用的。这种方法如图所示。

回文式检验

符号 / 状态	P	Q	空白
0	擦除 右边 状态 1	擦除 右边 状态 2	打印 Y 停止
1	右边 状态 1	右边 状态 1	左边 状态 3
2	右边 状态 2	右边 状态 2	左边 状态 4
3	擦除 左边 状态 5	擦除 打印 N 停止	
4	擦除 打印 N 停止	擦除 左边 状态 5	
5	左边 状态 5	左边 状态 5	右边 状态 0

霍奇斯方法的缺点是，尽管程序表只有 6 个状态，但计算机要浪费许多时间沿一串符号来回移位。如果计算机在拿第一个符号与最后一个符号进行比较之后，拿倒数第二个符号与第二个符号进行比较（而不是拿第二个符号与倒数第二个符号进行比较），然后拿第三个符号与倒数第三个符号进行比较，再拿倒数第四个符号与第四个符号进行比较，以此类推，那么它就可以节省时间。这种方法的程序表如下图所示，它需要 10 个状态。要缩短计算时间，必须以较长的程序作为代价。

10 个状态的回文式检验

状态符号	P	Q	空白
0	擦除 右边 状态 1	擦除 右边 状态 2	打印 Y 停止
1	右边 状态 1	右边 状态 1	左边 状态 3
2	右边 状态 2	右边 状态 2	左边 状态 4
3	擦除 左边 状态 5	打印 N 停止	
4	打印 N 停止	擦除 左边 状态 5	
5	擦除 左边 状态 6	擦除 左边 状态 7	打印 Y 停止
6	左边 状态 6	左边 状态 6	右边 状态 8
7	左边 状态 7	左边 状态 7	右边 状态 9
8	擦除 右边 状态 0	打印 N 停止	
9	打印 N 停止	擦除 右边 状态 0	

字母易位式检验

状态符号	P	Q	R	空白
0	擦除 打印 R 右边 状态 1	擦除 打印 R 右边 状态 2		打印 Y 停止
1	右边 状态 1	右边 状态 1	右边 状态 1	右边 状态 3
2	右边 状态 2	右边 状态 2	右边 状态 2	右边 状态 4
3	擦除 打印 R 左边 状态 5	右边 状态 3	右边 状态 3	打印 N 停止
4	右边 状态 4	擦除 打印 R 左边 状态 5	右边 状态 4	打印 N 停止
5	左边 状态 5	左边 状态 5	左边 状态 5	左边 状态 6
6	左边 状态 6	左边 状态 6	右边 状态 0	

最后一个建议是为图灵计算机编写一种程序表，可供计算机用于检验由空白单元分开的两串 P 和 Q 符号是否变移位置式的。而且，Y 符号同样代表“是”，N 符号代表“否”。这里需要提示一下，在计算机解题时，计算机会打印出一个假符号字母 R。有一种可能的答案似乎是正确的。

第九章　威利·洛曼无辜地死去了吗？

从某种基本意义上讲，计算机和数学家只是不容易识别的图灵计算机，知道这一点也许令人泄气。但在另一方面，从表面上看过于简单的图灵计算机，由于证明能够解各种各样的计算问题，从而又可被认为是鼓舞人心的。数学家与计算机之间理论上的相似性不仅适用于他们能解出的各种问题，而且也适用于他们不能解出的各种问题。

工业上每天都出现许多计算问题，若用任何已知的方法去解，则太费时间，现在都例行地由计算机去着手解决。然而工业需要的是对这些问题的解法，而计算机常常牵扯到程序设计人员的水平，他们往往不能编出最佳程序。其中有许多是众所周知的使旅行推销员感到为难的问题；已知一个城市与公路网络，要找一条推销员在往返旅程中到每个城市去一次的最短路线。仅有一种已知的算法用来解这种旅行推销员问题，就是可靠的逐步试探法，这种方法费力，缺乏预见性，只是对每一种可能性都进行尝试。看来，数学并未减轻威利·洛曼的烦恼。

过去 15 年内，数学家们都感到迷惘，他们寻求巧妙的、较快的算法都告失败，这是由于他们无知呢，还是这种问题本身存在内在的困难？按照当前的知识水平，暂时还没有较快的算法，甚至在理论上也没有。目前还没有人能够证明这一点。对证明的研究已是理论计算机科学中最为热门的课题，而且在这个领域中工作的数学家已被公认为是复合型理论学家。

当数学家们谈到保证解题方法时，他们的意思就是指算法。不要由于“算法”（algorithm）这个英语单词的发音令人生畏而摈弃它，它是 9 世纪波斯数学家阿布·贾法尔·穆罕默德·伊本穆萨·阿尔霍瓦里米的姓氏音译转讹而来的，他的语义遗产还包含有单词代数（algebra）在内。算法的音难读但不难懂。你早已了解什么是算法的直观概念。

你可曾记得，在你读小学时，你的英语老师让你制定出一整套令人厌烦的规定，去做诸如系鞋带一类枯燥无味的琐事，然后老师叫约翰尼·怀斯盖严格按照你的规定去系他的鞋带（与此同时，这个讨厌的老师还会让你大声念你的那一套规定）。

当然，他会立即出错——而且是个大错——因为你没有考虑一些看来好像是理所当然不成问题的基本步骤，就像系鞋带时理所当然要握住鞋带的塑料包头，而不是握住它的中部一样。如果你详详细细地写出，那么你就会得到一个有关系鞋带的规则系统，而这个规则系统不过是一个循序渐进的程序，在这个程序中，每一步都说得很明确，你可以按部就班地解决每个问题。每个步骤都要规定得清清楚楚，其间不允许留下任何靠可能、直觉、经验、解释或想象等方法来处理的细节。

当然，数学家们对于计算问题的算法要比系鞋带更感兴趣。两个整数相加的算法，根据小学老师教给我们的方法，是用纸和铅笔按照如下的明确步骤进行：把整数写成一行，一个数写在另一个数的上方，两数右端对齐，在它们下方划一横线，从右到左地进行计算，有时还“进位”1，而且照此步骤计算许多其他数的相加，也是不成问题的。这种算法应该包括如下法则，像“如果一个数 2 在另一个数 4 的上方，可在其下写一个数 6”和“如果一个数 3 在另一个数 6 的上方，可在其下写一个数 9”等法则。

算法的功能之一是其能用于一个问题的所有实例。例如加法算法可以

算出任何两个整数的和。你虽然花费时间去详尽写出一种算法的全部细节，但你却得到了一种能够保证工作的方法。计算机的程序或是单一的算法或是系列的算法。如果没有指令告诉该算法的每一步骤应该做些什么，那么计算机就同不能模拟系好鞋带一样，也不能进行两数相加的计算。程序设计员的作用在于编好完整的指令，换句话说，要编好完整的算法。当程序设计员责怪其程序中的错误时，他的意思是指在编写详尽算法或把算法译成计算机语言时，他犯了一个错误。

必须强调的是，算法的用户不管是一部机器还是一个人，不需要对算法做出判断。例如，加法算法的使用，不需要“什么是数字”这一概念。要应用算法时，你可以盲目地按照法则进行。比方说，你不必知道，5 是跟在 4 之后，7 是大于 3 等等，甚至你也不必知道你是在使用十进制的数制。哲学文献中已有许多篇幅谈论过，就计算机的思考能力而言，缺乏判断会意味着什么。但是，探讨这样一个引人兴趣的说法则使我们离题太远了。

数学家们都不大关心旅行推销员这一专题。对于一系列较小的城市与公路网络，由于没有多少可能的路线需要审查，因而找到解法是很容易的。甚至对于大的城市与公路网络，那也可能幸运地或者偶然地找到最佳的路程。当数学家们宣称某问题实际上是不可解时，他们的意思是，仅仅知道保证解法的许多方法，就像穷举搜索所有可能性的方法一样低效，即使对于最高级的超级计算机来说，这种穷举搜索法也是太慢的。

数学的行家对于快速（与可用）的算法和慢速（与不可用）的算法都有严格的确定方法。假设数字 n 是某问题大小的量度（对于旅行推销员问题，n 是城市与公路数目的量度）。对于快速的算法，随着计算问题规模的增大，完成算法所需的时间的增长不会大于 n（表示计算规模）的某个多项式。多项式是一种数学函数，诸如 2n（加倍）、3n（3 倍）、n^2（平方）、n^3（立方）、$3n^{10}$ 和 $64n^{100}$ 等。而对于慢速的算法，例如用于解旅行推销员问题的穷举搜索法，则其执行时间将按问题规模增加的指数增加，即 2^n、6^n 或 12^n 等。

当 n 的值小时（也就是说，对于简单的问题），已知的多项式函数可以等于甚至超过已知的指数函数，但是当 n 的值大时，任何指数函数都将迅速地超过任何多项式函数。例如，当 n 等于 2 时，多项式函数 n^2 等于 4，它等于指数函数 2n。但当 n 等于 10 时，n^2 只等于 100，而 2^n 却会像火箭上天那样猛增到 1，024。毫无疑问，指数函数的增加会大大超过多项式函数的增加，这曾使托马斯·马尔萨斯感到忧虑，因为他发现人类的人口是以指数函数增长的，而与之相比，食物的供应则只以多项式函数增长。

解旅行推销员问题，仅有已知的一种方法是按指数减慢的方法，即审查所有可能旅程的方法，这一事实意味着，在当今这个年代里，我们已不能对看来如此简单的问题有真正的了解。综合性理论学家总想试图证明这个迷惑人的猜想：不管我们如何努力尝试，我们对它都不会有任何了解，因为它就是不能理解的。

看来与旅行推销员问题似乎有点相似的许多问题，数学家们对它们已经有所了解。例如，请考虑，一位公路检查员，他负责检查某段公路网，旅行推销员可能就在这段公路网上驱车。这位检查员渴望回家去看妻子和孩子，他想知道，是否有一条来回的路程，只须经过每条马路一次，只经

过一次。但他并不关心城市，他只是想自己能走过公路的每个路段，而且还不重复。而从另一方面来说，旅行推销员却不关心公路，他只想去每个城市，每个城市只去一次，这样可把其汽车里程减到最短。

伦哈德·欧拉 1736 年的研究工作，轻而易举地回答了公路检查员的问题。欧拉是一位 29 岁的普鲁士数学奇才。原普鲁士城市柯尼斯堡（现为苏联城市加里宁格勒）位于普雷盖尔河的两岸，并且包括克尼霍夫岛以及河流岔口中部的一块狭长陆地。城市的 4 个区域由 7 座桥梁的网络连接起来。

据说，伊曼纽尔·坎特习惯于环绕城市进行长路程的保健散步运动，而且居民们也都想知道，是否可能有一条进行散步的来回路线，可以穿过所有 7 座桥梁，而每座桥梁只能穿过一次。由于桥梁的数目很小，这个问题可以用列举所有可能路线的方法（否定的方法）去求解，也就是说采用类似于旅行推销员这个小问题的、没有预见性的穷举法。

这个问题由多产数学家欧拉去解，欧拉是一位有 13 个孩子的父亲，同时还著有 80 本书的数学研究成果。传说，许多研究报告都是在第一次与第二次叫他去吃饭之间的 30 分钟时间内写出来的,他预见性地证明这种路程问题无解。数学的灵魂大力提倡分析最普通的例子。因此，欧拉不仅想为柯尼斯堡的居民，也想为各地喜欢桥梁散步的人们解决问题，他试图解答一个普遍性的问题：“ 有若干河流及其分支穿过某一地区，并在其上架设任意数量的桥梁，已知河流与桥梁的布局，求是否有可能在每座桥梁只穿过一次的情况下，穿过所有的桥梁。 ”如果你把陆地区域看成城市，把桥梁看成公路，那么你就可以认为，这个一般性问题与公路检查员所面临的问题相同。

为了解柯尼斯堡桥梁问题，欧拉用几何线表示每座桥梁，用几何点表示每块陆地。

在这幅图中，欧拉已把问题简化成基本线条，去掉了所有无关紧要的内容。比方说，线与点的表示无法区别桥梁是宽还是窄，是特定的桥梁还是连接同一陆地区域的其他桥梁，是大块陆地还是小块陆地，乃至是岛屿还是河岸等。这些区别也许在其他方面非常重要，但与穷举的非重复性散步方法无关。这是一种漂亮的数学表示法：它仅需要在手边保留那些有关的情况，从而使数学家免受枝节问题的干扰，更能集中注意力于问题本身。

欧拉已能证明，只有当点（陆地区域）为 0 或 2，形成的线（桥梁）为奇数时，才可以进行穿过所有桥梁的非重复散步。你只要稍加思考就可支持这一结论。如果你穿过一座桥梁到另一处陆地去，必须还有一座桥梁让你离去，否则你将被困在那里。大片陆地需带有偶数桥梁才能确保那里有一条进去的路，另有一条离去的路。要是大片陆地只带有奇数的桥梁，那只有在旅程的终点（在那里你不需要一座桥梁离去）和旅程的起点（在那里你不需要一座桥梁进去）才有可能进行非重复的旅行。由于只有一个起点和一个终点，因此只有两处陆地才能有奇数的桥梁。在柯尼斯堡，4 处陆地区域的每一处都连接了奇数的桥梁，即使没有比较严格的来回旅程条件，那么完全的非重复散步显然是不可能的。

欧拉关于任意数桥梁与任意数陆地区域的结论要比归纳成普通的常识重要得多，认识到这一点很重要。我们的推论只是简要地说明，如果欧拉

所断定的条件不能够满足，则非重复的旅行将是不可能的。欧拉的结论是很强有力的，直观上却不是很明显的：他证明了，如果这一简单条件得到满足，也就是说，当陆地区域数为 0 或 2，而且连接它们的桥梁数为奇数时，非重复的行程总是可能的。

要把欧拉的分析应用于一般情况，需要数出每处陆地区域的桥梁数。由于每座桥梁都要连接两处陆地区域，因此桥梁要两倍计数。如果桥梁数为 n，那么欧拉的分析需要 2n 个步骤。桥梁的计数可以作为一种算法列出公式，而且它将成为一种非常有效的算法，因为虽然问题变得越来越复杂，演算所花费的时间却仅多了一倍。而从另一方面看，所有可能旅程的穷举搜索法则将成指数地迅速增长为 2^n。

在旅行推销员问题中，对效率很低的穷举搜索法仍无简捷的方法。比方说，你仍不能计数出连接于每条公路的城市数，并根据这些数是奇数还是偶数来做出某种结论，或者就此而言，也不能根据这些数的其他性质得出结论。而且，这还不仅是我们不知道寻求那些性质的问题。还有可能是这些性质本来就不存在。这正是综合性理论学家都在努力证明的问题。

旅行推销员问题不仅仅是惟一的计算问题，许多数学家都不理解其快速算法。还有一整套叫做 NP-完全的问题，对于这类问题，人们仅知道其计算所需时间以指数方式激增。[①]在 NP-完全的问题中，另有一个众所周知的例子称为人群问题：已知有一大群人，比方说，共 100 人，他们之间是否有许多人，比方说，有 50 个人，全都彼此认识吗？

“你可以解这种问题，”美国麻省理工学院综合性理论学家迈克尔·赛普泽说道，“先投出 100 个点，每点表示一个人，然后在相应的彼此认识的两人的点之间划一直线。”于是你将希望这组的 50 个点全都有连线。赛普泽接着又说：“看起来它很像一个有关计算机方面的重大问题，然而它不是。我们知道，如何去解这种问题，仅有的一种方法实质上是查看 50 人小组的所有连线，它们的数量非常多，就像 10 的 29 次方。要解出这个问题，即使应用快速的计算机，也要好几百年。”

旅行推销员的问题、人群问题、以及所有其他 NP-完全的问题，都有难以理解的共同特点：如果有人声称，他对于这类问题中的任何一个特殊事例已经有了解法，那么要检验这个解法则是很容易的事。对于旅行推销员问题，只要检查所提出的旅程，并查明是否包括了每个城市一次。对于人群的问题，则要双向检查已被辨认全都互相认识而成群体的 50 个人。美国伯克利市加利福尼亚大学计算机科学教授理查德·卡普把 NP-完全的问题比作拼图玩具：“它们可能难于组合，但是当有人向你展示一幅完全的拼图时，你就能一下子知道问题已有正确解。”

NP-完全的问题还有一个醒目的特点，如果这类问题中的任何一个问题能够用快速算法求解，那么其他问题也都能用此法解出。而且，对于某类 NP-完全问题采用快速算法毫不费力，而且稍加改进，就可用于解任何其他 NP-完全问题。例如，如果人们发现了一种用于解旅行推销员问题的快速算法，那么数学家们就会自如地运用快速方法去解人群问题和所有其他的 NP-完全问题。因此，旅行推销员问题是否有快速解法与 NP-完全问题是否

[①] 如果你一定要知道的话，NP 表示非决定性的多项式，而 complete 一词则意味着这些问题是该类问题中最难的。

真的像看上去那样难这一较大问题有关。

美国电话电报公司的戴维·约翰逊说道：“我认为，现在每位数学家实际上都认为 NP-完全问题有内在的困难。”约翰逊是这一领域的权威人士，著有《计算机和难处理性：NP-完全理论指南》一书。他还说：“真正的问题是证明它。”

这种论点动摇了一些数学家的想法，他们认为他们也许能够证明旅行推销员问题及同类的其他问题都不会有快速解法——从来就没有过——即使未来让爱因斯坦一类大师来绞脑汁也不会有。他们怎么会提出要证明这样的问题？

目前的工作都集中在逻辑门上，它已被认为是计算机硬件中最基本的单元。在电子计算机内，逻辑门是一种组件，由任意数目的输入引线与一根输出引线组成。逻辑门也是一种二进制器件：每根引线中的信号都被认为或是 1、或是 0。（在电子学术语中，高电平对应于 1，低电平对应于 0。）

每一个逻辑门都能完成 3 种基本运算中的 1 种：“非”、“与”或“或”。这 3 种运算的名称都是根据布尔代数中已经使用的词“非”、“与”和“或”而得来的。布尔代数是 19 世纪 40 年代由乔治·布尔研究出来的一种开拓性的形式逻辑体系。布尔是一个贫穷补鞋匠的儿子，他自学数学，研究出符号逻辑体系，其中 1 表示真的，0 表示假的。尽管布尔的研究工作使他获得了爱尔兰科克大学的数学教授职位，但直到 100 多年后第一部电子计算机问世之后，他的逻辑体系才得到数学界的完全赏识。

在形式逻辑中（和日常的英语中），词“非”加在前面可把真语句变成假语句，而且反过来也一样。把它换成布尔代数的术语，则是“非”可把 1 转换为 0，0 转换为 1。因此，“非”逻辑门有一根输入引线，并把输入信号转变为其相反信号，即如果输入是 1，则输为 0，而如果输入为 0，则输出就为 1。

布尔“非”逻辑门

当然，词“与”用于连接单个语句成为复合语句，即如果每个组元都是真的，那么复合组元也是真的。现举一简单例子，“朱尔斯吃豆腐与吉姆吃多夫条形面包”，只有当朱尔斯和吉姆两个人都在吃上述的食物时，它才是一个真实语句。由于同样的理由，“与”门可接受两个或多个信号输入，如果所有的输入都是 1 时，那么输出也是 1，否则，则输出为 0。

布尔“与”逻辑门

词“或”也是用于连接语句成为复合语句，但只要一个或几个组元都是真的，则其复合组元也是真的。如果朱尔斯或者吉姆（或者他们两人）在吃他们各自的食物，那么“朱尔斯吃豆腐或吉姆吃多夫条形面包”才是真语句。同样地，“或”门可以接受两个或几个信号输入，但只要至少输入之一是 1 时，则其输出也是 1。

布尔“或”逻辑门

布尔代数的绝妙之处在于，1 和 0 不仅表示真的和假的，而且还可以表示任何两种不同的状态。例如在旅行推销员问题中，0 和 1 可以表示城市之间的相应关系：如果两个城市由一条公路连接，则以 1 表示，如果它

们没有公路连接，则以 0 表示。在人群的问题中，1 可以表示两个人成为朋友的状态（或者在该问题的图解表示法中，表示由一条线连接的两点），0 表示他们不是朋友的状态（表示没有线连接的两点）。

在计算机中，任何数目的“与”门、“或”门和“非”门都可以连接在一起，形成一种电路。例如下图示出 4 个“与”门和 1 个“或”门组成的一种小型电路，它可以用来求解人群问题的普通实例：在 4 个人的一组中，有 3 个人是朋友吗？

然而，随着人群问题的人数增加，用于已知解法的电路大小（也是逻辑门的数目）将按指数方式激增。如果数学家们能够证明，对于任何可能已知或未知解法，电路必按指数方式增大，那么他们就能证明人群问题没有快速算法。

数学家们还不知道如何开始这样的证明，已经转而考虑另一特殊的问题，这就是通常都有快速算法的奇偶函数，而且他们还试图以某些基本方式来限制电路，使得快速算法不再产生作用。（奇偶函数可在一串的 0 与 1 中确定是否产生偶数或奇数。）这种方法看来也许有些怪，其实它并不怪。数学家们对于如何证明电路必须是大型的了解甚少，因此为此目的而做的任何证明，甚至是某种人为的情况，也都将会有所进展，而且可以提供证明真正论点所需的数学工具。赛普泽说道：“这是数学中的普通方法。如果问题很大，可试图把它限制到某些范围，并求解其中一部分，希望这种分部解法使人们对原来的问题会有更深的了解。”

在这一领域内，早期的工作限制了电路的研究工作的深度，这里的深度是指逻辑门的层次数目。1981 年取得了第一批成果，当时美国卡内基-梅隆大学的赛普泽及其两位同事证明了，如果他们限制用于奇偶函数的电路深度，那么电路宽度的扩展快于任何多项式。1985 年，美国斯坦福大学的安德鲁·姚在这方面取得了更惊人的研究成果，他证明了电路的宽度不仅以超多项式的方式扩展，而且还以指数的方式扩展，这表明这种问题虽然受到人为的限制，但也有内在的困难。

姚的成果很快地传遍了数学界。赛普泽这样说道：“每个人都认为这个结果很满意，但也是非常复杂的。”姚的方法为他人铺平了道路，好几个研究人员很快地对他的结果做了改进。美国电话电报公司贝尔实验室数学科学部主任罗纳德·格雷厄姆说：“这很像开车的头 4 分钟路程，一旦有人学会它，那么人人都可以学会它。”

1985 年 8 月，美国麻省理工学院计算机学科研究生约翰·哈斯特德采用了姚的基本理论，但是简化了他的论据。哈斯特德说道：“在工作过程中，我获得了比较有力的结果。（在这种有限制的问题中）我们所知道如何设计的最小电路并不比我在理论上曾经证明它们应有的规模大出很多。”后来的证明都表明：数学家们实际上知道如何设计出并不比他们在理论上所推断的最佳电路差很多的电路。对于这些有限制的问题来说，不是数学上的无知，而是问题的本身排除了快速的解法。

苏联莫斯科大学的两位数学家阿·拉兹波洛夫和阿·安德烈耶夫在不限制电路深度但却限制所进行的运算方面取得了很大的成功。拉兹波洛夫又证明了如果不允许用“非”门的话，则用于人群问题的电路规模的增长将快于任何多项式的增长。而且，数学家们还在这里对这一结果做了改进，

它表明电路必须是按指数方式增大。安德烈耶夫通过禁止用“非”门还能够证明另一类问题也需要大规模电路。

这些成就使这一领域乐观起来，虽然还没有人知道怎样才能减少对电路的限制并证明在无限制的情况下，旅行推销员的问题的确很难。“还有很长的路程要走，”赛普泽这样说道，“6 年以前，我曾与人打过赌，我希望他还记住，将在 2000 年得出证明。我仍然信心十足，还有 12 年多的时间。”格雷厄姆还抱有更大的希望：“在以后 3 年内得到证明也不会让我吃惊。”

尽管人们普遍乐观，但在综合性理论方面（数学的一个分支学科，它表述了问题的难度）的研究人员，以他们的直觉已经知道他们会失败的。1985 年冬天，美国麻省理工学院的数学研究生戴维·巴林顿曾证明，计算机能够运算的某些原始表示法会比该领域中任何人所能设想的更有功效。这种原始表示法不包含“与”门、“或”门和“非”门，但却包含一个分支门，它也有两根输出引线。当分支门受到触发时，如果输入信号具有一定的指定值，则分支门就会沿两根引线之一送出一个信号；对于所有其他输入信号，分支门沿另一根引线送出一个信号。换句话说，分支门能够处理计算机程序中的语句，诸如“如果 x=5，转向步骤 4；对于所有其他 x，转向步骤 7”。

巴林顿又证明了，全部由门层次不超过 5 层的分支门构成的电路，可以解所谓的多数问题：在一串的 0 和 1 中，1 是不是多数？综合性理论学家普遍地（并且错误地）认为分支门限制于任何固定高度，不可能求解多数问题，更不用说严苛的五层限制了。

巴林顿说道：“我的证明很简单，但它令人惊奇，因为他们总是认为我所试图证明的都是假的。”巴林顿的结果也许没有多少实际用途——他又说：“除了它可以让我在一所好大学获得一个教师职位之外。”而且它还可以说服数学家们不要在复杂的综合性理论领域中如此自信。

第十章　计算机——未来的象棋之王

到此为止，我们所注意的大部分是计算机科学中的理论问题，计算机和人在原则上能进行哪些类型的计算。我们已经讨论的限制都是无条件的。如果综合性理论学家能够证明他们的推测是真实的，那么旅行推销员问题就不可能找到有效的解法。这既不是因为数学家的问题，也不是计算机缺少适当的运算工具；而是根本没有这种工具，将来也决不会有。

大多数的数学家和计算机科学家都不会遇到理论上难以超越的限制。他们所面临的障碍都是自我设置的，而且都是可以超越的，至少在原理上是可以超越的。一个主要的障碍——在数学之外的许多工作中也很突出——就是这样一种倾向：稳妥的做法是照搬被普遍接受的他人的解题方法，即使这些方法不是那么圆满。那些想靠自己的努力取得成就的人，最好一下子就能搞出名堂来，否则就会招来他人的嘲笑。本章内，让我们看看汉斯·伯利纳的开拓性工作，他制造了一台能够下好国际象棋的计算机。下一章，我们则将探讨 W．丹尼尔·希利斯的工作，他试图用他自己的改革性设计取代曾很好地为电子计算机服务了 40 年的基本体系结构。

汉斯·伯利纳是美国匹兹堡市卡内基-梅隆大学计算机学科的研究人员，他本人态度文雅，还很想跻身于世界佼佼者行列。他曾经有过这样的荣誉，现在也想为他的计算机成果赢得同样的荣誉。1968 年，他曾以 42 步一盘棋的卓越成绩击败了苏联足智多谋的国际象棋策略家 J．埃斯特林，成为国际象棋通信比赛的世界冠军，为此他曾扑在棋盘上琢磨战术整整 500 小时。1979 年，他又设计了称为 BKG（15 子棋）9．8 的计算机程序，并在蒙特卡洛城举行的大做广告的 15 子棋[①]比赛中，以 7－1 的压倒比分击败了世界 15 子棋冠军意大利的卢吉·维拉。伯利纳也和他自豪的父亲一样，他很高兴，BKG9．8 程序已成为第一台能在任何棋盘上或纸牌游戏比赛中击败人类世界冠军的机器。

现在，BKG9．8 程序已被搁置起来，世界 15 子棋联合会已禁止在正式比赛中应用计算机，但是，由伯利纳和他的研究生卡尔·埃贝林设计的一种称为 Hitech（高科技）的新计算机程序却在另一种棋盘竞赛场所中保持了计算机的荣誉。1985 年 10 月，Hitech 程序赢得了北美计算机国标象棋的冠军称号。这项成功与其他一连串击败人类天才的胜利一起，完全证明了 Hitech 程序在下国际象棋方面优于任何其他计算机，也优于参加美国国际象棋协会认可的各种比赛的 30，000 名高明棋手（“思维”人）的 99%。

现在，伯利纳已注视着弗雷德金奖金，这项 10 万美元的奖金将给能击败人类世界冠军的第一台计算机的设计师。Hitech 程序目前要击败人类世界冠军力量尚不足。但就伯利纳的顽强性格、教育情况与比赛纪录来看，其程序的前途是不可低估的。

若按年月顺序来看，伯利纳早先热爱国际象棋，而后才爱他的计算机。他 1929 年出生于德国， 8 岁时随父母迁居美国，定居在首都华盛顿。他发现那里的学校的要求比德国松得多，因此他寻求课堂外的挑战。在 1942 年的夏令营时，他看到了一些年轻人在下国际象棋，就向他们请教比赛规则。伯利纳回忆说：“甚至就在第一天，已有些棋手成为我的手下败将，

[①] 也可译为国际双陆棋（译者注）。

情况就是这样。我从此着了迷。”

两年以后，他是他所在地区国际象棋俱乐部的冠军，并且保住华盛顿地区最佳国际象棋俱乐部冠军的称号。伯利纳说道：“我父母从不鼓励我。他们警告我说，如果我把时间都花在下棋上，我将没有什么前途。如果没有人告诉我，谁知道我将成为什么样的人？”不过在短期内，伯利纳未控制自己的棋瘾。到了 1949 年，他终于赢得了人人盼望的华盛顿市国际象棋冠军称号，那时他刚刚 20 岁，这是个破纪录的年龄。

同年，美国数学家克劳德·香农发表了一篇颇有影响的论文，他在论文中概括地论述了如何编制计算机下国际象棋的程序。当时电子计算机刚刚问世，但是，下国际象棋已被作为在新生的人工智能领域中的一个重要的目标。它与其他智力游戏不同，国际象棋引起人们的兴趣是因为在控制的条件下，通过让计算机与人类选手对阵就可以精确判断出计算机在国际象棋上的能力。参加比赛的棋手都有数字的等级，这是根据他们与其他等级对手比赛时的成绩如何而定的。计算机也要取得等级，以反映它与人的等级棋手比赛所获得的成绩。

当计算机科学的先驱们努力把香农的想法付诸实践时，年轻的伯利纳正集中精力于下国际象棋。1954 年，他是这个国家中最佳的 12 名棋手之一，并保持了 12 年。50 年代初期，他阅读有关计算机下棋的第一批研究成果。他回忆说：“他们的把戏在我看来是相当可笑的。”

英国数学界杰出人物艾伦·马西森·图灵也是计算机的开拓者之一，他是人工智能方面有创造性的思想家（已在第八章中论述过），而且，惮精竭虑地穷究数学领域的奥秘。他还是一名国际象棋手，和爱因斯坦一样，即使算不上精通，也至少乐此不疲；也许由于他认为国际象棋是少数几种他未掌握的智力活动之一，因此他毕生热爱这项活动。不管情况如何，他至少撰写了 6 页有关以机械方式下国际象棋的配方性棋步，这实际上是一种计算机程序。虽然他还没有花费精力把下国际象棋的方法译成编码输入计算机，但他曾用这些配方棋步于 1952 年与阿利克·格伦尼对弈。阿利克·格伦尼是英国曼彻斯特大学的一名学生，他也是很有才能的计算机程序设计者，但却是一名不大高明的木材推销员。图灵的纸上下棋机（所以这么叫它是因为它还只是在纸张上存在）在那次对弈中失败了，但毕竟是首次用任意一种理想化的或者可以实现的计算机下棋。

图灵的配方是给每个棋子以数量价值，像国际象棋教科书所定级的那样，以便大体上反映各棋子的相对实力：王 1，000，后 10，车 5，象 3．5、马 3 和兵 1。在选择棋步时，都是接着走所有后续棋步，包括捉子在内，一直走到两方既不能吃子也不能给予将死的静止棋势时为止。对于每种静止棋势，两方的相对实力是把棋子的数值加在一起进行计算的，并把计算机的棋子数值看成正数，把对方的棋子数值看成负数。选择导致静止状况的棋步，在这种状态中，机器能使其相对实力增加到最大限度。

图灵的估值方案是能够找到求胜的棋步的，但是在静态情况下则无法使用。例如，它不能判别白方的头一步如何走，因为在比赛开始时，在其 20 个可能的棋步（16 个进兵步和 4 个上马步）中，没有一步棋捉子或者可能捉子，因此这 20 个静止棋势都是同样 0 值的相对实力，显然，要用该方案判断是很荒谬的。

图灵还用加权的方法来克服这个问题，在静态棋位中考虑诸如机动性

与王的安全性等因素。例如对兵来说，走兵越过自己的布阵之后，每横线增加 0．2，如果受到别的子而不是本方兵的保卫，则另加 0．3，如果不受到保卫，则要另减 0．3。对于车、象、马和后来说，如果走它们能走的法定棋步，则每走一步棋都增加其数值的平方根，如果这些棋步中至少有一步棋可以捉子，则另加 1 点。而且，要是车、象、或马（不包括后）受到保卫，得到保卫一次另外奖给 1 点，两次或两次似上另外奖给 2 点。如果王得到车的保卫，则加 0．3，如果与车保持均势，则加 0．2，要是以车保王未来仍能出现，则加 0．1。

图灵也考虑王的安全性。在他的估值方案中，王所要损失的点数取决于它易于受到攻击的程度。图灵设想王是另一个后，并计算这个后的机动性，用此来量度其受到攻击的程度。此外，图灵还给攻对方王棋的棋步增加 0．5，给立即能将对方王棋的威胁性棋步增加 1。

图灵的纸上下棋机

在静态情况下，纸上下棋机将按照其求值函数、最大的机动性、本方王的安全性以及对方王的易受攻击性来决定棋步。在 1952 年与格伦厄博弈时，纸上下棋机以 P－K_4 开局，即走王前兵两步，在 20 个可能棋步中，P－K_4 棋步具有最大的数值，这个棋步不仅可以进兵到第四横线，而且还可以提高后、王前象和王前马的机动性。早在第三步棋时，纸上下棋机走了一步软着的兵出击，但格伦尼并没有乘机利用它。在第二十九步棋时，由于纸上下棋机的求值函数示出格伦尼没有立即有效的捉子应步，因此它贪婪地用后吃掉一兵。

纸上下棋机的程序忽视一个简单然而可以压车的棋步，该棋步可以用下棋机的后看住对方的王，使得后可以强行捉子。最后，图灵这个安乐死控制论的倡导者，代表纸上下棋机主动认负。

纸上下棋机尽管非常原始，仍然有一些独到之处。例如，它认为，只有在没有任何捉子的可能时，实力的研究才有重要性。在棋盘上的某一棋位中，你可能缺少后，这种情况通常是很糟的，但只要是该你走子，你仍有机会，你可能捉住对方的后。你大概不需要一个估值的过程，它只不过统计出棋子的相对实力，却没有把可能的捉子考虑进去。

当图灵把诸如机动性与王的安全性等国际象棋知识的一些方面包括在求值函数之内时，他的思路是正确的。在与格伦尼博弈时，纸上下棋机的棋输掉了是由于这些知识还不够充分。它不能辨别在特定的棋局中的内在的危险性：王与后在同一纵列上。

伯利纳和其他国际象棋大师，甚至许多很不熟练的棋手都把这种棋局和不计其数的其他棋局牢记在他们脑子里。研究证明，人类国际象棋大师对棋局和棋位都有非凡的记忆力，而且这种优异的记忆力不一定会转移到与国际象棋无关的事物上。站在人的水准上，伯利纳觉得，他在棋盘上所享受到的成功的喜悦没有延续到教室中，至少在最初时没有。

伯利纳回忆说：“一些人往往刚上大学不久，就会遇到麻烦，我就是其中之一。本来，我曾是一名物理学的优等生，但是不知怎么一来，我走上了岔道。我一边打工，一边上学，终于攒够了钱来付学费，可以不再打工。这是一个关键性的错误，忽然间我有了很多时间，因此除了下国际象棋之外，我还打桥牌。很快地，我就成为华盛顿市 15 名最佳桥牌手之一。

一切都砸了锅。”

伯利纳服完兵役后，想返回学校。他接着回忆说：“我未能完成物理学学业，因为我的平均学分太低，因此我转修心理学。看来这是个广阔的研究领域，因为全是些有兴趣的事。”伯利纳是从物理学转来的，他期望能把事实归纳成理论，但是他失望地发现，情况恰好不是那样。

1954 年，伯利纳结婚了，在家庭生活与新工作之余，几乎没有时间打桥牌，不过他还是想方设法继续下国际象棋。他接着说道：“我在美国海军研究实验室从事称为人类工程的工作。那是非常严肃的工作，牵涉到心理学与物理学，与设备的设计有关。那是在 1955 年，当时计算机刚刚问世，实验室里也造出一部。我曾修过一门程序设计课程，大概编写过 20 行有关加数的程序，但是除此之外，我没有接触过计算机。”

“因为没有时间旅行去参加国际象棋比赛，我决定参加通信国际象棋活动。这又是另一项重大错误。它无休止地在棋盘上花去我更多的时间。随后的 13 年内，我参加了许多国际象棋的通信比赛，并且赢得了所有比赛。在世界通信锦标赛中，我必须下 16 盘棋。我估计，要思考每一步棋，平均需要花去 4 个小时的时间，一盘棋大约需要走 35 步，这就意味着，要赢得该比赛冠军，我要投入 2，200 多小时的时间。接着，我实际上还是放弃了该项比赛。”他考虑为了保持该项冠军还得再花 2，200 多小时的时间，是很不值的。

1961 年，伯利纳进了美国马里兰州贝塞斯达的国际商业机器公司（IBM），成为一名系统分析家，并且主要工作是面向军界。虽然他在那里工作了 8 年，而且奋力进取，升任了经理，但他仍觉得这项工作得不偿失：“如果你很认真地工作，这是一种可怕的生活。作为一名经理，你必须对上下都要负责任。你有一批人为你工作，但他们的确对工作毫不关心。还有一个家伙来自军界，他其实什么都不懂，还对你指手画脚，或提出一些无理要求。后来又有一个人接替了这个家伙的工作，他根本不知道第一个人想要什么，于是命令改变一切。我开始觉得，我所要做的工作应该是，在我回首往事时，能使我感到骄傲的工作。我希望从事研究工作。”

伯利纳继续进行用计算机远距离下棋的探索，但他看到进展很慢，感到失望。在 50 年代期间，学者们曾做过乐观的预测，但它与实验室内的成功不相吻合；例如，1957 年，美国卡内基-梅隆大学现代诺贝尔荣誉获得者罗伯特·西蒙就曾声称数字计算机将在 10 年内成为世界的国际象棋冠军。

计算机程序设计的重要性还没有完全得到认识。按照公众的看法，国际象棋大师就像一种人类的计算机：当他选择一步棋时，他在心目中还要探索几百步后续棋，如果我上了王前兵，那么他将同时攻我两车，而后我将捉他的后……都以惊人准确的闪电速度下棋。计算本来是计算机的主要功能，因此它们在国际象棋上似乎应该是天生的冠军。问题在于公众的这种看法是错误的，对于国标象棋大师来说，计算不是惟一的甚至不是成功的主要的秘诀。他们的成功更多地取决于对棋局的判断，而不是研究那些令人头痛的棋步。

荷兰的心理学家安德里安·德格鲁特发现，在典型的棋法中约有 38 步可能的法定棋步，而国际象棋大师平均只考虑其中的 1．76 棋步。换句话说，一位象棋大师通常根据自己曾经下过或看到别人曾经下过的成千上

万步棋，在他所能判断的两个候选棋步中进行选择，这种选择对实现该棋步的眼下和长远目标有利。美国的一位国际象棋特级大师威廉·隆巴迪老人曾经写道：“在实现目的之后，即取胜的布局转变成为数学上的强力取胜的时刻，计算最为常见。”只要花一两秒钟，就能一眼认出所熟悉的布局，这是象棋大师们在棋赛中具有惊人优势的根本原因。在动态的棋局中，简直没有时间进行预测。

许多早期的计算机程序都只局限于考虑选择候选棋步的数量（尽管它根本就不会是 1．76 这么小的数）。应用选择搜索方法的问题在于没有人知道如何用计算机语言，更不用说是用英语，来表示用于选择候选棋步的一般失效保险原理。 1966 年，由美国麻省理工学院的理查德·格林布拉特研究的早期选择搜索程序 MacHack 最为成功，它已成为在比赛中击败人类棋手（即使是最弱的一名棋手）的第一部国际象棋计算机。MacHack 程序还有幸驳倒了休伯特·德赖弗斯的看法，德赖弗斯是《计算机不能做些什么》一书的作者，他曾靠贬低计算机的能力而出了名。

然而 MacHack 的功能一般说来还有严重的缺陷。虽然它在下棋时能够胜任持续时间很长的棋局，但它还是易于突然犯下某种可笑的错误，而这种错误多少是由编入该计算机程序的象棋原理造成的。此外，它有时也会对某些巧妙但却显然违背了象棋原理的棋步视而不见。但是它已在比赛中击败了人类棋手，因而是计算机国际象棋的里程碑。

伯利纳回忆说：“我的上帝！当我听到有关 MacHack 程序取得胜利的消息时，我认为，尽管计算机国际象棋受到如此冷遇，尽管人们做了种种努力却收效甚微，但还是有希望的。我去拜访格林布拉特先生，虽然我还不完全理解计算机真的会按他所希望的去做，但我还是留下了深刻的印象。由于我离了婚，还没有再婚，我又一次有了许多时间，因而我自学计算机程序设计，并花去许多晚上和周末时间编写计算机国际象棋程序。我向美国国际商业机器公司申请让我到该公司在纽约的约克顿海特斯研究机构中从事计算机国际象棋的工作。他们答复说：‘我们不资助这类项目。而且，你还没有博士学位，因此，如果你能做些对公司有益的其他事的话，我们顶多让你稍微做一点这方面的工作。’”

“我认为，要达到我的目的，惟一的途径是获得博士学位，以便进入该公司。我对自己的基本情况很自负。我向几个学校提出了申请，但只有卡内基-梅隆大学接受我。”他在 1968 年获得世界通信国际象棋比赛冠军的胜利显然有助于他进入该校。

“因此，我是在 1969 年秋季 40 岁时成为一名学生的。这对我是多么大的震惊。我觉得我需要学习的东西实在太多了，像自动化理论、各种不同的程序设计语言、多种多样的硬件配置、以及人工智能本身等等。”伯利纳早年在高等学校中不喜欢的许多课程，现在反而都要修读它们。

在卡内基-梅隆大学时，伯利纳继续进行他在国际商业机器公司空余时间内开始的计算机程序设计工作。1970 年，在美国纽约市举行的第一届美国计算机国际象棋锦标赛上，一种叫做 J．Biit 的计算机程序（其英文发音与“正好由于它在那儿”的英文首字母缩写词的发音相近）做出相当不错的表演。J．Biit 程序也和 MacHack 程序一样，用选择搜索法工作。该程序的实力就是它的估值函数，即它所考虑每步棋的实力强弱如何都以数值来权衡，但是由于它是选择性搜索，因此有时甚至都不考虑某种正确棋

步，更不用说去走它了。伯利纳说道：“ 在某些具体情况下，它很有下棋的才华。但是这还不够。在所有不同类型的棋局中，你都必须是始终如一的正确。J．Biit 程序还不具备强大的实力，足以成功地应付整盘比赛。 ”

在第一届美国计算机国际象棋锦标赛上，J，Biit 程序败于国际象棋 3．0 程序，后者是美国西北大学研究生戴维·斯莱特和劳伦斯·阿特金设计的。3．0 程序的后来版本执行的不是选择搜索法，而是全方位搜索法：对所有可能的续步进行彻底的分析，一直到规定的某种深度。虽然全方位搜索法总是包含它看到的候选棋步中的正确棋步（因为它看到了所有棋步！），但在选择一步棋时效率却很低。很多时间都浪费在令人吃惊地探索无价值的棋步上，即使是最笨的人类推木式棋手对此也不会给予片刻的考虑。要是计算机能够看清博弈的最后结局，比方说像它能够在三连棋中所做的那样，那么，这些无用的努力将是毫无意义的。

国际象棋的数学可以证明全方位搜索的低效性。在人类国际象棋大师之间的对弈，典型的是对弈了 84 着棋（1 着棋即指定的一方走一步棋）。由于每个棋位平均有 38 步法定棋步，因此穷举搜索法必须考虑 38^{84} 个可能的棋位。那是一个庞大的数字：38^{84} 大于 10^{132}，即 1 的后面有 132 个 0。宇宙已经存在了大约 10^{18} 秒，因此，即使让计算机能够工作像宇宙年龄那么长的时间，每秒钟也要分析 10^{114} 个国标象棋棋位，才能看清博弈的结局。

在国际象棋比赛中，计算机也和人一样，不允许进行无限期的思考；40 步棋大约只能给定 120 分钟，每步棋平均 3 分钟。即使计算机减小了胃口，仅探索出后续几步棋所有可能的棋步，数学上也是不允许的。在只走两着棋之后，即每方各走一步棋之后，可能的棋势数就会超过 1，000。而走了 4 着棋之后，就可能有超过 100 万可能的棋势。

计算机不仅生成所有这些棋势，而且还要求出它们的值。计算机是通过数值加权的方法来相当粗略地达到上述目的，诸如考虑实力（即各方的子与兵的数量与特点）、机动性、中心方格与纵列的控制、兵的结构、王的安全性、等等。比方说，在 3 分钟结束时，无论走什么棋步都要使对手的潜在的最大增益降至最低的程度；这种策略，是从有关竞赛的数学理论借鉴而来的，它设想对方可看出你所看出的一切，力求确保自身的利益。

如果不是发现了 a－β 算法，全方位搜索法即使只局限于几着棋的深度，也是不实用的。a－β 算法是一种巧妙的求值方法，可以让计算机无需求出每种可能棋势的值就能选择它所要走的棋步。然而令人惊奇的是，所选择的棋步正是计算机考虑了每一种续步后所要走的同一步棋。这怎么可能呢？

假设计算机首先在一定范围内探索称之为 A 的某一特定棋步的所有后续棋步。设想两方都走最佳的弈法，计算机给 A 定的极小极大值比方说为 1。（在这种方案中，正值相当于计算机所具有的优势，而负值相当于计算机所处的劣势。优势值为 1，表示比对手多一兵，其他条件都相同。）现在，计算机开始对另一个叫做 B 的可选棋步求值，B 是特别愚蠢的一步棋，表示将后置于可以立即被对手的弱兵捉住的方格中。如果计算机现在分析对手的正常应着棋步——以兵捉后，并排除掉一种微小的可能性，即为了一次锐不可挡的进攻而英勇牺牲了后，那么，计算机将定这个棋势的数值为-9，它表示其对手已具有强大的优势。

求极小极大值

现代的计算机国际象棋靠的是极小极大值法：所走的棋步应使对手的可能最大增益降至最小程度。假设计算机可选择的棋步为 A 和 B。它看出了对手对 A 的最佳反应是走一步棋 a（图中的数目表示按照计算机的观点所产生的棋势的优劣程度如何）。这时计算机又考虑棋步 B，并看出了对手将应以 d，从而能保证时 B 取得比对 A 更好的结果。这时计算机有足够理由选择 A，而对手反应 e 或 f 的结果是什么都无关紧要。

计算机不需要考虑所有其他应着棋步的结果，其中也包括对手不能吃后，因为计算机已能识别对手的走棋路线是确保它自己对 B 步棋的应步能优于对 A 步棋的应步。因此，计算机根据自己的观点，知道走 A 步棋比走 B 步棋更为可取。

要有效地执行 a－β算法，计算机必须按顺序考虑各种棋步：在上述例子中，它必须先检验 A，再检验 B，并且在分析 B 时，必须先检验捉后的棋步，再考虑其他的应步。审查各种棋步的顺序取决于各种不同的探试法或一般经验。

例如，捉子探试法指令程序对那些涉及捉子的各种棋步给予最优先考虑。（这样捉子成为一着好棋的机会将更多一些，特别是如果被捉的子未受到保护时。这种方法还能帮助计算机减轻负担，对机器大有稗益。而棋盘上少了一个子，计算机考虑的应着棋步也就相应减少。）

杀子探试法始终监视着对手的哪一步棋被杀或被驳倒（一种特殊的棋步）。当计算机仔细考虑了另一步棋时，首先要研究杀方的反应。现举一特殊例子。计算机发现它所考虑的捉对方车的一步已被对手弈出将军棋步所驳倒，在仔细考虑替代的棋步时，它将首先决定是否要走避免被将军的棋步。换句话说，杀子探试法可用来识别并监视这种威胁，这里所指的是能立即将军的致命威胁。另一次探试优先考虑那些能将军的棋步，从而应了一句古老的格言：“常将，就能将死。”简单地说，这时计算机的做法就有些更像人了。

在全方位搜索法中，要是采用渐进地深入考虑所有的续步，而不是每次一步地充分考虑这些续步，那么就能做到省时省事。从棋盘上的某种棋势着手，首先分析所有可能的续步，然后分析某一特定的棋步，根据目前所进行的搜索，就能看到最佳的一步棋。再从这步棋开始，对其余的所有续步进行有效的分析，一直到两着棋的深度，并且再次找到其中最佳的一步棋。这种过程叫做迭代深化法，它不断重复下去，直到达到所期望的深度时为止。

有一种表记录了计算机已经求出值的棋势、对这些棋势所给定的数值、以及迄今已搜索到的最佳一步棋，通过这个表就可以提高全方位搜索法的有效性。在全方位搜索法中，各种棋势都往往会不止一次地出现，只要程序设计好，查找所求的数值的时间自然比重新计算的时间少，因此，这种表在节省时间方面是很有用的。

在 70 年代,美国西北大学的斯莱特和阿特金已能够利用变最大为最小求值法、a－β算法、捉子探试法与杀子探试法、迭代深化法和已经检验过的棋势表等各种方法成功地用国际象棋 3．0 程序的后来版本进行工作，而且，它也像图灵的纸上下棋机一样，深入地搜索了下国际象棋的战术棋路，

直到走到走不动的棋势为止。这就是国际象棋 4．7 程序，它下国际象棋的能力略低于国际象棋大师的水平。

1981 年，全方位搜索程序 Belle 由美国电话电报公司贝尔实验室的肯·汤姆森和乔·康登共同开发出来，它已成为第一部达到国际象棋大师级水平的计算机，进入全美国际象棋比赛最高棋手 1%的行列。Belle 程序的成功应归功于专为进行国际象棋运算而定制的硬件。华盛顿的官员显然很重视 Belle 程序。1981 年，当汤姆森和康登试图携带 Belle 程序去苏联莫斯科参加国际象棋表演比赛时，联邦局人员拘捕了他们。里根当局担心该程序会泄露军事秘密。而汤姆森却坚持认为，Belle 程序所知道的事情只是如何去下国际象棋。汤姆森告诉新闻界说：“ 在军事上可以使用 Belle 程序的惟一方式就是可以把它从飞机中扔出，也许你可以以此杀死某一个人。 ”这些日子，华盛顿已不大注意了，因为 Belle 程序的等级已滑落在国际象棋大师的水平之下，然而它仍然可以探索平均 8 着棋的深度，每秒钟分析 120，000 种棋势，弈出比较难对付的国际象棋。

当斯莱特、阿特金、汤姆森、康登及其他人应用全方位搜索法进行工作时，伯利纳却集中精力于求值函数上。伯利纳回忆说：“ 当时我正考虑德格鲁特关于国际象棋大师怎样弈棋的著名的研究——他们如何观察弈至一半的棋局变化，然后如何转向考虑别的方面，再如何回到考虑最初的棋局变化。看来那是正确的。至少那是我所考虑的如何下棋的方法。 ”另一方面，现有的计算机下国际象棋的程序，不会在变化中来回移动。它们随着特定的变化到达一定的深度，给最后的棋势求出数值，再转到另一种变化。

伯利纳接着说：“ 给定某一具体值的困难在于你不能出错。你可以弈出牺牲两子兵，以换取具有极强攻击力的棋势。如果你使用类似 α - β 的算法，你就能够弈出最后一种棋势，对此你必须赋值；要么为换取攻势值得抛弃两兵子，要么就不值得。无论你持哪种看法，都会在一定时间内出现错误。更确切地说，‘ 我还不能肯定。我已经丢掉两兵但拥有强攻势。也许实际上我可以将死王或者赢回的多于两兵，而我也许只是丢了两兵 ’，所以你先摆出问题，再进一步深入研究，看你能否解决它。 ”

“ 对于这类问题以及如何把计算机程序编写得更深入，我思考得很多。一个晚上，我忽然有一灵感：对于一种棋势，可以给定一个值，为什么不能以一系列的值取而代之？ ”

一系列值中最高值意味着棋势处于最佳状态，而最低值则相当于可能出现最坏的情况，计算机程序要对一系列值而不是对单一值进行比较，而且当这些值的范围太宽时，它还可以比较深入地考虑棋势，以便把最高值和最低值都包括进去。伯利纳说道：“ 这种想法是遗漏的组成要素。它是许多不可思议的事物之一，这类事在科学上隔一段时间就发生一次。你提出某一方案，那么突然间，一切都迎刃而解了。 ”使用系列值的想法已经成为众所周知的 B*算法（发音为“ B-星 ”），而且伯利纳还把它列为他的诀窍。

1975 年，当伯利纳完成计算机国际象棋博士论义时，他决定为计算机编写下 15 子棋的程序，这种棋是他最近向新岳父学习的。他发现 15 子棋对研究求值法是一个很吸引人的领域，因为在这种棋中进行搜索，不会让你探索得太深。在典型的 15 子棋棋势中，约有 400 多种可能性（21 组掷

骰点数和每组点数的约 20 种走棋法），与之相比，在典型的国际象棋棋势中，则“仅有”38 种可能性。

在 15 子棋的计算机程序 BKG 中，伯利纳没有沿用人工智能中按规则求值的一般做法，他注意到“在医疗诊断体系中，也许还有一种惯例，比如说，如果有一位患者，他有这样那样的疾病，而且其年龄已超过 6 周岁，那么可以给他以如此这般的治疗。可是忽然间来了一位患同样病的患者，但他的年龄仅为 5 周岁 9 个月，按照惯例，不能对他进行那种治疗。当然，那是错误的。因为你真正需要考虑的不是黑白分明的年龄截止点，而是由于某种原因需要考虑诸如年龄、体重以及一般健康情况等因素的平缓函数。在上述特定病例中，可以开出降低剂量的药方”。

“当你首次设计智能系统时，这几项考虑已不很重要了。它们远不及把基本信息输进计算机中那么重要。但是，如果你想与最佳的人竞争，那么你就不能按照一套完全不灵活的规则去工作。”

当然，伯利纳想以他的 15 子棋计算机程序与人类最佳棋手博奔，因此他没有认真地考虑较为惯用的方法，摈弃了把棋势分为几种类型而且每类都有不同求值函数的通则。相反，他却依赖数学上的单一复杂函数，这个函数包括大约 50 个不同的变量，与具有不同程度重要性的特定部分相一致，其重要性取决于博弈阶段。每个变量都由一个数值来替代，来衡量存在于已知棋势中相应特点的重要程度。这样一来每个数都是加权的：它们都乘以另一个数，这个数称为系数，用以表示对该点的特点所给予的注意力有多大（或多小）。随着博弈进程的变化，这些系数也平缓地变化着。

这种成功的方法叫做 SNAC 法（带有应用系数的非线性平缓函数法）。在 SNAC 法提出后，只有几个月的时间，BKG 程序就击败了人类 15 子棋冠军选手，这显然表明 SNAC 法是成功的。虽然 BKG 程序有一些掷骰子般的幸运，而且也曾有过少量较小的错误，但它还是一个强劲的棋手。

伯利纳根据他在计算机 15 子棋上获得的成功，知道找到一种平缓变化的函数对国际象棋上的有效求值法也是很关键的。在这一点上，惯用的一种方法也与通则有关。考虑一下王的棋势。当博弈到中盘时，你想把王躲藏在角落里，那里很可能少受骚扰。求值函数可以对王的实际位置与角落之间的棋盘方格进行计数；这个数愈大时，你的处境也愈坏。然而，在弈至残局时，那时只剩下几个子，将死的危险性甚微，于是王应该处于棋盘的中央，它在那里还可以起着很强的战子作用。所以在残局时，求值函数可以对王的实际位置与中央之间的间隔数进行计数。如果你采用了如下通则：BKG 程序在与人类的世界 15 子棋冠军卢吉·维拉对弈时赢得了胜利

BKG 程序在与维拉比赛的第一局中，掷出一个 4 点和一个 2 点。这时，BKG 程序（黑方）具有优势，但不得不留下一个暴露棋子。它走了 9-5 步和 9-7 步，在 7 点处，留有一个暴露棋子，它可能受到 13 组掷骰点数的攻击。从表面上看，好像走 5-1 步和 4-2 步比较安全，在 5 点处留下一个暴露棋子，它只可能受到 11 组掷骰点数的攻击，但这却是糟糕的走法，因为它在 9 点处会留下两子，当它们必须走步时，就有可能成为后来的暴露棋子。

“当棋盘上还有一定数目的子和兵时，棋局就是中盘，而当其只有很少几个子时，则是残局”，那么，你几乎要患精神分裂症了。

伯利纳接着说道：“你当然不想这样，棋势是连续性的——中盘是逐步转为残局的。由于残局的逐渐接近，你不再那么执意要让王走到角落，而是容许王缓慢地移到棋盘的中部。每当人人都承认残局终于来到时，王应该靠近棋盘的中央，而不是藏在角落里。”达到这一目的的方法是需要有一种缓慢变化的求值函数，而在中盘与残局之间不应有任意的差别，而且两者也不应有不同的求值函数。

BKG 程序在与维拉最后一局的比赛中，如图所示，掷出一个 5 点和一个 1 点。这时，BKG 程序走出了引起轰动的 13-8 步和 3-2 步。如果 BKG 程序的暴露棋子中任何一子受到进攻，那么它将有更多的时间去组成棋步，以阻止对方的棋子前进。反之，如果它们未受攻击，那么就能够在本方棋盘中形成据点，使维拉的棋子更难于回到本方的棋盘中，然后再逃脱掉。

的信息而工作，太阳牌计算机是 Hitech 程序的国际象棋的知识源。

Hitech 程序的成功秘诀在于它能更好地思考（由于 Oracle 程序）以及比呆板的对手快 50%的求值速度（因为它可以同时对一步以上的棋步顺序求值）。Hitech 程序执行全方位搜索法，平均每秒可以观察惊人的 175，000 种不同棋势，换句话说，每步棋 3 分钟内可以均摊到 3，000 万种棋势分析。伯利纳说道：“毫无疑问，人们要考虑 3，000 万种棋势需要花去他们一生的时间。”

Hitech 程序的速度及其智力水平已使它成为世界上最高级的国际象棋程序，优于几乎全部的苏联人棋手。伯利纳认为， Hitech 程序或其新一代程序在 1990 年的国际象棋对弈中击败人类棋王的可能性有 50%。为了达到这一目的，它计划把更多的知识输进 Oracle 程序，并使 Hitech 程序试用选择搜索法，或许还得用 B*算法。

Hitech 程序下国际象棋能下得多好？就此而言，任何一种计算机在某项智能活动中究竟能有多好？伯利纳说道：“我认为，我们将会发现，在输入计算机的一些信息开始与另一些信息相抵触之前，你能输入计算机的信息量是有限度的。”某些研究工作者试图借助于一种信任系统，来消除这种可能性。计算机对相抵触的信息不大注意，因为它的来源不可靠。

伯利纳接着说道：“但是我不认为信任系统就是答案。我认为，我们需要制造一种学习机，把它摆在架子上，观看录像带，并从基础学起。开始，可能学得很慢。也许要花 20 年时间，才能达到成年人的理解水平，那也就很好了。如果所得到的成果是有价值的，那么学习机本身也是值得的。然而，我不会屏息不语。学习机最终必定会出现，不是在 80 年代，或许是在 90 年代。”

第十一章　男孩和他的计算机

1986 年夏天的一个清晨，在马萨诸塞州坎布里奇，创办电子计算机公司的 30 岁科学家丹尼尔·希利斯正倒在椅子里，犯愁地凝视着一面空白的电视荧屏。他在键盘上输入了一些指令，屏面上显示出像一块投镖板的黑白线条图像。当希利斯按动按键时，设在大厅一间房间里的一个黑色光滑得像玻璃的 5 英尺高的立方体——希利斯设计的名为连接计算机——断断续续地出现大量狂乱闪亮的小红光，形成无法辨别的图像。

这种明显的随机性，也许就是计算机的未来。他说：“ 昨晚我们有个突破。这个计算机确实学到了，是它自己学会的，我从未告诉它是对还是错。 ”

希利斯和一个同事花了整个晚上编制连接机程序，把已经输人的有些变形的黑白线条图像加以分解清理。这是人们能做得很出色的被称为是视觉适应的原始范例。希利斯说：“ 如果我悄悄地给你戴上一副古怪的眼镜，使你视觉变形，你能学会正常地看东西。 ”但是大多数计算机不像人，它们不能从经验中学习。

那晚那个连接机是个例外。它收到一个变形图像之后，会显示它认为真正的图像是什么样子。希利斯从未告诉过它，它工作得多么出色。它与国际象棋计算机不同，国际象棋计算机不会后一盘棋比前一盘棋下得更好，除非程序编制员对程序加以改进，而连接机每次都有改进。经过几百次试验之后，它把图像显示得相当正确。

经过 3 分钟或 500 次试验之后，它完全纠正了变形。

对希利斯来说，这一突破并不是说连接机能做到视觉适应——虽然这种技术可能对解释模糊的照片有用，甚至可以想象对清理杂乱的密码电文也很有用，而是说它已经学会做这件事。如果它能学会做此事，无疑它也能学会做其他事。希利斯认为，假如人工智能模拟有一日不再是个梦想，这可太重要了。

连接机是新近出现的一种最引人注目的计算机，带有一个并行处理机，它正开始改变计算机科学。传统计算机，即使是功率大的，也只靠单独的处理机进行计算。连接机则根本不同；它利用 65，536 个小处理机，或叫做微型电脑的总体功率，一起工作，解决一个问题。

并行处理机仅仅是一个带有一个以上处理器的计算机，其基本原理较简单：2 个头比 1 个强，那么，如果 2 个头比 1 个强，为什么不用 4 个，或 16 个，甚至是 65，536 个头呢？从理论上说，增加的头，或处理器，加速计算机的转速，使它不仅能解决有关视觉和言语理解的人工智能模拟的问题，而且也能解决物理学家、工程师和军事策划家每日都面临的许多数学难题。

在某种程度上，伯利纳的国际象棋计算机是个并行处理机，它有 64 个芯片，每一芯片对应于棋盘上的一个方格。不过这些芯片只能求出象棋的步法数值，而希利斯的处理机的灵活性足以处理各种计算问题。

并行处理的概念听起来简单，但要把这种想法变成硅，就有难以克服的障碍。带有多少处理器才是最理想的呢？每一个处理器该有多灵巧呢？处理器应该如何连接起来，才能有效地联络和一起工作？

还有个困难就是如何编制程序或指示处理机解决某个具体问题。有些

问题就像汤姆·索耶油漆围篱的工作，很容易看清楚可以分配给几个工人去做。其他工作则更像马克·吐温的《哈克贝利·费恩历险记》，看不出吐温能从别的作家的帮助下得到什么益处。

连接机是对付这些困难的一种方法。 1986 年 8 月，电子计算机公司向第一个商业顾客佩金-艾尔摩公司交付了一部按比例缩小的带有 16，384 个处理器的连接机，价值 100 万美元。这部连接机安装在维吉尼亚州奥克登 MRJ 公司的佩金·艾尔摩智囊机构。这家公司承包美国国家航空和航天管理局和国防部的工程。MRJ 公司职员汤姆·克雷说：“ 在使用这部机器几周以后，我们解决了一个重要的军事问题。 ”假设你知道敌人雷达的位置和你要达到的目标，你应该选择哪条航路，才能把被敌人发现的机会减到最低程度？克雷说 :“ 这个问题经常出现，如同我们轰炸利比亚时那样。”这虽然是件普通的事，但数字分析却是大量的，而且总体解决办法是难以捉摸的。

希利斯的电子计算机公司于 1983 年 5 月成立。那时，有些公司从事研制人工智能模拟机，人们喜欢称它为智能计算机。那些公司在研制专家系统，模拟人类专家们某一特定活动，例如决定走哪一步棋、买什么证券、或在什么地方勘探石油。专家系统仍在流行，尽管新闻媒介和华尔街大肆宣传人工智能机，最好的专家系统只不过是愚蠢的学者；例如一个国际象棋计算机，除了下棋之外，不能做其他事。

成立电子计算机公司的长远目标不是研制专家系统，而是希利斯所说的业余系统，是一种有普通思考能力的计算机。正如该公司漂亮的宣传手册所说：“ 总有一天我们会制造出一种能思维的电子计算机，它将是一台具有真正智能的机器。它既能听又能说，是一台令我们骄傲的计算机。 ”如果这种夸张仅仅是公司要努力获得的东西，它可能还没有开始这项工作，但是作为达到其理想目标的手段，电子计算机公司有它制造第一部大规模并行处理机的短期目标。

即使这个目标非常宏大，但希利斯至少有如何实现它的主意。此外，那些对智能模拟曾经持怀疑态度的人，对并行处理的可能性也有兴趣。电子计算机公司的 30 多岁的女总裁雪利尔·汉德拉认为，为了达到这些目标，最好的办法是集中一些超级科学家，组成一个顾问班子。汉德拉曾经协助首创了生物工程公司——遗传学研究公司。今天，计算机公司的顾问有麻省理工学院教授、人工智能的先驱之一，马文·明斯基；诺贝尔奖获得者物理学家理查德·费因曼，他曾执行过总统委派的调查“ 挑战者 ”号事故的任务；原麻省理工学院院长、前总统约翰·肯尼迪和林登·约翰逊的科学顾问捷隆姆·魏斯纳；还有斯蒂芬·沃尔弗勒姆，他是一位曾在高等学术研究院工作过的青年物理学家，他 15 岁时发表过他第一篇科学论文。就连希利斯等人吃维希式胡萝卜汤、沙拉、葡萄干蛋糕和巴甫洛娃佳肴的公司美食食堂的职工也都很聪明，其中一个厨房工人因获得富布赖特奖学金而离开了公司。

随着电子计算机公司不断云集一批学术精英，许多外界人士视之为一个有高度文化修养的智囊机构，对智能模拟充满浪漫思想，却缺乏制造打蛋机所需的那种简易技能，更不用说是一种新颖的计算机了。然而，该公司得到哥伦比亚广播公司创始人威廉·佩雷和其他投资者的 1，600 万美元投资、国防部先进工程研究局的 470 万美元投资后，只花两年半时间就制

出了连接计算机。

身高六英尺、目光炯炯的顽皮的希利斯，不像是开创计算机结构革命的人。他的办公室距离他的母校麻省理工学院只有几个街区，看上去不像是个高科技工作场所，却很像是婴儿围栏。他的办公桌旁有一堆日本机械玩具、一个像牛一般大的卡纸板恐龙和一件推进器式防湿衣，穿上这种衣服可以在水上行走。这种防湿衣可能不是他的得意之作；他上大学时曾用钓鱼用具和许多修修补补的玩具，制成过一个巨大发滴答声的机械玩具。他说，玩具和小机件能使他浑身放松，头脑清醒。

希利斯说：“我要按照人脑的结构制造计算机，即使不够精确。人脑不像传统计算机只有一个处理机。它有很多东西——神经原——并行工作。那就是我把连接计算机设计成大规模并行工作的原因。”

希利斯并不是惟一给计算机增加处理器的人。可能有一些大学或公司正计划制造其他上百种多头计算机，这些机构主要是由企业提供小规模经费的科研单位。许多公司都宣称它们在卖并行处理机，但工业分析家对谁能提供真正的东西还有不同意见。所谓真正的东西就是一组处理机必须能够共同投入一项工作，而不是各自单独地处理不同的工作。（真正的并行处理等于在家务中妈妈和爸爸一同做饭；但妈妈做饭的时候，爸爸却在结算支票本，不管他做这事有多少用处，也是不行的。）国际商用电器公司是世界上最大的计算机公司，它也在花千百万美元在此领域进行研究工作，并希望在 1987 年搞出两个实验性的计算机设计和试验。可是，希利斯已成功地比其他人多连接好几万个处理器。

尽管在并行处理领域中存在一阵风的活动，其技术还处在萌芽状态。然而，对于计算机科学广泛一致的意见是，并行处理是将来的技术。1980 年，日本宣布了其第五代计算机规划，国家 10 年投入 10 亿美元制造一种新型计算机，能容易地与人交谈和与环境相互作用。日本人说，这项工作的中心就是并行处理。美国政府和工业界对此做出了警惕的反应。美国国防部先进工程研究局是在苏联人造地球卫星发射成功后成立的，以确保美国在尖端技术领域永不落后。美国公布了其计算机战略，即第五代计算机规划。作为这项规划的开始部分，美国国防部先进工程研究局准备投入 7，000 万美元。

卓越的数学家约翰·诺伊曼是老式计算机——传统的单一处理器——的灵魂。他在量子力学、弹道学、气象学、对策论及核武器设计等方面有所创新。他在 40 年代提出单一处理器的结构时，并不是因为懒惰或对计算目光短浅，而是因为他认为制造一个以上处理机的计算机技术根本不存在。既然晶体管和微型芯片尚未发明，最早的计算机是用笨重的真空管制造的，连只有一个处理机的通用计算机——1946ENIAC（电子数字积分计算机）——也占满了整个房间。

在诺伊曼的设计中，处理器与计算机的存储器是分开的，存储器不仅存储某一问题的数据，而且还存储运算该数据的指令。在 40 年代这种分离是讲得通的，因为牵涉到两种不同的技术。处理器是用速度快而较昂贵的真空管做的，而存储器则用速度较慢而价廉的水银延迟线做的。诺伊曼的想法是，编制计算机程序，使快速的真空管忙碌，迟缓的存储器相对地闲着。这就要求程序编制员设法分解一个问题，使之一步一步地解决，如希利斯所说：“使存储信息流过处理机。”大量数据和指令通过狭窄的通道，

在处理器和存储器之间来回地分流。

今天，处理器和存储器之间的明显区别不再有意义了，虽然只在一些原始的计算机里还会找到。处理器和存储器现在都用同样的材料——硅。尽管技术已经改变，但在传统计算机中让处理器忙于一步一步地解决一个问题的想法尚未改变，其结果是效能极低：97%的硅——用于存储器的部分——通常是闲着的，而只有 2%—3%的硅，在极端忙碌地工作。希利斯决定找出一种方法，以便更好地利用存储器和取代一次一步地解决问题。

希利斯有而诺伊曼没有的，是小而价廉的处理器。1970 年在加利福尼亚州的桑塔·圣克拉拉，有一家刚开业的小公司，名叫综合电子公司，或不太谦虚的话就叫它“智能”，曾设法把一个处理机的 2，300 组件做在一块八分之一英寸长、六分之一英寸宽的硅片上。微型处理器，或称“在一块芯片上的计算机”诞生了。在 40 至 50 年代，那种占满整个房间的计算机，现在只有拇指指甲那样大。

综合电子公司和其他公司不久就想出，如何成批生产微处理器，使工业都能普遍用上计算机，如同用电和水那样。按市场调查公司的统计，1975 年有 75 万个微处理器，1985 年有 3．53 亿个，1990 年会有 12 亿个。

综合电子公司在 70 年代初期带头搞微型化的时候，另一家初出茅庐的公司：基地设在明尼苏达州的克雷研制公司，却朝相反的方向进军。该公司隐居的创始人西摩·克雷，开始制造世界上最快的计算机，其方法是把芯片结合起来，制成一庞大超功率的处理机。在克雷第一台超级计算机里的处理机，克雷 I 号，形状像个巨大的字母 C，高六英尺，最宽处的直径为九英尺。该机比当时任何一个计算机快 5 至 10 倍。如果不是足智多谋的克雷想到用氟里昂管蜿蜒地通过，它发出的热量准会烧穿地板；老式冰箱的工艺，使他终于获得成功。

克雷研制公司已经制造了现有的 180 个超级计算机的三分之二。克雷 II 型计算机有 4 个处理机，采用了极有限的一些并行性元件，它是目前世界上最快的计算机，它比原来的克雷计算机快 6 至 12 倍。虽然这些计算机明显地比微处理机更快，但它们不成比例地昂贵。克雷 II 型计算机比一个简单的微处理机快 5，000 倍，但其价格高达 2，000 万美元，比微处理机贵几十万倍。这个难以接受的经济事实，是政府、大学和许多公司追求并行处理的一个主要原因，尽管其技术还没有达到希利斯相信它能达到的人工智能的水平。

并行处理的利害关系很大。工业部门及政府部门想当然地认为，年年都会有功率越来越强的计算机制造出来。在过去 40 年中，单一处理计算机的运算速度提高了 1，000 倍，这主要是通过缩小基本的电子元件，并提高集成度而实现的。然而，进一步提高单一处理计算机的速度可能行不通，因为设计遇到了基本物理限度这一障碍，例如电路中信号的传递速度不可能超过光速。可能只有利用一个以上处理机的功能，才能明显地改进其性能。

要一台计算机做必须带有智能的所有事情，单一处理机简直太慢了。一台希利斯称之为真正聪明的计算机——“业余系统”——必须能看，能懂人语，能读英文，能推理和能计划。希利斯说：“这些事，单一处理机的计算机难以胜任，因为做这些事需要大量信息。如果你想给它更多的信息，使它更聪明，其实你却使它更愚蠢，因为它存取信息的速度要慢得多。”

一台单一处理机的计算机，如果负责引导一个无人驾驶的军用运载工具，用了一年时间，才能“看出”一辆敌人坦克和一块巨石的区别，就毫无价值。并行处理可能是出路。把信息分给不同的处理机，可以保持速度。

从某种理论意义上讲，并行处理机具有的惟一优点，就是速度，认识到这一点是很重要的。艾伦·图灵对计算理论的贡献仅次于诺伊曼，他1937年的实验证明，给任何一个计算机足够的时间和信息存储，它可以做其他计算机能做的事。所以，任何能在并行处理机运转的程序，即使该机有许多处理机，单一处理机也是能够模拟的，尽管模拟是缓慢的。那么，从理论上说，所有计算机都是一样的。

然而在实践中，科学家所需要的是能快速行事的计算机，例如，他们希望能按正常的谈话速度同计算机谈话，不必等很长时间，就能得到它的回答。快速行事正是并行处理机针对单一处理机提出的保证，它不仅在人工智能问题上是这样，而且在解决气候模型、流体流量、等离子物理、亚原子粒子物理、战争处理和战略防御计划、里根总统的太空基地导弹防御计划、众所周知的星球大战等许多棘手的计算问题上也是这样。

丹尼·希利斯出生于巴尔的摩，是美国空军一个内科医生的儿子。他父亲到世界各地研究肝炎传染病，他一直跟随着他父亲。每到一地，他都制作一些奇妙的玩意儿。他曾做了一个固体燃料火箭，把蚱蜢送上天；他曾利用一个铁罐和一个轮转烤肉器的电动机，制成一个活动机器人。即使他进了麻省理工学院，在大学生和研究生期间，也继续做些古怪的玩具，例如，他做了一根短棒，拿着它在人们面前晃动，就能说话。

希利斯1974年在读大学一年级时，开始同当时47岁的马文·明斯基合作。自从40年前这一领域出现以来，明斯基就一直热心于人工智能研究工作。像希利斯一样，明斯基不但是一个深思熟虑的人，而且动手能力极强。1951年，他用300个真空管、一批马达和一个B-24轰炸机的自动驾驶仪，制出了第一台学习机，这是最早的电子学习机之一。这部机器像在心理实验中的老鼠一样，学着“钻”迷宫。1956年，明斯基同3个同事，组织了第一次人工智能会议。在那个会议上，人工智能领域才正式开始。两年后，他参与创立了麻省理工学院人工智能实验室，致力于制造从事诸如模拟推理那种非数值性工作的计算机。

当希利斯未经通报就冒冒失失走进明斯基的办公室时，这个年轻的能工巧匠和年长的计算机先驱初次会面了。明斯基，这位经验丰富的计算机科学家，正在试制一台能正确制图的便宜计算机。计算机内部构件——复杂的线路——都摊在他的桌子上。明斯基回忆说：“这个大学一年级学生出现了。他在办公室里踱来踱去。当他看见那些线路时，我们俩的谈话开始了，然后他指着其中的一根线路说：‘我不明白你为什么需要它，因为那边的一根可做同样的事。’我一看，他确实说得对。他给了我相当深刻的印象，因为他只凭他的直觉——他不知道那些线路是做什么用的！显然，这个大学一年级学生是个相当出色的人物。”

希利斯同明斯基第一次讨论的问题是：为什么一个计算机不能更像一个人呢？自从那次讨论之后，这个重要问题，一直萦绕在希利斯脑海中，其自然产物就是连接机。

希利斯说：“有许多事，人做起来轻而易举，而机器却办不到。你能制出一种机器，它能以它的准确力把一根小针顺利地插进一个小孔里。可

是，那机器虽具有那种准确性，却不能拿起一杯水而不让水溢出来。这是个矛盾——机器比人准确得多，但也笨拙得多。”在希利斯之前想到这种矛盾的人，通常把人的成功，归于他有一个与他相互作用的、准确的环境形象。希利斯发现这种解释是表面的；他认为，那水杯给人的形象不是静态的，是因有触觉的反馈而不断调整的：“如果你看我们怎样拿起一杯水而不让水溢出，这与我们手的位置如何准确或如何准确地用力毫无关系。有关的是我们的手指所得到的反馈很好——即使闭上眼睛也能做到，只需凭感觉就知道这事做得多好。如果做得不好，我们调整握力。”希利斯称这种快速反馈的作用过程为一种“受控制的幻觉”：我们对现实世界有个假设——一个幻觉——（以水杯的位置来说）来自我们手指感觉的反馈，使我们去调整水杯位置，我们的手指提供了有关调整过的水杯位置准确性的信息反馈，等等，一直到我们自信地拿起那杯子。

五年前，当希利斯是研究生时，他用 256 个小压力传感器在一个机器人的指尖里做了一种原始的反馈器，其用意是制造一个用控制幻觉来操作的机器手指，手指通过触摸，能辨别 6 种不同的东西，全是常用的坚固件——螺母、螺栓、垫圈、暗销、扁销和定位螺钉。手指对感觉到的东西有个“幻觉”（比方说，一个垫圈），然后它检验那个幻觉（比方说，用触摸垫圈当中的孔的方法）。在机器的有限的领域中，这方法是够好的了，但给手指任何别的东西，如一小块口香糖，它会自信地把它认作一种紧扣件。

在明斯基的指导下，希利斯写的硕士论文就是“手指”，并开始了并行处理的研究。6 个处理机，每个功率相当于一台 IBM 个人计算机，为手指提供了计算能力。从这个经验中，希利斯认识到，需要相当大的计算能力，才能把一切可辨认的东西提高到人的食指水平来辨认。希利斯不是谨慎行事的人；后来他把微处理机连在一起，那就是连接机的原型。

希利斯在考虑了计算机里的电子组件和人脑神经原（神经细胞）的区别之后，决定连接几万个处理器，每个处理器比电子游戏机的微芯片弱。神经原要慢 100 万倍，而人脑做一些简单的事，如区别一个男人和一个女人，认读手写的字母，或说出一个 4 个字母的花名与 hose 押韵，则比任何计算机快得多。人脑怎样做这些事，人们知道很少，但它那眩目的速度，无疑来源于它有比计算机更多的基本组件，大约有几千亿神经原，其数目可上下波动 10 倍。而且希利斯还说：“人脑的结构，就我们能看到的，是完全不同于传统计算机的，原因在于它用很多东西并行工作。所以那就是在连接机内制造许多并行结构的直觉原因。”

希利斯是第一个承认人脑和连接机比较类似的人。首先，神经原的连接关系可能有 100 兆个，这意味着画出线路图是不可能的。确实，连接关系是那样多并缠绕在一起，神经生物学家还未曾成功地绘制过单一神经原的图，更不用说所有的神经原了。因此，人脑不能为连接机提供一个如何把处理机连在一起的模式。然而，大规模的并行性是人脑基本的特征，看来那就值得试制一个与人脑相似的计算机结构，即使是相差很远和不精确也问题不大。

此外，希利斯认识到，大规模并行性可能会使计算机做许多事，例如图像的分析及识别，这些人们容易做的事，单一处理机计算机，却根本不能开始做。举个例子，还没有一个计算机能区别一只狗和一只猫。传统计

算机遇到障碍，因为它必须一点一点地分析一个图像。所有的点都储存在计算机的存储器中，而每次只能通过连接存储器和处理机的单一狭窄通道——“诺伊曼瓶口”，取出一个点，希利斯说，它像是通过一个窥视孔在画面上移动，细看画面，而不像人的视觉那样，马上可以处理整个形象。连接机有指望做得更好，因为每个处理器实际上是分配到形象的一个点，65，536 个处理器一起工作，就能分析整体形象。

希利斯在麻省理工学院写博士论文时开始研究连接机。明斯基回忆说：“在设计问题上，丹尼应该认真一点，我对他说：‘我希望你不要犯伊利阿克IV型计算机的错误。’他说：‘哦，什么是伊利阿克IV型计算机错误？’我告诉了他。”

伊利阿克IV型计算机是 70 年代伊利诺斯大学制造的一个庞大计算机。它有 64 个处理机，每个像个直立的钢琴那样大，因为是提前制成的。事实上，他们要用叉车插入部件。它花了七八年才制成，制成时却已经过时了。该大学把它送给了国家航空和航天管理局，该局答应使用它，但用起来非常困难。

在现有的技术条件下，那项工程过于雄心勃勃，并非明斯基所谓的伊利阿克IV型错误。他告诉希利斯，其概念本身就有缺陷。他说，限定所有 64 个处理机在同一时间里做完全同样的工作，是个错误，是个扩大的奥林匹克配乐游泳表演用的电子计算机翻版。明斯基告诉希利斯，处理机应该能独立工作。

“大约一个月后，”明斯基回忆说，“丹尼回来对我说：‘喂，我已决定犯伊利阿克IV型的错误了。’”希利斯告诉明斯基，问题不在于处理器做什么，而在于它们如何交换信息。他说，处理器间的信号在业务繁忙时阻塞了，这主要是由于连接线路限于二维。希利斯认识到，需要有个更充分的连接方案，尤其是他要连接的处理机不是 64 个，而是 65，536 个。信号交换将会像为 65，536 个客户服务的电话网络，这些客户每秒钟要打 2．5 亿次电话。那就是希利斯在设计连接机时所面临的主要技术难题。

最后，希利斯和电子计算机公司的同事们，决定搞三维结构，把结构内的处理机连接起来，如同形成一个 16 维的立方体。这意味着，每个处理机虽然只同其他 16 个处理机直接连接，它离其他 65，536 个处理机的任何一个，决不会超过 16 步。此外，信号堵塞的可能性减少了，因为在 16 维中，在任何两个处理机之间有无数的路线可通。

传递信息的方法也很新颖。希利斯描述信息传递系统如同介于使用邮政系统工作方法和老式电话系统工作方法之间的方式。

在邮政系统中，投递一封信件采用的路线，有很大灵活性。希利斯说：“如果邮政飞机已经载满，他们可以把你的信件交下班飞机寄出。”邮政系统的缺点是，如果你有很多话要说，你必须寄出大量的信件。电话系统的优点是，你能一直占线到你联系完毕。“你和我通话时，至少是打本地电话，有一条线是给我们的。但是，我们不说话的时候，那条线我们仍占用着。”连接机胜过这两种系统。“它好像是我寄一封信给你，那信系着一根线连着另一封信，后一封信再系一根线，连着第三封信，等等。这样我们就可以不间断地联系。有必要的话，我们可以把线割断——把余下的信从一条不同的路线寄出。”

当佩金-艾尔摩公司汤姆·克雷的上级叫他观察连接机时，他有些怀

疑。他回忆说：“我不能想象你怎么能控制 65，000 个处理机。听上去毫无事实根据，但结果却是容易的。不管我构思的是什么问题，它都运算得快得多。把一个问题的数据分散，让小块数据分到每个处理机里去，从大规模并行性获得的好处之多，是出乎意料的。”

连接机问世的时间还不够长，所以我们不知道它对人工智能会有什么贡献，但是它在不太特殊的领域中，已经证明是有用的，例如像缩短一些牵涉到文件检索、线路设计和气流模拟等日常而棘手问题的工作的时间。

文件检索是个较大问题的一部分，它是从大量信息——计算机科学家称之为数据库——里去搜寻某一特定的文件。这种问题未必多有趣，但却一直出现着。再者，当数据库相当庞大时，传统计算机的缓慢是无法容忍的。拿扫描《纽约时报》一年的文章这个问题来说，计算机世界中的伊夫林·伍德连接机能立刻阅读全部文章，因为每篇文章是有效地分配给每一个单独处理机的，而不像传统计算机那样逐篇地看。希利斯说：“你可以设想扬基体育场有 65，000 人，每人有一份不同的文件。你通过扩音系统宣布一个题目，然后每人读他的文件，看看是否与题目相符。”那就是连接机做的事，但只需花三百分之一秒时间，比任何计算机快几百倍。

电子电路的设计，是单一处理机计算机一项费力的基础工业工作。在一个芯片内，成千的电子元件需要连接起来。一旦元件之间的连接大体完成，元件线路必须确定，使连接线路的长度减到最短，并尽量避免交搭。传统计算机做此工作缓慢，它是一次一个元件地改变电路设计的。这一工作是留给连接机做的，因为它的每个处理机代表一个不同部件，容易检查部件的各种布置。确实，连接机正为其后代设计芯片，据说新一代连接机有 100 万个处理器。

连接机最令人兴奋的潜在应用，是模拟气流，甚至可在一项列入计划的飞机机翼设计中，进行气流模拟。计算机科学尚未达到这样一种水平，即航空工程师能在一个超级计算机上模拟一架新型飞机乃至一个机翼的设计，并对它的功率能有把握。描述一架飞机或一个机翼周围气流的数学方程式，是人或计算机非常难解的。即使制造一个按比例缩小的飞机模型，放在风道里运行得极好，也不能保证真正的飞机会飞。除了制造和检验一架实体样机之外，没有代用品。

斯蒂芬·沃尔夫拉姆这位身材矮胖、年近 30、戴眼镜、留着细面条似的头发和长鬓颊须、每时每刻都想吃冰淇淋的物理学家，是探讨连接机采用新方法来解决气流问题的智囊。麦克阿瑟基金会曾给他颁发过权威性奖状，证明他是个“天才”，见到他的人都同意他这个称号。

沃尔夫拉姆认为不必担心描述空气聚集作用的复杂数学，要倾全力于个别空气粒子。每一个处理机有效地分配给一个粒子。在沃尔夫拉姆的样机中，粒子都以同样的速度向六个方向之一的方向移动。一个简单的规律解释了一个粒子与另一个粒子相撞，粒子是如何分散的。虽然这个样机由于受到每个粒子的速度和方向的限制而相当原始，但它似乎很有前途，这显然是因为分子实际上不能解数学方程式，但可以说它们是高举起双臂积极参与的。

如果模型按计划工作，航空工程师将会从他计算机终端的荧屏上看到粒子轰击计划中的飞机机翼的设计。最近，沃尔夫拉姆和希利斯决定，采用现有的工艺，有可能在连接机里再增加几十万个处理器，一直到它像一

座小建筑物那样大。这样一个计算机要花 1，000 亿美元，而且需要消耗现有最大的发电站的能源。沃尔夫拉姆说：“ 用那个计算机，你能模拟整架飞机。 ”别人对这条新闻可能感到沮丧，但沃尔夫拉姆不是。他说：“ 它给我带来希望。因为，如果工艺发生改变，我们可能终于能够设计出一架飞机。 ”

电子计算机公司不乏乐观主义。计算机未来的应用，是公司餐厅里人们交谈的熟悉的话题。希利斯和他的同事们提到，总有一天连接机能解决传统计算机即使是慢慢地，也无法解决的问题。这样一个问题，要搜寻的不是文件而是图片，每幅图片分配给它自己的处理器。电子计算机公司高级科学家小盖伊·斯蒂尔说：“ 你可以设想问计算机：‘ 在哪几部影片里，有 3 个滑稽演员配角同滑稽演员泽罗·莫斯提尔一起演出？ ’或‘ 在哪些人造卫星照片里有玉米？ ’我肯定地说，解决这类问题需要大功率的并行处理能力。 ”

沃尔夫拉姆幻想用连接机模拟各种物理系统，以便可以完全省略数学方程式。希利斯盼望有朝一日有个与连接机相似的巨大同类，作为计算机电站，为整个城市每家每户及商业机构提供计算功率。明斯基计划用连接机了解人是怎样思维的，采用以每个处理机模拟一小组神经细胞的方法，来模拟人脑。

该公司总体上想开发连接机的多头工艺，以制造真正的人工智能机器人，会走动，会说话，完全像“ 星球大战 ”中那个通用和服从的、控制论的合作者 C3P0。希利斯说：“ 公司长远的目标是制造一个真正的机器人，家用机器人最终将会是家庭主要的帮手，同今天汽车一样重要。它会做你要它做的一切事：打扫房屋、拿报纸、收拾盘碟、喂狗。 ”

在国际商用电器公司，谨慎的实用主义而非乐观主义是法则。这个拥有 500 亿美元的大亨确信，计算的未来就位于并行处理之中，但对利用几万个低功能处理器是不是出路这一点，还不能肯定。国际商用电器公司拒绝对连接机做出官方的评论，但它的研究人员们说，希利斯对计算机神经细胞似的结构宣传太过分了，而使这位科学家更像是个追逐名声的人，就连他新搞的信息传递方案，也可能低估了信息堵塞的可能性。

国际商用电器公司副总裁、计算机科学主任阿贝·裴勒德说：“ 我希望对那些与并行处理有关的问题有个更好的理论性理解。 ”为了获得理解，通常守口如瓶的独往独来的国际商用电器公司正在同至少 8 所大学合作，大学的研究人员在采用不同的战略。国际商用电器公司的计算机科学家格雷格·普菲斯特说：“ 我们不能单干，我们的方法是浇水施肥，培养它们开花，看哪一朵花先开。 ”

国际商用电器公司预计 RP3 型和 GF11 型计算机这两朵花，将在 1987 年开放。RP3 是由普菲斯特牵头，40 人参加制作的计算机。它包含 512 个大功率的处理器。不像连接机那样是由较多的小功率的处理器组成，它们都不限于同时做同样的事，而能各自分别去做。在实践中，这种大功率的灵活性效果如何，尚待观察。

GF11 处理机不像 RP3 是个多面手的计算机，它只有一个目标，那就是检验物理学家关于物质特性的最基本理论。自从苏格拉底前的原子论哲学家时期以来 2，400 多年，人们曾经寻找物质不可分割的组成部分。在过去几十年中，实验家已经制造了大功率的机器，用越来越强大的力量，把物

质碎块一起加以粉碎；在那些互撞的碎片中，他们已辨认出 200 种以上亚原子微粒新种类，是质子和中子的奇特亲属，质子和中子是两个我们熟悉的原子核组成要素。这些粒子有许多又呈现内部结构的迹象。1964 年，理论物理学家假定每种有结构的粒子，是由叫做夸克的几种基本建筑块料的不同组合构成，这样就把像凌乱的动物园似的粒子群系统化了。在 70 年代初期，夸克成为量子色彩动力学，或称 QCD 的基础。QCD 是描述粒子是由什么构成的和它们如何相互作用的综合理论。

参加 GF11 工程的粒子物理学家唐·韦恩加登说：“ 今天，QCD 看上去有 5，500 万种方法是不错的，但所有这些方法，都是粗糙的和定性的。你所希望的，是有个准确的数字预测，以便你可以把它拿出去与一种实验结果相比较。 ”QCD 对奇特现象确实能做出准确的数字预测，大大超过实验物理的范围，例如一个快速质子，其规模大得像整个宇宙一样。从 QCD 抽出关于切实物质的预测，如普通物质中的质子，需要一系列棘手的计算，而这种计算，无论是人或任何现有的计算机都做不到。例如，计算一个稳态质子团，要求大约千兆次运算。做如此大量的运算，会占用一台克雷 I 型计算机 30 年，或占用一台个人计算机至少 20 万年，而 GF11 并行处理机只需用 4 个月，其结果与测定的物质相比较，可能会提供第一次精确的量子彩色动力学测验。

GF11 确实不像理论物理学范畴的计算机。由两个冰箱一般大的空调器进行冷却，它占满整个房间。40 万个芯片形成 576 个处理器，塞满 20 个类似特大型的体育场巨大的单人衣帽柜。那些处理机是用 200 英里长的线路连接起来的，形成 2，000 根多种颜色蜿蜒电缆。在国际商业电器公司大家知道它叫“ 蒙提的大蟒 ”，是以 GF11 机 3 位设计师之一的蒙提·邓诺埃的名字命名的。邓诺埃说：“ 那个把所有线路连在一起的人，他眼睛仍然蒙着一层薄翳。他曾经是音乐家，可现在他什么都干不了。 ”

那 576 个处理器的每一个，都能通过叫孟菲斯转换器超幂转换网络，同任何一个处理器联系。所有的信息，即使在同一个柜里的处理器之间，必须经过孟菲斯转换器发送，正像早期联邦捷运公司的快递服务那样，所有的包裹（即使一件，例如从芝加哥至底特律），都必须经过孟菲斯城市递送。该转换器能在同一时间内处理相当于 200 万次的电话通话。

与连接机中的 65，536 个处理器一样，GF11 中的 576 个处理器也都同时执行同样的指令，但它每个处理器的功率则更大。每个处理器能在 60 万亿之一秒时间里，用一个 7 位数乘一个 7 位数，比连接机中的一个处理器快 3，000 倍。这种极强的数字运行能力是计算质子质量所必需的。虽然 GF11 的设计是为了量子色彩动力学方面的计算，国际商业电器公司希望将这种计算机做些较小的调整之后，能解决计算量很大而传统计算机不能解决的其他科学问题。

GF11 和 RP3 计算机在进行制造的时候，佩金-艾尔摩的奥克顿智囊箱里的连接机在紧张地工作，它的小红灯迷人地闪烁着。战略防御计划小组需要用镜子，把激光光束弹射到太空，佩金-艾尔摩公司正在给连接机模拟这种镜子。

不论是否具有人工智能作用，连接机适用于战场指挥。“ 今天，一场战役会牵涉 10 万支部队，每支部队以每小时 25，000 英里的速度行动， ”佩金-艾尔摩公司汤姆·克雷说，“ 只需 15 分钟，战役就会完全结束，所

以你必须同许多方面保持联系，连接机就起这种作用。”

电子计算机公司的第一个主顾佩金-艾尔摩公司购置了连接机，是再高兴没有了。克雷说：“我们喜欢它，即使别人还不准备抛弃用单个处理器编程序的 40 年的经验。并行处理像摇摆舞。当初人们说：‘这是什么讨厌的东西？这个艾尔维斯·普雷斯利[①]是什么人？’但人们接受了它，人们也将会接受并行处理机。”

[①] 艾尔维斯·普雷斯利（ElvisPresley），1935—1977 年，美国著名摇滚乐歌唱家。译者注。

第四篇 “一人一票”

数学被卷入计算机是不足为怪的。从实质上说，计算机毕竟只是 0 和 1 这两个数字的操作机。最初的电子计算机是由像艾伦·图灵和约翰·冯诺伊曼这样的数学家设计出来的。

早在人们梦想着有计算机之前，哲学家和政治科学家们就在为建立一个民主国家的方法而大伤脑筋。那时，数学以令人惊奇和令人讨厌的方式伸出它那丑陋的头角。美国经济学家肯尼斯·阿罗获诺贝尔奖的研究工作说明实现完美的民主理想在数学上是不可能的。确实，不受欢迎的悖论不仅会在表决中出现，甚至在表决进行之前，在间接代表制中，决定分配给每一选区的代表名额时也会出现，如同美国众议院那样。

第十二章　数学中的民主

对策论是对冲突进行数学分析，它存在于政治、商业、军事或各项事务之中。对策论诞生于 1927 年，由数学全能行家约翰·冯纽尔曼创立。冯纽尔曼认识到经济与政治中的某些决策条件在数学上与某些策略对策等价。所以从分析这些对策中所学到的东西可以直接应用于现实生活中的决策上。在 1944 年冯纽尔曼与普林斯顿大学经济学家奥斯卡·摩尔根斯特朗合著的当代经典著作《对策论与经济行为》出版之前，对策论，也叫冲突的科学，是鲜为人知的。

对策论的部分智力感染力在于它的许多成果，如量子力学或相对论，似乎是直觉的，甚至是颠倒性的。典型的一个问题是 1948 年《美国数学月刊》提出的，它还不时地在文献中出现。有 3 位名叫阿尔、本和查理的男子，参加一个新式的以气球为目标的掷镖游戏。参加游戏者每位各持一气球，只要气球不破，就可以继续参赛，优胜者属于惟一保持气球完好的参赛者。投掷的每一轮参赛者都以抽签决定游戏的掷镖顺序，然后依次投掷一支习镖，他们对各自的投掷技巧全部心中有数：阿尔可以在 5 次中 4 次击破气球（命中率 80%）;而本则在 5 次中可 3 次击破气球（60%命中率）；查理却是每 5 次只有 2 次可以击破气球（40%命中率）。那么每位参赛者究竟采用什么策略呢？

掷镖游戏

答案很明显。每位掷镖者都得把目标对准较强对手的气球，因为如果把它击中，他所要面对的只是较弱的掷镖手。不过，如果所有 3 位参赛者全都采用这种切合实际的试探策略，那么他们会得到与掷镖技巧相反的结果！概率计算显示，查理这个最差的掷镖手，取胜的机会最大（37%）。而阿尔这个最好的掷镖手，获胜的机会最低，为 30%。本的获胜机会也只有 33%。

问题出在哪里？问题就在于阿尔和本自己互相拼斗时，查理几乎不受任何威胁。由于阿尔和本彼此都坚持他们开始的策略，而使查理增强了他的幸存能力。

“显而易见的策略”

对于阿尔和本两者来说，最佳的策略莫过于在把查理除掉之前彼此之间不进行争斗；而查理的最佳对抗策略仍然是把镖掷向较硬的对手阿尔。在这种形势下，阿尔和本获胜之机会分别增加到 44%和 46.5%，而查理获胜的机会则会戏剧性地下降到 9.1%。然而这种局面可能是不稳定的。因为它需要阿尔和本进行合作。虽然阿尔是最佳的掷镖手，但他还是没有取胜的最佳机会，他可能想欺骗本。但是如果他不能用欺骗的飞镖把本击败，则本可能回击，而且计算出来的获胜机会将会再次发生变化。

如果阿尔不与本合作，不论他是否可以欺骗本，他可能试用另一种策略，这个策略曾在耶鲁大学数学研究所经济学教授马丁·苏比克所著的《社会科学中的对策论：概念与解法》一书中讨论过。

主要观点是阿尔通过口头威胁，试图形成一种局面，使阿尔与本处于一种拼斗状态，但使查理不向他掷镖，如同第一种情况那样，而是把镖掷向本。阿尔声称，只要查理不向他掷镖，他也决不向查理的气球掷镖（而且总是把镖掷向本）。阿尔要让查理明白，如果查理向他掷镖，他会还击

的。假如有报复的威胁，则概率计算就会证明，查理最佳做法仅是向本的气球掷镖。如果本也攻击阿尔，则阿尔的总获胜机会仍为 44.4%，本则为 20%，查理却是 35.6%，阿尔虽然未能增加其获胜机会——百分率没有变化——但现在他是竞争中的领先者。

当然，本也不善罢甘休。因此他也会像阿尔那样，对查理发出警告：“只要你不向我掷镖，我也不向你掷镖。要是你向我攻击，我也以牙还牙。”面对来自两个对手的威胁，查理的最佳策略是不对两者中任何一位攻击，而是掷向空中，假定规则允许持这种消极态度的话！苏比克解释说，这种奇特的策略对查理来说是最好的，因为只要没有人攻击他，那么他在游戏第一阶段中的惟一目标就是在第二阶段中增加他与本的一对一的对抗，而不是与阿尔对抗。查理聪明的手腕已使他获胜的机会增加了 0.6%，因而对阿尔来说获胜的机会现在是 38.1%，对本来说则为 25.7%，对查埋来说则是 36.2%。不过这还不是最后的定论。如果阿尔扩大了他的威胁面，从而使查理不再向空中掷镖，那么局面就会变得愈加奇妙。

这个问题是对策论中诸多问题中典型的一个。其基本前提是每位参赛者都是有理性的，而且都是力图为自身利益考虑。这个问题的一项教益在于，显而易见的策略——每位参赛者都试图除掉较强的对手——并不一定是好策略。这就是我认为解法是反直觉的解释。当然，由于你更进一步地投身于对策论，那么你的直觉就会改变，而且如果它是完全意想不到的话，则意想不到的局面就会更加意想不到。气球战的另一项教益是，在缺乏有关参赛者能否联络、共谋、进行威胁或达成有约束力并可以实施的协议等信息的情况下，对可能的解法是不能进行正确评估的。在对策论中，往往需要了解这样的社会学因素。

无须试图进行严格的论证，我们就能很容易地理解，气球战可能类似于政治或经济的竞争。按照纽约大学政治学教授斯蒂温·布拉姆斯的看法：气球战的知识可以扩展到多位候选人的政治竞选上，诸如 1984 年新罕布什尔州的民主党总统预选，当时有 8 个候选人竞选。布拉姆斯说道：“看来这些候选人的最佳战略，莫过于在他的部分政治势力范围内追随最强的对手。如果你是一个自由主义者，而且另外还有两位自由主义者，那么你就要追随最强的一位。于是所发生的情况将是两位最强的对手就会彼此攻击，而且最弱者就会存留下来了。”这时，如果所发生的情况全面出现，那么最弱的候选人就会在其政治势力范围内幸存下来。布拉姆斯说：“这是没有办法的，强有力的候选人会在这类竞选场合中崭露头角。”

1951 年，美国经济学家肯尼思·阿罗令人信服地论证：任何可以想得出的民主选举制度可能产生出不民主结果，这一论证使数学家和经济学家感到震惊。阿罗这种令人不安的对策论论证立即在全世界学术界中引起了评论。

1952 年，后来在经济科学方面获诺贝尔奖的保罗·赛缪尔森这样写道：“它证明了探索完全民主的历史记录下的伟大思想也是探索一种妄想、一种逻辑上的自相矛盾。现在全世界的学者们——数学的、政治的、哲学的和经济学的——都在试图进行挽救，都试图挽救阿罗的毁灭性发现中能够挽救出的东西，对数学政治来说，这一发现就是 1931 年库尔特·哥德尔的数学逻辑的不可能证明一致性定理。”

阿罗的论证，称之为不可能性定理（因为它证明了完全民主在事实上

是不可能的），该论证已帮助他于 1972 年获得了诺贝尔经济科学奖。对策论中最早的和最惊人的成果之一，也就是阿罗的“毁灭性发现”所产生的影响使人们至今还能感觉到。

在民主投票中所固有的不民主悖论可以用一实例进行很好的解释。现有 3 位朋友，罗纳德、克拉拉和赫布，他们在辛苦工作一天之后，渴望吃一顿快餐。他们决定一起到 3 家餐馆（麦克唐纳、伯格王或温迪）中的一家去就餐。但 3 人不能取得一致意见。罗纳德渴望在麦克唐纳餐馆吃饭，那里有漂亮的分餐盘，里面装着油腻的汉堡包和大量新鲜的炸土豆条，至于其他两家餐馆，他喜欢伯格王，然后才是温迪。克拉拉想去吃牛排，因而他喜爱温迪胜过麦克唐纳，最后才是伯格王；赫布想吃大奶酪饼，因而最喜欢伯格王，最不喜欢麦克唐纳。

罗纳德	克拉拉	赫布
1 麦克唐纳	1 温迪	1 伯格王
2 伯格王	2 麦克唐纳	2 温迪
3 温迪	3 伯格王	3 麦克唐纳

快餐的选择

这 3 位朋友决定用表决方法解决问题，首先在麦克唐纳和温迪之间选择，然后在取胜者与伯格王之间进行表决。如果罗纳德、克拉拉和赫布每人都按他们所实际喜爱的投票，那么他们最后会选定伯格王（第二名则是温迪）。

麦克唐纳	温迪	
（罗纳德）	（克拉拉）	
对	对	伯格王
温迪	伯格王	
（克拉拉、赫布）	（罗纳德、赫布）	

诚实的投票

因为伯格王是克拉拉的最后选择，她会很不高兴。如果克拉拉在第一次投票不选择她真正喜爱的温迪，而改而投选她的第二选择麦克唐纳，那么她就能确保麦克唐纳在第一次和第二次中都能赢得表决。克拉拉由于开头违背了她自己的意愿而最终实现了所喜爱的结果，这就是悖论。

麦克唐纳	麦克唐纳	
（罗纳德、克拉拉）	（罗纳德、克拉拉）	
对	对	麦克唐纳
温迪	伯格王	
（赫布）	（赫布）	

不诚实的克拉拉

况且，即便罗纳德和赫布识破克拉拉的策略，他们也不能有效地加以干扰。赫布很生气，这是由于克拉拉巧妙的投票才使他的第三意愿餐馆成为获胜者。反之，克拉拉这一方的“诚实”投票就会使赫布的第一意愿成为获胜者。赫布试图说服罗纳德，让罗纳德和他一起合谋进行

某种不诚实的投票。但罗纳德不愿意参与，因为这样做也不可能改变他自己的处境。克拉拉的投票已使罗纳德的第一选择的餐馆成为获胜者。

表决顺序的改变也不能消除巧妙投票的可能性。它所能做的是给别人而不是克拉拉不诚实投票的机会。假定这 3 位朋友首先在伯格王和温迪之间进行表决，再对获胜者与麦克唐纳进行表决，如果他们全都“诚实地”投票，那么最终会选择麦克唐纳，使赫布大失所望。

伯格王	伯格王	
（罗纳德、赫布）	（赫布）	
对	对	麦克唐纳
温迪	麦克唐纳	
（克拉拉）	（罗纳德、克拉拉）	
	诚实的投票	

如果赫布足够机敏，能预见到这个结果，那么他应在第一次投巧妙的一票，以促使他们最终转向选择温迪。

伯格王	温迪	
（罗纳德）	（克拉拉、赫布）	
对	对	温迪
温迪	麦克唐纳	
（克拉拉、赫布）	（罗纳德）	
	不诚实的赫布	

其他可能的表决顺序——即首先在麦克唐纳和伯格王之间表决，而后在获胜者与温迪之间表决——情况也并不好些。

伯格王	麦克唐纳	
（赫布）	（罗纳德）	
对	对	温迪
麦克唐纳	温迪	
（罗纳德、克拉拉）	（克拉拉、赫布）	
	诚实的投票	

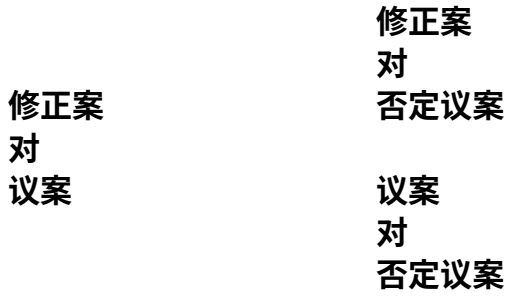
它只会给罗纳德以进行机敏投票的机会：

伯格王	伯格王	
（罗纳德、赫布）	（赫布、罗纳德）	
对	对	伯格王
麦克唐纳	温迪	
（克拉拉）	（克拉拉）	
	不诚实的罗纳德	

虽然这 3 位将要就餐者遇到的窘境是虚构的，但它却不是编造出来的。在一系列的投票中，是从 3 个或者更多候选者中选出一个获胜者，巧

妙投票的可能性可以在任何多数规则的表决中出现。

当美国众议院提出一项议案修正案时就会发生这样的情况。首先众议院要就修正案投票表决，如果获得通过，那么就应在修正案和完全否定议案之间进行第二次和最后表决。如果修正案未获通过，则第二次表决是在原议案和否定议案之间进行。



修正案的悖论

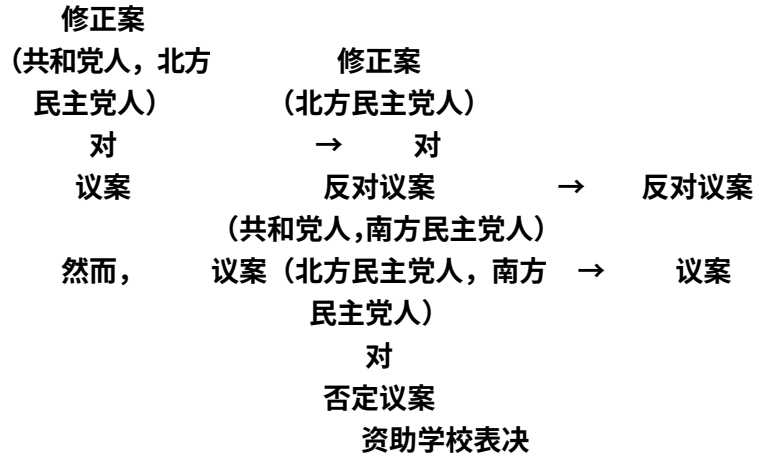
美国罗彻斯特大学的威廉·赖克在其《政治科学中的数学应用》一书中分析了 1956 年众议院关于要求联邦政府资助学校建设议案的表决情况。当时提出了修正案，要求联邦政府只向那些已经取消种族隔离学校的州进行资助。众议院实质上已分成三个利益集团：共和党人、北方民主党人和南方民主党人。反对联邦资助，但

赞成取消种族隔离的共和党人完全赞成否定议案，但相比之下，宁愿要修正案而不愿要原议案。而北方民主党人赞成修正案，但宁愿要原议案而不愿要否定议案。南方民主党人都是来自实行种族隔离学校的各州，他们赞成原议案，但宁愿要否定议案而不愿要修正案。

共和党人	北方民主党人	南方民主党人
1．否定议案	1．修正案	1．议案
2．修正案	2．议案	2．否定议案
3．议案	3．否定议案	3．修正案

对学校资助的投票意愿

对于修正案的表决，共和党人和北方民主党人一起投票，赢得了表决。但是在第二次表决，即在修正案和不否定议案之间表决时，共和党人与南方民主党人联合，否决了修正案。在这里，这种悖论表现为：在没有修正案的情况下，要在原议案和否定议案之间进行直接表决，则原议案无疑会赢得胜利！



赖克得出结论：“选择可能取决于表决顺序这种看法似乎还是不够的，这一事实可以用来扭曲立法程序的结果。它有可能会产生一种表决上的悖论，即使议案在悖论产生之前就已获得通过，也会使立法机构无法采取行动。立法议员可以提出修正案，使这种悖论得以产生，而且如果表决程序恰好正确的话，那么修正议案将会被否决。”

早在 18 世纪，法国数学家让-安托万-尼古拉斯·卡里塔特，德·孔多塞侯爵就看出了表决的悖论。他发现社会上往往有优先选择，但是如果是个人的优先选择，就被认为不合理而不加以考虑。现在回过头来考虑我们 3 位饥饿的朋友，罗纳德喜欢麦克唐纳胜过伯格王，而伯格王又胜过温迪。已知这些优先选择，要他喜爱温迪胜过麦克唐纳，对他说来是不合理的。然而，这些却恰恰是我们的朋友作为整体时的优先选择！在集体表决中，他们宁愿去麦克唐纳而不去伯格王，宁愿去伯格王而不去温迪，宁愿去温迪而不去麦克唐纳。所以，从数学的观点来看民主是不是有内在的不合理呢？

罗纳德的优先选择：

麦克唐纳→伯格王→温迪

因此：麦克唐纳→温迪

集体的优先选择：

在民主表决中的数学悖论已由世界上一位大对策学家史蒂文·布拉姆斯进行了广泛研究。他不仅把数学用于涉及表决方面的各种问题，还用于各种各样看来难以进行定量分析的问题。在他的《总统选举的对策》一书中，布拉姆斯使用对策论分析了理查德·尼克松总统的行为和最高法院关于那件迫使总统交出有罪的“白宫录音带”的案例。他在《圣经的对策》一书中把对策论用于分析旧约全书中上帝和人类的矛盾，并得出结论：上帝是个出色的策略家，一位敏感的、沉思的，又为他在世上的声誉所困扰的武断的神。在《高傲的神：如果他们存在，我们怎能知道？》一书中，他探讨了无所不知、无限权力、不朽的生命和不能理解性的对策论含义。布拉姆斯还将对策论应用于实际之中，从超级大国的矛盾和职业运动员的选拔到劳工管理谈判以及电视演播计划等种种主题。

布拉姆斯对应用数学感兴趣还得追溯到他在麻省理工学院当大学生

时，那时苏联刚刚发射了人造地球卫星。他曾有志于主修物理学，但他发现他在实验室里是一个十足笨头笨脑的人，从而打消了这个念头。那些损坏的设备，使他清醒了，他转而攻读数学，并在数学领域一直遥遥领先。他还选修比较新的政治科学系中大名鼎鼎的教授的课程。在那里他发现了他的专长：把数学应用于政治形势上。他的第一批成果主要涉及对国标贸易流通进行数学模拟的统计工作。离开麻省理工学院，他又到西北大学当研究生。因为他在政治科学方面有一种标新立异、特别的定量分析课程。

布拉姆斯说道：“像每一位有自尊心的政治科学家一样，我考虑应在政府中从事某些工作，但不愿意在和平队里干活。”在 1963 年和 1964 年夏季里，他先在国家卫生研究所任所长，而后又到国防部部长办公厅任职。当他完成研究生学业时，他已把整个身心投入国防分析研究所的工作，那是一家非盈利的研究机构。主要是为联席参谋长和国防部长办公室工作。布拉姆斯回忆道：“我被特别雇用从事如何在国防部进行决策的研究。在 6 个月内，我设计并预先试验了一种调查表。我将要进入战地并会见一些高层人物——副部长、将军、舰队司令——可是国防分析研究所所长停止了这些研究工作。这时越南战争升级，热化，而所长认为这项研究太成问题，特别是由于国防部是国防分析研究所的主要委托人。我感到非常恼怒，并且断定能够自由和独立地做我想做的事的惟一地方是大学。”

他开始在罗彻斯特大学教学，校内拥有国内最有效地进行定量分析的政治科学系。曾经分析 1956 年众议院关于学校建设问题投票的赖克当时正在罗彻斯特大学，于是布拉姆斯从他那里获益匪浅，对对策论产生了强烈的爱好。而且，布拉姆斯补充道：“从那时起，我从未离开过这个主题。”

对策论的评论家们不时指责它是一门诡诈科学，为赞成政治掮客的狡猾策略而打上了数学的印记。然而对策论不会产生表决的悖论，它只不过用形式的方法来认可它们而已。1956 年众议院就学校建设议案所做的悖论表决是自然产生的，而不是由于国会众议员们从马基雅维里式的某些对策论杂志中获得的提示得来的。

一旦悖论被正式认可，对策论就能有助于评估悖论通常是如何产生的。例如，现在我们看看法国数学家孔多塞的观察，由每个人投票决定的群体优先选择在悖论上可能是“非传递性”；如想吃快餐的群体，宁愿去麦克唐纳而不愿去伯格王，宁愿去伯格王而不愿去温迪，然而又喜爱温迪胜过麦克唐纳。如果这个群体由 3 个人组成（罗纳德、克拉拉和赫布），而仅当每个餐馆首先由一个人排序，其次由另一个人排序，第三再换一个人排序时，这种“非可递性”就将出现。假定所有可能的个人优先选择看来都是相等的，则整个群体的非可递性的机会为 5．6%。这个数字看来似乎不大，但要记住这个百分率只不过是针对了个人和 3 个选择对象的最简单情况。

布拉姆斯在《政治学中的悖论》一书中总结了更复杂情况中群体非传递性概率的最新研究，其结果是在选择对象和投票人数目增加的两种情况下，非传递性的概率才增加，但它对选择对象的数目更为敏感。如果选择对象固定数为 3 时，则悖论的可能性会略有增加，从 5．6%（投票人为 3 时）增加到 8．8%（投票人数接近于无穷大）。如果投票人固定数为 3 的时候，则悖论的可能性会陡然上升，从 5．6%（选择对象为 3 时）增加到 100%（由于选择对象数接近无穷大）。的确，布拉姆斯特别提到对于投票

人的任何固定数，由于选择对象数无穷地增加，悖论的概率必然会逐渐上升。

		选民数					
		3	5	7	9	11	∞
选	3	5.6％	6.9％	7.5％	7.8％	8.0％	8.0％
择	4	11.1％	13.9％	15.0％	15.6％	16.0％	17.6％
对	5	16.0％	20.0％	21.5％	23.0％	25.1％	25.1％
象	6	20.2％	25.5％	25.8％	28.4％	29.4％	31.5％
数	7	23.9％	29.9％	30.5％	34.2％	34.3％	39.9％
	∝	100％	100％	100％	100％	100％	100％

群体非传递性机会

摘自史蒂文·布拉姆斯著《政治学中的悖论》（纽约，1976 年自由出版社）第 42 页。

对策论中的数学可以与许多其他抽象数学学科中所涉及的数学进行简单的比较。但它决不是无价值的。的确，数学常常会导出反直觉的或者违背所预期的结果。数学的简明性不会使对策论的严密性比高维拓扑学的严密性更差，刊登这种问题的杂志也只有一小部分博士能够读懂。简明性甚至可能是优点：对策论中的数学是这样容易理解，从而几乎没有可能由于文献中的数学论述模糊难懂而引不起人们的兴趣。

美国数学学会的全体官员都认为布拉姆斯的论述有误。这样一个著名的数学家团体能出现差错的事实表明对策论的结果是如何令人吃惊。这种错误论述出现在美国数学学会的投票说明上，学会会员将使用该说明选出参加特别委员会的代表。对于这次投票，美国数学学会恢复了表决程序，采用单一的可转让投票制度（又称选择投票法）。它是 19 世纪 50 年代后期由不引人注意的英国律师托马斯·黑尔提出的，他曾撰写过两本书，批判传统的投票制度。

黑尔曾特别为下述事实所苦恼：在传统的比例代表制中，每个选区选举一位以上的候选人，实际上，为数甚多的少数选民可能会被剥夺掉选举权，尽管他们的原号码表明他们有资格选出代表。现考虑一个假设的选区，要从 4 位候选人中选出两位代表。把其中的两位候选人称作匈奴人阿蒂拉和吉·乔，他们都是典型的保守派人士，两人中阿蒂拉是极右人士。另外两位候选人是哈尔·汉道特和弗里达·弗里拉夫，他们都是自由派。两人中弗里拉夫更富有同情心。该选区内有 23 位选民，其中 13 位是保守派，10 位是自由派。23 位选民的选举意愿，按照对候选人的选择从第一选择到最后选择的顺序排列如下：

选民数	第一选择	第二选择	第三选择	第四选择
7	阿蒂拉	吉·乔	汉道特	弗里拉夫
6	吉·乔	阿蒂拉	汉道特	弗里拉夫
6	汉道特	弗里拉夫	吉·乔	阿蒂拉
4	弗里拉夫	汉道特	吉·乔	阿蒂拉

在选举中，每位选民允许选出两位候选人，阿蒂拉和吉·乔都将当选。因为这两位候选人每位都各得 13 票。结果是 10 位自由派选民将没有代表，

即使他们构成全体选民的 43%。而 13 位保守派选民仅构成全体选民的 57%，却有 100%的代表。

黑尔认为，所选出的代表应更精密地反映全体选民的构成，他巧妙地设计出一种复式选举制，它要求每位选民按其选举意愿顺序列出候选人名单，使选民能在候选人中间区别他们。然后把第一选择投票列成表格，而候选人只要达到定额选票，都要当选。

定额需要计算，它应是第一位选票的最小数，使得最大数目的候选人都能达到与候选席位数相符合的定额。例如上述例子中，有 23 位选民和 2 席候选席位，当选的定额应是 8 票；这样只有 2 位候选人（并非 3 位）能得到 8 票的第一位选票。定额定为 7 票又太低，因为有 3 位候选人可能会达到这个定额；由于只有两个待选席位，因此达到定额的候选人多出了一位。（一般说来，定额可用下法求出，即用选民数除以比待选席位大 1 的数，再加 1 即为定额数，但要舍去得出的任何分数。）

假设至少有一位候选人达到了定额选票，而且至少仍有一个席位空缺待选，那么当选的候选人超出定额的选票会按比例地转移到那些选民票数多的候选人身上。如果这种转移促成另一位候选人达到定额，那么他也当选；而且如果席位仍然未满，则超额的选票会再次按比例地转移。这个过程会继续下去，直到所有席位选满为止。如果在任何一处还有待选席位，但却没有超额选票转移，那么得票数最低的候选人就会被淘汰掉，而他的支持者会简单把他们的选票转移到他们选择的、票数最多的、仍在参加竞选的候选人身上。这个概念就是不会有选票作废的概念；如果选举需要选出的不只是一位候选人，可以在别处计票；如果把它分散在最少选票的候选人身上，也可以在别处计票。

理解这些选举规则的最好方法是把它们应用于具体实例上。

试把这些章程用于我们上面设想的选区内。由于定额是 8 票，4 位候选人中每位都不能达到定额。因此得票最少的候选人弗里达·弗里拉夫就被淘汰掉，而她的 4 位支持者将他们的选票转移给哈尔·汉道特，即他们的第二选择。如果弗里拉夫已从选举意愿表中淘汰掉，那么其顺序表如下：

选民数　选举意愿（从最好到最差）

7　　阿蒂拉　　吉·乔　　汉道特

6　　吉·乔　　阿蒂拉　　汉道特

10　　汉道特　　吉·乔　　阿蒂拉

现在哈尔·汉道特已超过定额 2 票，因此他已当选，他的超额两票已转移到吉·乔身上：

选民数　选举意愿（从最好到最差）

7　　阿蒂拉　　吉·乔

8　　吉·乔　　阿蒂拉

这时吉·乔也已达到定额票数，所以他赢得了另一席位。

汉道特和吉·乔的当选使黑尔兴奋：不论保守派还是自由派都有了代表，每个阵营中比较激进的候选人均未能当选。这样一种结果给约翰·斯图尔特·穆勒以深刻印象，他称颂黑尔的选举制是“在政府的理论和实践方面所做出的最伟大的改进之一”。今天，黑尔的选举制已广泛地用于澳大利亚、马耳他、爱尔兰共和国和北爱尔兰的立法选举和纽约市的学校董事会选举以及马萨诸塞州坎布里奇市的市政委员会选举上，更不必说许多

像美国数学学会这一类的专业组织的投票选举了。

美国数学学会的投票包括两种强硬的说法：“标出较少的候选人不会获得战术上的有利条件。”以及“按你的选举意愿顺序标出候选人，直到你认为不了解或你不感兴趣而没有标出的候选人，这是可取的。”而布拉姆斯举出了一个能够证明这种做法是不真实的例子，它可能有利于标出较少数的候选人。假定有 17 位选民，2 个待选席位和 4 位候选人，现称他们为格拉夫博士、迪济特博士、波因特博士、马尼福尔德博士，选民的选举意愿顺序如下：

组别	选民数	选举意愿顺序（从最好到最差）
A	6	格拉夫博士　迪济特博士　波因特博士　马尼福尔德博士
B	6	格拉夫博士　波因特博士　马尼福尔德博士　迪济特博士
C	5	格拉夫博士　马尼福尔德博士　迪济特博士　波因特博士

格拉夫博士赢得了 17 张选票，定额为 6 票，超额了 11 票。因此这 11 票需要转移。在这种情况下，选民们都支持当选者，不会再做其他选择了。而黑尔的选举章程（这是美国数学学会所遵循的）要求将超额的 11 票按比例地转移：11 票的 6／17 转移到 A 组，11 票的 6／17 转移到 B 组，而 11 票的 5／17 转移给 C 组，其结果如下：

组别	选民数	选举意愿顺序（从最好到最差）
A	3.9	迪济特博士　波因特博士　马尼福尔德博士
B	3.9	波因特博士　马尼福尔德博士　迪济特博士
C	3.2	马尼福尔德博士　迪济特博士　波因特博士

由于没有一个候选人能达到定额，得票最少的候选人马尼福尔德博士就被淘汰掉，而其支持者的 3.2 票会转移到他们选举的选票高的候选人波因特博士身上：

组别	选民数	选举意愿顺序（从最好到最差）
A	7.1	迪济特博士　波因特博士
B	3.9	波因特博士　迪济特博士

现在迪济特博士已超过 6 票定额，所以他与格拉夫博士一样，成为当选的候选人。

B 组的 6 位选民（其选举意愿顺序为格拉夫博士、波因特博士、马尼福尔德博士和迪济特博士）为他们的第一选择当选而高兴，但也感到不安，因为他们的最后选择也当了选。假定选举重复下去，一切照旧，那么 6 个选民中就有两位决定不去理会美国数学学会的说法（“标出较少的候选人不会获得战术上的有利条件”），而且都把选票投在格拉夫博士身上。这样选举意愿就会分成 4 类：

组别	选民数	选举意愿顺序（从最好到最差）
A	6	格拉夫博士　迪济特博士　波因特博士　马尼福尔德博士
B’	4	格拉夫博士　波因特博士　马尼福尔德博士　迪济特博士
B”	2	格拉夫博士
C	5	格拉夫博士　马尼福尔德博士　迪济特博士　波因特博士

在第一个顺序表上，格拉夫博士再次成为全体选民一致选择。他支持者的 11 票超额选票的 6／17 分配给 A 组，4／17 分配给 B’组，2／17 分

配给 B”组，还有 5／17 分配给 C 组。于是 B”组就被淘汰了。因为其成员除在第一选择外不能再标出其选举意愿了。因此情况形成如下：

组别	选民数	选举意愿顺序（从最好到最差）
A	3．9	迪济特博士　波因特博士　马尼福尔德博士
B’	2．6	波因特博士　马尼福尔德博士　迪济特博士
C	3．2	马尼福尔德博士　迪济特博士　波因特博士

在第一次选举中，第二位候选人未能达到定额，所以得票最低，也就是说波因特博士就被淘汰掉,而他的支持者的 2.6 张选票要归并到 C 组中：

组别	选民数	选举意愿顺序（从最好到最差）
A	3．9	波因特博士　马尼福尔德博士
C、B’	5．8	马尼福尔德博士　波因特博士

其余的两位候选人都少于定额的 6 票，但波因特博士由于票数较少而被淘汰，而马尼福尔德博士就被宣布当选。B 组中两位聪明的选民标出了不足的选票反而得到更可取的结果：他们的第三选择而不是第四选择就赢得了一个席位。

在实际的选举中，这样的结局可能难以实现，布拉姆斯写道：“我希望能搞清楚。我并不是说投票者会一成不变地把战略考虑搞得很绝对（在美国数学学会投票说明的反例中）。这些考虑不仅相当复杂，有时还由于其他选民在对策运用方面的反策略考虑而形成中立。相反，我认为投票者按选举意愿对所有候选人的顺序进行排列的意见，在黑尔选举制下并不总是合理的。”

况且，在布拉姆斯的反例中，如果 B 组中有太多的选民试图进行巧妙投票并投了不足的选票，那么结果会失控。假定 6 位选民中有 5 位在其投票中只投格拉夫博士，那么在第一次投票之后，情况就会变成：

组别	选民数	选举意愿顺序（从最好到最差）
A	3．9	迪济特博士　波因特博士　马尼福尔德博士
B’	0．6	波因特博士　马尼福尔德博士　迪济特博士
C	3．2	马尼福尔德博士　迪济特博士　波因特博士

由于没有一位候选人达到定额，因此波因特博士被迫退出，而其支持者加入 C 组；

组别	选民数	选举意愿顺序（从最好到最差）
A	3．9	迪济特博士　马尼福尔德博士
C、B’	3．8	马尼福尔德博士　迪济特博士

这次马尼福尔德博士必须退出竞选了，剩下的迪济特博士是获胜者，与原先 B 组的 6 位选民在他们的选票上排列全部 4 位候选人时他所处的位置一样。

由于惟恐你认为布拉姆斯的反例取决于当选票按比例地转移时而产生的分数，他解释了另一个反例，只是在这个反例中，全部选票由于候选人被淘汰而转移。这个实例涉及了 21 位选民，他们要从 4 位候选人当中选出 1 位代表。由于只有 1 位候选人被选，因此这种投票选举制是一种淘汰竞选，选举则在 1 位候选人获得 11 票的微弱多数后就立即终止。我把这个问题留给你，让你充当对策论学家的角色并解释一个反例。当然，其目标是

以下述方式确定选举意愿，即让一些选民可以从不理会美国数学学会的意见而得到好处。（在本章最后你会看到布拉姆斯所提出的反例。）

黑尔选举制的问题，要比这些公认的人为的反例深得多；仅仅知道某些选举意愿，或只有一些选民确切掌握有关他们竞选伙伴的全部选举意愿，这些难题就会出现，如果“敌对”的选民没有采取有效的对抗策略，或者如果相当多具有同样想法的选民不试图采用巧妙的花招，问题也同样会出现。罗彻斯特大学的吉迪恩·多隆和理查德·克罗尼克提请人们注意黑尔选举制的反常特点，即使所有选民都能诚恳地投出反映他们全部选举意愿的选票，这种反常特点也会出现。[①]多隆和克罗尼克注意到，在黑尔的选举制中，一位候选人如果接受附加选票，那么他可能受到损害。的确，多余的选票可能使一位当选者成为落选者。

为了理解这种反常的可能性，可考虑多隆和克罗尼克的例子。

并以我们的老朋友阿蒂拉、吉·乔、哈尔·汉道特和弗里达·弗里拉夫为例。这次该选区有 26 位选民，有 2 位候选人当选，所以定额为 9 票，26 位选民的意愿是多种多样的，不必划分自由派阵线和保守派阵线：

组别	选票数	选举意愿（从最好到最差）			
A	9	阿蒂拉	吉·乔	汉道特	弗里拉夫
B	6	汉道特	弗里拉夫	吉·乔	阿蒂拉
C	2	弗里拉夫	汉道特	吉·乔	阿蒂拉
D	4	弗里拉夫	吉·乔	汉道特	阿蒂拉
E	5	吉·乔	汉道特	弗里拉夫	阿蒂拉

由于阿蒂拉已经达到定额票，他当选了。阿蒂拉没有超额的选票，所以是最低票数的当选者，而吉·乔被淘汰了，他的 5 张选票转移给 B 组：

组别	选票数	选举意愿（从最好到最差）	
B、E	11	汉道特	弗里拉夫
C	2	弗里拉夫	汉道特
D	4	弗里拉夫	汉道特

汉道特拥有 11 张选票，因此当选了。

现考虑第二组选举意愿，除两位选民外，它与前一组相同，原先这两位选民宁愿投弗里拉夫票，不愿投汉道特票（C 组），现在改而投汉道特票，不投弗里拉夫票（C’组）。换句话说，C’组的选举意愿与 B 组的选举意愿相同。因而汉道特开始有 8 张第一位选票，比以前多了两票：

组别	选票数	选举意愿（从最好到最差）			
A	9	阿蒂拉	吉·乔	汉道特	弗里拉夫
B	6	汉道特	弗里拉夫	吉·乔	阿蒂拉
C’	2	汉道特	弗里拉夫	吉·乔	阿蒂拉
D	4	弗里拉夫	吉·乔	汉道特	阿蒂拉
E	5	吉·乔	汉道特	弗里拉夫	阿蒂拉

[①] 见多隆和克罗尼克著《单一的可转移选票：反常的社会选择功能的一个实例》，美国政治科学杂志 4 期（1977 年 5 月）：303—311 页。

阿蒂拉已再次立即当选，没有超额选票转移。然而这次最低票数当选者是弗里拉夫，不是吉·乔。而且弗里拉夫的 4 票与 E 组中的 5 票结合，选出吉·乔，超出定额：

组别	选票数	选举意愿（从最好到最差）	
B	6	汉道特	吉·乔
C’	2	汉道特	吉·乔
E、D	9	吉·乔	汉道特

这样的结果不太反常。回想一下，除了 2 位选民把汉道特从第二选择抬高到第一选择外，所有的选举意愿顺序都是一样的。这样就具有否定他的选举的效果。多隆和克罗尼克得出结论：“ 这简直太不公平，1 位候选人落选了，是因为他（或她）得到的选票过多了。大多数选民可能会十分反感和愤怒，被转让了，他们听到假想的（但是理论上是可能的）选举之夜的报道：‘ 奥格雷迪先生在今天选举中没有获得席位，但是，如果在第二个地方而不是在第一个地方有 5，000 名支持者投他的票，那么他会反败为胜的！’ ”

过多的选票能使一位当选者成为落选者这一反常的可能性，不仅仅是黑尔选举制的人为产物。美国电话电报公司贝尔实验室的数学家布拉姆斯和彼得·菲什伯恩在其合著的《认可的选举》一书中指出，它还可能困扰着类似于流行的相对多数选举这样的选举制，该选举制必然会产生 2 位得票最多的候选人之间的最后角逐。现在考虑 3 位候选人，马尔柯·迪拿芝、帕特里克·奥罗克、巴兹尔·杰斐逊，同时有 17 位选民，他们的选举意愿如下：

组别	选票数	选举意愿（从最好到最差）		
A	6	迪拿芝	奥罗克	杰斐逊
B	5	杰斐逊	迪拿芝	奥罗克
C	4	奥罗克	杰斐逊	迪拿芝
D	2	奥罗克	迪拿芝	杰斐逊

如果所有的选民都诚实地投票，那么迪拿芝（得 6 票）和奥罗克（得 6 票）将进行角逐，最后迪拿芝当选，11 票对 6 票。

现在设想除了最后一组选民把迪拿芝从第二选择抬高到第一选择之外，其余的选举意愿均相同：

组别	选票数	选举意愿（从最好到最差）		
A	6	迪拿芝	奥罗克	杰斐逊
B	5	杰斐逊	迪拿芝	奥罗克
C	4	奥罗克	杰斐逊	迪拿芝
D’	2	迪拿芝	奥罗克	杰斐逊

在第一次投票中，迪拿芝（8 票）和杰斐逊（5 票）进行角逐，于是迪拿芝输了，8 票对 9 票，因为奥罗克的 4 位支持者成为了杰斐逊的支持者，迪拿芝获得的支持虽有增加，但却反常地破坏了他的胜利。

布拉姆斯还认为，在不需要最后角逐的简单多数选举中，候选人在预选投票中有何进展的公告也可以产生同样的反常效果。假定上述的第一组选举意愿中有两位 D 组选民喜欢选奥罗克而不选迪拿芝，投票的结果将通知杰斐逊的支持者，他们支持的候选人已处于最后一名。于是杰斐逊的支持者得到了信息，他们必须放弃他们支持的候选人，策略性地转投他们的

第二选择意愿迪拿芝，迪拿芝因而将当选。假定上述的第二组选举意愿中，迪拿芝得到了 D 组选民的支持，投票结果将通知奥罗克的支持者，他们支持的候选人已处在最后一名。理所当然地，他们将转而支持杰斐逊。尽管迪拿芝也获得两位以上选民的支持，杰斐逊还是击败了迪拿芝。实际上，民意测验代替了第一轮投票，使实际选举相当于最后的角逐。

多隆在另一篇论文[①]中指出，黑尔选举制的另一种困境是：一位候选人在两个单独选区内都可以获胜，而在两个选区的合并投票时却会落选。在多隆的例子中，1 个候选人由 4 组选民选举。每个选区有 21 位选民，因此每个选区当选的定额是 11 票。

第一选区

组别	选票数	选举意愿（从最好到最差）			
A	8	阿蒂拉	吉·乔	汉道特	弗里拉夫
B	4	吉·乔	汉道特	弗里拉夫	阿蒂拉
C	3	汉道特	阿蒂拉	弗里拉夫	吉·乔
D	6	弗里拉夫	汉道特	吉·乔	阿蒂拉

第二选区

组别	选票数	选举意愿（从最好到最差）			
A	8	阿蒂拉	吉·乔	汉道特	弗里拉夫
B	4	吉·乔	汉道特	弗里拉夫	阿蒂拉
C	6	汉道特	阿蒂拉	弗里拉夫	吉·乔
D ’	3	弗里拉夫	阿蒂拉	吉·乔	汉道特

在两个选区内，最初时无一人达到定额 11 票。在第一选区，汉道特得到倒数第一位的选票，被淘汰了，他的支持者的选票都转给阿蒂拉，使阿蒂拉得到 11 票当选。在第二选区，阿蒂拉从选票最低的候选人弗里拉夫处获得 3 票，成为当选者。

现在再考虑当这两个选区合并成单一选区时会发生什么情况，其中 42 位选民的选举意愿仍然不变：

合并成一大选区

组别	选票数	选举意愿（从最好到最差）			
A	16	阿蒂拉	吉·乔	汉道特	弗里拉夫
B	8	吉·乔	汉道特	弗里拉夫	阿蒂拉
C	9	汉道特	阿蒂拉	弗里拉夫	吉·乔
D	6	弗里拉夫	汉道特	吉·乔	阿蒂拉
D ’	3	弗里拉夫	阿蒂拉	吉·乔	汉道特

现在当选定额是 22 票。由于选民的选举意愿完全相同，要是阿蒂拉不再当选，那么它将是反常地矛盾。但是反常的情况还是占优势。由于没有一个人能得到规定额选票，所以吉·乔被淘汰了，而其支持者的 8 票转移到他们的第二选择，也就是投汉道特的票：

合并成一大选区

[①] 《黑尔选举制是矛盾的》政治研究杂志第 27 期（1979 年 6 月）：283—286 页。

组别	选票数	选举意愿（从最好到最差）		
A	16	阿蒂拉	汉道特	弗里拉夫
B	8	汉道特	弗里拉夫	阿蒂拉
C	9	汉道特	阿蒂拉	弗里拉夫
D	6	弗里拉夫	汉道特	阿蒂拉
D’	3	弗里拉夫	阿蒂拉	汉道特

全部候选人再次都没有得到定额选票，因此得票最少的弗里拉夫被淘汰了。弗里拉夫在 D’组中的 3 位支持者把他们的选票转移到他们的第三选择阿蒂拉,而弗里拉夫 6 位在 D 组的支持者则转移他们的选票给汉道特：

合并成一大选区

组别	选票数	选举意愿（从最好到最差）	
A，D’	19	阿蒂拉	汉道特
B，C，D	23	汉道特	阿蒂拉

汉道特已得到 23 票，成为胜者。

这种反常结果也可能在相反的情况下，即当大选区划分成两个较小的选区时出现。不论合并成大选区或是划分成小选区，这种可能性“将使不公正地划分选区成为一种非常具有吸引力的选择，从而影响其选举结果”，多隆得出这样的结论。

而这决不是悖论的终结！布拉姆斯与菲什伯恩在一篇有趣的文章中[①]提醒人们注意黑尔选举制中两种扰乱人心的特点：不到场的悖论和挫折的大多数的悖论。在不到场的悖论中，对于排列在最后的一些候选人，增加的选票可以使该候选人成为一位当选者，而不是落选者。换句话说，一些把某候选人排列在最后的选民留在家里可能要比把该候选人填写在他们选票的最后好一些；在挫折的多数的悖论中，即使一些候选人可以在面对面角逐中击败其他每一位候选人，但却不能当选。（我极力主张那些渴望成为对策论专家的人们，去构思一些数字的例子，以便一一证明这些悖论；如果你未能成功，你可以随时请教布拉姆斯和菲什伯恩的可读性文章。）

挫折的多数的悖论不仅仅折磨着稀奇古怪的黑尔选举制，而且还折磨着许多普通的选举制，诸如简单多数选举制等。设想“自由派”先生（49%的优势），“温和派”先生（10%的优势）和“保守派”先生（41%的优势）之间进行三方竞选。现在考虑三派中每一位选民的第二选择。自由派选民当然喜欢“温和派”先生胜过“保守派”先生，因而在这些候选人之间的两方竞选中，“温和派”先生将当选。他获得选票的 59%（对“保守派”先生的 41%）；而保守派的选民们必定喜欢“温和派”先生胜过“自由派”先生。所以在这些候选人之间的两方角逐中，“温和派”先生可得 51%的选票（对“自由派”先生的 49%），也将当选。然而，在三方竞选中，“温和派”先生将落在最后。在一些预选中，如果没有候选人获得半数以上的多数票，那么要在两位得票最多的候选人中间进行最后的角逐。即使“温和派”先生在两方竞选中能够击败任何一个对手，但他也可能被阻止进入最后的角逐。

悖论还会更加深刻。假设在政治领域内，“自由派”先生是属于中间偏左的，而“保守派”先生只是中间略微偏右。那么，在“自由派”先生

[①] 见菲什伯恩和布拉姆斯的《选举投票的悖论》，数学杂志第 56 期（1983 年 9 月）：207—214 页。

和“保守派”先生中间进行最后竞选时，所有温和派选票都会投向“保守派”先生，使他因获得 51%的选票而当选。现在由于在选举意愿上有这样巧妙的联合，于是“保守派”先生要靠两票方可当选。“自由派”先生只靠一票就能当选，而“温和派”先生却具有在面对面竞争时击败任何一位对手的能力。所以说在你选择你的选举制时，也就选择了你的当选者。

布拉姆斯鼓吹一种选举制——认可选举制。它既可完全消除这里讨论的悖论，减低它发生的可能性，也可减少它的影响。这种认可选举以“一人多票”的原则取代由来已久的“一人一票”的原则。换句话说，虽然每位选民对每位候选人只能投一票，但是每位选民只要他喜欢就可以认可许多位候选人（即都投他们的票）。其概念就是，选民不必担心他的选票白白浪费在不受欢迎的候选人身上（比如说，在 1980 年的总统选举中的约翰·安德森），因为选民还可以再投另外他认可的候选人，不论他是谁。

在认可选举中，当选者将不是在简单多数选举中由于其对手分散了选票而获得胜利的候选人。认可选举制不太可能使多数派的希望受挫。而且当多数派还没有明确的选举意愿时（换句话说，当存在群体非可递性时，即当群体喜欢麦克唐纳胜过伯格王，喜欢伯格王胜过温迪，而喜欢温迪又胜过麦克唐纳时），认可选举制将就大多数人所赞同的意愿进行选择。我们可以看出，当罗纳德、克拉拉、赫布依靠 2 票来选择餐馆进餐时，那是多么有利于不诚实的投票，即为你的第二选择而不是你的第一选择投票。当有 3 位候选人时，认可选举制就可防止这种不诚实的投票：决不会出现有利于你投第二选择的票而不投第一选择的票这样的情况。此外，在认可选举制中，决不会出现留在家里并不去投票反而得利的情况，如同你在黑尔选举制中所做的那样，而且也不会在选区合并或分开时发生滑稽可笑的事情。

尽管认可选举制具有这些明显的优点，但显然没有被世界上任何公共论坛（除了少数专业学会外）所采用，只有在联合国安全理事会选举秘书长职位时采用过，其会员国可以投一人以上候选人的票。美国的纽约州和佛蒙特州都曾考虑采用认可选举制，但制定的议案已在州立法中被否决。对策论学家在影响公众政策方面所起的作用还是微不足道的，即使是在他提出一个建议，而该建议对社会的益处在数学上似乎是无懈可击的时候。

回答提出的问题

此处布拉姆斯提出的事例，可能有利于缩短你在黑尔选举制中的投票时间。现有 11 张选票和 4 位候选人竞选 1 席公职。

组别	选票数	选举意愿顺序（从最好到最差）
A	7	格拉夫博士　马尼福尔德博士　迪济特博士　波因特博士
B	6	马尼福尔德博士　格拉夫博士　迪济特博士　波因特博士
C	5	迪济特博士　马尼福尔德博士　格拉夫博士　波因特博士
D	3	波因特博士　迪济特博士　马尼福尔德博士　格拉夫博士

由于没有一位候选人获得 11 票，最低得票者波因特博士落选了，而他的支持者的 3 票都被转移给 C 组：

组别	选票数	选举意愿顺序（从最好到最差）
A	7	格拉夫博士　马尼福尔德博士　迪济特博士
B	6	马尼福尔德博士　格拉夫博士　迪济特博士

C、D　8　　迪济特博士　　马尼福尔德博士　　格拉夫博士

仍然没有一位候选人获得简单多数票，于是又有一位不受欢迎的候选人马尼福尔德博士被淘汰了。当他支持者的 6 票和 A 组的 7 票联合在一起时，格拉夫博士入选了，他获得 13 票。

D 组的 3 位选民不高兴，因为他们的最后选择竟是当选者。假设他们在选票上只标出第一选择的话，那么：

组别	选票数	选举意愿顺序（从最好到最差）
A	7	格拉夫博士　马尼福尔德博士　迪济特博士　波因特博士
B	6	马尼福尔德博士　格拉夫博士　迪济特博士　波因特博士
C	5	迪济特博士　马尼福尔德博士　格拉夫博士　波因特博士
D	3	波因特博士

同前面一样，最初没有一位候选人获得 11 票，于是波因特博士被淘汰了。然而这次他的 3 票没有被转移，因为他的支持者没有表明任何其他选择意愿。剩下 3 位候选人，迪济特博士现在成为最不受欢迎的候选人。当他的 5 票加入 B 组时，马尼福尔德博士就崭露头角成为当选者——一个更合 D 组选民胃口的结果。

第十三章　国会议员的数学游戏

1882 年，得克萨斯州议员诺加·米尔斯对数学进行了谴责，他的发言是人类最诚恳的演说之一。他说：“我认为数学是一门神圣的科学，它是启迪神灵的惟一科学，所说的都是正确的。我所受到的教育一直是：数学展示了真理，也知道在天文学、哲学、几何学和所有其他学科中，总有些问题需要推测，而数学如同《启示录》的声音一样，它开口时总是说：‘上帝是这样说的。’但是，这里有个新的数学体系表明，真理就是谬误。”

米尔斯所说的问题是共和国成立以来众议院一直面临的问题：每个州应该分配多少个代表？国会代表按比例分配的数学听起来像是采用简单的、人们拥护的一人一票的方法。但是，像直接选举方案一样，间接代表制却受着数学上悖论的严重困扰，从而遭到米尔斯议员的强烈抨击。直接选举方案的悖论是策略运筹学性质的，它牵涉到选举人合谋选举他们自己的候选人。国会代表分配的问题，只是每个州分配到的代表人数，而不是怎样选代表的问题。按比例分配属于应用数学领域，叫做社会选择理论。

为什么按比例分配是这样一个问题呢？美国宪法第一条第二款似乎提供了一个直接的答案：每个州派往众议院的代表人数应与本州人口成比例。问题是，虽然一个国会议员的忠心可分，而他的躯体却不可分；人就像便士或电荷或亚原子自旋状况一样，是量子化的。

假定你要在只有两个州的国家成立一个众议院：X 州有人口 11， Y 州有人口 23。每个州按其人口选派代表，最小的众议院会是怎样的呢？最小的众议院会有 34 个成员，如果成员少一些，则其中一个州（或两个州）会出现一个分数代表。换句话说，当 H（众议院的人数）少于 34 人，X 和 Y 就没有整数（分别为 X 州和 Y 州的代表人数）能符合等式 X＋Y＝H 和 X／Y＝11／23。为人口 34 而成立的一个 34 个成员的众议院，当然不是确切的间接代表制。

像我们有 50 个州这样大的国家，这些州的人口数量相互之间又没整倍数，问题就明显地复杂了。在一个特定规模的众议院，每个州的理想代表人数是按该州人口与总人口的比率乘众议院总成员数得出的。（因此，如果众议院有 235 个席位，在一个人口为 231，575，493 的国家里，人口为 2，559，253 的州有资格成为代表的理想数字为 2．597099 个：2，559，253／231，575，493×235。）既然这个理想数字可能是个分数，并且不允许代表出现四分之一这种数，那就需要有个更好的分配代表的方法了。

许多开国元勋，包括亚力山大·汉密尔顿、托马斯·杰佛逊和丹尼尔·韦伯斯特，曾提出他们各自的解决方法。财政部长汉密尔顿的方法最容易理解，他的方法于 1792 年经国会通过但紧接着被乔治·华盛顿否决——华盛顿在任 8 年中只行使过两次否决权，这是其中的第一次。按照汉密尔顿的方法，开始时先给每个州一个代表数，与其理想的代表的整数部分相等，舍弃其分数部分。换言之，如果佛蒙特州理想的代表人数为 3．62，它就有 3 个代表。在这个基础分配的代表人数上计算出代表总数，如果总数没有达到众议院要求的人数，就取那些舍弃了的最大分数值的州的代表，进众议院。

汉密尔顿的按比例分配方法很容易说明。下表显示 5 个州的人口和在一个有 26 个席位的众议院中，每个州所能获得的代表人数。

州	人 口	在众议院26个席位中的理想数	汉密尔顿第一轮分配数	汉密尔顿第二轮分配数
A	9，061	9．061	9	9
B	7，179	7．179	7	7
C	5，259	5．259	5	5
D	3，319	3．319	3	4
E	1，182	1．182	1	1
合计	26，000	26	25	26

用汉密尔顿的方法，在一个26席位的众议院，A、B、C、D和E开始时分别获得以下代表数：9、7、5、3和1，但只占26个席位中的25个席位，D州有最高分数（0.319），因而它可增加一个代表，共4个代表。

汉密尔顿的方法至少符合一个平等的原则：它给每一个州能够就近上下浮动的理想的代表数。换句话说，如果D州的理想代表数为3．319，他的方法总会给D州3个或4个代表，永远不会给2或5个代表。符合这个自然准则的方法据说能满足定额。许多别的方法不能满足定额，这定额似乎是你所希望的一种被认为是公平的按比例分配方法的最低的定额。

可是，汉密尔顿的方法违背另一个更难理解的公平准则。在我们5个州的例子里，设想众议院的规模由26个席位增加到27个：

州	人口	26席位的众议院		27席位的众议院	
		理想数	汉密尔顿分配数	理想数	汉密尔顿分配数
A	9，061	9．061	9	9．410	9
B	7，179	7．179	7	7．455	8
C	5，259	5．259	5	5．461	6
D	3，319	3．319	4	3．447	3
E	1，182	1．182	1	1．227	1
合计	26，000	26	26	27	27

在27席位的众议院，A、B、C、D和E各州分别获得9、8、6、3和1个代表数。奇怪的是，即使众议院的规模增加了，D 州却少了一个代表。这是汉密尔顿方法的一个严重缺点。可以这样想：虽然总人口和D州的人口都一点儿没有变，众议院人数增加了，D州的代表人数现在反而较少了。数学上一种令人痛苦的扭曲，叫做亚拉巴马悖论，使D州处于双重的不利境地（因为这种悖论是头一次在牵涉到亚拉巴马州的计算中发觉的）。上述5个州的例子是迈克尔·巴林斯基和H．佩顿·扬在一篇关于按比例分配的文章中虚构出来的。[①]巴林斯基和扬花了9年时间调查按比例分配问题中数学的悖论，研究按比例分配提案的政治辩论历史。我的大部分叙述是

[①] 巴林斯基和扬，“按比例分配的定额法”，美国数学月刊82（1975年8—9月）：701—730。

以他们的著作为基础的。

这个亚拉巴马矛盾——在一个更大的众议院一个州会失去一个代表——并不是华盛顿否决汉密尔顿提案的原因。确实没有证据能证明开国元勋们知道这种数学的特殊性。华盛顿在否决汉密尔顿提案时，是被国务卿托马斯·杰佛逊的论点所左右。杰佛逊告诫说：“不损害宪法是最基本的问题，他们耍弄的按比例分配数字的花招，是很危险的。”杰佛逊自己提出了一个方案，华盛顿采纳了，尽管其方案有违反定额的严重缺点。

在巴林斯基和扬的 5 个州例子中，因总人口（26，000）除以众议院规模（26）是 1，000，每一个众议院成员理想地代表着 1，000 个人。汉密尔顿的方法是把每州的人口除以 1，000，然后除了有最高分数的州外，其余州的分数全部舍弃，最高分数按需要入到整数，以凑满众议院人数。杰佛逊的方法不用 1，000 做除数（也叫最大除数方法），要求用最大的除数，以产生每个州的代表数，不变动这些数或舍弃其分数，以达到众议院的规模。换句话说，这些数绝不需要升值。在 5 个州的例子中，906．1 成为最大的除数，由此可得出以下结果：

州	人口	汉密尔顿 26 席位的最大除数 1，000	汉密尔顿分配数	杰佛逊 26 席位的最大除数 906．1	杰佛逊分配数
A	9，061	9．061	9	10．000	10
B	7，179	7．179	7	7．923	7
C	5，259	5．259	5	5．804	5
D	3，319	3．319	4	3．663	3
E	1，182	1．182	1	1．304	1
合计	26，000		26		26

如上表所示，杰佛逊和汉密尔顿的方法产生不同的结果。用杰佛逊的方法，A 州——人口最多的州——多得一个代表（D 州失去一个代表）。杰佛逊的方法帮助了 A 州并非侥幸，从数学上可以表明其方法对大州有利。他那高傲的演讲从未提到过数学的这种偏袒性，虽然，他这个精明的科学家无疑是完全意识到这一点的。但他赞成这种偏袒性，因为他和华盛顿一样，都是来自最大的州，弗吉尼亚（人口 630，558）。确实，1792 年第一次实行按比例分配众议院成员时，杰佛逊的方法（与汉密尔顿的方法相反）保证了弗吉尼亚州增加一个代表，从而损害了最小的特拉华州（人口 55，538）。

从 1792 年至 1841 年，杰佛逊的方法被采用了大约半个世纪左右。（我说的“左右”是因为有时众议院的规模没有预先固定，它受到政治利益的调整，使各州不会在一个新的按比例分配制度下失去代表。）丹尼尔·韦伯斯特意识到杰佛逊的方法没有给他的家乡新英格兰各州以充分的代表名额之后，说服国会采用一个新的按比例分配方案。同杰佛逊的方法一样，韦伯斯特的方法（也叫最大分数法）是以选择最大除数为基础的，但是得出的数字不是自动地舍弃分数，而是按照四舍五入的标准常规计算的。对 5 个州来说，最大除数是 957．2，这样 B 州的情况就比其他两个方法得出

的结果更好。

州	人口	韦伯斯特 26 席位的除数为 957.2	韦伯斯特分配数	汉密尔顿分配数	杰佛逊分配数
A	9，061	9．466	9	9	10
B	7，179	7．500	8	77	
A	5，259	5．494	5	5	5
A	3，319	3．467	3	4	3
A	1，182	1．235	1	1	1
合计	26，000		26	26	26

每走一步总有些国会议员反对增加众议院人数，但他们的呼吁无论怎样有说服力，其他人都充耳不闻。奇怪的是，对于一个较大规模的众议院来说，它的笨拙不便要比它的非法行为多。纽约州代表塞缪尔·考克斯说的话很有代表性。他说：“一个人不是因为身材高大而伟大。肥胖不是健康或严厉。喘息的肥胖病不一定是头脑机警的状态。成年人不需要大量的猪油和脂肪。”

没有按照汉密尔顿的方法做曾引起不小的后果：塞缪尔·蒂尔登 1876 年丧失了总统职位。在选举团里，每个州的选举人数与它的众议员和参议员人数相等。在那次著名的选举中，蒂尔登比卢瑟福·B．哈依斯多获得 264，292 张民众选票，但哈依斯却因比他多获一张选举团的选票而使他落选。巴林斯基和扬论证，如果按照法律上要求的汉密尔顿的方法做，蒂尔登就会获胜，因为支持他的一个州应该增加一个选举团成员，而支持哈依斯的州就少了一票。

1881 年当人口调查局的科长根据 1880 年人口统计，在调查历届众议院从 275 席位到 350 席位规模的按比例分配情况中，终于找出了亚拉巴马悖论。他写信告诉一位议员：“我进行这些计算的时候，我遇到所谓的‘亚拉巴马悖论’问题，我发现在议员总数 299 位中，亚拉巴马州分配到 8 个议员席位，但总数是 300 时，它只获得 7 个席位。”尽管如此，其后 20 年，亚拉巴马悖论的缺陷以在理论胜于在实践的方式继续存在。

接着在 1901 年众议院席位以 1900 年的人口统计为基础重新按比例分配时，亚拉巴马悖论成为一个实际问题，引起了激烈的辩论。大多数议员通过了一项议案，确定众议院规模为 357 个席位，科罗拉多州获两个席位。科罗拉多州议员约翰·C．贝尔谴责“由数学家推出的并称之为悖论的暴行”。他注意到，在其他每个拥有 350 至 400 席位的众议院，他的州会获得 3 个而不是 2 个议员席位。在 357 席位的众议院，缅因州也受到亚拉巴马悖论的损害，它的一位议员说：“这就像是数学和科学联合起来，把缅因州当作板羽球耍……当数学抓住缅因州的时候，愿上帝保佑她！”

在以后几十年中，杰出的数学家们向众议院进行标榜，并提供了复杂的公式，以避免亚拉巴马悖论，他们的公式对大多数政客来说，是莫明其妙的。其中一个公式在 1941 年弗兰克林·罗斯福签署“规定用等比例方法在若干州中按比例分配国会议员代表的法令”时被采纳了。

等比例法早在 20 年前由哈佛大学数学家爱德华·享廷顿提出。他认为，假设在许多州人口不同的情况下，把授于任何两个州的代表名额做比较，其中一个州的名额难免会短少，短多少可以计算。如果从境况较好的州转移一个代表到境况较差的州，能减少它们相对的短少数，就应该转移。例如，拿弗吉尼亚和马萨诸塞两州做比较，如发现弗吉尼亚处境较差，短少 3 个单位，从马萨诸塞转移一个代表到弗吉尼亚，局面就会转变为马萨诸塞少了两个单位，这个转移应该做，因为相对的短少数——2 个单位对 3 个单位来说——是减少了。倘若不是这种情况，而是转移使马萨诸塞州少了 4 个单位，那就不应转移，维持现状还公正一些。采用这种按比例分配代表的方式的用意是使相对的短少数减到最低程度。在那些没有成双做比较的州需要转移一个代表时，这种情况将会发生。

将相对的短少数降到最低，这个主意是有吸引力的，但如何衡量短少数呢？在等比例法中，计算短少数是先得出一个州的众议员选区平均数和另一个州的众议员选区平均数之间的差额，然后将该差额表示为较小选区规模的分数。在 5 个州的例子中，等比例法又产生另一种代表分配情况，有利于 C 州：

州	人口	平均选区规模	26 个席位按等比例分配
A	9，061	1，006．78	9
B	7．179	1，025．57	7
C	5，259	876．50	6
D	3，319	1，106．23	3
E	1，182	1，182．00	1
合计	26，000		26

根据上述短少数的计算情况，D 州短少了（1106.23—876．50）／876．50，或 0．2621。从 D 州转移一个代表到 C 州会把 C 州的平均选区规模改为 1，051．80，把 D 州改为 829．75。这种分配不大公正，因为短少数的相对量增加了，C 州短少了（1051，80—829.75）／829.75，或 0.2676。如果你玩弄上表中的数字，你会发现，再没有其他分配代表的方法比用这个短少数计算的方法更公正了。

可是，这个计算短少数的方法，不能先验地断定它是公正的。你可以只计算出两个规模之间的差数，而不必用分数表示出来。或者你可以计算出每个州每位居民所等于的代表的分数，然后把逐个州的分数之差减到最低。也可能还有其他同样自称公正的计算方法。

用类推法就可以理解短少的定义问题。如果我告诉你，鲍勃的年收入超过杰克 1 万美元，用这种计算法——收入的绝对差额——杰克少收入 1 万美元，但这并不能告诉你你想知道的有关他们的生活水平的一切事情。杰克可能每年只挣 1 万美元，在这种情况下，鲍勃比他多挣 100%。可是，如果杰克每年能挣到 100 万美元，在这种情况下，鲍勃就只比他多挣 1% 了。倘若申报的收入不是绝对按美元来报，而是按百分比报，则你需要的其他判断他们生活标准的信息就会有所删减。例如，假定你知道鲍勃比杰

克多挣 100%，这并没告诉你鲍勃在另外用现金买一幢 10 万美元的房子的情况下，是否能生活得同杰克一样好。如果鲍勃挣 20 万美元（杰克挣 10 万美元），他就能省出多余的现金。但是，如果他只挣 1 万美元（杰克挣 5，000 美元），他只能买一台家用计算机，买不起房子了。这说明没有一种计算收入差别的方法——不管是以绝对美元、百分比差额、或其他什么方法——可以先验地自称是最好的方法。计算各州派往众议院代表团的相对的代表短少程度，也同样如此。

正如巴林斯基和扬在《美国数学月刊》的一文中提到的那样，罗斯福和国会都不知道等比例法也违反定额。再者，它倾向于照顾较小的州（从 5 个州的例子中你可以看出这些缺点）。也许你开始认识到，除了由于无法分开一个国会议员所产生的明显不公正这一因素之外，每种按比例分配的制度都受到悖论的干扰。在巴林斯基和扬 1982 年出版的《公正的代表制：达到一人一票的理想》一书中，他们提出了一项数学论证：既能满足定额又能避免亚拉巴马悖论的按比例分配法是不存在的。

在社会选择理论的最佳方案中（应用数学的一门分支，提出个人的选择机会应该如何结合起来以形成社会的选择），巴林斯基和扬没有停留在只识别各种悖论上，而是继续研究它们是如何反复出现的。现实世界毕竟需要一个解决办法——一个又一个的分配代表的方案。显然，一种几乎可以一劳永逸地摆脱悖论的方法比令他们摸不着头脑的方法更可取。巴林斯基和扬能表明，在任意人口的资料的基础上，韦伯斯特的方法不论是对于大州还是小州都有利，而且比起其他不受亚拉巴马悖论的影响按比例分配的方法来更不违反定额。

巴林斯基和扬的强有力的分析会不会在国会掀起一个回到韦伯斯特的方法的运动呢？如果今天用这个方法（而不是等比例法），其惟一的差别就在于新墨西哥州会丢失一个席位，让给印第安纳州。在众议院人口调查委员会里，以巴林斯基和扬的分析观点为武器的印第安纳州代表团提出了恢复韦伯斯特方法的提案，可是没有引起多少兴趣（除了新墨西哥州代表团的发火之外），提案就在委员会里悄悄逝去了。啊，社会选择理论家真是难逃孤独的命运！