数说

2017.4

华中科技大学数学与统计学院

数学与统计学院科学与技术学会

《数说》期刊部

本期目录

AI 已杀入密码界，密码攻坚不再是人类的专利！

秦曾昌、 small_TAO

密码，不只是你打开手机时输入的那几个数字，它还关系到你银行里的存款、电脑里的裸照，甚至，世界和平。

电影《模仿游戏》（The Imitation Game）讲述的就是关于著名密码系统恩尼格玛（Enigma）的故事。这里不讨论电影中情节的真实性，但二战时纳粹德国正是利用了这套密码系统，隐秘而高效地传递着军事情报。恩尼格玛的最终破译成功地扭转了战局。人们普遍认为，它的破译使盟军在西欧的胜利提早了两年。

电影《模仿游戏》的海报。图片来源：wikipedia

一直以来，设计和破解密码都是人类的专利。然而随着密码学理论的提升与计算机能力的增强，现代的密码变得越来越复杂，人们开始寻求让机器替代人类的办法。不过这就涉及到一个问题：用 0 和 1 思考的“机器大脑”能学会对信息进行加密吗？

在谷歌大脑（Google Brain）的最新的研究成果《让对抗神经网络学习保护通信》（*Learningto Protect Communications with Adversarial Neural Cryptography*）中，人们就试图教会机器加密与解密信息[1]。这次，思考密码术的不再是人类的大脑，而是“神经网络”与“生成对抗网络”（Generative Adversarial Network）结合而成的机器之“脑”。

神经网络，生成对抗网络与密码术

神经网络

神经网络全称人工神经网络，是一种模仿动物神经系统结构和功能的计算模型。在经历过历史中的几度沉浮后，如今它已成为科研界与工业界的新宠，在人工智能及相关领域中炙手可热。

神经网络由大量的“感知机”（Perceptron）相互连接构成。感知机类似于生物神经系统中的神经元，是神经网络中最基本的单元。

神经网络并非生来就具备强大的功能，它也需要训练才能掌握技能。比如我们希望神经网络通过西瓜的外形判断瓜的甜度，一开始神经网络并不懂如何去判断，这时就需要分别把西瓜的外形和对应的甜度分别输入神经网络，以训练它去学习两者之间的对应关系。训练神经网络的过程实际上就是通过学习数据来调整每一个感知机参数的过程。神经网络读取数据样本后，感知机们会先根据现有模型参数进行计算，然后把输出的值与真实值进行比较，再将两者的差距反馈回去，以调整参数。经过反复多次“计算－比对－反馈－调整”的循环后，神经网络就能够准确地判断瓜甜还是不甜了。

生成对抗网络

很多时候训练数据的真实结果信息难以获得——比如不能把每个瓜切开尝尝。生成对抗网络利用模块间的对抗，巧妙地避开了这个问题。

生成对抗网络中主要有两个模块：负责生成的模块 G 和负责判别的模块 D。我们用模仿画作的例子来说明

两个模块的作用。G 是一位初出茅庐的画家，想要通过模仿名画的来提升自身能力。在每次模仿名画之后，G 画家会将自己的赝品与真品一同送给鉴定师 D。D 的主要任务便是鉴定送来的画哪一幅是真品哪一幅是赝品。刚开始，G 画家的水平一般，D 鉴定师能够很轻松的鉴定出真伪。随着 G 画家的模仿水平的提高，D 鉴定师无法分辨真伪。这个时候，我们便可以说 G 画家的模仿水平相当的优秀了。这也是我们想要的结果，模仿能力卓绝的生成模块 G。

人类的密码术

说完网络，再说说密码术。在密码术中，能够直接代表原文含义的信息称为明文；经过加密处理之后隐藏原文含义的信息称为密文。加密与解密便是明文与密文相互转换的过程，而密钥是用来加密与解密的工具。密钥好比一本双语字典，你既可以用它把明文翻译成密文，也可以通过它查找密文所对应的明文是什么。在信息保密过程中，密钥的安全格外重要。因为找到秘钥就是找到了加密和解密的方法，密码也就迎刃而解。早期的密码设计有替换法与位移法。替换法

就是有规律的使用一组字母来代替原有字母，例如每个字母用上一个字母取代，“abc”替换为“zab”；移位法就是将字母顺序重新排列，例如“Key”变成“yeK”。这样的密码可以分别使用穷举法和统计法进行破解。后来密码的书写发生了手写到机器书写的转变，这也使得密码的编写变得千变万化。

不过，这是人类的密码术。作为机器之脑的神经网络也能“想”出类似的技术对信息进行加密吗？

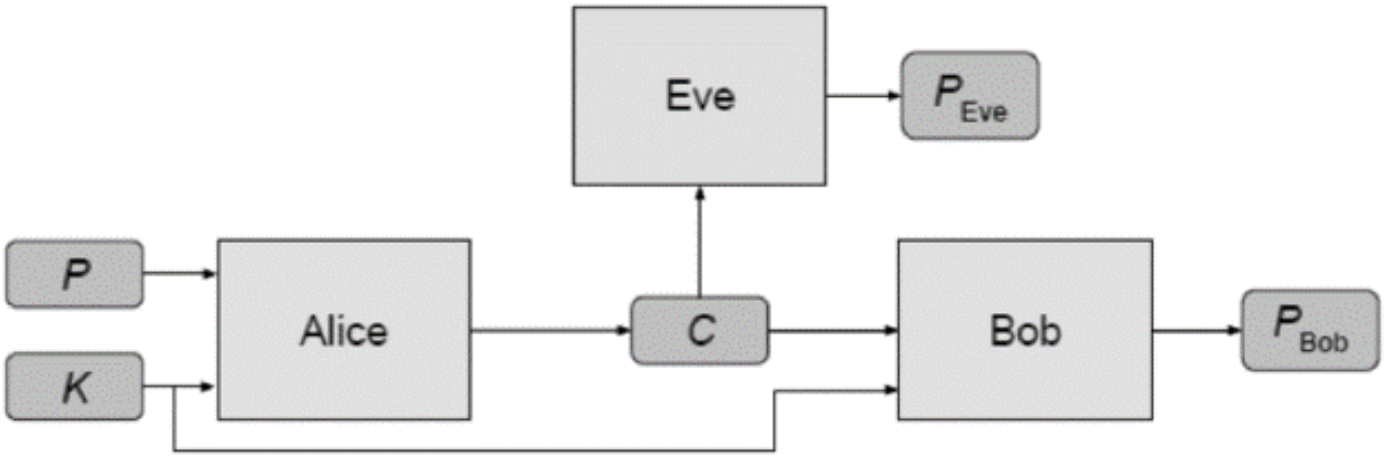
机器能学会加密信息吗？

回到谷歌大脑最新的研究上。研究者向神经网络 A 中投入明文和密钥数据，它的计算结果会作为密文，与密钥一起交给另一个神经网络 B，并由 B 进行解密。而 A、B 组成的生成对抗网络，则会试图在对抗中使解密出的数据趋近原始明文。当然，整个过程中神经网络并不懂“明文”“密文”的概念，因为研究人员丝毫没有向它们透露人类密码术的相关知识。它们只知道自己收到了数据，又要输出数据。研究者通过这

样的方式，探究神经网络能否自己“思考”出机器的密码术来实现对信息加密、解密的功能。

实际操作中，研究者设计了一种通用的保密情况，叫做对称加密模型。对称加密是指沟通双方有公共的密钥，而窃听者没有。研究者在该模型中加入了三个独立的神经网络模块，分别取名为 Alice、Bob 和 Eve。这三个神经网络模块共同构成了对抗神经网络的主体。

我们可以把它们想象成是三个人：Alice 想和 Bob 进行秘密沟通，而 Eve 想要窃取他们的通信。为了防止秘密被 Eve 知道，Alice 制定了密钥并共享给 Bob。通信的时候，Alice 首先通过密钥将信息进行加密，然后将加密后的信息发送出去。这时 Bob 和 Eve 都能接收到信息，不同的是，Bob 可以通过共享的密钥对信息解密，而 Eve 需要自己想办法猜测信息的内容。

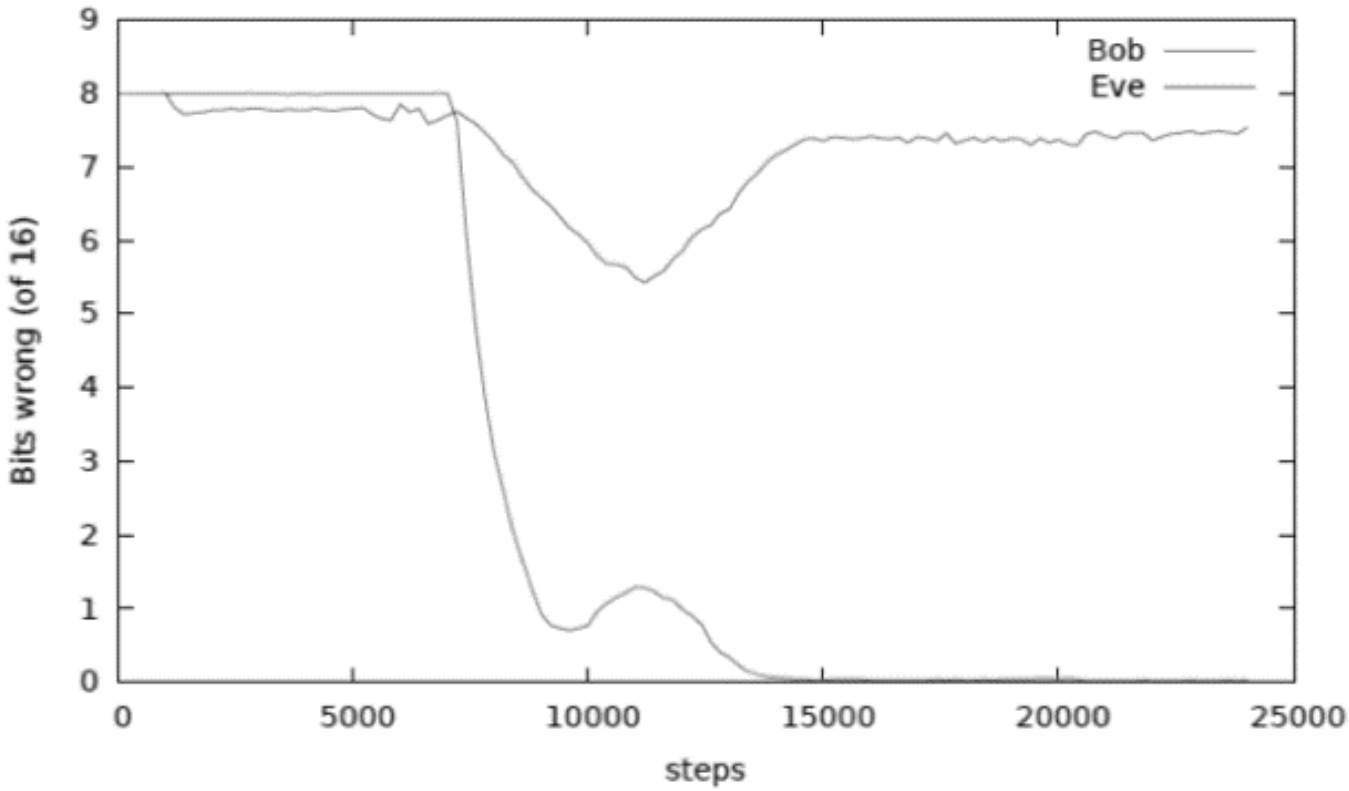


方框分别代表着三个独立的神经网络，P 是明文，K 是密钥，C 是密文，PBob 和 PEve 分别是 Bob 与 Eve 对密文的预测结果。 参考文献：arXiv:1610.06918

如图所示，K 是 Alice 和 Bob 共享的密钥，P 便是要进行加密的信息。C 是 Alice 转换出的密文，它会被 Eve 和 Bob 收到并进行解密，两人各自解密得到的结果则为 PBob 和 PEve。研究者通过统计 PBob 和 PEve 中与 P 相同的数据有几位来计算解密结果的准确性。

当然，我们希望 PBob 与 P 越接近越好，而 PEve 与 P 值差距越大越好。这表示通过 Bob 解密的信息是准确的，而窃听者难以通过 Eve 得到被加密的信息。

基于以上这些设置，研究者开始对这个加密模型训练。每一次的训练过程中，神经网络 Alice 会接收到 4096 套 K 和 P 作为训练样本。K、P 都是 16 位二进制数据，Bob 和 Eve 输出的解密文件也是 16 位二进制数据。通过统计每次训练后 Bob 和 Eve 解密结果的与明文 P 的对应数位的数字，研究人员得到了如下图的结果：



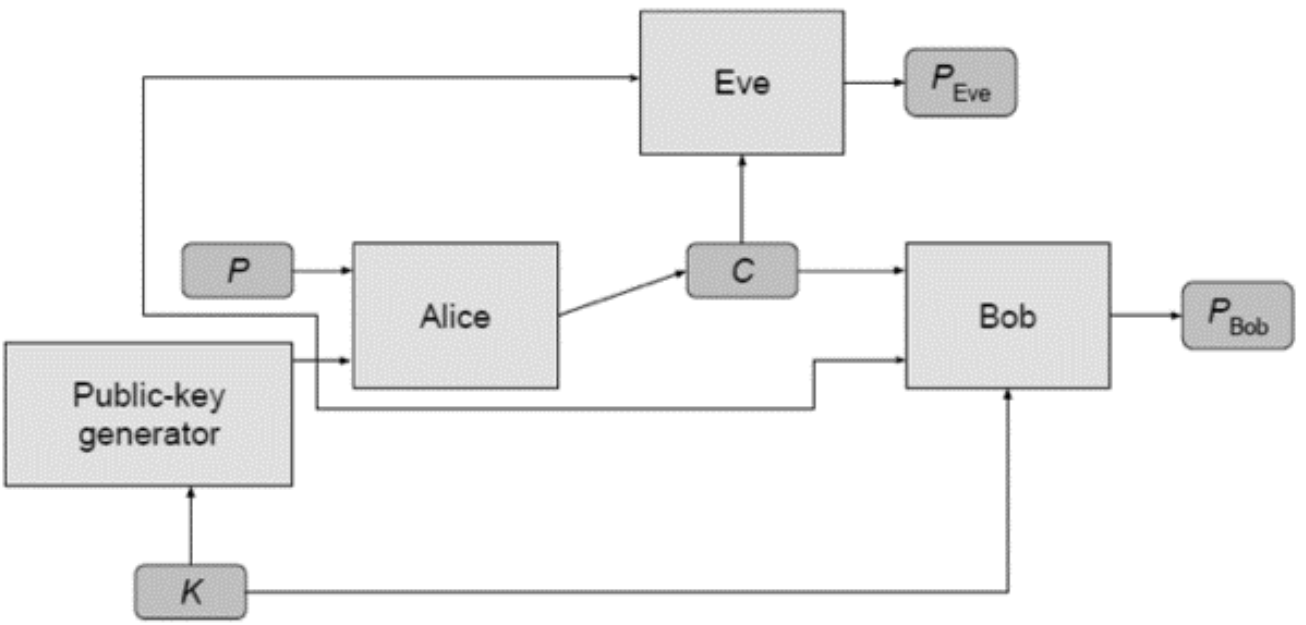
Bob 和 Eve 解密信息的错误率随实验次数的变化曲线。横轴是训练次数，纵轴是错误的字节数。红线与绿线分别代表着 Bob 与 Eve 错误字节数的变化情况。

在进行到 10000 次左右的时候，Bob 迷之反击了 Eve。参考文献：arXiv:1610.06918

训练刚开始的时候，Bob 和 Eve 的错误位数都是 8，对于一个 16 位的二进制文本来说，随便生成的 16 位数字在概率上错误位数就是 8——这时 Bob 和 Eve 都还没有具备解密的能力。伴随的神经网络之间的对抗，每个神经网络不断的调整其中感知机参数的数值，Alice 和 Bob 也逐渐获得了极强的加密与解密能力。当迭代进行到 7000 次的时候，Bob 预测明文的错误率大幅度的下滑。在 15000 次训练之后，Bob 预测的错误位数已经几乎为 0，而此时 Eve 的错误位数为仍徘徊在 8 左右。也就是说 Eve 的破解密码的能力基本上仍然等于瞎猜，这时 Alice 发出的信息非常安全。

经过这样的训练后，研究人员得到了一个具有极强加密能力的神经网络 Alice。虽然研究人员并没有教给 Alice 任何密码术的知识，但 Alice 已经在对抗中习得了保密信息的技巧。

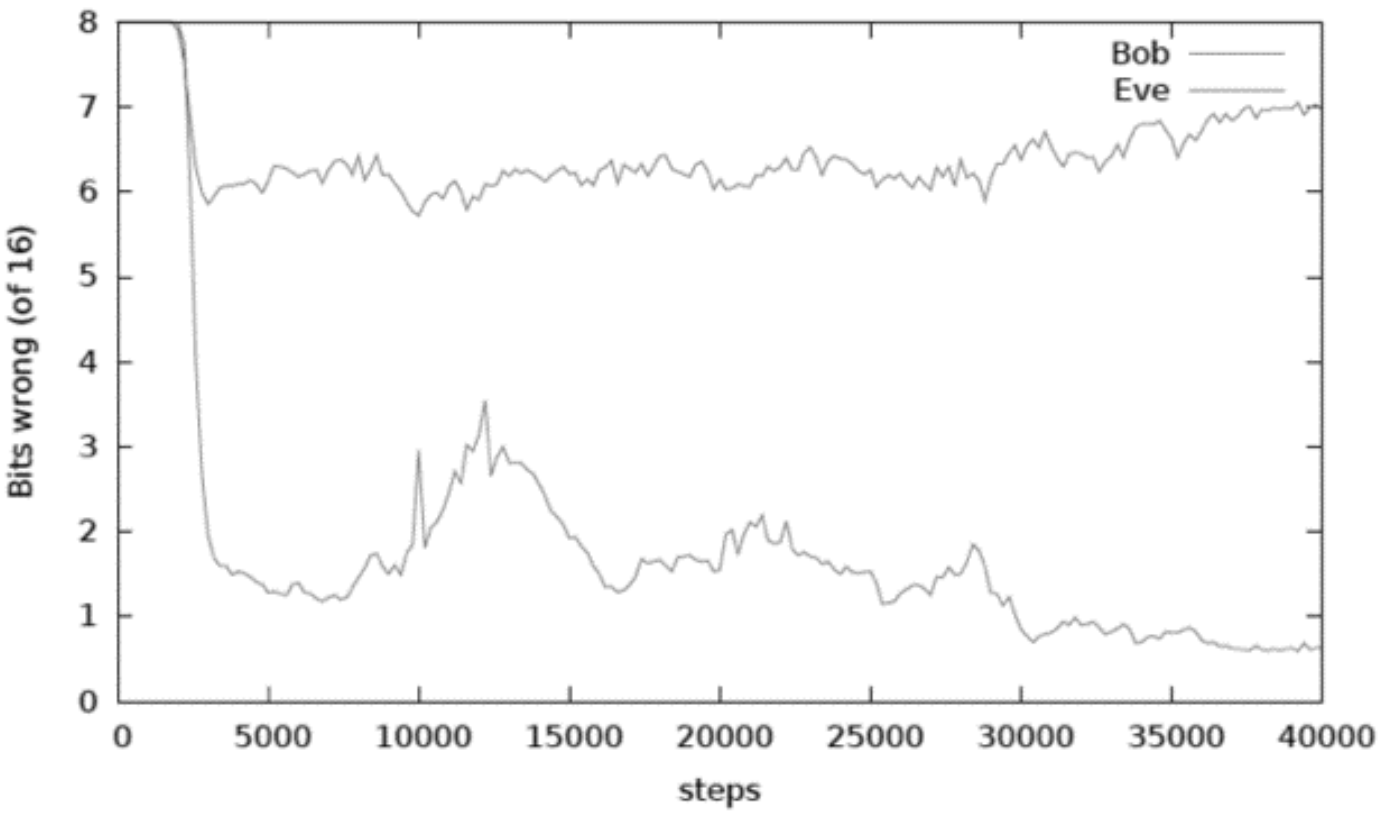
在研究了对称加密模型之后，研究者们还对非对称的加密模型进行了研究。与对称加密模型不同的是，这一次只有 Bob 拥有密钥 K，Alice 和 Eve 拥有由 K 生成的公钥。公钥是由密钥按照一定规则生成的，它包含了密钥的部分信息。



与之前的研究相比，该结构中多了公钥，Alice、Bob 与 Eve 都能接收到该公钥。参考文献：
arXiv:1610.06918

经过同样的训练后，研究者们得到了非对称加密模型的解密准确率。这次的保密效果没有预想中的好，测

试结果也比对称加密模型更难解读。在绝大多数的测试中，Eve 的错误字节都在 8 以下，甚至与 Bob 的错误率相当。也就是说在非对称加密模型中，Eve 几乎总能窃取到 Alice 和 Bob 的秘密信息。下图展示的是一个保密效果较好（也就是 Eve 错误率较高）的测试结果，图中 Eve 的错误字节数也下降到了 7：



Bob 和 Eve 解密信息的错误率随实验次数的变化曲线(非对称)，即使在保密效果较好的情况下，Eve 仍能获取少量信息。参考文献：arXiv:1610.06918

这个结果说明，将对称模型改为非对称加密模型对于对抗神经网络的训练结果有着很大的影响。对于这样的变化，研究员们计划通过两种途径来增强在非对称模型下 Alice 的保密效果，分别是使用新的神经网络或者是新颖的训练方式。但进一步的研究将会如何进行，我们还要等待谷歌大脑的新论文。

除了更换保密模型，研究员还将对称模型中明文和密钥的数据位数由 16 位变成 32 位以及 64 位。位数变化后测试的结果与原来的结果是相同的，即 Alice 发出的信息依然能够被很好的保护起来。这就说明该对抗神经网络能够加密更多的信息。如果扩展到 128 位、256 位，甚至成千上万位呢？如果结果依然相同，那么 Alice 的加密能力就有希望用于海量数据的加密与保护。

在这里我们不禁要问，在对称模型下，只用“0”和“1”思考的神经网络为何能够表现的如此优秀。

遗憾的是我现在无法给出答案。目前所有这方面的研究中对此并有没有很明确地解释。可以说神经网络对

于科学家们来讲依旧是一种难解释的“黑箱模型”。对于现在的神经网络来说，尚缺乏一套完整系统的理论指导。在神经网络研究快速发展起来之前，我们还需要更多像谷歌大脑这样的探索。

为什么要让机器学习数据加密？

你是否还记得阿尔法围棋（AlphaGo）和它的升级版“大师”（Master）在围棋界搅起的血雨腥风？我们暂且不谈论阿尔法围棋的框架结构，只是简单地说说它对我们的影响。阿尔法围棋在对弈的过程中会落下与我们固有思想不同的棋子，这种机器的“思维”在一定程度上会给我们提供不一样的思考方式，帮助我们更好地探究围棋的技巧。

谷歌大脑的这次新颖且大胆的研究则是一次密码学中的尝试，期待着机器的思维能够为传统的信息加密技术提供新颖的想法。在训练神经网络的过程中，研究人员并没有将密码学相关的算法放进模型中，而是通过神经网络之间的对抗，让 Alice 自己获得了高超的加密能力。当然这并不是说我们已经能抛开密码学，

转而依赖神经网络的自身学习能力了。考虑到神经网络的安全性与稳定性，Alice 的“密码术”还不能立刻用于生活中的信息加密。但是另一方面，一旦我们能够稳定的使用神经网络对数据进行加密且确保加密内容难以被破解，便可以将其利用在日常的信息加密中，甚至用于国家安全信息的保护。

也许，机器密码术的时代已经不远了。

作者介绍：

秦曾昌　英国布里斯托大学（University of Bristol）计算机系硕士，布里斯托大学工程数学系的人工智能博士。

small_TAO2016 北航研究生在读

超级建模师

数学建模感想

Eric Huang

纪念逝去的大学数学建模：两次校赛，两次国赛，两次美赛，一次电工杯。从大一下学期组队到现在，大三下学期，时间飞逝，我的大学建模生涯也告一段落。感谢建模路上帮助过我的学长和学姐们，滴水之恩当涌泉相报，写下这篇感想，希望可以给学弟学妹们一丝启发，也就完成我的想法了。拙劣的文笔，也不知道写些啥，按顺序随便写写吧。

我是怎么选择建模的：

大一上，第一次听到数学建模其实是大一上学期，not 大一下学期。某次浏览网页偶然发现的，源于从小对数学，哲学以及历史的崇敬吧（虽然大学没敢选择其中任何一个专业，尤其是数学和哲学，怕太难了，学不好），我就坚定了学习数学建模的想法。通过翻阅学校发的学生手册还是神马的资料，发现我们学校有数学

建模竞赛的。鉴于大一上啥数学知识都没有，也就没开始准备，把侧重点放在找队友上。

一次打乒乓球，认识了两位信电帅哥，以后也会一起打球。其中一位（M）很有学霸潜质，后来期末考试后，我打听了他的高数成绩，果然的杠杠滴，就试探性的问了下，要不要一起参加建模，嗯，成功！

第二位队友是在大一上学期认识的（向她请教了很多关于转专业的事情），但是是第二学期找她组队的。老样子，打听成绩，一打听吓一跳，是英语超好，微积分接近满分的女生 F（鄙人第二学期转入了她的学院）。果断发送邀请，是否愿意一起组队，嗯，成功。

关于找队友：在信息不对称的情况下，优先考虑三人的专业搭配，比如或信电的小伙伴负责编程和理工科题建模，经济金融统计负责论文和统计建模，数学计算专业的全方位建模以及帮忙论文，个人感觉这样子比较好。由于建模粗略地可以分为建模，编程，论文，三块，整体上是一人负责一块的，但是绝对不能走极端，每个人就单单的负责一块，这样子的组合缺乏沟通和互动。应该要在培训中磨合，结合每个人的个人特点。主要负责哪几块，辅助哪几块。

接下来就到了第一次校赛了：第一次还是挺激动的，

因为之前问了几个学长学姐说，建模都是要通宵的，于是我们也做好了通宵的准备。第一次拿到的题目是关于一个单位不同工作部门不同饮食习惯的人，健康水平的关系。后来回顾过来，这其实是一个比较简单的统计分析题。但是想当年可没有这等觉悟，做题全靠office，对着题目想半天也不知道该怎么做。做的过程很痛苦，但是也很兴奋，校赛三等奖的结果证明了光有一股热情是不行的，需要恶补大量知识。

推荐新手入门书目：

数学模型（姜启源、谢金星），

数学建模方法与分析.（新西兰Mark.M. Meerschaert）.

第一本是姜老先生写的，很适合新手，在内容编排上也是国产风格，按模型知识点分类，一块一块讲，面面俱到。第二本是新西兰的，我是大二的时候看这本书的，只看了前面一部分。发现这本书挺适合新手，它是典型的外国教材风格，从一个模型例子开始，娓娓道来，跟你讲述数学建模的方方面面，其中反复强调的一个数学建模五步法，后来细细体会起来的确很有道理，看完大部分这本书的内容，就可以体会并应用这个方法了。

（第一次校赛，就是因为五步法的第一步，都没有做到）。对了，还有老丁推荐的一本，美利坚合众国数学建模竞赛委员会主席 Giordano 写的 A first course in mathematic modeling，有姜启源等翻译的中文版，but 我没能在图书馆借到，所以没看过，大家有机会可以看看。

怎么建模

第一次国赛前的放假开始学校培训，我提前借了一大堆书，把卡都借满了。第一次国赛前的那次培训，对我而言，这段时期是收获最大的时期，比其他任何时间段都来得大。

这段时间内，我们三个人都很辛苦。白天培训要学习很多知识，完了只能休息半天，然后开始比赛，周而复始。 之前我的打算是，白天上课学习，晚上回去复习当天的内容，再看些其他东西。But 我太高估自己了，晚上基本是玩玩三国杀之类的小游戏放松，然后第二天再去上课。嗯，心态放好，身体最重要。^_^

通过这几次培训，基本上队伍形成了 F 专业写论文，我和 M 负责建模和编程。其中我偏重建模和全队调度。

大家在培训的时候，要慢慢养成五步建模法：

五步法说明:

第一步:提出问题.

大家可能会想,题目不是已经给出问题了吗? 是的,但是这里的提出问题是指:用数学语言去表达。首先,题目一定要通读若干遍,“看不懂,读题目;看不懂,读题目”,如此反复循环的同时查阅相关资料。这通常需要大量的工作,而且要根据题目的特点做一些假设。

看的差不多了,就开始用数学形式提出问题,当然,在这之前,先引用或者定义一些专业术语。 接下来进行符号说明,统一符号(这点很重要,三个人之间便于沟通,论文便于展现),并列出整个问题涉及的变量,包括恰当的单位,列出我们已知或者作出的假设(用数学语言描述,比如等式,不等式)。做完这些准备工作后,就开始正式提出问题啦。用明确的数学语言写出这个问题的表达式,加上之前的准备工作,就构成了完整的问题。

这部分的内容反映到论文结构上,相当于前言,问题提出,模型建立部分。注意,刚开始建立的模型很挫没关系,我们随时可以返回来进行修改的。

第二步:选择建模方法.

在有了用数学语言表述的问题后，我们需要选择一个或者多个数学方法来获得解。许多问题，尤其是运筹优化，微分方程的题目，一般都可以表述成一个已有有效的标准求解形式。这里可以通过查阅相关领域的文献，获得具体的方法。为什么不是查阅教材呢？基本上教材讲的都是基础的，针对特定问题的，教材上一般找不到现成的方法，但是教材依然是很重要的基础工具，有时候想不出思路，教材（比如姜启源那本）翻来翻去，会产生灵感，可以用什么模型。

第三步:推导模型的公式.

我们要把第二步的方法实现出来，也就是论文的模型建立部分。我们要对建立的问题进行变形，推导，转化为可以运行标准方法解答的形式。这部分通常是借鉴参考文献的过程，做一些修改，以适应本题的情况。

第四步:求解模型.

这里是编程的队友登场的时刻了。

统计模型：SPSS,Eviews，Stata ，都是菜单式操作，easy 的。

数据分析：R，数据库 SQL Server，IBMDB2

微分方程：Maple,Mathematic,MATLAB

运筹规划：Matlab，Lingo

智能算法：Matlab，R

时间序列:统计模型中的那些软件,或者 R,Matlab

图像处理：Matlab，C++

总结： Matlab 是必须的，再来个 SPSS，一般情况下够用了。

第五步:回答问题.

也就是论文的讨论部分。这部分是对你整篇论文成果的总结，一定要写的有深度。除此之外，通常还要写上一些灵敏度分析，如果是统计模型的话，要有模型检验。论文通常会需要画一些图表，可以使用 Matlab、R 等软件来画跟数据有关的图，使用 Visio 或者 PPT 画流程图之类的图。

关于比赛的一些个人体会

1、 国赛和美赛是有区别的国赛讲究实力,美赛讲究创新。

美赛不一定要多高级的方法，但是一定要有创意。而国赛，组委会往往是有一个模糊的“标准答案”在的，按部就班做下来就好了。注意不要一次性就建立复杂

模型了，老外看重的是你的思维，你的逻辑，不像国赛，看重的是你的建模编程实力，要使用各种高大上的方法。拿到一个问题，可以先建立一个初等模型，讨论下结果；再逐渐放宽条件，把模型做的复杂一点。即 Basic model -> Normal model -> Extended model 的思路。这个思维在美赛中很好，这么做下来基本都能得金奖的，鄙人这次也是按照这样的流程，拿了个金奖。

2、**文献为王**

文献为王。建模的题目，基本上是某个教授的研究课题，凭我们本科生的水平，基本上做不到对题目的深刻理解。所以要多看文献。

看文献也有技巧：刚拿到题目，先查一下相关背景资料，了解题目是哪方面的。接下来看文献，找一下硕士论文，博士论文以及综述性质的文章，硕博论文一般都会详细介绍下整个课题的国内外研究情况，综述就更不用说了，它就是对大量原始研究论文的数据、资料和主要观点进行归纳整理、分析提炼而写成的论文。看完这些，就可以比较有深度地把握题目，也知道如果我们要进行创新的话，往哪方面走。

接下来，可以根据小组三人讨论的结果，有针对性的看一下有深度的文献，文献看得多了，就可以考虑开

始创新了，像爱因斯坦那样开辟相对论等新领域的创新，是很有难度的，但是我们可以退而取其次，不是有句话叫做“他山之石，可以攻玉”吗？

我们要做的就是组合创新！ 领域内组合创新，把一个学者的方法嫁接到另一个学者的模型上。 以及交叉领域创新，把把自然科学的知识用到社会科学上，或者用社会科学解释自然科学的结果等等。（这里就可以体现，跨专业建模队伍的先天优势了：不同专业对同一个问题的思维是不同的，可以擦出创意的火花）

PS：图书馆有买很多数据库，可以免费看论文。免费的话 google 学术是无敌的，国内文献貌似没有良好的分享平台，实在找不到论文也可以百度文库死马当活马医。

平时可以多注册一些网站，数学中国，校苑数模，matlab 技术论坛，pudn 程序员，研学论坛，stackoverflow 等。上传些资料，攒积分要从娃娃抓起，不要等到比赛了看到好资料还“诶呀，积分不够”。

想法很重要。建模思维是一种很难学习到的东西，站在巨人的肩膀上，多看文献，负责建模的同学辛苦了。

3、掌握一点数据处理的技巧

建模的题目，A.B 两道题。基本上是一题连续，一题离散；一题自然科学（理工科），另一题社会科学（经济管理）。这样的分布的，大家平常做题的时候就可以有所侧重，曾经有一支美帝的队伍，专攻离散题，貌似拿了连续两届的 outstanding.

掌握一点数据处理的技巧是很有必要的。比如数据缺失值的处理，插值与拟合等。尤其是数据缺失值的处理，基本上 A,B 题都有可能涉及，建议熟练掌握。

4、关于编程水平

More generally,软件操作水平几乎决定了一个队伍的结果上限。MATLAB 是必备的，必须要熟练掌握各种模型的实现。此外，SPSS(或者 R)也是要掌握的。Mathematic 和 MATLAB 的替代性很强，不掌握也没关系（仅在建模方面，mathematic 当然也是很强大的）。What’s more 建模比赛举办这么多年，用到 lingo 的情况几乎很少了，也可以不学 lingo. And

现在的题目动不动就要粒子群等智能算法，强烈建议大家至少熟练掌握一种智能算法.

MATLAB 推荐书目基础：

MATLAB 揭秘　郑碧波 译 （本书讲的极其通俗易懂，适合无编程经验的）

精通 matlab2011a　张志涌

提升：数学建模与应用：司守奎 （囊括了各类建模的知识，还附有代码，很难得，工具书性质的）

Matlab 智能算法 30 个案例分析　史峰,王辉等

《MATLAB 统计分析与应用：40 个案例分析》数字图像处理(MATLAB 版)　冈萨雷斯 （13 国赛碎纸片复原居然涉及了图像处理,所以列在这里了.可看可不看,太专业化了）

书很多的.总之,要达到熟练运用 matlab 进行运筹优化,数据处理,微分方程的地步. 数理统计可以交给 SPSS,R ,其中 SPSS 无脑操作上手快.

5、格式规范：

看国赛一等奖，美赛国内人得特等奖的论文，格式规范方面绝对很到位，大家可以参考。国外人的特等奖论文，大都不重视格式，人家的优势在于模型实力

与创意、母语写作。所以在美赛格式规范方面，参考国内特奖的论文。

PS：有时间的队伍可以学习以下 Latex，用 Latex 写出来的论文，比 word 不知道好了多少倍。Latex 书目推荐：

LaTeX 插图指南

一份不太简短的 Latex 介绍

LaTeX-表格的制作 汤银才

参考文献常见问题集

latex 学习日记　　Alpha Huang

论坛：Ctex BBS

结束语：什么是数学的思维方式？观察客观世界的现象，抓住其主要特征，抽象出概念或者建立模型；进行探索，通过直觉判断或者归纳推理，类比推理以及联想等作出猜测；然后进行深入分析和逻辑推理以及计算，揭示事物的内在规律，从而使纷繁复杂的现象变得井然有序。这就是数学的思维方式。----------丘维声《抽象代数基础》前言

小朋友的涂鸦（一）：从

8 和 9 说起

方弦

看到题目，你也许会问：8 和 9，两个普通的数字，又有什么可说的呢？但在数学家眼中，这两个数字可不寻常：9 比 8 大 1，8 是一个立方数，它是 2 的立方，而 9 是一个平方数，它是 3 的平方。8 和 9，就是一个立方数紧紧挨着平方数的例子。那么，数学家自然会问：还有没有别的立方数，它紧紧挨着一个平方数呢？

或者用数学的语言来说，$x^2 - y^3 = 1$这个方程，除了$x = 3, y = 2$外，还有别的正整数解吗？

我们先在直觉上探索一下，平方数和立方数，当它们越变越大的时候，在所有正整数当中也会越来越稀疏。就像两个越来越不喜欢出外的人，即使是邻居，也许一开始会打个照面，但之后出门的次数越来越少，也就越来越不可能碰上面。数学家们甚至猜测，即使不限定于平方数和立方数，就算是任意大于 1 的次方数，它们“碰面”也只有 8 和 9 这一回。用严谨的数学语言来说，

就是方程$x^a - y^b = 1$，在a和b大于 1 的条件下，只有一组解，就是$x = 3, a = 2, y = 2, b = 3$。这又被称为卡特兰猜想（Catalan's conjecture）。

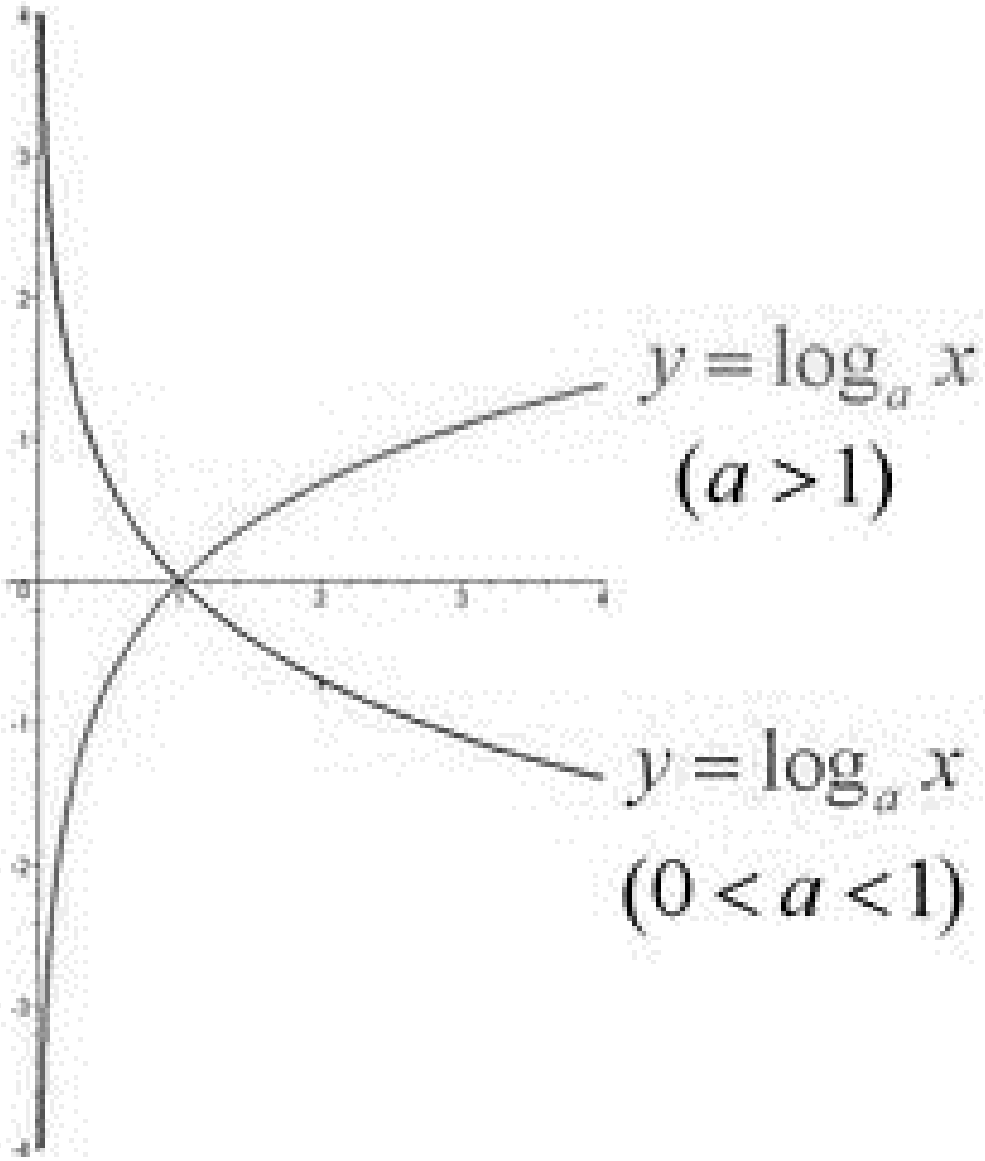
直觉上，卡特兰猜想应该是对的，但直觉毕竟是直觉，它不是数学证明。虽然平方数和立方数它们越来越稀疏，但是正整数有无限多个，它们有无数次碰面的机会，谁知道它们会不会在通向无限地平线的路途中就抓住了又一次机会呢？所以，我们需要数学证明，只有数学证明，才能从逻辑上根本地否决这种可能性。

我们来看看数学家是怎么思考的。

数学家们想要的是一个数学证明。我们重新考虑方程$x^a - y^b = 1$。在这个方程里什么东西最麻烦呢？减法很简单，等于号很简单，剩下的就是乘幂操作了。那么，有什么办法能去掉乘幂这个麻烦事呢？这个办法就是对数，大家在中学都学过。对数能将乘幂转化为更简单的乘法：$\ln(x^a) = a\ln(x)$。我们先将方程改写成$x^a = y^b + 1$，然后两边取对数，就得到了$a\ln(x) = \ln(y^b + 1)$

现在，方程里最麻烦的又是什么呢？就是对数里边的加法，因为对数和乘法很友好，但跟加法实在谈不来，$\ln(x + y)$并没有一个好的表达式。有什么方法可以绕过

去呢？我们想到，y^b是一个次方数，它可以非常大，要多大有多大，而相比之下，加上去的这个 1 非常小非常小，小得几乎可以忽略不计。而对数函数增长得又非常慢非常慢，ln(20)大概是 3，ln(400)大概是 6，要想对数值增加 3，原来的数要增加 20 倍，要等到10^{13}，也就是万亿，对数值才达到 30。而对于一万亿来说，这个小小的 1 实在是零头中的零头。



但数学是严谨的，虽然这个 1 很小，带来的影响更小，但我们不能直接说可以把 1 去掉。但这难不倒数学家：既然不是直接相等，划个界限总可以吧？用一点简单的高等数学，我们可以得到如下的不等式：

$$bln(y) < ln(y^b + 1) < bln(y) + y^{-b}$$

也就是说，去掉 1 和不去掉 1，对于对数值的影响只有y^{-b}，也就是y^b的倒数。因为y^b可以非常大，它的倒数也就非常小。如果它增长十倍，它的倒数就会变成原来的十分之一。我们刚才说到，y^b要达到万亿，它的对数值达到 30，这时候它的倒数，也就是加 1 造成的误差，只有万亿分之一。这是个什么概念呢？相当于在测量地球到太阳的距离时，不小心多加了根头发丝。在现实世界中，即使多么严谨的测量，这种程度的误差可能也就放过去了。但在数学中，无论多小的误差，不应该舍弃的时候就不能舍弃。

将这个误差的结论代入原来的方程，我们得到：

$$|aln(x) - bln(y)| < y^{-b}$$

也就是说，我们要寻找两个正整数，它们的对数值的某个倍数非常接近。这就需要对正整数的对数进行深入的研究。在 1966 年到 1967 年，数学家阿兰·贝克(Alan

Baker）写出了一系列的文章，其中给出了正整数乃至所谓“代数数”（也就是多项式方程的解），它们的对数的倍数之间距离的一个下界。也就是说，上面的不等式左边其实不会太小，它会大于某一个关于a, b, x, y的函数，可以写成：

$$C(x,y,a,b) < |aln(x) - bln(y)|$$

那么，如果我们能证明对于绝大部分的x, y, a, b都有$C(x,y,a,b) > y^{-b}$，那么两个不等式就会产生矛盾，方程也就不可能有整数解，这不就解决了卡塔兰猜想了吗？

当然，实际上这种简单粗暴的方法并不能解决问题。C(x, y, a, b)这个函数，虽然可以明确计算出来，然而得出的函数太小，不足以解决问题。但引出矛盾的方法不只一种。为了证明这类型的结论，贝克发明了一种方法，可以在不同的角度上引出矛盾。而另一位数学家Tijdeman 利用贝克的方法，找到了一个巧妙的角度，证明了当a和b足够大的时候，方程必定没有解。而此前人们已经证明了，当a和b固定的时候，关于x和y的方程最多只有有限个解，而且给出了这些解的一个上

Alan Baker

界。结合两个结果，数学家们证明了，整个关于a, b, x, y

的方程最多只有有限个解。现在在波尔多大学的数学家米歇尔·朗之万（Michel Langevin）计算出了一个明确的上界：

$$e^{e^{e^{e^{730}}}}$$

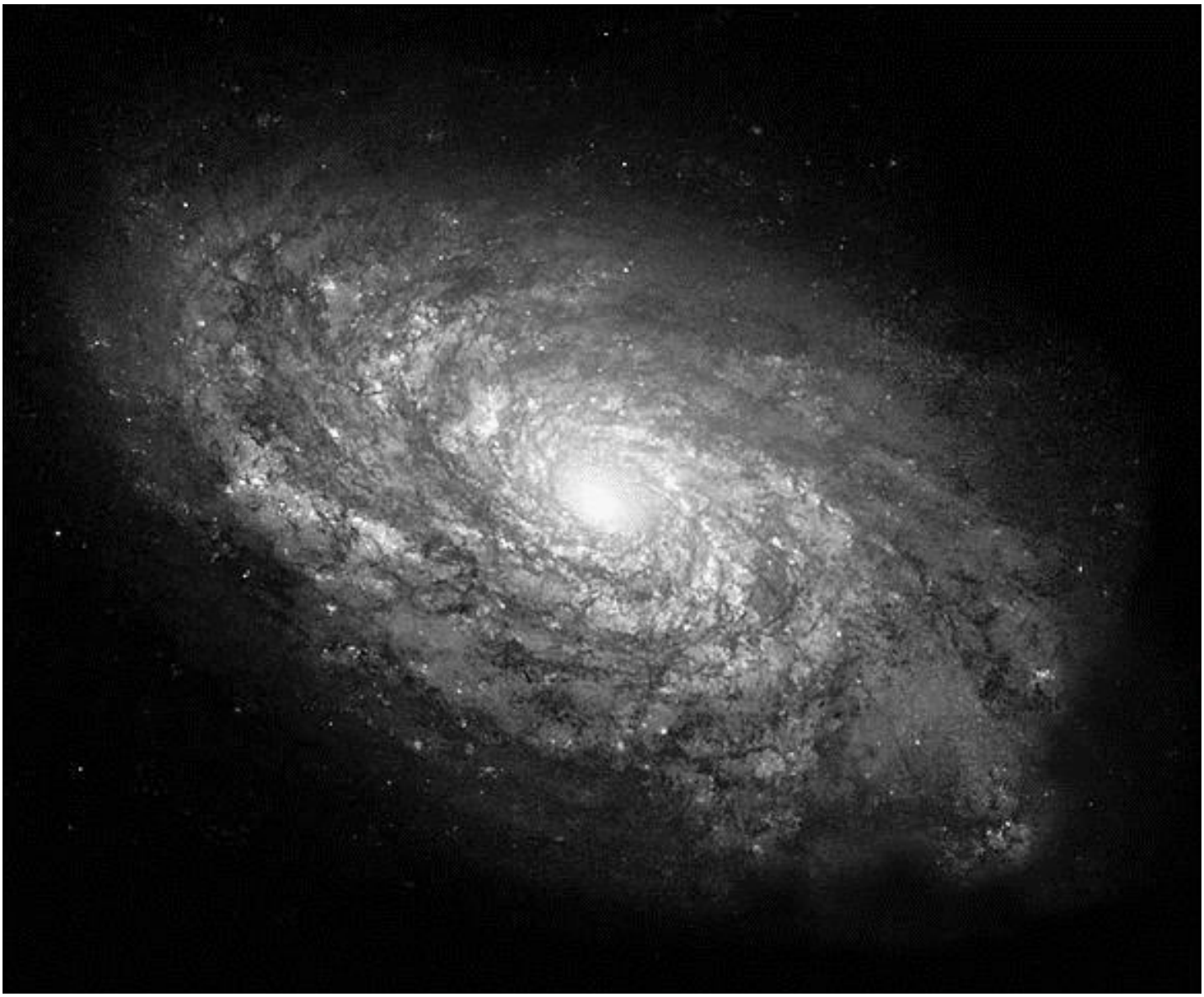
也就是说，只要检查比这个数小的所有正整数，如果没有找到别的解，那么就说明 8 和 9 是唯一一对靠在一起的次方数。但这个任务看起来容易，做起来却是无计可施。

$e^{e^{e^{e^{730}}}}$ 有多大？在现实中，能与其相比的数字根本不存在，即使是 1 后面添上宇宙里所有的原子当作 0，这样得到的无量大数，还是连零头的零头都赶不上。对于这么大的数字，表达它都有困难，更何况检查！

你可能觉得，这样找正整数的对数之间的关系，又有什么用呢？好不容易得出一个结果，却只是“原则上可以验证”，根本不能实际计算，这种方法又有什么用？但不要忘记，方法之所以是方法，就是因为它能应用到许多问题上。贝克的这套方法，可以应用到所谓的“丢番图方程”，也就是系数和解都是正整数的方程。大家

耳熟能详的费马大定理，可能大家不太熟悉的完美长方体问题，都是悬而未决的丢番图方程。而对这类方程的研究，涉及数论的方方面面。贝克的方法给丢番图方程地研究带来了全新的工具，他也因此获得了 1970 年的菲尔兹奖，那时离他发表相关论文还不到四年。

数目远超银河中原子个数，图片来自 Wikipedia



但卡特兰猜想仍然悬而未决。要等到 2002 年，罗马

尼亚的数学家 Preda Mihăilescu 才最终证明了卡特兰猜想。他的方法大量用到了分圆域与伽罗华模的知识，这些都是代数数论中的艰深概念，哪怕是稍稍涉猎，恐怕也需要本文十倍以上的篇幅才能讲个大概。但无论如何，我们现在终于可以确定，8 和 9 在自然数中的确是绝无仅有的一对，在无限的可能中，唯一一对能紧靠在一起的次方数。

卡特兰猜想还有别的变体，比如说人们猜想，对于任意的正整数 k，间距为 k 的次方数对只有有限个。对这些变体的探索也非常引人入胜。

但这不是这篇文章的主题。

从整数到多项式

我们在中学里就学过多项式。对于一个变量 x，我们取它的一些次方x^a, x^b等等，乘上系数，然后加起来，就得到了一个多项式，比如说$x^7 + 6x^3 + 4$，就是一个关于x的多项式。在这里，我们考虑那些系数都是复数的多项式，也就是复系数多项式。

数学家们很早就发现，这些多项式与正整数有一种神奇的相似性：可以做加法、减法、乘法，也可以分解因数，可以求最大公约数和最小公倍数，同样有着唯一分解定理：正整数可以唯一分解成素数的乘积，而多项

式也能唯一分解成所谓“不可约多项式”的乘积。基本上，在数论中对正整数性质的研究，很多都可以直接搬到多项式上来。于是，遇上有关正整数的问题，把它迁移到多项式之中，未尝不是一个提出问题的好办法。自然，因为多项式本来结构就比较复杂，相关的问题也更难解决，但这不妨碍数学家的步伐，毕竟他们要攻克的就是难题。

> 注：更准确地说，因为正整数和多项式都组成了所谓的“欧几里德整环”（Eucliean domain），所以它们共享非常多的数论性质，比如说，它们都是所谓的“主理想整环”，它们的所有理想都是主理想，也就是某个元素的倍数组成的理想。此处插播一则笑话：为什么 QQ 只有 QQ 群？因为 QQ 没有理想……

在 1965 年，Birch、Chowla、Hall 和 Schinzel 问了一个问题：如果有两个多项式P和Q，它们是互质的，那么P的平方和Q的立方之间的差距，也就是说$P^2 - Q^3$，可以有多小？这个问题很显然是卡塔兰猜想的延伸。卡塔兰猜想最原始的版本问的是，除了 8 和 9 以外，平方数和立方数的距离能不能达到 1。而 Birch 等人现在问的是，多项式平方和立方的距离最小能达到多少？

当然，要回答这个问题，首先要想办法衡量多项式的

大小。对于不同的多项式P(x)，当x趋向于正无穷时，P(x)趋向无穷的速度各有千秋，而决定这个速度的主要因素，就是多项式的次数，也就是多项式中x的最高次方是多少。所以，我们选择多项式的次数作为衡量多项式大小的标尺。现在，我们可以用更严谨的方式叙述那四位数学家的问题：

对于某个正整数k，假设有两个互质的多项式P, Q，其中P的次数是$3k$，Q的次数是$2k$。那么，多项式$R = \mathrm{P}^2 - Q^3$的次数最小可以有多小？

我们能看出来，在这个问题中P和Q的次数不是随便选取的。如果P的平方和Q的立方次数不一样的话，那么R就跟P, Q一样大。只有上面的选择方法，才能至少使两者的最高次项互相抵消，使问题变得不那么无聊。另外，对于任何一个例子，我们只要将所有多项式都乘上一个合适的常数，就能得到另一个本质上相同的例子。所以，我们只考虑本质上不同的那些例子。

在论文中，四位数学家给出了一个$\mathrm{k} = 5$的例子：

$$\mathrm{P} = \frac{1}{27}t^{15} + \frac{1}{3}t^{12} + \frac{4}{3}t^{9} + \frac{8}{3}t^{6} + \frac{5}{2}t^{3} + \frac{1}{2}$$

$$\mathrm{Q} = \frac{1}{9}t^{10} + \frac{2}{3}t^{7} + \frac{5}{3}t^{4} + \frac{4}{3}t$$

$$\mathrm{R} = \frac{1}{36}t^6 + \frac{7}{54}t^3 + 4$$

在这个例子里，P, Q, R的次数分别是 15、10 和 6。虽然P^2 和Q^3 的次数都是 30，但是它们凑巧在前 24 项的系数都相同，而它们的差仅仅只是一个六次多项式，真是一个难得的巧合。但数学家总是有些贪心，面对这个例子，他们想的是：能不能把R的次数再压低一点？能不能找到差距更小的平方多项式和立方多项式？这个想法非常自然，但在反反复复的尝试中，似乎找不到次数更低的例子了。于是，这四位数学家就猜想：这个例子是不是已经无法改进了呢？他们提出了这样的猜想：

对于两个互质的多项式P, Q, 假设其中P的次数是$3k$，Q的次数是$2k$。那么，多项式$\mathrm{R} = \mathrm{P}^2 - Q^3$的次数至少也有$k+1$，而且总能找到使R的次数恰好是$k+1$的例子，也就是说这个下界是紧的。

在刚才的例子中$k = 5$ ，而R的次数恰好就是 5+1=6，符合猜想。数学家们想寻找更多的这样达到最小差距的例子，尝试在其中寻找规律。但出人意料的是，$k = 5$的第二个例子，要到 35 年之后的 2000 年，才被 Elkies 发现，而且这个例子的复杂度远远超出了预期。在上面

的例子中，我们看到的系数都是相对简单的分数。而现在，请看 Elkies 的这个例子：

$$\begin{aligned}P = x^{15} - 3x^{14} + 51x^{13} - 67x^{12} + 969x^{11} + 33x^{10} \\ + 10963x^9 + 9729x^8 + 96507x^7 \\ + 108631x^6 + 580785x^5 \\ + 700503x^4 + 2102009x^3 \\ + 1877667x^2 + 3904161x \\ + 1164691\end{aligned}$$

$$\begin{aligned}Q = x^{10} - 2x^9 + 33x^8 - 12x^7 + 378x^6 + 336x^5 \\ + 2862x^4 + 2652x^3 + 14397x^2 \\ + 9922x + 18553\end{aligned}$$

$$\begin{aligned}R = -2^6 3^{15}(5x^6 - 6x^5 + 111x^4 + 64x^3 + 795x^2 \\ + 1254x + 5477)\end{aligned}$$

在这个新例子中，多项式的系数大大膨胀了，这就解释了为什么寻找第二个例子花了这么长的时间。我们也能从另一个侧面窥见这个问题的难度。比方说，我们希望用待定系数法寻找例子：先将多项式P, Q的系数都设为未知数（最高次的系数设为 1），然后计算R的所有系数，它们都是之前未知数的多项式。在$k = 5$的情况下，我们要求R从x^{29} 到x^7的这 23 个系数都是 0，这样就得到了 23 个方程。将它们联立起来，就得到了一个

关于 25 个变量的 23 个方程组成的高次方程组，理论上只需要解出这个方程组，就能得到所有的例子。但问题是，这个方程组的总次数是 6198727824，大约是六十亿！这样的方程，不要说是人脑，就是计算机也几乎无法解开。但至少，我们知道这些系数都是所谓的“代数数”，也就是代数方程的解。这样庞大而困难的问题，难免令人望而却步。寻找新的例子已经如此困难，更不要说穷尽所有例子了。

但有一帮数学家，光是看了看问题，在餐巾纸上随手涂鸦了一下，就拍着胸脯宣称：$k=5$的情况一共就只有 4 个例子，还有两个就继续找吧；不光这样，对于任意k的情况，我们都能证明你们的猜想是对的，而且还能帮你们计算所有本质上不一样的例子一共有多少个。

这是什么魔法？

文章来自 方弦 在科学松鼠会发表的文章《小朋友的涂鸦（一）：从 8 和 9 说起》

童哲老师说说：行列式是什么

作者介绍：童哲，万门大学校长。18 岁厦门双十中学校运会 1500 米金牌;19 岁物理竞赛全省第一保送北京大学；20 岁北京大学校运会蝶泳第四名；22 岁法国巴黎高师入学考试全球前十名考入；24 岁获得巴黎高师 Mr.MEGA 称号;25 岁创办全国第一所网络大学— 万门大学；26 岁录制多门公开课并在 50 多所大学做演讲；27 岁创办在线教育公司成为 CEO；28 岁万门大学课程超过 150 门影响百万人

行列式这个“怪物”定义初看很奇怪，一堆逆序数什么的让人不免觉得恐惧，但其实它是有实际得不能更实际的物理意义的，理解只需要三步。

1. 行列式$det(A)$是针对一个$n \times n$的矩阵A而言的。A表示一个n维空间到n维空间的线性变换。那么什么是线性变换呢？无非是一个压缩或拉伸啊。假想

原来空间中有一个n维的立方体（随便什么形状），其中立方体内的每一个点都经过这个线性变换，变成n维空间中的一个新立方体。

2. 原来立方体有一个体积V_1，新的立方体也有一个体积V_2。

3. 行列式$det(A)$是一个数对不对？这个数其实就是$\frac{V_2}{V_1}$，结束了。就这么简单？没错，就这么简单。

所以说：行列式的本质就是一句话：**行列式就是线性变换的放大率！**

理解了行列式的物理意义，很多性质你根本就瞬间理解到忘不了！！！比如这个重要的行列式乘法性质：

$$det(A) \times det(B) = det(BA)$$

道理很简单，因为放大率是相乘的啊！

你先进行一个A变换，再进行一个B变换，放大两次的放大率，就是式子左边。你把“先进行A变换，再进行B变换”定义作一个新的变换，叫做“BA”，新变换的放大律就是式子右边。然后你要问等式两边是否一定相等，我可以明确告诉你：too simple 必须相等。因为其实只是简单的把事实陈述出来了。这就好像：“ 你经过股票投资，把 1 块钱放大 3 被变成了 3 块

钱，然后经过实业投资，把 3 块钱中的每一块钱放大 5 倍成了 5 块钱。请问你总共的投资放大率是多少？”

$$3 \times 5 = 15$$

翻译成线性代数的表达就是：$det(A) \times det(B) = det(BA)$ 。这还不够！我来解锁新的体验！

刚刚咱们说到行列式其实就是线性变换的放大率，所以你理解了$det(A) \times det(B) = det(BA)$：那么很自然，你很轻松就理解了：$det(AB) = det(BA)$。So easy，因为$det(AB) = det(A) \times det(B) = det(BA)$

同时你也必须很快能理解了**“矩阵A可逆”完全等价于“$\mathbf{det}(A) \neq 0$”**。因为再自然不过了啊，试想$det(A) = 0$是什么意思呢？不就是线性变换A把之前说的n维立方体给拍扁了啊？！这就是《三体》中的”降维打击”有木有!!!如来神掌有木有!!!直接把 3 维立方体 piaji 一声~一掌拍成 2 维的纸片，纸片体积多少呢？当然是 0 啦！

请注意我们这里说的体积都是针对n维空间而言的，$det(A) = 0$ 就表示新的立方体在n维空间体积为 0，但是可能在$\mathrm{n}-1$维还是有体积的，只是在n维空间的标准下为 0 而已。好比一张纸片，“2 维体积”也就是面

积可以不为0，但是“3维体积”是妥妥的0。

所以凡是$det(A)=0$的矩阵都是要流氓，因为这样的变换以后就再也回不去了，降维打击是致命性的。这样的矩阵必然是没有逆矩阵A^{-1}的。这就是物理意义和图象思维对理解数学概念的重要性。

当然要证明也是小菜一碟轻而易举的：由$AA^{-1}=I$可知$det(A)\times det(A^{-1})=det(I)=1$。这怎么可能啊？$det(A)=0$了，那么$det(A^{-1})$等于多少呢？毫无办法，只能不存在。一个矩阵怎么可能行列式不存在呢？只能是因为A^{-1}不存在。所以A自然不可逆。

我来加点儿烧脑的：

傅里叶变换也可以求行列式!!!

是的你没有听错，大名鼎鼎的傅里叶变换$F(k)=\int_{-\infty}^{\infty}f(x)e^{ikx}dx$ 居然也可以求行列式!!!

首先一定有很多人要问责我，是不是没有学过行列式，因为按照绝大多数教科书来说，行列式是这样定义的：

$$\det(A)=\sum_{\sigma\in S_n}sgn(\sigma)\prod_{i=1}^{n}A_{\sigma(i)i}$$

然后还有什么好说的，拿到一个矩阵各种化简然后算就好了呗，可是怎么说傅里叶变换也可以求行列式？

傅里叶变换又不是一个矩阵，更别说矩阵元A_{ij}了。我在痴人说梦吗？但是，等等！桥度麻袋，“傅里叶变换”里面有个"变换"，难道它也是“线性变换”？！！！一检查，还真的是。所有函数$f(x)$就组成了一个向量空间，或者说线性空间。可是为什么呢？从高中咱们就熟悉的$f(x)$明明是函数啊，怎么就变成了向量v呢？向量v不是一个n维空间中的箭头吗？长得也不像啊。

其实 “所有$f(x)$组成的集合” 确实满足一切线性空间的定义，比如：

1，向量$f(x)$和向量$g(x)$可以相加，并且有交换律$f(x)+g(x)=g(x)+f(x)$

2，存在零向量$f(x)=0(x)$，即处处值为零的函数

3，任何一个向量$f(x)$都存在一个与之对应的逆向量$-f(x)$，使得相加之和等于零向量$f(x)+\big(f(-x)\big)=0$

以及存在数乘以及分配率等性质…… 总之“所有向量$f(x)$组成的集合”完美满足线性空间的 8 条黄金法则。

原来咱们熟悉的函数$f(x)$身世可不一般啊，其实它是一个掩藏得很好的向量！！！对，我没有说错，因为所有函数$f(x)$组成的集合构成了一个线性空间！而且还是无穷维的线性空间！！！一旦接受了向量$f(x)$是向量的

设定，周围的一切都变得有趣起来了！

接下来不妨思考一下，傅里叶变换$F(k)=\int_{-\infty}^{\infty}f(x)e^{ikx}dx$是把一个函数$f(x)$变成了另一个函数$F(k)$，难道不可以理解为把一个线性空间中的向量$f(x)$变成了另一个线性空间中的向量$F(k)$吗？！而且这个变换是妥妥的线性的，完美地满足线性变换的定义：$A(v_1+v_2)=Av_1+Av_2$　以及$A(k\times v_1)=k\times Av_1$。因为积分变换的线性性：$f(x)+g(x)$的傅里叶变换　$=\int_{-\infty}^{\infty}\big(f(x)+g(x)\big)e^{ikx}dx=\int_{-\infty}^{\infty}f(x)e^{ikx}dx+\int_{-\infty}^{\infty}g(x)e^{ikx}dx=f(x)$的傅里叶变换+$g(x)$的傅里叶变换.

加法达成。当然数乘也轻松满足：$\int_{-\infty}^{\infty}(kf(x))e^{ikx}dx=k\int_{-\infty}^{\infty}f(x)e^{ikx}dx$。于是乎，我们通过以上内容知道了一个重要的结论：**傅里叶变换其实也是线性变换，所以也可以求行列式!!!**（其实傅里叶变换作为一个线性变换不但可以求行列式，更可以求它的特征向量!!比如$f(x)=e^{-x^2/2}$，以及其他很多很多东东，恭喜你又一扇新世界的大门被打开了。千万不要小看傅里叶变换，比如量子力学不确定性原理的秘密就都在这里了）

言归正传那么傅里叶变换神秘的行列式的值$det(F)$究竟是多少呢？难道这个无穷维线性变换也可以求出

行列式吗？那我就把$det(F)$求出来给你看：

很明显的问题是这是一个比较困难的问题，因为求傅里叶变换的行列式让我们觉得没有工具可以用，行列式的定义式毫无用武之地。毕竟没有谁能够写出傅里叶变换的$\infty \times \infty$矩阵表达式并套用公式。所以一定要用到其他的化简办法，例如对称性啊等等。不妨先回顾一下之前的结论，对于任何可逆线性变换A有如下性质：

$$det(A) \times det(A^{-1}) = det(I) = 1$$

如果把傅里叶变换F看做是一个无穷维的A，那么也一定满足这个性质。所以只要求出了傅里叶变换的逆变换的行列式，求一个倒数就得到了傅里叶变换的行列式。哎？问题变得更难了。傅里叶变换的逆变换？若傅里叶变换是：$F(k) = \int_{-\infty}^{\infty} f(x)e^{ikx}dx$则它的逆变换是：

$$f(k) = \frac{1}{2\pi}\int_{-\infty}^{\infty} F(x)e^{-ikx}dx$$ （说明傅里叶变换可逆，因为表达式都出来了）

现在的问题是，正负变换，我都不会求行列式，唯一知道的是$det(F) \times det(F^{-1}) = 1$,

为之奈何？我们还需要至少一个表达式能够反映二者的关系，连立起来才能够求解。

没问题，因为这两个变换真是太像了，像到几乎完全

对称。差异点仅仅在于逆变换多一个乘积系数$\frac{1}{2\pi}$，以及积分因子e^{ikx}多了一个负号。除此之外完全是同一个线性变换。而积分因子e^{ikx}多一个负号是什么意思？意味着复数空间的手性定义相反，i变成了$-i$，左手变成右手，或者说虚数部分取负号实数部分不变。这样的手性改变，并不会改变线性变换的体积放大率（之前的知识）。于是乎在线性变化的方法率的意义下，傅里叶变换和它的逆变换放大率是一样的（还差一个乘积系数$\frac{1}{2\pi}$）。

于是也就是说$\det(F^{-1}) = \frac{1}{2\pi}\det(F)$, 结合之前的式子$det(F) \times det(F^{-1}) = 1$，我们很容易得到$\det(F) = \sqrt{2\pi}$（更严格来说更对称的傅里叶变换版本$F(k) = \frac{1}{2\pi}\int_{-\infty}^{\infty} f(x)e^{ikx}dx$的行列式为 1）

是的，你已经求出来了，虽然神一般的无穷维行列式的计算公式并没有出现，但你确实求出来了。

再附送大家一个彩蛋：都说求导可以把一个函数$f(x)$

变成另一个函数$f'(x)$，如果我们把“求导这个操作”D当做是一个线性变换，发现其实也是完全合理的：$D: f(x) \to f'(x)$

线性性完美地满足：$D: k_1 f(x) + k_2 g(x) \to k_1 f'(x) + k_2 g'(x)$

那么请问"求导作为函数空间下的线性变换行列式”等于多少呢？思考一下。

$$\det(D) = 0$$

因为，它是不可逆的！你要问我兹次不兹次？我可以明确告诉你，不可逆的线性变换都是耍流氓，行列式都等于零。不要没事就搞个大新闻。

（全剧终，数学中的严格性在本文中并不能体现，请海涵。）

数学建模融入经济

数学中的案例及分析

钱和平，徐清舟

一．怎么才能保证宏观经济稳定.

在完全自由竞争的市场经济中会经常出现供大于求导致价格下降供不应求导致价格上涨这样的循环往复的局面，有的振幅小趋向平衡有的振幅越来越大，如果没有外界如政府的干预，将导致经济崩溃．下面我们用导数和微分建模讨论政府应该采取什么样的措施才能保证宏观经济的稳定．对于一个特定商品的需求与供给同时依赖于许多因素，如它的价格、其它商品的价格、消费者的偏 爱、消费者人数、消费者的收入等．为了简化对问题的分析，假定其它因素暂时保持某种状态不变，只考虑与价格的关系．在许多市场上，时间不能看成连续变量而应该看成是离散变量，我们用整数来标记生产和购买的时间．生产者可根据以前的信息决定其第（n＋1）批生产的产品的总量，假设他做决定

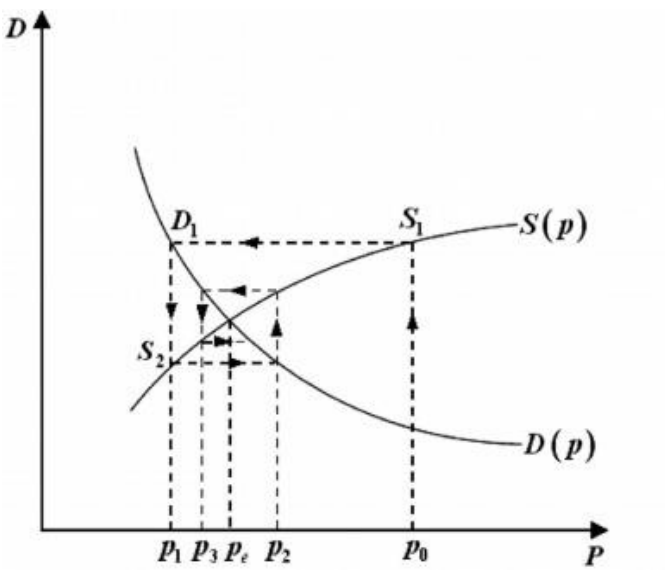
是基于第 n 次市场的行为，记S_{n+1}为$n+1$次市场的总合供给，则有：

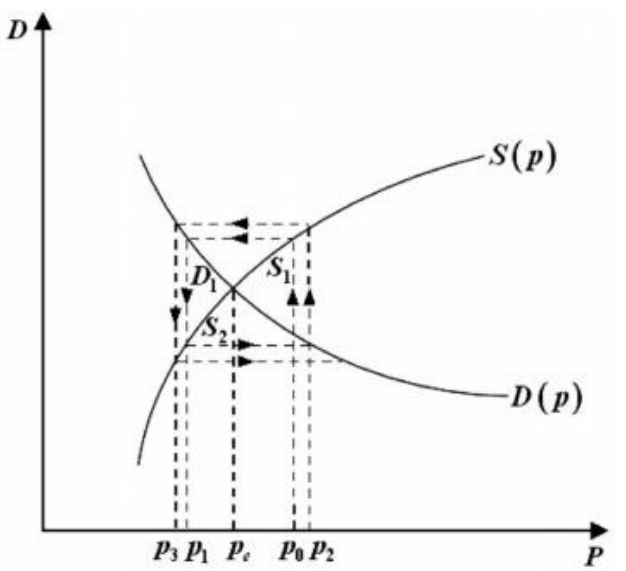
$$S_{n+1} = S(p_n) \tag{1.1}$$

其中p_n为第n次市场的价格．设市场是一个理想竞争市场，很快就出现均衡，即第n次市场上供给等于需求

$$D(p_n) = S_n = S(p_{n-1}) \tag{1.2}$$

方程(1.1)和方程(1.2)就确定了市场上的价格．一般情况下，需求随着价格上涨而减少，供给随着价格上涨而增加．如图 1，图 2，在同一坐标系上画上总合需求曲线和总合供给曲线





左图 1　点 p ＝ p e 是稳定的平衡点

右图 2　点 p ＝ p e 是不稳定的平衡点

图中的虚线形似蛛网，图 1 中，蛛网向内部前进趋向于点$\mathrm{p}=\mathrm{p}_e, \mathrm{D}(\mathrm{p}_e)=S(p_e)$. 在这个点上，价格不再变化，表明点$\mathrm{p}=\mathrm{p}_e$是稳定的平衡点，意味着商品的供需与价格趋向稳定．图 2 中，蛛网向外部前进远离点$\mathrm{p}=\mathrm{p}_e$，即点$\mathrm{p}=\mathrm{p}_e$是不稳定的平衡点，意味着商品的供需与价格将出现越来越大的振荡．这种用需求曲线和供给曲线分析市场经济稳定性的图示法在经济学中称蛛网模型．我们分析一下图 1 和图 2 的不同之处就会发现，需求曲线比供给曲线陡峭，有利于经济的稳定．为了进一步分析这种现象，下面利用导数和微分工具来定量分析蛛网模型．令$\Delta\mathrm{p}=\mathrm{p}-\mathrm{p}_e$，则有

$$\Delta\mathrm{D}=\mathrm{D}(\mathrm{p})-\mathrm{D}(p_e)=D'(p_e)(p-p_e)+o(p-p_e);$$

$$\Delta\mathrm{S}=\mathrm{S}(\mathrm{p})-\mathrm{S}(p_e)=S'(p_e)(p-p_e)+o(p-p_e)$$

当$\Delta\mathrm{p}$很小时，有

$$\mathrm{D}(\mathrm{p})\approx\mathrm{D}(p_e)+\mathrm{D}'(p_e)(p-p_e),$$

$$\mathrm{S}(\mathrm{p})\approx\mathrm{S}(p_e)+\mathrm{S}'(p_e)(p-p_e)$$

从而近似有

$$\mathrm{D}(\mathrm{p}_n)=\mathrm{D}(p_e)+\mathrm{D}'(p_e)(p_n-p_e),$$

$$\mathrm{S}(\mathrm{p}_{n-1})=\mathrm{S}(p_e)+S'(p_e)(p_{n-1}-p_e)$$

注意到$\mathrm{D}(\mathrm{p}_n)=\mathrm{S}(\mathrm{p}_{n-1}), \mathrm{D}(p_e)=\mathrm{S}(p_e)$，所以不难得

到

$$p_n = (p_0 - p_e)\left(\frac{S'(p_e)}{\mathrm{D}'(p_e)}\right)^n + p_e$$

如果系统稳定，那么必须$\left(\frac{S'(p_e)}{\mathrm{D}'(p_e)}\right)^n \to 0(n \to \infty)$, 于是有$|\mathrm{D}'(p_e)| > |S'(p_e)|$，即需求曲线变化强于供给曲线变化时，系统是稳定的．模型中$|\mathrm{D}'(p_e)|$表示价格下跌一个单位时需求量上升的幅度，$|S'(p_e)|$表示价格上涨１个单位时（下一时期）商品供应的增加量．它要求人们对商品的消费能力适当高于商品的供给能力，有利于宏观经济的稳定．一方面，政府在控制物价的同时，应出台更多的刺激消费政策，扩大人们的消费需求，提高人们的消费能力．另一方面，政府要正确处理好增长投资和拉动消费的关系，不管商品价格如何变化，都要 保证商品的有效供给，当供应量少于需求时，从外地收购或调拨，投入市场；当供过于求时，收购过剩部分，维持商品上市量不变．

二・怎样定价才能提高收益．

在争夺客户的战争中，价格战是企业管理者手中最常挥动的武器，体现了企业为实现自己的营销目标而实行的定价艺术和技巧．定价过高，会影响消费者的经

济利益从而失去消费者；定价过低，则会影 响企业的收益目标和企业的长期发展．那么怎样定价才能提高收益呢？下面用微分学的知识建模来回答这个问题．假设某商品的需求函数用$\mathrm{D}=\mathrm{D}(\mathrm{p})$ 表示，且可微.$\frac{\Delta p}{p}$为价格p的相对该变量，$\frac{\Delta D}{D}$为需求 D 的相对该变量，则称

$$\lim_{\Delta p\to 0}\frac{\Delta D}{D}\Big/\frac{\Delta p}{p}=\lim_{\Delta p\to 0}\frac{\Delta D}{\Delta p}\frac{p}{D}=\frac{p}{D}\frac{dD}{dp}$$

为该商品的需求价格弹性，简称需求弹性，记为$\varepsilon_p=\frac{p}{D}\frac{dD}{dp}$. 需求弹性$\varepsilon_p$表示某商品需求量D对价格p的变动的反应程度．由于需求函数为价格减函数，故需 求弹性为负值．当商品价格上涨（或下跌）１％时，其需求量将减少（或增加）约$\left|\varepsilon_p\right|\%$. 在商品经济中，商品经营者关心的是提价$(\Delta p>0)$或降价$(\Delta p<0)$对总收益的影响．设销售收益 R=Dp，则当$\Delta p$很小时，有

$$\Delta\mathrm{R}\approx\mathrm{dR}=\mathrm{d}(\mathrm{Dp})=\mathrm{Ddp}+\mathrm{pdD}=\left(1+\varepsilon_p\right)Ddp,$$

于是有

$$\Delta\mathrm{R}=\left(1-\left|\varepsilon_p\right|\right)D\Delta p.$$

由此可知，当$\left|\varepsilon_p\right|>1$（高弹性）时，降价可使总收

益增加，薄利多销多收益，一般指一些非必需品的且容易找到替换物的商品；当$|\varepsilon_p| < 1$（低弹性）时，提价可使总收益增加，一般指社会必需品，如粮食等；当$|\varepsilon_p| = 1$（单位弹性）时，提价或降价对总收益没有明显的影响.

三·广告越多越好吗？

广告是通过一定媒体向用户推销产品或承揽服务以达到增加了解和信任以致扩大销售目的的一种 促销形式．当今世界，商业广告已十分发达，尤其是一种新产品、新技术的出现，靠行政手段推广，既缓慢 又有局限性，而通过广告直接与消费者见面，激发和诱导消费，能使新产品、新技术迅速在市场上站稳脚跟，获得成功．那么，广告量越多越好吗？下面通过微分方程建模解释和分析这个问题

设x(t)表示对某商品的购买量,X_0表示该商品的最高需求水平，y(t)表示对该商品的广告量，Y_0表示广告量的最高限制．商品的需求发展速度$\frac{dx}{dt}$受当前该商品的需求量x(t) 与实际的商品需求发展潜力$(1-\frac{x}{X_0})$ 影响；同时也受广告量y(t) 的影响，当y(t) 不超过Y_0

时，广告能促进消费，当y(t) 超过Y_0，消费者往往会出现逆反心理，甚至顾虑该商品是否有质量问题等而影响x(t). 广告的投入速度$\frac{dy}{dt}$受消费者对该商品需求量的影响，于是有下面的广告与购物的微分方程模型:

$$\begin{cases} \frac{dx}{dt} = \mu x\left(1 - \frac{x}{X_0}\right) + ky(1 - \frac{y}{Y_0}) \\ \frac{dy}{dt} = r(X_0 - x) \end{cases} \tag{3.1}$$

其中μ, k, r是正常数, μ表示某商品的实际购买水平对该商品的购买速度增长潜力的影响系数, k表示广告量对商品的购买速度的影响系数，r 表示商品的实际购买水平对单位时间内的广告量的影响系数.

系统(3.1)有两个奇点是$P(X_0, 0), Q(X_0, Y_0)$.

对于P点，(3,1)的线性近似系统的特征方程为

$$\begin{vmatrix} -\mu - \lambda & k \\ -r & -\lambda \end{vmatrix} = 0,$$

即

$$\lambda^2 + \mu\lambda + kr = 0,$$

$$\lambda_{1,2} = \frac{-\mu \pm \sqrt{\mu^2 - 4kr}}{2}$$

当$\mu^2 - 4kr > 0$时P是稳定的结点，当$\mu^2 - 4kr < 0$时P是稳定的焦点。

对于Q点，(3.1)的线性近似系统的系数矩阵为

$$\begin{pmatrix} -\mu & -k \\ -r & 0 \end{pmatrix}$$

特征方程为

$$\lambda^2 + \mu\lambda - kr = 0,$$

$$\lambda_{1,2} = \frac{-\mu \pm \sqrt{\mu^2 + 4krY}}{2}$$

故Q点是鞍点

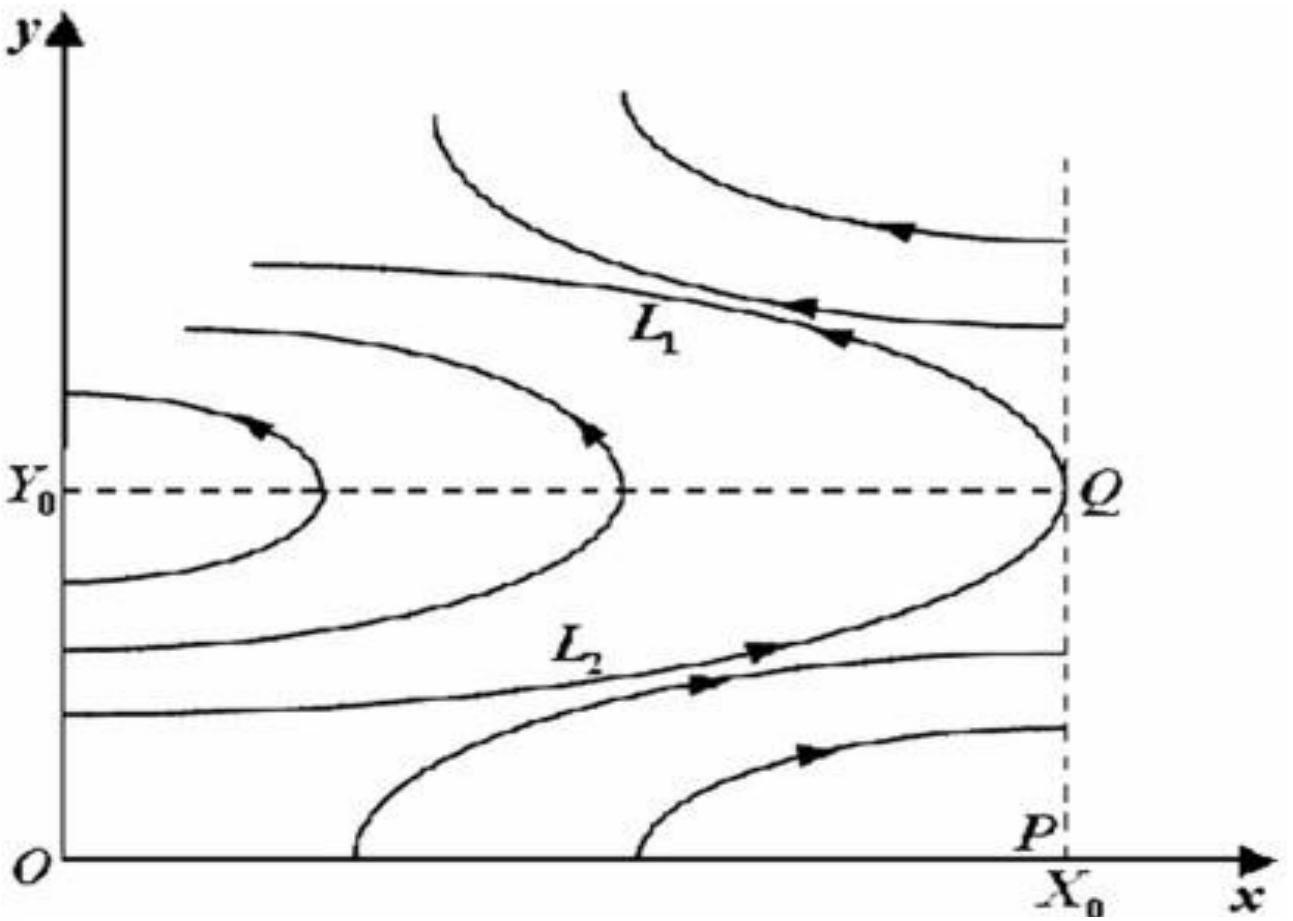


图 3 系统(3.1)的相图

系统(3.1)的相图如图 3，从相图上我们可以看到，当广告量不超过Y_0 时，广告有促销作用，$x(t)$ 随时间之增加而增加；当广告量超过Y_0，$x(t)$ 单调减少，广告过多引起了副作用．两条鞍点分界线L_1和L_2所夹的区域内，随时间的推移，购买量将变成零，对于t_0时刻的购买量$x(t_0)$，要有一个合适的广告量与之相匹配，使得$(x(t_0),y(t_0))$ 落在L_2下方的区域内，才能使购买量随时间的推移而达到最大．如果$(x(t_0),y(t_0))$落在L_2上方，则随着时间的推移，购买量将变成零，这就是广告偏多的负面影响．

本文引用自《大学数学》Vol28 No.3

刷题：求证 n 阶矩阵 A 为对称矩阵的充要条件为 $\mathbf{A^2 = A^T A}$

题解提供：华小数

分析：题目要证 A 为对称矩阵，，即 $A^T=A \Leftrightarrow A-A^T=0$,即证一个矩阵等于零。我们从“证明一个负数等于零”的做法中寻求思路：

由于复数没有大小的关系，因此直接证一个复数 $Z=0$ 比较困难。我们通常的做法是证 Z 的模 $|Z|=0$。因为模是一个实数，因此有大小关系，证明起来比较方便。

那对于矩阵，如何让给他一个模呢？先来搞清楚什么是模。

定义：V 为一个线性空间，任取 V 中元素 α，都有一个实数||α||与之对应，且满足：

（i）||α||≥0，∀α∈V，且||α||=0⇔α=0(要用到的)

（ii）||kα||=|k|·||α||，k 为实数

（iii）||α+β||≤||α||+||β||

则称||·||为 V 上的一个模（范数）。

可以看到，模实际上就是距离概念的推广。

下面来给矩阵 A 赋一个模，自然地，考虑 A^2，但这对我们没有帮助，我们应该考虑 A^TA。

设 $A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$，则 $A^TA=$

$$\begin{pmatrix} a_{11}^2+a_{21}^2+\cdots+a_{n1}^2 & 0 & \cdots \\ 0 & a_{12}^2+a_{22}^2+\cdots+a_{n2}^2 & \\ \vdots & & \ddots \\ 0 & 0 & \cdots \end{pmatrix}$$

出现了很多平方项，但模是一个实数，而 A^TA 是一个矩阵，怎么办？

我们对 A^TA 取迹，$tr(A^TA)=a_{11}^2+a_{21}^2+\cdots+a_{n1}^2+a_{11}^2+a_{12}^2+\cdots+a_{n2}^2+\cdots+a_{1n}^2+\cdots a_{nn}^2$(全体对角元之和)

于是可以定义 A 的模$||A||=\sqrt{tr(A^TA)}$，显然$||\cdot||$满足我们提出的三点要求。特别地，有$||A||=0\Leftrightarrow A=0\Leftrightarrow tr(A^TA)=0$。于是，今后要证一个实矩阵 B=0,只需证 $tr(B^TB)=0$。

证明：（必要性）显然

（充分性）$A^T-A=0$

$\Leftrightarrow tr[(A^T-A)^T\ (A^T-A)]=0$

$\Leftrightarrow tr[(A-A^T)\ (A^T-A)]=0$

$\Leftrightarrow tr[AA^T-(A^T)^2-A^2+A^TA]=0$

$\Leftrightarrow tr(A^TA)-tr[(A^T)^2]-tr(A^2)+tr(A^TA)=0(*)$

$\because A^2=A^TA$

$\therefore tr(A^TA)=\ tr(A^2)$

于是(*)式$\Leftrightarrow tr(A^TA)=\ tr[(A^T)^2]$

为证这点，我们指出关于迹的两个事实：

① $tr(B^T)=tr(B)$(直接将矩阵乘开即得)

② $tr(AB)=tr(BA)$

$\therefore tr[(A^T)^2]=\ tr[(A^2)^T]$

$=\ tr(A^2)$

$=\ tr(A^TA)$

$=\ tr(AA^T)$

于是命题得证。

注记：题目中要求 A 为实矩阵，因此由 $a_{11}^2+\ a_{21}^2+\cdots+a_{n1}^2+a_{11}^2+\ a_{12}^2+\cdots+\ a_{n2}^2+\cdots+\ a_{1n}^2+\cdots a_{nn}^2=0$ 可以推出 $a_{11}=\cdots=a_{1n}=\cdots=\ a_{n1}=\cdots=\ a_{nn}=0$

我们指出，若 A 为复数域上的矩阵，可以定义 $||A||=\sqrt{tr(\overline{A}^TA)}$，其中$\overline{A}$表示对 A 的每一个元素取共

轭，于是要证一个复矩阵 A=0，只需证$tr(\overline{A}^T A)$=0。所以

A 为共轭对称矩阵

$$\Leftrightarrow \overline{A}^T = A$$

$$\Leftrightarrow \overline{A}^T - A = 0$$

$$\Leftrightarrow \mathrm{tr}\left[\overline{(\overline{A}^T - A)}^T \left(\overline{A}^T - A\right)\right] = 0$$

$$\Leftrightarrow \mathrm{tr}\left[(A^T - \overline{A})^T \left(\overline{A}^T - A\right)\right] = 0$$

$$\Leftrightarrow \mathrm{tr}\left(\mathrm{A}\overline{A}^T\right) - \mathrm{tr}\left[\left(\overline{A}^T\right)^2\right] - tr(A^2) + tr\left(\overline{A}^T A\right) = 0$$

$$\Leftrightarrow \mathrm{tr}(\mathrm{A}^2) = tr\left(\overline{A}^T A\right) = 0$$

$$\Leftrightarrow A^2 = \overline{A}^T A$$（这里要用到$\mathrm{tr}(\mathrm{A}^T\overline{\mathrm{A}} = \mathrm{tr}\left(\mathrm{A}\overline{A}^T\right)$）

因此，一个 n 级复矩阵 A 为共轭对称矩阵$\Leftrightarrow \mathrm{A}^2 = \overline{A}^T A$

四色问题——平凡问题中的复杂

不久前上映的《嫌疑人 X 的献身》里出现的四色问题一定给大家留下了很深刻的印象。那，我们一起来记录细节吧

定理概要

提出者

Francis Guthrie

提出时间

1852 年

应用学科

拓扑学、图论

适用领域范围

排程和分配问题，~~地图编辑~~

地图绘制并不需要四色定理：他只要着色，不需要用最少的颜色。实际画地图时一般不用四种颜色

四色问题又称四色猜想、四色定理，是世界近代三大数学猜想之一（世界三大数学猜想即费马猜想、*四色猜想*和哥德巴赫猜想）。地图四色定理（Four color theorem）最先是由一位叫古德里（Francis Guthrie）的英国大学生提出来的。

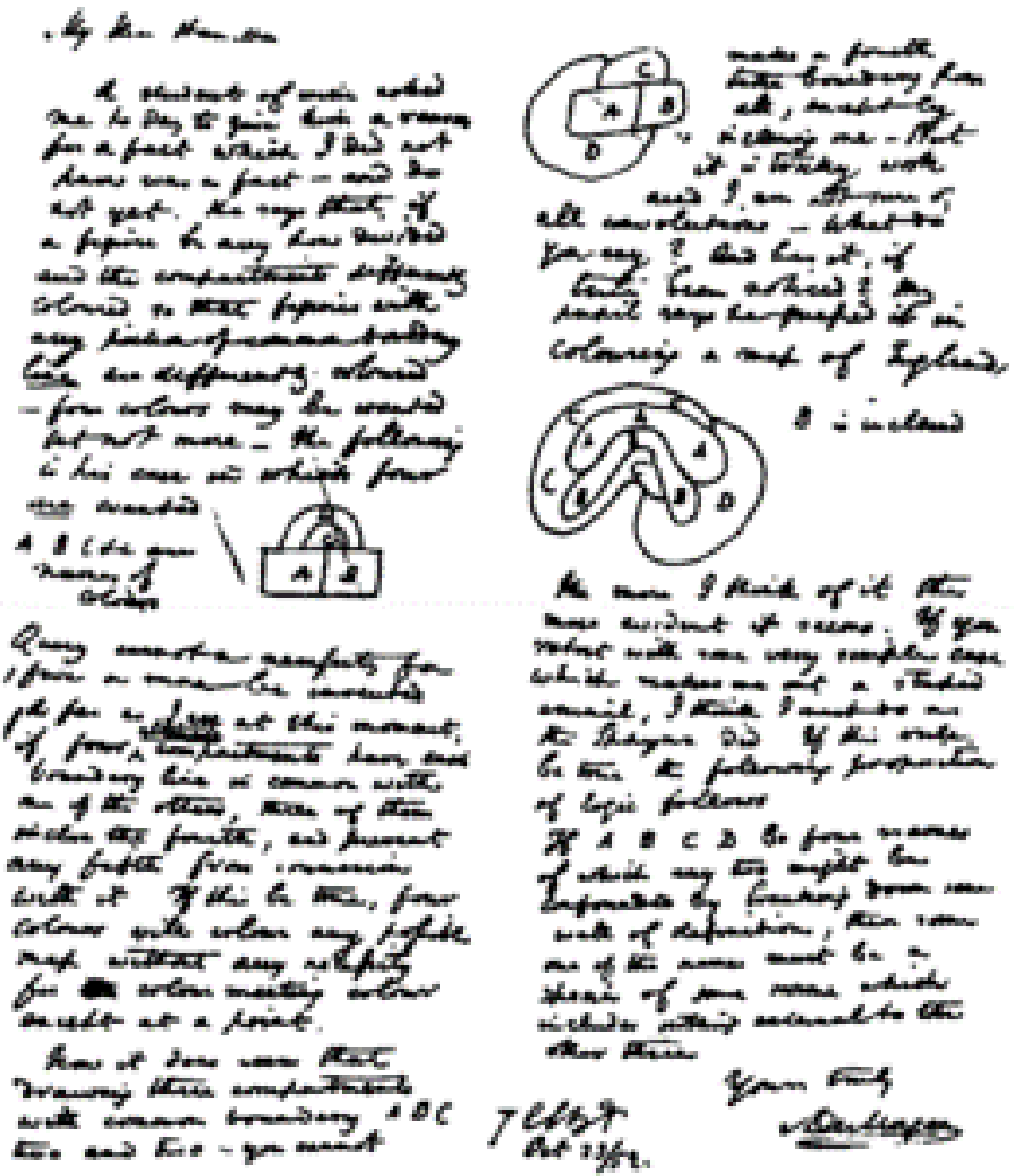
四色问题的内容是“任何一张地图只用四种颜色就能使具有共同边界的国家着上不同的颜色。”也就是说在不引起混淆的情况下一张地图只需四种颜色来标记就行。

用数学语言表示即“将平面任意地细分为不相重叠的区域，每一个区域总可以用 1234 这四个数字之一来标记而不会使相邻的两个区域得到相同的数字。”这里所指的相邻区域是指有一整段边界是公共的。如果两个区域只相遇于一点或有限多点就不叫相邻的。因为用相同的颜色给它们着色不会引起混淆。

发展简史

- **问题的提出**

1852 年，毕业于伦敦大学的格斯里（FrancisGuthrie）来到一家科研单位搞地图着色工作时，发现每幅地图都可以只用四种颜色着色。这个现象能不能从数学上加以严格证明呢？他和他正在读



大学的弟弟决心试一试，但是稿纸已经堆了一大叠，研究工作却是没有任何进展。

1852 年 10 月 23 日，他的弟弟就这个问题的证明请教了他的老师、著名数学家德·摩尔根，摩尔根也没有能找到解决这个问题的途径，于是写信向自己

的好友、著名数学家哈密顿爵士请教，但直到 1865 年哈密顿逝世为止，问题也没有能够解决。

1872 年，英国当时最著名的数学家凯利正式向伦敦数学学会提出了这个问题，于是四色猜想成了世界数学界关注的问题，世界上许多一流的数学家都纷纷参加了四色猜想的大会战。

从此，这个问题在一些人中间传来传去，当时，三等分角和化圆为方问题已在社会上“臭名昭著”，而“四色瘟疫”又悄悄地传播开来了。

• 肯普的研究

1878～1880 年两年间，著名的律师兼数学家肯普(Alfred Kempe)和泰勒(Peter Guthrie Tait)两人分别提交了证明四色猜想的论文，宣布证明了四色定理。

大家都认为四色猜想从此也就解决了，但其实肯普并没 v 有证明四色问题。11 年后，即 1890 年，在牛津大学就读的年仅 29 岁的赫伍德以自己的精确

计算指出了肯普在证明上的漏洞。他指出肯普说没有极小五色地图能有一国具有五个邻国的理由有破绽。不久泰勒的证明也被人们否定了。人们发现他们实际上证明了一个较弱的命题——五色定理。就是说对地图着色，用五种颜色就够了。

不过，让数学家感到欣慰的是，郝伍德没有彻底否定肯普论文的价值，运用肯普发明的方法，郝伍德证明了较弱的五色定理。这等于打了肯普一记闷棍，又将其表扬一番，总的来说是贬大于褒。真不知可怜的肯普律师是什么心情。 追根究底是数学家的本性。一方面，五种颜色已足够，另一方面，确实有例子表明三种颜色不够。那么四种颜色到底够不够呢？这就像一个淘金者，明明知道某处有许多金矿，结果却只挖出一块银子，你说他愿意就这样回去吗？

• 肯普的错误中的贡献

肯普是用归谬法来证明的，大意是如果有一张正规的五色地图，就会存在一张国数最少的“极小正

规五色地图”，如果极小正规五色地图中有一个国家的邻国数少于六个，就会存在一张国数较少的正规地图仍为五色的，这样一来就不会有极小五色地图的国数，也就不存在正规五色地图了。这样肯普就认为他已经证明了“四色问题”，但是后来人们发现他错了。

四色猜想在短短的两年时间里被一个并非“专业”数学家的“外行人”解决，让很多当初认为这个问题是难题的数学家觉得，这个问题也许并没有涉及到数学中深层的本质难点。对四色问题的研究逐渐减少，数学家们已经将其视为事实。刘易斯·卡罗尔将四色问题化为游戏：一方设计地图，另一方来为其着色。1886 年，英国男校克里夫顿学院（德语：Clifton College）校长将四色问题作为给全校学生挑战的难题，要求答案长度“不得超过一页纸的文字，30 行算式以及一页纸的图”。

德国数学家菲利克斯·克莱因甚至将这个问题和 1840 年莫比乌斯提出并解决的另一个问题相混淆

起来，认为四色问题不过是后者的直接推论。这个误解被几何学家理查德·巴尔策（德语：Heinrich Richard Baltzer）在 1885 年重复，导致直到 21 世纪仍有类似的传言。而实际上莫比乌斯解决的是完全图K_5，不是平面图的问题，与四色问题没有直接联系。

然而，在肯普的证明发表的 11 年之后，珀西·约翰·希伍德（英语：Percy John Heawood）发表一篇文章，指出肯普的证明中包含一个错误。希伍德在文章中遗憾地指出，他无法修正这个错误，以得到一个四色问题的正确证明，因此他的文章更多是摧毁而非建设（rather destructive than constructive）。不过，尽管无法得到四色定理，希伍德仍然在肯普的思路上前进，得到一个较弱的定理：五色定理。

根据希伍德的说明，肯普的错误在于证明 5 邻国是可约构形时，构造两条肯普链以换色，然而第二

次换色时，肯普的方法并不总是成功的。希伍德提供一个包含 25 个国家的地图作为反例。

希伍德的报告是由肯普自己提交给伦敦皇家数学学会的。肯普承认自己的证明中存在缺陷，并且他未能去除这个缺陷。然而希伍德的工作并没有受到应有的重视。数学界普遍认为这只是无关紧要的错误，很快就能得到纠正。1894 年创刊的《L'intermédiaire des mathématiciens》杂志以四色问题作为头一个征解问题，结果很快就收到解答，称其已被解决，并引用了肯普、泰特等人的论文。E. 吕卡的《娱乐数学》（Récréations mathématiques）第四卷提到肯普的证明，但丝毫没提到希伍德已经指出肯普证明的错处。

直到世纪之交时，数学家们仍旧认为，四色问题所需要的只是某个灵光一现的妙想。一个广为流传的故事是闵可夫斯基在教拓扑学课时提到四色问题，说："这个问题一直没有解决，只是因为试图解决它的都是三流的数学家"。他声称要在课上证明之，但

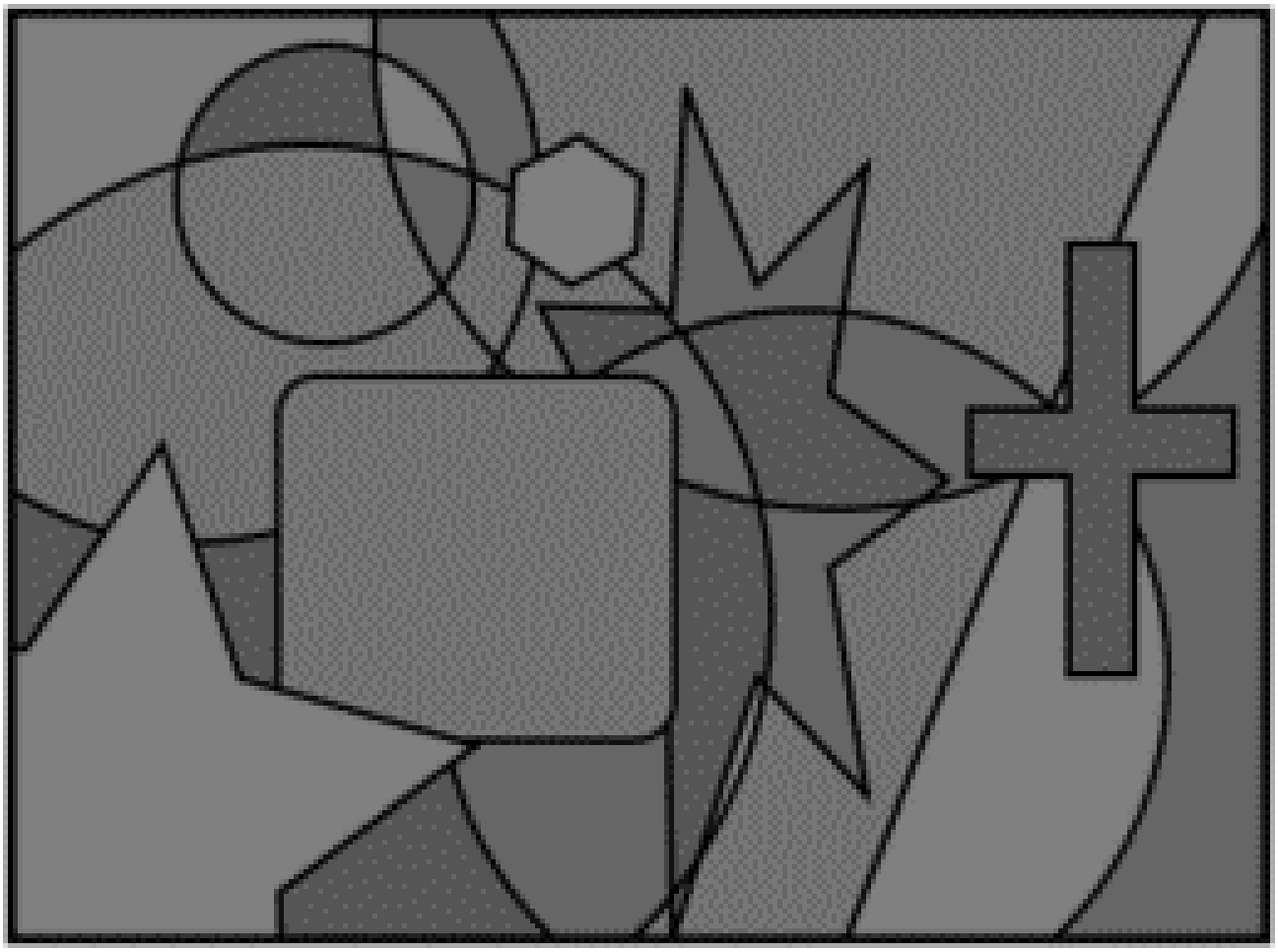
直到下课仍然无法成功，在耗费若干堂课的时间后，只能承认失败

不过肯普的证明阐明了两个重要的概念，对以后问题的解决提供了途径。**第一个概念是“构形”**。他证明了在每一张正规地图中至少有一国具有两个、三个、四个或五个邻国，不存在每个国家都有六个或更多个邻国的正规地图，也就是说，由两个邻国，三个邻国、四个或五个邻国组成的一组“构形”是不可避免的，每张地图至少含有这四种构形中的一个。

肯普提出的另一个概念是“可约”性。“可约”这个词的使用是来自肯普的论证。他证明了只要五色地图中有一国具有四个邻国，就会有国数减少的五色地图。自从引入“构形”，“可约”概念后，逐步发展了检查构形以决定是否可约的一些标准方法，能够寻求可约构形的不可避免组，是证明“四色问题”的重要依据。但要证明大的构形可约，需要检查大量的细节，这是相当复杂的。

• **缓慢的进展**

人们发现四色问题出人意料地异常困难，曾经有许多人发表四色问题的证明或反例，但都被证实是错误的。后来，越来越多的数学家虽然对此绞尽脑汁，但一无所获。于是，人们开始认识到，这个貌似容易的题目，其实是一个可与费马猜想相媲美的难题。　进入 20 世纪以来，科学家们对四色猜想的证明基本上是按照肯普的想法在进行。



四色定理的本质就是在平面或者球面无法构造有五个或者五个以上的两两相连的区域，如果有五个以上两两相连区域，第五个区域至少与一个区域同一种颜色。这个理论在其他构造中是显然的，例如在环面上（亏格为 1），需要 7 色，就是因为环面不能构造 8 个两两相连区域。在亏格为 2 的双环面上，需要 8 色，就是不能构造 9 个区域两两相连。

20 世纪起，欧洲数学界对四色定理的研究出现停滞。相反地，这个问题在美国得到更多的关注。不少杰出的数学家研究了这个问题，并作出很大贡献。一部分的努力是修正肯普的证明；另一方面的努力是延续泰特的思路，将四色问题进行转化，以使用更多有力的数学工具。

对四色问题的转化在泰特之后并未停止过。从拓扑学的版本转化至图染色的版本后，希伍德又在 1898 年提出新的变形。肯普和泰特已经注意到，证明四色问题只需要考虑三个国家有共同“交点”的情况，更多国家有共同交点的情形可以转化为前者。因

此这样对应的染色图中，每个顶点恰会连出三条边。这样的图被称为“三度图”（trivalent map）。希伍德观察到，如果三度图中任意由边围成的区域，边的个数都是 3 的倍数，那么图可以被 4-染色。他进一步发现，只要存在一种给图的顶点赋值+1 或-1 的方法，使得每个区域的顶点数字之和都被 3 整除，那么图可以被 4-染色。可以证明，4-染色和存在赋值方法是等价的。

在美国，数学家对四色定理的研究从未停止过。除了约翰·霍普金斯大学的皮尔斯以及斯多利等人外，另一个研究者是保罗·温尼克（英语：Paul Wernicke）。从当时的学术圣地哥廷根大学毕业的温尼克来到美国后在肯塔基大学任教。他 1904 年发表的论文中已经出现了可约性的雏形。然而美国数学界在四色问题上首次实质性的进展出现在 1912 年后。普林斯顿大学的奥斯瓦尔德·维布伦（经济学家托尔斯坦·范伯伦的侄子）是这波浪潮的先锋。他的工作重心是拓扑学，1905 年证明了若尔当曲线定理。对庞

加莱发展出的新代数工具有深入了解的他，很自然地开始对四色定理的研究。他使用有限几何学的观念和有限域上的关联矩阵（英语：incidence matrix）作为工具，将四色问题转化成有限域系数空间上的方程问题。这个方向被后来的密码学家、数学家威廉·托马斯·塔特（英语：William Thomas Tutte）称为“量化方法”（the quantitative method）。同年，他的普林斯顿同僚乔治·戴维·伯克霍夫也开始探索这个方向，但一年之后他开始转向肯普的方法，也即是塔特所称的“定性方法”（the qualitative method），并提出可约环（reducible ring）的概念。1913 年，伯克霍夫发表名为《地图的可约性》（The Reducibility of Maps）的论文，利用可约环证明了：由不超过 12 个国家构成的地图都能用四色染色。1922 年，伯克霍夫的学生菲利普·富兰克林（英语：Philip Franklin）运用同样的方法，将结论加强到：不超过 25 个国家构成的地图都能用四色染色。**由于别克霍夫首次证明四色定理对不超过 12**

个国家的地图成立，历史上证明的可染色地图的国家数上限记录被称为别克霍夫数。

伯克霍夫等人的证明是肯普的方法的延续和系统化，归纳为寻找一个不可避免的可约构形集（an unavoidable set of reducible configurations）。这个理念已经体现在肯普的证明中。他首先说明任一地图中必然存在以下四种构形：2 邻国国家、3 邻国国家、4 邻国国家和 5 邻国国家；然后证明每种构形都是可约构形。后来希尔将这种分类方式称为“不可避免集”。伯克霍夫的构想是使用反证法：反设存在至少需要五种颜色染色的地图，那么其中必然存在国家数最小的“极小五色地图”（five-chromatic map）。这个地图必然是“不可约的”（irreducible）。而只要找到一组构形，使极小五色地图中不可避免地会出现其中一种构形，并且每个构形都是可约的，那么就能够通过约化，将地图的国家数减少，从而导致矛盾

肯普找的不可避免集由四种构形组成，但他无法证明最后一种（5 邻国国家）的可约性，因此伯克霍夫开始寻找刻画不可避免集的新方法。他提出以相邻国家连成的环来将整个地图 M 分为三个部分：环内部分 A、环外部分 B 以及环本身 R。若环上的国家数为 n 就称其为 n-环。如果 R 的任意染色都不妨碍 A 进行染色，那么就可以“忽略”A 而将 M 的染色问题约化为 B+R 的染色问题。这时便称 A+R 是可约构形，R 称为可约环。伯克霍夫证明了：当 R 是 4-环，或者 R 是 5-环且 A 中国家不止一个，或者 A+R 是“伯克霍夫菱形”时，A+R 都是可约的构形。因此极小五色地图不可能包含这些构形。富兰克林进一步证明：极小五色地图中必定包含三个邻接的五边国（5 邻国的国家），或者邻接的两个五边国与一个六边国，或者邻接的一个五边国和两个六边国。他从而得出一系列的可约构形，形成了 25 国以下地图的不可避免的可约构形集。因此推出，极小五色地图必定至少包含 26 个国家

这种方法的终极目标是找到所有地图的不可避免的可约构形集。然而随着国家数增多，要找到不可避免集并证明其可约化性就越难。这主要是因为随着环的增大，染色的方法数目会迅速增大。6-环的 4-染色方法有 31 种，而 12-环则有 22144 种。因此对大环围成的构形验证可约性是十分繁杂的工作。1926 年，C.N.Reynolds 将别克霍夫数从 25 提高到 27。1938 年，富兰克林将其推进到 31。1941 年，C.E.Winn 将之提高到 35。而直到 1968 年，别克霍夫数才更新为 40

• 计算机证明

高速数字计算机的发明，促使更多数学家对“四色问题”的研究。电子计算机问世以后，由于演算速度迅速提高，加之人机对话的出现，大大加快了对四色猜想证明的进程。就在 1976 年 6 月，在美国伊利诺斯大学的两台不同的电子计算机上，用了 1200

个小时，作了 100 亿个判断，结果没有一张地图是需要五色的，最终证明了四色定理，轰动了世界。

> “如果四色问题有一个不依赖计算机的证明，我会更加开心，但我也愿意接受阿佩尔和哈肯的证明——谁叫我们别无选择呢？（I would be much happier with a computer-free proof of the four color problem, but I am willing to accept the Appel–Haken proof – beggars cannot be choosers.）”

这是一百多年来吸引许多数学家与数学爱好者的大事，当两位数学家将他们的研究成果发表的时候，当地的邮局在当天发出的所有邮件上都加盖了“四色足够”的特制邮戳，以庆祝这一难题获得解决。

四色定理是第一个主要由电脑验证成立的著名数学定理。这一证明刚开始并不被所有的数学家接受。1979 年，逻辑哲学和数学哲学家托马斯·蒂莫兹佐（英语：Thomas Tymoczko）在《四

色定理及其哲学意义》一文中提出，四色定理与其证明能否称之为“定理”和“证明”，尚有疑问。“证明”的定义也需要进行再次审视。蒂莫兹佐的理由包括两点：**一方面，计算机辅助下的证明无法由人力进行核查审阅，因为人无法重复计算机的所有运算步骤；另一方面，计算机辅助的证明无法形成逻辑上正则化的表述，因为其中的机器部分依赖于现实经验的反馈，无法转换为抽象的逻辑过程**。即便在数学界中，对四色定理证明的误解也存在着。有的数学家认为证明是杰出的进展，也有人认为依赖计算机给出的证明很难令人满意。也有人认为，计算机辅助证明数学定理不过是对人的能力进行延伸的结果，因为电子计算机不过是依照人的逻辑来进行每一步的操作，实际上只是将人能够完成的工作用更短的时间来完成。还有人将计算机辅助证明和传统证明的差别比喻为借助天文望远镜发现新星和用肉眼发现新星的区别。

针对证明过程冗长、难以理解的问题，哈肯等人也着手对证明进行改良。简化证明的一个方向是寻

找更小的不可避免集和更加容易验证的可约构形。哈肯等人很快将不可避免构形集的大小从 1936 个改进到 1476 个。1994 年，罗宾·托马斯等人又将其改进到只包含 633 个构形、32 个放电规则的放电过程推出的不可避免构形集。由于著名的前车之鉴，数学家们对证明进行详细审视，发现了大量缺漏和错误。特别是厄里奇·史密德等人曾经检查人工证明部分的 40%，并发现放电过程中的一个关键性错误。幸好，这些缺陷和错误都是能够修正的。不过，修正的工作也持续了若干年，才最终完成。修正过程中也出现各种传言，说四色定理的证明其实是错误的。1986 年，哈肯和阿佩尔应《数学情报（英语：Mathematical Intelligencer）》杂志的邀请写了一篇短文，用清晰易懂的语言总结他们的证明工作。1989 年，最终的定稿以单行本的形式出版，超过 400 页。

对于机器证明的可靠性问题，2004 年 9 月，数学家乔治·龚提尔（英语：Georges Gonthier）使用证明验证程序 Coq 来对当时交由计算机运算的算法程

序进行形式上的可靠性验证。证明验证程序是一个由法国开发的软件，能够从逻辑上验证一段电脑程序是否正常运行，并且是否达到了它应该达到的逻辑目的。验证表明，四色定理的机器验证程序确实有效地验证所有构形的可约性，完成了证明中的要求。至此，除了机器硬件、软件可能存在问题外，四色定理的理论部分和计算机证明算法部分都得到验证。（**本文末有相关论文链接**）

严格叙述

• 拓扑学阐述

最初的染色问题是用几何学的概念描述的。严谨的版本则需要用到拓扑学的概念来定义。设有一欧几里得平面或其一部分，将其划分为互不重叠的区域的集合。一个“地图”为以下划分方式

①将平面划分为有限个区域，使得任意两个区域的交集是空集，所有的区域的并集是整个平面；

②所有区域中，只有一个区域是无界区域，其余区域都是有界区域。

所谓有界区域，是指能够用一个长和宽都有限的矩形覆盖的区域。无界区域则是不能用这样的矩形覆盖的区域。每个区域相当于通俗说法中的“国家”，而区域之间的边界（“国家”之间的“国界线”）则定义为连续不自交的曲线，也称为连续简单曲线。连续简单曲线是指一个从$[0,\ 1]$映射到平面$\mathbf{R^2}$的连续函数 c 的像集：$C = \{C(t); t\epsilon[0,1]\}$，并且要满足：

任意

$$0 \leq t_1 < t_2 \leq 1$$

，只要不是

$$t_1 = 0, t_2 = 1$$

，就必定有$c(t_1) \neq c(t_2)$，这样说明曲线不与自身相交（没有“打结”的地方）。如果$c(0) \neq c(1)$，就称曲线为弧，否则称曲线为圈。可以看出，用边界定义地图更为本质：

平面$\boldsymbol{R^2}$中的一张地图是指有限个简单曲线的集合：

$\mathrm{L} = \{\mathrm{C}_1, \mathrm{C}_2 \ldots \mathrm{C}_m\}, m \in N, m \geq 2$，其中

$$\forall 1 \leq \mathrm{i} \leq \mathrm{m}, \mathrm{C}_i = \{\mathrm{c}_i(\mathrm{t}); \mathrm{t} \in [0,1]\}$$

，c_i 为$[0,1]$映射到$\mathbf{R^2}$的连续函数。并且任意$1 \leq \mathrm{i} < \mathrm{j} \leq \mathrm{m}$，曲线$\mathrm{C}_i$和$\mathrm{C}_j$要么没有交点（交集为空集），要么交点是两线的一个公共顶点$\mathrm{E}_{i,j} = c_i(\epsilon_1) = c_j(\epsilon_2)$，$\epsilon_1, \epsilon_2 \in \{0,1\}$。

L中每一条连续简单曲线称为地图的**边**。任意边的端点称为**顶点**。可以说，一张地图实际上是由一个简单有界平面图定义的。定义地图的边和顶点后，设所有属于边或顶点的点为**中性点**，其集合设为$\mathrm{N}_L = \{x; x \in C_i, 1 \leq i \leq m\}$，则 L将其余的点划分为若干个道路连通的开集。用拓扑学的语言来说，每个“国家”是$\mathrm{R}^2 - N_L$的一个极大连通子集。或者说，取一个非中性点x，所有能够从x，经过一条不含中性点的弧到达的点构成的集合，就是一个国家。这样定义的国

家必然满足之前所说的特性，只有一个无界国家。要注意的是这里定义的国家必然是没有飞地的。

最后可以定义染色。假设将使用到的颜色编号为1,2,3 …, n号颜色，为地图染色是指一个将地图中的国家映射到{1,2,3, …, n}上的函数。一个可行的 n-染色方案是指使得相邻的国家对应的颜色不同的函数。四色定理说明：每个地图都存在可行的 4-染色方案。

- **图论阐述**

拓扑学版本的四色问题阐述可以转化为更为抽象的图论版本。这里的转化指的是一种对偶的概念。即将一个地图转化为图论中的一个无向平面图。具体来说，是将地图中的每一个国家用其内部的一个点代表，作为一个顶点。如果两个国家相邻，就在两个顶点之间连一条线。这样得到的图必然是一个平面图（不会有两条边相交），而与每个国家选取的代表点无关。四色定理可以叙述为：必然可以用四种颜色给平面图的顶点染色，使得相连的顶点颜色不同。

要注意的是，并非所有的地图都可以转化为图论中的平面图。如果一个国家有飞地的话，就不能用只一个点来代表一个国家。另外，如果一个国家是“国中国”，那么即便可以地图其转化为平面图，也会造成讨论上的不便。但是，“国中国”的着色十分容易解决，因为它只有一个邻国，只需将它染成和邻国不一样的颜色就可以。所以在大部分有关四色问题的讨论中可以忽略“国中国”的情形。同样地，只有两个邻国的情形也可以被忽略。如果规定不能够有四个或者以上的国家有公共边界，那么地图转化成的平面图里面，每个区域都是至多由三条边围成的。这样的地图被称为正规地图。如果任何一个顶点都连出三条边，那么就称其为“三度图”（trivalent map）。可以证明，如果存在四色定理的反例，那么国家数最少的反例必定是三度图。因此在四色问题的证明过程中，常常会假设地图对应的图是三度图

*文章部分资料引用自维基百科

扫描二维码下载 Georges Gonthier 在计算机软件 Coq 的帮助下找到四色定理形式证明（pdf 格式）

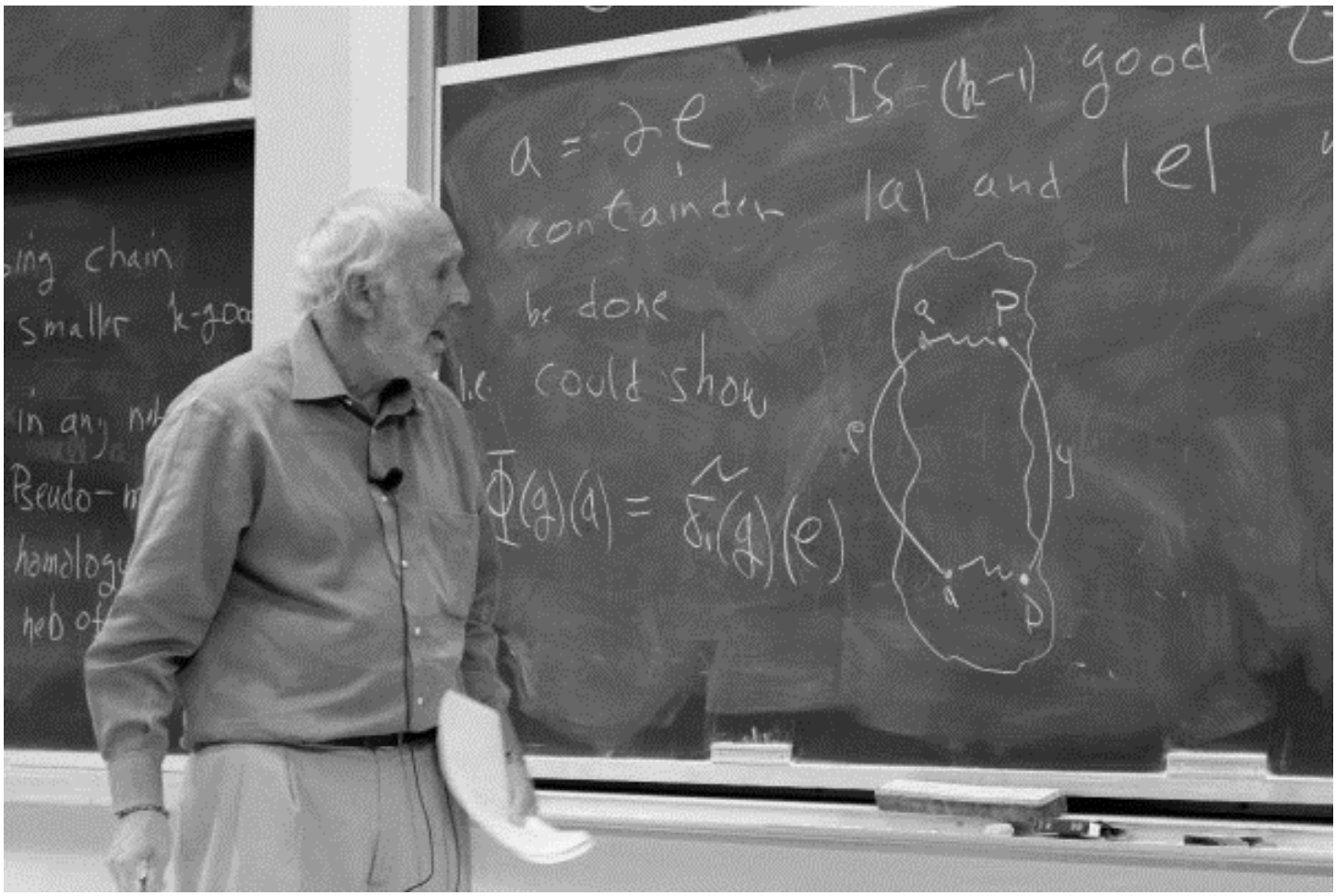
西蒙斯和有用的数学

有人说数学是所有自然科学的基石，没有数学就不会有人类的灿烂科技。可是现实中的数学总是伴随着非议，学生们的声音尤其尖锐。几年前，在微博上有一个热门话题，就赤裸裸地叫做**“数学滚出高考”**。有调查显示，超过 7 成网友投出了赞成票，他们觉得学数学就是浪费生命。也许有人觉得，数学除了那些科学家搞搞研究外，对大众根本没有意义。学好数学最多让人成为一个“书呆子”，什么

微积分、几何、概率论根本百无一用。然而，这世界上就是有这么个例子，他的存在让你黑数学的行为显得极度的无知。

每当你对数学充满了憎恨和挫败时，他又总会跳出来“教你做人”，告诉你数学究竟怎么用。

他 23 岁就拿下加州大学伯克利分校的数学博士学位。30 岁就成为了数学系主任，一手振兴纽约州立大学石溪分校的数学专业。另外，他还跟著名华裔数学家陈省身合作创立了**陈-西蒙斯理论**，还获得了五年一届的**几何学最高奖维布伦奖**。后来又**“提点”了好基友杨振宁**，帮他解决了很多数学上的细节问题。这才让杨振宁毫无



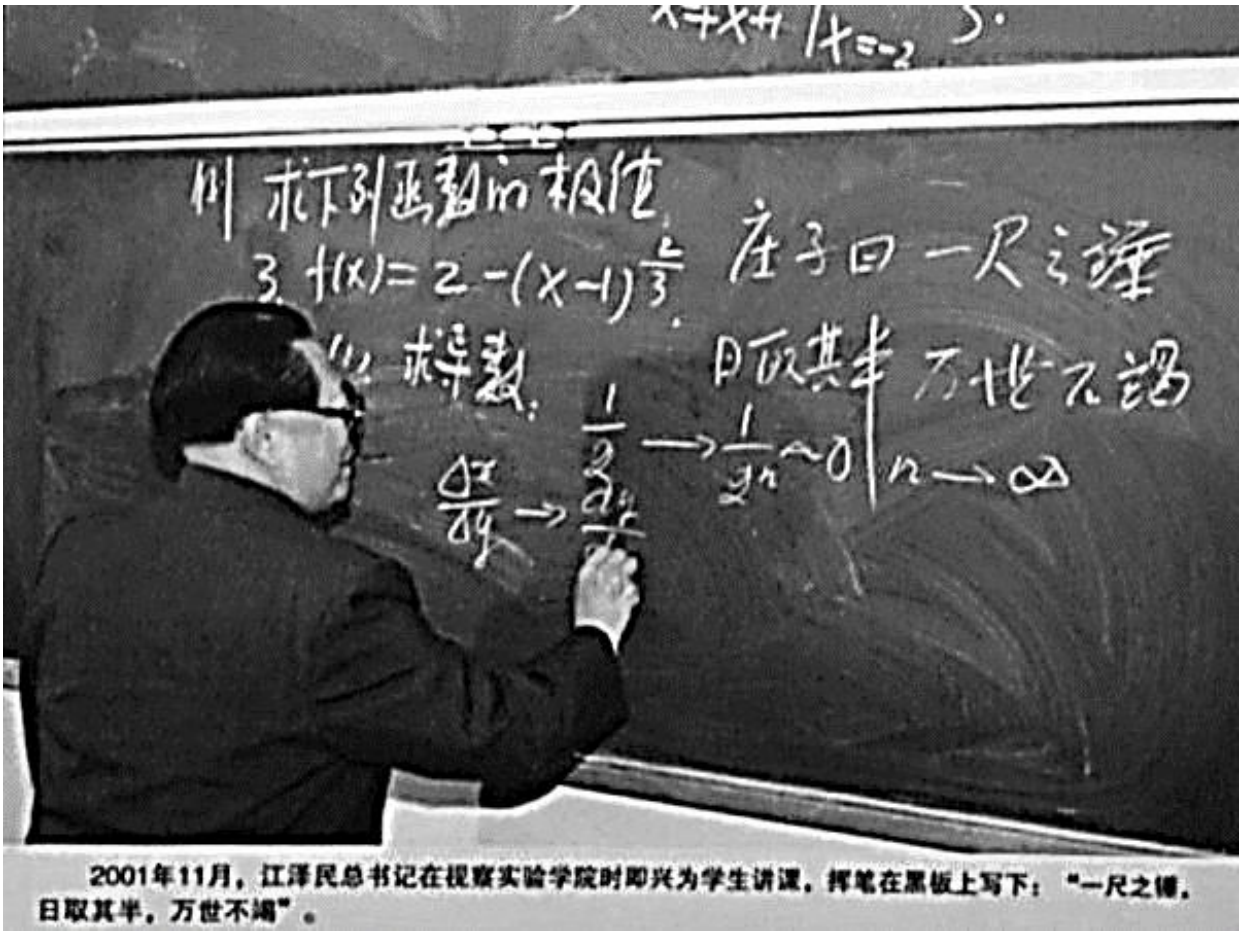
障碍地完善著名的**“杨-米尔斯理论”**。他靠着一套神秘的数学模型，不依靠任何金融界的“老江湖”，成为了世界上最能赚钱的基金经理。**他的基金成立 20 多年来，几乎未亏损，平均年回报率高达 35%，什么“股神”、“大鳄”都不放在眼里。他用实际行动告诉世界，学好数学，吊打巴菲特，索罗斯不是梦。**

在美国马萨诸塞州，有一家名不见经传的鞋厂，老板是个犹太人。他每天疲于生意上的奔波，生活无趣且乏味。儿子詹姆斯·西蒙斯的降生让他又喜又惊。自己唯一的儿子似乎聪明绝顶，以至于让他怀疑起了隔壁的老王。

果不其然，童年的西蒙斯就表现出了非凡的数学天赋。他偶然间想到一个充满哲学意味的问题：**如果油箱里的汽油每次只用一半，那是不是永远用不完呢？**这个问题在西方被称作芝诺悖论，在东方我们常说**“日取其半，万世不竭”**。

西蒙斯少年老成，高中毕业后考入麻省理工学院，仅仅一年就达到了毕业生的水平。20 岁拿到了学士学位，23 岁又在加州大学伯克利分校拿到博士学位。

可好戏才刚刚开始，西蒙斯博士的跌宕人生大戏正



2001年11月，江泽民总书记在视察实验学院时即兴为学生讲课，挥笔在黑板上写下："一尺之锤，日取其半，万世不竭"。

式开演。

毕业后，他阴差阳错地被美国国家安全局（就是监控全球的那个）召入麾下，成为了一名密码破译工作者。那段时间，西蒙斯拿着国家的高薪水，还能腾出一半的工作时间搞搞数学研究。简直就是中国人最向往的公务员生活，他自然也很享受。结果没做两三年，西蒙斯心血来潮耿直地在时代周刊的采访上怒斥

一位退役的陆军上将。责他为美军介入越南战争辩护，顺带黑了一把美军。

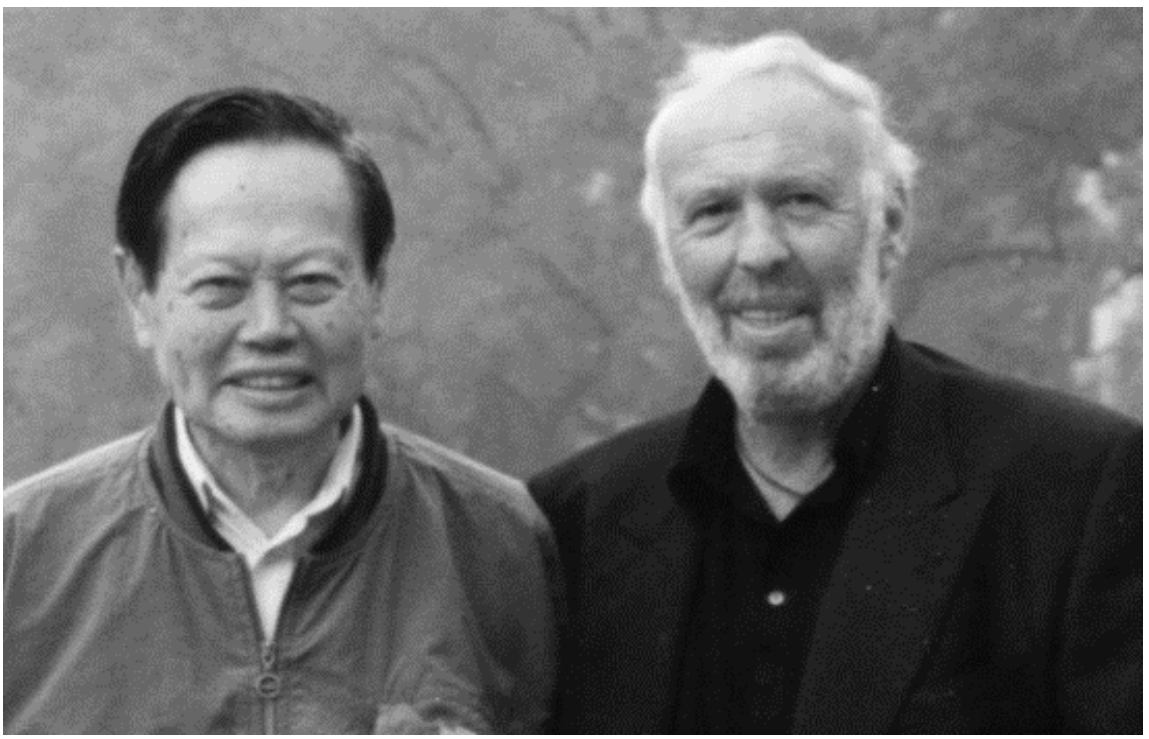
图：青年西蒙斯

他没想到的是，这位陆军上将正是他所在情报机构的顶头上司。当面跟老板互怼，没有丝毫政治觉悟，不炒你炒谁？一不留神丢了金饭碗，西蒙斯有些挫败，心想：既然吃不了皇粮，那就重新搞搞科研吧。那个年代，他一个数学博士在学校混口饭吃还是没什么压力的。于是，西蒙斯来到了纽约州立大学石溪分校，上来就想应聘数学系的主任。没想到教务长不但爽快地答应了，还流露出一丝邪魅的笑容。直到西蒙斯签下了聘书，教务长这才握住他的双手，语重心长地说：“西蒙斯啊，我很感激

你，你是我们这个系里唯一 一个真的想要这份工作的。”

全世界都以为西蒙斯被坑了，但是人家可不这么想。西蒙斯在石溪分校做科研一做就是 8 年，这 8 年里发生了很多事。**不仅把年轻的数学系硬生生地搞起来，成了全美的数学圣地，还搞了两个大新闻。**

一个是和中国著名的数学家陈省身先生合作，发表了论文《典型群和几何不变式》。创立了**陈-西蒙斯**理论，如今被广泛应用到数学、物理等各个领域。两年后西蒙斯因此获得了几何学的最高奖**——5 年颁发一次的维布伦奖**。另一个是结识了当时同样在纽约州立大学石溪分校工作的杨振宁。好基友杨振宁其实很欣



赏西蒙斯，常常邀请他到自己的办公室给他讲讲物理。杨振宁当时是什么人物啊，已经是物理学的大牛、诺贝尔奖的得主了。西蒙斯虽然对物理学一窍不通，但是出于对朋友的尊敬还是会前来欣赏杨振宁的“天书”。

西蒙斯整整听杨振宁讲了 3 年，竟也渐渐看懂了一些。他发现杨振宁这三年一直卡在一些其实已经被解决了的数学问题上，没有什么进展。**经过西蒙斯的提点，好基友杨振宁终于扫清数学上的障碍，完善了伟大的杨-米尔斯理论。杨振宁还为此专门发表过一篇文章感谢西蒙斯。**西蒙斯和杨振宁两人的丰功伟绩是石溪分院的骄傲。到现在其几何学和物理学机构都还

是叫**“杨振宁理论物理研究所”**和**“西蒙斯几何物理中心”**。

拿了几何学最高奖，又在物理学上插了一手，西蒙斯在学术界已经没什么可以留念的了。他问陈省身：**你说我是到政界守护 GDP 好呢？还是去华尔街搞搞金融好呢？**陈省身还是建议他别去政界搅浑水了，就凭他那点政治觉悟，搞不好连命都保不住。西蒙斯一想也觉得很有道理，那就去华尔街玩玩吧。

说话间，西蒙斯就成立了自己的第一家投资公司，正式下海。

前十年里，西蒙斯按照传统的方式运作他的对冲基金。每天都根据最新的消息以自己的经验和眼光决断，频繁地调整决策。

> **“对冲，是一种降低部分风险的投资方式，往往指两笔走势相关联，但方向相反的交易。一个简化的例子就是防晒霜与雨伞，不论天气晴或雨，两者的需求量有变化，但总量大致不变，虽然降低了收益，但也规避了部分的风险。**

虽然有赚有赔，但靠着灵光的脑子总体还是有些盈利，只是心理压力实在太大。哪天自己老了，想不过来了，很有可能从人生赢家变成抠脚屌丝。西蒙斯想，这样下去不是办法啊，有没有什么手段可以让他躺着就能赚钱？于是他想到自己的老本行数学，这些看似随机的价格走势背后一定有数学规律可循！不过很遗憾，西蒙斯所研究的微分几何，拓扑学似乎帮不上什么。可是人家有人脉啊，数学界扛把子不是白当的，挖几个专家还是轻而易举的。

他重新成立了基金公司，起名“文艺复兴科技”，从社会各界挖来了一大票程序员、数学家、密码学家等等等等。

西蒙斯打算让这些专家建立一个能反映现实价格走势的数学模型。用数学模型捕捉市场机会，由计算机自行决策交易，还起名为“大奖章基金”（指的就是他的维布伦奖章）。

新公司蓄势待发，可令人惊讶的是这里面没有什么搞金融的专家。华尔街看西蒙斯的公司简直就像是看笑话一样，甚至都开盘赌他几年倒闭了。然而，西蒙斯的新公司还真的就不行了，第一年只盈利了不到

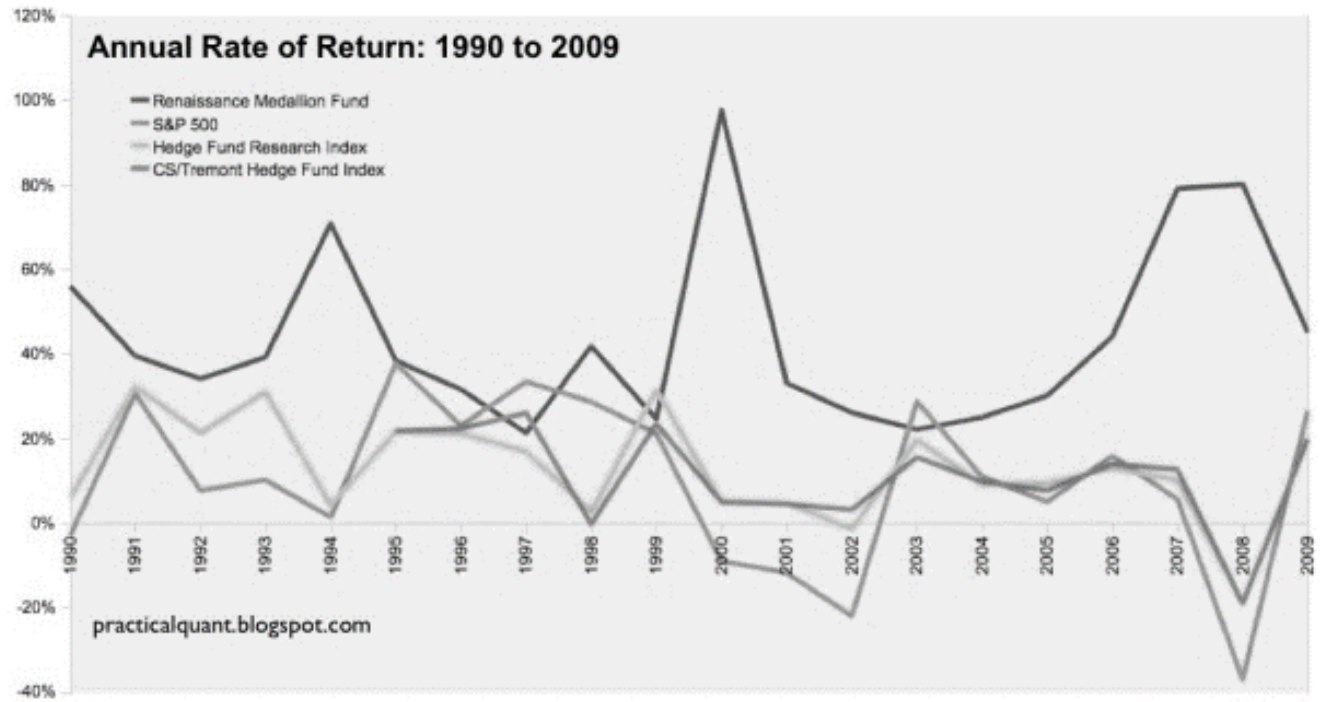
10%，聊胜于无。第二年直接就大亏 30%，吓得西蒙斯赶紧叫停整改。

西蒙斯又请来了一位数学大师亨利·劳佛对模型进行优化。经过半年的冥思苦想，两人做出了一个艰难的决定，放弃模型中的宏观数据，专注于短线交易。这下可算是找对了路子，大奖章基金重启的第一年就大赚了 55.9%。

之后的 20 年里，大奖章基金从未亏损过，堪称金融界的一大奇迹。

即使在最不景气的 2008 年，大盘下跌超过 30%的情况下，大奖章基金竟然还大赚了 80%！

大奖章年均 35%的回报率，吊打“金融大鳄”索罗斯和“股神”巴菲特 10 余个百分点。



图：从 1990 年开始，大奖章基金就没亏损过

西蒙斯也靠他的大奖章基金成为了全球收入最高的对冲基金经理。叱咤金融界 20 余年，西蒙斯又玩腻了，从掌门人的位置上退了下来，去搞慈善了。

西蒙斯就是能在涉足的领域里混风生水起，然后挥一挥衣袖，留下一段传奇。

其实他的存在就一个很好的例子，但并不只是证明学好数学究竟有多重要。而是证明，就算数学滚出了高考界，改考打游戏，能考高分的可能还是原来的那帮人。**数学只是众多人生战场中的一个，就算换再多的战场也不意味着能改变什么。**

文章来自 SME 情报员 在知乎专栏发表的文章《他拿几何学最高奖、提点杨振宁，转行玩金融却还能“吊打”巴菲特》

本文已由《数说》期刊获得作者授权发表，如需转载请联系原作者。

征稿启事

《数说》，由数学与统计学院科学技术协会主办的数学知识性期刊，每两月发行一期，旨在提升同学们的数学素养，培养同学们的数学兴趣，开拓大家的视野，使大家对数学有着更深的理解与热爱。

本期刊由数院科协期刊部负责编辑整理，由黄永忠与王湘君两位老师负责审稿，我们严肃的态度，保证对每一份来稿文件严谨的对待。

同时，我们会根据稿件质量，适当给予稿酬。

如果你对课内的知识有一些感悟，无论是解题技巧，亦或回首前面的课程有了新的收获想要向大家分享，我们愿意作为一个平台，记录并分享你的感悟。

如果你最近看了一本书，当然，得与数学相关喔。你的读后有感，我们愿意倾听，你的收获与疑问，我们愿意与你交流。在交流后，或许我们可以在期刊上将它分享给更多热爱数学的人。

如果你认为读过或是写过的学术论文对热爱数学，正在学习数学的同学有帮助，愿意推荐分享给他们，也可以向我们推荐。

当然，相较于推荐一些内容，我们更愿意看到各位同学与老师的原创内容，如果在原创内容中你引用

了其他资料，请别忘了标明出处哟。

同时，我们也接受与数学领域相交汇的内容，比如计算机，物理等学科的投稿，如果能够对数学知识提供一定得理解帮助或是应用推广，还会被采纳喔。

除了一些感悟，如果在学习过程中，你遇到了一些问题，或是在思考过程中有些内容难以理解，也可以整理之后向我们投稿，我们将对这些问题进行处理总结，在期刊栏目中提供我们的思路。

投稿地址及稿酬咨询：hustmaths@163.com

如果对我们的期刊有什么期望或是一些改进意见，也可以通过此地址向我们表达你的意见，我们会不断改正，不断进步。

谨代表《数说》期刊部欢迎您的来稿。