主编/李芸 编辑/温新红 校对/何工劳 Tel:(010)62580617 E-mail:news@stimes.cn

成就现代科学技术的数学

——从手机背后的数学谈起

■ 宗传明

近年来，在国家重视和媒体宣传下，人们已经形成了“数学很重要”的共识。人们认识到数学在科学技术的每一个分支和环节都发挥着重要作用。很难想象没有数学支撑的天文学和物理学会是什么样子，更难想象没有数学保障的航空航天技术会怎样。

其实，在国家大力提倡原始创新并寻求突破“卡脖子”技术的今天，我们更应当认识到数学在现代科学技术中不只是配角，在某些最关键的科技进程中还起了决定性的作用。

以我们最熟悉的高科技产品智能手机为例。手机是带通信功能的微型电脑，它的智能是由阿兰·图灵和约翰·冯·诺伊曼等数学家设计赋予的，它的通信功能是由克劳德·香农的信息论、诺伯特·维纳的控制论和现代密码学保障的。而计算机、信息论、控制论和现代密码学的诞生和发展都是由数学奠基主导的。

计算机的诞生

电子计算机是上世纪最伟大的一项发明。它不仅给科学技术的每一个领域都带来了翻天覆地的变化，更是改善了每个人的日常生活，甚至改变了我们的思维方式并且深刻影响到人类文明未来的发展。

自从远古时期以来，人们就不断探索发明高效的计算工具以延伸我们解决问题的能力：3000多年前，人们发明了算盘；400多年前，英国数学家约翰·纳皮尔发明了对数，在此基础上人们制造出了计算尺；1642年，法国数学家布莱士·帕斯卡制造出了可以进行加减运算的算术机；1671年，德国数学家戈特弗里德·威廉·莱布尼兹制造出了可以进行乘除运算的乘法机；1833年前后，英国数学家查尔斯·巴贝奇分别设计制造了可执行运算程序的差分机和分析机。

在电子计算机的早期发展过程中，许多科学家和工程师做出了杰出的贡献：1930年，美国科学家范内瓦·布什在麻省理工学院建造了最早的模拟机；1936年，英国数学家阿兰·图灵在数理逻辑（数学的一个分支）的基础上提出了计算机的理论构架，不仅肯定计算机的计算功能，而且赋予它逻辑推理的使命；1940年前后，德国工程师康拉德·楚泽提出了计算机程序控制的概念并独立建造了模型机；1945年，美国数学家约翰·冯·诺伊曼根据大脑的记忆功能提出了具有存储程序的电子计算机方案。

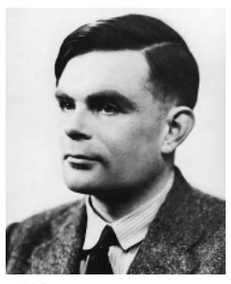
在这些先驱探索的基础上，电子计算机得以在1945年前后在英国和美国诞生并迅速发展。

阿兰·图灵1912年生于伦敦。1931年他考入剑桥大学国王学院学习数学，深受数理逻辑学家库尔特·哥德尔、阿隆佐·邱奇和戴维·希尔伯特的影响。1936年他发表了《论数字计算在决断难题中的应用》。该论文描述了一种可以辅助数学研究的机器，后来被人们称为图灵机。这个设想首次赋予机器进行符号逻辑推理的使命，为后来计算机和人工智能的产生和发展奠定了基础。

1938年，图灵在邱奇的指导下获普林斯顿大学数学博士学位。二战期间，他应召到英国情报中心布莱切利公园从事破译德军密码的工作。他领导了世界上最早的电子计算机的研制工作并成功破译了德军的密码。战后一段时间，图灵一直参与领导英国在曼彻斯特大学的电子计算机研制工作。1966年，为纪念他对计算机科学的奠基性工作，美国计算机协会（ACM）设立了阿兰·图灵奖。

约翰·冯·诺伊曼1903年生于匈牙利首都布达佩斯。1926年，他在利奥珀德·费耶的指导下获得布达佩斯大学数学博士学位。随后，他到德国哥廷根大学担任数学家希尔伯特的助手，深受其数理逻辑理论的影响。1930年，他移民美国，历任普林斯顿大学数学教授、普林斯顿高等研究院数学教授。基于数理逻辑理论，他开始研究计算机的建造。1945年，他提出了一个能存储程序的电子计算机方案，具体介绍了制造电子计算机和程序设计的思想。这一方案确定计算机由五个部分组成：运算器、控制器、存储器、输入和输出设备。

约翰·冯·诺伊曼



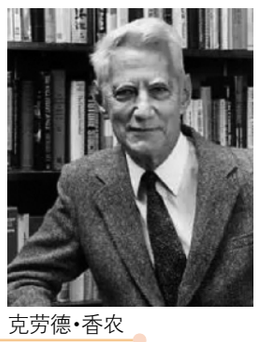
阿兰·图灵

1999年，为纪念他对计算机科学的奠基性工作，美国电气与电子工程师协会（IEEE）设立了约翰·冯·诺伊曼奖。

近100年来，随着科学技术的高速发展，电子计算机已从最初的电子管数字机逐步发展成为晶体管数字机、集成电路数字机，直到今天的大规模集成电路计算机。操作系统也发生了翻天覆地的变化。但是，无论硬件和软件怎么发展，计算机一直沿用图灵和冯·诺伊曼的设计思想。

信息论的诞生

自从有人类活动以来，人们就要面对信息可靠传递的问题：手势、声音、文字、电报、电话、互联网，等等。



克劳德·香农

1837年，英国发明家查尔斯·惠斯通、威廉·库克和美国发明家塞缪尔·莫尔斯几乎同时发明了电报。1860年和1876年，意大利发明家安东尼奥·穆齐和美国发明家亚历山大·贝尔分别制造出了电话。1895年，意大利发明家伽利尔摩·马可尼首次成功收发了无线电报。

这些新技术为大规模远距离信息传输提供了手段，但又迎来了如何保障准确、高效的传输的挑战。1924年，贝尔实验室的科学家哈利·奈奎斯特开始研究影响电报传输速度的因素，首次对信息传输速度给出了定量刻画。1928年，同在贝尔实验室的拉尔夫·哈特利更进一步定量研究了通信系统传输信息的能力，并试图度量系统的信道容量。

在奈奎斯特和哈特利的工作基础上，1948年克劳德·香农发表了划时代的论文《通信的数学理论》，从而宣告信息论的诞生。这篇论文和他于1949年发表的另一篇论文一起奠定了现代信息论的基础。香农的工作首次在概率统计和几何空间基础上为通信过程建立了数学模型，并通过数学模型推导出一些最重要的量化原理（即信息论三大定理）。这些模型和原理不仅引导了信息论的理论研究，也保障了通信工程技术的各个环节。

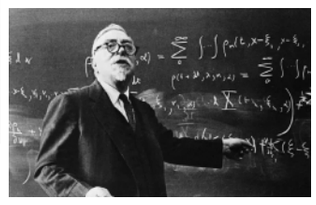
克劳德·香农1916年生于美国密歇根州。他于1940年在弗兰克·希区柯克指导下获得麻省理工学院数学博士学位。1941年他加入贝尔实验室数学部，工作到1972年。自1956年起他同时兼任麻省理工学院教授，1978年成为名誉教授。1972年，为纪念他对信息论的奠基性贡献，IEEE信息论学会设立了克劳德·香农奖。

近一个世纪过去了，随着计算机技术的飞速发展，信息通信已通过手机和互联网成为每个人日常生活的一部分。在这一发展过程中，组合数学、图论、数论等数学学科多次起到极其关键的作用，如纠错码和极化码，许多著名数学家也做出了杰出的贡献。

控制论的诞生

控制论的诞生也是20世纪最伟大的科学成就之一。控制论是数学、计算机技术、无线电通信、神经生理学、语言等多学科相互交叉的产物。它以各类系统所共同具有的通信和控制方面的特征为对象，研究它们根据周围环境的某些变化来调整自己运动的规律。

自动控制的想法由来已久。1760年前后，詹姆斯·瓦特曾在他的蒸汽机上安装一个调速器以自动调节蒸汽机的运行速度。1858年，阿弗雷德·华莱士对此做了研究和解释。1868年，著名物理学家和数学家詹姆斯·麦克斯韦研究了自动调速器，首次从理论上探讨这种自我调节装置。1927年，贝尔实验室的工程师哈罗德·布莱克开始探索利用负反馈的信息控制放大器。1932年，奈奎斯特发现了负反馈放大器的稳定性条件。1943年，阿图罗·罗森布鲁斯、诺伯特·维纳和朱利安·毕格罗利用数学模型研究了利用反馈信息的控制问题。1945年，维纳把反馈概念推广到一般控制系统，把反馈理解为从受控对象的输出中提取一部分信息作为下一步输入，从而对再输出发生影响的过程。



诺伯特·维纳

1948年，诺伯特·维纳出版了著名的《控制论——或关于在动物和机器中控制和通信的科学》一书，标志着控制论作为一门学科的诞生。维纳把控制论看作是一门研究机器、生命社会中控制和通信的一般规律的科学。更具体地说，是研究动态系统在变化的环境条件下如何保持平衡状态或稳定状态的科学。

控制的基础是信息，一切信息传递都是为了控制，而任何控制又都有赖于信息反馈来实现，在微分方程、最优化、概率统计、模糊数学的基础上建立数学模型进行量化研究。

诺伯特·维纳1894年生于美国密苏里州。1913年，他在卡尔·施密特和乔西亚·罗伊斯的指导下获哈佛大学数学博士学位。随后，他先后游学于英国剑桥大学和德国哥廷根大学，在伯特兰·罗素、高德菲尔·哈代、希尔伯特等著名数学家指导下研究数学。此后，他一直在麻省理工学院任教。1935年8月至1936年5月，他曾在清华大学讲授数学，对华罗庚有极大影响和帮助。1967年，为纪念他对控制论的奠基性贡献，美国工业和应用数学学会（SIAM）设立了诺伯特·维纳奖。

自从维纳创立控制论以来，冯·诺伊曼、列夫·庞特里亚金、贾奎斯·利昂斯等杰出数学家进一步开拓完善了这一理论。

如今，控制论已广泛应用于航空航天、机器人系统、人工智能等高科技产业。不夸张地说，如果没有控制理论就没有今天的航空航天成就。

数学奠定现代密码学的基础

1969年，互联网在美国西部诞生。这些计算机网络以一组通用的协议相连，形成逻辑上统一的计算机体系。使用互联网可以将信息瞬间发送到数千公里之外，它是信息社会的基础。

赫尔曼（左）和迪菲

李维斯特（左）、沙米尔（中）和阿德曼

随着信息时代的到来，信息安全成为一个突出问题。在军事通信中，敌方总是希望截获并破译对方的通信指令。二战期间，密码曾经是某些战争胜负的决定因素，例如西西里登陆、阿拉曼战役、中途岛海战和击落山本五十六大将的座机。在普通通信中，从高级黑客到低级诈骗犯都想窃取别人的信息。所以，现代密码学应运而生。

1976年，美国密码学家惠特菲尔德·迪菲和马丁·赫尔曼提出了公开密钥密码体制的思想。

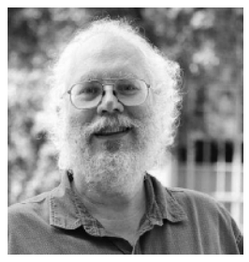
该体制不同于传统的密码体制，它要求密钥成对出现，一个为加密密钥（公钥），另一个为解密密钥（私钥），且不能从公钥推导出私钥。这样，即便窃密方知道加密的密钥也难以破解密码。由于这一革命性的方案，迪菲和赫尔曼荣获2015年度图灵奖。

1977年，麻省理工学院的三位数学家罗纳德·李维斯特、阿迪·沙米尔和莱纳德·阿德曼基于数学中的大整数分解问题首次实现了这一思想，提出了RSA加密方案。

早在古希腊时期，欧几里得就已经证明，每一个正整数都可以被唯一地分解为素数的乘积。但是，当整数很大时，如何找到具体的分解方式却是一个非常困难的数学问题。正是因为这一问题的复杂性，RSA密码体系的安全性才得以保障。由于这一方案，李维斯特、沙米尔和阿德曼荣获2002年度图灵奖。

自1976年以来，数学家和密码学家又建立了多种基于基础数学困难问题的密码体系。例如，基于离散对数的加密体系、基于椭圆曲线的加密体系，等等。这些密码体系的应用极大地推动了信息科学和产业的发展，为网络时代的信息安全提供了保障。从此，原本被认为“无用”的基础数学直接进入了高技术的最核心领域。

数学护航量子科技



彼得·绍尔

作者供图

近30年来，量子科学与技术得到了飞速的发展。尽管还在实验探索阶段，但量子计算机已被广泛地认为是下一次技术革命的发动机。在量子计算机时代，计算机的智能性和计算速度将极大地提高。这将给许多科学问题的解决带来希望和曙光。

1994年，美国贝尔实验室的数学家彼得·绍尔提出了量子算法，并应用于密码学。他的工作表明在量子计算机时代，基于整数分解的公钥密码体系将被攻破。也就是说，RSA密码体系在量子攻击下将不再安全。绍尔于1985年在麻省理工学院获数学博士学位，是当代享誉世界的数学家。

在绍尔的先驱工作基础上，人们进一步证明，在量子计算机时代，基于离散对数的密码体系和基于椭圆曲线的密码体系等多种广泛应用的密码体系都将被攻破。量子科学给现行的实用密码体系带来了严峻的挑战和危机。

早在1840年，伟大的数学家弗里德里希·高斯提出了格的概念。近两百年过去了，在许多数学家的努力下，格理论发展成为一个重要的数学分支。

1996年，美国数学家米克劳斯·阿杰泰在格理论的基础上构建了一套密码加密体系。阿杰泰于1976年在匈牙利布达佩斯大学获数学博士学位，自1991年起在美国IBM研究院工作。20多年过去了，人们至今没有找到攻破这一密码体系的量子算法。

密码学家普遍认为，格密码体系是能够抵抗量子算法攻击的。与此同时，人们也在不断地探索新的抗量子攻击的密码体系，为量子时代的科技护航。

科学技术的发展是无止境的。在不友好的国际环境下，落后就会挨打。所以，我们必须认清科技创新的源头，布局人才、埋头苦干，以求抢占先机。在过去的一个世纪中，数学已经证明它在科技革命中不可替代的智能作用。在未来的科技革命中，数学也一定不会缺席。

（作者系天津大学讲席教授）

“地球的皮肤”该如何保养

■ 荆淮侨 本报记者 李芸

对于人类而言，土壤是和阳光、空气、水一样重要的存在。但是，在很多人眼里，土壤又是司空见惯、没有什么“存在感”的。

在中科院南京土壤研究所（以下简称南土所）研究员张甘霖看来，作为覆盖在地球表面的一层有生命的疏松物质，土壤像皮肤一样维持着陆地生命的存续。

可是，我们对土壤是如此陌生，不知道如何保养这一“地球的皮肤”，甚至不知道土壤是如何形成的、形成速率有多快、土壤是不是也会生老病死、世界上最古老的土壤在哪里、土壤与人之间到底是什么关系，等等。

邮票背后的土壤“密码”

作为一个学科，国际土壤科学的研究起步于20世纪初。那是一个将书信作为学者们进行学术交流的主要方式的年代，因土壤攸关粮食生产和环境保护，常常成为邮票设计的主题之一。

“土壤学是重视交流的学科，土壤学家曾用邮票传递科学的火种，大量土壤学的知识也得以通过邮票启迪大众。”土壤科学家、南土所研究员龚子同表示，邮票不仅让公众知晓更多土壤学的知识，也让科研人员从中受益。

生于上世纪30年代的龚子同，早年曾留学苏联沃龙涅什大学，始终保持着与许多国际土壤学界专家通信的习惯。几十年间，他与国外学界的上百封往来信件和明信片，以及随之而来的邮票，让众多学生了解到更多国外土壤研究进展，并成为土壤科普知识的窗口。

“世界上很多国家都非常重视土壤保护，希望通过邮票的方式，传递一些和土壤有关的理念。”南土所特别研究助理杨顺华经常协助龚子同整理资料，多次听过这些书信以及邮票的故事。

于是，杨顺华和同门的博士研究生张楚一起，在网上搜集整理了几十个国家和土壤有关的上千枚邮票，补充进了龚老师的邮票集。并以此为基础，于2021年12月在科学出版社出版了一本土壤科普书《土壤：地球的皮肤——从邮文化讲述土壤学的故事》。

在图书创作过程中，杨顺华发现，这种“接地气”的邮票设计在国外十分常见，国外还曾专门发行了以“州土”为主题的邮票。

“所谓州土（State Soil），和国内的市花是同样的概念。在美国的每个州，都有属于自己的州土。”杨顺华感慨，将这些内容集合起来，无论是公众还是科研人员，都能很方便地了解土壤的种类和分布。如果中国各省份都发行“省土”邮票，一定会是一件很有意义的事。

从农耕入手的中国土壤视角

从《土壤：地球的皮肤——从邮文化讲述土壤学的故事》一书中可以看出，相较而言，国内的邮票设计更多从耕地和粮食安全角度来看待土壤，也更能引起广泛关注。“这体现出我们对土地的重视。”杨顺华说，但从另一个角度，人们往往更多地从农业利用和管理方面去研究土壤，而较少关注土壤自身的形成和发展。

作为重要的自然资源，土壤为人类社会发展提供了基本的食物。数据显示，地球上95%的食物来源于土壤，土壤保存了至少1/4的全球生物多样性，是粮食、饲料、燃料和纤维生产的根基，不仅为生态系统和人类提供多种服务，还能抵御和适应气候变化。

“从历史上看，中国对土地和土壤有着悠久的开发使用历史。”杨顺华介绍，在明代永乐年间，北京丰台地区就建立了专为宫廷服务的菜园，其土壤很有可能已经发育为肥熟旱耕人为土。

在半干旱—干旱地区，如著名的河西走廊，长期引用浑水灌溉，边灌边淤，再加上耕作培肥，土壤越来越厚的同时，也越来越肥沃，逐渐形成了灌淤旱耕人为土。

而东北平原，从几百年前的“闯关东”开始，逐渐成为中国重要的粮仓。但由于长期过度开发利用、气候变化等多种因素的影响，东北黑土地也出现了不同程度的退化问题，比如耕作层有机质含量的锐减、黑土层的“变薄”和“变硬”等。

为此，中国科学院联合相关省区共同发起“黑土粮仓”科技会战，用科技创新支撑黑土地永续利用。南土所作为国内的主要研究力量，有多名研究人员参与其中。

科研人员在考察土壤。

受访者供图

《土壤：地球的皮肤》书封

受访者供图

“对于中国人来说，‘吃饱’是最重要的事。”张甘霖介绍，19世纪时，德国化学家李比希提出了养分“归还学说”，认为任何一种作物都会消耗土壤肥力，因此必须施用肥料，使土壤肥力的消耗和养分的归还保持平衡。

“这一发现极大地促进了化肥工业的发展，大大增加了作物产量，从而促进了人类社会的繁荣。”张甘霖表示，现如今“吃好”成为大众更关心的问题，土壤则是这一切的基础。“东北大米之所以有口皆碑，离不开肥沃的黑土地。现在通过科技会战，我们也希望能为用好养好黑土地筑牢基础。”

了解为地球“护肤”的知识点

当下，粮食问题已是全球瞩目的热点。而保护好土壤，无疑是人类避免危机加深和走出困境的“基础的基础”。

张甘霖表示，目前土壤面临的最大威胁是土壤侵蚀，也就是水土流失，每5秒钟就有一个足球场面积大小的表层土壤被侵蚀。然而，生态环境的脆弱性在于，破坏很容易，恢复起来却相当难。

联合国粮农组织的研究显示，地球表面形成2~3厘米厚的土壤可能需要长达千年的时间。因此，土壤资源来之不易。与此同时，受到战乱、极端天气等影响，全球的粮食产量也面临很多不确定性，一些国家甚至限制了粮食出口。

“土壤科学离普通人并不遥远，也实实在在影响着每个人的生活。”张楚表示，除地球土壤外，还存在月球表面的“月壤”、火星表面的“火星土壤”。但只有地球土壤具有肥力，更加凸显地球土壤的独特性和多样性。

“都说‘万物土中生’，土壤是地球陆地生命发生、进化和演化延续发展的根基。”北京师范大学环境学院教授李天杰表示，对于“刚开了头”的土壤学科普，需要大家给予更多的关注。

社址：北京市海淀区中关村南一条乙3号 邮政编码：100190 新闻热线：010-62580699 广告发行：010-62580707 传真：010-62580899 广告经营许可证：京海工商广登字20170236号 零售价：1.00元 年价：218元 工人日报社印刷厂印刷 印厂地址：北京市东城区安德路甲61号