

定理机器证明

赵子都

定理机器证明(The Machine Demonstration of Theorems),就是把人们证明定理的一般知识和规则以适当形式存贮到计算机中,让机器通过运转,自动地证明定理,既是早期人工智能研究的重要课题,又属知识工程的范畴。有深奥的哲学原理。我国数学家吴文俊在中国古代数学思想的启迪下,所创立的“定理机器证明”方法,在国际上独树一帜,并在定理机器证明领域内树立了影响深远的里程碑,被誉为吴方法。本文简要介绍了吴方法的梗概。

1 定理机器证明的缘起、意义

数学,不论是学习还是创新,最耗时费力的劳动,往往消耗在定理的证明上,而不是在真理的发明、发现上。数学是一门严谨的科学,证明是完全必要的,证明的严密性也是完全必需的。因此,数学工作者爱好证明,重视证明,但也常常为证明之艰难而困扰着。在数学史上有许多欲证而不能的猜想,如18世纪德国数学家哥德巴赫(Goldbach)提出的猜想,即所谓哥德巴赫猜想。猜想,若再通过严格的数学来论证,通过研究推导,被证明了的猜想,就直接变成定理,下面谈的“四色猜想”就是著名的一例。

17世纪,德国数学家、哲学家莱布尼兹(Leibniz)提出一个宏伟思想:制造一种推理机器,把人类关于理性的归纳和演绎机械化。但在莱布尼兹时代,由于生产力发展水平不高,这种以机器模拟人脑思维活动的研究没有能得到迅速的发展,因而推理机没有制造出来。但莱布尼兹思想的价值仍存在。这就是对以后的布尔代数和数理逻辑起到了促进和完善作用,也是以后电子计算机创立的一种“催化剂”,1937年,英国数学家图灵(Turing)发表了《理想自动机》的论文,该文给出了可计算性这一概念的严格的数学定义,并论证了任何需要精确地加以确定的计算过程,都能由图灵机完成。为人们清晰地描绘出理想自动机的蓝图,为以后电子计算机的创立奠定了基础。经过以后几代人的艰苦努力,美籍匈牙利数学家冯·诺伊曼(Von Ne-

umann)等人在图灵提出的一般机器的概念的启迪下,终于在1946年研制出了世界上第一台电子数字计算机,这是人类历史上具有划时代意义的大事。

计算机,顾名思义,是一种计算的机器,具有快速运算的能力。它首先使人们从繁琐复杂而又十分单调的四则运算劳动中解放出来,从而结束了几千年来,数学家只是用一只笔和一张纸进行研究的手工式劳动,能把大量的时间用在真理的发现和发明上;其次,由于电子计算机又具有逻辑推理和判断功能以及存贮功能,对某些艰深的定理的证明,可以借助于计算机来实现。它对于科学,特别是对于数发展的影响是难以估量的。如同望远镜之于天文学、显微镜之于生物学打开了人类认识自然的奥妙一样,计算机和计算机科学的发展为数学的发展开拓了新的天地,它不仅使一些长期因计算量浩大而不可设想的问题有了解决的可能,且某些或某类数学定理的证明,也可以在计算机上来实现。即把质的困难转化成量的复杂,而后者对于计算机来说是轻而易举的,因而使得定理的证明化难为易,这就是定理机器证明,也称为定理的机械化或自动化证明。

证明定理是人类特有的智能行为,是逻辑演算的过程。定理机器证明就是把人类证明定理的过程通过一套符号体系加以形式化,变成一系列能在计算机上自动实现的符号演算过程,也即把具有智能特点的推理演算过程机械化。

用机器证明数学定理的想法最初是由莱布尼兹提出来的,本世纪70年代,德国数学家希尔伯特(Hilbert)创立了数理逻辑,为机器证明定理提

供了理论和方法。另一方面,电子计算机的问世和发展,又为机器证明定理提供了物质条件。因此,使证明机械化的研究蓬勃发展起来。1950年,波兰数学家塔斯基(Tarski)提出并证明了:一切初等几何和初等代数范围内的命题都可以用机械化方法判定。令人惋惜的是,塔斯基的方法和后来其他人的改进都极为繁复而难于实现,但它对后来的影响是巨大的。以后,数理逻辑的发展和完善为机器证明定理提供了一种强有力的描述语言。1958年,美国的西蒙(Simon)、纽维尔(Newell)和肖乌(Shaw)三人通过研究人证明定理的心理过程提出了一个称为“逻辑理论家”的程序(LT)。这个程序不是刻板的固定算法程序,而是模拟了人用数理逻辑证明定理时的思维过程、规则和所采取的策略、技巧以及简化的步骤。它在计算机中先贮一些公理,然后用分解、代入和替换等方法来处理待证明的问题,如果这些子问题最终能变换成已知的公理或已证明过的定理形式,那么这个问题就得证了。西蒙等人利用这一程序,在大型计算机上证明了罗素——怀特海的名著《数学原理》第二章的全部定理。1956年,美国数学家罗宾逊(Robinson)提出归结原理。这一原理与西蒙等人的证法相反,他的基本出发点是要证明任何一个命题为真,都可以通过证明其否定为假来得到,归结原理的提出使机器证明获得了某些突破,虽然不少人在计算机上加以实现,但由于时间和空间的限制,这种理论精美的方法,终不能达到实用的程度。值得提出的是,50年代末美籍中国学者、数理逻辑学家王浩教授发明了“王浩算法”,他把整个机器证明过程规则化,整个系统由十七条规则及三个主要过程P、Q_{AE}、Q组成。过程P用于处理命题运算,过程Q_{AE}用于处理最小辖域区域形中的AE谓词演算,Q用于处理一阶逻辑运算。王浩于1958年在IBM704机上,用三分钟时间证明了《数学原理》一书中*1——*5的约220个命题演算定理,1959年他在不到四分钟的计算时间内完成了*9——*13的133条一阶逻辑运算定理的证明。我国数学家吴文俊教授称:“王浩在机器证明上的突破性成果早已脍炙人口,而其有关机器证明的一些精辟论点,诸如以量的复杂取代质的困难,以及基础机证与特例机证应有区别等论点,更是发人深思和使人深受启迪”。但这些方法的弊端是,它难于保证证明全部定理。

2 四色问题、吴文俊方法的出现

古代的地图,大都是五颜六色,使人看了眼花缭乱,能否减少颜色直至四种就可把不同国家或地区的边界区别开来,这就是著名的“四色问题”,也称为“四色猜想”,最早是由德国数学家麦比乌斯(Möbius)于1840年提出来的,是图论也是拓扑学中一百多年来一直困扰人们的著名难题。尽管它的严格的数学证明很艰难,但陈述却简而易懂:对于平面或球面(如地图仪)上任何地图的涂色中,不管有多少个国家或地区,也不管它们怎样设置,至多只用四种颜色对地图涂色,就可以使相邻的国家或地区着有不同的颜色。只用三种颜色有时显然是不够的。如欧洲的卢森堡,被德、法、比三国所包围,没有四种颜色是分不清的。但可以证明,五种颜色一定够用。这就是五色定理。问题是四种颜色是否够用,这就是有名的四色问题。

用四种颜色对地图着色,虽原本是一种猜想,但到目前为止,尚未发现有四种以上颜色涂色的现代地图。可是它的严格的数学证明却是很繁琐而艰难的。许多数学家(如德国的冯可斯基)对它的难度估计得并不充分,虽认真研究了四色问题,试图用数学方法来加以证明,结果无一不是以失败而告终。直到1874年,美国数学家肯普(Kempe)才给出了一个精致巧妙的证明方法,证明“四色”的答案是正确的。但遗憾的是1890年,数学家海伍德(Heawood)发现肯普的推理有一个漏洞,所以正确的答案并不因之成立。后来有许多人设法弥补那个漏洞,但却没有一个人能成功。虽然如此,肯普方法的价值仍旧存在,这就是他的思考路线带给了我们一成果。成果之一就是海伍德利用肯普的思考路线证明了对所有的地图,五种颜色是足够的,这就是上面所说的“五色定理”。但仍没有判断出“四色猜想”的真伪。到了本世纪七十年代,某些深有卓见的数学家指出:“四色猜想”是一个正确的定理,但它需要一种数学中前所未有的方法来证明,这个方法是不能单靠人力所能胜任的。石破天惊,证明奇迹般地出现了。1976年,美国伊利诺斯大学的青年数学家阿佩尔(Apple),哈肯(Haken)和计算机专家莫尔(Mohre)共同合作,他们依从肯普的思考路线,根据一些不可避免图

形,将四色问题分为2300多类(这种分类比肯普的分类细致得多,而且每一分类都很复杂),借助于数理逻辑使证明形式化的方法,利用计算机按照他们所设计的程序,用了1200个小时的机器时间(若用现有的高速计算机也需要300个小时的机器时间),作了近100亿个逻辑判断,从而完成了“四色猜想”的证明,终于使“四色猜想”变成了“四色定理”,悬置了一百二十多年未能解决的著名数学难题得到了肯定的回答。如此繁重的计算工作量和如此之多的逻辑判断,如果不是依靠计算机的高速度运算和大容量贮存,光靠数学家几千年来传统的手工式劳动来完成,据估算,大约得需要三十万年。这简直是一个不可思议的大难题。因此,四色问题的解决,被列为1976年科学上的重大研究成果。但这一成果的重大意义还不仅在于四色问题本身的解决,还因为这个方法的本身对数学中的很多难题,突破了数学理论传统的证明方法,开创了人和机器合作去解决问题的新途径,从而导致了“定理机器证明”这一崭新思想方法的确立。

机器证明定理本身的艰难是显而易见的,不过,《数学原理》中三百条定理,毕竟是平凡的陈述,是微不足道的定理,利用计算机证明“四色猜想”也只能算是计算机辅助证明。这种“一理一证”的极端方式不应视为定理机器证明的主流。定理机器证明应极大地限度地兼顾通用性。因此,定理机器证明的进一步发展必须要开创全新的局面。

机器证明思想在我国古代已有萌发,中国的古代数学基本上是一种机械化的数学。例如,汉初完成的名著《九章算术》中,对开平方、开立方的机械化过程,就有许多说明。在开平方法中是借用一根算筹^①来表示未知量的平方,在开立方法中借用一根算筹来表示未知量的立方,这就给所列出的筹式一个代数方程的意义,开平方或开立方的各个演算步骤也就是解方程、求正根的过程。在宋、元时代,我国更创立了“天元术”,引进了相当于现代未知数概念的天元、地元、人元、物元,把许多问题,特别是几何问题转化成代数方程与方程组的求解问题。这个方法用在几何上就相当于几何的代数化,十二世纪,杨辉、李冶、朱世杰又引进了相当于现代多项式的概念,建立了多项式的运算法则和

消元法有关的代数工具,使几何代数化的方法得到了系统的发展,几何的代数化实际上就是现代解析几何的前身。我们知道,法国数学家笛卡尔17世纪创立的解析几何,确实能使几何问题代数化,即用坐标法把几何问题化为代数问题,但并没有实现几何定理的机械化证明。我国当代杰出的数学家、中科院学部委员吴文俊教授在深入研究中国古代数学,特别是在研究《九章算术》的基础上,在中国古代数学的机械化与外数化的光辉思想启迪下,独辟蹊径,利用最先进的、具有推理判断功能和贮存功能的现代化计算机——电子计算机(电脑)把质的困难转化成量的复杂,提出了自己独具特色的机械化判定方法,于1977年以题为“几何定理判定问题与机械化方法”,在具有国际影响的学术刊物《中国科学》第六期上发表,又于1984年在科学出版社出版了世界上第一部关于几何定理机器证明的学术专著《几何定理机器证明的基本原理(初等几何部分)》,在机器证明领域内建立了影响深远的里程碑。吴文俊用他自己建立的机器证明方法和用他自己编写的程序,在计算机上成功地证明了非欧几何、元几何、线几何以及微分几何的六百多条重要定理。这些定理大多是不平凡的,而证明每条定理所用的机器时间才几秒钟,其中还有些是过去不被人知的新定理。吴文俊的方法在世界上不胫而走,受到了国际学术界高度的重视并引起了强大的反响,被誉为吴方法。它的出现标志着机器证明定理和发现艰深而不平凡的新定理正变为现实可行,从而结束了具有数千年历史的人们只靠一只笔和一张纸的手工式的初等几何定理的证明。今后,如果人们在初等几何范围内提出新命题而不知其真伪时,只要把该命题化成代数问题,用吴方法编成程序,上机一试便知分晓,从而使数学家得以摆脱繁琐的手工式劳动(计算和证明),腾出时间和精力,把聪明才智用到真正创造性的工作中去,这必将大大推动数学的发展。

为了研究和学习吴方法,推动吴方法的发展,在国家有关科技部门的支持下,中国科学院系统科学研究所于1990年成立了以吴文俊为核心的中国数学机械化研究中心,不仅在理论和方法上充实了吴方法,而且在多项式领域、非线性规划、机器人

①算筹:古代未知数不是用符号,而是用筹来表示的,“筹”是用竹子制成的一种计算工具,有时也表示运算,所以叫算筹。

学、控制论和几何模型等应用研究方面也获得了具有国际水平的成果,特别是在自动推理领域,吴方法具有划时代的意义,是近十年中自动推理领域最激动人心的突破性进展。

现在欧、美一些国家竞相研究吴方法,并邀请吴文俊前往讲学,如80年代初期,美国数学会邀请吴文俊教授出席在科罗拉多举行的机器证明会议,会上对吴方法给予了极高的评价。会议录《当代数学—机器证明25年》一书,有1/4的篇幅是吴文俊方法的论文。1984年,美国《自动推理杂志》破例重印了吴文俊方法奠基性论文:“几何定理判定问题与机械化方法”。

3 吴文俊方法的基本思想简介

在数学里要求证明的问题,往往是由条件和结论两部分所组成。所谓数学证明,众所周知,就是根据所给的条件,已有的定义、公理以及已被证明成立的定理,按照一定的推理格式导出结论。这在相当大的程度上要依赖于人们的智慧、才能和经验,并且需要较长的时间致使人们望而却步。几何定理的证明更是这样,吴文俊教授认为,我国几何学的发展是始终与数量关系形影不离的。现代几何学的许多重要领域,例如微分几何与代数几何,往往一开始就假定了一个数系(一般是一个数域,甚至是一个特殊的实数域或复数域),由此构成仿射空间或投影空间,然后用坐标或以函数与导数间的关系来引进各种几何图形,如曲线、曲面及其几何关系等。看来,在数的基础上建立起整个几何学的体系这已是大势所趋,但也不能不考虑几何学的直观背景与来源,以及它的基础问题。如何从原始的现实形象提炼出一套几何学的公理系统,又如何从公理系统发展成坐标系统,使几何定理的证明完全化成代数问题,使代数方法得以在几何上发挥作用,看起来是平凡的,但作起来也并非轻而易举之事。首先,因为解决这些代数问题计算量过大,使人望而却步;其次,由于代表几何关系而出现的那些代数式往往杂乱无章,使人们无所措手。幸而现在出现了电子计算机,对繁杂的计算已经有了有效的处理办法。因此,如何把杂乱无章的代数关系处理得井然有序,使计算机得以在证明几何定理上发挥威力,便成为问题的关键所在。对此,吴文俊证

明了如果一种几何的附属数系是一个数域,即乘法是可以交换的,则假设与终结部分都可由多项式等式关系来表达的那类定理的证明都可以机械化。这一类定理称为等式型定理。它的机械化问题可归结为一个纯代数式的机械化问题。包括了几何学中最主要的大部分定理。事实上,有序或无序的常用几何学、投影几何学、非欧几何学等,它们的几何定理都有机械化证法。因此,在理论上,这些几何学的定理证明,都可以借助于计算机来实现。对此,吴文俊教授已出版了《几何定理机器证明的基本原理(初等几何部分)》,把几何定理的机器证明分成以下三个步骤:

(1)几何的代数化与坐标化,从几何的公理系统出发,引进数系统与坐标系统,使任意几何定理的证明问题成为纯代数问题;

(2)几何的机械化,将几何定理假设部分的代数关系式进行整理,然后依确定步骤验证定理终结部分的代数关系式是否可以从假设部分已整理成序的代数关系式中推出;

(3)用计算机作最后验证,依据第二部中所确定的步骤编成程序,并在计算机上实施,以得出定理是否成立的最后结论。

由于现在的计算机尚只能识别有限的事物,因此几何定理机器证明的一个先决条件是第二步中所确定的代数关系式必须是以有限的形式出现。例如这些代数关系式都是以多项式的形式出现,且其系数都是整数,则对于计算机的使用只是依据第二步中所确定的步骤编制程序的问题,不会有任何实质性的困难。如果一门几何可以找到这样三个步骤(事实上只要前两个步骤即可)来完成定理的证明,我们就说这门几何可以机械化,并把可以机械化的这一结论称为机械化定理。由以上所述可以看出,由公理化到机械化大体上经历了如下一个过程:

公理化→代数化→坐标化→机械化

一门几何学能否机械化并不显然。按吴方法,几何的公理、定理与证明,实质上都可以用有限次的构造步骤来叙述以至完成,这也就为我们提供了几何定理证明有可能机械化的依据。吴文俊证明了:奠基于各种公理系统的每种初等几何学,只要相当于乘法交换律的某一公理成立(即乘法是可以交换的),则假设与终结部分都可以由多项式等式

表达的那类定理的证明,大都可以机械化。这些几何定理的证明,可以借助于计算机来实现,这一类定理即前面说过的等式型定理。可以机械化的几何包括了多种有序或无序的常用几何学(即欧氏几何的那种初等几何)、投影几何、非欧几何与元几何等。

以上说的几何定理证明了机械化,其寻求的是一般方法,不仅适用于个别的定理,而且适用于整个某一类型的定理,甚至可以说是某一种几何的所有定理,只要依照上述的方法进行有限步之后,就可以对整个某一定理得到统一的证真或证伪而无分难易,其中几何的代数化乃是关键之一步。

值得提出的是,吴方法不仅能证明几何定理,而且在其他数学领域或物理学科上也大有用场。例如还可以推广到代数几何等领域。美国数学家乌拉,为了要探讨应用中广泛出现,而现代数学又对之还无能为力的非线性现象,便是在计算机上进行试验,发现了一些规律。近年来,微分方程孤立子解的获得,就是首先在计算机的荧光屏上发现的。这是应用数学上的一个重大突破。吴文俊教授本人还曾利用他的方法,在开普勒定律之下,成功地证明了著

名的万有引力定律。最后我们引用著名的工程控制论专家、中国科学院院士、国家科委主任、清华大学兼职博士生导师指导教授宋健的话来结束本文:

“吴文俊机器证明理论,为高度公理化的数学金字塔,通向现代社会建立了一座桥梁,必将对社会经济、生活、生产以及科研产生不可估量的影响。”

主要参考资料

- 〔1〕吴文俊“几何定理判定问题与机械化方法”《中国科学》,北京,1977年第六期
- 〔2〕吴文俊 几何定理机器证明的基本原理(初等几何部分),北京,《科学出版社》(1984年)
- 〔3〕吴文俊“数学的机械化”北京,《百科知识》1980年第3期
- 〔4〕程为民等,“四色问题及其计算辅助证法简介”重庆《计算机应用与应用数学》,1977年第5期
- 〔5〕梁宗巨 世界数学史简编,沈阳,辽宁人民出版社(1980年)

【作者简介】赵子都,1925年生,锦州辽宁工学院数学系教授。

(本文责任编辑 贾云祥)

· 书讯 ·

《东方的智慧》出版

《东方的智慧——东方自然观与科学的发展》一书是国家教委社会科学基金资助课题——“东西方科学思想比较研究”的主要成果,最近已由江苏科技出版社出版。这部著作的撰写出版,历时六年。作者林德宏、张相轮两位教授倾注了大量的心血。全书47.8万字,是近年来科学思想比较研究方面的重要学术著作,也是关于东方文化的严肃论著。本书系统地论述了东方自然观形成的历史背景,它的基本内容和特征,对涉及东方自然观的各方面问题作了详细分析,使读者对内容丰富、思想深邃而又具有一定神秘色彩的东方自然观有较全面的了

解。本书还论述了东方自然观与科学发展的关系,着重指出近代西方科学、特别是牛顿机械论同现代科学发展的冲突。要彻底清除机械论的影响,需要从东方自然观中汲取辩证的有机论思想,从东方智慧中获得新的启迪。

《东方的智慧》一书材料翔实,文笔流畅,颇具可读性。读者从中可以把握东方自然观的精髓,并了解东方智慧对未来科学发展的价值。购书者可同江苏科技出版社发行科联系。地址:南京市中央路146号,邮政编码210009。

(苏讯)