数学机械化研究回顾与展望

吴文俊

中国科学院数学与系统科学研究院系统所

一、数学机械化的历史背景——脑力劳动机械化

Norbert Wiener 在他的名著《控制论》里提到，第一次工业革命是用机器来代替手，即“由于机器的使用手的价值降低了”。我们可以换一种说法，过去工业革命时代的特征是用某种机器来减轻甚至代替体力劳动。同样，按照 Wiener 的说法，现在正在进行的工业革命，是使用某种适当的工具来使得人脑在做某些简单与规则化决定时的价值降低。我们可以说，新的工业革命时代的特征是用某种新型的机器来减轻甚至代替某些脑力劳动。简单地说，过去的工业革命是体力劳动的机械化，现在正在进行的工业革命是脑力劳动的机械化。

脑力劳动机械化的思想，并不是在有了计算机以后，或者在 Wiener 提出来以后才有的。事实上这种思想在很早的年代就已经有了。M. Kline 在他的名著《古今数学思想》中提到了 Descartes 关于脑力劳动机械化的思想。他说：“Descartes 认为，代数应该可以把数学机械化，使得思维变得简单，不需要再让头脑费很大的力气。数学的创造也极可能成为自动的。… 甚至逻辑原理和方法也可以被符号化，并且整个系统都能被用来把所有的推理过程机械化。” Leibniz 也有同样的想法。Kline 在其书中讲到：“代数可以将几何推理符号化甚至机械化，这种力量使 Descartes 和 Leibniz 印象深刻。…，Leibniz 开始了一个更加雄心勃勃的计划。… Leibniz 对于一种广义计算（broad calculus）的可能性产生了兴趣，这种计算可以使人在所有的领域都能机械地、不费力地进行推理。… 一般的科学可以提供用于思考的通用语言，各种概念…可以用机械的方式结合起来”。

历史上已经有许多用某种方式减轻甚至代替脑力劳动的尝试。我们可以举些例子。第一个例子就是 Napier 创造了对数。利用对数可以将对于脑力劳动来说比较费劲的乘法、除法变成对于脑力劳动来说相对比较简单的加法、减法。第二个例子是，Descartes 在他 1637 年的名著《几何学》中提出了一些几何代数化的想法。就是引入后来所说的坐标系，它使得对于脑力劳动来说比较艰难的几何推理变成脑力劳动相对轻微的代数计算。第三，Pascal 和 Leibniz 相继在十七世纪制造了一些计算机器。Pascal 用这些机器来进行加法运算，把加法这种脑力劳动完全用机器来代替。而 Leibniz 改进了 Pascal 的机器，使其既能做加法又能做乘法。这是用机器来代替脑力劳动的创新。Leibniz 用拉丁文写了一篇文章来介绍他的机器是怎样使用的，后来被人翻译成英文。他在这篇文章中说：“一个出色

的人像奴隶一样把时间浪费在计算的劳动上是很不值得的。如果有了机器，这种工作可以放心地交给任何人。” Leibniz 的意思是不要把时间浪费在加减乘除这样烦琐的脑力劳动上，只要靠机器自动做就可以了。当然我们也可以推而广之，加减乘除可以这样做，别的脑力劳动也可以这样做。

脑力劳动机械化从 Descartes 和 Leibniz 提出比较笼统的想法以来，有了如下进展：首先， Boole 创立了现在所说的 Boole 代数，他把思维在某种程度上形式化，用代数形式加以描述。这是一个很大的进步，比起 Leibniz 和 Descartes 的想法至少有了某种程度的数学化。在 19 世纪至 20 世纪，两位数学哲学家，A.N. Whitehead 和 B. Russell，在 1910-1913 年出版了《数学原理》，里面罗列了几百条数学定理。到了二十世纪，D. Hilbert 正式提出了数学公理化的概念，还创立了数理逻辑这门学科，特别是在数理逻辑里面创立了证明理论，而且他还提出来数学本身的相容性问题。Hilbert 在最后的若干年尽力来证明数学是相容的，是不会产生矛盾的。

前面都是理论方面的进展，在实际应用方面，J. Herbrand 创立了一种可以用来证明任何定理的算法。可是这一算法是不完全的，因为照此算法进行下去，不能保证可以在有限步骤之内结束证明。这种算法提供了一种进行推理的途径，任何定理都可以根据这种推理方式一步一步进行下去。假定在有限的步骤之内结束了，定理就被证明了。如果不能在有限步内结束，就不能得出结论。因此这种算法是不完全的。但是它提供了一种方法，可以使推理过程实现一定程度的自动化。因为 Herbrand 在数学的逻辑推理方面提供了一般的方法，所以后来美国能源部 Argonne 实验室的一些教授提出建立 Herbrand 奖来纪念他在这方面的贡献。1931 年，奥地利数理逻辑学家 Goedel 发表了一篇论文，向 Hilbert 的计划泼了一盆冷水。Hilbert 想证明数学是圆满无缺的，是相容的，不会出问题。Goedel 说不见得是这样。他提出了不完全定理，说有些逻辑系统和有些定理，尽管我们知道是对的，可是不一定能够证出来。结果使得 Hilbert 数学圆满无缺的想法彻底破产。

以上这些结果都是反面的，Herbrand 的工作算是比较正面的，但是并不能够提供任何真正有效的证明方法。1950 年，波兰数学家 A. Tarski 发表了一篇文章，证明初等代数和初等几何定理可以用一种算法来证明或否决。这是完全正面的一个结果，可以给出一个算法证明或否定代数和几何定理。也正因为这个结果，Tarski 计划制造一些类似计算机的逻辑证明机来进行几何和代数定理的证明。这当然是非常了不起的，可是他的算法复杂到了一定程度，不要说当时的计算机，就是现在的计算机，恐怕也不能用他的方法得出有意思的结果来。在 Tarski 之后，70 年代美国进行了许多试验，用 Tarski 的办法来证一些几何定理。他们能够证出来的最复杂的一个定理是：假定有 1、2、3、4、5 五个点，知道 1、2、3，1、

2、4 和 1、2、5 分别在一条直线上，结论是 3、4、5 在一条直线上。这个定理在我们看来就像没有说一样。所以说 Tarski 的算法在理论上是完美无缺的，可是在实际上行不通。因为它的过程太复杂了。后来有美国、奥地利等国的数学家把 Tarski 的方法加以改进，增加它的效率。可是到现在为止，用这些改进了的方法能够证明的定理还是很简单的。

另一方面，1950 年以来，一些计算机科学家，像 McCarthy、Minsky、Newell 等人，提出了一个想法：是否可以利用计算机进行某种脑力劳动，由此成长起来一门新的学问——人工智能。这是用计算机来代替脑力劳动的一次成功的尝试。比如说用计算机来进行翻译、诊断病情、与人下棋，各种专家系统、机器人踢足球等等。人工智能发展到现在已经五十年了，现在还在进行之中。

另外，我们还要提到王浩先生的工作。他有一篇关于数理逻辑的很长的文章，标题叫“Toward Mechanical Mathematics”——我的数学机械化的名称不是我创造的，正是看到王浩先生的这个文章，联系到我们的工作，于是才有了数学机械化这个名称。他在文章中提到：“一个应用逻辑的新的分支产生的时机已经成熟，这个分支可以被称为`推理分析’，它可以像计算数学处理数值那样来处理证明。我相信这种方法在不远的将来会导致用机器证明很难的新定理。… 适用于所有数学问题的普遍的判定方法是不存在的，可是形式化看来可以保证让机器做一大部分工作，而这些工作占据了今天的数学家们的宝贵时间。”可以说，我们做的数学机械化，正是像王浩先生所说的“推理分析”。它对待定理的证明就像计算数学对待数值那样，而且在不远的将来可以证明很难的定理。事实上我们的数学机械化可以说已经做到一定程度了，对几何定理的证明可以说不在话下。我们的方法也已经推广到微分情形，微分几何定理的证明应该也可以说不在话下，只是我们的机器设备和软件环境还跟不上。理论上应该可以做到这一步。

计算机科学大师 D. Knuth 在《计算机科学与数学的关系》这篇文章里说：“所谓计算机科学说穿了就是算法的研究。算法是把许多知识统一起来的有效途径，但是算法的研究一直要等到计算机器的出现才可能实现。”Knuth 说，并不是有了计算机才有计算机科学的。事实上计算机科学在计算机出现的很长一段时间以前就已经有了。总而言之，计算机科学深深植根于历史之中。先有计算机科学，然后才有计算机。

事实上，计算机科学很久以前在古代中国就已经存在了。中国古代的数学是一种算法形式的数学，其主要的结论不是由定理的形式来表示，而是用算法的形式表示的。不光在理论上要求知道 why，而且还要知道 how，要知道是怎么做出来的。我们可以举很多中国历史上的例子。就拿加减乘除来说，加减乘除都是根

据某种算法一步一步进行的，这正是中国古代的传统。很早以前就有加减乘除这种我们大家现在都很熟悉的算法了，一直流传到现在。这是最简单的算法。还有很多其他的算法。如解线性联立方程，现在大家都知道高斯消去法，其实在公元前二世纪《九章算术》里就讲得清清楚楚。高斯消去法出现在高斯的一篇天文方面的著作中。他要观测行星的运行进行计算，归结到某种线性联立方程。可是这篇文章因为考虑了特殊的天文方面的计算问题，他的方程组是有特殊形式的，而我们的《九章算术》是没有任何特殊形式的。总之，古代的中国数学，有以下一些特色：它重视应用，甚至是高度实用的。它重视计算，是计算性，构造性，也是算法性的。大部分的重要结果都以“术”的形式表示，而“术”通常相当于现代的算法。依据它即可编成程序在计算机上实施。依照 Knuth“计算机科学是一种算法科学”的观点，我国古代数学乃是一种计算机科学。它在进入计算机时代的今天，其内在的意义与可能的影响更是不言而喻的。

二. 计算机时代中国的数学机械化研究

由于我国古代数学思想方法与成就的启发，也是为了满足在计算机时代实现脑力劳动机械化的需要，我们从上世纪七十年代末，即开始从事应用计算机于数学的研究工作。

大部分的人， 只要学习过几何的，就会对几何定理证明的艰难曲折有所体会。几何定理证明自古就被认为是脑力劳动的典型活动，也是自然被选为脑力劳动机械化最初尝试的问题。在我国古代数学的影响之下，我们于1976之末，对几何定理尝试寻找机械化的证明方法。为此我首先应用坐标系统，把几何定理转变为纯代数的形式。经过几个月的艰苦尝试，终于发现了某种算法，足以用代数的处理证明初等几何中很主要的一部分定理。此后已有成百上千艰深的几何定理，在计算机上轻而易举地得到了证明，甚至还发现了不少过去未知的新定理。此后这一几何定理证明的算法式方法，逐渐发展成一般性的数学机械化方法，并以解多项式方程组为其核心内容之一。

根据我国古代先哲的思想路线，结合现代数学中的某些技术，我们得出了解任意多项式方程组的零点分解算法。若以Zero(PS)来表示多项式方程组所有零点的集合，则所得的结果可用若干个具有特定的三角形式的方程组的零点来表示Zero(PS)。这些定理足以对特征为零的任意多项式方程组PS=0给出其全部零点或解答的显式构造。我们关于几何定理的机械化证明方法，实际上是上述解多项式

方程组一般方法的一项具体应用，又一个应用是已知有关系但不知具体形式时确定其显式关系式。

上述多项式方程组的解法，也已推广至微分情形。对于所谓代数型微分方程组DPS=0，也有相应的零点分解定理，足以给出某种意义下的全部解答或零点。与代数情形相同，这一方法已应用于微分几何定理的机器证明，以及未知微分关系的自动发现。特别是，我们曾应用这一方法，从观察性的Kepler定理，自动得出牛顿反平方定律。此外对于物理与各种科学中涌现的各种偏微分方程，用这一方法已确定其全部孤立子型的解答，取得了很大成功。这里对各种方程用的是统一的同一方法，而流行文献则对各别方程须用各别的方法，这些方法既曲折艰难，还往往漏掉一些应有的解答。

一个投影的复代数簇，通常定义为相应齐次多项式组所有（齐次）零点的集合。对于投影代数簇，在无奇点的情形，可以通过簇的切丛来定义著名的陈（省身）类与陈（省身）数。但对于有奇点的情形，则由于切丛不再存在，现在所用的方法，须要通过艰难曲折的途径来定义广义的陈类与陈数。而且这种方法是无法计算的。即使在极其简单的情形，也难确定出相应的陈类与陈数来。与之相反，我们解多项式方程组所使用的方法，可以使我们对有任意奇点的投影簇，都能直接而自然地引进广义的陈类和陈数。例如在陈数间有著名的Miyaoka丘成桐不等式。这一不等式只在某种没有奇点的二维复平面上才成立。而用我们的方法，则对任意维数的超曲面，无论有无奇点，都发现了大批陈类与陈数间的等式与不等式，而这些关系却只须经过简单的计算即可得出。上述Miyaoka-丘的不等式，只是一个很极端的特殊情形，且其成立不需要无奇点的限制。

优化问题或极大极小问题，广泛出现于各种科学与工程技术的领域之中。无疑它们对我国的经济建设有极其重要的意义。这种问题往往用计算数学的方法，通过各种逐步收敛逼近来解决。但这样的方法通常只能得出个别且是局部的优化值。在目标函数与限制条件都是多项式型这种自然界相当频繁出现的情形时，我们解多项式方程组的一般方法，提供了一种有效手段，足以定出真正最大或最小的全局最优值来，只要它们真正存在即可。特别是现已受到重视的例如双层规划的情形，在文献中曾有些具体例子，用我们的方法进行验算，发现文献中所给出的所谓最优值，事实上并非最优，而与用我们的方法所给出的真正的最优

值相距甚远。

以上主要讲了我们在机器证明、代数方程组符号求解、微分方程组符号求解、实数方程的优化问题方面的工作。我国的研究人员还提出其他的机械化方法。包括机器证明的几何定理自动发现的代数方法与演绎数据库方法、消点法与 Clliford 代数方法、几何计算的共形代数与零括号代数、几何自动作图方法、机器证明的数值并行法、实数方程求解的完全判别式方法、差分方程与差分微分混合方程的零点分解定理、有限域方程求解的零点分解定理、微分与差分方程符号解的自动求解方法、方程求解的数值－符号混合算法。这些工作扩大了数学机械化的使用范围、提高了计算效率。

微分与代数方程求解是基本的计算问题之一。科学与工程中的很多问题往往自然地导致方程组的求解，因之我们的解方程方法在科学与技术中自然地得到了广泛的应用。与其他学科交叉研究已经取得进展的问题包括理论物理中著名的杨-Mills 方程与杨-Baxeter 方程求解、机构学的研究、天体力学中中心构形问题、化学反应的平衡点计算问题、计算机科学中的自动推理问题与 SAT 问题等。我们的方法在高科技领域也得到成功的应用，包括计算机辅助设计中的曲面拼接问题、图像压缩技术、智能 CAD 中的几何约束求解问题、计算机视觉中的 PnP 定位问题与线画图的识别问题、硬件的正确性验证问题、编码与密码中的某些问题、机器人中的 Puma 形串联与 Stewart 并联机构的设计与分析。具体请参考本文后面所列目录。

依据我们的方法，开发了智能软件平台 MMP，具有独立自主而不依赖于其他任何同类系统的特性，已经完成，这一系统的核心功能之一，即是我们代数与微分方程组解法的算法。

三. 数学机械化的未来展望

人类正在进入崭新的信息时代或计算机时代，它以计算机这一强有力工具的出现为其特殊标志之一。从 18 世纪以来，人类曾经历过几次工业革命时期，这些革命可以理解为以体力劳动的机械化为其特色，在来临的时代中，我们将面对另一种新型的工业革命，它可以理解为以脑力劳动的机械化为其特色。数学是一种典型的脑力劳动，它被公认为是所有科学技术的基础，同时数学又具有最广

泛的应用性，各种活动都离不开数学的参与。因之在所有的脑力劳动中，数学的机械化应该有最大的优先权与迫切性。此外，数学又具有表述上清晰，简明，确切等特点，而其他脑力劳动都很难具有所有这些特点，因此在所有脑力劳动中，数学应该最容易做到机械化。我们在几何定理证明机械化取得的成功，说明以上的说法决非虚语。

我们之所以提出数学的机械化，还是为了迎合在计算机时代实现脑力劳动机械化的需要。但是，我们现在的数学机械化，还只处于一种初始的阶段，即以定理的机械化证明来说，我们的成功还只限于很狭窄又不那么重要的初等几何或（局部）微分几何的范围，然而，数学的各个领域都有它自己的定理证明，它们的机械化须依赖于这一领域的特有方式，而不必归之于多项式方程组的求解。此外，从数理逻辑得知，如果所考虑的数学领域范围过大，则这一领域的定理证明依逻辑学家的辞藻可能是不可判定的，而依我们的辞藻是根本不能机械化的。但若领域范围过于狭窄，则又可能根本不包含什么在数学上有任何意义的定理。为此我们曾提出过下面今后需要考虑的规划：

把数学的全部尽可能用各种领域覆盖起来，使得每一领域既足够小因而机械化成为可能，又足够大使它能够含有相当多的定理或问题，它们都在数学上富有韵味。

就多项式方程组的求解而言，我们所用的是所谓符号计算的方法，与通常所用的数值计算的方法有根本区别。这种符号计算方法往往导致庞大的多项式，其项数甚至可远在千百万之上，往往超出了计算机的负担能力。要使我们的方法在实际上切实可行，看来只有发展一些能结合符号计算与数值计算两者之长的所谓混合计算方法，而这种方法当然应有严格的数学上的依据。

当代的数学大体上由微积分发展而来，因之带有某种无限的性质，但计算机则只能处理有限性的事物，处理的方式也是有限性的，因之数学中处理有限性的组合数学，在计算机时代中将越来越显得重要，尤其是因为它可处理与国防紧密相关的信息安全等问题，因而其重要性更显得突出。为此我们应对组合数学的算法式研究，给予比以往更多的重视。

我们已经指出如何由 Kepler 的观察定律自动导出牛顿的反平方定律。这提供了从实验到理论自动发现这一一般方法的一个实例。这一方法应在今后各种科

学领域作出进一步的尝试。

最后，我们发展数学机械化的目的不仅仅是为数学研究提供一个有力工具，更主要的是为我国高技术中的脑力劳动提供工具。我们的方法已经用于自动证明定理、自动发现物理规律、计算机图形学、智能 CAD、计算机视觉、图像压缩、机器人、数控等关键技术的研制中。我们还希望加强在这方面的努力，使得数学机械化方法为我国高技术的发展做出实质性贡献。

参考文献

1. S.C. Chou, *Mechanical Geometry Theorem Proving*, D. Reidel, 1988.
2. S.C. Chou, X.S. Gao, and J.Z. Zhang，*Machine Proof in Geometry*, World Scientific, Singapore, 1994
3. 高小山，王定康，裘宗燕，杨宏，《*方程求解与机器证明－基于 MMP 的问题求解*》，科学出版社，2006.
4. X.S. Gao and D.M. Wang (eds), *Mathematics Mechanization and Applications*, Academic Press, (2000).
5. H. Li. *Invariant Algebras and Geometric Reasoning*. World Scientific, Singapore. 2007.
6. D. Kapur and J. L. Mundy (eds.), *Geometric Reasoning*, MIT Press, 1989.
7. D.M. Wang. Elimination Methods. Springer, Springer, Wien, 2000.
8. 吴文俊，几何定理机器证明的基本原理(初等几何部分)，科学出版社（1984 *Basic Principles of Mechanical Theorem Proving in Geometries*,（英语翻译），Springer, Wien, 1994.
9. W.T. Wu, *Mathematics Mechanization*, Science Press / Kluwer Acad. Publisher, (2000).
10. 杨路，张景中，候晓荣，非线性代数方程组与定理机器证明，上海科技出版社，1996。
11. 数学机械化研究报告（MM-Preprints），中科院数学机械化重点实验室，第 1-26 期, (1987-2006), http:/www.mmrc.iss.ac.cn/mmpreprints.

简历。

吴文俊现任中国科学院数学与系统科学研究院研究员，中国科学院院士。主要研究拓扑学、数学机械化与中国古代数学史。吴文俊曾获得首届国家自然科学一等奖，第三世界科学院数学奖，陈嘉庚数理科学奖，首届香港求是科技基金会杰出科学家奖，Herbrand 自动推理杰出成就奖，首届国家最高科技奖，劭逸夫数学科学奖。