吴文俊与数学机械化

高小山　中国科学院数学与系统科学研究院

1、数学机械化纲领

吴文俊于 1978 年发表几何定理机器证明的第一篇论文[7]后，主要精力转向数学机械化研究。他不仅提出了数学机械化的主要方法，还花了大量时间遍寻各种可以用他的方法解决的应用问题，并亲自动手编制计算机程序给出这些应用问题的具体解答。对此，有些同行表示不理解，认为像吴文俊这样杰出的数学家应该致力于像拓扑学那样的核心数学领域。但是，吴文俊从不为之所动，究其原因，是因为吴文俊关于数学机械化的研究体现了他自 20 世纪 70 年代末形成的关于数学发展的观点。

1974 年，吴开始研读中国数学史文献。他发现，中国古代数学的显著特点是其构造性与算法化，而且算法化思想在数学的发展中起到了非常重要的作用。吴文俊指出：回顾数学发展史，主要有两种思想，一是公理化思想，另一是机械化思想。前者源于希腊，后者则贯穿整个中国古代数学。这两种思想对数学发展都曾起过巨大作用。从汉初完成的《九章算术》中对开平方、开立方的机械化过程的描述到宋元时代发展起来的求解高次代数方程组的机械化方法，对数学的发展起了巨大的作用。公理化思想在现代数学、尤其是纯粹数学中占据着统治地位。然而，回顾数学史可以发现，数学的多次重大跃进无不与机械化思想有关。例如，对近代数学起着决定作用的微积分也得益于经阿拉伯人传入欧洲的中国数学的机械化思想。因此，吴认为应该重视机械化思想对于数学发展的作用。

机械化思想过去在数学研究中未能得到足够重视，主要有两个原因。

在理论上，机械化方法是不完备的。逻辑学家对于定理证明机械化的探索，得到的结论大都是否定的。例如，Godel 证明初等数论的机械化是不可能的。即使是正面的结果，例如，Tarski 关于初等代数可机械

化证明的算法太过繁琐，以至于不能证明非平凡的定理。有鉴于此，吴文俊提出，虽然不是所有的数学分支都可以机械化，但是确实有很多非常重要的数学分支是可以有效机械化的。从方法上，适用范围太大的方法、如理论上可以证明所有定理的归结法，其效率必然低。应该针对具体的数学分支发展特殊的高效算法。

在实践方面，机械化思想的实际应用需要大量的计算。而人的计算能力是有限的。计算机的出现使得数学的机械化成为可能，从而会对数学的发展发挥重大的影响。吴讲到“不久的将来，计算机之于数学家，势将与显微镜之于生物学家，望远镜之于天文学家那样不可或缺。” 计算机提供了一个有力工具，使数学有可能像其他自然科学一样，跻身科学试验行列。

吴文俊进一步提出，数学的机械化不仅对于数学有重大意义，而且还在新的技术革命中扮演重要角色。这是因为，数学的机械化将带动脑力劳动的机械化。“枪炮的出现使人们在体力上难分强弱，而个人用计算机将使得人们在智力上难分聪明愚鲁。” “但是，也不必妄自菲薄。大量繁复的事情交给计算机去做了，人脑将仍然从事更富有创新性的劳动。”数学是典型的脑力劳动，因此在脑力劳动机械化过程中有其特殊地位。不仅如此，数学是自然科学与高科技的理论基础，数学方法的创新有可能带动科学发展与技术进步。因而，数学机械化又有其迫切性。此外，数学具有表达精确、论证严谨等特点，数学机械化在各类脑力劳动的机械化中又易于实现。

基于以上认识，吴文俊在写于 1979-1981 年期间的几篇文章中明确提出了发展数学机械化的重要性，并给出了后来称之为“数学机械化纲领”的指导思想：“在数学的各个学科选择适当的范围，即不至于太小以致失去意义，又不至太大以致于不可机械化，提出切实可行的方法，实现机械化，推动数学发展。”在 1985 年“刘徽数学讨论班”的讲演中，吴文俊勾勒了他对于数学机械化发展的具体设想。以代数方程求解的吴-Ritt 特征列方法为核心，他提出应该研究：初等几何定理的机器证明与机器发现，微分几何定理的机器证明与机器发现，未知关系的机器推导，超越函数间的代数关系，计数几何，高次代数方程求解问题，因子分解问题，代数几何，微分几何，不变量问题，不等式关系，构造性代数几何与微分代数几何。吴还特别重视数学机械化的应用。他在“攀登项目”答辩时说道“应用是数学机械化的生命线”。在吴的带领与鼓励下，数学机械化方法被应用到理论物理、密码学、计算机辅助设计、计算机视觉与模式识别、计算机图形学、信息压缩、机器人与机构学、数控系统等多个领域。

吴自己关于数学机械化的研究也遵循以上想法。吴选择了初等几何定理的机器证明作为突破口。这是因为，几何推理自古以来被认为是推理的典范，以困难和技巧强著称，而且自 1950 年以来多位计算机学家进行了探索，但没有找到好的方法。吴借鉴了著名逻辑学家王浩提出的、以计算的复杂来换取质的困难的思想，将初等几何定理机器证明问题转化为代数几何中方程解集的包含问题，从而提出了几何定理机器证明的第一个高效算法，取得了几何定理机器证明的突破。以下引用 1997 年吴文俊获得国际自动推理最

高奖“Herbrand 自动推理杰出贡献奖”的授奖词(Automated Deduction, 1997, Springer)，其中对吴的工作给予了详尽的描述与评价：

“吴文俊在自动推理界以他于 1977 年发明的（定理证明）方法著称。这一方法是几何定理自动证明领域的一个突破。”“几何定理自动证明首先由 Herbert Gerlenter 于 20 世纪 50 年代开始研究。虽然得到了一些有意义的结果，但在“吴方法”出现之前的二十年里这一领域进展甚微。在不多的自动推理领域中，这种被动局面是由一个人完全扭转的。吴文俊很明显是这样一个人。”“吴的工作由 20 世纪 80 年代初期在德克萨斯大学学习的周咸青介绍给了西方学术界。周咸青（基于吴方法）的证明器证明了数百条几何定理，进一步显示了吴方法的潜力。至此，几何定理证明的研究已全面复兴，变为自动推理界最活跃与成功的领域之一。”“吴继续深化、推广他的方法，并将这一方法用于一系列几何，包括平面几何、代数微分几何、非欧几何、仿射几何、与非线性几何。不仅限于几何，吴还将他的方法用于由开普勒定理推出牛顿定理；用于解决化学平衡问题和求解机器人方面的问题。吴的工作将几何定理证明从自动推理的一个不太成功的领域变为最成功的领域之一。在很少的领域中，我们可以讲机器证明优于人的证明。几何定理证明就是这样的一个领域。”

2、数学机械化理论与方法

吴文俊关于几何定理机器证明的方法主要依赖一种关于代数几何的构造性理论。吴早在 20 世纪 60 年代就在中国科大开设了代数几何课程，“代数簇”一词既由吴文俊翻译命名。吴于 1965 年前后引进了具有奇异点的代数簇的陈省身示性类，早于国外类似工作十余年。在 20 世纪 70 年代末，为了几何定理机器证明的需要，吴发展了美国数学家 Ritt 关于特征列的理论，提出了以吴-Ritt 零点分解定理为核心的构造性代数几何理论。

代数几何是近代数学的核心分支。长期以来，形成了各种流派。当前流行的代数几何研究方法大都是存在性的。近二十年来，代数几何的构造性理论也蓬勃发展，并在诸多方面得到重要应用。除吴-Ritt 零点分解定理外，还有 Groebner 方法、周炜良形式等构造性方法。以下主要介绍吴-Ritt 零点分解定理。

简单说，吴-Ritt 零点分解定理是将一般形式的代数簇分解为所谓“三角列”形式。用三角列表示代数簇后，很多的性质变得非常容易计算，从而使得代数几何中的众多问题得到构造性解决。

设 $K[x_1,\cdots,x_n]$ 是域 K 上以 $x_1,\cdots,x_n$ 为变元的多项式组成的多项式环。设 E 是 K 的一个扩域。设 S 为多项式集合，我们用 $\mathrm{Zero}(S)$ 表示 S 中的多项式在 E 上的公共零点的集合。设 G 是另一多项式，$\mathrm{Zero}(S/G)$ 表示是 S 的但不是 G 的零点所组成的集合，称为拟代数集。

吴-Ritt 零点分解定理就是要给出任意拟代数簇的一个构造性描述。为此，我们需要下面的概念。一个多项式组称为升列，如果通过变量重新命名后可以写成如下形式

$$A_1(u_1,\cdots u_q,y_1)=I_1y_1^{d_1}+y_1\text{的低次项}$$

$A_2(u_1,\cdots u_q,y_1,y_2)=I_2y_2^{d_2}+y_2$的低次项

.....

$A_p(u_1,\cdots u_q,y_1,\cdots,y_p)=I_py_p^{d_p}+y_p$的低次项，

其中 $p+q=n$， $I_i\neq 0$ 称为 A_i 的初式。设 $A=[A_1,\cdots,A_p]$， J 为 A_i 的初式的乘积，我们认为 $\mathrm{Zero}(A/J)$ 的结构已经确定。如果进一步假定 A 是不可约的，则$\mathrm{SAT}(AS)=$对 AS 做伪除法余式为零的多项式的集合是一个素理想。

设 PS 为一多项式的非空集合，一升列 CS： $f_1,\cdots,f_r$ 称为 PS 的吴特征列，如果 $f_i\in\mathrm{Ideal}(PS)$ 且对任一多项式 $f\in PS$， f 对 CS 的余式为零。我们有

定理 2.1 (吴-Ritt 零点分解定理). 对一非空多项式集合 PS 与一多项式 G 有：

$$\mathrm{Zero}(PS/G)=\bigcup_k\mathrm{Zero}(A_k/J_kG)$$

其中 A_k 是升列， J_k 为 A_k 中多项式的初式之乘积。

在上述定理中，通过对诸 A_k 中的多项式依次做代数扩域上的因式分解并计算$\mathrm{SAT}(ASC)$ 的基，可以得到：

定理 2.2 (代数簇的唯一分解). 对任意多项式的非空集合 PS ，我们可以求得不可约升列 A_i 与素理想 $\mathrm{SAT}(A_i)$ 的生成基 PS_i 使得

$$\mathrm{Zero}(PS)=\bigcup_i\mathrm{Zero}(\mathrm{SAT}(A_i))=\bigcup_i\mathrm{Zero}(PS_i)$$

且以上分解中任何一个分支都不能去掉。

作为升列的应用，吴文俊提出母点可以由不可约升列显式给出。设 E 为数域 K 的扩域。 E^n 中点 m 称为点 z 的母元或 z 称为 m 的子元，如果对任意 $F(x)\in K[x]$ 由 $F(m)=0$ 可以推出 $F(z)=0$。点 m 的所有子元的集合记为 $\mathrm{Spec}(m)$。不难证明 $\mathrm{Spec}(m)$ 是一个不可约代数簇，点 m 称其母点。

设 $A=\{f_1(u,y_1),f_2(u,y_1,\mathrm{y}_2),\cdots,f_1(u,y_1,\cdots,\mathrm{y}_p)\}$ 为一个不可约升列。将变量 u 代换为一组自由变量后可以依次求得 $y_1,\cdots,y_p$ ，从而得到 A 的一组解 a ，称为升列 A 的母点。我们有

定理 2.3 设不可约升列 A 的母点为 $m(A)$ ，则 $\mathrm{Zero}(\mathrm{SAT}(A))=\mathrm{Spec}(m(A))$。

也就是说，任意不可约代数簇的母点均可表示为一个不可约升列的母点。所以，我们可以用不可约升列作为母点的构造性表示。吴还给出了由升列求相应素理想的 Chow 形式的方法。由此，得到了不可约代数簇不同表示的转换算法：

一般理想的生成基 ⇒ 母点 ⇒ Chow 形式 ⇒ 素理想的生成基。

投影可以看作结式概念的推广。设 PS 是 $K[u_1,\ldots,u_m,x_1,\cdots,x_n]$ 中的多项式集合，D 是其中多项式，E 是 K 的代数闭包，我们定义投影的概念如下

$$\mathrm{Proj}_{x_1\wedge x_n}\mathrm{Zero}(PS/D)=\left\{e\in E^m \mid \exists a\in E^n, \text{使得}(e,a)\in \mathrm{Zero}(PS/D)\right\}$$

不难看出，投影实际上给出了一个方程组对于变量 x_i 有解的条件。作为零点分解定理的应用，吴证明了：

定理 2.4 拟代数集的投影是若干拟代数集的并。进一步，存在一个算法在有限步内求得下面分解

$$\mathrm{Proj}_{x_1\wedge x_n}\mathrm{Zero}(PS/D)\mathrm{Y}_{i=1}^{s}\mathrm{Zero}(A_i/HI_i)$$

其中 A_i 是 $K(U)$ 中的升列， H 是 $K(U)$ 中的多项式， I_i 是 AS_i 的初式之乘积。这里 U 代表变量 $u_1,\cdots,u_m$。

对一般代数簇，Grothendieck 引进了陈省身示性类的概念，但须假定代数簇没有奇点。利用不可约代数簇母点的概念，吴文俊于 1965 年对具有任意奇点的代数簇成功地建立了陈省身示性类的概念。当代数簇光滑时，吴给出的定义就是通常的陈省身示性类。而且他所定义的陈示性类是具体可计算的。由于文革的耽搁，这一理论未能得到及时发展。1980 年后，应用这一定义，吴、石赫证明了丘成桐-Miyaoka 不等式的多种推广。刘先仿证明了吴定义的陈类是有理等价类，并用这一定义给出了计算代数曲线亏格的新公式。刘先仿还证明了吴的定义于 20 世纪 70 年代出现的另外两种定义之间的关系：Mather 的定义与吴的定义等价，但 MacPheson 的定义与吴的定义不同。

吴文俊特征基方法发表后导致了一系列对这一方法的研究。Gallo 与 Mishra 分析了多项式特征基的计算复杂性问题。Chou 与高小山提出了另一种弱特征基并证明了特征基的单纯性。Kalkbrener、张景中、杨路等提出了正规升列与无公因子升列的概念及其计算方法。Lazard、王东明等人研究了各种升列的代数性质。Richardson 研究了吴-Ritt 零点分解定理在一类解析函数中的推广。李洪波研究了吴-Ritt 零点分解定理在 Clifford 代数中的推广。 李邦河提出了带重数的特征列方法。Maza 等人发展了基于高性能计算的特征列方法。

吴文俊还将以上方法推广至微分多项式，得到了微分代数方程的零点分解定理。 这一工作也有众多的追随者。吴文俊还首先指出，由 Buchberger 引入的 Groebner 基实际上可以由基于偏微可积理论中的 Riquier-Janet 理论导出。最近，高小山等给出了代数差分方程的吴-Ritt 零点分解定理。至此，吴-Ritt 零点分解定理与特征列方法已经可以用于代数、代数微分、代数差分三类方程，涵盖了一大类数学与应用问题。相关的工作可参见[1,3,6,9,10,11]。

3、数学机械化方法的应用

吴文俊选择方程求解作为其数学机械化研究的主要内容是有一定的必然性的。17 世纪，笛卡尔（Descartes）曾提出一般问题求解的下列构想：

任意问题的解答

→数学问题的解答

→代数问题的解答

→方程组求解

→单个方程求解

Polya 评价道：“这一构想虽未成功，但它仍不失为一个伟大的设想。即使失败了，它对于科学发展的影响比起千万个成功的小设想来，仍然要大的多。”这是因为虽然这一设想不能涵盖所有问题，但却包括了大量有意义的问题。例如，几何定理机器证明的吴方法就是方程求解方法的成功应用。

3.1 几何自动推理的吴方法

定理证明机械化思想由来已久，一些原始想法可以追溯到 17 世纪的莱布尼兹（Leibniz）和笛卡尔（Descartes）。现在流行的几何自动推理方法可以分为三类：以 Herbrand 理论及归结法为代表的逻辑方法；以 Newell，Simon 等人为代表的人工智能方法；以 Tarski 理论与吴方法为代表的代数方法。

几何定理证明的机械化可以追溯到 20 世纪 30 年代，Tarski 证明了实闭域的判定算法，从而给出了初等几何的判定算法。这一算法虽经 Seirdenberg, Collins 等人的改进，仍然太繁杂以至于不能证明有意义的几何定理。在计算机上尝试证明几何定理始自 20 世纪 50 年代末 Gelernter 等人的经典工作。但此后几十年这方面进展不大。主要问题是所发现的方法均不够有效。吴文俊引入的基于代数计算的方法是第一个可以有效证明困难几何定理的方法。经过吴与其他人的后续工作，现在的情况是我们不仅可以有效地证明几何中的大部分定理，而且可以自动发现定理。不仅可以证明初等几何中的定理，还可以证明微分几何、力学中的定理。不仅可以证明定理，还可以生成定理的最短证明、多种证明。

几何定理机器证明的吴方法是吴-Ritt 零点分解定理的直接应用。通过建立坐标系，几何定理的假设可以写成多项式方程组 HS：

$$HS=\{h_1(x_1,\cdots,x_n)=0,\cdots,h_r(x_1,\cdots,x_n)=0\},$$

结论写为：$C(x_1,\cdots,x_n)=0$。则几何定理正确与否等价于方程组 $HS=0$ 的解是否是 $C=0$ 的解。这一问题等价于根理想的包含问题。应用零点分解定理可以解决如下。由吴-Ritt 零点分解定理

$$\mathrm{Zero}(HS)=\mathrm{Y}_{i=1}^{t}\mathrm{Zero}(A_i/J_i)$$

其中 A_i 是不可约升列，J_i 是 A_i 中多项式的初式的乘积。我们有：结论 $C=0$ 在复零点集 $\mathrm{Zero}(AS_i/DI_i)$ 所对应的图形上正确当且仅当 $\mathrm{prem}(C,AS_i)=0$。由此，几何定理证明变为代数计算问题。

吴进一步观察到，应用以上方法证明几何定理存在若干问题。问题之一是几乎所有几何定理都是在某些在定理中没有明确给出的条件之下成立的。吴给出的算法不仅可以证明几个几何定理是否一般正确，而且可以给出定理成立的非退化条件。直观上讲，这等价于几何定理除了在一个低维的空间外成立，而我们可以不去关心这个低维空间的具体形式。这样做可以换来定理证明效率的提高。

吴-Ritt 分解定理不仅可以证明定理，还可以自动发现定理。原理如下：设 A 为分解中得到的升列，而 $A_1(u_1,\cdots,u_q,y_1)$ 为 AS 中第一个多项式。则我们实际上是求得了独立变量 U 与变量 y_1 之间的关系。这类问题实际上是求方程的流形解。在几何中这种问题经常遇到，几何公式的推导与轨迹方程的计算就是这样两类问题。吴曾设想用这一方法处理双曲空间中四面体的体积公式的公开问题。

上述想法可以推广至更一般的形式。给定一个复数（实数，微分）域上的一阶谓词逻辑公式

$$f = Q_1 x_{s_1} \cdots Q_k x_{s_k}(\varphi)$$

其中 Q_i 是谓词∃或者∀，φ 是一个语句。利用第 2 节中的投影定理与量词消去法消去变量 $x_{s_i},\cdots,x_{s_k}$，得到一个只含自由变量的公式 g 使得 f 与 g 在复数域上等价。我们实际上发现了一个新定理 g。这一方法又称为量词消去法。这实际上是定理自动证明最一般的形式。

吴还进一步提出了微分几何定理的机器证明方法。吴在访问美国能源部 Argonne 实验室时得知他们在研究如何由开普勒行星运动的经验定律自动推导牛顿万有引力定理，但结果并不理想。吴使用其特征列方法圆满地解决了这一问题。

吴方法于 20 世纪 70 年代末出现后，在国际上引发了一场关于几何定理机器证明研究与应用的高潮，若干结集出版的工作可见[1,2,3,4,5,6,11]。当时的一些情况可以参见周咸青教授的回忆文章。我本人的一些经历也可说明当时人们对这一工作的重视。我于 1988 年在吴文俊先生指导下获得博士学位后，赴美国德克萨斯大学 Austin 分校计算机系从事博士后研究。该校是美国人工智能研究的主要中心之一。在与 Boyer 等知名学者攀谈时，他们经常挂在嘴边的话是：吴是真正有创新性的学者。也有人对我讲，你来美国不是学习别人东西的，而带着中国的方法来的。我曾于 2008 年 3 月到位于意大利西西里岛的 Catania 大学参加纪念 Carrà-Ferro 的学术研讨会。受吴的工作的影响，该校的 Carrà-Ferro、Gallo 等人曾从事微分几何定理证明研究。时任计算机系主任的 Gallo 在其讲话中说道：二十年前，我们在同一个会议室开会，当时的明星客人是吴文俊（The star guest is Wu Wentun）。

3.2 基于吴-Ritt 零点分解定理的方程求解算法

零点分解定理实际上给出了方程符号求解的一个一般方法：由此可以给出方程组解的完整结构，在高维情形可以给出解流形。我们可以将方程求解的数学机械化方法归纳为几个主要步骤：首先，使用零点分解定理将一般的代数方程组变为若干三角形式的方程组或单变量的求解，进而可以通过函数分解将单个方程的求解简化为低次单变量方程的求解，对于不能再进一步化简的方程发展构造性算法进行解析求解。

沿着以上思路，吴本人以及数学机械化中心的科研人员做了大量的研究，包括：代数方程组的实根隔离，微分方程的函数分解，微分方程解析求解算法等。

代数方程组求解主要有两种方法：数值计算法与符号计算法。数值计算法有 Newton-Ralphson 迭代方法与同伦法等；符号计算法有 Groebner 基法、特征列法与结式法等。一般讲数值计算法具有速度快、应

用范围广等优点，但也有误差控制难、只能给出局部解等缺点。符号计算法则可以给出完全的精确解，但常遇到因中间多项式过大而导致的计算困难。最近的研究热点是将数值计算与符号计算相结合的混合运算。吴提出的符号计算与数值计算的混合算法主要解决了两个问题：

H1: 混合计算中的误差估计问题。

H2: 多项式的近似因式分解。

问题 H1：吴将一个近似数 a 表示为 a_0+t_0，其中 $|t_0|<10^{-N}$，$N>0$。将 t_0 当作变量，通过用特征基方法可以得到一个单变量多项式方程：

$$C_1=(a_0+T_0)x_1^n+\cdots+(a_n+T_n)$$

其中 a_i 为常数，T_i 为 $t_1,\cdots,t_r$ 的多项式。我们可以求解下列方程：

$$C_{10}=a_0x_1^n+\cdots a_n$$

两者之间的误差，可以用 Ostrowski 定理估计。

问题 H2：**设** $f,g,h\in Q[x_1,t_1,\cdots,t_r]$，其中 t_i 为取值很小的变量。我们说 f 可以 S 阶近似分解为 $g*h$，如果 $f-gh$ 对于 $t_1,\cdots,t_r$ 的阶数 $\geq S+1$。吴给出了将多项式近似分解为两个多项式乘积的算法。吴还证明了这一算法可以提供将多元多项式因式分解转换为单元多项式因式分解的多项式算法。

3.3.全局优化算法与不等式自动证明.

上面的方法是对复数域而言的。在 20 世纪 30 年代 Tarski 证明了实闭域的可判定性，从而证明了初等几何与初等代数的可判定性。这里，‘初等’是指一阶量词逻辑所能描述的公式，一般可以写为下列前束公式

$$F=(Q_kX_k)\cdots(Q_rX_r)\phi(X_1,\cdots,X_r)$$

其中 Q_i 代表量词，$\phi(x_1,\cdots,x_r)$ 为一个无量词公式。在 F 中 $x_1,\cdots,x_{k-1}$ 被称为自由变量，而 $x_k,\cdots,x_r$ 被称为约束变量。仅含束约变量的公式称为语句。

量词消去法是指：对上面给定的前束公式 F，给出一不含量词的公式 $\phi(x_1,\cdots,x_{k-1})$ 与之等价。

在已有的解决上述问题的算法中 Collins 提出的 CAD 算法最为有效，并且已在计算机上实现。这一算法处理不等式问题是完全的，但效率较低。针对一些常见的与不等式有关的问题，吴提出了求解下列优化问题的算法。

问题：设 D 为欧氏空间 R^n 中的区域，f 为 R^n 上的实多项式，试决定 f 在条件

$$h_i=0,\quad i=1,\cdots,n,\quad g\neq 0$$

下在区域 D 上的最大或最小值。这里涉及的函数都是多项式。

对于上述问题，吴证明了下面吴有限核定理。设 $HS=\{h_1,\cdots,h_n\}$，则存在一算法确定 f 在

Zero$(HS/g)\cap D$ 上的有限个值的集合 K，使得

K 中的最小值 $=f$ 在 $\mathrm{Zero}(HS/g)\cap D$ 上的最小值，

K 中的最大值 $=f$ 在 $\mathrm{Zero}(HS/g)\cap D$ 上的最大值。

这一算法的基本想法是首先用吴-Ritt 零点分解定理将 $\mathrm{Zero}(HS/g)$ 化为 $\mathrm{Zero}(A/J)$，其中 A 为升列，且 J 中包含 AS 的初式与隔离子。用拉格朗日方法求极值，可以证明极值的个数是有限的且包含在一个单变量多项式的零点之中。

吴将上述算法用于解决如下问题：给出多项式方程有正根的判断条件，非线性规划，机器人碰撞问题及代数与几何不等式自动证明。这一工作也有众多的后续工作。

3.4. 吴方法的其他应用

吴文俊特别强调方程求解算法的应用，并身体力行将他的方法用于解决力学、物理、化学等领域与机器人等高科技的问题。吴的方法还被用于多项式因式分解，发现微分系统新的极限环，求解微分方程的行波解与孤立子解，理论物理，几何造型中的曲面形式转换问题，一阶逻辑公式的证明，计算机视觉，控制理论，连杆设计问题，智能 CAD 与计算机动画。参见[3,4,10].

4、评价与影响

吴文俊关于数学机械化的工作获得了国内外学术界的高度评价与重视。具体表现在下面几个方面。

高度评价

早在 1982 年，美国人工智能协会主席 W. Bledsoe 和两位麦卡锡（McCarthy）奖获得者 R. S. Boyer 和 J. S. Moore 联名致信我国主管科技工作的领导人，赞扬吴的工作是“最近十年中自动推理领域出现的最为激动人心的进展”。他们认为：“在过去两年中，我们这个领域（自动推理）最好的工作之一是吴的工作。吴的平面几何自动定理证明的工作是一流的。他独自使中国在该领域进入国际领先地位。”

论文[8]是吴文俊关于数学机械化工作最重要的论文，给出了方程求解的特征列方法与几何定理机器证明原理。本文后由国际自动推理权威杂志 JAR 全文转载。JAR 编委专门为转载写了短评(JAR,2, 219-220, 1986)，对这一论文给予高度评价。其中提到：“几何是激发人类思考‘我们怎样推理？’这一问题的最古老的数学分支之一。因此几何自动推理的任何进展都特别有意义。由中国科学院系统科学所杰出中国数学家吴文俊完成的如下论文，不仅建立了几何高效推理的基础（lay founndation），而且马上建立的一个杰出的标准（remarkable standard）来衡量以后出现的几何定理证明器。”

JAR 主编 Kapur 在他的多篇文章中引用吴的工作，称 “吴的工作使几何定理自动证明领域得到复兴。”他认为“可以毫不夸张地说，吴的工作使几何自动推理领域发生了革命性变化。吴的初始工作以及吴和其它人的后续工作是过去十年中自动推理领域中最重要得进展。”Kapur 本人还研究吴方法的各种改

进，并将吴方法用于定理证明与计算机视觉。

自动推理领域创始人之一，JAR 前主编 L. Wos 认为“吴在自动推理领域的杰出贡献是不可磨灭的。”“没有一个数学领域象自动推理这样从一个人那里得到这样多的贡献。”

吴文俊与 David Mumford 于 2006 年共同获得邵逸夫数学奖。吴文俊获奖主要是由于他对于“数学机械化这一交叉领域的贡献”。授奖词中提到：“吴的这一方法使该领域发生了一次彻底的革命性变化，并导致了该领域研究方法的变革。通过引入深邃的数学想法，吴开辟了一种全新的方法，该方法被证明在解决一大类问题上都是极为有效的，而不仅仅是局限在初等几何领域。”

广泛影响

吴的工作自 20 世纪 80 年代中期传到国外，引起了国际自动推理与计算机代数领域的高度重视。一些情况可以参见周咸青教授的回忆文章。吴的工作使得几何定理自动证明及与之有关的消去法研究变为热门的研究方向。国外大学与科研机构连续召开研讨会介绍这方面内容。其中有：

1. “Geometric Reasoning”, Oxford University, 1986. 会议文集作为国际著名刊物 AI（人工智能）的专辑出版，后又在 MIT 出版社出版[4]。

2. “Computer-Aided Geometric Reasoning”, INRIA, France, 1987.

3. “International Workshop on Algorithmic Aspect of Geometry and Algebra,” Cornell University, 1988.

很多有影响的国际会议如 ACM-ISSAC（符号计算）与 CADE（自动推理）还设立关于吴方法的分会。目前，关于数学机械化的国际会议有 “几何自动推理国际”系列会议与“亚洲计算机数学”系列会议。

吴方法被编入国际上非常流行的软件 MAPLE。关于几何定理证明的吴方法被编入“几何专家”软件，并在科技界甚至台湾和大陆数百所中、小学中使用。

Springer， Kluwer，MIT，Academic，World Scientific 等出版社出版了关于吴方法的专著。其主要内容是关于吴方法的改进与应用。吴方法还在由 Springer 出版的研究生与大学生教材与专著中被列专门章节介绍。

众多奖励

吴文俊相继荣获第三世界科学院“数学奖”、陈嘉庚基金会“数理科学奖”、香港求是科技基金会“杰出科学家奖”。特别是在，1997 年获得了国际自动推理最高奖“Herbrand 自动推理杰出成就奖”。该奖的获奖人包括自动推理创始人之一 Larry Wos，自动推理创始人之一、前美国人工智能学会主席 Woody Bledsoe，归结法的发明人 Alan Robinson 等。2000 年获得首届国家最高科技奖。2006 年获得有东方诺贝尔奖之称的邵逸夫奖。

得到大力支持

数学机械化研究得到国家科研领导部门的重视与支持。国家自然科学基金委通过多种形式支持数学机械化研究。1990 年，国家科委拨专款支持数学机械化研究，中科院批准成立数学机械化研究中心并多次拨款支持数学机械化研究，2002 年成立数学机械化重点实验室。1992 年国家“八五”攀登计划项目“机器证明及其应用”立项。1998 年国家重点基础研究发展规划项目“数学机械化与自动推理平台”立项，2004 年国家重点基础研究发展规划项目“数学机械化方法及其在信息技术中的应用”立项。在美国，周咸青主持的关于几何推理的科研小组从 1985 年起连续得到美国自然科学基金委五次支持。

参考文献

[1] Chou S C. Mechanical Geometry Theorem Proving, D. Reidel Pub. Company, Dordrecht, 1988。

[2] Chou S C, Gao X S and Zhang J Z. Machine Proof in Geometry, World Scientific Publishing Co., Singapore, 1994

[3] Gao X S and Wang D. Mathematics Mechanization and Applications, Academic Press, London, 2000.

[4] Kapur D and Mundy J. Geometric Reasoning, MIT Press, 1988.

[5] Li H. Invariant Algebras and Geometric Reasoning. World Scientific, Singapore. 2008。

[6] Wang D. Elimination Methods, Springer, 2001.

[7] Wu W T. On the decision problem and the mechanization of theorem-proving in elementary geometry, Scientia Sinica，1978, 21: 159-172.

[8] Wu W T. Basic principles of mechanical theorem-proving in elementary geometries, J. Sys. Sci. & Math. Scis.,1984, 4: 207-235. Re-published in J. Automated Reasoning, 1986, 2: 221-252.

[9] Wu W T. Basic principles of mechanical theorem proving in geometries, (in Chinese), Science Press, Beijing (1984). English translation, Springer (1994).

[10] Wu W T. Mathematics-Mechanization, 1999, Science Press.

[11] Yang L, Zhang J.Z and Hou X R. Non-linear Algebraic Equations and Automated Theorem Proving, Shanghai Science and Education Pub., 1996.