一、基本信息

实验室中文名称：中国科学院数学机械化重点实验室

实验室英文名称：Key Laboratory of Mathematics Mechanization (KLMM) ，CAS

实验室代码： **2002DP173012**

依托单位： 中国科学院数学与系统科学研究院

实验室主任： 李洪波

实验室学术委员会主任：李邦河

通讯地址： 北京海淀区中关村东路 55 号

联系人： 周代珍、李佳

联系电话： 82541851

传真： 82541809

E-MAIL： **dzhou@mmrc.iss.ac.cn**； **jiali@mmrc.iss.ac.cn**

网址： http://mmrc.amss.cas.cn/

学科与学位点：

	学科 1		学科 2		学科 3	
	名称	代码	名称	代码	名称	代码
学科分类	数学				计算机科学与技术	
硕士点	基础数学	070101	应用数学	070104	计算机科学与技术	080605
博士点	基础数学	070101	应用数学	070104	计算机科学与技术	080605
博士后站	基础数学	070101	应用数学	070104		
研究性质	□基础研究 □应用基础研究					
归口领域(选 1 项)	□数理					

注：学科与代码可参考国务院学位办颁布的“授予博士、硕士学位和培养研究生的学科、专业目录”

二、实验室概况

数学机械化研究的意义与实验室的发展简介

在目前的信息时代，计算机可以认为是人脑的延伸，电子计算机的飞速发展，为人类实现脑力劳动的机械化创造了物质条件。逐步实现脑力劳动机械化，将为科学研究与高新技术创新提供有力工具，使科研工作者摆脱繁琐的甚至是人力难以胜任的工作，将自己的聪明才智集中到更高层次的创新性研究上，提高我国知识与技术创新的效率。在以产业革命为先导的体力劳动机械化过程中，我国落后于发达国家，长期处于被动的局面。今天，脑力劳动机械化的进程刚刚起步，我们应该牢牢把握这个机遇，努力使我国在知识经济时代居于有利地位。

实现数学的机械化是实现脑力劳动机械化的重要基础。数学为其他学科提供描述问题的语言与解决问题的有效方法，是自然科学与高新技术的重要理论基础，是联络科学与技术的纽带。正是由于数学的基础性，每个时代都有与之相适应的数学。为利用计算机的强大计算能力，数学的很大一部分内容正在转变为计算机可以理解的语言和可以操作的对象，具体讲就是数学的离散化、算法化与软件化。这样的数学可以称之为机械化数学。

上世纪五十年代，电子计算机刚刚产生，人工智能的创始者 Newell 等人就开始研究用计算机证明数学定理。这些研究在理论上取得了重大进展，出现了以 Robinson 归结法为代表的一系列方法。但在证明效率上，这些方法未能取得本质突破。二十世纪七十年代出现了符号计算研究领域，研究具体数学问题的求解与计算方法。MIT 推出了第一代符号计算通用软件 MACSYMA，产生了轰动性影响。今天，数学和计算机的交叉正在成为数学发展的主要潮流之一，产生了诸如计算代数、计算数论、计算群论、计算几何等新兴学科。符号计算研究还导致了 Maple、Mathematica 等商用数学软件的出现，在科学与高新技术研究中得到广泛应用。

正是在此背景下，吴文俊院士在二十世纪七十年代提出了数学机械化的设想，概括为如下的“数学机械化纲领”:

- 在数学的各个学科选择适当的范围实现机械化，推动数学发展与脑力劳

动机械化;

- 应用数学机械化方法解决相关高科技领域的关键问题。

1990 年，中国科学院批准成立“数学机械化中心”。科学院在中心成立的批复中指出：“为了保证吴文俊教授建立的机器证明理论持续不断地发展，进一步形成数学机械化研究的良好环境，经研究，同意你所(系统所)建立《中国科学院系统科学所数学机械化研究中心》”。强调“望你所按照科技体制改革的精神，以开放实验室的方式，联合国内外学术力量，为数学机械化研究做出更大的成绩”。

数学机械化研究中心建立以来，取得了一系列高水平的科研成果，并获得了十数项国内重要奖励与六项重要国际奖励，包括国家最高科技奖(00), 劭逸夫数学奖(06), Herbrand 自动推理杰出成就奖(97), 第三世界科学院数学奖(90), 陈嘉庚数理科学奖(93)、香港求是科技基金会杰出科学家奖(94)，国家自然科学二等奖一项(97)，中科院自然科学一等奖(95)，求是杰出青年学者奖两项(98,99)，ACM/SIGSAM 杰出论文奖三项(06,07,11)。数学机械化中心还作为主持单位承担了八五国家攀登项目，九五攀登项目，三个“973”项目，和两个基金委创新群体项目。

实验室万哲先院士从 20 世纪 60 年代开始，在离散数学的重要方向：有限域上典型群的几何学取得系统的研究成果，并开创了该方向的多个应用领域，包括区组设计、格、编码理论及信息安全中的认证码等。万哲先还是我国最早从事信息安全与通讯理论中的编码和密码学研究的几个数学家之一。他的工作不仅在国内外获得同行的广泛引用，还为我国国防建设做出了重要贡献，曾获中国科学院科技进步一等奖，国家自然科学三等奖，中国科学院自然科学奖一等奖和华罗庚奖。为加强离散数学与信息安全方面的研究，数学与系统科学研究院于 2001 年成立“信息安全研究中心”。

2002 年，中国科学院批准以“数学机械化中心”与“信息安全研究中心”为基础，成立数学机械化重点实验室。

背景介绍：计算机数学与数学机械化

计算机数学，顾名思义，是研究应用计算机解决各类问题需要的数学。计算机数学关注“什么是可以计算的”，对于可计算的问题，则关注设计求解该问题的最好算法。所以，我们可以简单地说计算机数学是研究算法的数学。计算机科学大师 D. Knuth 将计算机科学定义为研究算法的学问。其实，计算机数学是数学与计算机科学的交叉领域：计算机数学是计算机科学的理论基础，也是研究计算与算法的数学分支。

计算机数学大致可以分为以下三部分。

首先，为算法研究提供数学工具的是离散数学。与传统的连续数学或分析数学不同，离散数学研究离散对象的数学结构，主要包括：集合论、图论、组合数学、抽象代数等。纯粹数学更关心数学对象的结构与分类，而离散数学则侧重研究相关的算法问题。例如，对于数论中的素数，数学家更关心的是素数的分布，而计算机数学则更关心是否存在分解大整数的快速算法。另一方面，两者又密切相关。大整数分解算法的研究需要数论、代数几何等学科的支撑。一个明显的事实是，由于计算机的广泛使用，离散数学在近半个多世纪以来得到了复兴。一些连续数学分支，为了借助计算机求解，也发展了离散化理论。例如，微分方程求解的有限元方法，即通过离散化将微分方程求解变为代数方程求解。又例如，为了处理计算机图形学中出现的离散曲线与曲面，出现了离散微分几何。

其次，关于算法共性的研究已经形成一个专门的学科，即计算理论或理论计算机科学，其核心内容是判定性问题与计算复杂度理论。从算法角度研究一个问题，首先需要知道是否存在求解给定问题的算法，即判定性问题或可计算问题。许多重大数学问题由于判定性问题的研究得到澄清。例如，一个公理体系内的所有命题是否可以判断？什么是可计算的？特别是，实数是否可以计算？等等。对于一个可判定的问题，我们需要设计求解该问题的“好的算法”。一个算法的好坏，可以从其时间计算复杂度与空间计算复杂度来判断。所谓时间计算复杂度可以简单理解成求解问题所需的步骤数，而空间计算复杂度则是求解问题所需要的存贮空间。计算复杂度理论的主要任务是对各种计算问题根

据其计算复杂度进行分类。

最后，数学本身也因为计算机的使用而得到了长足的发展。一些重大的遗留问题，如四色定理与 Kepler 猜想，借助计算机得到了解决。更重要的是，出现了一批借助计算机研究数学自身的分支，如计算数学或数值计算(一般不归在计算机数学)、自动推理、计算机代数、计算数论、计算代数几何、计算拓扑、计算几何、符号分析等。这里，每一个学科的出现都有双重目的。例如，计算数论不仅丰富了数论的内涵，还是密码与编码等重要信息技术的数学基础。近二十年来，数学和计算机科学中的一些强有力工具和最新研究成果被用到编码理论和密码学中，不仅促进了编码理论和现代密码学的飞速发展，也刺激了数学和计算机科学中的一些分支的发展。例如，编码理论中的 Berlekamp 分解算法和 Berlekamp-Massey 算法是符号计算中若干算法的基础。如今，算法这一概念，就像方程、公式一样，已经成为日常数学语言的一部分。

计算机最初(现在也仍然是)主要应用于工程计算，其中主要用到的是近似计算。一个自然的问题是：计算机是否可以通过进行精确的计算与推理用于数学研究？我们是否可以利用计算机的强大计算能力自动或半自动地解决数学问题？由于定理证明是数学最核心的内容，我们是否可以用计算机证明定理？

吴文俊在上世纪 70 年代末就敏锐地指出，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起到重大影响。他将可以借助计算机进行计算与推理的数学称为机械化数学。所谓机械化是指刻板化与规格化。十七世纪以来，以蒸气机为代表的工业革命是以机器代替人的体力劳动，数学机械化则是用计算机部分代替人类数学计算和演绎的脑力劳动。电子计算机的飞速发展，使得数学的机械化正在逐步成为现实。在数学发展过程中，演绎倾向与算法倾向此消彼长，两种倾向总是交替地处于主导地位，但并不是严格对立的；探索新算法可以导致数学的重大发现，如解析几何与微积分，而且构造性的演绎往往具有很高的实用价值。

电子计算机的出现不过数十年，而算法的概念却源远流长。回顾数学发展史，主要有两种思想：一是公理化思想，另一是算法化或机械化思想。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，无一不与数学机械化思想有关，并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，检查数学史可以发现，数学的多次重大跃进无不与机械化思想有关。数学启蒙中的四则运算由于代数学的出现而实现了机械化。线性方程组求解中的消去法是机械化思想的杰作。对近代数学起着决定作用的微积分也是得益于经阿拉伯传入欧洲的东方数学的机械化思想。在现代纯粹数学研究中，机械化思想也一直发挥着重大作用。Hilbert 倡导的数学判定性问题的研究导致了数理逻辑的突破性发展并为计算机的设计原理做了准备。E. Cartan 关于微分方程、微分几何及李群的著作中经常显现出机械化特色。H. Cartan 关于代数拓扑学同调群计算的工作可以看作是机械化思想的成功范例。

数学机械化思想的明确提出可以追溯到 17 世纪法国思想家 R. Descartes。Descartes 认为，代数可以将数学机械化，使思维变得简单，不再需要繁复的脑力劳动，数学创造也极可能成为自动。甚至逻辑原理和方法也可以被符号化，进而所有的推理过都实现机械化。Descartes 还将他这一设想具体化，提出一个求解一般问题的具体构想：将任意问题的解答归结为数学问题的解答，将数学问题的解答归结为代数问题的解答，将代数问题的解答归结为方程组求解，最后方程组的求解可以归结为单个方程求解。Polya 评价到：“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，但却包括了大量有重要意义的问题。

G. Leibniz 发展了 Descartes 的想法，并开始了一个更加雄心勃勃的计划。Leibniz 提出应该发展一种广义计算，这种计算可以使人们在所有的领域都能机械地、不费力地，通过一种像算术与代数那样的演算来达到精确的推理。这种方法将“使真理昭然若揭，颠扑不破，就像是建立在机械化的基础之上。”

Descartes 和 Leibniz 提出的想法是比较笼统的。19 世纪中叶，G. Boole 创立了现在所说的 Boole 代数，把思维在某种程度上形式化，用代数形式加以描述。这一工作比起 Leibniz 和 Descartes 的想法至少有了某种程度的数学化。20 世纪 20 年代，D. Hilbert 正式提出了所谓的“Hilbert 计划”，试图通过公理化建

立数学的严格基础。特别是，Hilbert 在其计划中提出了判定性问题，即是否存在一个算法“机械化”地判定每个数学分支中所有命题的正确性。

1931 年，奥地利数理逻辑学家 Goedel 证明，即使是 Peano 算术这样简单的数学系统，也存在定理，尽管我们知道是对的，却不能够证出来。Hilbert 希望证明数学是圆满无缺的，是相容的，是可以判断的。Goedel 的结论指出，Hilbert 计划太过理想，对于很多数学学科，Hilbert 的数学公理化计划无法实现。Goedel 的结论是革命性的，人们首次严格证明有的知识是不可以推出或计算的。Hilbert 计划虽然不能完整实现，但对数学发展的影响是巨大的。计算理论与机械化数学都可以说是在 Hilbert 判定性问题的直接影响下产生的。

前面提到，从 Descartes 到 Hilbert，都是机械化数学的支持者与倡导者。机械化数学发展的相对滞后与相关问题的计算复杂性密切相关。首先，Goedel、Turing 的结果否定了整个数学学科机械化的可能性。这些反面结果影响巨大，以至于形成了数学不可以机械化的固定思维。实际上恰恰相反，与 Goedel 的著名结果几乎同时，法国数学家 J. Herbrand 在 1931 年写出了题为“论算术的相容性”的论文。Herbrand 创立了一种证明定理的算法。这种算法提供了一种进行推理的途径，如果一个命题存在一个证明，则算法在有限的步骤之内结束并给出命题的证明。这一算法是半判定性的，即算法对于某些输入可能不中止，从而不能得出结论。结合 Goedel 的结果，我们可以看到，Herbrand 实际上已经给出了 Hilbert 判定问题理论上的完整解答。由 Goedel 的结果，有些定理是不能够由公理推出的。此时，Herbrand 的算法将不中止。其余的定理都可以由公理推出，而对于这些定理，Herbrand 的算法将给出证明。那么，数学定理的机器证明问题是否解决了？答案当然是否定的。Herbrand 算法的主要问题在于，其计算复杂度是指数的。虽然理论上可行，但实际上不能用于在计算机上证明非平凡的数学定理。

真正在计算机上自动证明定理始于上世纪 50 年代中期。一些计算机科学家，包括 Newell、Simon、Shaw 等人，创立了人工智能学科，尝试利用计算机进行某种脑力劳动，特别地证明数学定理。由此成长起来一门新的学问—自动推理或机器证明。自动推理前期的主流工作是对 Herbrand 算法的改进，希望通过发展各种技巧简化 Herbrand 算法的计算复杂度。但是，一般机器证明算法的发展并不理想，因为定理证明是一个计算复杂度非常高的问题。机器证明的主

流逐渐演变为机器验证。

机器验证的主要思路是使用一些高效但不完全的自动推理工具进行自动推理。在自动推理不能进行下去的时候，允许用户通过增加引理等手段提供证明思路。如此多次反复，最后由计算机将证明自动生成。由此生成的证明，虽然不是完全自动的，却是严格验证的。机器验证的思路是成功的。一些重要的数学猜想，借助于计算机验证得到解决。基于这一思路开发的软件已经是计算机芯片正确性验证软件的核心技术。

1976 年 K. Appel 与 W. Haken 宣布借助计算机证明了图论中的四色定理。这一证明由于“不可读”，未能被广泛接收。1997 年，Robertson 等人基于 Appel 与 Haken 的思路，给出了四色定理一个更简单的证明，使得四色定理的证明得到了初步承认。2005 年，G. Gonthier 借助通用机器验证软件平台 Coq 给出了四色定理的第一个真正的“机器证明”，即这一证明是经过计算机自动检验的，因此可信度非常高。

另外一个著名的例子是 Kepler 猜想的解决。Kepler 猜想是关于球在空间中最佳堆积的猜想，已经有四百多年的历史。H. Thomas 使用计算机验证了大量的情形，并最终宣称证明了这一猜想。与 Appel 与 Haken 的遭遇不同，Thomas 的结果基本得到数学界的承认，并发表在数学顶级杂志《数学年刊》上。

在以上两个例子中，虽然著名的猜想被证明,但是用于证明的方法仅仅是针对这两个问题，似乎并未产生广泛的应用。现在，我们介绍了两种极端情形。Herbrand 算法非常一般，但是不能解决具体问题。四色定理与 Kepler 猜想的证明方法又非常特殊，不能用于其他问题。那么，有没有一条可行的中间之路呢？回答是肯定的。

我们用吴文俊关于几何定理机器证明的工作给予说明。

几何定理机器证明是人工智能创始时即最早尝试的数学问题，主要原因是几何推理自古被认为是严格推理的典范，而且一般认为几何定理的证明技巧性很强。但是，基于人工智能方法所开发的软件效率不高，只能证明非常简单的几何定理。1950 年，波兰数学家 A. Tarski 证明初等代数和初等几何定理可以用一种代数算法来证明或否定，即初等几何是可以判定的。但是 Tarski 算法的复

杂度太高，以至于不能用来证明有意义的定理。吴文俊于 1978 年发表了几何定理机器证明的代数方法，在几何定理机器证明方面取得突破。“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 Kepler 定律推出 Newton 定律；用于解决化学平衡问题；与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。”

受到自己工作的启发，吴文俊在写于 1979-1981 年期间的几篇文章中明确指出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”的研究思路：“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，又不至太大以至于不可机械化，提出切实可行的方法，实现机械化，推动数学发展，并以此为基础解决高科技问题。” 吴文俊的基本想法是 Herbrand 的方法太广，以至于不够有效，而 Appel 与 Haken 类型的方法又应用范围太窄，不能为他人所用。数学机械化正确之路应该是选择有意义的一类问题，发展统一求解的高效算法，逐步实现数学的机械化。近年来蓬勃发展的符号计算、计算代数几何、计算数论、计算群论、计算拓扑、符号分析等新兴学科无疑说明了吴文俊以上观点的正确性。

"数学机械化"是脑力劳动机械化在数学科学的学术实践。数学机械化思想继承了中国古代数学的传统，它的着眼点在数学，但又具有明显的交叉性。

实验室的主要研究方向

实验室主要研究方向包括：数学机械化理论、信息安全的数学理论、数学机械化方法的高技术应用与智能软件开发。具体介绍如下：

- **数学机械化理论。**

(1) 符号计算

符号计算主要研究在计算机上如何有效的进行符号公式的精确计算，是计算机数学的基础。符号计算对于计算机数学的作用正如数值计算对于计算数学。符号计算形成于 20 世纪 60 年代，当时的标志性成果是多项式 GCD 与因式分解的快速算法。符号计算主要研究内容包括：基本代数运算的符号算法、矩阵的符号算法、多项式系统的符号算法、微分与差分方程的符号算法、符号分析等。以符号计算为基础的数学软件 Mathematica 与 Maple 已经被广泛使用。代数与微分非线性方程组的求解算法一般是指数的。为了提高符号算法解决实际问题的能力，人们提出混合计算方法，通过将符号计算、数值计算、优化算法等结合，得到速度快又能保证计算结果正确的可信算法。

(2) 计算代数几何

计算代数几何研究、设计和应用求解多项式方程组的算法，这些算法描述、操作、分解多项式方程组定义的代数簇。 它的理论基础来源于经典消元理论、代数特征列方法、 Groebner 基理论和奇点消解理论等；它的算法实现基于符号计算软件。

计算代数几何的主要研究成果包括：代数曲线与曲面的参数化与隐式化、代数簇的特征列表示、代数簇的不可约分解、多项式理想维数和 Hilbert 多项式的计算、多项式理想的准素分解、稀疏结式理论等；这些算法和相应的技术导致了代数几何的新的应用。 例如：几何定理机器证明、计算机辅助几何设计、机器人学、编码和密码学、芯片设计和数独游戏等。

(3) 计算几何

计算几何是由函数逼近论、微分几何、代数几何、计算数学等形成的边缘学科，研究几何目标在计算机环境内的数学表示、编辑、计算和传输等方面的理论与方法及相关的应用。另外一种理解是，计算几何是计算机科学的一个分

支，研究可以采用几何术语陈述的算法，同时也是一个数学分支，研究几何算法中产生的纯粹几何问题。计算几何的产生主要受计算机图形学、计算机辅助设计/制造（CAD/CAM）和数学可视化的推动。它在机器人运动规划和可视化、地理信息系统、集成电路设计、计算机辅助工程、计算机视觉中也有重要应用。计算几何也常常被称为 CAGD(Computer Aided Geometric Design，计算机辅助几何设计)， 1972 年在美国举行 CAGD 第一次国际会议，标志计算几何学科的形成。

计算几何的主要分支包括三个：（i）组合计算几何：也称为算法几何，其中几何体以离散的形式出现，包括点、线段、多边形、多面体等，典型算法包括凸包计算、Delaunay 三角化、网格生成等；（ii）数值计算几何：也称为计算机辅助几何设计，或者叫几何建模，其中几何体以连续的数值形式出现，典型算法包括参数化方法、水平集方法等，研究如何描述现实世界中的曲线、曲面以方便在 CAD/CAM 系统进行计算，目前已广泛应用于造船、航空、汽车及众多工业产品的外形设计和制造领域；（iii）符号计算几何：也称为几何演绎或几何推理，其中几何体以符号代数中的元素的形式出现，包括符号系数或整系数的代数曲线和曲面，涉及的符号代数包括交换代数、格拉斯曼代数、张量代数等，典型算法包括几何自动推理的特征列方法、几何不变量方法等，研究几何体、几何量和几何约束之间的未知关联。

苏步青先生开创了我国计算几何研究的先河，他首次给出了三次参数曲线存在两拐点的充要条件及一个重要的相对仿射不变量并于 1981 年出版了我国计算几何方面的首部专著《计算几何》。

(4) 计算拓扑

计算拓扑是拓扑学与计算几何和计算复杂性理论交叉的一门科学，也称为算法拓扑，主要研究两类问题，一类是拓扑问题求解的有效算法，另一类是使用拓扑方法解决来自其他领域的算法问题。主要分支包括：（i）算法三维流形理论，通过整数线性规划算法研究三角化三维流形的同胚识别、构造、分解、双曲结构的寻找等；（ii）算法扭结理论，包括扭结的亏格、亚历山大多项式的计算，通过算法将平面扭结转换为带尖的三角化等；（iii）计算同伦论：包括球面和其他简单拓扑空间的同伦群计算、多项式方程组求解的同伦算法等；（iv）点云数据的非线性结构分析，采用代数拓扑、离散计算几何、非线性逼近和统

计等技术对三维点云数据进行计算机处理，包括奇异点等特征的识别、分割、匹配、压缩，以及其他定性性质。 目前，计算拓扑在蛋白质结构分析，分子动力学模拟，图像分割、压缩与重建等方面发挥着一定作用。

(5) 计算群论

计算群论主要借助计算机研究群的结构与判定问题，是群论和算法复杂性理论的交叉学科。计算群论起源于 1911 年 Dehn 所提的 “字问题”。假定一个有限群的生成元以及生成关系给定，“字问题”是问能否找到一个算法判定该群中的两个表达式是否相同。计算群论的在上世纪六十年代开始受到广泛关注。这个领域吸引越来越多的人的注意，主要是因为关于群的很多计算靠手工完成是不现实的，而借助计算机则可能提供高效算法。计算群论是计算代数的一个分支，由于其很强的专业性一般作为一个独立的研究方向。

有限生成群的“字问题”是计算群论的一个基本问题。代表性成果包括：Novikov 与 Boone 证明“字问题”是不可判定的，有限生成群倍集计数的 Todd–Coxeter 算法与 Knuth–Bendix 算法。计算群论的其他主要结果包括：计算置换群阶数的 Schreier–Sims 算法，计算群的随机元素的乘积置换算法，对所有阶数小于 2000 的有限群的完全枚举，所有零散单群矩阵表示的计算，代数与微分 Galois 群的计算。两个广泛用于群论计算的计算机代数软件是 GAP 与 Magma.

(6) 符号分析

符号分析主要研究与求解微分和差分方程相关的代数理论和符号算法。研究的内容包括：积分与求和的理论和算法、对称群方法、微分不变量的计算、微分与差分的 Galois 理论、局部解和闭形式解、算子代数和组合恒等式证明等。这门学科的代数基础包括交换代数、非交换代数和代数群理论；其分析学背景包括：复分析、级数理论，相容性条件和李群等。

除了求解微分和差分方程，符号分析的结果还可以应用于特殊函数的表示和操作，组合恒等式证明。符号分析的著名算法有：计算不定积分的 Risch 方法， 计算线性常微分方程 Liouville 解的 Kovacic 方法和 Singer 方法，证明组合恒等式的 Zeilberger 方法等。

(7) 自动推理

自动推理是人工智能的重要研究方向，不仅有重大的理论意义，而且对实

际应用有深远的影响。人工智能的国际权威 R.S. Boyer 在周咸青、高小山和张景中的专著《Machine Proofs in Geometry》的前言中指出:“…构造和算法具有重大的实际意义。把计算约化为机械过程是计算工业(computing industry)的根基。每当一个数学领域从一些彼此不太相关的定理进化为一套统一的方法,就可能产生重大的应用。例如:把微积分的计算约化为查积分变换表的工作对于现代工程(modern engineering)的出现具有决定意义”。实验室在几何定理自动证明与发明、几何自动作图、几何不变量方法等方向已建立系统的机械化方法,在国际上具有明显的优势。

(8) 混合计算

数值计算具有速度快、适用范围广的特点,但是一般不能保证结果的整体正确性,符号计算可以对一大类问题提供完整与准确的解答,但是大部分已知的符号计算方法复杂度很高。符号-数值混合计算试图结合这两种算法,针对一大类问题,发展速度快并且可以给出满足这类问题完整求解所必需精度的可验证或误差可控算法。我们在基本的代数运算(例如:因式分解、最大公因子等),非线性代数方程组求解,全局优化等问题的混合算法方面做出重要工作。将继续这方面的研究并开拓新的研究方向,例如代数曲线曲面的可信逼近、半正定规划等。

(9) 非线性数学物理方程

非线性数学物理方程出现在很多重要的重要科学领域,例如 Bose-Einstein 凝聚态、材料、非线性光学、金融物理、生物、海洋学等。研究它们的非线性波结构及动力学性质具有重要的意义。数学机械化方法为非线性系统具有物理意义的解的求解问题提供了一般方法。我们系统第提出了求解非线性数学物理方程的高效机械化算法,并给出了在 Bose-Einstein 凝聚态、光学与金融等中有重要意义的物质波与畸形波解。

- **信息安全的数学理论。**

现代密码学是数学在信息科学中的杰出应用。密码技术作为解决信息安全问题的核心技术已获广泛共识。代数、数论、分析、几何等在密码算法的设计和分析中都起着核心的作用。

现代密码学诞生于 20 世纪 70 年代中期，主要有两个标志：

(i) DES (Data Encryption Standard) 于 1975 年 3 月 17 日被 The Federal Register 第一次公布，经过广泛公开的讨论于 1977 年 1 月 15 日作为数据加密的标准算法被采纳。

(ii)1976 年 Diffie and Hellman 提出公钥密码学，后来两人因此而获得图灵奖。公钥密码系统有两个密钥，一个是加密密钥，可以公开。另一个是解密密钥，要保密，不能公开。传统密码的加密密钥和解密密钥都要保密。公钥密码的提出，标志着密码学的新方向，是密码学的一场革命。

密码学主要分两部分：密码算法和密码协议。密码算法主要有加密算法、签名算法、Hash 函数、伪随机数生成器等。密码协议主要有密钥分发、密钥协商、身份识别、消息认证、秘密共享、多方安全计算、零知识等。它们都是密码学的重要内容。下面主要谈谈最重要的加密算法。

加密算法分为对称密码算法和公钥密码，对称密码又分为流密码和分组密码。

当今世界上大范围广泛使用的加密算法有 AES(Advanced Encryption Standard)，这是分组密码，是 DES 的升级版；以及两个广泛使用的公钥密码 RSA 和 ECC（椭圆曲线密码)；还有各种流密码算法，它们由于速度快、安全性高而倍受军方欢迎。

第一个实用的公钥密码系统于 1978 年由三个人 Rivest, Shamir, Adleman 所发明，后来这三人因此获得计算机科学的最高奖图灵(Turing)奖。他们的密码系统如下：选取两个大素数 p 和 q，作乘积 N=pq。选取 e 与(p-1)(q-1)互素，找 d 使 ed-1 能被(p-1)(q-1)整除。公钥是(N,e)，私钥是(p,q,d)。加密算法：对于明文 m，密文为 c=m^e mod N. 解密算法：收到密文 c，明文 m=c^d mod N.

RSA 密码系统基于的数学难题是：给了两个大素数 p 和 q，作乘积 N=pq 是很容易的，但是从 N 要找出 p 和 q 却是很困难的。这就是著名的大整数分解问题。整数的唯一分解定理是初等数论的内容，是我们每个人都熟悉的。如此巧妙运用数论是非常了不起的。

从 RSA 的公钥(N,e)找出私钥(p,q,d)，针对一般情形，目前最好的方法还是去分解 N，即把两个大素数 p 和 q 找出来。RSA 系统要投入实用，要解决两个

问题，即如何生成大素数，及如何判别素数。这两个问题经过许多数学家的努力，已经完满解决了。

由于 RSA 公钥密码系统的出现，大整数分解问题这一古老的数学问题焕发出青春的活力，吸引了全世界计算机科学家和数学家的极大兴趣，人们发明了各式各样的分解整数的算法。

从古老的试除法，到现代的各种方法，运用了当今前沿的数学知识，如代数数论和代数几何。这些现代的分解算法中有连分式方法、类群方法、椭圆曲线方法、二次筛法。

当今最好的分解算法是一般数域筛法,运用了代数数论的深刻知识,是 1993 年由几个计算机科学家和数论学家所共同发明的。运用这些现代的分解算法，人们可以分解许多大整数，这在以往是不可想象的。然而，由于密码学的强大动力，寻找更快更好的分解算法仍然是未结束的故事。现代密码学仍然强烈影响着数学的发展。

这些都是基于传统的电子计算机的公钥密码。然而 1994 年，P.Shor 发明了关于整数分解问题和离散对数问题的有效的量子算法，这意味着一旦实用量子计算机出现,RSA 和 ECC 将不能使用，因此必须研究能抵抗量子算法攻击的公钥密码体制。因为至今没有发现求解 NP-难问题的有效量子算法，因此人们把目光投向了基于 NP-难问题的密码体制，这些候选体制有：基于背包问题的体制，这是基于背包问题这个 NP-难问题，但是现有提出的体制都被攻破。

多变量密码体制，这是基于有限域上非线性方程组求解这个 NP-难问题，但是现有提出的体制都被攻破；基于线性码的密码体制，这是基于有限域上随机线性码译码这个 NP-难问题，但是没有实用的体制被设计出来；基于格的密码体制， 这是基于格的最近向量、最短向量求解这个 NP-难问题，这是最有希望的能抵抗量子攻击的体制，现今有一个有效的体制即 NTRU 还是安全的。

有限域理论

有限域理论是现代代数学的重要分支之一。近五十年来，由于它在组合、编码、密码和通信等学科的广泛应用，而逐步形成富有特色的代数学核心内容。有限域研究可以追溯到费尔马、欧拉、高斯和伽罗华等著名数学家。近几十年，随着计算机科学的发展，有限域理论得到深入发展与广泛应用。特别是，有限

域理论是编码与密码学的重要数学基础。实验室在有限域的正规基与有限域上的方程求解方面有重要工作。

密码分析

在今天的信息社会，信息安全由于涉及国家的政治安全、军事安全、经济安全等众多方面而成为一个重要的研究领域。传统的密码系统和各种密码应用方案依赖于大整数分解和计算离散对数的困难性。而 P. Shor 于 1996 年证明在量子计算模型之下，存在多项式时间算法来求解这两个问题。这样现有的许多密码系统受到挑战。最近出现的新的密码体系与数学机械化研究的主要内容—方程求解的符号算法密切相关。例如 2001 年由美国 NIST 选中新的高级加密标准 AES，它的安全性取决于有限域上大规模非线性多变量方程组的不可解性。针对信息安全，特别是密码中的核心问题，发展新的数学方法，对提高我国的信息安全研究能力具有十分深远的意义。数学机械化与符号计算由于为代数计算、群论、数论、代数几何、自动推理等的研究提供了强有力的工具，在信息安全方面有着广泛的应用前景。

安全多方计算理论

安全多方计算是研究处在分布式环境下的多个参与者如何计算某个共同的函数并保证计算结果的正确性以及各自输入的保密性，它是分布式密码学和分布式计算研究的一个基本问题，具有广泛的应用背景，如电子选举，电子拍卖，安全数据库访问等。自 1982 年 Yao 提出两方计算问题和 1987 年 Goldreich 等人研究一般多方计算问题以来，经过二十多年的发展，安全多方计算在传统模型下已经取得了较为完整的理论结果。随着现代信息化社会的发展，电子商务和电子政务中关于信息系统的安全性以及隐私保护等问题日益突出，这使得安全多方计算的实际应用成为迫切需求。面向实际应用，前期的安全多方计算理论在效率和建模需要极大的提高和改进。本实验室提出并研究了安全多方计算的并行模型，发展了安全多方计算的新工具，极大提高了安全多方计算协议的执行效率。在这些工作的基础上，我们将继续研究实用环境下的安全多方计算理论，包括安全多方计算的异步通信模型、理性模型等，推进安全多方计算的实际应用。

- **数学机械化在高新技术中的应用。**

基于数学机械化方法的高档数控系统

由于数控技术对国民经济和国防安全所具有的重要作用和战略意义，西方发达国家不仅把高档数控机床和高性能数控系统视为具有高利润的高技术产品，而且一直将其列为超越经济价值的战略物资，对我国采取技术封锁、限制和歧视的政策。数控系统是数控机床的“大脑”，直接决定数控机床的性能，而样条插补与空间刀补是数控系统的关键技术，被列为国家 16 个科技重大专项之一的《高档数控机床与基础制造装备》的重要研究内容。

目前高档数控系统的技术发展趋势是高速度、高精度、高效率。数控系统的若干核心技术，如最优插补、空间刀补、动力学分析与误差补偿，是实现高速、高精控制的基础。这些问题可以归结为几何计算、非线性方程组求解与最优控制问题。以数控加工的效率为例，机床的加速能力与最大加工速度是由机床的性能决定的。但是由于精度与加工曲面形状的限制，最大加工速度往往很难达到。因此，研究在精度范围内如何充分利用机床的加速能力实现最优插补就变为提高加工效率的关键问题之一。通过发展高效、可信、最优算法，对数字化设计制造与数控系统中关键问题达到实时、可靠、完全性，可以为提升我国复杂曲面类零件设计制造与数控加工的水平提供算法基础。

数字化设计制造技术是数学、计算机与机械制造结合的产物，被认为是当代最具影响的十项关键技术之一。在其发展的每个历史关头，数学方法都起了关键的作用。例如，计算机辅助设计(CAD)的核心功能，曲面造型、参数化设计、协同设计等，直接建立在计算几何、计算代数几何、自动推理、运筹学等数学分支的基础上。计算机辅助工程(CAE)的核心功能是分析加工工件的动力学性质，其主要工具是求解相关的偏微分方程。计算机辅助制造(CAM)用于设计复杂工件的加工路径，密切依赖于代数方程求解、几何计算与优化算法。又例如，包括机、电、液、控等多个领域子系统构成的复杂产品的制造过程可以通过引入连续—离散混合、微分—代数耦合的新型方程系统(PDAE)统一建模。由此导致了研究 PDAE 的相容性、归约、求解、降阶、死锁与欠约束处理等问题。

数学机械化研究为数控技术的研究注入了新的思想。早在 90 年代初，吴文

俊院士就提出了有关曲面拼接问题的数学机械化方法，可以用于解决数控系统中的样条曲线和曲面插补等问题。我们还提出了并联机构广义 Stewart 平台，用于并联机构与机床。

研究交叉领域中的微分差分代数方程组有多种方法，其中包括数学机械化方法。应用中的方程组的系数可能有一定的误差，因此符号一数值混合计算是研究应用中 PDAE 的必要工具。符号一数值混合计算还可应用于对连续变量离散化和初值问题。

我国现有的高档数控系统中，其核心功能仍以直线插补与圆弧插补为主，且缺少空间刀补等功能。因此，在国家“高档数控机床与基础制造装备”重大科技专项中，特别将运动控制插补与空间刀补等技术列为“十一五”期间国产高档数控系统的目标参数。

运动控制插补与空间刀补的关键是空间曲面和曲线逼近、微分不等式下的最优控制与规划、参数恢复等各种几何与代数计算问题。这些都是数学机械化研究的核心内容。我们通过高档数控技术与数学机械化方法的融合，通过参加国家重大科技专项，自主创新，开发出支持高速、高精、高质量的高端数控加工的插补和刀补软件，对推动我国作为制造第一大国到强国将做出积极的贡献。

近年来，我们在数控系统的关键问题:样条插补与空间刀补方面取得重要进展，提出了直线段插补的最优算法、参数曲线最优插补的线性规划算法和凸优化算法、具有跟踪误差补偿功能的参数曲线插补算法、基于曲面重构的空间刀补方法等，获得了 6 项专利，并在国内企业得到若干应用。实验室参加了中科院数控联盟,并主持了国家科技重大科技《基于国产 CPU 的高档数控系统研制》的一个子课题。我们将以此为基础，进一步研究数控系统中的关键问题，为开发高速、高精、高质量的数控系统做出贡献。

基于数学机械化理论的智能软件平台的开发

我们开发的几何智能软件“几何专家”在国际上得到广泛应用与高度评价。我们开发的 MMP 是第一个从符号计算基本运算出发将数学机械化方法系统予以高效地实现，并广泛应用的软件。与国际商用的计算机代数系统 Maple 和 Mathematica 不同，我们的软件可以在网络上直接使用，有利于数学机械化方法

的应用与推广。

以上的几个研究方向有着密切的联系：几何定理机器证明和几何计算首先是通过坐标或不变量把几何问题代数化，然后利用符号或符号-数值混合算法进行计算和推导。符号计算软件是方程求解的基本计算工具，而自动推理和几何计算对符号计算提出新的问题，提供新的思路的发展。信息安全与有限域上的方程组求解密切相关，编码理论中的 Berlekamp 分解算法和 Berlekamp-Massy 算法是符号计算中若干算法的基础。任何自动推理过程、几何计算和符号计算的算法都必需通过软件实现来接受实践的检验，并通过软件解决实际中的问题。方程求解与几何计算方法是研究数控系统关键技术的算法基础。

实验室总体定位

数学机械化重点实验室的战略目标是**引领数学机械化研究，发展数学机械化理论与高效算法，**为科学研究与高技术研究中的脑力劳动的机械化提供有力工具，为提高我国知识与技术创新的效率做出实质性贡献。

实验室应用数学机械化方法**解决信息安全、数控技术、机器人、计算机辅助设计(CAD)等高科技领域的关键问题，开发基于数学机械化方法的智能软件，**为我国相关高技术领域的技术创新创造条件。

实验室是**凝聚和培养相关学科具有重要国际影响的杰出人才，进行数学机械化方面高层次国际学术交流的中心。**

研究特色：以基础研究为主，同时兼顾应用基础研究，在数学与计算机科学的交叉领域，包括数学机械化、信息安全的数学理论、数学机械化方法的高科技应用方面，面向学科前沿、面向国家发展需求，努力做出突破性、原创性和关键性成果，保持实验室作为国际上符号计算主要研究中心之一的地位。

实验室发展的近期目标是在数学机械化的主要方向：方程的符号求解、混合运算、几何推理与计算、密码分析、信息安全理论、基于数学方法的高档数控算法等方面做出突破性成果，培养和造就数学机械化研究的一批高水平人才。长期目标(2025)是开辟新的研究方向，整体推动数学机械化的发展。

三、人员信息

1、学术委员会

序号	姓名	性别	国别	学委会职务	职称	是否院士	工作单位
1.	李邦河	男	中国	主任	院士	是	中科院数学院
2.	高小山	男	中国	副主任	研究员	否	中科院数学院
3.	万哲先	男	中国	委员	院士	是	中科院数学院
4.	陆汝钤	男	中国	委员	院士	是	中科院数学院
5.	张景中	男	中国	委员	院士	是	中科院成都计算机所
6.	林惠民	男	中国	委员	院士	是	中科院软件所
7.	黄民强	男	中国	委员	院士	是	中科院系统所
8.	陈永川	男	中国	委员	院士	是	南开大学
9.	张继平	男	中国	委员	教授	否	北京大学
10.	王东明	男	中国	委员	教授	否	北航、广西民族大学
11.	宗传明	男	中国	委员	教授	否	北京大学
12.	林东岱	男	中国	委员	研究员	否	中科院信息工程所
13.	王小云	女	中国	委员	教授	否	清华大学
14.	陈发来	男	中国	委员	教授	否	中国科技大学
15.	李洪波	男	中国	委员	研究员	否	中科院数学院

2、队伍建设

研究单元

序号	研究单元	学术带头人	其它研究人员名单
1.	数学机械化研究中心	吴文俊、李邦河、高小山、孙笑涛、李洪波、李子明、支丽红、王定康、闫振亚	冯如勇、袁春明、程进三、黄　雷、李　博、陈绍示、李　伟
2.	信息安全研究中心	万哲先、刘卓军、韩　阳、邓映蒲	张志芳、冯秀涛、冷福生、周　凯、潘彦斌
3.	高档数控系统研究组	高小山、李洪波	袁春明、贾晓红

固定人员名单

序号	姓名	性别	出生日期	职务	职称	所学专业	工作性质
1.	吴文俊	男	1919.5		院　士	数学机械化	研究
2.	万哲先	男	1927.1		院　士	代数、编码	研究
3.	李邦河	男	1942.7		院　士	拓扑、代数几何	研究
4.	高小山	男	1963.10		研究员	符号计算	研究
5.	李洪波	男	1968.3		研究员	几何推理	研究
6.	刘卓军	男	1958.3		研究员	信息安全	研究
7.	李子明	男	1962.6		研究员	符号计算	研究
8.	支丽红	女	1969.6		研究员	混合计算	研究
9.	韩　阳	男	1971.10		研究员	代数表示论	研究
10.	王定康	男	1965.3		研究员	符号计算	研究
11.	闫振亚	男	1974.3		研究员	数学物理	研究
12.	邓映蒲	男	1971.5		研究员	信息安全	研究
13.	冯如勇	男	1978.6		副研究员	符号计算	研究
14.	张志芳	女	1980.10		副研究员	信息安全	研究
15.	袁春明	男	1979.12		副研究员	符号计算	研究
16.	程进三	男	1976.8		副研究员	符号计算	研究
17.	贾晓红	女	1981.9		副研究员	计算几何	研究
18.	冯秀涛	男	1978.8		副研究员	信息安全	研究
19.	周　凯	男	1981.9		所聘副研	代数、编码	研究
20.	潘彦斌	男	1982.4		所聘副研	信息安全	研究
21.	陈绍示	男	1983.7		所聘副研	符号计算	研究
22.	冷福生	男	1980.5		助研	代数数论	研究

23.	黄　雷	男	1980.1		助研	符号几何计算	研究
24.	李　博	男	1982.9		助研	生物数学	研究
25.	李　伟	女	1985.9		助研	微分代数几何	研究
26.	吴天骄	男	1959.9		工程师		技术
27.	周代珍	女	1965.3		秘书		管理
28.	李　佳	女	1984.12		学术秘书		管理

注：工作性质：研究、技术、管理、其他，从事科研工作的兼职管理人员其工作性质为研究。

客座人员情况

序号	姓名	性别	出生日期	职务	职称	所学专业	工作性质
1.	孙笑涛	男	1962.10		研究员	代数几何	研究

重要人才情况

序号	人员姓名	荣誉称号	获得年份
1.	高小山	杰青、百人	1997、1999
2.	李洪波	百人、杰青	1997、2009
3.	孙笑涛	杰青、百人	2000

注：杰青、“千人计划”、“百人计划”等。

创新研究群体

类型	研究方向	学术带头人	参加人员	获得年份
国家基金委创新研究群体	数学机械化方法及其在信息技术中的应用	高小山	李洪波、孙笑涛、李子明、刘卓军、王定康、支丽红、闫振亚、冯如勇、袁春明、程进三、黄雷、李伟等	2009-2011 2012-2014

注：基金委创新群体等

国内外学术组织任职情况

序号	姓名	学术组织名称	职务	任职开始时间	任职结束时间
1.	高小山	中国数学会	副理事长	2012	
2.	高小山	中国工业与应用数学会	副理事长	2009	
3.	高小山	中国图学学会	常务理事	2010	
4.	高小山	中国密码学会密码数学专业委员会	副主任	2010	
5.	高小山	ACM SIGSAM Advisory Committee Board	委员	2006	
6.	高小山	ICIAM Member Committee	委员	2016	
7.	高小山	2016 ISSAC Program Committee	主席	2015	2016
8.	高小山	第八届全国计算机数学学术会议程序委员会	委员	2016	2016
9.	刘卓军	System Safety Society	会员	2011	
10.	刘卓军	中国数学会计算机数学专业委员会	委员	2012	
11.	刘卓军	中国优选法统筹法与经济数学研究会	常务理事	2010	
12.	刘卓军	全国风险管理标准化技术委员会(SAC/TC 310)	副主任委员	2007	
13.	刘卓军	中关村品牌协会	常务副会长	2011	
14.	刘卓军	国家质检总局第一届进出口商品风险管理专家委员会	专家委员	2015	
15.	李洪波	中国数学会计算机数学专业委员会	副主任	2012	2016
16.	李洪波	全国工业机械电气系统标准化技术委员会安全控制系统分技术委员会	委员	2011	

17.	李洪波	北京数学会	理事	2011	
18.	李洪波	第八届全国计算机数学学术会议程序委员会	委员	2016	2016
19.	李子明	中国数学会计算机数学专业委员会	主任	2011	2016
20.	李子明	国际计算机协会 SIGSAM	秘书	2014	2016
21.	李子明	中国数学会	理事	2012	
22.	李子明	第八届全国计算机数学学术会议程序委员会	委员	2016	2016
23.	王定康	中国数学会计算机数学专业委员会	秘书长	2010	2016
24.	支丽红	Thematic Program on Computer Algebra	委员	2015	
25.	支丽红	Symbolic and Numeric Computation	委员	2004	
26.	支丽红	中国数学会计算机数学专业委员会	主任	2016	2019
27.	支丽红	中国数学会	理事	2015	
28.	支丽红	MICA2016 组织委员会	委员	2016	2016
29.	闫振亚	中国数学会计算机数学专业委员会	委员	2011	
30.	闫振亚	2016 可积系统与偏微分方程国际学术研讨会学术委员会	委员	2016	2016
31.	邓映蒲	中国密码学会理事会	常务理事	2011	
32.	邓映蒲	中国数学会计算机数学专业委员会	委员	2011	
33.	邓映蒲	中国电子学会信息论分会	委员	2010	
34.	邓映蒲	中国密码学会密码数学理论专业委员会	委员	2014	

35.	邓映蒲	第八届全国计算机数学学术会议程序委员会	委员	2016	2016
36.	冯如勇	国际符号与代数计算年会程序委员会	委员	2015	2016
37.	袁春明	第八届全国计算机数学学术会议程序委员会	副主席	2016	2016
38.	程进三	CASC2016 程序委员会	委员	2016	2016
39.	贾晓红	中国数学会计算机数学专业委员会	秘书长	2016	2019
40.	贾晓红	中国工业与应用数学学会全国几何设计与计算专业委员会	委员	2016	
41.	贾晓红	第九届全国几何设计与计算学术会议程序委员会	委员	2016	2016
42.	贾晓红	第八届全国计算机数学学术会议程序委员会	委员	2016	2016
43.	贾晓红	中国计算机图形学大会程序委员会	委员	2016	2016
44.	潘彦斌	中国数学会计算机数学专业委员会	委员	2016	2019
45.	潘彦斌	Cryptology 2016 程序委员会	委员	2016	2016
46.	陈绍示	2016 ISSAC Poster Committee	主席	2015	2016
47.	陈绍示	第八届全国计算机数学学术会议程序委员会	委员	2016	2016
48.	李伟	2016 ISSAC Poster Committee	委员	2015	2016

国内外学术期刊任职情况

序号	姓名	学术期刊名称	职务	开始时间	结束时间
1.	万哲先	**《Algebra Colloquium》**	主编		

2.	万哲先	**《Annals of Combinatorics》**	编委		
3.	万哲先	**《Discrete Applied Mathematics》**	编委		
4.	万哲先	**《Finite Fields and Their Applications》**	编委		
5.	万哲先	**《Journal of Combinatorics, Information and System Sciences》**	编委		
6.	李邦河	**《数学物理学报》**	主编		
7.	李邦河	**《东北数学》**	编委		
8.	李邦河	**《数学季刊》**	编委		
9.	李邦河	**《数学学报》**	编委		
10.	李邦河	**《系统科学与数学》**	编委		
11.	高小山	**《 Journal of Systems Science and Complexity》**	主编		
12.	高小山	**《Journal of Symbolic Computation》**	编委		
13.	高小山	**《 International Journal of Computers Communications & Control》**	编委		
14.	高小山	**《Electronic Journal of Mathematics and Technology》**	编委		
15.	高小山	**《中国科学：数学》**	编委		
16.	高小山	**《计算机辅助设计与图形学学报》**	编委		
17.	高小山	**《中国图象图形学报》**	编委		
18.	高小山	**《中国高校应用数学学报》**	编委		
19.	高小山	**《数学研究与评论》**	编委		
20.	刘卓军	**《 The International System Safety Society》**	**Member**		
21.	刘卓军	**《系统科学与数学》**	编委		
22.	李洪波	《 Journal of Systems Science and Complexity》	编委		

23.	李洪波	《 **Advances in Applied Clifford Algebras**》	编委		
24.	李子明	《**Journal of Symbolic Computation**》	编委		
25.	李子明	《系统科学与数学》	副主编		
26.	支丽红	《**Journal of Symbolic Computation**》	编委		
27.	支丽红	《**Mathematics in Computer Science**》	编委		
28.	支丽红	《**ACM Communications in Computer Algebra**》	编委		
29.	支丽红	《**SIAM Journal on Applied Algebra and Geometry**》	编委		
30.	支丽红	《**Theoretical Computer Science**》	特辑编委		
31.	支丽红	《系统科学与数学》	编委		
32.	闫振亚	《**Plos ONE**》	学术编委		
33.	闫振亚	《应用数学学报》	编委		
34.	邓映蒲	《密码学报》	编委		
35.	邓映蒲	《 **Journal of Systems Science and Complexity**》	编委		
36.	邓映蒲	《系统科学与数学》	编委		
37.	张志芳	《 **Journal of Systems Science and Complexity**》	编委		
38.	袁春明	《系统科学与数学》	编委		
39.	程进三	《**AMS Mathematics Reviews**》	编委		
40.	陈绍示	《**ACM Communicatons in Computer Algebra**》	编委		

3、人才培养

在读研究生及博士后一览表

序号	硕士生	博士生	博士后	导师姓名
1.	周　亮			李洪波
2.	姜文嵘			支丽红
3.	陈淑延			闫振亚
4.	姚姗姗			李子明，贾晓红
5.	何笑鸥			刘卓军
6.	冯　爽			冯如勇
7.	李　阳			李洪波
8.	肖方慧			王定康
9.	文钧屹			程进三
10.	程恒喆			冯秀涛
11.	谢天元			邓映蒲
12.	刘　欣			韩　阳
13.	张雅倩			张志芳
14.	李　爽			李邦河
15.	史　帅			李洪波
16.	葛京通			支丽红
17.	郭　婧			李子明
18.	王贺松			王定康
19.	王　丽			闫振亚
20.	马鸿宇			袁春明
21.	张文剑			程进三

22.	赵明阳			贾晓红
23.	骆丽夏			邓映蒲
24.	刘　珍			潘彦斌
25.		黄　章		高小山
26.		赵明勇		高小山
27.		文　勇		李洪波
28.		董　磊		李洪波
29.		邵长鹏		李洪波
30.		黄　辉		李子明
31.		张　熠		李子明
32.		王立波		刘卓军
33.		王　础		支丽红
34.		温子超		闫振亚
35.		张　凡		万哲先，邓映蒲
36.		刘仁章		万哲先
37.		荆瑞娟		高小山
38.		王　杰		高小山
39.		郝志伟		支丽红
40.		王　慧		邓映蒲
41.		张凝鹏		韩　阳
42.		杨江帅		万哲先
43.		廖茂东		邓映蒲
44.		黄巧龙		高小山
45.		齐嘉悦		高小山
46.		胡又壬		高小山

47.		李　昕		闫振亚
48.		姜　懋		刘卓军
49.		李加宁		邓映蒲
50.		陈　勇		闫振亚
51.		宓振鹏		袁春明
52.		杨志红		支丽红
53.		李秋萍		刘卓军
54.		窦孝杰		程进三
55.		付士辉		冯秀涛
56.		周义满		韩　阳
57.		白　剑		王定康
58.		陈俣翱		高小山
59.		王　凯		韩　阳
60.		杜　昊		李子明
61.		李　璋		李洪波
62.		鲁　东		王定康
63.		张国强		闫振亚
64.		郑　策		韩　阳
65.		徐敬可		张志芳
66.		李昊宇		邓映蒲
67.		王建华		刘卓军
68.		朱超超		冯如勇
69.			闻小永	闫振亚
70.			沈雨佳	闫振亚
71.			黄　冲	王定康

72.			林　望	支丽红
73.			张　强	高小山
74.			李建伟	高小山

毕业研究生一览表

序号	姓名	学位	导师姓名	毕业时间
1.	黄　冲	博士后	刘卓军	
2.	张　强	博士后	高小山	
3.	黄　章	博士	高小山	
4.	赵明勇	博士	高小山	
5.	文　勇	博士	李洪波	
6.	邵长鹏	博士	李洪波	
7.	董　磊	博士	李洪波	
8.	黄　辉	博士	李子明	
9.	张　熠	博士	李子明	
10.	王　础	博士	支丽红	
11.	张　凡	博士	万哲先，邓映蒲	
12.	刘仁章	博士	万哲先	
13.	周　亮	硕士	李洪波	

研究生获奖一览表

序号	获奖名称	获奖人员	指导教师
1.	ISSAC 2016 最佳学生论文奖	张　熠	李子明
2.	ISSAC 2016 杰出女学生奖	黄　辉	李子明
3.	2016 年支持“率先行动”联合资助优秀博士后项目	沈雨佳	闫振亚
4.	国家奖学金	郝志伟	支丽红
5.	中科院数学院院长奖学金特等奖	郝志伟	支丽红
6.	中科院数学院院长奖学金特等奖	王　杰	高小山
7.	中科院数学院院长奖学金优秀奖	陈　勇	闫振亚
8.	中科院数学院院长奖学金优秀奖	李加宁	邓映蒲
9.	阿美奖学金特等奖	李　昕	闫振亚
10.	阿美奖学金优秀奖	宓振鹏	吴文俊、袁春明
11.	阿美奖学金优秀奖	王　慧	冯秀涛
12.	阿美奖学金优秀奖	王立波	刘卓军
13.	中国科学院研究生院三好学生标兵	郝志伟	支丽红
14.	中国科学院研究生院三好学生	陈　勇	闫振亚
15.	中国科学院研究生院三好学生	杜　昊	李子明
16.	中国科学院研究生院三好学生	李昊宇	邓映蒲
17.	中国科学院研究生院三好学生	王　杰	高小山

18.	中国科学院研究生院三好学生	荆瑞娟	高小山
19.	中国科学院研究生院三好学生	窦孝杰	程进三
20.	中国科学院研究生院三好学生	赵明勇	高小山
21.	中国科学院研究生院三好学生	张　凡	万哲先、邓映蒲
22.	中国科学院研究生院三好学生	付士辉	冯秀涛
23.	中国科学院研究生院优秀学生干部	宓振鹏	吴文俊、袁春明
24.	中国科学院研究生院优秀学生干部	白　剑	王定康
25.	中国科学院研究生院优秀学生干部	鲁　东	王定康

注：全国百篇优秀博士学位论文、院长奖学金等。

四、科研工作与成果

（一）概述实验室年度承担课题情况，当年到位经费情况等。

本年度实验室承担

国家“863”计划项目子课题 1 项，

国家自然科学基金面上项目 8 项，

国家自然科学基金青年基金 3 项，

国家科技支撑计划项目 1 项。

（二）按研究方向或研究单元介绍实验室本年度有代表性的研究工作进展。

实验室继续在数学机械化理论与算法、密码与编码理论、数学机械化的应用等三个主要方向取得进展，共发表和接收论文 51 篇。代表性进展如下：

1、数学机械化理论与算法：

(1.1) 微分与差分代数（高小山、李子明、冯如勇、袁春明、李伟、陈绍示）

差分 Toric 簇与差分二项式理想

二项式理想是非线性代数中较为简单的一类理想，其中一类纯差形式的二项式对应的代数簇是 Toric 簇. 在 Laurent 代数多项式环中，二项式理想(Toric 簇)与格、多面体几何有着天然的联系，也为代数几何的研究提供了丰富的例子。由于格在多边形理论，密码，组合学等有着广泛的应用，对代数的二项式理想与 Toric 簇的研究已经较为成熟。对于 Laurent 代数情形的二项式理想，其理想的标准基的计算虽然可以通过 Groebner 基的计算得到，但从计算复杂度上来说，这一方法并不有效。较为有效的方法是通过对生成元的指标（即整数向量）来进行运算，或者说可以转化为格上的运算，从而可以应用 Smith 正交化或者 Hermite 标准型来给出相应二项式理想的标准形式。通过这一标准型，可以判定理想的成员问题。对于差分情形，差分 Toric 簇与差分二项式理想的性质还未被研究过。我们利用差分单项式与 Z[x]模之间的对应关系，来研究差分 Toric 簇与 Laurent 情形的差分二项式理想的基本性质。我们给出了差分 Toric 簇与一类差分二项式理想之间的一一对应关系，给出了判定一个 Laurent 差分二项式理想是素的、自反的算法，并

基于此给出了差分二项式情形的零点分解理论与算法，从而解决了 Laurent 差分二项式情形下的理想成员问题和完备理想成员问题。此外，我们还证明了差分二项式理想的完备闭包还是二项式的，并给出了差分 Toric 簇的几类等价定义。

偏微分有限系统的奇点消去

通过研究线性微分、差分方程的奇点， 我们可以了解方程解的渐近性质。在单变元情形，多项式系数的线性微分方程的解的奇点必然是首项系数多项式的零点，反之不然。不对应于解的奇点的这些零点成为方程的表观奇点（Apparent Singularity）。这类奇点可以通过在方程左边复合上特定阶数的微分算子而消去，这个过程称为奇点消去。单变元情形的奇点理论与算法已经相当完备，但是多变元情形相应理论与算法都是未知的。

近来，我们与 Manuel Kauers 合作利用非交换 Groebner 基理论将表观奇点的概念从常微分情形推广到了偏微分有限系统情形，并给出了基于 Ore 算子的最小左公倍式 (LCLM) 计算的奇点消去算法。该算法效率远远优于已有的算法。文章发表在符号计算领域权威期刊 《Journal of Symbolic Computation》上。

线性差分方程 Galois 群计算

将 Hrushovksi 算法推广到差分情形，首次给出了计算线性差分方程 Galois 群的算法，该结果目前已被计算数学方面的重要杂志《Mathematics of Computation》接收。与 Michael Singer 合作研究了差分 Galois 理论中的反问题，即什么样的线性代数群是线性差分方程的 Galois 群，这方面的研究已经取得了部分进展。利用三个圆锥曲线的 Jacobian 曲线完整确定它们的相交关系，该结果已发表在符号计算领域的权威杂志《Journal of Symbolic Computation》上。

Z[x]格上的模方法

给出了 Z[x]格上计算其一种特殊的 Groebner 基(GHNF)的模方法。不同于已有的模方法，我们选用的素数是 Unlucky 的，所得到的算法在次数较低的情况下是目前已知最快的。这方面的工作已被符号计算领域权威期刊 《Journal of Symbolic Computation》接收。

微分周簇与微分周形式

应用模型论证明了微分周簇的存在性，从而完全解决了微分代数几何中的相关公开问题，将代数周簇理论推广到了微分情形，填充了微分模空间(moduli space)研究的空白。论文 Differential Chow Varieties Exist 已被 Jounal of the London Mathematical Society 接收并将于近期发表。

证明了特征列形式的 Jacobi 阶数界猜想，给出了计算微分周形式的算法，相关论文发表在 Advances in Applied Mathematics.

给出了有效 Luroth 定理的一个更优的次数界，相关论文发表在 LNCS 上.

发展了偏微分代数几何中的相交理论，证明了偏微分相交定理；以相交定理为基础，定义了偏微分周形式，证明了它的基本性质，特别引入了偏微分次数的概念；并证明了一类偏微分周簇的存在性。

Zeilberger 算法与在邻差算子的计算

解决了 Zeilberger 算法关于三变元有理函数的终止性问题。我们将该问题转化成双变元有理函数的可求和性的判定，然后利用 2014 年本人在可求性判定问题上的工作给出了判定三变元有理函数的邻差算子存在的充分必要条件，从而解决该情形的终止性问题。在终止性问题上，已有的工作都局限于双变元函数，这是首次突破该局限。

在邻差算子的计算方面，提出了基于约化的构造代数函数邻差算子的高效算法。Hermite 约化只处理有理函数。为了处理代数函数，Trager 在其博士论文中将 Hermite 约化算法推广到了代数函数情形。 我们首先将超指数，超几何情形的多项式约化推广到代数函数情形，然后结合 Trager 的约化算法给出了计算代数函数邻差算子的新算法，同时我们还给出了邻差算子的阶的新的上界。与经典的方法相比较，我们算法效率更佳，并且所给出的上界更优。文章的评审意见认为“This is an excellent paper, solving an interesting point…”。文章发表于 ISSAC2016。

(1.2) 符号、代数与几何计算（万哲先、李洪波、王定康、韩阳、周凯、黄雷、贾晓红）

经典不变量计算与几何代数

研究经典括号代数的拉直算法的改进和线性四元数方程的无分量显式解。前者显著改进了 G.-C. Rota 基于 Capelli 算子的拉直算法，后者完全解决了自 Sylvester 以来一直未解决的一个经典问题。

通过将 3 维射影空间中的直线映射到六维空间中， 3 维射影变换群被嵌入到 6 维正交和反正交变换群中。通过正交变换分解成反射复合的个数的分类，将所有两个反射的复合变换按照 4 维矩阵约当标准型的不同分成 6 类，从而给出 Cl(3,3) 上所有平面旋转的一个分类。

Groebner 基计算

在计算多项式系统的 Groebner 基的 GVW 算法加以改进，并用于布尔多项式系统，实验结果表面效率有很大的提高。

在 F2 上的多项式系统的 Groebner 基的计算中，提出将多项式转换为数值矩阵的行中的元素的高效算法，并具体实现。计算结果表明 Greobner 基的计算效率得到很大提高。

在多项式理想的相关计算中， Rabinowitsch 技巧非常有用。我们将该技巧进行推广，从而使得该技巧的使用范围得到很大的提高。并可以自然地推广到参数 Groebner 基的计算中。

范畴论

证明了任意一个局部有限箭图的路范畴模去一个允许单项式理想所得的商范畴与任意一个对偶化范畴的张量积范畴的加法包的幂等完备必为对偶化范畴。进而证明了上述张量积范畴上的有限表现函子范畴必为对偶化范畴，且有 Auslander-Reiten 序列。作为应用，可构造出大量新的对偶化范畴，并可证明各种各样的复形范畴有几乎可裂序列。

高考数学和奥数问题的机器求解

立足于高中数学大纲中关于数列、三角函数和立体几何的知识点，在研发过程中总结发展出若干机器求解方法，并用软件 Maple 实现：

对往年高考试卷中出现的等差、等比数列和三角函数问题，以及奥数竞赛中的立体几何问题，发展出一套划分类型的归类算法。对其中的若干类问题各自进行数学建模，使之可以转化为可以符号求解的问题。

改进已有的基于 Groebner 方法、特征列方法、向量代数、共形几何代数方法的机器推理方法，使之更适合于具体类型的问题。

整合上面几点，编写了一个可以解决部分数列、三角函数和立体几何问题的 Maple 软件。目前对已有的全国高考数学真题、奥数竞赛立体几何真题和训练题进行自测和封闭他测，都取得了预期的效果。

两二次曲面交线和有理曲线曲面的 mu 基理论

完成了“两椭球构型的分类、穷举及分层”的工作。构型分析是比相对位置分析、交线拓扑分析更加深入的一种几何关系分析，该工作也是计算机图形学中首个以一对曲面的构型为切入点的工作。

初步完成了“Canal 曲面的 mu 基”的前期理论工作。该工作提出跳过参数方程、直接给出三个伴随曲面的动平面的方法，并由此可算出曲面的 mu 基，该 mu 基准确恢复了曲面的参数方程。

(1.3) 多项式可信计算（支丽红、程进三）

提出了一种基于矩量矩阵半正定松弛方法的符号---数值混合算法求理想的实根理想。通过将几何对合理论与半正定矩量矩阵的性质相结合,我们提出了正维情形下半正定松弛方法终止的判定准则，证明了在 Delta-正则坐标系下判定定理中的条件一定在有限步的半正定松弛内满足，并给出了在实根理想和根理想之间的一个理想的 Groebner 基（对合基）。将算法推广到求半代数簇的实根理想的 Groebner 基（对合基）。

回答了 15 年前的 Erich Kaltofen 和 Wenshin Lee 提出的关于多元多项式稀疏插值提前终止的公开问题。给出了过采样何时能够保证稀疏插值的数值稳定性的精确刻画。给出了如何通过随机旋转，增加插值项之间的距离，减少采样点的个数。

提出多项式方程组根的精炼的新方法。基于我们新的精炼方法实现了根的验证。实验数据显示我们的方法可以计算的规模要比已有方法大的多。

2. 编码与密码（刘卓军、邓映蒲、张志芳、冯秀涛、潘彦斌、冷福生）

Bent 函数的构造

早在 1976 年 Rothaus 提出了 Bent 函数的概念，数学上它与组合学中的一些对象密切相关，在密码、编码、序列设计等领域也有重要应用。是抵抗相关攻击的一类重要函数。之前所构造的 bent 函数基本上都是二次的，而我们的工作是给出了一种方法，以此可以构造任意次数的 bent 函数。因此，构造出的函数从理论上讲，不但对抵抗相关攻击，而且对抵抗代数攻击也具有意义。

2009 年 Schmidt 提出了 Z4-值的 bent 函数，由于其在 CDMA 通信系统中的成功应用，因此这类函数得到了广泛而深入的研究。我们对 q 是素数方幂的情形给出了 Zq-值广义 bent 和超 bent 函数的完全刻画。为进一步应用奠定了理论基础。

素数判定问题中的 Bosma 问题

对形如 h*2^n±1 的数，Bosma 在 1993 年提出问题：是否存在有限条序列，其初值是固定的（即不依赖于 n），由这些序列的同余性质可以判定出这种数的素性（即对所有的 n）？其中 h 是固定的奇数。Bosma 本人对 h 不被 3 整除时肯定地解决了这个问题，主要用了二次互反律。Berrizbeitia & Berry 于 2004 年对 h 不被 5 整除时肯定地解决了这个问题，主要用了 4 次互反律。我们对 h 不被 17 整除时肯定地解决了这个问题，主要用了 8 次和 16 次互反律。相关论文发表在《Journal de Théorie des Nombres de Bordeaux》上。

局部修复码的构造和分布式存储系统保密信息提取

构造了两类(r,t)-局部修复码，一类具有循环码结构，其信息率和相对极小距离比已有的一般构造都有较大提高，另一类由线性空间的包含矩阵得到，具有很高的信息率。

对二元局部修复码的极小距离和信息率的上界进行了改进，在某些参数情

形下优于前人的参数界。

研究了基于 MDS 编码的分布式存储系统进行保密信息提取的最低通信代价，具体考虑了抵抗 T>1 个数据库合谋，以及一次提取多个信息的问题，已得到一些初步结果。

序列密码设计与分析

有限域上的迹逆函数是一类重要的布尔函数，已被许多密码算法采用，例如 SFINKS、RAKAPOSHI、SCSC 等。评估这些算法在抗代数攻击方面的能力需要研究其代数性质。然而当前国际公开文献上仅仅只是给出其代数免疫度的一些界的信息，例如 NGG 上界和 Bayev 下界。针对迹逆函数，我们证明了 D.K. Dalai 关于迹逆函数代数免疫度的猜想是正确的，给出了其代数免疫度的确切值，并进一步刻画了其在快速代数攻击方面的一些弱特性。

S 盒作为重要的混淆部件被广泛用在对称密码设计中。为了提供好的混淆特性，一般要求 S 盒具有好的密码学性质，譬如好的差分特性，好的非线性度，高的代数次数等。最近 Perrin 等人在美密会 CRYPTO2016 上提出了两种新的分别被称作为 Open Butterfly 和 Closed Butterfly 的构造 4 差分的 S 盒结构，他们通过实验发现这些结构的非线性度也是最优的，并提出相应的猜想。我们推广了他们提出的两种 Butterfly 结构，并证明了推广的 Butterfly 结构的差分至多是 4 差分的，且其非线性度总是达到最优，从而证明了 Perrin 等人的相关猜想是正确的。此外，我们还进一步确定了推广的两种 Butterfly 结构的差分谱特征、Walsh 谱特征、代数次数和置换特性等密码学性质。

对 GGH 型签名体制的攻击

对使用最近平面算法进行签名的 GGH 型签名体制做了成功的攻击。之前学界已经知道如何对使用 Round-Off 算法进行签名的 GGH 型签名体制进行攻击，但对使用最近平面算法进行签名的 GGH 型签名体制还不能进行伪造。我们提出了一个新的算法，使得可以有效地获得一个等价私钥，从而伪造任意消息的签名。

Hermite 标准型算法

计算 Hermite 标准型是一个非常经典且古老的计算问题。我们的新算法更易理解，和目前最快的算法拥有理论上一样的时间复杂度。同时，我们给出了一个新的启发式算法，新算法在现实运行中表现得很好，在高维情况下比 NTL 中实现的算法要更快。

3. 数学机械化应用

(3.1) 数控插补算法（高小山、李洪波、袁春明）

连续直线段路径的运动规划方法

为满足高档数控机床对高速度、高精度加工的需求，作为数控系统核心组成的给进运动规划技术一直是研究的热点问题。当前数控系统常用的加工指令包括连续直线段指令和参数曲线指令，并存在相应的加减速运动规划方法。随着人们对机械产品加工精度和加工效率需求的提高，传统的数控运动规划方法已不能满足高速高精度数控加工的性能要求。连续直线段路径（或称 G01 路径）是当今数控系统、CAM 软件等主流支持的路径表述形式。由于路径在转角处固有的切向不连续性，当前针对此类路径广泛应用的运动规划方法存在起停频繁、运动效率低下等问题，很难同时实现路径的高速度和高精度加工。因此进一步对此类路径的运动规划方法进行研究，提高其运动效率及运动精度仍然具有明显的实际意义。

为提高 G01 路径的运动效率，本研究工作提出了一种局部转角过渡算法和全局的前瞻运动规划方法。不同于以往转角过渡方法将过渡路径和过渡速度分别进行规划，本工作给出了一种联立过渡轨迹生成方法。对路径的每一个转角构造过渡曲线，在过渡曲线的选择上，以固定加速度形式实现转角过渡，进而获得二次多项式形式的过渡曲线。为充分利用设备的加速性能，我们对转角加速度进行优化，获得了局域最优的加速度。在误差控制方面，我们证明了转角过渡曲线的最大轮廓误差点是存在且唯一的，且最大轮廓误差方向与轮廓误差的设定值大小无关等性质。为进一步提高转角过渡速度，我们提出了改进转角过渡模型，以转角的最大误差轮廓点作为转角支撑点，充分利用转角过渡空间，从而获得最大转角通过速度。

本方法相比于当前广泛研究的路径拟合加 S 形加减速方法的特点为： (1). 实现了路径与速度的联立优化，通过适时调整转角过渡轨迹的轮廓实现加减速的调整； (2). 可考虑轴方向约束和局部可调整约束界，利于方法灵活地应用于多种场景；(3). 所给出的改进转角过渡模型，可充分利用转角过渡空间，提高转角通过效率。大量数据测试表明：我们提出的算法相比于当前广泛研究的运动规划方法有更高的转角通过速度和更迅速的加减速能力，这得益于算法中提出的改进转角过渡模型和考虑轴向加减速约束。

复杂动力学约束下的光滑轨迹运动规划

Jerk 约束的光滑轨迹由于具有连续的加减速变化特征，在实际数控系统中具有广泛的应用。通常在中低速加工应用中，jerk 约束的光滑轨迹可以满足加工需求，但受到数控伺服系统的运动性能限制，在高速、高负载数控加工过程中，伺服系统的动态响应性能将会严重下降，单纯通过抑制加减速变化率来达到误差可控的方式将严重影响加工效率，因此需要考虑驱动器动力学模型的引入。虽然完全动力学约束下生成的时间最优轨迹有更好的性能，但由于驱动器动力学模型的引入，不加处理地直接优化求解将非常耗时。

本工作给出了完全动力学约束下光滑轨迹的高效求解方法。基于时间最优轨迹具有的重要性质，我们通过引入虚拟变量实现了非线性约束的线性化近似，证明了这种近似的可行性，进而获得了完整动力学约束轨迹规划问题的一种凸优化的表述，从而获得了问题的高效求解。后续大量的实例测试，验证了我们提出的凸优化表述方法获得的最优轨迹和原始问题的最优轨迹是十分接近的，并且在轨迹运动时间、跟踪精度上也具有相似的性能。

加工轮廓误差约束下的参数曲线路径运动规划方法

参数曲线路径的运动规划是当前数控领域的热点研究内容。受益于参数曲线路径的光滑性，当前存在多种规划方法，包括基于多段加减速模式的梯形、S 形运动规划方法，基于最优化的方法和基于相平面分析的方法等。传统以最小化运动时间为指标的运动规划具有不连续的加减速运动，在实际应用中将诱导机床振动进而影响加工质量。为提高规划轨迹的实用性，通常在规划问题中引入 jerk 约束，获得光滑的加减速运动。由于 jerk 约束与加工误差之间不存在明确的数学关系，此类方法仅可以定性地提高加工精度。

本工作在轨迹规划阶段即同步估计此规划轨迹在执行时的加工轮廓误差，通过以估计的轮廓误差为限制条件，对轨迹进行调整，以达到对加工精度进行定量控制的目的。由于对于任一给定的轨迹和确定的控制系统，其相应的加工轮廓误差是可以估计的，我们以闭环控制系统的误差传递函数为基础，实现了数控系统各驱动轴跟踪误差的估计，并进一步将轮廓误差表述为规划轨迹速度、加速度和加加速度的线性函数，获得了含轮廓误差约束轨迹规划问题的最优控制表述。针对问题表述的非线性，我们给出了相应的问题局部线性化处理方法，最终实现了问题的凸优化求解。

相比之下，常规的轨迹光滑化方法由于无法定量的估计轨迹的加工精度，因此规划阶段为保证规划轨迹在快速加工时仍具有较好的响应和精度，在速度约束、加速度约束等的设置都会偏向于保守。本工作通过在规划阶段以所估计的加工误差为参考约束，在约束设置上可以更加合理，进而得到的优化轨迹在运动时间、加工精度上都具有优势。后续大量的实验测试，验证了我们提出的轮廓误差受限的轨迹相比常规的 jerk 约束光滑轨迹在轨迹加工精度和加工效率上均具有明显的优势，且提出的凸优化求解方法保证了问题求解的高效性和稳定性。

多点遍历问题的最小时间运动规划

多点运动规划问题广泛存在于多种机器人应用中，如工业机械臂的钻孔、焊接、路由检测过程等。由于机械臂运动具有的非线性特征，传统的最短距离运动规划并非最合适的规划模式。

本工作以最短遍历时间为规划指标，通过优化任务点遍历顺序、相邻路径点转移路径及速度等，获得满足机械臂动态性能的最小时间加工轨迹。由于最小时间多点运动规划问题为典型的混合整数最优控制问题，本工作采用解耦求解策略，将复杂的混合整数规划问题解耦为一个纯整数变量的最小时间 TSP 问题和一系列的纯连续变量的点-点最小时间路径规划子问题。在点-点运动规划问题上，采用直接优化方法进行求解并获得相应的最小转移时间。多组实例测试，验证了我们提出的最小时间策略相比最短路径策略和最小角位移策略有更高的运动效率。

基于可行域的球头刀具五轴加工路径设计

五轴数控加工中的 G 代码生成包含两个方面的问题；刀触点/刀心点的轨迹和刀姿。如果使用的刀具是球头刀，那么这两个问题可以分开来考虑。

我们针对球头刀，给出了计算在每个刀位点的刀姿可行域 C-space 的算法。给定每个刀位点的刀姿可行域后，我们设计了一个基于图的最短路算法的刀姿优化方法。我们引入差分图的概念，使得到的刀姿与传统方法比较具有更好的光滑度和力学性能。

基于高阶切触的平底刀具五轴加工路径设计

平底刀具是真正实现五轴同步变化提高加工精度的加工方式。传统方法采用一阶切触模型，不利于提高加工带宽，而采用二阶切触会造成过切，在精加工阶段并不适用。已有文献未能建立正确的三阶切触的局部微分几何模型，因而无法导出描述等残高模式下的相邻刀轨变化的微分方程。

我们利用局部无穷小估计和 Maple 软件，导出了三阶切触的局部微分几何模型和等残高模式下的相邻刀轨变化的微分方程，并提出了求解一阶切触加工曲线段与三阶切触加工曲线段之间的光滑拼接加工曲线的优化模型，给出了等残高模式下最大三阶切触的平底刀具路径规划算法。模拟实验表明，我们的方法比已有其他高阶切触路径规划方法具有更好的加工带宽。

(3.2) 非线性数学物理方程（闫振亚）

研究了具有不同 PT-对称外势条件作用下的若干非线性波方程（如非局域、高阶）的可积性、PT-对称线性 Hamilton 算子实谱的参数范围、PT-对称非线性波结构及其稳定性，研究结果发表在《Sci. Rep.》、《Chaos》,《Appl. Math. Lett.》等杂志。

基于 Lax 对，通过特征函数的谱参数展开，提出了广义摄动的 Darboux 变换方法，并研究了非线性非局域 Schrodinger 方程和离散耦合系统的高阶极端孤子解和怪波解以及它们的稳定性等，结果发表在《Chaos》等上。

(3.3) 系统科学（李邦河、刘卓军、李博）

数据科学

大数据概念日益受到关注，促进了发展数据科学的问题。一般说来，人们会关注一个一个的对象（样本），每个对象都会包含若干属性，习惯上 n x p 矩阵能够描述相当大类的问题，其中 n 是样本规模，p 是每个样本包含的属性数目，在很多情形，p 会比 n 大得多。如何确定 p 个属性之间的关联性，应用有需求，方法有挑战。我们基于 BHTA 方法形成了一套根据样本信息找寻属性关联组的方法。其中的一个技术环节是 D-Score 的计算。围绕中医病案特征分析，我们已整理出 3000 多人的诊病信息，并对病证结合的辩证施治方面开展了分析工作。这个工作还待进一步深入。

网络科学

有限时间收敛的 gossip 算法一直是国际学术界的空白：渐近算法在有限时间内只能给出近似结果，有限时间收敛算法则可以给出精确结果。我们与合作者构造性给出了确定性 gossip 有限时间收敛算法。我们证明了非近似算法存在的充分必要条件完全由网络点的个数决定。证明了我们构造的算法是理论上可能存在的最快的算法。证明了不存在有限时间收敛的量子 gossip 算法。论文发表在国际公认最顶尖的计算机网络杂志 IEEE/ACM Transactions on Networking 上。

我们与合作者一起研究了一类基本的量子混杂网络模型。我们使用投影测量作为控制手段。测量结果则通过经典通讯网络传播。我们给出了集中式的最优控制方式。我们还发展了一套分布式量子比特投影算法，证明了在该分布式量子比特投影算法下，各量子比特的量子状态将会几乎处处达到一致。论文已在 2016 年澳大利亚控制会议上报告，得到较好反馈。

酶动力学

继续深入研究酶动力学中的 Michaelis-Menten 模型。早在 2000 年的时候，Schnell, S.和 P. K. Maini 就提出了该模型中的反拟稳态假设，并运用其分析了酶浓度很高情况下的化学反应过程。但是这一假设是否总是成立，假设的严格表述是什么，这些问题都没有解决。我们现在已写出该假设的严格数学表述，并给出了证明。进一步，我们发现该定律在更为复杂的可逆模型中仍然有可能成立。

（三）介绍本年度实验室重大成果，研究成果的水平和影响等。

代表性成果 1、线性差分方程 Galois 理论中的正问题（冯如勇）

线性差分方程的Galois理论主要研究线性差分方程解之间的代数关系以及由这些代数关系所确定的变换群。这里我们所提及的差分算子指的是移位算子，即将未定义 x 变为 x+1。 如通常的 Galois 理论，正问题与反问题是线性差分方程 Galois 理论的两个基本问题。所谓正问题是指给定线性差分方程计算出其 Galois 群；而反问题则要确定什么样的群才是线性差分方程的 Galois 群。对于正问题，van der Put 与 Singer 对于对角型线性差分方程给出求 Galois 群的算法；Hendriks 在 1998 年对于二阶线性差分方程给出求 Galois 群的算法；此外，对于常系数的线性差分方程，Singer 在 2012 年给出求解算法。而对于反问题，van der Put 与 Singer 在其专著《Galois Theory of Difference Equations》中提出了如下猜测：一个 GL(n,C)中代数子群是 n 阶线性差分方程的 Galois 群当且仅当它关于其含幺联通分支求商所得的商群是循环群。目前该猜测只在一些特殊情形获得证明。

基于线性微分情形的 Hrushovski 算法并利用线性差分方程 Picard-Vessoit 扩张的特殊结构，我们首次给出求任意阶有理函数系数的线性差分方程 Galois 群的算法，完整解决了线性差分方程 Galois 理论中的正问题。文章结构已经被计算数学的顶级杂志《Mathematics of Computation》接受并已在线登出。在关于线性差分方程 Galois 理论的综述性论文《Algebraic and algorithmic aspects of linear difference equations》中，Singer 提到“…the first question has been recently answered positively for linear difference equations over Q(x) by Ruyong Feng”，其中“the first question” 即指正问题。另外，我们在正问题方面的工作有望用于解决反问题，目前我们已经在这方面取得了部分进展。

代表性成果 2、对 Hanser-Slamanig 等价类上保结构签名体制的安全性分析（潘彦斌）

在 2014 年亚密会上，Hanser 和 Slamanig 提出了一个新的密码学本原：等价类上保结构签名体制。该体制可以对消息空间中的任意一组等价类进行签名。利用该签名体制，他们成功构造了一个有效的多展示属性基匿名证明系统，从而可以对任意多属性进行编码。关于该签名体制的安全性，他们声称基于一般群模型假设，该体制具有适应性选择消息攻击下的强不可伪造性。然而， Fuchsbauer

指出该安全性论断在参数为 2 的情况下并不成立，即，当参数为 2 时，我们总可以通过适应性选择消息查询，然后以极大概率构造出一对成功的消息签名对。

我们进一步研究了该体制，并得到了如下结果：对任意参数，对更弱的敌手，我们只需要非适应性选择消息查询，就能成功构造出有效的消息签名对；而通过适应性选择消息查询，我们甚至可以伪造任意给定消息的签名。

相关论文发表在著名国际密码学会议 CT-RSA2016。

国家科研项目一览表（经费单位：万元）

序号	项目类别	项目名称	开始时间	结束时间	总经费	本年实到经费	负责人
1.	“863”计划项目子课题	初等数学问题求解关键技术及系统	2015	2018	70	0	黄　雷
2.	国家数学交叉中心	数学化制造与高档数控中的数学方法	2016	2016	61	61	李洪波
3.	国家数学交叉中心	多领域统一工业数学模型中的微分和差分代数混合计算	2016	2016	41.5	41.5	李子明
4.	国家数学交叉中心	信息安全和密码体系	2016	2016	31.5	31.5	邓映蒲
5.	国家自然科学基金面上项目	基于签名的 Groebner 基算法及其应用	2014	2017	50	10	王定康
6.	国家自然科学基金面上项目	素数判定与整数分解	2015	2018	60	18	邓映蒲
7.	国家自然科学基金面上项目	（半）代数系统的几何结构分析的高效算法及其应用	2015	2018	65	19.5	程进三
8.	国家自然科学基金面上项目	Hochschild（上）同调及其在代数表示论中的应用	2016	2019	52.68	22.5	韩　阳
9.	国家自然科学基金面上项目	凸代数几何中的若干问题研究	2016	2019	53.8	22.5	支丽红
10.	国家自然科学基金面上项目	PT-对称的非线性波方程的波结构及其稳定性分析研究	2016	2019	59.7	25	闫振亚

11.	国家自然科学基金面上项目	流密码算法设计与分析机械化方法研究	2016	2019	78	32.5	冯秀涛
12.	国家自然科学基金面上项目	格上最短向量问题的求解算法研究	2016	2019	77.2	32.5	潘彦斌
13.	国家自然科学青年基金	酶动力学中若干数学问题的研究	2014	2016	22	0	李博
14.	国家自然科学青年基金	微分、差分周形式与稀疏结式的理论与高效算法	2014	2016	22	0	李伟
15.	国家自然科学青年基金	Wilf-Zeilberger 理论的算法设计，复杂度分析及其应用	2016	2018	19.96	10.2	陈绍示
16.	国家科技支撑计划项目	产品质量安全风险监测指标获取及筛查技术研究	2013	2016	75	0	刘卓军
17.	教育部留学回国启动经费	Zeilberger 方法在含参微分伽罗瓦理论中的应用	2015	2018	3	0	陈绍示
18.	中国科学院项目	重大交叉学科前沿发展路线图战略研究	2016	2016	100	100	高小山
19.	中国科学院项目	中国科学院青年创新促进会	2014	2018	40	10	闫振亚
20.	中国科学院项目	中国科学院青年创新促进会	2014	2018	40	10	冯如勇
21.	中国科学院项目	中国科学院青年创新促进会	2015	2019	40	10	袁春明
22.	中科院 STS 计划	城市综合评价模型研究	2015	2017	35	15	刘卓军

23.	中国电子科技集团公司第三十研究所	一种基于格的公钥密码体制的设计	2015	2017	14	5.6	潘彦斌
24.	中国科学院信息工程研究所国家重点实验室开放课题	格基约化与提取	2016	2017	10	5	潘彦斌
25.	中国科学院信息工程研究所国家重点实验室开放课题	CAESAR 竞赛认证加密算法安全性分析	2015	2016	10	5	冯秀涛
26.	中国科学院项目	2015 年支持“率先行动”联合资助优秀博士后项目	2016	2017	10	10	李建伟
27.	中国科学院项目	2016 年支持“率先行动”联合资助优秀博士后项目	2016	2018	10	10	沈雨佳
28.	中国博士后科学基金会	中国博士后科学基金	2016	2017	5	5	李建伟
29.	中国博士后科学基金会	中国博士后科学基金	2016	2017	5	5	沈雨佳
合计	---	---	---	---		517.3	---

注：项目类别请填国家重大专项，“973”计划，“863”计划，国家科技支撑计划项目，国家自然科学基金，行业性重大专项，院先导性专项、部委项目等。

国际合作项目一览表

序号	合作国别	合作单位	项目名称	开始时间	结束时间	总经费	本年实到经费	负责人
1.								
合计	---	---	---	---	---			---

注：国际合作项目指双方单位正式签订协议书的国际合作科研项目

横向合作及其它项目一览表

序号	委托单位	项目名称	开始时间	结束时间	总经费	本年实到经费	负责人
合计	---	---	---	---			---

注：横向协作项目指有正式合同书的项目

国家重点实验室专项经费自主研究课题一览表

序号	课题名称	开始时间	结束时间	总经费	本年度经费	负责人
合计	---	---	---			---

获奖等重要成果

序号	成果名称	获奖类别	等级	完成人及排序
1.		第九届“陈景润未来之星”		潘彦斌
2.	微分 Chow 形式与稀疏微分结示	2016 年度数学院突出科研成果		李伟、袁春明、高小山
3.		2016 年度系统所关肇直奖		陈绍示
4.		2016 年中国高被引学者(爱思唯尔发布)		高小山
5.		2016 年中国高被引学者(爱思唯尔发布)		闫振亚

发表论文列表

序号	论文题目	刊物名称/卷期页码	作者	通讯作者	影响因子
1.	Combinatorics of Hybrid Sets	Proceedings of SYNASC'16, 60-64, IEEE, 2016	Shaoshi Chen, Stephen M. Watt	Shaoshi Chen	
2.	Desingularization of Ore Operators	Journal of Symbolic Computation, 74(C): 617-626, 2016	Shaoshi Chen, Manuel Kauers, Michael F. Singer	Shaoshi Chen	
3.	Existence Problem of Telescopers: Beyond the Bivariate Case	Proceedings of ISSAC'16, pp. 167–174, ACM Press, 2016	Shaoshi Chen, Qing-hu Hou, George Labahn, Ronghua Wang	Shaoshi Chen	
4.	Reduction-Based Creative Telescoping for Algebraic Functions	Proceedings of ISSAC'16, pp. 175–182, ACM Press, 2016	Shaoshi Chen, Manuel Kauers, Christoph Koutschan	Shaoshi Chen	
5.	Some Open Problems Related to Creative Telescoping	Journal of Systems Science and Complexity	Shaoshi Chen, Manuel Kauers	Shaoshi Chen	
6.	Explicit primality criteria for h. 2^n\pm 1	Journal de Th éorie des Nombres de Bordeaux, Vol. 28 No.1 pp. 55-74 (2016)	Dandan Huang, Yingpu Deng	Yingpu Deng	
7.	The Sum of Binomial Coefficients and Integer Factorization	Integers: Electronic Journal of Combinatorial Number Theory，2016(A42)：1-18	Yingpu Deng , Yanbin Pan	Yingpu Deng	
8.	Computing the intersections of three conics according to their Jacobian curve	J. Symbolic Comput. 175–191, 73, 2016	Ruyong Feng, Li-Yong Shen	Ruyong Feng	
9.	On the computation of the Galois groups of linear difference equations	Mathematics of Computation	Ruyong Feng	Ruyong Feng	

10.	On algebraic immunity of trace inverse functions on finite fields of characteristic two	Journal of Systems Science and Complexity, 2016, 29(1):272-288	Feng Xiutao, Gong Guang	Feng Xiutao	
11.	祖冲之序列密码算法	信息安全研究,2016.12	冯秀涛	冯秀涛	
12.	Binomial difference ideals	Journal of Symbolic Computation, 80(3), 665-706, 2017	X.S. Gao, Z. Huang, C.M. Yuan	X.S.Gao	
13.	Minimum time corner transition algorithm with confined feedrate and axial acceleration for nc machining along linear tool path	Int J Adv Manuf Technol, doi:10.1007/s00170-016-9144-9	Q. Zhang, X.S. Gao, H.B. Li, M.Y. Zhao	X.S.Gao	
14.	Time-optimal path tracking for robots under dynamics constraints based on convex optimization	Robotica, 34(9), 2116–2139, 2016	Q. Zhang, S. Li, J.X. Guo, X.S. Gao	X.S.Gao	
15.	Toric Difference Variety	Journal of Systems Science and Complexity	X.S. Gao, Z. Huang, J. Wang, C.M. Yuan	X.S.Gao	
16.	Reducing homological conjectures by n-recollements	Algebra Representation Theory 19 (2016), no. 2, 377-395	Y.Y. Qin, Y. Han	Y. Han	
17.	Brauer-Thrall type theorems for derived category	Algebra Representation Theory 19（2016）, no.6, 1369-1386	C. Zhang, Y. Han	Y. Han	
18.	Matrices of SL(4,R) that are the Product of Two Skew-Symmetric Matrices	Advances in Applied Clifford Algebras, 2016, pp.1-15	L. Dong, L. Huang, C. Shao, Y. Wen	L. Huang	
19.	Capacity constrained blue-noise sampling on surfaces	Computers & Graphics, Vol. 55, 44---54, 2016	S. Zhang, J. Guo, H. Zhang, X. Jia, D.-M. Yan, J.-H. Yong, P. Wonka	X. Jia	

20.	Continuous Detection of the Variations of the Intersection Curves of Two Moving Quadrics in 3-Dimensional Projective Space	Journal of Symbolic Computation, Vol. 73, 221-243, 2016	X. Jia, W. Wang, Y.-K. Choi, B. Mourrain, C. Tu	X. Jia	
21.	Finite-Time Convergent Gossiping	IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 24, NO. 5, OCTOBER 2016	Guodong Shi, Bo Li, Johansson, M., Johansson, K.H.	Guodong Shi	
22.	Challenging Theorem Provers with Mathematical Olympiad Problems in Solid Geometry	Mathematics in Computer Science, 10(1): pp 75-96, 2016	Changpeng Shao, Hongbo Li, Lei Huang	Hongbo Li	
23.	Symbolic Geometric Reasoning with Advanced Invariant Algebras	In: I.S. Kotsireas et al. (Eds.): MACIS 2015, LNCS 9582, pp. 35–49, Springer International Publishing Switzerland, 2016	Hongbo Li	Hongbo Li	
24.	Computation of differential Chow forms for ordinary prime differential ideals	Advances in Applied Mathematics. 72, 77-112, 2016	Wei Li, Ying-Hong Li	Wei Li	
25.	Differential Chow varieties exist	Journal of the London Mathematical Society, 2016	James Freitag, Wei Li, Thomas Scanlon	Thomas Scanlon	
26.	Simple Differential Field extensions and Effective Bounds	MACIS, LNCS, 343-357, Springer-Verlag，2016	James Freitag, Wei Li	James Freitag	
27.	Dembowski-Ostrom Polynomials from Reversed Dickson Polynomials	J. Syst. Sci. Complex (2016)29: 259 - 271	Zhang Xiaoming, Wu Baofeng, Liu Zhuojun	Liu Zhuojun	
28.	基于先验信息的产品质量安全多阶段抽样方法研究	中国安全生产技术科学，2016 年，159 - 163	朱建明, 刘卓军 孙红军	刘卓军	
29.	Cryptanalysis of the Structure-Preserving Signature Scheme on Equivalence Classes from Asiacrypt 2014	Proc. of CT-RSA 2016, Springer, LNCS, vol. 9610, pp. 291–304, 2016	Yanbin Pan	Yanbin Pan	

30.	On random nonsingular Hermite Normal Form	Journal of Number Theory，164：66~86, 2016	Gengran Hu, Yanbin Pan, Renzhang Liu, Yuyun Chen	Yanbin Pan	
31.	Solving Low-Density Multiple Subset Sum Problems with SVP Oracle	Journal of System Science and Complexity (2016) 29: 228–242, 2016	Yanbin Pan, Feng Zhang	Yanbin Pan	
32.	Two Types of Special Bases for Integral Lattices，Proc. of WISA 2015	Springer, LNCS, vol. 9503, pp. 87–95, 2016	Renzhang Liu, Yanbin Pan	Yanbin Pan	
33.	An improvement over the GVW algorithm for inhomogeneous polynomial systems	Finite Fields and Their Applications. Vol. 41, No. 4, (2016), 174 - 192	Yao Sun, Zhenyu Huang, Dingkang Wang, Dongdai Lin	Zhenyu Huang	
34.	On Implementing the Symbolic Preprocessing Function over Boolean Polynomial Rings in Groebner Basis Algorithms Using Linear Algebra	Journal of Systems Science and Complexity. Vol. 29 No. 3 (2016) 789-804	Yao Sun, Zhenyu Huang, Dongdai Lin, Dingkang Wang	Zhenyu Huang	
35.	Solving the Perspective-Three-Point Problem Using Comprehensive Groebner Systems	Journal of Systems Science and Complexity, 2016,29(5): 1446-1471	Jie Zhou, Dingkang Wang	Dingkang Wang	
36.	The Lightest 4x4 MDS Matrices over GL(4, F2)	INSCRYPT 2016	Ting Li, Jian Bai, Yao Sun, Dingkang Wang, Dongdai Lin	Dingkang Wang	
37.	Automated Reducible Geometric Theorem Proving and Discovery by Gröbner Basis Method	Journal of Automated Reasoning	Jie Zhou, Dingkang Wang, Yao Sun	Jie Zhou	
38.	The Generalized Rabinowitsch Trick Deepak	Springer PROMS 040	Deepak Kapur, Yao Sun, Dingkang Wang, Jie Zhou	Dingkang Wang	

39.	Dynamics of higher-order rational solitons for the nonlocal nonlinear Schrödinger equation with the self-induced parity-time-symmetric potential	Chaos, 26 (2016) 063123	Xiaoyong Wen, Zhenya Yan, Yunqing Yang	Zhenya Yan	
40.	Higher-order rational solitons and rogue-like wave solutions of the (2+1)-dimensional nonlinear fluid mechanics equations	Commun Nonlinear Sci Numer Simulat 43 (2017) 311	Xiaoyong Wen, Zhenya Yan	Zhenya Yan	
41.	Higher-order vector discrete rogue-wave states in the coupled Ablowitz-Ladik equations: Exact solutions and stability	Chaos, 26 (2016) 123110	Xiaoyong Wen, Zhenya Yan, B. A. Malomed	Zhenya Yan	
42.	Nonlocal general vector nonlinear Schrodinger equations: Integrability, PT symmetribility, and solutions	Appl. Math. Lett. 62 (2016) 101	Zhenya Yan	Zhenya Yan	
43.	On stable solitons and interactions of the generalized Gross-Pitaevskii equation with PT- and non-PT-symmetric potentials	Chaos 26 (2016) 083109	Zhenya Yan, Yong Chen, Zichao Wen	Zhenya Yan	
44.	Solitonic dynamics and excitations of the nonlinear Schrödinger equation with third-order dispersion in non-Hermitian PT -symmetric potentials	Sci. Rep. 6 (2016) 23478	Yong Chen, Zhenya Yan	Zhenya Yan	
45.	Stability, integrability and nonlinear dynamics of PT-symmetric optical couplers with cubic cross-interactions or cubic-quintic nonlinearities	Chaos, 27 (2017) 013105	Xin Li, Zhenya Yan	Zhenya Yan	

46.	A Modular Algorithm to Compute the Generalized Hermite Normal Form for Z[x]-Lattices	Journal of Symbolic Computation, 2016, 1-26	R.J. Jing, C.M. Yuan	C.M. Yuan	
47.	Tool orientation optimization for 5-axis machining with C-space method	Int J Adv Manuf Technol, 2016, 1-13	Z. Mi, C.M. Yuan, X. Ma, L.Y. Shen	C.M. Yuan	
48.	Two classes of (r, t)-locally repairable codes	IEEE International Symposium on Information Theory, 2016:445-449	Anyu Wang, Zhifang Zhang, Dongdai Lin	Zhifang Zhang	
49.	域规模严格小域码长的最优 LRC 构造	《中国科学：数学》(中文版), 47(11), 2017	Anyu Wang, Zhifang Zhang	Zhifang Zhang	
50.	A Certificate for Semidefinite Relaxations in Computing Positive-Dimensional Real Radical Ideals	Journal of Symbolic Computation, 72, 1-20, 2016	Yue Ma, Chu Wang , Lihong Zhi	Lihong Zhi	
51.	Numerical Sparsity Determination and Early Termination	Proc. of ISSAC 2016: 47-254	Zhiwei Hao, Erich L Kaltofen, Lihong Zhi	Lihong Zhi	

出版专著

序号	著作名称	作者	出版单位	出版日期
1	MENELAUS THEOREM - Menelaus 定理	吴文俊	哈尔滨工业大学出版社	2016.1
2	Commutative Algebra: An Introduction	W. Hoffman, X. Jia, H. Wang	Mercury Learning & Information	2016.5.13

授权发明专利

序号	专利名称	申请号/专利号	申报/授权	完成人及排序
1	一种序列密码实现方法和密钥流生成方法及装置	201310717039.0	授权	冯秀涛

其它成果（如新医药、新农药、新软件证书（不是著作权登记书）、国家标准等）

五、学术交流

数学机械化重点实验室在本年度组织承办了多项国际国内学术会议，邀请了国内外各个领域内的专家学者进行学术交流，为实验室的老师学生提供了一个及时交流科研成果的机会和平台。

举办的国际国内学术会议一览表

序号	会议名称	会议类别	主办单位	会议主席	会议日期	参加人数
1.	第八届全国计算机数学学术会议（CM2016）	国内	中科院数学院	陈之兵	2016.11.11-13	130

注：会议类别分为国际、国内（国内学术会议主要指全国性的会议）

参加的学术会议一览表

序号	报告名称	报告人	会议名称	地点	时间
1.	Proof of the Wilf-Zeilberger Conjecture	陈绍示	Algorithms and Complexity in Mathematics, Epistemology, and Science (ACMES2016)	加拿大	2016.05
2.	Existence Problem of Telescopers: Beyond the Bivariate Case	陈绍示	12th International Conference on Symmetries and Integrability of Difference Equations (SIDE12)	加拿大	2016.07
3.	Bivariate Extension of Abramov's Algorithm for Rational Summation（邀请报告）	陈绍示	The Waterloo Workshop on Computer Algebra (WWCA 2016)	加拿大	2016.07
4.	Thesixthdwarfofsymboliccomputation	陈绍示	Milestones in Computer Algebra (MICA 2016)	加拿大	2016.07
5.	Existence Problem of Telescopers: Beyond the Bivariate Case	陈绍示	The 41th International Symposium on Symbolic and Algebraic Computation(ISSAC2016)	加拿大	2016.07
6.	A New Method For Verifying the Isolated Singular Zeros of Polynomial Systems	程进三	第八届全国计算机数学学术会议（CM2016）	深圳	2016.11

7.	Algorithm for computing the factor ring of an ideal in Dedekind domain with finite rank （邀请报告）	邓映蒲	Mathematical Theory Applied in Coding and Cryptography	三亚	2016.01
8.	The computation of the Galois groups of linear difference equations （邀请报告）	冯如勇	12th International Conference on Symmetries and Integrability of Difference Equations (SIDE12)	加拿大	2016.07
9.	Parallel differential telescoping （邀请报告）	冯如勇	Algebraic Statistics and Symbolic Computation	日本	2016.07
10.	Parallel telescoping （邀请报告）	冯如勇	第七届微分代数及其相关课题国际会议(DART VII)	美国	2016.09
11.	一类差分方程系统的统计特性研究 （邀请报告）	冯秀涛	密码青年论坛	长沙	2016.06
12.	Optimal NC Interpolation	高小山	International Workshop on Industrial Mathematics	巴西	2016.05
13.	Characteristic Set Method for Solving Boolean Equations （邀请报告）	高小山	中国密码学会 2016 年密码数学理论学术会议	银川	2016.08
14.	Proper smooth local DG algebras are trivial （邀请报告）	韩　阳	Hochschild Cohomology in Algebra, Geometry, and Topology	德国	2016.02
15.	A construction of dualizing categories by tensor products of categories （邀请报告）	韩　阳	The 17th Workshop and International Conference on Representations of Algebras	美国	2016.08
16.	一元一次四元数方程的简单形式解	黄　雷	第八届全国计算机数学学术会议（CM2016）	深圳	2016.11
17.	Mu-Bases for DupinCyclides	贾晓红	Computational Algebra and Geometric Modeling	墨西哥	2016.08
18.	On configurations of Ellipsoids （邀请报告）	贾晓红	2016 科学工程与计算青年研讨会	北京	2016.09
19.		贾晓红	几何设计与计算（GDC2016）	合肥	2016.07
20.		贾晓红	中国计算机辅助设计与图形学(CAD&CG)大会	杭州	2016.11

21.	Agreeing Over Quantum Hybrid Networks: Centralized and Distributed Solutions	李　博	2016 Australian Control Conference	澳大利亚	2016.11
22.	Committee Size And Resistance To Information Manipulation	李　博	INFORMS Annual Meeting 2016	美国	2016.11
23.	Symbolic Computations, Integrable Systems and Their Applications （邀请报告）	李洪波	Workshop on Mathematics Mechanization	上海	2016.04
24.	Line Geometric Model of Three-Dimensional Projective Geometry （邀请报告）	李洪波	In: GAGIS 2016	南京	2016.08
25.	Differential Chow Varieties Exist	李　伟	Seminar on Set Theory	北京	2016.04
26.	Partial Differential Chow Forms and a Type of Partial Differential Chow varieties （邀请报告）	李　伟	第七届微分代数及其相关课题国际会议(DART VII)	美国	2016.09
27.	Abramov's Influence on the research work at KLMM （邀请报告）	李子明	The Waterloo Workshop on Computer Algebra (WWCA 2016)	加拿大	2016.07
28.	大数据潮涌 安全性何寻 （邀请报告）	刘卓军	VR & Big Data 企业应用之道大咖分享会	北京	2016.10
29.	大数据：认清趋势 实现价值 （邀请报告）	刘卓军	2016 年合肥市经信系统大数据产业发展高级研修班	贵阳	2016.11
30.	Cryptanalysis of the SPSS on Equivalence Classes from Asiacrypt 2014	潘彦斌	CT-RSA2016	美国	2016.03
31.	Lattice-based Public-key Cryptography （邀请报告）	潘彦斌	第三届“复杂性与安全性的碰撞”学术会议	北京	2016.04
32.	A New Algorithm to Compute HNF （邀请报告）	潘彦斌	密码与编码数学基础理论青年论坛	长沙	2016.06
33.	A New Algorithm to Compute HNF （邀请报告）	潘彦斌	有限域及其应用国际研讨会	天津	2016.06

34.	Cryptanalysis of the SPSS on Equivalence Classes from Asiacrypt 2014 （邀请报告）	潘彦斌	数学及其交叉学科学术研讨会	武汉	2016.11
35.	A New Algorithm to Compute HNF （邀请报告）	潘彦斌	密码学与云计算安全研讨会	北京	2016.11
36.	Solving RSSP with lp-norm SVP Oracle （邀请报告）	潘彦斌	理论密码学研讨会	北京	2016.12
37.	New Results on A Class of Multivariate Polynomial Matrix Factorizations	王定康	第八届全国计算机数学学术会议（CM2016）	深圳	2016.11
38.	The Lightest 4x4 MDS Matrices over GL(4, F2)	王定康	第八届全国计算机数学学术会议（CM2016）	深圳	2016.11
39.	PT-symmetric nonlinear waves （邀请报告）	闫振亚	2016 非线性数学物理与可积系统北京学术会议	北京	2016.04
40.	Rogue waves of nonlinear wave equations （邀请报告）	闫振亚	可积系统首届星海论坛	大连	2016.11
41.	Binomial partial difference ideals	袁春明	计算机代数应用会议 (ACA2016)	德国	2016.08
42.	An Integer Programming-Based Bound for Locally Repairable Codes	张志芳	Mathematical Theory Applied in Coding and Cryptography 2016	三亚	2016.01
43.	Singleton-Type bound for locally repairable codes	张志芳	第三届中韩编码理论会议	北京	2016.08
44.	Numerical sparsity determination and early termination （邀请报告）	支丽红	The 41th International Symposium on Symbolic and Algebraic Computation(ISSAC2016)	加拿大	2016.07
45.	Hybrid symbolic and numeric computation （邀请报告）	支丽红	Milestones in Computer Algebra (MICA 2016)	加拿大	2016.07
46.	Sparse interpolation of polynomials （邀请报告）	支丽红	Sparse Interpolation, Rational Approximation and Exponential Analysis (16w5038)	墨西哥	2016.10

47.	稀疏多项式插值 （邀请报告）	支丽红	第八届全国计算机数学学术会议（CM2016）	深圳	2016.11

注：如属特邀报告或者邀请报告，请在报告名称后注明；张贴报告不用列出。

开放课题一览表（经费单位：万元）

序号	课题名称	开始时间	结束时间	总经费	本年度经费	负责人	室内合作人
1.	符号数值混合计算	2016.5	2016.12	1	1	杨争峰	支丽红

六、运行管理

固定资产情况

建筑面积（平方米）	设备总台（件）数	设备总值（万元）
1200	120	200

30 万以上仪器设备使用情况

序号	设备名称	设备型号	购买时间	价格(万元)	使用总时间（小时）	非本室使用时间（小时）
1	AC 摇篮式五轴联动加工中心	XH714-5X	2013 年	75	200	0
合计	---	---	---			

大型仪器设备的开放、共享及成效。

七、学术委员会

中国科学院数学机械化重点实验室第四届学术委员会第二次会议于 2016 年 4 月 8 日在中国科学院数学与系统科学研究院南楼 420 召开。实验室学术委员会主任李邦河院士，副主任高小山研究员，万哲先院士，林惠民院士，北京航空航天大学/广西民族大学王东明教授，北京大学宗传明教授，中科院信息工程研究所林东岱研究员，清华大学王小云教授，中国科学技术大学陈发来教授，实验室主任李洪波研究员等 10 位学术委员会委员参加了本次会议。国家自然科学基金委数学科学处雷天刚处长也应邀参加了本次会议。此外实验室副主任李子明研究员，支丽红研究员，数学院科研处主管实验室事宜的王晓欢博士也参加了本次会议。

会议由实验室学术委员会主任李邦河院士主持。首先实验室主任李洪波研究员汇报了实验室 2015 年的工作成果，接着对实验室 2016 年的工作研究提出了计划设想，最后提出了实验室目前遇到的困难：研究队伍不够壮大，研究领域不够宽阔以及研究生招生难等问题。随后，张志芳副研究员、李伟助理研究员分别作了“局部修复码的最优极小距离”和“微分周簇的存在性”学术报告。

在听完实验室主任以及两位青年科研人员的汇报后，与会的专家领导肯定了实验室在 2015 年取得的成绩，同时对实验室目前存在的问题提出了很多宝贵的建议。雷天刚处长认为实验室招研究生困难是因为宣传的不够多，很多人都不了解“数学机械化”的含义，不了解实验室研究的方向内容，在招生季的时候要在各个高校多宣传，此外举办大学生夏令营也是一种很好的宣传方式。对于实验室的发展，雷天刚处长认为近几年实验室在机器证明、自动推理、符号计算等方向发展的很好，但是在信息安全和数控技术方向进展比较缓慢，人才比较匮乏，研究力量不足，尤其数控技术是国家的战略需求，实验室可以考虑进一步发展这个方向。王东明教授讲到了最近很热门的 AlphaGo，说明了人工智能的重要性，同时吴文俊先生在早些年前也研究过人工智能，说明数学和人工智能的关系很密切，而且现在人工智能的发展非常迅速，建议实验室未来多增加一个研究方向：智能数学。宗传明教授认为用数学机械化论证超级数学难题很有意义，但是对所有数学问题用机械化的方法论证目前看还是比较遥远。陈发来教授认为数学机械化是以符号计算作为基础和推理，数学机械化的应用领域很广，同时指出目前实

验室的基础研究相对窄一些，做的人比较少，建议实验室未来可以有更多的人投入到基础研究中。此外，林惠民院士，林东岱研究员，王小云教授都和实验室的领导和青年科研人员进行了学术探讨，对实验室的发展提出了宝贵的意见和建议。

最后李邦河院士感谢了各位专家领导对实验室的指导，针对目前遇到的困难，接下来会认真总结，汲取好的想法，借鉴好的经验，使得研究领域不断拓宽，研究内容与时俱进，吸引更多人才，壮大研究队伍，进一步提高国内外的影响力。

学术委员会合影

八、实验室大事记

1、新期刊 SIAM Journal on Applied Algebra and Geometry 于 2016 年首次发行。实验室的支丽红研究员担任期刊的编委。

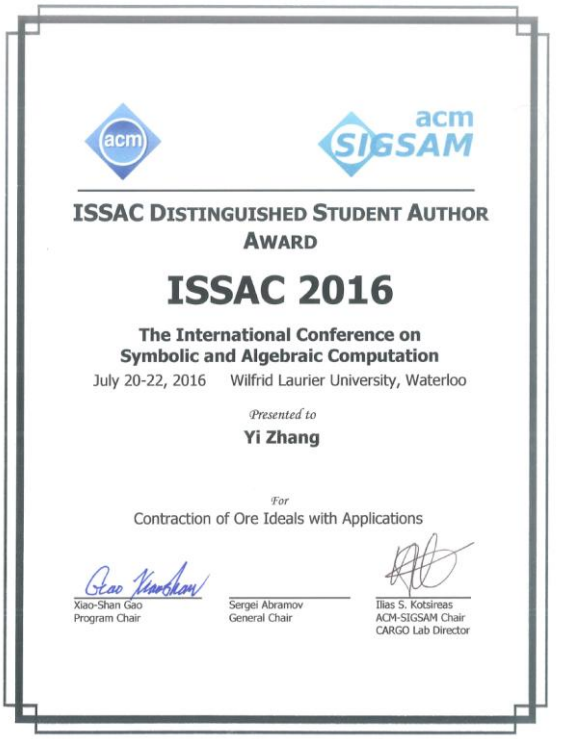
2、 1 月 28 日上午，国务院侨办党组成员江岩同志专程来到我院著名数学家吴文俊家中，看望这位德高望重的老院士。江岩向吴先生提前致以新春的祝贺和亲切的问候，并与他促膝谈心。

江岩详细询问了吴先生的身体和生活情况，希望他保重身体。吴先生对国务院侨办领导的关心表示衷心的感谢。他们在一起还畅谈了数学学科方面的研究情况以及吴先生的日常工作生活情况等，气氛非常热烈。

国务院侨办国内司司长王萍、北京市政府侨办主任刘春锋、中科院京区党委常务副书记马扬、中科院数学院执行院长王跃飞、海淀区副区长陈双等国务院侨办、北京市侨办、中科院、海淀区等相关领导同志陪同慰问。

3、2016 年 7 月在加拿大滑铁卢召开的第 41 届国际符号和代数计算会议(ACM ISSAC 2016)上，张熠获 ISSAC 2016 最佳学生论文奖，论文题目是：Contraction

of Ore Ideals with Applications.。黄辉获 ISSAC 2016 杰出女学生奖，论文题目是：New Bounds for Hypergeometric Creative Telescoping。



ISSAC DISTINGUISHED STUDENT AUTHOR AWARD

ISSAC 2016

The International Conference on Symbolic and Algebraic Computation

July 20-22, 2016 Wilfrid Laurier University, Waterloo

Presented to

Yi Zhang

For

Contraction of Ore Ideals with Applications

Xiao-Shan Gao
Program Chair

Sergei Abramov
General Chair

Ilias S. Kotsireas
ACM-SIGSAM Chair
CARGO Lab Director

ISSAC 2016

41st International Symposium on Symbolic and Algebraic Computation

Distinguished Female Student Award

New Bounds for Hypergeometric Creative Telescoping.

Hui Huang, Chinese Academy of Sciences and Johannes Kepler University.

This award is endowed with 250 CAD.

Program Committee Chair
Xiao-Shan Gao

General Co-Chair
Eugene Zima

4、2016 年 11 月 11 日，全国计算机数学专业委员会第八次全国会员代表大会暨换届会议在深圳市明华国际会议中心召开。会议由专委会主任李子明主持。李子明主任宣读了《中国数学会分支机构管理条例》和《中国数学会章程》中相关条款的要求，并由专委会秘书长王定康对第六届委员会候选人的入选标准和名单（草案）产生过程做了较详细的解释说明。经讨论，专委会产生了第三届委员会候选人名单。

全体 82 名参会会员代表无记名投票选出由 97 名委员组成的第三届专业委员会。共发出选票 82 张，收回 82 张，有效票 80 张。李子明主任委员宣布了选举结果：中国数学会理事、中国科学院数学院研究员支丽红担任第三届专业委员会主任，中国科学技术大学数学科学学院教授陈发来、北京大学数学科学学院教授夏壁灿、天津大学应用数学中心教授侯庆虎、广西民族大学副校长吴尽昭担任副主任，中国科学院数学院副研究员贾晓红担任秘书长。最后，专委会新任主任、副主任及秘书长分别发言讨论未来工作设想。

中国数学会计算机数学全国会员代表大会完成了全部议程，完成了委员会的顺利换届，为学会后续工作打下了坚实基础。

5、第八届全国计算机数学学术会议（CM2016）于 11 月 11 日至 11 月 13 日在深圳市明华国际会议中心召开。本次学术会议由中国数学会计算机数学专业委员会主办，深圳大学数学与统计学院、中国科学院数学机械化重点实验室承办。来自国内科研院所、大专院校的专家学者及在校学生近 150 人参加了此次会议。

11 月 11 日上午举行了开幕式，由深圳大学数学与统计学院副院长汤建良主持，中国数学会副理事长、中国科学院数学与系统科学研究院副院长高小山研究员致开幕词。原中国计算机数学专委会委员长、中国科学院数学院研究员李子明和本届大会主席、深圳大学数学与统计学院院长陈之兵教授分别致欢迎辞。会议期间，中国科学院数学院的支丽红研究员做了＂Numerical Sparsity Determination and Early Termination＂的邀请报告，中国科学技术大学的杨周旺教授做了＂基于影像数据的智能医疗决策＂的邀请报告，台湾义守大学的张耀祖教授做了＂有限域上迹的研究＂的邀请报告。Maple 公司也应邀做了产品介绍。此外，还安排了 37 位研究人员在本次会议的分组会议上做了学术报告。

6、实验室刘卓军研究员和学生吴保峰的论文 Linearized polynomials over finite fields revisited 获得 Finite Fields and Their Applications 杂志的引用率前五名。

7、2017 年 1 月 12 日上午中央组织部人才工作局孙学玉局长一行到我院吴文俊研究员家致以春节问候。中国科学院办公厅高春东副主任、人事局人才处杨中波处长和我院王跃飞院长、高小山副院长等陪同。

8、中共中央政治局常委、中央书记处书记刘云山16日上午，代表习近平总书记和党中央，登门看望我院吴文俊院士，向他致以诚挚问候和新春祝福。

刘云山来到吴文俊院士家中，关切询问吴文俊院士的身体和生活状况，对他在数学机械化领域作出的开拓性贡献表示钦佩。吴文俊院士建议坚定对我国数学发展的信心，加大对基础研究支持力度，增强原始创新能力。刘云山说，科技工作者要弘扬老一辈科学家报国为民的高尚情怀，把人生价值融入实现中华民族伟大复兴的中国梦，创造无愧于时代和人民的业绩。

吴文俊院士对习近平总书记和党中央的亲切关怀深表感谢，对党的十八大以来党和国家新的发展成就高度赞誉，表示科技工作者赶上了好时代，要继续发挥作用，为促进我国科技发展贡献力量。刘云山说，建设创新型国家、建设世界科技强国，是我国科技工作的重大战略任务。要增强责任担当，坚定不移走中国特色自主创新道路。要坚持以新发展理念为引领，聚焦国家重大发展战略，加快各领域科技创新。要大兴识才爱才敬才用才之风，深化人才发展体制机制改革，推动形成有利于人才创新创造的制度环境和政策环境。

中共中央政治局委员、中央组织部部长赵乐际陪同看望。中央组织部常务副部长陈希、中国科学院白春礼院长和有关部门负责同志参加看望活动。

九、研究所对国家重点实验室和院重点实验室的年度考核意见

我院按照有关规定对该实验室的申请材料进行了严格审核，确认内容属实，数据准确可靠。我院认为该实验室组织管理得当，成果突出，在科研、人才培养、学术交流和实验室建设等方面取得了重要的进展，同意该实验室报送以上年报。