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特殊符号解

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(Turing)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一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、张立先

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		所聘副研	信息安全	研究
19.	周　凯	男	1981.9		所聘副研	代数、编码	研究
20.	陈绍示	男	1983.7		所聘副研	符号计算	研究
21.	冷福生	男	1980.5		助研	代数数论	研究
22.	黄　雷	男	1980.1		助研	符号几何计算	研究

23.	潘彦斌	男	1982.4		助研	信息安全	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.	张立先	女	1982.10		项目助研	高档数控	研究
27.	吴天骄	男	1959.9		工程师		技术
28.	周代珍	女	1965.3		秘书		管理
29.	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

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	2016
2.	高小山	中国工业与应用数学会	副理事长	2009	2015
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	第八届国际工业与应用数学大会（ICIAM2015）	秘书长	2015	2015
7.	高小山	2016 ISSAC Program Committee	主席	2015	2016
8.	刘卓军	System Safety Society	会员	2011	
9.	刘卓军	中国数学会计算机数学专业委员会	委员	2012	2016
10.	刘卓军	中国优选法统筹法与经济数学研究会	常务理事	2010	2015
11.	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	2016
12.	刘卓军	中关村品牌协会	常务副会长	2011	2016
13.	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	专家成员	2015	
14.	李洪波	中国数学会计算机数学专业委员会	副主任	2012	2016
15.	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	

16.	李子明	中国数学会计算机数学专业委员会	主任	2011	2015
17.	李子明	中国数学会	理事	2012	2015
18.	李子明	ACM SIGSAM	秘书	2012	2015
19.	李子明	2015 ISSAC Program Committee	成员	2014	2015
20.	王定康	中国数学会计算机数学专业委员会	秘书长	2010	2016
21.	支丽红	Thematic Program on Computer Algebra	委员	2015	
22.	支丽红	Symbolic and Numeric Computation	委员	2004	2016
23.	支丽红	SIAM AG 2015 Program Committee	委员	2015	
24.	支丽红	中国数学会	理事	2015	
25.	邓映蒲	中国密码学会理事会	理事	2011	
26.	邓映蒲	中国数学会计算机数学专业委员会	委员	2011	
27.	邓映蒲	中国电子学会信息论分会	委员	2010	
28.	冯如勇	国际符号与代数计算年会程序委员会	成员	2015	2016
29.	程进三	Computer Algebra in Scientific Computing Program committe	委员	2015	2015
30.	程进三	第七届全国计算机数学学术会议程序委员会	副主席	2015	2015
31.	陈绍示	2016 ISSAC Poster Committee	主席	2015	2016
32.	李伟	2016 ISSAC Poster Committee	成员	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	**《 The Open Artificial Intelligence Journal》**	编委		
15.	高小山	**《Electronic Journal of Mathematics and Technology》**	编委		
16.	高小山	**《中国科学：数学》**	编委		
17.	高小山	**《计算机辅助设计与图形学学报》**	编委		
18.	高小山	**《中国图象图形学报》**	编委		
19.	高小山	**《中国高校应用数学学报》**	编委		
20.	高小山	**《数学研究与评论》**	编委		

21.	刘卓军	**《 The International System Safety Society》**	**Member**		
22.	刘卓军	**《系统科学与数学》**	编委		
23.	李洪波	《 Journal of Systems Science and Complexity》	编委		
24.	李洪波	**《 Advances in Applied Clifford Algebras》**	编委		
25.	李子明	**《Journal of Symbolic Computation》**	编委		
26.	李子明	**《系统科学与数学》**	副主编		
27.	李子明	**《 Journal of Systems Science and Complexity》**	编委		
28.	支丽红	**《Journal of Symbolic Computation》**	编委		
29.	支丽红	**《Mathematics in Computer Science》**	编委		
30.	支丽红	**《 ACM Communications in Computer Algebra》**	编委		
31.	支丽红	**《SIAM Journal on Applied Algebra and Geometry》**	编委		
32.	支丽红	**《Theoretical Computer Science》**	特辑编委		
33.	闫振亚	**《Abstract and Applied Analysis》**	编委		
34.	闫振亚	**《 Journal of Engineering and Applied Science》**	编委		
35.	闫振亚	**《 Bulletin of Mathematical Analysis and Applications》**	编委		
36.	闫振亚	**《 International Journal of Birfurcation and Chaos》**	客座编委		
37.	闫振亚	**《Plos ONE》**	学术编委		
38.	邓映蒲	**《密码学报》**	编委		
39.	邓映蒲	**《 Journal of Systems Science and Complexity》**	编委		

40.	邓映蒲	**《系统科学与数学》**	编委		
41.	张志芳	**《 Journal of Systems Science and Complexity》**	编委		
42.	袁春明	**《系统科学与数学》**	编委		
43.	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.	张文哲			王定康
2.	熊纯文			冯如勇
3.	闫方驰			闫振亚
4.	周　亮			李洪波
5.	杜　昊			李子明
6.	李　璋			李洪波
7.	姜文嵘			支丽红
8.	鲁　东			王定康
9.	张国强			闫振亚
10.	郑　策			韩　阳
11.	徐敬可			张志芳
12.	李昊宇			邓映蒲
13.	陈俣翱			高小山
14.	陈淑延			闫振亚
15.	姚姗姗			李子明，贾晓红
16.	何笑鸥			刘卓军
17.	冯　爽			冯如勇
18.	李　阳			李洪波
19.	肖方慧			王定康
20.	文钧屹			程进三
21.	程恒喆			冯秀涛

22.	谢天元			邓映蒲
23.	刘　欣			韩　阳
24.	王　凯			韩　阳
25.	张雅倩			张志芳
26.		祝　炜		高小山
27.		李应弘		高小山，冯如勇
28.		周　洁		吴文俊，王定康
29.		刘　越		李洪波
30.		邵长鹏		李洪波
31.		胡耿然		黄民强，邓映蒲
32.		吕　昌		胡　磊
33.		王安宇		万哲先，张志芳
34.		王　晗		刘卓军
35.		黄丹丹		黄民强，邓映蒲
36.		秦永云		韩　阳
37.		黄　章		高小山
38.		赵明勇		高小山
39.		文　勇		李洪波
40.		董　磊		李洪波
41.		黄　辉		李子明
42.		张　熠		李子明
43.		王立波		刘卓军
44.		王　础		支丽红
45.		温子超		闫振亚
46.		张　凡		万哲先，邓映蒲

47.		刘仁章		万哲先
48.		荆瑞娟		高小山
49.		王　杰		高小山
50.		郝志伟		支丽红
51.		王　慧		邓映蒲
52.		张凝鹏		韩　阳
53.		杨江帅		万哲先
54.		廖茂东		邓映蒲
55.		黄巧龙		高小山
56.		齐嘉悦		高小山
57.		胡又壬		高小山
58.		李　昕		闫振亚
59.		姜　懋		刘卓军
60.		李加宁		邓映蒲
61.		陈　勇		闫振亚
62.		宓振鹏		袁春明
63.		杨志红		支丽红
64.		李秋萍		刘卓军
65.		窦孝杰		程进三
66.		付士辉		冯秀涛
67.		周义满		韩　阳
68.		白　剑		王定康
69.			杨云青	闫振亚
70.			闻小永	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.	杨云青	博士后	闫振亚	
2.	祝　炜	博士	高小山	
3.	李应弘	博士	高小山，冯如勇	
4.	王　晗	博士	刘卓军	
5.	刘　越	博士	李洪波	
6.	周　洁	博士	王定康	
7.	王安宇	博士	万哲先，张志芳	
8.	胡耿然	博士	黄民强，邓映蒲	
9.	黄丹丹	博士	黄民强，邓映蒲	
10.	吕　昌	博士	胡　磊	
11.	秦永云	博士	韩　阳	
12.	张文哲	硕士	王定康	
13.	熊纯文	硕士	冯如勇	
14.	闫方驰	硕士	闫振亚	

研究生获奖一览表

序号	获奖名称	获奖人员	指导教师
1.	AGACSE 首届 David Hestenes 论文奖	邵长鹏	李洪波
2.	AGACSE 首届 David Hestenes 论文奖	董　磊	李洪波
3.	2015 年支持“率先行动”联合资助优秀博士后项目	李建伟	高小山
4.	国家奖学金	王　础	支丽红
5.	中国科学院大学院长优秀奖	吕　昌	胡　磊
6.	中科院数学院优秀毕业生	王安宇	万哲先，张志芳
7.	中科院数学院院长奖学金特等奖	王　础	支丽红
8.	中科院数学院院长奖学金优秀奖	邵长鹏	李洪波
9.	中科院数学院院长奖学金优秀奖	温子超	闫振亚
10.	中科院数学院院长奖学金优秀奖	张　凡	万哲先、邓映蒲
11.	中国科学院研究生院三好学生	王　础	支丽红
12.	中国科学院研究生院三好学生	黄丹丹	黄民强，邓映蒲
13.	中国科学院研究生院三好学生	邵长鹏	李洪波
14.	中国科学院研究生院三好学生	温子超	闫振亚
15.	中国科学院研究生院三好学生	董　磊	李洪波

16.	中国科学院研究生院三好学生	胡耿然	黄民强，邓映蒲
17.	中国科学院研究生院三好学生	吕　昌	胡　磊
18.	中国科学院研究生院三好学生	张　凡	万哲先、邓映蒲
19.	中国科学院研究生院三好学生	付士辉	冯秀涛
20.	中国科学院研究生院优秀学生干部	荆瑞娟	高小山

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“973”计划项目 1 项，
国家“973”计划项目子课题 4 项，
国家“863”计划项目子课题 1 项，
国家自然科学基金面上项目 5 项，
国家自然科学基金青年基金 5 项，
国家科技支撑计划项目 1 项。

（二）按研究方向或单元，介绍实验室本年度有代表性的研究进展。

本年度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 48 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）

微分与差分稀疏结式：

方程求解的消去理论是数学机械化的主要研究内容，也是数学机械化方法诸多应用的基础。结式给出超定方程组有公共解的充分必要条件，是代数几何的基本概念和消去理论的主要工具之一。代数稀疏结式由著名学者 Gelfand 等于上世纪 90 年代提出，构成了稀疏消去理论的基石。

本工作将稀疏结式这一数学机械化的核心理论与算法推广到了微分、差分方程系统，扩大了数学机械化方法的适用范围，是数学机械化的重要突破。我们建立了 Laurent 微分多项式系统的稀疏结式理论和计算这一微分稀疏结式的单指数算法。通过引进 Laurent 微分的符号指数矩阵，给出了用矩阵的秩来刻画稀疏微分结式存在的充要条件，从而将微分关系转化成线性代数关系。证明了

微分稀疏结式阶的上界是 Jacobi 界，这是关于微分消元理想的阶的最好上界。给出微分稀疏结式次数的估计，以此为基础给出了计算 Laurent 微分多项式系统的稀疏结式的单指数时间复杂度的算法。论文发表在计算理论顶尖杂志 FoCM(2015，67 页)。

我们进一步发展了差分方程的稀疏结式理论，发表在符号计算主要杂志 JSC。部分成果曾获美国计算机协会(ACM)符号与代数计算专业委员会(SIGSAM)颁发的 ISSAC 2011 唯一杰出论文奖。授奖词称："微分结式是微分代数和结式理论中一个***重要、困难与全新（original）的问题***。结式是***基本(fundamental)***的数学对象。作者一举严格定义了稀疏微分结式，证明了稀疏微分结式的一些***重要的性质***，并设计了一个基于矩阵运算计算稀疏微分结式的单指数算法。该***高效算法***将会对应用数学和计算科学领域中若干问题起到影响。我们预计这篇文章将会***阐明并开启***微分代数、结式理论、复杂性理论、线性代数和组合学中新问题的研究。"

差分 Toric 簇与差分二项式理想：

代数簇是代数几何的基本研究对象， 而 Toric 簇是非线性情形下相对比较简单的一类代数簇。在代数情形，Toric 簇对应的理想是 Laurent 二项式理想，也是代数情形下非线性非平凡的理想中最简单的一类，其对应的运算是格上的运算，这方面的研究已经非常成熟。在前两年, 我们研究了差分 Toric 簇与差分二项式理想的基本性质, 并将二项式的运算与 Z[x]模上的运算联系起来。今年, 我们进一步研究了 Z[x]模上的 Groebner 基的基本性质, 并基于其性质给出了计算 Groebner 基的高效算法, 给出了复杂度的估计。

微分周簇的存在性：

我们发展了微分周形式理论，定义了微分周坐标；通过微分周形式给出了微分簇的一些新的不变量，例如主微分次数与微分次数，并对微分代数闭链定义了由四个不变量构成的指标(index)。

称微分周簇是存在的，如果所有具有相同指标的微分代数闭链的微分周坐标构成的集合是高维空间中的一个微分可构造集。与 UC Berkeley 的模型论专家 T. Scanlon、J. Freitag 合作研究，最终利用模型论和 Scanlon 关于"Jet and

prolongation space”的结果证明了微分周簇的存在性。我们的主要想法是将由所有具有相同指标的微分代数闭链构成的集合可定义地（definably）嵌入到代数周簇的有限并中,并且证明象集是代数周簇中的一个微分可构造集。这里，由于我们是在微分闭域的模型中考虑问题，而微分闭域的模型论（DCF_0）具有量词消去，从而每一个可定义集合(definable set)都是可构造集。而在证明象集是可定义集时，我们用到了代数闭域的模型论（ACF）、微分闭域的模型论（DCF）中一些可定义性质。

微分周形式的算法：

Jacobi 阶数界猜想最早是由著名数学家 Jacobi 提出的，后经微分代数创始人 Ritt 用严格的代数语言陈述从而成为微分代数中一个经典的猜想问题。Jacobi 界猜想是讲：给定 n 个 n 元的微分多项式方程，假设它们有公共解，则其每个微分维数为零的不可约分支的阶数以系统的 Jacobi 数为上界。前人只对 n=1 或线性情形证明了该猜想成立，但一般情形至今仍然是公开问题。我们的主要结果是对给定微分特征列的微分素理想证明了它的阶数上界以特征列的 Jacobi 数为上界，作为推论证明了 Golubitsky 等人提出的另一猜想成立。另外我们估计了微分周形式的次数上界，并基于阶数和次数界的估计给出了计算微分周形式的单指数算法。相关论文发表在 Advances in Applied Mathematics.

Lüroth 定理的有效次数界：

Lüroth 定理是讲给定 m 个关于微分未定元 u 的微分有理函数，它们生成的微分扩域是基域的单扩张，即存在一个新的微分有理函数使得微分扩域可由此元素生成，我们称此元素为 Lüroth 生成元。而有效 Lüroth 定理问题是要给出 Lüroth 生成元的阶数与次数上界，从而可为 Lüroth 生成元的计算提供依据。D’Alfonso 等人曾给出阶数界与次数界，并且证明了该阶数界是最优的。我们的工作主要是给出一个更小的次数上界，从而优化了次数界。

Zeilberger 算法关于混合超几何项的终止性问题：

通过前期关于混合超几何项的结构定理，我们利用约化算法给出了判定双变元混合超几何项的 6 类邻差算子 (Telescoper) 存在的充分必要条件。与非混合 3 种情形一起，彻底解决了 Zeilberger 算法在双变元超指数-超几何情形的终止性问题。文章发表在符号计算领域权威期刊 JSC。

邻差算子的计算：

我们改进了已有关于超几何项的 Abramov-Petkovsek 约化算法，并基于该改进的约化算法给出了计算双变元超几何项的邻差算子的新算法。该算法的程序实现在效率上优于商业软件 Maple 的程序。文章发表于 ISSAC 2015。

微分差分方程的奇点分析：

多项式系数的线性微分差分方程的奇点为首项系数的零点，但是这些零点不一定是方程解的奇点。这类零点被称为伪奇点。我们给出了基于 Ore 算子的最小左公倍式(LCLM)计算的奇点消去算法，其效率远优于已有的算法。文章发表在符号计算领域权威期刊 JSC。

线性微分差分方程 Galois 群的算法：

基于 Hrushovski 文章的结果， 我们改进了 Hrushovski 原先的结果并完整给出了计算线性微分方程 Galois 群的算法，结果发表在《Advances in Applied Mathematics》。同时，我们将 Hrushovski 算法推广到线性差分方程情形。对于任意有理函数系数的线性差分方程，我们给出了算法求其 Galois 群。该算法是首个完整的计算线性差分方程 Galois 群的算法。

(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）

几何代数：

本年度主要工作集中在对经典的线几何射影变换与对偶模型建立完全性，并发展经典螺旋理论到射影变换。该项工作的介绍性摘要获得 AGACSE2015 唯一的最佳论文奖（Hestenes 奖）。这是几何代数应用领域国际上首次设立的奖项。

Groebner 基计算：

我们利用参数 Groebner 系统，全面地分析了计算机视觉中的 P3P 问题，给出了 P3P 问题实解个数的完全分类。我们对局部环中的带签名标准基算法进行了研究，并在计算机代数系统上实现。对 Groebner 基算法实现进行了研究，结合 F4,F5 算法思想，研究了利用矩阵计算和签名结构来计算大规模的 Groebner 基。

计算几何：

提出连续运动及变形的两二次曲面交线形态变化的符号检测算法：是首个关于检测二次曲面交线形态变化的成果，也是首个关于二次曲面连续碰撞检测的代数计算方法。

完成了两椭球相交形态的代数分类和穷举。过去多数关于碰撞检测的研究都关注其交线情况，然而在粒子物理模拟等应用中，更多的诉求集中在对两椭球相交的交体情况的判断。例如对于两椭球 A, B, “A 穿透 B，且 A 被分为三个部分”与“B 穿透 A，且 B 被分为三个部分”这两种情况，具有相同的交线情况，但显然 A ,B 的地位是不对等的，我们将所有这类的相交形态做穷举（20 种）并给出代数判定条件。

曲面蓝噪声采样及网格生成：关于最大化泊松圆盘采样和曲面重新网格化的工作发表于 ***Computers &Graphics***. 该工作在权威国际会议 *Shape Modeling International Conference* 上作了大会报告。

Cartan 行列式猜想与 Gorenstein 对称猜想：

Grothendieck 及其学生 Verdier 创建了导出范畴与三角范畴理论，Beilinson、Bernstein 和 Deligne 创建了三角范畴的 recollement 理论，代数的导出范畴的 recollement 与 tilting 理论、局部化理论、代数的整体维数、Hochschild 维数、K-理论、Hochschild（上）同调、循环同调等同调不变量密切相关。为澄清代数的导出范畴的 recollement 与代数的 Cartan 行列式、（Kontsevich-Soibelman）同调光滑性、Gorenstein 性之间的关系，我们引入了三角范畴的 n-recollement 及 n-导出单代数的概念，推广了三角范畴的 recollement 理论，并将代数的无界、上有界、下有界、有界导出范畴的 recollement 统一到代数的无界导出范畴 n-recollement 的研究框架下；证明了代数的导出范畴的 n-recollement （$n \geq 2$）中，中间代数的 Cartan 行列式恰为两边代数的 Cartan 行列式的乘积，从而揭示了代数的导出范畴的 n-recollement 与代数的 Cartan 行列式之间的关系；证明了代数导出范畴的 n-recollement （$n \geq 3$）中，中间代数为同调光滑的当且仅当两边代数为同调光滑的，从而澄清了代数导出范畴的 n-recollement 与代数的同调光滑性之间的关系；证明了代数的导出范畴的 n-recollement （$n \geq 4$）中，中间代数为 Gorenstein 的当且仅当两边代数为 Gorenstein 的，从而揭示了代数的导

出范畴的 n-recollement 与代数的 Gorenstein 性之间的关系。

作为上述结果的应用，我们将 Cartan 行列式猜想约化到 1-导出单代数，将 Gorenstein 对称猜想约化到 2-导出单代数，从而缩小了 Cartan 行列式猜想与 Gorenstein 对称猜想的研究范围。

有限域上非奇异 Hermitian 矩阵构造的迷向酉图：

Hubaut(1975)研究了有限域上非奇异 Hermitian 矩阵构造的迷向酉图 $U(n,q^2)$, 他证明了当 n>=6 时,$U(n,q^2)$是强正则图,并计算了它们的参数。C. Godsil, G. Royle(2001)研究了有限域上的辛群构造的辛图 Sp(2v,q), 计算了它们的参数, 并确定了 Sp(2v, 2)的自同构群。

根据前两者的工作,我们利用有限域上的酉群重新构造了迷向酉图 $U(n,q^2)$, 证明了当 n＝2 或 3 时，$U(2, q^2)$和 $U(3,q^2)$分别是顶点个数为 q+1 和 q^3+1 的完全图。当 n≧4 时，证明 $U(n, q^2)$是强正则的并计算了它的参数，当 n≠4,5 时确定了 $U(n, q^2)$的自同构群。其后我们研究了迷向酉图 $U(n, q^2)$的次成分,计算了它的参数，确定 $U(n, q^2)$的第一次成分是共边正则的，第二次成分是边正则的，并确定了第二次成分的自同构群。

迷向酉图 $U(n,q^2)$第一次成分自同构群的确定是一个比较困难的问题。2015 年我们对 n≧6 时确定了 $U(n,q^2)$的第一次成分的自同构群, 揭示了 $U(n,q^2)$第一次成分的自同构群和 $U(n,q^2)$的自同构群两者之间的联系, 发现前者是后者在顶点[e_1]上的固定子群在第一次成分上的限制。

一般来说, 整体的自同构群在局部上限制不是局部的自同构群, 两者只会在特定条件下才会相等；反过来, 两者如果相等也揭示了整体与局部之间对称性的某种联系。我们针对 $U(n, q^2)$与其第一次成分的参数, 通过组合计数的方法比较两者自同构群的数目, 发现它们是相等的, 从而确定了两者之间的联系。

这一问题的解决同时使我们得到了一个代数保持方面问题的答案: 设有限域上的 Hermitian 矩阵所对应的二次型的所有零点组成的集合记为 V, 同时以该 Hermitian 矩阵定义 V 上零点之间的一种联接关系,与 V 中任一非零零点 x 都有联接关系的零点组成的集合记为 V_x, 那么问 V_x 上到自身的保持联接关系的双射能否延拓成 V 上到自身的双射且仍然保持这样的联接关系不变? 通过把该

仿射情形的问题转化成射影的情况，再利用图论的语言就变成去研究 $U(n, q^2)$ 与其第一次成分自同构之间的关系，在 $n \geqq 6$ 时，我们对上述代数保持问题给出了肯定的回答。

这种通过有限域上的典型群构造的图(辛图，酉图，正交图)与其第一次成分之间，我们推测都会存在这样的联系存在。这种数学上整体与局部的对称性的联系是很出人意料的。我们将在未来的工作中进一步对此进行深入的研究。

(1.3) 多项式可信计算（支丽红、程进三）

实代数簇上线性函数的优化：

对于实代数簇上线性函数的优化问题，研究其最优值和最优值解如何依赖于目标函数的参数，即其最优值函数，有助于我们求解相应优化问题及分析其代数复杂度。当所考虑的代数簇为不可约、光滑且紧致时，其相应对偶代数簇的定义多项式即为优化问题的最优值函数。当实代数簇非紧致或非光滑时，我们研究了其相应对偶代数簇的定义多项式与最优值函数的关系。我们证明了如果光滑的不可约实代数簇的凸闭包的径向锥(recession cone)是有向的（pointed），则其相应对偶代数簇的定义的不可约多项式也是优化问题的最优值函数。对于非光滑的情形，利用分层降维技巧，将原可行域中的奇点作为低一维空间中的代数集考虑。通过不断递归降维，将奇点转化为光滑点考虑，再利用非紧致光滑条件下所得结果，也得到了最优值函数与可行域对偶代数簇定义多项式的关系。对于病态的情形，也即最优值函数在某些参数取值恒为零的情形，我们通过计算推广的极代数簇（modified polar variety），构造了一系列的多项式系统满足：对任何参数值，必对应于其中一个多项式系统，该系统可以约化成一个单变元多项式，其相应的有限多个根包含了优化问题在该参数值上的最优值。

非紧致的基本半代数集凸包的半定表示：

假定半代数集是紧致且满足阿基米德条件，根据正零点定理，此半代数集上任何非负线性多项式可由其对应的二次模中的线性多项式逼近。因此，可以通过一系列的半定规划松弛，得到一列谱多面体投影来逼近原半代数集的凸包。

然而在非紧致条件下，不能直接应用正零点整理，我们利用齐次化技巧，考虑半代数集在更高一维空间中生成的锥与此空间中单位球的交集。通过分析生成凸锥的特性，考虑其与单位球相交构成的紧致集合，利用正零点定理得到凸锥的半定表示，进而利用非齐次化技巧将生成的谱多面体投影还原到原半代数集所在空间，从而得到其半定表示。我们首次给出非紧致的基本半代数集凸包的半定表示存在的充分和必要条件。

混合计算：

给定实系数多项式环中具有正维实代数簇的理想， 我们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. 我们证明了在 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）。我们将算法推广到求半代数簇的实根理想的 Groebner 基。

代数曲线曲面的拓扑结构分析和逼近：

在分析代数曲线的拓扑结构和逼近中，求解双变元系统是一个基本的步骤。提出了改进的 Newton 迭代逼近，也就是在进行 Newton 迭代的过程中, 对可行会出现的跟踪跳线进行规避, 结合曲线的拓扑结构控制迭代步长, 使得迭代逼近限定在一个可控区域内, 这样既保证了逼近是保拓扑的,也同时控制了逼近精度。我们的工作在面对德国学者 Olive Labs 提出的代数曲线的可信可视化中面临的挑战性问题中表现出色: 高阶相切奇点, 拥有复杂奇点结构的代数曲线保拓扑的可视化方面效果优于同类方法。

2. 编码与密码（刘卓军、邓映蒲、张志芳、冯秀涛、潘彦斌、冷福生）

环类域对应：

类域论是代数数论的核心内容。经典的类域论是关于代数数域的代数整数环的某种对应，对于代数整数环的满秩子环即 order 也有类似对应，这被称为关

于 order 的类域论。已知的结果只有 Cox 于 1989 年在其书《Primes of the Form x^2+ny^2》对虚二次域的 order 利用二次型理论建立了类域论。我们对任意代数数域的 order 建立了类域论，并把它应用到虚二次域上不定方程 $p= x^2+ ny^2$ 的整可解性问题上，其中 p 是虚二次域中的素元，即主理想(p)是素理想。我们的方法不同于 Cox 的方法，这一工作已经在《Science China: Mathematics》发表。

特殊数的素数判定：

素数判定问题在 2004 年被三个印度学者 Agrawal- Kayal- Saxena 证明是 P 问题，但他们给出的 AKS 算法由于复杂性太高仅具理论意义而没有实际价值。另一方面，对于特殊数存在更快速的素数判定方法，这方面经典的例子有对于 Mersenne 素数的 Lucas-Lehmer 判别法和对于 Fermat 素数的 Pépin 判别法。我们给出了广义 Fermat 素数判定的二次确定性多项式时间算法，其中使用了代数数论中的高次互反律以及我们自己导出的一个 2p 次特殊互反律。这一工作已经被数论专门杂志《Acta Arithmetica》正式发表。另外，对于形如 Ap^n+w_n 的数，我们利用 Eisenstein 的 p 次互反律给出了它们的二次时间的确定性素数判定算法，解决了 F. Lemmermeyer 在 2000 年提出的一个公开问题。这一成果发表在算法专门杂志《Journal of Discrete Algorithms》。

格与代数攻击：

我们证明了对任意整格，都存在两种特殊格基，一种是格基各向量之间的夹角都在 60 度到 120 度之间；另一种是格基可分为两个集合的不交并，每个集合内的基向量两两正交。相关论文被 WISA2015 接收。

我们完成了对 2014 年亚密会上新提出的 HS 签名体制的攻击，严格证明了其在适应性选择消息攻击下是可伪造的，在非适应性选择消息攻击下不会是存在性不可伪造的；相关论文被 CT-RSA2016 接收。

轻量级序列密码算法研制：

参与总装备部信息通信保密实验室轻量级序列密码算法研制工作，主要负责轻量级序列密码算法研制和安全评估工作。该算法将参加国家密码管理局轻量级序列密码标准候选算法竞选。2015 年 10 月已将研制的密码算法、实现方

法和安全评估等技术文档提交。目前该算法处于非公开评估阶段。

对采用模加运算的密码算法进行差分故障分析：

模加是一个非常重要的密码运算部件，已经被用许多密码算法设计中。差分故障分析是一种针对密码算法实现的一种侧信道攻击方法。对采用模加运算的密码算法进行差分故障分析时，往往会导出一类模加差分方程。我们改进了 B. Debraize 和 I.M. Corbella 等人提出的利用 Gröbner 基方法求解上述模加差分方程的方法，并将之应用到 SPECK 一族分组密码算法，将 H. Tupsamudre 等人针对 SPECK 族算法的注入故障个数由 n/3 大幅降到了 log(n)。相关结果已经发表在国际会议 FDTC 2015。

DNS 异常流量检测及抗攻击研究进展：

出于各种原因，存在着对 DNS（域名服务器）不同种类的攻击。DDoS 攻击是分布式的拒绝服务攻击，攻击者通常会利用多台计算机发动攻击，目的是造成被攻击对象出现堵塞而瘫痪。显然，预防拒绝服务攻击意义重大。我们的研究成果概括为，提出了 IP 威胁度的概念；设计了评价 IP 威胁度的综合指标；建立了基于广义马氏距离和校准马氏距离的计算 IP 威胁度的模型；用 C 语言开发出了以实现 IP 威胁度计算为主要内容的软件包。

发生 DDoS 攻击的一个根本原因是存在来自不同 IP 对 DNS 服务器发出大量访问请求，因此每个发出访问请求的 IP 都对域名服务系统的安全稳定运行具有一定程度的威胁。基于对域名服务器内记录的报文日志文件进行分析，我们提出和设计了 9 个刻画 IP 威胁度的指标，并引入了对多维数据进行综合分析的马氏距离建模方法。由于直接应用马氏距离方法遇到了技术上的障碍，因此我们有针对性地提出了广义马氏距离和校准马氏距离方法。这些技术模型和进行多指标综合分析以实现IP威胁度计算的功能已经在用C语言开发的软件包中得以实现。

基于实际报文日志数据做出的检验分析结果表明：1. 利用综合指标评测 IP 威胁度的效果比利用单个指标评价 IP 威胁度更具有优势；2. 基于 IP 威胁度不同阈值的选取能够有效控制访问域名服务器的流量，通过将 IP 威胁度高的 IP 请求进行屏蔽是实现减缓域名服务器异常流量压力的合理策略；3. “综合指标

+基于马氏距离概念的计算模型”给出了分析判断拒绝服务攻击源的一种新的可用技术。

我们的研究成果说明，IP 威胁度的阈值将成为减缓域名服务器异常流量压力的一个可调节的控制变量。

分布式存储系统的局部修复码：

确定了参数范围 n1>n2 内局部修复码的最优极小距离。首先我们给出一个基于求解整数规划问题的极小距离上界，改进了前人的相关成果；然后在二元扩域上构造了达到该上界的码，从而说明我们得到的上界是紧的。

对于任意的局部性要求 r 和可达性要求 t，设计了满足(r,t)性质的二元局部修复码，码的信息率达到 r/(r+t)，高于前人的乘积码构造。该码在热点数据存储方面有重要应用价值。

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、张立先）

5 轴数控加工中的刀轴轨迹优化：

5 轴数控加工中的 G 代码的生成中, 包含两个方面的问题: 刀触点(刀心点)的轨迹(3 维)和刀姿(2 维)。 如果使用的刀具是球头刀(常作为精加工刀具), 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. 对于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。在该算法中, 我们引入了差分图的概念, 使得得到的刀姿与原有方法比较具有更好的光滑度和力学性能。

(3.2) 非线性数学物理方程（闫振亚）

时空（PT)-对称复外势的非线性 Schroedinger 方程解及其稳定性：

提出了具有PT-对称外势的非线性Schroedinger方程在吸引和排斥两种相互作用下统一的亮孤子解族，并且给出了线性特征值问题的PT-对称的相变破缺和为破缺的参数区域，发现非线性项能够将线性PT-对称的相变破缺点激发到稳定的非线性波状态。结果发表在国际重要期刊《Phys. Rev. A》、《Phys. Rev. E》上，并且被美国物理学会PRE封面图像专栏收录。

可积非线性波方程（组）的怪波解结构：

发现在非线性三种相互作用下（即吸引、排斥和混合），系统都拥有怪波解及其弹性相互作用，五阶非线性Schrodinger方程的五阶项系数能够调控非线性波从怪波结构退化为有理孤子形态（这可以从波的极值点个数来确定）。分析了怪波的时间传播。

结果发表在国际重要期刊《Phys. Rev. E》、《Chaos》等上,并且被《Chaos》2015年第10期和12期分别选为当期唯一的“FEATURED ARTICLE”（特别推荐论文）。

(3.3) 系统科学（李邦河、刘卓军、李博）

有限时间收敛的Gossiping算法：

与澳大利亚国立大学的石国栋以及瑞典皇家理工学院的M. Johansson, K.H. Johansson合作完成有关有限时间收敛的Gossiping算法的文章, 已被世界网络科学方面的顶级期刊IEEE/ACM TRANSACTIONS ON NETWORKING接收。在该文中，我们给出了确定性的对称gossiping算法有限时间收敛的充分必要条件，并给出了最快算法。给出了收敛速度最快的确定性非对称gossiping算法。

一个有N个节点的网络,每个节点i在时刻t都有一个取值。对称的gossiping算法，是指在时刻t+1，采取某种方式选取两个节点i和j，同时改变两个节点的取值为两点取值的平均值，其他点取值不变。取点的方式可以是确定性的，这种算法称为确定性的gossiping算法。也可以是随机取点，这种算法称为是随机gossiping算法。最终的目的是使得每个点的取值趋向同一个值。事实上这个共同值是整个网络各个节点初始值的平均值。例如，我们可以用这种算法计算

一大片地区的平均温度，平均 PM2.5 值等等。这一问题是许多领域的基础性问题，尤其是计算机科学领域。我们证明有限步确定性全局收敛的对称 gossiping 算法存在的充分必要条件是节点数 N 是 2 的幂次，并给出最快的收敛算法。

非对称的 gossiping 算法，是指在时刻 t+1，采取某种方式选取两个节点 i 和 j，只改变其中一个节点的取值为两点的平均值其他点取值不变。我们证明总存在有限步确定性全局收敛的非对称 gossiping 算法，并给出最快的收敛算法。

产品质量安全风险监测指标获取及筛查技术研究进展：

消费品量大面广，与之相关联的伤害数目大，伤害类型复杂。避免和减少由消费品造成的伤害，民众关心社会关注。通过国际比较，我们认为美国的伤害监测系统 NEISS，欧盟的不安全产品通报系统 RAPEX 都是非常值得借鉴的工作。为此，有很多基础性的技术方法需要提出和完善。作为支撑性的工作，我们完成的研究成果包括：

1. 提出可用于产品督察的基于伤害先验信息的多阶段抽样方案

多阶段抽样的好处是可以充分应用先验知识，尽可能节省成本。我们已根据消费者保护协会提供的数据，针对电视机及家具产品检验了多阶段抽样方法。验证了多阶段抽样方案的可行性。

2. 设计了基于二项分布的产品潜在事故率推断的小样本方法

产品安全问题有别于产品质量，由于产品质量安全所涉及的不仅仅是产品合格率，更应注重导致安全事故的潜在事故率，考虑到产品事故检测的过程是对总体潜在事故率的评估，每一个样本的检测则是相互独立的，满足二项分布检验的条件，所以可以通过样本集分布数据对总体分布进行二项分布假设检验。

利用二项分布检验方法可以实现的功能包括：（1）小样本状况（样本量较小）下的总体事故率检验，对于样本量没有严格限制，可以根据检验成本以及经费预算确定样本量；（2）利用检验的结果对给定的总体事故率做出显著性判断；（3）利用二项分布检验的表格推断总体事故率的区间估计。特别需要指出的是，这里的小样本方法不在于检验而在于推断。

3. 建立了产品质量安全指数的理论模型

为持续观察产品质量安全变化情况，一个自然的基础性工作是建立产品质量安全指数。我们提出在建立产品质量安全指数时，需要重点关注人的不当使用行为因素、产品质量因素和产品设计因素。这与大量消费品安全事故的主要原因相一致。产品质量安全指数的价值和效果还需要通过一定时间的实施及分析来判别。

4. 提出基于分层抽样方法产品伤害信息监测网的建设方案

类似于美国的NEISS系统，从医院获取产品伤害信息是非常明智的选择，因为这里能提供真实的伤害信息，而不仅仅是在有些情况下反映的是人们的情绪信息。

我国目前各类医院数量很大，超过2万多家。要求每家医院都定期提供这样的信息是不现实的，这样的工作只能通过少数定点医院进行，称这样的医院为检测医院或样本医院。样本医院是在全国所有医院中按概率抽样方法抽取的，在此基础上建立消费品质量人身伤害监测系统。

我们提出的具体方案是将全国按东部、中部、西部分成三个区域，全部医院按三级、二级、一级及未定级分为四级，综合考虑得到12个分层。各层内进行PPS方式抽样。以此为基础，我们可以通过从样本医院获取的产品伤害信息来推断整体的产品安全形势和趋势。

（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、微分周簇的存在性与计算微分周形式的算法（李伟）

在我的博士论文中，我们发展了微分周形式理论，定义了微分周坐标；通过微分周形式给出了微分簇的一些新的不变量，例如主微分次数与微分次数，并对微分代数闭链定义了由四个不变量构成的指标(index)；定义了微分周簇，称微分周簇是存在的，如果所有具有相同指标的微分代数闭链的微分周坐标构成的集合是高维空间中的一个微分可构造集；并用构造性方法证明了一类特殊

的微分周簇是存在的。但是对一般情形, 微分周簇的存在性没有得到证明。该问题的主要困难在于对一组由微分多项式和代数多项式组成的混合系统目前还没有混合消元理论与算法。

本人在 UC Berkeley 访问期间与模型论专家 T. Scanlon、J. Freitag 合作研究，最终利用模型论和 Scanlon 关于“Jet and prolongation space”的结果证明了微分周簇的存在性。我们的主要想法是将由所有具有相同指标的微分代数闭链构成的集合可定义地（definably）嵌入到代数周簇的有限并中,并且证明象集是代数周簇中的一个微分可构造集。这里，由于我们是在微分闭域的模型中考虑问题，而微分闭域的模型论（DCF_0）具有量词消去，从而每一个可定义集合(definable set)都是可构造集。而在证明象集是可定义集时，我们用到了代数闭域的模型论（ACF）、微分闭域的模型论（DCF）中一些可定义性质。相关论文已上传 Arxiv 并已投稿到 Jounal of London Mathematics Society.

Jacobi 阶数界猜想最早是由著名数学家 Jacobi 提出的，后经微分代数创始人 Ritt 用严格的代数语言陈述从而成为微分代数中一个经典的猜想问题。Jacobi 界猜想是讲：给定由 n 个 n 元微分多项式方程构成的系统，假设系统有公共解，则其每个微分维数为零的不可约分支的阶数以系统的 Jacobi 数为上界。前人只对 n=1 或线性情形证明了该猜想成立，但一般情形至今仍然是公开问题。

我们的主要结果是对给定微分特征列的微分素理想证明了它的阶数以特征列的 Jacobi 数为上界，作为推论证明了 Golubitsky 等人提出的另一猜想成立。另外我们估计了微分周形式的次数上界，并基于阶数和次数界的估计给出了计算微分周形式的单指数算法。相关论文发表在 Advances in Applied Mathematics.

代表性成果 2、局部修复码的最优极小距离（张志芳）

局部修复码是一种分布式数据存储编码，在云存储中有重要应用。它的一个主要特点是当系统中某些节点发生故障时，只通过连接少数其它节点就可以恢复失效节点的存储数据，从而保证系统的稳定性并使得修复效率大幅提高。目前，在微软，Facebook 等公司已经有实际平台在使用相关的编码技术，局部修复码是当前信息科学领域的一个研究热点。

码的极小距离是刻画其容错能力的一个重要参数，极小距离越大对应码的容错能力越强。给定码长、维数等其它主要参数，确定码的极小距离的界是一个在理论研究和实际应用中都非常有意义的问题。在传统的编码理论中已有很多经典结果，如 Singleton 界，Plotkin 界，Hamming 界，Gilbert-Vashamov 界等。

局部修复码由于增加了局部修复性的条件，很多经典的编码界无法达到。Gopalan 等人在 2012 年给出局部修复码的一个类似 Singleton 界，相关文章获得 2014 年 IEEE 的通信和信息论领域的联合论文奖。然而，这个界在参数 r+1 不整除 n 时的许多情形下是达不到的。后续的很多工作或者推广、或者部分地改进了这个界，也有一些优秀的工作涉及到在特定参数条件下具体构造达到该界的最优码。

我们得到了参数 n1>n2 时极小距离的一个改进的上界，并在二元扩域上给出达到该上界的局部修复码的显式构造，从而说明我们的上界在此参数范围内是紧的。这里 n1=[n/(r+1)], n2=n1(r+1)-n，可以看到，n1>n2 的条件实际上涵盖了 $r\leqslant\sqrt{n}$ 这一类参数取值范围。由于在实际存储系统为了保证较高的节点修复效率，r 的取值一般都不会太大，因此可以说，对于实际存储系统用到的大部分局部修复码的参数，我们已经确定了相应的最优极小距离，并给出最优码的显式构造。并且，我们的最优码在二元扩域上给出，比一般有限域上的码更便于工程实现。我们关于局部修复码的工作目前已有 2 篇论文发表于信息论权威期刊 IEEE Transactions on Inf. Theory, 根据 Google Scholar 统计，目前这两篇论文已分别被引用 7 次和 26 次。该项成果入选中科院数学与系统科学研究院 2015 年十大科研进展。

发表文章：

1. Anyu Wang, Zhifang Zhang: An Integer Programming-Based Bound for Locally Repairable Codes. IEEE Transactions on Information Theory 61(10): 5280-5294 (2015).

2. Anyu Wang, Zhifang Zhang: Repair Locality With Multiple Erasure Tolerance. IEEE Transactions on Information Theory 60(11): 6979-6987 (2014).

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.	“973”计划项目	数学机械化方法及其在数字化设计制造中的应用	2011	2015			高小山
2.	“973”计划项目子课题	数学机械化理论与算法	2011	2015	571	113	高小山
3.	“973”计划项目子课题	基于混合计算的误差可控算法	2011	2015	344	68	支丽红
4.	“973”计划项目子课题	基于数学机械化方法的高档数控系统	2011	2015	424	84	李洪波
5.	“973”计划项目子课题	中医原创思维与健康状态辨识方法体系研究	2011	2015	20	0	刘卓军
6.	“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	39.51	黄雷
7.	国家数学交叉中心	数学化制造与高档数控中的数学方法	2015	2015	67.8	67.8	李洪波
8.	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	2015	2015	59	59	李子明
9.	国家数学交叉中心	信息安全和密码体系	2015	2015	35.8	35.8	邓映蒲
10.	国家自然科学基金面上项目	代数的 Hochschild 同调与同调维数	2012	2015	43	0	韩阳

11.	国家自然科学基金面上项目	非自治光学畸形波的激发机理、参量调控和动力学研究	2012	2015	56	0	闫振亚
12.	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
13.	国家自然科学基金面上项目	素数判定与整数分解	2015	2018	60	0	邓映蒲
14.	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	0	程进三
15.	国家自然科学青年基金	基于格的公钥密码体制的安全性分析	2013	2015	22	0	潘彦斌
16.	国家自然科学青年基金	mu 基理论及其在计算几何中的应用	2013	2015	22	0	贾晓红
17.	国家自然科学青年基金	有限域上若干问题的研究	2013	2015	22	8.8	周凯
18.	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	8.8	李博
19.	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	8.8	李伟
20.	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	20	刘卓军
21.	质检公益性行业科研专项项目	综合标准化组织管理及标准综合体规划研究	2013	2015	38	0	刘卓军

22.	质检公益性行业科研专项项目	标准化系统工程方法及应用研究	2013	2015	18	0	刘卓军
23.	教育部留学回国启动经费	曲线曲面的逼近	2012	2015	3	0	程进三
24.	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	3	陈绍示
25.	解放军 61569 部队	序列算法设计评估规范	2015	2015	15	10.5	冯秀涛
26.	解放军	若干基础问题研究	2014	2015	20	10	潘彦斌
27.	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
28.	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
29.	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
30.	中科院信工所重点实验室开放课题	CAESAR 竞赛认证加密算法安全性分析	2015	2015	5	5	冯秀涛
合计	---	---	---	---		582.01	---

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.	法国	INRIA/CNRS	LIAMA 中法实验室项目： ECCA	2010	2015	5万欧元	1.2万欧元	支丽红
合计	---	---	---	---	---		1.2万欧元	---

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.	Elements of line geometry with geometric algebra	AGACSE 首届 David Hestenes 论文奖		李洪波、黄雷、董磊、邵长鹏
2.	Elements of line geometry with geometric algebra	首届 AGACSE 青年学者奖杯		黄雷
3.		爱思唯尔 2015 年中国高被引学者		高小山
4.		爱思唯尔 2015 年中国高被引学者		闫振亚
5.		入选 Elsevier 2014 年度中国高被引学者榜单		闫振亚
6.		《中国科学：数学》优秀服务奖		高小山
7.	局部修复码的最优极小距离	中科院数学院 2015 年度十大科研进展		张志芳、王安宇
8.		2015 年度系统所关肇直奖		李伟

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.	A Modified Abramov-Petkovsek Reduction and Creative Telescoping for Hypergeometric Terms	Proc. of ISSAC 2015, New York, ACM Press. pp. 117-124	Shaoshi Chen, Hui Huang, Manuel Kauers, Ziming Li	Shaoshi Chen	
2.	Desingularization of Ore Operators	Journal of Symbolic Computation 08/2014; 74. DOI: 10.1016/j.jsc.2015.11.001	Shaoshi Chen, Manuel Kauers, Michael F. Singer	Shaoshi Chen	
3.	On the Existence of Telescopers for Mixed Hypergeometric Terms	Journal of Symbolic Computation, 74(5/6), pp. 617-626, 2016	Shaoshi Chen, Frederic Chyzak, Guofeng Fu, Ruyong Feng, Ziming Li	Shaoshi Chen	
4.	A generic position based method for real root isolation of zero-dimensional polynomial systems	J. Symb. Comput. 68: 204-224，2015	Jin-San Cheng, Kai Jin	Jin-San Cheng	
5.	On the topology and visualization of plane algebraic curves	Computer Algebra in Scientific Computing,Volume 9301 of Lecture Notes in Computer Science, pp 245-259	Kai Jin, Jin-San Cheng, Xiao-Shan Gao	Kai Jin	
6.	New results on nonexistence of generalized bent functions	Designs, Codes and Cryptography, Vol.75 No.3 p. 375-385	Yupeng Jiang, Yingpu Deng	Yingpu Deng	
7.	On orders in number fields: Picard groups, ring class fields and applications	Science China: Mathematics, Vol.58 No.8 pp. 1627-1638	Lv Chang, Yingpu Deng	Yingpu Deng	
8.	Primality test for numbers of the form Ap^n+w_n	Journal of Discrete Algorithms, Vol.33 pp. 81-92	Yingpu Deng, Lv Chang	Yingpu Deng	

9.	Primality test for numbers of the form (2p)^{2^n}+1	Acta Arithmetica, Vol.169 No.4 pp. 301-317	Yingpu Deng, D Huang	Yingpu Deng	
10.	Hrushovski's algorithm for computing the Galois group of a linear differential equation	Adv. in Appl. Math 65,1-37,2015	Ruyong Feng	Ruyong Feng	
11.	Improved Differential Fault Analysis on the Block Cipher SPECK	IEEE Fault Diagnosis and Tolerance in Cryptography, 2015	Yuming Huo, Fan Zhang, Xiutao Feng, Liping Wang	Xiutao Feng	
12.	Curve fitting and optimal interpolation for CNC machining under confined error using quadratic B-splines	Computer-Aided Design, 66, 62-72, 2015	Z. Yang, L.Y. Shen, C.M. Yuan, X.S. Gao	X.S.Gao	
13.	Iso-scallop Tool-path Generation of 5-axis CNC Machining for Cyclide Patches	Proc. of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 229(7), 1144-1156, 2015	C. Min, X.S. Gao	X.S.Gao	
14.	Sparse Difference Resultant	Journal of Symbolic Computation, 68, 169-203, 2015	W. Li, C.M. Yuan, X.S. Gao	X.S.Gao	
15.	Sparse Differential Resultant for Laurent Differential Polynomials	Found. Comput. Math. (2015) 15:451–517	W. Li, C.M. Yuan, X.S. Gao	X.S.Gao	
16.	Tractable Algorithm for Robust Time-Optimal Trajectory Planning of Robotic Manipulators under Confined Torque	International Journal of Computers, Communications & Control, 10(1), 123-135, 2015	Q. Zhang, S. Li, J.X. Guo, X.S. Gao	X.S.Gao	
17.	Time Optimal Feedrate Generation with Confined Tracking Error based on Linear Programming	J Syst Sci Complex, 28(1), 80-95, 2015	J.X. Guo, Q. Zhang, X.S. Gao, H. Li	X.S.Gao	
18.	A bimodule approach to the strong no loop conjecture	J. Pure Appl. Algebra 219 (2015), no. 6, 2139-2143	Y. Han	Y. Han	

19.	Continuous Detection of the Variations of the Intersection Curves of Two Moving Quadrics in 3-Dimensional Projective Space	Journal of Symbolic Computation,73, 221-243	X. Jia, Wenping Wang, Yi-King Choi, Bernard Mourrain, Changhe Tu	X. Jia	
20.	Efficient Maximal Possion Disk Sampling and Remeshing on Surfaces	Computers & Graphics,46,72-79	Jianwei Guo, Dongming Yan, X. Jia, Xiaopeng Zhang	Dongming Yan	
21.	Finite-Time Convergent Gossiping	IEEE/ACM Transactions on Networking，在线发表,2015	Guodong Shi, Bo Li, Johansson, M., Johansson, K.H.	Bo Li	
22.	Elements of line geometry with geometric algebra	Early Proc. AGACSE '15, S.X. Descamps, J.M.P. Serra, R.G. Calvet (eds), FIB, Barcelona, ISBN: 978-84-606-9982-8, 2015, pp. 195-204	Hongbo Li, Lei Huang, Lei Dong, Changpeng Shao	Hongbo Li	
23.	Visual Tracking via Sparse and Local Linear Coding	IEEE Transactions on Image Processing. 2015; 24(11): 3796-3809	Guofeng Wang, Xueying Qin, Fan Zhong, Yue Liu, Hongbo Li	Xueying Qin	
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.	Difference Chow Form	Journal of Algebra, 428 (2015): 67-90	Wei Li, Ying-Hong Li	Wei Li	
26.	Differential Chow varieties exist	ArXiv:1504.03755, 2015	James Freitag, Wei Li, Tom Scanlon	Tom Scanlon	
27.	Simple Differential Field extensions and Effective Bounds	Proceedings of MACIS, Lecture notes in computer science, 2015	James Freitag, Wei Li	James Freitag	

28.	A Combinatorial Condition and Boolean Functions with Optimal Algebraic Imunity	J Syst Sci Complex (2015) 28(3): 725–742	Qingfang Jin, Zhuojun Liu, Baofeng Wu, Xiaoming Zhang	Qingfang Jin	
29.	基于广义和校准马氏距离对 IP 地址威胁度的诊断	《中国科学院大学学报》, 2015, 32(1): 18-24	钞婷, 李启寨, 刘卓军, 孙才, 孙云刚	李启寨	
30.	标准综合体再认识	《中国标准化》, 2, 2015	刘卓军, 黄冲	刘卓军	
31.	Relations Between Minkowski-Reduced Basis and θ-orthogonal Basis of Lattice	The 8th International Conference on Image and Graphics – ICIG 2015, LNCS 9219,169-179	Yuyun Chen, Gengran Hu, Renzhang Liu, Yanbin Pan, Shikui Shang	Yuyun Chen	
32.	Two Types of Special Bases for Integral Lattices	The 16th International Workshop on Information Security Applications - WISA 2015	Renzhang Liu, Yanbin Pan	Renzhang Liu	
33.	Controlling temporal solitary waves in the generalized inhomogeneous coupled nonlinear Schrodinger equations with varying source terms	J. Math. Phys. 56 (2015) 053508	Y. Q. Yang, Z. Y. Yan, D. Mihalache	Zhenya Yan	
34.	Dynamical behaviors of optical solitons in parity–time symmetric sextic anharmonic double-well potentials	Phys. Lett. A 379 (2015) 2025-2029	Z. C. Wen, Z. Y. Yan	Zhenya Yan	
35.	Generalized perturbation (n, M)-fold Darboux transformations and multi-rogue-wave structures for the modified self-steepening nonlinear Schrodinger equation	Phys. Rev. E 92, 012917 (2015)	X. Y. Wen, Y. Q. Yang, Z. Y. Yan	Zhenya Yan	

36.	Integrable PT-symmetric local and nonlocal vector nonlinear Schrodinger equations: A unified two-parameter model	Appl. Math. Lett. 47 (2015) 61-68	Zhenya Yan	Zhenya Yan	
37.	Novel wave structures in the two-dimensional cubic-quintic nonlinear Schrodinger equation with space-modulated potential and nonlinearities	Nonlinear Dyn. 82(2015) 119-129	Zhenya Yan	Zhenya Yan	
38.	Rogue waves, rational solitons, and modulational instability in an integrable fifth-order nonlinear Schrödinger equation	Chaos 25, 103112 (2015)	Y. Q. Yang, Z. Y. Yan, B. A. Malomed	Zhenya Yan	
39.	Spatial solitons and stability in self-focusing and defocusing Kerr nonlinear media with generalized parity-time-symmetric Scarff-II potentials	Phys. Rev. E 92, 022913 (2015)	Z. Y. Yan, Z. C. Wen, C. Hang	Zhenya Yan	
40.	Solitons in a nonlinear Schroedinger equation with PT-symmetric potentials and inhomogeneous nonlinearity: Stability and excitation of nonlinear modes	Phys. Rev. A 92, 023821 (2015)	Z. Y. Yan, Z. C. Wen, V. V. Konotop	Zhenya Yan	
41.	Two-dimensional vector rogue-wave excitations and controlling parameters in the two-component Gross-Pitaevskii equations with varying potentials	Nonlinear Dynamics 79(4),1-15	Zhenya Yan	Zhenya Yan	
42.	Achieving arbitrary locality and availability in binary codes	2015 IEEE International Symposium on Information Theory, arXiv:1501.04264, 2015	Anyu Wang, Zhifang Zhang	Zhifang Zhang	

43.	An Integer Programming-Based Bound for Locally Repairable Codes	IEEE Transactions on Information Theory, 61(10), 5280-5294, 2015	Anyu Wang, Zhifang Zhang	Zhifang Zhang	
44.	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	
45.	Optimizing a parametric linear function over a non-compact real algebraic variety	Proc. of ISSAC 2015: 205-212	Feng Guo, Mohab Safey EI Din, Chu Wang, Lihong Zhi	Lihong Zhi	
46.	Optimization Problems over Noncompact Semialgebraic Sets	Proc. of ISSAC 2015: 13-14	Lihong Zhi	Lihong Zhi	
47.	Semidefinite Representations of Non-compact Convex Sets	SIAM Journal on Optimization 25(1): 377-395, 2015	Feng Guo, Chu Wang, Lihong Zhi	Lihong Zhi	
48.	Automorphisms of subconstituents of unitary graphs over finite fields	Linear and Multilinear Algebra, 2015	Zhenhua Gu, Zhe-XianWan, Kai Zhou	Kai Zhou	

出版专著

序号	著作名称	作者	出版单位	出版日期
1	怪波的数学理论及其应用	郭柏灵, 田立新, 闫振亚, 凌黎明	浙江科技出版社	2015

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

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.	第三届国际符号和数值计算混合算法国际会议（The Third Workshop on Hybrid Methodologies for Symbolic-Numeric Computation）	国际	中科院数学院	支丽红	2015.8.10-14	80
2.	第五届计算机辅助制造、工程与数控中的数学与算法国际会议(5th International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control)	国际	中科院数学院	李洪波	2015.8.10-14	60
3.	第六届微分代数以及相关领域国际研讨会(The Sixth International Workshop on Differential Algebra and Related Topics(DART-VI))	国际	中科院数学院	高小山	2015.8.10-14	60
4.	计算机辅助几何设计相关的曲线曲面专题研讨会(Symposium on Curves and Surfaces in Computer Aided Geometric Design)	国际	中科院数学院	贾晓红 程进三	2015.8.13	20
5.	第七届全国计算机数学学术会议（CM2015）	国内	中科院数学院	李嘉禹	2015.10.30-11.2	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.	Modified Abramov-Petkovsek Reduction and Creative Telescoping for Hypergeometric Terms	陈绍示	The 40th International Symposium on Symbolic and Algebraic Computation(ISSAC2015)	英国	2015.07
2.	Reduction-based Algorithms for Creative Telescoping	陈绍示	SIAM Conference on Applied Algebraic Geometry 2015	韩国	2015.08
3.	Reduction-based Algorithms for Creative Telescoping	陈绍示	The Sixth International Workshop on Differential Algebra and Related Topic	北京	2015.08
4.	Solving polynomial system with linear univariate representation	程进三	Application of Computer Algebra 2015(ACA2015)	希腊	2015.07
5.	On the topology and visualization of plane algebraic curves	程进三	CASC2015	德国	2015.09
6.	Certifying and Computing the simple roots of zero-dimensional polynomial system	程进三	Third Workshop on Hybrid Methodologies for Symbolic-Numeric Computation	北京	2015.08
7.	Solving polynomial system with linear univariate representation	程进三	Triangular decomposition of polynomial systems: solvers and applications	北京	2015.08
8.	How Many Regions Does a Real Algebraic Curve Divide the Plane?	程进三	Curves and Surfaces in Computer Aided Geometric Design	北京	2015.08
9.	广义 Fermat 素数的判定（邀请报告）	邓映蒲	International Conference on Coding Theory, Cryptography and Related Topics	扬州	2015.04
10.	素数判定与整数分解	邓映蒲	编码与密码学高级研讨班	北京	2015.06
11.	谈谈整数分解（邀请报告）	邓映蒲	中国密码学会密码数学理论专业委员会 2015 年学术研讨会	福州	2015.09
12.	Nonexistence of two classes of generalized bent functions（邀请报告）	邓映蒲	2015 年组合与编码国际研讨会	合肥	2015.10
13.	On the computation of the Galois group of linear difference equations	冯如勇	Differential and Difference Equations: Analytic, Arithmetic and Galoisian Approaches	法国	2015.10

14.	Improved Differential Fault Analysis on the Block Cipher SPECK	冯秀涛	Workshop on Fault Diagnosis and Tolerance in Cryptography	法国	2015.09
15.	Efficient and Robust Time-Optimal CNC Interpolation under Dynamic Constraints	高小山	5th International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control (MAMENC)	北京	2015.08
16.	Binomial Difference Ideal and Toric Difference Variety（邀请报告）	高小山	International Workshop on Computational Approaches to Algebraic Geometry	三亚	2015.09
17.	Differential and Difference Chow Form and Sparse Resultant（邀请报告）	高小山	International Workshop on Differential and Difference Equations: Analytic, Arithmetic, and Galoisian Approaches	法国	2015.10
18.	Differential and Difference Chow Form, Sparse Resultant, and Toric Variety（邀请报告）	高小山	第七届全国计算机数学学术会议（CM2015）	合肥	2015.11
19.	An algebraic approach of computing the variations of the intersection curve of two moving quadrics	贾晓红	Curves and Surfaces in Computer Aided Geometric Design	北京	2015.08
20.	Role of Moving Planes and Moving Spheres Following Dupin Cyclides	贾晓红	5th International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control(MAMENC)	北京	2015.08
21.	Elements of line geometry with geometric algebra	黄雷	Applied Geometric Algebra in Computer Science and Engineering 2015(AGACSE2015)	西班牙	2015.07
22.	任意内积空间的二向量完全正交分解的算法	黄雷	第七届全国计算机数学学术会议（CM2015）	合肥	2015.11
23.	Syzygies for the basis-free definition of quaternionic or Clifford polynomial ring.	李洪波	Joint Mathematics Meetings 2015	美国	2015.01

24.	An Alternative Method for Computing the Zariski Closure of a Regular Set（邀请报告）	李洪波	GC 2015-International Seminar on Geometric Computation	南宁	2015.02
25.	On the Approximate Expression of Scallop Height under High-Order Contact	李洪波	5th International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control(MAMENC)	北京	2015.08
26.	A Contest of Three Provers by Mathematical Olympiad Problems in Solid Geometry	李洪波	第七届全国计算机数学学术会议（CM2015）	合肥	2015.11
27.	Symbolic Geometric Reasoning with Advanced Invariant Algebras（邀请报告）	李洪波	MACIS 2015 (Sixth International Conference on Mathematical Aspects of Computer and Information sciences)	德国	2015.11
28.		李　伟	Arithmetic and Algebraic Differentiation: Witt vectors, number theory and differential algebra	美国	2015.05
29.	On the existence of differential Chow varieties	李　伟	Second Vaught's Conjecture Conference	美国	2015.06
30.	On the existence of differential Chow varieties	李　伟	The Sixth International Workshop on Differential Algebra and Related Topic	北京	2015.08
31.	Simple Differential Field extensions and Effective Bounds	李　伟	MACIS 2015 (Sixth International Conference on Mathematical Aspects of Computer and Information sciences)	德国	2015.11
32.	微分周簇的存在性	李　伟	系统科学青年学者论坛	北京	2015.12
33.	Reductions for Integration, Summation and Creative Telescoping（邀请报告）	李子明	The Sixth International Workshop on Differential Algebra and Related Topic	北京	2015.08

34.	两个人的对话：Offensive vs Defensive	刘卓军	第 4 届海峡两岸资讯安全研讨会	台湾	2015.01
35.	安全生产领域创新趋势	刘卓军	第九届北京安全文化论坛	北京	2015.11
36.	Cyber Space Security: Offensive vs Defensive	刘卓军	Workshop on Automated Reasoning at Toyama	日本	2015.11
37.	Solving Random Subset Sum Problem by l p -norm SVP Oracle	潘彦斌	2015 年编码理论与密码学及相关课题国际研讨会	扬州	2015.04
38.	Lattice-Base Public-Key Cryptography	潘彦斌	数论与密码青年学者研讨会	北京	2015.07
39.	The Generalized Rabinowitsch's Trick	王定康	Application of Computer Algebra 2015(ACA2015)	希腊	2015.07
40.	Discovering geometric theorems by using parametric Groebner basis	王定康	Symposium on Symbolic Computation and Automated Reasoning 2015	北京	2015.11
41.	PT-symmetric nonlinear waves（邀请报告）	闫振亚	第 6 届国际非线性数学物理会议暨第 13 届全国可积系统会议	潍坊	2015.08
42.	Rogue wave solutions of the higher-order nonlinear Schroedinger equation（邀请报告）	闫振亚	第三届全国光孤子会议	金华	2015.10
43.	Efficient Groebner bases computation for Z[x] lattice	袁春明	Application of Computer Algebra 2015(ACA2015)	希腊	2015.07
44.	Binomial difference ideal and toric difference variety	袁春明	The Sixth International Workshop on Differential Algebra and Related Topic	北京	2015.08
45.	Tool orientation optimization for 5-axis machining with C-space method	袁春明	5th International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control(MAMENC)	北京	2015.08

46.	Avoiding 5-axis singularities using additional matrix transformation	张立先	5th International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control(MAMENC)	北京	2015.08
47.	Optimal locally repairable codes	张志芳	2015 年编码理论与密码学及相关课题国际研讨会	扬州	2015.04
48.	Binary locally repairable codes from designs	张志芳	2015 年组合与编码国际研讨会	合肥	2015.10
49.	Locally Repairable Codes for Distributed Storage Systems	张志芳	系统科学青年学者论坛	北京	2015.12
50.	Semidefinite Representations of Non-compact Convex Sets（邀请报告）	支丽红	2015 International Symposium on Symbolic and Numeric Computation	德国	2015.06
51.	Optimization Problems over Noncompact Semialgebraic Sets（邀请报告）	支丽红	The 40th International Symposium on Symbolic and Algebraic Computation(ISSAC2015)	英国	2015.07
52.	Optimizing a Parameteric Linear Function over a Non-compact Real Algebraic Variety	支丽红	SIAM Conference on Applied Algebraic Geometry 2015	韩国	2015.08

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.	遥感数据的模式识别算法研究	2015.5	2015.12	1	1	谢福鼎	闫振亚
2.	非刚性二维形状的内蕴相似性分析以及结构对称性检测	2015.5	2015.12	1	1	韩丽	袁春明
3.	数控系统的最优控制方法	2015.5	2015.12	1	1	李树荣	王定康
4.	符号数值混合计算	2015.5	2015.12	1	1	杨争峰	支丽红

5.	基于凸代数几何的多项式优化问题研究	2015.5	2015.12	1	1	郭峰	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、实验室大事记

1、中国科学院数学机械化重点实验室第四届学术委员会第一次会议于 2015 年 3 月 31 日在中科院数学与系统科学研究院召开，万哲先院士、陆汝钤院士、李邦河院士、林惠民院士、高小山研究员、北京大学张继平教授、清华大学王小云教授、李洪波研究员，以及新一届的学术委员会委员：北京航空航天大学王东明教授、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等 10 多位实验室学术委员会成员参加了会议。中科院前沿科学与教育局重点实验室处李云龙副研究员应邀参加了会议。此次会议由实验室学术委员会主任李邦河院士主持。

实验室主任李洪波研究员首先介绍了计算机数学目前国际发展、实验室前五年的发展情况以及 2014 年实验室的评估情况，接着从数学机械化核心算法以及数学机械化应用方面重点介绍了实验室后五年的工作设想，最后提到了实验室目前的团队建设问题。随后，邓映蒲研究员、贾晓红副研究员分别作了素数判定以及几何建模的学术报告。

在听完汇报后，与会专家们对实验室取得的成绩表示了认同，同时专家们也提出了多项建设性的意见。林惠民院士与实验室科研人员进行了学术探讨与指导，对实验室的人才培养给出了建议。张继平教授与实验室科研人员进行了学术探讨与指导，对实验室的团队建设给出了建议。宗传明教授认为实验室研究的的数学机械化、编码密码等很有前途，与实验室科研人员进行了学术探讨与指导，并对实验室引进人才给出了建议。王小云教授认为实验室的研究有新意，是目前的热点，与实验室科研人员进行了学术探讨与指导，并对实验室的人才培养提出了建议。林东岱研究员与实验室科研人员进行了学术探讨与指导，对实验室的团队建设给出了建议。王东明教授认为实验室的自动推理、数学机械化、符号计算在国际上处于领先水平，影响大。但是如果想要取得更大的成绩，王东明教授建议开创新的研究领域，把研究新问题的重要性马上显示出来，

不仅可以扩大实验室的影响，同时可以吸引更多的人才来实验室。

李邦河院士最后总结提出要做应用数学就要做实际的问题，要接地气，这样研究才有意义，同时建议实验室组织人才力量，将吴方法发扬光大，扩大吴方法在国际上的影响力，这样可以大大促进实验室发展，提高实验室的学术地位。

2、 2015 年计算机辅助制造、工程与数控中的数学与算法国际会议（MAMENC2015）于 2015 年 8 月 10-14 日在国家会议中心召开。会议邀请了美国、以色列、匈牙利、韩国、德国等国家的大学与科研单位，以及国内的清华大学、华中科技大学、中国科学技术大学、中国科学院大学、中国科学院沈阳计算技术研究所、中国科学院沈阳自动化研究所、北京航空航天大学、南昌大学、辽宁师范大学等单位的 60 余位老师和研究生参加。

会议由中国科学院数学与系统科学研究院李洪波研究员（国家数学与交叉科学中心先进制造部主任、中国科学院数学机械化重点实验室主任）致开幕词。以色列国家技术研究所 (Technion)副所长 Moshe Shpitalni 教授；匈牙利布达佩斯技术和经济大学 Gabor Stepan 教授（匈牙利科学院院士、欧洲科学院院士 member of the Academy of Europe)；美国 Michigan 大学副校长 S. Jack Hu 教授；韩国 Seoul National University 副校长 Myung-Soo Kim 教授；以色列国家技术研究所 (Technion) 计算机系副系主任 Gershon Elber 教授；美国波音公司工业科学家 Thomas Grandine 博士；中国科学院数学与系统科学研究院副院长高小山研究员；TU Berlin 机床刀具与制造技术系 Eckart Uhlmann 教授（由 Bernd Peukert 代讲）；华中科技大学 Chen-Han Lee 教授；清华大学朱煜教授等分别做了各自研究领域的大会报告。

计算机辅助制造、工程与数控中的数学与算法国际会议今年是第五次举办，此次会议是第八届国际工业与应用数学大会（ICIAM2015）的嵌入会议，由中国科学院数学与系统科学研究院数学机械化实验室承办，经费来源为国家数学

与交叉科学中心、中国科学院数学与系统科学研究院、中国科学院系统科学研究所、中国科学院数学与系统科学研究院数学机械化实验室等。此次会议邀请众多国际国内著名专家学者做报告，促进了数字化制造领域国内外科研单位之间的交流与合作，对数学与先进制造领域学术研究的交叉与融合起到了重要作用。

3、2015 年 8 月 13 日，计算机辅助几何设计相关的曲线曲面专题研讨会(Symposium on curves and surfaces in computer aided geometric design)在国家会议中心召开。该会议旨在为从事计算代数几何理论研究与从事计算机辅助几何设计及计算机图形学研究的学者们在曲线曲面相关理论和应用方面搭建桥梁，以促进彼此探索新领域研究新问题。会议邀请了美国、以色列、西班牙、韩国等国家的科研单位、及国内包括中国科学院大学、浙江大学、中国科技大学、哈尔滨工业大学等众多高校的 60 余名科研人员参与。

会议由中国科学院数学与系统科学研究院副研究员贾晓红致开幕词，并由中国科学院数学与系统科学研究院副研究员程进三及美国莱斯大学计算机系教授 Ron Goldman 协同主持。会议从计算代数几何与几何建模两个角度阐述曲线曲面的相关理论和应用。在计算代数几何理论方面，著名代数几何学家、美国 Amherst college 教授 David Cox、美国 Louisiana State University 教授 Jerome Hoffman、西班牙 University of Barcelona 教授 Carlos D'Andrea 及美国 Southeast Missouri State University 教授 Haohao Wang 均对曲线曲面的 Syzygy 模理论（mu 基理论）的现状与未来做了精彩报告。在几何建模相关的应用方面，计算几何的资深前辈：以色列 Tel-Aviv University 教授 David Levin、美国莱斯大学计算机系教授 Ron Goldman、韩国 Seoul National University 副校长 Myung-Soo Kim 教授及以色列国家技术研究所 (Technion) 计算机系副系主任 Gershon Elber 教授均做了精彩报告。另外，中国科学院数学与系统科学研究院副研究员程进三、中国科学院数学与系统科学研究院副研究员贾晓红、浙江大学副教

授蔺宏伟及合肥工业大学副教授王旭辉等青年学者也对其新近科研成果做了报告。

此次会议是第八届国际工业与应用数学大会（ICIAM2015）的嵌入会议，由中国科学院数学与系统科学研究院数学机械化实验室承办，经费来源为国家数学与交叉科学中心、中国科学院数学与系统科学研究院、中国科学院系统科学研究所、中国科学院数学与系统科学研究院数学机械化实验室等。此次会议促进了国内外科研单位之间的合作与交流，对计算代数几何理论与几何建模相关应用的交叉起到了融合作用。

4、第三届国际符号和数值计算混合算法国际会议作为第八届国际工业与应用数学大会（ICIAM2015）的嵌入会议于 2015 年 8 月 10 日-14 日在国家会议中心成功举办。美国 Georgia Tech 大学 Anton Leykin 教授,美国 North Carolina State University 大学 Erich Kaltofen 教授（ACM Fellow），香港 The Hong Kong Polytechnic University 大学 Xiaojun Chen 教授, 法国 CNRS 研究所 Jean B. Lasserre 研究员（SIAM Fellow）做了精彩的邀请报告。 来自美国，法国、加拿大、比利时、日本、阿根廷、中国的 25 位专家做了精彩的大会报告。参会人员 80 余人来自 10 多个国家与地区。 会议由中国科学院数学与系统科学研究院支丽红研究员（主席）与美国 North Carolina State University 大学 Erich Kaltofen 教授、加拿大 Waterloo 大学 Mark Giesbrecht 教授、法国 Paris 6, Universite Pierre et Marie Curie 大学 Mohab Safey El Din 共同组织。 会议得到中国科学院数学与系统科学研究院、交叉中心、973 项目“数学机械化方法及其在数字化设计制造中的应用”和国家自然科学基金委“基于符号-数值混合计算的误差可控算法及应用”项目的支持。

此次会议促进了符号和数值混合计算领域专家学者之间的交流与合作。为参会人员提供展示原创性研究结果，了解符号和数值混合计算的最新进展。

5、“第六届微分代数以及相关领域国际研讨会”于 2015 年 8 月 10 日至 8 月 14 日在北京举行。会议主题包括代数微分与差分方程、微分代数群、微分代数与模型理论、微分及差分 Galois 理论、微分不变量、D-模理论以及 Riemann-Hilbert 对应、外微分与可积系统、Rota-Baxter 代数及其应用、计算微分与差分代数、微分与差分代数的应用等。本次会议与会人员约 60 人，其中有来自美国、英国、德国、奥地利、西班牙、俄罗斯、阿根廷、哥伦比亚、伊朗等国外与会人员约 30 人。本次会议总共邀请了 28 位国内外微分代数以及相关领域的专家学者做了报告，其中 3 个 1 小时报告、25 个 30 分钟报告。本次会议促进了国内外学者的了解与交流，加强了合作，特别是为国内青年科研人员与国外专家学者的合作提供了良好的交流平台。本次会议有助于青年研究人员了解微分代数领域最新的进展以及有待解决的难题，同时也有助于传播国内科研人员在本领域的学术成果。

6、数学机械化国际暑期学校于 2015 年 8 月 17 日至 8 月 21 日在中国科学院数学与系统科学研究院新楼 N204 成功举行。本次暑期学校由中国科学院数学机械化重点实验室主办，并得到了中国科学院数学与系统科学研究院的大力支持。

暑期学校的主讲教授分别为：美国 Armhest 大学的 David Cox 教授，西班牙巴塞罗那大学的 Carlos D'Andrea 教授，美国北卡州立大学的 Erich Kaltofen 教授，奥地利 Linz 大学的 Manuel Kauers 教授，德国亚琛工业大学的 Michael Wibmer 副教授。课程主题涉及符号计算，符号-数值混合计算，线性微分、差分方程的算法理论，计算代数几何，差分代数及伽罗瓦理论等。来自全国十几所重点院校以及部分科研单位的 100 多名研究生以及青年教师参加了暑期培训。此次暑期学校扩大了学员们在相关研究领域的知识面，并且促进了他们与国际知名学者之间的学术交流。

7、973 项目“数学机械化方法及其在数字化设计制造中的应用”课题结题总结与学术交流会于 2015 年 9 月 12－14 日在北京举行。课题验收专家组成员包括：南京大学吕建院士，中科院软件所林惠民院士，浙江大学彭群生教授，西安电子科技大学马建峰教授，北京航空航天大学王东明教授，北京应用物理与计算数学研究所江松研究员，北京大学查红彬教授，北京航空航天大学赵罡教授，华中科技大学李振瀚教授，中科院软件所詹乃军研究员，中科院计算技术研究所李华研究员，中国科学院数学与系统科学研究院高小山研究员。

会议将分为两个阶段进行：9 月 12－13 日：项目结题总结与学术报告会。项目承担人对项目启动以来取得的主要学术进展、人才培养、学术交流进行了认真总结。9 月 14 日，4 个课题组的课题组长从发表的论文、论著、获奖、申请专利、培养研究生情况、学术交流等方面详细汇报了各自的工作情况。专家组对各个课题与项目的总体情况进行了认真评议，提出了结题意见。

专家组对项目的总体执行情况进行了认真评估，认为本项目过去五年在数学机械化理论与算法、数字化设计制造方面取得了突破性进展，发表了大批高质量论文，在国际顶尖杂志上发表了多篇论文，获得了 3 个国家级奖励与多个主要国际奖励，数学机械化成果进一步得到了国际数学界的承认。项目取得的成果显示，本项目圆满完成了任务书规定的任务，达到了项目预期目标。

8、第七届全国计算机数学学术会议（CM2015）于 10 月 30 日至 11 月 2 日在合肥高速开元酒店召开。本次学术会议由中国数学学会计算机数学专业委员会主办，中国科学技术大学数学科学学院和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 1 3 0 人参加了会议。

会议期间，中国科学院数学与系统科学研究院的高小山研究员做了 " Differential and Difference Chow Form, Sparse Resultant, and Toric Variety " 的邀请报告，中国科学技术大学的刘利刚教授做了 " 3D 打印中的几何与计算问题 " 的邀请报告，北京大学的宗传明教授做了 " 正四面体的堆积理论以及一些计算结

果 " 的邀请报告，浙江大学的梁友栋教授也做了特邀报告。Maple 公司也应邀做了产品介绍。此外，会议还安排了 37 位研究人员在本次会议的分组会议上做了学术报告。