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

联系电话： 82541851

传真： 82541809

E-MAIL： dzhou@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

实验室基本概况

"数学机械化"是我国数学家吴文俊先生在七十年代末开始倡导的一个研究领域，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。

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。

自动推理是与数学机械化密切相关的学科。自动推理源于人工智能，主要研究推理的自动化与机械化。国外主要以逻辑为基础开展自动推理研究，而吴方法的基础是代数几何。国际上自动推理界在注意发展新方法的同时，积极开展应用研究，如程序正确性验证，自动程序生成等。

信息安全理论是研究信息在传输或存储过程中保证信息的"可靠性"、"完整性"、"秘密性"、"真实性"等要求的一门科学。现代密码学和纠错编码理论等都是信息安全理论的基础。密码学自 1976 年 Differ 和 Hellman 提出公钥密码体制以来，得到了迅猛发展。1985 年 Koblitz 和 Miller 提出将椭圆曲线用于公钥密码体制。椭圆曲线密码体制现在不仅是一个重要的理论研究领域，而且已经作为民用信息安全技术走向产业化。

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。

1990 年，中国科学院批准成立数学机械化中心。数学机械化中心建立三十多年以来，取得了一系列高水平的科研成果，获得了十余项国内外重要奖励。特别值得指出的是，吴文俊先生获 1997 年自动推理最高奖"Herbrand 自动推理杰出成就奖"。这一荣誉表明吴方法已经被国际学术界认为是自动推理领域经典性的工作。由于在数学机械化与拓扑学方面的杰出贡献，吴文俊先生于 2000 年获得首届"国家最高科学技术奖"，并于 2006 年获得"邵逸夫数学科学奖"。

数学机械化研究得到国家领导部门的充分肯定和大力支持。国家科技部在"21 世纪科学发展趋势"的报告中，将数学机械化列为重大科学问题；国家自然科学基金委员会和中国科学院在"九五"规划中，都将数学机械化列为优先发展的研究领域。

数学机械化中心作为主要承担单位，主持了八五国家攀登计划项目"机器证明及其应用"，九五攀登项目"数学机械化及其应用"，"973"项目"数学机械化与自动推理平台"，"数学机械化方法及其在信息技术中的应用"以及"数学机械化方法及其在数字化设计制造中的应用"，并以这些项目为依托积极组织国内外数学机械化合作研究与学术交流。经过二十多年的努力，数学机械化中心已经成为国际数学机械化研究、学术交流与人才培养的中心。

2003 年，数学机械化中心与信息安全中心联合成立了数学机械化重点实验室。

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。**

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。

几何计算：计算机辅助设计、计算机图形学、计算机视觉、虚拟现实、机器人与数控技术等信息技术中很多关键问题可以表示为几何问题的推理与计算。传统的几何建模都基于参数表示，所构造的几何形体一般都比较规则，并且拓扑结构也比较简单。近年来，得益于三维激光测量技术的进步，三维几何数据的获取能力得到了大大提高，使得我们需要处理关于复杂形体的海量数据。随着设计形体的复杂程度越来越高，传统的几何造型技术已无能为力。发展新的几何建模技术对于计算机用于高档数控系统、医疗技术、军事技术都有着重要意义。基于方程求解和不变量代数的方法，实验室成员提出了工程几何方法、关于计算机作图的 C 树分解方法和共形几何代数模型，在计算机辅助设计、数控系统、计算机视觉、计算机图形学的研究中得到重要应用。

符号计算：符号计算利用计算机准确地表示和操作数学对象，描述数学结构，并进行无误差计算和推导。国际计算机协会(ACM)成立之初就设立了符号与代数计算专业委员会(SIGSAM)，符号计算软件(例如： Maple 和 Mathematica)已成为工程计算和教育的基本工具之一。实验室在符号计算方面的工作主要包括：方程求解、符号分析、混合计算等。方程的符号求解是吴文俊开创的数学机械化方法

的核心思想的继承和进一步发展，目前范围已从传统的代数方程组，扩展到微分、差分和有限域方程组。符号求解在代数与常微情形已经成熟，今后研究的重点将是偏微分方程、差分方程、非交换方程、有限域上非线性方程的机械化方法。实验室成员在符号分析方面的工作得到国际上的高度重视，设计的若干关于符号分析的算法已进入国际著名的符号计算软件 Maple。

符号分析：符号分析是指利用计算机表示和操作函数、积分、级数等含有“无穷信息”的数学对象，它在物理和控制论中有广泛的应用。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。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。

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。

- **信息安全的数学理论。**

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。

计算数论：计算数论在密码设计与分析中有重要应用。实验室主要研究大整数的素性检验、因数分解、超椭圆曲线分类等。

密码分析： 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方程组的不可解性。数学机械化方法为有限域上非线性方程组求解提供了有力工具，在密码分析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，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。本实验室提出并研究安全多方计算的并行模型，在此基础上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。

- **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。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。近年来，我们在数控系统的关键问题：空间刀补与样条插补方面取得重要进展，提出了直线段和曲线段插补的最优算法、基于曲面重构的空间刀补方法，并申请了专利。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。

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。

计算机数学概述

1、什么是计算机数学

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。需要说明的是，离散数学研究的侧重点与传统数学有所不同。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。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。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。

2、历史回顾

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。

3、计算理论

A. Turing 因为提出计算理论的基本概念 Turing 机，被誉为现代计算机奠基人之一。Turing 这一研究的起因是希望回答 Hilbert 计划中的可判定性问题。为了回答可判定性问题，首先需要明确可以用于判断的计算手段。为此，Turing 改进了 Goedel 的想法，提出著名的 Turing 机。Turing 机不是一种具体的机器，而是一种计算模型。根据 Church-Turing 假设，用任意算法可以计算的问题，都可以用 Turing 机计算。换句话说，Turing 机为计算这个抽象术语提供了一个严格的数学模型，从而为算法的严格研究奠定了基础。在其论文中，Turing 证明 Turing 机的停机问题是不可判定的，即不存在一个算法，判定 Turing 机对于所有可能的输入是否停机，从而给出了 Hilbert 可判定性问题的又一个反例。

著名的不可判定的数学问题，除了 Goedel 与 Turing 所给的例子之外，还有

Hilbert 第十问题：任意整数系数多项式方程是否存在整数解是不可判定的。

在计算理论中，关于不可判定性的研究属于基础理论范畴。如前所述，计算机数学更关心的是如何实现高效计算。所以，计算复杂性理论成为计算理论的主流。

计算复杂性主要研究算法的复杂度，包括时间与空间复杂度，即对于给定的输入，在 Turing 机上用多少步骤与多少存储空间可以完成所给的计算。其中又以时间复杂度最为重要。设输入的大小是 n，则在 n 的多项式时间内可以用 Turing 机求解的问题的集合记为 P，在 n 的指数时间内可以用 Turing 机求解的问题的集合记为 EXPTIME。显然，P 是 EXPTIME 的真子集。一般认为，P 中的问题是可以在计算机上大规模高效求解的。所以对于 P 中问题的界定变为计算复杂性的核心问题。

一类介于 P 与 EXPTIME 之间的计算问题，NP 类，在计算复杂性中扮演关键角色。NP 类是指由非确定型 Turing 机在多项式时间内可以解决的判定问题。所谓非确定型 Turing 机，是指在一步计算中可以根据不同条件选择多种执行步骤的 Turing 机。通俗地讲，P 问题是指能够在普通计算机上多项式时间内求解的判定问题，而 NP 问题则是指那些在普通计算机上能够在给定正确信息下，可以在多项式时间内验证的判定问题。很显然，P 属于 NP，那么 NP 是否属于 P？这就是著名的“P=NP？”问题，是计算复杂性的核心研究问题。

20 世纪 70 年代，S.A. Cook 发现 NP 问题中最困难的问题具有特殊性质。Cook 证明，如果这类问题中的一个属于 P，则所有其他 NP 问题都属于 P。由此，Cook 引入了 NP 完全的概念，第一次明确提出了“P=NP？”问题。

人们之所以关注 NP 完全问题，是因为在各个领域遇到的大多数自然的难解问题，最终都发现是 NP 完全问题。NP 完全问题类非常丰富，存在于数学、优化、人工智能、生物、物理、经济、工业等各个领域。如果能够解决 P 与 NP 两个问题类之间的关系，则解决了这些问题的算法复杂度问题，具有非常重大的实际意义。

70 年代人们对 NP 完全问题的研究主要是横向发展，也就是以许多不同的计算模型来分析难解问题的本质。已经发现的 NP 完全问题超过千个，涉及几乎所有数学学科的计算问题，如数理逻辑、图论、数论、拓扑、代数、组合优

化、几何、对策论等。因此，我们可以应用多个数学学科的知识以多种不同的手段研究这一问题。例如，在 Smale 提出的本世纪 18 个重大数学未决问题中，他选择了下列源自传统数学的 NP 完全问题作为“P=NP？”问题的代表：给定 Z_2 上关于 n 个变量的 k 个多项式，问是否存在多项式时间的算法判定它们在 Z_2^n 上有公共零点。对多种 NP 完全问题的研究使我们对难解问题有了更深的认识，另一方面也产生了一些预想不到的应用。例如，基于 NP 完全理论，密码学取得了革命性突破，建立了公钥密码体系。

到了 80 年代中，NP 完全问题的研究有了纵向的突破，在许多表面看来并不相关的计算问题之间发现了深刻的刻画关系。这些刻画关系不但解决了几个令人困扰多年的问题，同时也刺激了其它相关领域的发展。其中一个重大的结果是概率可验证明(PCP)对 NP 类的刻画，由此得出了许多组合优化问题近似解的 NP 完全难近似性，从而刺激了近似算法的研究。90 年代，人们又研究了新的计算模型比如量子计算机和命题证明系统。新工具的引入无疑增加了这一问题的内涵。例如，可以问：在量子计算机模型下是否存在类似“P=NP？”的问题；是否具有量子多项式时间算法求解某类 NP 完全问题? 另一个研究热点是参数复杂性理论，将 NP 完全问题的参数区别对待。例如图的顶点覆盖问题，它的参数有图的顶点个数 n 和覆盖子集尺寸 k，而如果固定参数 k，则顶点覆盖问题是多项式时间可解的，但是其运行时间是 k 的指数函数。于是研究 NP=P 问题，可以分解为各个 NP 完全问题的固定参数如何影响其 NP 完全性的问题。

一般认为，“P=NP”是不成立的。如果这一结论正确，那么希望通过研究某个具体的 NP 完全问题解决 P=NP？问题的途径是不可行的。P=NP？问题的解决可能需要全新的数学理论。因此，Smale 将 P=NP？问题称为“计算机科学为数学带来的一个礼物。” 这一问题被 Clay 研究所列为七个千僖问题之一。

既然“P=NP”被认为是不成立的，而现实应用中又存在如此之多的 NP 完全问题，怎样有效求解这些 NP 完全问题变为计算复杂性的又一核心问题。NP 完全问题的计算困难性是对于 Turing 机的确定型算法而言，因而寻找高效算法必须使用新的计算模型。下面介绍几种常用的计算模型，主要是并行算法、随机算法、近似算法与量子算法。

NP 完全问题应用最为广泛的求解算法是各种随机搜索算法。例如，由 J. Holland 发明的遗传算法，是模仿动物基因进化过程设计的优化问题的求解算

法。遗传算法是一种基于随机选择与并行计算的贪心算法。这类算法已被广泛应用于各种问题的求解，但是由于算法的复杂性，其理论分析非常困难，还远未取得实质性进展。随机算法虽然在 NP 完全问题求解方面未取得实质性理论进展，却为很多其他计算问题提供了有效的途径，已经成为一种非常有效的计算手段。

近似算法用于求解优化问题，希望用多项式时间算法给出某个 NP 完全优化问题真正最优值的某个百分比。对于近似算法，NP 完全问题可以分为三类。最容易的一类，例如背包问题，我们可以设计一系列算法在多项式时间内求的任意接近其最优解的近似解。中间的一类，我们可以设计近似算法求的其最优值的某个固定比例 r (0<r<1)。最困难的一类，对于任意的 r (0<r<1)，近似求解其 r 最优值也是 NP 困难的。近似算法的主要目标是对计算问题根据其近似计算的复杂度进行分类。

另一种思路是采取完全不同于 Turing 机的计算模型，例如量子计算。量子计算是借助于量子力学原理设计的一种计算模型，其主要特点是高度并行与随机性。1994 年 P. Shor 证明可以用量子算法在多项式时间内分解大整数。由于大整数分解的困难性是 RSA 密码体制安全性的基础, 这一工作引发了人们关于量子算法的关注。有趣的是，到目前为止，利用量子算法可以实质性提高速度的问题并不多。特别地，量子算法还不能实质性降低求解 NP 完全问题计算复杂度。

当然，计算复杂性学科也还有很多其他的重要问题。例如，我们还不知道若干具有重要应用背景的计算问题的计算复杂性。下面举例说明。

目前，我们还不知道大整数因子分解问题是否属于 P。由于大整数因子分解计算困难性是现在广泛使用的密码 RSA 的安全性基础, 所以研究大整数因子分解的快速算法及其计算复杂度具有重要意义。

两个 n×n 矩阵如果按照通常的方法做乘法, 其计算复杂度大致是 n^3。1969 年 Strassen 提出“快速乘法”算法，其计算复杂度大致为 n^2.807。现在已知的计算复杂度最好的算法的复杂度大致是 n^2.37。人们猜想，矩阵乘法的计算复杂度可以接近 n^2。由于矩阵乘法在各种计算中大量使用，寻找快速有效的矩阵乘法算法有重要的意义。

4、机械化数学

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？

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。分别介绍如下。

(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) 计算数论与现代密码学

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。

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.	吴文俊	男	中国	委员	院士	是	中科院数学院
4.	万哲先	男	中国	委员	院士	是	中科院数学院
5.	陆汝钤	男	中国	委员	院士	是	中科院数学院
6.	张景中	男	中国	委员	院士	是	中科院成都计算机所
7.	林惠民	男	中国	委员	院士	是	中科院软件所
8.	黄民强	男	中国	委员	院士	是	中科院系统所
9.	陈永川	男	中国	委员	院士	是	南开大学
10.	冯克勤	男	中国	委员	教授	否	清华大学
11.	吴　可	男	中国	委员	教授	否	首都师范大学
12.	李克正	男	中国	委员	教授	否	首都师范大学
13.	李　华	男	中国	委员	研究员	否	中科院计算机所
14.	张继平	男	中国	委员	教授	否	北京大学
15.	王小云	女	中国	委员	教授	否	清华大学
16.	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、胡　磊、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	几何代数	研究
6.	刘卓军	男	1958.3		研究员	信息安全	研究
7.	孙笑涛	男	1962.10		研究员	代数几何	研究
8.	李子明	男	1962.6		研究员	符号计算	研究
9.	胡　磊	男	1967.3		研究员	密码学	研究
10.	支丽红	女	1969.6		研究员	混合计算	研究
11.	韩　阳	男	1971.10		研究员	代数表示论	研究

12.	王定康	男	1965.3		研究员	符号计算	研究
13.	闫振亚	男	1974.3		研究员	复杂非线性波	研究
14.	邓映蒲	男	1971.5		研究员	信息安全	研究
15.	冯如勇	男	1978.6		副研究员	符号计算	研究
16.	张志芳	女	1980.10		副研究员	信息安全	研究
17.	袁春明	男	1979.12		副研究员	符号计算	研究
18.	程进三	男	1976.8		副研究员	符号计算	研究
19.	冯秀涛	男	1978.8		所聘副研	信息安全	研究
20.	周　凯	男	1981.9		所聘副研	代数、编码	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.	贾晓红	女	1981.9		助研	计算几何	研究
25.	李　博	男	1982.9		助研	生物数学	研究
26.	陈绍示	男	1983.7		助研	符号计算	研究
27.	李　伟	女	1985.9		助研	微分代数几何	研究
28.	张立先	女	1982.10		项目助研	高档数控	研究
29.	吴天骄	男	1959.9		工程师		技术
30.	周代珍	女	1965.3		秘书		管理
31.	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。

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
4.	胡　磊	百人	2001

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、邓映蒲、冯如勇、张志芳、袁春明、程进三、黄雷、李伟等	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	2016
2.	高小山	中国系统工程学会	副理事长	2010	2014
3.	高小山	中国工业与应用数学会	副理事长	2009	2015
4.	高小山	中国图学学会	常务理事	2010	2014
5.	高小山	中国密码学会密码数学专业委员会	副主任	2010	2014
6.	高小山	ACM SIGSAM Advisory Committee Board	委员	2006	2014
7.	刘卓军	中国数学会计算机数学专业委员会	委员	2012	2016
8.	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
9.	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
10.	刘卓军	中关村品牌协会	常务副会长	2011	2016
11.	李洪波	中国数学会计算机数学专业委员会	副主任	2012	2016
12.	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	2014
13.	李子明	中国数学会计算机数学专业委员会	主任	2011	2016
14.	李子明	中国数学会	理事	2012	2016
15.	李子明	ACM SIGSAM	秘书	2012	2015
16.	王定康	中国数学会计算机数学专业委员会	秘书长	2010	2016

17.	支丽红	ISSAC 指导委员会	主席	2011	2014
18.	支丽红	国际符号与数值混合计算指导委员会	委员	2004	2016
19.	支丽红	2014 国际符号和数值计算会议	主席	2014	2014
20.	邓映蒲	中国密码学会理事会	理事		
21.	邓映蒲	中国数学会计算机数学专业委员会	委员		
22.	邓映蒲	中国电子学会信息论分会	委员		
23.	程进三	SNC 程序委员会	委员	2014	2014
24.	程进三	CASC 程序委员会	委员	2014	2014
25.	程进三	ICMS 程序委员会	委员	2014	2014
26.	程进三	全国计算机数学学术会议程序委员会	副主席	2014	2014
27.	陈绍示	ISSAC2014 程序委员会	委员	2013	2014

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	**《东北数学》**	编委		
7.	李邦河	**《数学季刊》**	编委		

8.	李邦河	**《数学学报》**	编委		
9.	李邦河	**《系统科学与数学》**	编委		
10.	李邦河	**《数学物理学报》**	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	**《系统科学与数学》**	主编		
17.	高小山	**《系统工程理论与实践》**	副主编		
18.	高小山	**《中国科学：数学》**	编委		
19.	高小山	**《计算机辅助设计与图形学学报》**	编委		
20.	高小山	**《中国图象图形学报》**	编委		
21.	高小山	**《中国高校应用数学学报》**	编委		
22.	高小山	**《数学研究与评论》**	编委		
23.	刘卓军	**《 The International System Safety Society》**	**Member**		
24.	刘卓军	**《系统科学与数学》**	编委		
25.	李洪波	**《系统科学与数学》**	编委		
26.	李洪波	**《 Advances in Applied Clifford Algebras》**	编委		
27.	李子明	**《Journal of Symbolic Computation》**	编委		
28.	李子明	**《系统科学与数学》**	副主编		

29.	李子明	《 **Journal of Systems Science and Complexity**》	编委		
30.	支丽红	《**Journal of Symbolic Computation**》	编委		
31.	支丽红	《**Mathematics in Computer Science**》	编委		
32.	支丽红	《**ACM Communications in Computer Algebra**》	编委		
33.	支丽红	《**Theoretical Computer Science**》	特辑编委		
34.	闫振亚	《**Abstract and Applied Analysis**》	编委		
35.	闫振亚	《**Journal of Engineering and Applied Science**》	编委		
36.	闫振亚	《**Bulletin of Mathematical Analysis and Applications**》	编委		
37.	闫振亚	《**International Journal of Birfurcation and Chaos**》	客座编委		
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	导师姓名	硕士生	博士生	博士后
1.	万哲先	杨江帅		
2.	邓映蒲	廖茂东		
3.	支丽红	郝志伟		
4.	王定康	张文哲		
5.	邓映蒲	王　慧		
6.	冯如勇	熊纯文		
7.	韩　阳	张凝鹛		
8.	高小山	荆瑞娟		
9.	高小山	王　杰		
10.	闫振亚	闫方驰		
11.	闫振亚	陈　勇		
12.	袁春明	宓振鹏		
13.	支丽红	杨志红		
14.	刘卓军	李秋萍		
15.	程进三	窦孝杰		
16.	冯秀涛	付士辉		
17.	王定康	白　剑		
18.	李洪波	周　亮		
19.	张志芳	周义满		
20.	李子明	杜　昊		
21.	刘卓军	朱　海		

22.	李洪波	李　璋		
23.	支丽红	姜文嵘		
24.	王定康	鲁　东		
25.	闫振亚	张国强		
26.	韩　阳	郑　策		
27.	张志芳	徐敬可		
28.	邓映蒲	李昊宇		
29.	万哲先		孙志强	
30.	李洪波		李　阁	
31.	高小山		郭建新	
32.	高小山		闵　程	
33.	支丽红		郭庆东	
34.	刘卓军		张晓明	
35.	黄民强，邓映蒲		张　凤	
36.	吴文俊，程进三		金　凯	
37.	刘卓军		黄　冲	
38.	韩　阳		章　超	
39.	高小山		祝　炜	
40.	高小山，冯如勇		李应弘	
41.	吴文俊，王定康		周　洁	
42.	李洪波		刘　越	
43.	李洪波		邵长鹏	
44.	黄民强		胡耿然	
45.	胡　磊		吕　昌	
46.	万哲先，张志芳		王安宇	

47.	刘卓军		王　晗	
48.	黄民强，邓映蒲		黄丹丹	
49.	韩　阳		秦永云	
50.	高小山		黄　章	
51.	高小山		赵明勇	
52.	李洪波		文　勇	
53.	李洪波		董　磊	
54.	李子明		黄　辉	
55.	李子明		张　熠	
56.	刘卓军		王立波	
57.	支丽红		王　础	
58.	闫振亚		温子超	
59.	万哲先，邓映蒲		张　凡	
60.	万哲先		刘仁章	
61.	高小山		黄巧龙	
62.	高小山		齐嘉悦	
63.	高小山		胡又壬	
64.	闫振亚		李　昕	
65.	刘卓军		姜　懋	
66.	邓映蒲		李加宁	
67.	闫振亚			于发军
68.	闫振亚			杨云青
69.	闫振亚			闻小永
70.	王定康			黄　冲

毕业研究生一览表

序号	姓名	学位	导师姓名	毕业时间
1.	于发军	博士后	闫振亚	
2.	闵　程	博士	高小山	
3.	郭建新	博士	高小山	
4.	张晓明	博士	刘卓军	
5.	黄　冲	博士	刘卓军	
6.	李　阁	博士	李洪波	
7.	郭庆东	博士	支丽红	
8.	金　凯	博士	吴文俊，程进三	
9.	孙志强	博士	万哲先	
10.	张　凤	博士	黄民强，邓映蒲	
11.	章　超	博士	韩　阳	

研究生获奖一览表

序号	获奖名称	获奖人员	指导教师
1.	2014 年度国际符号和代数计算会议(ISSAC) 杰出 Poster 奖	黄　辉	李子明
2.	中科院数学院优秀毕业生	郭建新	高小山
3.	国家奖学金	王安宇	万哲先、张志芳
4.	中科院数学院院长奖学金特等奖	王安宇	万哲先、张志芳
5.	中科院数学院院长奖学金优秀奖	胡耿然	黄民强
6.	中科院数学院院长奖学金优秀奖	黄　辉	李子明
7.	中科院数学院院长奖学金优秀奖	李应弘	高小山
8.	中科院数学院院长奖学金优秀奖	吕　昌	胡　磊
9.	中国科学院研究生院三好学生	刘　越	李洪波
10.	中国科学院研究生院三好学生	张　凡	万哲先、邓映蒲
11.	中国科学院研究生院三好学生	赵明勇	高小山
12.	中国科学院研究生院三好学生	温子超	闫振亚
13.	中国科学院研究生院三好学生	吕　昌	胡　磊
14.	中国科学院研究生院三好学生	王安宇	万哲先、张志芳
15.	中国科学院研究生院三好学生	李应弘	高小山

16.	中国科学院研究生院三好学生	王　础	支丽红

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

国家基金委创新群体项目 1 项,

国家“973”计划项目 1 项,

国家“973”计划项目子课题 4 项,

国家自然科学基金重点项目 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 6 项,

国家科技支撑计划项目 1 项。

（二）按研究方向或研究单元，分别介绍实验室本年度有代表性的研究工作进展。

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，这三个主要研究方向取得进展，共发表和接收论文 46 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）

差分方程稀疏结式理论与高效算法：

结式给出超定方程组有公共解的充分必要条件。它在多项式方程系统求解的复杂度研究中被广泛应用，是代数几何与符号计算的基本概念和消去理论的主要计算工具之一。考虑到实际当中遇到的多项式大多是稀疏的。著名学者

Gelfand 等于上世纪 90 年代提出稀疏结式这一概念。它构成了稀疏消去理论的基石。

我们对于 Laurent 差分 essential 系统建立了稀疏差分结式理论。首先，我们定义了 Laurent 差分 essential 系统并给出了一个系统是差分 essential 的判别法则，并给出了稀疏差分结式的矩阵表示。其次，对于 Laurent 差分 essential 系统定义了稀疏差分结式并给出了其基本性质，特别是这些结式的次数与阶数的上界。最后，基于阶数和次数界给出了计算 Laurent 差分 essential 系统的稀疏微分结式的单指数算法。相关论文发表在符号计算杂志主要杂志《Journal of Symbolic Computation》。

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。一个自然的问题是，对于差分 Toric 簇与差分二项式理想，其定义与性质是怎样的？我们在去年工作的基础上，给出了 Laurent 差分二项式理想是否完备的判别方法，并给出了相应的算法。进一步的，我们给出了计算 Laurent 差分二项式理想完备闭包的算法，同时给出了基于 Z[x]模上运算的素分解算法。对于差分二项式理想，我们证明了其完备闭包是也是二项式理想，并且给出了其素分解的分解算法（在非二项式情形，这一分解算法并不存在）。

Telescoper：

我们给出了多变元超几何函数存在并行 telescoper 的充要条件并发展了相应的算法用以判定其存在性以及当其存在时将其求出，同时还将所得结果应用于带参数微分 Galois 理论中的计算问题，还将超指数情形的结果推广到代数函

数情形。我们确定了关于微分算子，shift 算子以及 q-shift 算子相容的有理函数的结构，解决了混合超几何项的 Telescoper 算子的存在性，并且利用这些结果给出了微分算子，shift 算子以及 q-shift 算子情形的 Zeilberger 算法的终止性判定条件，彻底解决了 Zeilberger 算法关于双变元混合超几何项的终止性问题。

我们将 Apagoudu-Zeilberger 方法从一阶线性微分-差分情形推广到了高阶情形, 提出了高阶情形的正则函数概念, 并证明对于这类函数, 经典的 Telescoper 算子总是存在的。我们提出了含参微分 1-形式的 Parallel Telescoper 算子的概念, 证明了这类算子对系数为 D-finite 函数的闭形式一定存在，并给出了超指数情形计算这类算子的算法。

我们从理论上解决了双变元有理函数的可求和问题，即判定给定有理函数 f(x, y) 是否可以写成

$$f(x, y) = g(x+1, y) – g(x, y) + h(x, y+1) – h(x,y),$$

其中 g, h 也为双变元有理函数。这是将经典的 Gosper 算法从单变元超几何情形向多元情形推广的第一步。基于该工作，近期南开大学候庆虎教授和他的学生提出了判定可求和性的高效算法。

(1.2) 符号与几何计算（李邦河、李洪波、韩阳、王定康、黄雷、贾晓红）

不变除法：

如果输入的多项式在一般线性群下不变，如何定义有效的除法算法使得结果依然不变，是几何计算的基本问题之一。我们提出第一个基于标准括号多项式的不变除法，并用来证明基于坐标的不变理想就是基于括号的不变理想。

不同代数表示和代数处理下的同一问题的符号计算结果的等价性问题，是符号计算的基础问题。我们求出符号个数变元的四元数变元多项式生成理想的消去基底 i,j,k 后的理想，找到一组简单的生成元，完全解决了不依赖于基底的四元数变元多项式符号处理的完全性问题。

Groebner 基计算：

我们研究了布尔多项式环中的多项式理想，利用线性代数和矩阵运算的相关技术来实现Groebner基的高效计算。我们还研究了并提出了局部环上的多项式理想的签名Groebner基算法，并证明了算法的正确性和终止性。

Hilbert 第 15 问题：

在 Hilbert 15 问题上取得某些进展。 例如对 Schubert 的一个重要公式给出了严格的证明， 并将其从三维推进到任意维。 在美国的 University of Minnesota 和 University of Michigan 作过 报告。

线几何的代数描述：

众所周知，Pluecker 坐标提供了三维射影空间中的直线的 6 维表示，使得三维保定向射影变换诱导了 Pluecker 坐标空间中的特殊正交变换。反过来，为了从直线构造点和平面的射影变换，需要将 Pluecker 坐标空间中的特殊正交变换转换成三维保定向射影变换。我们建立了这一转换的显示简洁表达式，并得到了一系列重要的特殊变换之间的转换，完全解决了这一逆向转换问题。

两曲面交线几何变化的检测：

两曲面交线几何变化的检测是比两曲面的碰撞检测更为复杂的问题。该问题虽尚未真正出现在实际工业应用中，但未来机器人应用领域中有比曲面碰撞检测更加深入的前景。我们通过符号计算方法检测两二次曲面构成的曲面簇相应的 Jordan 标准型的变化，将时间轴划分为交线拓扑恒定的区域段，在各段分别进行交线几何的符号计算。我们已将该算法应用于二次曲面复合体的碰撞检测中，文章在 2014 年新加坡举办的 Geometric Modeling and Processing 国际会议上做了大会报告, 并已被推荐发表在计算机图形学的期刊 Graphics Model 上。

Dupin Cyclide 的 mu 基：

Dupin Cyclide 是新近活跃在建筑几何领域的经典代数曲面。我们通过研究

伴随 Dupin Cyclide 的动平面和动球面, 建立了 Dupin Cyclide 的 mu 基系列理论。该理论直接建立了曲面隐式方程与参数表达的内蕴联系，并且给出 Dupin Cyclide 上点的简易逆公式表达。

生成高质量三角网格的新方法：

高质量三角形网格的生成方法是图形学以及数字几何处理领域的一个研究热点。现有的曲面网格生成研究主要针对如何提高三角形的质量，而忽略了网格顶点的整体分部。在许多领域的应用中，都要求采样点的分布既满足随机性又满足均匀性，这些性质统称为蓝噪声性质，蓝噪声性质和人类的视觉感知系统密切相关，在图像合成，真实感绘制，机器人路径规划等领域有着大量应用。我们研究了在曲面网格上进行蓝噪声优化采样，并利用优化的采样点生成高质量三角网格的方法，以解决现有的网格生成方法生成的网格顶点分布差、不适于物理模拟、且不易控制最小角度的缺点。相关成果已经有两篇论文发表在几何处理的最国际顶级会议 EurographicsSymposiumon Geometry Processing（SGP）（推荐到图形学顶级期刊 Computer Graphics Forum 上）及几何建模权威会议 Shape Modeling International (SMI) Conference（推荐到图形学重要期刊 Computers & Graphics 上），后者还获得了 2014 年 SMI 国际会议的最佳论文提名奖（该会议评出最佳论文一名，最佳论文提名奖两名）。

(1.3) 多项式可信计算（支丽红、程进三）

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

实代数簇的凸闭包的径向锥是有向的，则其相应对偶代数簇的定义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。

我们研究了多项式系统孤立奇异根的可信验证问题。利用区间验证方法和宽度为 1 的特殊情形下重结构的参数化表示，我们提出了一种计算近似奇异根可信误差界的新算法，其可以验证一个带有微小扰动的多项式系统，在误差界内有一个宽度为 1 的孤立奇异根. 对于一般的孤立奇异根，我们提出一种带光滑参数 deflation 技术，并且基于这种技术，我们将验证宽度为 1 的孤立奇异根的算法推广到了一般情形. 数值实验表明，算法对于带有近似系数的多项式系统和复的孤立奇异根同样适用。文章发表于 SIAM Journal of Numerical Analysis。

我们给出了空间曲线一般位置的判定定理，基于这个定理给出了空间曲线拓扑的分析算法，并给出了其复杂度分析。我们还给出了平面代数曲线零阶 Betti 数的一个计算公式与一个相关定理。

2. 编码与密码

(2.1) 计算数论（邓映蒲）

素数判定是计算数论的重要问题，一直就受到数学家和计算机科学家的注意和研究。早期 Gauss、Fermat 等人就研究过它。在著名的公钥密码体制 RSA 中就使用了大素数。为了确保这些数的确是素数，就需要使用素数判定算法。故素数判定方法对于 RSA 公钥密码的安全性有重要的影响。目前素数判定方法有确定性算法以及概率性算法。确定性算法由于其计算量过大而不实用。在概率性算法中，比较简单实用而快速的是著名的 Miller-Rabin 算法。它基于强

伪素数的性质。如果我们知道以前几个素数为基的最小强伪素数的精确值，则判定小于这个精确值的数是否为素数的方法可以由概率性算法变为确定性算法，因为只需要用前几个素数作基，看它是否通过了 Miller-Rabin 判别法。通过前 8 个素数为基的最小强伪素数的精确值早在 1993 年便已经知道。当时 Jaeschke 还给出了以前9、10、11 个素数为基的强伪素数的上界。而后 Zhenxiang Zhang 几次改进了上界并最后猜测了这些强伪素数的精确值。我们证明了 Zhenxiang Zhang 的猜测，给出了通过前 9、10、11 个素数为基的最小强伪素数的精确值。论文发表在计算数学的顶级杂志《Mathematics of Computation 》上。

有理数域或整数环中的覆盖系是Erdös提出的，在Exact覆盖系方面有个经典的结果，即覆盖系的模数必须有重复的，这一结果能否推广到代数数域上是个自然的问题。Illinois的 S. Kim在2012年证明了这一结果在某些二次域中仍然成立。我们彻底解决了这一问题，即我们证明了这一结果对任意的代数数域都成立。论文发表在《The Quarterly Journal of Mathematics（Oxford）》(2014年3月)上。

(2.2) 密码攻击（潘彦斌、冯秀涛）

攻破 Selvi-Vivek-Rangan 签名方案：

Selvi-Vivek-Rangan 在 2012 年的澳大利亚密码会议 ACISP2012 发表了第一个基于身份的确定性签名方案，并给出了安全性证明。后来有人发现其安全性证明是错的，并攻破了它。我们独立地提出了另一种攻击方法，可以利用公钥伪造任意签名，也攻破了这一签名方案，论文发表在今年的澳大利亚密码会议 ACISP2014 上。

CAESAR 竞赛：

CAESAR 竞赛是一个由日本发起的面向全球征集认证密码的竞赛。我们围绕 CAESAR 竞赛中的基于流密码算法的认证算法展开安全性，破译了 Sablier、

PANDA-s、FASER128 和 FASER256 等一系列密码算法，其中针对 PANDA-s 和 FASER128/FASER256 的工作导致这两个算法被 CAESAR 竞赛淘汰。我们针对 FASER128/256 的工作得到设计者的高度评价，他们认为我们的工作是”drag it out the back, and shoot it in the head!”。

公钥与签名：

首先，我们给出了利用 p 范数 SVP oracle 能解决的子集和问题的密度上界，填补了之前从 2 范数到无穷范数之间的空白，更好地刻画了 p 范数 SVP 的复杂性，并发现了当 p>=3 时，利用 p 范数 SVP oracle 就能解决密度为 1 的子集和问题。相关论文发表在 PKC2014 上。PKC 是公钥领域最顶级的会议之一。其次，我们分析了 2012 年澳密会上提出的 Selvi-Vivek-Rangan 签名体制。该体制号称是第一个确定性的基于身份的签名体制。我们指出可以在多项式时间内伪造该体制的签名，相关文章被 ACISP2014 接收。我们还完成了对 NTRUSign 利用最近平面算法进行签名时的攻击，完成了低维循环格最短向量系数在格基下的刻画，以及发现了随机 HNF 的若干统计性质，完成了对 2014 年亚密会上新提出的 HS 签名体制的攻击。

(2.3) 编码（刘卓军、张志芳、周凯）

在进行复杂数据的网络分析过程中，我们提出了 I-ANP 方法，即逆向网络分析方法，这和传统的层次分析形成反向的互补方式，该方法在对多属性数据类型分析中，有助于自动提炼出二级指标。在 DNS 异常流量检测及抗攻击理论和方法研究中，提出 IP 威胁度的概念，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。

我们构造了一大类兼具多种良好密码学性质的 MAI 函数，部分工作成果发表在信息论领域的国际顶级会议“2014 IEEE International Symposium on Information Theory”（ISIT 2014）

我们完成了 locality (r, delta)_c 的一般性定义，极小距离上界，以及最优码的构造。我们的定义从组合的角度给出了多节点失效时仍然保证局部 r-修复特性的新方法，能够在很大程度上提升码的极小距离。我们建立了局部可修复编码的极小距离和修复集合组合结构之间的一般联系，得到了计算极小距离上界的一般性框架,，对相当大参数范围内（满足实用需求）的局部修复码确定了极小距离的上界，并在二元扩域上给出了最优的码的构造。

以万先生为代表所做的有限几何方面的工作具有强烈的典型群的研究背景。万先生的著作《Geometry of Classical Groups over Finite Fields》更是为这方面的研究奠定了坚实的基础。这些工作在区组设计，认证码的研究等方面皆有广泛的应用。我们之前利用有限域上的酉群构造了一类具有良好对称性的强正则图，现在我们对其子图进行了研究，并研究两者之间的关系问题。相应的我们继续研究了奇特征的有限域上的正交群构造的具有良好对称性的强正则图及其子图。

伪随机序列的应用领域非常广泛，它在测距系统，扩频通信，多终端系统辨识，码分多址通信，全球定位系统，软件测试，雷达导航和密码学中都有应用，尤其是寻找具有良好性质的序列有很大的需求。我们对有限分裂类型的谐振代码字典（一类具有好的相关性的序列）给出了一种封闭的表示形式，而对于有限非分裂类型的谐振代码字典的计算给出了完全的算法，该算法具有很好的可操作性。

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）

数控机床中的非线性误差估计与控制：

建立了 5 轴机床的典型刀具空间的 Hausdorff 距离由机床的 5 个独立控制参

数约束的不等式关系，从理论上为估计与控制由坐标变换引起的非线性误差建立了严格基础。

数控数据距离可控的二次 B 样条曲线拟合：

对于数控中给出的 G01 代码，其插补问题是数控加工中的一个基本问题。如果针对 G01 代码表示的折线段直接加工，那么加工的质量会比较差并且加工速度较为缓慢。我们考虑将拟合曲线段与数据折线段之间的 Hausdorff 距离作为拟合约束，从而得到符合距离控制的二次 B 样条拟合曲线。我们进一步完善了所设计的二次时间样条的拟合算法，给出了严格满足距离误差精度以及速度和加速度约束的时间样条拟合曲线，该曲线具有最短加工时间。

五轴数控加工过程出现的奇异问题消除：

对 S 件五轴数控加工过程出现的奇异问题进行分析，提出通过改变工件在机床坐标系中的姿态，消除奇异问题。对所提方法在沈阳计算所的蓝天数控系统和数控机床上进行了加工验证，取得了预期的效果。

(3.2) 酶动力学（李邦河、李博）

我们继续深化研究了酶动力学中的数学问题，同时进行了网络科学方面的研究，在 The 21st International Symposium on Mathematical Theory of Networks and Systems 国际会议、European Meeting of the Econometric Society (2014) 、Midwest Economics Association 2014 Annual Meeting 三个国际会议上做了小组报告。

(3.3) 非线性物理方程的特殊解（闫振亚）

我们提出空间调控的复数域中非线性色散的 GP(m,n)模型，对于不同的非线性色散和相互作用的情况，分析了该模型的包络 compacton 解等，该结果在《Stud. Appl. Math.》发表。我们研究了带源的一维 GP 方程的物质波结构问题，通过考

虑它的平凡相位解和非平凡相位解， 在不同类型的外势条件下，研究了该模型的波进展，给出了一些有意义的周期波解结构等，并且分析了物质波的传播进程等，该结果发表在《J. Math. Anal. Appl.》。我们还研究了 Bose-Einstein 凝聚态中(2+1)-维时空调制的耦合 GP 方程组的怪波解问题, 发现在非线性三种相互作用下（即吸引、排斥和混合），该系统都拥有怪波解结构，并且分析了参数对怪波结构的影响。

（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、素数判定与覆盖系（邓映蒲）。

（1） 计算数论——素数判定问题：

素数判定是计算数论的重要问题，一直就受到数学家和计算机科学家的注意和研究。早期 Gauss、Fermat 等人就研究过它。在著名的公钥密码体制 RSA 中就使用了大素数。为了确保这些数的确是素数，就需要使用素数判定算法。故素数判定方法对于 RSA 公钥密码的安全性有重要的影响。目前素数判定方法有确定性算法以及概率性算法。确定性算法由于其计算量过大而不实用。在概率性算法中，比较简单实用而快速的是著名的 Miller-Rabin 算法。它基于强伪素数的性质。如果我们知道以前几个素数为基的最小强伪素数的精确值，则判定小于这个精确值的数是否为素数的方法可以由概率性算法变为确定性算法，因为只需要用前几个素数作基，看它是否通过了 Miller-Rabin 判别法。通过前 8 个素数为基的最小强伪素数的精确值早在 1993 年便已经知道。当时 Jaeschke 还给出了以前 9、10、11 个素数为基的强伪素数的上界。而后 Zhenxiang Zhang 几次改进了上界并最后猜测了这些强伪素数的精确值。我们证明了 Zhenxiang Zhang 的猜测，即给出了通过前 9、10、11 个素数为基的最小强伪素数的精确值。我们的论文发表在计算数学的顶级杂志《Mathematics of Computation 》上。

（2）组合数论：

有理数域或整数环中的覆盖系是Erdös提出的，在Exact覆盖系方面有个经典的结果，即覆盖系的模数必须有重复的，这一结果能否推广到代数数域上是个自然的问题。Illinois的 S.Kim在2012年证明了这一结果在某些二次域中仍然成立。我们彻底解决了这一问题，即我们证明了这一结果对任意的代数数域都成立。我们所用的方法完全不同于S.Kim的方法。Kim的方法主要是用生成函数的方法，我们的方法是代数性的，利用了理想的素理想唯一分解定理和中国剩余定理以及格理论中的结果。我们的论文发表在牛津大学的数学杂志《The Quarterly Journal of Mathematics（Oxford）》(2014年3月)上。

代表性成果 2、计算几何新方法（贾晓红）。

（1）伴随 Dupin Cyclide 的 mu 基理论的建立：

Mu 基理论源于动曲线与动曲面理论，是近年来用以研究曲线和曲面性质的新的代数工具，因其良好的代数与几何性质，成为联结曲线和曲面的参数表示与隐式表示之间的桥梁，是 Syzygy 模理论在计算机辅助几何设计和几何建模领域的新应用。在过去的二十年中，平面有理曲线、空间有理曲线及有理直纹面的 mu 基理论及算法已趋于完善，而因一般有理曲面的 Sygyzy 模在齐次参数表示下通常非自由模，其 mu 基概念、理论及算法都缺乏深入的研究。

我们研究了新近频繁出现在建筑几何中的曲面 Cyclide 的 mu 基理论，解答了建筑几何与几何建模中迫切需要但无具体结论的几个关于 cyclide 的问题，包括：1、cyclide 的点逆公式，即对于 cyclide 曲面上任意一点，快速准确写出该点对应的参数对；2、如何从任意姿态、任意位置的某 cyclide 的隐式方程中快速提取其位置、姿态及形状参数信息；3、伴随 cyclide 阿动平面与动球面之间的关系，以及它们与 cyclide 之间的几何联系；4、如何从任意姿态、任意位置的某 cyclide

的隐式方程出发直接写出其 mu 基。

不同于以往寻找 mu 基的手段（从参数方程出发），我们首次从隐式方程（任意位置、姿态及形状参数）出发给出 cyclide 的 mu 基。我们的成果将大大简化建筑几何及图形学中某些涉及 cyclide 的算法，是 Syzygy 模理论在工业环境中的新应用，也是我们过去数年在 mu 基理论方向的新进展。该成果发表于计算机辅助几何设计的最权威期刊 Computer Aided Geometric Design 上。

（2）在空间中连续运动及变形的二次曲面的连续碰撞检测（及交线形态变化）的符号计算方法：

碰撞检测是计算机辅助制造、仿真学、机器人学、计算机游戏等多领域的重要问题。由于真实世界的物体表面形态过于复杂，通常人们用简单包围盒逼近真实物体，从而将碰撞检测简化到包围盒上。低次代数曲面是包围盒的首选。

我们研究了在空间中连续运动及变形的两二次曲面的交线形态变化的符号计算方法，该问题比单纯的碰撞检测（检测交线由实向虚或由虚向实）更加深刻。区别于传统碰撞检测算法的是，我们提供的是符号计算方法，一次性计算出碰撞（或交线形态变化）的所有时刻，不需经过帧采样的数值手段，从而不会遗漏碰撞关键帧，检测的可靠性大大提高。

我们的成果也是首个通过纯代数手段研究交线形态变化的算法。该成果发表于符号计算 的权威期刊 Journal of Symbolic Computation 上。我们也已将该成果应用于计算机游戏及机器人中，成果发表于计算机图形学的权威国际会议 Geometric Modeling and Processing 2014 上。

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	141	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	45	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	24	李洪波
5.	国家基金委创新群体项目	数学机械化及其在信息领域的应用	2012	2014	600	200	高小山
6.	“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	6	刘卓军
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	2013	2014	51	51	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	2013	2014	31.5	31.5	李子明
9.	国家数学交叉中心	信息安全和密码体系	2013	2014	31.5	31.5	邓映蒲
10.	国家自然科学基金重点项目	基于符号-数值混合计算的误差可控算法及其应用	2011	2014	260	78	支丽红

11.	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
12.	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
13.	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	0	王定康
14.	国家自然科学基金面上项目	素数判定与整数分解	2015	2018	60	27	邓映蒲
15.	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	29.25	程进三
16.	国家自然科学青年基金	微分差分多项式系统高效消元算法研究	2012	2014	22	0	袁春明
17.	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	8.8	潘彦斌
18.	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	8.8	贾晓红
19.	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
20.	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	13.2	李博
21.	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	13.2	李伟
22.	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	30	刘卓军

23.	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	19	刘卓军
24.	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	9	刘卓军
25.	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
26.	中国科学院项目	中国科学院青年创新促进会	2011	2014	40	10	张志芳
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
合计	---	---	---	---		805.05	---

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	2014	5 万欧元	0	支丽红
合计	---	---	---	---	---		0	---

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.	Improved Abramov-Petkovsek's Reduction and Creative Telescoping for Hypergeometric Terms	ISSAC 2014 杰出 Poster 奖		陈绍示、黄辉、李子明
2.	Efficient Maximal Possion Disk Sampling and Remeshing on Surfaces	SMI2014 Honorable Mention Award		贾晓红 3/4
3.		中国科学院“卢嘉锡奖青年科技奖”		袁春明
4.		第七届“陈景润未来之星”		陈绍示
5.	Zeilberger 算法的终止性，效率及其推广	2014 年度数学院突出科研成果		陈绍示、冯如勇、李子明
6.	酶动力学中的拟稳态定律及参数估计	2014 年度数学院突出科研成果		李博、李邦河
7.		2014 年度系统所关肇直奖		贾晓红

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.	On the Summability of Bivariate Rational Functions	Journal of Algebra, 409(2):320–343, 2014	Shaoshi Chen, Michael F. Singer	Shaoshi Chen	
2.	On the Existence of Telescopers for Mixed Hypergeometric Terms	Journal of Symbolic Computation. 68:1-26, 2015	Shaoshi Chen, Frederic Chyzak, Guofeng Fu, Ruyong Feng, Ziming Li	Shaoshi Chen	
3.	Parallel Telescoping and Parameterized Picard-Vessiot Theory	In: Proc. of ISSAC 2014: Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation, New York, ACM Press. pp. 99--106	Shaoshi Chen, Ruyong Feng, Ziming Li, Michael F. Singer	Shaoshi Chen	
4.	A Generalized Apagodu-Zeilberger Algorithm	In: Proc. of ISSAC 2014: Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation, New York, ACM Press. pp. 107--114	Shaoshi Chen, Manuel Kauers, Christoph Koutschan	Shaoshi Chen	
5.	Multiplicity Preserving Triangular Set Decomposition of Two Polynomials	Journal of Systems Science and Complexity. issue 6,2014	Jin-San Cheng, Xiao-Shan Gao	Jin-San Cheng	
6.	Isotopic epsilon-meshing of real algebraic space curves	SNC 2014: 118-127	Kai Jin, Jin-San Cheng.	Jin-San Cheng	
7.	Finding a Deterministic Generic Position for an Algebraic Space Curve	CASC 2014: 74-84	Jin-San Cheng, Kai Jin	Jin-San Cheng	
8.	Exact covering systems in number fields	The Quarterly Journal of Mathematics,Vol.65 No1, 211-223,2014	Yupeng Jiang, Yingpu Deng	Yingpu Deng	

9.	Strong pseudoprimes to the first eight prime bases	Mathematics of Computation, Vol.83 No290, 2915-2924,2014	Yupeng Jiang, Yingpu Deng	Yingpu Deng	
10.	A new attack against the Selvi-Vivek-Rangan deterministic identity based signature scheme from ACISP 2012	ACISP 2014, Lecture Notes in Computer Science Vol.8544,pp.148-161,2014	Yanbin Pan, Yingpu Deng	Yanbin Pan	
11.	Sparse Difference Resultant	Journal of Symbolic Computation, 2014	W. Li, C.M. Yuan, X.S. Gao	X.S.Gao	
12.	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	
13.	Tractable Algorithm for Robust Time-Optimal Trajectory Planning of Robotic Manipulators under Confined Torque	International Journal of Computers, Communications & Control, 2014	Q. Zhang, S.R.Li J.X. Guo, X.S. Gao	X.S.Gao	
14.	Iso-scallop Tool-path Generation of 5-axis CNC Machining for Cyclide Patches	Journal of Engineering Manufacture,2014	C.Min, X.S. Gao,	X.S.Gao	
15.	Recollements and Hochschild theory	Journal of Algebra 397 (2014), 535-547	Y. Han	Y. Han	
16.	Role of Moving Planes and Moving Spheres of Cyclides	Computer Aided Geometric Design,31,148-183,2014	X. Jia	X. Jia	
17.	Blue-Noise Remeshing with Farthest Point Optimization	Computer Graphics Forum, 32(5),167-176,2014	D.M. Yan, J. Guo, X. Jia, X.P. Zhang, Peter Wonka	D.M. Yan	
18.	Computing Perspective Projections in 3-Dimensions Using Rotors in the Homogeneous and Conformal Models of Clifford Algebra	Advances in Applied Clifford Algebras,24,465-491,2014	R. Goldman, S. Mann, X. Jia	S. Mann	

19.	Continuous Collision Detection for Composite Quadric Models	Graphics Models,76,566-579,2014	Y.K. Choi, W.Wang, B.Mourrain, C. Tu, X. Jia, F.Sun	Y.K. Choi	
20.	Efficient Maximal Possion Disk Sampling and Remeshing on Surfaces	Computer & Graphics,46,72-79,2015	J. Guo, D. Yan, X. Jia, X. Zhang	D. Yan	
21.	Rademacher fuction, Jacobi symbols, quantum and classical invariants of lens spaces	Gu Chaohao memory Volume(Frontiers in Differential Geometry, Partial Differential Equations and Mathematical Physics)，169-188,World Scientific,2014	Banghe Li, Tianjun Li	Banghe Li	
22.	Reduction among Bracket Polynomials	In: Proc. of ISSAC 2014: Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation, New York, ACM Press. pp. 304--311	Hongbo Li, Changpeng Shao, Lei Huang, Yue Liu	Hongbo Li	
23.	Estimation and Control of the Geometric Error in a Linear Interpolator with Parabola Blending	Proceedings of the ASME International Mechanical Engineering Congress and Exposition 2013. IMECE2013-62877, V02AT02A084	Hongbo Li	Hongbo Li	
24.	Difference Chow Form	Journal of Algebra, 428 (2015): 67-90	Wei Li, Ying-Hong Li	Wei Li	
25.	微分周形式与稀疏微分结式	中国科学：数学,44(3),211-220,2014	Wei Li	Wei Li	

26.	Constructing Boolean Functions With Potentially Optimal Algebraic Immunity Based on Additive Decompositions of Finite Fields	2014 IEEE International Symposium on Information Theory,2014	Baofeng Wu, Qingfang Jin, Zhuojun Liu, Dongdai Lin	Baofeng Wu	
27.	A Note on Two Classes of Boolean Functions with Optimal Algebraic Immunity	J Syst Sci Complex (2014) 27: 785–794	Baofeng Wu, Zhuojun Liu, Qingfang Jin, Xiaoming Zhang	Baofeng Wu	
28.	Constructing 2m-Variable Boolean Functions with Optimal Algebraic Immuntity Based on Polar Decomposition of F22m	International Journal of Foundations of Computer Science, 25(5), 537–551, 2014	Jia Zheng, Baofeng Wu, Yufu Chen, Zhuojun Liu	Baofeng Wu	
29.	A new proof to the complexity of the dual basis of a type-I optimal normal basis over finite fields	Journal of University of Chinese Academy of Sciences,31(5),586-589,2014	Baofeng Wu, Kai Zhou, Zhuojun Liu	Baofeng Wu	
30.	基于模糊理论的消费品安全风险评估方法	数学的实践与认知,44(1),2014	于彭, 刘卓军, 张永光	刘卓军	
31.	用 BHTA 方法研究糖调节与中医体质的关联关系	数学的实践与认知,44,2014	刘卓军, 黄冲, 张永光	黄冲	
32.	Solving Random Subset Sum Problem by lp -norm SVP Oracle	Public-Key Cryptography – PKC 2014, LNCS 8383,399-410	Gengran Hu, Yanbin Pan, Feng Zhang	Yanbin Pan	
33.	A Method to Determine if Two Parametric Polynomial Systems Are Equal	LNAI,56(6),537-544,2014	Jie Zhou, D.K. Wang	D.K. Wang	
34.	On Implementing the Symbolic Preprocessing Function over Boolean Polynomial Rings in Groebner Basis Algorithms Using Linear Algebra	Journal of Systems Science and Complexity,2014	Y. Sun, Zhenyu Huang, Dongdai Lin D.K. Wang	Y. Sun	

35.	Two-dimensional vector rogue-wave excitations and controlling parameters in the two-component Gross-Pitaevskii equations with varying potentials	Nonlinear Dynmics (2014, online, (DOI) 10.1007/s11071-014-1829-8)	Zhenya Yan	Zhenya Yan	
36.	Localized analytical solutions and parameters analysis in the nonlinear dispersive Gross-Pitaevskii mean-field GP(m, n) model with space-modulated nonlinearity and potential	Stud. Appl. Math. 132,266-284,2014	Zhenya Yan	Zhenya Yan	
37.	Parameters controlling matter waves in the one-dimensional generalized Gross-Pitaevskii equation with the varying potential and source	J. Math. Anal. Appl. 423,1370-1399,2015	Zhenya Yan	Zhenya Yan	
38.	Matrix formulae of differential resultant for first order generic ordinary differential polynomials	Computer Mathematic, 479-503, 2014	Z.Y. Zhang , C.M. Yuan, X.S. Gao	C.M. Yuan	
39.	Repair Locality With Multiple Erasure Tolerance	IEEE Transactions on Information Theory,60(11),6979-6987 ,2014	Anyu Wang, Zhifang Zhang	Zhifang Zhang	
40.	Repair locality from a combinatorial perspective	Proc. IEEE Int. Symp. Inf. Theory (ISIT),2014,1972-1976.	Anyu Wang, Zhifang Zhang	Zhifang Zhang	
41.	Verified Error Bounds for Isolated Singular Solutions of Polynomial Systems	SIAM J. NUMER. ANAL.52(4),1623-1640, 2014	Nan Li, Lihong Zhi	Lihong Zhi	
42.	Optimizing a linear function over a noncompact real algebraic variety	SNC 2014: 39-40	Feng Guo, Chu Wang, Lihong Zhi	Lihong Zhi	

43.	Symbolic-numeric algorithms for computing validated results	In: Proc. of ISSAC 2014: Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation, New York, ACM Press.	Lihong Zhi	Lihong Zhi	
44.	A Certificate for Semidefinite Relaxations in Computing Positive-Dimensional Real Radical Ideals	Journal of Symbolic Computation, 2015	Yue Ma, Chu Wang , Lihong Zhi	Lihong Zhi	
45.	Semidefinite Representations of Non-compact Convex Sets	SIAM J. OPTIM,2015	Feng Guo, Chu Wang, Lihong Zhi	Lihong Zhi	
46.	On the Construction of Finite Oscillator Dictionary	Communications in Algebra, 42(8),2427-3437,2014	Rongquan Feng, Zhenhua Gu, Zilong Wang, Hongfeng Wu, Kai Zhou	Hongfeng Wu	
47.	Subconstituents of unitary graphs over finite fields	Linear and Multilinear Algebra, 62(7),925-937,2014	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	Computer Mathematics	Ruyong Feng, Wen-Shin Lee, Yosuke Sato	Springer	2014.5

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.	基于插补精度和加速度限制的变插补周期曲插补方法	ZL201210369252.2	授权	张立先，李洪波，高小山
2.	拐角多周期恒加加速度过渡的 S 曲线加加减速直线插补方法	ZL201210287472.0	授权	张立先，李洪波，高小山

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.	第五届国际符号和数值计算会议（2014 International Conference on Symbolic-Numeric Computation）	国际	中科院数学院	支丽红	2014.7.28-31	65
2.	第四届计算机辅助制造、工程与数控中的数学与算法国际会议(4rd 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	2014.10.23-25	60
3.	第六届全国计算机数学学术会议（CM2014）	国内	中科院数学院	周巢尘	2014.10.31-11.3	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.	A Generalized Apagodu-Zeilberger Algorithm	陈绍示	The 39th International Symposium on Symbolic and Algebraic Computation(ISSAC2014)	日本	2014.07
2.	Proof of the Wilf-Zeilberger Conjecture	陈绍示	重庆大学第一届组合数学及其应用会议	重庆	2014.10
3.	Desingularization of linear difference operators	陈绍示	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11

4.	Computing the topology of algebraic space curves	程进三	International Short-School/Conference on Affine Algebraic Geometry & the Jacobian Conjecture	天津	2014.07
5.	Isotopic epsilon-meshing of real algebraic space curves	程进三	Symbolic and Numeric Computation（SNC2014）	上海	2014.07
6.	Finding a deterministic generic position for an algebraic space curve	程进三	全国工业与应用数学学术年会	昆明	2014.08
7.	Finding a deterministic generic position for an algebraic space curve	程进三	Computer Algebra in Scientific Computing（CASC2014）	波兰	2014.09
8.	Finding a deterministic generic position for an algebraic space curve	程进三	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
9.	New results on nonexistence of generalized bent functions	邓映蒲	第六届有限域及其应用国际研讨会	北京	2014.06
10.	Generalized bent functions	邓映蒲	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
11.	二项式系数的和与整数分解（邀请报告）	邓映蒲	2014 年首都师范大学信息安全会议	北京	2014.12
12.	Hrushovski's Algorithm for Computing Galois Groups of Linear Di erential Equations	冯如勇	American Mathematical Society Central Section Meeting	美国	2014.04
13.	Parallel Telescoping for Hypexponential and Algebraic Functions	冯如勇	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
14.	Cryptanalysis on the Authenticated Cipher Sablier	冯秀涛	International Conference on Network and Systems Security	西安	2014.10
15.	CAESAR 竞赛认证密码的安全性分析	冯秀涛	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
16.	Binomial Difference Ideal and Toric Difference Variety	高小山	The 20th Application of Computer Algebra	美国	2014.07
17.	Efficient and Robust Time-Optimal CNC Interpolation under Dynamic Constraints（邀请报告）	高小山	4th International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control	北京	2014.10

18.	Hochschild homology dimension conjecture: 1 decade（邀请报告）	韩阳	代数与表示论会议	北京	2014.06
19.	Proper smooth local dg algebras are trivial & When is a simple module self-compact? （邀请报告）	韩阳	代数表示论与相关课题全国高级研讨会	乌鲁木齐	2014.07
20.	Brauer-Thrall type theorems for derived category	韩阳	The 16th International Conference on Representations of Algebras	三亚	2014.08
21.	Reduction among Bracket Polynomials	黄雷	The 39th International Symposium on Symbolic and Algebraic Computation(ISSAC2014)	日本	2014.07
22.	四元数未定元多项式的 Groebner 基系统	黄雷	中国工业与应用数学学会第十三届年会	昆明	2014.08
23.	括号代数 Groebner 基的定义与计算	黄雷	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
24.	括号代数的 Groebner 基	黄雷	中科院系统所青年学者报告会	北京	2014.11
25.	Proof of a formula of Schubert and its generalization	李邦河	University of Michigan	美国	2014.9
26.	Proof of a formula of Schubert and its generalization	李邦河	University of Minnesota	美国	2014.10
27.	Behavioral Heterogeneity and Financial Markets: Crossed Markets under Informationally Efficient Pricing	李博	The Midwest Economics Association 2014 Annual Meeting	美国	2014.03
28.	When do gossip algorithms converge in finite time?	李博	The 21st International Symposium on Mathematical Theory of Networks and Systems	荷兰	2014.07
29.	The Gröbner Basis Theory of Bracket Polynomials	李洪波	Joint Mathematics Meetings	美国	2014.01
30.	Sparse Difference Resultant	李　伟	Women and Mathematics	北京	2014.08

31.	Parallel Telescoping and Parameterized Picard--Vessiot Theory	李子明	The 39th International Symposium on Symbolic and Algebraic Computation(ISSAC2014)	日本	2014.07
32.	A Unique Signature Scheme Based on Candidate Multilinear Maps	刘卓军	The Third World Congress on Computing and Information Technology (WCIT2014)	马来西亚	2014.12
33.	有限域上复合多项式的差分性质研究	刘卓军	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
34.	A Three-Level Sieve Algorithm for the Shortest Vector Problem（邀请报告）	潘彦斌	2014 年密码算法前沿论坛	北京	2014.06
35.	A New Attack against the Selvi-Vivek-Rangan Deterministic Identity Based Signature Scheme from ACISP 2012	潘彦斌	19th Australasian Conference on Information Security and Privacy, ACISP 2014	澳大利亚	2014.07
36.	Solving Random Subset Sum Problem by lp-norm SVP Oracle	潘彦斌	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
37.	On Implementing Signature-based Grobner Basis Algorithms Using Linear Algebraic Routines from M4RI	王定康	The 20th Application of Computer Algebra	美国	2014.07
38.	Parametric Groebner Bases: Algorithms and Applications	王定康	Symposium on Symbolic Computation and Automated Reasoning	日本	2014.10
39.	Automatic Proving and Discovering of Geometric Theorems	王定康	CDZ Workshop GZ1115 on Computation and Reasoning with Constraints	北京	2014.11
40.	Matter and rogue waves of some generalized Gross-Pitaevskii equations with varying potentials and nonlinearities（邀请报告）	闫振亚	Int. Conf. on Symmetry method, Applications, and Related Fields	加拿大	2014.05
41.	畸形(怪)波	闫振亚	中国工业与应用数学学会第十三届年会	昆明	2014.08

42.	Localized wave structures and parameters modulation of the inhomogeneous Gross-Pitaevskii equations with varying potentials and nonlinearities（邀请报告）	闫振亚	中国数学会 2014 学术年会	新乡	2014.09
43.	Sparse Differential Resultants	袁春明	International Short-School/Conference on Affine Algebraic Geometry & the Jacobian Conjecture	天津	2014.07
44.	Curve Fitting and Interpolation under Confined Error	袁春明	4rd International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control	北京	2014.10
45.	Difference binomial ideals	袁春明	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
46.	Avoiding 5-axis Singularities Using Additional Matrix Transformation	张立先	4th International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control	北京	2014.10
47.	基于变插补周期的曲线插补方法	张立先	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
48.	Locally Repairable Codes For Distributed Storage Systems	张志芳	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11
49.	Certification via Symbolic-Numeric Computations（邀请报告）	支丽红	2014 NIMS Thematic Program on Applied Algebraic Geometry	韩国	2014.05
50.	Symbolic-numeric algorithms for computing validated results（邀请报告）	支丽红	The 39th International Symposium on Symbolic and Algebraic Computation(ISSAC2014)	日本	2014.07
51.	Optimizing a linear function over a noncompact real algebraic variety	支丽红	2014 International Symposium on Symbolic and Numeric Computation	上海	2014.07

52.	Verified Error Bounds for Isolated Singular Soulutions of Polynomial Systems（邀请报告）	支丽红	中国工业与应用数学学会第十三届年会	昆明	2014.08
53.	Semidefinite Representations of Non-Compact Convex Sets	支丽红	第六届全国计算机数学学术会议（CM2014）	重庆	2014.11

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.	空间数据挖掘中的数学方法研究	2014.5	2014.12	1	1	谢福鼎	王定康
2.	多项式系统实根验证	2014.5	2014.12	1	1	杨争峰	支丽红
3.	平面代数曲线的 0–th Betti 数	2014.5	2014.12	1	1	张明波	程进三

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	0	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三届学术委员会第五次会议于 2014 年 1 月 24 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黄敏副局长、中科院前沿科学与教育局实验室处薛艳杰副处长、中科院基础局数学物理处王永祥处长、国家自然科学基金委数理学部雷天刚处长应邀参加了会议。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从科研进展、国内外合作交流、人才培养等方面向与会各位专家汇报了 2013 年度数学机械化重点实验室工作进展情况。随后，按实验室研究方向由王定康、陈绍示分别作了学术报告。与会专家们听取了两个报告后，对报告内容产生了浓厚的兴趣，充分肯定了报告的成果。

专家们在会议中提出了很多建设性的意见。在科研成果的展示方面，认为应该突出科研特色，展示主要研究成果。在科研队伍的描述方面，认为科研队伍的描述应采用梯队形式，老中青相搭配，突出中青年科研人员。林惠民院士指出实验室理论研究要保持传统课题的优势，高瞻远瞩，注重积累，在新课题上有所突破。陆汝钤院士充分肯定我实验室在酶动力学方面的工作。张继平教授提出要切合国际前沿做好工作，注重和国际上的交流合作。李邦河院士和冯克勤教授提出可以在计算数论上面联合优势人才做出好的工作。李华研究员提出更新研究的软硬件，提高竞争力。薛艳杰副处长讲了今年实验室评估的要点，要注重重大成果，国家重大需求，关键科学问题。希望实验室的成果是围绕实验室的长期发展目标的成果。王永祥处长给实验室的人才梯队建设提出了建设性意见。

2、中国科学院数学与系统科学研究院、中科院沈阳计算技术研究所、中科院沈阳自动化所于 2014 年 6 月 29 日至 7 月 1 日在沈阳进行了学术交流会议。会议

还邀请了加拿大的 McMaster 大学的 Allan D. Spence 副教授作学术演讲，上述单位的 40 余位老师和研究生参加了本次学术交流会议。 在交流过程中，还组织了相关研究人员参观了沈阳计算所的数控加工车间与相关的先进数控设备、沈阳自动化所的机器人及加工样件。

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）主持。中国科学院数学与系统科学研究院、中科院沈阳计算技术研究所、中科院沈阳自动化所的科研人员与学生分别介绍了最近 2 年的新的工作与遇到的问题。

本次交流会议促进了中国科学院数学与系统科学研究院、中科院沈阳计算技术研究所、中科院沈阳自动化所三家单位之间的交流与合作，对促进三家单位在数控技术上的理论与实际加工的交叉与融合起到了重要作用。

3、2014 年 7 月在日本神户召开的第 39 届国际符号和代数计算会议(ACM ISSAC 2014)上，本实验室有 3 篇论文被接受。ISSAC 是符号和代数计算方面最权威的国际会议。3 篇被接受论文是

1) Hongbo Li, Changpeng Shao, Lei Huang and Yue Liu. Reduction among Bracket Polynomials.

2) Shaoshi Chen, Ruyong Feng, Ziming Li and Michael F. Singer. Parallel Telescoping and Parameterized Picard-Vessiot Theory.

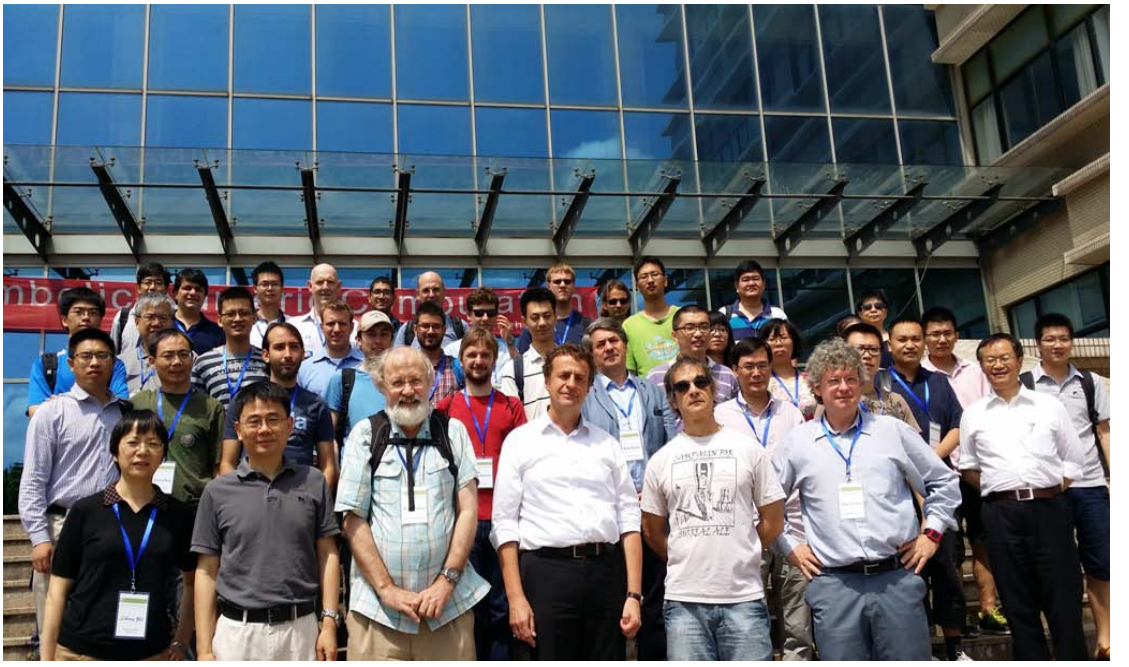
3) Shaoshi Chen, Manuel Kauers and Christoph Koutschan. A Generalized Apagodu-Zeilberger Algorithm.

此次大会支丽红研究员应邀做 tuorial，题目为：Symbolic-numeric algorithms for computing validated results（http://www.issac-conference.org/2014/tutorials.html).。

陈绍示、黄辉、李子明获 ISSAC 2014 杰出 Poster 奖。该 Poster 的题目是：Improved Abramov-Petkovsek's Reduction and Creative Telescoping for HypergeometricTerm（http://www.issac-conference.org/2014/awards.html)。

4、 第五届国际符号和数值计算会议于 7 月 28-31 在中国上海召开。符号和数值混合计算方面最权威的国际会议。已在中国 2005、日本 2007、加拿大 2009、美国 2011 举办过。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。本次会议促进符号计算和数值计算领域的专家学者的交流与合作，共同探讨发展更快、更稳定可信的混合计算算法和理论。会议在线性、多项式和微分代数中的符号数值混合算法；代数几何、非线性优化、几何计算中的符号和数值混合计算； 混合算法在优化、验证等中的应用等方面进行了交流。

本次会议有 65 人左右，其中外宾 20 人左右，内宾 45 人左右，代表来自美国、法国、英国、德国，日本，新加坡等国家和地区。有国内多位院士和杰出青年基金获得者参加，他们不仅代表了中国在这个领域的最高水平, 也反映出了世界上在这个领域的一流水平和最新研究成果。特邀报告人包括美国 North Carolina State University 大学的 Erich Kaltofen 教授、美国 UC Berkeley 大学 Bernd Sturmfels 教授， 英国 U. of Cambridge 大学 Lawrence Paulson 教授等。



5、2014 年 10 月 14 日，数学机械化重点实验室参加了中国科学院前沿科学与教育局组织的重点实验室现场评估，会议由理论物理研究所张肇西院士主持，评估专家包括自动化研究所刘德荣研究员，信息工程研究所林东岱研究员，北京应用物理与计算数学研究所江松研究员，北京大学吴学兵教授，南京大学周济林教授，武汉物理与数学研究所梅刚华研究员，西安光学精密机械研究所王屹山研究员，北京师范大学付建宁教授，理论物理研究所陈晓松研究员，理化技术研究所李来风研究员，宁波材料技术与工程研究所许高杰研究员。科学院相关部门领导以及主管也参加了此次评估会议。

首先由实验室主任李洪波研究员做过去五年工作报告并回答了专家组提问。高小山研究员以及邓映蒲研究员分别做了实验室代表性成果的学术报告并回答了专家提问。接着专家组成员进行现场考察，听取了王定康研究员数学机械化软件演示、冯秀涛助理研究员密码软件演示、张立先助理研究员数控演示，参观了实验室展板，检查了项目合同，年报，论文，专利，实验室有关规章制度、博士后名单、研究生及其导师名单、代表性活动图片等各类材料。

专家组听取了实验室的工作报告和代表性成果报告，进行了质询，对实验室进行了现场考察。经认真讨论，认为实验室在微分差分系统的数学机械化方法、符号与数值混合计算、非线性系统的构造性理论方法、信息安全的数学基础以及高档数控中的高效插补与刀补算法等方面取得了系列突出的具有国际影响研究成果，理论算法与实际应用联系紧密，成绩显著。同时专家组也对实验室未来的发展提出了建设和意见：加强相关算法的软件研究力度，提高实验室自主算法的成果转化及应用，服务于国家需求；采取有力措施，吸引和稳定从事软件开发和交叉研究的人员，以满足承担重大国家需求；进一步拓展与其他学科的交叉和应用，增加数学机械化方法对其他学科的影响力。

除了现场评审，在今年的 9 月科学院还对实验室进行了会议评估，在会议评估中实验室取得了优秀。

6、2014 年计算机辅助制造、工程与数控中的数学与算法国际会议（MAMENC 2014）于 2014 年 10 月 23-25 日在中国科学院大学国际会议中心（怀柔）召开。会议邀请了新西兰、加拿大、泰国、俄罗斯等国家的大学与科研单位，以及国内的华中科技大学、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、浙江大学、中国科学院大学、北京航空航天大学、大连理工大学、西北工业大学、中国石油大学等单位的 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）主持并致开幕词。University of Auckland 的 Xun W Xu 教授，Thammasat University 的 Stanislav S. Makhanov 教授，University of Waterloo 的 Kaan Erkorkmaz 教授，中国科学院沈阳计算技术研究所的于东研究员，中国科学院数学与系统科学研究院的高小山研究员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四次举办，此次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。会议网站见：http://mmrc.iss.ac.cn/cnc/cnc2014/。

7、第六届全国计算机数学学术会议（CM2014）于 10 月 31—11 月 3 日在重庆市万友康年酒店召开。本次会议由中国数学会计算机数学专业委员会主办，中国科学院重庆绿色智能技术研究院、中国科学院成都信息技术股份有限公司、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 130 人参加了会议，会议得到了中国数学会的赞助。大会主席周巢尘院士、973 首席科学家高小山研究员、中国科学院重庆绿色智能技术研究院的领导在大会上作了精彩的发言，并预祝大会圆满成功。高小山研究员也代表计算机数学学会做了发言，回顾了学会的历届会议，学会对整个中国计

算机数学发展的引导作用，同时也展望了学会未来的发展方向。

会议邀请国际著名的华人数学家、Michigan State University 的 Tien-Yien Li（李天岩）教授做了题为 “Solving Real Polynomial Systems by Real Homotopies”的邀请报告；北京大学许超教授做了题为“基于多模态特征的图像分析”的邀请报告，夏壁灿教授做了题为“不等式机器证明的一些进展”的邀请报告。会议还安排了 28 位研究人员在分组会议上做了学术报告。973 项目“数学机械化方法及其在数字化设计制造中的应用”也进行了学术交流与年度汇报会。

8、2014 年 11 月 13 日，国家数学交叉科学中心（以下简称“交叉中心”）中期检查评审会在数学院召开，这是科学院对交叉中心中期评估工作中继国际函评及经费检查后的最后一个环节。中科院邓麦村秘书长、发展规划局张凤副局长、前沿科学与教育局黄敏副局长、相关部门负责同志，科学院邀请的相关领域评审专家，数学院相关院领导，交叉中心正副主任、学术委员会正副主任、研究部主任及研究专题负责人等 40 余人出席会议。会议由邓麦村秘书长主持，

专家评审部分由专家组组长西安交通大学徐宗本院士主持。

邓麦村秘书长首先感谢各位专家出席评审会，并介绍了先导专项的特点，本次中期检查的目的和要求。随后，发展规划局张凤副局长就中期检查的具体部署情况进行了详细介绍。

此次评审会议分为两部分：一是听取中心专项、6 个研究部及合肥分中心自中心成立以来的工作汇报；二是由专家组进行讨论评议。

交叉中心主任郭雷院士首先从中心的成立背景、总体目标和主要任务入手，介绍了中心成立以来在科技目标完成、组织管理保障、资源配置绩效、人才团队建设、未来工作计划等五个方面的工作。随后，交叉中心 6 个交叉研究部及合肥分中心负责人也分别进行汇报并回答提问。数学与先进制造交叉研究部主任李洪波研究员代表先进制造部进行了汇报。

评审专家分别从专项和项目层面，就交叉中心进展情况进行了评议和讨论。西安交通大学徐宗本院士、国家工业和信息化部杨学山副部长、国家自然科学基金委陈宜瑜院士、华中科技大学熊有伦院士、中科院动物所康乐院士、合肥工业大学杨善林院士、北京邮电大学乔建永校长、清华大学周坚教授、浙江大学包刚教授、中国空间技术研究院李勇研究员、国家纳米科学中心张忠研究员等在听取汇报、审阅资料、现场提问的基础上，针对专项任务书的目标和计划进度等检查重点，充分肯定了专项实施三年以来取得的进展和成果，并对下一步工作计划提出重要建议。

除了现场评审，在今年的 8 月及 10 月，科学院还分别对交叉中心进行了函评及经费检查。函评采取的方式是国际评估，针对每个项目的研究方向，科学院选取若干小同行专家，在历时一个多月的函评阶段，对中心专项、6 个研究部及 1 个分中心的进展报告进行了网上评审。评审专家包括多位国际知名学者。本次中期评估对下阶段进一步调整中心科研布局，顺利完成中心五年目标具有

重要意义。

9、2014 年 12 月 15 日上午在数学院南楼 213 会议室召开了“AC 摇篮式五轴联动加工中心”验收会议。参加此次验收的人员包括中科院数学院副院长高小山研究员，李洪波研究员，清华大学李铁民副教授，中科研物理所机加工厂高太原厂长、贺建伟副厂长，中科院数学院院长业务助理潘建中研究员，中科院数学院综合处处长马鲁，中科院数学院财务与资产管理处处长冯丽平，中科院数学院安全与物业管理中心主任范同春，中科院数学院图书与网络管理中心主任兼综合处副处长冯雷，中科院数学院综合处政府采购主管周宏，中科院数学院综合处综合档案主管许清以及桂林机床股份有限公司代表唐海明，沈阳高精数控技术有限公司代表臧辉、丛振华。

会议由验收小组组长高小山副院长主持，首先由验收小组副组长李洪波研究员介绍了机床购置以及验收测量的情况，接着桂林机床股份有限公司代表唐海明介绍了机床的安装以及调试工作，沈阳高精数控技术有限公司代表臧辉介绍了机床测量验收情况，随后验收小组成员参观了先进制造数控加工实验室，做了机床实地考察。验收小组就机床操作流程，机床厂家售后，机床放置环境安全等问题与厂商代表进行了咨询与沟通。经过讨论，验收小组认为厂商已按合同技术指标要求完成了现场安装和系统调试，性能测试指标达到使用方要求的技术参数和合同要求，具备了正式运行的条件，同意通过“AC 摇篮式五轴联动加工中心”的验收。

此次验收会同时进行了“AC 摇篮式五轴联动加工中心”管理、技术、商务以及财务档案验收，中科院数学院综合处综合档案主管许清查看了各类档案文件，认为各类档案已经完备，同意通过该项目档案验收。

“AC 摇篮式五轴联动加工中心”是国家数学与交叉科学中心先进制造部购买的一台设备，用于进行插补、刀补和误差补偿实验，支该设备支持研究、开发与评价基于数学机械化方法的高档数控系统核心控制功能与算法。

10、973 项目“数学机械化方法及其在数字化设计制造中的应用”专家汇报会于 2014 年 12 月 17 日在中国科学院数学与系统科学研究院召开。项目责任专家吕建院士、彭群生教授，项目专家组成员林惠民院士、李邦河院士，高小山、林浒(于东代)、陈发来(邓建松代)，科技部基础研究管理中心谢夏等出席了会议，项目首席科学家高小山研究员以及四个项目课题组长参加了会议。

项目首席科学家高小山研究员介绍了项目的整体情况，随后四个课题组长高小山研究员、支丽红研究员、邓建松教授、李洪波研究员分别汇报了各自课题 2014 年的进展情况。听取报告后，与会专家肯定了项目取得的成绩，同时为项目进一步的工作提出了建设性意见，特别是在数字化设计制造方面需要凝聚研究内容，在项目执行的最后一年集中攻关。

本项目成员 2014 年微分差分方程符号求解理论与算法、密码体制的分析与设计、构造性代数几何理论、代数与几何方法、基于混合计算的误差可控算法、复杂数字曲面几何特征识别、曲面造型理论、高档数控算法与系统、光刻机与伺服控制建模与计算等方面取得重要进展。获得教育部自然科学奖二等奖、ISSAC 最佳 Poster 奖、辽宁省技术发明二等奖、辽宁省科技进步三等奖、中国科学院卢嘉锡青年科学家奖、中国科学院系统科学研究所关肇直青年研究奖、中科院数学院陈景润未来之星等，发表论文 126 篇，其中 SCI 收录 80 余篇，新授权发明专利 9 项，新申请发明专利 8 项，圆满完成了计划任务。

11、数学与系统科学研究院第七届“陈景润未来之星”揭晓，实验室助理研究员陈绍示入选。数学与系统科学研究院 2014 年突出科研成果揭晓，实验室陈绍示、冯如勇、李子明 “Zeilberger 算法的终止性，效率及其推广”以及李博、李邦河 “酶动力学中的拟稳态定律及参数估计”入选。