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： 62541834

传真： 62630706

E-MAIL： dzhou@mmrc.iss.ac.cn

网址： http://www.mmrc.iss.ac.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。

数学机械化不仅是数学研究的实质性进展，而且在高科技领域获得了一批理论成果，可望解决尖端技术产业中的若干项技术问题，包括曲面造型，机构分析，几何设计，计算机视觉，信息安全等，为促进我国技术产业的发展做出积极的贡献。

除高科技领域外，数学机械化的方法还被成功地用于解决其他领域的很多问题：理论物理中的杨振宁 - Baxter 方程求解，天体力学中的多体问题，化学平衡方程求解，小波构造的优化，命题逻辑与一阶谓词逻辑定理证明，非线性发展方程的行波解算法，等等。

在国际上，计算机与数学的交叉正在成为数学研究新的增长点，出现了计算代数、计算群论、计算几何、计算数论等新兴学科。符号计算是研究在计算机上进行准确的数学演算和与之相关的数学理论的学科，是数学机械化的主要工具。近年来一批专业化的学术机构已在世界各地纷纷成立。符号计算软件

Maple, Mathematica 已经在数学与工程领域被广泛使用。８０年代以来，解（微分）代数多项式方程组是国际符号计算界的热点，其主要方法是 Groebner 基方法。90 年代欧共体跨国研究项目 POSSO(POlynomial System SOlving) 及作为 POSSO 的延续项目 FRISCO 关注的问题，与我们开展数学机械化研究课题有许多相同之处。所不同的是，我们所用的是我国数学家自己发展起来的一套方法和理论。

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。

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。

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。

(1) 利用组合学、代数数论和有限几何来研究信息科学，特别是编码理论，是信息科学中的一个热门研究方向。
(2) 代数几何码是上世纪八十年代由苏联数学家发现的，这一发现使代数几何通过编码理论被天才地用到通信工程中去。 由于代数几何码卓越的纠错和检错性能，持续二十多年，代数几何码的研究仍然是信息论的一个热点。
(3) Turbo 码是法国学者 1993 年发现的一种新的差错控制码，这种码的纠错性能几乎接近 Shannon 限，在远程数据通信、数据的磁记录等应用领域是性能最好的码。
(4) 时空码是美国学者 Tarokh 和 Calderbank 等人发现的一种码，它在多通道、多天线、无线通信信道例如手机通信中，可以极大地改进信道的性能。
(5) 量子纠错码和量子密码是量子信息论的两个基本方面，研究量子计算和量子算法是当今信息科学中的最前沿方向之一。

总体目标与学术方向

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。

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。**目前实验室主要研究自动推理、几何计算、符号计算与混合计算，特别是求解各类方程的高效算法。

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。**包括有限域理论、计算数论、密码学和安全多方计算。

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。

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.	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.	陆汝钤	男	中国	委员	院士	是	中科院数学院
9.	陈永川	男	中国	委员	院士	是	南开大学
10.	吴　可	男	中国	委员	教授	否	首都师范大学
11.	张继平	男	中国	委员	教授	否	北京大学
12.	李克正	男	中国	委员	教授	否	首都师范大学
13.	冯克勤	男	中国	委员	教授	否	清华大学
14.	李　华	男	中国	委员	研究员	否	中科院计算机所
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		所聘副研	符号计算	研究
19.	冯秀涛	男	1978.8		所聘副研	信息安全	研究
20.	冷福生	男	1980.5		助研	代数数论	研究
21.	周　凯	男	1981.9		助研	代数、编码	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.	张立先	女	1982.10		项目助研	高档数控	研究
28.	李　伟	女	1985.9		项目助研	微分代数几何	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、冯如勇、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	常务理事	2009	2012
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	2013
6.	高小山	ACM SIGSAM Jenks Memorial Prize 评奖委员会	委员	2012	2013
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	2012	2016
14.	李子明	中国数学会	理事	2012	2016
15.	李子明	ACM SIGSAM	顾问	2010	2015
16.	王定康	中国数学会计算机数学专业委员会	秘书长	2010	2013

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	2014
19.	邓映蒲	中国密码学会理事会	理事		
20.	邓映蒲	中国数学会计算机数学专业委员会	委员		
21.	邓映蒲	中国电子学会信息论分会	委员		

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》**	副主编		
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 A》**	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.	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		

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.	闫振亚	王晓云		
2.	支丽红	刘　琦		
3.	万哲先	杨江帅		
4.	邓映蒲	廖茂东		
5.	支丽红	郝志伟		
6.	王定康	张文哲		
7.	邓映蒲	王　慧		
8.	冯如勇	熊纯文		
9.	韩　阳	张凝鹛		
10.	高小山	荆瑞娟		
11.	高小山	王　杰		

12.	闫振亚	闫方驰		
13.	闫振亚	陈　勇		
14.	袁春明	宓振鹏		
15.	支丽红	杨志红		
16.	刘卓军	李秋萍		
17.	程进三	窦孝杰		
18.	冯秀涛	付士辉		
19.	王定康	白　剑		
20.	李洪波	周　亮		
21.	张志芳	周义满		
22.	李子明		黄　辉	
23.	闫振亚		温子超	
24.	支丽红		王　础	
25.	万哲先，邓映蒲		张　凡	
26.	万哲先		刘仁章	
27.	李洪波		邵长鹏	
28.	李洪波		文　勇	
29.	李子明		张　熠	
30.	高小山		黄　章	
31.	高小山		赵明勇	
32.	万哲先		孙志强	
33.	李洪波		李　阁	
34.	高小山		郭建新	
35.	高小山		闵　程	
36.	支丽红		郭庆东	

37.	刘卓军		张晓明	
38.	黄民强，邓映蒲		张　凤	
39.	吴文俊，程进三		金　凯	
40.	刘卓军		李晓明	
41.	支丽红		李　楠	
42.	支丽红		李子佳	
43.	高小山		张　可	
44.	韩　阳		陈　慧	
45.	李洪波		姚守彬	
46.	刘卓军		吴保峰	
47.	王定康		马晓栋	
48.	邓映蒲		姜宇鹏	
49.	闫振亚		姜东梅	
50.	刘卓军		黄　冲	
51.	韩　阳		章　超	
52.	高小山		祝　炜	
53.	李洪波		刘　越	
54.	黄民强		胡耿然	
55.	胡　磊		吕　昌	
56.	万哲先		王安宇	
57.	刘卓军		王　晗	
58.	李洪波		王立波	
59.	高小山，冯如勇		李应弘	
60.	黄民强，邓映蒲		黄丹丹	
61.	韩　阳		秦永云	

62.	吴文俊，王定康		周　洁	
63.	李洪波		董　磊	
64.	高小山		黄巧龙	
65.	支丽红			梁　野
66.	支丽红			李　喆
67.	闫振亚			于发军
68.	闫振亚			杨云青

毕业研究生一览表

序号	姓名	学位	导师姓名	毕业时间
1.	梁　野	博士后	支丽红	
2.	李　喆	博士后	支丽红	
3.	李晓明	博士	刘卓军	
4.	张　可	博士	高小山	
5.	李　楠	博士	支丽红	
6.	李子佳	博士	支丽红	
7.	陈　慧	博士	韩　阳	
8.	马晓栋	博士	王定康	
9.	姚守斌	博士	李洪波	
10.	吴保峰	博士	刘卓军	
11.	姜宇鹏	博士	邓映蒲	
12.	姜冬梅	博士	闫振亚	
13.	王晓云	硕士	闫振亚	
14.	刘　琦	硕士	支丽红	

研究生获奖一览表

序号	获奖名称	获奖人员	指导教师
1.	2013 年度国际符号和代数计算会议(ISSAC)最佳学生论文奖	郭庆东	支丽红
2.	中国科学院优秀博士学位论文	李　伟	高小山
3.	中国科学院院长优秀奖	姜宇鹏	邓映蒲
4.	国家奖学金	郭建新	高小山
5.	国家奖学金	郝志伟	支丽红
6.	中科院数学院院长奖学金特等奖	郭建新	高小山
7.	中科院数学院院长奖学金优秀奖	郭庆东	支丽红
8.	中科院数学院院长奖学金优秀奖	张　凤	邓映蒲
9.	中国科学院研究生院三好学生标兵	郭建新	高小山
10.	中国科学院研究生院三好学生	郭庆东	支丽红
11.	中国科学院研究生院三好学生	郝志伟	支丽红

12.	中国科学院研究生院三好学生	廖茂东	邓映蒲
13.	中国科学院研究生院三好学生	张　凡	邓映蒲
14.	中国科学院研究生院三好学生	邵长鹏	李洪波
15.	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，

国家杰出青年基金项目 1 项，

国家自然科学基金重大项目子课题 1 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 4 项，

国家自然科学基金青年基金 5 项，

国家密码发展基金 1 项，

中国科学院重要方向性项目 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 48 篇。此外，冯秀涛参加的 LTE 序列密码设计与分析项目的工作，获得 2013 年国家技术发明二等奖。博士生郭庆东获 2013 年度 ISSAC 最佳学生论文奖。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）

初步建立了稀疏差分结式理论和差分 Chow 形式理论，给出了稀疏差分结式存在的充要条件，以及计算稀疏差分结式的单指数算法。首先，我们定义了稀疏差分结式，给出了稀疏差分结式存在的充要条件。其次，证明了稀疏差分结式的基本性质，特别证明了稀疏差分结式具有明显优于微分结式的一些性质，例如稀疏差分结式的精确次数是 BKK 数， 稀疏差分结式可以表示成两个矩阵行列式的比值等。最后，给出了阶及次数界的估计，并基于阶数和次数界给出了计算稀疏差分结式的单指数算法，相关论文发表在 ISSAC 2013 会议文集上。

Toric 簇是代数几何中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？我们给出了差分 Toric 簇的几种等价定义，研究了差分 Toric 簇与差分二项式理想的对应关系，证明了差分 Toric 簇与一类差分二项式理想是一一对应的。对于 Laurent 差分二项式理想，我们将其上的运算对应到 Z[X] 模上的运算，从而可以算法化地判定一个 Laurent 差分二项式理想是否是素的，自反的以及其对应的簇是否是 Toric 簇。此外，所设计的算法也可以用来计算一个 Laurent 差分二项式理想的素分支，自反闭包和 Z[X] 饱和理想。

超指数函数是符号计算中最简单的一类非有理函数，但超指数函数的不定积分不一定是超指数函数。我们给出了超指数情形的 Hermite 约化方法，把一个超指数函数唯一地写成一个超指数可积的函数和一个超指数不可积函数之和，不仅化简了超指数函数积分的计算，而且导致了一种新的计算超指数函数的

Telescoper 的新算法，大幅度提高了计算效率。同时还得到了关于 telescoper 阶的新的上界。该上界是目前最紧的。

此外，我们给出了计算线性微分方程 Galois 群的 Hrushovski 算法的改进版本，估计出了计算中所需要的重要的界。确定了关于微分算子，差分算子以及 q-差分算子相容的有理函数的结构，给出了微分算子，差分算子以及 q-差分算子情形的 Zeilberger 算法的终止性判定条件。

(1.2) 符号与几何计算（李洪波、王定康、黄雷、贾晓红）

我们研究各种不变多项式的标准型，以及不变多项式之间的不变除法。对如下符号代数系统：（1）四元数变元多项式环；（2）三维正交几何的高级不变量多项式；（3）n 维黎曼流形的曲率分量构成的多项式，得到了如下结果：（1）在由 $1,i,j,k$ 和四元数变元定义的四元数变元多项式环中，对只含四元数变元的子环给出了等价的不需要 $1,i,j,k$ 的定义；在四元数变元采取共轭相邻序下，给出了四元数变元多项式的标准型及相应算法；（2）给出了三维正交几何的高级不变量多项式的两类标准型；（3）给出了曲率分量构成的多项式的标准型及相应算法。以上结果分别是无坐标三维正交计算的基础，以及 n 维黎曼流形局部坐标计算的基础。

我们提出了计算参数多项式系统的 Groebner 基和参数 Groebner 系统的算法；是相关算法中效率最高的。F5 算法是最好的计算多项式系统的 Groebner 基算法。我们给出 F5 算法正确性的严格证明。此外，我们提出了一个代数扩域上的因式分解的多项式时间算法，比传统算法（指数复杂度）效率提高数十到数百倍。

圆纹面(cyclide)因其特殊良好的几何性质，已经逐渐成为建筑几何、几何建模中重要的基本元素。我们将两圆纹面的交线的拓扑情况进行了分类及穷举，并且设计了符号计算方法来确定给定两圆纹面的交线的拓扑。该算法仅需要确定两个四次单变元多项式的根的个数，十分简洁高效, 可以嵌入几何建模的诸多问题中。

两曲面交线拓扑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拓扑的符号计算。目前我们已将该算法应用于二次曲面复合体的碰撞检测中。

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. 该简易逆公式将加速诸多 Cyclide 涉及的工业计算。

空间有理曲线的奇异点计算是 CAGD 中的重要问题。已有算法多局限于将空间曲线投影至多个平面，因而易产生冗余结果且效率较低，并且难以提供可靠的理论保障。我们提出了利用动曲线曲面（mu 基）和稀疏结式计算空间有理曲线上奇异点的符号计算方法。该方法不仅可以解出空间有理曲线上的基本奇点，而且可以由每个奇点展开该曲线的奇点树。该方法不产生冗余结果，且有完整的理论保障。

(1.3) 多项式可信计算（支丽红、程进三）

在多项式系统的实根计算中，提出存在性可信验证的两种方法：基于实代数几何和同伦算法；基于矩量矩阵核范数极小化算法。可以处理超定和欠定的多项式系统，也可以验证奇异实解。

在线性矩阵不等式有理解可行性判定与计算中，给出了有理系数线性矩阵不等式是否存在有理解的验证准则和高效算法。 新算法使得判定一个有理系数多项式是否存在有理多项式平方和表出的算法复杂度较法国巴黎六大 Safey 教授与本人在 2010 年 SIAMOPT 上给出的算法复杂度有了显著改进。美国加州大学伯克利分校 Sturmfels 教授于 2008 年提出一个问题：如果一个有理系数多项式存在实系数多项式平方和分解，其是否存在有理系数多项式平方和分解？我们给出了 Sturmfels 问题反例的第一个计算机验证。

通过改进局部一般位置方法，克服了瓶颈计算问题，应用到一般的多项式方程组的求解中，比原来的方法提高了很多倍，特别是在双变元情形下，大大高于国际同行可计算的规模和计算效率。

提出了新的确定空间曲线拓扑的方法：通过分析两个平面曲线的拓扑来得到空间曲面的拓扑。在得到拓扑的基础上，我们又得到了空间曲线的有理参数逼近表示，其中分子分母都是一次多项式。

2. 编码与密码

(2.1) 素数判定方法（邓映蒲、潘彦斌、冷福生）

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算法。确定性算法由于其计算量过大而不适用。在概率算法中，比较简单实用的是著名的 Miller-Rabin 算法。它基于强伪素数的性质。如果我们知道前某些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。

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 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。

最短向量问题（SVP）是格中经典的困难问题之一。几乎所有格密码体制的安全性均与 SVP 的困难性有关。我们提出了一个指数时间求解 SVP 的三层随机筛法。该算法是目前已知求解 SVP 理论上最快的算法。

L 函数是数论中重要的组成部分。Deling 证明了多项式 f 的 L 函数逆根的 p-adic order 是[0,1]区间的有理数。而我们将其改进为[0,1]区间内有限种形式的有理数，并以此对 L 函数牛顿多边形进行了分类。我们进一步证明了，求解 L 函数逆根的 p-adic order 只需要对超过某个常数的具体两个 p 值进行计算即可。

(2.2) 轻量级流密码（冯秀涛）

A2U2 是由丹麦学者 D. Mathieu、C. Damith 和 L. Torben 等人提出的一个轻量级流密码，拟用于 RFID 电子标签加密，该算法发表在 RFID 专业的国际顶级会议 IEEE RFID。

针对 A2U2，我们给出了在已知明文攻击模型下的实时密钥恢复方法，至多需要 210 个比特的明密文数据，时间复杂度不超过 2^{25}，在个人 PC 上只需数秒钟便可恢复出全部密钥比特，远优于丹麦学者 M. Abdelraheem 等人给出的复杂度为 2^{49}*C 的分析结果。此外，我们攻击方法采用的已知明文攻击模型较加拿大 Q. Chai 和 G. Gong 等人提出的选择明文攻击模型更一般，意味着 A2U2 算法已经被彻底破解。

(2.3) 分布式存储编码（张志芳）

针对分布式存储编码的局部修复要求，从组合的角度提出新的局部性概念，将局部修复结构改变为互不相交的子集合。这种结构上的变化使得在同样的局部容错能力下码的最小距离得到提升，提高了整体系统的可靠性。并且，可以实现多渠道的并行修复，解决了热点数据节点的访问拥塞问题。

在这种新的局部性定义下，证明了最小距离的上界，并给出一定参数条件下达到上界的具体构造。特别地，构造了一类最小距离接近最优，并且信息率趋于 1 的局部可修复编码。

(2.4) 有限域（万哲先、刘卓军、周凯）

给出了有限域上线性化多项式代数结构的两种新的刻画，进而得到了有限域上线性化置换多项式的求逆公式，并显式确定了几类有限域上特殊形式的线性化置换多项式的逆多项式。

引入了利用有限预拟域构造密码学中 PS 型 bent 和广义 bent 函数的方法，显式表达出了几类 PS 型 bent 和广义 bent 函数。它们是继 PSap 函数之后三十多年来首次被表达出的 PS 型 bent 函数。

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）

针对求解带有高阶运动学约束的时间最优控制问题，我们借助控制参数化方法，证明加速度约束的最优速度规划问题可以参数化为一个线性规划问题，从而给出了原问题求解的多项式时间算法。通过引入虚拟 jerk 约束的概念，将 Jerk 有界问题划归成了一个具有线性规划的凸优化问题。该算法在清华实验室的数控铣床机床上进行实验，得到了很好的效果。

我们首次提出了两类给定路径情形的跟踪误差有界控制模型，并给出了相应高效算法。新模型的建立和相应高效算法的提出，意味着带有高阶动力学和运动学约束的时间最优意义下的速度优化问题的数值解基本被解决，这对 CNC 过程的全智能开放端口的建设具有重要意义。

我们考虑了带动力学约束的时间最优轨迹规划问题。与以往的工作不同，我们的模型旨在通过开环的方法来控制加工过程中的跟踪误差。新的问题是一个带有高阶 ODE 约束的最优控制问题。我们建立了相应的约化理论，将原问题可以划归成一个仅含高阶运动学约束的时间最优控制问题，引入了双层规划的想法处理高阶运动学约束，将虚拟跟踪误差约束和 jerk 约束加强为线性约束。这样整个问题缩放成一个凸优化问题，大大提高了算法的效率。我们在 University of British Columbia 的 Fadal 数控铣床上进行了实验，得到了理论预期的效果。

根据跟踪误差开环控制的思想，我们还考虑了一类给定 G 代码情况下 Jerk 约束下的时间最优速度优化问题，G01 代码之间是由时间参数的三次样条连接的路径。在处理动力学约束的时候，我们构造了 ODE 约束的一个特解，由此给出了通解的表达形式。这样，带有 ODE 约束的跟踪误差约束可以被一个虚拟的跟踪误差的上界来控制住。至此，整个问题可以完全求解。我们同样在 University of British Columbia 的 Fadal 数控铣床上进行了实验，得到了理论预期的效果。给定 G 代码路径的轨迹规划问题在 robot 领域经常被采用，因此我们的结果也对机械臂领域的轨迹规划有重要的借鉴意义。

(3.2) 酶动力学（李邦河、李博）

2013 年，我们在数学上严格证明了酶动力学中从上世纪三十年代使用至今的可逆模型中的拟稳态假设。因此，我们称其为可逆模型下的拟稳态定律。这一假设的基本重要性表现在它被写在各种生物化学和化学动力学教科书里。

该工作推广了 2008 年我们发表在 J. Phys. Chem. A 上的工作。原工作讨论了不可逆模型下的拟稳态假设，证明了其正确性。但是真实的生化过程是可逆的。研究不可逆模型的目的其实是为了研究可逆模型。可逆模型拥有更广，更精确的应用前景。

(3.3) 非线性物理方程的特殊解

对一维非线性光学中带有外势的时空调制高阶非线性 Schrodinger 方程，我们通过变换获得了该模型的畸形波解, 由于该解中含有任意函数, 这些解展示了丰富的畸形波的变化进程, 对于分析非自治畸形波的物理机理具有重要的意义。这方面结果发表在国际重要期刊 J. Opt.上。

提出具有 PT-对称非线性 Gross-Pitaevskii 方程的物质波解，并且研究了它们的数学结构和物理性质。论文发表在 Phil. Trans. R. Soc. A 上。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，该结果被 Stud. Appl. Math. 在线发表。

（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、参数多项式系统 Groebner 基的相关研究：提出了计算 CGB 和 CGS 的最有效的算法，比之前已有的算法效率提高出几十到几百倍。（王定康）

含参数的多项式系统的求解问题是数学研究中一个非常基本的问题。数学、其他科学以及工程实际中提出的许多问题都可以归结为含参数的代数方程组的求解问题。因此，对参数多项式系统的研究显得极为基础，也极为重要。

一个含参数的多项式方程组包含两种量，一类是参数，通常作为输入的一部分而给出，它们的取值可以是任意的；另一类是变量，也就是未知数，它们的取值依赖于参数的取值，它们也正是我们所要求解的量。不同的参数取值会使得方程组有很大的不同，因此，含参数的方程组求解要比无参数的情况复杂的多。很多用来求解无参数代数方程组的方法对于含参数的方程组已经不再适

用，而另有一些方法需要改进后才能用于求解含参数的方程组。

Groebner 基方法是求解代数方程组的一种非常重要的方法。对于不含参数的多项式系统的 Groebner 基的相关研究已经相对成熟，也有不少有效的算法。参数情形下的 Groebner 基的研究相对更困难，研究结果也更少。

1992 年，Weispfenning 提出了参数情形下的 Groebner 基的概念：Comprehensive Groebner Bases (CGB) 和 Comprehensive Groebner System(CGS)。设 k 是一个数域，u1,…,um 是参数，x1,…,xn 是变元。假设 K 是 k 的一个扩域，通常情况下 K 是一个包含 k 的代数闭域。将多项式环 k[u1,…,um,x1…,xn]记作 R. 对于 R 中的一个集合（或理想）F， R 中的有限集合 G 称为是 F 的 Comprehensive Groebner bases (CGB) 如果对于 K^m 中的任意一个元素(a1,…,am), G(a1,…,am,x1,…,xn) (即 G 中元素的参数 u1,…,um 分别被 a1,…,am 代替) 都是 F（a1,…,am,x1,…,xn）在多项式环 K[x1,…,xn]中生成理想的 Groebner 基。（通常我们还要求 G 是 F 生成理想中的子集）

如果 K^m 中的子集 C1,…,Cs 两两不相交，而且它们的并集就是 K^m 自己，我们称 C1,…,Cs 是 K^m 的一个有限分区。对于 R 中的一个集合（或理想）F，集合 (C1, G1)…,(Cs, Gs) 称作是 F 的 Comprehensive Groebner System (CGS)，如果满足：对于 K^m 的任意一个元素(a1,…,am)，如果(a1,…,am)是某个 Ci(1 • i• m)中的元素，Gi(a1,…,am,x1,…,xn)一定是 F（a1,…,am,x1,…,xn）在多项式环 K[x1,…,xn]中生成理想的 Groebner 基。

CGB 和 CGS 都可以看作是经典的 Groebner 基概念在参数情形的推广。CGB 和 CGS 是用来求解参数代数方程组的重要工具。Weispfenning 的在他的论文中不仅提出了 CGB 的概念，而且给出了一个构造 CGB 的直接算法。CGB 通常包含了很多信息，以至于可以从 CGB 中很容易的构造出 CGS. 通常情况下，CGB 的规模小于其所对应的 CGS，因而可以说 CGB 是用一个“浓缩”的形式包含了 CGS 等量的信息。

Weispfenning 在 1992 年发表的这篇文章可以说是用 Groebner 基方法求解参数代数方程组的一个里程碑，然而，从计算的角度来说，他所提出的计算 CGB 的算法效率并不十分令人满意。在这以后，学术界关于参数 Groebner 基的研究主要集中在设计新算法来提高计算 CGB 或 CGS 的效率。

1995 年，Kapur 提出了“约束多项式”的概念。所谓“约束多项式”就是一个有序二元对，由约束表达式和多项式构成。约束表达式通常可以看成是关于参数的一些函数，当参数取确定的值时，约束表达式将会返回一个明确的“真”和“假”值。Kapur 在他的文章中介绍了基于“约束多项式”的两种不同的求解参数方

程组的方法：参数 Grobner 基方法和参数特征列方法。方法的思路是很直接也是很易懂的：参数多项式进行运算时，通常需要假设其首项的系数（含参数）不为零。通过引入约束多项式，当参数满足约束时，就能够明确判定多项式的首项系数是否为零。当首项系数不能被明确的判定为非零时，我们称这个约束多项式是歧义的；否则成为非歧义的。歧义的约束多项式，通常可以通过增加约束从而变成非歧义的。除此之外，其他的运算步骤与原来的基本算法（Grobner 基和特征列）基本相同。

因此，Kapur 实际上就是在计算 Grobner 基的过程中，讨论每个生成多项式的首项系数是否非零，这个想法是很直接的，但是计算的复杂度仍然较高，缺乏实际应用价值。

2002 年，Montes 提出了一种计算 CGS 的方法，他称之为 Discussing Groebner bases （DISPGB）。该算法的目的是获得所有可能的参数值所对应的不同的 Grobner 基。2004 年，陈等实现了 Kapur 的想法，提出了分区参数 Groebner 基的概念和计算方法。陈等将 CGS 用于机器证明这一领域，提出了一个几何定理机器证明以及自动发现的新方法。

从理论的角度来看，Montes 提出的 DISPGB 和 Kapur 的参数 Groebner 基非常相似的，只是形式略微不同。从效率上来说，上述的这些方法（Weisfenning,Kapur,Montes,陈等）无论是计算 CGB 还是计算 CGS 都不能令人满意。

在 2006 年，Sato 和 Suzuki 提出了一个计算 CGS 的高效算法(SS 算法)。该算法大大的提高了计算 CGS 的效率。在该算法的基础上，他们又提出了一个计算 CGB 的算法。虽然 SS 算法较以前的算法在效率上有了明显的提升，但是 SS 算法还可以被进一步的改进。在这之后，Nabeshima 对 SS 算法进行了优化，然而这一优化并不本质。他们还研究了冯诺依曼正则环下的参数 Grobner 基及相关算法。

我们对 SS 算法进行深入的研究，提出了一个计算参数多项式系统 CGS 的一个快速方法。我们从理论上证明了在计算 CGS 的过程中，一些分支完全是多余的，大大减小了分支数目，避免了冗余计算。我们对参数约束也进行了优化，使得效率得到进一步的提高。我们又进一步提出了一个同时计算 CGS 和 CGB 算法。只要利用我们提出的思想和方法，所有计算 CGS 的算法都可被很自然地推广，用来计算 CGB。

我们的研究结果得到了评审专家的一致好评。西班牙专家 Montes 对我们提出的算法和他自己过去的算法进行了实验和比较，实验数据表明我们的算法比

他自己的算法要有效得多。因此他将我们的算法实现，并嵌入到著名的符号计算软件 Singular (Singular release 3-1-5: grobcov.lib).

代表性成果 2、超指数函数的 Hermite 约化与 Telescoper 计算 (Hermite Reduction and Creative Telescoping for Hyperexponential Functions)（陈绍示、李子明）

上世纪 90 年代，组合数学家 Zeilberger 提出了可以证明一大类组合恒等式的机械化算法。 Zeilberger 算法的核心是对给定的多变元函数 f(t,x), 构造出非平凡的多项式系数的线性微分或差分算子 L(t, Dt) 与满足一定条件的多变元函数 g(t, x) ,使得 L(f) = Dx(g)。算子 L 与函数 g 分别称为 f 的 Telescoper 与 Certificate。该算法已经在许多主要计算机代数系统如 Maple 与 Mathematica 中实现并得到广泛应用。Zeilberger 算法的终止性与效率优化研究已经成为当前符号计算的主要课题之一。

超指数函数是一类满足多项式系数的一阶偏微分方程组的特殊函数。该类函数是有理函数，指数函数，简单根式函数的一种推广。与离散情形的经典超几何项一并称为线性微分或差分方程的闭形式解。1990 年，Almkvist 与 Zeilberger 基于微分 Gosper 算法给出了双变元超指数函数的 Telescoper 的构造算法。这也是通行商业软件中所用的算法。

在 2010 年，我们基于有理函数积分的 Hermite 约化方法，提出了计算双变元有理函数的 Telescoper 的新算法，并且证明了该算法的复杂度比已有的算法低。2013 年，我们首先将有理函数的 Hermite 约化方法推广到了超指数情形。该推广大大简化了超指数函数是否为超指数可积的判定效率。基于推广的 Hermite 约化算法，我们提出了计算双变元超指数函数 Telescoper 的高效算法。

新算法的最大优点是可以把 Telescoper 的计算与 Certificate 的计算分离开来。这在实际应用中非常重要，因为 Certificate 往往存储空间很大可实际又不需要该信息。通过与商业软件 Maple 中的程序对比，我们的算法的效率优于经典的 Almkvist-Zeilberger 算法。

论文发表于 2013 年国际符号与代数计算年会的会议录中。这项工作受到审稿人和与会者的好评。部分审稿意见摘录如下：

审稿意见一："…. While similar reductions have been developed in previous works, the new and remarkable achievement of the present work is the equivalence that H is hyperexponential integrable if and only if its residual form is zero. This result then gives immediately rise to a new creative telescoping algorithm for bivariate hyperexponential functions and to a bound on the order of the minimal telescoper ...."

审稿意见二："I think the paper is nice, in particular in case 4 when the standard complement consists of a sequence of powers with two gaps in them (illustrated in

Example 7), I found that case to be surprisingly interesting. ... it improves the state of the art in telescoping; the fact that a certificate is no longer needed is an important contribution …"

陈绍示简介：

男，实验室 2013 年度新引进助理研究员，获得中科院数学院与法国巴黎 Ecole Polytechnique双博士学位，其后在奥地利RISC研究所和美国北卡州立大学数学系做博士后。主要研究领域为符号分析，被国际著名学者认为是“clearly belongs to the highest ranked mathematicians of his age”，“among the best of his generation in all of Symbolic Computation and certainly **the best** new Ph.D. in the last several years working in the intersection of this field and Combinatorics”，“one of the brightest rising stars in symbolic computations and automatic summation and algorithmic proof theory for special function identities”。他证明了组合学中著名的Wilf-Zeilberger猜想（1992 年提出）。此外，“His new algorithm for definite integration of rational functions is much faster than any previously known method and was received with surprise and astonishment by the scientific community.”

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	257	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	111	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	90	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	5	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	2012	2013	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	2012	2013	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	2012	2013	31.5	31.5	邓映蒲

10.	国家自然科学基金重大项目	“信息处理中的关键数学问题”子课题:网络通信中的多方安全计算和优化设计	2010	2013	35	0	胡磊
11.	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	72	支丽红
12.	国家自然科学基金面上项目	流密码和格密码中相关问题研究	2011	2013	30	0	邓映蒲
13.	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
14.	国家自然科学基金面上项目	复杂非线性物质波系统的外势约束和解析解研究	2011	2013	22	0	闫振亚
15.	国家自然科学基金面上项目	Groebner 基算法及其应用	2014	2017.12	50	25	王定康
16.	国家自然科学青年基金	代数方程组求解与代数曲线曲面的可信计算	2011	2013	16		程进三
17.	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	6.6	袁春明
18.	国家自然科学青年基金	安全多方计算的模型和方法研究	2011	2013	16	0	张志芳
19.	专项基金天元	现代密码设计中的关键数学问题	2014.1	2014.12	18	18	邓映蒲
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			75	25	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			38	19	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			18	9	刘卓军
23.	神华科学技术研究院委托项目	跨国公司大型能源项目情报收集、分析系统研究			7	7	刘卓军
24.	中科院网络中心开放课题	DNS 异常流量检测及抗攻击理论和方法研究	2012	2013	12		刘卓军
25.	国家密码发展基金	序列密码中的若干问题研究	2012	2013	8	4	冯秀涛
26.	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
27.	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
28.	中国科协项目	老科学家学术成长资料采集工程	2010	2013	40		吴天骄
29.	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	13.2	潘彦斌
合计	---	---	---	---	2848	985.8	---

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	NSFC/ANR	代数系统的准确、可信计算	2009	2013	（45 万/30 万欧元）	0	支丽红
2.	法国	INRIA/CNRS	LIAMA 中法实验室项目： ECCA	2010	2014	5 万欧元	0.8 万欧元	支丽红
合计	---	---	---	---	---			---

注：国际合作项目指双方单位正式签订协议书的国际合作科研项目

横向合作及其它项目一览表

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

注：横向协作项目指有正式合同书的项目

国家重点实验室专项经费自主研究课题一览表

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

获奖等重要成果

序号	成果名称	获奖类别	等级	完成人及排序
1.	LTE 序列密码算法的设计与分析	国家技术发明奖	二等奖	冯秀涛 5/6
2.	数控加工中的插补方法	中国科学院数学与系统科学研究院 2013 年度十大科研进展		袁春明、张立先、高小山、李洪波
3.	2013 年度系统所关肇直奖			程进三
4.	中国科学院优秀教师奖			高小山

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 Note on the Diagonal Theorem of Bivariate Rational Formal Power Series (in Chinese)	Acta Mathematica Sinica Chinese Series, 56 (2): 203--210, 2013	Xiaoli Wu, Shaoshi Chen	Shaoshi Chen	
2.	Desingularization Explains Order-Degree Curves for Ore Operators	Proceedings ISSAC'13, pp. 157–164, ACM Press, 2013	Shaoshi Chen, Maximilian Jaroschek, Manuel Kauers, Michael F. Singer	Shaoshi Chen	
3.	Hermite Reduction and Creative Telescoping for Hyperexponential Functions	Proceedings ISSAC'13, pp. 77–84, ACM Press, 2013	Alin Bostan, Shaoshi Chen, Frédéric Chyzak, Ziming Li, Guoce Xin	Shaoshi Chen	
4.	A Generic Position Based Method for Real Root Isolation of Zero-Dimensional Polynomial Systems	Journal of Symbolic Computation, 2013	Cheng, J.-S., Jin, K.	Cheng, J.-S.	
5.	Certified Rational Parametric Approximation of Real Algebraic Space Curves with Local Generic Position Method	Journal of Symbolic Computation, 58 (2013): 18--40	Cheng, J.-S., Jin, K., Lazard, D	Cheng, J.-S.	
6.	Multiplicity Preserving Triangular Set Decomposition of Two Polynomials	Journal of Systems Science and Complexity, 2013	Cheng, J.-S., Gao, X.-S.	Cheng, J.-S.	
7.	Results on permutation symmetric Boolean functions	Journal of Systems Science and Complexity,Vol.26 No.2, 302-312,2013	Yanjuan Zhang, Yingpu Deng	Yingpu Deng	
8.	Cubic Spline Trajectory Generation with Axis Jerk and Tracking Error Constraints	Int J Precis Eng Manuf, 14(7), 1141-1146, 2013	K. Zhang, J.X. Guo, X.S. Gao	X.S.Gao	

9.	Efficient Time Optimal Feedrate Planning under Dynamic Constraints for High-order CNC Servo System	Computer-Aided Design, 45 (2013) 1538-1546	J.X. Guo, K. Zhang, Q. Zhang, X.S. Gao	X.S.Gao	
10.	Intersection Theory in Differential Algebraic Geometry: Generic Intersections and the Differential Chow Form	Trans. Amer. Math. Soc, 365(9), 4575-4632,2013	X.S. Gao, W. Li, C.M. Yuan	X.S.Gao	
11.	Practical smooth minimum time trajectory planning for path following robotic manipulators	Proc. American Control Conference 2103, 17-19, Washington DC, 2013	Q. Zhang, S. Li, X.S. Gao	X.S.Gao	
12.	Time-optimal interpolation for five-axis CNC machining along parametric tool path based on linear programming	Int J Adv Manuf Technol, 69(5), 1373-1388, 2013	W. Fan, X.S. Gao, C.H. Lee, K. Zhang, Q. Zhang	X.S.Gao	
13.	Tracking Error Reduction in CNC Machining by Reshaping the Kinematic Trajectory	J Syst Sci Complex, 26(5), 800-817,2013	J.X. Guo, Q. Zhang, X.S. Gao	X.S.Gao	
14.	Efficient algorithm for time-optimal feedrate planning and smoothing with confined chord error and acceleration	Int J Adv Manuf Technol. 66(9), 1685-1697, 2013	K. Zhang, C.M. Yuan, X.S. Gao	X.S.Gao	
15.	Recollements and Hochschild theory	Journal of Algebra 397 (2014), 535-547	Y. Han	Y. Han	
16.	Topological Classifications of the Intersection Curves of Two Ring Tori	Computer Aided Geometric Design,30,181-198,2013	X. Jia, C. Tu W. Wang	X. Jia	
17.	Using a Bivariate Sparse Resultant to Find the Singularities of Rational Space Curves	Journal of Symbolic Computation, 53,1-25,2013	X. Shi, X. Jia R. Goldman	X. Jia	
18.	Small slopes of Newton polygon of L-function	Journal of Number Theory	Fusheng Leng, Banghe Li	Fusheng Leng	

19.	Quasi-Steady-State Laws in reversible model of enzyme kinetics	J Math Chem (2013) 51:2668–2686.	Bo Li, Banghe Li	Bo Li	
20.	一类 Riemann 张量指标表达式的标准型完全分类及其在微分几何中的应用 s	中国科学: 数学 2013 年第 43 卷第 4 期: 399-408.	刘姜, 李洪波, 张立先	李洪波	
21.	Geometric Error Control in the Parabola-Blending Linear Interpolator	J Syst Sci Complex (2013) 26: 777–798	Hongbo Li, Lixian Zhang	Hongbo Li	
22.	Space cutter radius compensation method for free form surface end milling	International Journal of Advanced Manufacturing Technology, DOI 10.1007/s00170-012-4674-2	Li Han, Xiao-Shan Gao, Hongbo Li	Li Han	
23.	Two Proofs on Max-Min-Max Principle of Jerk Control in Time-Optimal Rectilinear Motion	Mathematics in Computer Science, 2013, Volume 7, Issue 2, 229-236.	Hongbo Li, Lixian Zhang	Hongbo Li	
24.	Sparse Difference Resultant	Proceedings ISSAC'13, pp. 275–282, ACM Press, 2013	W. Li, C.M. Yuan, X.S.Gao	Wei Li	
25.	基于时间序列建模和控制图的异常交易检测方法	数学的实践与认识，2013 年 5 月	刘卓军，李晓明	刘卓军	
26.	Linearized Polynomials over Finite fields revisited	Finite Fields Appl.2(2013) 79-100	B.F.Wu, Z.J.Liu	Zhuojun Liu	
27.	The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2	Finite Fields Appl.24(2013) 136–147	B.F.Wu, Z.J.Liu	Zhuojun Liu	
28.	A Three-Level Sieve Algorithm for the Shortest Vector Problem	Selected Areas in Cryptography 2013（SAC 2013）	Feng Zhang, Yanbin Pan, Gengran Hu	Yanbin Pan	
29.	Improvements on Reductions among Different Variants	The 14th International Workshop on Information Security Applications (WISA2013)	Gengran Hu, Yanbin Pan	Yanbin Pan	

30.	A New Proof for the Correctness of the F5 Algorithm	Science in China,Series A:Mathematics,56(4),745-756,2013	Y. Sun, D.K. Wang	D.K. Wang	
31.	An Efficient Algorithm for Computing a Comprehensive Groebner System of a Parametric Polynomial Systems	Journal of Symbolic Computation,49,27-44,2013	D. Kapur, Y.Sun, D.K. Wang	D. Kapur	
32.	An Efficient Algorithm for Factoring Polynomials over Algebraic Extension Field	Science in China,Series A:Mathematics,56(6),1155-1168,2013	Y. Sun, D.K. Wang	D.K. Wang	
33.	An Efficient Method for Computing Comprehensive Groebner Bases	Journal of Symbolic Computation,52,124-142, 2013	D. Kapur, Y.Sun, D.K. Wang	D.K. Wang	
34.	Complex PT-symmetric nonlinear Schrodinger equation and Burgers equation	Phil. Trans. R. Soc. A 371(2013) 0120059	Zhenya Yan	Zhenya Yan	
35.	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. 2013 (online)	Zhenya Yan	Zhenya Yan	
36.	Optical rogue waves in the generalized inhomogeneous higher-order nonlinear Schrodinger equation with modulating coefficients	Journal of Optics 15(2013) 064012	Zhenya Yan, C. Dai	Zhenya Yan	
37.	Time-optimal interpolation for CNC machining along curved tool pathes with confined chord error	Journal of Systems Science and Complexity, 26, 836-870, 2013	C.M. Yuan, K. Zhang, W. Fan	C.M. Yuan	
38.	Pre-compensation of contour errors in Five-Axis CNC machine tools	International Journal of Machine Tools and Manufacture. 74,1–11, 2013	K. Zhang, A. Yuen, Y. Altintas	K. Zhang	

39.	Smooth trajectory generation for five-axis machine tools	International Journal of Machine Tools and Manufacture. 71,11–19, 2013	A. Yuen, K. Zhang, Y. Altintas	K. Zhang	
40.	Exact cooperative regenerating codes with minimum-repair-bandwidth for distributed storage	IEEE INFOCOM 2013-IEEE Conference on Computer Communications.	Anyu Wang, Zhifang Zhang	Zhifang Zhang	
41.	Rational secret sharing as extensive games	Scinece China Information Sciences,56(3),1-13,2013.	Zhifang Zhang	Zhifang Zhang	
42.	Computing the Nearest Singular Univariate Polynomials with Given Root Multiplicities	Theoretical Computer Science 479, 1, 2013, Pages 150–162	Zijia Li, Lihong Zhi	Lihong Zhi	
43.	Computing rational solutions of linear matrix inequalities	Proceedings ISSAC'13, pp. 197–204, ACM Press, 2013	Qingdong Guo, Mohab Safey El Din, Lihong Zhi	Lihong Zhi	
44.	Verified Error Bounds for Isolated Singular Solutions of Polynomial Systems: Case of Breadth One	Theoretical Computer Science Volume 479, 1, 2013, Pages 163–173	Nan Li, Lihong Zhi	Lihong Zhi	
45.	Verfied error bounds for real solutions of positive-dimensional polynomial systems	Proceedings ISSAC'13, pp. 371–378, ACM Press, 2013	Zhengfeng Yang, Lihong Zhi, Yijun Zhu	Lihong Zhi	
46.	On the Construction of Finite Oscillator Dictionary	Communications in Algebra, Pulishing online	Rongquan Feng, Zhenhua Gu, Zilong Wang, Hongfeng Wu, Kai Zhou	Hongfeng Wu	
47.	Subconstituents of orthogonal graphs of odd characteristic continued	Linear Algebra and its Applications, 439(10), 2861-2877, 2013	Zhenhua Gu, Zhe-XianWan, Kai Zhou	Kai Zhou	

48.	Subconstituents of unitary graphs over finite fields	Linear and Multilinear Algebra, Pulishing online	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	李代数 (第二版)	万哲先	高等教育出版社	2013

出版译著

序号	译作名称	译者	出版单位	出版日期
1.	系统安全必读（System Safety Primer）	刘卓军	美国 Create Space Publisher	2013.03
2.	故障树分析读本（Fault Tree Analysis Primer）	刘卓军	美国 Create Space Publisher	2013.09
3.	高阶逻辑辅助证明系统（A Proof Assistant for HOL）	陈光喜，刘卓军	北京理工大学出版社	2013.05

授权发明专利

序号	专利名称	申请号/专利号	申报/授权	完成人及排序
1.	一种通过计算零维三角多项式系统所有实根及其重数进行曲面绘制的方法和系统	ZL201220005095.2	授权	李家，程进三，高小山
2.	基于 S 曲线加减速控制的多周期拐角小直线段插补方法	201210211398.4	授权	张立先，孙瑞勇，李洪波，高小山
3.	一种序列密码构建方法及密钥流生成方法	201310717039.0	申请	冯秀涛

其它成果（如新医药、新农药、新软件证书（不是著作权登记书）、国家标准等）

五、学术交流

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

举办的国际国内学术会议一览表

序号	会议名称	会议类别	主办单位	会议主席	会议日期	参加人数
1.	2013 年可信计算研讨会	国内	中科院数学院	支丽红	2013.4.19-20	40
2.	第五届全国计算机数学学术会议（CM2013）	国内	中科院数学院	李子明 王定康	2013.8.18-21	130
3.	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”学术交流与汇报会	国内	中科院数学院	高小山	2013.9.27-29	40
4.	计算机辅助制造、工程与数控中的数学与算法国际会议	国际	中科院数学院	李洪波	2013.10.24-25	60
5.	973 项目“数学机械化方法及其在数字化设计制造中的应用”学术交流与汇报会	国内	中科院数学院	高小山	2013.11.29-30	70
6.	数学机械化战略研讨会	国内	中科院数学院	李洪波	2013.12.19	70

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.	Desingularization Explains Order-Degree Curves for Ore Operators	陈绍示	The 38th International Symposium on Symbolic and Algebraic Computation(ISSAC2013)	美国	2013.06
2.	Residues and Telescopers for Hyperexponential Functions	陈绍示	第五届全国计算机数学学术会议（CM2013）	长春	2013.08
3.	A New Criterion for the Existence of Real Zeros of Polynomial Systems	程进三	Applications of Computer Algebra（ACA）	西班牙	2013.07
4.	Isotopic e-Meshing of Real Algebraic Space Curves	程进三	第五届全国计算机数学学术会议（CM2013）	长春	2013.08
5.	素数判定	邓映蒲	中国密码学会密码数学理论专委会 2013 年学术研讨会	天津	2013.08
6.	素数判定	邓映蒲	第五届全国计算机数学学术会议（CM2013）	长春	2013.08
7.	序列密码算法安全（邀请报告）	冯秀涛	2013 第九届中国网络科学论坛	北京	2013.04
8.	关于有限域上迹逆函数的代数免疫度（邀请报告）	冯秀涛	2013 密码数学理论学术研讨会	天津	2013.08
9.	Sparse Differential Resultant	高小山	International Conference on Differential Algebra and Related Areas, Lille France, June 2013	法国	2013.06

10.	Efficient Time Optimal Interpolation for CNC Machining	高小山	数控技术研讨会与论坛，台中，12 月 5 日，2013	台湾	2013.12
11.	Time Optimal Interpolation for CNC Machining	高小山	中科院国家数学交叉中心-香港中文大学研讨会, 11 月 12 日，香港中文大学，2013	香港	2013.11
12.	A proof of extension conjecture （邀请报告）	韩阳	The fourth Hochschild cohomology conference	阿根廷	2013.08
13.		黄雷	第五届全国计算机数学学术会议（CM2013）	长春	2013.08
14.		黄雷	3rd International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control	北京	2013.10
15.	Estimation and Control of the Geometric Error in a Linear Interpolator with Parabola Blending	李洪波	ASME 2013 International Mechanical Engineering Congress & Exposition	美国	2013.11
16.	Sparse Difference Resultant	李 伟	The 38th International Symposium on Symbolic and Algebraic Computation(ISSAC2013)	美国	2013.06
17.	Hermite Reduction and Creative Telescoping for Hyperexponential Functions	李子明	The 38th International Symposium on Symbolic and Algebraic Computation(ISSAC2013)	美国	2013.06
18.	Computing Decompositions for Hypergeometric Terms （邀请报告）	李子明	Conference on Applied Algebraic Geometry	美国	2013.08
19.		刘卓军	31th International System Safety Conference	美国	2013.08

20.	R-LWE 的一个经典约化	刘卓军	第五届全国计算机数学学术会议（CM2013）	长春	2013.08
21.	用 BHTA-copula 方法研究中医体质网络关系	刘卓军	世界中医药学联合会体质专业委员会第 2 届学术年会	广州	2013.08
22.	基于 BHTA - copula 方法的中医体质网络构建与关键节点的挖掘	刘卓军	第 15 届中国管理科学学术年会	长沙	2013.10
23.	An Efficient Algorithm for Computing Branch Groebner Systems and Its Applications in Algebraic Cryptanalysis	王定康	Applications of Computer Algebra（ACA）	西班牙	2013.07
24.	Sparse differential and difference resultant（邀请报告）	袁春明	Differential Algebra and Related Topics V (DART V)	法国	2013.06
25.	数控数据距离可控的二次 B 样条曲线拟合	袁春明	第五届全国计算机数学学术会议（CM2013）	长春	2013.08
26.	Approximate NC Data with Quadratic Splines under Confined Error	袁春明	3rd International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control	北京	2013.10
27.	Exact cooperative regenerating codes with minimum-repair-bandwidth for distributed storage	张志芳	IEEE INFOCOM 2013-IEEE Conference on Computer Communications	意大利	2013.04

28.	Node Repair in Distributed Storage Systems	张志芳	全国编码与密码数学理论研讨会	湖南	2013.06
29.	Computing rational solutions of linear matrix inequalitie	支丽红	The 38th International Symposium on Symbolic and Algebraic Computation(ISSAC2013)	美国	2013.06
30.	Verfied error bounds for real solutions of positive-dimensional polynomial systems	支丽红	The 38th International Symposium on Symbolic and Algebraic Computation(ISSAC2013)	美国	2013.06

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.	数控系统的最优控制方法	2013.5	2013.12	1	1	李树荣	王定康
2.	非线性数学物理方程的数学机械化方法研究及应用	2013.5	2013.12	1	1	谢福鼎	闫振亚

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）
合计	---	---	---			

大型仪器设备的开放、共享及成效。

七、实验室大事记

1、2013 年 1 月 16 日， 中国科学院院长白春礼一行看望我院资深院士吴文俊先生，向吴先生致以新春的问候并亲切询问了他的身体和工作情况，对他为我国数学界做出的卓越贡献表示由衷敬意。94 岁高龄的吴先生精神依然矍铄，话语间充满爽朗的笑声。吴先生对领导的关心表示感谢。数学院的执行院长王跃飞， 副院长高小山也一同看望。

2、全国政协副主席、科技部部长万钢亲切看望了国家最高科学技术奖获奖者吴文俊院士和徐光宪院士。

2013 年 2 月 6 日下午，万钢部长来到 2000 年度国家最高科学技术奖获奖者吴文俊院士家中，代表科技部向吴院士拜年并致以新春祝福，感谢他在拓扑学和数学机械化领域做出的卓越贡献。吴院士对科技部在拓扑学和数学机械化领域的长期支持表示感谢，并就数学机械化的发展、人才培养等问题与万部长进行了交流探讨。万部长就全国科技工作情况和基础研究工作的进展与吴院士进行了交流，叮嘱吴院士要保重身体，并希望吴院士对科技工作多提宝贵意见。

离开吴文俊院士家，万钢部长又来到 2008 年度国家最高科学技术奖获奖者徐光宪院士家中，代表科技部对徐院士表示问候并致以新春祝福，感谢他对我国稀土化学事业所做的巨大贡献，并与徐院士及其学生就全国科技工作情况，特别是稀土材料化学的研究发展问题进行了交流。临离开徐院士家，万部长叮嘱徐院士要保重身体，并希望徐院士对科技工作多提宝贵意见。

国家科学技术奖励工作办公室邹大挺主任、张木副主任及有关单位领导等一起陪同看望。

3、在美国波士顿召开的第 38 届国际符号和代数计算会议(ACM ISSAC'13)上，本实验室有 4 篇论文被接收。ISSAC 是符号和代数计算方面最权威的国际会议。4 篇被接收论文是：

1) Qingdong Guo, Mohab Safey El Din, Lihong Zhi. Computing rational solutions of linear matrix inequalities.

2) Zhengfeng Yang, Lihong Zhi, Yijun Zhu. Verified Error Bounds for Real Solutions of Positive-dimensional Polynomial Systems.

3) Wei Li, Chun-Ming Yuan and Xiao-Shan Gao. Sparse Difference Resultant.

4) Alin Bostan, Shaoshi Chen, Frederic Chyzak, Ziming Li, Guoce Xin. Hermite Reduction and Creative Telescoping for Hyperexponential Functions.

实验室博士生郭庆东获 2013 年度 ISSAC 最佳学生论文奖。文章给出了线性矩阵不等式定义的凸集上有理点的存在性判定和计算。

4、中国科学院数学机械化重点实验室第三届学术委员会第四次会议于 2013 年 3 月 22 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、张景中院士、林惠民院士等 10 多位实验室学术委员会成员参加了会议。中科院基础局数学物理处王永祥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 2012 年度数学机械化重点实验室工作进展情况，指出实验室在过去一年里科研工作稳步提高，取得多项重要成果；数学机械化重点实验室主持的国家基础研究发展计划（973）项目“数学机械化方法及其在数字化设计制造中的应用”中期评估顺利通过；实验室组织召开了多次国际和国内会议，如：中法微分方程国际研讨会，第五届有限域及其应用国际研讨会，基于混合计算的误差可控算法研讨会，计算机辅助制造工程和数控中的数学与算法国际会议，第十届亚洲计算机数学会议，构造性微分代数研讨会等。随后李子明、冯秀涛分别作了代表性工作的学术报告。

在听完汇报后，与会专家们提出了多项具有建设性的意见。冯克勤教授认为实验室信息安全密码方面的工作做的比较好，有很多研究方向都很热门，许多科研人员的工作走在了世界前列，特别指出了实验室的研究课题“分布式存储”目前在国际上很流行，希望实验室可以保持这个势头，继续努力。

张景中院士肯定了目前实验室的研究水平，认为实验室研究成果突出，理论水平较之以前有显著的提高，得到了国内外同行的认可。他同时指出，之前实

验室的软件工作还需要继续，目前实验室还没有形成一个可以与大家共享的平台，这也是我们与国际上的差距。

李华研究员首先肯定了实验室在 2012 年取得的成绩，接着就开发软件平台给出了建议。李华研究员有着丰富的计算机软件开发经验，认为想要做出一个成熟的软件平台，需要投入大量的人力、物力、财力，需要各方面的协调讨论，需要有数学机械化背景的计算机人才等等。

王永祥处长指出目前实验室数学机械化和信息安全方面理论做的好，算法做的好，接下来需要进一步考虑开发软件平台，这样才更具有优势，同时对实验室购买的五轴联动数控机床的安置存放和维护给出了办法。

5、 2013 年可信计算研讨会于 4 月 19 日-20 日在北京西郊宾馆举办。会议邀请了中国科学院软件所、中国科学院数学与系统科学院研究院、清华大学、北京大学、华东师范大学、中国科学院成都计算所、中国科学院重庆研究院、北京应用物理与计算数学研究所等单位的 40 余名老师和研究生参加。会议由中国科学院数学与系统科学研究院支丽红研究员发起组织，会议得到 973 项目“数学机械化方法及其在数字化设计制造中的应用”和自然基金委基于符号-数值混合计算的误差可控算法及应用项目的支持。

此次会议促进了可信计算领域各科研单位之间的交流与合作。为参会人员提供展示原创性研究结果，了解可信计算的最新进展，交换想法与观点的一个平台。

6、2013 年 7 月 18 日上午，国家自然科学基金委杨卫主任一行来到吴文俊院士家中看望这位为数学发展做出巨大贡献的 94 岁高龄科学家。杨卫主任就国家自然科学基金如何引领和支持我国数学研究的发展，听取了吴文俊院士的意见和建议。吴先生回顾了中国数学的发展历程，谈到在上世纪 80 年代，吴先生同陈省身先生、北京大学程民德先生、南开大学胡国定先生一起，积极促进设立数学天

元基金，谋划数学学科的发展。他还十分关心当今中国数学的发展和人才培养问题。

7、第五届全国计算机数学学术会议（CM2013）于 8 月 18 日至 21 日在吉林长春名人酒店召开，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。 会议期间，大连理工大学大学徐利治教授做了题为“介绍一个公式类一• -△类”、大连理工大学王仁宏教授做了题为“分片代数簇中的一些论题”、澳门科技大学齐东旭教授做了题为“On the Problem of Global Grid Systems”、中国科学院数学与系统科学研究院段海豹研究员做了题为“Schubert calculus and cohomologies of Lie groups”、美国 State University of New York at Stony Brook, 顾险峰做了题为“Computational Conformal Geometry: Theory, Algorithm and Applications”的邀请报告。此外，会议还安排了 45 位研究人员在本次会议的分组会议上做了学术报告，并举行了关于计算机教育的专题研讨会。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，吉林大学数学学院和中国科学院数学机械化重点实验室承办。

8、国家数学与交叉科学中心交叉学术论坛暨 2013 年计算机辅助制造、工程与数控中的数学与算法国际会议（MAMENC2013）于 2013 年 10 月 24-25 日在中国科学院数学与系统科学研究院召开。会议邀请了土耳其、法国、意大利、加拿大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、南京航空航天大学等单位的 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。加拿大英属哥伦比亚大学（University of British Columbia）的 Hsi-Yung Feng 教授，土耳其科奇大学（Koc University）的 Ismail Lazoglu 教授，华中科技大学的 Chen-Han Lee 教授，法国卡尚高等师范学校自动化生产研究高校实验室（ENS Cachan – LURPA）的 Sylvain Lavernhe 副教授，加拿大麦克马斯特大学（McMaster University）的 Allan D.Spence 副教授，意大利帕尔马大学（University of Parma）的 Corrado Guarino Lo Bianco 副教授等分别做了各自研究领域的大会报告。

“数学与交叉科学学术论坛”由中科院国家数学与交叉科学中心（NCMIS）发

起主办，分别由中心 6 个交叉研究部结合自身特色根据不同主题承办。论坛旨在面对自然科学、工程技术与社会经济等应用领域对数学的需求，共同探讨实际应用领域重要问题对数学的需要，以期共同推动问题驱动的应用数学与交叉科学的的研究与发展，推动实际领域重要问题的解决。

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三次举办，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。

9、973 项目“数学机械化方法及其在数字化设计制造中的应用”学术交流与汇报会于 2013 年 11 月 29 日-30 日在中国科学院数学与系统科学研究院召开。科技部基础研究管理中心辛圣炜博士，项目专家组成员熊有伦院士，项目咨询专家强文义教授等出席了会议，项目组成员及研究生 70 余人参加了会议。

科技部基础研究管理中心辛圣炜博士介绍了 973 项目相关情况、年终总结的意义以及应该注意的问题，建议各项目组组长及成员在汇报时，着重汇报课题间的协作工作、课题对项目整体目标的贡献、课题解决的科学问题等方面的工作。973 项目在验收时需要提交科普文章以及科技报告。最后辛圣炜博士希望专家以及项目成员多提建设性的意见、建议。项目首席科学家高小山研究员介绍了项目的整体情况，四个课题组长分别汇报了各自课题的总体情况。随后项目成员分别汇报了一年来的进展。

本项目成员 2013 年在微分差分方程符号求解理论与算法、构造性代数几何、基于混合计算的误差可控算法、密码分析、复杂数字曲面几何特征识别、曲面造型理论、5 轴数控加工中的轨迹规划、5 轴数控系统中的最优插补、高档数控系统核心模块等方面取得重要进展。发表论文 100 余篇，新授权发明专利 5 项，新申请发明专利 13 项，获得国家技术发明二等奖、第十四届陈省身数学奖、公安部科学技术二等奖、ACM/SIGSAM “ISSAC”最佳学生论文奖等重要奖励，圆满完成了计划任务。