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。今天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，也为很多高科技问题的解决提供了有力的工具。我们的方法已在许多高科技领域获得了一批理论成果，具备了解决尖端技术产业中实际问题的条件。包括曲面造型，机器人位置分析，几何设计，计算机视觉，智能ＣＡＤ，信息安全和数字图象的高速高保真传输。通过进一步努力，这些理论研究成果有望能够实实在在地解决若干项技术问题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-Massy 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	
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、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		副研究员	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		所聘副研	符号计算	研究
18.	程进三	男	1976.8		所聘副研	符号计算	研究
19.	冷福生	男	1980.5		助研	代数数论	研究
20.	周　凯	男	1981.9		助研	代数、编码	研究
21.	冯秀涛	男	1978.8		助研	信息安全	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.	张立先	女	1982.10		项目助研	高档数控	研究
27.	李　伟	女	1985.9		项目助研	微分代数几何	研究
28.	吴天骄	男	1959.9		工程师		技术
29.	周代珍	女	1965.3		秘书		管理
30.	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、2010
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	2011	2016
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	2012
10.	李洪波	中国数学会计算机数学专业委员会	副主任	2012	2016
11.	李子明	中国数学会计算机数学专业委员会	主任	2012	2016
12.	李子明	中国数学会	理事	2012	2016
13.	李子明	ACM SIGSAM	顾问	2010	2015
14.	王定康	中国数学会计算机数学专业委员会	秘书长	2010	2013
15.	支丽红	国际符号与数值混合计算指导委员会	委员	2004	2014
16.	支丽红	ISSAC 指导委员会	委员	2011	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》**	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》**	副主编		
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	**《系统科学与数学》**	编委		
24.	李洪波	**《系统科学与数学》**	编委		
25.	李洪波	**《Advances in Applied Clifford Algebras》**	编委		
26.	李子明	**《Journal of Symbolic Computation》**	编委		
27.	李子明	**《Journal of Systems Science and Complexity》**	编委		
28.	支丽红	**《Journal of Symbolic Computation》**	编委		
29.	支丽红	**《Mathematics in Computer Science》**	编委		
30.	支丽红	**《ACM Communications in Computer Algebra》**	编委		
31.	闫振亚	**《Abstract and Applied Analysis》**	编委		
32.	闫振亚	**《Journal of Engineering and Applied Science》**	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.	王定康	王继斌		
4.	闫振亚	岳志强		
5.	李子明	康　劲		
6.	李子明	黄　辉		
7.	闫振亚	温子超		
8.	支丽红	王　础		
9.	万哲先，邓映蒲	张　凡		
10.	万哲先	刘仁章		
11.	李洪波	邵长鹏		
12.	李洪波	文　勇		
13.	王定康	张　熠		
14.	万哲先	杨江帅		
15.	邓映蒲	廖茂东		
16.	支丽红	郝志伟		
17.	王定康	张文哲		
18.	邓映蒲	王　慧		
19.	冯如勇	熊纯文		
20.	韩　阳	张凝鹛		

21.	高小山	荆瑞娟		
22.	高小山	黄　章		
23.	高小山	赵明勇		
24.	高小山	王　杰		
25.	闫振亚	闫方驰		
26.	万哲先		孙志强	
27.	李洪波		李　阁	
28.	高小山		郭建新	
29.	高小山		闵　程	
30.	支丽红		郭庆东	
31.	刘卓军		张晓明	
32.	黄民强，邓映蒲		张　凤	
33.	吴文俊		金　凯	
34.	刘卓军		李晓明	
35.	李邦河		吴小胜	
36.	高小山		李　伟	
37.	支丽红		郭　峰	
38.	李洪波		刘元杰	
39.	李子明		付国锋	
40.	王定康		樊　伟	
41.	高小山		郭磊磊	
42.	支丽红		马　玥	
43.	刘卓军		柳　刚	
44.	刘卓军		靳庆芳	
45.	刘卓军		戴照鹏	

46.	支丽红		李　楠	
47.	支丽红		李子佳	
48.	高小山		张　可	
49.	韩　阳		陈　慧	
50.	李洪波		姚守彬	
51.	刘卓军		吴保峰	
52.	王定康		马晓栋	
53.	邓映蒲		姜宇鹏	
54.	闫振亚		姜东梅	
55.	刘卓军		黄　冲	
56.	韩　阳		章　超	
57.	高小山		祝　炜	
58.	李洪波		刘　越	
59.	黄民强		胡耿然	
60.	胡　磊		吕　昌	
61.	万哲先		王安宇	
62.	刘卓军		王　晗	
63.	李洪波		王立波	
64.	高小山，冯如勇		李应弘	
65.	黄民强，邓映蒲		黄丹丹	
66.	韩　阳		秦永云	
67.	吴文俊，王定康		周　洁	
68.	高小山			张智勇
69.	支丽红			梁　野
70.	支丽红			李　喆

71.	闫振亚，李洪波			于发军

毕业研究生一览表

序号	姓名	学位	导师姓名	毕业时间
1.	张智勇	博士后	高小山	
2.	吴小胜	博士	李邦河	
3.	李　伟	博士	高小山	
4.	郭　峰	博士	支丽红	
5.	付国锋	博士	李子明	
6.	郭磊磊	博士	高小山	
7.	樊　伟	博士	王定康	
8.	刘元杰	博士	李洪波	
9.	戴照鹏	博士	刘卓军	
10.	马　玥	博士	支丽红	
11.	靳庆芳	博士	刘卓军	
12.	柳　钢	博士	刘卓军	
13.	王继斌	硕士	王定康	
14.	岳志强	硕士	闫振亚	
15.	康　劲	硕士	李子明	

研究生获奖一览表

序号	获奖名称	获奖人员	指导教师
1.	中国科学院普巴奖学金一等奖	李　伟	高小山
2.	中国科学院普巴奖学金三等奖	马　玥	支丽红
3.	中国科学院院长优秀奖	李　伟	高小山
4.	中国科学院永安期货奖学金优秀奖	付国锋	李子明
5.	中国科学院永安期货奖学金优秀奖	吴小胜	李邦河
6.	中国科学院博时奖学金	李　楠	支丽红
7.	中科院数学院院长奖学金优秀奖	李　楠	支丽红
8.	中科院数学院院长奖学金优秀奖	吴保峰	刘卓军
9.	中科院数学院院长奖学金优秀奖	姜宇鹏	邓映蒲
10.	中国科学院研究生院三好学生	马　玥	支丽红
11.	中国科学院研究生院三好学生	岳志强	闫振亚

12.	中国科学院研究生院三好学生	李　楠	支丽红
13.	中国科学院研究生院三好学生	刘　琦	支丽红
14.	中国科学院研究生院三好学生	张晓明	刘卓军
15.	中国科学院研究生院三好学生	闵　程	高小山
16.	中国科学院研究生院三好学生	樊　伟	王定康
17.	中国科学院研究生院优秀学生干部	付国锋	李子明

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 3 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。

1、符号分析与微分代数几何：

（1.1）线性微分算子（李子明）：

很多特殊函数可以通过线性微分方程和初值条件唯一确定和表示。在这种表示下，函数的加法对应于线性微分算子的最小左公倍式。我们完成线性微分算子最小左公倍式的快速计算的工作，给出了估计最小左公倍式阶数和系数次数的最优界，设计了新的计算最小左公倍式的算法。相关结果发表于 2012 年国际符号与代数计算年会的会议录中。

（1.2）超几何函数（李子明、冯如勇）：

Zeilberger 算法的终止性等价于 Telscoper 的存在性。关于二元超指数函数，二元超几何项和 q-超几何项，Telescoper 的存在的必要充分条件是已知的。我们初步完成了微分-差分和 q-差分情形下，混合超几何项 Telescoper 存在性的判定的的充分必要条件。

Ore-Sato 结构定理给出了超几何函数的结构，即超几何函数可以写成有理函数以及一些阶乘项的乘积。我们将这一结果推广到 q-超几何函数。我们证明了在可驯的混合情形下，任一 q-超几何函数都可以写成有理函数与 q-阶乘项的

乘积，并且进一步刻画了 q-阶乘项的结构。

（1.3）多元多项式的函数分解（冯如勇）：

由于多元多项式的函数分解是 NP 难问题，它可被用于构造一类公开密钥。Ye, Dai 以及 Lam 等人在 1999 年提出了基于微分以及齐次化的方法对多元多项式进行函数分解。Faugere 以及 Perret 等人随后进一步发展了该方法。Ye 等人的方法假设对于大多数情形，因子可以从微分所得的多项式经过线性组合恢复出来。Ye 等人在文章中提出了这一假设但未能证明。我们证明了 Ye 等人提出的猜测，并且为他们的方法提供了严格的数学证明。同时我们还证明在一般情形下，非齐次多元多项式的分解可以从它的齐次化多项式的分解中得到。

（1.4）微分结式与微分稀疏结式（李伟、袁春明、高小山）：

我们在微分结式理论的基础上建立了微分稀疏结式的理论，同时给出了计算微分稀疏结式的高效算法。我们给出了微分稀疏结式存在的充分必要条件，证明了微分稀疏结式具有类似于微分结式的性质，比如分次齐次性、Poisson 类型的分解公式等。同时，还给出了稀疏微分结式的阶及次数界的估计，以此为基础给出了计算稀疏微分结式的单指数算法。

接着这一工作，我们研究了 Laurent 微分多项式系统的稀疏结式，给出了 Laurent 微分多项式系统结式存在的充要条件，并给出了一个仅依赖于多项式支集的矩阵判别方法。通过研究稀疏微分结式的基本性质，得到了结式表达式中多项式的阶数与次数界。特别地，我们给出了稀疏微分结式关于阶数的 Jacobi 界。基于这些界，我们给出了计算稀疏微分结式的关于输入规模的单指数复杂度算法。

微分结式的矩阵表示可以极大地简化结式的表达与计算。我们考虑了两个任意次数的一阶单变元微分多项式的结式的矩阵表示问题，证明了基于我们方法构作的矩阵是非奇异的，微分结式则是所构作矩阵行列式的非零因子。通过结合代数稀疏结式的方法，我们进一步证明了在一阶单变元情形，微分结式是代数稀疏结式的非零因子。

我们将上述理论推广到差分情形，除证明了稀疏差分结式具有类似于稀疏微分结式的性质，特别还证明了差分结式具有明显优于微分结式的一些性质，例如差分结式的精确次数是 BKK 数，差分结式可以表示成两个矩阵行列式的比值等。

2、计算代数几何及相关研究：

（2.1）四元数多项式环的定义理想和标准型（李洪波、黄雷）：

由四元数变量通过四元数乘法生成的多项式是最简单的结合但非交换多项式的例子之一；关于这种多项式的约化、分解在三维欧氏几何符号计算中有重要意义。本工作提出并证明了纯虚四元数变元生成的四元数多项式环的生成理想，经计算猜测该理想 Groebner 基的一般形式，之后给出证明。作为自然结果，得到了四元数多项式的标准型的一般形式。

以上结果并不限于四元数本身，适用于三维空间上的多数几何代数。这一工作开启了三维空间上的高级几何不变量代数的标准型计算、除法和公因式理论研究的大门。对于张量代数中的理想的 Groebner 基计算的经典算法，我们也做了改进。

（2.2）代数表示论中的 No loop conjecture（韩阳）：

No loop conjecture 说的是整体维数有限的代数一定没有 loop。我们研究了高阶完备版本的 No loop conjecture，引入了代数的截面循环的概念，证明了整体维数有限的代数一定没有2-截面循环，更强地，有2-截面循环的代数其 Hochschild 同调维数无限。证明了 monomial 代数整体维数有限当且仅当其 Hochschild 同调维数有限，当且仅当代数无截面循环。

（2.3）曲线的奇点计算（贾晓红）：

空间有理曲线的奇异点计算是 CAGD 中的重要问题。已有方法局限于将空间曲线投影至多个平面的方法，易产生冗余结果且效率较低，难以提供可靠的理论保障。仅就曲线上基本奇异点的计算而言，已有的算法多为数值检测方法，其准确性易受曲线局部拓扑与几何情况的干扰。关于这些基本奇异点附近奇点树的展开，长期以来仅有代数几何领域的理论分析，而无 CAGD 领域人员开发出的实际算法。

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。我们通过曲线的 mu 基构造了两个双变元多项式。原曲线上奇异点的所有信息, 包括位置及重数全部转化到新构造的两个平面代数曲线的交点上。我们由此提出了快速展开平面有理曲线上奇点树的符号算法，该算法不产生冗余信息，不仅计算出曲线的基本奇点，也展开了每个奇点邻域的所有无限接近奇点。该方法不产生冗余结果，且有完整的理论保障。

（2.4）零维理想的多项式表示与可解多项式代数上的 Groebner 基（王定康）：

多项式方程求解的方法有很多种，其中 0 维系统的有理表示是一种有效和常用的方法。我们给出了一种计算 0 维理想的多项式的有效算法，也就是给出了 0 维理想的一种同构关系的构造方法。

对可解多项式代数，提出了基于签名的 Groebner 基算法，将基于签名的 Groenber 算法推广到非交换情形。提出了去除多余 S-对的准则，除去了几乎所有多余的 S-对，从而极大的提高了算法的效率。对基于签名的 Groebner 基的算法终止性进行了研究，说明了算法的终止性不依赖于 S-对的选取顺序，而已知的算法终止性都依赖于 S-对的处理顺序。

3、混合计算与 CAGD：

（3.1）非线性系统在孤立重根处的局部对偶空间基底（支丽红）：

提出了一种快速计算非线性系统在孤立重根处的局部对偶空间基底的新算法。该算法适用于最普遍的宽度为 1 的重根，即系统在重根处的 Jacobian 矩阵的列亏秩为 1 的情形。新算法的自由度只是变量的个数减 1，且矩阵大小与重根的重数无关，所以在存储空间和计算速度上都大大优于之前的算法；文章被国际符号计算杂志 JSC 接收，审稿意见指出文章中的算法十分简单并且可能是相同输出条件下在计算时间和存储空间上是效率最高的(the most efficient)。

新算法与规则化的 Newton 迭代相结合，对于宽度为 1 的近似重根， 构造出了基于近似重根局部结构的近似根的精化算法，并且证明了新的近似重根的精化算法的二次收敛性。新算法中矩阵规模与系统在重根处的 Jacobian 矩阵一致，是 Newton 法在近似重根处的推广。文章发表在 SIAM 数值分析杂志 SIAM Journal on Numerical Analysis。

我们还对已有的延拓方法精化重根的算法做了进一步的改进，新的算法能处理的多项式系统的规模更大，并且效率更高，并且与区间计算相结合，给出了奇异根的扰动范围的可信验证。文章被国际理论计算机杂志 Theoretic Computer Science 接受。

（3.2）多元多项式的下确界（支丽红）：

计算多元多项式 f 在由一组多项式等式限制条件定义的可行域上的下确界。

假设可行域是光滑等维的，并且由等式限制条件中的多项式定义的理想是根理想，我们构造了一组多项式集合及其相应的截断代数簇，证明在一般坐标系下，多项式 f 在可行域上正定当且仅当在构造的每一个截断代数簇上，该多项式等价于多项式平方和，因此对于 f 的下界有基于半正定规划(SDP)的代数验证。

为降低问题的规模，我们还研究如何减少添加的多项式限制条件的个数。通过引入新的变量，我们的方法还可以用于求解带不等式约束条件的多项式优化问题。与同类方法相比较，我们的新方法对可行域的假设条件更弱且不要求下确界可以达到。我们利用问题稀疏性解决多项式全局优化问题中下确界为渐近值时发生的数值问题。

我们结合广义临界值和多项式平方和理论，给出带限制条件的求解多项式最优值的方法。该方法不要求多项式必须达到最优值，与同类方法比较，我们的方法计算更为简单，且不需要较强的假设条件。研究了 Hilbert-Artin 有理表示问题的不可行验证，论文被在法国举行的第 37 届国际符号和代数计算会议(ISSAC'12) 接收。

（3.3）多项式系统实根求解（支丽红、程进三）：

研究了将多项式系统实根求解的问题转化为矩量矩阵核范数极小化问题，并利用半正定低秩矩阵恢复 AFPC-BB 算法求解。我们给出了算法完整的收敛性分析和在 Maple 和 Matlab 中的实现(MMCRSolver)。如果多项式系统有无穷多个实根，MMCRSolver 仍能求出其中部分孤立实点或是在代数流形上的实点。

我们提出局部一般位置方法，将一般的零维多项式系统的根的每个坐标表示为一些单变元多项式的根的线性组合。与现有的著名的 RUR（有理单变元）相比，我们的 LUR（线性单变元表达）的主要优势是在精度控制上。最多需要做一个精炼就可以达到所要求的精度。而这是 RUR 所做不到的。我们运用局部一般位置方法，给出了 0 维三角列多项式系统根的线性单变元表达，同时也给出了根的重数。

（3.4）曲线、曲面求交（贾晓红、程进三）：

圆纹面因其特殊良好的几何性质，已经逐渐成为建筑几何、几何建模中的重要元素。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。我们的算法最终仅归结于确定两个四次单变元多项式的根的个数，十分简洁高效。文章已发表于 CAGD 上。我们还完成了 cyclide 曲面 mu 基性质的研究，及由任意 cyclide 隐式表达计算其 mu 基的算法。

低次代数曲面经常被用于几何建模中，低次代数曲面的碰撞检测也广泛应用于机器人、计算机动画、游戏及粒子碰撞中。我们继过去二次曲面的连续碰撞检测的工作后，提出了两个连续变换下的二次曲面的交线拓扑的变化检测。我们首先通过某些矩阵 jordan 标准型变化的检测，来提取交线拓扑变化的时间点。这些时间点将时间轴分为若干连续区域，我们继而通过 Segre characteristic 和 index sequence 两个指标确定每个时间区域内交线的具体拓扑。据我们了解，这是首次将碰撞检测问题深化至交线拓扑变化问题的研究结果。

我们针对一类特殊的求交问题：两曲面中一个可以容易隐式化，给出了确定两个曲面交线的确定性算法，相关文章在 CAGD 发表。

（3.5）空间曲线的可信逼近（高小山、袁春明）：

将参数代数曲线转换为隐式形式是计算机辅助设计中的重要研究问题。本文提出一个算法可用三次 B 样条曲线可信逼近给定的参数空间曲线。这里，可信逼近是指逼近曲线与原曲线具有相同的几何特性如拓扑、奇异点等，还可以任意逼近原曲线。由于空间三次曲线具有良好的性质，该逼近算法为空间参数曲线的隐式化提供了一种切实可行的算法。我们提出了一种新的优化方法来选择三次有理 Bezier 曲线的权重，并证明了我们给出的方法通过细分可以收敛到原曲线。实验结果表明，用我们的方法近似空间曲线，可以用很少的三次 Bezier 曲线段来得到高精度的逼近。这一工作发表在 CAGD 上。

4、密码与编码：

（4.1）关于 NTRU 的广播攻击（潘彦斌，邓映蒲）：

对公钥体制的广播攻击是1988年首先由 Hastad 提出来的。Plantard 和 Susilo 则于2009年首先考虑了针对格密码体制的广播攻击，但他们的攻击对 NTRU 体制却不起作用。NTRU 是公认的目前最有效的公钥体制之一，同时也是 IEEE 1363.1标准和金融服务业 x9标准。NTRU 是唯一实用的可抵抗量子攻击的公钥密码体制。

广播攻击是一种较弱的攻击方式，它容许发送者同时把一个消息发送给多人。通过引入线性化的思想，我们首先提出了针对 NTRU 的有效的成功的广播攻击，证明了 NTRU 在广播环境中的直接应用存在重大安全问题。在此基础上，通过对 NTRU 体制循环结构的利用，我们进一步改进了该攻击，大大降低了其时间复杂性。我们的攻击是第一个成功的针对 NTRU 的广播攻击，以前对 NTRU

没有成功的广播攻击。我们的攻击算法是多项式时间的，这揭露了 NTRU 在这种攻击模式下的某种弱点。

（4.2）针对流密码 A2U2 的实时恢复密钥攻击（冯秀涛）：

A2U2是由丹麦学者 D. Mathieu、C. Damith 和 L. Torben 等人2011年提出的一个轻量级流密码算法，拟用于 RFID 电子标签加密。我们在已知明文攻击模型下给出了针对该算法的一个实时密钥恢复攻击方法，在个人 PC 上只需数秒钟便可以恢复出全部种子密钥，从而彻底破解了该算法。

（4.3）分布式存储系统的编码理论和方法（张志芳）：

分布式数据存储是分布式计算的基础，也是数据管理发展的趋势。当前热门的云存储、网盘服务等都是分布式存储的具体应用。我们这方面主要成果是：构造出第一个一般参数条件下最小带宽的合作再生码。

再生码是 2007 年基于网络编码理论的发展而提出的一种新的分布式存储编码方法，它的主要特点是能够使节点修复时的带宽达到最小。2010 年提出了面对多节点失效时的合作修复模式。随后，具有最小带宽的合作再生码仅在参数 n=d+r 并且 d=k 的条件下给出，这在实际使用中是相当受限的。我们利用双变元多项式插值的技巧，通过在消息矩阵的两边同时使用 MDS 性质，突破了先前的限制条件，得到的构造在一般参数值 n,k,d,r 下都达到最小修复带宽。同时，我们分析了这一类码的线性空间结构，进而证明了它们不能做到最优访问的修复。

5、有限域理论：

（5.1）有限域方程求解的特征列方法（高小山）：

我们将方程求解的吴特征列算法推广到了有限域情形，得到了高效的有限域方程求解算法，并通过这个算法能精确地给出零点的个数。对于布尔环的特殊情况，我们对整个算法给出了完整的复杂度分析，证明是单指数时间算法，大大优于一般特征列算法的复杂度。我们还给出一个无乘法的吴特征列算法，并证明这一算法的关键步骤：整序原理，具有多项式复杂度。另外编程实现了算法，并利用这一程序成功的解决了 S. Cook 提出的矩阵乘法挑战的 6 阶情况，这是目前所知的最好结果。该工作发表于 Journal of Symbolic Computation。

（5.2）数域中的 exact covering systems（邓映蒲）：

有理数域或整数环中的 exact covering systems 有个经典的结果，即覆盖系统的模数必须有重复的，这一结果能否推广到代数数域上，是一个自然的问题。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，即这一结果对任意的代数数域都成立。论文被牛津大学的老牌数学杂志 Quarterly Journal of Mathematics 接受发表。

（5.3）Bent 函数（刘卓军）：

研究了有限域上的线性化多项式，给出其全体构成的代数结构的新的刻画。利用二元 Knuth 预半域构造出了一类新的 PS Bent 函数，并求出其对偶函数，这是继 Dillion 的 PS_{ap} 函数类之后又一类可以显式表达的 Bent 函数。

对完全非线性函数，给出了 4 类平面函数的显式表达。在利用伽罗瓦环上的 trace 形式构造出 4 元广义 Bent 函数方面，推广了 K.U. Schmidt 构造的一类伽罗瓦环上的广义 Bent 函数。

在特征为 2 的有限域上，利用 reversed Dickson 多项式构造给出构造 DO 多项式的充要条件，并给出上述 DO 型多项式何时是 APN 函数的完全刻画。

（5.4）有限域上典型群构造的强正则图的次成分（周凯）：

虽然有限域上典型群构造的强正则图的次成分很有可能已经不再具有强正则这么好的性质，但是也会具有弱一点的性质，比如拟强正则或者是 Deza 图。我们证明酉图的次成分是拟强正则图，还找到了其中的第二次成分的自同构群。文章被杂志 Linear and Multilinear Algebra 接收。

6、在物理、化学、高档数控中的应用：

（6.1）非线性物理方程（闫振亚）：

对于二维 Bose-Einstein 凝聚态中带有初值的有限区域的 Dilichlet 问题，基于保角映射和 Cauchy-Riemann 方程及其广义形式，提出系统的构造性方法，首次研究二维空间调控 GP / NLS 方程的 Dirichlet 问题的若干解析解，分析了解的演化规律，这对于理论物理学家和实验人员的应用提供精确的依据。评审专家认为该论文是 quite rare, value, useful method。发表在国际权威数学物理期刊《Phys. Rev. E》上，论文发表后并很快以全文形式被美国物理协会电子期刊《Virtual Journal of Atomic Quantum Fluids》收录。

研究了一维 Bose-Einstein 凝聚态中具有 double-well 势的时空调制的 GP 方程。基于椭圆函数，提出了两组精确解，并且利用数值分析研究了解的稳定性

问题，发表在国际权威数学物理期刊《Phys. Rev. E》上，论文发表后并很快以全文形式被美国物理协会电子期刊《Virtual Journal of Atomic Quantum Fluids》收录。

研究了离散时空调制的非线性 Schroedinger 方程的 rogon 解，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，对于分析非自治离散畸形波的物理机理具有重要的意义。发表在国际重要期刊《J. Math. Anal. Appl.》上。

首次提出PT-对称的短脉冲物理模型，并且研究了它们的数学结构和物理性质，论文发表在国际重要期刊《J. Phys. A :Math. Theor.》和英国皇家学会《Phil. Trans. R. Soc. A》上。该成果被Mihalache（美国光学学会Fellow）等人【Phys. Rev. A 86, 063825 (2012)】大篇幅引用和正面评价："Another interesting recent theoretical study by Yan [49] deals with complex PT-symmetric extensions of the nonlinear ultrashort light pulse model. A family of interesting complex PT-symmetric extensions of the short pulse equation was presented and unique properties of these equations with some chosen parameters were studied; see Ref. [49]. In particular, Yan [49] obtained exact solitary wave solutions, doubly periodic wave solutions, and compacton solutions."

[49] Zhenya Yan, J. Phys. A: Math. Theor. 45, 444035 (2012).

研究的主要成果获 2012 年中科院数学院突出科研成果奖。

（6.2）酶动力学基本模型（李邦河、李博）：

本年度，我们有一项工作发表在 J Math Chem 杂志上。在该文章中，我们提出了一种新的方法来测量酶动力学基本模型中的全部三个反应数率参数。理论上，实验测量越靠近末端结果会越精确，但是，如果测量太靠近反应末端，不可避免的实验误差反而会给参数的估计带来较大的误差。在反应末端附近，新方法的估计效果更好。我们不必要像原方法那样在过于靠近反应末端的时候测量反应物的浓度。新方法不只能在反应末端给出三个速率参数的优秀估计，在拟稳态的时候同样也可以给出优秀的估计。

（6.3）多运动约束下的轨迹插补算法（高小山、李洪波、袁春明、张立先）：

轨迹插补算法是高档数控系统的核心算法之一。我们针对 G01 代码与参数曲线两种典型的刀具路径，设计了各种约束下的最优插补算法，实现了五轴数控加工，显著提高了加工速度与加工质量。

微小直线段加工：研究加加速有界情况下的轨迹插补，以及基于变插补周期的曲线插补。基于加加速有界的微小直线段加工算法可以保证加工过程中加速度连续，降低机床震动，提高加工质量。而基于变插补周期的曲线插补算法，在满足加速度有界的情况下，降低曲线插补的计算复杂性。

参数曲线的最优运动插补算法。为减少机床振动和提高加工精度，我们提出了一种“加加加速”有界的最优加速模式，给出了加速度二阶光滑的基于关键点法的插补算法。对于“加加速”有界的最优插补问题，我们给出了一个基于状态空间法的贪心算法以及一个基于线性规划的快速算法。对于“加速”有界的最优插补问题，我们则给出了计算复杂度非常低的最优数值算法。以上算法在五轴数控机床上进行了实际加工，验证了算法设计的目标。

（三）介绍本年度实验室重大成果，研究成果的水平和影响等。

代表性成果 1、线性微分算子最小左公倍式的计算（李子明）

符号计算软件可以高效率地表示和操作代数对象，例如，有理数，多项式，矩阵等。目前一个热点问题是如何利用计算机表示和操作含有无穷信息的对象，例如：函数，级数，积分和求和公式等。由于很多常见的函数和序列可以通过线性微分和差分方程和初值条件唯一确定和表示，自九十年代以来，人们开始利用线性微分和差分算子来表示和操作这类含有无穷信息的对象。在这种表示下，函数的加法对应于线性微分和差分算子的最小左公倍式。

上个世纪初，Ore 和 Poole 分别给出了两个线性微分算子的最小左公倍式的算法。前者依赖于非交换的欧几里德算法，后者把问题化为线性方程组求解。1998 年，Li 利用非交换子结式改进了 Ore 的方法。但利用这些方法计算多个算子的最小左公倍式的效率较低。为此，van Hoeij 在 90 年代末设计了第一个直接计算多个微分算子最小最小左公倍式的算法。Abramov 等在 2006 年改进了该方法在退化情形下效率较低的弱点。但以上各种算法的复杂度分析一直是空白。换言之，我们一直不知道多个线性微分算子表示的函数相加的复杂度。其本质困难是 van Hoeij 算法比较复杂，由此出发，很难利用输入算子度量输出算子的大小。

我们定义了一个 Sylvester 型的结构矩阵，由此给出了多个线性微分算子的最小左公倍式的阶和系数次数的最优上界，并设计了计算多个线性微分算子最小左公倍式的算法和复杂度分析，证明了该算法对于输出是 quasi-optimal 的。

论文发表于 2012 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：“This is a long-awaited paper about which rumors had been circulating in the community for some time already. I am glad to finally see it finished and I recommend it strongly for ISSAC'12."

审稿意见二："This paper presents several significant improvements in the algorithms for solving the important problem of computing least (and also "shortest") common left multiples of linear ordinary differential operators with polynomial coefficients. The asymptotic complexity of the proposed algorithm is lower than that of all other known algorithms in terms of the maximal order of the given operators."

审稿意见三："This paper has five main contributions: (1) a new algorithm for computing the LCLM of several operators; (2) complexity analyses of a number of existing LCLM algorithms; (3) an upper bound for the total degree of the existence of nonzero left common multiples of non minimal order; (4) an implementation of their new method in Magma; (5) a really nice literature review.

In my opinion this paper is a clear accept. It is well written, the mathematics is correct and the results are interesting and significant. All five contributions are significant."

审稿意见四："This paper provides a detailed complexity analysis for the computation of left common multiples of linear differential operators with polynomial coefficients. The paper is well written, presents a careful analysis of previous work (including detailed complexity analysis of several previously known algorithm), as well as a new algorithm."

代表性成果 2、流密码的设计与分析（冯秀涛）

流密码是主流的密码体制之一，主要用于通信领域中保护通信信息的安全，其研究属于传统密码学领域。我院冯秀涛博士一直从事该领域最前沿的问题研究，在流密码算法设计、典型分析方法和基础理论等方面均取得一些阶段性成果，主要包括：

（1）在密码算法研制方面，参与了祖冲之(ZUC)算法和 LOISS 算法的设计与分析工作。其中前者已于 2011 年 9 月被 3GPP 选为 LTE 国际标准，于 2012 年 3 月被选为国家行业加密标准。祖冲之算法是我国第一个成为国际商业密码标准的密码算法，其国际标准化成功是我国在国际商业密码标准领域中的一次重大突破。冯秀涛博士在祖冲之算法国际标准化期间，担任了欧洲 3GPP SAGE 组织祖冲之算法安全评估专家组成员，负责组织祖冲之算法的技术分析和安全评估工作，以及组织祖冲之算法的修改工作和相关标准的撰写工作，为祖冲之算法的国际标准化推进成功作出突出贡献。

（2）在典型分析方法方面，提出了面向字节的猜测确定分析，并将之应用到 eSTREAM 胜选算法 SOSEMANUK 和 Rabbit 上，给出当前针对猜测确定分析最好的结果，其中前者发表在密码学三大会议之一的亚密会上。针对轻量级流密码算法 A2U2，给出了在已知明文攻击模型下低数据复杂度的实时密钥恢复攻击方法，在个人 PC 上只需数秒钟便可恢复出全部种子密钥。

（3）在基础理论方面，彻底解决了 C. Xing 提出的关于多重序列的 d-perfect 特性的猜想；给出了定长多重序列联合线性复杂度的分布和期望；研究了模 2n-1 加法的线性性质和渐进性质，为祖冲之算法的设计提供了理论支撑。

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	414	116	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	249	70	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	329	93	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	550	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	7	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	2011	2012	104	104	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	2011	2012	21	21	李子明
9.	国家数学交叉中心	信息安全和密码体系	2011	2012	21	21	邓映蒲

10.	国家杰出青年基金项目	高级几何不变量方法	2009	2012	140	0	李洪波
11.	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
12.	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	156	支丽红
13.	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	12	邓映蒲
14.	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	18.7	韩阳
15.	国家自然科学基金面上项目	多项式方程组求解及其在机器证明中的应用	2010	2012	22	0	王定康
16.	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	8.8	闫振亚
17.	中国科学院方向性项目	复杂系统研究	2010	2012	200	0	高小山
18.	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	0	程进三
19.	国家自然科学青年基金	微分、差分方程的 Galois 理论及 liouvillian 解算法	2010	2012	16	6.4	冯如勇
20.	国家自然科学青年基金	面向字的流密码的设计与分析	2010	2012	18	17.1	冯秀涛
21.	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	15.4	袁春明

22.	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
23.	国家标准委委托项目	基于战略思维和系统思想的标准化管理方法及机制优化研究	2011	2012	15	15	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	6	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	3	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	20	吴天骄
合计	---	---	---	---		924.4	---

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）	18 万欧元	支丽红
2	法国	INRIA/CNRS	LIAMA 中法实验室项目： ECCA	2010	2014	5 万欧元	1.3 万欧元	支丽红
合计	---	---	---	---	---		19.3 万欧元	---

注：国际合作项目指双方单位正式签订协议书的国际合作科研项目

横向合作及其它项目一览表

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

注：横向协作项目指有正式合同书的项目

国家重点实验室专项经费自主研究课题一览表

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

获奖等重要成果

序号	成果名称	获奖类别	等级	完成人及排序
1.	北京市科学技术奖：构造性理论与算法及其在复杂非线性系统中的应用		二等奖	闫振亚
2.	科技兴检奖：消费品质量安全影响因子研究及标准研制		一等奖	刘卓军
3.	中国科学院数学与系统科学研究院 2012 年度突出科研成果奖：复杂畸形波和物质波的构造与调控研究			闫振亚
4.	2012 年度系统所关肇直奖			袁春明

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	Homeomorphic approximation of the intersection curve of two rational surfaces	Computer Aided Geometric Design, 29(8), 613-625, 2012	L. Shen, J. Cheng, X. Jia	L. Shen	1.178
2	Local Generic Position for Root Isolation of Zero-Dimensional Triangular Polynomial Systems	2012,CASC,pp.186~197	Jia Li, Jin-San Cheng, Elias P. Tsigaridas	J.S. Cheng	
3	Root Isolation of Zero-dimensional Polynomial Systems with Linear Univariate Representation	Journal of Symbolic Computation, 47 (2012) 843-858	J.S. Cheng，X.S. Gao，L. Guo	J.S. Cheng	
4	Boolean functions optimizing most of the cryptographic criteria	Discrete Applied Mathematics, Vol. 160 No. 4-5 pp. 427–435(2012)	Ziran Tu, Yingpu Deng	Yingpu Deng	
5	Exact covering systems in number fields	The Quarterly Journal of Mathematics (Oxford)	Yupeng Jiang, Yingpu Deng	Yingpu Deng	

6	Results on permutation symmetric Boolean functions	Journal of Systems Science and Complexity	Yanjuan Zhang, Yingpu Deng	Yingpu Deng	
7	On Functional Decomposition of Multivariate Polynomials with Differentiation and Homogenization	J Syst Sci Complex, 25(2), 329-347, 2012.	S.W. Zhao, R. Feng, X.S. Gao	R. Feng	
8	多变元 q-超几何项的乘法分解	系统科学与数学 2012, 32（8）, 1-14	陈绍示、冯如勇、付国锋、 康劲	冯如勇	
9	A Real-time Key Recovery Attack on the Lightweight Stream Cipher A2U2	11th International Conference on Cryptology and Network Security-CANS 2012, LNCS 7712, pp.12-22, 2012	Zhenqing Shi, Xiutao Feng, Dengguo Feng, Chuankun Wu	Xiutao Feng	
10	A greedy algorithm for feed-rate planning of CNC machines along curved tool paths with confined jerk for each axis	Robotics and Computer Integrated Manufacturing, 28 (2012) 472-483.	K. Zhang, X.S. Gao, H. Li, C.M. Yuan	X.S.Gao	1.668
11	Characteristic Set Algorithms for Equation Solving in Finite Fields	Journal of Symbolic Computation, 47 (2012) 655-679.	X.S. Gao, Z. Huang	X.S.Gao	
12	Differential Chow form for projective differential variety	Journal of Algebra, 370(2012) 344–360	W. Li, X.S. Gao	X.S.Gao	
13	Interpolation of parametric CNC machining path under confined jounce	Int J Adv Manuf Technol. 62, 719–739, 2012	Fan W., Gao X.S., Yan W., Yuan C.M.	X.S.Gao	1.113
14	Sparse Differential Resultant for Laurent Differential Polynomials.	ArXiv:1111.1084v3, June 2012, 70 pages (submitted).	W. Li, C.M. Yuan, X.S.Gao.	X.S.Gao	
15	Hochschild homology and truncated cycles	Proc. Amer. Math. Soc. 140 (2012), 1133-1139	P.A. Bergh, Y. Han, D. Madsen	Y. Han	
16	Topological Classification of Non-degenerate Intersections of Two Ring Tori	Computer Aided Geometric Design, Vol. 30, 181 - 198, 2013	X. Jia, C. Tu W. Wang	X. Jia	1.178

17	Using Smith Forms to Compute All the Singularities of Rational Planar Curves	Computer Aided Geometric Design, Vol. 29, 296 - 314, 2012	X. Jia R. Goldman	X. Jia	1.178
18	Using a Bivariate Sparse Resultant to Find the Singularities of Rational Space Curves	Journal of Symbolic Computation, 2013. In press	X. Shi, X. Jia R. Goldman	X. Jia	0.719
19	An improved method to measure all rate constants in the simplest enzyme kinetics model	J Math Chem (2012) 50:752–764.	Banghe Li, Bo Li, Yuefeng Shen	Banghe Li	
20	The reason of Hopf's and Oleinik's proofs for countability of shocks being wrong.	Sci.ChinaMath. (2012) 55(4):727-729.	Banghe Li	Banghe Li	
21	Young measures as probability distributions of Loeb spaces.	Proc.Amer.Math.Soc.140 (2012), No.1,207-215.	Banghe Li, Tianhong Li	Banghe Li	
22	Discrete Interpolation of G01 Codes in 2D Machining under Bounded Accelerations	Math. Comput. Sci. (2012) 6:327–344.	Hongbo Li, Xiaoshan Gao, Lixian Zhang, Ruiyong Sun	Hongbo Li	
23	Power Series Solution for Isoscallop Tool Path Generation on Free-form Surface with Ball-end Cutter	Math. Comput. Sci. (2012) 6:281–296.	Hongbo Li, Shoubin Yao, Ge Li, Yuanjie Liu, Lixian Zhang	Hongbo Li	
24	Two Proofs on Max-Min-Max Principle of Jerk Control in Time-Optimal Rectilinear Motion	Math. Comput. Sci. (2012) 7	Hongbo Li, Lixian Zhang	Hongbo Li	
25	Sparse Difference Resultant	ArXiv:1212.3090v1, Dec. 2012. (submitted).	W. Li, C.M. Yuan, X.S.Gao.	Wei Li	
26	Fast Computation of Common Left Multiples of Linear Ordinary Differential Operators	ISSAC'12, pages 99-106, 2012	Alin Bostan, Frédéric Chyzak, Ziming Li, Bruno Salvy	Ziming Li	

27	A Note on Two Classes of Boolean Functions with Optimal Algebraic Immunity	Journal of Systems Science and Complexity	Zhuojun Liu	Zhuojun Liu	
28	An Algebraic Broadcast Attack against NTRU	ACISP 2012, LNCS 7372, pp. 124–137, 2012	Jintai Ding, Yanbin Pan, Yingpu Deng	Yanbin Pan	
29	An Efficient Broadcast Attack against NTRU	In Proc. of Asia CCS 2012, ACM New York, NY, USA, pp. 22-23, 2012.	Jianwei Li, Yanbin Pan, Mingjie Liu, Guizhen Zhu	Yanbin Pan	
30	二维格的覆盖半径	系统科学与数学 2012 Vol. 21 (7): 908-914.	姜宇鹏，邓映蒲，潘彦斌	潘彦斌	
31	A Signature-Based Algorithm for Computing Groebner Bases in Solvable Polynomial Algebras	Proceedings of ISSAC 2012, 351-358. July 22-25	Y. Sun, D.K. Wang, X.D. Ma Y. Zhang	D.K. Wang	
32	Computing Polynomial Univariate Representations of Zero-dimensional Ideals by Groebner Basis	Science China Mathematics June 2012, Volume 55, Issue 6, pp 1293-1302	X.D. Ma, Y. Sun, D.K. Wang	D.K. Wang	
33	Complex PT -symmetric extensions of the nonlinear ultra-short light pulse model	J. Phys. A: Math. Theor. 45 (2012) 444035	Zhenya Yan	Zhenya Yan	
34	Matter-wave solutions in Bose-Einstein condensates with harmonic and Gaussian potentials	Phys. Rev. E 85 (2012) 056608	Yan Z, Jiang D.	Zhenya Yan	
35	Nonautonomous discrete rogue wave solutions and interactions in an inhomogeneous lattice with varying coefficients	J. Math. Anal. Appl. 395 (2012) 542	Zhenya Yan， Dongmei Jiang	Zhenya Yan	
36	Two-dimensional superfluid flows in inhomogeneous Bose-Einstein condensates	Phys. Rev. E 85 (2012) 016601	Zhenya Yan, V. V. Konotop, A. V. Yulin, W. M. Liu	Zhenya Yan	
37	Certified approximation of parametric space curves with cubic B-spline curves.	Computer Aided Geometric Design, 29 (2012) 648-663	L.Y. Shen, C.M. Yuan, X.S. Gao	L.Y. Shen	1.178

38	Exact Cooperative Regenerating Codes with Minimum-Repair-Bandwidth for Distributed Storage	IEEE INFOCOM 2013 mini-conference.	Anyu Wang, Zhifang Zhang	Zhifang Zhang	
39	Threshold changeable secret sharing schemes revisited	Theoretical Computer Science 418: 106-115 (2012).	Zhifang Zhang, Yeow Meng Chee, San Ling, Mulan Liu, Huaxiong Wang	Zhifang Zhang	
40	Computing Isolated Singular Solutions of Polynomial Systems: Case of Breadth One	SIAM Journal on Numerical Analysis, 50(1): pp. 354-372, 2012	Nan Li, Lihong Zhi	Lihong Zhi	
41	Computing the Nearest Singular Univariate Polynomials with Given Root Multiplicities	Theoretical Computer Science	Zijai Li, Lihing Zhi	Lihong Zhi	
42	Determining singular solutions of polynomial systems via symbolic-numeric reduction to geometric involutive forms	Journal of Symbolic Computation Volume 47 Issue 3, March, 2012 Pages 227-238	Xiaoli Wu, Lihong Zhi	Lihong Zhi	
43	Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients	Journal of Symbolic Computation, 47(1), pp. 1-15, 2012/1	Erich L. Kaltofen, Bin Li, Zhengfeng Yang, Lihong Zhi	Lihong Zhi	
44	Global optimization of polynomials restricted to a smooth variety using sums of squares	Journal of Symbolic Computation Volume 47, Issue 5, May 2012, Pages 503 – 518	Aurélien Greuet, Feng Guo, Mohab Safey El Din, Lihong Zhi	Lihong Zhi	
45	Verified Error Bounds for Isolated Singular Solutions of Polynomial Systems: Case of Breadth One	arXiv:1201.3443[math.NA]	Nan Li, Lihong Zhi	Lihong Zhi	

出版专著

序号	著作名称	作者	出版单位	出版日期
1	《Mathematics in Computer Science》专辑	Hongbo Li, R. Farouki, Dingkang Wang	Springer	2012.09

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线插补方法	201210369252.2	申报	张立先，李洪波，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	申报	张立先，高小山，李洪波，孙瑞勇
3.	拐角多周期恒加加速度过渡的 S 曲线加减速直线插补方法	201210287472.0	申报	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.	中法微分方程国际研讨会	国际	中科院数学院	高小山	2012.4.16-27	100
2.	第五届有限域及其应用国际研讨会	国际	中科院数学院	刘卓军	2012.6.28-30	100
3.	基于混合计算的误差可控算法	国内	中科院数学院	支丽红	2012.7.1-2	30
4.	973 项目“数学机械化方法及其在数字化设计制造中的应用”项目中期总结与学术交流会	国内	中科院数学院	高小山	2012.8.13-14	150
5.	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	2012.10.25-26	50
6.	第十届亚洲计算机数学会议	国际	中科院数学院	李子明	2012.10.26-28	90
7.	构造性微分代数研讨会	国内	中科院数学院	高小山	2012.11.24-26	45
8.	数学机械化战略研讨会	国内	中科院数学院	李洪波	2012.12.18-19	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.	Local Generic Position for Root Isolation of Zero-Dimensional Triangular Polynomial Systems	程进三	Computer Algebra in Scientific Computing	斯洛文尼亚	2012.09

2.	信息安全和密码体系	邓映蒲	北航—中科院交叉学科研讨会	北京	2012.03
3.	The sum of binomial coefficients and integer factorization	邓映蒲	International Workshop on Coding and Cryptography	上海	2012.05
4.		邓映蒲	第五届有限域及其应用国际研讨会	北京	2012.06
5.	二项式系数的和与整数分解	邓映蒲	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”中期总结与学术交流会	北京	2012.08
6.	信息安全和密码体系	邓映蒲	中国科学院数学与系统科学研究院国家数学与交叉科学中心信息技术研究部专题工作交流会	北京	2012.09
7.	Computing the Galois groups of linear differential-difference equations	冯如勇	2012 Joint Mathematics Meetings	美国	2012.01
8.	On the Structure of Compatible Rational Functions	冯如勇	French-Chinese School on Differential and Functional Equations	武汉	2012.04
9.	On the Structure of Compatible Rational Functions	冯如勇	18th International Conference on Applications of Computer Algebra (ACA 2012)	保加利亚	2012.06
10.	求解布尔非常方法及其复杂性	高小山	逻辑、计算与信息研讨会	北京	2012.04

11.	Sparse differential resultant for Laurent differential polynomials	高小山	French-Chinese School on Differential and Functional Equations	武汉	2012.04
12.	Sparse Differential Resultant for Laurent Differential Polynomials	高小山	18th International Conference on Applications of Computer Algebra (ACA 2012)	保加利亚	2012.06
13.	Differential Chow Form and Differential Sparse Resultant （邀请报告）	高小山	Differential and difference equations, integrable systems, model theory	英国	2012.09
14.	Efficient Time-Optimal Interpolation for CNC Machining along Curved Tool Paths （邀请报告）	高小山	International Workshop on Mathematics and Algorithms for Computer-Aided Manufacturing, Engineering and Numerical Control	北京	2012.10
15.		韩阳	第十四届全国代数表示论会议	合肥	2012.06
16.		韩阳	Workshop and International Conference on Representations of Algebras, Bielefeld University, Germany.	德国	2012.08
17.	Hattori-Stallings trace and character （邀请报告）	韩阳	The Second Cross Strait Workshop in Algebra, National Cheng Kung University, Tainan	台湾	2012.12
18.	Perspective projection in the homogeneous and conformal models using rotors	贾晓红	Applied Geometric Algebras in Computer Science and Engineering 2012	法国	2012.07
19.	Approximate Rational Solutions to Rational ODEs Defined on Discrete Differentiable Curves	李洪波	2012 Joint Mathematics Meetings	美国	2012.01
20.		李洪波	ASME 2012 International Mechanical Engineering Congress & Exposition	美国	2012.11

21.	Sparse Differential Resultant for Laurent Differential Polynomials	李 伟	French-Chinese School on Differential and Functional Equations	武汉	2012.04
22.	Sparse Differential Resultant for Laurent Differential Polynomials	李 伟	International Workshop on Multiple Zeta Values, Rota-Baxter Algebras and Related Topics	兰州	2012.08
23.	Factorization of Linear Differential Operators	李子明	French-Chinese School on Differential and Functional Equations	武汉	2012.04
24.		李子明	2012International Symposium on Symbolic and Algebraic Computation	法国	2012.07
25.	Applying the System Safety Methodologies on Consumer Product Safety	刘卓军	Australian System Safety Conference	澳大利亚	2012.05
26.	Linearized Comprehensive Base of Finite Fields and Planar DO Polynomials	刘卓军	第五届有限域及其应用国际研讨会	北京	2012.06
27.		刘卓军	30th International System Safety Conference	美国	2012.08
28.	Constructing Generalized Bent Functions from Trace Forms over Galois Rings	刘卓军	Asian Symposium on Computer Mathematics	北京	2012.10
29.	复杂数据特征变换及其在中医体质分类中的应用	刘卓军	第九届世界中医药大会	马来西亚	2012.11
30.	Cryptanalytic Techniques for Public-Key Cryptosystems （邀请报告）	潘彦斌	Workshop on Advancements in Cryptanalytic Techniques	马来西亚	2012.05
31.	Cryptanalysis of Some Lattice-Based Public-Key Cryptosystems （邀请报告）	潘彦斌	Cryptology 2012, Malaysia	马来西亚	2012.06

32.	An Algebraic Broadcast Attack against NTRU	潘彦斌	International Workshop on Finite Fields and Their Applications	北京	2012.06
33.		潘彦斌	17th Australasian Conference on Information Security and Privacy.	澳大利亚	2012.07
34.	Strongly Regular Graphs from Classical Groups （邀请报告）	万哲先	上海代数组合国际会议	上海	2012.08
35.	Computing Signature Based Groebner Basis for the ideals of Differenctial Operators	王定康	Differential Schemes and Differential Cohomology	加拿大	2012.06
36.	A Signature-Based Algorithm for Computing Groebner Bases in Solvable Polynomial Algebras	王定康	The 37th International Symposium on Symbolic and Algebraic Computation	法国	2012.07
37.	A New Method of automatic Geometric Theorem Proving and Discovery by Comprehensive Groebner Systems	王定康	The 9th International Workshop on Automated Deduction in Geometry	英国	2012.09
38.	Computation of Zero Divisors in Residue Class Rings of Parametric Polynomial Ideal （邀请报告）	王定康	The 10th The Asian Symposium on Computer Mathematics	北京	2012.10
39.	Matter wave solutions in Bose-Einstein condensates	闫振亚	French-Chinese School on Differential and Functional Equations	武汉	2012.04
40.	Matter wave solutions in Bose-Einstein condensates with some potentials （邀请报告）	闫振亚	偏微分方程与数学物理国际学术研讨会	江苏	2012.05

41.	Two-dimensional matter wave solutions in Bose-Einstein condensates （邀请报告）	闫振亚	高性能科学计算与学科建设研讨会	北京	2012.08
42.	复杂非线性波的构造性算法及其在物理中的应用	闫振亚	中国科学院数理交叉培训班	北京	2012.09
43.	非自治复杂非线性系统的畸形波研究	闫振亚	可积性计算学术研讨会	上海	2012.10
44.	Differential chow form	袁春明	French-Chinese School on Differential and Functional Equations	武汉	2012.04
45.	Differential Chow Forms	袁春明	18th International Conference on Applications of Computer Algebra (ACA 2012)	保加利亚	2012.06
46.	Multi-period Turning Interpolation Algorithm for High-Speed Machining of Continuous Line Segments with limited Acceleration, Jerk and Chord Error	张立先	ASME 2012 International Mechanical Engineering Congress & Exposition	美国	2012.11
47.		张志芳	第五届有限域及其应用国际研讨会	北京	2012.06
48.	Computing Real Solutions of Polynomial Systems via Low-Rank Moment Matrix Completion	支丽红	2012 International Symposium on Symbolic and Algebraic Computation	法国	2012.07
49.	Computing real solutions of polynomial systems via low-rank moment matrix completion	支丽红	The 21st International Symposium on Mathematical Programming	德国	2012.08

50.	Verified Error Bounds for Isolated Singular Solutions of Polynomial Systems	支丽红	Asian Symposium on Computer Mathematics	北京	2012.10
51.	Verified Error Bounds for Isolated Singular Solutions of Polynomial Systems （邀请报告）	支丽红	2012 Japan workshop on symbolic computation	日本	2012.12

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.	Isabelle/HOL 系统与应用研究	2012.5	2012.12	1	1	陈光喜	刘卓军
2.	Groebner 基算法的理论与实现	2012.5	2012.12	1	1	孙　瑶	王定康
3.	区间多项式系统的零点研究	2012.5	2012.12	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）
合计	---	---	---			

大型仪器设备的开放、共享及成效。

七、实验室大事记

1、法国 Grenoble 召开的第 37 届国际符号和代数计算会议(ACM ISSAC'12)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) Alin Bostan, Frederic Chyzak, Ziming Li, Bruno Salvy: Fast Computation of Common Left Multiples of Linear Ordinary Differential Operators.

2) Xiaodong Ma, Yao Sun, Dingkang Wang and Yang Zhang: A Signature-Based Algorithm for Computing Groebner Bases in Solvable Polynomial Algebras.

3) Feng Guo, Erich Kaltofen and Lihong Zhi: Certificates of Impossibility of Hilbert-Artin Representations of a Given Degree for Definite Polynomials and Functions.

4) Yue Ma and Lihong Zhi: Computing Real Solutions of Polynomial Systems via Low-Rank Moment Matrix Completion.

2、中国科学院数学机械化重点实验室第三届学术委员会第二次会议于 2012 年 3 月 20 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 2011 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，获国内外奖励多项，发表专著 2 部，译著 1 本，论文 47 篇；数学机械化重点实验室主持、多所大学与研究所承担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”顺利立项；实验室组织召开了多次国际和国内会议，如：可信计算国际会议，计算机辅助制造工程和数控中的数学与算法国际会议，信息安全与密码学术研讨会，第四届全国计算机数学学术会议，实验室战略发

展研讨会等。

随后，按实验室研究方向由闫振亚、袁春明分别作了学术报告。与会专家们听取了两个报告后，提出了多项具有建设性的意见。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。

专家们在会议中也对实验室开放课题得设立，实施提出了很多建设性的意见。林惠民院士提出理论研究要深入实际，解决实际问题。陆汝钤院士提出要以理论创新为主。张继平教授提出要深入技术前沿，使理论研究与技术充分结合。雷天刚处长建议理论研究要在实际应用中主动提出新思路、新想法，并且要确认实验室大的方向。王永祥处长指出目前以技术为导向，建议在建模上下功夫，将研究成果转化为技术创新，同时提出了两个方向性问题：一是对数控技术的定位，二是在应用方面是否要发展经济数学。

3、首届吴文俊人工智能科学技术奖揭晓

新华网北京 5 月 1 4 日电（记者余晓洁）首届吴文俊人工智能科学技术奖 1 4 日在京揭晓。北京邮电大学钟义信教授的“构建信息科学理论基础，创新人工智能核心理论”获吴文俊人工智能科学技术奖成就奖；广东工业大学蔡文研究员等完成的“拓论及其应用”获创新奖一等奖。

此外，北京邮电大学和国瑞数码安全系统有限公司杨义先等完成的“时空混沌密码与信息安全技术”项目、北京工商大学韩力群等完成的“智能烤烟烟叶质量特征检测与分级系统”项目、中国科学院自动化研究所汤淑明等完成的“智能交通技术带来的节能降耗”项目分获进步奖二等奖。

“获奖同志是广大智能科学技术工作者的优秀代表。希望大家珍惜荣誉，谦虚谨慎，再接再厉，为推动经济社会发展和科技进步创造新的业绩。”中国科协副主席赵沁平说。

吴文俊是我国著名数学家、首届国家最高科学技术奖获得者。他开创的数学机械化在国际上被誉为“吴方法”。此后人工智能、并联数控技术、模式识别等诸多领域取得的重大科研成果，背后都有数学机械化的广泛应用。

据中国人工智能学会副理事长谭铁牛介绍，吴文俊人工智能科学技术奖设有成就奖、创新奖和进步奖，每年评奖一次，奖励在智能科学技术领域取得重大突破，做出卓著贡献的科技工作者和管理者。

4、第五届有限域及其应用国际研讨会（简称 FFA2012）于 6 月 28 日至 30 日在中国科学院数学与系统科学研究院召开。来自美国、加拿大、新加坡以及台湾义守大学、香港科技大学、北京大学、中科院数学与系统科学研究院、中科院信息工程研究所等国内外 60 余所高校和科研单位的 100 余位专家及研究生参加了会议。

会议开幕式于 6 月 28 日上午隆重举行，由中科院数学与系统科学研究院刘卓军研究员主持。中科院数学与系统科学研究院席南华院士（学术院长）、万哲先院士、清华大学冯克勤教授先后在开幕式上致辞。

本次会议邀请了国内外 14 位专家学者作大会报告， 其中有 University of California 的万大庆教授、University of Delaware 的向青教授、Nanyang Technological University 的林杉教授、University of Southern California 的黄铭德教授、University of South Florida 的侯向东教授等，他们分别对各自近期的研究成果做了介绍。此外，来自全国各高校和科研单位的 30 余位研究人员和研究生做了分组报告。会议报告的内容主要涉及有限域理论以及有限域在组合学、通讯理论、密码学、编码理论、组合设计等方面的应用。

有限域及其应用国际研讨会是由万哲先院士发起的国际性学术会议，至今已成功举办四届，本次会议是第五届。会议得到了中国科学院数学与系统科学

研究院、国家数学与交叉科学中心等组织机构的大力支持，为海内外有限域领域的专家、学者、研究生提供了一个及时交流科研成果的机会和平台，对于国内外有限域及其应用研究领域的深入发展起到了积极的推动作用。

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” 召开“项目中期总结与学术交流会”

973 项目“数学机械化方法及其在数字化设计制造中的应用”中期总结与学术交流会于 8 月 13-14 日在中科院数学与系统科学研究院召开。科技部基础司李非、科技部基础研究管理中心王公仆出席了会议。项目中期评审专家组由项目专家组成员、项目领域专家咨询组责任专家、项目外同行专家和项目依托部门管理专家组成。

科技部李非博士介绍了 973 项目相关情况、中期评估的意义以及应该注意

的问题，希望本项目能够满足三个“更加”：更加聚焦国家重大需求，更加强化科学目标导向，更加注重优秀团队建设。项目依托单位代表，中科院基础局王永祥处长希望本项目在完成项目任务的同时，把科学上的突破转化为技术上优势。首席科学家介绍了项目整体情况，项目四个课题组分别作了汇报。从发表的论文、论著、获奖、申请专利、培养研究生情况、学术交流、以及课题的预期目标等方面详细汇报了各自的工作进展。

项目中期评估专家组对项目的总体执行情况进行了认真评估，认为本项目过去两年在数学机械化理论与算法、基于混合计算的误差可控算法、基于数学机械化方法的复杂加工曲面设计制造与基于数学机械化方法的高档数控系统方面取得了重要进展，圆满完成了任务书规定的任务，发展势头非常好，为项目今后三年的发展打下了坚实的基础。评审会前，项目还召开了学术交流会，项目承担人总结了项目启动近两年以来的进展。

6、 2012 年计算机辅助制造、工程与数控中的数学与算法国际会议于 2012 年 10 月 25-26 日在中国科学院数学与系统科学研究院召开。会议邀请了美国、英国、意大利、法国、比利时、以色列等国家的大学与科研单位的，以及国内的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、华中科技大学、大连理工大学、西北工业大学、清华大学等单位的 50 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。以色列理工学院（Technion Israel Institute of Technology）的 Moshe Shpitalni 教授，法国国家信息与自动化研究院（INRIA Sophia Antipolis）的 Bernard Mourrain 教授，中国科学院数学与系统科学研究院副院长高小山研究员，大连理工大学的孙玉文教授，伊利诺斯州厄巴纳-香槟大学（University of

Illinois at Urbana-Champaign）的 Placid M. Ferreira 教授，西北工业大学的张卫红教授，意大利帕多瓦大学（University of Padova）的 Alberto Trevisani 副教授等分别做了各自研究领域的大会报告。

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。

7、第十届亚洲计算机数学会议(The Tenth Asian Symposium on Computer Mathematics)于 2012 年 10 月 26-28 日在中国科学院数学与系统科学研究院召开。参加会议的外宾分别来自会议来自美国、加拿大、奥地利、日本、法国、瑞士、比利时等。国内的来宾分别来自北京大学、南开大学、华东师范大学、吉林大学、大连理工大学、北京航空航天大学、北京科技大学、黑龙江大学、深圳大学和中科院等。共有 90 余人参加了会议，其中研究生 30 多人。

中国科学院数学与系统科学研究院副院长高小山研究员致开幕词。北卡罗莱纳州立大学（North Carolina State University）的 Erich Kaltofen 教授、苏黎世联邦理工学院（ETH Zürich）的 Markus Püschel 教授、奥地利科学院（RICAM, Austrian Academy of Sciences）的 Josef Schicho 教授分别作了大会邀请报告。会议共有 45 个学术报告。会议文集将由 Springer (Beijing)出版。

第十届亚洲计算机数学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。会议主席是本实验室的李子明研究员，程序委员会主席是比利时安德卫普大学的 Wen-shin Lee 博士和实验室的冯如勇博士。组织委员会主席是实验室的袁春明博士。

亚洲计算机数学会议是由中科院数学机械化研究中心和日本符号与代数计算协会在 1995 年共同创立的一个系列会议。该会议为参会人员提供展示原创性研究结果，了解计算机数学的最新进展，交换想法与观点的一个平台。会议网站见：http://www.mmrc.iss.ac.cn/ascm/ascm2012/

8、数学机械化实验室 2012 年年终总结会议于 2012 年 12 月 18 日-19 日在温都水城召开。首先由实验室主任李洪波研究员做 2012 年实验室工作总结报告。接着实验室 20 余位成员一一对 2012 年的工作成果以及研究进展进行了汇报。汇报完成后实验室主任李洪波研究员对实验室 2013 年的发展进行了规划并且对实验室各项任务的分工进行了安排。随后实验室成员中国科学院数学与系统科学研究院副院长高小山研究员对大家在 2013 年的工作提出了更高的要求。最后实验室成员大家各抒已见对实验室的发展献计献策。