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					
硕士点	基础数学	070101	应用数学	070104	管理科学与工程	120100
博士点	基础数学	070101	应用数学	070104	管理科学与工程	120100
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，可以看到演绎倾向与算法倾向的此消彼长。两种倾向总是交替地处于主导地位。值得注意的是，探询新算法可以导致数学的重大发现，如解析几何与微积分；而且构造性数学往往具有很高的实用价值。数学机械化研究的深入开展，不仅会进一步丰富数学科学的传统内容，也将进一步丰富其交叉性学科的内容，从而在总体上促进数学科学的发展。

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。

数学机械化研究又有明显的交叉性。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， 天体力学中共心多体问题， 化学平衡中的方程求解，小波构造的优化，命题逻辑与一阶谓词逻辑中的定理证明 ,非线性发展方程的行波解的算法等等。

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，中国科学院在批准成立数学机械化中心。数学机械化中心建立二十年以来，取得了一系列高水平的科研成果，并获得了十项国内重要奖励与两项国际奖励。特别值得指出的两项奖励是（1）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"。这一荣誉进一步表明吴方法已经被国际学术界认为是自动推理领域最基本与经典性工作。（2）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"。

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"与"973"项目"数学机械化与自动推理平台",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。

当前信息技术正在给社会生产力带来一场革命，但由于大量敏感信息通过互联网进行交换，信息的不安全性带来严重的社会问题。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，它以数学和计算机科学等学科为基础，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，他们第一次用椭圆曲线成功地实现了已有的一些公钥密码算法包括 Differ-Hellman 算法。现在椭圆曲线密码体制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。

(1) 利用代数组合、代数数论、计算代数和有限几何的经典工具和最新成果来研究信息科学，特别是编码理论，在当前是数学家和通信技术专家的公同的领域，也是信息科学中的一个热门的研究方向。 (2) 代数几何码是上世纪八十年代由苏联数学家发现的，这一发现使数学中最抽象的分支之一• • 代数几何，通过编码理论被天才地用到通信工程中去。 由于代数几何码的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中的一个热点。 (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，在诸如远程数据通信、数据的磁记录等广泛的应用领域是性能最好的码。 (4) 时空码（即 Space-Time 码）是美国学者 Tarokh 和 Calderbank 等人几年前发现的一种码，它用在多通道、多天线、无线通信信道--例如手机通信中，可以极大地改进这些信道的性能。 (5) 计算的复杂性理论和 Shannon 的信息论是现代密码学的两大理论支柱。复杂性理论作为数学和信息科学共同的领域，将受到更加广泛的关注。 (6) 量子纠错码和量子密码是量子信息论的两个基本方面，它们都基于量子计算和量子算法。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以及进行数学机械化方面高层次国际学术交流的中心。**

实验室以基础研究为主，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，面向学科前言、面向国家发展需求，努力做出突破性、原创性和关键性成果，保持数学机械化主要国际研究中心之一的地位。

实验室的近期(2015)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系统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，加强实验室作为数学机械化主要国际研究中心之一的地位。

实验室的长期(2025)目标是整体推动数学机械化的发展，开辟新的研究方向，成为国际上数学机械化科学研究、学术交流与高级人才培养的主要中心。

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和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。方程求解是对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。研究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。我们在符号计算研究方面关注的重点是非线性方程求解,方程求解是数学研究的基本问题之一；科学研究与高新技术研究中很多问题往往可以转化为各种方程的求解问题。数学机械化方法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最著名的符号计算软件 Maple。

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、密码学和安全多方计算与计算数论。

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。有限域研究可以追溯到费尔马、欧拉、高斯和伽罗华等著名数学家。近几十年，随着计算机科学的发展，有限域理论得到深入发展与广泛应用。特别是，有限域理论是编码与密码学的重要数学基础。实验室在有限域的正规基与有限域上的方程求解方面有重要工作。

密码分析：在今天的信息社会，信息安全由于涉及国家的政治安全、军事安全、经济安全等众多方面而成为一个重要的研究领域。传统的密码系统和各种密码应用方案依赖于大整数分解和计算离散对数的困难性。而 P. Shor 于 1996 年证明在量子计算模型之下，存在多项式时间算法来求解这两个问题。这

样现有的许多密码系统受到挑战。最近出现的新的密码体系与数学机械化研究的主要内容 - 方程求解的符号算法密切相关。例如 2001 年由美国 NIST 选中新的高级加密标准 AES，它的安全性取决于有限域上大规模非线性多变量方程组的不可解性。针对信息安全，特别是密码中的核心问题，发展新的数学方法，对提高我国的信息安全研究能力具有十分深远的意义。数学机械化与符号计算由于为代数计算、群论、数论、代数几何、自动推理等的研究提供了强有力的工具，在信息安全方面有着广泛的应用前景。

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

- **数学机械化在高新技术中的应用**

基于数学机械化方法的高档数控系统。由于数控技术对国民经济和国防安全所具有的重要作用和战略意义，西方发达国家不仅把高档数控机床和高性能数控系统视为具有高利润的高技术产品，而且一直将其列为超越经济价值的战略物资，对我国采取技术封锁、限制和歧视的政策。对于我国技术尚不完善的 5 轴联动以上的高性能数控系统产品，发达国家至今仍对我国进行限制。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。我们还提出了并联机构广义 Stewart 平台，用于并联机构与机床。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与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。

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

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	研究员	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	研究员	是	中科院数学院
4.	万哲先	男	中国	委员	研究员	是	中科院数学院
5.	张景中	男	中国	委员	研究员	是	中科院成都计算机所
6.	林惠民	男	中国	委员	研究员	是	中科院软件所
7.	黄民强	男	中国	委员	研究员	是	中科院系统所
8.	陆汝钤	男	中国	委员	研究员	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	其它固定人员名单
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	闫振亚、冯如勇、黄雷、程进三
2.	信息安全研究中心	万哲先、刘木兰、胡磊、刘卓军、邓映蒲	张志芳、冷福生、周凯、潘彦斌，冯秀涛
3.	高档数控系统研究组	高小山、李洪波、王定康	袁春明、贾晓红

固定人员名单

序号	姓名	性别	出生日期	职务	职称	所学专业	工作性质
1.	吴文俊	男	1919.5		院 士	数学机械化	研究
2.	万哲先	男	1927.1		院 士	代数、编码	研究
3.	李邦河	男	1942.7		院 士	拓扑、代数几何	研究
4.	高小山	男	1963.10		研究员	自动推理、符号计算	研究
5.	李洪波	男	1968.3		研究员	自动推理、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	研究
12.	王定康	男	1965.3		副研究员	符号计算	研究
13.	邓映蒲	男	1971.5		副研究员	信息安全	研究
14.	闫振亚	男	1974.3		副研究员	复杂非线性波	研究
15.	冯如勇	男	1978.6		副研	符号计算	研究
16.	张志芳	女	1980.10		副研	信息安全	研究
17.	袁春明	男	1979.12		助研	符号计算	研究
18.	冷福生	男	1980.5		助研	代数数论	研究
19.	周　凯	男	1981.9		助研	代数、编码	研究
20.	吴天骄	男	1959.9		工程师	数学机械化	技术
21.	程进三	男	1976.8		助研	符号计算	研究
22.	黄　雷	男	1980.1		助研	数学机械化	研究
23.	潘彦斌	男	1982.4.2		助研	信息安全	研究
24.	贾晓红	女	1981.9		助研	计算几何	研究
25.	冯秀涛	男	1978.8		助研	信息安全	研究
26.	周代珍	女	1965.3		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、黄雷等	2010 - 2012

注：基金委创新群体等

国内外学术组织任职情况

序号	姓名	学术组织名称	职务	任职开始时间	任职结束时间
1.	高小山	中国数学会	副理事长	2012	
2.	高小山	中国系统工程学会	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.	刘卓军	中国数学会计算机数学专业委员会	委员		
7.	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
8.	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	2007.11	2012
9.	李洪波	中国数学会计算机数学专业委员会	副主任		
10.	李子明	中国数学会计算机数学专业委员会	主任	2012	
11.	李子明	中国数学会	理事		
12.	支丽红	国际符号与数值混合计算指导委员会	委员		
13.	支丽红	中国数学会计算机数学专业委员会	委员		
14.	支丽红	ISSAC 指导委员会	委员	2011	2014
15.	王定康	中国数学会计算机数学专业委员会	秘书长	2010	2013
16.	李子明	ACM SIGSAM	顾问		

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.	李子明	《Journal of Symbolic Computation》	编委		
26.	李子明	《Journal of Systems Science and Complexity》	编委		
27.	李洪波	《Advances in Applied Clifford Algebras》	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	2011	
32.	闫振亚	《J. Engineering and Applied Science》	编委	2007	

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.	王定康	王继斌		
2.	闫振亚	岳志强		
3.	李子明	康　劲		
4.	黄民强	胡耿然		
5.	胡　磊	吕　昌		
6.	支丽红	刘　琦		
7.	高小山	李应弘		
8.	王定康	周　洁		
9.	闫振亚	王晓云		
10.	韩　阳	秦永云		
11.	万哲先	王安宇		
12.	李洪波	刘　越		
13.	高小山	祝　炜		
14.	万哲先		孙志强	
15.	李洪波		李　阁	
16.	高小山		郭建新	
17.	高小山		闵　程	
18.	支丽红		郭庆东	
19.	刘卓军		张晓明	
20.	黄民强，邓映蒲		张　凤	

21.	李子明		陈绍示	
22.	刘卓军		李晓明	
23.	王定康		张　梅	
24.	高小山		赵尚威	
25.	李洪波		孙瑞勇	
26.	李洪波		张立先	
27.	李邦河		吴小胜	
28.	高小山		李　伟	
29.	支丽红		郭　峰	
30.	李洪波		刘元杰	
31.	李子明		付国锋	
32.	王定康		樊　伟	
33.	高小山		郭磊磊	
34.	支丽红		马　玥	
35.	刘卓军		柳　刚	
36.	刘卓军		靳庆芳	
37.	刘卓军		戴照鹏	
38.	支丽红		李　楠	
39.	支丽红		李子佳	
40.	高小山		张　可	
41.	韩　阳		陈　慧	
42.	李洪波		姚守彬	
43.	刘卓军		吴保峰	
44.	王定康		马晓栋	
45.	邓映蒲		姜宇鹏	

46.	吴文俊		姜东梅	
47.	刘卓军		黄　冲	
48.	韩　阳		章　超	
49.	高小山			张智勇
50.	支丽红			梁野
51.	支丽红			李喆
52.	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.	李晓明	博士	刘卓军	
2.	张立先	博士	李洪波	
3.	张　梅	博士	王定康	
4.	赵尚威	博士	高小山	
5.	孙瑞勇	博士	李洪波	

研究生获奖一览表

序号	获奖名称	获奖人员	指导教师
1.	中科院数学院院长奖学金优秀奖	付国锋	李子明
2.	中科院研究生院三好学生	郭庆东	支丽红
3.	中科院数学院院长奖学金优秀奖	吴小胜	李邦河
4.	许国志博士后工作奖励基金	梁野	支丽红
5.	中科院博时奖学金	马玥	支丽红
6.	中科院数学院院长奖学金特等奖	李伟	高小山
7.	ISSAC 杰出论文奖	李伟	高小山
8.	2011 年度中科院数学院十大科研进展	李伟	高小山
9.	中科院研究生院三好学生	李伟	高小山

注：全国百篇优秀博士学位论文、院长奖学金等。

四、科研工作与成果

（一）概述实验室年度承担课题情况，当年到位经费情况等。

本年度实验室承担国家基金委创新群体项目 1 项，

国家“973”计划项目 3 个课题，

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 3 项，

国家自然科学基金青年基金 3 项，

中国科学院重要方向性项目 1 项，

横向课题 1 项。

（二）按研究方向或研究单元，分别介绍本年度研究工作主要进展。

1、数学机械化

- **微分稀疏结式**

结式给出超定方程组有公共解的充分必要条件，是代数几何与符号计算的基本概念和消去理论的主要计算工具之一，同时也在多项式方程系统求解的复

杂度研究中被广泛应用。因为结式可以一步消去多个变元，它可以定义在系数是参数的方程系统上,而且应用结式可以高效地求解一类零维多项式方程系统，所以结式在很多情况下都是方程求解首选方法。代数稀疏结式由著名学者Gelfand 等于上世纪 90 年代提出，充分考虑了多项式的稀疏结构，它构成了稀疏消去理论的基石。稀疏结式的次数依赖于多项式的牛顿多面体和他们的混合体积，而不再是多项式的总次数，从而对稀疏方程求解取得实质性改进。

本工作建立了微分稀疏结式理论和计算微分稀疏结式的高效算法。关于微分结式的论文《Sparse Differential Resultant》获国际计算机协会(ACM)符号与代数计算专业委员会(SIGSAM)颁发的ISSAC 2011 唯一杰出论文奖。授奖词完整总结了论文的主要贡献 :“微分多项式系统结式是微分代数和结式理论中一个**重要、困难与全新（original）的问题**。作者**首次严格定义了微分结式和稀疏微分结式**，证明了稀疏微分结式的一些重要的性质，并设计了一个基于矩阵运算计算稀疏微分结式的单指数算法。该**高效算法**将会对应用数学和计算科学领域中若干问题起到影响。我们预计**这篇文章将会阐明并开启微分代数、结式理论、复杂性理论、线性代数和组合学中新问题的研究**。”

“ISSAC 杰出论文奖”由 ACM/SIGSAM 颁发，选自当年在 ISSAC 上报告的论文。ISSAC 是符号和代数计算方面最主要的国际会议，ISSAC2001 是第 36 届 ISSAC 会议。

- **微分 Chow 形式**

Chow 形式给出超定方程组与一个代数簇相交的充要条件 ,是代数几何的基本概念，在消去理论、超越数论、方程求解、代数计算复杂度方面有重要应用。

为了定义微分 Chow 形式，我们首先发展了微分一般(generic)相交理论、证明了**一般微分维数猜想**，即 r 个 n 变元一般微分多项式生成的微分理想$[f_1,\ldots,f_r]$的维数至少是 n-r ,还证明其阶数是 $f_1,\ldots,f_r$ 的阶数之和。以微分相交理论为基础，建立了微分 Chow 形式理论，证明了其基本性质，特别给出了微分周形式的 Poisson 类型的分解公式与一类微分代数 cycle 的周簇。作为应用，第一次严格定义了微分结式，并给出了其性质。

相关 58 页的论文已经被Trans of AMS接收。审稿人认为 :"这是一篇重要的、**开创性(ground-breaking)的文章**,有可能**极大地推动微分代数几何的深入研究**。作为代数周形式的一个**引人入胜(intriguing)而又完全自然的推广**，微分周形式应该引起代数几何学家们的重视。建立微分周形式的性质需要**独创力(ingenuity)**和对微分消去理论的全面知识。"

- **超指数-超几何函数的结构**

我们刻画了超指数-超几何函数的结构。这一结果可以用于 Zeilberger 算法的终止性判定问题。我们利用微分和差分代数给出了自动证明组合恒等式的著名方法 Creative Telescoping 在连续-离散情形下的终止条件，为算法实现提供了严格的数学基础；给出了 Creative-Telescoping 应用于有理函数的复杂度分析。相关结发表在符号计算主要会议 ISSAC2010 和 ISSAC2011。关于超几何-超指

数函函数结构的工作，审稿人评价:“已知的结果仅关于二元函数，该工作不仅刻画了多元的结构，而且还包括 q-情形，是一个**非常不平凡的推广(highly nontrivial generalization)。”应邀在 2011 年微分方程与计算机代数研讨会和 FoCM 大会的符号分析研讨会上做邀请报告。**

- **离散可微曲线上定义的有理常微分方程的近似有理解**

提出了离散可微曲线的概念，它由空间中的离散点列和附着在上面的离散射从构成，从而使得常微分方程可以定义在离散可微曲线。针对这种曲线上的有理常微分方程，研究它的近似有理解，提出了一个完全的算法，能够根据一步追踪法的追踪方式，自动生成近似有理符号解，而且保证算法不能生成近似有理符号解当且仅当原方程不存在近似有理解。

- **混合算法**

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。新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；特别地，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。

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，且该方法不要求多项式必须达到最优值，与同类方法比较，该方法计算更为简单，且不需要较强的假设条件。

矩阵恢复问题广泛地出现在控制、信号处理、系统识别等许多领域中。此问题可以凸松弛为矩阵核范数极小化问题，尽管此问题能利用半定规划方法求解，但此类方法存在计算量大、速度慢、处理的矩阵规模小等问题。针对计算中的关键问题，我们提出了一种新的求解 Gram 矩阵核范数极小化问题的一阶算法----改进的不动点迭代算法（FPC-BB），并给出了算法的收敛性分析。在此方法基础上，我们又提出一种加速的不动点迭代算法（AFPC-BB）。它既保持了 FPC-BB 算法的简单易实现的特点，又将原算法线性的收敛速度提高为二次收敛。数值实验显示我们的算法对于低秩 Gram 矩阵的近似或精确恢复问题较以往主流算法提速明显，且实现方便，占用内存少，更适合大规模矩阵的处理。近期研究发现，该算法还可以用于多项式系统的部分实根的快速求解。

- **非线性系统求解**

提出了 Bose-Einstein 凝聚态中原子输运过程中的非线性物理模型,即带源的变系数广义 GP 方程, 通过约化和 Mious 变换给出了该模型的很多类型的物理意义的解, 并且分析了解的演化规律, 以及与增益项和源振幅的关系, 这对于理论物理学家和实验人员的应用提供精确的依据. 发表在国际权威数学物理期刊

《Phys. Rev. A》上，该论文的解的图像入选被美国物理学会的 PRA Kaleidoscope 专栏，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》(2011. Vol. 3, No.9)收录。

研究了金融市场中的非线性耦合金融模型，解析地提出了向量金融畸形波解，并且分析了该解的演化规律，这或许为进一步研究金融危机和风暴提供有效的依据，该成果被国际著名期刊《Phys. Lett. A》接受，国际评审专家称："A strong technical paper, highly relevant for the current economic crisis"。

研究了(2+1)-维非局部 Schrodinger 方程，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，对于分析高维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。

首次提出了具有非线性色散项的变系数 K(m,n)模型，并且提出了该模型的含有任意可微函数的 compacton 解和孤波班图解，并且给出了 m=n 情况下模型的守恒律．发表在国际重要期刊《Appl. Math. Comput.》上。

- **参数 Grobener 基算法研究**

在 ISSAC 2011 上发表了计算多项式系统 Groebner 基的关于 F5 算法的一般化。同时证明其一般标准的正确性，并且在特定条件下证明了算法的终止性。

在 ISSAC 2011 上还发表了同时计算参数 Groebner 基和参数 Groebner 系统的高效算法。

对非交换情形的Groebner基计算进行了研究，提出了拟交换的概念，并在拟交换情形下，给出了一种计算Groebner基的判断标准，在此标准下进行Groebner基的计算的效率将大大提高。

2、信息安全

- **Cai-Cusick 密码体制的攻击**

基于格结构的密码被认为是最可能成功的抵抗量子攻击的密码体制。Cai-Cusick密码体制于 1998 年提出，是三个主要的格密码体制之一。国际上很多密码分析学者都曾试图攻击Cai-Cusick格密码体制，但都没有取得成功。我们改变了以往密码分析学者试图恢复私钥的做法，直接从恢复消息入手，成功地给出了十余年来首个对Cai-Cusick体制的有效的唯密文攻击，彻底攻破了该体制。这一结果发表在IEEE Transactions on Information Theory．审稿意见称“The paper **completely break（完全攻破）** the Cai-Cusick lattice-based cryptosystem。”“The attack is **quite efficient**, having essentially the same complexity as decoding using the legitimate private key”。

- **布尔函数的构造**

具有好的密码性质的布尔函数在流密码和分组密码的设计中起着核心的作用。代数免疫度反映了布尔函数抵抗代数攻击的能力，具有最优代数免疫度的布尔函数的构造在近几年的研究中十分热门。非线性度量化了布尔函数抵抗线性攻击的能力，Bent 函数即是具有最高非线性度的布尔函数。我们在这方面的工作有两篇论文：

(1) 构造了具有最优代数免疫度的Bent函数，这是第一次构造出非线性度和代数免疫度都最优的布尔函数。还构造了具有多项最优密码性质的布尔函数，即平衡的，具有最优代数次数，具有最优代数免疫度，非线性度至今最好的布

尔函数。加拿大滑铁卢大学龚光教授评价说“I believe that it is the best work that I have seen in recent years。”该项成果发表在国际著名杂志Designs，Codes and Cryptography 2011，已经被引用18次。

(2) 构造了平衡的，1-弹性的，具有最优代数次数，具有最优代数免疫度，非线性度很高的布尔函数。这是首次构造具有如此之多的密码性质的布尔函数。该论文已被国际著名杂志Discrete Applied Mathematics接受发表。审稿意见认为“I find this paper suitable for publishing in DAM journal since it presents an important method for the design of cryptographically strong Boolean functions，and at the same time this work is of **great importance（非常重要）** for the future research in this field”。

另外，我们在论文中提出了关于整数模加法进位的一个猜想，该猜想在我们的布尔函数的构造中发挥了关键的作用，现在该猜想引起了国际上的极大兴趣，并称其为**“Tu-Deng猜想”**，在欧洲和美国有多个研究团队试图解决我们的猜想，取得了一些部分结果并发表了论文。

- **序列与有限域上方程求解的近似算法**

我们在对多条序列的研究中提出了严格最佳有理逼近的新定义，并给出了与之相应的综合问题的算法．这种方式放弃了逼近时对公分母的要求而允许有不同的分母出现，能得到的逼近轮廓包含有所给定的多条序列的更多信息，还研究了这两种逼近的关系．结果发表在信息论的主要杂志 IEEE Trans. Inform. Theory。

有限域上方程组求解是密码学中非常重要的问题，该问题已被证明是 NP-完全问题，所以考虑其优化问题的近似算法具有很重要的意义。我们研究了有限域上二次方程组求解的近似算法，即 MAX-MQ 问题。证明了随机赋值方法是 MAX-MQ 问题的一个近似比为 q+q^(-n/2)的多项式时间算法，其中 q 是域的元素个数，n 是变元数。这一结果发展了国际著名的理论计算机学家 Håstad(1993)的结果，并结合 Håstad(2001)的结果，得出 MAX-MQ 问题的极小近似比为 q，从而彻底给出了该问题近似算法的复杂性估计。该结果发表在 Theoretical Computer Science 上。

3、数控系统关键算法

- **jounce（加加速度关于时间的一阶导数）有界条件下的最优插补**

在数控装置中，为了保证机床在启动或停止时不产生冲击或震动,必须设计专门的加减速控制规则。高速高精数控系统中，更应避免加减速结束时的加速度突变，以减小机械冲击,得到好的加工效果。实际测验告诉我们，对加加速度进行限制可以有效地减少震动，提高加工质量。我们探讨了 jounce（加加速度关于时间的一阶导数）有界条件下的速度规划问题。提出一种基于样条曲线的加加速度连续的速度规划算法，避免了加速度的跳跃。速度规划采用“七段”式的加加速度方式,既做到加加速度的连续，又尽量加快加工速度。最后，将所提出的算法应用到实际的加工仿真实例中。从最终的仿真结果上看，基本上达到了预期的效果。

（三）介绍本年度实验室重大成果及其水平和影响等。

- **微分 Chow 形式与微分结式**

方程求解的消去理论与符号算法是数学机械化的主要研究内容,也是数学机械化方法诸多应用的基础。本工作将方程符号求解的基本概念与重要工具—稀疏结式与 Chow 形式—推广到了代数微分方程情形。本工作给出了一般(generic)微分相交理论,建立了微分 Chow 形式理论,证明了其基本性质。建立了 Laurent 微分多项式系统的微分稀疏结式理论并给出了计算稀疏结式的高效算法。

关于微分结式的论文获国际计算机协会(ACM)符号与代数计算专业委员会(SIGSAM)颁发的 2011 唯一“ISSAC 杰出论文奖”。授奖词完整总结了论文的主要贡献：“微分多项式系统的结式是微分代数和结式理论中一个**重要、困难与全**

新（original）的问题。作者**首次严格定义了微分结式和稀疏微分结式**，证明了稀疏微分结式的一些**重要性质**，并设计了一个基于矩阵运算计算稀疏微分结式的单指数算法。该**高效算法**将会对应用数学和计算科学领域中若干问题**起到影响。**我们预计**这篇文章将会阐明并开启微分代数、结式理论、复杂性理论、线性代数和组合学中新问题的研究。**”

关于微分Chow形式的58页的论文已经被Trans of AMS接收。审稿人认为 :“这是一篇重要的、**开创性(ground-breaking)的文章**,有可能**极大地推动微分代数几何的深入研究。**作为代数**Chow**形式的一个**引人入胜(intriguing)而又完全自然的推广**，微分周形式应该引起代数几何学家们的重视。作为关于微分周形式的**首篇论文**，它提供了从微分多项式代数中的符号计算到符号计算在微分多项式理想零点几何中的应用的一个**急需过渡(much-needed transition)。**建立微分周形式的性质需要**独创力(ingenuity)**和对微分消去理论的全面知识。”

- **Cai-Cusick 密码体制的攻击**

基于格结构的密码被认为是最可能成功的抵抗量子攻击的密码体制。Cai-Cusick密码体制于 1998 年提出，是三个主要的格密码体制之一。国际上很多密码分析学者都曾试图攻击Cai-Cusick格密码体制，但都没有取得成功。我们改变了以往密码分析学者试图恢复私钥的做法，直接从恢复消息入手，成功地给出了十余年来首个对Cai-Cusick体制的有效的唯密文攻击，彻底攻破了该体制。这一结果发表在IEEE Transactions on Information Theory．审稿意见称“The paper **completely break（完全攻破）** the Cai-Cusick lattice-based cryptosystem。”“The attack is **quite efficient**, having essentially the same complexity as decoding using the legitimate private key”。

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	2010.8	2015.8			高小山
2.	“973”计划项目子课题	数学机械化理论与算法	2010.8	2015.8	414	298	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	2010.8	2015.8	249	179	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	2010.8	2015.8	329	236	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	2008	2011	550	50	高小山
6.	国家杰出青年基金项目	高级几何不变量方法	2009	2012	140		李洪波
7.	国家基金重点项目	代数的组合及同调方法	2008	2011	140		万哲先
8.	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		王定康
9.	国家自然科学基金面上项目	经典几何的符号计算与几何分解	2009	2011	18		李洪波

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		胡磊
11.	横向	密码学理论	2009	2011	10		高小山
12.	中国科学院方向性项目	复杂系统研究	2010	2012	200		高小山
13.	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	16	程进三
14.	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
15.	青年基金	安全多方计算的模型和方法研究	2011	2013.	16	6.4	张志芳
16.	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
17.	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
合计	---	---	---	---		812.6	---

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			（45 万/30 万欧元）		支丽红
2	法国	INRIA, France	中法联合培养博士项目	2007	2011	1 万欧元		李子明
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
	信息工程研究所	密码学研究	2009	2012	30		高小山
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.	十一五’国家科技计划执行突出贡献奖，2011，科技部			高小山
2.	2011 年度 ISSAC 杰出论文奖			李伟，袁春明，高小山
3.	2011 年度中科院数学院十大科研进展			李伟，袁春明，高小山
4.	2011 年度中科院数学院十大科研进展			闫振亚

发表论文列表

序号	论文题目	刊物名称/卷期页码	作者	通讯作者	影响因子
1	Sparse Differential Resultant	Proc. ISSAC 2011, ACM Press, San Jose, 225-232, 2011.	W. Li, X.S. Gao, C.M. Yuan,	X.S. Gao	
2	Threshold Changeable Secret Sharing Schemes Revisited	Theoretical Computer Science, 418: 106-115 (2012).	Z. Zhang, Y. Chee, S. Lin, M. Liu, H. Wang	Z. Zhang	
3	On the structure of compatible rational functions	Proc. ISSAC 2011，pp. 91-98	Shaoshi Chen ,Ruyong Feng， Guofeng Fu	Shaoshi Chen	
4	微分、差分域中的 Wronskian 行列式	系统科学与数学 ,2011 年 31(5) 620-628	李应弘，冯如勇	冯如勇	
5	理性密钥共享的扩展博弈模型	中国科学：信息科学, 2012, 42(1) 32-46.	张志芳, 刘木兰	张志芳	
6	数控机床高速微线段插补算法与自适应前瞻处理	中国科学, 技术科学 E 辑, 2011, 6(41), 744-789	张立先, 孙瑞勇, 高小山, 李洪波	李洪波	
7	Approximate Rational Solutions to Rational ODEs Defined on Discrete Differentiable Curves.	Proceedings of ISSAC 2011, pp. 217-224, June 8-11, San Jose, USA	Hongbo Li, Ruiyong Sun, Shoubin Yao, Ge Li	Hongbo Li	

8	Line Geometry in Terms of the Null Geometric Algebra over R(3,3)	Guide to Geometric Algebra in Practice, Springer London, 2011, pp. 253-272	Hongbo Li, Lixian Zhang	Hongbo Li	
9	On Geometric Theorem Proving with Null Geometric Algebra.	Guide to Geometric Algebra in Practice, Springer London, 2011, pp. 195-215	Hongbo Li, Yuanhao Cao.	Hongbo Li	
10	Projective geometric theorem-proving with Grassmann-Cayley algebra.	Hermann Grassmann, from Past to Future, Springer Basel AG, pp. 275-286, 2011	Hongbo Li	Hongbo Li	
11	Rogon-like solutions excited in the two-dimensional nonlocal nonlinear Schrödinger equation	Journal of Mathematical Analysis andAppl. 2011卷 82 期 3 页码 036610	Yan Zhenya	Yan Zhenya	
12	Nonautonomous matter waves in a waveguide	PHYSICAL REVIEW A 2011卷 84 期 6 页码 023627	Yan Zhenya， Xiao-fei Zhang，W. M. Liu	Yan Zhenya	
13	Vector financial rogue waves	Phys. Lett. A 2011卷 375 期 29 页 码 4274	Yan Zhenya	Yan Zhenya	
14	Exact solutions of nonlinear dispersive K(m,n) model with variable coefficients	Applied Mathematics and Computation 2011卷 217 期	Yan Zhenya	Yan Zhenya	
15	Curve fitting and optimal interpolation on CNC machines based on quadratic B-splines.	Science China, Information Sciences, 54(7), 1407-1418, 2011.	M. Zhang, W. Yan, C.M. Yuan, D.K. Wang and X.S.Gao	M. Zhang	

16	Collision and intersection detection of two ruled surfaces using bracket method	Computer Aided Geometric Design 28, 114-126,2011.	Y. Chen, L.Y. Shen, C.M. Yuan	Y. Chen	
17	A general NTRU-like framework for constructing lattice-based public-key cryptosystems	In: S. Jung and M. Yung (Eds.): WISA 2011, Springer LNCS Vol.7115, pp. 109–120(2011)	Yanbin Pan, Yingpu Deng	Yingpu Deng	
18	Solving Polynomial Systems via Symbolic-Numeric Reduction to Geometric Involutive Form	Journal of Symbolic Computation, 3(47), pp 227-238, 2012/3/1	Xiaoli Wu and Lihong Zhi	Lihong Zhi	
19	Global optimization of polynomials restricted to a smooth variety using sums of squares	Journal of Symbolic Computation	Aurelien Greuet, Feng Guo, Mohab Safey El Din, Lihong Zhi	Lihong Zhi	
20	Computing the multiplicity structure of an isolated singular solution: case of breadth one	Journal of Symbolic Computation	Nan Li and Lihong Zhi	Lihong Zhi	
21	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	Kaltofen, Erich L., Li, Bin,Yang, Zhengfeng, Zhi,Lihong	Lihong Zhi	
22	Computing Isolated Singular Solutions of Polynomial Systems: Case of Breadth One	SIAM Journal of Numerical Analysis	Nan Li and Lihong Zhi	Lihong Zhi	
23	The Minimum-Rank Gram Matrix Completion via Modified Fixed Point Continuation Method	ISSAC 2011, pp 241-248, 2011/6/8	Yue Ma and Lihong Zhi	Lihong Zhi	
24	Computing Comprehensive Groebner Systems and Comprehensive Groebner Bases Simultaneously	Proc. ISSAC 2011, ACM Press, San Jose, 337-344, 2011.	D.Kapur, Y. Sun, D.K.Wang	D.K. Wang	

25	A Generalized Criterion for Signature Related Groebner Basis Algorithms	Proc. ISSAC 2011, ACM Press, San Jose, 193-200, 2011.	Y. Sun, D.K. Wang	D.K. Wang	
26	On Computing Groebner Bases in the Rings of Differential Operators	Science China, Series A. June 2011 Vol. 54 No. 6: 1077-1087	X.D. Ma, Y. Sun D.K.Wang	D.K. Wang	
27	The F5 Algorithm in Buchberger's Style	J Syst Sci Complex (2011) 24: 1218–1231	Y.Sun D.K.Wang	D.K. Wang	
28	Intersection Theory in Differential Algebraic Geometry: Generic Intersections and the Differential Chow Form	Accepted by Trans. AMD	X.S. Gao, W. Li, C.M. Yuan		
29	Characteristic Set Algorithms for Equation Solving in Finite Fields	Accepted by Journal of Symbolic Computation	X.S. Gao and Z. Huang.		
30	Root Isolation of Zero-dimensional Polynomial Systems with Linear Univariate Representation	Accepted by Journal of Symbolic Computation	J.S. Cheng, X.S. Gao, L. Guo		
31	A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity.	Designs, Codes and Cryptography, Vol.60, No.1, 1—14 (2011).	Ziran Tu, Yingpu Deng		
32	Proper Reparametrization for inherently improper unirational varieties	Journal of Systems Science and Complexity, 24(2), 367-380, 2011	L. Shen, E. Chionh, X.S. Gao, J. Li.		
33	An Introduction to Java Geometry Expert	ADG 2008, LNAI 6301, 189-195, Springer, 2011	Zheng Ye, Shang-Ching Chou, and Xiao-Shan Gao		
34	A ciphertext-only attack against the Cai-Cusick lattice-based public-key cryptosystem.	IEEE Transactions on Information Theory, Vol.57, No.3, 1780—1785 (2011).	Yanbin Pan, Yingpu Deng		

35	A new lattice-based public-key cryptosystem mixed with a knapsack.	In: D. Lin, G. Tsudik, and X. Wang (Eds.): CANS 2011, Springer LNCS Vol.7092, pp. 126–137(2011)	Yanbin Pan, Yingpu Deng, Yupeng Jiang, Ziran Tu		
36	Subsconstituents of orthogonal graphs of odd characteristic	Linear Algebra and its Applications;434(2011)2430-2447	Zhe-Xian Wan;Zhen-hua Gu		
37	Almost all points on the real axis can be original points of shock waves	SCIENCE CHINA; January 2011 Vol. 54 No. 1: 1-8	LI Bang-He		
38	Young measures as probability distributions of Loeb spaces	Proc. Amer. Math. Soc. 140 (2012), no. 1, 207–215.	Li, Bang-He;Li, Tian-Hong		
39	An improved method to measure all rate constants in the simplest enzyme kinetics model	Journal of Mathematical Chemistry	Banghe Li, Bo Li and Yuefeng Shen		

出版专著

序号	著作名称	作者	出版单位	出版日期
1	Finte Fields and Galois Rings	Zhe-Xian Wan	World Scientific,Singapore	2011

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

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.	973 项目“数学机械化方法及其在数字化设计制造中的应用”项目启动与学术交流会	国内	中科院数学院	高小山	2011.3.17-18	50
2.	“可信计算国际会议”	国际	中科院数学院	支丽红	2011.7.7-20	60
3.	计算机辅助制造工程和数控中的数学与算法	国际	中科院数学院	李洪波	2011.10.24-26	80
4.	信息安全与密码学术研讨会	国内	信息安全中心	万哲先	2011.10.24-26	45
5.	“数学机械化方法及其在数字化设计制造中的应用”	国内	中科院数学院	高小山	2011.11.26-28	150
6.	第四届全国计算机数学学术交流会	国内	中科院数学院	李子明	2011.11.26-28	

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.	Topological Classification of Intersection Curves of Two Ring Tori	贾晓红	Geometric Modelling 2011, Dagstuhl, Germany	德国莱布尼茨数学中心	2011.05

2.	Distribution-Aware image Color Transfer	贾晓红	Siggraph Asia 2011	香港城市大学	2011.12
3.	An algebraic approach for continuous collision detection of two ellipsoids	贾晓红	International Workshop on Mathematics and Algorithms for Computer Aided Manufacturing, Engineering and numerical control	北京	2011.11
4.	Approximate rational solutions of rational ODEs defined on differentiable discrete curves	李洪波	ISSAC 2011	美国	2011.6
5.	Exact solution of path planning with constant scallop height	李洪波	MAMENC	北京	2011.10
6.	Differential Chow Form and Differential resultant	袁春明	Foundations of Computational Mathematics(FoCM'11)	匈牙利布达佩斯	2011.7.12-14
7.	Differential Chow Form and Differential Resultant	高小山	Second Workshop on Differential Equations by Algebra Methods.	Austria	2011.2.8-12
8.	Time-optimal interpolation for CNC machining	高小山	7th International Congress on Industrial & Applied Mathematics	Canada	July 18 – 22
9.	Sparse Differential Resultant	高小山	ACM ISSAC 2011	USA	6 月 6 - 12
10.	Time-Optimal Interpolation Algorithms for CNC Machining	高小山	数学与机械学博士生交叉学科创新论坛	武汉	2011 年 10 月 27 31
11.	On the structure of Comaptible Rational Functions	李子明	微分方程和计算机代数研讨会	奥地利	2011.2

12.		李子明	第 36 届国际符号与代数计算年会	美国圣荷西	2011.6
13.	Termination Criteriaon Creative Telescoping （邀请）	李子明	计算数学基础大会	匈牙利	2011.7
14.	Solving Singular Polynomial Systems via Symbolic-numeric method	支丽红	国际符号与代数计算年会（ISSAC）	美国	2011.6
15.		支丽红	国际符号和数值计算会议（SNC）	美国	2011.6
16.		闫振亚	国际理论中心(ICTP)	意大利	2011.06.01-15
17.	大会邀请报告	闫振亚	International Symposium on PT-symmetric non-Hermitian Quantum Mechanics	德国	2011.9
18.	大会邀请报告	闫振亚	Cross-Strait Conference on integrable systems and related Topics	江苏常熟	2011.10
19.	Recollement and Hochschild theory （邀请报告）	韩阳	海峡两岸代数学学术研讨会	厦门	2011.7.11-7.15
20.	Recollement and Hochschild theory （邀请报告）	韩阳	Shanghai conference on representation theory of algebras	上海	Ocotober 2-7, 2011
21.	大会邀请报告	邓映蒲	中国密码学会密码数学理论专业委员会 2011 年度学术研讨会	北京	2011.12

22.	大会邀请报告	邓映蒲	第三届编码与密码的数学理论研讨会	天津	2011.7
23.	A General NTRU-Like Framework for Constructing Lattice-Based Public-Key Cryptosystems	潘彦斌	The 12th International Workshop on Information Security Applications (WISA2011)	韩国济州	2011.8
24.	A New Lattice-Based Public Key Cryptosystem Mixed with a Knapsack	潘彦斌	The 10th International Conference on Cryptography and Network Security	三亚	2011.12

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.	Reid-Zhi 混合消元法的应用	2011.5	2011.12	1	1	吴 晓丽	支丽红
2.	复杂非线性波方程解的构造研究和动力学分析	2011.5	2011.12	1	1	王 晓丽	闫振亚
3.	复杂曲面数控加工中的干涉检测方法	2011.5	2011.12	1	1	韩丽	高小山
4.	基于 Isabelle/HOL 的自动证明技术与应用研究	2011.5	2011.12	1	1	陈光喜	刘卓军
5.	Einstein 求和约定下的多项式化简和标准型	2011.5	2011.12	1	1	刘姜	李洪波

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、2011年3月，实验室高小山研究员被国家科技部授予“十一五”国家科技计划执行突出贡献奖。 他负责的973项目“数学机械化及其在信息技术中的应用”在数学机械化方法及其在 信息安全理论、生物特征识别、几何建模、并联数控机床领域的应用取得重要成果。

2、 国家重点基础研究发展规划项目——“数学机械化方法及其在数字化设计制造中的应用”项目启动与学术交流会于2011年3月17日—18日在京召开。出席本次会议的有科技部基础司重大项目处张延东处长与李非博士、科技部基础研究管理中心宋海刚博士、国家基金委数理学部数学处雷天刚处长、中科院基础局数理处王永祥处长、数学与系统科学研究院王跃飞书记，以及项目咨询组专家何新贵院士、强文义教授，项目专家组成员吴文俊、万哲先、熊有伦、李邦河、林惠民院士等。项目负责人高小山研究员主持会议。

张延东处长在讲话中指出， “十二五”期间，973项目应该特别注意三个方面。一是应重点突出、涉及面不宜太广，要重点研究面向若干国家重大需求的关键问题；二是更加突出强化科学目标导向，从需求中提炼重大科学问题，推动我国基础研究的发展；三是更加注重团队建设。他希望本项目在前期取得的突出成绩的基础上，再上一个台阶。

王永祥处长强调，科学院的办院方针是面向国家战略需求，面向世界科学前沿，加强原始科学创新，加强关键技术创新与集成，为国家安全和社会可持续发展做出贡献。科学院将继续发挥基础研究的优势，将其转化成变革性技术，从而推动产业结构的升级。作为项目的依托单位，将继续为项目提供良好的环境和平台。

王跃飞书记首先对科技部和科学院对数学院的支持表示感谢，表示数学院将从人力、物力、财力上继续对973项目进行大力支持，保证项目的顺利实施，希望项目在中国科学院国家数学与交叉科学中心的平台上圆满完成任务。

熊有伦与李邦河院士代表项目专家组发言。他们指出，数字化、信息化、智能化、网络化代表了制造领域的主流方向，在工程和制造领域，将问题深层次化后就会变成数学问题，如何实现从制造到制造科学的飞跃，数学机械化是非常重要的，并期望本项目在数学与先进制造交叉领域取得辉煌成果。

高小山介绍了立项背景、研究内容、预期目标、课题设置、研究队伍、工

作安排等。他指出，本项目将重点从“数学机械化理论与高效算法”和“数字化设计制造与数控系统”两大方面来进行研究，针对数字化设计制造与数控系统核心问题，发展高效算法，达到实时性、精确性、最优化；总结出有共性的数学与算法问题，开拓数学机械化新方向，努力保持我们的特色与在若干方面的领先地位。

项目组成员及相关领域的专家学者50余人出席了会议。与会专家就数学机械化最新进展与数字化设计与数控系统核心问题进行了学术交流。

3、2011年6月8日-11日，在美国圣荷西(硅谷, San Jose, USA) 召开的第36届国际符号和代数计算会议(ACM ISSAC'11)上，本实验室有7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。7篇被接收论文是

1) Hongbo Li, Ruiyong Sun, Shoubin Yao and Ge Li. Approximate Rational Solutions for Rational ODEs Defined on Discrete Differentiable Curves.
2) Wei Li, Xiao-Shan Gao and Chun-Ming Yuan. Sparse Differential Resultant.
3) Shaoshi Chen, Ruyong Feng, Guofeng Fu and Ziming Li. On the Structure of Compatible Rational Functions.
4) Leilei Guo and Feng Liu. An Algorithm for Computing Set-Theoretic Generators of an Algebraic Variety.
5) Yue Ma and Lihong Zhi. The Minimum-Rank Gram Matrix Completion via Fixed Point Continuation Method.
6) Yao Sun and Dingkang Wang. A Generalized Criterion for Signature Related Groebner Basis Algorithms.

7) Deepak Kapur, Yao Sun and Dingkang Wang. Computing Comprehensive Groebner Systems and Comprehensive Groebner Bases Simultaneously.

其中，李伟、高小山研究员和袁春明助理研究员的论文荣获唯一的杰出论文奖。授奖词指出：“微分多项式系统结式是微分代数和结式理论中一个重要、困难与全新的问题。作者首次严格定义了微分结式和稀疏微分结式，证明了稀疏微分结式的一些重要的性质，并设计了一个基于矩阵运算计算稀疏微分结式的单指数算法。该高效算法将会对应用数学和计算科学领域中若干问题起到影响。我们预计这篇文章将会阐明并开启微分代数、结式理论、复杂性理论、线性代数和组合学中新问题的研究。”

获奖论文是同一课题组关于微分相交理论、微分周(Chow)形式与微分结式系列工作的一部分。此前，他们关于微分周形式的长文已经被Trans of AMS接收。审稿人认为：“这是一篇重要的、开创性的文章,有可能极大地推动微分代数几何的深入研究。作为代数周形式的一个引人入胜而又完全自然的推广，微分周形式应该引起代数几何学家们的重视。建立微分周形式的性质需要独创力和对微分消去理论的全面知识。”

“ISSAC杰出论文奖”由“国际计算机科学协会(ACM)”符号与代数计算专业委员会颁发，选自当年度在ISSAC上报告的论文。ISSAC是符号和代数计算方面最权威的国际会议。这是本次会议颁发的唯一杰出论文奖。

4、 由中国科学院数学与系统科学研究院主办，法国巴黎六大、广西民族大学协办的“可信计算国际会议”（International Workshop on Certified and Reliable Computation）于2011年7月17-20日在广西南宁召开。来自美国、法国、英国、加拿大、比利时、中国香港和内地近60名专家学者和研究生 参加了此次会议。

本次会议围绕就如何为科学工程计算和信息技术领域出现的实际问题提供可靠的或可验证的计算解决方案，会议报告了基于符号计算、数值计算、 符号和数值混合计算的可信算法在机器人、生物、信号处理、密码学等领域中的最新进展。大会共邀请9位国际知名学者作邀请报告，23人作会议报告。会议的召开为更好地发挥我国在符号和数值计算已有的优势，继续研究快速、稳定、误差可控的算法，以及我国可信计算软件的开发和研制提供更有效的数学方法。本次会议 的圆满召开，得到中国科学院数学与系统科学研究院，科技部973项目，国家基金委中法合作项目，中法计算科学、自动化和应用数学联合实验室，广西民族大学，数学机械化重点实验室的大力支持。

5、由中科院数学院信息安全中心主办的信息安全与密码学术研讨会于2011年10月13日至15日在杭州召开，来自中科院数学院，中科院软件所，中科院研究生院，北京大学，北京航空航天大学，复旦大学，上海大学，广州大学，山西大学等单位的专家学者和研究生共四十多人参加了会议。

本次会议围绕密码学和信息安全领域的重要数学问题进行讨论，邀请了六位国内知名学者就相关问题作了精彩报告，内容涵盖了密码学基础理论部分的秘密共享理论和椭圆曲线密码体质，以及当前广泛关注和研究的量子密码和多变量密码，还介绍了网络环境下实体定位的安全性问题。这些报告反映了当前密码学和信息安全领域研究的前沿问题，兼顾了理论研究热点和实际应用需求，具有很好的启发性和拓展性。此次会议给该领域的学者和青年学生提供了一个良好的合作与交流平台，对于我单位在国内信息安全和密码研究领域的深入发展起到积极的推动作用。

6、由国家数学与交叉科学研究中心先进制造交叉研究部主办的计算机辅助制造工程和数控中的数学与算法国际会议于10月24日-26日在数学院召开。来自美国、 意大利、韩国以及清华大学、华中科技大学、中国科技大学、北京航空航天大学、中科院数学院等国内各高校和研究单位的80余位专家及研究生参加会议。

大会报告涉及数字化加工制造和数控系统控制的诸多领域，包括五轴数控加工中的路径规划、CAD/CAM 在工业和医疗中的应用、机器人路径规划、数控加工最优插补算法、数控加工中的误差补偿等方面。华中科技大学的熊有伦院士、美国加州大学戴维斯分校的 Rida T. Farouki 教授、意大利乌迪内大学的 Alessandro Gasparetto 教授、 台湾国立中正大学的 Hong-Tzong Yau 教授、中科院数学与系统科学研究院的高小山研究员等分别做相关研究方向的大会邀请报告。此外，来自全国各高校和科研单位的 30 余位老师和研究生也做了学术报告。此次国际会议的召开，促进了国内外数字化制造领域各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融合起了重要作用。

7、973 项目“数学机械化方法及其在数字化设计制造中的应用”2011 年度总结与第四届计算机数学(CM2011)学术交流会于 11 月 26 日至 28 日在广州大学召开。来自国内科研院所、大专院校的专家学者及在校学生近 150 人参加了会议。

本次会议由中国数学会计算机数学专业委员会主办，广州大学计算机科学与教育软件学院、广州大学数学与信息科学学院、中国科学院数学机械化重点实验室共同承办。广州大学张景中院士任大会主席。会议期间，克莱姆森大学（Clemson University）终身教授高绪洪(Shuhong Gao)作题为“Primary decomposition of polynomial ideals”、中国科学院研究生院胡磊教授作题为“方程求解与代数密码分析”、首都师范大学教授辛国策作题为“MacMahon 分拆分析在固定维数下的多项式算法”的特邀报告。此外，会议还安排 55 位专家学者做专题报告，内容涉及信息安全、微分方程、数控系统、多项式代数、符号与

数值计算、计算机数学应用、图像处理与计算几何、微分差分代数、计算几何与自动推理、实代数等内容，这些报告基本反映了我国当前计算机数学的研究动态和展现了计算机数学研究与应用的学术水平。与会人员围绕上述报告进行了广泛、深入的交流，会场内外学术氛围浓郁、研讨热烈。

会上，973 项目"数学机械化方法及其在数字化设计制造中的应用" 课题组分四组做了专题汇报会，汇报了项目的进展情况和研究成果。

8、实验室李伟、高小山研究员和袁春明助理研究员关于微分周形式和微分结式的工作，以及实验室闫振亚研究员关于金融畸形波（financial rogue waves）的工作被评为2011年度中科院数学院十大科研进展中的两项。闫振亚首次得到了一类非线性期权价格模型两种类型的精确解，即金融畸形波解。这一工作被美国麻省理工学院百年期刊《技术评论》以“经济物理学家预言畸形金融波”为题进行了报道。 另外，美国百年期刊《大众科学》也对这一工作以“经济物理学家认为畸形波可以解释金融市场的波动性”为题进行了报道。