Printed in Beijing

2010
ANNUAL REPORT

中国科学院数学机械化重点实验室

2010年度报告

数学机械化重点实验室
Key Laboratory of Mathematics Mechanization
Address: No.55, Zhongguancun Donglu, Beijing 100190
Tel: 86-10-62541834
Fax: 86-10-62630706
Http://www.mmrc.iss.ac.cn/

Key Laboratory of Mathematics Mechanization
Chinese Academy of Sciences

目 录

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	应用数学	070104	基础数学	070101	管理科学与工程	120100
博士点	基础数学	70101	应用数学	70104	管理科学与工程	120100
博士后站	基础数学	70101	应用数学	70104		

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

1. 数学机械化研究的意义与实验室的发展简介

在目前的信息时代，计算机可以认为是人脑的延伸，电子计算机的飞速发展，为人类实现脑力劳动的机械化创造了物质条件。逐步实现脑力劳动机械化，将为科学研究与高新技术创新提供有力工具，使科研工作者摆脱繁琐的甚至是人力难以胜任的工作，将自己的聪明才智集中到更高层次的创新性研究上，提高我国知识与技术创新的效率。在以产业革命为先导的体力劳动机械化过程中，我国落后于发达国家，长期处于被动的局面。今天，脑力劳动机械化的进程刚刚起步，我们应该牢牢把握这个机遇，努力使我国在知识经济时代居于有利地位。

实现数学的机械化是实现脑力劳动机械化的重要基础。数学为其他学科提供描述问题的语言与解决问题的有效方法，是自然科学与高新技术的重要理论基础，是联络科学与技术的纽带。正是由于数学的基础性，每个时代都有与之相适应的数学。为利用计算机的强大计算能力，数学的很大一部分内容正在转变为计算机可以理解的语言和可以操作的对象，具体讲就是数学的离散化、算法化与软件化。这样的数学可以称之为机械化数学。

上世纪五十年代，电子计算机刚刚产生，人工智能的创始者 Newell 等人就开始研究用计算机证明数学定理。这些研究在理论上取得了重大进展，出现了以 Robinson 归结法为代表的一系列方法。但在证明效率上，这些方法未能取得本质突破。二十世纪七十年代出现了符号计算研究领域，研究具体数学问题的求解与计算方法。MIT 推出了第一代符号计算通用软件 MACSYMA，产生了轰动性影响。今天，数学和计算机的交叉正在成为数学发展的主要潮流之一，产生了诸如计算代数、计算数论、计算群论、计算几何等新兴学科。符号计算研究还导致了 Maple、Mathematica 等商用数学软件的出现，在科学与高新技术研究中得到广泛应用。

正是在此背景下，吴文俊院士在二十世纪七十年代提出了数学机械化的设想，概括为如下的**“数学机械化纲领”**:

- **在数学的各个学科选择适当的范围实现机械化，推动数学发展与脑力劳动机械化;**
- **应用数学机械化方法解决相关高科技领域的关键问题。**

1990 年，中国科学院批准成立“数学机械化中心”。科学院在中心成立的批复中指出：**“为了保证吴文俊教授建立的机器证明理论持续不断地发展，进一步形成数学机械化研究的良好环境，经研究，同意你所(系统所)建立《中国科学院系统科学所数学机械化研究中心》”。**强调“望你所按照科技体制改革的精神，以开放实验室的方式，联合国内外学术力量，为数学机械化研究做出更大的成绩”。

数学机械化研究中心建立以来，取得了一系列高水平的科研成果，并获得了数十项国内重要奖励与六项重要国际奖励，包括国家最高科技奖(00)，劭逸夫数学奖(06)，Herbrand 自动推理杰出成就奖(97)，第三世界科学院数学奖(90)，陈嘉庚数理科学奖(93)、香港求是科技基金会杰出科学家奖(94)，国家自然科学二等奖一项(97)，中科院自然科学一等奖(95)，求是杰出青年学者奖两项(98,99)，ACM/SIGSAM 杰出论文奖两项(06,07)。数学机械化中心还做为主持单位承担了八五国家攀登计划项目，九五攀登项目与两个“973”项目。

实验室万哲先院士从 20 世纪 60 年代开始，在离散数学的重要方向：有限域上典型群的几何学取得系统的研究成果，并开创了该方向的多个应用领域，包括区组设计、格、编码理论及信息安全中的认证码等。万哲先还是我国最早从事信息安全与通讯理论中的编码和密码学研究的几个数学家之一。他的工作不仅在国内外获得同行的广泛引用，还为我国国防建设做出了重要贡献，曾获中国科学院科技进步一等奖，国家自然科学三等奖，中国科学院自然科学奖一等奖和华罗庚奖。为加强离散数学与信息安全方面的研究，数学与系统科学研究院于 2001 年成立“信息安全研究中心”。

2002 年，中国科学院批准以“数学机械化中心”与“信息安全研究中心”为基础，成立数学机械化重点实验室。**实验室在 2004 年科学院组织的数理学科重点实验室评估中被评为优秀。**

2. 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。

3. 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.	吴　可	男	中国	委员	教授	否	首都师范大学
10.	张继平	男	中国	委员	教授	否	北京大学
11.	李克正	男	中国	委员	教授	否	首都师范大学
12.	冯克勤	男	中国	委员	教授	否	清华大学
13.	陈永川	男	中国	委员	教授	否	南开大学
14.	李华	男	中国	委员	研究员	否	中科院计算机所
15.	王晓云	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、研究队伍单元

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、潘延斌
3.	高档数控系统研究组	高小山、李洪波、王定康	袁春明

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、有限几何	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	计算代数、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、微分方程	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	符号计算、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、软件开发	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、符号计算	研究
15.	冯如勇	男	1978.6		副研	符号计算	研究
16.	袁春明	男	1979.12		助研	符号计算	研究
17.	张志芳	女	1980.10		助研	信息安全	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.	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
2.	李洪波	杰青、百人	1997
3.	孙笑涛	杰青、百人	
4.	胡　磊	百人	

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.	万哲先	天津南开大学组合中心学术委员会	主任		
2.	万哲先	福州大学“离散数学与理论计算机科学研究中心”学术委员会	主任		
3.	万哲先	山东理工大学学术委员会	主任		
4.	高小山	国际符号与代数年会(ISSAC)指导委员会	主席	2008	2009
5.	高小山	ACM SIGSAM Jenks 软件奖评审委员会	成员	2010	2011
6.	高小山	中国数学会计算机数学专业委员会	主任	2007	2011
7.	高小山	中国系统工程学会	副理事长	2010	2014
8.	高小山	中国工业与应用数学会	常务理事	2009	2012
9.	高小山	中国图学学会	常务理事	2010	2014
10.	高小山	中国密码学会密码数学专业委员会	副主任	2010	2013
11.	刘卓军	中国数学会计算机数学专业委员会	委员		
12.	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
13.	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
14.	李洪波	中国数学会	常务理事		
15.	李洪波	中国数学会计算机数学专业委员会	副主任		
16.	李子明	中国数学会	理事		

17.	李子明	中国数学会计算机数学专业委员会	委员		
18.	支丽红	国际符号与数值混合计算指导委员会	委员		
19.	支丽红	中国数学会计算机数学专业委员会	委员		
20.	王定康	中国数学会计算机数学专业委员会	秘书长	2010	2013
21.	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	任职开始时间	任职结束时间
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	**《自动化学报》**	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.	李洪波	**《Advances in Applied Clifford Algebras》**	编委		
29.	支丽红	**《Journal of Symbolic Computation》**	编委		
30.	支丽红	《Mathematics in Computer Science》	编委		
31.	支丽红	**《ACM Communications in Computer Algebra》**	编委		

3、人才培养

在读研究生及博士后一览表

序号	导师姓名	硕士生	博士生	博士后
1.	万哲先	孙志强		
2.	李洪波	李阁		
3.	王定康	王继斌		
4.	闫振亚	岳志强		
5.	高小山	郭建新		
6.	高小山	闵程		
7.	李子明	康劲		
8.	支丽红	郭庆东		
9.	刘卓军	张晓明		
10.	黄民强，邓映蒲	张凤		
11.	黄民强	胡耿然		
12.	胡磊	吕　昌		
13.	支丽红	刘　琦		
14.	高小山	李应弘		
15.	王定康	周　洁		
16.	闫振亚	王晓云		
17.	韩阳	秦永云		
18.	万哲先	王安宇		
19.	李洪波	刘　越		
20.	高小山	祝　炜		
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.	高小山			张智勇

毕业研究生一览表

序号	姓名	学位	导师姓名	毕业时间
1.	陈绍示	**博士**	李子明	
2.	曹源昊	**博士**	李洪波	
3.	孙瑶	**博士**	王定康	
4.	黄震宇	**博士**	高小山	
5.	李博	**博士**	李邦河	
6.	张艳娟	**博士**	万哲先	
7.	潘彦斌	**博士**	万哲先，邓映蒲	

研究生获奖一览表

序号	获奖名称	获奖人员	指导教师
1.	2010 年度中国科学院数学院院长奖学金优秀奖	赵尚威	高小山
2.	2010 年度中国科学院数学院院长奖学金优秀奖	郭峰	支丽红
3.	2010 年度中国科学院博时奖学金优秀奖	赵尚威	高小山
4.	2010 年度中科院系统所许国志博士后奖励基金	张志勇	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，

国家重大专项子课题 1 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 2 项，

国家基金重点项目 1 项，

国家科技支撑计划项目 1 项，

国家自然科学基金面上项目 5 项，

国家自然科学基金青年基金 3 项，

中国科学院重要方向性项目 3 项，

横向课题 1 项。

以上合计的当年到位经费总额：709.3 万元。

（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

- **微分差分方程的符号求解**
  - 给出了超指数-超几何函数的结构，并将其应用于判定超指数-超几何函数是否存在 Telescopers。证明了超指数-超几何函数的 Telescopers 的存在性。这一结果保证了对于超指数-超几何函数，Zeilberger 算法的终止性。
  - 将微分域中关于 Wronskian 行列式的结果以及差分域中关于 Carosatian 行列式的结果推广到微分差分混合域以及特征非零的域。
  - 对叶顶峰以及 Faugere 等人提出的基于微分以及齐次化的多变元多项式函数分解的算法，给出理论分析并证明对叶顶峰等人文章中的一个猜测给出严格证明。
- **微分代数**
  - 微分情形的相交定理并不成立：即 n 维空间中的 r 维微分代数簇与 s 维微分代数簇的交并不一定是 r+s-n 维；而维数问题，即 n 维空间中的 r 个多项式的维数是否是 n-r 维（非空）的还停留在猜想阶段。针对上述问题，我们研究了微分素理想的相交理论，给出了系数充分一般的情形下的微分相交理论与维数定理。
  - 鉴于代数情形的 Chow 形式理论在代数几何中的重要作用 ,我们给出了微分 Chow 形式的定义及其基本性质。同时，利用微分 Chow 形式的理论，给出了微分结式的定义。
  - 研究了微分的不变量理论，给出了微分素理想阶的几种等价定义，同时定义了线性变换下不变的微分次数。
- **三维高级射影不变量代数的建立**

  射影几何的高级不变量代数是 Cayley 括号代数，它是基于点的构造，但是几何体的代数乘法不满足结合律，使用起来颇受限制。今年我们从线几何的代数描述出发，证

明了线几何自然实现了 SO(3,3)和 SL(4)的同构 ,因而可以通过线来构造基于几何代数的三维高级射影不变量。这项工作在并联机构的奇异位型分析中有重要作用。

- **混合计算**
  - 设计了基于二元多项式近似最大公因子的快速图像盲复原算法，将过去已有同类算法的时间复杂度从 O(n^4)提高到 O（n^2*log(n)），并且能在几秒内将模糊的像素为 1024x1024 的图像清晰地恢复出来。
  - 结合广义临界值和多项式平方和理论，给出一种求解多项式全局最优值的方法，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。当多项式最优值是渐进临界值时，其半正定方法求解过程往往具有很大的数值问题，对于这一问题给出理论原因和初步的解决方法。
  - 研究了实多元多项式正定半径的计算和验证。新方法基于 Lagrange 乘子法，并结合半正定规划和有理系数平方和，给出了一类非负但不能写成多项式平方和的多项式的正定性的新的判定方法。
  - 研究了凸集中有理点的计算复杂度。并给出了单指数复杂度的新算法。
- **Groebner 基的计算**
  - Groebner 基的算法研究：研究了计算多项式理想 Groebner 基的 F5 算法，提出了和 F5 等价的 F5B 算法，并且给出了完整的 F5/F5B 算法的正确性证明。在此基础上，提出了一个对一般化的广义 F5 算法，并且证明了该算法的正确性。该广义 F5 算法包含了到目前的为止所有的 F5 类的算法，使这些算法都成为该算法的特定形式。
  - 微分算子系统的 Groebner 基的计算：给出了一个微分算子系统是否是 Groebner 基的充分必要条件。我们将微分算子系统的非交换性问题转换为了一个交换性的问题。从而，利用我们证明中给出了充分必要条件可以大大减少计算量，从而极大地提高了相关算法的效率。
  - 参数 Grobener 基和参数 Groebner 系统：提出了一个高效的同时计算参数多项式系统的 Groebner 基和参数 Groebner 系统的算法，从实际计算结果看，我们的算法是相关的算法中最高效的。

- 零维理想的多项式表示：通过研究零维 Groebner 基的性质，提出了一个计算零维理想的簇的多项式表示的算法。从而对任意的零维多项式系统，我们可以构造了该零维系统的一个同构。
- 软件方面：（1）实现了一个高效的同时计算参数 Groebner 基及 Groebner 系统的算法。（2）实现了一个零维系统的多项式表示的算法。

- **代数系统求解**
  - 基于多项式系统的三角分解一般都不保重数，而多项式系统分支的重数却是刻画其定义的代数簇的结构的一个重要信息。基于重数的重要性，我们研究了多项数系统的保重数的三角分解，给出了两个多项式构成的代数簇分支的保重数的无平方及相互不交（分支不同）三角分解。从而能够计算分支的重数。特别地，对二元二多项式构成的零维系统，可将其零点分解成三角形式并计算每个零点的重数。
  - 我们提出的零维系统局部一般位置方法可以将代数系统的零点表示为一些单变元多项式零点的线性组合。这个表示的优点是能够很好地控制近似零点的逼近精度。我们将零维的局部一般位置方法推广了高维，如维数 d，使得代数簇的零点可以表示为一些 d+1 维空间中超曲面的零点的线性组合。逼近代数族的零点问题可以转化了逼近 d+1 维空间中超曲面的问题，逼近精度可以很好地控制。

- **复杂非线性波、对称和符号分析**
  - 研究了源于非线性光学和 BEC 中重要的(3+1)-维变系数广义非线性 Schrodinger 方程的 rogue 波解，发表在国际权威数学物理期刊《Phys. Rev. E》上,并且该论文的解的图像入选被美国物理学会的 PRE kaleidoscope（http://pre.aps.org/kaleidoscope/pre/82/3/036610），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》(2010. Vol. 2, No.10)收录。
  - 首次提出畸形子(rogon)的概念，并且首次提出了变系数非线性 Schrodinger 方程的类 rogon 解，该论文发表于国际核心期刊《Phys. Lett. A》，关于光畸形波 (optical rogue waves)的研究成果，被国际著名的美国 Wolfram 研究公司(开发著名符号计算软件 Mathematica 等)邀请我们加入他们的 Wolfram Demonstrations Project。

- 首次研究了变系数一维非线性 Schrodinger 方程的半直线上解析解和它们的动力性质，发表在国际权威数学物理期刊《Phys. Rev. A》，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》(2010. Vol. 2, No.7)收录。
- 研究了金融非线性模型，提出金融 rogue waves，并且被 MIT《技术评论》和美国《大众科学》报道，发表在《Commun. Theor. Phys.》上。

- **《Java 几何专家》**

它是一个基于互联网的几何智能作图与定理自动证明软件，由两部分组成，一部分是几何作图器，另一部分是定理证明器。基于 Java 的软件平台与具体计算机型号与操作系统类型无关，可以在任意计算机上运行。这对数学机械化方法的应用与推广具有重要意义。关于《Java 几何专家》的两篇论文于 2010 年发表在国际自动推理主要杂志“Journal of Automated Reasoning”。《Java 几何专家》主要功能如下：

- 实现了动态几何的基本功能，包括自由拖动，几何变换，动态测量。
- 实现了几何定理机器证明的吴方法，面积法与推理数据库方法。我们还以此为基础发展了生成传统证明的方法与软件。
- 与《几何专家》相比，《Java 几何专家》实现了几何定理证明的动态图形显示。即对于几何定理证明中的每一步，可以给出动态显示效果，提高了定理证明的可读性。

2、信息安全

- **理性的密钥共享和安全多方计算**
  - 针对理性密钥共享的多轮交互的序贯性特点，以扩展博弈为基本模型严格讨论策略的合理性。指出前人广泛采用的惩罚策略由于危害到施行者的自身利益，从而降低了对被惩罚人的威慑。进而提出新的有限次惩罚策略，证明了在该策略下达到博弈的一个序贯均衡，因此既有效地惩罚了偏离行为，又很好地维护了施行者的利益。在同时广播信道的假设下，设计了达到序贯均衡的(2,2)-门限理性密钥共享体制，并且讨论了如何扩展到一般的(t,n)-门限，和实现分发人离线等问题。
  - 在标准通信模型下（即点对点的、非同时通信信道），设计了信息论意义下的理性密钥共享体制。其中，所设计的(2,2)-门限体制达到了 •-Nash 均衡，• 是关于密钥长度的一个可忽略函数。该体制较之前[KN-STOC08]的设计更加有效，即子密钥长度只是原来的一半，并且形式更加简单。所设计的(t,n)-门限体制达到了最优的(t-1)-弹性和 •-Nash 均衡，• 关于参与者人数是指数小的。

- **密码学**
  - Cai-Cusick 格公钥密码体制的彻底破解：该体制是 1998 年在加拿大的 SAC（Selected Areas in Cryptography）会议上提出的，作为实用的基于格的公钥密码体制 10 多年来一直未被成功分析。我们提出了一个唯密文攻击，时间是多项式时间的，从而一举攻破存在十年之久的 Cai-Cusick 基于格的公钥密码体制，发表在国际著名刊物 IEEE Transactions on Information Theory（2011 年 3 月）。
  - 具有多项最佳密码性质的布尔函数的构造：作为对称密码的核心，具有良好密码性质的布尔函数一直是国际上的研究热点，以往人们关注于某项或某两项最佳密码性质的布尔函数的构造，我们构造了两族具有最优密码性质的布尔函数，一是构造了最优代数免疫度的 Bent 函数，这是代数免疫度和非线性度第一次同时达

到最优；二是构造了具有平衡性、最优的代数次数、最优的代数免疫度、至今最好的非线性度的一族布尔函数。我们的论文获得国际同行的高度评价，将发表在 Designs, Codes and Cryptography(2011).所提出的一个关于模加法进位的猜想得到国际同行的高度关注。

- **格密码**
  - 提出了一种新的混合了背包结构的基于格公钥密码体制，密钥规模合理，加解密速度很快，可以作为一种实用的公钥密码体制。
  - 提出了一种用于构造格密码体制的框架，从而能轻易的构造一批格密码体制。
  - 提出了针对 NTRU 的有效的广播攻击，证明了 NTRU 在广播环境中不再安全，这也是密码学中第一个针对 NTRU 的广播攻击。

- **代数表示论**
  - Hochschild 同调、整体维数与箭图组合：提出 No loops conjecture 的高阶版本——No truncated cycles conjecture。证明了 Hochschild 同调维数有限，特别地整体维数有限，的代数无 2-truncated cycles。从而将 Solotar-Vigue-Poirrier 的结果推广到非分次非局部具有任意长度 2-truncated cycle 的代数上。证明了 monomial 代数的整体维数有限当且仅当其 Hochschild 同调维数有限，当且仅当其无 truncated cycles。
  - 导出范畴的 recollement 与代数的光滑性：证明了代数的导出范畴的 recollement 诱导张量积代数及反代数的导出范畴的 recollement ,从而给出 recollement 的张量积及反代数构造方法。将代数的导出范畴的 recollement 中的三角函子实现为导出函子，证明了代数的导出范畴的 recollement 中，中间的代数为光滑的当且仅当两边的代数为光滑的。从而说明“代数的光滑性为 smashing 局部性质”。

- **有限域**

- 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，这样做的好处是得到的逼近轮廓包含有所给定的多条序列的更多信息。我们也研究了这两种逼近的关系。这一结果已发表在杂志 IEEE Trans. Inform. Theory 上。
- 利用有限域上的酉群构造了迷向酉图。证明了当 n=2 或 3 时，U(2,q^2)和 U(3,q^2)分别是顶点个数为 q+1 和 q^3+1 的完全图。当 n>3 时，证明 U(n,q^2)是强正则的并计算了它的参数。当 n 不为 4 和 5 时确定了 U(n,q^2)的自同构群。

3、数控系统关键算法

- **G01 代码多周期最优拐角插补算法**

对于微小直线段(G01 代码)插补的难点在于怎样高速通过两条相邻直线段连接处(简称拐角)。过去在拐角过渡时，采用将速度降为零、等速过渡或圆弧过渡等方法。这些方法未能充分利用机床的加速度，插补速度尚有提高余地。为此，我们提出了微小直线段基于多周期最优拐角过渡的插补算法，这一算法在整体上保证各轴加速度不会超过机床各轴最大加速度，编程速度和允许最大加工误差，并且实现了拐角处的最优插补。经过加工实验表明，与传统方式相比，根据参数不同，整体加工速度可以提高 50%-180%。本成果已获得发明专利：

“基于二次 B 样条曲线对 G01 代码的拟合及插补方法”。授权公告日: 2010 年 8 月 25 日。

为了提高线段连接处的速度，采用了多插补周期过渡和充分利用机床各驱动轴加速度的方法，根据加工误差和速度优化函数确定拐角通过的速度上限，根据 bang-bang 控制和前瞻速度限制曲线来确定拐角通过的速度，在相当一般的意义下达到了全局速度最优，并给出了理论证明。

为了有效降低直线加减速方式加速度的突变引起机床振动，采用了基于多周期拐角插补方法的 S 曲线加减速控制方式，根据加工误差和速度优化函数确定拐角通过的速度

和加速度上限，根据 bang-bang 控制和前瞻技术来确定拐角通过的速度和加速度。算法满足实时加工的需求，并使得加工质量有了明显提高。

- **数控系统样条加工曲线的插补方法**

将样条曲线作为数控系统的直接输入是数控系统的新趋势与研究热点。我们从以下三个方面提出了新的方法，解决了若干基于样条曲线插补的关键难题。

(1)基于二次有理 B 样条的曲线拟合与曲线插补方法

在高速高精数控加工中，避免对微小线段加工产生震动的一种解决方案是将所需要加工的形状用样条曲线重新进行描述，通常采用的办法是样条插值。但是，如果插值曲线通过所有数据点，则不仅不能达到数据压缩的目的，而且精度也不能得到相应保证。另外，在数据点非常稠密的情况下，曲线可能频繁起伏，显得不光顺。此外，如果需要加工的样条曲线次数较高，在运动规划中所需计算量非常大，很难做到实时插补。因此，需要寻找次数低、压缩比较高且适合插补计算的样条曲线。在曲线插补控制方面，国内现有算法要么用匀速方式进行插补，没有速度规划；要么只是考虑了合成加速度的限制，而没有考虑到各个分轴的加速能力，未能充分利用各个分轴的最大加速度能力。Timar 等人提出了一种基于各轴最大加速能力的一般样条曲线的最优插补控制方法。这一方法对于高次(三次及三次以上)的样条曲线，要做相应的运动规划计算极为复杂，在现有的软件和硬件环境下无法做到实时计算。

针对上述现有技术中的困难和缺点，我们提出了一种 G01 代码的自适应二次 B 样条拟合及插补控制方法。该方法具有计算速度快，加工精度高，工作性能稳定且适用范围广泛的特定，可以满足高速高精数控加工的需要。与现有插补方法相比，我们所提出的基于二次 B 样条曲线的 G01 代码拟合及插补控制方法具有以下优点：通过自适应选择特征点插值，实现了用低次(二次)样条对加工路径具有的较高压缩比的拟合；根据二次 B 样条曲线的特点，极大地简化了 Timar 等人文章中的算法，得到了可以实时计算的插补方法，且充分利用了各轴的最大加速能力，在整体上达到了加工时间最优。实验结果显示，这一方法与多周期最优拐角过渡算法效果相当。本成果获得发明专利：

“基于二次 B 样条曲线对 G01 代码的拟合及插补方法”。授权公告日: 2010 年 8 月 25 日。

(2) 基于弓高误差与切向加速度限制的曲线最优插补

数控加工的核心内容是曲线的插补与速度规划。在高速高精数控加工中，加工时的误差控制是非常严格的，这就需要我们在规划每点处的速度时要考虑弓高误差的限制。

另外，由于机床能力的限制，需要考虑加速度的限制。通常情况下，速度规划的约束有两种：分轴加速度限制和切向加速度限制。我们考虑切向加速度限制的情况，对数控系统给出的参数曲线，我们给出了在弓高误差与切向加速度约束下时间最优的速度规划算法。

(3) 基于分轴加加速度有界的数控加工速度规划“贪心”算法

数控加工中沿着给定路径的速度规划是一类重要的问题，由于机床各轴驱动力是有限的，因此做速度规划时分轴加速度必须加以限制。Bobrow，Shiller，Timar 等人给出了沿着给定路径的分轴加速度有界条件下最优速度规划方法。但是由于并不能保证加速度的连续性，这会导致加工过程中驱动力的突然改变从而产生震颤，增加了轮廓误差。避免产生震颤的方法之一是要求加加速度有界，从而得到加速度连续的速度规划。但是没有人给出在分轴加加速度有界下的连续模型的速度规划算法。

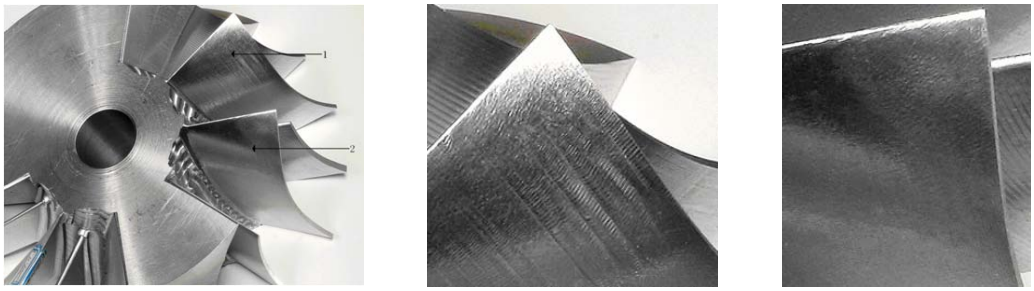
我们考虑了在分轴加加速度有界条件下沿给定路径（至少二阶可微曲线）的速度规划问题。我们首先证明了在此条件下最优速度规划一定满足 Bang-Bang 控制，即每个时刻至少一个轴的加加速度达到边界值。进一步地，我们提出如下的速度规划“贪心”准则：“尽可能使用最大的参数加加速度”，并设计出了在此准则下的最优速度规划算法。我们提出的加加速度有界的速度规划算法主要有两个关键部分：第一是确定控制轴，以及在控制轴确定后如何计算速度的积分曲线。为此，我们引入了换轴曲面，即积分曲线通过这种曲面时需要更换控制轴。积分曲线的计算则需要求解一类二阶微分方程，我们给出了这一问题的解析解。第二个关键部分是引入与使用 VLS（速度限制曲面）进行速度规划，以此来确保各轴加加速度不会超出约束。

（三）介绍本年度实验室重大成果及其水平和影响等。

1、**高档数控系统最优插补与空间刀补取得重要进展**

在高档数控系统的最优插补与空间刀补方面取得重要进展，提出了多周期过渡插补方法、基于二次样条函数的最优插补方法以及基于曲面重构的空间刀补方法，以上三项关键技术分别在 2010 年 8 月、12 月获得三项发明专利授权，并在沈阳计算所的蓝天数控系统上实现，使得数控加工的速度明显提高，加工质量得到显著改善。

为了实现复杂曲面高速高精加工，针对连续微小线段加工中速度方向频繁突变而制约整体加工速度的困难，课题组从数学建模与最优算法方面对这一问题进行了深入研究，提出了多周期过渡插补方法和快速前瞻算法，并证明了该方法在一定条件下达到了时间最优。该方法在蓝天数控系统上实现，实验结果表明，与已有算法相比，加工速度提高了 50%-180%，加工质量有显著提高，见图 1：



全局图　　局部（原来算法）　　（新算法）

图 1 加工的叶片图

样条曲线插补是数控加工的新趋势与研究热点. 我们提出的基于二次样条函数的拟合与最优插补方法与已有插补方法相比 ,实现了用低次样条对加工路径具有的较高压缩比的拟合，插补方法在整体上达到了加工时间最优，加工精度高，计算速度快，工作性能稳定且适用范围广泛。

针对数控加工因刀具磨损或换刀需重新生成加工程序而降低生产效率的问题 ,我们提出了基于曲面重构的空间刀补方法。这一方法首次实现了仅依赖加工程序进行在线刀补，使得加工干涉点显著降低（见图 2），提高了生产效率和加工质量。

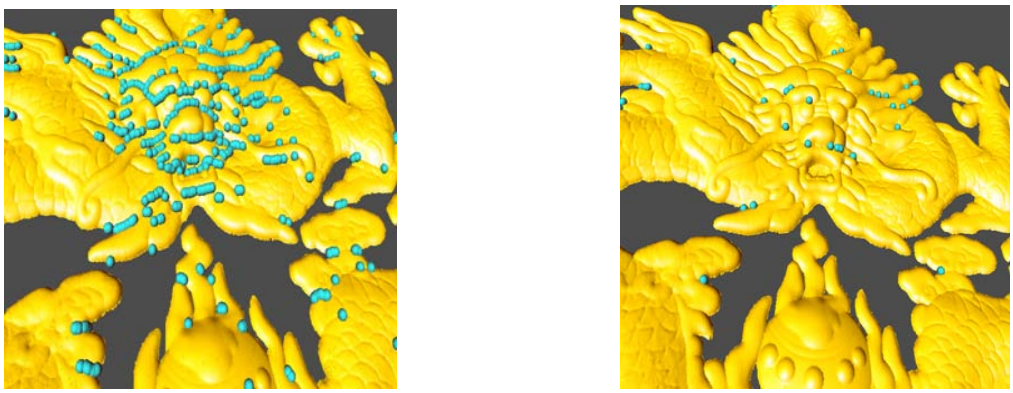


图 2 空间刀补前后干涉点对比

2、金融畸形波的研究 (Financial Rogue Waves)

美国 MIT 的学者 Black 和 Scholes 于 1973 年在《Journal of Political Economy》提出著名的 Black-Scholes 期权定价模型[1]

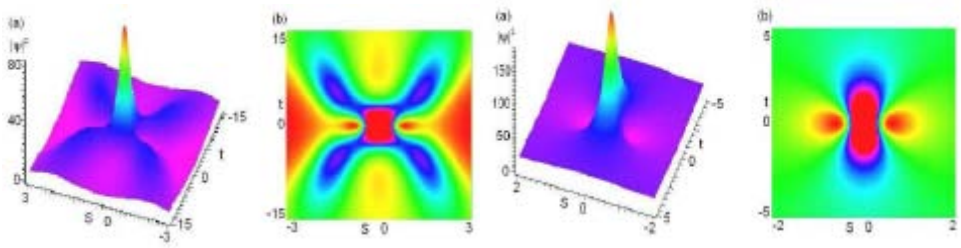
$$\partial_t u = -\frac{1}{2}(\sigma s)^2 \partial_{ss} u - rs\,\partial_s u + ru,$$

与此同时，MIT 的另一教授 Merton 也独立地提出了相同的模型[2]。之后，该模型受到了人们的普遍的关注与好评，1997 年第 29 届诺贝尔经济学奖授予哈佛商学院的 Merton 教授和斯坦福大学的 Scholes 教授。为了使得该模型更有效地适应于不同的金融市场，人们对它进行了很多方面的发展。基于 Lo 的现代适应性市场假设、Elliott 波市场理论和量子神经系统计算等理论，2010 年，澳大利亚学者 Ivancevic 提出用非线性的期权价格模型，即非线性 Schrodinger 方程：

$$\mathrm{i}\partial_t \psi = -\frac{1}{2}\sigma \partial_{ss}\psi - \beta|\psi|^2\psi, \qquad (\mathrm{i} = \sqrt{-1})$$

来描述金融市场波动性的变化规律。

最近，我们通过研究该非线性期权价格模型，在国际上首次显式地提出了它的两种类型的精确解，即金融畸形波解（或金融怪波解）(financial rogue waves)。



美国麻省理工学院百年期刊《技术评论》(Technology Review）以“Econophysicist Predicts Rogue Financial Waves （经济物理学家预言畸形金融波）”为题对我们的工作进行了报道，文中提到: “Today Zhenya Yan at the Institute of Systems Science in Beijing says that rogue waves can also occur in financial systems, and in particular in equity markets.”、“Yan, who points out today that one solution of a nonlinear wave system is a rogue wave, an event of far greater magnitude than would be expected by any standard method of analysis.”、“That's interesting. There's no shortage of anecdotal evidence for the existence of financial rogue waves. Look at the Asian financial crisis of 1997 or the current global financial crisis. But econophysicists will want more than that to confirm that financial rogue waves really exist.”。

另外，美国百年期刊《大众科学》(Popular Sciences）也对我们的工作以“Econophysicist Claims Rogue Waves Could Account for Volatility in Financial Markets （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， 文中指出“Now, Chinese researchers are positing that rogue waves can occur in financial systems, and could account for events like the 1997 Asia crisis or the current credit crisis sweeping the globe”、“Rogue waves, which we know to be real in other wave-like systems, could solve for the black swan events -- like the subprime mortgage debacle or savings and loan crisis -- that periodically appear as if from

nowhere and shake markets to their cores.”。

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.	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	200	高小山
2.	中科院重要方向性项目	基于数学机械化方法的高档数控系统研制	2008	2010	352	70	高小山
3.	国家重大专项“基础制造装备与数控机床”项目	基于龙芯的高档数控系统研制	2009	2010	88	88	李洪波
4.	国家杰出青年基金项目	高级几何不变量方法	2009	2012	140	84	李洪波
5.	国家基金重点项目	群与代数的表示论和代数组合论			140	56	万哲先
6.	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	22	王定康

7.	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	6	李洪波
8.	国家自然科学基金面上项目	符号和数值混合方法求解多项式方程组	2008	2010	21	8.4	支丽红
9.	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”	2010.1.1	2013.12.31	35	15.6	胡磊
10.	横向	密码学理论	2009	2011	10		高小山
11.	中国科学院方向性项目	复杂系统研究	2010	2012	200		高小山
12.	国家科技支撑计划项目	消费品质量安全影响因子原理与模型研究	2008	2010		40	刘卓军
13.	基金委青年基金	代数方程组求解与代数曲线曲面的可信计算	2011	2013			程进三
14.	中国科学院知识创新重要专项	数学理论研究	2010	2010	50	50	邓映蒲
15.	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	18	邓映蒲
16.	国家自然科学基金 青年基金	安全多方计算的模型和方法研究	2011	2013.	16	9.6	张志芳
17.	基金委青年基金	微分、差分方程的 Galois 理论及求 liouvillian 解的算法研究	2010	2012	16	9.6	冯如勇

18.	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	14	闫振亚
合计	---	---	---	---		691.2	---

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
	法国	NSFC/ANR	代数系统的准确、可信计算			（45万/30万欧元）	28	支丽红
	法国		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	10	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.	何梁何利基金科学与技术奖			李邦河
2.	第七届中国青年女科学家奖			支丽红

发表论文列表

序号	论文题目	刊物名称/卷期页码	作者	通讯作者	检索/影响因子
1	On the Topology of Real Algebraic Plane Curves	Mathematics in Computer Science, 4: 113–137, 2010.	Jinsan. Cheng, S. Lazard, L. Peñaranda, M. Pouget, F. Rouillier, and E. Tsigaridas	Marc Pouget	
2	Implicitization using univariate resultants	Journal of Systems Science and Complexity, 23(4), 804-814	L.Y. Shen, C.M. Yuan	L.Y. Shen	SCI/ 0.586
3	Visually Dynamic Presentation of Proofs in Plane Geometry, Part 1. Basic Features and the Manual Input Method	Journal of Automated Reasoning, 45, 213–241, 2010.	Z. Ye, S.C. Chou, X.S. Gao	Z. Ye	SCI
4	Visually Dynamic Presentation of Proofs in Plane Geometry, Part 2. Automated Generation of Visually Dynamic Presentations with the Full-Angle Method and the Deductive Database Method	Journal of Automated Reasoning, 45, 213–241, 2010.	Z. Ye, S.C. Chou, X.S. Gao	Z. Ye	SCI
5	Characteristic Set Algorithms for Equation Solving in Finite Fields	Accepted by Journal of Symbolic Computation, 2010.	X.S. Gao and Z. Huang	X.S. Gao	SCI
6	Curve fitting and time-optimal interpolation on CNC machines	Accepted by Science China, Series F	M. Zhang, W. Yan, C.M. Yuan, D. Wang, X.S. Gao	M. Zhang	SCI
7	High speed interpolation for micro-line trajectory and adaptive real-time lookahead in CNC machining	accepted by Science China, Series F	L.X. Zhang, R.Y . Sun, X.S. Gao, H. Li	L.X. Zhang	SCI
8	Articulation-Constrained Skeleton Extraction	Proc. IPCV2010, 441-446, CSREA Press, 2010	L. Han and X.S. Gao	L. Han	

9	Counting isomorphism classes of pointed hyperelliptic curves of genus 4 over finite fields with even characteristic	Acta Mathematica Sinica, English Series, Vol. 26, No. 6, pp. 1019-1054 (2010)	Huah Chu, Ying Pu Deng, Tse-Chung Yang	Yingpu Deng	SCI
10	A Ciphertext-Only Attack Against the Cai-Cusick Lattice-Based Public-Key Cryptosystem	IEEE Transactions on Information Theory, Vol.57, No.3, March 2011, pp. 1780-1785	Yanbin Pan, Yingpu Deng	Yingpu Deng	SCI
11	Computing rational points in convex semi-algebraic sets and SOS decompositions	SIAM Journal on Optimization	Mohab Safey El Din and Lihong Zhi	Mohab Safey El Din	SCI/1.202
12	Transforming linear functional systems into a fully integrable systems. Accepted by Journal of Symbolic Computation.	Accepted by Journal of Symbolic Computation	Z. Li M. Wu	M. Wu	SCI
13	Complexity of creative telescoping for bivariate rational functions	Proc of ISSAC 2010	A. Bostan, S, Chen F. Chyzak Z. Li	S. Chen	EI
14	Liouvillian solutions of difference- differential equations	*Journal of Symbolic Computation* /45(3), 287–305	Ruyong Feng, Michael Singer and Min Wu	Ruyong Feng	SCI
15	An algorithm to compute Liouvillian solutions of prime order linear difference-differential equations	Journal of Symbolic Computation /45(3), 306–323	Ruyong Feng, Michael Singer and Min Wu	Ruyong Feng	SCI
16	Nonautonomous “rogons” in the inhomogeneous nonlinear Schrödinger equation with variable coefficients	*Phys. Lett. A*, 374 (2010) 672	Zhenya Yan	ZhenyaYan	SCI
17	Dynamics of inhomogeneous condensates in contact with a surface,	*Phys. Rev. A*, 81 (2010) 063610.	Yu. V. Bludov, Z. Y. Yan, and V. V. Konotop,	Yu. V. Bludov	SCI

18	Exact analytical solutions for the generalized non-integrable nonlinear Schrödinger equation with varying coefficients	*Phys. Lett. A*, 374 (2010) 4838	Zhenya Yan	ZhenyaYan	SCI
19	Three-dimensional rogue waves in nonstationary parabolic potentials	Phys. Rev. E, 82 (2010) 036610.	ZhenyaYan，V. V. Konotop, and N. Akhmediev,	ZhenyaYan	SCI
20	Financial rogue waves	*Commun. Theor. Phys*., 54 (2010) 947	Zhenya Yan	ZhenyaYan	SCI
21	A New Algorithm for Computing Comprehensive Groebner Systems.	Proc of ISSAC 2010	Deepak Kapur, Yao Sun and Dingkang Wang.	Dingkang Wang	EI
22	图表追踪的一种机器实现方法	中国科学，40（7）：661-672，2010	谢正，叶征，李洪波，黄雷	谢正	SCI
23	数控插补中基于运动曲线的局部优化和基于前瞻控制的整体优化	系统科学与数学，2010 30 (11): 1548-1561	张立先，孙瑞勇，李洪波，高小山	张立先	
24	一类单圈 T 函数的判定	系统科学与数学 2010 30 (11): 1540-1547	刘卓军，戴照鹏，吴保峰	刘卓军	
25	SDPTools:基于 Maple 的高精度求解 SDP 软件包	系统科学与数学 2010 30 (11): 1512-1521	郭峰	郭峰	
26	基于改进的不动点迭代算法的低秩 Gram 矩阵的恢复	系统科学与数学 2010 30 (11): 1501-1511	马玥	马玥	
27	Line Geometry in Terms of the Null Geometric Algebra over R(3,3), and Application to the Inverse Singularity Analysis of Generalized Stewart Platforms	Geometric Algebra in Practice, Springer, 2010	Hongbo Li, Lixian Zhang	Hongbo Li	EI
28	On Geometric Theorem Proving with Null Geometric Algebra	Geometric Algebra in Practice, Springer, 2010	Hongbo Li, Yuanhao Cao	Hongbo Li	EI

29	Parametrization of 3D conformal transformations in conformal geometric algebra	Applications of Geometric Algebra in Computer Science and Engineering, Birkhauser, 2010	Hongbo Li	Hongbo Li	EI
30	Collision and intersection detection of two ruled surfaces using bracket method	Computer Aided Geometric Design, doi:10.1016/j.cagd.2010.11.002	Y. Chen, L.Y. Shen, C.M. Yuan	Y. Chen	SCI
31	安全事故现状与趋势分析方法研究	中国管理科学，2010，18（4）：pp.183－192	刘卓军，柳刚	刘卓军	
32	国内安全生产事故的时间特征分析	数学的实践与认识，2010 年 11 月，40（22），pp. 147－155	刘卓军，柳刚	刘卓军	
33	消费品宏观质量评价模型与应用	数学的实践与认识，2010 年 12 月，40（24），pp. 68－76	于彭，黄冲，刘卓军	于彭	
34	基于逐步回归分析的消费品伤害类型研究	中国管理科学，2010，18(专辑)，pp. 706－711	刘卓军，柳刚	刘卓军	
35	消费品伤害形成机理的多层网络模型	中国管理科学，2010，18(专辑)，pp. 165－170	刘卓军，于彭	刘卓军	
36	Complexity of creative telescoping for bivariate rational functions	Proc. ISSAC 2010	Alin Bostan, Shaoshi Chen, Frédéric Chyzak and Ziming Li	Ziming Li	EI
37	Global Optimization of Polynomials Using Generalized Critical Values and Sums of Squares	Proc. ISSAC 2010	Feng Guo, Mohab Safey El Din and Lihong Zhi	Feng Guo	EI
38	Blind Image Deconvolution via Fast Approximate GCD	Proc. ISSAC 2010	Zijia Li, Zhengfeng Yang and Lihong Zhi	Zijia Li	EI

39	Computing the Radius of Positive Semidefiniteness of a Multivariate Real Polynomial Via a Dual of Seidenberg's Method	Proc. ISSAC 2010	Sharon Hutton, Erich Kaltofen and Lihong Zhi	Sharon Hutton	EI
40	Unitary Graphs and Their Automorphisms	Annals of Combinatorics, Volume 14, Issue 3 (2010), Page 367-395	Zhe-xian Wan, Kai Zhou	Kai Zhou	SCI
41	Strict Optimal Rational Approximants of Multisequences	IEEE Trans. Inf. Theory, vol.56, no.4, pp. 1719-1728, April 2010	Zhe-xian Wan, Kai Zhou	Kai Zhou	SCI EI
42	The Reason of Hopf's and Oleinik's Proofs for Countability of Shocks Being Wrong	中国科学（接收）	李邦河	李邦河	SCI
43	Unconditionally secure rational secret sharing in standard communication networks	**13th International Conference on Information Security and Cryptology, Korea, 2010. (LNCS, Springer)**	Zhifang Zhang, Mulan Liu	Zhifang Zhang	

出版专著

序号	著作名称	作者	出版单位	出版日期

授权发明专利

序号	专利名称	专利号	授权日期	发明人
1.	数控系统基于多周期最优拐角的小直线段插补方法	ZL 2009 1 0083950.4	2010.8.25	李洪波；张立先，孙瑞勇，高小山

2.	基于二次 B 样条曲线对 G01 代码的拟合及插补方法	ZL 2009 1 0082732.9	2010.8.25	张梅；袁春明，闫伟，王定康，李洪波，高小山
3.	基于曲面重构的三轴数控机床刀具的半径补偿方法	ZL 2009 1 0089707.3	2010.12.8	高小山，李洪波，张立先

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

国际合作方面取得的突出成绩。

1、第四届微分代数以及相关领域国际研讨会于 2010 年 10 月 27 日至 10 月 30 日在中科院数学与系统科学研究院举行。会议主题包括微分差分方程、微分代数群、微分代数以及模式理论、微分差分维数理论、微分差分Galois理论、微分不变量、D模以及Riemann-Hilbert对应、积分-微分算子以及微分Rota-Baxter算子、计算以及应用微分差分代数等。本次会议与会人员约 70 人，其中有来自美国、英国、德国、奥地利、西班牙、俄罗斯、阿根廷等国外与会人员约 30 人；研究生约 20 人。会议共计 10 个 50 分钟报告、16 个 25 分钟报告以及 12 个Poster。本次会议的目的是促进国内外微分代数领域研究人员的交流与合作并扩大青年科研人员的视野。

2、第四届有限域及其应用国际研讨会于 2010 年 5 月 28 日-30 日在北京大学举行。会议主题是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。研讨会的目的是使有限域方面的学者交流他们的最新研究成果。本次研讨会的参与者为 70 人左右。一些著名的学者与会，其中包括丁存生（香港科技大学），周文贤（台湾中央研究院数学所），王强（加拿大 Carleton University），候向东（美国 University of South Florida)，黄铭德（美国 University of South California），向青（美国 University of Delaware）,邢朝平（新加坡南洋理工大学），张耀祖（台湾义守大学），Shuhong Gao（美国 Clemson University），颜松远（英国 University of Bedfordshire）以及国内学者万哲先，冯克勤，冯荣权，韩文报，戚文峰，洪绍方，曹永林，麻常利，符方伟等。有限域及其应用会议由万哲先院士发起，每两年举办一次，已经成为有限域方面有影响的系列学术会议。

国内合作取得的突出成绩。

2010 年 10 月 19 日至 22 日 ,第三届全国计算机数学学术会议在上海华东师范大学举行。来自中国科学院和全国各地高等院校共 41 个单位的 150 多名教师、研究生参加了本次学术会议。本次会议的主题包括数学机械化理论、算法和软件实现，符号与数值混合计算、可信计算等计算机数学的新方法，计算机数学在信息安全、程序验证、机器人和数控系统的应用，计算机图形学、模式识别、计算生物学等领域中的数学方法，其他计算机应用领域和软件设计领域的数学方法。

华东师大软件学院何积丰院士参加了开幕式。南开大学陈永川、清华大学 Jean-Pierre Jouannaud 和贾仲孝、中国科学技术大学陈发来等四名学者在会议上做了邀请报告， 58 名研究人员在本次会议的分组会议上做了学术报告。这些报告介绍了各自工作中的最新结果和工作领域的前沿方法，学术报告的工作领域包括特征列方法和 Groebner 基等数学机械化理论、算法与软件设计问题，微分方程自动求解，微分代数，实代数算法及其应用，图像处理、模式识别，计算机辅助设计、机器人控制、数控机床系统控制，优化

算法，混合计算方法、程序验证和可信计算，信息安全、计算生物学问题等。会议中讨论热烈，会议之间来自不同单位的研究人员还进行了各种其它形式的深入交流，讨论了将来拟开展的合作。部分优秀学术报告论文将在《系统科学与数学》专辑上发表。

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，华东师范大学高可信计算上海市重点实验室和中国科学院数学机械化重点实验室承办。会议期间，计算机数学专业委员会举行了 2010 年专业委员会会议，会议讨论了专业委员会今后的工作。

4、2010 年 11 月 30 日，数学与先进制造交叉应用研究部召开的为期三天的计算机辅助制造(CAM)与数控加工专题研讨会在北京闭幕。我部科研人员及其他研究所和高校等近 20 位多名专家、教授参加了研讨会。研讨会主要就“复杂曲面数控加工 CAM 系统及其应用”，“基于 TGA 理论的薄壁件侧锐加工变形预测”，“复杂曲面的刀路规划算法”等关键问题研究等相关技术问题做了专题报告。中科院数学院科研人员就国际多轴数控加工中的刀轨规划等问题的最新进展做了专题介绍。本研讨会围绕以上相关问题展开了热烈讨论和交流。沈阳自动化所的刘伟军、卞宏友、赵吉宾等专家和大连理工大学的孙玉文教授分别作了会议发言。中国科技大学的邓建松教授对计算机辅助制造与数控加工相关

方面的工作提供了一些重要建议和材料。本次会议对于数学与先进制造部与国内相关单位进一步合作开展数控加工与 CAM 中关键算法问题的研究有重要促进作用。

5、根据中国科学院数学与系统科学研究院的部署，“数学与先进制造交叉应用研究研讨会”暨国家数学科学交叉应用中心制造材料部咨询会于2010年5月21日召开。参加本次会议的有来自清华大学、华中科技大学、浙江大学、中科院沈阳计算所、中科院沈阳计算所等我国先进制造领域优势单位以及相关数学领域的专家学者50余人，包括我国制造领域著名学者孙家广、熊有伦、谭建荣院士以及吴文俊、崔俊芝、张景中院士。中国科学院基础局数理处王永祥处长、数学院与系统科学研究院洪佳林副院长、潘建中院长助理也应邀出席。

王永祥处长首先介绍了中国科学院“创新2020”科技创新跨越方案的目标、任务和主要举措，并充分肯定了本次会议的重要意义，指出交叉研究可以打破原先各自为政的院系壁垒，以项目平台的形式加强合作，取得更大成就。洪佳林副院长宣读了郭雷院长为本次会议召开的来信，指出：数学科学交叉应用研究中心的筹备经过了长期的酝酿，得到中科院各级领导及相关业务局的大力支持，凝聚了多方智慧和努力。中心的建立对数学院乃至数学科学及应用的发展具有重要意义。数学院院将在充分听取和吸收大家意见及建议的基础上，依托我院在人才与学科等方面的现有基础和综合优势，与相关人员和部门通力合作，大力推动各项研究工作的顺利实施和开展。

会议分为两个阶段。上午由制造科学领域专家做邀请报告，提出先进制造领域对数学的需求；下午，国家数学科学交叉应用中心数学与制造材料交叉研究部科研人员报告了取得的成果与工作计划并与会专家进行了讨论。

计算机辅助设计著名专家孙家广院士提出了信息科学与数学交叉研究的七个重要问题。先进制造技术、机器人学著名专家熊有伦院士介绍了几何推理及其在制造领域中的应用。机械设计与数字化制造著名专家谭建荣院士提出了制造信息化中存在的关键数学问题。此外，王立，于东，刘伟军，陈立平分别提出了航天技术、数控技术、数字化制造技术与数字化设计技术中的若干关键数学问题。

高小山代表数学院介绍了数学与先进制造交叉应用研究部的工作设想，提出将整合科学院从事数学与制造研究的相关队伍，通过与其他相关单位开展实质性合作，形成制造材料数学方法研究的基地；并通过承担国家重大任务，为国家战略需求服务。陈发来、李洪波、于丹分别作了题为《复杂曲面建模与等几何分析》、《高档数控系统中的插补与刀补》、《航天航空纳米材料加工技术中的统计学问题》的报告。

与会专家针对数学与先进制造交叉进行了深入讨论，一致肯定了数学与先进制造交叉应用的重要性和必要性，表示迫切需要数学专家介入这些领域提供数学方面的支持。崔俊芝院士指出在高新科技领域，关键技术的基础研究应该作为一项长期性的事业型工作来做，现在却经常作为短平快的项目来看待，重视短期收益，忽视长远效益，而

中科院数学科学交叉应用研究中心的成立正是对这一空白的补充，具有科学性、前瞻性与战略性。中科院软件所戴国忠研究员认为，先进制造这一领域的范围很广，数学的学科也很多，如何有效地将两者结合起来，从中选取几个点做精，是值得大家思考的问题。我国对一些制造信息领域投入资金较高，但是现在核心软件还是要依靠国外，原因何在值得深思？与会专家还为数学与制造研究部提出了建设性意见。

研讨会在热烈的讨论中落下帷幕，与会专家全面分析了目前面临的形势，积极建言献策，拓宽了思路，深化了认识，明确了努力的方向，增强了发展的责任感、使命感和紧迫感。同时，本次会议也增进了数学院与我国制造科学优势单位的进一步沟通与了解。高小山表示，我们将吸收专家们的建设性意见，进一步汇总融入到数学科学交叉应用研究中心的建设、实施方案中。这次会议对研究中心各项工作起到积极的指导和重要推动作用，对研究中心未来的发展具有重要意义。

实验室作为本领域公共研究平台的作用。

举办的国际国内学术会议一览表

序号	会议名称	会议类别	主办单位	会议主席	会议日期	参加人数
1.	第三届全国计算机数学学术会议	全国	计算机数学专业委员会	杨路，支丽红		150
2.	第四届微分代数及相关领域国际研讨会	国际	数学机械化重点实验室	高小山	2010 年 10 月 27--30 日	70
3.	有限域及其应用	国际		万哲先		
4.	计算机辅助制造(CAM)与数控加工专题研讨会		数学机械化重点实验室	李洪波		
5.	中国科学院数学机械化重点实验室战略研讨会		数学机械化重点实验室		2010 年 11 月 10--12 日	30

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.	Articulation-Constrained Skeleton Extraction	高小山	IPCV2010	美国	
2.	有限域上方程求解的特征列方法	高小山	中法联合项目会议	Paris	
3.		高小山	ISSAC2010	Munich	
4.	有限域上方程求解的特征列方法	高小山	密码数学研讨会	北京	
5.	Root Isolation of Zero-dimensional Polynomial Systems with Linear Univariate Representation	程进三	中法合作报告会	法国巴黎六大	2010 年 6 月
6.	Differential Chow Form	袁春明	第四届微分代数国际研讨会	北京	2010.10.27
7.	Geometric Theorem Proving with Null Geometric Algebra	李洪波	AGACSE	荷兰	2010 年 5 月
8.	R(3,3) Model of Line Geometry and Application to Inverse Singularity Analysis of GSPs	李洪波	GraVisMa	捷克	2010 年 9 月
9.	Functional Decomposition of Multivariate Polynomial	李子明	中法联系项目会议	法国巴黎六大	
10.	有限域上小亏格超椭圆曲线的计数	**邓映蒲**	第二届全国编码与密码数学理论研讨会	福建省福州市	2010 年 7 月 19 日－ 7 月 23 日
11.	A New Lattice-Based Cryptosystem Mixed with a Knapsack	**潘彦斌**	第四届有限域及其应用国际研讨	**北京**	2010 **年** 5 **月** 28 **日** -30 **日**
12.	Factoring RSA Module with q^–1 mod p Revisited	**潘彦斌**	**第十二届全国代数学术会议**	**兰州**	2010.6.20-2010.6.26
13.	线性密钥共享和安全多方计算（邀请报告）	张志芳	第二届全国编码密码数学理论研讨会	福州	2010.8
14.	Unconditionally Secure Rational Secret Sharing Schemes in Standard Communication Networks	张志芳	The 13th International Conference on Information Security and Cryptology (ICISC 2010)	韩国首尔	2010.12

15.	Hochschild homology and truncated cycles （邀请报告）	韩阳	Hochschild cohomology: Structures and Applications	法国马赛	2010 年 6 月 7-11 日
16.	代数的表示型：昨天、今天和明天 （特邀报告）	韩阳	第十二届全国代数会议	兰州	2010 年 6 月 21-25 日
17.	Global Optimization of Polynomials Using Generalized Critical Values and Sums of Squares.	支丽红	The International Symposium on Symbolic and Algebraic Computation (ISSAC 2010)	德国慕尼黑	2010 年 7 月 25-28
18.	Blind Image Deconvolution via Fast Algorithm for Computing Approximate Greatest Common Divisor of Polynomials.	支丽红	The International Symposium on Symbolic and Algebraic Computation (ISSAC 2010)	德国慕尼黑	2010 年 7 月 25-28
19.	Computing the radius of positive semidefiniteness of a multivariate real polynomial via a dual of Seidenberg’s method.	支丽红	The International Symposium on Symbolic and Algebraic Computation (ISSAC 2010)	德国慕尼黑	2010 年 7 月 25-28
20.	A New Algorithm for Computing Comprehensive Groebner Systems.	王定康	The International Symposium on Symbolic and Algebraic Computation (ISSAC 2010)	德国慕尼黑	2010 年 7 月 25-28
21.	Complexity of the Creative Telescoping for Bivariate Rational Functions.	李子明	The International Symposium on Symbolic and Algebraic Computation (ISSAC 2010)	德国慕尼黑	2010 年 7 月 25-28
22.	Exact solutions of three-dimmensional GP equation with variable coefficients	闫振亚	第三届非线性数学物理国际会议暨全国第十届孤立子与可积系统学术研讨会 会议	厦门,	2010. 8. 20-24
23.	Rogue waves of the higher-dimensional generalized GP equation with variable coefficients	闫振亚	首届全国近可积系统的数学方法及其在物理学中的应用研讨会	北京	2010. 10. 9-10
24.	Rogue wave solutions of nonlinear Schrodinger equation with variable coefficients	闫振亚	第三届计算机数学学术研讨会	上海	2010.10. 19-22

25.	Exact Solutions to Three-Dimensional Generalized Nonlinear Schrödinger Equations with Varying Potential and Nonlinearities	闫 振亚	第四届微分代数及相关主题国际研讨会	北京,	2010.10.27-30

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.	构造具有高代数免疫性的布尔函数	2010.5	2011.4	1	1	涂自然	邓映蒲
2.	流形上的偏微分方程的误差可控的数值算法研究	2010.5	2011.4	1	1	谢正	李洪波
3.	Java 版几何专家的开发与推广	2010.5	2011.4	1	1	叶征	高小山
合计	---	---	---			---	---

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

国家、省部领导人视察实验室的图片及说明。

1、2010 年 12 月 2 日，国务院国务委员刘延东、中国科学院院长路甬祥等领导参加中国科学院国家数学与交叉研究中心成立仪式。期间到数学机械化重点实验室考察工作，听取了数学机械化研究的最新进展，特别是近期在数控系统方面的工作。

2、2010 年 5 月 4 日下午，中国科学技术部在北京举行小行星命名仪式。中国科学院国家天文台施密特 CCD 小行星项目组发现并获得国际永久编号的 4 颗小行星，经国际天文学联合会小天体命名委员会批准，以中国的 4 位科学家命名，以表彰他们做出的突出贡献。其中国际永久编号第 7683 号小行星永久命名为“吴文俊星”， 同时获此殊荣还有高性能计算机专家金怡濂院士、航天专家王永志院士和气象学家叶笃正院士。下图为科技部万钢部长为吴文俊院士颁发证书。

3、李邦河院士荣获 2010 年度“何梁何利基金科学与技术奖”。10 月 20 日下午，何梁何利基金 2010 年度颁奖大会在北京钓鱼台国宾馆隆重举行。中共中央政治局委员、国务委员刘延东，全国人大常委会副委员长、中科院院长路甬祥，全国政协副主席、科技部部长万钢，全国政协副主席何厚铧等出席颁奖大会。

4、8 月 7 日上午，中共中央政治局常委、国务院总理温家宝登门看望了吴文俊先生，向他献上寓意吉祥和祝福的鲜花，致以深情的问候和良好的祝愿。 温家宝总理多次强调，要尊重知识，尊重人才，要和科学家交朋友。每年登门看望德高望重、贡献卓越的老一

代科学家，已经成为他就任总理以来的惯例。温总理还看望了何泽慧、朱光亚、王大珩先生等。