目 录

组织结构

实验室成员

名誉主任：　吴文俊

主任：　高小山

副主任：　李洪波，李子明

成员：　吴文俊，万哲先，李邦河，石　赫，刘木兰，王世坤，高小山，段海豹，孙笑涛，李洪波，刘卓军，李子明，王定康，支丽红，马玉杰，闫振亚，韩　阳，邓映蒲，吴天骄，冯如勇，袁春明，张志芳，冷福生，周　凯

秘书：　周代珍

实验室网站：　http://www.mmrc.iss.ac.cn

电话：　010－62541834

传真：　010－62630706

实验室学术委员会

主任：　万哲先

副主任：　石　赫

委员：　吴文俊，张景中，李邦河，陆汝钤，林惠民，黄民强，杨　路，刘木兰，吴　可，冯克勤，张继平，陈永川，李克正，高小山，李洪波

实验室相关机构

数学机械化研究中心

主任：　李洪波

副主任：　李子明，支丽红

信息安全研究中心

主任：　刘木兰

副主任：　邓映蒲

实验室成员简表

序号	姓　名	专　　业	研　究　方　向	职　　称
1.	吴文俊	数学	数学机械化	院士
2.	万哲先	数学	代数、编码、有限几何	院士
3.	李邦河	数学	拓扑、代数几何	院士
4.	高小山	数学	自动推理、符号计算	研究员
5.	李洪波	数学	自动推理、几何代数	研究员
6.	石　赫	数学	数学机械化	研究员
7.	刘木兰	数学	信息安全	研究员
8.	刘卓军	数学	计算代数、信息安全	研究员
9.	王世坤	数学	应用数学、微分方程	研究员
10.	段海豹	数学	计算拓扑、代数几何	研究员
11.	孙笑涛	数学	代数几何	研究员
12.	李子明	数学	符号计算、微分方程	研究员
13.	王定康	数学	数学机械化、软件开发	副研究员
14.	支丽红	数学	符号计算、混合计算	副研究员
15.	韩　阳	数学	代数表示	副研究员
16.	邓映蒲	数学	信息安全	副研究员
17.	闫振亚	数学	微分方程	副研究员
18.	马玉杰	数学	代数几何	助理研究员
19.	冯如勇	数学	符号计算	助理研究员
20.	袁春明	数学	符号计算	助理研究员
21.	张志芳	数学	信息安全	助理研究员
22.	冷福生	数学	代数数论	助理研究员
23.	周　凯	数学	代数、编码	助理研究员
24.	吴天骄	数学	数学机械化	工程师

实验室博士后与研究生

博士生：王培宏、张艳硕、刘姜、吴晓丽、王怀富、李家、顾振华、沈跃峰、涂自然、陈绍示、于彭、孙瑶、黄震宇、李博、张艳娟、潘彦斌、曹源昊、张立先 、李晓明、李灵光、林贤祖

硕士生：周升田、李斌、张梅、赵尚威、孙瑞勇、羊正正、吴小胜、李伟、郭峰、刘元杰、付国峰、樊伟、郭磊磊、刘莎丽、陈慧、姜宇鹏、吴保峰、马晓栋、姚守彬、李楠、张可、李子佳、辛赫、张淑英、敖仑昊

博士后：许宁、闫伟、韩丽

毕业及授予学位情况

毕业博士： 柴凤娟、王灯山、谢正、王培宏、张贵林、黄雷

一、实验室学术委员会年会

中国科学院数学机械化重点实验室学术委员会会议于 2008 年 4 月 16 日在中科院数学与系统科学研究院召开。莅临会议的专家有万哲先院士、陆汝钤院士、李邦河院士、林惠民院士、黄民强院士等 12 位实验室学术委员会成员。中国自然科学基金委信息科学学部秦玉文主任、数理天文处张文岭处长、中科院基础局数学物理处王永祥处长以及中科院综合计划局科研基地处周鼐博士应邀参加了会议。

此次会议由学术委员会主任万哲先院士主持，实验室常务副主任李洪波研究员汇报了实验室 2007 年的研究进展以及在学术交流、开放课题和实验室建设等方面取得的成绩。实验室主任高小山研究员作了 “数学机械化方法在信息技术中的应用”的学术报告。

在听取了工作汇报的基础上，专家们对实验室工作进行了认真的审议和讨论，充分肯定了这一年来试验室在中科院的关心和支持下所取得的巨大进展。专家特别列举出实验室李洪波研究员因关于高级不变量代数理论的工作获得国际计算机协会 (ACM) SIGSAM 所颁发的“ISSAC 杰出论文奖”。该项工作被国际同行认为是符号机器证明领域的一个突破，其意义超出该领域本身。并且肯定了实验室与中科院沈阳计算所联合承担的科学院重要方向性项目“基于数学机械化方法的高档数控系统研制”，认为该项目将数学机械化研究的理论成果与数控技术相融合，转化为具体的应用技术，为我国装备制造业的发展做出了贡献，为申请国家重大专项奠定了基础。

与会专家在对实验室一年工作进行回顾的同时，也对实验室的工作提出了具体的建设性意见。专家们指出实验室应该以数学机械化为核心研究内容，加强基于混合计算的高可信算法、数学机械化方法在数控技术中的应用、密码理论等新兴学科方面的部署，响应科技面向国家战略需求的号召，为解决关系国计民生和国家安全的重大问题做出更大贡献。

二、实验室开放课题

实验室 2008 年度共批准 12 项开放课题，其中以来访项目为主。实验室通过开放课题，加强了与国内重要相关单位的合作，加强了对国内相关领域青年人才的引导与扶植。

2008 年开放课题支持项目

序号	课题名称	承担单位	承担人	课题编号 合作老师
1	几何推理与 JAVA 几何专家软件研制	浙江大学/Wichita State University	周咸青	KLMM08012 高小山
2	方程的智能算法求解与粒子群优化	北京邮电大学	赵新超	KLMM0801 高小山
3	基于有理 SOS 的可信计算研究	华东师范大学可信计算重点实验室	杨争峰	KLMM0809 支丽红
4	线性微分-差分系统的维数判定算法		吴　敏	KLMM0810 李子明
5	数控系统中的数学方法		申立勇	KLMM0702 袁春明
6	统一零知识理论及其在混淆中的应用	清华大学	袁征	KLMM0808 刘卓军
7	符号计算在 Darboux 变换构造中的应用	清华大学	林润亮	KLMM0803 闫振亚
8	自动证明的仿射括号代数应用深入研究	中央财经大学	张　宁	KLMM0804 李洪波
9	几何不变量分析及其应用	中国石油大学	李宗民	KLMM0805 李洪波
10	微分-差分方程（离散方程）可积系统生成的理论、方法及应用	上海大学	夏铁成	KLMM0806 李子明
11	若干重要非线性方程的对称性约化与精确解	宁波大学	李　彪	KLMM0807 王世坤
12	线性偏微分-差分方程的 Galois 理论及应用	湖北大学	郑大彬	KLMM0811 李子明

三、实验室客座人员与来访学者

姓　名	工 作 单 位	访 问 时 间
杨争锋	华东师大软件学院	2008. 11
Stephen Watt	University of Western Ontario, Canada	2008.4
Hoon Hong	North Carolina State University, USA	2008.4
Frabrice Rouillier	INRIA, France	2008.4
Moulay Barkatou	University of limoges, France	2008.6
Shuhong Gao	Clemson University, USA	2008.6
Dingzhu Du	University of Texas at Dallas, USA	2008.6
Songyuan Yan	Bedford University, UK	2008.6
Jintai Ding	University of Cincinnati, USA	2008.6
Haohao Wang	Southeast Missouri State University, USA	2008.6
Ling San	Nanyang Technological University, Singapore	2008.6
Huaxiong Wang	Nanyang Technological University, Singapore	2008.6
Y. Kodama	Ohio State University, USA	2008.6.
J. William Hoffman	Louisiana State University, USA	2008.7
Deepak Kapur	University of New Mexico, USA	2008.7
J. C．Leon	INP Grenoble, France	2008.10
D. Mecheluchi	University Dijon, France	2008.10
Chaoping Xing	Nanyang Technological University, Singapore	2008.10
Jiwu Wang	Oita University, Japan	2008.11
Erich Kaltofen	North Carolina State University, USA	2008.11
Mohab Safey El Din	Pierre et Marie Curie University, France	2008.11
Manuel Mantildeas	Departamento de Física Terica II, Universidad Complutense de Madrid	2008.11

四、实验室开放日

5 月 20 日是中国科学院北京公众科学日，来自北京航空航天大学等高校的大学生和一些中小学师生参加了此次“实验室开放日”活动。本次活动得到了系统所领导和职工的大力支持。实验室研究生向同学们介绍数学机械化重点实验室的历史沿革、发展情况，并以通俗易懂的方式向同学们讲解实验室的研究方向、课题内容和研究手段等。实验室研究生还为师生们演示了数学机械化平台软件（MMP）。

此次活动受到了参观同学的热烈欢迎，激发了参观者的浓厚兴趣。通过与科研人员的进一步接触，使参观者对科研工作有了更深层次的了解，感受到了科研人员的敬业精神。活动结束后，大家纷纷表示，要努力学习，夯实基础，为祖国的经济社会建设做出贡献。部分高校学生更是表示了希望将来有机会能到实验室来深造的愿望。

一、研究工作情况

本年度数学机械化重点实验室在科研进展、人才培养、国内外合作交流等方面持续发展，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，论文 51 篇，其中 SCI 论文 37 篇，EI 论文 5 篇；实验室组织召开了第二届中法系统求解及应用研讨会和第二届全国计算机数学学术会议(CM 2008)，为数学机械化领域的国际国内交流合作提供了重要平台。数学机械化重点实验室作为主要发起单位还参加了中国科学院数控技术创新联盟，在高精、高速数控系统的研制方面取得重要进展。

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“数学机械化与自动推理平台”在 10 月 7 日举行的“973”计划 10 周年纪念大会上，被科技部授予“973 计划优秀团队”称号。本项目在数学机械化理论与算法、图像压缩、并联机构与数控机床、自动推理平台开发、曲面造型等多个方向取得突破性进展。

实验室高小山研究员经投票当选为“符号和代数计算国际会议"(ISSAC)指导委员会主席，任期一年。ISSAC 是符号和代数领域最具权威的国际会议，已经有 33 年历史。ISSAC 指导委员会由六名委员组成，其职责是负责 ISSAC 的学术与组织管理。

实验室闫振亚副研究员由于在微分方程机械化算法与可积系统等方面的研究工作获得 2008 年度中国科学院卢嘉锡青年人才奖。袁春明老师入选数学与系统科学院首届“陈景润未来之星”计划。他的主要研究方向是微分-差分混合系统的特征列方法。他与合作者发展了微分-差分混合系统的特征列算法与预解式方法，扩展了数学机械化方法的适用范围。

主要科研成果:

- **布尔多项式的特征列方法**

特征列方法是数学机械化的核心内容。这一工作针对一类新的方程类型，布尔多项式，发展了相应的特征列方法与算法。给出了布尔多项式的吴特征列方法，包括整序原理与零点分解定理。由于布尔多项式的特殊性，所给出的特征列方法与一般的特征列方法相比，具有以下优点：(1)给出了分离首一零点分解定理, 并得到方程组解的个数的明确的表示公式。(2) 证明了改进的整序原理可以在 n 步数内终止，其中 n 是变量个数。(3) 给出了只需要多项式加法的零点分解算法，有效地控制了算法对于空间的需求。在 C 语言中实现了所提的特征列方法。引进了求解方程组的分支-空间平衡原则，以此为基础给出了特征列算法的多种形式。给出了特征列方法的并行实现与基于 SZDD 的实现，大大提高了程序的效率、压缩了需要占用的内存空间，得到求解布尔多项式组的高效软件。应用特征列方法分析了一类基于非线性寄存器的流密码。通过对变量个数从 40 到 128 的问题进行的大量实验，证实了我们的方法是有效的。 （高小山，袁春明）

- **代数曲线与曲面拓扑的确定与可信逼近**

代数曲线与曲面的拓扑确定与可信逼近是几何造型中的重要问题。我们得到以下结果。(1) 对于代数曲线与曲面给出了确定拓扑的符号-数值混合算法，这一算法在关键点的确定与分支个数的计算方面引入了基于区间计算的数值算法，显著提高了计算效率。(2) 对于代数曲线与曲面给出了计算其可信逼近的算法。所谓可信逼近是指拓扑正确且可以任意逼近曲线曲面的线性逼近。这一算法首先利用符号-数值混合算法逼近曲线与曲面的奇异部分，然后用一种新的 Marching Cube 算法逼近曲面的光滑部分。这样得到了计算速度快的可信逼近算法。（高小山，程进三）

- **Clifford 差分环**

欧氏几何与正交几何的主要区别在于前者具有平移变换与正交变换的复合。一个位移可以用两个位置向量的差表示，因而展开 n 个位移的乘积就是表达式指数膨胀的过程。为避免这种膨胀，考虑不展开一阶差分的乘积下的化简和标准型，就是 Clifford 差分环的主要研究内容。 本项工作在 2 维情形有突出进展，得到 ISSAC 2008 审稿意见的好评。（李洪波）

- **指标微分多项式的化简和标准型**

爱因斯坦求和约定是符号 n 维几何计算的一个重要工具，是张量计算的基础。在流形上的可微坐标变换下的微分多项式的化简和标准型，是张量判定和几何不变量计算的一项核心内容，但是迄今没有完全的算法。本项工作提供了第一个完全的算法，尽管局限在微分的阶数小于等于 2 的情形。（李洪波）

- **二元域上多项式方程求解与布尔环上的多项式方程组求解的软件**

对二元域或布尔环上多项式系统进行研究，利用布尔环的性质提出了新的计算准则，从而减少了 Groebner 基的计算，提高了算法效率。参与组织“多变元密码学”讨论班，对多变元密码学的相关问题进行了研究。开发的布尔环上的多项式方程组求解的软件虽然只是一个初步的版本，但从计算结果看，实现效果还是相当令人满意的。在以后的工作中将进一步完善该软件。（王定康）

- **Ore 多项式**

研究利用 Ore 多项式计算非线性控制论中的转移函数。在国际计算数学基础大会，符号分析研讨会上作 45 分钟邀请报告。研究利用 Ore 多项式的分解形式决定两个微分或差分算子是否相似，相关文章已投稿。利用局部化模计算完全可积系统，给出决定多元超指数函数是否代数相关的算法, 相关结果在计算机数学年会上作报告

给出非交换主理想长度为 2 的元素的相似判定法则，并应用于判定二阶线性微分和差分算子的相似性。（李子明）

- **半正定规划在多项式符号和数值混合计算中出现的多项式全局最优问题的应用**

将数值计算中的半正定规划与实代数理论和有理数矩阵计算等相结合，计算多项式全局

最优问题的可信最优解。通过分析多项式因式分解和最大公因子计算中的半正定规划问题的特殊稀疏结构，成功地运用半正定规划和多项式平方和得到了这些问题的全局最优解。更为重要是将半正定规划算法的有数值误差的输出，通过牛顿迭代、有理数向量重构和有理投影等运算，给出基于有理多项式平方和的准确的无数值误差的全局最优的可信验证。将德国汉堡大学著名区间计算专家 Siegfried Rump 的有关因子系数界的计算从 7 提升到 14。（支丽红）

- **基于对合系统的近似多项式重根的局部结构分析和高精确计算**

研究了基于对合系统的近似多项式重根的局部结构分析和高精确计算。对于近似重根，我们计算近似根所满足的微分条件的个数和阶数，然后将牛顿迭代推广到相应的局部商环上来提高重根的精度。我们不仅在理论上首次证明了广义牛顿算法的二次收敛性，而且试验结果也显示算法有非常好的二次收敛性。一般问题只需一次和两次迭代就收敛。另外，我们还给出了算法的多项式计算复杂度分析。符号延拓和数值消元方法还可以与矩量方法相结合，计算实多项式方程组的全部实根。对解决实际应用问题提供了非常可靠和有效的方法。（支丽红）

- **PT-对称拓展原理和新的复 PT-对称系统的构造**

基于两种不同的 PT-对称拓展原理，基于著名的非 PT-对称 Burgers 方程，国际上首次构造出了两簇新的复 PT-对称系统。并且给出了一些代表性的非线性波方程的解析解(如 compacton 解和 peakon 解等)和守恒律。另外，利用这两种原理，还提出了很多高维复非线性 PT-对称波方程。这一成果完善了非 PT-对称和 PT-对称波方程到复非 PT-对称波方程的转换。审稿专家认为，研究成果非常有意义，不仅仅对于量子力学或量子场论中的研究课题具有很好的价值，而且将为物理、工程和数学研究者对非线性系统的研究打开新的局面（open new door）。（闫振亚）

- **非线性波方程解析解的构造**

提出新的具有非线性色散项的高维 KP 方程，并且给出了它们的高维 compacton 解。另外，基于两种不同的变换，提出了变系数 mKdV 方程的单变量和双变量解析解。基于简化的 Rikitake 系统，提出了新的三函数构造性求解算法，可用于获得大批非线性波方程的椭圆函数解，周期解和有理解。（闫振亚）

- **新的超混沌系统的构造和同步与控制研究**

基于已知的混沌系统，通过引入一个新的状态，提出了一个新的超混沌系统，并且研究了它的全局指数同步与控制问题。提出了新的具有非线性色散项的(2+1)-维 KP 方程，并且给出了它们的 compacton 解；提出了变系数 mKdV 方程的单变量和双变量解析解。基于已知的混沌系统，通过引入一个新的状态，提出了一个新的超混沌系统，并且研究了它的全局指数同步与控制问题。（闫振亚）

- **线性差分微分混合方程的 liouvillian 函数解**

基于线性差分微分混合方程的 Galois 理论，给出了一个线性差分微分混合方程存在在 Liouvillian 函数解的判定条件并给出了该混合方程是不可约的并且存在 Liouvillian 函数解时的标准形式。当线性差分微分方程的阶数是素数时，我们给出了一个求它的所有 Liouvillian 函数解的算法。（冯如勇）

- **差分代数的素理想判定与有理曲线**

运用特征列方法给出了判定一个差分特征列表示的理想为素的简单的判别准则。有理曲线的近似恰当化问题和一类空间参数曲线的隐式化问题。我们给出了近似恰当指数的定义，并根据这一指数计算出曲线的恰当的近似有理参数表示形式。另一方面，我们用单变元结式方法来隐式化一类空间参数曲线，算法的效率比现有的方法更高。（袁春明）

- **微分代数情形的 effective Mordell 猜测**

研究微分代数情形的 effective Mordell 猜测，得到了有理解个数的有效上界，并将有理解的个数与拓扑性质结合起来。相关结果得到了审稿人的好评。（马玉杰）

- **安全多方计算与超椭圆曲线分类**

提出具有 3-乘性的线性密钥共享体制概念，给出了一般性构造，并揭示了它与具有强乘性的线性密钥共享体制之间的联系。该概念的提出为解决公开问题“具有强乘性的线性密钥共享体制的一般性有效构造”开辟了一条新的思路。同时，将具有 3-乘性的线性密钥共享体制用于安全多方计算协议的构造中，可以显著地减少信息交互的轮数复杂度。文章被 2008 年的亚密会录取，审稿人评价该文"technically solid","nice handle","interesting observation"等。精确计算了奇特征有限域上亏格 4 超椭圆曲线同构类的数目。（张志芳，邓映蒲，刘木兰）

- **基于数学机械化方法的高档数控系统研制**（高小山，李洪波，王定康，袁春明）

(1) 多周期最大加速拐角过渡插补算法

提出了短直线插补的多周期最大加速拐角过渡算法，充分利用了机床的加速度，实现了加速有界(或加加速有界)条件下的最优拐角过渡。以此为基础给出了 G01 代码的整体插补算法，并在蓝天数控系统中实现了这算法。实验显示新算法显著提高了加工速度与质量，在同等条件下，拐角多周期过渡算法比传统小线段过渡算法的加工速度提高了一倍，比传统拐角匀速过渡算法提高了 50%。在相同加工条件下，拐角多周期算法的加工表面更清晰。这一方法将申请发明专利。

(2) 自适应数据压缩方法

对于给定的 G01 代码，首先根据曲率、挠率对 G 代码进行分段，然后对每段进行数据逼近，再根据误差情况自动调整分段与逼近情况。对 CAM 系统生成的微小直线段进行曲线拟合。在利用微小直线段的几何进行分段的基础上，提出了利用最小二乘方法，A 样条方法，对分段的微小直线段进行拟合，并且在分段处进行光滑连接。模拟结果显示该方法有很好的拟合效果，满足实际零件加工的需求，具有精度高、计算速度快的特点。

(3) 样条曲线的最优插补算法

对由样条描述的加工路径，实现了分轴控制的插补算法，在整体上达到了最优。

(4) 5 轴机床的空间刀补

提出了通过刀位点与切触点的轨迹对应，得到曲面的法向信息的公式，实现 5 轴联动的空间刀补。

(5) 基于曲面重构的干涉检验与空间刀补

通过刀心轨迹的曲面重构，提出了由刀心轨迹恢复加工路径与加工方向的算法，以此为基础，为刀具的局部干涉检验与 3 轴机床的空间刀补提供了有效算法。

二、奖励与荣誉

1. 实验室高小山研究员经投票当选为“符号和代数计算国际会议"(ISSAC)指导委员会主席，任期一年。ISSAC 是符号和代数领域最具权威的国际会议，已经有 33 年历史。ISSAC 指导委员会由六名委员组成，其职责是负责 ISSAC 的学术与组织管理。

2. 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“数学机械化与自动推理平台”在 10 月 7 日举行的“973”计划 10 周年纪念大会上，被科技部授予“973 计划优秀团队”称号。本项目在数学机械化理论与算法、图像压缩、并联机构与数控机床、自动推理平台开发、曲面造型等多个方向取得突破性进展。

3. 实验室闫振亚副研究员由于在微分方程机械化算法与可积系统等方面的研究工作获得 2008 年度中国科学院卢嘉锡青年人才奖。论文获得 2008 年辽宁省自然科学优秀论文二等奖。

4. 实验室袁春明老师入选数学与系统科学院首届“陈景润未来之星”计划。袁春明主要研究微分-差分混合系统的特征列方法。他与合作者发展了微分-差分混合系统的特征列算法与预解式方法，扩展了数学机械化方法的适用范围。

5. 实验室李邦河院士、李子明研究员获得研究院第二届优秀教师奖。

6. 博士后韩丽荣获 2008 年度许国志博士后工作奖励基金。

研究生获奖

1. 李家获得中国科学院研究生院 2007-2008 学年三好学生标兵称号。吴晓莉、李斌、张艳硕、付国锋、 郭峰、沈跃峰被评为中科院三好学生。
2. 沈跃峰获得研究院第六届院长奖学金特等奖。
3. 李家获得第六届院长奖学金优秀奖。
4. 顾振华获首届博时奖学金（优秀奖）。

一、专著与专利

专著 2 本：

1. H. Li. *Invariant Algebras and Geometric Reasoning*. World Scientific, 2008 ,Singapore.
2. 刘木兰、张志芳.密钥共享体制和安全多方计算. 北京:电子工业出版社,2008.2，ISBN 978-7-121-05792-2 .

发明专利 1 项：

一种由圆柱副、圆柱副和球面副构成的并联机构

专利号：ZL 2006 1 0109345.6

授权公告日：2008 年 7 月 30 日

完成人：高小山、廖启征

二、期刊论文

1. F. Chai, X.S. Gao and C.M .Yuan. A Characteristic Set Method for Solving Boolean Equations and Applications in Cryptanalysis of Stream Ciphers. *Journal of Systems Science and Complexity*, 2008,21(2)：191-208. (SCI)
2. R. Feng, X.S. Gao, and Z. Huang. Rational Solutions of Ordinary Difference Equations. *Journal of Symbolic Computation*, 2008, 43:746-763. (SCI)
3. X.S. Gao and M. Zhang. Decomposition of Differential Polynomials. *Applicable Algebra in Engineering, Communication and Computing*, 2008,19(1):1-25. (SCI)
4. J. Li, L. Shen and X.S. Gao. Proper Reparametrization of Rational Ruled Surface. *Journal of Computer Science and Technology*, 2008, 23(2):290-297.
5. X.S. Gao, J. van der Hoeven, C.M. Yuan, and G. Zhang. Characteristic Set Method for Differential-Difference Polynomial Systems, *Le Matematiche*,2008 , Vol 63:19-21.
6. X.S. Gao, Y. Luo and C.M. Yuan. A Characteristic Set Method for Difference Polynomial Systems, accepted by *Journal of Symbolic Computation*. (SCI)
7. J.S. Cheng, X.S. Gao and C.K. Yap. Complete Numerical Isolation of Real Roots in Zero-dimensional Triangular Systems, accepted by *Journal of Symbolic Computation*. (SCI)
8. H. Li, L. Zhao and Y. Chen. A Symbolic Approach to Polyhedral Scene Analysis by Parametric Calotte Propagation. *Robotica*, 2008,26: 483-501.(SCI)
9. D. Wang, Z. Yan and H. Li. Some special types of solutions of a class of the (N+1)-dimensional nonlinear wave equations. *Computers and Mathematics with Applications*, 2008, 56: 1569-1579. (SCI)
10. D. Wang, H. Li. Symbolic computation and non-travelling wave solutions of (2+1)-dimensional nonlinear evolution equations. *Chaos, Solitons and Fractals*,2008, 38: 383-390. (SCI)
11. D. Wang, H. Li, J. Wang. The novel solutions of auxiliary equation and their application to the (2+1)-dimensional Burgers equations. *Chaos, Solitons, and Fractals* ,2008,38: 374-382. (SCI)
12. D. Wang, H. Li. Single and multi-solitary wave solutions to a class of nonlinear evolution

equations. *Math. Anal. Appl*, 2008, *343*: 273-298. (SCI)

13. L. Huang, H. Li. Complex brackets and balanced complex first-order difference polynomials in 4-dimensional Minkowski space. *Science in China Series A*,2008 ,38(7): 750-760.(SCI)
14. Z. Xie, H. Li. A note on discrete connections on regular lattice. *Commun. Theor. Phys*. 2008 (accepted). (SCI)
15. Z. Xie, H. Li. Applications of exterior difference systems to variations in discrete mechanics. *J. Phys. A: Math. Theor*. 2008, 41: 085208. (SCI)
16. Z. Xie, H. Li. Exterior difference systems and invariance properties of discrete mechanics. *J. Phys. A: Math. Theor*. (accepted), 2008. (SCI)
17. Z. Xie, H. Li. Formal integrability criteria for nonlinear partial difference equations, *Acta Appl. Math*, 2008, doi: 10.1007/s10440-008-9312-5. (SCI)
18. J. Liu, H. Li and Y. Cao. Simplification and normalization of indexed differentials involving coordinate transformation. *Science in China Series A* (accepted), 2008. (SCI)
19. H. Li. From geometric algebras to advanced invariant computing, *J. Sys. Sci. Math.* 2008, 28(8): 915-929.
20. Z. Li and H. Wang. A criterion for the similarity of length-two elements in a noncommutative PID. Accepted by *J. Sys. Sci. and Compl.* (SCI)
21. B. Li, J.W. Nie and L.H. Zhi . Approximate GCDs of polynomials and sparse SOS relaxations. *Theoretical Computer Science*, 2008,409(2)：200-210.（SCI）
22. G. Reid and L.H. Zhi. Solving polynomials systems via symbolic-numeric eliminational method .*Journal of Symbolic Computation*, to appear 2008. （SCI）
23. E. Kaltofen, J.P. May, Z.F. Yang and L.H. Zhi. Approximate factorization of multivariate polynomials using singular value decomposition. *Journal of Symbolic Computation*, 2008,43(5):359-376.（SCI）
24. B.Y. Li, Z.J. Liu and L.H. Zhi .A Structured Rank-revealing Method for Sylvester Matrix. *Journal of Computational and Applied Mathematics*, 2008,213 pp.212-223.（SCI）
25. Y.S. Zhang, Z.J. Liu. Efficient threshold multi-secret sharing scheme among weighted participants. *Computer Engineering and Design*, 2008,29(4):814.
26. Y.S. Zhang, Z.J. Liu. Dynamic Generalized Threshold Multi-Secret Sharing Scheme among Weighted Participants. *Journal of Beijing University of Posts and Telecommunications*, 2008,31(1).
27. Y. Deng and M. Liu. Counting isomorphism classes of pointed hyperelliptic curves of genus 4 over finite fields with odd characteristic. European Journal of Combinatorics, 2008, 29 (6): 1436--1448. (SCI)
28. Z.Y. Yan. New binary travelling-wave periodic solutions for the modified KdV equation. *Phys. Lett. A*, 372 (2008) 969. (SCI)
29. Z.Y. Yan. Complex PT-symmetric extensions of the non PT-symmetric Burgers equation. *Phys. Scr*. 77(2008) 025006. (SCI)
30. Z.Y. Yan**.** The modified KdV equation with variable coefficients: Exact uni/bi-variable travelling wave-like solutions. *Appl. Math. Comput*, 203 (2008) 106. (SCI)
31. Z.Y. Yan, P. Yu. Hyperchaos synchronization and control on a new hyperchaotic attractor. *Chaos, Solitons and Fractals*, 35 (2008) 333. (SCI)
32. F. Xie, Z.Y. Yan**.** Compactons and noncompactons to three-dimensional Kadomtsev

–Petviashvili equation with nonlinear dispersion. *Chaos, Solitons and Fractals*, 36 (2008) 278 . (SCI)

33. F. Xie, Z.Y. Yan, Exactly fractional solutions of the (2+1)-dimensional modified KP equation via some fractional transformations. *Chaos, Solitons and Fractals*, 36 (2008) 1108. (SCI)
34. Y. Chen and Z.Y. Yan. Chaos control in a new three-dimensional chaotic T system, *Commun. Theor. Phys*. 45(2008)941. (SCI)
35. R.Y. Feng and J.P .Yu. Mechanical theorem proving in the surfaces using the characteristic set method and Wronskian determinant. *Science in China Series A: Mathematics*, 2008,51(10):1763-1774.(SCI)
36. Z. Zhang, M. Liu and L. Xiao. Rearrangements of Access Structures and Their Realizations in Secret Sharing Schemes. *Discrete Mathematics*,308 (2008), pp. 4882-4891.（SCI）
37. Z. Wan, Z. Gu. Orthogonal graphs of odd characteristic and their automorphisms. *Finite Fields and Their Applications*,2008, 14:291-313.(SCI)
38. Z. Wan. A Generalization of Witt's Theorem and Sylvester's Law of Nullity. *Algebra Colloquium* 2008, 15:181-184. (SCI)
39. B.H .Li, Y.F. Shen and B. Li, Quasi-Steady State Laws in Enzymy Kinetics, J. Phys. Chem. A .2008, 112(11):2311-2321. (SCI)
40. B.H .Li, Y.F. Shen and B. Li, New algorithm for computing the minimum Hausdoff distance between two point sets on a line under translation, Information Processing Letters, 2008,106: 52-58. (SCI)
41. B.H. Li, B. Li and Y.F. Shen, A Novel Approach to Measure All Rate Constants in the Simplest Enzyme Kinetics Model, Journal of Mathematical Chemistry, 2008. (SCI)
42. 石赫. SU(2)规范场得恰当形式（欧空间）. *系统科学与数学*，2008，28（7）:859-866.
43. 石赫. SU(3)规范场得恰当形式（欧空间）. *数学学报*，2008，51（5）:833-840.
44. Z. Yuan. Provable secure digital watermarking scheme. *Journal on Communications*, 2008, 29(9).

三、会议文集论文

1. H.B. Li and L. Huang. Complex Brackets, Balanced Complex Differences, and Applications in Symbolic Geometric Computing. *In Proceedings of the 2008 International Workshop on Symbolic-Numeric Computation*, Austria , 2008,ACM Press. (EI)
2. E. Kaltofen, B. Li, Z.F. Yang and L.H. Zhi. Exact Certification of Global Optimality of Approximate Factorizations via Rationalizing Sums-of-Squares with Floating Point Scalars. *In Proceedings of the 2008 International Workshop on Symbolic-Numeric Computation.* Austria , 2008,ACM Press. pp. 155-163. （EI）
3. J. Li and Z.X. Gao. A Modified van der Waerden Algorithm to Decompose Algebraic Varieties and Zero-Dimensional Radical Ideals. Springer-Verlag, Berlin Heidelberg, 2008, *ASCM 2007*, LNAI 5081, 246-262. (EI)
4. Z. Zhang, M. Liu, Y. M. Chee, S. Ling, and H. Wang, Strongly multiplicative and 3-multiplicativelinear secret sharing schemes, Advances in Cryptology, *ASIACRYPT 2008*, LNCS 5350, 19-36, Springer. （SCI）
5. X.L. Wu and L.H. Zhi. Computing the multiplicity structure from geometric involutive form.

In Proceedings of the 2008 Internat. Symp. Symbolic Algebraic Comput, 2008, ACM Press, pp. 325-332. （EI）

6. Y. Chen, H. Li. Symbolic Approach to Reconstruct Polyhedral Scene from Single 2D Line Drawing. *In Proceedings of the 2008 IEEE International Conferences on Cybernetics & Intelligent Systems and Robotics, Automation & Mechatronics*, Chengdu, September 22-24, 2008 (EI)
7. B.H. Li, D.K. Wang. An Algorithm for Transforming Regular Chair into Normal Chain, D. Kapur (ed.): *ASCM 2007*, LNAI 5081, pp. 236-245, 2008.

四、 数学机械化研究报告

“数学机械化研究报告”(MM-Preprints)由数学机械化重点实验室编辑，始于1987年，主要收录实验室成员当年完成的论文，以便于与国内外同行交流。现已全部上网。

第27期“数学机械化研究报告”收录以下论文 (http://www.mmrc.iss.ac.cn/mmpreprints)：

1. Jin-San Cheng, Xiao-Shan Gao, and Jia Li ,Root Isolation for Bivariate Polynomial Systems with Local Generic Position Method ,Vol. 27, 122-136, December, 2008.
2. Jin-San Cheng, Xiao-Shan Gao, and Jia Li, Topology Determination and Isolation for Implicit Plane Curves, Vol. 27, 137-149, December, 2008.
3. Jin-San Cheng, Xiao-Shan Gao, and Jia Li, Ambient Isotopic Meshing of Implicit Algebraic Surface with Singularities, Vol. 27, 150-183, December, 2008.
4. Shangwei Zhao, PCP Theorem And Hardness Of Approximation For MAX-SATISFY Over Finite Fields, Vol. 27, 1-15, August, 2008.
5. Shangwei Zhao and Xiao-Shan Gao , Minimal Achievable Approximation Ratio for MAX-MQ over Finite Fields, Vol. 27, 16-24, December, 2008.
6. Kai Zhou, A Remark on Linearized Permutation Polynomials, Vol. 27, 25-28, December, 2008.
7. Ruyong Feng, Michael F. Singer and Min Wu, Liouvillian Solutions of Linear Difference-Differential Equations, Vol. 27, 29-70, December, 2008.
8. Wu Wen-Tsun and Wu Tianjiao, On a Method of Integer-Factorization Based on Chinese Remainder Theorem, Vol. 27, 71-79, December, 2008.
9. Chunming Yuan and Xiao-Shan Gao, A Criterion for Testing Whether the Saturated Difference Ideal Is Prime, Vol. 27, 80-88, December, 2008.
10. Ziming Li and Huaifu Wang,,A Criterion for the Similarity of Length-Two Elements in a Noncommutative PID, Vol. 27, 89-103, December, 2008.
11. Xiaoli Wu and Lihong Zhi, Determining Singular Solutions of Polynomial Systems via Symbolic-numeric Reduction to Geometric Involutive Form, Vol. 27, 104-121, December, 2008.

科研项目

一、在研项目

项 目 名 称	类 别	负责人
数学机械化及其在信息领域的应用	973 项目 2004－2009	高小山
差分与微分方程的数学机械化方法	973 项目子课题 2004－2009	李子明
数学机械化理论与核心算法	973 项目子课题 2004－2009	李洪波
信息安全的基础理论与数学机械化方法	973 项目子课题 2004－2009	刘木兰
数学机械化及其在信息领域的应用	国家基金委优秀群体项目 2008－2011	高小山
基于数学机械化方法的高档数控系统研制	中科院重要方向性项目 2008－2010	高小山 李洪波 王定康 袁春明
有限维线性微分差分方程组的 Galois 理论和算法	基金面上项目 2007-2009	李子明
非线性波与符号分析	中科院优秀博士论文科研基金 2006-2008	闫振亚
非线性光学中模型构造性研究	中科院知识创新工程青年人才领域前沿项目 2007-2008	闫振亚
数学机械化	国家最高奖奖励基金	吴文俊
群与代数的表示论和代数组合论	国家基金重点项目	万哲先
中法联合培养博士	中法联合培养博士项目 2007-2011	李子明

二、“973”项目:数学机械化方法及其在信息技术中的应用

1．项目年度学术交流与汇报会

2008 年 10 月 24 日，国家重点基础研究发展计划（973）项目"数学机械化及其在信息技术中的应用"学术交流与汇报会同时在中国石油大学举行。项目首席专家介绍了项目的总体情况，课题组长介绍了各课题组情况。2008 年度，本项目在面向学科前沿和重大应用背景的研究、人才培养、学术合作与交流等方面全面完成了年度计划，在几何堆积与覆问题、Clifford 差分环、组合恒等式机器证明、微分方程 PT-对称研究、符号实代数理论与应用研究、程序验证、代数免疫度、分组密码体制、三维空间曲线旋转最小框架、T 网格上的样条函数、成分数据的特征提取等方面取得突出成果。项目承担人共发表论文 350 余篇；获得奖励 8 项，包括一项国家科技进步二等奖与维也纳科学技术大学颁发的 von Prechtl 奖章；在国际会议上做邀请报告 18 项，申请/授权专利 14 项，培养研究生 120 余名。

2．项目取得的主要成果

2008 年度，本项目在面向学科前沿和重大应用背景的研究、人才培养、学术合作与交流等方面全面完成了年度计划，在几何堆积与覆盖问题、Clifford 差分环、组合恒等式机器证明、微分方程 PT-对称研究、符号实代数理论与应用研究、程序验证、代数免疫度、分组密码体制、三维空间曲线旋转最小框架、T 网格上的样条函数、成分数据的特征提取等方面取得突出成果。

本项目分为 7 个课题组，共有项目成员 86 人、研究生 310 人，2008 年主要成果统计如下。

论文			获奖		学术报告			专利	人才培养		
总数	SCI	EI	国际	国内	特邀	国际	组织		博士后	博士	硕士
350	165	142	2	6	18	80	18	14	5	40	80

本项目成员获得国际奖励 2 项，获得维也纳科学技术大学颁发的 von Prechtl 奖章，在由新加坡 Fusionopolis 主办的 Star Challenge 2008 语音视频检索国际竞赛初赛中斩获第一名。

本项目成员获得国内奖励 7 项，包括：国家科技进步二等奖、教育部科技进步一等奖、陈省身数学奖、科学前沿中国卓越研究奖等。参与项目的研究生获得国际会议 Best Student Award、International Timetabling Competition 第二名、博时奖学金特等奖、数学院特等奖、中科院院长特别奖和全国优秀博士论文提名奖等。

课题成员发表了一批高水平论文。发表的杂志包括：ACM Transactions on Graphics, IEEE Transactions on Signal Processing, IEEE Trans. Information Theory, IEEE Trans. Visualization and Computer Graphics, IEEE Trans. System, Man and Cybernetics, IEEE Trans. Circuits and Systems, Theoretical Computer Science, Journal of Symbolic Computation, Computer Aided Geometric Design, Advances in Math., Trans. of the AMS, J. Combin. Theory Ser. A.。课题成员还参加了一批高水平的国际会议，包括 ACM SIGGRAPH、ACM ISSAC 和 ASIACRYPTO 等等。

三、中科院项目《基于数学机械化方法的高档数控系统研制》

2008 年 1 月 26 日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》启动，由数学机械化实验室与中科院沈阳计算所联合承担。本项目的目标是针对高档数控系统高速、高精、高效的发展趋势，基于科学院的综合技术优势，实现学科交叉与融合，开发出新型的基于数学机械化方法的高档数控系统，为申请国家重大专项奠定基础。

经过一年的执行，项目取得重要进展，完成了计划任务。提出了最优拐角多周期变速过渡算法插补算法，验证显示新算法显著提高了加工速度与支持空间刀补的 5 轴联动数学方法，并在蓝天数控系统中实现。实验显示新算法显著提高了加工速度与质量，实现了自动空间刀补的功能。这些成果为项目的下一步实施奠定了基础。

2008 年 7 月 30 日，由中科院沈阳计算技术研究所、数学与系统科学研究院、计算技术研究所、沈阳自动化研究所和电工研究所共同发起的中国科学院数控技术创新联盟在沈阳成立。创新联盟旨在发挥中国科学院数控技术的综合优势，通过技术的原始创新和集成创新，开发具有自主知识产权的高档数控系统。为我国逐步走出高档数控系统核心技术受制于人的

局面做出了重要贡献。

项目简报如下：

简报 1. 项目第一次现场交流会纪要

2008 年 3 月 6 日至 7 日，本项目立项以来的第一次现场交流会在沈阳计算所举行。参加会议的包括系统所的高小山、李洪波、王定康、袁春明等五人和沈阳计算所的林浒、于东、杨东升、刘峰等十几名科研人员。会议通过现场调研对支持空间刀补的 5 轴联动数学方法、运动控制插补的数学机械化算法等进行了研讨，进一步明确与细化了项目实施方案。

3 月 6 日上午，林浒、高小山两位所长首先就各所的参加项目人员情况、项目准备情况做了介绍，对数控系统中的空间刀补和曲线插补探讨了相关数学问题的解决思路，并对可行性进行了分析。之后由林浒所长带队参观沈阳计算所的数控系统生产线和具体的数控机床加工，针对具体数控机床，现场讨论了项目的研究思路。与会人员还参观了沈阳计算所研发部的 CAD/CAM/CNC 软件演示，明确了各个程序段的输入、输出等细节，对现有的数控系统中需要改进的问题也有了进一步的认识。

3 月 6 日下午至 3 月 7 日下午，项目人员就刀补和插补的具体细节进行了讨论，明确与细化了项目实施方案：

- 首先启动曲线插补研究，针对 A 样条、B 样条、与三次多项式样条三种样条函数的插补进行分析，完成相关的理论研究和算法分析及实现；争取在直线段插补的基础上提出基于样条曲线插补的具体算法与实施方案，尽快启动编程。详见附件 1。
- 对于刀补方面，将参考西门子的相关资料，进一步探讨研究。对已有的几种方案进行研究确定一种实施方案，于 2008 年下半年编程实现。详见附件 2。
- 会议还商定，项目组将定期进行研讨，以确保按计划完成项目。

简报 2. 项目第二次现场交流会纪要

2008 年 5 月 24 日至 25 日，本项目第二次现场交流会在数学与系统科学研究院举行。参加会议的包括沈阳计算所的马跃、于东、杨东升、吴文江等六人和系统所的高小山、李洪波、王定康、袁春明等九名科研人员。会议通过九场学术报告和认真讨论，对运动控制插补的数学机械化算法形成了比较完整的方案，为下一步实施编程提供了基础；对支持空间刀补的 5 轴联动数学方法有了重要的进展；并决定首先针对两种典型的数控机床实施所提方案，尽快在工程化应用方面取得进展。

5 月 24 日，由系统所的 5 位科研人员做了关于 G 代码分割、代码压缩与拟合、基于样条曲线的运动控制插补、空间刀补及误差检测等问题的学术报告。大家通过认真讨论，确定了其中与技术相关的关键理论细节。5 月 25 日，由沈阳计算所的 4 位科研人员做了关于蓝

天数控系统功能与结构、运动控制关键技术、空间刀补、压缩与样条插补等问题的技术报告。通过理论方法与关键技术的相互交流，明确了如下实施方案与阶段性目标：

- 对于运动控制插补方面，首先根据曲率、挠率对 G 代码进行分段，然后对每段进行数据压缩或插值，在此基础上进行实时插补。对上述实施方案，将于 2008 年下半年启动编程。
- 对于刀补方面，通过参考西门子的相关资料，进一步研究发现可以通过刀位点与切触点的轨迹对应，得到曲面的法向信息，从而实现 5 轴联动的空间刀补。
- 经过商议，首先针对木工机械和雕铣机床两种典型数控系统实施上述方案，尽快产生可工程化应用的阶段性成果。

简报 3. 项目第三次现场交流会纪要

2008 年 7 月 30 日至 31 日，本项目第三次现场交流会在沈阳计算所举行。参加会议的包括系统所的高小山、李洪波、王定康等八人和沈阳计算所的马跃、于东、杨东升、吴文江等十几名科研人员。本次会议主要对第二次会议拟定的以高速加工为项目的切入点，并首先在木工机械和雕铣机床两种机床上进行验证方案的进展情况进行了学术研讨。在运动控制方面，对高速加工中程序段的高效处理形成了比较完整的数学机械化算法；在空间刀补方面，针对无干涉情况，形成了具体的解决方案，并对仿真结果进行了分析与讨论；同时，会议进一步明确与细化了下一阶段工作。

7 月 30 日下午，由沈阳计算所的技术人员以木工机械和雕铣机床为例，做了关于高速加工的技术报告。报告介绍了木工机械和雕铣机床的加工特点，对数控系统的特殊要求，以及沈阳计算所现有系统的控制算法以及控制效果。7 月 31 日上午，与会人员参观了木工机械和雕铣加工机床，现场讨论、分析了机床的加工特点和对数控系统控制的特殊需求；之后，由系统所的技术人员做了关于高速加工中程序段处理方法的数控机械化算法报告。报告介绍了加工程序小线段分组、小线段组的多项式拟合、误差检验、多项式曲线光顺连接和多项式曲线插补速度规划等一系列数学算法。7 月 31 日下午，系统所技术人员做了关于空间刀补的技术报告，报告介绍了各种刀具的空间刀具半径补偿的数学算法，并探讨了非线性误差、干涉等问题。会议通过学术报告和认真讨论，明确了下一步的具体工作：

- 在运动控制方面，对小线段加工程序压缩算法做进一步的仿真试验，对压缩算法的计算量和计算时间进行分析和测试，完善多项式曲线的插补算法，完成上述算法的软件编码，制定在数控系统中实现上述算法的方案并着手实施，在年底形成面向木工机械与雕铣机床的阶段性成果。
- 在空间刀补方面，进一步分析刀具半径补偿中的轨迹变化和干涉问题，设计相应的处理算法，制定在数控系统中实现上述算法的方案，并在 5 轴联动数控机床上着手验证。

简报 4. 项目第四次现场交流会纪要

2008 年 10 月 22 日至 11 月 6 日，本项目第四次现场交流会在沈阳计算所举行。参加会议的包括系统所的李洪波、张立先等三人和沈阳计算所的于东、杨东升、吴文江等十几名科研人员。本次会议主要针对高速加工中的速度规划问题，基于前几次技术交流所形成的理论结果，由系统所与沈阳计算所的技术人员共同设计并实施基于数学机械化方法高档数控系统速度规划的技术方案。方案在配套蓝天数控系统的数控机床中进行了验证，分析方案中存在的问题，并确定了下阶段的工作目标与工作计划。

10 月 22 日上午，首先由系统所的技术人员做了关于高速直线插补的拐角多周期变速过渡算法与关于平面折线的局部运动插补的技术报告。10 月 22 日下午，围绕系统所提出的新算法，基于蓝天数控系统的体系结构，双方技术人员经讨论，确定了算法与现有蓝天数控系统间的接口以及具体实施方案。2008 年 10 月 23 日至 11 月 6 日，经双方技术人员的共同努力，在蓝天数控系统中设计并实现了拐角多周期变速过渡算法与局部运动插补算法，验证显示新算法显著提高了加工速度与质量。具体实验结果如下：

- 通过对电机空载情况下加工数据的分析，验证了拐角多周期过渡算法的正确性；
- 在同等条件下，拐角多周期过渡算法比传统小线段过渡算法的加工速度提高了一倍，比传统拐角匀速过渡算法提高了 30%；
- 在相同加工条件下，拐角多周期算法的加工表面更清晰，整体加工效果好，但数控机床 Y 轴仍有轻微振动。

2008 年 11 月 6 日通过对本次实验进行总结，明确了下一阶段要解决的工作目标：

- 将目前 YZ 平面上的拐角多周期过渡算法扩展到三维空间，并针对 Y 轴的振动问题，设计基于加速度规划方法的解决方案；
- 将拐角多周期过渡算法融入蓝天数控产品中，改善现有产品对复杂曲线的处理能力，以形成阶段性成果。

一、学术会议

实验室成员组织或参与组织了 5 次学术会议，中心成员出访 29 次，接待国外学者来访 21 次。其中学术会议情况介绍如下：

1. 2008 年 4 月 10 日，“布尔代数求解”研讨会在京举行。该次会议由中科院数学机械化重点实验室与中科院软件所计算机科学国家重点实验室联合举办。实验室学术委员会主任万哲先院士参加了会议。贾祥雪、高小山、黄震宇分别就 SAT 问题主流研究、布尔方程求解的特征列方法及其在密码分析中的应用、求解布尔方程的 Groebner 方法与 XL 方法做了报告。共有 30 余位科研人员与研究生参加了本次学术交流活动。本次研讨会的成功举办发挥了数学机械化重点实验室在布尔代数领域的理论、人才方面的优势。实验室通过与国内相关研究单位的联合，对这一研究领域的发展起到了极大的促进作用。

2. 2008 年 4 月 26-28 日，第二届中法系统求解及应用研讨会（France/China Workshop on Solvers for Algebraic Systems and Applications）举行。会议由数学机械化重点实验室主办，法国巴黎六大、法国国家计算机与控制研究所（INRIA）、北京航天航空大学、北京大学协办。会议还邀请了加拿大西安大略大学教授 Stephen Watt，美国北卡州立大学教授 Hoon Hong 和法国 INRIA 主任研究员 Frabrice Rouillier 做邀请报告。本次会议主要议题为代数系统的求解和应用。与会学者讨论了符号方法、数值方法以及混合算法求解多项式系统的实根、复根和流形解，并探讨其在密码、机器人等领域的应用。中法国际合作项目 Chinese-Salsa 的成员就进一步合作研究和学生培养等进行了广泛的探讨和交流。作为加强国际交流合作的一个重要平台，研讨会在促进代数系统求解与应用的研究发展方面发挥重要作用。

3. 为推动我院的密码学研究，同时为有志于从事密码学研究的研究生与青年科研人员提供一个学习相关基础知识和前沿科研成果的机会，我院于 6 月 16 日－21 日举办了“密码学

及相关学科暑期班”。此次暑期班由中国科学院数学机械化重点实验室、中国科学院数学与系统科学研究院信息安全研究中心、中国数学学会计算机数学专业委员会联合承办，并且得到了中国科学院数学与系统科学研究院复杂系统国际研究团队的大力支持。在暑期班上堵丁柱教授（美国）、颜松远教授（英国）、丁津泰教授（美国）分别讲授了计算复杂性、计算数论和多变元密码学。来自全国二十余所高校及研究机构的 80 位研究生与青年教师参加了暑期班。本次暑期班一方面使国内学者与研究生了解了密码学领域的研究现状与研究热点，开阔了视野，扩大了知识面；另一方面为他们提供了与国际科学家进行思想交流的平台，真正达到了交流思想、增长知识、结识同行、促进交流合作的目的。通过本次会议也提高了与会人员的英文写作与交流水平。

4. 2008 年 6 月 16－18 日，第三届有限域及其应用会议在河南省郑州市召开，会议由科学院系统所与国家数字程控交换技术研究工程中心主办。中国科学院万哲先院士任本次会议主席，清华大学、北京大学等国内外多家高校和科研机构的 60 多位专家学者参加了本次会议。有限域及其应用会议为年度会议，本年度会议的主题包括：指数和应用，以及与多项式、本原元、矩阵、椭圆曲线、密码学等相关的性质与算法研究。在会上，多位报告者展示了自己研究的课题，研究的过程、方法以及取得的研究成果，并与大家进行了深入地探讨和广泛的交流。与会学者一致认为本次会议的多项报告涉及有限域领域的国际前沿问题，并且通过交流，拓展了大家的研究思路，推动了有限域领域研究的进一步发展。

5. 2008 年 10 月 24 日至 10 月 27 日，由中国数学学会计算机数学专业委员会主办、中国石油大学（华东）信息与控制工程学院与中国科学院数学机械化重点实验室承办的“第二届全国计算机数学学术会议(CM 2008)”，在山东省青岛市中国石油大学（华东）隆重召开。来自全国 33 所高校和科研院所的 120 多位代表及中国石油大学（华东）部分师生共 200 余人出席了本次会议。本届会议邀请了西安交通大学徐宗本教授、澳门科技大学齐东旭教授、新加坡南洋理工大学邢朝平教授、中国科学院软件所张健教授做特邀报告。本届会议还以分组报告的形式组织了 60 余场报告，主题涉及微分代数、微分方程、组合与图论、实代数方法、编码与密码、计算机视觉与模式识别、有限域、优化算法、控制方法等计算机数学领域

的理论及应用。代表们欢聚一堂，讨论热烈，交流充分，对计算机数学有了更加深入的认识，为计算机数学未来的发展打下了坚实的基础。

6. 2008 年 12 月 24 日至 12 月 25 日，中国科学院数学机械化重点实验室战略研讨会在京召开。实验室的成员悉数参加了本次研讨会。所有与会人员报告和总结了近年来在科研方面取得的进展，并对今后的工作进行了展望。随后大家齐聚一堂，回顾和总结了实验室在过去遇到的各种实际问题，并各抒己见，对实验室的发展贡献了各自的观点和看法。最后，研讨会制定了实验室未来几年的发展规划。整个过程中，与会代表们讨论热烈，交流充分，这次会议将对实验室今后的发展产生深远的影响。

二、参加国际学术会议

1. 高小山，参加国际会议“Computers in Scientific Discovery IV”, 2008.4, 上海，作报告“Automated Geometric Theorem Proving and Automated Diagram Generation”。(邀请报告)
2. 高小山，参加国际会议“International Workshop on Symbolic Real Algebra and Trustworthy Computing”, 2008.3, 上海，作报告“Topology Determination and Meshing for Algebraic Curves and Surfaces”。(邀请报告)
3. 高小山，参加国际会议“International Conference on Differential Algebra”, 2008.3, 意大利，作报告“Characteristic Set Method for Differential-Difference Polynomial Systems”。
4. 高小山，参加国际会议“ACM ISSAC”, 2008.7, 奥地利，作报告“A Characteristic Set Method for Solving Equations over Finite Fields”。
5. 高小山，参加国际会议“Automated Deduction in Geometry”, 2008.9, 上海，作报告：“An Introduction to Java Geometry Expert”。

6. 高小山，参加国际会议“IDMME Virtual Concept: Workshop on Geometric Constraints in Design”, 2008.10, 北京，作报告：“Geometric Constraint Solving and Applications”。
7. 高小山、黄震宇，参加国际会议“Inscrypt 2008: 3th International SKLOIS Conference on Information Security and Cryptology”, 2008.12, 北京，作报告：“A characteristic set method in finite fields”。
8. 万哲先，参加“群论及其相关领域国际会议”，2008 .3,徐州,作学术报告“Witt’s Theorem and Sylvester’s Law of Inertia”。
9. 李子明，参加国际会议“FoCM’08”，2008，香港。作报告“研究利用 Ore 多项式计算非线性控制论中的转移函数”。
10. 李子明，参加国际会议“ISSAC’08”2008，奥地利。
11. 刘卓军，参加国际会议“2008 International System Safety Regional Conference”，2008，新加坡。
12. 刘卓军，参加“2008 1st International Conference on Symbolic Computation and Cryptography”,2008，北京。
13. 刘卓军，参加“第三届有限域及其应用国际研讨会”，2008，郑州。
14. 王定康，参加“FOCM’08”国际会议，2008，香港。
15. 王定康，参加 MAP 研讨班与国际会议，2008.7，意大利。
16. 支丽红， 参加“FOCM’08”国际会议，2008，香港，作学术报告“符号数值方法求解多项式方程的奇异解”。
17. 支丽红，参加 MAP 研讨班与学术会议，2008.7，意大利，作“符号和数值方法求解多项式方程组”的报告。
18. 支丽红，参加国际会议“ISSAC’08”2008，奥地利。
19. 邓映蒲，参加欧洲密码学 2008 年学术年会“Eurocrypt 2008”，2008 年 4 月，土耳其。
20. 邓映蒲，参加美国密码学 2008 年学术年会“Crypto 2008”，2008 年 8 月，美国。
21. 闫振亚 ，参加“Similarity: Generalizations, Applications and Open Problems”, 2008.8.10-15，加拿大，作报告“(2+1)-dimensional generalized Burgers equation: Painleve analysis, Backlund transformation and similarity reductions”。（邀请报告）
22. 韩阳，参加国际会议“Representation theory of finite dimensional algebras”,2008.2，Oberwolfach, Germany 。
23. 韩阳,参加会议“American Mathematical Society – Shanghai Mathematical Society Joint Meeting”， 2008.12 ,Fudan University, Shanghai, China。
24. 冯如勇，参加微分代数以及相关问题会议(Differential Algebra and Related Topics)，2008.11，美国鲁格斯大学纽瓦克校区。
25. 袁春明，参加 MAP 研讨班与学术会议，2008.7，意大利，作了“关于有限域 F2 上特征

列方法”的报告。

三、参加国内学术会议

1. 高小山，参加国内会议“中国工业数学学术年会”, 2008 8, 郑州，作学术报告“ A Characteristic Set Method for Solving Boolean Equations”。
2. 万哲先，参加 “有限域及其应用第三次研讨会”，2008 .6，郑州。
3. 李子明，参加“第二届全国计算机数学学术会议”，2008.10.24-27，青岛。
4. 刘卓军，参加“第二届中国计算机数学学术会议”，2008.10.24-27，青岛。
5. 刘卓军，参加“第十届中国管理科学学术会议”，2008，合肥。
6. 王定康，参加“第二届全国计算机数学学术会议”，2008.10.24-27，青岛。
7. 支丽红，参加“第二届全国计算机数学学术会议”，2008.10.24-27，青岛。
8. 韩阳，参加“第十届全国代数表示论会议”，2008.8.23,南京大学。
9. 韩阳，参加“第十一届全国代数会议”，2008 .10. 19，湖南张家界。
10. 闫振亚，参加“第二届全国计算机数学会议”, 2008.10.24-27，青岛 ，作报告“The modified KdV equation with variable coefficients: Exact uni/bi-variable travelling wave-like solutions”。
11. 袁春明，参加“第二届中国计算机数学学术会议”，2008.10.24-27，青岛，作报告“差分素理想的一个判别准则”。
12. 邓映蒲，参加“中国密码学 2008 年学术年会－ChinaCrypt 2008”，2008.10，武汉。
13. 邓映蒲，参加第二届全国计算机数学学术会议，2008.10，青岛。

四、实验室成员出访

- 闫振亚，访问香港大学， 2008.1-2
- 冯如勇，访问北卡州立大学数学系，美国，2008
- 袁春明，访问了意大利 ICTP，2008.7-8
- 支丽红，访问了意大利 ICTP，2008.7-8

一、数学机械化讨论班

数学机械化讨论班始自 1985 年，以下列出 2008 年的学术报告。

2008-11-12	Mohab Safey El Din INRIA,UPMC,Univ Paris 06 LIP6，France	Real Solving Polynomial Systems with the Critical Point Method: From Theory to Practice
2008-11-12	Erich Kaltofen North Carolina State University, USA	A Fraction Free Matrix Berlekamp/Massey Algorithm
2008-7-9	Deepak Kapur University of New Mexico Albuquerque, NM, USA	Multivariate Resultants based on Cayley-Dixon's Method
2008-6-14	Prof. Ling San Nanyang Technological University, Singapore	Perfect Nonlinear Functions, Codes and Secret Sharing Schemes
2008-6-14	Huaxiong Wang Nanyang Technological University, Singapore	Some Combinatorial Approaches in Secret Sharing Schemes
2008-6-4	HaoHao Wang Southeast Missouri State University, USA	Using Syzygies to find implicit equations of parametric surfaces with base points
2008-5-14	Prof. Moulay Barkartou University of Limoge, France	Super irreducible decompostion of linear differentia equations
2008-4-20	Jintai Ding University of Cincinnati, USA	Multivariate Cryptography
2008-4-16	Ding-Zhu Du University of Texas at Dallas, USA	Computational Complexity
2008-4-16	Song Y. Yan Bedford University, UK	Computational Number Theory
2008-4-10	贾祥雪 中科院数学与系统科学研究院	SAT 问题主流研究纵览
2008-4-10	高小山 中科院数学与系统科学研究院	A Characteristic Set Method for Solving Boolean Equations and Applications in Cryptanalysis
2008-4-10	黄震宇 中科院数学与系统科学研究院	求解布尔方程的Groebner方法与XL方法

二、专题讨论班

题　目	时　间	主持人
特征列方法	每周一、三下午	高小山
经典几何计算	每周二下午	李洪波
非交换环理论	每周三晚上	李子明
微分与差分特征性	每周三下午	李子明
计算代数几何引论	每周一上午	王定康
数值与符号混合计算	每周五下午	支丽红
代数几何及其应用	每周六下午	李邦河
数学物理讨论班	每周四	王世坤
生物信息学	每周一下午	李邦河
有限域及其应用	每周五上午	万哲先
密码学进展	每周五下午	邓映蒲

万哲先	《Algebra Colloquium》主编 《Annals of Combinatorics》编委 《Discrete Applied Mathematics》编委 《Finite Fields and Their Applications》编委 《Journal of Combinatorics, Information and System Sciences》编委 天津南开大学组合中心学术委员会主任 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 山东理工大学学术委员会主任
李邦河	《东北数学》编委 《数学季刊》编委 《数学学报》编委 《系统科学与数学》编委 《数学物理学报》编委
高小山	《Journal of Systems Science and Complexity》**副主编** 《Journal of Symbolic Computation》 **编委** 《International Journal of Computers Communications & Control》**编委** 《The Open Artificial Intelligence Journal》**编委** 《Electronic Journal of Mathematics and Technology》**编委** **《系统科学与数学》副主编** **《系统工程与应用》副主编** **《中国科学 A》编委** **《计算机辅助设计与图形学学报》编委** **《中国图象图形学报》编委** **《中国高校应用数学学报》编委** 国际符号与代数年会(ISSAC)指导委员会主席(2008-2009) 中国数学会计算机数学专业委员会主任 中国系统工程学会副理事长 中国工业与应用数学会常务理事
王世坤	《数学学报》编委 《数学进展》编委
刘木兰	《系统科学与数学》编委
刘卓军	《系统科学与数学》编委
李洪波	《系统科学与数学》编委

	《自动化学报》编委 中国数学会计算机数学专业委员会副主任
李子明	《Journal of Symbolic Computation》编委 《Journal of Systems Science and Complexity》编委. ACM SIGSAM, Advisor
支丽红	《Journal of Symbolic Computation》编委 《Mathematics in Computer Science》编委 国际符号与数值混合计算指导委员会委员。

1. 2008 年 1 月 18 日新春佳节即将到来之际，中共中央总书记、国家主席、中央军委主席胡锦涛亲切看望吴文俊院士，代表党中央向他表示衷心的祝福。 总书记同吴老一家人促膝而坐，深情交谈。他说，长期以来，吴老站在数学科学的前沿，潜心研究，勇于探索，取得了一系列原创性成就，特别是在拓扑学、数学机械化领域作出了杰出贡献，为国家、为民族争了光。吴文俊笑着对总书记说，我希望自己能够做得再好一些。现在年轻一代都成长起来了，他们的底子比我们这一代更扎实，希望寄托在他们的身上。 胡锦涛点点头，赞赏地说，年轻人的迅速成长，也与您的提携、培养有很大的关系。您热爱祖国、追求真理、勇攀高峰、无私奉献的崇高精神，值得广大科技工作者学习。

随后，胡锦涛与吴文俊围绕基础科学研究探讨了起来。 总书记说，基础研究是科技进步的先导，是自主创新的源泉。只有以深入的基础研究作后盾，才能不断提高原始创新能力，增强国家发展的后劲。我们不仅要大力加强应用研究，而且要高度重视基础研究。 吴文俊回答道，我非常赞同总书记的观点。我们之所以能在应用领域取得一些成功，关键是我们的数学研究有扎实的基础。我们不能忽视基础研究。

总书记又说，从党和政府来讲，第一要充分认识基础研究的战略意义和重大作用，第二要加大在这方面的投入力度，第三要重视培养从事基础研究的人才特别是创新人才，第四要营造宽松的学术环境，推动我国基础研究取得更多优秀成果。 吴老连声称好，他高兴地说，总书记的这些重要思想，对科技界是一个极大的鼓舞。感谢党中央对科技界的重视和关心。

交谈中，胡锦涛诚恳地对吴老说，党的十七大强调要坚持走中国特色自主创新道路，建设创新型国家。这方面的任务十分繁重、十分艰巨，需要广大科技工作者不懈努力。吴老学识渊博、经验丰富，希望您为发展我国科技事业多提宝贵意见和建议。吴文俊向总书记提出，建议中央进一步制定鼓励政策，为自主创新创造良好的环境。

2. 2008 年 1 月 25 日，政协第十届全国委员会常务委员会第二十次会议，通过了中国人民政治协商会议第十一届全国委员会委员名单。李邦河院士当选为政协第十一届全国委员会委员。

3. 2008 年 10 月 24 日至 10 月 27 日，第二届全国计算机数学学术会议(CM 2008)，在山东省青岛市中国石油大学（华东）隆重召开。来自全国 33 所高校和科研院所的 120 多位代表及中国石油大学（华东）部分师生共 200 余人出席了本次会议。李邦河院士对吴文俊院士创建数学机械化和机械化数学的经历进行了回顾，并对计算机数学的未来发展表示充满信心。李邦河院士还应邀在中国石油大学做了公众报告。

4. 2009 年 1 月 5 日，全国人大副委员长、中国科学院院长路甬祥来到吴文俊院士家中看望吴文俊院士，向他恭贺新春和亲切问候，并就数学的发展与应用进行了深入交谈。

5. 2009 年 1 月 22 日，科技部曹健林副部长来到吴文俊院士家中看望吴文俊院士，向他恭贺新春和亲切问候，国家奖励办领导陪同看望。