2008 年 1 月 19 日，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

目 录

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

秘书：　周代珍，王莎莎

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

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.	刘卓军	数学	符号运算、信息安全	研究员
8.	刘木兰	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	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.	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：

谢端强、柴凤娟、王灯山、谢　正、王培宏、黄　雷、熊　涛、张贵林、张艳硕、李　家、刘　姜、吴晓丽、王怀富、张振华、冷福生、沈跃峰、周　凯、顾振华、孙　瑶、黄震宇、曹源昊、周升田、陈绍示、李　博、张艳娟、潘彦斌

硕士生：

李　斌、张　梅、赵尚威、孙瑞勇、羊正正、樊　伟、郭磊磊、李　伟、付国锋、郭　锋、刘元杰、于　彭

毕业及授予学位情况

出站博士后：申立勇

毕业博士：　周城雄、沈亚良、袁春明、张志芳

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第一届学术委员会第四次会议于 2007 年 3 月 24 日在中科院数学与系统科学研究院召开。吴文俊院士、万哲先院士、李邦河院士、林惠民院士等 11 位实验室学术委员会成员出席了会议。国家自然科学基金委信息科学学部刘克处长、数理学部张文岭处长、中科院基础局数力天处王永祥副处长、中科院综合计划局科研基地处周鼐博士应邀参加了会议。

会议由学术委员会主任万哲先院士主持。实验室副主任李洪波研究员汇报了实验室 2006 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申请创新研究群体“机器智能中的数学机械化方法”的预答辩。

专家们对实验室工作进行了认真的审议和讨论，对一年来的工作予以充分肯定，一致强调，实验室应该继续发挥在数学机械化理论方面的优势，同时更多地关注国家需求。专家们对研究群体的定位、研究方向等方面提出了具体的建设性意见，指出这一群体在数学和信息科学领域开展交叉研究，在基础研究方面做出了很多出色的工作，并且已经将数学机械化应用于计算机视觉、信息安全等领域。专家们建议应该进一步面向国家战略需求，运用数学机械化这一先进工具，解决信息科学中的挑战性理论与算法问题，为信息科学的发展做出贡献。

二、实验室开放课题

实验室通过以下专项经费支持开放课题：

- “数学机械化应用推广专项经费”
- “吴文俊数学与天文丝路基金研究计划”
- “数学机械化思维与非数学机械化思维”研究基金
- “中国科学院数学机械化重点实验室开放课题”研究基金

本年度共批准 12 项开放课题，其中以来访项目为主。

2007 年开放课题支持项目

序号	课题名称	承担单位	承担人
1.	微分和差分多项式的分解	中国科技大学	张明波
2.	混合计算	美国北卡州立大学	杨争峰
3.	差分--微分维数多项式算法研究	北京航空航天大学	周　梦
4.	位移结构矩阵在符号数值混合计算中的应用	东北师范大学	李冰玉
5.	混合结式理论及其应用	天津工程师范学院	孙维昆
6.	借助特征列方法构造 Gröbner 基	电子科技大学	李永彬
7.	代理转换加密理论研究与实现	江西财经大学	谭作文
8.	数学物理方程的求解、不变量 及等价性问题研究	大连理工大学	梅建琴
9.	计算微分差分代数	湖北大学	郑大彬
10.	求解非线性波方程和格的计算机代数研究	辽宁师范大学	谢福鼎
11.	黎曼几何的符号计算与定理机器证明的算法	中央民族大学	曹丽娜
12.	若干重要非线性系统的机械化求解研究	宁波大学	李　彪

三、实验室客座人员与访问学者

姓　名	工 作 单 位	访 问 时 间
谢福鼎	辽宁师范大学	2007.7
谭作文	江西财经大学	2007.8
李冰玉	东北师范大学	2007.8
张明波	中国科技大学	2007.8
郑大彬	湖北大学	2007.8
吴　敏	华东师范大学	2007.8
李玉奇	宁波大学	2007.8
李　彪	宁波大学	2007.8
Miles Reid	University of Warwick, UK	2007.4
Marc Moreno Maza	University of Western Ontario, Canada	2007.5
Eric Schost	University of Western Ontario, Canada	2007.5
Zhijun Qiao	University of Texas at Austin, USA	2007.5
Chandrajit Bajaj	University of Texas at Austin, USA	2007.5
Karl Sigmund	University of Viena, Austria	2007.6
Paul S. Wang	Kent State University, USA	2007.6
Frederic Chyzak	INRIA, France	2007.6
Ludovic Perret	Univ. Paris 6, France	2007.6
Jean-Charles Faugere	Univ. Paris 6, France	2007.6
Philippe B. Trebuchet	Univ. Paris 6, France	2007.6
Agnes Szanto	North Carolina University, USA	2007.6
Erich Kaltofen	North Carolina University, USA	2007.7
Hidetsune Kobayashi	Nihon University, Japan	2007.8

Jing-Ping Wang	University of Kent, UK	2007.9
Wenchang Chu	Lecce University, Italy	2007.9
Greg Reid	University of Western Ontario, Canada	2007.12
Wen-Xiu Ma	University of South Florida, USA	2007.12

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、北京邮电大学等高校的大学生和一些中小学师生参观了数学机械化重点实验室。实验室秘书王莎莎介绍了从 1990 年数学机械化中心成立一直到现在，数学机械化重点实验室的历史沿革、发展情况、研究领域以及重要的学术进展。实验室研究生黄雷、李家、张艳硕、王怀富等进行了数学机械化平台软件演示。参观的同学们对实验室的介绍和演示表现出了浓厚的兴趣，踊跃提问，并表示希望将来有机会能到实验室来深造。

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取得可喜进展，获国内外奖励 2 项，发表专著 2 部，论文 69 篇，其中 SCI 论文 32 篇，EI 论文 7 篇；组织召开了第二届中美符号计算联合研讨会、第一届全国计算机数学学术会议，并批准了 12 个实验室开放课题。

在加拿大举行的第 32 届国际符号和代数计算会议(ISSAC'07)上，实验室李洪波研究员的论文获得本年度唯一的“ISSAC 杰出论文奖”。 “ISSAC 杰出论文奖”由“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。这是数学机械化重点实验室成员第二次获得这一奖项。

实验室支丽红副研究员因在符号数值混合计算方面的工作获得系统所“关肇直青年研究奖”。支丽红与合作者将结构矩阵方法引入到混合计算，提出了 GCD、因式分解这些基本运算的快速混合计算方法以及近似超定多项式方程组求解方法。

主要科研成果：

- **几何不变量理论**

1. 高级不变量代数理论

完成了以共形几何代数、零括号代数、零几何代数、零 Grassmann-Cayley 代数为核心的高级不变量代数理论，后两者是今年建立的。它们是经典不变量理论在经典几何中的发展，为不变量理论的有效符号计算奠定了基础。该项工作获得获 ISSAC 2007 杰出论文奖。据介绍，它为欧氏几何符号计算的简化提供了巨大的改进，以前数十万项都难以完成的计算，现在只要一两项就能完成。该工作的基础是共形几何代数和零括号代数，而它们都是由李洪波研究员等建立的。国际同行认为，该项工作是符号机器证明领域的一个突破，其意义超出该领域本身。（李洪波）

2. 几何代数中的新理论与算法

建立了几何代数中转量的压缩理论与算法、消阶理论与算法、三维几何的向量三角函数和向量复数理论与算法；它们的作用将在具体的几何应用中得到体现。其中的消阶理论与算法已经在经典几何和微分几何计算中表现了惊人的简化计算效果。（李洪波）

- 特征列理论与算法

1. 微分-差分方程的特征列方法

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，微分-差分(DD)方程，发展相应的特征列方法与算法。我们首先证明了 DD 多项式系统的诺特性质，即任意 DD 多项式组的零点与有限个 DD 多项式组的零点相同。我们证明了 DD 升列的若干基本性质，得到了 DD 升列是其饱和理想的特征列的充分必要条件，DD 自反素理想和强 DD 不可约升列之间的一一对应关系。特别是证明了真不可约升列是正规的、自反的与非平凡的，由此给出了判定一个升列是正规升列的构造性条件。 以此为基础，建立了 DD 情形的零点分解定理，并利用零点分解定理解决了 DD 多项式系统的完备理想成员问题。进一步研究了常微分－差分混合问题的零点结构，构作了常微分－差分的特征列所对应的差分核，解决了这一代数结构下的根理想判定问题。这一工作将数学机械化方法推广到一种新的方程类型。(高小山，袁春明等)

2. 三角形式的多项式系统的实根隔离算法

对给定的零维三角列多项式系统，我们引进了所谓的 evaluation bound(EB)并给出了计算三角形方程组的 EB 的方法。以此为基础，给出了基于所谓 sleeve 函数隔离三角形方程组实根的充分条件与有效算法。这一工作首次给出隔离三角形方程组的重根的算法。(高小山，程进三等)

3. 直纹面的恰当有理表示

代数曲面的恰当参数化不仅是一个重要的公开算法问题，还在计算机图形学与几何造型设计中存在广泛应用。我们对于代数直纹面完全解决了这一问题：首先对定义在非恰当格点上的直纹面给出算法，使其定义在恰当格点上，然后将非恰当直纹面恰当化问题变为求一个平面曲线的恰当化问题，从而给出了直纹面的恰当化算法。（高小山，申立勇等）

4. 多项式系统求解

(1) 提出了一种将多项式系统分解为正则升列的方法。给出了将正则升列转换为正规升列的高速算法。从算法的测试中可以看出我们算法的效率比已有方法有效得多。
(2) 对代数扩域上多项式的因式分解问题进行了研究，提出了一种基于矩阵特征多项式的代数扩域上多项式的因式分解算法。
(3) 提出了一种将代数簇分解成不可约代数簇的新方法。（王定康）

- 微分与差分方程的构造性方法

1. 线性微分差分系统

研究了 Ore 模的局部化问题，由此给出了 Ore-Laurent 模的简单刻画。证明了超指数函数在常数域和有理函数域上线性相关的判定法则。研究了实初等函数的分类问题，证明了在任何实超越初等扩张中，反正切函数集合和对数函数集合的交集等于空集。研究了微分算子相似性的判定问题，证明了两个 2 阶可约微分算子相似的充要条件是一类特殊的含参 Risch 方程有有理解。（李子明）

2. 一阶代数微分方程的代数通解

将函数域上的计数理论用于一阶代数微分方程的代数通解的研究，给出了判定一阶代数微分方程的代数通解存在性的有效判别法，并给出了代数通解的显式表示。从符号计算的角度实现了 Poincaré 关于一阶代数微分方程的经典定理以及 Schwartz 关于代数曲线双有理自变换的有限性定理。（马玉杰）

3. Fourier 超函数

给出了热方程的解与 Hermite 热方程的解之间的精确关系。证明了 Hermite 热方程的某一类解的边界决定了唯一的（扩张）Fourier 超函数，反之，任意（扩张）Fourier 超函数均为该类 Hermite 热方程的解的边界。这是迄今关于 Fourier 超函数和扩张 Fourier 超函数最好的表示定理。（李邦河）

4. 生物化学中的应用

证明了酶动力学中的拟稳定态假设恒正确，从而使这一写入生物化学教科书的具有八十多年历史的假设成为一个定律。被审稿人称为“outstanding paper”,“novel analysis”。文章即将在化学方面的一流杂志Journal of Physical Chemistry上发表。（李邦河）

● 有限域在密码学中的应用

1. 有限域中离散对数公式的简证

设F_q为有限域，α 为一生成元，对任意$a\in F_q$，设$a=\alpha^y$，$y\in[1, q-1]$，则称y为a对于底 α 的离散对数。1986 年，Mullen和White得到公式:

$$y \equiv -1+\sum_{i=1}^{q-2}\frac{a^i}{\alpha^i-1} \bmod p.$$

1990 年，Nidderreiter 给了这个公式一个简单证明，但要假定 $q\geq 3$。现在我们对一切 q 给出一个更简单证明，该证明将在 Discrete Mathematics 上发表。（万哲先）

2. 有限域的第 I 种类型最优正规基的对偶基的复杂度

流密码中常涉及有限域的一些计算，采用正规基比较方便。复杂度最小的正规基称为

最优正规基。1992 年，高绪红和 H.W. Lenstra 确定了只有两类最优正规基，称为 I 类或 II 类。在他们的证明中可见 II 类正规基是自对偶的，但 I 类正规基的对偶基是什么？以及它的复杂度怎样，是悬而未决的公开问题。2007 年我们算出了 I 类正规基的对偶基及其复杂度，解决了这一公开问题。（万哲先，周凯）

3. 数个线性移存器序列的乘积

流密码通常是由线性移存器序列经组合产生。数个线性移存器序列按位相乘就是最简单的一种组合方式。设有m个线性移存器序列，其极小多项式为$\sigma_1(x)$到$\sigma_m(x)$。今对其乘积序列定义了两个多项式Z和A，证明了乘积序列的极小多项式$n(x)$适合A| $n(x)$和$n(x)$|Z. 当m=2 时，这是Göttfert和Nidderreiter的工作，我们从 2 推广到m。（万哲先，周凯）

- **密码学与信息安全**

1. 秘密共享

构造了权重不同参与者之间的秘密共享方案、多重秘密和动态的秘密共享方案，以及防欺诈和可验证的秘密共享方案。这些工作的基础——特殊差分方程的秘密共享方案，是我们首先提出的。我们还基于线性码理论构造了一个新的秘密协商方案，它不同于以往的密钥协商方案，不必基于假设，具有高效性和灵活性。我们还构造了动态口令的认证方案，给出了无可信中心的秘密协商和密钥共享方案。（刘卓军，张艳硕）

2. 密码学与信息安全

在流密码的代数攻击方面，给出了代数免疫度为 1 的布尔函数的计数公式及这种函数的紧的非线性度上界。基于图的连通性构造了一个理想的具有乘性的线性密钥共享体制，可以用于设计高效的安全多方计算协议。此外，提供了除已知的门限存取结构、自对偶存取结构以外，又一类新的可以被理想的乘性线性密钥共享体制实现的存取结构。完成专著《密钥共享体制和安全多方计算》。（刘木兰，邓映蒲）

3. 理想的乘性线性密钥共享体制的构造

乘性的线性密钥共享体制对于多方计算中安全地计算乘法至关重要，而理想的密钥共享体制其数据扩散达到最低，从而具有很高的效率。我们基于图的连通性构造了一类理想的具有乘性的线性密钥共享体制，可以用于设计高效的安全多方计算协议。此外，提供了除已知的门限存取结构、自对偶存取结构以外，又一类新的可以被理想的乘性线性密钥共享体制实现的存取结构。结果发表在 IEEE Trans. Information Theory 上。(刘木兰，张志芳)

4. 基于图上随机游动的密钥共享体制

设计了一类理想的密钥共享体制，可以通过图上的随机游动来进行主密钥的重构，使得密钥重构算法的空间复杂度由一般的多项式级别降低到对数级别，同时保持时间复杂度没有增加，只是产生了一个可忽略的错误概率。(刘木兰，张志芳)

5. 保护隐私的联合求解线性方程组

基于安全多方计算的思想解决了保护隐私的联合求解线性方程组的问题，即多个参与者，每人私自持有方程组的一部分，可以联合求出这个方程组的解，同时不泄漏各自掌握的方程信息。(刘木兰，张志芳)

- 复杂非线性波、混沌同步与控制

1. 通过分离变量, 提出了一个有效的算法, 用于求解大批(N+1)-维实数域和复数域中非线性微分方程含有任意函数的非行波类型的解析解。
2. 首次提出了新的具有非线性色散项的耦合 Klein-Gordon (CKG(m,n,k))方程和耦合的非线性 Schrödinger (GCNLS(m,n,p,q))方程, 并且给出它们的包络 compacton 解。
3. 给出了高维 KP 方程的 Wronskian 行列式解，并研究了解的性质。
4. 研究了类 Lorenz 混沌系统的 Hopf 分歧问题。
5. 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。另外，基于线性反馈、自适应反馈和它们的组合反馈方法, 研究了一个具有双混沌系统的完全和滞后同步。
6. 提出了一类修正的超混沌 Rossler 系统的若干全局指数(滞后)同步的有效控制器。
7. 应美国 Nova Science 出版社主编之邀撰写论著《Computer Physics Research Trends》中的一章。（闫振亚）

- 混合计算

研究了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。将稀疏平方和技术应用于多项式近似最大公因子、因式分解的计算。探讨了半正定规划在近似多项式方程组求解中的应用。还研究了基于对合系统的近似多项式重根的精确计算。另外，将结构扰动方法应用于有理函数的插值计算稳定计算。（支丽红）

- 结合代数

证明了代数与模的拟 Koszul 性为 Morita 不变量。一个有限群分次代数为拟 Koszul 的当且仅当其 smash 积如此。此外，证明了一个有限群分次代数的 smash 积的 Yoneda 代数与其 Yoneda 代数的 smash 积同构。应用这些结果得到代数 Koszul 性与有限 Galois 覆盖之

间的关系。利用有限 Galois 覆盖，由一个给定 quiver 及关系的 Koszul 代数，可以构造许多新的 Koszul 代数，而且它们的 quiver 及关系能够直接给出。(韩阳)

二、奖励

1. 在加拿大举行的第 32 届国际符号和代数计算会议(ISSAC'07)上，实验室李洪波研究员的论文 “A Recipe for Symbolic Geometric Computing: Long Geometric Product, BREEFS and Clifford Factorization”获得本年度唯一的“ISSAC 杰出论文奖”。“ISSAC 杰出论文奖”由“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。这是数学机械化重点实验室成员第二次获得这一奖项。李洪波研究员的论文为欧氏几何符号计算的简化提供了巨大的改进，以前数十万项都难以完成的计算，现在只要一两项就能完成。该工作的基础是共形几何代数和零括号代数，而它们都是由李洪波研究员等建立的。国际同行认为，该项工作是符号机器证明领域的一个突破，其意义超出该领域本身。
2. 实验室支丽红副研究员因在符号数值混合计算方面的工作获得 2006 年度“关肇直青年研究奖”。支丽红与合作者将结构矩阵方法引入到混合计算，提出了 GCD、因式分解这些基本运算的快速混合计算方法以及近似超定多项式方程组求解方法。
3. 实验室万哲先院士、李邦河院士获得数学与系统科学研究院优秀指导教师奖。

研究生获奖

1. 实验室研究生张志芳获得由瑞士科技部设立的应用数学欧拉奖，并得到瑞士政府资助参加了 2007 年 7 月在瑞士举行的第六届国际工业与应用数学大会。
2. 实验室研究生王灯山、王怀富、张艳硕、袁春明被评选为 2006-2007 年三好学生。张志芳被评为优秀毕业生。
3. 实验室博士生冷福生、周凯获得 2007 年度中国科学院数学与系统科学研究院院长奖学金特等奖。
4. 实验室博士生王灯山获得 2007 年度中科院“宝洁优秀博士生”奖、2007 年度中科院数学院院长奖学金优秀奖、2007 年度中国科学院研究生院澳大利亚 BHP Billiton 奖学金。 BHP Billiton 奖学金由中国科学院研究生院与澳大利亚 BHP Billiton 公司联合奖学金评审委员会审核评议，2007 年科学院共有 25 位在学研究生获得这一奖励。

一、专著与专利

专著 2 本：

1. 李子明等，《计算机代数》，清华大学出版社，2007。
2. 闫振亚，复杂非线性波的构造性理论及其应用, 北京：科学出版社，2007。

发明专利 1 项：

由圆柱副、圆柱副和球面副构成的并联机构

发明人：高小山、廖启征

专利号：ZL 2004 1 0073712.2

授权时间：2007 年 5 月 2 日

二、期刊论文

1. Bingyu Li, Zhuojun Liu and Lihong Zhi: A Fast Algorithm for Solving the Sylvester Structured Total Least Squares Problem, *Signal Processing*, 87 (2007) pp. 2313-2319. (SCI)
2. Bingyu Li, Zhuojun Liu and Lihong Zhi: A Structured Rank-revealing Method for Sylvester Matrix, *Journal of Computational and Applied Mathematics*, February, 2007. (SCI)
3. Dongxia Sun and Lihong Zhi: Structured Low Rank Approximation of a Bezout Matrix, *Mathematics in Computer Science*, Birkhäuser, Basel, 2007.
4. X. Zhao and X.S. Gao, Binary Affinity Genetic Algorithm, *Journal of Heuristics*, 13, 133-150, 2007. (SCI)
5. X. Zhao, X.S. Gao, and Z. Hu, Evolutionary Programming Based on Non-uniform Mutation, *Applied Mathematics and Computation* 192, 1-11, 2007. (SCI)
6. W.T. Wu and X.S. Gao, Mathematics Mechanization and Applications after Thirty Years, *Front. Comput. Sci. China*, 1(1), 1-8, 2007.
7. Q. Lin, X.S. Gao, Y Liu, G Dai, Complete Method Based on Geometric Constraint Solving (in Chinese), *Journal of CAD and CG*, 19(7), 828-834, 2007. (EI)
8. J. Li, L. Shen, X.S. Gao, Proper Reparametrization of Rational Ruled Surface, accepted by *JSCT* (SCI)
9. X.S. Gao and M. Zhang, Decomposition of Differential Polynomials, accepted by *AAECC*. (SCI)

10. Zheng Xie and Hongbo Li , Exterior Difference System on Hypercubic Lattice，*Acta Appl. Math.* (2007) 99: 97–116. (SCI)
11. D. Wang, H. Li , Elliptic Equation'S New Solutions and Their Applications to Two Nonlinear Partial Differential Equations, *Applied Mathematics And Computation* 188: 761-772, 2007. (SCI)
12. D. Wang, H. Li, Symbolic Computation and Non-Travelling Wave Solutions of (2+1)-Dimensional Nonlinear Evolution Equations, *Chaos, Solitons and Fractals* 2007, doi: 10.1016/j.chaos.2007.07.062. (SCI)
13. 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* 2007, doi: 10.1016/j.chaos.2006.11.025. (SCI)
14. 张宁、李洪波, 仿射括号代数理论与算法及其在几何定理机器证明中的应用, *中国科学* A辑, 2007, 37(5): 523-531. (SCI)
15. Z. Li, M. Wu, On Solutions of Linear Functional Systems and Factorization of Laurent-Ore Modules, *Latest Advances in Symbolic Algorithms*, World Scientific, 2007.
16. Shengqiang Liu, Zhuojun Liu, Jianliang Tang, A Delayed Marine Bacteriophage Infection Model, *Applied Mathematics Letters*, 20 (2007) pp. 702 – 706. (SCI)
17. Shengqiang Liu, Zhuojun Liu, Permanence of General Stage-Structured Consumer-Resource Models, *Journal of Computational and Applied Mathematics*, 201 (2007) pp. 381—388. (SCI)
18. L.P. Huang, Z.J. Liu, Similarity Reduction of Matrix over a Quaternion Division Ring, *Linear Algebra and Its Applications* 427 (2-3): 317-332 Dec 1, 2007. (SCI)
19. 刘卓军，代理签名研究进展，*北京电子科技学院学报*，Vo. 15, No. 2, 2007. pp. 5--10.
20. 张艳硕、刘卓军，基于差分的特殊权限（m+n,t1+t2）门限秘密共享, *计算机工程与应用*, 2007 年 4 月 12 期 2007，vol.43（12）20-22.
21. 张艳硕、刘卓军、杜耀刚，特殊权限下权重不同参与者之间的广义门限秘密共享方案，*计算机工程与应用*，2007 年 6 月 17 期，vol.43（17）15-17.
22. 张艳硕、刘卓军，基于特殊权限的另一门限秘密共享方案，*计算机工程与应用*，2007 年 7 月（20）：143-144.
23. 张艳硕、刘卓军，基于特殊差分方程的安全的多重秘密门限共享方案，*计算机应用*，2007 年 8 月：1913-1914.
24. 张艳硕、刘卓军，基于特殊差分方程的安全可验证的门限秘密共享，*计算机工程与应用*，2007（23）：6-7.
25. Yanshuo Zhang, Zhuojun Liu, Dynamic and Verifiable Secret Sharing among Weighted

Participants, *J. Syst. Sci. & Complexity*, (2007) 20: 481– 485. (SCI)

26. 张艳硕、刘卓军, 有门限可认证的多重秘密密钥协商方案, *计算机应用*, 2007（10）: 2450 – 2452.
27. 张艳硕、刘卓军 无可信中心的动态多重秘密(m+n,t1+t2)门限方案，*通信学报*, Vol. 28, No. 11A, Nov. 2007, pp. 172 – 176.
28. 刘卓军、吴尽昭，集成电路验证技术，*中国基础科学*，2007(3)，第 9 卷，总第 57 期，pp. 11 – 14.
29. 王培宏、刘卓军、唐志鹏，基于数据包络分析的风险投资环境有效性研究，*管理科学*，第 4 卷，第 5 期，2007 年 9 月，pp. 584 – 587.
30. 刘卓军、周城雄，中国数字内容产业的创新模式分析，*中国软科学*，2007(6), 总第 198 期，pp. 111 – 114.
31. 马玉杰, 最大 Abel 商群为局部循环群的可解群, *数学学报*, 50:4, 2007.
32. Y. Ma, On a Characterization of Quasicyclic Groups, *Glasnik Matematicki*, Vol. 42, No.2 (2007).
33. D. Wang, An Algorithm for Decomposing a Polynomial System into Normal Ascending Sets, *中国科学* (A 辑) 2007 卷 50 期: 1441－1450. (SCI)
34. 吴天骄，关于吴方法在双层规划中的应用, *武汉数学物理学报*，Vol.27, No.1, Ser. A, 2007.
35. Z. Yan, Separation Transformation and Envelope Solutions of the Higher Dimensional Complex Nonlinear Klein–Gordon Equation. *Phys. Scr.*, 75 (2007) 320. (SCI)
36. Z. Yan, New Exact Solution Structures and Nonlinear Dispersion in the Coupled Nonlinear Wave Systems. *Phys. Lett. A*, 361 (2007) 194. (SCI)
37. Z. Yan, Similarity Transformations and Exact Solutions for A Family of Higher-Dimensional Generalized Boussinesq Equations. *Phys. Lett. A*, 361 (2007) 223. (SCI)
38. Z. Yan, Hopf Bifurcation in the Lorenz-Type Chaotic System, *Chaos, Solitons and Fractals*, 31 (2007) 1135. (SCI)
39. Z. Yan, Multiple Solution Profiles to the Higher-Dimensional Kadomtsev Petviashvilli Equations via Wronskian Determinant, *Chaos, Solitons and Fractals*, 33 (2007) 951. (SCI)
40. Z. Yan, Globally Exponentical Hyperchaos (Lag) Synchronization in a Family of Modified Hyperchaotic Rossler Systems. *Int. J. Bifurcation and Chaos*, 17 (2007) 1759-1774. (SCI)
41. Z. Yan, Linear Feedback Control, Adaptive Feedback Control and Their Combination for Chaos (Lag) Synchronization of Lc Chaotic Systems, *Chaos, Solitons and Fractals*, 33 (2007) 419. (SCI)
42. H. Li, L. Zhao, Y. Chen, A Symbolic Approach to Polyhedral Scene Analysis by Parametric

Calotte Propagation, *Robotica*, doi: 10.1017/S0263574707003918, 04 Dec. 2007. (SCI)

43. Yingpu Deng, Lifeng Guo; Mulan Liu, Constructions for Anonymous Secret Sharing Schemes Using Combinatorial Designs, *Acta Math. Appl. Sinica*, English Series, 23 (2007), 67--78.
44. Y.G. Xu, Y. Han, Hochschild (Co) Homology of Exterior Algebras, *Comm. Algebra*, 35 (2007), 115-131. (SCI)
45. Y.G. Xu, Y. Han and Wenfeng Jiang, Hochschild Cohomology of Truncated Quiver Algebras, *Science in China*, Ser. A. 50 (2007), 1-10. (SCI)
46. Banghe Li; Zhi Lu, Smooth Free Involution of H \Bbb CP^3 and Smith Conjecture for Imbeddings of S^3 in S^6, *Math. Ann.* 339 (2007), 879--889. (SCI)
47. Banghe Li, Yaqing Li, Guangtian Zhu, Application of Irreducible Decomposition of Polynomials over Algebraic Extension Fields in Cryptography, *Acta Anal. Funct. Appl*. 9 (2007), 18--20.
48. Banghe Li, Tianjun Li, On the Diffeomorphism Groups of Rational and Ruled 4-Manifolds, *J. Math. Kyoto Univ*. 46 (2006), 583--593.
49. Banghe Li, Relating Fourier Hyperfunctions and Extended Fourier Hyperfunction to Hermite Heat Equation. *Acta Anal. Funct. Appl*. 8 (2006), 295--303.
50. Banghe Li, Explicit Relation between the Solutions of the Heat and the Hermite Heat Equation*, Z. Angew. Math. Phys.* 58 (2007)959-968
51. Banghe Li, Tianjun Li, Circle-Sum and Minimal Genus Surfaces in Ruled 4-Manifolds, *Proc. Amer. Math. Soc*. 135 (2007), 3745--3753. (SCI)
52. Zhexian Wan, Kai Zhou, On the Complexity of the Dual Basis of a Type I Optimal Normal Basis, *Finite Fields Appl*. 13 (2007), 411--417. (SCI)
53. Mulan Liu, Liangliang Xiao, Zhifang Zhang, Multiplicative Linear Secret Sharing Scemes Based on Connectivity of Graphs, *IEEE Transactions on Information Theory*, 53 (2007), 3973--3978. (SCI)
54. 刘木兰，肖亮亮，张志芳，一类基于图上随机游动的密钥共享体制，*中国科学* E 辑: 信息科学, 第 37 卷, 第 2 期, 199-208, 2007. (SCI)
55. Yu Shang, Guidong Wang, Xiaoning Wu, Shikun Wang and Yun-Kau Lau, Solitonic Information Transmission in General Relativity, *Commun. Theor. Phys.* (Beijing, China), 2007, No.4, pp. 663-664.
56. Guihua Tian, Shikun Wang and Shuquan Zhong, Stability Problem of Rindler spacetime, *Chinese Physics*, Vol. 16 No. 10, October (2007), pp. 2889-2895.
57. Guihua Tian, Shikun Wang and Shuquan Zhong, Approach to a Cauchy Problem in Stability

study of the Schwarzschild Black Hole, *Chinese Phys. Lett.*, Vol. 24, No. 6 (2007), pp. 1475.

58. 王世坤、张会萍，紧黎曼面上一类线丛截面空间的基，*数学学报*，Vol. N0. 1, Jan, pp. 1-10 (2007）(SCI)
59. Xiangmao Ding，Guidong Wang and Shikun Wang, On Current Superalgebra and Twisted Conformal Field Theory, *Commun. Theor. Phys.* (Beijing, China) 47 (2007), pp. 69-77.

三、会议文集论文

1. Lihong Zhi, Numerical Optimization in Hybrid Symbolic-numeric Computation, In *Proceedings of the 2007 International Workshop on Symbolic-Numeric Computation*, New York, N. Y., 2007. ACM Press, pp. 33-35. (EI)
2. Erich Kaltofen, Zhengfeng Yang and Lihong Zhi, On Probabilistic Analysis of Randomization in Hybrid Symbolic-Numeric Algorithms. In *Proceedings of the 2007 International Workshop on Symbolic-Numeric Computation*, New York, N. Y., 2007. ACM Press, pp. 11-17. (EI)
3. Bin Li, Jiawang Nie and Lihong Zhi, Approximate GCDs of Polynomials and SOS Relaxation. In *Proceedings of the 2007 International Workshop on Symbolic-Numeric Computation*, New York, 2007. ACM Press, pp. 205-206. (EI)
4. Erich Kaltofen, Bin Li, Kartik Sivaramakrishnan, Zhengfeng Yang, and Lihong Zhi, Lower Bounds for Approximate Factorizations via Semidefinite Programming, In *Proceedings of the 2007 International Workshop on Symbolic-Numeric Computation*, New York, N. Y., 2007. ACM Press, Pp. 203-204. (EI)
5. J.S. Cheng, X.S. Gao, and C.K. Yap, Complete Numerical Isolation of Real Zeros in General Triangular Systems, *Proc. ISSAC 2007*, 92-99, ACM Press, New York, 2007. (EI)
6. H. Li, A Recipe for Symbolic Geometric Computing：Long Geometric Product, BREEFS, and Rational Clifford Factorization, *Proc. ISSAC 2007*, 261-268, ACM Press. (EI)
7. Zhuojun Liu and Zuowen Tan, A New Type of Collusion Attacks against Threshold Proxy Signature Schemes. *International Conference on Convergence Information Technology*, Korea, 2007.
8. Ziran Tu, Yingpu Deng, Algebraic Immunity Hierarchy of Boolean Functions. *密码学进展—ChinaCrypt'2007*，中国密码学会 2007 年会论文集, 3－8 (2007).
9. 张志芳，保护隐私的联合求解线性方程组，*密码学进展—Chinacrypt 2007*, 217-224.
10. Xinan Ren, Shikun Wang, A solution of Yang-Mills Equation on BdS Spacetime, *Proc. of IS-CJW*, Ursula Carow-Watamura et al. (eds.) World Scientific, 2007.

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26期“数学机械化研究报告”收录以下论文 (http://www.mmrc.iss.ac.cn/mmpreprints)：

1. He Shi, The special Yang-Mills gauge fields, Vol. 26, 1-18, June, 2007.
2. He Shi, New forms of Yang-Mills gauge fields, Vol. 26, 19-35, June, 2007.
3. He Shi, New types of Yang-Mills gauge fields, Vol. 26, 36-54, June, 2007.
4. Fengjuan Chai, Xiao-Shan Gao and Chunming Yuan, A Characteristic Set Method for Solving Boolean Equations and Applications in Cryptanalysis of Stream Ciphers, Vol. 26, 55-76, February, 2008.
5. Xiao-Shan Gao and Zhenyu Huang, A Characteristic Set Method for Equation Solving in Finite Fields, Vol. 26, 77-92, February, 2008.
6. Jia Li and Xiao-Shan Gao, A Modified van der Waerden Algorithm to Decompose Algebraic Varieties and Zero-dimensional Radical Ideals, Vol. 26, 93-109, February, 2008.
7. Bingyu Li, Zhuojun Liu, Lihong Zhi, Structured Condition Numbers of Sylvester Matrices, Vol. 26, 110-114, February, 2008.
8. Shaoshi Chen, Ruyong Feng, Ziming Li and Huaifu Wang, An Exercise on Real Elementary Functions in the Book "Symbolic Integration I" (second edition), Vol. 26, 115-125, February, 2008.
9. Ruyong Feng and Ziming Li, A Note on Discriminants of Univariate Polynomials, Vol. 26, 126-127, February, 2008.

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
基于几何代数符号计算的几何分解	面上基金项目 2004-2007	李洪波
数值和符号混合计算	青年基金项目 2004-2007	支丽红
复杂非线性波动方程解析解的 数学机械化和图像分析	青年基金项目 2004-2007	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
代数学中的组合方法	国家基金重点项目 2004-2007	万哲先

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

2007 年 11 月 11－13 日，国家重点基础研究发展规划(973)项目“数学机械化方法及其在信息技术中的应用”2007 年学术交流与汇报会在南昌大学召开。国家科技部基础司钱小勇博士、国家科技部基础研究管理中心宋海刚博士参加会议。在听取了项目介绍后，钱小勇博士表示，本 973 项目在中期评估中取得了优异成绩,希望项目承担人员继续能力，争取圆满完成项目任务。项目首席专家高小山研究员介绍了项目的总体执行情况，各个课题组长介绍了课题组 2007 年的研究进展、学术交流情况，部分课题承担人员介绍了自己在 2007 年取得的重要学术进展。

2．项目取得的主要成果

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，在高级不变量的代数理论、微分-差分特征列方法、计算几何、组合算法、*n* 维多项式矩阵的分解、密码分析、模式识别基础理论、语音识别、并联机构在 IC 制造设备关键部件中的应用、基于网格的数学机械化系统研制等方面取得突出成果。2007 年主要成果统计如下：

论文				学术报告		专著	专利	人才培养			软件登记
总数	国际	SCI	EI	特邀	国际			博士后	博士	硕士	
337	244	161	102	22	48	14	13	9	48	98	4

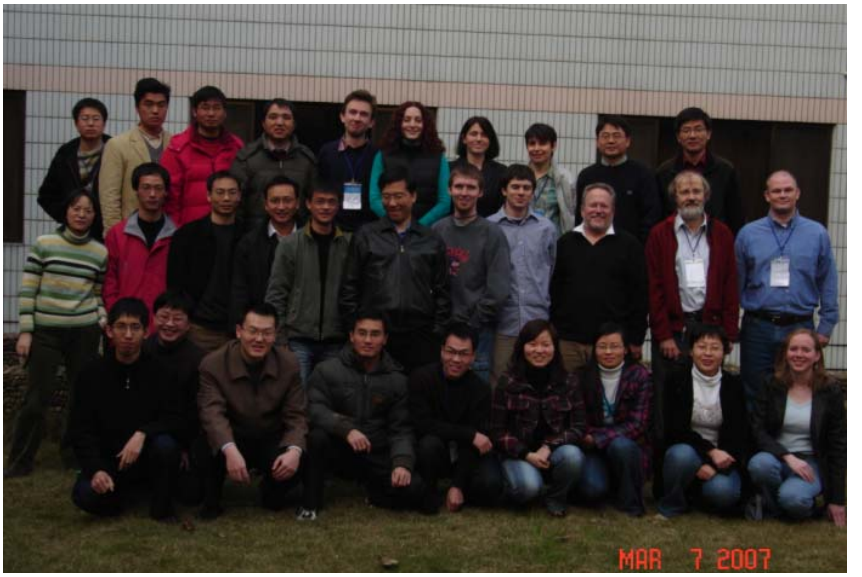
本项目成员获得国际奖励 1 项，为 ACM/SIGSAM ISSAC 2007 杰出论文奖。另外，参加了“第四届国际中文自然语言处理 Bakeoff”评测，获 6 项第一名。

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、密码科技进步一等奖 、陈省身数学奖、上海市自然科学二等奖、北京市科技进步二等奖、教育部“新世纪优秀人才资助计划”；参加项目的研究生获得奖励包括：瑞士科技部们颁发的欧拉数学奖，中科院数学与系统科学研究院院长奖学金特等奖 2 项、宝钢教育基金优秀学生奖特等奖和一项上海市优秀研究生论文等。

一、学术会议

实验室成员组织或参与组织了 6 次学术会议，中心成员出访 22 次，接待国外学者来访 17 次。其中学术会议情况介绍如下：

1、2007 年 3 月 5—9 日，第 2 届中美符号计算联合研讨会在浙江大学举行。该研讨会得到中美双方的自然基金委员会、中科院数学与系统科学院、系统科学研究所等单位的资助。主办单位是中科院数学机械化重点实验室、北京航空航天大学理学院、浙江大学数学系和美国北卡罗莱纳州立大学数学系。共有 39 人参加会议，其中美方 11 人。 研讨会包括 4 个短课程（short courses），15 个学术报告(research presentations) 和小组讨论(group discussions)。中美双方的学者和研究生在几何约束求解、多项式因式分解、混合计算和微分差分方程求解等方面进行了学术交流和探讨，为进一步的合作打下了坚实的基础。



2、2007 年 7 月 5—6 日，“离散联络理论及其应用”研讨会在中国高等科学技术中心举行。该研讨会由中科院数学机械化重点实验室、中科院理论物理所和首都师范大学数学系联合主办，由中国高等科学技术中心承办，共有三十余人参加会议。研讨会的内容包括三个方面：离散联络理论，离散可积系统，和在离散数据的采集、离散模型的建立等方面的应用。实验室的博士生谢正同学在研讨会上做了两场主报告，介绍了他在外差分系统及其在离散力学和差分方程等方面的应用的工作。

3、2007 年 11 月 11－13 日，国家重点基础研究发展规划(973)项目“数学机械化方法及其在信息技术中的应用”2007 年学术交流与汇报会在南昌大学召开。

4、2007 年 11 月 12—13 日，第一届全国计算机数学学术会议在南昌大学国际学术交流中心隆重举行。本次大会由中国数学学会计算机数学专业委员会主办，由中国科学院数学机械化重点实验室与南昌大学承办。这次大会是中国数学学会计算机数学专业委员会被批准成立以来组织的第一次全国性学术活动。与会代表来自于中国科学院、北京大学、清华大学、香港大学、浙江大学、北京航空航天大学、华东师范大学、中山大学、北京邮电大学、吉林大学以及南昌大学等 40 多座高校和科研院所。120 余名从事计算机数学研究的专家学者齐聚一堂，回顾了我国计算机数学所取得的辉煌成就，并对今后面临的任务和发展方向展开了深入的研讨。

5、2007 年 8 月 18—20 日，为庆祝万哲先院士 80 华诞，中国科学院系统科学研究所、中国科学院数学机械化重点实验室、清华大学数学科学系在京联合举办了“代数及相关领域国际会议”。参加会议的有来自世界各地的学者 140 人。这次会议还得到了国家自然科学基金委员会、美国自然科学基金委员会和国际数学联盟等的支持。

6、第 8 届亚洲计算机数学会议(ASCM 2007)于 2007 年 12 月 15-17 日在新加坡举行。本次会议由新加坡国立大学主办，中科院系统科学研究所、中国科学院数学机械化重点实验室协办。会议收到来自 20 个国家的 65 篇投稿。经过程序委员会审查，接受论文 23 篇，短文 13 篇。亚洲计算机数学会议由中国科学院数学机械化中心与日本符号与代数协会于 1995 年创立，已经成为国际计算机数学的重要论坛。实验室高小山、李子明、王定康等人参加了本次会议。

二、参加国际学术会议

1. 冯如勇，参加国际会议“中美符号计算会议”，2007，杭州，作报告"Rational Solutions of Algebraic Difference Equations"。
2. 高小山，共同主持(co-chair)了 ACM SAC-GCR: “Geometric Constraints and Reasoning”分会，2007，韩国。
3. 高小山，参加国际会议“ACM ISSAC2007”, 2007.7, 加拿大，作报告“Complete Numerical Isolation of Real Zeros in General Triangular Systems”。
4. 高小山，参加国际会议“中美符号计算会议”, 2007. 3, 杭州，作报告“Characteristic Set Method for Differential-Difference Polynomial Systems”。
5. 高小山，参加国际会议“ACM Symposium on Applied Computing” , 2007. 3, 韩国。组织了“GCR”分会。
6. 高小山，参加国际会议“MEGA 2007: Method Effective for Algebraic Geometry” , 2007.6, 奥地利，作报告“Characteristic Set Method for Differential-Difference Polynomial Systems”与“Proper Reparametrization of Rational Parametrization of Algebraic Surfaces”。
7. 高小山、李家，参加“ASCM 2007: Asian Symposium on Computer Mathematics”，2007.12，新加坡，作报告“A Modified van der Waerden Algorithm to Decompose Algebraic Varieties as Irreducible Ones”。
8. 高小山、张桂林，参加“ASCM 2007: Asian Symposium on Computer Mathematics”，2007.12，新加坡，作报告“Characteristic Set Method for Partial Difference Polynomial Systems”。
9. 李洪波，参加“International Symposium on Symbolic and Algebraic Computation” 2007.7.29-2007.8.1，加拿大，作报告“A Recipe for Symbolic Geometric Computing: Long Geometric Product, BREEFS and Clifford Factorization”。
10. 李子明，参加“Sino-USA Symbolic Computation Collaboration Workshop”，2007.3，杭州，作报告“Univariate Ore Polynomial Rings in Computer Algebra”。
11. 李子明，参加“International Symposium on Symbolic and Algebraic Computation” 2007.7.29-2007.8.1，加拿大。
12. 李子明，参加“Asian Symposium on Computer Mathematics”(ASCM 2007), 2007.12，新加坡。
13. 刘卓军，参加“2007 International Conference on Convergence Information Technology”, 2007.11.21-23，韩国，作报告“A New Type of Collusion Attacks against Threshold Proxy Signature Schemes”。

14．马玉杰，参加“Workshop on Categorification, Quantization and Clusters”2007.9.10-14，北京，作报告“Characterization of rational indecomposable modules”。

15．王定康，参加“Asian Symposium on Computer Mathematics”(ASCM 2007), 2007.12，新加坡，作报告“An Algorithm for Transforming Regular Chain into Normal Chain”。

16．张志芳，参加 “亚洲密码学 2007 年学术年会－AsiaCrypt 2007 ”，2007.12, 马来西亚。

17．张志芳，参加“International Conference on Algebra and Related Areas”，2007.8，清华大学。

18．支丽红，参加“2007 International Workshop on Symbolic-Numeric Computation”，加拿大，作报告“Numerical Optimization in Hybrid Symbolic-numeric Computation”。

19．支丽红，参加“2007 IMA Thematic Year on Applications of Algebraic Geometry”，明尼苏达大学，美国应用数学研究院。

20．支丽红，参加“NSF CDI Workshop on The Role of Symbolic, Numeric and Algebraic Computation in Cyber-Enabled Discovery and Innovation”，2007.10.30-31，华盛顿，美国，Poster: “Solve Rump’s Model Problem by Semidefinite Programming”。

三、参加国内学术会议

1．邓映蒲，参加“中国密码学 2007 年学术年会－ChinaCrypt 2007”，2007.10，成都，西南交通大学。

2．高小山，参加“全国几何计算与设计学术会议”，2007.8，兰州，作报告“Proper Reparametrization of Rational Parametrization of Algebraic Surfaces”（邀请报告）。

3．李洪波，参加“中国数学会 2007 年会”，2007.11.1-3，北京，作报告“高级不变量代数与符号几何计算”。

4．李洪波，参加“第一届全国计算机数学学术会议”，2007.11.12-15，南昌，作报告“从几何代数到高级不变量理论”。

5．李子明，参加“中国数学会 2007 年会”，2007.11.1-3，北京，作报告“Factoring Linear Functional Systems”。

6．李子明，参加“第一届全国计算机数学学术会议”，2007.11.12-15，南昌。

7．刘卓军，参加“中国密码学 2007 年学术年会－ChinaCrypt 2007”，2007.10，成都西南交通大学。

8．马玉杰，参加“第一届全国计算机数学学术会议”，2007.11.12-15，南昌，作报告“一类侵彻问题的模拟计算”。

9．王定康，参加“中国密码学 2007 年学术年会－ChinaCrypt 2007”，2007.10，成都

西南交通大学。

10．王定康，参加“第一届全国计算机数学学术会议”，2007.11.12-15，南昌，作报告“参数椭圆曲线的 Zeta 函数的计算”。

11．闫振亚，参加“第一届全国计算机数学学术会议”，2007.11.12-15，南昌，作报告“A family of (N+1)-dimensional generalized NLS equations”。

12．袁春明，参加“第一届全国计算机数学学术会议”，2007.11.12-15，南昌，作报告“Characteristic Set Method for Differential-Difference Systems”。

13．张志芳，参加“中国密码学 2007 年学术年会－ChinaCrypt 2007”，2007.10，成都，西南交通大学。

四、实验室成员出访

1．冯如勇，访问国际理论物理中心，意大利，2007年4 -6月。

2．冯如勇，访问北卡州立大学，美国，2007年9 -12月。

3．高小山，访问纽约大学Courant研究所，美国，2007年12月。

4．李子明，访问法国信息与自动化研究所（INRIA），法国，2007年6月。

5．闫振亚，访问ICTP，意大利，2007年9月。

6．支丽红，访问IMA, Minneapolis，美国，2007年1-3月。

7．支丽红，访问NCSU，Raleigh，美国，2007年10月。

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 2007 年的学术报告。

时间	报告人	内容
2007-12-20	Greg Reid University of Western Ontario, Canada	Implicit Differential Bases for PDE - Their Discretizations and Applications
2007-12-13	Prof Wen-xiu Ma University of South Florida, USA	Casorati Solutions of Integrable Equations
2007-11-1	Chu Wenchang, Lecce University, Italy	Liouville's Theorem for Theta Function Identities
2007-10-25	张立先, 燕山大学	五轴数控机床空间刀补问题概要
2007-9-20	Dr. Eckhard Hitzer University of Fukui, Japan	Directional Uncertainty in Clifford Algebra
2007-9-5	Prof. Jing Ping Wang University of Kent, UK	Structure of (2+1)-Dimensional Commutative and Noncommutative Integrable Hierarchies
2007-8-21	吴敏，华东师范大学	Gröbner Bases for Differential and Difference Modules
2007-8-21	Hidetsune Kobayashi Nihon University, Japan	Towards Automatic Reasoning
2007-6-28	Jean-Charles Faugere INRIA, University Paris 6, France	The F5 Algorithm and Applications in Cryptology
2007-6-27	Frederic Chyzak INRIA, Rocquencourt, France	Differential Equations for Algebraic Functions
2007-6-6	Karl Sigmund Austria	Public Goods, Reciprocity and Enforcement
2007-6-4	Ruoming Jin Kent State University, USA	Scalable Data Mining: System and Algorithms

2007-6-4	Paul S. Wang Kent State University, USA	Features and Advantages of WME: a Web-based Mathematics Education System
2007-6-1	Prof. Zhijun Qiao University of Texas - Pan American, USA	Integrable Peaked Soliton Equations
2007-5-28	Eric Schost University of Western Ontario, USA	Solving Toeplitz- and Vandermonde -Like Linear Systems with Large Displacement Rank
2007-5-25	Prof. Eacuteric Schost University of Western Ontario, USA	An Overview of some Complexity Aspects for Computations with Triangular Sets
2007-5-24	Chandrajit Bajaj University of Texas at Austin, USA	Algebraic Splines for Molecular Modeling
2007-5-22	Marc Moreno Maza University of Western Ontario, Canada	Component-level Parallelization of Triangular Decompositions
2007-5-17	Marc Moreno Maza University of Western Ontario, Canada	Comprehensive Triangular Decomposition
2007-4-16	Guilin Wang I2R, Singapore	On the Generic and Efficient Constructions of Secure Designated Confirmer Signatures
2007-4-10	Prof. Miles Reid University of Warwick, UK	Lecture on Mckay Correspondence and Derived Categories (3)
2007-4-6	Prof. Miles Reid University of Warwick, UK	Lecture on Mckay Correspondence and Derived Categories (2)
2007-4-4	Prof. Miles Reid University of Warwick, UK	Lecture on Mckay Correspondence and Derived Categories (1)
2007-3-27	Prof. George Bluman University of British Columbia, Canada	Introduction to Similarity Methods
2007-1-11	Jinzhi Lei，清华大学	Nonlinear Differential Galois Theory

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	每周四下午	李洪波
非交换环理论	每周五下午	李子明
积分与微分模的算法	每周三晚上	李子明
计算代数几何引论	每周一下午	王定康
数值与符号混合计算	每周五下午	支丽红、王定康
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

吴文俊	《Journal of Automated Reasoning》 编委
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	《系统科学与数学》副主编 《Journal of Systems Science and Complexity》副主编 《Journal of Symbolic Computation》 编委 《系统工程与应用》副主编 《中国科学》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 International Journal of Computers 编委 Communications & Control 编委 国际符号与代数年会(ISSAC)指导委员会委员 中国系统工程学会副理事长
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
李子明	ACM SIGSAM, Advisor 《Journal of Symbolic Computation》编委 《Journal of Systems Science and Complexity》编委.
支丽红	《Journal of Symbolic Computation》编委

1. 2008 年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. 2007 年新年刚过，全国人大常委会副委员长、中国科学院院长路甬祥在相关人员的陪同下，来到吴文俊院士家里，与吴院士就数学与现实生活的结合、鼓励青年科学家开拓新的方向、互联网在中国的应用进展与科学需求等问题，进行了深切的交谈。

3. 2007 年 2 月 8 日，国家科技部李学勇副部长向吴文俊致以新春问候，并询问了他的生活和研究工作情况。李学勇副部长还与吴文俊就我们国家的基础研究等问题进行了愉快的交谈。李学勇副部长对吴文俊院士获得“劭逸夫数学科学奖”表示祝贺。吴文俊院士表示，数学机械化研究长期得到科技部的支持，有一个稳定的环境，才得以有今

天的成果与研究队伍。吴文俊院士还表示，希望数学机械化方法可以得到应用，为国家的发展做出贡献。

4．2007 年 10 月 30 日下午，数学与系统科学研究院第六届“思源纵横，大师讲坛”活动在思源楼一层报告厅隆重举行。此次活动邀请的主讲人为吴文俊院士, 报告会由数学与系统科学研究院院长郭雷院士主持。报告会上，吴文俊院士从消去法的历史谈起，深入浅出地介绍了消去法和代数几何的几个重要问题，特别提到消去法的思想起源于我国，并鼓励青年学子们努力工作，积极探索，把我国的数学事业发扬光大。主持人郭雷院长随后为吴先生的报告总结了三个特点：思维敏捷、深入浅出、富有洞察力，并号召同学们以吴文俊院士为榜样，为我国数学事业的发展努力奋斗。

5．2007 年 6 月 5 日下午，吴文俊院士应邀参加中国科技大学 50 周年校庆第二次新闻发

布会，并在该校学术报告厅作了名为《中国传统数学的实质》的报告。

6. 清华大学数学科学系、中科院系统所、中科院数学机械化重点实验室于 2007 年 8 月 18-20 日在京联合主办了代数及相关领域国际会议。8 月 19 日举行了庆祝万哲先院士 80 华诞的晚宴。许多单位派来了代表或发来贺信、贺电，敬送花篮。人大常委会副委员长、中国科学院院长路甬祥发来了热情洋溢的贺信。丘成桐先生的条幅“万岁始于八十，哲思堪比先贤”（王元院士书写）格外引人注目。研究院院长郭雷院士、清华大学冯克勤教授、中国数学会理事长文兰院士分别致词。杨乐院士、黄敦教授、吴佑寿院士和李邦河院士在晚宴上讲了话。

7. 2007 年 11 月 12—13 日，第一届全国计算机数学学术会议在南昌大学前湖校区国际学术交流中心隆重举行。李邦河院士在开幕式上发表了热情洋溢的讲话，并应邀作了两小时的“华罗庚讲座”报告，题为《在四维流形中的曲面》。

8. 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。

庆祝万哲先院士 80 华诞