中国科学院数学与系统科学研究院

数学机械化重点实验室

(http://www.mmrc.iss.ac.cn)

年 报

2003
Annual Report

Key Laboratory of Mathematics Mechanization,

Academy of Mathematics and Systems Sciences,

Chinese Academy of Sciences

目 录

前 言

数学机械化重点实验室于 2002 年底由中国科学院批准成立，成员主要来自数学与系统科学研究院数学机械化中心、信息安全中心以及国家“973”项目“数学机械化与自动推理平台” 在研究院工作的项目承担人，实验室正式成员 16 人。

本年报总结了实验室 2003 年度在科研、学术交流、人才培养、课题争取等方面的工作。实验室成员本年度在几何自动作图、齐性模型、混合运算、微分方程求解，与数学机械化软件开发等方面取得重要进展，共出版专著 4 部，发表杂志论文 41 篇、会议集论文 16 篇，其中 SCI 论文 35 篇。值得指出的是 2003 年国内研究人员在 JSC 上共发表论文 7 篇，其中 5 篇出自实验室成员。另外，根据《2003 年度中国科技论文统计结果》，实验室成员闫振亚在 2003 年数学类 SCI 收录论文并列全国第一。

由实验室主持的“973”项目“数学机械化与自动推理平台” 经过五年执行于 2003 年 12 月 9 日进行了结题验收。通过本项目的执行，数学机械化在理论研究、应用研究与软件平台开发都取得了实质性突破。在项目的支持下，吴文俊院士于 2000 年荣获首届 “国家最高科技奖”；石青云院士等提出的“多成份变换”技术被图像压缩国际标准 JPEG2000 采纳；开发了具有自主产权的智能自动推理平台，得到国际学术界高度评价；并联机构研究成果已经在我国亟待解决的大型数控机床与大规模集成电路制造方面发挥重要作用。在人才培养方面也取得突出成绩。项目执行期间共有七人获得国家杰出青年基金，两人获得教育部长江学者称号，两人进入科学院百人工程。这些成果的取得充分显示了数学机械化思想的优越性。

一个实验室的成功归根结底要看我们能否取得重要的科研成果。在这方面，实验室的吴文俊、万哲先、李邦河院士为我们青年科研人员树立了榜样。让我们共同努力，将数学机械化重点实验室办成出成果、出人才的国际知名研究机构。

• 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，吴新文

成　员：　　吴文俊，万哲先，李邦河，高小山，石　赫，李洪波，吴新文，刘木兰，刘卓军，吴　可，王世坤，费少明，杜　宏，李子明，王定康，支丽红，马玉杰，闫振亚

兼职教授：　　Shang-Ching Chou, Paul S. Wang, 吴文达，王东明

秘　书：　　周代珍

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，杨　路，刘木兰，吴　可，冯克勤，张继平，陈永川，李克正，高小山

实验室网站：http://www.mmrc.iss.ac.cn

电话：10－62541834

传真：10－62630706

实验室所属机构：

数学机械化研究中心

主任：　　高小山

副主任：　　李洪波，李子明

信息安全研究中心

主任：　　刘木兰

副主任：　　吴新文

● 主要科研工作简介·

1、数学机械化自动推理平台 MMP 开发

首次从底层开始，完整与高效地实现了数学机械化方法，开发了有自主产权的、不依赖其他软件系统的数学机械化自动推理平台 MMP，并形成了系列应用模块，实现了若干数学问题与高科技问题的自动求解。MMP 的支撑系统部分包括编程语言，图形界面；MMP 的基本运算部分任意精度的数系统，多项式运算，符号线性代数；MMP 的核心部分包括多项式系统，常微分系统，偏微分系统的吴方法；MMP 的应用模块包括几何自动推理模块，非线性微分方程孤波解的自动求解模块，组合恒等式自动证明模块，过渡曲面自动生成模块，6R 机器人模拟模块，四连杆机构的综合模块。

MMP 的创新性在于软件的开发与理论研究紧密结合，以我国自行开创的数学机械化方法为基础，研制具有其他同类软件所不具有的自动推理功能，预计将为我国科研、工程中的脑力劳动提供有力工具。主要特点如下（1）首次完整与高效地实现了数学机械化方法，得到有自主产权的、不依赖其他系统的数学机械化软件。（2）几何推理应用模块 MMP/Geometer 实现了几何定理的自动证明、发现与几何图形的自动生成，在国际同类软件中处于领先地位，被法国专家 Caferra 称为 “重要与具有代表性”的几何推理系统 ,被巴西学者 Bortolossi 称为 “一个杰作(masterpiece),代表了几何定理证明器的当前水平”，获第四届亚洲数学技术大会 “最佳论文”奖.（3）实根判定、微分方程求解、组合恒等式证明、自动生成过渡曲面、机器人模拟、四连杆综合与模拟模块等，将吴文俊几何定理机器证明的成果推广至数学的其他领域与若干高科技领域。（4）MMP 已在 CAGD、计算机视觉、CAD、机器人、控制、振动工程、生物动力学、孤立子、机构学、电力系统、微分动力系统等方面得到应用。

2、几何自动作图的方法与应用

在几何自动作图方面提出了 C-树分解方法可以将任意几何作图问题分解为某类极小的作图问题。这一方法的复杂度为顶点个数的四次多项式。通过 C－树分解，一般的几何作图问题可以归结为三种基本模式：显示构造、广义 Stewart 平台、复杂构型。其中 Stewart 平台是应用最广泛的并联机构，是过去 20 年并联机构研究的焦点。我们从自动推理角度出发提出了广义 Stewart 平台的观念，给出了在一定意义下所有一般并联机构的，给出了实现方法与平台的正解数目。我们还给出了所有 2D 广义 Stewart 平台的解析解与一类由三个距离与三个角度决定的 3D 广义 Stewart 平台的解析解与最佳实解个数。这一工作具有很大的发展前途，可能会产生重要影响。将几何自动作图方法用于以下问题的研究：

- P3P 问题的研究。该问题是计算机视觉基本问题之一,在机器人、计算机动画、视觉校准中有重要应用。**P3P** 解的分类是一个长期未解决的公开问题。我们给出了其解的个数的完全分类与完整解析解，彻底解决了这一公开问题，并以此为基础发展了求解 P3P 问题的高效完整算法。有关论文被机器智能与视觉方面权威的 IEEE T. PAMI 发表为“regular paper”。又证明了 P4P 问题具有唯一解的概率为一。有关论文已投 IEEE T. PAMI。

3、基于 Clifford 括号代数的几何计算方法

基于齐性模型和 Clifford 括号代数的二维欧氏几何计算, 继续产生新的分解技术,能够得到结论由条件表示的完全分解形式, 其意义已超出机器证明本身. 基于 Cayley 代数方程组求解和几何分解的三维射影重建, 得到的无分叉参数化中的参数个数最少, 而且能够通过几何推理得到线形构造序列.

4、偏微分方程的分解与求解

在微分代数的研究方面，我们给出了第一个分解偏微分模的算法，该方法是目前国际上唯一的分解偏微分模的完整算法; 以及第一个计算解空间为有限维的齐次线性偏微分方程组的所有超指数函数解的算法， 该方法也是目前国际上唯一的计算全部超指数函数解的方法。并且建立了 Ore 多项式子结式理论和无分式(fraction-free)算法的基础。子结式算法已在 Maple 的商用软件包 OreTools 中实现。其中一个已经包括在商用计算机代数软件 Maple 8 和 Maple 9 中，Maple 的商用软件包中实现的由国内研究人员设计的算法并不多见的; 该软件包包括了目前效率最高的处理 Ore 多项式的方法。 其中包括我们设计的计算最大右公因子（GCRD）的 Modular 算法， 计算最小左公倍式(LCLM)的线性方程法以及子结式算法。有关工作在 M. van der Put 和 M. Singer 在其新书 (Springer 2003)：Galois theory of Linear Differential Equations，(page 417)中引用。

5、GCD 近似求解

应用结构矩阵和正交分解求解近似 GCD, 将线性代数的最新成果 displacement 结构运用于混合计算, 将计算复杂度从 3 次降为 2 次, 并且证明了快速算法仍然是稳定的, 从而使近似 GCD 算法不仅在实际计算而且在理论上都较以往有了很大的进步. 我们的研究第一次指出了多项式的近似公共根在单位圆附近的特殊分布是导致很多已知算法失败的主要原因, 而利用正交分解中出现的低次多项式关于单位圆的分解将帮助我们解决近似 GCD 的稳定求解问题. 我们的算法可以稳定快速求解次数达到 2000 的近似多项式 GCD. 算法也已经包括在商用计算机代数软件 Maple 9 中。关于近似多项式方程组的稳定求解的工作已被成功地应用于完全求解计算机视觉中的重要问题--相机定位. 特别地, 首次解决了奇异构形邻域内的定位问题.

6、非线性微分方程的求解与变换

提出了一个研究微分方程的非古典势对称的途径，开辟了一个研究方程对称的广义区域，并将该思想用于非线性热传导方程，获得了新的对称和精确解。利用 Weistrass 椭圆函数，发展了一种广义的算法，用于获得非线性微分方程的更多类型的双周期解，利用该算法得到了一些非线性微分方程（组）的新的双周期解。基于 Backlund 变换和一些广义的非行波变换，研究了一些高维非线性微分方程的非行波解，其中包含有任意的解析函数，因此具有丰富的结构，对于解释一些物理现象是有意义的。对于非线性微分方程对应的双线性方程，给出了一个获得 Wrongskian 行列式的解的具体算法步骤，并验证了该算法的有效性。

根据《2003 年度中国科技论文统计结果》闫振亚在 2003 年数学类 SCI 收录论文全国并列第一。

7、参数多项式方程组的解的个数

提出一种新的正则升列的概念，给出一种基于特征列方法的多项系统的正则零点分解的新算法。提出一种计算带有参数的多项式方程组的解的个数的算法，可以计算参数多项式方程组解的最多个数和方程组有各种个数解时参数需要满足的条件。给出计算拟代数簇的投影算法。

8、微分曲线的亏格

研究了如何将代数几何方法应用于代数微分方程的研究的问题，首次给出了微分方程的亏格的定义，并研究了低亏格情形的代数微分方程的解空间的性质及其自同构群等，得到了关于一阶微分方程的一些新结果，对尚处于雏形阶段的微分代数几何的研究有较大的意义。

9、码的重量谱

一般 k 维 q 元线性码重量谱的确定问题是一个难题。至今仅确定了链、几乎链、近链这三类线性码的几手所有重量谱。今年我们进一步用有限射影几何方法，克服了情况数目极多的困难，选择合适的子空间集，确定了一大类称为断链码的几乎所有重量谱。

● 完成和发表论著和论文目录•

一、 著作与文集：

1．万哲先, Lectures on Finite Fields and Galois Rings, World Scientific, Singapore, 2003.
2．万哲先, Advances in Algebra, (ed. with K. P. Shum and J. P. Zhang), World Scientific,Singapore,2003.
3．王东明, 杨路, 支丽红等, 《符号计算选讲》, 清华大学出版社, 2003.
4．李子明，Computer Mathematics, World Scientific, Singapore, 2003.(with W. Sit (eds)
5．吴文俊，《数学机械化》，科学出版社，2003.
6．胡作玄、石赫, 《吴文俊之路》,上海科学技术出版社，2003.

二、 期刊论文

1. 支丽红， Hybrid method for computing the nearest singular polynomials, **The Japan Journal of Industrial and Applied Mathematics** (to appear 2004) (with M. Noda, H. Kai, W. Wu).
2. 支丽红，QR factoring to compute the GCD of univariate approximate polynomials, **IEEE Trans. on Signal Processing.** (to appear 2004) (with Rob.Corless, Stephen Watt).
3. 马玉杰，The coexponent of a finite p-group, **Comm. Alg.** (2003), 31(7), 3497-3504. (with H. Bai and J. P. Zhang)
4. 李子明， Factoring Linear Partial Differential Systems with Finite-dimensional Solution Spaces. **Journal of Symbolic Computation,** Vol 36 (2003), 443 –471.（with Fritz Schwarz and Serguei Tsarev）
5. 李洪波，(2003). Clifford algebra, geometric computing and reasoning. ***Chinese Adv. in Math*.** 32(4): 405-415.
6. 李洪波， Automated Theorem Proving in Projective Geometry with Cayley and Bracket Algebras I. Incidence Geometry. **J. of Symbolic Computation** 36(5): 717-762.(with Yihong Wu (2003).)
7. 李洪波， Automated Theorem Proving in Projective Geometry with Cayley and Bracket Algebras II. Conic Geometry. **J. of Symbolic Computation** 36(5): 763-809.(with Yihong Wu (2003).)
8. 刘木兰， Recommenal Underlying Fields of Elliptic Curve Cryptosystems, **J. of Systems Science and information** vol.1, No.4, 639-641. (with J. Li)
9. 刘木兰， Regular points in system spaces, **Linear Algebra and Applications** 365 (2003), 201-213.
10. 刘卓军，The Membership Problem of Binormal Skew Polynomial Ring,

Communications in Algebra, Vol. 31, Issue 1, 2003. （with Liu, J. W. and Wang, M. S.）

11. 刘卓军， The Term Orderings Which Are Compatible with Composition(II), **Journal of Symbolic Computation**, Vol. 35, Issue 2, 2003.（with Liu, J. W. and Wang, M. S.）
12. 刘胜强， Necessary-sufficient conditions for permanence and extinction in Lotka-Volterra system with distribute delays, ***Applied Mathematics & Letters,*** 16 (2003): 911-917.（with Lansun Chen）
13. 闫 振 亚， New families of non-travelling wave solutions to a new (3+1)-dimensional potential-YTSF equation, ***Phys. Lett. A,*** 318（2003）78.
14. 闫振亚，Jacobi elliptic function solutions of nonlinear wave equations via the new sinh-Gordon equation expansion method, ***J. Phys. A: Math. Gen***., 36(2003) 1961.
15. 闫振亚， Painleve analysis, auto-Backlund transformations and exact solutions for a simplified model for reacting mixtures, ***Physica A***, 326(2003) 344.
16. 闫振亚，The new extended Jacobian elliptic function expansion algorithm and its applications in nonlinear mathematical physics equations, ***Comput. Phys. Commun.***, 153(2003) 154.
17. 闫振亚，Modified nonlinearly dispersive mK(m,n,k) equations: II. Jacobi elliptic function solutions, ***Comput. Phys. Commun.***, 153(2003) 1.
18. 闫振亚，Modified nonlinearly dispersive mK(m,n,k) equations: I. new compacton solutions and solitary pattern solutions, ***Comput. Phys. Commun***., 152 (2003) 25.
19. 闫振亚，The Riccati equation with variable coefficients expansion algorithm to find more exact solutions of nonlinear differential equations, ***Comput. Phys. Commun***., 152 (2003) 1.
20. 闫振亚，New families of exact solitary patterns solutions for the nonlinearly dispersive R(m, n) equations, ***Chaos, Solitons & Fractals,*** 15(2003) 891 .
21. 闫振亚，Generalized method and its application in the higher-order nonlinear Schrodinger equation in nolinear optical fibres, ***Chaos, Solitons & Fractals***, 16(2003) 759.
22. 闫振亚，Constructing exact solutions for two-dimensional nonlinear dispersion Boussinesq equation. II: Solitary pattern solutions, ***Chaos, Solitons & Fractals***, 18（2003）869.
23. 闫振亚，A sinh-Gordon equation expansion method to construct doubly periodic solutions for nonlinear differential equations, ***Chaos, Solitons & Fractals***, 16 （2003）291.
24. 闫振亚，Two types of hierarchies of evolution equations associated with the extended Kaup-Newell spectral problem with an arbitrary smooth function,

Chaos, Solitons & Fractals, 15（2003）639.

25. 杜宏，Automorphism group of Lie algebra C(t) d/dt. *J. Syst. Sci. Complex.* **16** (2003), no. 2, 209-212.
26. 吴可， Canonical form and seperability of PPT states in $C^2\times C^M\times C^N$ composite quantum systems, **Inter. J. of Quantum Information, 1 No.3** (2003), 1-11. （with X. H. Wang, S. M. Fei, Z. X. Wang ）
27. 吴可， General volume –preserving mechanical systems, **Lett. Math. Phys. 64** (2003), 235-243. （with B.Zhou, H.Y. Guo）
28. 吴可， General volume –preserving mechanical systems via cohomology, **Commun. Theor. Phys. 40** (2003), 595-600.（with B.Zhou, H.Y. Guo）
29. 吴可,Canonical form and seperability of PPT states in $C^2\times C^2\times C^2\times C^N$ composite quantum systems, **Commun. Theor. Phys., 40** (2003), 515-518. （with S. M. Fei, X.H. Gao, X. H. Wang and Z. X. Wang）
30. 吴可，Seperability of rank two quantum states on multiple quantum spaces with different dimensions, **Inter. J. of Quantum Information,** No.1 (2003), 37-49. (S. M. Fei, X.H. Gao, X. H. Wang, Z.X. Wang)
31. 吴可**,** Separability of rank-two quantum states in $C^M\times C^N$ composite quantum systems, **Commun. Theor. Phys., 39** (2003) , 525-528.（with S.M. Fei, X.H. Gao, X.H. Wang, Z.X. Wang ）
32. 吴可， Total variation in Hamiltonian formalism and symplectic-energy integrators, **J. Math. Phys., 44** (2003), 1688-1702. （withJ. B. Chen, H. Y.Guo）
33. 吴新文 Lee-metric decoding of BCH and Reed-Solomon codes, ***Electronics Letter***, vol. 39, no. 21, pp.1522-1525, 2003. (with M. Kuijper, P. Udaya)
34. 杜宏，A Geometric Approach to dimS^1_2(Delta_MS). **AMS/IP Studies in Advanced Mathematics**, Volume 34, 2003, 67-70.
35. 高小山， Involutive Characteristic Set of Partial Differential Polynomial Systems, **Science in China (A),** 33(2), 97-113, 2003. （withY. Chen）
36. 高小山，Cheng, Complete Solution Classification for the Perspective-Three-Point Problem, **IEEE Trans. PAMI,** 930-943, 25(8), 2003. （with X. R. Hou, J. Tang and H.）
37. 高小山， Solving spatial basic geometric constraint configurations with locus intersection, **Computer Aided Design**, 111-122, 36(2), 2003. （with C.M. Hoffmann and W. Yang）
38. 高小山，Implicitization for Differential Rational Parametric Equations, **Journal of Symbolic Computation**, 811-824, 36(5), 2003.
39. 高小山，Geometric Constraint Solving and Simulation of Complex Linkages, (in Chinese), **J. of CAD&CG,** 517-522, 15(5), 2003.（with G. Zhang and W. Yang）
40. 李邦河, Smooth minimal genera for small negative classes, **Topology Appl.** 132

(2003), 1-15.

41. 李邦河, A method to solve algebraic equations up to multiplicities via Ritt-Wu's characteristic sets, **Acta Anal. Func. Appl.** 5(2003), 97-109.
42. 蒋鲲，朱长才，高小山。参数化 CAD 模型中参数的有效范围。**计算机辅助设计与图形学学报**， 2003， 15(8), 1016-1020。
43. 蒋鲲，高小山，岳晶岩。参数化模型欠、过和完整约束的判定算法。**软件学报**, 2003, 14(12), 2100-2105。

三、发表在会议文集上的论文：

1. 万哲先，On the Hensel lift of a polynomial, Differential Geometry and Related Topice, Proceedings of the International Conference on Modern Mathematics and the International Symposium on Differential Geometry in Honor of Professor Su Buchin on the Centenary of His Birth, Sept.19-23, 2001,ed. By Gu Chaohao et al., World Scientific, Singapore, 2002, 250-256.
2. 万哲先，Moor-Penrose generalized inverses of matrices over division rings with involutions, Advances in Algebra, Proceedings of the ICM Satellite Conference in Algebra and Related Topics, ed. by K. P. Shum et al., World Scientific, Singapore, 2003, 244-250.
3. 王世坤， A Hadamard Theorem on Algebraic Curves，Proceeding of International Conference of geometric function in several complex variables，World Scientific Press，2003。（with Hui-Ping Zhang）
4. 支丽红， Determination of approximate symmetries of differential equations. Workshop on Group Theory and Numerical Analysis, Montreal, AMS, Canada, 2003。(with G.Reid, F..Lemair, J. Bonasia)
5. 支丽红， A complete symbolic-numeric linear method for camera pose determination, In: Proc. of the 2003 International Symposium on Symbolic and Algebraic Computation, Scotland, ACM Press, 215-223, 2003.（with G. Reid, J.Tang）
6. 支丽红，Displacement structure in computing the approximate GCD of univariate polynomials, In: Computer Mathematics III, Z. Li and W. Sit (eds), 288-298, 2003.
7. 李洪波， A bracket method for judging the intersection of convex bodies. In: *Computer Mathematics*, Z. Li and W. Sit (eds), World Scientific, pp. 227-239. (with Ying Chen (2003).)
8. 李洪波，(2003). Clifford Algebras and Homogeneous Geometric Models. In: *Some Problems on the Protein Structure Analysis.* CCAST-WL Workshop Series 147, H. Guan et al (eds), Beijing, pp. 91-121.

9. 刘卓军， Zero-knowledge proof system vs asymmetric cryptosystem, symmetric cryptosystem, First MiAn International Conference on Applied Cryptography and Network Security, Kunming, China, October 2003. （with Tang, C .M., Wang, M. S.,
10. 吴新文， "A Lee-metric decoding algorithm for Reed-Solomon codes over GF(p)," *Proceedings of the 7th International Symposium on Digital Signal Processing and Communication Systems*, Cold Coast, Australia, December, 2003. （with M. Kuijper, P. Udaya）
11. 高小山， Classification and Solving of Merge Patterns in Geometric Constraint Solving, in Proc. Shape Modeling and Applications, 2003, 89-90, Seoul Korea, IEEE press, 2003.（with G. Zhang）
12. 高小山， Geometric Constraint Solving via C-tree Decomposition, ACM SM03, 45-55, Seattle, USA, ACM Press, New York, 2003.（with G. Zhang）
13. 高小山， Zero Decomposition Tree for Counting the Number of Solutions for Algebraic Parametric Equation Systems, in Computer Mathematics III, Z. Li and W. Sit (eds), 130-145, World Scientific, Singapore, 2003. （with D.K. Wang）
14. 高小山， Geometric Constraint Solving with DM-decomposition, Proc. 8th International Conference on CAD/Graphics, Enhua Wu, Hanqiu Sun, Dongxu Qi(eds.), Welfare Printing Limited (Macau), 2003, 240-250.（with K. Jiang and Jing-Yan Yue.）
15. 刘卓军, 对小额电子支付方案的改进,中国计算机大会, 北京, 2003. （合作者：唐春明）
16. 刘卓军，基于面向对象技术的无穷精度数系统的研制与开发，中国计算机大会 2003。（合作者：杨宏，林东岱）
17. 刘木兰.线性多密钥共享体制， 中国计算机学会信息保密专业委员会论文集，第十三卷，303-317，2003.10. (合作者：肖亮亮)

四、第 22 期研究报告论文：

研究报告是数学机械化中心自 1986 年开始编印研究论文的预印本，刊载数学机械化方向的最新研究成果，在国内外进行交流中发挥了重要作用。论文请见网站：http://www.mmrc.iss.ac.cn/pub/mm-pre.html

下面列出 MM Research Preprints No 22, 2003 年论文目录。

1. WuWen-tsun, On Algebrico-Differential Equations-Solving
2. Cheng Jin-San and Gao Xiao-Shan , Constructing Blending Surfaces for Two rbitrary Surfaces
3. Feng Ru-Yong and Gao Xiao-Shan, Polynomial General Solution for First Order ODEs with Constant Coeffcients

4. Feng Ru-Yong and Gao Xiao-Shan, Rational General Solutions of Ordinary Differential Equations
5. Gao Xiao-Shan, Lei De-Li, Liao Qizheng and Zhang Gui-Fang, Generalized Stewart Platforms and their Direct Kinematics
6. Gao Xiao-Shan and Li Ming, Rational Quadratic Approximation to Real Plane Algebraic Curves
7. Gao Xiao-Shan and Li Ming , A Dynamic Solid Modelling Tool based on Symbolic Interpolant for Scattered Data with Normal Vectors
8. Gao Xiao-Shan and Tang Jian-Liang , On the Probability of the Number of Solutions for the Perspective *n* Point Problem
9. Gao Xiao-Shan and Zhang Gui-Fang , Geometric Constraint Solving Based on Connectivity of Graph
10. Gao Xiao-Shan and Zhang Ming-Bo ,Decomposition of Di®erential Polynomials
11. Lei De-Li and Du Hong, On a Problem of Steinhaus
12. Li Hong-Bo and Zhao Li-Na , A Symbolic Approach to Polyhedral Scene Analysis by Parametric Calotte Propagation
13. Tang Chun-Ming, Liu Zhuo-Jun and Wang Ming-Sheng , An improved identity-based ring signature scheme from bilinear pairings
14. Tang Chun-Ming, Liu Zhuo-Jun and Wang Ming-Sheng , Improved Tseng-Jan's group signature schemes
15. Tang Chun-Ming, Liu Zhuo-Jun and Wang Ming-Sheng, Proving in Zero-Knowledge that a Committed Integer $a \bullet 0$ or $a\ a \bullet 0$ (*mod N*)
16. Tan Zuo-Wen, Liu Zhuo-Jun, A Novel Identity-based Group Signature Scheme from Bilinear Maps
17. Wang Bao-Shan , Modular Representations of Direct Products
18. Yan Zhen-Ya, An improved algebra method and its applications in nonlinear wave equations
19. Yan Zhen-Ya , The Riccati equation with variable coeffcients expansion algorithm to ¯nd more exact solutions of nonlinear differential equations
20. Yan Zhen-Ya , Symbolic Computation and New Soliton-Like Solutions of the 1+2D Calogero-Bogoyavlenskii-Schif Equation
21. Yan Zhen-Ya, Painleve analysis and similarity solutions to the (2+1)-dimensional nonlinear volution equation
22. Yan Zhen-Ya , Integrability for two types of (2+1)-dimensional generalized Sharma-Tasso-Olver integro-differential equations
23. Yan Zhen-Ya , Modified nonlinearly dispersive *mK*(*m; n; k*) equations:II. Jacobi elliptic function solutions
24. Yan Zhen-Ya , Optical solitary wave solutions to nonlinear Schrodinger equation

with cubic-quintic nonlinearity in non-Kerr media
25. Yan Zhen-Ya , Painleve analysis, auto-Backlund transformations and exact solutions for a simplified model for reacting mixtures
26. Yan Zhen-Ya , Jacobi elliptic function solutions of nonlinear wave equations via the new sinh-Gordon equation expansion method
27. Yan Zhen-Ya, New families of non-travelling wave solutions to a new (3+1)-dimensional potential-YTSF equation
28. Yan Zhen-Ya , The Weierstrass elliptic function expansion method and its applications in nonlinear wave equations
29. Yuan He-Jun , Entropy of Partitions on Quantum Logic and its Applications

● **科研项目·**

项目名称	类别	负责人
数学机械化与自动推理平台	973 项目	高小山
构造性微分代数几何	973 项目子课题	石赫、吴可
全局优化与方程求解	973 项目子课题	李洪波
自动推理平台开发	973 项目子课题	王定康
流形与复形的拓扑学	973 项目子课题	李邦河
数学机械化	国家最高奖奖励基金	吴文俊
几何自动作图与智能 CAD	杰出青年基金配套“百人计划”课题	高小山
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
电子支付系统研究	国家基金项目	刘木兰
“十五”国家密码发展	省部委项目	刘木兰
数学机械化与自动推理平台	中科院创新基金	高小山，李洪波
数学机械化	所长创新基金	李洪波
复杂系统理论与应用研究	中科院知识创新工程重要方向项目	高小山
拟线性双曲型方程组的理论和代数几何研究	所长创新基金	万哲先
代数几何码的构造和高速译码及其应用	国家基金	吴新文
求解方程	横向	高小山

“九七三”项目: “数学机械化与自动推理平台”执行情况

1、课题验收

根据科技部关于 1998 年立项 973 项目结题验收的通知，“数学机械化与自动推理平台”项目于2003年10月10、11日在北京举行“课题验收及学术报告会”。项目的咨询专家袁宗保，何新贵先生，科技部的韩苍穹，中科院基础据的金铎、齐禾、王永祥出席了会议，项目对五年来的工作予以总结。

各课题组长对所承担课题五年来的执行情况作了 30 分钟的总结报告，每个课题组有 3 名学术骨干做了专题报告。在报告中介绍了过去五年来取得的主要进展，并就提出的问题展开了热烈的讨论。

由项目专家、咨询专家与依托单位管理专家组成的验收专家组对各个课题的执行情况进行了认真审查。认为了各个课题圆满完成了计划任务，并取得重要进展。并结合答辩情况给各小组的评分。项目八个课题平均得分 93。

2、项目验收

1998 年首批立项的国家基础研究发展规划项目“数学机械化与自动推理平台”于 2003 年 12 月 9 日进行结题验收。项目首席科学家高小山做了总结报告，李志斌、杨路、封举富、王定康介绍了本项目四项有代表性的科研成果，项目学术指导吴文俊院士做了即席讲话。

自 1998 年启动以来，本项目执行顺利，在有关部门的指导与帮助下，积极开展学术交流、协同攻关，经过全体项目承担人的共同努力，圆满地完成了工作计划。

数学机械化研究是我国学者开创的一个基础研究领域，是中国古代数学思想在信息时代的复兴。数学机械化研究在国际上产生了重要影响。本项目在数学机械化的理论研究、数学机械化方法在相关高科技领域的应用基础研究、以及自动推理平台开发方面都取得实质性进展。

本项目的标志性成果包括：吴文俊院士于 2000 年荣获首届“国家最高科技奖”，数学机械化研究获得科学界的高度评价。石青云院士等提出的“多成份变换”技术被图像压缩国际标准 JPEG2000 采纳,标志着我们在国际竞争中有了一席之地。成功开发了具有自主产权的智能自动推理平台，形成系列应用模块，得到国际学术界高度评价。并联机构研究成果已经开始在我国亟待解决的大型数控机床与大规模集成电路制造方面发挥重要作用。

在数学机械化理论方面，这一项目在微分方程求解、全局优化、不等式机器证明、几何自动作图、几何代数算法、混合算法、组合算法、逻辑推理和搜索算法方面取得一系列原创性成果，发表了大量高水平论文,获得奖励 36 项。

在数学机械化方法的高技术应用方面，我们解决了静态与视频图像压缩、图像重建、纠错码、复杂曲面造型、信息隐藏、基于并联机构的数控技术等方面的关键理论问题。并联机构研究成果已经开始在我国亟待解决的大型数控机床与大规模集成电路制造方面发挥重要作用。申请了 28 项发明专利，包括 2 项美国专利。

在软件开发方面，以我们自己发展的方法为基础，完成了“数学机械化自动推理平台”MMP 的开发、并形成系列应用模块。这一软件具有自主知识产权与一定的智能性，预计将为我国科研、工程中的脑力劳动提供有力工具。

本项目在人才培养方面也取得突出成绩。项目执行期间共有七人获得国家杰出青年基金，两人获得教育部长江学者称号，两人进入科学院百人工程。

通过项目的实施，推进了数学机械化理论研究，解决了若干我国迫切需要发展的信息和相关高科技领域的若干关键基础理论问题，成功开发了具有自主知识产权与一定智能性的数学机械化自动推理平台。这些成果的取得充分显示了数学机械化思想的优越性。另一方面，根据吴文俊院士提出的“数学机械化纲领”，数学机械化研究还处于初始阶段，具有广阔的发展空间与应用前景。

• 学术交流•

举办的学术会议

1. 由数学机械化研究中心主办的“第六届亚洲计算机数学会议”(ASCM'2003)于2003 年 10.23-25 在北京召开。会议主席由吴文俊院士担任；程序委员会主席由美国纽约城市大学的 William Y. Sit 教授和中国科学院数学与系统科学研究院李子明副研究员担任。有来自中国，美国，加拿大，法国，日本，泰国，韩国，新加坡，西班牙，台湾等约十个国家与地区的约 110 名有关计算机数学方面的专家学者参加了这次大会。美国新墨西哥大学的 Deepak Kapur 教授和日本神户大学的 Nobuki Takayam 教授分别作了题为“Multivariate Resultants based on Cayley- Dixon’s Method” 和“Algebraic Algorithms for D-modules and Numerical analysis” 大会邀请报告。本次大会的主要议题是：符号计算，自动推理，计算机几何辅助设计，计算代数，计算几何，并行和分布式计算，网络计算，以及软件开发等等。会议文集由新加坡 World Scientific 出版。ASCM 系列会议是由数学机械化中心与日本符号计算协会于1995 年创立，每两年举办一次，主要在亚洲国家举办，参加者来自世界各地。第七届 ASCM 将于 2005 年在韩国举办。
2. 2003 年 10 月 23 日“几何约束求解研讨会” 北京数学与系统科学研究院 来自法国、 西班牙、中国台北与国内的七位学者做了学术报告。
3. 王世坤：十一月六日到十二月六日，和高科技中心联合举办“广义相对论工作月”。
4. 2003 年 10 月 10－11 日 “数学机械化与自动推理平台”课题验收及学术报告会中科院数学与系统科学研究院 参加会议人数：80
5. 王世坤：九月六日到十二月二十九日，“数学物理讨论班”。
6. 万哲先 群与代数组合研讨会，2003,09.05-07. 苏州，30 人左右
7. 吴可：七月二十八日到八月一日，和高科技中心联合举办“保结构算法讨论班”。
8. 王世坤：六月十五日到七月十五日，和晨兴中心联合举办“数学物理讨论班：

旋量分析”。

9. 2003 年 1 月 10－11 日 “数学机械化软件研讨会”在黑龙江大学召开。 来自全国的 30 名有关数学机械化软件的研究和开发方面的学者参加了这次会议，并且介绍了相关软件的开发情况。

参加国际学术会议

1. 高小山，Classification and Solving of Merge Patterns in Geometric Constraint Solving ，International Conference on Shape Modeling, May, 2003, Korea.
2. 高小山，Geometric Constraint Solving via C-tree Decomposition ，ACM Symposium on Solid Modeling**,** June 2003, Seattle, USA.
3. 高小山，Zero Decomposition Tree for Counting the Number of Solutions for Algebraic Parametric Equation Systems, ASCM, Beijing, Oct. 2003.
4. 刘木兰, Isomorphism classes of hyper elliptic cusses of genus 2 over finite fields with Characteristic 2, The Second East Asian Conference on Algebra and Combinatory, Kyushu university, Japan, Nov. 17-21, 2003.
5. 唐春明，刘卓军，Zero-knowledge proof system vs asymmetric cryptosystem, symmetric cryptosystem，First MiAn International Conference on Applied Cryptography and Network Security，On 16-18 October 2003
6. 吴可，王世坤，Recent Developments in Several Complex Variables, Cauchy-Riemann Geometry and Complex algebraic Geometry, Nov. 20-24, 2003, University of Hongkong.
7. 吴可,王世坤, 邀请报告 “Global solutions of Einstein-Dirac equation on the conformal space”, University of Hongkong。
8. 万哲先, Geometry of Matrices of L. K. Hua, 信息组合与复杂度，Bielefeld, Germany 2003.
9. 万哲先, Adjacency preserving mappings of symmetric and hermitian matrices EACAC2, Fukuoka, Japan, 2003. 11.17-21.
10. 万哲先，Symplectic Graphs and Their Automorphisms, Northeastern Asian Conference, 14-18, Dec, 2003.
11. Xinwen Wu, The 7th International Symposium on Digital Signal Processing and Communication Systems, Cold Coast, Australia, 8-11, December, 2003.
12. 支丽红，A complete symbolic-numeric linear method for camera pose determination. ISSAC 2003, 8 月 3-6.
13. 支丽红, Displacement structure in computing the approximate GCD of univariate polynomials. ASCM**,** 2003(中国) 10 月 23-25。
14. 支丽红, Determination of approximate symmetries of differential equations. Workshop on Group Theory and Numerical Analysis, Montreal, AMS, Canada, 2003, 5 月 26-31.
15. 李子明, Hyperexponential Solutions of D-finite Systems 微分代数讨论班 Hunter

College, 纽约，美国.

16. 李子明, Factoring D-finite Systems 微分代数讨论班, Hunter College, 纽约.

参加国内学术会议

1. 吴文俊，2003 年 11 月 28 日中国科学人文论坛, “计算机时代的东方数学”.
2. 吴文俊, 2003 年 11 月 27 日在 The 1st Asian Symposium on Programming Language and Systems 上作 On a Method of Global Optimization 报告.
3. 吴文俊, 2003 年 11 月 19 日, 在中国智能学会 2003 全国学术大会、可拓学创立 20 年庆祝大会、中韩智能系统学术研讨会上作“计算机时代脑力机械化与科学技术现代化” 报告
4. 吴文俊，2003 年 11 月 17 日，在广东工业大学, “拓扑学到机器证明”.
5. 刘木兰, 10 月 15-18 日，2003 中国计算机学会信息保密专业委员会学术年会在河南信阳召开，会上作“线性多密钥共享体制”的报告,，.
6. 高小山, 2003.10. 在武汉召开的“中国数学会学术会议年会”上作“构造性微分代数几”的报告。
7. 刘木兰, 2003 年 8 月 23-28 日在山西师范大学召开的“中国数学会 2003 年全国群论研讨会”上作“信息安全理论与数学科学”。
8. 王宝山, 2003 年 8 月在“中国数学会全国群论会议”作“关于 p-局部秩”的报告
9. 唐春明，刘卓军，在“中国计算机大会”上，作“对小额电子支付方案的改进”的报告。
10. 王世坤，Two points function in conformal field theory, Recent Developments in mathematical physics, Hangzhou, July, 003.
11. 吴文俊, 2003 年 1 月 10 日在“数学机械化软件研讨会”, “计算机时代的脑力劳动机械化与数学机械化”的报告。

实验室成员出访

1. 李子明 2003.1-12 在加拿大滑铁卢大学计算机系, 符号计算。
2. 马玉杰 2003 年 1 月－2003 年 5 月, 美国麻省大学数学系。
3. 刘胜强, 2002 年 2 月 12 至 16 日，访问日本九州大学。
4. 刘胜强, 2003 年访问意大利 Urbino 大学两个月。
5. 吴新文, 澳大利亚墨尔本大学, 2003 年 3 月至 12 月
6. 马玉杰 2003 年 6 月－2003 年 10 月, 法国国家科学中心 Painlevé 实验室。
7. 支丽红 8 月到美国北卡罗利大学数学系访问。
8. 支丽红 8 月到美国南加州大学数学系访问。
9. 万哲先, 2003 年 2 月,应邀访问德国 Bielefeld 大学。

10. 万哲先, 2003 年 9 月访问美国 Blomsburg 大学。
11. 李洪波 9 月访问美国亚利桑那州立大学。
12. 吴可,10 月 13－11 月 1 日到日本本茨城大学, 学术交流。10 月 21－24 日，日本京都大学汤川(YUKAWA)研究所, 学术交流,11 月 28 日访问日本 KEIO 大学。
13. 吴可，王世坤, 11 月 19－25 日赴香港大学, 学术会议。
14. 高小山，7 月 1 日－8 月 30 日，SUNY Stony Brook.

• 讨论班•

数学机械化讨论班: 每周四定期举行，以下列出 2003 年的主要活动内容。

3 月 12 日	Feng Ruyong	Newton Polygon Method To solve polynomial and Differential Equations
3 月 3 日	Lina Zhao	3D Interpretation of single line drawing
3 月 13 日	曾广兴 (南昌大学)	Catching endpolnts of intervals in a semialgebraic subset
3 月 26 日	LuoYong	S-System Approach to Non linear Modeling with applications in Molecular Design
4 月 3 日	黄文奇 （华中科技大）	NP 难问题计算中的拟物拟人方法
4 月 4 日	黄文奇 (华中科技大学）	蛋白质折叠计算
4 月 10 日	方伟武 （中科院数学所）	全局优化问题求解研究的一些情况介绍
4 月 17 日	李邦河（系统所院士）	A method to solve algebraic equations ip to multiplicities via Ritt-Wu method*
4 月 21 日	张绪平教授（北京工业大学）	柔性冗余度机器人弹性震动控制研究
3 月 5 日	Lei Deli	On the Numbetr of Solutions for the 6D General Stewart Platform
8 月 30 日	Prof. Kobayashi （日本大学）	Formalization of Ring Theory
9 月 17 日	Prof.Wang Wenping (University of HongKang)	Collision Detection for Ellipses under Rational Motion
10 月 25 日	Prof.Takayama Nobuki (Kobe university, Japan)	Algorithms for D-modules and Applications in Numerical Computation
10 月 27 日	Prof.Stephen M.	The current Status of Mathml and Math

	Watt (Univ of Western Ontario)	on the Web
11 月 13 日	马玉杰	Introduction to Differential Algebraic Geometry
12 月 11 日	Prof.Jill Slay	Quantifying cross-cultural effects in the design,engineering and development of complex information systems

专题讨论班

数学机械化(博士课程)	1 月－每周四下午	高小山主持
构造性微分代数几何	1 月－每周三下午	高小山主持
几何计算	1 月－每周一下午	李洪波主持
计算代数几何引论	1 月－每周二、五下午	王定康主持
数值与符号混合计算	1 月－每周五上午	支丽红主持
符号计算与信息安全	1 月－每周四晚上	刘卓军
信息安全基础理论（安全复方计算和随机算法）	7 月－	刘木兰

• 研究生、博士后、访问学者•

博士后：刘胜强、王宝山、谢福鼎、高莹、邓映蒲、安丰稳

博士生：林强,李明、吴敏、赵丽娜、唐春明、刘枫、雷德利、陈雪峰、冯如勇、王新民、罗勇、于建平、袁和军、赵新超、谭作文、孙维昆、曹南斌、曹丽娜、陈颖、杨争峰、郑大彬、程进三、张明波、李冰玉、徐荣华、张宁、肖亮亮、郭丽峰、曹正军

硕士生：张艳硕、李鹏、袁春明、李广伟、王全、张帅、熊涛、黄雷、龙红量、林隆、秦龙、张贵林、张志芳、周凯、冷福生

毕业及授予学位情况：

出站博士后：赵纪满

博士：孙永利、汤建良、张桂芳、李玉奇、吕仁才、蒋云峰

硕士：王新民、程贯中、张岩、程进三、岳晶岩、孟晓辉

研究生所获奖励：

1. 博士后刘胜强获 2002 年度中国博士后基金一等。
2. 博士生朱长才获 2002 年度宝洁优秀博士生奖学金。
3. 博士生李明获中科院数学与系统科学研究院院长奖学金特别奖。
4. 博士生唐春明获中科院数学与系统科学研究院院长奖学金优秀奖。
5. 博士生李明申请的中科院科学与社会实践资助专项项目“逆向工程的研究及其动态软件的应用”得到资助。

兼职教授：

Shang-Ching Chou （Wichita State Univ）

Paul S. Wang （Kent State Univ）

Dongming Wang（法国 CNRS）

吴文达（北京市计算中心）

访问学者：

曾广兴：南昌大学

杨 宏：北京市计算中心

孟晓晖：锦州师范大学

侯春旺: 中国石油大学

• 开放课题•

实验室通过以下专项经费支持开发课题。

- "数学机械化应用推广专项经费"申请办法
- "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

实验室第一批在研开放课题如下。

序号	课题名称	承担单位	承担人
1	基于吴方法的非线性演化方程孤波自动求解软件包	华东师范大学	李志斌*柳银萍、张善卿、徐桂琼贺筠
2	吴消元法证明恒等式的研究	大连理工大学	王天明*王毅、赵玉珍等
3	串联机器人逆解及仿真通用软件研制及开发	北京邮电大学自动化学院	廖启征*
4	数学机械化方法在工程图绘制理论中的应用	数学与系统科学研究院 北京航空航天大学	石赫*宁涛、 孙永利、熊歆宾
5	电力系统基本计算	上海交大学电力学院	陈陈*曹国云等
6	吴方法推广教学、讲座与吴方法在机构学中应用	北京理工大学 刘惠林#	张同庄*丁洪生、关靄雯、荣辉、 傅铁、史长虹等
7	数学机械化方法在航空天、天文。海洋力学贺理论物理领域的若干应用	北京航空航天大学流体力学研究所	高以天*田播、魏光美 张玉平、赵可昳
8	隐式代数曲面拼接平台	吉林大学	冯果忱，张树功，周蕴时等
9	动力系统软件开发	温州师范学院系统科学所	陆征一

10	数学机械化在数学物理中的应用	大连理工大学	陈勇
11	数学机械化方法在CAD 中的应用	黑龙江大学	蒋鲲

注：*为课题负责人

• 实验室人员学术机构任职•

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

高小山

《系统科学与数学》，副主编

Journal of Symbolic Computation，编委

Journal of System Science and Complexity，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

中国数学会，常务理事

中国图象图形学会，理事

刘木兰

《系统科学与数学》编委

刘卓军

《系统科学与数学》编委