ISSAC 2005

International Symposium on

Symbolic and Algebraic Computation

and

AMC and IAMC Workshops

Program

July 23-27, 2005

Beijing, China

PROGRAM

July 23	08:20-12:00 14:00-17:30	AMC Workshop	Room 101
July 24	09:00-11:30	Tutorial 1	Room 106
	13:00-15:30	Tutorial 2	Room 102
	16:00-18:30	Tutorial 3	Room 102
	08:30-12:15 13:45-16:30	IAMC Workshop	Room 104
	08:30-11:50	AMC Workshop	Room 101
	19:00-	Reception	Ju-Fu-Ting (聚福厅) Friendship Palace
July 25	08:30-08:40	Opening	Main Lecture Room
	08:40-10:20	Session 1	
	10:40-12:45	Session 2	
	14:00-15:00	Invited Talk	
	15:15-16:30	Session 3	
	16:45-18:25	Session 4	
	18:25-19:25	ISSAC Business Meeting	
July 26	08:30-10:10	Session 1	Main Lecture Room
	10:30-12:35	Session 2	
	13:30-13:50	Maple10.0 Demo	
	14:00-15:00	Invited Talk	
	15:15-16:30	Session 3	
	17:40-19:20	Session 4	
	16:30-17:40	Poster Session	Room 101
	16:30-17:40	Software Demo	Main Lect Room
	19:30 -	Banquet	Banquet Hall Building No.1
July 27	08:30-10:10	Session 1	Main Lecture Room
	10:30-12:35	Session 2	
	13:30-13:50	Maple10.0 Demo	
	14:00-15:00	Invited Talk	
	15:15-16:30	Session 3	
	16:45-18:25	Session 4	
	18:25 -19:25	SIGSAM Business	

All lectures are in the Meeting Hall （北京友谊宾馆，会议楼）

Conference Information

Conference Venue: Meeting Hall of the Beijing Friendship Hotel
（北京友谊宾馆，会议楼）

Registration and Information:

- July 24, 08:00－19:00. Lobby of Building No. 1
- July 25-27, 08:00－19:00. Room 104 of Meet Hall

Lunches and dinners are served at the Cafeteria (咖啡厅) inside the Friendship Palace. Tickets for registered participants are in the registration bags. Extra tickets could be purchased at the registration table.

Emails: Participants may use the computers in Room 101 to check their emails

Taxi：Taxies are available at the front door of the grand building

Saturday, July 23

AMC Workshop

7:30-12:00 **Registration of the Workshop**

8:20-8:30 **Opening of the Workshop (Chair: Zhuojun Liu)**

Chair: Mulan Liu

8:30-9:30 Nicolas T. Courtois

General principles of algebraic attacks and new design criteria for components of symmetric ciphers

9:30-10:30 Frederik Armknecht

On the existence of low-degree equations for algebraic attacks

10:30-11:00 **Break**

Chair: Mingsheng Wang

11:00-11:20 Chunxia Xu

An algorithm to determine the annihilators of Boolean function and a class of invariant of algebraic attacks

11:20-11:40 Xijin Tang

Improve the behavior of XL family by reducing the excrescent multiply monomials

11:40-12:00 Yonghui Zheng

Conditional factorization based on lattice theory for integers of a special form

12:00-13:00 **Lunch**

Chair: Chaoping Xing

14:00-15:00 Xiaotie Deng

Modular security analysis for an anonymous roaming protocol

15:00-16:00 Jintai Ding

Perturbation of multivariable public key cryptosystems

16:00-16:30 **Break**

Chair: Dongdai Lin

16:30-16:50 Zhifang Zhang

Multiparty computation based on connectivity of graphs

16:50-17:10 Zhiyuan Yan

A private-key cryptosystem based on the rank metric

17:10-17:30 Guangwu Xu

Protocols for sharing a product

In The Evening: **Poster Session**

Sunday, July 24

Tutorials

09:00-11:30 Arnaud Tisserand （Room 106）

Tutorial: Algorithms and Number Systems for Hardware Computer Arithmetic

13:00-15:30 Evelyne Hubert （Room 102）

Tutorial: Differential algebra and triangulation decomposition algorithms

16:00-18:30 Jan Verschelde （Room 102）

Tutorial： Homotopy Methods for Solving Polynomial Systems

IAMC Workshop

08:30 -- 09:00 Registration and Refreshments

09:00 -- 09:15 Welcome and Workshop Theme

Session Chair: Paul S. Wang

09:15 -- 10:30 **Invited Speech: Stephen M. Watt**

A Framework for Pen-Based Mathematical Computing

10:30 -- 11:00 **Break**

Session Chair: Dongdai Lin

11:00--11:25 Andreas Strotmann

Multilingual Access to Mathematical Exercise Problems

11:25--11:50 Maria Angelica de O. Camargo-Brunetto and Cleberson Vidotte Costa

Web-based Education for Algebraic and Numerical Mathematics

11:50--12:15 Wei Su, Lian Li, Paul Wang

Lesson Page Structure and Customization in WME

Session Chair: Norbert Kajler

13:45 -- 15:00 **Prof. Hai Jin**

Invited Speech: The ChinaGrid and its Impact on e-Science in China

15:00 -- 15:15 **Break**

Session Chair: Laureano Gonzalez

15:15--15:40 Xun Lai and Paul Wang

An SVG Based Tool for Plane Geometry and Mathematics Education

15:40--16:05 R. Alexander Milowski

XML Pipelining for Mathematical Computation

16:05--16:30 Jian Zhan, Lian Li

MICE: A Mathematical Integrated Computation Environment

16:30 -- 16:45 **Break**

16:45 -- 18:15 **System Demos**

Demo Chair: Dongdai Lin

Demo -- GeoSVG: An SVG-based Web-oriented Dynamic Geometry Software
Xun Lai, Department of Computer Science, Kent State University, USA

Demo -- WME: Web-based Mathematics Education Pilot Site
Paul Wang, Department of Computer Science, Kent State University, USA

Demo -- Lesson Page Customization in WME
Sue Wei, Lanzhou University PRC and Kent State University, USA

AMC Workshop

Chair: Xiaotie Deng

8:30-9:30 Chaoping Xing
Constructions of authentication codes and hash families through curves

9:30-10:00 **Break**

Chair: Zhuojun Liu

10:00-10:20 Zhengjun Cao
Suspending-factor and redundant data in several signature schemes

10:20-10:40 Haibo Sun
An improved efficient self-healing group key distribution

10:40-11:00 Rongquan Feng
On the 2-ranks of the Maiorana-McFarland bent functions

11:00-11:20 Hong Xu
Autocorrelations of *l*-sequences with certain shifts

11:20-11:40 Fengxiang Zhu
The stability of 2^n-periodic binary sequences with 2^n-1 linear complexity

11:40-11:50 Closing of the Workshop: Zhuojun Liu

Lunch and Reception

12:00-14:00 **Lunch**

19:00- **Reception** (Ju-Fu-Ting (聚福厅) inside the Friendship Palace)

Monday, July 25

08:30-08:40 **Opening Remarks**

Session Chair: Kazuhiro Yokoyama

08:40-09:05 J. de Kleine, M. Monagan, A. Wittkopf
Algorithms for the Non-monic case of the Sparse Modular GCD Algorithm

09:05-09:30 Daniel Lichtblau
Half-GCD and Fast Rational Recovery

09:30-09:55 Erich Kaltofen, Pascal Koiran
On the Complexity of Factoring Bivariate Supersparse (lacunary) Polynomials

09:55-10:20 Michael Monagan
Probabilistic Algorithms for Computing Resultants

10:20-10:40 **Coffee Break**

Session Chair: Marko Petkovsek

10:40-11:05 Alin Bostan, Thomas Cluzeau, Bruno Salvy
Fast Algorithms for Polynomial Solutions of Linear Differential Equations

11:05-11:30 M. van Hoeij, J.-A. Weil
Solving Second Order Linear Differential Equations with Klein's Theorem

11:30-11:55 Manuel Bronstein, Ziming Li, Min Wu
Picard-Vessiot Extensions for Linear Functional Systems

11:55-12:20 Biao Li, Yong Chen, Qi Wang
Exact Analytical Solutions to the Nonlinear Schroedinger Equation Model

12:20-12:45 Dongming Wang, Bican Xia
Stability Analysis of Biological Systems with Real Solution Classification

12:45-14:00 **Lunch** （Cafeteria (咖啡厅) inside the Friendship Palace）

Session Chair: George Labahn

14:00-15:00 Bruno Salvy
Invited Talk：D-finiteness: Algorithms and Applications

15:00-15:15 **Coffee Break**

Session Chair：**Frederic Chyzak**

15:15-15:40 Sergei A. Abramov, Marko Petkovsek
Gosper's Algorithm and Accurate Summation as Definite Summation Tools

15:40-16:05 Carsten Schneider
Finding Telescopers with Minimal Depth for Indefinite Nested Sum and Product Expressions

16:05-16:30 Costermans, Enjalbert, Hoang Ngoc Minh, Petitot
Structure and Asymptotic Expansion of Multiple Harmonic Sums

16:30-16:45 **Coffee Break**

Session Chair：Paul Wang

16:45-17:10 Stefan Gerhold, Manuel Kauers
A Procedure for Proving Special Function Inequalities Involving a Discrete Parameter

17:10-17:35 D.J. Jeffrey, Pratibha, K.B. Roach
Affine Transformations of Algebraic Numbers

17:35-18:00 Lu Yang, Zhenbing Zeng
An Open Problem on Metric Invariants of Tetrahedra

18:00-18:25 C. E. Oancea, S. M. Watt
Domains vs Expressions: An Efficient High-level Interface Between Aldor and Maple

18:25-19:25 **ISSAC Business Meeting**

19:30- **Dinner** （Cafeteria (咖啡厅) inside the Friendship Palace）

Tuesday, July 26

Session Chair: Lihong Zhi

08:30-08:55 O. A. Carvajal, F. W. Chapman, K. O. Geddes
Hybrid symbolic-numeric integration in multiple dimensions via tensor -product series

08:55-09:20 Greg Reid, Jan Verschelde, Allan Wittkopf, Wenyuan Wu
Symbolic-Numeric Completion of Differential Systems by Homotopy Continuation

09:20-09:45 Aude Rondepierre, Jean-Guillaume Dumas
Algorithms for Hybrid Optimal Control. Part I: Symbolic/Numeric Control of Affine Dynamical Systems

09:45-10:10 Laurent Tournier
Approximation of Dynamical Systems using S-Systems Theory: Application to Biological Systems

10:10-10:30 **Coffee Break**

Session Chair：Daniel Lichtblau

10:30-10:55 Dima Grigoriev, Fritz Schwarz
Generalized Loewy-Decomposition of D-Modules

10:55-11:20 Sergey P. Tsarev
Generalized Laplace Transformations and Integration of Hyperbolic Systems of Linear Partial Differential Equations

11:20-11:45 J.M. Aroca, J. Cano, R. Feng, X.S. Gao
Algebraic General Solutions of Algebraic Ordinary Differential Equations

11:45-12:10 Delphine Boucher
Non Complete Integrability of a Magnetic Satellite in Circular Orbit

12:10-12:35 Jeffrey Adams, B. David Saunders, Zhendong Wan
Signature of Symmetric Rational Matrices and the Unitary Dual of Lie Groups

12:35-14:00 **Lunch** （Cafeteria (咖啡厅) inside the Friendship Palace）

13:30-13:50 Maple10.0 Demo (Main Lecture Room)

Session Chair: Peter Paule

14:00-15:00 Bruno Buchberger

Invited Talk: A View on the Future of Symbolic Computation

15:00-15:15 **Coffee Break**

Session Chair: Robert Corless

15:15-15:40 A. Zobnin

Admissible Orderings and Finiteness Criteria for Differential Standard Bases

15:40-16:05 X. Dahan, M. M. Maza, E. Schost, W. Wu, Y. Xie

Lifting Techniques for Triangular Decompositions

16:05-16:30 Alain Bretto, Luc Gillibert, Bernard Laget

Symmetric and Semisymmetric Graphs Construction using G-graphs

16:30-17:40 **Poster Session (at Room 104)**

16:30-17:40 **Software Demo (at the Main Lecture Room)**

Session Chair: Mark Giesbrecht

17:40-18:05 Christopher W. Brown, Scott McCallum

On Using Bi-equational Constraints in CAD Construction

18:05-18:30 J. Beaumont, Russell Bradford, J.H

Adherence is Better than Adjacency: Computing the Riemann Index using CAD

18:30-18:55 Hirokazu Anai, Shinji Hara, Kazuhiro Yokoyama

Sum of Roots with Positive Real Parts

18:55-19:20 Fangjian Huang, Shengli Chen

Schur Partition for Symmetric Ternary Forms and Readable Proof to Inequalities

19:30 - **Banquet** (Banquet Hall inside the Building No.1)

Wednesday, July 27

Session Chair: Michael Monagan

08:30-08:55 Jiansong Deng, Falai Chen, Liyong Shen

Computing the Mu-Bases of Rational Curves and Surfaces Using the Polynomial Matrix Factorization

08:55-09:20 J. Rafael Sendra, Sonia Perez-Diaz

Partial Degree Formulae for Rational Algebraic Surfaces

09:20-09:45 Andre Galligo, Jean Pascal Pavone

Selfintersections of a Bezier Bicubic Surface

09:45-10:10 Bradford Hovinen, Wayne Eberly

A Reliable Block Lanczos Algorithm over Small Finite Fields

10:10-10:30 **Coffee Break**

Session Chair: Howard Cheng

10:30-10:55 William J. Turner
Preconditioners for Singular Black Box Matrices

10:55-11:20 Arne Storjohann, Gilles Villard
Computing the Rank and a Small Nullspace Basis of a Polynomial Matrix

11:20-11:45 Markus A. Hitz
On Computing Nearest Singular Hankel Matrices

11:45-12:10 J. Dumas, C. Pernet, Z. Wan
Efficient Computation of the Characteristic Polynomial

12:10-12:35 Zhuliang Chen, Arne Storjohann
A BLAS based C Library for Exact Linear Algebra on Integer Matrices

12:35-14:00 **Lunch** （Cafeteria (咖啡厅) inside the Friendship Palace）

13:30-13:50 Maple10.0 Demo (Main Lecture Room)

Session Chair: Xiao-Shan Gao

14:00-15:00 Wen-Tsun Wu
Invited Talk: On a Finite Kernel Theorem for Polynomial-Type Optimization Problems and Some of its Applications

15:00-15:15 **Coffee Break**

Session Chair: Hongbo Li

15:15-15:40 Weibo Mao, Jinzhao Wu
Application of Wu's Method to Symbolic Model Checking

15:40-16:05 Eric Schost
Multivariate Power Series Multiplication

16:05-16:30 Jeremy R. Johnson, Werner Krandick, Anatole D. Ruslanov
Architecture-aware Classical Taylor Shift by 1

16:30-16:45 **Coffee Break**

Session Chair: Alin Bostan

16:45-17:10 Bernard Mourrain, Philippe Trebuchet
Generalized Normal Forms and Polynomial System Solving

17:10-17:35 Christiaan van de Woestijne
Deterministic Equation Solving over Finite Fields

17:35-18:00 Barry H. Dayton, Zhonggang Zeng
Computing the Multiplicity Structure in Solving Polynomial Systems

18:00-18:25 Erich Kaltofen, Dmitriy Morozov, George Yuhasz
Generic Matrix Multiplication and Memory Management in LinBox

18:25 -19:25 **SIGSAM Business Meeting**

19:30 - **Dinner** （Cafeteria (咖啡厅) inside the Friendship Palace）

Posters

July 26, 16:30-17:40, Room 101

H. Cheng, B. Gergel, E. King, E. Zima
Space-Efficient Evaluation of Hypergeometric Series

M. M. Benghorbal
A Unified Formula for Integer and Fractional Order
Symbolic Derivatives and Integrals of a Rational Polynomial.

J. Cheng, X.S. Gao, M. Li
Intrinsic Topological Representation of Real Algebraic Surfaces

T. Sasaki, D. Inaba
An Approach to Singularity from Extended Hensel Construction

E. Hubert, I. Kogan
Rational and Replacement Invariants of a Group Action

V. Pan
Polynomial Root Finding with Matrix Eigen-Solving

F. San Segundo, J. R. Sendra, J. Sendra
Offsets From the Perspective of Computational Algebraic Geometry

S. Rueda
Finite Fans, Actions of Torii and D-Modules

X.S. Gao, G. Zhang
2D and 3D Generalized Stewart Platforms

S. Watt
Algebraic Generalization

W. Krandick, K. Mehlhorn
New Bounds For the Descartes Method

Z.M. Li, Z.Dabin
Computation with Hyperexponential Functions

T. Wolf
The Package CRACK for Solving Large Overdetermined Systems

F.Lemaire, M. Moreno Maza, Y. Xie
The RegularChains Library in Maple

X. Dahan, E. Schost, M. Moreno Maza, W. Wu, Y. Xie
On the Complexity of the D5 Principle

S. Gao, M. Zhu
Irreducible Decomposition of Monomial Ideals

N. Belov, C. Koeck, W. Krandick, J. Shaffer
Mobile Mathematics Communication

A. Griewank, S. Heinz
Scarcity

Software Exhibitions

July 26, 16:30-17:40, at the Main Lecture Room

J. Abbott, A. Bigatti, M. Caboara, and L. Robbiano
CoCoALib News

The LinBox Group
LinBox, A Demonstration

R. A. Milowski
Monos Algebra Software

G. Moroz with J.-C. Faugère and F. Rouillier
Discriminant Variety Maple Package

B. Mourrain, J. P. Pavone, O. Ruatta, P. Trébuchet, and E. Tsigaridas
SYNAPS: A Library for Symbolic and Numeric Computation

D. G. Richardson and W. Krandick
Software Demonstration: New Memory Semantics for SACLIB

F. Schwarz
ALLTYPES: An ALgebraic Language and TYPE System

T. Wolf and W. Neun
Software Demo of the Program CRACK

ISSAC2005

Sponsored by ACM

Hosted by

Key Laboratory of Mathematics Mechanization

with financial support from

National Natural Science Foundation of China

Maplesoft

Academy of Mathematics and Systems Science

Institute of Systems Science

Key Laboratory of Mathematics Mechanization

Institut National De Recherche En Informatique Et En Automatique