

Curriculum Vitae For **Erich Kaltofen**

March 5, 2012

Table of Contents

Education	2	Grants	19
Professional Positions	2	Service External to the University	21
Keywords of Subjects	2	University Committees Served	27
Research Students	3	Invited Lectures	28
Publications	6	Awards and Citations	37
Courses Taught	17		

Note: My Internet homepage has links to the online versions of the above sections. The online documents contain most of my teaching and research material, including course notes, publications, software, and lectures with transparencies and sound tracks. Links are active in this document.

Education

Ph.D. (Computer Science): Rensselaer Polytechnic Institute, Troy, New York 1982

Adviser: Bobby F. Caviness

Thesis title: *On the Complexity of Factoring Polynomials with Integer Coefficients.*

M.S. (Computer Science): Rensselaer Polytechnic Institute, Troy, New York 1979

Adviser: S. Kamal Abdali

Project title: *An Attributed $LL(1)$ Compilation of Pascal into the λ -Calculus.*

Undergraduate (Technical Mathematics): Johannes Kepler University, Linz, Austria 1976

Passed *Erste Diplomprüfung* (first comprehensive examination towards diploma) *mit Auszeichnung* (with highest honors).

Professional Positions

Permanent Positions

1996 – present	Professor of Mathematics and Associate Member of Computer Science at North Carolina State University
1992 – 1995	Professor of Computer Science at Rensselaer Polytechnic Institute
1988 – 1992	Associate Professor at Rensselaer Polytechnic Institute
1984 – 1987	Assistant Professor at Rensselaer Polytechnic Institute
1982 – 1983	Assistant Professor of Computer Science at the University of Toronto
1981 – 1982	Lecturer of Computer Science at the University of Delaware
1978 – 1981	Research Assistant at Rensselaer Polytechnic Institute
1977 – 1978	Teaching Assistant at Rensselaer Polytechnic Institute

Visiting Positions

2006 – Spring	Visiting Scholar at the Massachusetts Institute of Technology
2005 – Summer	Professeur invité, Laboratoire de l'Informatique du Parallélisme Ecole Normale Supérieure de Lyon, France
2000 – October and December	General Member at the Mathematical Sciences Research Institute in Berkeley, California, for the Algorithmic Number Theory Program
2000 – June and 1999 – Jan.	Chaire municipale, Laboratoire de Modélisation et Calcul (LMC), Institut d'Informatique et de Mathématiques Appliquées de Grenoble (IMAG), France
1997 – July	Visiting Research Scientist at Simon Fraser University in Vancouver, British Columbia, Canada.
1991 – Spring	Visiting Associate Professor at the University of Toronto
1985 – Fall	Research Fellow at the Mathematical Sciences Research Institute in Berkeley, California, for the Computational Complexity Program
1985 – Summer	Visiting Scientist at the Tektronix Computer Research Laboratory in Beaverton, Oregon
1982 – Summer	Visiting Research Associate at Kent State University
1979 – Summer	Programmer for the Interactive Graphics Center at Rensselaer Polytechnic Institute

Keywords of Subjects

Computational Algebra and Number Theory, Design and Analysis of Sequential and Parallel Algorithms, Symbolic Computation Systems and Languages, Internet Mathematics Technology.

Students and Postdocs for Whom **Erich Kaltofen** Has Been Research Advisor

1 List of graduate students who have finished (only degree(s) from Kaltofen are listed)

- Didier Deshommes (MS Dec 07)
- Angel Luis Díaz (PhD May 97, MS Dec 93)
PhD Thesis: *FOXBOX: a System for Manipulating Symbolic Objects in Black Box Representation*
Currently Permanent Staff Member at IBM T. J. Watson Research Center in Yorktown Heights, New York.
- Timothy Scott Freeman (MS May 85)
- **Markus Alois Hitz** (PhD May 98, MS Dec 88)
PhD Thesis: *Efficient Algorithms for Computing the Nearest Polynomial With a Constrained Root*
Currently Prof. in Math. & Comput. Sci. at North Georgia College & State University
- David Hooton (MS Dec 85)
- Sharon E. Hutton (PhD Aug 11)
PhD Thesis: *Exact Sums-of-Squares Certificates in Numeric Algebraic Geometry*
Currently at **Wofford College**, South Carolina.
- Gregory Manug Imirzian (MS May 86)
- **Lakshman Yagati N.** (PhD Dec 90, MS May 87)
PhD Thesis: *On the Complexity of Computing Gröbner Bases for Zero-Dimensional Ideals*
1990 Robert F. McNaughton Award for the best computer science graduate student.
Currently at Google Inc.
- **Wen-shin Lee** (PhD Dec 01, MS Aug 99)
PhD Thesis: *Early Termination Strategies in Sparse Interpolation Algorithms*
Currently at the Math. and Comput. Sci. Dept. at the University of Antwerp, Belgium.
- **Austin Anthony Lobo** (PhD Dec 95, MS May 83)
PhD Thesis: *Matrix-Free Linear System Solving and Applications to Symbolic Computation*
Currently Assoc. Prof. in Math. & Comput. Sci. at **Washington College** in Chestertown, Maryland.
- **John Paul May** (PhD Aug 05)
PhD Thesis: *Approximate Factorization of Polynomials in Many Variables and Other Problems in Approximate Algebra via Singular Value Decomposition Methods*
Shared 2004 Lowell S. Winton and Nicholas J. Rose Award for outstanding graduate work in mathematics.
Currently at Maplesoft.
- Anton Prenneis (MS May 95)
- Kurt Schmitz (MS May 90)
- **William Jonathan Turner** (PhD Aug 02)
PhD Thesis: *Black Box Linear Algebra With the LinBox Library*
Shared 2002 Lowell S. Winton and Nicholas J. Rose Award for outstanding graduate work in mathematics.
Currently Assoc. Professor of Mathematics & Computer Science at Wabash College.
- **Thomas Valente** (PhD Dec 92)
PhD Thesis: *A Distributed Approach to Proving Large Numbers Prime*
Currently Assoc. Prof. in **Math. & Comput. Sci.** at Hampden-Sydney College.
- Alison White (MS May 94)

- **George Yuhasz** (PhD May 09)
PhD Thesis: *Berlekamp/Massey Algorithms for Linearly Generated Matrix Sequences*
Currently Assist. Prof. at Moorehouse College.

2 List of Kaltofen's current graduate students

- Matthew T. Comer (PhD)
PhD Thesis: *in progress*
- Feng Guo (PhD)
PhD Thesis: *visiting from KLMM, CAS, Beijing, China, Feb 2011–Jan 2012 (advisee of Lihong Zhi)*
- Michael Nehring (PhD)
PhD Thesis: *in progress (on leave)*

3 List of Kaltofen's post doctoral fellows

- **Zhengfeng Yang**, Ph.D. Chinese Academy of Sciences, Beijing; August 2006–December 2007.

4 External doctoral committee membership

- Luca De Feo, École Polytechnique, Paris, France, December 2010
- Mark Giesbrecht, Computer Science, University of Toronto, December 1992
- Michael Monagan, Computer Science, University of Waterloo, October 1989
- Daniel S. Roche, Computer Science, University of Waterloo, April 2011
- Sibylle Schupp, Informatik, University of Tübingen, Germany July 1996
- Zhendong Wan, Computer & Inform. Sciences, University of Delaware, July 2005
- Yuzhen Xie, Computer Science, University of Western Ontario, September 2007

5 External graduate trainee

- A. Vermeerbergen, Ecole Normale Supérieure de Lyon, France; Summer 1991.

6 Undergraduate research students

- Anderson Patrick Bryan (Spring 1988)
- King C. Chan (Summer 1993)
- Imin Chen (visiting from Queen's University, Kinston Canada, Summer 1991)
- Rostyslav Cisyk (Summer 1994)
- Angel Díaz (Summer 1990)
- Gregory Fisher (Fall 1984)
- L. Haralambos (Spring 1995)
- F. Harfouche (visiting from Syracuse University, Summer 1989)
- Scott Keith (Spring 1990)

- Mark Lavin (Fall 2003)
- Dmitriy Morozov (Fall 2002 and Spring 2003)
- D. Norris-Jones (Spring 1995)
- Philip Smyth (visiting from Hamilton College, Summer 1987)
- Grace Tseng (Summer 1986)
- C. Ryan Vinroot (Fall 1997 and Spring 1998)

Publications By Erich Kaltofen

In the following the EKbib and BASE URL is <http://www.math.ncsu.edu/~kaltofen/bibliography/>. Many of my publications are accessible through links in the Reference section of both the web [BASE/index.html](#) and this pdf document. In general, the URLs of the pdf or gzipped postscript files of my papers are [EKbib/y/l.pdf](#) or [EKbib/y/l.ps.gz](#), where y is the year of publication (last two digits) and l is the citation key in the [BASE/kaltofen.bib](#) file (replacing colons with underscores for compatibility with Microsoft Windows). The items thus retrieved are copyrighted by the publishers or by E. Kaltofen.

1 Major Research Results

1.1 Polynomial Factorization

- Polynomial-time algorithms for multivariate polynomial factorization with coefficients from a field [5, 6, 25, 27] or the algebraic closure of a field [19, 85]; deterministic polynomial-time irreducibility testing [35] and distinct degree factorization [121] of multivariate polynomials over a large finite field; computing the nearest multivariate polynomial with factor of constant degree and complex coefficients in polynomial time [105].
- Polynomial-time sparse multivariate polynomial factorization algorithms by introducing the straight-line program [42, 39, 34, 31, 24, 20] and the black box representations of polynomials [57, 81].
- Subquadratic-time polynomial factorization of univariate polynomials over a finite field [82, 97]; asymptotically fastest polynomial factorization algorithm over high algebraic extensions of finite fields [93].
- Polynomial-time computation of small degree factors of supersparse (lacunary) multivariate polynomials over the rational and algebraic numbers [129, 127].

1.2 Linear Algebra

- Rank algorithm for a black box matrix via Wiedemann's method but without binary search [58].
- Processor-efficient parallel algorithms for solving general linear systems over a field [62, 66].
- Parallel algorithms for matrix canonical forms [32, 54].
- Probabilistic analysis [80] and implementation [76, 89, 102] of the block Wiedemann parallel sparse linear system solver.
- Asymptotically fast solution of Toeplitz-like linear systems over any field including a finite field [80, 77].

- Probabilistic analysis of the Lanczos sparse linear system solver over finite fields [94].
- Baby steps/giant steps algorithms for computing the determinant of an integer matrix [109, 112, 124]; fastest algorithm known in terms of bit operations for the characteristic polynomial.
- Analysis and fraction-free realization of the matrix Berlekamp/Massey algorithm [132, 141].

1.3 Sparse Polynomial Interpolation

- Asymptotically fast and modular versions of the Zippel and Ben-Or/Tiwari algorithms [38, 53, 148].
- Early termination versions of the Zippel and Ben-Or/Tiwari algorithms [107, 119].
- Algorithms for computing the sparsest shift of polynomials [113, 118].
- Recovery of multivariate sparse rational functions [135, 134].

1.4 Divisions and Algebraic Complexity Theory

- Polynomial-length separate computation of the numerator and denominator of a rational function given by a straight-line program [39].
- Asymptotically fast multiplication of polynomials over a ring [64].
- Fast division-free computation of the determinant and the characteristic polynomial of a matrix over a commutative ring [67, 109, 124].
- Integer division with remainder in residue number systems via Newton iteration [83].
- Removal of divisions of in fractions of determinants and formulas [138].
- Valiant universality of determinants of symmetric matrices for formulas [149].

1.5 Computational Number Theory

- Use of Weber equations for the Hilbert class fields arising in the Goldwasser-Kilian/Atkin primality prover [14, 12, 48, 60].

1.6 Hybrid Symbolic/Numeric Computation

- Stability of roots of polynomials with respect to coefficient perturbations [99, 105].
- Approximate factorization [137, 122] and numerical irreducibility testing [117] of multivariate polynomials over the complex numbers.
- Approximate multivariate polynomial greatest common divisor computation [125, 130] and computation of the nearest singular polynomial [130].
- Exact certification of global optima via semidefinite programming and rationalization of sums-of-squares [139, 140, 142].
- Well- and ill-conditionedness of polynomial inequalities [144].

1.7 Software

- DAGWOOD: a system for manipulating polynomials given by straight-line programs [40]. The archive directory of the Lisp program source code is at [BASE/./software/dagwood](#).
- DSC: the distributed symbolic manipulation tool [61, 71, 75, 79]. The archive directory of the C, C++, Lisp, and Maple program source code is at [BASE/./software/dsc](#).
- FOXBOX: a plug-and-play symbolic system component for objects in black box representation [98]. The archive directory of the C++ program source code and the NTL and Saclib library binaries (solaris and linux elf) is at [BASE/./software/foxbox](#).
- WILISS: an implementation of the block Wiedemann algorithm [84, 102]. The archive directory of the C program source code is at [BASE/./software/wiliss](#).
- LINBOX: a generic library for exact black box linear algebra [111, 126]. The homepage including downloads can be found at www.linalg.org.
- APPFAC: a package for approximate multivariate complex polynomial factorization and GCD [130, 137, 122]. The directories of the Maple code and experiments are at [BASE/./software/appfac](#) and [BASE/./software/manystln](#).
- ARTINPROVER: a Matlab+Maple package for computing exact sum-of-squares certificates for global accurate lower bounds.

1.8 Paper on Pedagogy and Significant Instructional Software

- Undergraduate abstract algebra from a computational point of view [92]. The Mathematica packages and notebooks are at [BASE/./courses/ComputAlgebra/Mathematica](#).
- A demonstration implementation in Maple of the RSA public crypto system is at [BASE/./software/rsa](#).
- A demonstration package in Maple of algorithms in linear algebra is at [BASE/./courses/LinAlgebra/Maple/RefPkg/](#) (see [README.html](#)).
- An STL-like implementation in C++ of the container class binary search tree is at [BASE/./courses/DataStruct/C++Examples/BinSearchTree](#).
- A C++ implementation of common sorting algorithms is at [BASE/./courses/DataStruct/C++Examples/Sorting](#).

1.9 Surveys

- Four surveys on polynomial factorization [116, 68, 56, 7].
- Three surveys on algebraic algorithms [101, 95, 33].
- A survey on sparse linear systems [90] and one on the computational complexity of matrix determinants [123].
- A list of open problems [106].
- A survey on parallelizing straight-line programs [70].
- The seven dwarfs of symbolic computation [146].

References

- [156] Feng Guo, Erich L. Kaltofen, and Lihong Zhi. Certificates of impossibility of Hilbert-Artin representations of a given degree for definite polynomials and functions, March 2012. URL: <http://arxiv.org/abs/1203.0253>.
- [155] Erich Kaltofen and Arne Storjohann. The complexity of computational problems in exact linear algebra. In *Encyclopedia of Applied and Computational Mathematics* [-1], page to appear. URL: [EKbib/11/KS11.pdf](#).
- [154] Erich Kaltofen and Grégoire Lecerf. Section 11.5. Factorization of multivariate polynomials. In *Handbook of Finite Fields* [-2], page to appear. URL: [EKbib/11/KL11.pdf](#).

- [153] Erich L. Kaltofen, Wen-shin Lee, and Zhengfeng Yang. Fast estimates of Hankel matrix condition numbers and numeric sparse interpolation. In *SNC'11 Proc. 2011 Internat. Workshop on Symbolic-Numeric Comput.* [-3], pages 130–136. URL: [EKbib/11/KLY11.pdf](#).
- [152] Erich L. Kaltofen, Michael Nehring, and B. David Saunders. Quadratic-time certificates in linear algebra. In *Proc. 2011 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2011* [-4], pages 171–176. URL: [EKbib/11/KNS11.pdf](#).
- [151] Bruno Grenet, Erich L. Kaltofen, Pascal Koiran, and Natacha Portier. Symmetric determinantal representation of weakly skew circuits. In *Proc. 28th Internat. Symp. on Theoretical Aspects of Computer Science, STACS 2011* [-5], pages 543–554. Journal version in [149]. URL: [EKbib/11/GKKP11.pdf](#).
- [150] Matthew T. Comer and Erich L. Kaltofen. On the Berlekamp/Massey algorithm and counting singular Hankel matrices over a finite field, October 2010. Accepted for publication in *J. Symbolic Comput.*, 13 pages.
- [149] Bruno Grenet, Erich L. Kaltofen, Pascal Koiran, and Natacha Portier. Symmetric determinantal representation of formulas and weakly skew circuits. In Leonid Gurvits, Philippe Pébay, J. Maurice Rojas, and David Thompson, editors, *Randomization, Relaxation, and Complexity in Polynomial Equation Solving*, pages 61–96. American Mathematical Society, Providence, Rhode Island, USA, 2011. Contemporary Math., vol. 556. URL: [EKbib/10/GKKP10.pdf](#).
- [148] Erich L. Kaltofen. Fifteen years after DSC and WLSS2 What parallel computations I do today [Invited lecture at PASCO 2010]. In *PASCO'10 Proc. 2010 Internat. Workshop on Parallel Symbolic Comput.* [-6], pages 10–17. URL: [EKbib/10/Ka10_pasco.pdf](#).
- [147] Erich L. Kaltofen. Final Report on NSF Workshops (Grant CCF-0751501) *The Role of Symbolic, Numeric and Algebraic Computation in Cyber-Enabled Discovery and Innovation (CDI)* NSF, October 30–31, 2007 *Future Directions of Symbolic Computation Research And Their Applications to the Domain Sciences* Univ. Rhode Island, April 30–May 1, 2009, May 2010. 32 pages; includes Executive Summary, Workshops' Findings and Summaries of 7 Panel Discussions.
- [146] Erich L. Kaltofen. The “Seven Dwarfs” of symbolic computation, April 2010. Manuscript prepared for the final report of the 1998–2008 Austrian research project SFB F013 “Numerical and Symbolic Scientific Computing,” Peter Paule, director, URL: [EKbib/10/Ka10_7dwarfs.pdf](#).
- [145] Erich L. Kaltofen and Michael Nehring. Super-sparse black box rational function interpolation. In *Proc. 2011 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2011* [-4], pages 177–185. URL: [EKbib/11/KaNe11.pdf](#).
- [144] Sharon E. Hutton, Erich L. Kaltofen, and Lihong Zhi. Computing the radius of positive semidefiniteness of a multivariate real polynomial via a dual of Seidenberg’s method. In *Proc. 2010 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2010* [-7], pages 227–234. URL: [EKbib/10/HKZ10.pdf](#).
- [143] Erich Kaltofen and Mark Lavin. Efficiently certifying non-integer powers. *Computational Complexity*, 19(3):355–366, September 2010. URL: [EKbib/09/KaLa09.pdf](#).
- [142] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. A proof of the Monotone Column Permanent (MCP) Conjecture for dimension 4 via sums-of-squares of rational functions. In *SNC'09 Proc. 2009 Internat. Workshop on Symbolic-Numeric Comput.* [-8], pages 65–69. URL: [EKbib/09/KYZ09.pdf](#).
- [141] Erich Kaltofen and George Yuhasz. A fraction free matrix Berlekamp/Massey algorithm, February 2009. Manuscript, 17 pages.
- [140] Erich L. Kaltofen, Bin Li, Zhengfeng Yang, and Lihong Zhi. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *J. Symbolic Comput.*, 47(1):1–15, January 2012. In memory of Wenda Wu (1929–2009). URL: [EKbib/09/KLYZ09.pdf](#).
- [139] Erich Kaltofen, Bin Li, Zhengfeng Yang, and Lihong Zhi. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In *ISSAC 2008* [-9], pages 155–163. URL: [EKbib/08/KLYZ08.pdf](#).
- [138] Erich Kaltofen and Pascal Koiran. Expressing a fraction of two determinants as a determinant. In *ISSAC 2008* [-9], pages 141–146. URL: [EKbib/08/KaKoi08.pdf](#).
- [137] Erich Kaltofen, John May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials using singular value decomposition. *J. Symbolic Comput.*, 43(5):359–376, 2008. URL: [EKbib/07/KMYZ07.pdf](#).
- [136] Peter Borwein, Erich Kaltofen, and Michael J. Mossinghoff. Irreducible polynomials and Barker sequences. *ACM Communications in Computer Algebra*, 162(4):118–121, December 2007. Published by SIGSAM. URL: [EKbib/07/BKM07.pdf](#).
- [135] Erich Kaltofen and Zhengfeng Yang. On exact and approximate interpolation of sparse rational functions. In *ISSAC 2007 Proc. 2007 Internat. Symp. Symbolic*

- Algebraic Comput.* [-10], pages 203–210. URL: [EKbib/07/KaYa07.pdf](#).
- [134] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. On probabilistic analysis of randomization in hybrid symbolic-numeric algorithms. In *SNC'07 Proc. 2007 Internat. Workshop on Symbolic-Numeric Comput.* [-11], pages 11–17. URL: [EKbib/07/KYZ07.pdf](#).
- [133] Erich Kaltofen, Bin Li, Kartik Sivaramakrishnan, Zhengfeng Yang, and Lihong Zhi. Lower bounds for approximate factorizations via semidefinite programming (extended abstract). In *SNC'07 Proc. 2007 Internat. Workshop on Symbolic-Numeric Comput.* [-11], pages 203–204. URL: [EKbib/07/KLSYZ07.pdf](#).
- [132] Erich Kaltofen and George Yuhasz. On the matrix Berlekamp-Massey algorithm, December 2006. Manuscript, 29 pages. Submitted.
- [131] Wolfram Decker, Mike Dewar, Erich Kaltofen, and Stephen Watt, editors. *Challenges in Symbolic Computation Software*, number 06271 in Dagstuhl Seminar Proceedings. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2006. Includes Abstracts Collection and Executive Summary by the editors. URL: [Dagstuhl/portals/index.php?semnr=06271](#).
- [130] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. In *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.* [-13], pages 169–176. URL: [EKbib/06/KYZ06.pdf](#).
- [129] Erich Kaltofen and Pascal Koiran. Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields. In *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.* [-13], pages 162–168. URL: [EKbib/06/KaKoi06.pdf](#).
- [128] Erich Kaltofen and Lihong Zhi. Hybrid symbolic-numeric computation. In *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.* [-13], page 7. Tutorial abstract. URL: [EKbib/06/KaZhi06.pdf](#).
- [127] Erich Kaltofen and Pascal Koiran. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In *ISSAC'05 Proc. 2005 Internat. Symp. Symbolic Algebraic Comput.* [-14], pages 208–215. ACM SIGSAM's ISSAC 2005 Distinguished Paper Award. URL: [EKbib/05/KaKoi05.pdf](#).
- [126] Erich Kaltofen, Dmitriy Morozov, and George Yuhasz. Generic matrix multiplication and memory management in LinBox. In *ISSAC'05 Proc. 2005 Internat. Symp. Symbolic Algebraic Comput.* [-14], pages 216–223. URL: [EKbib/05/KMY05.pdf](#).
- [125] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Structured low rank approximation of a Sylvester matrix. In *Symbolic-Numeric Computation* [-12], pages 69–83. Preliminary version in [-15], pp. 188–201. URL: [EKbib/05/KYZ05.pdf](#).
- [124] Erich Kaltofen and Gilles Villard. On the complexity of computing determinants. *Computational Complexity*, 13(3-4):91–130, 2004. URL: [EKbib/04/KaVi04_2697263.pdf](#); Maple 7 worksheet URL: [EKbib/04/KaVi04_2697263.mws](#).
- [123] E. Kaltofen and G. Villard. Computing the sign or the value of the determinant of an integer matrix, a complexity survey. *J. Computational Applied Math.*, 162(1):133–146, January 2004. Special issue: Proceedings of the International Conference on Linear Algebra and Arithmetic 2001, Rabat, Morocco, 28–31 May 2001, S. El Hajji, N. Revol, P. Van Dooren (guest eds.). URL: [EKbib/02/KaVi02.pdf](#).
- [122] Shuhong Gao, Erich Kaltofen, John P. May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials via differential equations. In *ISSAC 2004 Proc. 2004 Internat. Symp. Symbolic Algebraic Comput.* [-16], pages 167–174. ACM SIGSAM's ISSAC 2004 Distinguished Student Author Award (May and Yang). URL: [EKbib/04/GKMYZ04.pdf](#).
- [121] Shuhong Gao, E. Kaltofen, and A. Lauder. Deterministic distinct degree factorization for polynomials over finite fields. *J. Symbolic Comput.*, 38(6):1461–1470, 2004. URL: [EKbib/01/GKL01.pdf](#).
- [120] Wayne Eberly and Erich Kaltofen. Early termination in Shoup's algorithm for the minimum polynomial of an algebraic number. 16 pages, 2004.
- [119] Erich Kaltofen and Wen-shin Lee. Early termination in sparse interpolation algorithms. *J. Symbolic Comput.*, 36(3–4):365–400, 2003. Special issue Internat. Symp. Symbolic Algebraic Comput. (ISSAC 2002). Guest editors: M. Giusti & L. M. Pardo. URL: [EKbib/03/KL03.pdf](#).
- [118] Mark Giesbrecht, Erich Kaltofen, and Wen-shin Lee. Algorithms for computing sparsest shifts of polynomials in power, Chebychev, and Pochhammer bases. *J. Symbolic Comput.*, 36(3–4):401–424, 2003. Special issue Internat. Symp. Symbolic Algebraic Comput. (ISSAC 2002). Guest editors: M. Giusti & L. M. Pardo. URL: [EKbib/03/GKL03.pdf](#).
- [117] Erich Kaltofen and John May. On approximate irreducibility of polynomials in several variables. In *ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput.* [-17], pages 161–168. URL: [EKbib/03/KM03.pdf](#).

- [116] Erich Kaltofen. Polynomial factorization: a success story. In *ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput.* [-17], pages 3–4. Abstract for invited talk. URL: [EKbib/03/Ka03.pdf](#).
- [115] J. Grabmeier, E. Kaltofen, and V. Weispfenning, editors. *Computer Algebra Handbook*. Springer Verlag, Heidelberg, Germany, 2003. 637 + xx pages + CD-ROM. Includes E. Kaltofen and V. Weispfenning §1.4 Computer algebra – impact on research, pages 4–6; E. Kaltofen §2.2.3 Absolute factorization of polynomials, page 26; E. Kaltofen and B. D. Saunders §2.3.1 Linear systems, pages 36–38; R. M. Corless, E. Kaltofen and S. M. Watt §2.12.3 Hybrid methods, pages 112–125; E. Kaltofen §4.2.17 FoxBox and other blackbox systems, pages 383–385. URL: [EKbib/01/symnum.pdf](#).
- [114] L. Chen, W. Eberly, E. Kaltofen, B. D. Saunders, W. J. Turner, and G. Villard. Efficient matrix preconditioners for black box linear algebra. *Linear Algebra and Applications*, 343–344:119–146, 2002. Special issue on *Structured and Infinite Systems of Linear Equations*, edited by P. Dewilde, V. Olshevsky and A. H. Sayed. URL: [EKbib/02/CEKSTV02.pdf](#).
- [113] Mark Giesbrecht, Erich Kaltofen, and Wen-shin Lee. Algorithms for computing the sparsest shifts for polynomials via the Berlekamp/Massey algorithm. In *Proc. 2002 Internat. Symp. Symbolic Algebraic Comput. (ISSAC’02)* [-19], pages 101–108. Journal version in [118]. URL: [EKbib/02/GKL02.pdf](#).
- [112] Erich Kaltofen. An output-sensitive variant of the baby steps/giant steps determinant algorithm. In *Proc. 2002 Internat. Symp. Symbolic Algebraic Comput. (ISSAC’02)* [-19], pages 138–144. URL: [EKbib/02/Ka02.pdf](#).
- [111] J.-G. Dumas, T. Gautier, M. Giesbrecht, P. Giorgi, B. Hovinen, E. Kaltofen, B. D. Saunders, W. J. Turner, and G. Villard. LinBox: A generic library for exact linear algebra. In *Proc. First Internat. Congress Math. Software ICMS 2002, Beijing, China* [-18], pages 40–50. URL: [EKbib/02/Deta102.pdf](#).
- [110] Erich Kaltofen, Michael McLean, and Larry Norris. ‘Using Maple to grade Maple’ assessment software from North Carolina State University. In *Proceedings 2002 Maple Workshop*, Waterloo, Canada, 2002. Waterloo Maple Inc. With Dmitriy Morozov, John May and William Turner. URL: [EKbib/02/KMN02.pdf](#).
- [109] E. Kaltofen and G. Villard. On the complexity of computing determinants. In *Proc. Fifth Asian Symposium on Computer Mathematics (ASCM 2001)* [-20], pages 13–27. Invited contribution; extended abstract, journal version in [124]. URL: [EKbib/01/KaVi01.pdf](#); Maple 6 worksheet URL: [EKbib/01/KaVi01.mws](#).
- [108] E. Kaltofen. Algorithms for sparse and black box matrices over finite fields (invited talk). Bibliography for my talk on May 23, 2001 at the Sixth International Conference on Finite Fields and Applications (Fq6) in Oaxaca, Mexico, 6 pages. URL: [EKbib/01/Ka01_Fq6.pdf](#), 2001.
- [107] E. Kaltofen, W.-s. Lee, and A. A. Lobo. Early termination in Ben-Or/Tiwari sparse interpolation and a hybrid of Zippel’s algorithm. In *Proc. 2000 Internat. Symp. Symbolic Algebraic Comput. (ISSAC’00)* [-21], pages 192–201. URL: [EKbib/2K/KLL2K.pdf](#).
- [106] E. Kaltofen. Challenges of symbolic computation my favorite open problems. *J. Symbolic Comput.*, 29(6):891–919, 2000. With an additional open problem by R. M. Corless and D. J. Jeffrey. URL: [EKbib/2K/Ka2K.pdf](#).
- [105] M. A. Hitz, E. Kaltofen, and Lakshman Y. N. Efficient algorithms for computing the nearest polynomial with a real root and related problems. In *Proc. 1999 Internat. Symp. Symbolic Algebraic Comput. (ISSAC’99)* [-22], pages 205–212. URL: [EKbib/99/HKL99.pdf](#).
- [104] L. Bernardin, B. Char, and E. Kaltofen. Symbolic computation in Java: an appraisal. In *Proc. 1999 Internat. Symp. Symbolic Algebraic Comput. (ISSAC’99)* [-22], pages 237–244. URL: [EKbib/99/BCK99.pdf](#).
- [103] E. Kaltofen and M. Monagan. On the genericity of the modular polynomial GCD algorithm. In *Proc. 1999 Internat. Symp. Symbolic Algebraic Comput. (ISSAC’99)* [-22], pages 59–66. URL: [EKbib/99/KaMo99.pdf](#).
- [102] E. Kaltofen and A. Lobo. Distributed matrix-free solution of large sparse linear systems over finite fields. *Algorithmica*, 24(3–4):331–348, July–Aug. 1999. Special Issue on “Coarse Grained Parallel Algorithms”. URL: [EKbib/99/KaLo99.pdf](#).
- [101] A. Díaz, I. Emiris, E. Kaltofen, and V. Pan. Algebraic algorithms. In M. J. Atallah, editor, *Algorithms & Theory of Computation Handbook*, pages 16.1–16.27. CRC Press, Boca Raton, Florida, 1999. URL: [EKbib/99/DEKP99.ps.gz](#).
- [100] H. Hong, E. Kaltofen, and M. Singer, editors. East Coast Computer Algebra Day ’99 (April 24, 1999) Abstracts of invited talks and presented posters. *SIGSAM Bulletin*, 23(2):43–52, June 1999.
- [99] M. A. Hitz and E. Kaltofen. Efficient algorithms for computing the nearest polynomial with constrained roots. In *Proc. 1998 Internat. Symp. Symbolic Algebraic Comput. (ISSAC’98)* [-23], pages 236–243. URL: [EKbib/98/HiKa98.pdf](#).

- [98] A. Díaz and E. Kaltofen. FOXBOX a system for manipulating symbolic objects in black box representation. In *Proc. 1998 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'98)* [-23], pages 30–37. URL: [EKbib/98/DiKa98.pdf](#).
- [97] E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. *Math. Comput.*, 67(223):1179–1197, July 1998. URL: [EKbib/98/KaSh98.pdf](#).
- [96] M. A. Hitz and E. Kaltofen. The Kharitonov theorem and its applications in symbolic mathematical computation. Unpublished paper, North Carolina State Univ., Dept. Math. URL: [EKbib/97/HiKa97_kharit.pdf](#), May 1997.
- [95] A. Díaz, E. Kaltofen, and V. Pan. Algebraic algorithms. In A. B. Tucker, editor, *The Computer Science and Engineering Handbook*, chapter 10, pages 226–248. CRC Press, Boca Raton, Florida, 1997. Expanded version in [101]. URL: [EKbib/97/DKP97.ps.gz](#).
- [94] W. Eberly and E. Kaltofen. On randomized Lanczos algorithms. In *Proc. 1997 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'97)* [-24], pages 176–183. URL: [EKbib/97/EbKa97.pdf](#).
- [93] E. Kaltofen and V. Shoup. Fast polynomial factorization over high algebraic extensions of finite fields. In *Proc. 1997 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'97)* [-24], pages 184–188. URL: [EKbib/97/KaSh97.pdf](#).
- [92] E. Kaltofen. Teaching computational abstract algebra. *J. Symbolic Comput.*, 23(5-6):503–515, 1997. Special issue on education, L. Lambe, editor. URL: [EKbib/97/Ka97_jsc.pdf](#).
- [91] M. Hitz and E. Kaltofen, editors. *Proc. Second Internat. Symp. Parallel Symbolic Comput. PASCO '97*, New York, N. Y., 1997. ACM Press.
- [90] E. Kaltofen. Blocked iterative sparse linear system solvers for finite fields. In C. Roucairol, editor, *Proc. Symp. Parallel Comput. Solving Large Scale Irregular Applic. (Stratagem '96)*, pages 91–95, Sophia Antipolis, France, 1996. INRIA. URL: [EKbib/96/Ka96_stratagem.ps.gz](#).
- [89] E. Kaltofen and A. Lobo. Distributed matrix-free solution of large sparse linear systems over finite fields. In A. M. Tentner, editor, *Proc. High Performance Computing '96*, pages 244–247, San Diego, CA, 1996. Society for Computer Simulation, Simulation Councils, Inc. Journal version in [102]. URL: [EKbib/96/KaLo96_hpc.pdf](#).
- [88] M. Samadani and E. Kaltofen. On distributed scheduling using load prediction from past information. Unpublished paper, 1996.
- [87] E. Kaltofen and A. Lobo. On rank properties of Toeplitz matrices over finite fields. In *Proc. 1996 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'96)* [-25], pages 241–249. URL: [EKbib/96/KaLo96_issac.pdf](#).
- [86] Ú. Erlingsson, E. Kaltofen, and D. Musser. Generic Gram-Schmidt orthogonalization by exact division. In *Proc. 1996 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'96)* [-25], pages 275–282. URL: [EKbib/96/EKM96.pdf](#).
- [85] E. Kaltofen. Effective Noether irreducibility forms and applications. *J. Comput. System Sci.*, 50(2):274–295, 1995. URL: [EKbib/95/Ka95_jcss.pdf](#).
- [84] A. Díaz, M. Hitz, E. Kaltofen, A. Lobo, and T. Valente. Process scheduling in DSC and the large sparse linear systems challenge. *J. Symbolic Comput.*, 19(1–3):269–282, 1995. URL: [EKbib/95/DHKL95.pdf](#).
- [83] M. A. Hitz and E. Kaltofen. Integer division in residue number systems. *IEEE Trans. Computers*, 44(8):983–989, 1995. URL: [EKbib/95/HiKa95.pdf](#).
- [82] E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. In *Proc. 27th Annual ACM Symp. Theory Comput.*, pages 398–406, New York, N.Y., 1995. ACM Press. Journal version in [97]. URL: [EKbib/95/KaSh95.ps.gz](#).
- [81] A. Díaz and E. Kaltofen. On computing greatest common divisors with polynomials given by black boxes for their evaluation. In *Proc. 1995 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'95)* [-26], pages 232–239. URL: [EKbib/95/DiKa95.ps.gz](#).
- [80] E. Kaltofen. Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems. *Math. Comput.*, 64(210):777–806, 1995. URL: [EKbib/95/Ka95_mathcomp.pdf](#).
- [79] M. Samadani and E. Kaltofen. Prediction based task scheduling in distributed computing. In *Proc. 14th Annual ACM Symp. Principles Distrib. Comput.*, page 261, New York, N. Y., 1995. ACM Press. Brief announcement of [78, 88].
- [78] M. Samadani and E. Kaltofen. Prediction based task scheduling in distributed computing. In B. K. Szymanski and B. Sinharoy, editors, *Languages, Compilers and Run-Time Systems for Scalable Computers*, pages 317–320, Boston, 1996. Kluwer Academic Publ. Poster session paper of [88]. URL: [EKbib/95/SaKa95_poster.ps.gz](#).
- [77] E. Kaltofen. Asymptotically fast solution of Toeplitz-like singular linear systems. In *ISSAC'94* [-27], pages 297–304. Journal version in [80]. URL: [EKbib/94/Ka94_issac.pdf](#).

- [76] E. Kaltofen and A. Lobo. Factoring high-degree polynomials by the black box Berlekamp algorithm. In *ISSAC'94* [-27], pages 90–98. URL: [EKbib/94/KaLo94.ps.gz](#).
- [75] K. C. Chan, A. Díaz, and E. Kaltofen. A distributed approach to problem solving in Maple. In R. J. Lopez, editor, *Maple V: Mathematics and its Application*, Proceedings of the Maple Summer Workshop and Symposium (MSWS'94), pages 13–21, Boston, 1994. Birkhäuser. URL: [EKbib/94/CDK94.ps.gz](#).
- [74] E. Kaltofen and V. Pan. Parallel solution of Toeplitz and Toeplitz-like linear systems over fields of small positive characteristic. In *Proc. First Internat. Symp. Parallel Symbolic Comput. PASC0 '94* [-28], pages 225–233. URL: [EKbib/94/KaPa94.pdf](#).
- [73] E. Kaltofen. Direct proof of a theorem by Kalkbrener, Sweedler, and Taylor. *SIGSAM Bulletin*, 27(4):2, 1993. URL: [EKbib/93/Ka93_sambull.ps.gz](#).
- [72] E. Kaltofen. Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems. In G. Cohen, T. Mora, and O. Moreno, editors, *Proc. AAEECC-10*, volume 673 of *Lect. Notes Comput. Sci.*, pages 195–212, Heidelberg, Germany, 1993. Springer Verlag. Journal version in [80]. URL: [EKbib/93/Ka93_sambull.ps.gz](#).
- [71] A. Díaz, M. Hitz, E. Kaltofen, A. Lobo, and T. Valente. Process scheduling in DSC and the large sparse linear systems challenge. In A. Miola, editor, *Proc. DISCO '93*, volume 722 of *Lect. Notes Comput. Sci.*, pages 66–80, Heidelberg, Germany, 1993. Springer Verlag. Journal version in [84]. URL: [EKbib/93/DHKL93.pdf](#).
- [70] E. Kaltofen. Dynamic parallel evaluation of computation DAGs. In J. Reif, editor, *Synthesis of Parallel Algorithms*, pages 723–758. Morgan Kaufmann Publ., San Mateo, California, 1993. URL: [EKbib/93/Ka93_synthesis.ps.gz](#).
- [69] E. Kaltofen. Computational differentiation and algebraic complexity theory. In C. H. Bischof, A. Griewank, and P. M. Khademi, editors, *Workshop Report on First Theory Institute on Computational Differentiation*, volume ANL/MCS-TM-183 of *Tech. Rep.*, pages 28–30, Argonne, Illinois, December 1993. Argonne National Laboratory. URL: [EKbib/93/Ka93_diff.pdf](#).
- [68] E. Kaltofen. Polynomial factorization 1987-1991. In I. Simon, editor, *Proc. LATIN '92*, volume 583 of *Lect. Notes Comput. Sci.*, pages 294–313, Heidelberg, Germany, 1992. Springer Verlag. URL: [EKbib/92/Ka92_latin.pdf](#).
- [67] E. Kaltofen. On computing determinants of matrices without divisions. In *Proc. 1992 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'92)* [-29], pages 342–349. URL: [EKbib/92/Ka92_issac.pdf](#).
- [66] E. Kaltofen and V. Pan. Processor-efficient parallel solution of linear systems II: the positive characteristic and singular cases. In *Proc. 33rd Annual Symp. Foundations of Comp. Sci.*, pages 714–723, Los Alamitos, California, 1992. IEEE Computer Society Press. URL: [EKbib/92/KaPa92.pdf](#).
- [65] E. Kaltofen. Efficient solution of sparse linear systems. *Lect. Notes, Rensselaer Polytechnic Instit., Dept. Comput. Sci.*, Troy, New York, 1992.
- [64] D. G. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.*, 28(7):693–701, 1991. URL: [EKbib/91/CaKa91.pdf](#).
- [63] E. Kaltofen. Effective Noether irreducibility forms and applications. In *Proc. 22nd Annual ACM Symp. Theory Comput.*, pages 54–63, New York, N.Y., 1991. ACM Press. Journal version in [85].
- [62] E. Kaltofen and V. Pan. Processor efficient parallel solution of linear systems over an abstract field. In *Proc. SPAA '91 3rd Ann. ACM Symp. Parallel Algor. Architecture*, pages 180–191, New York, N.Y., 1991. ACM Press. URL: [EKbib/91/KaPa91.pdf](#).
- [61] A. Díaz, E. Kaltofen, K. Schmitz, and T. Valente. DSC A system for distributed symbolic computation. In *Proc. 1991 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'91)* [-30], pages 323–332. URL: [EKbib/91/DKSV91.pdf](#).
- [60] E. Kaltofen and N. Yui. Explicit construction of Hilbert class fields of imaginary quadratic fields by integer lattice reduction. In D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn, and M. B. Nathanson, editors, *Number Theory New York Seminar 1989–1990*, pages 150–202. Springer Verlag, Heidelberg, Germany, 1991. URL: [EKbib/91/KaYui91.pdf](#).
- [59] E. Kaltofen and M. F. Singer. Size efficient parallel algebraic circuits for partial derivatives. In D. V. Shirkov, V. A. Rostovtsev, and V. P. Gerdt, editors, *IV International Conference on Computer Algebra in Physical Research*, pages 133–145, Singapore, 1991. World Scientific Publ. Co. URL: [EKbib/91/KaSi91.pdf](#).
- [58] E. Kaltofen and B. D. Saunders. On Wiedemann's method of solving sparse linear systems. In H. F. Mattson, T. Mora, and T. R. N. Rao, editors, *Proc. AAEECC-9*, volume 539 of *Lect. Notes Comput. Sci.*, pages 29–38, Heidelberg, Germany, 1991. Springer Verlag. URL: [EKbib/91/KaSa91.pdf](#).

- [57] E. Kaltofen and B. Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *J. Symbolic Comput.*, 9(3):301–320, 1990. URL: [EKbib/90/KaTr90.pdf](#).
- [56] E. Kaltofen. Polynomial factorization 1982-1986. In D. V. Chudnovsky and R. D. Jenks, editors, *Computers in Mathematics*, volume 125 of *Lecture Notes in Pure and Applied Mathematics*, pages 285–309. Marcel Dekker, Inc., New York, N. Y., 1990. URL: [EKbib/90/Ka90_survey.ps.gz](#).
- [55] E. Kaltofen. Computing the irreducible real factors and components of an algebraic curve. *Appl. Algebra Engin. Commun. Comput.*, 1(2):135–148, 1990. URL: [EKbib/90/Ka90_aaecc.pdf](#).
- [54] E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Parallel algorithms for matrix normal forms. *Linear Algebra and Applications*, 136:189–208, 1990. URL: [EKbib/90/KKS90.pdf](#).
- [53] E. Kaltofen, Lakshman Y. N., and J. M. Wiley. Modular rational sparse multivariate polynomial interpolation. In S. Watanabe and M. Nagata, editors, *Proc. 1990 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'90)*, pages 135–139. ACM Press, 1990. URL: [EKbib/90/KLW90.pdf](#).
- [52] D. Rebne and E. Kaltofen. Computer mathematics systems and a trilateral approach to human resource development in technical occupations. In N. Estes, J. Heene, and D. Leclercq, editors, *Proc. 7th International Conference on Technology and Education*, volume 1, pages 251–253, Edinburgh, United Kingdom, 1990. CEP Consultants Ltd.
- [51] E. Kaltofen, editor. *Algebraic Computational Complexity*. Academic Press, London, October 1990. Special issue volume 9, number 3 (March 1990) of *J. Symbolic Comput.*
- [50] E. Kaltofen. Computing the irreducible real factors and components of an algebraic curve. In *Proc. 5th Symp. Comput. Geometry*, pages 79–87. ACM Press, 1989. Journal version in [55].
- [49] E. Kaltofen and S. M. Watt, editors. *Computers and Mathematics*. Springer Verlag, Heidelberg, Germany, 1989.
- [48] E. Kaltofen, T. Valente, and N. Yui. An improved Las Vegas primality test. In *Proc. 1989 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'89)* [-31], pages 26–33. URL: [EKbib/89/KVY89.pdf](#).
- [47] J. Canny, E. Kaltofen, and Lakshman Yagati. Solving systems of non-linear polynomial equations faster. In *Proc. 1989 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'89)* [-31], pages 121–128. URL: [EKbib/89/CKL89.pdf](#).
- [46] E. Kaltofen. Parallel algebraic algorithm design. Lect. Notes, Rensselaer Polytechnic Instit., Dept. Comput. Sci., Troy, New York, July 1989. Tutorial at 1989 Internat. Symp. Symb. Algebraic Comput., Portland, Oregon; contains [45]. URL: [EKbib/89/Ka89_parallel.ps.gz](#).
- [45] E. Kaltofen. Processor efficient parallel computation of polynomial greatest common divisors. Unpublished paper included in [46]. URL: [EKbib/89/Ka89_gcd.ps.gz](#), July 1989.
- [44] E. Kaltofen and H. Rolletschek. Computing greatest common divisors and factorizations in quadratic number fields. *Math. Comput.*, 53(188):697–720, 1989. URL: [EKbib/89/KaRo89.pdf](#).
- [43] E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Mr. Smith goes to Las Vegas: Randomized parallel computation of the Smith normal form of polynomial matrices. In J. H. Davenport, editor, *Proc. EUROCAL '87*, volume 378 of *Lect. Notes Comput. Sci.*, pages 317–322, Heidelberg, Germany, 1989. Springer Verlag. Journal version in [54].
- [42] E. Kaltofen. Factorization of polynomials given by straight-line programs. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 375–412. JAI Press Inc., Greenwich, Connecticut, 1989. URL: [EKbib/89/Ka89_slpfac.pdf](#).
- [41] B. Gregory and E. Kaltofen. Analysis of the binary complexity of asymptotically fast algorithms for linear system solving. *SIGSAM Bulletin*, 22(2):41–49, April 1988. URL: [EKbib/88/GrKa88.pdf](#).
- [40] T. S. Freeman, G. Imirzian, E. Kaltofen, and Lakshman Yagati. DAGWOOD: A system for manipulating polynomials given by straight-line programs. *ACM Trans. Math. Software*, 14(3):218–240, 1988. URL: [EKbib/88/FIKY88.pdf](#).
- [39] E. Kaltofen. Greatest common divisors of polynomials given by straight-line programs. *J. ACM*, 35(1):231–264, 1988. URL: [EKbib/88/Ka88_jacm.pdf](#).
- [38] E. Kaltofen and Lakshman Yagati. Improved sparse multivariate polynomial interpolation algorithms. In *Symbolic Algebraic Comput. Internat. Symp. ISSAC '88 Proc.* [-32], pages 467–474. URL: [EKbib/88/KaLa88.pdf](#).
- [37] G. L. Miller, V. Ramachandran, and E. Kaltofen. Efficient parallel evaluation of straight-line code and arithmetic circuits. *SIAM J. Comput.*, 17(4):687–695, 1988. URL: [EKbib/88/MRK88.pdf](#).

- [36] E. Kaltofen and B. Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. In *Proc. 29th Annual Symp. Foundations of Comp. Sci.*, pages 296–305. IEEE, 1988. Journal version in [57].
- [35] E. Kaltofen. Deterministic irreducibility testing of polynomials over large finite fields. *J. Symbolic Comput.*, 4:77–82, 1987. URL: [EKbib/87/Ka87_jsc.ps.gz](#).
- [34] E. Kaltofen. Single-factor Hensel lifting and its application to the straight-line complexity of certain polynomials. In *Proc. 19th Annual ACM Symp. Theory Comput.*, pages 443–452. ACM, 1987. URL: [EKbib/87/Ka87_stoc.pdf](#).
- [33] E. Kaltofen. Computer algebra algorithms. In J. F. Traub, editor, *Annual Review in Computer Science*, volume 2, pages 91–118. Annual Reviews Inc., Palo Alto, California, 1987. URL: [EKbib/87/Ka87_annrev.pdf](#).
- [32] E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Fast parallel computation of Hermite and Smith forms of polynomial matrices. *SIAM J. Alg. Discrete Math.*, 8:683–690, 1987. URL: [EKbib/87/KKS87.pdf](#).
- [31] E. Kaltofen. Uniform closure properties of p-computable functions. In *Proc. 18th Annual ACM Symp. Theory Comput.*, pages 330–337. ACM, 1986. Also published as part of [39] and [42]. URL: [EKbib/86/Ka86_stoc.pdf](#).
- [30] E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Fast parallel algorithms for similarity of matrices. In *Proc. 1986 Symp. Symbolic Algebraic Comput. (Symsac '86)* [-33], pages 65–70. Journal version in [32] and [54].
- [29] T. S. Freeman, G. Imirzian, E. Kaltofen, and Lakshman Yagati. DAGWOOD: A system for manipulating polynomials given by straight-line programs. In *Proc. 1986 Symp. Symbolic Algebraic Comput. (Symsac '86)* [-33], pages 169–175. Journal version in [40].
- [28] G. L. Miller, V. Ramachandran, and E. Kaltofen. Efficient parallel evaluation of straight-line code and arithmetic circuits. In *Proc. Second International Workshop on Parallel Computing and VLSI – AWOC '86*, volume 227 of *Lect. Notes Comput. Sci.*, pages 236–245, 1986. Journal version in [37].
- [27] Joachim von zur Gathen and E. Kaltofen. Factoring multivariate polynomials over finite fields. *Math. Comput.*, 45:251–261, 1985. URL: [EKbib/85/GaKa85_mathcomp.ps.gz](#).
- [26] Joachim von zur Gathen and E. Kaltofen. Factoring sparse multivariate polynomials. *J. Comput. System Sci.*, 31:265–287, 1985.
- [25] E. Kaltofen. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM J. Comput.*, 14(2):469–489, 1985. URL: [EKbib/85/Ka85_sicomp.pdf](#).
- [24] E. Kaltofen. Computing with polynomials given by straight-line programs I; greatest common divisors. In *Proc. 17th Annual ACM Symp. Theory Comput.*, pages 131–142. ACM, 1985. Also published as part of [39] and [42].
- [23] E. Kaltofen. Sparse Hensel lifting. In *EUROCAL 85 European Conf. Comput. Algebra Proc. Vol. 2* [-34], pages 4–17. Proofs in [22]. URL: [EKbib/85/Ka85_eurocal.pdf](#).
- [22] E. Kaltofen. Sparse Hensel lifting. Technical Report 85-12, Rensselaer Polytechnic Instit., Dept. Comput. Sci., Troy, N. Y., 1985. URL: [EKbib/85/Ka85_techrep.pdf](#).
- [21] E. Kaltofen and H. Rolletschek. Computing greatest common divisors and factorizations in quadratic number fields. In *EUROCAL 85 European Conf. Comput. Algebra Proc. Vol. 2* [-34], pages 279–288. Journal version in [44].
- [20] E. Kaltofen. Computing with polynomials given by straight-line programs II; sparse factorization. In *Proc. 26th Annual Symp. Foundations of Comp. Sci.*, pages 451–458. IEEE, 1985. URL: [EKbib/85/Ka85_focs.ps.gz](#).
- [19] E. Kaltofen. Fast parallel absolute irreducibility testing. *J. Symbolic Comput.*, 1(1):57–67, 1985. Misprint corrections: *J. Symbolic Comput.* vol. 9, p. 320 (1989). URL: [EKbib/85/Ka85_jsc.pdf](#).
- [18] E. Kaltofen. Effective Hilbert irreducibility. *Information and Control*, 66:123–137, 1985. URL: [EKbib/85/Ka85_infcontr.ps.gz](#).
- [17] E. Kaltofen and V. Pan. The integer manipulation techniques can compete with the linear algebra methods for solving sparse linear systems. Tech. Rep. 85-6, State Univ. of New York at Albany, Comp. Sci. Dept., 1985.
- [16] E. Kaltofen. The algebraic theory of integration. *Lect. Notes*, Rensselaer Polytechnic Instit., Dept. Comput. Sci., Troy, New York, 1984. URL: [EKbib/84/Ka84_integration.pdf](#).
- [15] E. Kaltofen. Effective Hilbert irreducibility. In *Proc. EUROSAM '84* [-35], pages 275–284. Journal version in [18].

- [14] E. Kaltofen and N. Yui. Explicit construction of the Hilbert class field of imaginary quadratic fields with class number 7 and 11. In *Proc. EUROSAM '84* [-35], pages 310–320. URL: EKBib/84/KaYui84_eurosam.ps.gz.
- [13] E. Kaltofen. A note on the Risch differential equation. In *Proc. EUROSAM '84* [-35], pages 359–366. URL: EKBib/84/Ka84_risch.ps.gz.
- [12] E. Kaltofen and N. Yui. The modular equation of order 11. In *Third Macsyma Users' Conference*, pages 472–485. General Electric, 1984.
- [11] E. Kaltofen. On a theorem by R. Dedekind. In H. W. Lenstra, Jr., J. K. Lenstra, and P. van Emde Boas, editors, *DOPO LE PAROLE*. Album in Honor of A. K. Lenstra's Doctorate, Amsterdam, May 1984.
- [10] E. Kaltofen. On the complexity of finding short vectors in integer lattices. In *Proc. EUROCAL '83*, volume 162 of *Lect. Notes Comput. Sci.*, pages 236–244, Heidelberg, Germany, 1983. Springer Verlag. URL: EKBib/83/Ka83_eurocal.pdf.
- [9] Joachim von zur Gathen and E. Kaltofen. Factoring multivariate polynomials over finite fields. In *Proc. 1983 ICALP*, volume 154 of *Lect. Notes Comput. Sci.*, pages 250–263, Heidelberg, Germany, 1983. Springer Verlag. Journal version in [27].
- [8] E. Kaltofen, D. R. Musser, and B. D. Saunders. A generalized class of polynomials that are hard to factor. *SIAM J. Comput.*, 12(3):473–485, 1983. Also chapter 2.2 in [4].
- [7] E. Kaltofen. Polynomial factorization. In B. Buchberger, G. Collins, and R. Loos, editors, *Computer Algebra*, pages 95–113. Springer Verlag, Heidelberg, Germany, 2 edition, 1982. URL: EKBib/82/Ka82_survey.ps.gz.
- [6] E. Kaltofen. A polynomial-time reduction from bivariate to univariate integral polynomial factorization. In *Proc. 23rd Annual Symp. Foundations of Comp. Sci.*, pages 57–64. IEEE, 1982. Journal version in [25]. URL: EKBib/82/Ka82_focs.pdf.
- [5] E. Kaltofen. A polynomial reduction from multivariate to bivariate integral polynomial factorization. In *Proc. 14th Annual ACM Symp. Theory Comput.*, pages 261–266. ACM, 1982. Journal version in [25].
- [4] E. Kaltofen. *On the complexity of factoring polynomials with integer coefficients*. PhD thesis, Rensselaer Polytechnic Instit., Troy, N. Y., December 1982. See also [7, 8, 25]. URL: EKBib/82/Ka82_thesis.pdf.
- [3] E. Kaltofen, D. R. Musser, and B. D. Saunders. A generalized class of polynomials that are hard to factor. In *Proc. 1981 ACM Symp. Symbolic and Algebraic Comput.*, pages 188–194. ACM, 1981. Journal version in [8].
- [2] E. Kaltofen and S. K. Abdali. An attributed LL(1) compilation of Pascal into the lambda-calculus. Technical Report CS-8103, Rensselaer Polytechnic Instit., Math. Sci. Dept., Troy, N. Y., 1981.
- [1] E. Kaltofen. *LISP/370 under the Michigan Terminal System*. Rensselaer Polytechnic Instit., Math. Sci. Dept., Troy, N. Y., August 1980.
-
- Books where papers are located
- [-1] Björn Enquist, editor. *Encyclopedia of Applied and Computational Mathematics*. Springer, 2012, to appear. Mathematics of Computer Science, Discrete Mathematics, Håstad, Johan (field editor).
- [-2] Gary L. Mullen and Daniel Panario, editors. *Handbook of Finite Fields*. CRC Press, 2012, to appear.
- [-3] M. Moreno Maza, editor. *SNC'11 Proc. 2011 Internat. Workshop on Symbolic-Numeric Comput.*, New York, N. Y., 2011. Association for Computing Machinery.
- [-4] Anton Leykin, editor. *Proc. 2011 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2011*, New York, N. Y., 2011. Association for Computing Machinery.
- [-5] Christoph Dürr and Thomas Schwentick, editors. *Proc. 28th Internat. Symp. on Theoretical Aspects of Computer Science, STACS 2011*, LIPIcs. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Germany, 2011.
- [-6] M. Moreno Maza and Jean-Louis Roch, editors. *PASCO'10 Proc. 2010 Internat. Workshop on Parallel Symbolic Comput.*, New York, N. Y., 2010. ACM.
- [-7] Stephen M. Watt, editor. *Proc. 2010 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2010*, New York, N. Y., 2010. Association for Computing Machinery.
- [-8] Hiroshi Kai and Hiroshi Sekigawa, editors. *SNC'09 Proc. 2009 Internat. Workshop on Symbolic-Numeric Comput.*, New York, N. Y., 2009. ACM Press.
- [-9] David Jeffrey, editor. *ISSAC 2008*, New York, N. Y., 2008. ACM Press.
- [-10] Christopher W. Brown, editor. *ISSAC 2007 Proc. 2007 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2007. ACM Press.
- [-11] Jan Verschelde and Stephen M. Watt, editors. *SNC'07 Proc. 2007 Internat. Workshop on Symbolic-Numeric Comput.*, New York, N. Y., 2007. ACM Press.
- [-12] Dongming Wang and Lihong Zhi, editors. *Symbolic-Numeric Computation*. Trends in Mathematics. Birkhäuser Verlag, Basel, Switzerland, 2007.
- [-13] Jean-Guillaume Dumas, editor. *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2006. ACM Press.

- [14] Manuel Kauers, editor. *ISSAC'05 Proc. 2005 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2005. ACM Press.
- [15] Dongming Wang and Lihong Zhi, editors. *Internat. Workshop on Symbolic-Numeric Comput. SNC 2005 Proc.*, 2005. Distributed at the Workshop in Xi'an, China, July 19–21.
- [16] Jaime Gutierrez, editor. *ISSAC 2004 Proc. 2004 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2004. ACM Press.
- [17] J. R. Sendra, editor. *ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2003. ACM Press.
- [18] Arjeh M. Cohen, Xiao-Shan Gao, and Nobuki Takayama, editors. *Proc. First Internat. Congress Math. Software ICMS 2002, Beijing, China*, Singapore, 2002. World Scientific.
- [19] T. Mora, editor. *ISSAC 2002 Proc. 2002 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2002. ACM Press.
- [20] Kiyoshi Shirayanagi and Kazuhiro Yokoyama, editors. *Computer Mathematics Proc. Fifth Asian Symposium (ASCM 2001)*, volume 9 of *Lecture Notes Series on Computing*, Singapore, 2001. World Scientific.
- [21] C. Traverso, editor. *Internat. Symp. Symbolic Algebraic Comput. ISSAC 2000 Proc. 2000 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2000. ACM Press.
- [22] S. Dooley, editor. *ISSAC 99 Proc. 1999 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1999. ACM Press.
- [23] O. Gloor, editor. *ISSAC 98 Proc. 1998 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1998. ACM Press.
- [24] W. Küchlin, editor. *ISSAC 97 Proc. 1997 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1997. ACM Press.
- [25] Lakshman Y. N., editor. *ISSAC 96 Proc. 1996 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1996. ACM Press.
- [26] A. H. M. Levelt, editor. *Proc. 1995 Internat. Symp. Symbolic Algebraic Comput. ISSAC'95*, New York, N. Y., 1995. ACM Press.
- [27] *ISSAC '94 Proc. Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1994. ACM Press.
- [28] H. Hong, editor. *First Internat. Symp. Parallel Symbolic Comput. PASCO '94*, Singapore, 1994. World Scientific Publishing Co.
- [29] P. S. Wang, editor. *Internat. Symp. Symbolic Algebraic Comput. 92*, New York, N. Y., 1992. ACM Press.
- [30] S. M. Watt, editor. *Proc. 1991 Internat. Symp. Symbolic Algebraic Comput. ISSAC'91*, New York, N. Y., 1991. ACM Press.
- [31] *Proc. ACM-SIGSAM 1989 Internat. Symp. Symbolic Algebraic Comput. ISSAC '89*, New York, N. Y., 1989. ACM Press.
- [32] P. Gianni, editor. *Symbolic Algebraic Comput. Internat. Symp. ISSAC '88 Proc.*, volume 358 of *Lect. Notes Comput. Sci.*, Heidelberg, Germany, 1988. Springer Verlag.
- [33] B. W. Char, editor. *Proc. 1986 Symp. Symbolic Algebraic Comput. Symsac '86*, New York, N. Y., 1986. ACM.
- [34] B. F. Caviness, editor. *EUROCAL 85 European Conf. Comput. Algebra Proc. Vol. 2*, Lect. Notes Comput. Sci., Heidelberg, Germany, 1985. Springer Verlag.
- [35] J. Fitch, editor. *EUROSAM 84 Internat. Symp. Symbolic Algebraic Comput. Proc.*, Lect. Notes Comput. Sci., Heidelberg, Germany, 1984. Springer Verlag.

Courses That Erich Kaltofen Has Taught

1 Graduate Courses (32 semester-long courses total)

- MA-792, MA-591**, *Topics in Symbolic Computation*, North Carolina State Univ., **Spring 2007**, Spring 2003, Spring 2002 (co-taught with Hoon Hong), Spring 2001 (co-taught with Michael F. Singer).
- MA-792**, *Special Topics: Advanced Programming for Mathematicians*, North Carolina State Univ., **Spring 2011**; 7 lectures on Python taught by Mark Lavin. **Spring 2008**.
- MA-591**, *Special Topics: The C/C++/Java Programming Languages*, North Carolina State Univ., **Fall 2004**; 9 lectures on Javascript taught by Hoon Hong. **Fall 2003**.
- MA-591**, *Programming Languages for Mathematicians*, North Carolina State Univ., **Fall 2002**, **Fall 2000**, **Fall 1999**, and **Fall 1998**.
- MA-581/CSC-691**, *Topics in Symbolic Mathematical Computation*, North Carolina State Univ., **Fall 1996**.
- MA-522**, *Computer Algebra*, North Carolina State Univ., **Fall 2009**; **Fall 2006**; Fall 2004; taught 9 lectures. Fall 2001; co-taught with Hoon Hong.
- 66-6240**, *Symbolic Mathematical Computation*, Rensselaer Polytech. Inst., **Fall 1991**, Spring 1989, Spring 1987, and Spring 1985.
- 66-6965**, *Parallel Algorithm Design*, Rensselaer Polytech. Inst., **Spring 1995** (video course), **Spring 1994**, Spring 1992, and Fall 1988.
- 66-6090**, *Advanced Programming*, Rensselaer Polytech. Inst., Fall 1987.
- 66-6210**, *Analysis of Algorithms*, Rensselaer Polytech. Inst., Fall 1990, Fall 1986, and Fall 1984.
- 66-6962**, *Complexity Theory*, Rensselaer Polytech. Inst., Spring 1984.
- CSC 2412**, *Applied Algebra*, Univ. of Toronto, **Spring 1991 (one of three parts)**, and Spring 1983.
- CSC 2429**, *Topics in Theory of Computation*, Univ. of Toronto, **Fall 1983**.

2 Undergraduate Courses (59 semester-long courses total)

- MA-410 (senior)**, *Theory of Numbers*, North Carolina State Univ., **Spring 2012**, **Spring 2011**, **Spring 2010**, **Spring 2009**, **Spring 2008**, **Spring 2007** and **Spring 2005**.
- MA-405 (senior)**, *Linear Algebra and Matrices*, North Carolina State Univ., **Spring 2012**, **Spring 2009** and **Spring 1996**.
- 66-496 (senior)**, *Computational Abstract Algebra*, Rensselaer Polytech. Inst., **Spring 1990**.
- 66-436 (senior)**, *Data Structures*, Rensselaer Polytech. Inst., **Fall 1995**, **Fall 1994**, **Fall 1993**, 2 sections in **Fall 1992**, **Spring 1992**, **Fall 1988**, and **Spring 1988**.
- MA-351 (junior)**, *Introduction to Discrete Mathematical Models*, North Carolina State Univ., **Fall 2011**, **Fall 2010**, **Fall 2009**, **Fall 2008**, **Fall 2007**, **Fall 2006**, **Fall 2004**, **Fall 2003**, **Fall 2002**, **Fall 2001**, **Fall 1999**.
- MA-305 (junior)**, *Elementary Linear Algebra*, North Carolina State Univ., **Spring 2004** (Internet course), **Spring 2003** (Internet course), **Spring 2002** (Internet course), **Spring 2001** (Internet course), **Spring 2000** (Internet course), **Spring 1998** (Internet course), **Fall 1997** (Internet course), and **Spring 1997**. Icon used by MIT OpenCourseware project.
- CSC-311 (junior)**, *Data Structures*, North Carolina State Univ., **Fall 1996**
- CSC 364 (junior)**, *Effective and Efficient Computing*, Univ. of Toronto at Erindale, Spring 1983.

CSC 348 (junior), *Introduction to Algebra and Algebraic Computing*, Univ. of Toronto at Erindale, Fall 1982 and Fall 1983.

66-209 (sophomore), *Computing Languages*, Rensselaer Polytechnic Inst., **Fall 1994**, **Fall 1993**, **Summer 1993** (C++ segment), **Spring 1993**, Fall 1990, and 2 sections in Fall 1989; LISP segments of four sections: Fall 1986, Spring 1985, Fall 1984, and Spring 1984.

CSC 139 (freshman), *Introduction to Computer Programming*, Univ. of Toronto at Erindale, Fall 1982.

CIS 171 (freshman), *Introduction to Computer Science II*, Univ. of Delaware, 3 sections in Spring 1982.

CIS 170 (freshman), *Introduction to Computer Science I*, Univ. of Delaware, 3 sections in Fall 1981.

3 High School Summer Camps (5 summers)

Symbolic Computation Systems for Young Scholars: Development and Industrial Applications Rensselaer Polytechnic Inst. Summer 1990, 1991, 1992, 1994, and **1995**.

Grants Awarded To Erich Kaltofen

1 Individual Grants

AF:Small: Efficient Exact/Certified Symbolic Computation By Hybrid Symbolic-Numeric and Parallel Methods, National Science Foundation, 2011-2014, \$425,000.

Model Discovery and Verification With Symbolic, Hybrid Symbolic-Numeric and Parallel Computation, National Science Foundation, 2008-2011, \$300,000.

Workshop on Advanced Cyber-Enabled Discovery & Innovation (CDI) Through Symbolic and Numeric Computation, National Science Foundation, 2007-2009, \$40,905.

Challenges in Linear and Polynomial Algebra in Symbolic Computation Algorithms, National Science Foundation, 2005-2009, \$329,371.

Fast Bit Complexity in Symbolic Computation Algorithms, National Science Foundation, 2003-2006, \$310,604.

Optimization, Randomization, and Generalization in Symbolic Computation, National Science Foundation, 2000-2003, \$262,153.

Multi-Use "Plug-And-Play" Software Packages for Black Box and Inexact Symbolic Objects, National Science Foundation, 1997-2000, \$215,233.

Project 25: Internet Course Development, North Carolina State University, 1997, \$13,750.

Efficient Computer Algorithms for Symbolic Mathematics. National Science Foundation, 1994-1997, \$227,069.

Efficient Computer Algorithms for Symbolic Mathematics. National Science Foundation, 1991-1994, \$191,000. Research Experiences for an Undergraduate supplement, Summer 1993 and 1994, \$5,000.

Efficient Las Vegas Primality Testing. National Security Agency, 1990, \$18,700.

Studies on the Sequential and Parallel Complexity of Computer Algebra Problems. National Science Foundation, 1987-1990, \$132,600. Pittsburgh NSF Supercomputing Center supplement, 1988-1990.

Computational Abstract Algebra. Educational supplement to previous grant, 1990, \$9,690.

Computer Algebra Development Equipment. Tektronix Inc., 1985, \$15,000; upgrade 1988, \$11,000.

Complexity Year. Fellowship, Mathematical Sciences Research Institute, 1985, \$14,350.

Complexity Studies in Computer Algebra. National Science Foundation, 1985-1986, \$55,000.

Efficient Algorithms for Diophantine Problems with Emphasis on Polynomial Factorization. Natural Sciences and Engineering Research Council of Canada, 1983, CD\$10,000.

Efficient Algorithms for Factoring Polynomials and Computing Galois Groups. Connaught Fund (University of Toronto), 1983, CD\$16,000.

2 Shared Grants

Ky and Yu-Fen Fan Fund Travel Grant, American Mathematical Society, 2010, \$3,500; for Dr. Zhengfeng Yang's visit to North Carolina State University.

MSRI Workshop on Hybrid Methodologies for Symbolic-Numeric Computation, Society for Industrial and Applied Mathematics as part of SIAM's NSF block grant, 2010, \$19,700; with Mark Giesbrecht, Daniel Lichtblau, Seth Sullivant, and Lihong Zhi.

Scientific Computing Research Environments for the Mathematical Sciences (SCREMS): Parallel Computer Algebra. National Science Foundation, 2005-2008, \$90,000; with Aloysius Helminck, Hoon Hong, Irina Kogan, Michael Singer and Agnes Szanto.

Workshops for NCSU/China Research and Educational Partnership In Symbolic Computation, National Science Foundation, 2005-2007, \$23,320; with Michael Singer, Hoon Hong and Agnes Szanto.

International Conference on Applied Computer Algebra National Science Foundation, 2003, \$10,000; with Hoon Hong and Agnes Szanto.

ITR/ACS: Collaborative Research LinBox: A Generic Library for Exact Black Box Linear Algebra National Science Foundation, 2001-2004, \$370,000; with Carl D. Meyer; University of Delaware: Bobby F. Caviness, B. David Saunders, Qing Xiang; Washington College (Maryland): Austin A. Lobo.

Scientific Computing Research Environments for the Mathematical Sciences. National Science Foundation, 1999-2002, \$49,735; with Aloysius Helminck, Hoon Hong, and Michael Singer.

East Coast Computer Algebra Day. National Science Foundation, 1998, \$8,900; with Hoon Hong and Michael Singer.

Theory and Practice of Parallel Linear Algebra in Computer Algebra. National Science Foundation, 1998-2001, travel support to Grenoble, France, with B. D. Saunders and A. A. Lobo at the University of Delaware, \$17,500.

East Coast Computer Algebra Day. National Science Foundation, 1996, \$8,240; with S. Dooley and B. Trager.

Enhancements for a Young Scholars Program. Strategic Initiatives, Rensselaer Polytechnic Institute, 1994, \$15,000; with M. S. Krishnamoorthy and D. Rebne.

Symbolic Computation Systems for Young Scholars: Development and Industrial Applications. National Science Foundation, 1994–1995, \$59,214; with M. S. Krishnamoorthy and D. Rebne.

Symbolic Computation Systems for Young Scholars. IBM and Center for Innovative Undergraduate Education at Rensselaer Polytechnic Institute, 1992, \$8,000; with M. S. Krishnamoorthy and D. Rebne.

A Workshop on Integrated Symbolic-Numeric Computing at ISSAC '92. National Science Foundation, 1992, \$10,000; submitted on behalf of the ISSAC '92 organizing committee as conference chairman.

CISE 1991 Minority Graduate Fellowship Honorable Mention. National Science Foundation, 1991–1992, \$6,000; with Angel Díaz.

Computationally Efficient Algebraic Methods for Solving Geometric Modeling Problems. New York State Center for Advanced Technology in Automation and Robotics, 1990, \$7,098; with Lakshman Y. N.

Symbolic Computation Systems for Young Scholars: Development and Industrial Applications. National Science Foundation, 1990–91, \$62,000; with D. Rebne.

Research Experience in Computer Science for Undergraduates. National Science Foundation, 1989–91, \$120,000, shared with 10 others; project director R. Ingalls.

Computing Environments for Mathematical Applications. National Science Foundation, CISE infrastructure grant, 1988–93, \$2,000,000, shared with 20 others; project directors J. Flaherty and J. Modestino.

Integrating Undergraduate Research into the Computer Science Department. National Science Foundation, 1987, \$40,000, shared with 10 others; project director R. Ingalls.

Computer Research Equipment. National Science Foundation, 1985, \$80,000, shared with four others.

Scientific Computation Group. Natural Sciences and Engineering Research Council of Canada, 1983, CD\$62,000, shared with nine others; project director K. R. Jackson.

Erich Kaltofen's Service External To The University

1 Offices in professional organizations

- ACM Special Interest Group for Symbolic and Algebraic Manipulation: Chair 1993-95, Vice-chair 1987–89, Secretary 1985–87, Advisory Board 2003–04.
- ACM/SIGSAM 2011 Richard D. Jenks Memorial Prize for Excellence in Computer Algebra Software Engineering, Chair of the selection committee.
- Nominating committee ACM Special Interest Group on Symbolic & Algebraic Manipulation, Chair 1996, Member 2007.
- ACM National Lecturer, 1989–91.

2 Editorships of journals, books, and proceedings

- Member of the editorial board, *Journal of Symbolic Computation*, since 1988.
- Associate editor, *Applicable Algebra in Engineering, Communication and Computing*, since 1990.
- Scientific advisory board member, *Oberwolfach References on Mathematical Software – ORMS*, since 2005.
- Co-editor, *Computer Algebra Handbook*, Springer Verlag, 2002; with Johannes Grabmeier and Volker Weispfenning.
- Co-editor, *Proceedings Second International Symposium on Parallel Symbolic Computation*, ACM Press, July 1997; with Markus A. Hitz.
- Associate editor, *SIAM Journal on Computing*, 1988–1991.
- Guest editor, *Journal of Symbolic Computation*, for a special issue on ‘Algebraic Computational Complexity,’ March 1990. Also appeared as paperback in October 1990.
- Co-editor, *Proceedings of Computers and Mathematics 1989*, Springer Verlag, June 1989; with Stephen Watt.

3 Offices in professional conferences

3.1 General conference (co-)chair

- Co-organizer with Mark Giesbrecht, Daniel Lichtblau and Lihong Zhi, “**Hybrid Methodologies for Symbolic-Numeric Computation**,” SIAM-NSF-MSRI Special Workshop, Mathematical Sciences Research Institute (MSRI), Berkeley, California, November 17–19, 2010.
- Co-organizer with B. Malcolm Brown, Shin’ichi Oishi and Siegfried M. Rump “**Computer-assisted Proofs — Tools, Methods and Applications**,” 5-Day Seminar at the **Schloss Dagstuhl International Conference and Research Center for Computer Science**, Germany, November 2009.
- Co-organizer with Lenore Mullin “**NSF Workshop on Future Directions of Symbolic Computation Research And Their Applications to the Domain Sciences**,” 1 and 1/2-Day Workshop at the University of Rhode Island, April 30–May 1, 2009.
- Co-organizer with Lenore Mullin and Alvin Thaler “**NSF CDI Workshop on The Role of Symbolic, Numeric and Algebraic Computation in Cyber-Enabled Discovery and Innovation (CDI)**,” 1 and 1/2-Day Workshop at the **National Science Foundation**, Arlington, Virginia, October 2007.
- Co-organizer with Wolfram Decker, Michael Dewar and Stephen Watt “**Challenges in Symbolic Computation Software**,” 5-Day Seminar at the **Schloss Dagstuhl International Conference and Research Center for Computer Science**, Germany, July 2006.

- Co-organizer with Shuhong Gao, Mark van Hoeij and Victor Shoup “The Computational Complexity of Polynomial Factorization,” 5-Day Workshop at the American Institute of Mathematics Research Conference Center, Palo Alto, California, May 2006.
- Co-organizer with Wolfram Decker, Keith Geddes and Stephen Watt “Challenges,” in Linear and Polynomial Algebra in Symbolic Computation Software 5-Day Workshop at the Banff International Research Station (BIRS), Canada, October 2005.
- Co-organizer with Hoon Hong and Agnes Szanto of the “International Conference on Applications of Computer Algebra ACA 2003,” North Carolina State University, July 2003.
- “International Symposium on Symbolic and Algebraic Computation (ISSAC),” London, Ontario, Canada, July 2001.
- Co-organizer with H. Hong and M. Singer of the “East Coast Computer Algebra Day,” North Carolina State University, April 1999.
- “International Symposium on Symbolic and Algebraic Computation (ISSAC),” Berkeley, California, July 1992.
- Co-organizer with M. Singer and R. Zippel of the workshop “Parallel Algebraic Computation,” Mathematical Sciences Institute, Cornell University, May 1990.
- Co-organizer with C. Hoffmann and C. Yap of the workshop “Algorithms in Algebra and Geometry,” Mathematical Sciences Institute, Cornell University, July 1988.

3.2 Program committee (co-)chair

- 2009 International Symposium on Symbolic and Algebraic Computation ISSAC’09, Korea Institute for Advanced Study, Seoul, Korea, July 28-31, 2009
- Second International Symposium on Parallel Symbolic Computation (PASCO’97), Maui, July 1997.
- Computers & Mathematics, MIT, June 1989.
- Coordinator for North America and program committee member, 1988 International Conference on Symbolic and Algebraic Computation, Rome, Italy, July 1988.

3.3 Conference organization committee member

- Organizing committee member with Mark Giesbrecht (chair), George Labahn, Daniel Lichtblau, and Lihong Zhi of the Fields Institute Workshop on Hybrid Methodologies for Symbolic-Numeric Computation, Waterloo, Canada, November 2011.
- Local arrangements committee member, SIAM Conference on Applied Algebraic Geometry 2011, Raleigh, October 2011.
- Organizing committee member with Bruce Char, Victoria Powers (chair) and Stephen M. Watt of the “East Coast Computer Algebra Day,” Emory University, May 15, 2010.
- Organizing committee member with B. Char, Ed Lamagna (chair) and B. David Saunders of the “East Coast Computer Algebra Day,” University of Rhode Island, May 2009.
- Organizing committee member, Interactive Parallel Computation in Support of Research in Algebra, Geometry and Number Theory, Mathematical Sciences Research Institute (MSRI), Berkeley, California, January 29–February 2, 2007.
- Steering committee, International Workshop on Symbolic-Numeric Computation (SNC), elected to member for the term 2005-2007.
- Scientific committee member, IMACS Conferences on Applications of Computer Algebra (ACA), October 1998–present.
- Steering committee, International Symposium on Symbolic and Algebraic Computation (ISSAC), elected to member-at-large for the term 2002-2005; elected chair 2004-2005.

- Advisory council, [East Coast Computer Algebra Day 2005](#), Ashland University, Ohio, April 2005.
- Advisory committee member, [East Coast Computer Algebra Day 2004](#), Wilfried Laurier University, Waterloo Canada, May 2004.
- Advisory board member, East Coast Computer Algebra Day 2003, Clemson University, April 2003.
- Advisory board member, [Euro-Par](#), October 1999–present.
- Scientific committee member, [International Symposium on Applications of Computer Algebra \(ISACA2000\)](#), Goa, India, October 2000.
- Proposal writer for the East Coast Computer Algebra Day (ECCAD'96), IBM T. J. Watson Research Center.

3.4 Special session organizer

- Co-organizer with Angel Díaz of the special session “Mathematics on the Internet,” IMACS Conference on Applications of Computer Algebra (ACA), Madrid, Spain, June 1999.
- Co-organizer with Gilles Villard of the special session “Parallel Computer Algebra,” IMACS Conference on Applications of Computer Algebra (ACA), Albuquerque, New Mexico, May 1995.

3.5 Program committee member

- [SIAM Conference on Applied Algebraic Geometry 2011](#), Raleigh, October 2011.
- [Symbolic-Numeric Computation SNC 2011](#), San Jose, July 2011.
- [Algebraic and Numeric Biology ANB 2010](#), RISC, Castle of Hagenberg, Austria, July 2010.
- [Parallel Symbolic Computation PASCO'10](#), Grenoble, France, July 2010.
- [Parallel Computer Algebra PARCA 2010](#), Tambov State University, Russia, June 2010.
- [Milestones in Computer Algebra MICA 2008: A Conference in Honour of Keith Geddes' 60th Birthday](#), Stonehaven Bay, Trinidad and Tobago, May 2008.
- [Algebraic Biology 2008](#), RISC, Castle of Hagenberg, Austria, July 2008.
- [Parallel Symbolic Computation PASCO'07](#), University of Western Ontario, Canada, July 2007.
- [Algebraic Biology 2007](#), RISC, Castle of Hagenberg, Austria, July 2007.
- [The Third IASTED International Conference on Advances in Computer Science and Technology ACST 2007](#) Phuket, Thailand, April 2007.
- [International Symposium on Symbolic and Algebraic Computation ISSAC 2006](#), Genova, Italy, July 2006.
- [International Workshop on Symbolic-Numeric Computation](#), Xi'an, China, July 2005.
- [International Symposium on Symbolic and Algebraic Computation ISSAC 2004](#), Santander, Spain, July 2004.
- [15th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes](#), Toulouse, France, May 2003.
- [International Symposium on Symbolic and Algebraic Computation ISSAC 2002](#), Lille, France, July 2002.
- 14th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes, Melbourne, Australia, November 2001.
- [International Symposium on Symbolic and Algebraic Computation ISSAC 2000](#), St. Andrews, Scotland, August 2000.
- [13th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes](#), Honolulu, November 1999.

- [EURO-PAR'99](#), Toulouse, France, August 1999.
- 28th ACM Symposium on the Theory of Computing (STOC), Philadelphia, 1996.
- CONPAR 94 - VAPP VI, J. Kepler University, Linz, Austria, September 1994.
- Symposium on Quantifier Elimination and Cylindrical Algebraic Decomposition, Research Institute for Symbolic Computation, Linz, Austria, October 1993.
- International Symposium on Symbolic and Algebraic Computation, Tokyo, Japan, August 1990.
- 1986 ACM Symposium for Symbolic and Algebraic Computation, Waterloo, Canada, July 1986.

3.6 Invited speaker

See Invited Lectures by Erich Kaltofen on page [28](#).

3.7 Panel member

- ‘Forward Looking Session’ panel at the “SIAM Conference on Applied Algebraic Geometry [AAG '11](#),” Raleigh, October 8, 2011.
- ‘Trends in symbolic computation development and applications’ panel at the “International Conference on Applications of Computer Algebra [ACA 2003](#),” Houston, June 2011.
- Panel at the conclusion of [SIAM/MSRI Workshop](#) on Hybrid Methodologies for Symbolic-Numeric Computation, Berkeley, November 19, 2010.
- ‘The Spectacular Successes and Failures of Symbolic Computation’ panel at [NSF Workshop](#) on Future Directions of Symbolic Computation Research And Their Applications to the Domain Sciences at the University of Rhode Island, May 1, 2009.
- ‘Convincing the Public about the Importance of Mathematical Research’ panel at the Fourth International Conference on Symbolic and Numerical Scientific Computing [SNSC '08](#) at RISC Linz, Hagenberg, Austria, July 24, 2008.
- ‘Hybrid Symbolic-Numeric Computing’ panel at the “East Coast Computer Algebra [Day](#)” at Shepherd University, Shepherdstown, West Virginia, May 2008.
- ‘Computer Algebra: What Is It Now? And What Should It Be Tomorrow?’ panel at the “East Coast Computer Algebra [Day](#)” at Washington College, Maryland, April 2007.
- ‘What Will Be the Next Killer Application of Computer Algebra’ panel at the seminar “[Challenges](#)” in Symbolic Computation Software at the International Conference and Research [Center](#) for Computer Science in Dagstuhl castle, Germany, July 2006.
- ‘The Next Killer App for Computer Algebra’ panel at the “International Conference on Applications of Computer Algebra [ACA 2003](#),” North Carolina State University, July 2003.
- ‘Problem Solving Environments for Distributed and Heterogeneous Environments’ panel at the “Scientific Integrated Development Environments for Knowledge, Information, and Computing ([SIDEKIC98](#))” workshop in Santa Fe, New Mexico, December 1998.

3.8 Session chair (no other conference office)

- “[Workshop B1. Approximate Commutative Algebra](#),” at the Radon Institute for Computational and Applied Mathematics in Linz, Austria, February 2006.
- “[Sixth International Conference on Finite Fields and Applications \(Fq6\)](#),” Oaxaca, Mexico, May 2001.
- “Generic Programming” meeting at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, April 1998.
- “Complexity Theory” meeting at the Mathematical Research Institute in Oberwolfach, West Germany, November 1996.

- Workshop on “Symbolic-Numeric Algebra for Polynomials (SNAP 96)” at INRIA Sophia Antipolis, France July 1996.
- “Computer Algebra – Software” meeting at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, February 1996.
- International Symposium on Symbolic and Algebraic Computation (ISSAC’95), Montreal, July 1995.
- “Complexity Theory” meeting at the Mathematical Research Institute in Oberwolfach, West Germany, November 1994.
- 9th International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (AAECC-9) in New Orleans, October 1991.
- “Complexity Theory” meeting at the Mathematical Research Institute in Oberwolfach, West Germany, November 1990
- “Complexity Theory” meeting at the Mathematical Research Institute in Oberwolfach, West Germany, November 1988.
- Workshop on “Computer algebraic integration and solution of differential equations” at the IBM T. J. Watson Research Center in Yorktown Heights, New York, November 1987.
- “Complexity Theory” meeting at the Mathematical Research Institute in Oberwolfach, West Germany, November 1986.

3.9 Invited participant (no talk)

- IMA “Hot Topic” **Workshop** “The Evolution of Mathematical Communication in the Age of Digital Libraries” at the Institute for Mathematics and Its Application at the University of Minnesota, December 2006.
- Workshop “Intelligent Human Augmentation & Virtual Environments (**WIHAVE**)” at UNC Chapel Hill, North Carolina, October 2002.
- Workshop “Interactive Tools for Teaching Computer Science” at Duke University, March 1996.
- Workshop “Computational Real Algebra and Geometry” at the Mathematical Sciences Institute at Cornell University, August 1992.
- Workshop “Computational Number Theory” at the DIMACS NSF Science and Technology Center at Rutgers University, March 1991.
- Workshop “Number Theory and Algorithms” at the Mathematical Sciences Research Institute in Berkeley, California, March 1990.
- Workshop “Computer Algebra Systems,” in Dallas, Texas, organized by Southern Methodist University and Texas Instruments, February 1987.
- Workshop “Parallel and Distributed Computing” at the Mathematical Sciences Research Institute in Berkeley, California, May 1986.
- Workshop “The computational complexity of algebraic and numerical problems” in Düsseldorf, organized by the German association of mathematicians (DMV), September 1984.

4 Review of programs, proposals, publications, and software

4.1 Program reviews and committee service

- Report on the Habilitation Thesis by Dr. Jean-Guillaume Dumas at the at the Joseph Fourier University Grenoble-1, France, June 2010.
- Search committee, University of Grenoble, France, 1999.
- External advisory board member, NSF infrastructure grant on establishing a Ph.D. in Computational Sciences, University of Puerto Rico, July 1995.

4.2 Proposal reviews

- Alexander von Humboldt fellowship application (Germany).
- Army Research Office.
- Austrian Science Foundation (FWF).
- Engineering and Physical Sciences Research Council, Great Britain.
- Israeli Science Foundation.
- Israel-USA Binational Science Foundation.
- National Science Foundation (32 proposals and four panels).
- National Research Council/American Mathematics Society on behalf of proposals submitted to the National Security Agency (4 proposals).
- Natural Sciences and Engineering Research Council of Canada (11 proposals).
- Netherlands Mathematics Research Foundation.

4.3 Reviews of papers submitted to journals

- ACM Transactions on Mathematical Software.
- Applicable Algebra in Engineering, Communication, and Computing.
- Discrete & Computational Geometry.
- IEEE Transactions on Parallel and Distributed Systems.
- Information and Control.
- Information Processing Letters.
- Journal of Algorithms.
- Journal of Complexity.
- Journal of Computer and System Sciences.
- Journal of Parallel and Distributed Computing.
- Journal of Symbolic Computation.
- Journal of the ACM.
- Linear Algebra and its Applications.
- matemática contemporânea of the Brazilian Math. Society.
- Mathematical Reviews.
- Mathematics of Computation.
- Parallel Computing Journal.
- SIAM Journal on Computing.
- SIAM Review.
- Theoretical Computer Science.

4.4 Reviews of software

- Scientific Advisory Board, [Oberwolfach Reference on Mathematical Software](#).
- 2004 and 2006 Richard D. Jenks Memorial Prize for Excellence in Computer Algebra Software Engineering.

University Committees On Which Erich Kaltofen Has Served

Committee	Office	Place	Time
Genomic Science Faculty	member	NCSU	1999–present
Scholarly Publ. Reposit. Adv. Council	member	NCSU Library	2007–08
Advisory, Genomic Science Initiative	member	NCSU	1997–99
Project 25	participating faculty	NCSU	1997
Research Advisory Council	member	NCSU College of PaMS	2004–07
On-line Instruction	member	NCSU College of PaMS	1999–2001
Graduate Program (Majors)	member	NCSU Math Dept	2006–09, 2003–04
Ph.D. Preliminary Exam	member	NCSU Math Dept	2009–present
Putnam Exam	member	NCSU Math Dept	2004–09
Awards and Publicity	member	NCSU Math Dept	2006–present
Library	member	NCSU Math Dept	2006–present
Web Page	member	NCSU Math Dept	2006–09
Personnel Evaluation	member	NCSU Math Dept	2005–06
Graduate Recruiting	member	NCSU Math Dept	2004–06 2002–03, 1996–97
Peer Teaching Evaluations	member	NCSU Math Dept	2002–04
Calculus Technology	member	NCSU Math Dept	2000–03
Symbolic Computation Recruiting	member	NCSU Math Dept	2000–01
Symbolic Computation Recruiting	co-chair	NCSU Math Dept	1996–97
Computing	member	NCSU Math Dept	2008–09, 1996–98
Faculty Senate	senator	RPI	1994–95
New Staff	member	RPI CS Dept	1992–95, 1988–90
Graduate Admission	member	RPI CS Dept	1994–95
Laboratory	member	RPI CS Dept	1994–95, 1990–92
Graduate Curriculum	member	RPI CS Dept	1991–94, 1984–87
PhD Qualifying Exam	member	RPI CS Dept	1993–95, 1984–88
Curriculum Task Force	member	RPI School of Science	1993–94
Library	representative	RPI CS Dept	1992–93
Chairperson Search	member	RPI CS Dept	1990–91
Theoretical Aspects in CS Seminar	organizer	RPI CS Dept	1984, '86, '87

Invited Lectures By Erich Kaltofen

1 Introduction

In the following the BASE URL for the online document is <http://www.math.ncsu.edu/~kaltofen/bibliography>. Some of my lectures have been recorded for access through the Internet and links to the transparencies and possibly audio can be found in the online document at [BASE/lectures/lectures.html](#) or in this document. You may use any of my transparencies for your own purposes, provided you acknowledge my authorship and copyright.

2 Invited Lectures at Conferences

213. “What Is Hybrid Symbolic-Numeric Computation?” Invited Lecture at the “Fields Institute Workshop on Hybrid Methodologies for Symbolic-Numeric Computation” “Fields Institute Workshop on Hybrid Methodologies for Symbolic-Numeric Computation,” Waterloo, November 16, 2011.
212. “Fast Estimates of Hankel Matrix Condition Numbers and Numeric Sparse Interpolation,” Invited Lecture at the Minisymposium ‘Algorithms in Real Algebraic Geometry and Applications’ at the “SIAM Conference on Applied Algebraic Geometry AAG ’11,” Raleigh, October 7, 2011.
211. “What Is Hybrid Symbolic-Numeric Computation?” Invited Lecture at “SYNASC 2011 – the 13th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing,” Timisoara, Romania, September 27, 2011.
210. “What Is Hybrid Symbolic-Numeric Computation?” Invited Lecture at the CRC 2011 – International Workshop on Certified and Reliable Computation in Nan-Ning, GuangXi, China, July 17, 2011.
209. “Fast Estimates of Hankel Matrix Condition Numbers and Numeric Sparse Interpolation,” Invited Lecture at the 15th International Conference on Applications of Computer Algebra ACA 2011 in Houston, Texas, June 29, 2011.
208. “Fifteen years after DSC and WLSS2: what parallel computations I do today,” Invited Lecture at the 2010 International Workshop on Parallel Symbolic Computation PASCO 2010 at the University of Grenoble, France, July 22, 2010.
207. “The indomitable Berlekamp/Massey algorithm,” Invited Lecture at Jo60 A Modern Computer Algebraist at the Bonn-Aachen International Center for Information Technology b-it, Bonn, May 27, 2010.
206. “Certifying the Radius of Positive Semidefiniteness Via Our ARTINPROVER Package,” Invited Lecture at the Workshop on Convex Algebraic Geometry at the Banff International Research Station, Canada, February 15, 2010.
205. “ARTINPROVER: a truly hybrid symbolic/numeric global optimization algorithm,” Invited Lecture at the AMS-SIAM Special Session on Applications of Algebraic Geometry at the Joint Mathematics Meeting, San Francisco, California, January 16, 2010.
204. “ARTINPROVER: a Truly Hybrid Symbolic/Numeric Global Optimization Algorithm,” Invited Lecture at the NSF-NAIS Workshop Intelligent Software: the Interface Between Algorithms and Machines Edinburgh, Scotland, October 19, 2009.
203. “Exact Certification in Global Polynomial Optimization Via Sums-Of-Squares of Rational Functions With Rational Coefficients” (same as 201), Lecture at the 15th International Conference on Applications of Computer Algebra (ACA 2009), Montreal, Canada, June 27, 2009.
202. “Supersparse Interpolation: Mathematics + Algorithmic And Computational Thinking = Mathematics Mechanization,” Invited Lecture at the International Conference on Mathematics Mechanization ICM ’09 in honor of Prof. Wen-tsun Wu’s 90th birthday, Beijing, China, May 11, 2009.
201. “Exact Certification in Global Polynomial Optimization Via Sums-Of-Squares of Rational Functions With Rational Coefficients,” Invited Lecture at the AMS Special Session on Concrete Aspects of Real Positive Polynomials Spring Central Sectional Meeting, Urbana, Illinois, March 28, 2009.
200. “Rump’s Model Problem and the Computer Search for Records in Number Theory,” Invited Lecture at the AMS Special Session on SAGE and Mathematical Research Using Open Source Software at the Joint Mathematics Meeting, Washington, DC, January 8, 2009.
199. “Exact Certification in Global Polynomial Optimization Via Rationalizing Sums-Of-Squares,” Invited lecture at the Workshop on Approximate Commutative Algebra ApCoA 2008 at RISC Linz, Hagenberg, Austria, July 25, 2008.
198. “The Seven Dwarfs of Symbolic Computation and the Discovery of Reduced Symbolic Models,” Invited lecture at the Fourth International Conference on Symbolic and Numerical Scientific Computing SNSC ’08 at RISC Linz, Hagenberg, Austria, July 24, 2008. Transparencies at [BASE/08/fields.pdf](#).

197. 196. “The Algebraic Synthesis of Algorithms Part 1: The Transposition Principle Part 2: Elimination of Divisions,” Two invited tutorial lectures at the International Conference on Rewriting Techniques and Applications **RTA 2008** at RISC Linz, Hagenberg, Austria, July 14, 2008.
195. “Model Discovery and Verification With Hybrid Symbolic-Numeric Computation,” Lecture at the **East Coast Computer Algebra Day** at Shepherd University, Shepherdstown, West Virginia, May 2008.
194. “Expressing a Fraction of Two Determinants as a Determinant,” Plenary Lecture at the CMS Winter 2007 **Meeting** in London, Canada, December 2007.
193. “On probabilistic analysis of randomization in hybrid symbolic-numeric algorithms,” Invited Lecture at the 2007 International Workshop on Symbolic-Numeric Computation (**SNC’07**) at the University of Western Ontario in London, Canada, July 2007.
192. “**Efficient linear algebra algorithms in symbolic computation**,” Invited Plenary Lecture at the 14th Conference of the International Linear Algebra Society (**ILAS 2007**) at Shanghai University, China, July 2007.
191. “**On probabilistic analysis of randomization in hybrid symbolic-numeric algorithms**,” Short Report at the ‘**Complexity Theory**’ meeting at the Mathematical Research **Institute** in Oberwolfach, Germany, June 2007.
190. “Finding small degree factors of multivariate super-sparse (lacunary) polynomials over algebraic number fields,” Invited Lecture at the **Workshop** on Computational Challenges Arising in Algorithmic Number Theory and Cryptography at the **Fields Institute** in Toronto, Canada October 2006. Transparencies at [BASE/06/fields.pdf](#).
189. 188. 187. 186. “Computer Algebra,” Four lectures at the **Summer School** on Mathematics, Algorithms, and Proofs, DIMA/DISI, University of Genova, Italy August 28 – September 2, 2006. Transparencies at [BASE/06/MAPlinbox.pdf](#), [BASE/06/MAPPolyfac.pdf](#), [BASE/06/MAPssparse.pdf](#), [BASE/06/MAPsncintro.pdf](#), and [BASE/06/MAPissackYZ.pdf](#).
185. “Enabling Breakthrough: Manuel Bronstein’s Impact on the Infrastructure of Symbolic Computation Research,” Invited Lecture at **CAFE** Computer Algebra and Functional Equations, an international conference, in memory of Manuel Bronstein at INRIA Sophia Antipolis, France, July 13, 2006. Transparencies at [BASE/06/manuel.pdf](#) and [BASE/06/PiledHigherDeeper.html](#).
184. “Hybrid Symbolic-Numeric Computation,” Invited Tutorial given jointly with Lihong Zhi at the International Symposium on Symbolic and Algebraic Computation **ISSAC 2006** at Genova, Italy, July 9, 2006. Abstract at [BASE/index.html#KaZhi06](#).
183. “Errors in Variables and Hybrid Symbolic-Numeric Methods,” Invited Lecture at the **Scientific Session** on Applications and Recent Developments in Symbolic Computation 2006 at the CAIMS-MITACS 2006 Joint Annual Conference in Toronto, Canada, June 18, 2006.
182. “Approximate Factorization of Complex Multivariate Polynomials My Lessons Learned,” Keynote Lecture at the Special Semester on Gröbner Bases and Related Methods 2006: **Workshop B1**. Approximate Commutative Algebra at the Radon Institute for Computational and Applied Mathematics in Linz, Austria, February 2006. Transparencies at [BASE/06/groebner.pdf](#). Maple worksheet at [BASE/06/groebner.txt](#).
181. “Approximate Factorization of Complex Multivariate Polynomials,” Invited Lecture at the AMS-SIAM **Special Session** on Symbolic-Numeric Computation and Applications at the Joint Mathematics Meeting, San Antonio, Texas, Jan 15, 2006.
180. “The Art of Symbolic Computation,” Invited Plenary Lecture at the Conference on Applications of Computer Algebra (**ACA 2005**), Nara City, Japan, August 2005. Transparencies at [BASE/05/aca.pdf](#). Maple worksheet at [BASE/05/aca.txt](#).
179. “On the complexity of factoring sparse polynomials,” Lecture at the ‘Complexity Theory’ meeting at the Mathematical Research **Institute** in Oberwolfach, Germany, June 2005. Transparencies at [BASE/05/oberwolfach.pdf](#).
178. “Tellegen’s principle and the synthesis of algorithms,” Lecture at the 33rd Theoretical Computer Science **Spring School** Computational Complexity Montagnac-les-truffes, Alpes de Haute Provence, France, May 2005. Transparencies at [BASE/05/montagnac.pdf](#) and [BASE/05/95montagnac.pdf](#).
177. “The role of algorithms in symbolic computation,” Lecture at the **East Coast Computer Algebra Day**, Ashland University, Ashland, Ohio, March 2005. Transparencies at [BASE/05/eccad.pdf](#).
176. “On the complexity of factoring bivariate supersparse and straight-line polynomials,” Lecture at the **Finite Fields: Theory and Applications** meeting at the Mathematical Research **Institute** in Oberwolfach, Germany, December 2004.
175. “Approximate Factorization of Multivariate Polynomials via Differential Equations,” Lecture at the seminar ‘**Real Computation and Complexity**’ at the International Conference and Research **Center** for Computer Science in Dagstuhl castle, Germany, February 2004. Transparencies at [BASE/04/dagstuhl.pdf](#).

174. "Polynomial Factorization: a Success Story," Invited Lecture at the Internat. Symp. Symbolic Algebraic Comput. (ISSAC 2003) Philadelphia, USA, August 2003. Transparencies at [BASE/03/issac.pdf](#). Maple worksheets at [BASE/03/issac1.txt](#), [BASE/03/issac2.txt](#). Abstract at [BASE/index.html#Ka03](#).
173. "Separation Bounds from Polynomial Reducibility," 'Numerical Polynomial Algebra' Minisymposium Lecture at the [First Joint Meeting of CAIMS & SIAM](#) (24th Annual Meeting of CAIMS / SCMAI and 2003 SIAM Annual Meeting), Montreal, Canada, June 2003. See [BASE/index.html#KM03](#).
172. "On the Complexity of the Determinant," Lecture at the 'Complexity Theory' meeting at the Mathematical Research Institute in Oberwolfach, Germany, April 2003. Transparencies at [BASE/03/oberwolfach.pdf](#).
171. "Efficient Problem Reductions in Linear Algebra," Lecture at the 8th International Conference on Applications of Computer Algebra (ACA), at the University of Thessaly in Volos, Greece, June 2002. Transparencies at [BASE/02/aca.pdf](#).
170. "On the complexity of computing determinants and other challenges in symbolic computation," at the [ASCM 2001](#) The Fifth Asian Symposium on Computer Mathematics at Ehime University in Matsuyama, Japan, September 2001. Talk given by video tape due to the terrorist events of September 11. Transparencies at [BASE/01/ascm.pdf](#).
169. "Efficient linear algebra algorithms in symbolic computation," Invited Lecture at the AMS-IMS-SIAM Joint [Summer Research Conference](#) on Fast Algorithms in Mathematics, Engineering and Computer Science at Mount Holyoke College, Massachusetts, August 2001. Transparencies at [BASE/01/holyoke.pdf](#).
168. "Algorithms for sparse and black box matrices over finite fields," Invited Lecture at the Sixth International Conference on Finite Fields and Applications (Fq6) in Oaxaca, Mexico, May 2001. Transparencies at [BASE/01/fq6.pdf](#). Bibliography at [BASE/index.html#Ka01:Fq6](#).
167. "On the Complexity of Computing Determinants," Invited Lecture at the 'Finite Fields and Applications' meeting at the Mathematical Research Institute in Oberwolfach, Germany, January 2001. Transparencies at [BASE/01/oberwolfach.pdf](#).
166. "Teaching Math over the Internet: A new challenge for computer algebra," Tutorial lecture at the International Symposium on Symbolic and Algebraic Computation ISSAC 2000 at St. Andrews, Scotland, August 2000. Transparencies at [BASE/2K/issactut.ppt](#). Realaudio at <http://courses.ncsu.edu/MA305/audio/issac2K.ra> (3.6M).
165. "Computer Algebra in the New Century: The Road Ahead," Lecture at the Computer Algebra Minisymposium at the 3rd European Congress of Mathematics at Barcelona, Spain, July 2000. Transparencies at [BASE/2K/ecm.pdf](#).
164. "Efficient Algorithms for Computing the Nearest Polynomial With Parametrically Constrained Roots and Factors," Lecture at the AMS-IMS-SIAM Joint [Summer Research Conference](#) on Symbolic Computation: Solving Equations in Algebra, Geometry and Engineering at Mount Holyoke College, Massachusetts, June 2000. Transparencies at [BASE/2K/holyoke.pdf](#).
163. "Efficient Algorithms for Computing the Nearest Polynomial With Parametrically Constrained Roots and Factors," Lecture at the Workshop on Symbolic and Numerical Scientific Computation (SNSC'99) at Johannes Kepler University Linz, Austria, August 1999. Transparencies at [BASE/99/snsc.pdf](#).
162. "Algebraic Complexity and Algorithms: Recent Advances and New Open Problems," Plenary Lecture at the 'Complexity Theory' meeting at the Mathematical Research Institute in Oberwolfach, Germany, November 1998. Transparencies at [BASE/98/oberwolfach.ps.gz](#).
161. "Massively Parallel Algorithms in Symbolic Computing," Lecture at the workshop "Parallel Symbolic Computation" at the Mathematical Sciences Research Institute, Berkeley, California, October 1998. Transparencies at [BASE/98/msri.ps.gz](#). Realaudio at <http://courses.ncsu.edu/MA305/audio/msri98.ra> (6.2M).
160. 159. "Challenges of Symbolic Computation My Favorite Open Problems," Lecture at the East Coast Computer Algebra Day, Naval Academy, Annapolis, Maryland, April 1998. Transparencies at [BASE/98/eccad.ps.gz](#); Lecture at the 1998 IMACS Conference on Applications of Computer Algebra (ACA), Prague, Czech Republic, August 1998. Realaudio at <http://courses.ncsu.edu/MA305/audio/aca98.ra> (5.7M).
158. "Generic Programming with Black Boxes," Lecture at the seminar 'Generic Programming' at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, April 1998. Transparencies at [BASE/98/dagstuhl.ps.gz](#).
157. "Factoring Polynomials over Finite Fields by Modular Polynomial Composition," Lecture at the seminar 'Computational Aspects of Commutative Algebra and Algebraic Geometry' at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, May 1997. Transparencies at [BASE/97/dagstuhl.ps.gz](#), [BASE/97/dagstuhlfig.ps.gz](#).

156. "Factoring Polynomials over High Algebraic Extensions of Finite Fields," Lecture at the 'Complexity Theory' meeting at the Mathematical Research Institute in Oberwolfach, Germany, November 1996.
155. "Blocked Iterative Sparse Linear System Solvers," Lecture at the Symposium on Parallel Computing for Solving Large Scale and Irregular Applications (Stratagem '96), INRIA Sophia Antipolis, France July 1996.
154. "Factoring High-Degree Polynomials over Finite Fields New Theory, Faster Practice," Lecture at the Second Magma Conference on Computational Algebra, Marquette University, Milwaukee, May 1996.
153. "Generic Symbolic Programming in C++ an Example," Lecture at the seminar 'Computer Algebra – Software' at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, February 1996.
152. "Complexity Theory in the Service of Algorithm Design," Lecture at the Conference on Algebraic Complexity in the memory of Jacques Morgenstern, INRIA Sophia Antipolis, France May 1995. Transparencies at [BASE/95/morgenstern.pdf](#).
151. "Parallel Matrix-free Linear System Solving and Symbolic Math Applications," Lecture at the East Coast Computer Algebra Day, University of Delaware, April 1995.
150. "Factoring High-degree Polynomials on a Computer Network," Minisymposium lecture at the 7th SIAM Conference on Parallel Processing for Scientific Computing, San Francisco, February 1995.
149. "Subquadratic-Time Factoring of Polynomials over Finite Fields," Lecture at the 'Complexity Theory' meeting at the Mathematical Research Institute in Oberwolfach, Germany, November 1994.
148. "Future Directions of Computer Algebra," Lecture at the 1994 Maple Technical Retreat, Sparrow Lake, Canada, June 1994.
147. "Polynomial Factorization," Lecture at the Symposium on Quantifier Elimination and Cylindrical Algebraic Decomposition (in honor of Prof. George E. Collins's 65th birthday), RISC Linz, Austria, October 1993.
146. "Parallel Solution of Sparse Linear Systems with Symbolic Entries," Lecture at the 'Applicable Algebra' meeting at the Mathematical Research Institute in Oberwolfach, Germany, February 1993. Transparencies at [BASE/93/oberwolfach.ps.gz](#).
145. "Parallel Sparse Linear System Solving," Lecture at the 'Complexity Theory' meeting at the Mathematical Research Institute in Oberwolfach, Germany, November 1992.
144. "Processor-Efficient Parallel Solution of Systems of Linear Equations," Lecture at the seminar 'Algebraic Complexity and Parallelism' at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, July 1992.
143. "Processor-Efficient Parallel Solution of Systems of Linear Equations," Minisymposium lecture at the 6th SIAM Conference on Discrete Mathematics, Vancouver, Canada, June 1992.
142. "Computing Determinants of Matrices without Divisions," Lecture at the 5th Mid-Atlantic Algebra Conference, George Mason University, Fairfax, Virginia, May 1992.
141. "A Decade of Research on Polynomial Factorization," Lecture at the 1st Latin American Symposium on Theoretical Informatics, São Paulo, Brazil, April 1992.
140. "Factoring Polynomials over the Algebraic Closure," Lecture at the seminar 'Algorithms in Computer Algebra' at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, December 1991.
139. "Processor-Efficient Parallel Solution of Linear Systems," Lecture at the Parallel Scientific Computation Workshop, Rensselaer Polytechnic Institute, October 1991; Lecture at the seminar 'Efficient Interpolation Algorithms' at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, December 1991.
138. "Processor-Efficient Parallel Solution of Linear Systems," Lecture at the Parallel Scientific Computation Workshop, Rensselaer Polytechnic Institute, October 1991; Lecture at the seminar 'Efficient Interpolation Algorithms' at the International Conference and Research Center for Computer Science in Dagstuhl castle, Germany, December 1991.
137. "On Wiedemann's Method of Solving Sparse Linear Systems," Lecture at the 9th Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes in New Orleans, October 1991.
136. "DSC A System for Distributed Symbolic Computation," Lecture at the 'Symbolic Software for Mathematical Research' workshop at the DIMACS NSF Science and Technology Center at Rutgers University, March 1991.
135. "Effective Noether Irreducibility Forms and Applications," Lecture at the 'Complexity Theory' meeting at the Mathematical Research Institute in Oberwolfach, Germany, November 1990.
134. "Efficient Size Bounds for Noether Irreducibility Forms and Applications to Parallel Problems on Hyper-Surfaces," Lecture at the 'Purdue Conference on Algebraic Geometry and Its Applications' in Honor of S. Abhyankar's 60th Birthday, June 1990.
133. "Processor Efficient Algebraic Computation," Lecture at the 'IV International Conference on Computer Algebra in Physical Research' at the Joint Institute for Nuclear Research in Dubna, Soviet Union, May 1990.

132. “Decomposing an Algebraic Curve,” Minisymposium Lecture at the SIAM Conference on Geometric Design, Tempe, Arizona, November 1989.
131. “Parallel Algebraic Algorithm Design,” Half-Day Tutorial at the 1989 International Symposium for Symbolic and Algebraic Computation, Portland, Oregon, July 1989.
130. “Computing the Irreducible Complex and Real Components of an Algebraic Curve,” Lecture at the RISC-Workshop on ‘Combinatorics and Computational Algebraic Geometry’ at the Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria, May 1989.
129. “Size Efficient Parallel Algebraic Circuits for Partial Derivatives,” Lecture at the ‘Complexity Theory’ meeting at the Mathematical Research Institute in Oberwolfach, West Germany, November 1988.
128. “Explicit Construction of the Hilbert Class Field of Imaginary Quadratic Fields,” Lecture at the ‘Computational Number Theory’ meeting at the Mathematical Research Institute in Oberwolfach, West Germany, May 1988.
127. “Factoring into Sparse Polynomials Made Easy,” Lecture at the conference ‘Toronto Experience: 20 Years of Computer Science Research,’ University of Toronto, May 1988.
126. “Randomized Parallel Computation of Matrix Canonical Forms,” Lecture at the ‘Foundations of Computing’ workshop by the Max Planck Institute for Mathematics and by the Department of Computer Science of the University in Bonn, West Germany, June 1987.
125. “Computing with Polynomials Given by Straight-Line Programs,” Lecturer at the ‘Complexity Theory’ meeting at the Mathematical Research Institute in Oberwolfach, West Germany, November 1986.
124. “Polynomial Factorization,” Lecturer in the short-course ‘Computer Algebraic Algorithms’ at the conference ‘Computers in Mathematics’ at Stanford University, August 1986.
123. “Multivariate Polynomial Factorization: From Curves to van der Monde Determinants,” Lecture at the workshop ‘Computational Algebra and Number Theory’ at the Mathematical Sciences Research Institute, Berkeley, California, October 1985.
122. “Deterministic Irreducibility Testing of Polynomials over Large Finite Fields,” presentation at the AMS-IMS-SIAM Joint Summer Research Conference on Computational Number Theory, Arcata, California, August 1985.

3 Invited Colloquia and Seminar Lectures

121. “The Art of Hybrid Symbolic-Numeric Computation,” Distinguished Faculty Colloquium at the Dept. of Mathematics at North Carolina State University, “[Video archive](#),” Raleigh, February 16, 2012.
120. “Sixteen years after DSC and WLSS2: what parallel computations I do today,” (same as 208), Seminar Lecture at the Shanghai Key Laboratory of Trustworthy Computing, East China Normal University [ECNU](#), Shanghai, China, July 23, 2011.
119. “Two complexity results from convex optimization Valiant’s determinants symmetricized and matrix definiteness certified,” Seminar Lecture at the Key Laboratory of Mathematics-Mechanization [KLMM](#), Institute of Systems Sciences, Chinese Academy of Sciences, Beijing, China, July 12, 2011.
118. “Quadratic-Time Certificates in Linear Algebra,” Theory Seminar Lecture at the University of Toronto, Canada, April 8, 2011.
117. “Exact Certification in Global Polynomial Optimization via Sums-Of-Squares of Polynomials and Rational Functions with Rational Coefficients,” Seminar Lecture at the University College Dublin [UCD](#), Ireland, May 31, 2010.
116. “A Fraction Free Matrix Berlekamp/Massey Algorithm,” Seminar Lecture at the Key Laboratory of Mathematics-Mechanization [KLMM](#), Institute of Systems Sciences, Chinese Academy of Sciences, Beijing, China, November 12, 2008.
115. Same as 195, Invited talk at the Joint Lab Meeting (JLM) of the Ontario Research Centre for Computer Algebra (ORCCA) at the University of Waterloo, June 2008.
114. “On Exact and Approximate Interpolation of Sparse Rational Functions,” Colloquium at Tsukuba University, Japan, March 2007.
113. “The Art of Symbolic Computation,” Applied Mathematics Colloquium at Massachusetts Institute of Technology, April 2006. Transparencies at [BASE/06/mit.pdf](#). Maple worksheets at [BASE/06/groebner.txt](#) and [BASE/05/aca.txt](#).
112. “The Art of Symbolic Computation,” Computer Science Colloquium at North Carolina State University, October 2004. Transparencies at [BASE/04/ncsu.pdf](#). Maple worksheets at [BASE/04/nyu.txt](#) and [BASE/03/risc1.txt](#).
111. “Approximate Factorization of Complex Multivariate Polynomials,” Computer Science Colloquium at New

- York University, September 2004. Transparencies at [BASE/04/nyu.pdf](#). Maple worksheet at [BASE/04/nyu.txt](#).
110. “On the Complexity of Computing Determinants,” Computer Science Colloquium at Duke University, October 2003. Transparencies at [BASE/03/duke.pdf](#).
 109. “The Art of Symbolic Computation,” Colloquium at the Research Institute for Symbolic Computation in Linz, Austria, May 2003. Transparencies at [BASE/03/risc.pdf](#). Maple worksheets at [BASE/03/risc1.txt](#), [BASE/03/risc2.txt](#).
 108. “The art of symbolic computation,” Colloquium at the University of Waterloo, Canada, March 2002. Transparencies at [BASE/02/waterloo.pdf](#).
 107. “Deterministic polynomial-time algorithms for polynomial factorization modulo a large prime,” Seminar at the École Normale Supérieure in Lyon, France, June 2001.
 106. “Symbolic computation in the new century The road ahead,” Colloquium at Clemson University, April 2001. Transparencies at [BASE/01/clemson.pdf](#).
 105. “On the Complexity of Computing Determinants,” Lecture in the ‘Algorithmic Number Theory Program’ at the Mathematical Sciences Research Institute, Berkeley, California, November 2000. Transparencies at [BASE/2K/msri.pdf](#).
 104. Same as [165](#), Colloquium at the Institut d’Informatique et de Mathématiques Appliquées de Grenoble (IMAG), France, July 2000.
 103. “Early Termination in Ben-Or/Tiwari Sparse Interpolation and a Hybrid of Zippel’s Algorithm,” Seminar lecture at the University of Western Ontario, Canada, February 2000. Transparencies at [BASE/2K/uwo.pdf](#).
 102. “Generic programming: C++ vs. Java,” Object Technologies Seminar, University of Delaware, November 1999. Transparencies at [BASE/99/udel.pdf](#).
 101. 100. “Efficient Algorithms for Computing the Nearest Polynomial With A Real Root and Related Problems,” Seminar lectures at the Institut d’Informatique et de Mathématiques Appliquées de Grenoble, France and the Eidgenössische Technische Hochschule in Zurich, Switzerland, January 1999. Transparencies at [BASE/99/imagethz.ps.gz](#).
 99. Same as [160](#), Simon Fraser University, Center for Experimental and Constructive Mathematics, Vancouver, July 1998.
 98. “The Black Box Representation of Symbolic Mathematical Objects: New Algorithms, Record Breaking Computations,” Pacific Institute for the Mathematical Sciences (PIMS) 1997 Distinguished Lecture Series, Simon Fraser University, Vancouver, March 1997.
 97. “Matrix-free Polynomial Factorization,” Center for Computing Sciences Colloquium, Institute for Defense Analysis, Bowie, Maryland, November 1995.
 96. “Parallel Symbolic Computation by Black Boxes,” Colloquium at Indiana University Purdue University at Indianapolis, April 1995.
 95. “Polynomial Factorization and Applications,” Special Colloquium at Florida State University, April 1995.
 94. “Parallel Matrix-free Linear System Solving and Symbolic Math Applications,” Special Seminar Lecture at North Carolina State University, March 1995.
 93. “Factoring High-Degree Polynomials by the Black Box Berlekamp Algorithm,” Colloquium at the State University of New York at Albany, April 1994.
 92. “Factoring a High-Degree Polynomial on Many Computers,” Seminar Lecture at Virginia Polytechnic Institute and State University, March 1994.
 91. 90. 89. “Parallel Solution of Sparse Linear Systems with Symbolic Entries,” Seminar Lecture at the Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria, February 1993; Lecture at the University Tübingen, Germany, October 1993; Lecture at IBM Heidelberg, Germany, October 1993.
 88. “Solving Sparse Systems of Linear Equations (With Symbolic Entries),” Seminar Lecture at Xerox PARC, July 1992.
 87. “Polynomial Factorization and Applications,” Special Seminar Lecture at North Carolina State University, April 1992.
 86. “Solving Sparse Systems of Linear Equations (with Symbolic Entries),” Seminar Lecture at Virginia Polytechnic Institute and State University, March 1992.
 85. “Parallel Algebraic Computation: Theory & Practice,” Colloquium at Radford University, March 1992.
 84. “Polynomial Factorization and Applications,” Colloquium at Williams College, October 1991.
 83. “Parallel Algebraic Computation: Theory and Practice,” Seminar Lecture at the University of Waterloo, May 1991.
 82. “Processor Efficient Parallel Solution of Linear Systems,” Seminar Lecture at the University of Toronto, April 1991.
 81. “Effective Noether Irreducibility Forms and Applications,” Seminar Lecture at Queen’s University in Kingston, Canada, April 1991.

80. "Parallel Symbolic Computation A Beginning," Lecture at the New York State Center for Advanced Technology in Computer Applications and Software Engineering, Syracuse University, March 1991.
79. "Effective Noether Irreducibility Forms and Applications," Seminar Lecture at the Eidgenössische Technische Hochschule in Zurich, Switzerland, November 1990.
78. "Processor Efficient Parallel Program Transformations," Colloquium at Louisiana State University, November 1989.
77. "How to Solve Systems of Non-Linear Equations Faster," Seminar Lecture at Carnegie-Mellon University, September 1989.
76. "An Improve Las Vegas Primality Test," Colloquium at the University of Saarbrücken, West Germany, June 1989.
75. "How to Solve Systems of Non-Linear Equations Faster," Colloquium at Cornell University, February 1989.
74. "Implicit Representations of Symbolic Data and Applications," Seminar Lecture at Syracuse University, February 1989.
73. 72. 71. 70. "How to Solve Systems of Non-Linear Equations Faster," Seminar Lecture at the University of Illinois at Urbana-Champaign, April 1988, at the Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria, June 1988, Colloquium at the University of Alberta in Edmonton, September 1988, and Seminar Lecture at the National Science Foundation, October 1988.
69. "The Problem of Factoring Polynomials," Colloquium at the University of Indiana in Bloomington, December 1987.
68. "Computing with Polynomials Given by Straight-Line Programs: Theory and Practice," RISC-Colloquium at the Johannes Kepler University in Linz, Austria, June 1987.
67. "Fast Multiplication of Polynomials over Arbitrary Rings," Colloquium at the University of Zürich, Switzerland, June 1987.
66. "Fast Parallel Computation of Canonical Forms of Polynomial Matrices," Seminar Lecture at the University of Southern California, February 1987.
65. "Computer Algebra," Colloquium at Oakland University, Rochester, Michigan, January 1987.
64. "The Problem of Factoring Polynomials," Seminar Lecture at the University of California in Los Angeles, May 1986.
63. "Computing with Polynomials Given by Straight-Line Programs: Theory and Practice," Seminar Lecture at the Massachusetts Institute of Technology, April 1986.
62. "The Complexity Year: A Personal Perspective," Colloquium at the University of Delaware, March 1986.
61. "Computing with Polynomials Given by Straight-Line Programs: Theory and Practice," Seminar Lecture at the University of Toronto, March 1986.
60. "Uniform Closure Properties of P-Computable Functions," Seminar Lecture at Stanford University, November 1985.
59. "Computing with Polynomials Given by Straight-Line Programs," Seminar Lecture at the University of California at Berkeley, September 1985.
58. "Computer Algebra: Theory and Practice," Colloquium at the Tektronix Computer Research Laboratory in Beaverton, Oregon, August 1985.
57. 56. 55. 54. "Computing with Polynomials Given by Straight-Line Programs," Seminar Lecture at Kent State University, March 1985, at the University of Toronto, March 1985, Colloquium at the University of Washington, June 1985, and Colloquium at the University of Oregon, July 1985.
53. "Fast Parallel Computation of Hermite and Smith Forms of Polynomial Matrices," Colloquium at the State University of New York in Albany, February 1985.
52. "Introduction to Computer Algebra and the Computer Algebra System Macsyma," Colloquium at the University of Ottawa, June 1984.
51. "Arithmetic in Imaginary Quadratic Fields," Seminar Lecture at the University of Toronto, May 1984.
50. "Fast Parallel Absolute Irreducibility Testing and Factoring," Colloquium at the Massachusetts Institute of Technology, May 1984.
49. 48. "On the Sequential and Parallel Complexity of Polynomial Factorization," Colloquium at Harvard University, October 1983, and Colloquium at the General Electric Research and Development Center in Schenectady, March 1984.
47. 46. "An Introduction to the MACSYMA Computer Algebra System," Colloquium and live demonstration in the Mathematics and Physics Dept. at the University of Toronto, November and December 1983.
45. "Polynomial-Time Polynomial Factorization—a Tutorial," Seminar Lecture at the University of Waterloo, June 1983.

44. “Three Uses of VAXIMA: How to Break the Multiplicative Knapsack Encryption Scheme, how to Compute Polynomials with Dihedral Galois Group, and how to Locate a Company for Maximum Profit,” Colloquium at Kent State University, May 1983.
43. 42. 41. “Some Recent Results for Factoring Polynomials in Polynomial Time,” Colloquium at Purdue University, February 1983, Seminar Lecture at the T. J. Watson IBM Research Center, April 1983, and Colloquium at Dartmouth College, April 1983.
40. 39. “Factoring Multivariate Integer Polynomials in Polynomial Time,” Seminar Lecture at the Massachusetts Institute of Technology, July 1982, and Seminar Lecture at Bell Laboratories, Murray Hill, July 1982.
38. 37. 36. “The Problem of Factoring Polynomials with Integer Coefficients,” Colloquium at Cornell University, November 1981, Colloquium at Rensselaer Polytechnic Institute, April 1982 and Colloquium at the University of Toronto, April 1982.
35. “On Integer Polynomials that are Exponentially Hard to Factor,” Colloquium at the University of Delaware, March 1981.
34. “Compiling Pascal into the Lambda Calculus,” Mathematics Seminar at the Johannes Kepler University in Linz, June 1979.

4 Other Talks

33. “Supersparse Black Box Rational Function Interpolation,” **Seminar** in the Department of Computer Science at the University of Calgary, February 19, 2010.
32. Same as **194**, Lecture in the Symbolic Computation Seminar at North Carolina State University, December 2007.
31. “Fast Algorithms for Polynomial Factorization: a Selection,” Lecture at the Second NCSU-China Symbolic Computation Collaboration **Workshop** at Zhejiang University, Hangzhou, China, March 2007. Transparencies at [BASE/07/hangzhou.pdf](#).
30. “Errors in variables and hybrid symbolic-numeric methods,” Joint Lecture in the Numerical Analysis and Symbolic Computation Seminars at North Carolina State University, September 2006.
29. “Finding Small Degree Factors of Multivariate Supersparse (Lacunary) Polynomials Over Algebraic Number Fields,” Lecture at the seminar ‘**Challenges in Symbolic Computation Software**’ at the International Conference and Research **Center** for Computer Science in Dagstuhl castle, Germany, July 2006.
28. “Approximate Complex Multivariate Polynomial Factorization,” Lecture in the Ph.D. Seminar at the College of Computer and Information Science at Northeastern University, April 2006.
27. Same as **178**. Lecture at the First NCSU-China Symbolic Computation Collaboration **Workshop** at North Carolina State University, October 2005.
26. “On the complexity of factoring bivariate supersparse (lacunary) polynomials,” Lecture in the Symbolic Computation Seminar at North Carolina State University, January 2005.
25. Same as **171**. Lecture at the Mathematics Mechanization Research Center, Institute of Systems Sciences, Chinese Academy of Sciences, Beijing, China, August 2002.
24. Same as **163**. Lecture in the Numerical Analysis Seminar at North Carolina State University, September 1999.
23. “Efficient Algorithms for Computing the Nearest Polynomial with Constrained Roots,” Simon Fraser University, Center for Experimental and Constructive Mathematics, Vancouver, July 1998. Transparencies at [BASE/98/sfu.ps.gz](#).
22. “Mathematics on the Internet New Problems, Suggested Solutions,” Presentation at the 1997 Instructional Technologies Expo, North Carolina State University, September 1997. HTML document at <http://www.math.ncsu.edu/~kaltofen/ssg/Erich/Expo97/expo97.html>
21. “Factoring High-Degree Polynomials over Finite Fields New Theory, Faster Practice,” Lecture in the Algebra Seminar at North Carolina State University, November 1996.
20. “Polynomial Factorization over High Algebraic Extensions of Finite Fields,” Special Seminar at the University of Delaware, May 1996.
19. “Parallel Matrix-free Linear System Solving and Computational Complexity Theory,” Special Seminar at Florida State University, April 1995.
18. “Teaching Computational Abstract Algebra,” Workshop on New Technology for Symbolic Computational Mathematics and Applications in Research and Education, Center for Computer Aids for Industrial Productivity, Rutgers University, June 1994.
17. “Asymptotically Fast Solution of Toeplitz-Like Singular Linear Systems,” invited Presentation at 884th meeting of the AMS at Syracuse University, September 1993.
16. “Symbolic Computation,” MP&O Research Seminar Lecture in the Management Department at Rensselaer Polytechnic Institute, April 1990.

15. "Processor Efficient Computation of Partial Derivatives," Lecture at the Parallel Circus, Rensselaer Polytechnic Institute, April 1989.
14. 13. "Polynomial Factorization," and "Parallel Algorithms for Algebraic Problems," two Lectures given for the shortcourse 'Algorithmic Methods in Computer Algebra,' organized by A. Miola at the College G. Reiss Romoli in L'Aquila, Italy, April 1988.
12. "Cryptography: Where Theoretical Computer Science Becomes a National Security Issue," Lecture given for the Pi Mu Epsilon Mathematics Honor Society at Rensselaer Polytechnic Institute, February 1988.
11. "Fast Multiplication of Polynomials over Arbitrary Rings," Seminar Lecture at IBM T. J. Watson Research Center, August 1987.
10. "Las Vegas-RNC Computation of the Smith Normal Form of Polynomial Matrices," Presentation at the Princeton Forum on Algorithms and Complexity, March 1987.
9. "Computing with Polynomials Given by Straight-Line Programs," informal Presentation at the 12th Symposium on Mathematical Foundations of Computer Science in Bratislava, Czechoslovakia, August 1986.
8. "Macsyma Seminar," demonstration of Macsyma to the Physics Department at the University of Toronto, December 1983.
7. "An Alternate Construction of Succinct Certificates for Normal Univariate Irreducible Polynomials with Integer Coefficients," invited Presentation at 793rd meeting of the AMS in Bryn Mawr, Pennsylvania, March 1982.

5 ACM Lectures

6. 5. 4. 3. "Computational Algebra and Number Theory: A Technological Wonder of our Times," Lecture at the Western Massachusetts ACM Chapter in Springfield, Massachusetts, October 1989; Lecture at the ACM Student Chapter at Louisiana State University, November 1989; Lecture at the Fourth Congress on Computer Science Applications of the Puerto Rico ACM Student Chapter in Ponce, Puerto Rico, April 1990; Lecture at the ACM Student Chapter at Lawrence University, Appleton, Wisconsin, April 1991.
2. 1. "Parallel Algebraic Computation: A Beginning," Lecture at the Virginia Polytechnic Institute ACM Student Chapter, April 1991; Lecture at the ACM Student Chapter at Lawrence University, Appleton, Wisconsin, April 1991.

Awards And Citations For Erich Kaltofen

1 Awards

- **ACM Fellow**, 2009.
- ACM SIGSAM's ISSAC 2005 Distinguished Paper Award for **my paper** "On the complexity of factoring bivariate supersparse (lacunary) polynomials" with Pascal Koiran presented at the International Symposium on Symbolic and Algebraic Computation in Beijing, China in July 2005.
- Early Career Award, Rensselaer Polytechnic Institute, April 1989.
- IBM Faculty Development Award, July 1985–87, \$60,000.
- Joaquin B. Diaz Prize for best graduate student in Mathematical Sciences at Rensselaer Polytechnic Institute, May 1982.
- Fulbright Exchange Student Award, July 1977.
- **Bronze Medal** at the International Mathematical Olympiad 1972 and 1974.

2 Public Citations

- Top ranked author in Scientific Computing, **Microsoft Academic Search**, 2009–2010.
- Remarks on the Rubik's Cube problem cited by Pat Greenhouse in the **Boston Globe June 25, 2007**.
- Listed among "Most cited authors in Computer Science," <http://citeseer.ist.psu.edu/allcited.html>, August 2005.
- Appeared in the video "Invitation to Discover" promoting the Mathematical Sciences Research Institute at Berkeley; the interview was filmed by George Csicsery in the Treasurer's office at the National Academy of Sciences in Washington, D.C. on October 29, 2001.
- Remarks on the US government's "Clipper Chip" proposal cited by I. Clements in "Proposed Decoding Device Generates Debate," *The Sunday Gazette*, December 26, 1993.
- Observations on symbolic computation technology cited by D. Bjerklie in "Crunching Symbols," in the Trends section of *Technology Review* **95**/3, pp. 15–16, April 1992.
- Work on randomized algebraic algorithms cited by T. A. Heppenheimer in "Symbolic Manipulation Computer Algebra," *MOSAIC* **22**/4, p. 34, Winter 1991.
- Remarks on cryptography cited by O. Anderson in the Special Report "Encryption affords highest security for computers," *Capital District Business Review*, December 7-13, 1988, p. 25.
- Listed in *American Men and Women of Science*, two most recent editions.
- Listed in *Who's Who in the East*, 24th edition.