Publications by Erich Kaltofen

December 3, 2018

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 compatibilty 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, 86]; deterministic polynomial-time irreducibility testing [36] and distinct degree factorization [122] of multivariate polynomials over a large finite field; computing the nearest multivariate polynomial with factor of constant degree and complex coefficients in polynomial time [106].
- Polynomial-time sparse multivariate polynomial factorization algorithms by introducing the straight-line program [43, 40, 35, 31, 24, 20] and the black box representations of polynomials [58, 82].
- Subquadratic-time polynomial factorization of univariate polynomials over a finite field [83, 98]; asymptotically fastest polynomial factorization algorithm over high algebraic extensions of finite fields [94].
- Polynomial-time computation of small degree factors of supersparse (lacunary) multivariate polynomials over the rational and algebraic numbers [130, 128].

1.2 Linear Algebra

- Rank algorithm for a black box matrix via Wiedemann's method but without binary search [59].
- Processor-efficient parallel algorithms for solving general linear systems over a field [63, 67].
- Parallel algorithms for matrix canonical forms [33, 55].
- Probabilistic analysis [81] and implementation [77, 90, 103] of the block Wiedemann parallel sparse linear system solver.
- Asymptotically fast solution of Toeplitz-like linear systems over any field including a finite field [81, 78].
- Probabilistic analysis of the Lanczos sparse linear system solver over finite fields [95].
- Baby steps/giant steps algorithms for computing the determinant of an integer matrix [110, 113, 125]; fastest algorithm known in terms of bit operations for the characteristic polynomial.
- Analysis and fraction-free realization of the matrix Berlekamp/Massey algorithm [158, 159].

1.3 Sparse Polynomial Interpolation

- Asymptotically fast and modular versions of the Zippel and Ben-Or/Tiwari algorithms [39, 54, 147].
- Early termination versions of the Zippel and Ben-Or/Tiwari algorithms [108, 120].
- Algorithms for computing the sparsest shift of polynomials [114, 119].
- 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 [40].
- Asymptotically fast multiplication of polynomials over a ring [65].
- Fast division-free computation of the determinant and the characteristic polynomial of a matrix over a commutative ring [68, 110, 125].
- Integer division with remainder in residue number systems via Newton iteration [84].
- Removal of divisions of in fractions of determinants and formulas [138].
- Valiant universality of determinants of symmetric matrices for formulas [148].

1.5 Computational Number Theory

- Use of Weber equations for the Hilbert class fields arising in the Goldwasser-Kilian/Atkin primality prover [14, 12, 49, 61].

1.6 Hybrid Symbolic/Numeric Computation

- Stability of roots of polynomials with respect to coefficient perturbations [100, 106].
- Approximate factorization [137, 123] and numerical irreducibility testing [118] of multivariate polynomials over the complex numbers.
- Approximate multivariate polynomial greatest common divisor computation [126, 131] and computation of the nearest singular polynomial [131].
- Exact certification of global optima via semidefinite programming and rationalization of sums-of-squares [139, 140, 141],
- Well- and ill-conditionedness of polynomial inequalities [143].

1.7 Software

- DAGWOOD: a system for manipulating polynomials given by straight-line programs [41]. The archive directory of the Lisp program source code is at `BASE/../software/dagwood`.
- DSC: the distributed symbolic manipulation tool [62, 72, 76, 80]. 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 [99]. 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 [85, 103]. The archive directory of the C program source code is at `BASE/../software/wiliss`.
- LinBox: a generic library for exact black box linear algebra [112, 127]. The homepage including downloads can be found at `www.linalg.org`.
- AppFac: a package for approximate multivariate complex polynomial factorization and GCD [131, 137, 123]. 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 [93]. 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 [117, 69, 57, 7].
- Three surveys on algebraic algorithms [102, 96, 34].
- A survey on sparse linear systems [91] and one on the computational complexity of matrix determinants [124].
- A list of open problems [107].
- A survey on parallelizing straight-line programs [71].
- The seven dwarfs of symbolic computation [145].

References

[177] Erdal Imamoglu and Erich L. Kaltofen. On computing the degree of a Chebyshev polynomial from its value. Manuscript, November 2018. 9 pages.

[176] Erdal Imamoglu, Erich L. Kaltofen, and Zhengfeng Yang. Sparse polynomial interpolation with arbitrary orthogonal polynomial bases. In *ISSAC '18 Proc. 2018 ACM Internat. Symp. Symbolic Algebraic Comput.* [-1], pages 223–230. In memory of Bobby F. Caviness (3/24/1940–1/11/2018). URL: `EKbib/18/IKY18.pdf`.

[175] Jean-Guillaume Dumas, Erich L. Kaltofen, David Lucas, and Clément Pernet. Elimination-based certificates for triangular equivalence and rank profiles. Manuscript, December 2017. 27 pages.

[174] Jean-Guillaume Dumas, Erich L. Kaltofen, Gilles Villard, and Lihong Zhi. Polynomial time interactive proofs for linear algebra with exponential matrix dimensions and scalars given by polynomial time circuits. In *ISSAC '17 Proc. 2017 ACM Internat. Symp. Symbolic Algebraic Comput.* [-2], pages 125–132. In memory of Wen-tsun Wu (5/12/1919–5/7/2017). URL: EKbib/17/DKVZ17.pdf.

[173] Erich L. Kaltofen, Clément Pernet, Arne Storjohann, and Cleveland A. Waddell. Early termination in parametric linear system solving and rational function vector recovery with error correction. In *ISSAC '17 Proc. 2017 ACM Internat. Symp. Symbolic Algebraic Comput.* [-2], pages 237–244. URL: EKbib/17/KPSW17.pdf.

[172] Mark Giesbrecht, Joseph Haraldson, and Erich Kaltofen. Computing approximate greatest common right divisors of differential polynomials. *CoRR*, abs/1701.01994, 2017. URL: http://arxiv.org/abs/1701.01994.

[171] Zhiwei Hao, Erich L. Kaltofen, and Lihong Zhi. Numerical sparsity determination and early termination. In *ISSAC'16 Proc. 2016 ACM Internat. Symp. Symbolic Algebraic Comput.* [-3], pages 247–254. URL: EKbib/16/HKZ16.pdf.

[170] Jean-Guillaume Dumas, Erich Kaltofen, Emmanuel Thomé, and Gilles Villard. Linear time interactive certificates for the minimal polynomial and the determinant of a sparse matrix. In *ISSAC'16 Proc. 2016 ACM Internat. Symp. Symbolic Algebraic Comput.* [-3], pages 199–206. URL: EKbib/16/DKTV16.pdf.

[169] Jean-Guillaume Dumas, Erich L. Kaltofen, and Clément Pernet, editors. *PASCO '15: Proc. 2015 Internat. Workshop Parallel Symbolic Comput.*, New York, N. Y., 2015. ACM.

[168] Andrew Arnold and Erich L. Kaltofen. Error-correcting sparse interpolation in the Chebyshev basis. In *ISSAC'15 Proc. 2015 ACM Internat. Symp. Symbolic Algebraic Comput.* [-4], pages 21–28. URL: EKbib/15/ArKa15.pdf.

[167] Erich L. Kaltofen and Zhengfeng Yang. Sparse multivariate function recovery with a small number of evaluations. *J. Symbolic Comput.*, 75:209–218, July/August 2016. Special Issue on ISSAC 2014, URL: EKbib/15/KaYa15_jsc.pdf.

[166] Erich L. Kaltofen. Cleaning-up data for sparse model synthesis: when symbolic-numeric computation meets error-correcting codes. In *SNC'14 Proc. 2014 Internat. Workshop on Symbolic-Numeric Comput.* [-6], pages 1–2. URL: EKbib/14/Ka14.pdf.

[165] Brice B. Boyer and Erich L. Kaltofen. Numerical linear system solving with parametric entries by error correction. In *SNC'14 Proc. 2014 Internat. Workshop on Symbolic-Numeric Comput.* [-6], pages 33–38. URL: EKbib/14/BoKa14.pdf.

[164] Jean-Guillaume Dumas and Erich L. Kaltofen. Essentially optimal interactive certificates in linear algebra. In *ISSAC 2014 Proc. 39th Internat. Symp. Symbolic Algebraic Comput.* [-7], pages 146–153. URL: EKbib/14/DuKa14.pdf.

[163] Erich L. Kaltofen and Clément Pernet. Sparse polynomial interpolation codes and their decoding beyond half the minimal distance. In *ISSAC 2014 Proc. 39th Internat. Symp. Symbolic Algebraic Comput.* [-7], pages 272–279. URL: EKbib/14/KaPe14.pdf.

[162] Erich L. Kaltofen and Zhengfeng Yang. Sparse multivariate function recovery with a high error rate in evaluations. In *ISSAC 2014 Proc. 39th Internat. Symp. Symbolic Algebraic Comput.* [-7], pages 280–287. URL: EKbib/14/KaYa14.pdf.

[161] Erich L. Kaltofen. Symbolic computation and complexity theory transcript of my talk. In *Computer Mathematics 9th Asian Symp. (ASCM2009), Fukuoka, 10th Asian Symp. (ASCM2012), Beijing* [-5], pages 3–7. URL: EKbib/13/Ka13.pdf.

[160] Erich Kaltofen and Zhengfeng Yang. Sparse multivariate function recovery from values with noise and outlier errors. In *ISSAC 2013 Proc. 38th Internat. Symp. Symbolic Algebraic Comput.* [-8], pages 219–226. URL: EKbib/13/KaYa13.pdf.

[159] Erich Kaltofen and George Yuhasz. A fraction free matrix Berlekamp/Massey algorithm. *Linear Algebra and Applications*, 439(9):2515–2526, November 2013. URL: EKbib/08/KaYu08.pdf.

[158] Erich Kaltofen and George Yuhasz. On the matrix Berlekamp-Massey algorithm. *ACM Trans. Algorithms*, 9(4), September 2013. URL: EKbib/06/KaYu06.pdf.

[157] Brice Boyer, Matthew T. Comer, and Erich L. Kaltofen. Sparse polynomial interpolation by variable shift in the presence of noise and outliers in the evaluations. In *Computer Mathematics 9th Asian Symp. (ASCM2009), Fukuoka, 10th Asian Symp. (ASCM2012), Beijing* [-5], pages 183–197. URL: EKbib/13/BCK13.pdf.

[156] Matthew T. Comer, Erich L. Kaltofen, and Clément Pernet. Sparse polynomial interpolation and Berlekamp/Massey algorithms that correct outlier errors in input values. In *ISSAC 2012 Proc. 37th Internat. Symp. Symbolic Algebraic Comput.* [-9], pages 138–145. URL: EKbib/12/CKP12.pdf.

[155] Feng Guo, Erich L. Kaltofen, and Lihong Zhi. Certificates of impossibility of Hilbert-Artin representations of a given degree for definite polynomials and functions. In *ISSAC 2012 Proc. 37th Internat. Symp. Symbolic Algebraic Comput.* [-9], pages 195–202. URL: EKbib/12/GKZ12.pdf; URL: http://arxiv.org/abs/1203.0253.

[154] Erich Kaltofen and Arne Storjohann. The complexity of computational problems in exact linear algebra. In *Encyclopedia of Applied and Computational Mathematics* [-10], page to appear. URL: EKbib/11/KS11.pdf.

[153] Erich Kaltofen and Grégoire Lecerf. Section 11.5. Factorization of multivariate polynomials. In *Handbook of Finite Fields* [-11], pages 382–392. URL: EKbib/11/KL11.pdf.

[152] 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.* [-13], pages 130–136. URL: EKbib/11/KLY11.pdf.

[151] 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* [-14], pages 171–176. URL: EKbib/11/KNS11.pdf.

[150] 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* [-15], pages 543–554. Journal version in [148]. URL: EKbib/11/GKKP11.pdf.

[149] Matthew T. Comer and Erich L. Kaltofen. On the Berlekamp/Massey algorithm and counting singular Hankel matrices over a finite field. *J. Symbolic Comput.*, 47(4):480–491, April 2012. URL: EKbib/10/CoKa10.pdf.

[148] 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.

[147] 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.* [-16], pages 10–17. URL: EKbib/10/Ka10_pasco.pdf.

[146] 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.

[145] Erich L. Kaltofen. The "Seven Dwarfs" of symbolic computation. In *Numeric and Symbolic Scientific Computing Progress and Prospects* [-12], pages 95–104. URL: EKbib/10/Ka10_7dwarfs.pdf.

[144] Erich L. Kaltofen and Michael Nehring. Supersparse black box rational function interpolation. In *Proc. 2011 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2011* [-14], pages 177–185. URL: EKbib/11/KaNe11.pdf.

[143] 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* [-17], pages 227–234. URL: EKbib/10/HKZ10.pdf.

[142] Erich Kaltofen and Mark Lavin. Efficiently certifying non-integer powers. *Computational Complexity*, 19(3):355–366, September 2010. URL: EKbib/09/KaLa09.pdf.

[141] 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.* [-18], pages 65–69. URL: EKbib/09/KYZ09.pdf.

[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* [-19], 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* [-19], 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.* [-20], 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.* [-21], 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.* [-21], pages 203–204. URL: EKbib/07/KLSYZ07.pdf.

[132] 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.

[131] 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.* [-23], pages 169–176. URL: EKbib/06/KYZ06.pdf.

[130] 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.* [-23], pages 162–168. URL: EKbib/06/KaKoi06.pdf.

[129] Erich Kaltofen and Lihong Zhi. Hybrid symbolic-numeric computation. In *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.* [-23], page 7. Tutorial abstract. URL: EKbib/06/KaZhi06.pdf.

[128] Erich Kaltofen and Pascal Koiran. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In *ISSAC'05 Proc. 2005 Internat. Symp. Symbolic Algebraic Comput.* [-24], pages 208–215. ACM SIGSAM's ISSAC 2005 Distinguished Paper Award. URL: EKbib/05/KaKoi05.pdf.

[127] 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.* [-24], pages 216–223. URL: EKbib/05/KMY05.pdf.

[126] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Structured low rank approximation of a Sylvester matrix. In *Symbolic-Numeric Computation* [-22], pages 69–83. Preliminary version in [-25], pp. 188–201. URL: EKbib/05/KYZ05.pdf.

[125] 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.

[124] 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.

[123] 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.* [-26], pages 167–174. ACM SIGSAM's ISSAC 2004 Distinguished Student Author Award (May and Yang). URL: EKbib/04/GKMYZ04.pdf.

[122] 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.

[121] Wayne Eberly and Erich Kaltofen. Early termination in Shoup's algorithm for the minimum polynomial of an algebraic number. 16 pages, 2004.

[120] 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.

[119] 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.

[118] Erich Kaltofen and John May. On approximate irreducibility of polynomials in several variables. In *ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput.* [-27], pages 161–168. URL: EKbib/03/KM03.pdf.

[117] Erich Kaltofen. Polynomial factorization: a success story. In *ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput.* [-27], pages 3–4. Abstract for invited talk. URL: EKbib/03/Ka03.pdf.

[116] 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.

[115] 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.

[114] 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)* [-29], pages 101–108. Journal version in [119]. URL: EKbib/02/GKL02.pdf.

[113] Erich Kaltofen. An output-sensitive variant of the baby steps/giant steps determinant algorithm. In *Proc. 2002 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'02)* [-29], pages 138–144. URL: EKbib/02/Ka02.pdf.

[112] 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* [-28], pages 40–50. URL: EKbib/02/Detal02.pdf.

[111] 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.

[110] E. Kaltofen and G. Villard. On the complexity of computing determinants. In *Proc. Fifth Asian Symposium on Computer Mathematics (ASCM 2001)* [-30], pages 13–27. Invited contribution; extended abstract, journal version in [125]. URL: EKbib/01/KaVi01.pdf; Maple 6 worksheet URL: EKbib/01/KaVi01.mws.

[109] 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.

[108] 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)* [-31], pages 192–201. URL: EKbib/2K/KLL2K.pdf.

[107] 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.

[106] 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)* [-32], pages 205–212. URL: EKbib/99/HKL99.pdf.

[105] L. Bernardin, B. Char, and E. Kaltofen. Symbolic computation in Java: an appraisement. In *Proc. 1999 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'99)* [-32], pages 237–244. URL: EKbib/99/BCK99.pdf.

[104] E. Kaltofen and M. Monagan. On the genericity of the modular polynomial GCD algorithm. In *Proc. 1999 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'99)* [-32], pages 59–66. URL: EKbib/99/KaMo99.pdf.

[103] 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.

[102] 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.

[101] 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.

[100] 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)* [-33], pages 236–243. URL: EKbib/98/HiKa98.pdf.

[99] 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)* [-33], pages 30–37. URL: EKbib/98/DiKa98.pdf.

[98] 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.

[97] 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.

[96] 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 [102]. URL: EKbib/97/DKP97.ps.gz.

[95] W. Eberly and E. Kaltofen. On randomized Lanczos algorithms. In *Proc. 1997 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'97)* [-34], pages 176–183. URL: EKbib/97/EbKa97.pdf.

[94] 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)* [-34], pages 184–188. URL: EKbib/97/KaSh97.pdf.

[93] 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.

[92] M. Hitz and E. Kaltofen, editors. *Proc. Second Internat. Symp. Parallel Symbolic Comput. PASCO '97*, New York, N. Y., 1997. ACM Press.

[91] 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.

[90] 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 [103]. URL: EKbib/96/KaLo96_hpc.pdf.

[89] M. Samadani and E. Kaltofen. On distributed scheduling using load prediction from past information. Unpublished paper, 1996.

[88] E. Kaltofen and A. Lobo. On rank properties of Toeplitz matrices over finite fields. In *Proc. 1996 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'96)* [-35], pages 241–249. URL: EKbib/96/KaLo96_issac.pdf.

[87] Ú. Erlingsson, E. Kaltofen, and D. Musser. Generic Gram-Schmidt orthogonalization by exact division. In *Proc. 1996 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'96)* [-35], pages 275–282. URL: EKbib/96/EKM96.pdf.

[86] E. Kaltofen. Effective Noether irreducibility forms and applications. *J. Comput.*

System Sci., 50(2):274–295, 1995. URL: EKbib/95/Ka95_jcss.pdf.

[85] 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/DHKLV95.pdf.

[84] 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.

[83] 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 [98]. URL: EKbib/95/KaSh95.ps.gz.

[82] 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)* [-36], pages 232–239. URL: EKbib/95/DiKa95.ps.gz.

[81] 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.

[80] 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 [79, 89].

[79] 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 [89]. URL: EKbib/95/SaKa95_poster.ps.gz.

[78] E. Kaltofen. Asymptotically fast solution of Toeplitz-like singular linear systems. In ISSAC'94 [-37], pages 297–304. Journal version in [81]. URL: EKbib/94/Ka94_issac.pdf.

[77] E. Kaltofen and A. Lobo. Factoring high-degree polynomials by the black box Berlekamp algorithm. In ISSAC'94 [-37], pages 90–98. URL: EKbib/94/KaLo94.ps.gz.

[76] 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.

[75] 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. PASCO '94* [-38], pages 225–233. URL: EKbib/94/KaPa94.pdf.

[74] 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.

[73] 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. AAECC-10*, volume 673 of *Lect. Notes Comput. Sci.*, pages 195–212, Heidelberg, Germany, 1993. Springer Verlag. Journal version in [81]. URL: EKbib/93/Ka93_aaecc.ps.gz.

[72] 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 [85]. URL: EKbib/93/DHKLV93.pdf.

[71] 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.

[70] 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.

[69] 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.

[68] E. Kaltofen. On computing determinants of matrices without divisions. In *Proc. 1992 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'92)* [-39], pages 342–349. URL: EKbib/92/Ka92_issac.pdf.

[67] 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.

[66] E. Kaltofen. Efficient solution of sparse linear systems. Lect. Notes, Rensselaer Polytechnic Instit., Dept. Comput. Sci., Troy, New York, 1992.

[65] 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; [32] contains an alternate algorithm.

[64] 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 [86].

[63] 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.

[62] 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)* [-40], pages 323–332. URL: EKbib/91/DKSV91.pdf.

[61] 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.

[60] 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.

[59] 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. AAECC-9*, volume 539 of *Lect. Notes Comput. Sci.*, pages 29–38, Heidelberg, Germany, 1991. Springer Verlag. URL: EKbib/91/KaSa91.pdf.

[58] 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.

[57] 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.

[56] E. Kaltofen. Computing the irreducible real factors and components of an algebraic curve. *Applic. Algebra Engin. Commun. Comput.*, 1(2):135–148, 1990. URL: EKbib/90/Ka90_aaecc.pdf.

[55] 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.

[54] 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.

[53] 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.

[52] E. Kaltofen, editor. *Algebraic Computational Complexity.* Academic Press, London, October 1990. Special issue volume 9, number 3 (March 1990) of *J. Symbolic Comput.*

[51] 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 [56].

[50] E. Kaltofen and S. M. Watt, editors. *Computers and Mathematics.* Springer Verlag, Heidelberg, Germany, 1989.

[49] E. Kaltofen, T. Valente, and N. Yui. An improved Las Vegas primality test. In *Proc. 1989 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'89)* [-41], pages 26–33. URL: EKbib/89/KVY89.pdf.

[48] 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)* [-41], pages 121–128. URL: EKbib/89/CKL89.pdf.

[47] 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 [46]. URL: EKbib/89/Ka89_parallel.ps.gz.

[46] E. Kaltofen. Processor efficient parallel computation of polynomial greatest common divisors. Unpublished paper included in [47]. URL: EKbib/89/Ka89_gcd.ps.gz, July 1989.

[45] 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.

[44] 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 [55].

[43] 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., Greenwhich, Connecticut, 1989. URL: EKbib/89/Ka89_slpfac.pdf.

[42] 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.

[41] 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.

[40] 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.

[39] E. Kaltofen and Lakshman Yagati. Improved sparse multivariate polynomial interpolation algorithms. In *Symbolic Algebraic Comput. Internat. Symp. ISSAC '88 Proc.* [-42], pages 467–474. URL: EKbib/88/KaLa88.pdf.

[38] 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.

[37] 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 [58].

[36] E. Kaltofen. Deterministic irreducibility testing of polynomials over large finite fields. *J. Symbolic Comput.*, 4:77–82, 1987. URL: EKbib/87/Ka87_jsc.pdf.

[35] 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.

[34] 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.

[33] 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.

[32] David G. Cantor and Erich Kaltofen. Fast multiplication of polynomials over arbitrary rings. Technical Report 87-35, Rensselaer Polytechnic Instit., Dept. Comput. Sci., Troy, N. Y., December 1987. URL: EKbib/87/CaKa87_techrep.pdf; [65] contains an alternate algorithm.

[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 [40] and [43]. 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)* [-43], pages 65–70. Journal version in [33] and [55].

[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)* [-43], pages 169–175. Journal version in [41].

[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 [38].

[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 [40] and [43].

[23] E. Kaltofen. Sparse Hensel lifting. In *EUROCAL 85 European Conf. Comput. Algebra Proc. Vol. 2* [-44], 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* [-44], pages 279–288. Journal version in [45].

[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.pdf.

[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* [-45], 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* [-45], pages 310–320. URL: EKbib/84/KaYui84_eurosam.pdf.

[13] E. Kaltofen. A note on the Risch differential equation. In *Proc. EUROSAM '84* [-45], pages 359–366. URL: EKbib/84/Ka84_risch.pdf.

[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] Carlos Arreche, editor. *ISSAC '18 Proc. 2018 ACM Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2018. Association for Computing Machinery.

[-2] Michael Burr, editor. *ISSAC '17 Proc. 2017 ACM Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2017. Association for Computing Machinery.

[-3] Markus Rosenkranz, editor. *ISSAC'16 Proc. 2016 ACM Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2016. Association for Computing Machinery.

[-4] *ISSAC'15 Proc. 2015 ACM Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2015. Association for Computing Machinery.

[-5] Ruyong Feng, Wen-shin Lee, and Yosuke Sato, editors. *Computer Mathematics 9th Asian Symp. (ASCM2009), Fukuoka, 10th Asian Symp. (ASCM2012), Beijing.* Springer, DOI: 10.1007/978-3-662-43799-5, 2014.

[-6] Jan Verschelde and Stephen M. Watt, editors. *SNC'14 Proc. 2014 Internat. Workshop on Symbolic-Numeric Comput.*, New York, N. Y., 2014. Association for Computing Machinery.

[-7] Katsusuke Nabeshima, editor. *ISSAC 2014 Proc. 39th Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2014. Association for Computing Machinery.

[-8] Manuel Kauers, editor. *ISSAC 2013 Proc. 38th Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2013. Association for Computing Machinery.

[-9] Joris van der Hoeven and Mark van Hoeij, editors. *ISSAC 2012 Proc. 37th Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2012. Association for Computing Machinery.

[-10] Björn Enquist, editor. *Encyclopedia of Applied and Computational Mathematics.* Springer, 2015, to appear. Mathematics of Computer Science, Discrete Mathematics, Håstad, Johan (field editor).

[-11] Gary L. Mullen and Daniel Panario, editors. *Handbook of Finite Fields.* CRC Press, Taylor & Francis Group, Boca Raton, Florida, 2013.

[-12] Ulrich Langer and Peter Paule, editors. *Numeric and Symbolic Scientific Computing Progress and Prospects.* Springer Verlag, Wien, 2012.

[-13] M. Moreno Maza, editor. *SNC'11 Proc. 2011 Internat. Workshop on Symbolic-Numeric Comput.*, New York, N. Y., 2011. Association for Computing Machinery.

[-14] Anton Leykin, editor. *Proc. 2011 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2011*, New York, N. Y., 2011. Association for Computing Machinery.

[-15] 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.

[-16] M. Moreno Maza and Jean-Louis Roch, editors. *PASCO'10 Proc. 2010 Internat. Workshop on Parallel Symbolic Comput.*, New York, N. Y., 2010. Association for Computing Machinery.

[-17] Stephen M. Watt, editor. *Proc. 2010 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2010*, New York, N. Y., 2010. Association for Computing Machinery.

[-18] Hiroshi Kai and Hiroshi Sekigawa, editors. *SNC'09 Proc. 2009 Internat. Workshop on Symbolic-Numeric Comput.*, New York, N. Y., 2009. ACM Press.

[-19] David Jeffrey, editor. *ISSAC 2008*, New York, N. Y., 2008. ACM Press.

[-20] Christopher W. Brown, editor. *ISSAC 2007 Proc. 2007 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2007. ACM Press.

[-21] Jan Verschelde and Stephen M. Watt, editors. *SNC'07 Proc. 2007 Internat. Workshop on Symbolic-Numeric Comput.*, New York, N. Y., 2007. ACM Press.

[-22] Dongming Wang and Lihong Zhi, editors. *Symbolic-Numeric Computation*. Trends in Mathematics. Birkhäuser Verlag, Basel, Switzerland, 2007.

[-23] Jean-Guillaume Dumas, editor. *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2006. ACM Press.

[-24] Manuel Kauers, editor. *ISSAC'05 Proc. 2005 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2005. ACM Press.

[-25] 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.

[-26] Jaime Gutierrez, editor. *ISSAC 2004 Proc. 2004 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2004. ACM Press.

[-27] J. R. Sendra, editor. *ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2003. ACM Press.

[-28] Arjeh M. Cohen, Xiao-Shan Gao, and Nobuki Takayama, editors. *Proc. First Internat. Congress Math. Software ICMS 2002, Beijing, China*, Singapore, 2002. World Scientific.

[-29] T. Mora, editor. *ISSAC 2002 Proc. 2002 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2002. ACM Press.

[-30] 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.

[-31] C. Traverso, editor. *Internat. Symp. Symbolic Algebraic Comput. ISSAC 2000 Proc. 2000 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2000. ACM Press.

[-32] S. Dooley, editor. *ISSAC 99 Proc. 1999 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1999. ACM Press.

[-33] O. Gloor, editor. *ISSAC 98 Proc. 1998 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1998. ACM Press.

[-34] W. Küchlin, editor. *ISSAC 97 Proc. 1997 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1997. ACM Press.

[-35] Lakshman Y. N., editor. *ISSAC 96 Proc. 1996 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1996. ACM Press.

[-36] A. H. M. Levelt, editor. *Proc. 1995 Internat. Symp. Symbolic Algebraic Comput. ISSAC'95*, New York, N. Y., 1995. ACM Press.

[-37] *ISSAC '94 Proc. Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1994. ACM Press.

[-38] H. Hong, editor. *First Internat. Symp. Parallel Symbolic Comput. PASCO '94*, Singapore, 1994. World Scientific Publishing Co.

[-39] P. S. Wang, editor. *Internat. Symp. Symbolic Algebraic Comput. 92*, New York, N. Y., 1992. ACM Press.

[-40] S. M. Watt, editor. *Proc. 1991 Internat. Symp. Symbolic Algebraic Comput. ISSAC'91*, New York, N. Y., 1991. ACM Press.

[-41] *Proc. ACM-SIGSAM 1989 Internat. Symp. Symbolic Algebraic Comput. ISSAC '89*, New York, N. Y., 1989. ACM Press.

[-42] P. Gianni, editor. *Symbolic Algebraic Comput. Internat. Symp. ISSAC '88 Proc.*, volume 358 of *Lect. Notes Comput. Sci.*, Heidelberg, Germany, 1988. Springer Verlag.

[-43] B. W. Char, editor. *Proc. 1986 Symp. Symbolic Algebraic Comput. Symsac '86*, New York, N. Y., 1986. ACM.

[-44] B. F. Caviness, editor. *EUROCAL 85 European Conf. Comput. Algebra Proc. Vol. 2*, Lect. Notes Comput. Sci., Heidelberg, Germany, 1985. Springer Verlag.

[-45] J. Fitch, editor. *EUROSAM 84 Internat. Symp. Symbolic Algebraic Comput. Proc.*, Lect. Notes Comput. Sci., Heidelberg, Germany, 1984. Springer Verlag.

2 How to Access the Bib Files

My publication list with clickable links to retrieve the papers and BibTeX citation entries is posted on the Internet in three forms.

1. The BibTeX database files, BASE/kaltofen.bib, BASE/strings.bib, and BASE/crossrefs.bib. Note that my bibliography file is viewable in an html browser, although you may have to change the suffix to .html, or make a symbolic link/shortcut with a .html suffix to it. The locations of my papers are mirrored in the ekurl fields, so that you can retrieve my papers by viewing the downloaded BASE/kaltofen.bib file in your browser. The talk field is used for links to talks that discuss the material in the papers, e.g., at the conferences where the papers were presented. If you reuse my transparencies, please acknowledge their origin.

2. An Internet html document BASE/index.html produced by LaTeX2HTML.

3. A pdf document BASE/kaltofen.pdf with hyperlinks that are in the note fields of my bibliography file BASE/kaltofen.bib. The links can be reproduced using the hyperref.sty package and defining the EKhref macro.