

Field Theory

Computational Methods

12-04

- [1] Gregory V. Bard, Nicolas T. Courtois, and Chris Jefferson. Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over $\text{GF}(2)$ via SAT-solvers. *IACR eprint:2007:024*, 14 pages, 2007.
- [2] Thomas Beth, Jörn Müller-Quade, and Rainer Steinwandt. Computing restrictions of ideals in finitely generated k -algebras by means of Buchberger's algorithm. *J. Symbolic Comput.*, 41(3-4):372–380, 2006.
- [3] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt. Complexity issues in bivariate polynomial factorization. In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 42–49, New York, NY, USA, 2004. ACM Press.
- [4] Guillaume Chèze and Grégoire Lecerf. Lifting and recombination techniques for absolute factorization. *J. Complexity*, 23(3):380–420, 2007.
- [5] Akpodigha Filatei, Xin Li, Marc Moreno Maza, and Éric Schost. Implementation techniques for fast polynomial arithmetic in a high-level programming environment. In *ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, pages 93–100, New York, NY, USA, 2006. ACM Press.
- [6] Katharina Geissler and Jürgen Klüners. Galois group computation for rational polynomials. *J. Symbolic Comput.*, 30(6):653–674, 2000.
- [7] Kiran S. Kedlaya. Search techniques for root-unitary polynomials. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 71–81. Amer. Math. Soc., Providence, RI, 2008.
- [8] Sara Khodadad and Michael Monagan. Fast rational function reconstruction. In *ISSAC 2006*, pages 184–190. ACM, New York, 2006.

- [9] Hsin-Chao Liao and Richard J. Fateman. Evaluation of the heuristic polynomial GCD. In *ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation*, pages 240–247, New York, NY, USA, 1995. ACM Press.
- [10] Michael Monagan. Maximal quotient rational reconstruction: An almost optimal algorithm for rational reconstruction. In *ISSAC 2004*, pages 243–249. ACM, New York, 2004.
- [11] Jörn Müller-Quade and Rainer Steinwandt. Basic algorithms for rational function fields. *J. Symbolic Comput.*, 27(2):143–170, 1999.
- [12] Jörn Müller-Quade and Rainer Steinwandt. Gröbner bases applied to finitely generated field extensions. *J. Symbolic Comput.*, 30(4):469–490, 2000.
- [13] Leonard Soicher and John McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3):273–281, 1985.
- [14] Allan Steel. A new scheme for computing with algebraically closed fields. In *Algorithmic Number Theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 491–505. Springer, Berlin, 2002.
- [15] Allan K. Steel. Computing with algebraically closed fields. *J. Symbolic Comput.*, To appear, 2009.
- [16] Rainer Steinwandt. On computing a separating transcendence basis. *SIGSAM Bulletin*, 34(4), 2000.