Computational Methods

13-04

[1] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze, *Computation of the decomposition group of a triangular ideal*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 3-4, 279–294. MR MR2104299 (2005h:13036)

[2] Fatima Abu Salem, Shuhong Gao, and Alan G. B. Lauder, *Factoring polynomials via polytopes*, ISSAC 2004, ACM, New York, 2004, pp. 4–11. MR MR2126918 (2006a:13040)

[3] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita, *Comparison between XL and Gröbner basis algorithms*, Advances in Cryptology—Asiacrypt 2004, Lecture Notes in Comput. Sci., vol. 3329, Springer, Berlin, 2004, pp. 338–353. MR MR2150425 (2006k:13056)

[4] Philippe Aubry and Marc Moreno Maza, *Triangular sets for solving polynomial systems: A comparative implementation of four methods*, J. Symbolic Comput. **28** (1999), no. 1-2, 125–154, Polynomial elimination—algorithms and applications. MR MR1709420 (2000g:13017)

[5] Mohamed Ayad and Peter Fleischmann, *On the decomposition of rational functions*, J. Symbolic Comput. **43** (2008), no. 4, 259–274. MR MR2402031 (2009a:13047)

[6] Bernd Bank, Marc Giusti, Joos Heintz, Mohab Safey El Din, and Eric Schost, *On the geometry of polar varieties*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 1, 33–83. MR 2585564

[7] Aurélie Bauer and Antoine Joux, *Toward a rigorous variation of Coppersmith's algorithm on three variables*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 361–378. MR MR2449220

[8] Karim. Belabas, Mark van Hoeij, J. Klüners, and Allan Steel, *Factoring polynomials over global fields*, Journal de Théorie des Nombres de Bordeaux (2009), no. 21, 15–39.

[9] 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** (2006), no. 3-4, 372–380. MR MR2202557 (2006j:13027)

[10] Alin Bostan, Bruno Salvy, and Éric Schost, *Fast algorithms for zero-dimensional polynomial systems using duality*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 4, 239–272. MR MR2020362 (2005b:13050)

[11] Richard Brent and Paul Zimmermann, *A multi-level blocking distinct degree factorization algorithm*, Finite Fields and Applications, Contemporary Mathematics, vol. 461, 2008.

[12] Michael Brickenstein and Alexander Dreyer, *PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials*, J. Symbolic Comp. **44** (2009), no. 9, 1326–1345.

[13] Michael Brickenstein, Alexander Dreyer, Gert-Martin Greuel, Markus Wedler, and Oliver Wienand, *New developments in the theory of Gröbner bases and applications to formal verification*, J. Pure Appl. Algebra **213** (2009), no. 8, 1612–1635. MR MR2517997

[14] Stanislav Bulygin and Ruud Pellikaan, *Bounded distance decoding of linear error-correcting codes with Gröbner bases*, J. Symb. Comput. **44** (2009), no. 12, 1626–1643.

[15] Daniel Cabarcas, *An Implementation of Faugère's F4 Algorithm for Computing Gröbner Bases*, Master of Science Thesis, University of Cincinnati, 2010.

[16] G. Chèze and S. Najib, *Indecomposability of polynomials via Jacobian matrix*, J. Algebra **324** (2010), no. 1, 1–11. MR 2646027

[17] Mihai Cipu, *Gröbner bases and Diophantine analysis*, J. Symbolic Comput. **43** (2008), no. 10, 681–687. MR MR2426566

[18] Jennifer de Kleine, Michael Monagan, and Allan Wittkopf, *Algorithms for the non-monic case of the sparse modular GCD algorithm*, Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation: ISSAC'05, ACM, New York, 2005, pp. 124–131 (electronic). MR MR2280538

[19] Wolfram Decker and Theo de Jong, *Gröbner bases and invariant theory*, Gröbner bases and applications (Linz, 1998), London Math. Soc. Lecture Note Ser., vol. 251, Cambridge Univ. Press, Cambridge, 1998, pp. 61–89. MR MR1699814 (2000m:13007)

[20] Harm Derksen, *Computation of invariants for reductive groups*, Adv. Math. **141** (1999), no. 2, 366–384. MR MR1671758 (2000a:13013)

[21] Harm Derksen and Gregor Kemper, *Computational Invariant Theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002, , Encyclopaedia of Mathematical Sciences, 130. MR MR1918599 (2003g:13004)

[22] Clémence Durvye and Grégoire Lecerf, *A concise proof of the Kronecker polynomial system solver from scratch*, Expo. Math. **26** (2008), no. 2, 101–139. MR MR2413831

[23] Tobias Eibach, Enrico Pilz, and Gunnar Völkel, *Attacking Bivium using SAT solvers*, Theory and Applications of Satisfiability Testing, SAT 2008, Lecture Notes in Computer Science, vol. 4996, Springer, Berlin, 2008, pp. 63–76.

[24] Tobias Eibach, Gunnar Völkel, and Enrico Pilz, *Optimising Gröbner bases on Bivium*, Math. Comput. Sci. **3** (2010), no. 2, 159–172.

[25] Nicholas Eriksson, *Toric ideals of homogeneous phylogenetic models*, ISSAC 2004, ACM, New York, 2004, pp. 149–154. MR MR2126937 (2005j:92017)

[26] Jeffrey B. Farr and Shuhong Gao, *Computing Gröbner bases for vanishing ideals of finite sets of points*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes, Lecture Notes in Comput. Sci., vol. 3857, Springer, Berlin, 2006, pp. 118–127. MR MR2243500 (2007c:13039)

[27] ———, *Gröbner bases and generalized Padé approximation*, Math. Comp. **75** (2006), no. 253, 461–473 (electronic). MR MR2176409

[28] Jean-Charles Faugère, Guillaume Moroz, Fabrice Rouillier, and Mohab Safey El Din, *Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities*, ISSAC '08: International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM, 2008, pp. 79–86.

[29] Akpodigha Filatei, *Implementation of fast polynomial arithmentic in Aldor*, Master of Science thesis, University of Western Ontario, 2006.

[30] Shuhong Gao, Daqing Wan, and Mingsheng Wang, *Primary decomposition of zero-dimensional ideals over finite fields*, Math. Comp. **78** (2009), no. 265, 509–521. MR MR2448718

[31] Karin Gatermann, *Computer algebra methods for equivariant dynamical systems*, Lecture Notes in Mathematics, vol. 1728, Springer-Verlag, Berlin, 2000. MR MR1755001 (2001k:37040)

[32] Karin Gatermann and Frédéric Guyard, *Gröbner bases, invariant theory and equivariant dynamics*, J. Symbolic Comput. **28** (1999), no. 1-2, 275–302, Polynomial elimination—algorithms and applications. MR MR1709907 (2000f:13006)

[33] V. P. Gerdt and Yu. A. Blinkov, *On selection of nonmultiplicative prolongations in computation of Janet bases*, Programming and Computer Software **33** (2007), no. 3, 147–153.

[34] V. P. Gerdt and Yu. A. Blinkov, *Strategies for selecting non-multiplicative prolongations in computing Janet bases*, Programmirovanie (2007), no. 3, 34–43. MR MR2347312

[35] Vladimir P. Gerdt, *Involutive algorithms for computing Gröbner bases*, Computational Commutative and Non-commutative Algebraic Geometry, NATO Sci. Ser. III Comput. Syst. Sci., vol. 196, IOS, Amsterdam, 2005, pp. 199–225. MR MR2179201

[36] Vladimir P. Gerdt and Yuri A. Blinkov, *On computing Janet bases for degree compatible orderings*, Proceedings of the 10th Rhine Workshop on Computer Algebra (Basel), 2006, University of Basel, Basel, 2006, pp. 107–117.

[37] Massimo Giulietti, *Inviluppi di k-archi in piani proiettivi sopra campi finiti e basi di Gröbner*, Rendiconti del Circolo Matematico di Palermo **48** (1999), no. 1, 191–200.

[38] Marc Giusti, Grégoire Lecerf, and Bruno Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211. MR MR1817612 (2002b:68123)

[39] Marc Giusti and Éric Schost, *Solving some overdetermined polynomial systems*, ISSAC '99: Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC) (New York), ACM, 1999, pp. 1–8 (electronic). MR MR1802060 (2002b:65084)

[40] Hoans-Christian Graf von Bothmer, Oliver Labs, Josef Schicho, and Christiaan van de Woestijne, *The Casas-Alvero conjecture for infinitely many degrees*, J. Algebra **316** (2007), no. 1, 224–230. MR MR2354861

[41] Gert-Martin Greuel, Santiago Laplagne, and Frank Seelisch, *Normalization of rings*, J. Symbolic Comput. **45** (2010), no. 9, 887–901.

[42] Renault Guénaél and Yokoyama Kazuhiro, *Multi-modular algorithm for computing the splitting field of a polynomial*, ISSAC '08: International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM, 2008, pp. 247–254.

[43] David Harvey, *A cache-friendly truncated FFT*, Theor. Comput. Sci. **410** (2009), no. 27-29, 2649–2658.

[44] David Harvey, *Faster polynomial multiplication via multipoint Kronecker substitution*, J. Symbolic Comp. **44** (2009), no. 10, 1502–1510.

[45] Mikael Johansson, *Computation of Poincaré-Betti series for monomial rings*, Rend. Istit. Mat. Univ. Trieste **37** (2005), no. 1-2, 85–94 (2006). MR MR2227050 (2007b:13020)

[46] Gregor Kemper, *Computational invariant theory*, The Curves Seminar at Queen's. Vol. XII (Kingston, ON, 1998), Queen's Papers in Pure and Appl. Math., vol. 114, Queen's Univ., Kingston, ON, 1998, pp. 5–26. MR MR1690811 (2000c:13007)

[47] ———, *An algorithm to calculate optimal homogeneous systems of parameters*, J. Symbolic Comput. **27** (1999), no. 2, 171–184. MR MR1672128 (2000a:13046)

[48] ———, *The calculation of radical ideals in positive characteristic*, J. Symbolic Comput. **34** (2002), no. 3, 229–238. MR MR1935080 (2003j:13039)

[49] ———, *Computing invariants of reductive groups in positive characteristic*, Transform. Groups **8** (2003), no. 2, 159–176. MR MR1976458 (2004b:13006)

[50] Simon King, *Fast computation of secondary invariants*, 2007.

[51] ———, *Minimal generating sets of non-modular invariant rings of finite groups*, 2007.

[52] Alexey Koloydenko, *Symmetric measures via moments*, Bernoulli **14** (2008), no. 2, 362–390.

[53] Teresa Krick, *Straight-line programs in polynomial equation solving*, Foundations of Computational Mathematics: Minneapolis, 2002, London Math. Soc. Lecture Note Ser., vol. 312, Cambridge Univ. Press, Cambridge, 2004, pp. 96–136. MR MR2189629

[54] G. Lecerf, *Quadratic Newton iteration for systems with multiplicity*, Found. Comput. Math. **2** (2002), no. 3, 247–293. MR MR1907381 (2003f:65090)

[55] Grégoire Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity **19** (2003), no. 4, 564–596. MR MR1991984 (2004j:68200)

[56] ———, *Fast separable factorization and applications*, Appl. Algebra Engrg. Comm. Comput. **19** (2008), no. 2, 135–160. MR MR2389971 (2009b:13069)

[57] ———, *New recombination algorithms for bivariate polynomial factorization based on Hensel lifting*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 2, 151–176. MR 2600710

[58] Xin Li, Marc Moreno Maza, Raqeeb Rasheed, and Eric Schost, *High-performance symbolic computation in a hybrid compiled-interpreted programming environment*, International Conference on Computational Sciences and Its Applications. ICCSA. June 30- July 3, 2008, 2008, pp. 331–341.

[59] Xin Li, Marc Moreno Maza, and Éric Schost, *Fast arithmetic for triangular sets: from theory to practice*, ISSAC 2007, ACM, New York, 2007, pp. 269–276. MR MR2402271

[60] Xin Li, Marc Moreno Maza, and Éric Schost, *Fast arithmetic for triangular sets: from theory to practice*, J. Symbolic Comput. **44** (2009), no. 7, 891–907. MR MR2522589

[61] A. Marschner and J. Müller, *On a certain algebra of higher modular forms*, Algebra Colloq. **16** (2009), 371–380.

[62] Mbakop Guy Merlin, *Eziente losung reeller polynomialer gleichungssysteme*, PhD Thesis, Humboldt-Universität, Berlin, 1999.

[63] V. A. Mityunin and E. V. Pankratiev, *Parallel algorithms for Gröbner-basis construction*, J. Math. Sci. (N. Y.) **142** (2007), no. 4, 2248–2266.

[64] Michael Monagan and Mark van Hoeij, *A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions.*

[65] Teo Mora, *The FGLM problem and Möller's algorithm on zero-dimensional ideals*, Sala, Massimiliano (ed.) and Mora, Teo (ed.) and Perret, Ludovic (ed.) and Sakata, Shojiro (ed.) and Traverso, Carlo (ed.), Gröbner Bases, Coding, and Cryptography, Springer, Berlin, 2009.

[66] Marc Moreno Maza, Greg Reid, Robin Scott, and Wenyuan Wu, *On approximate triangular decompositions in dimension zero*, J. Symbolic Comput. **42** (2007), no. 7, 693–716. MR MR2348057

[67] Bernard Mourrain, *Generalized normal forms and polynomial system solving*, ISSAC'05: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2005, pp. 253–260 (electronic). MR MR2280555

[68] Bernard Mourrain and Philippe Trébuchet, *Stable normal forms for polynomial system solving*, Theoret. Comput. Sci. **409** (2008), no. 2, 229–240. MR MR2474338 (2009m:13036)

[69] Jörn Müller-Quade and Rainer Steinwandt, *Basic algorithms for rational function fields*, J. Symbolic Comput. **27** (1999), no. 2, 143–170. MR MR1672124 (2000a:13043)

[70] ———, *Gröbner bases applied to finitely generated field extensions*, J. Symbolic Comput. **30** (2000), no. 4, 469–490. MR MR1784753 (2001i:13040)

[71] G. H. Norton and A. Salagean, *Cyclic codes and minimal strong Gröbner bases over a principal ideal ring*, Finite Fields Appl. **9** (2003), no. 2, 237–249. MR MR1968033 (2004d:13039)

[72] Graham H. Norton and Ana Sălăgean, *Strong Gröbner bases for polynomials over a principal ideal ring*, Bull. Austral. Math. Soc. **64** (2001), no. 3, 505–528. MR MR1878902 (2003a:13036)

[73] Daniel Robertz, *Noether normalization guided by monomial cone decompositions*, J. Symbolic Comput. **44** (2009), no. 10, 1359–1373. MR MR2543424

[74] Fabrice Rouillier, Mohab Safey El Din, and Éric Schost, *Solving the Birkhoff interpolation problem via the critical point method: An experimental study*, ADG '00: Revised Papers from the Third International Workshop on Automated Deduction in Geometry (Zurich, 2000) (Jürgen Richter-Gebert and Dongming Wang, eds.), Lecture Notes in Computer Science, vol. 2061, Springer-Verlag, Berlin, 2001, Lecture Notes in Artificial Intelligence, pp. viii+325. MR MR1908025 (2003a:68007)

[75] Luciano Sbaiz, Patrick Vandewalle, and Martin Vetterli, *Groebner basis methods for multichannel sampling with unknown offsets*, Appl. Comput. Harmon. Anal. **25** (2008), no. 3, 277 – 294.

[76] Roberto La Scala and Viktor Levandovskyy, *Letterplace ideals and non-commutative Gröbner bases*, J. Symbolic Comp. **44** (2009), no. 10, 1374–1393.

[77] Éric Schost, *Degree bounds and lifting techniques for triangular sets*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2002, pp. 238–245 (electronic). MR MR2035255 (2005a:13054)

[78] ———, *Complexity results for triangular sets*, J. Symbolic Comput. **36** (2003), no. 3-4, 555–594, International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille). MR MR2004042 (2004m:68295)

[79] ———, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), no. 5, 349–393. MR MR1959170 (2003k:13035)

[80] R. James Shank and David L. Wehlau, *Computing modular invariants of p-groups*, J. Symbolic Comput. **34** (2002), no. 5, 307–327. MR MR1937464 (2003j:13006)

[81] Jessica Sidman and Seth Sullivant, *Prolongations and computational algebra*, Canad. J. Math. **61** (2009), no. 4, 930–949. MR MR2541390

[82] Allan Steel, *Conquering inseparability: Primary decomposition and multivariate factorization over algebraic function fields of positive characteristic*, J. Symbolic Comput. **40** (2005), no. 3, 1053–1075. MR MR2167699

[83] Till Stegers, *Faugère's F5 algorithm revisited*, Masters thesis, Technische Universiteit Darmstadt, 2005.

[84] Rainer Steinwandt, *Decomposing systems of polynomial equations*, Computer Algebra in Scientific Computing—CASC'99 (Munich), Springer, Berlin, 1999, pp. 387–407. MR MR1729638 (2000j:12012)

[85] ———, *Implicitizing without tag variables*, Proceedings of the 8th Rhine Workshop on Computer Algebra, 2002, pp. 217–224.

[86] Rainer Steinwandt and Jörn Müller-Quade, *Freeness, linear disjointness, and implicitization—a classical approach*, Beiträge Algebra Geom. **41** (2000), no. 1, 57–66. MR MR1745579 (2001a:12011)

[87] Mark van Hoeij, *Factoring polynomials and the knapsack problem*, J. Number Theory **95** (2002), no. 2, 167–189. MR MR1924096 (2003f:13029)

[88] Pawel Wocjan, *Brill-Noether algorithm construction of geometric Goppa codes and absolute factorization of polynomials*, Ph.D. thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 1999, p. 108.