Noro, Masayuki; **Yokoyama, Kazuhiro**

Usage of modular techniques for efficient computation of ideal operations. (English)

Zbl 1402.13026
Math. Comput. Sci. 12, No. 1, 1-32 (2018).

Modular techniques are a powerful tool in computer algebra to improve the performance of the computations over the field of rationals to avoid the growth of intermediate coefficients. The main idea is to choose some lucky prime numbers, performing the computation modulo these primes and then reconstruct the the desired object by using the Chinese remainder theorem. In [J. Symb. Comput. 35, No. 4, 403–419 (2003; Zbl 1046.13018)], *E. A. Arnold* proposed an approach to test the luckiness of a given prime. For example, she defined a Hilbert lucky prime: A prime number p is called Hilbert lucky prime for an ideal if, modulo p, the Hilbert function of the ideal is preserved. In the paper under review, the authors discuss different notions of a lucky prime which have been already proposed in the literature and define also a new notion of an affine Hilbert lucky prime. In addition, they apply the modular techniques for the computation of Gröbner bases, and some ideal operations.

Reviewer: Amir Hashemi (Isfahan)

MSC:

13P10 Gröbner bases; other bases for ideals and modules (e.g., Janet and border bases)

Keywords:

Gröbner basis; modular computation; ideal operation

Software:

moddiq.lib; SINGULAR

Full Text: DOI

References:

[1] Adams, W.W., Loustaunau, P.: An Introduction to Gröbner Bases. Graduate Studies in Mathematics 3. American Mathematical Society, Providence (1994) · Zbl 0803.13015

[2] Afzal, D., Kanwal, F., Pfister, G., Steidel, S.: Solving via Modular Methods. In: Bridging Algebra, Geometry, and Topology, Springer Proceedings in Mathematics \& Statistics, vol. 96, pp. 1-9 (2014) · Zbl 1328.13037

[3] Arnold, E, Modular algorithms for computing Gröbner bases, J. Symb. Comput., 35, 403-419, (2003) · Zbl 1046.13018 · doi:10.1016/S0747-7171(02)00140-2

[4] Böhm, J; Decker, W; Fieker, C; Pfister, G, The use of bad primes in rational reconstruction, Math. Comput., 84, 3013-3027, (2015) · Zbl 1326.13018 · doi:10.1090/mcom/2951

[5] Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms, Undergraduate Text in Mathematics, 4th edn. Springer, New York (2015) · Zbl 1335.13001 · doi:10.1007/978-3-319-16721-3

[6] Dahan, X; Kadri, A; Schost, É, Bit-size estimates for triangular sets in positive dimension, J. Complex., 28, 109-135, (2012) · Zbl 1246.13039 · doi:10.1016/j.jco.2011.05.001

[7] Dahan, X., Moreno Maza, M., Schost, É., Wu, W., Xie, Y.: Lifting techniques for triangular decompositions. In: Proceedings of ISSAC 2005, pp. 108-115. ACM Press (2005) · Zbl 1360.14146

[8] Dahan, X., Schost, É: Sharp estimates for triangular sets. In: Proceedings of ISSAC 2004, pp. 103-110. ACM Press (2004) · Zbl 1134.13308

[9] Decker, W; Greuel, G-M; Pfister, G; Matzat, BH (ed.); Greuel, GM (ed.); Hiss, G (ed.), Primary decomposition: algorithms and comparisons, 187-220, (1998), Berlin

[10] Faugère, J-C, A new efficient algorithm for computing Gröbner bases (F_4), J. Pure Appl. Algebra, 139, 61-88, (1999) · Zbl 0930.68174 · doi:10.1016/S0022-4049(99)00005-5

[11] Gräbe, H, On lucky primes, J. Symb. Comput., 15, 199-209, (1993) · Zbl 0787.13016 · doi:10.1006/jsco.1993.1014

[12] Greuel, G.-M., Pfister, G.: A Singular Introduction to Commutative Algebra. Springer, Berlin (2002) · Zbl 1023.13001 ·

doi:10.1007/978-3-662-04963-1

[13] Idrees, N; Pfister, G; Steidel, S, Parallelization of modular algorithms, J. Symb. Comput., 46, 672-684, (2011) · Zbl 1229.13002 · doi:10.1016/j.jsc.2011.01.003

[14] Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 2. Springer, Berlin (2005) · Zbl 1090.13021

[15] Orange, S; Renault, G; Yokoyama, K, Efficient arithmetic in successive algebraic extension fields using symmetries, Math. Comput. Sci., 6, 217-233, (2012) · Zbl 1300.12006 · doi:10.1007/s11786-012-0112-y

[16] Noro, M.: Modular algorithms for computing a generating set of the syzygy module. In: Computer Algebra in Scientific Computing CASC 2009, LNCS, vol. 5743, pp. 259-268. Springer (2009) · Zbl 1239.13037

[17] Noro, M; Yokoyama, K, A modular method to compute the rational univariate representation of zero-dimensional ideals, J. Symb. Comput., 28, 243-263, (1999) · Zbl 0945.13010 · doi:10.1006/jsco.1999.0275

[18] Noro, M; Yokoyama, K, Implementation of prime decomposition of polynomial ideals over small finite fields, J. Symb. Comput., 38, 1227-1246, (2004) · Zbl 1137.13318 · doi:10.1016/j.jsc.2003.08.004

[19] Noro, M., Yokoyama, K.: Verification of Gröbner basis candidates. In: Mathematical Software-ICMS 2014, LNCS, vol. 8592, pp. 419-424. Springer (2014) · Zbl 1434.13029

[20] Pauer, F, On lucky ideals for Gröbner bases computations, J. Symb. Comput., 14, 471-482, (1992) · Zbl 0776.13014 · doi:10.1016/0747-7171(92)90018-Y

[21] Pfister, G, On modular computation of standard basis, Anal. Stiint. Univ. Ovidius Constanta, 15, 129-138, (2007) · Zbl 1199.13032

[22] Renault, G., Yokoyama, K.: Multi-modular algorithm for computing the splitting field of a polynomial. In: Proceedings of ISSAC 2008, pp. 247-254. ACM Press (2008)

[23] Romanovski, V; Chen, X; Hu, Z, Linearizability of linear systems perturbed by fifth degree homogeneous polynomials, J. Phys. A Math. Theor., 40, 5905-5919, (2007) · Zbl 1127.34020 · doi:10.1088/1751-8113/40/22/010

[24] Romanovski, V; PreŠern, M, An approach to solving systems of polynomials via modular arithmetics with applications, J. Comput. Appl. Math., 236, 196-208, (2011) · Zbl 1225.13029 · doi:10.1016/j.cam.2011.06.018

[25] Steidel, S, Gröbner bases of symmetric ideals, J. Symb. Comput., 54, 72-86, (2013) · Zbl 1277.13001 · doi:10.1016/j.jsc.2013.01.005

[26] Sasaki, T; Takeshima, T, A modular method for Gröbner-bases construction over ${\mathbb{Q}}$ and solving system of algebraic equations, J. Inf. Process., 12, 371-379, (1989) · Zbl 0757.13012

[27] Sturmfels, B.: Gröbner Bases and Convex Polytopes, AMS University Lecture Series, vol. 8. American Mathematical Society, Providence (1996) · Zbl 0856.13020

[28] Traverso, C.: Gröbner trace algorithms. In: Proceedings of ISSAC 1988, LNCS, vol. 358, pp. 125-138. Springer (1988)

[29] Traverso, C, Hilbert functions and the buchberger algorithm, J. Symb. Comput., 22, 355-376, (1997) · Zbl 0922.13019 · doi:10.1006/jsco.1996.0056

[30] von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, Cambridge (1999) · Zbl 0936.11069

[31] Winkler, F, A p-adic approach to the computation of Gröbner bases, J. Symb. Comput., 6, 287-304, (1988) · Zbl 0669.13009 · doi:10.1016/S0747-7171(88)80049-X

[32] Yokoyama, K.: Usage of modular techniques for efficient computation of ideal operations—(Invited Talk). In: Computer Algebra in Scientific Computing CASC 2012, LNCS, vol. 7442, pp. 361-362 (2012)