Caruso, Xavier; **Le Borgne, Jérémy**

A new faster algorithm for factoring skew polynomials over finite fields. (English)

Zbl 1373.16046
J. Symb. Comput. 79, Part 2, 411-443 (2017).

Summary: In this paper, we provide an algorithm for the factorization of skew polynomials over finite fields. It is faster than the previously known algorithm, which was due to [*M. Giesbrecht*, J. Symb. Comput. 26, No. 4, 463–486 (1998; Zbl 0941.68160)]. There are two main improvements. The first one is obtained through a careful study of the structure of the quotients of a skew polynomial ring, using theoretical results relating skew polynomial rings and Azumaya algebras. The second improvement is provided by giving faster sub-algorithms for the arithmetic in skew polynomial rings, such as multiplication, division, and extended Euclidean division.

MSC:

16S36 Ordinary and skew polynomial rings and semigroup rings
16Z05 Computational aspects of associative rings (general theory)
16H05 Separable algebras (e.g., quaternion algebras, Azumaya algebras, etc.)

Keywords:

skew polynomial; factorization; Azumaya algebra

Full Text: DOI

References:

[1] Anderson, Frank W.; Fuller, Kent R., Rings and categories of modules, Graduate Texts in Mathematics, vol. 13, (1992), Springer-Verlag New York, MR 1245487 (94i:16001) · Zbl 0765.16001

[2] Azumaya, Gorô, On maximally central algebras, Nagoya Math. J., 2, 119-150, (1951), MR 0040287 (12,669g) · Zbl 0045.01103

[3] Bürgisser, Peter; Clausen, Michael; Shokrollahi, M. Amin, Algebraic complexity theory, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 315, (1997), Springer-Verlag Berlin, With the collaboration of Thomas Lickteig. MR 1440179 (99c:68002) · Zbl 1087.68568

[4] Bostan, Alin; Caruso, Xavier; Schost, Éric, A fast algorithm for computing the characteristic polynomial of the \textit{p}-curvature, (ISSAC'14, (2014), ACM New York), 59-66 · Zbl 1325.68265

[5] Gabidulin, È. M., Theory of codes with maximum rank distance, Probl. Pereda. Inf., 21, 1, 3-16, (1985), MR 791529 (87f:94036) · Zbl 0585.94013

[6] Giesbrecht, Mark, Factoring in skew-polynomial rings over finite fields, J. Symb. Comput., 26, 4, 463-486, (1998), MR 1646671 (99i:16053) · Zbl 0941.68160

[7] Grothendieck, Alexander, Le groupe de Brauer. I. algèbres d'Azumaya et interprétations diverses, Sémin. Bourbaki, 9, 199-219, (1964-1966), Soc. Math. France, Paris, Exp. No. 290. MR 1608798 · Zbl 0186.54702

[8] Ikehata, Shûichi, Azumaya algebras and skew polynomial rings, Math. J. Okayama Univ., 23, 1, 19-32, (1981), MR 620719 (82j:16013) · Zbl 0475.16002

[9] Ikehata, Shûichi, Azumaya algebras and skew polynomial rings. II, Math. J. Okayama Univ., 26, 49-57, (1984), MR 779774 (86e:16001) · Zbl 0565.16002

[10] Jacobson, Nathan, Finite-dimensional division algebras over fields, (1996), Springer-Verlag Berlin, MR 1439248 (98a:16024) · Zbl 0874.16002

[11] Kaltofen, Erich; Shoup, Victor, Subquadratic-time factoring of polynomials over finite fields, Math. Comput., 67, 223, 1179-1197, (1998), MR 1459389 (99m:68097) · Zbl 0902.11053

[12] Katz, Nicholas M., \textit{p}-adic properties of modular schemes and modular forms, (Modular Functions of One Variable, III, Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972, Lecture Notes in Mathematics, vol. 350, (1973), Springer Berlin), 69-190, MR 0447119 (56 #5434)

[13] Kedlaya, Kiran S.; Umans, Christopher, Fast modular composition in any characteristic, (IEEE Annual Symposium on Foundations of Computer Science, (2008)), 146-155

[14] Le Gall, François, Powers of tensors and fast matrix multiplication, (ISSAC 2014—Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation, (2014), ACM New York), 296-303 · Zbl 1325.65061

[15] Neumann, Peter M.; Praeger, Cheryl E., Derangements and eigenvalue-free elements in finite classical groups, J. Lond. Math. Soc. (2), 58, 3, 564-586, (1998), MR 1678151 (2000a:20153) · Zbl 0936.15020

[16] Ore, Oystein, Theory of non-commutative polynomials, Ann. Math. (2), 34, 3, 480-508, (1933), MR 1503119 · Zbl 0007.15101

[17] Revoy, Philippe, Algèbres de Weyl en caractéristique \textit{p}, C. R. Acad. Sci. Paris Sér. A-B, 276, A225-A228, (1973) · Zbl 0265.16007

[18] Von Zur Gathen, Joachim; Gerhard, Jurgen, Modern computer algebra, (2003), Cambridge University Press New York, NY, USA · Zbl 1055.68168

[19] von zur Gathen, Joachim; Giesbrecht, Mark; Ziegler, Konstantin, Composition collisions and projective polynomials, (ISSAC 2010—Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, (2010), ACM New York), 123-130, MR 2920545 · Zbl 1321.68546