Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

A new faster algorithm for factoring skew polynomials over finite fields

Xavier Caruso [a], Jérémy Le Borgne [b]

[a] Université Rennes 1, IRMAR, Campus de Beaulieu, 35042 Rennes Cedex, France
[b] IRMAR & ENS Rennes, Campus de Ker Lann, Avenue Robert Schuman, 35170 Bruz, France

ARTICLE INFO

Article history:
Received 4 September 2015
Accepted 10 February 2016
Available online xxxx

Keywords:
Skew polynomial
Factorization
Azumaya algebra

ABSTRACT

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 Giesbrecht (1998). 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.

0. Introduction

The aim of this paper is to design a new algorithm for factorization in rings of skew polynomials over finite fields. These noncommutative rings have been widely studied, including from an algorithmic point of view, since they were first introduced by Ore in 1933. Today, one important application for the study of skew polynomials over finite fields is related to some error-correcting codes introduced in Gabidulin (1985).

The first significant results in terms of effective arithmetics in these rings, including an algorithm for factoring a skew polynomial as a product of irreducible elements, appear in Giesbrecht's paper (Giesbrecht, 1998). In the present paper, we give a factorization algorithm whose complexity improves on Giesbrecht's. We also describe various fast-multiplication algorithms for skew polynomials, and some additional algorithms such as Euclidean division and gcd.

E-mail addresses: xavier.caruso@normalesup.org (X. Caruso), jeremy.leborgne@ens-rennes.fr (J. Le Borgne).

http://dx.doi.org/10.1016/j.jsc.2016.02.016
0747-7171/© 2016 Elsevier Ltd. All rights reserved.

Let k be a finite field of characteristic p, and let σ be an automorphism of k. We denote by k^σ the subfield of k fixed by σ, and by q its cardinality. Let also r denote the order of σ on k; the extension k/k^σ is then cyclic of degree r. The ring $k[X, \sigma]$ of skew polynomials with coefficients in k is a noncommutative ring, on which multiplication is determined by $X \cdot a = \sigma(a) \cdot X$ for all $a \in k$. As we will see in the first section, a skew polynomial can always be factored as a product of irreducible skew polynomials. However, such a factorization is not unique in general.

In the second section, we will study more carefully the structure of skew polynomial rings, by putting them in the framework of Azumaya algebras. The structure theorem we will rely on is the following:

Theorem. *(Cf. Theorem 2.1.2, see also Ikehata, 1984, Theorem 2.) The ring $k[X, \sigma][1/X]$ is an Azumaya algebra over its centre $k^\sigma[X^r][1/X^r]$.*

This Theorem appears in Ikehata (1984). We will give a relatively short proof of this result, which makes this paper self-contained.

This Theorem has many important consequences for our purpose. The first one is the existence of a *reduced norm* map $k[X, \sigma] \to k^\sigma[X^r]$, which turns out to have very nice properties related to factorizations. More precisely, we shall explain how it can be used to establish a close link between factorizations of a skew polynomial and basic linear algebra over finite extensions of k^σ.

The third section of the paper deals with algorithmic aspects of arithmetic in skew polynomial rings. We start by giving various fast-multiplication algorithms and, as usual, we derive from them efficient algorithms to compute Euclidean division and gcd.

Then, we reach the core algorithm of this paper: the factorization algorithm, which is presented in the fourth section. Making an intensive use of the theory developed previously, we obtain a very efficient probabilistic algorithm to factor a skew polynomial as a product of irreducible skew polynomials, `SkewFactorization`. Before stating our complexity theorem, we recall the soft-O notation: if u_n and v_n are two sequences, the notation $u_n = \tilde{O}(v_n)$ means that there exists a positive integer k such that $u_n = O(v_n \log^k v_n)$.

Theorem. *(Cf. Theorem 4.3.4.) The algorithm `SkewFactorization` factors a skew polynomial of degree d in $k[X, \sigma]$ with average complexity*

$$\tilde{O}(dr^3 \log q + d \log^2 q + d^{1+\varepsilon} (\log q)^{1+o(1)}) + F(d, k^\sigma)$$

bit operations, for all $\varepsilon > 0$. Here $F(d, K)$ denotes the complexity of the factorization of a (commutative) polynomial of degree d over the finite field K.

Remark 1. In the above Theorem, the computation model we use is the computation tree model (see Bürgisser et al., 1997, §4.4).

Remark 2. Let ω be an exponent strictly greater that 2 such that the complexity of the matrix multiplication is $\tilde{O}(n^\omega)$ for input matrices of size $n \times n$. If we assume further that $\log q$ remains bounded, there is a variant of Theorem 4.3.4 stating that `SkewFactorization` runs with complexity $\tilde{O}(dr^\omega + d^{1+\varepsilon}) + F(d, k^\sigma)$ bit operations. We note that this version, when it applies, is generally stronger (the factor r^3 is replaced by r^ω).

Today, the best (average) complexity known for polynomial factorization, due to Kedlaya and Umans (2008) (improving a former algorithm by Kaltofen and Shoup, 1998), is:

$$F(d, K) = (d^{3/2+o(1)} + d^{1+o(1)} \log q) \cdot (\log q)^{1+o(1)}$$

bit operations, where q is the cardinality of K. Assuming this value for $F(d, K)$, we see that the terms $d \log^2 q$ and $d^{1+\varepsilon} (\log q)^{1+o(1)}$ are negligible compared to $F(d, K)$. If furthermore $r^3 \ll d$, so is the term $dr^3 \log q$. With this extra assumption, the complexity of our algorithm is then comparable to the complexity of the factorization of a *commutative* polynomial of the same degree.

Please cite this article in press as: Caruso, X., Le Borgne, J. A new faster algorithm for factoring skew polynomials over finite fields. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.02.016