Factoring in Skew-Polynomial Rings

Mark Giesbrecht

Department of Computer Science
University of Toronto
email: mwg@theory.utoronto.ca

Abstract

Efficient algorithms are presented for factoring polynomials in the skew-polynomial ring $K[x; \sigma]$, a non-commutative generalization of the usual ring of polynomials $K[x]$, where $K$ is a finite field and $\sigma: K \rightarrow K$ is an automorphism. Applications include fast functional decomposition algorithms for a class of polynomials in $K[x]$ whose decompositions are "wild" and previously thought to be difficult to compute. Also presented is a fast probabilistic algorithm for finding zero divisors in any finite associative algebra over $K$.

1 Introduction

A central problem in computer algebra is factoring polynomials in $K[x]$, where $K$ is a finite field and $x$ is an indeterminate. In this paper we present efficient factorization algorithms in a natural non-commutative generalization of the ring $K[x]$, the skew-polynomial ring $K[x; \sigma]$, where $\sigma: K \rightarrow K$ is a field automorphism. $K[x; \sigma]$ is the ring of all polynomials in $K[x]$ under the usual component-wise addition, and multiplication defined by $xa = \sigma(a)x$ for any $a \in K$. For example, if

$$f = x^2 + a_1 x + a_0 \in K[x; \sigma],$$
$$g = x + b_0 \in K[x; \sigma],$$

then

$$f + g = x^2 + (a_1 + 1)x + (a_0 + b_0),$$
$$fg = x^3 + (a_1 + \sigma^2(b_0))x^2 + (a_1\sigma(b_0) + a_0)x + a_0 b_0,$$
$$gf = x^3 + (\sigma(a_1) + b_0)x^2 + (a_1 b_0 + \sigma(a_0))x + a_0 b_0,$$

where $\sigma^2(a) = \sigma(\sigma(a))$ for any $a \in K$. When $\sigma = id$, the identity automorphism on $K$, the ring $K[x; \sigma]$ is the usual ring of polynomials $K[x]$ with $xa = ax$ for all $a \in K$. Skew-polynomial rings have been studied since Ore (1933) and complete treatments are found in Jacobson (1943), McDonald (1974), and Cohn (1985).

Assume throughout that $K$ has size $p^k$, where $p$ is a prime and $k \geq 1$. For any $f, g \in K[x; \sigma]$, $\deg(fg) = \deg f + \deg g$, where $\deg: K[x; \sigma] \setminus \{0\} \rightarrow \mathbb{N}$ is the usual polynomial degree function. This implies $K[x; \sigma]$ is integral (zero is the only zero divisor), and while
not in general a unique factorization domain, it is a principal left ideal ring endowed with a right Euclidean algorithm. As in the commutative case, a non-zero \( f \in K[x; \sigma] \) is irreducible if whenever \( f = gh \) for some non-zero \( g, h \in K[x; \sigma] \), then either \( \deg g = 0 \) or \( \deg h = 0 \). It follows that any \( f \in K[x; \sigma] \) can be written as \( f = f_1 \cdots f_k \), where \( f_1, \ldots, f_k \in K[x; \sigma] \) are irreducible. This factorization may not be unique, and adjacent factors may not be interchangeable. Consider two factoring problems:

(i) The complete factorization problem: given any \( f \in K[x; \sigma] \), find irreducible \( f_1, \ldots, f_k \in K[x; \sigma] \) such that \( f = f_1 \cdots f_k \).

(ii) The bi-factorization problem: given \( f \in K[x; \sigma] \) and \( s < \deg f \), determine if there exist \( g, h \in K[x; \sigma] \) with \( f = gh \) and \( \deg h = s \), and if so, find such \( g \) and \( h \).

This separation of the factoring problem into two cases more completely captures the full complexity of factoring in a non-commutative ring without unique factorization. We reduce the bi-factorization problem to the complete factorization problem. The complete factorization problem is in turn reduced to the problem of determining whether a finite dimensional associative algebra \( A \), over a finite extension field \( F \) of \( F_p \), possesses a non-trivial zero divisor, and if so, finding one. Both these reductions are deterministic and polynomial-time. The problem of determining whether \( A \) has any non-trivial zero divisors, and producing one if it does, is shown by Rónyai (1987) to be reducible (in deterministic polynomial-time) to factoring polynomials in \( F_p[z] \). Berlekamp’s (1970) factoring algorithms for \( F_p[z] \) yield deterministic algorithms for complete and bi-factorization in \( K[x; \sigma] \) requiring time \( (n \xi p)^{O(1)} \), and probabilistic algorithms requiring expected time \( (n \xi \log p)^{O(1)} \), on input \( f \in K[x; \sigma] \) of degree \( n \).

Our faster algorithm for finding zero divisors in any associative algebra \( A \) yields a faster probabilistic algorithm for factoring in skew-polynomial rings. Rónyai’s method for finding zero divisors in \( A \) is an application of his more general algorithm for computing an explicit decomposition of \( A \), a considerably more complicated problem. His algorithm is quite involved, and Rónyai only shows it to be polynomial-time and does not calculate the running time explicitly. In Section 5 we present a simple, fast, and practical probabilistic solution to the problem of determining whether or not \( A \) has any non-trivial zero divisors, and producing a pair multiplying to zero if it does. The algorithm relies on an upper bound on the density of elements in \( A \) whose minimal polynomials are irreducible. This algorithm for finding zero divisors yields faster probabilistic algorithms for complete and bi-factorizations of \( f \in K[x; \sigma] \) of degree \( n \), which require expected time \( n^4 \cdot (\xi \log p \log n)^{O(1)} \). Rónyai (1990) also presents a number of applications of finding zero divisors in finite associative algebras to problems in computational linear algebra and group theory.

Applications of Skew-Polynomial Rings

Linearized polynomials represent a difficult or “wild” case for algorithms which functionally decompose polynomials, for which no general algorithms are known (Zippel (1991) presents recent progress on this problem, which we discuss below). We present very fast algorithms for the functional decomposition of linearized polynomials.

The linearized polynomials over \( K \), in an indeterminate \( \lambda \), are those of the form

\[ \sum_{0 \leq i \leq n} a_i \lambda^i \quad (\text{where } a_0, \ldots, a_n \in K) \]

The set \( A_K \) of all linearized polynomials in \( K[\lambda] \) forms a ring under the usual polynomial addition (+), and functional composition (\( \circ \)) —