Information and Computation 262 (2018) 22–39

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

On the complexity of noncommutative polynomial factorization [☆]

V. Arvind [a,*], Pushkar Joglekar [b], Gaurav Rattan [c,1]

[a] Institute of Mathematical Sciences (HBNI), Chennai 600113, India
[b] Vishwakarma Institute of Technology, Pune, India
[c] RWTH Aachen, Lehrstuhl für Informatik 7, 52074 Aachen, Germany

ARTICLE INFO

Article history:
Received 2 December 2016
Received in revised form 28 March 2018
Available online 30 August 2018

Keywords:
Polynomial factorization
Noncommutative polynomials
Arithmetic circuits
Identity testing
Complexity classes

ABSTRACT

In this paper we study the complexity of factorization of polynomials in the free noncommutative ring $\mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ of polynomials over the field $\mathbb{F}$ and noncommuting variables $x_1, x_2, \ldots, x_n$. Our main results are the following:

- Although $\mathbb{F}\langle x_1, \ldots, x_n\rangle$ is not a unique factorization ring, we note that *variable-disjoint* factorization in $\mathbb{F}\langle x_1, \ldots, x_n\rangle$ has the uniqueness property. Furthermore, we prove that computing the variable-disjoint factorization is polynomial-time equivalent to Polynomial Identity Testing (both when the input polynomial is given by an arithmetic circuit or an algebraic branching program). We also show that variable-disjoint factorization in the black-box setting can be efficiently computed (where the computed factors will be also given by black-boxes).
- As a consequence of the previous result we show that homogeneous noncommutative polynomials and multilinear noncommutative polynomials have unique factorizations in the usual sense, which can be efficiently computed.
- Finally, we discuss a polynomial decomposition problem in $\mathbb{F}\langle x_1, \ldots, x_n\rangle$ which is a natural generalization of homogeneous polynomial factorization and prove some complexity bounds for it.

1. Introduction

Let $\mathbb{F}$ be any field and $X = \{x_1, x_2, \ldots, x_n\}$ be a set of n free noncommuting variables. Let X^* denote the set of all free words (which are monomials) over the alphabet X with concatenation of words as the monoid operation and the empty word ϵ as identity element.

The *free noncommutative ring* $\mathbb{F}\langle X\rangle$ consists of all finite $\mathbb{F}$-linear combinations of monomials in X^*, where the ring addition $+$ is coefficient-wise addition and the ring multiplication $*$ is the usual convolution product. More precisely, let

[☆] A preliminary version of this paper appeared in the proceedings of *Mathematical Foundations of Computer Science*, 2015 – 40th International Symposium, MFCS 2015, Milan.

[*] Corresponding author.
E-mail addresses: arvind@imsc.res.in (V. Arvind), joglekar.pushkar@gmail.com (P. Joglekar), rattan@informatik.rwth-aachen.de (G. Rattan).

[1] Work done while the author was a PhD student at The Institute of Mathematical Sciences (HBNI), Chennai, India.

https://doi.org/10.1016/j.ic.2018.05.009
0890-5401/© 2018 Elsevier Inc. All rights reserved.

$f, g \in \mathbb{F}\langle X\rangle$ and let $f(m) \in \mathbb{F}$ denote the coefficient of monomial m in polynomial f. Then we can write $f = \sum_m f(m)m$ and $g = \sum_m g(m)m$, and in the product polynomial fg for each monomial m we have

$$fg(m) = \sum_{m_1 m_2 = m} f(m_1)g(m_2).$$

The *degree* of a monomial $m \in X^*$ is the length of the monomial m, and the degree $\deg f$ of a polynomial $f \in \mathbb{F}\langle X\rangle$ is the degree of a largest degree monomial in f with nonzero coefficient. For polynomials $f, g \in \mathbb{F}\langle X\rangle$ we clearly have $\deg(fg) = \deg f + \deg g$.

A *nontrivial factorization* of a polynomial $f \in \mathbb{F}\langle X\rangle$ is an expression of f as a product $f = gh$ of polynomials $g, h \in \mathbb{F}\langle X\rangle$ such that $\deg g > 0$ and $\deg h > 0$. A polynomial $f \in \mathbb{F}\langle X\rangle$ is *irreducible* if it has no nontrivial factorization and is *reducible* otherwise. For instance, all degree 1 polynomials in $\mathbb{F}\langle X\rangle$ are irreducible. Clearly, by repeated factorization every polynomial in $\mathbb{F}\langle X\rangle$ can be expressed as a product of irreducibles.

In this paper we study the algorithmic complexity of polynomial factorization in the free ring $\mathbb{F}\langle X\rangle$.

1.1. Polynomial factorization problem

The problem of polynomial factorization in the *commutative* polynomial ring $\mathbb{F}[x_1, x_2, \ldots, x_n]$ is a classical well-studied problem in algorithmic complexity culminating in Kaltofen's celebrated efficient factorization algorithm [13,14]. Kaltofen's algorithm builds on efficient algorithms for univariate polynomial factorization; there are deterministic polynomial-time algorithms over rationals and over fields of unary characteristic and randomized polynomial-time over large characteristic fields (von zur Gathen and Gerhard's textbook [11] contains a comprehensive and excellent treatment of the subject). The basic idea in Kaltofen's algorithm is essentially a randomized reduction from multivariate factorization to bivariate and trivariate polynomial factorization using Hilbert's irreducibility theorem. These, in turn, can be reduced to univariate factorization. Thus, we can say that Kaltofen's algorithm uses randomization in two ways: the first is in the application of Hilbert's irreducibility theorem, and the second is in dealing with *univariate* polynomial factorization over fields of large characteristic. In a recent paper Kopparty et al. [15] have shown that the first of these requirements of randomness can be eliminated, assuming an efficient algorithm as subroutine for the problem of *polynomial identity testing* for small degree polynomials given by circuits. More precisely, it is shown by Kopparty et al. [15] that over finite fields of unary characteristic (or over rationals) polynomial identity testing is deterministic polynomial-time equivalent to multivariate polynomial factorization, for the class of general arithmetic circuits.

Thus, in the commutative setting it turns out that the complexity of multivariate polynomial factorization is closely related to polynomial identity testing (whose deterministic complexity is known to be related to proving superpolynomial size arithmetic circuit lower bounds).

1.2. Noncommutative polynomial factorization

The study of noncommutative arithmetic computation was initiated by Nisan [16]. He showed exponential size lower bounds for algebraic branching programs that compute the noncommutative permanent or the noncommutative determinant. For the noncommutative polynomial identity testing problem, Bogdanov and Wee [6] give a randomized polynomial-time algorithm for polynomial degree noncommutative arithmetic circuits. For noncommutative algebraic branching programs, Raz and Shpilka give a deterministic polynomial-time algorithm for the white-box case [17]. More recently, a deterministic quasi-polynomial time identity testing algorithm for black-box algebraic branching programs has been obtained [10]. Proving superpolynomial size lower bounds for noncommutative arithmetic circuits computing an explicit polynomial like, for example, the noncommutative permanent, is open. Likewise, obtaining a deterministic polynomial-time identity test for polynomial degree noncommutative circuits is open.

In this context, it is interesting to ask if we can relate the complexity of noncommutative factorization to noncommutative polynomial identity testing. However, there are various mathematical issues that arise in the study of noncommutative polynomial factorization.

Unlike in the commutative setting, the noncommutative polynomial ring $\mathbb{F}\langle X\rangle$ is *not* a unique factorization ring. A well-known example is the polynomial

$$xyx + x$$

which has two factorizations: $x(yx + 1)$ and $(xy + 1)x$. Both $xy + 1$ and $yx + 1$ are irreducible polynomials in $\mathbb{F}\langle X\rangle$.

There is a detailed theory of factorization in noncommutative rings [8,9]. We will mention an interesting result on the structure of polynomial factorizations in the ring $R = \mathbb{F}\langle X\rangle$.

Two elements $a, b \in R$ are *similar* if there are elements $a', b' \in R$ such that $ab' = a'b$, and (i) a and a' do not have common nontrivial left factors, (ii) b and b' do not have common nontrivial right factors.

Among other results, Cohn [9] has shown the following interesting theorem about factorizations in the ring $R = \mathbb{F}\langle X\rangle$.