Electronic Colloquium on Computational Complexity, Revision 4 of Report No. 22 (2022)

On Efficient Noncommutative Polynomial Factorization via Higman Linearization *

V. Arvind[†] Pushkar S Joglekar[‡§]

Abstract

In this paper we study the problem of efficiently factorizing polynomials in the free noncommutative ring $\mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ of polynomials in noncommuting variables $x_1, x_2, \ldots, x_n$ over the field $\mathbb{F}$. We obtain the following result:

> Given a noncommutative algebraic branching program[1] of size s computing a noncommutative polynomial $f \in \mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ as input, where $\mathbb{F} = \mathbb{F}_q$ is a finite field, we give a randomized algorithm that runs in time polynomial in s, n and $\log_2 q$ that computes a factorization of f as a product $f = f_1 f_2 \cdots f_r$, where each f_i is an irreducible polynomial that is output as a noncommutative algebraic branching program.
>
> The algorithm works by first transforming the given algebraic branching program computing f into a linear matrix L using Higman's linearization of polynomials. We then factorize the linear matrix L and recover the factorization of f. We use basic elements from Cohn's theory of free ideals rings combined with Ronyai's randomized polynomial-time algorithm for computing invariant subspaces of a collection of matrices over finite fields.

Keywords: Noncommutative Polynomials, Arithmetic Circuits, Factorization, Identity testing.

*A preliminary version was presented at the 37th Computational Complexity Conference, CCC'22, [AJ22].

†Institute of Mathematical Sciences, Chennai, India and Chennai Mathematical Institute, Siruseri, Kelambakkam, India, `email: arvind@imsc.res.in`

‡Vishwakarma Institute of Technology, Pune, India, `email: joglekar.pushkar@gmail.com`

§Author would like to thank SERB for the funding through the MATRICS project, File no. MTR/2018/001214

[1] This strengthens the main result in earlier versions of this paper where the algorithm was only for noncommutative arithmetic formulas.

ISSN 1433-8092

Contents

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 $f, g \in \mathbb{F}\langle X\rangle$ 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 $\mathbb{F}\langle X\rangle$. The factorization algorithm is by an application of Higman's linearization process followed by factorization of a matrix with linear entries (under some technical conditions) using Cohn's factorization theory.

It is interesting to note that Higman's linearization process [Hig40] has been used to obtain a deterministic polynomial-time algorithm for the RIT problem. That is, the problem of testing if a noncommutative rational formula (which computes an element of the free skew field $\mathbb{F}\langle\!\langle X\rangle\!\rangle$) is zero on its domain of definition [GGdOW20, IQS17, IQS18, HW15].

1.1 Overview of the results

The main result of the paper is the following.

Theorem (Main Theorem)**.** *Given a multivariate noncommutative polynomial $f \in \mathbb{F}_q\langle X\rangle$ for a finite field*[2] *$\mathbb{F}_q$ by a noncommutative algebraic branching program of size s as input, a factorization of f as a product $f = f_1 f_2 \cdots f_r$ can be computed in randomized time* $\mathrm{poly}(s, \log_2 q, |X|)$*, where each $f_i \in \mathbb{F}_q\langle X\rangle$ is an irreducible polynomial that is output as an algebraic branching program.*

The proof has three broad steps described below.

- **Higman linearization and Cohn's factorization theory** Briefly, given a noncommutative polynomial $f \in \mathbb{F}\langle X\rangle$, we can transform it into a linear matrix L such that $f \oplus I = PLQ$,

[2] We present the detailed randomized algorithm over large finite fields. In the case of small finite fields we obtain a deterministic $\mathrm{poly}(s, q, |X|)$ time algorithm with minor modifications.

where P is an upper triangular matrix with polynomial entries and all 1's diagonal and Q is a lower triangular matrix with polynomial entries and all 1's diagonal, P and Q are the matrices implementing the sequence of row and column operations required for the Higman linearization process. Now, as observed by Garg et al [GGdOW20] (in their work on rational identity testing), if f is given by a noncommutative formula as input then the above Higman linearization can be carried out in polynomial time. We strengthen their observation with a modified Higman linearization process that we call Block-Higman linearization (to emphasize that the modification works with matrix blocks) and show the more general result that if f is given by an ABP as input we can still compute its Higman linearization as defined above in polynomial time.

- **Ronyai's common invariant subspace algorithm** Next, the most important tool algorithmically, is Ronyai's algorithm for computing common invariant subspaces of a collection of matrices over finite fields [Rón90]. We show that Ronyai's common invariant subspace algorithm can be repeatedly applied to factorize a linear matrix $L = A_0 + \sum_{i=1}^{n} A_i x_i$, into a product of irreducible linear matrices provided A_0 is invertible and $[A_1 A_2 \cdots A_n]$ has full row rank or $[A_1^T A_2^T \cdots A_n^T]^T$ has full column rank. The later conditions are called as right and left monicity of the linear matrix L respectively. With some technical work we can ensure these conditions for a linear matrix L that is produced from a polynomial f by Higman linearization. Then Ronyai's algorithm yields the factorization of L into a product of irreducible linear matrices (upto multiplication by units). Here, Cohn's theory of factorization of noncommutative linear matrices gives us sufficient useful information about the structure of irreducible linear matrices.

- **Recovering the factors of f** Finally, we design a simple linear algebraic algorithm for trivializing a matrix product $AB = 0$, where A is a linear matrix and B is a column vector of polynomials from $\mathbb{F}\langle X\rangle$, using which we are able to extract the irreducible factors of f from the factors of L. An invertible matrix M with polynomial entries *trivializes* the relation $AB = 0$ if the modified relation $(AM)(M^{-1}B) = 0$ has the property that for every index i either the i^{th} column of AM is zero or the i^{th} row of $M^{-1}B$ is zero. While such matrices M exist for any matrix product $AB = 0$ with entries from $\mathbb{F}\langle X\rangle$, we obtain an efficient algorithm in the special case when A is linear and B's entries are polynomials computed by small arithmetic circuits. This special case is sufficient for our application.

There are some additional technical aspects we need to deal with. Let $L = A_0 + \sum_{i=1}^{n} A_i x_i$ be the linear matrix obtained from $f \in \mathbb{F}_q\langle X\rangle$ by Higman linearization, where $X = \{x_1, x_2, \ldots, x_n\}$ and $A_i \in \mathbb{F}_q^{d\times d}, 0 \le i \le n$. If A_0 is an invertible matrix then it turns out that the problem of factorizing L can be directly reduced to the problem of finding a common invariant subspace for the matrices $A_0^{-1}A_i, 1 \le i \le n$. In general, however, A_0 is not invertible. Two cases arise:

(a) The polynomial f is *commutatively nonzero*. That is, it is nonzero on $\mathbb{F}_q^n$ (or on $\mathbb{F}^n$ for a small extension field $\mathbb{F}$). In this case, by the DeMillo-Lipton-Schwartz-Zippel Lemma [DL78, Sch80, Zip79], we can do a linear shift of the variables $x_i \leftarrow x_i + \alpha_i$ in the polynomial f, for α_i randomly picked from $\mathbb{F}_q$ (or $\mathbb{F}$). Let the resulting polynomial be f' and let its Higman linearization be $L_{f'}$. In $L_{f'}$ the constant matrix term A_0' will be invertible with high probabilty, and the reduction steps outlined above will work for $L_{f'}$. Furthermore, from the factorization of f' we can efficiently recover the factorization of f. Section 4 deals with Case (a), with Theorem 4.10 summarizing the algorithm for factorizing f. Theorem 4.6 describes the algorithm for factorization of the linear matrix $L_{f'}$, and the factor extraction lemma (Lemma 4.9) allows us to efficiently recover the factorization of f' from the factorization of $L_{f'}$.

(b) In the second case, suppose f is zero on all scalars. Then, for example by Amitsur's theorem [Ami66], for a random matrix substitution $x_i \leftarrow M_i \in \mathbb{F}^{2s\times 2s}$ the matrix $f(M_1, M_2, \ldots, M_n)$ is *invertible* with high probability, where s is the formula size of f.[3] [4] Accordingly, we can consider the factorization problem for shifted and dilated linear matrix $L' = A_0 \otimes I_\ell + \sum_{i=1}^{n} A_i \otimes (Y_i + M_i)$ which will have the constant matrix term invertible, where each Y_i is an $\ell \times \ell$ matrix of distinct noncommuting variables, where $\ell = 2s$. Recovering the factorization of L from the factorization of L' requires some additional algorithmic work based on linear algebra. A lemma from [HKV20] (refer Section 5 and the Appendix for the details) turns out to be crucial here. The algorithm handling Case (b) is described in Section 5. Indeed, the new aspect of the algorithm is factorization of the dilated matrix L' from which we recover the factorization of the Higman linearization L_f of f. The remaining algorithm steps are exactly as in Section 4.

1.2 Small Finite fields

We now briefly explain the deterministic poly$(s, q, |X|)$ time factorization algorithm (when $\mathbb{F}_q$ is small). There are two places in the factorization algorithm outlined above where randomization is used: first, to obtain a matrix tuple $(M_1, M_2, \ldots, M_n)$ such that $f(M_1, M_2, \ldots, M_n)$ is invertible, which ensures that the constant matrix term of the linear matrix L' is invertible. When $q = \Omega(d)$, where $d = \deg f$, it suffices to randomly pick $M_i \in \mathbb{F}_q^{2s\times 2s}$. However, if $q < d$ we can choose entries of the matrices M_i from a small extension field $\mathbb{F}_{q^k}$ such that $q^k = \Omega(d)$. Thereby, we will obtain factorization of L' and subsequently that of the polynomial f over the extension field $\mathbb{F}_{q^k}$. However, we can use the fact that the finite field $\mathbb{F}_{q^k}$ can be embedded using the regular representation of the elements of $\mathbb{F}_{q^k}$ in the matrix algebra $\mathbb{F}_q^{k\times k}$. Thus, we can obtain from $(M_1, M_2, \ldots, M_n)$ a matrix tuple $(M_1', M_2', \ldots, M_n')$ with $M_i' \in \mathbb{F}_q^{2sk\times 2sk}$ such that $f(M_1', M_2', \ldots, M_n')$ is invertible. This will ensure that the linear matrix L' can be factorized over the field $\mathbb{F}_q$ which will allow us to obtain a complete factorization of f into irreducible factors over $\mathbb{F}_q$.

In order to get a deterministic polynomial-time algorithm for finding such matrices $M_i', 1 \le i \le n$ we will use the fact that the polynomial f is given by a small noncommutative formula and hence has a small algebraic branching program. Then, using ideas from [RS05, For14, ACDM20] we can easily find such matrices M_i' in deterministic polynomial time.

Next, we notice that Ronyai's algorithm for finding common invariant subspaces of matrices over $\mathbb{F}_q$ is essentially a polynomial-time reduction to univariate polynomial factorization over $\mathbb{F}_q$. We can use Berlekamp's deterministic poly(q, D) algorithm for the factorization of univariate degree D polynomials over $\mathbb{F}_q$. Putting it together, we can obtain a deterministic poly$(s, q, |X|)$ time

[3] Amitsur's theorem strengthens the Amitsur-Levitski theorem [AL50] often used in noncommutative PIT algorithms [BW05].

[4] In the actual algorithm we pick the matrices M_i using a result from [DM17]

algorithm for factorization of $f \in \mathbb{F}_q\langle X\rangle$ as a product of irreducible factors over $\mathbb{F}_q$.

1.3 Finite fields versus Rationals

Unfortunately, the algorithm outlined above does not yield an efficient algorithm for noncommutative polynomial factorization over rationals. The bottlneck is the problem of computing common invariant subspaces for a collection of matrices over $\mathbb{Q}$. Ronyai's algorithm for the problem over finite fields [Rón90] builds on the decomposition of finite-dimensional associative algebras over fields. Given an algebra $\mathcal{A}$ over a finite field $\mathbb{F}_q$ the algorithm decomposes $\mathcal{A}$ as a direct sum of minimal left ideals of $\mathcal{A}$ which is used to find nontrivial common invariant subspaces. However, as shown by Friedl and Ronyai [FR85], over rationals the problem of decomposing a *simple* algebra as a direct sum of minimal left ideals is at least as hard as factoring square-free integers.

1.4 Related research

The study of factorization in noncommutative rings is systematically investigated as part of Cohn's general theory of noncommutative free ideal rings [Coh06, Coh11] which is based on the notion of the weak algorithm. In fact, there is a hierachy of weak algorithms generalizing the division algorithm for commutative integral domains [Coh06].

Algorithmic: To the best of our knowledge, the complexity of noncommutative polynomial factorization has not been studied much, unlike the problem of commutative polynomial factorization [vzGG13, Kal89, KT90]. Prior work on the complexity of noncommutative polynomial factorization we are aware of is [AJR18] where efficient algorithms are described for the problem of factoring *homogeneous* noncommutative polynomials (which enjoy the unique factorization property, and indeed the algorithms in [AJR18] crucially use the unique factorization property). When the input homogeneous noncommutative polynomial has a small noncommutative arithmetic circuit (even given by a black-box as in Kaltofen's algorithms [Kal89, KT90]) it turns out that the problem is efficiently reducible to commutative factorization by set-multilinearizing the given noncommutative polynomial with new commuting variables. This also works in the black-box setting and yields a randomized polynomial-time algorithm which will produce as output black-boxes for the irreducible factors (which will all be homogeneous). When the input homogeneous polynomial is given by an algebraic branching program there is even a deterministic polynomial-time factorization algorithm. Indeed, the noncommutative factorization problem in for homogeneous polynomials efficiently reduces to the noncommutative PIT problem [AJR18], analogous to the commutative case [KSS15], modulo the randomness required for univariate polynomial factorization in the case of finite fields of large characteristic. The motivation of the present paper is to extend the above results to the inhomogeneous case.

Mathematical: From a mathematical perspective, building on Cohn's work there is a lot of research on the study of noncommutative factorization. For example, [BS15, BHL17] focus on the lack of unique factorization in noncommutative rings and study the structure of multiple factorizations. The research most relevant to our work is the study of noncommutative analogues of the Nullstellensatz by Helton, Klep and Volcic [HKV18, HKV20]. In these papers the authors study the free singularity locus of a noncommutative polynomial $f \in \mathbb{F}\langle X\rangle$ where $\mathbb{F}$ is an algebraically closed field of characteristic zero (in [HKV20] mostly they consider complex numbers). This is the set of all matrix tuples $\bar{M} \in \mathcal{L}_n(f)$ (in all matrix dimensions d) where $\mathcal{L}_n(f) = \{\bar{M} \mid \det f(\bar{M}) = 0$, where $\bar{M}$ is an n-tuple of matrices$\}$. It turns out that $f \in \mathbb{F}\langle X\rangle$ is irreducible if and only if for all $d \geq d_0$ for some d_0 the hypersurface $\mathcal{L}_d(f)$ is irreducible which in turn holds iff $\det f(\bar{X})$ is an irreducible commutative polynomial, where $\bar{X}$ are generic matrices with commuting variables of dimension $d \geq d_0$. However, d_0 turns out to be exponentially large.

Plan of the paper. In Section 2 we present basic definitions and the background results from Cohn's work on factorization. In Section 3 we further present some results from Cohn's work relevant to the paper. In Section 4 we present the factorization algorithm for polynomials f that does not vanish on scalars and in Section 5 we present the algorithm for the general case.

2 Preliminaries

In this section we give some basic definitions and results relevant to the paper, mainly from Cohn's theory of factorization. Analogous to integral domains and unique factorization domains in commutative ring theory, P.M. Cohn [Coh06, Coh11] has developed a theory for noncommutative rings based on the weak algorithm (a noncommutative generalization of the Euclidean division algorithm) and the notion of free ideal rings. We present the relevant basic definitions and results, specialized to the ring $\mathbb{F}\langle X\rangle$ of noncommutative polynomials with coefficients in a (commutative) field $\mathbb{F}$, and also for matrix rings with entries from $\mathbb{F}\langle X\rangle$.

The results about $\mathbb{F}\langle X\rangle$ in Cohn's text [Coh06, Chapter 5] are stated uniformly for algebraically closed fields $\mathbb{F}$. However, those we discuss hold for any field $\mathbb{F}$ (in particular for $\mathbb{F}_q$ or a small degree extension of it). The proofs are essentially based on linear algebra.

Since we will be using Higman's linearization [Hig40] to factorize noncommutative polynomials, we are naturally lead to studying the factorization of linear matrices in $\mathbb{F}\langle X\rangle^{d\times d}$ using Cohn's theory.

Definition 2.1. [Coh06] *A matrix M in $\mathbb{F}\langle X\rangle^{d\times d}$ is called* full *if it has (noncommutative) rank d. That is, it cannot be decomposed as a matrix product $M = M_1 \cdot M_2$, for matrices $M_1 \in \mathbb{F}\langle\!\langle X\rangle\!\rangle^{d\times e}$ and $M_2 \in \mathbb{F}\langle\!\langle X\rangle\!\rangle^{e\times d}$ with $e < d$.*

Remark 2.2. *Based on the notion of noncommutative matrix rank [Coh06], the square matrix $M \in \mathbb{F}\langle X\rangle^{d\times d}$ is full precisely when it is invertible in the skew field $\mathbb{F}\langle\!\langle X\rangle\!\rangle$. That is, M is full if and only if there is a matrix $N \in \mathbb{F}\langle\!\langle X\rangle\!\rangle^{d\times d}$ such that $MN = NM = I_d$, where I_d is $d \times d$ identity matrix.*

We note the distinction between full matrices and units in the matrix ring $\mathbb{F}\langle X\rangle^{d\times d}$.

Definition 2.3. *A matrix $U \in \mathbb{F}\langle X\rangle^{d\times d}$ is a* unit *if there is a matrix $V \in \mathbb{F}\langle X\rangle^{d\times d}$ such that $UV = VU = I_d$, where I_d is $d \times d$ identity matrix.*

Clearly, units in $\mathbb{F}\langle X\rangle^{d\times d}$ are full. Examples of units in $\mathbb{F}\langle X\rangle^{d\times d}$, which have an important role in our factorization algorithm, are upper (or lower) triangular matrices in $\mathbb{F}\langle X\rangle^{d\times d}$ whose diagonal entries are all *nonzero scalars*. Full matrices, in general, need not be units: for example, the 1×1 matrix x, where x is a variable, is full but it is not a unit in the ring $\mathbb{F}\langle X\rangle^{1\times 1} = \mathbb{F}\langle X\rangle$.

Remark 2.4. *Full non-unit matrices are essentially non-unit non-zero-divisors. For the factorization of elements in* $\mathbb{F}\langle X\rangle^{d\times d}$*, units are similar to scalars in the factorization of polynomials in polynomial rings. Cohn's theory [Coh06] considers factorizations of full non-unit elements in* $\mathbb{F}\langle X\rangle^{d\times d}$*.*

We next define *atoms* in $\mathbb{F}\langle X\rangle^{d\times d}$, which are essentially the irreducible elements in it.

Definition 2.5. *A full non-unit element* A *in* $\mathbb{F}\langle X\rangle^{d\times d}$ *is an* atom *if* A *cannot be factorized as* $A = A_1A_2$ *for full non-unit matrices* A_1, A_2 *in* $\mathbb{F}\langle X\rangle^{d\times d}$*.*

Noncommutative polynomials do not have unique factorization in the usual sense of commutative polynomial factorization.[5] A classic example [Coh06] is the polynomial $x + xyx$ with its two different factorizations

$$x + xyx = x(1 + yx) = (1 + xy)x,$$

where $1 + xy$ and $1 + yx$ are distinct irreducible polynomials.

Definition 2.6. *Elements* $A \in \mathbb{F}\langle X\rangle^{d\times d}$ *and* $B \in \mathbb{F}\langle X\rangle^{d'\times d'}$ *are called* stable associates *if there are positive integers* t *and* t' *such that* $d + t = d' + t'$ *and units* $P, Q \in \mathbb{F}\langle X\rangle^{(d+t)\times(d+t)}$ *such that* $A \oplus I_t = P(B \oplus I_{t'})Q$*.*

It is easy to check that the polynomials $1 + xy$ and $1 + yx$ are stable associates.

Notice that if A and B are full non-unit matrices that are stable associates then A is atom if and only if B is atom. Furthermore, we note that stable associativity defines an equivalence relation between full matrices over the ring $\mathbb{F}\langle X\rangle$.

We observe that the problem of checking if two polynomials in $\mathbb{F}\langle X\rangle$ given as arithmetic formulas are stable associates or not has an efficient randomized algorithm (Lemma 3.5).

Now we turn to the problem of noncommutative polynomial factorization. By Higman's linearization [Hig40, Coh06], given a polynomial $f \in \mathbb{F}\langle X\rangle$ there is a positive integer ℓ such that f is stably associated with a *linear matrix* $L \in \mathbb{F}\langle X\rangle^{\ell\times\ell}$, that is to say, the entries of L are affine linear forms.[6] Higman's linearization process is a simple algorithm obtaining the linear matrix L for a given f, and it plays a crucial role in our factorization algorithm. We first describe it and then recall an effective version [GGdOW20] which gives a simple polynomial-time algorithm to compute L when f is given as a non-commutative arithmetic formula. Then we state our stronger result showing that even if f is given by an algebraic branching program as input we can compute its Higman linearization in deterministic polynomial time.

Higman's linearization process

We describe a single step of the linearization process. Given an $m \times m$ matrix M over $\mathbb{F}\langle X\rangle$ such that $M[m, m] = f + g \times h$, apply the following:

[5] However, as shown by Cohn, using the notion of stable associates there is a more general sense in which noncommutative polynomials have "unique" factorization [Coh06].

[6] More generally, by Higman's linearization any matrix of polynomials M is stably associated with a linear matrix $L \in \mathbb{F}\langle X\rangle^{\ell\times\ell}$ for some ℓ.

- Expand M to an $(m+1)\times(m+1)$ matrix by adding a new last row and last column with diagonal entry 1 and remaining new entries zero:

$$\left[\begin{array}{c|c} M & 0 \\ \hline 0 & 1 \end{array}\right].$$

- Then the bottom right 2×2 submatrix is transformed as follows by elementary row and column operations

$$\begin{pmatrix} f+gh & 0 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} f+gh & g \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} f & g \\ -h & 1 \end{pmatrix}$$

Given a polynomial $f \in \mathbb{F}\langle X\rangle$ by repeated application of the above step we will finally obtain a *linear matrix* $L = A_0 + \sum_{i=1}^{n} A_i x_i$, where each $A_i, 0 \le i \le n$ is an $\ell \times \ell$ over $\mathbb{F}$, for some ℓ. The following theorem summarizes its properties.

Theorem 2.7 (Higman Linearization)**.** [Coh06] *Given a polynomial $f \in \mathbb{F}\langle X\rangle$, there are matrices $P, Q \in \mathbb{F}\langle X\rangle^{\ell\times\ell}$ and a linear matrix $L \in \mathbb{F}\langle X\rangle^{\ell\times\ell}$ such that*

$$\left(\begin{array}{c|c} f & 0 \\ \hline 0 & I_{\ell-1} \end{array}\right) = PLQ \tag{1}$$

with P upper triangular, Q lower triangular, and the diagonal entries of both P and Q are all 1's (hence, P and Q are both units in $\mathbb{F}\langle X\rangle^{\ell\times\ell}$).

Instead of a single f, we can apply Higman linearization to a matrix of polynomials $M \in \mathbb{F}\langle X\rangle^{m\times m}$ to obtain a linear matrix L that is stably associated to M. We first recall the algorithmic version of Garg et al. [GGdOW20] in this general form.

Theorem 2.8. [GGdOW20, Proposition A.2] *Let $M \in \mathbb{F}\langle X\rangle^{m\times m}$ such that $M_{i,j}$ is computed by a non-commutative arithmetic formula of size at most s and bit complexity at most b. Then, for $k = O(s)$, in time $\mathrm{poly}(s,b)$ we can compute the matrices P, Q and L in $\mathbb{F}\langle X\rangle^{\ell\times\ell}$ of Higman's linearization such that*

$$\left(\begin{array}{c|c} M & 0 \\ \hline 0 & I_k \end{array}\right) = PLQ.$$

, where $\ell = m+k$. Moreover, the entries of the matrices P and Q as well as P^{-1} and Q^{-1} are given by polynomial-size algebraic branching programs which can also be obtained in polynomial time.

We will sometimes denote the block diagonal matrix $\left(\begin{array}{c|c} M & 0 \\ \hline 0 & I_k \end{array}\right)$ by $M \oplus I_k$.

We now state our strengthening of Theorem 2.8 which enables us to factorize noncommutative polynomials given as algebraic branching programs. The complete proof is presented in the appendix.

Theorem 2.9. *Let $M \in \mathbb{F}\langle X\rangle^{m\times m}$ such that each entry $M_{i,j}$ is a polynomial computed by a non-commutative algebraic branching program of size at most s and bit complexity at most b. Then,* *for $k = O(s)$, in time* $\mathrm{poly}(s,b)$ *we can compute the matrices P, Q and L in $\mathbb{F}\langle X\rangle^{\ell\times\ell}$ of Higman's linearization such that*

$$\left(\begin{array}{c|c} M & 0 \\ \hline 0 & I_k \end{array}\right) = PLQ.$$

, where $\ell = m+k$. Moreover, the entries of the matrices P and Q as well as P^{-1} and Q^{-1} are given by polynomial-size algebraic branching programs which can also be obtained in polynomial time.

As P and Q are units with diagonal entries all 1's, the matrix M is full iff the linear matrix L is full. Also, the scalar matrix $M(\overline{0})$ (obtained by setting all variables to zero) is invertible iff the scalar matrix $L(\overline{0})$, similarly obtained, is invertible.

Invariant Subspaces and Ronyai's Algorithm

Definition 2.10. *Let $A_1, \ldots, A_n \in \mathbb{F}^{d\times d}$. A subspace $V \subseteq \mathbb{F}^n$ is called as common invariant subspace of $A_1, \ldots, A_n$ if $A_i v \in V$ for all $i \in [n]$ and $v \in V$.*

Clearly 0 and $\mathbb{F}^n$ are, trivially, common invariant subspaces for any collection of matrices. The algorithmic problem is to find a *non-trivial* common invariant subspace if one exists. Ronyai [Rón90] gives a randomized polynomial-time algorithm for this problem when $\mathbb{F}$ is finite field.

Theorem 2.11. [Rón90] *Given $A_1, \ldots, A_n \in \mathbb{F}_q^{d\times d}$ there is a randomized algorithm running in time polynomial in $n, d, \log q$ that computes with high probability a non-trivial common invariant subspace of $A_1, \ldots, A_n$ if such a subspace exists, and outputs "no" otherwise.*

Remark 2.12. *We should note here, the classical Burnside's theorem [Bur05] for matrix algebras over algebraically closed fields. It essentially shows that the algebra generated by $A_1, A_2, \ldots, A_n$ is the full matrix algebra iff there is no nontrivial common invariant subspace.*

Remark 2.13. *As already mentioned in the introduction, Friedl and Ronyai [FR85] have shown that over rationals the problem is at least as hard as factoring square-free integers, and hence likely to be intractable.*

Noncommutative Formulas, Algebraic branching programs

Next we recall standard definitions of a noncommutative formulas and noncommutative algebraic branching programs (ABPs). More details about noncommutative arithmetic computation can be found in Nisan's work [Nis91]:

A *noncommutative arithmetic circuit* C over a field $\mathbb{F}$ and indeterminates $x_1, x_2, \ldots, x_n$ is a directed acyclic graph (DAG) with each node of indegree zero labeled by a variable or a scalar constant from $\mathbb{F}$: the indegree 0 nodes are the input nodes of the circuit. Internal nodes, representing gates of the circuit, are of indegree two and are labeled by either a + or a × (indicating the gate type). Furthermore, the two inputs to each × gate are designated as left and right inputs prescribing the order of gate gate multiplication. Each internal gate computes a polynomial (by adding or multiplying its input polynomials), where the polynomial computed at an input node is just its label. A special gate of C is the *output* and the polynomial computed by the circuit C is the polynomial computed at its output gate. An arithmetic circuit is a *formula* if the fan-out of every gate is at most one.

A noncommutative *algebraic branching program* (ABP) is a layered directed acyclic graph with one source and one sink. The vertices of the graph are partitioned into layers numbered from 0 to d, where edges may only go from layer i to layer $i+1$. The source is the only vertex at layer 0 and the sink is the only vertex at layer d. Each edge is labeled with a linear linear form in the noncommuting variables $x_1, x_2, \ldots, x_n$ The size of the ABP is the number of vertices. The polynomial in $\mathbb{F}\langle X\rangle$ computed by the ABP is defined as follows: the sum over all source-to-sink paths of the product of the linear forms by which the edges of the path are labeled.

3 Some Basic Results

In this section we present some basic results required for our factorization algorithm.

Monic linear matrices

Definition 3.1. [Coh06] *Let $L = A_0 + A_1x_1 + \ldots + A_nx_n \in \mathbb{F}\langle X\rangle^{d\times d}$ be a linear matrix, where each A_i is a $d \times d$ scalar matrix over $\mathbb{F}$. Then L is called* right monic *if the $d \times nd$ scalar matrix $[A_1\ A_2\ \ldots\ A_n]$ has full row rank. Equivalently, if there are matrices $B_1, \ldots, B_n \in \mathbb{F}^{d\times d}$ such that $\Sigma_{i=1}^n A_iB_i = I_d$ (i.e. the matrix $[A_1\ A_2\ \ldots\ A_n]$ has right inverse).*

Similarly, L is left monic *if the $nd \times d$ matrix $[A_1^T\ A_2^T\ \ldots\ A_n^T]^T$ has full column rank. L is called* monic *if it is both left and right monic.*

The next two results from Cohn [Coh06] are important properties of monic linear matrices.

Lemma 3.2. [Coh06] *A right (or left) monic linear matrix in $\mathbb{F}\langle X\rangle^{d\times d}$ is not a unit in $\mathbb{F}\langle X\rangle^{d\times d}$.*

Proof. Let $L = A_0 + \sum_{i=1}^n A_ix_i$ be right monic, where each $A_i \in \mathbb{F}^{d\times d}$. By definition, there are matrices $B_i \in \mathbb{F}^{d\times d}, 1 \le i \le d$ such that $\sum_{i=1}^d A_iB_i = I_d$. Now, suppose L is a unit. Then there is a matrix $C \in \mathbb{F}\langle X\rangle^{d\times d}$ such that $CL = I_d$. Let the maximum degree of polynomials occurring in C be k, and let $\hat{C} \in \mathbb{F}\langle X\rangle^{d\times d}$ denote the degree k component of C (so each nonzero entry of $\hat{C}$ is a homogeneous polynomial of degree k). Clearly, $\hat{C}\cdot(\sum_{i=1}^n A_ix_i) = 0$. The homogeneity of $\hat{C}$'s entries implies that $\hat{C}A_i = 0$ for each i. Hence, $\sum_{i=1}^n \hat{C}A_iB_i = 0$ which implies $\hat{C} = 0$, contradicting the assumption that $C \in \mathbb{F}\langle X\rangle^{d\times d}$ is the inverse of L. The case when L is left monic is symmetric. □

Let $f \in \mathbb{F}\langle X\rangle$ be a nonzero polynomial and L be a linear matrix obtained from f by Higman linearization as in Equation 10. Clearly, L is a full linear matrix. We show that we can transform L to obtain a full and right (or left) monic linear matrix L' that is stably associated to f. Furthermore, we can efficiently compute L' and the related transformation matrices.

Theorem 3.3. [Coh06] *Let $L = A_0 + \sum_{i=1}^n A_ix_i$ be a full linear matrix in $\mathbb{F}\langle X\rangle^{d\times d}$ obtained by Higman linearization from a non constant polynomial $f \in \mathbb{F}\langle X\rangle$. Then there are deterministic* $\mathrm{poly}(n, d, \log_2 q)$ *time algorithms that compute units $U, U' \in \mathbb{F}\langle X\rangle^{d\times d}$ and invertible scalar matrices $S, S' \in \mathbb{F}_q^{d\times d}$ such that:*

1. *$ULS = L' \oplus I_r$, and L' is right monic. Moreover, if L is not right monic then $r > 0$.*

2. $S'LU' = L' \oplus I_{r'}$, and L' is left monic. Moreover, if L is not left monic then $r' > 0$.

Proof. We prove only the first part. The second part has an essentially identical proof.

We present a proof with a polynomial-time algorithm for computing L'. If L is already right monic there is nothing to show. Otherwise, the row rank of the matrix $B = [A_1 \ A_2 \ \cdots \ A_n]$ is strictly less than d. By row operations we can drive at least one row of B to zero. So, there is an invertible scalar matrix $U_1 \in \mathbb{F}^{d\times d}$ such that $U_1 B$ has its last row as zeros. Now $U_1 A_0$ must have its last row non-zero since L is a full linear matrix. So the last row of $U_1 L$ has only scalar entries and at least one of these is non-zero. By a column swap applied to $U_1 L$ we can bring this non-zero scalar α in the $(d,d)^{th}$ position. Hence, the $(d,d)^{th}$ entry of $U_1 L S_1$ is nonzero, where S_1 is the matrix implementing the column swap. Now, with suitable row operations using the last row, we can make all entries above the $(d,d)^{th}$ entry of the d^{th} column zero. Applying column operations we can make all entries of the d^{th} row to the left of the $(d,d)^{th}$ entry zero. The resulting matrix is of the form $RU_1 L S_1 S' = \tilde{L} \oplus 1$, where the unit R is a linear matrix and S' is an invertible scalar matrix implementing the row and column operations.

If $\tilde{L}$ is not right monic, we can recursively apply the above procedure on $\tilde{L}$ until we finally obtain a unit $\tilde{U} \in \mathbb{F}\langle X\rangle^{d\times d}$ and a scalar invertible matrix $\tilde{S} \in \mathbb{F}^{d\times d}$ such that $\tilde{U}\tilde{L}\tilde{S} = L' \oplus I_r$, for some positive integer $r < d$, such that L' is right monic.

To see why this recursive procedure terminates for $r < d$, note that the dimension of matrix $\tilde{L}$ is reducing by 1 in each recursive step and the matrix $\tilde{L}$ obtained is a stable associate of L. So, if $r = d$ it would imply L is a unit which is a contradiction as we know that L is obtained via Higman linearization on a non-constant polynomial f, so L is noninvertible.

Putting $U = RU_1\tilde{U}$ and $S = S_1\tilde{S}$ we have $ULS = L' \oplus I_r$ where L' is right monic as desired. It is clear that the entire construction is polynomial time bounded, and that we have small ABPs for the entries of U. □

Remark 3.4. *By repeated application of the algorithm in Theorem 3.3 we can compute units $U_1, U_2 \in \mathbb{F}\langle X\rangle^{d\times d}$ such that $U_1 L U_2 = L' \oplus I_r$, where L' is* both left and right monic*. Such a two-sided monic L' is called* monic *in [Coh06].*

For our factorization algorithm, it suffices to compute an L' that is either left or right monic that is associated to L as in Theorem 3.3. It turns out that either a left monic or a right monic L' suffices to use Ronyai's common invariant subspace algorithm to factorize L' (and hence also L) as we show in Theorem 4.6. More importantly, the fact that matrices S and S' in Theorem 3.3 are scalar is important for the factor extraction algorithm as discussed in Theorem 4.10.

Lemma 3.5. *Given polynomials $f, g \in \mathbb{F}\langle X\rangle$ as input by noncommutative arithmetic formulas, we can check in randomized polynomial time if f and g are stable associates.*

Proof. Given f and g, using Higman linearization we first compute in polynomial time full and monic linear matrices A and B such that f and A are stable associates and g and B are stable associates (see Theorem 3.3 and Remark 3.4). Now, f and g are stable associates iff A and B are stable associates. As both A and B are full and monic linear matrices, they are stable associates iff both A and B are matrices of the same dimension, say d, and there are scalar invertible matrices P and Q in $\mathbb{F}^{d\times d}$ such that $PA = BQ$ [Coh06, Theorem 5.8.3], where $\mathbb{F} = \mathbb{F}_q$ or a small field extension. Letting the $2d^2$ entries of P and Q be variables, we can find a linearly independent set of solutions to $PA = BQ$ in polynomial time. Now, there exists invertible P and Q in the solution set iff the degree-$2d$ polynomial $\det P \times \det Q$ is nonzero on the solutions to $PA = BQ$. We can check this by the DeMillo-Lipton-Schwartz-Zippel Lemma [DL78, Sch80, Zip79] by evaluating $\det P$ and $\det Q$ on a random linear combination of the basis of solutions to $PA = BQ$. This will be correct with high probablity. □

The next result shows how irreducibility (more generally, the property of being an atom) is preserved by Higman linearization.

Theorem 3.6. *Let $f \in \mathbb{F}\langle X\rangle$ be a nonconstant polynomial and L be a full linear matrix stably associated with f (obtained via Higman linearization).Then the polynomial f is irreducible iff L is an atom.*

We give a self-contained proof of the above theorem, using the following (suitably paraphrased) result of Cohn.

Lemma 3.7 (Matrix Product Trivialization)**.** [Coh11, pp. 198] *Let $A \in \mathbb{F}\langle X\rangle^{m\times n}$ and $B \in \mathbb{F}\langle X\rangle^{n\times s}$ be polynomial matrices such that their product $AB = 0$. Then there exists a unit $P \in \mathbb{F}\langle X\rangle^{n\times n}$ such that for every index $i \in [n]$ either the i^{th} column of the matrix product AP is all zeros or the i^{th} row of the matrix product $P^{-1}B$ is all zeros.*

Proof of Theorem 3.6. By Higman linearization, we have upper and lower triangular matrices P and Q, respectively, such that

$$f \oplus I_s = PLQ,$$

for some positive integer s.

Now, if f is not irreducible then we can write $f = f_1 f_2$, where f_1 and f_2 are both nonconstant polynomials in $\mathbb{F}\langle X\rangle$. Hence $f \oplus I_s$ factorizes as the product of non-units $(f_1 \oplus I_s) \cdot (f_2 \oplus I_s)$, which implies the factorization

$$L = P^{-1}(f_1 \oplus I_s)(f_2 \oplus I_s)Q^{-1}.$$

Now, we claim $P^{-1}(f_1 \oplus I_s)$ and $(f_2 \oplus I_s)Q^{-1}$ are non-units. Suppose $P^{-1}(f_1 \oplus I_s)$ is a unit. Then $f_1 \oplus I_s$ is a unit which would imply there is an invertible matrix $M \in \mathbb{F}\langle X\rangle^{d\times d}$ such that $(f_1 \oplus I_s)M = I_{s+1}$. But that implies $f \cdot M_{1,1} = 1$ which is impossible since f_1 is a nonconstant polynomial. Similarly, $(f_2 \oplus I_s)Q^{-1}$ cannot be a unit. Hence L is not an atom.

Conversely, suppose L is not an atom. Then we can factorize it as $L = M_1 M_2$, where $M_1, M_2 \in \mathbb{F}\langle X\rangle^{d\times d}$ are full non-units. Therefore, we have the factorization

$$f \oplus I_s = (PM_1)(M_2Q).$$

Writing the matrices PM_1 and M_2Q as 2×2 block matrices, we have:

$$\left(\begin{array}{c|c} f & 0 \\ \hline 0 & I_s \end{array}\right) = \left(\begin{array}{c|c} c_1 & c_3 \\ \hline c_2 & c_4 \end{array}\right) \cdot \left(\begin{array}{c|c} d_1 & d_3 \\ \hline d_2 & d_4 \end{array}\right).$$

From the $(2,1)^{th}$ matrix block on the left hand side of the above equation, we obtain the following matrix identity:

$$0 = \begin{pmatrix} c_2 & c_4 \end{pmatrix} \cdot \begin{pmatrix} d_1 \\ d_2 \end{pmatrix},$$

where $C = (c_2\ c_4)$ is in $\mathbb{F}\langle X\rangle^{s\times(s+1)}$ and $D = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$ is in $\mathbb{F}\langle X\rangle^{(s+1)\times 1}$. By Lemma 3.7 there is a unit $U \in \mathbb{F}\langle X\rangle^{(s+1)\times(s+1)}$ such that for every $1 \le i \le s+1$ either the i^{th} column of $C'' = C \cdot U$ is all zeros or the i^{th} row of $D'' = U^{-1}D$ is all zeros. Note that D'', and hence D, cannot be the all zeros column as M_2Q is full. So, at least one entry of D'' is nonzero. Hence, at least one column of C'' is all zeros. By a suitable column permutation matrix Π we can ensure that the first column of $C \cdot U\Pi$ is all zeros. Clearly, first entry of $\Pi^{-1}U^{-1}D$ is nonzero. Writing $f \oplus I_s$ as a product of $C' = PM_1U\Pi$ and $D' = \Pi^{-1}U^{-1}M_2Q$ we have

$$\left(\begin{array}{c|c} f & 0 \\ \hline 0 & I_s \end{array}\right) = \left(\begin{array}{c|c} c'_1 & c'_3 \\ \hline c'_2 & c'_4 \end{array}\right) \cdot \left(\begin{array}{c|c} d'_1 & d'_3 \\ \hline d'_2 & d'_4 \end{array}\right),$$

where c'_2 is an all zeros column and d'_1 is nonzero. From the $(2,2)^{th}$ matrix block of the above equation, we obtain $c'_4 d'_4 = I_s$ so c'_4 and d'_4 are units. By observing $(2,1)^{th}$ matrix block of the above equation we get $c'_4 d'_2 = 0$, which implies d'_2 is an all zeros column as c'_4 is unit. It follows that $f = c'_1 \cdot d'_1$. Furthermore, it is a nontrivial factorization because both c'_1 and d'_1 are non-units (because C' and D' are non-units, and c'_4 and d'_4 are units). ☐

Let $L \in \mathbb{F}\langle X\rangle^{d\times d}$ be a full and right (or left) monic linear matrix. Let $L = A_0 + \sum_{i=1}^{n} A_i x_i$. For a positive integer ℓ let $M_i, i \in [n]$ be $\ell \times \ell$ scalar matrices with entries from $\mathbb{F}$ (or a small degree extension of $\mathbb{F}$). Let $Y_i, i \in [n]$ be $\ell \times \ell$ matrices whose entries are distinct noncommuting variables $y_{ijk}, 1 \le j, k \le \ell$. Then the evaluation of the linear matrix L at $x_i \leftarrow Y_i + M_i, 1 \le i \le n$ is the $d\ell \times d\ell$ linear matrix in the y_{ijk} variables:

$$L' = A_0 \otimes I_\ell + \sum_{i=1}^{n} A_i \otimes M_i + \sum_{i=1}^{n} \sum_{j,k=1}^{\ell} (A_i \otimes E_{jk}) \cdot y_{ijk}$$

Lemma 3.8. *There is a positive integer $\ell \le 2d$ such that for randomly picked $\ell \times \ell$ matrices $M_i, i \in [n]$ (with entries from $\mathbb{F}$ or a small degree extension field) the matrix $A_0 \otimes I_\ell + \sum_{i=1}^{n} A_i \otimes M_i$ is an invertible matrix.*

Proof. Since $L \in \mathbb{F}\langle X\rangle^{d\times d}$ is a full linear matrix, it has noncommutative rank d. Hence, by the result of [DM17] for the generic $2d \times 2d$ matrix substitution $x_i \leftarrow X_i, i \in [n]$, where X_i is a matrix of distinct commuting variables, the commutative rank of $L(X_1, X_2, \ldots, X_n)$ is $2d^2$ (which means it is invertible). Hence there is a least $\ell \le 2d$ such that the commutative rank of $L(X_1, X_2, \ldots, X_n)$ is $d\ell$, where X_i are generic $\ell \times \ell$ matrices with commuting variables. Hence, by the DeMillo-Lipton-Schwarz-Zippel lemma [DL78, Sch80, Zip79] the rank of the scalar matrix $L(M_1, M_2, \ldots, M_n)$ is $d\ell$, where M_i is a random scalar matrix with entries from $\mathbb{F}$ or a small extension. ☐

Finally, we state and prove a *modified version* of a result due to Cohn that allows us to relate the factorization of a polynomial $f \in \mathbb{F}\langle X\rangle$ to the factorization of its Higman linearization L. The proof is given in the appendix.

Theorem 3.9. [Coh06, Theorem 5.8.8] *Let $C \in \mathbb{F}\langle X\rangle^{d\times d}$ be a full and right monic (or left monic) linear matrix for $d > 1$. Then C is not an atom if and only if there are $d \times d$ invertible scalar* *matrices S and S' such that*

$$SCS' = \begin{pmatrix} A & 0 \\ D & B \end{pmatrix} \tag{2}$$

where A is an $r \times r$ full right (respec. left) monic linear matrix and B is an $s \times s$ full right (respec. left) monic linear matrix such that $r + s = d$.

Remark 3.10. *In [Coh06] the theorem is proved under the stronger assumption that C is monic. However, as we show, it holds even for C that is right monic or left monic with minor changes to Cohn's proof. We require the above version for our factorization algorithm.*

4 Polynomial factorization: commutatively non-zero case

Recall that $\mathbb{F}\langle X\rangle$ denotes the free noncommutative polynomial ring $\mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ and our goal is to give a randomized polynomial-time factorization algorithm for input polynomials in $\mathbb{F}\langle X\rangle$ given as arithmetic formulas when $\mathbb{F} = \mathbb{F}_q$ is a finite field of size q.

A polynomial $f \in \mathbb{F}\langle X\rangle$ is *commutatively nonzero* if $f(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ for scalars $\alpha_i \in \mathbb{F}$ (or a small extension field of $\mathbb{F}$).

In this section we will present the factorization algorithm for commutatively nonzero polynomials.[7] It has three broad steps:

(i) We transform the given polynomial f to a full and *right (or left) monic* linear matrix L by first the Higman linearization of f followed by the algorithm in the proof of Theorem 3.3.

(ii) Next, we factorize the full and right (or left) monic linear matrix L into atoms.

(iii) Finally, we recover the irreducible factors of f from the atomic factors of L.

We formally state the three problems of interest in this paper.

Problem 4.1 (FACT($\mathbb{F}$)).
Input *A noncommutative polynomial $f \in \mathbb{F}\langle X\rangle$ given by an arithmetic formula.*
Output *Compute a factorization $f = f_1 f_2 \cdots f_r$, where each f_i is irreducible, and each f_i is output as an algebraic branching program.*

Problem 4.2 (LIN-FACT($\mathbb{F}$)).
Input *A full and right (or left) monic linear matrix $L \in \mathbb{F}\langle X\rangle^{d\times d}$.*
Output *Compute a factorization $L = F_1 F_2 \cdots F_r$, where each F_i is a full linear matrix that is an atom.*

Problem 4.3 (INV($\mathbb{F}$)).
Input *A list of scalar matrices $A_1, A_2, \ldots, A_n \in \mathbb{F}^{d\times d}$.*
Output *Compute a nontrivial invariant subspace $V \subset \mathbb{F}^d$ or report that the only invariant subspaces are 0 and $\mathbb{F}^d$.*

[7] In the next section we will deal with the general case. The algorithm is more technical in detail, although in essence the same.

In the three-step outline of the algorithm, for the second step we will show that factoring a full and right (or left) monic linear matrix is randomized polynomial-time reducible to the problem of computing a common invariant subspace for a collection of scalar matrices. For the third step, we will give a polynomial-time algorithm (based on Lemma 3.7) to recover the irreducible factors of f from the atomic factors of L.

Remark 4.4. *We use Ronyai's randomized polynomial-time algorithm [Rón90] to solve the problem of computing a a common invariant subspace for a collection of matrices over $\mathbb{F}_q$. Over rational numbers $\mathbb{Q}$, even for a special case the problem of computing a common invariant subspace turns out to be at least as hard as factoring square-free integers [FR85]. Hence, our approach to noncommutative polynomial factorization does not yield an efficient algorithm over $\mathbb{Q}$.*

Suppose $f \in \mathbb{F}\langle X\rangle$ is given by a noncommutative arithmetic formula. Since f has small degree we can check if it is commutatively nonzero in randomized polynomial-time by the DeMillo-Lipton-Schwatrtz-Zippel test [DL78, Sch80, Zip79] and, if so, find $\alpha_i \in \mathbb{F}, i \in [n]$ such that $f(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ (if $\mathbb{F}$ is small, we pick α_i from a small extension field). Furthermore, by a linear shift of the variables $x_i \leftarrow x_i + \alpha_i, i \in [n]$ followed by scaling we can assume $f(\overline{0}) = 1$. Note that from the factorization of the linear shift of f we can recover the factors of f by shifting the variables back, and irreducibility is preserved by linear shift. For the rest of this section we will assume $f(\overline{0}) = 1$.

Let $L = A_0 + \sum_{i=1}^{n} A_i x_i$. As $f(\overline{0}) = 1$, we have $L(\overline{0}) = A_0$ is an invertible matrix. We now present an efficient algorithm for factoring L as a product of linear matrices $L_1 L_2 \cdots L_r$, where each L_i is an atom.

Remark 4.5. *The factorization algorithm for arbitrary full and right (or left) monic linear matrices (in which A_0 need not be invertible) is similar but more involved. It is based on Lemma 3.8 and is dealt with in the next section.*

4.1 Algorithm for a special case of LIN-FACT($\mathbb{F}_q$)

Theorem 4.6. *There is a randomized polynomial-time algorithm for the following two special cases of the* LIN-FACT($\mathbb{F}_q$) *problem:*

1. *Given a full right monic matrix L as input such that $L(\overline{0})$ is an invertible matrix, the algorithm outputs a factorization of L as a product of linear matrices that are atoms.*
2. *Given a full left monic matrix L as input such that $L(\overline{0})$ is an invertible matrix, the algorithm outputs a factorization of L as a product of linear matrices that are atoms.*

Proof. We present the algorithm only for the first part, as the second part has essentially the same solution.

Let $L = A_0 + \sum_{i=1}^{n} A_i x_i$ in $\mathbb{F}\langle X\rangle^{d\times d}$ be such an instance of LIN-FACT($\mathbb{F}_q$). We can write $L = A_0 \cdot L'$ where L' is the full and right monic linear matrix

$$L' = I_d + \sum_{i=1}^{n} A_0^{-1} A_i x_i.$$

Clearly, it suffices to factorize the linear matrix L' into atoms.

First we show that L' is an not atom iff matrices $A_0^{-1}A_i$, $1 \le i \le n$ have a nontrivial common invariant subspace. By Theorem 3.9, L' is not an atom if and only if we can write $S_1 L' S_2 = \begin{pmatrix} B & 0 \\ D & C \end{pmatrix}$ for invertible scalar matrices S_1 and S_2, where B and C are full and right monic linear matrices, and D is some linear matrix. Equating the constant terms on both sides of the above equation we have $S_1 S_2 = \begin{pmatrix} B_0 & 0 \\ D_0 & C_0 \end{pmatrix}$ as the constant term of L' is I_d. Thus the matrices $S_1 S_2$ and its inverse also has the same block form which implies that $S_1 L' S_1^{-1} = S_1 L' S_2 (S_1 S_2)^{-1}$ also has the same block form. It follows that the n matrices $A_0^{-1}A_i, 1 \le i \le n$ have a nontrivial common invariant subspace. Conversely, if the matrices $A_0^{-1}A_i, 1 \le i \le n$ have a nontrivial common invariant subspace then we have a basic change scalar matrix S such that $SL'S^{-1}$ has the block form $\begin{pmatrix} L_1 & 0 \\ * & L_2 \end{pmatrix}$, where L_1 and L_2 are full and right monic linear matrices. So by Theorem 3.9 L' is not an atom. So we have established, L' (and hence L) is not an atom iff matrices $A_0^{-1}A_i$, $1 \le i \le n$ have a nontrivial common invariant subspace. We will use Ronyai's randomized polynomial-time algorithm for finding a nontrivial common invariant subspace for matrices $A_0^{-1}A_i, 1 \le i \le n$ over finite field $\mathbb{F}_q$.

If there is no nontrivial invariant subspace then the linear matrix L' (and hence L) is an atom. Otherwise, by repeated application of Ronyai's algorithm we will obtain a basis change scalar matrix T which when applied to L' yields a linear matrix in the following *atomic block diagonal form*:

$$TL'T^{-1} = \begin{pmatrix} L_1 & 0 & 0 & \dots & 0 \\ * & L_2 & 0 & \dots & 0 \\ * & * & L_3 & \dots & 0 \\ & & & \ddots & \\ * & * & * & \dots & L_r \end{pmatrix}, \qquad (3)$$

where for each $j \in [r]$, the full right monic linear matrix $L_j \in \mathbb{F}\langle X \rangle^{d_j \times d_j}$ is an atom, and each $*$ stands for some unspecified linear matrix. It is now easy to factorize $TL'T^{-1}$ as a product of atoms by noting one step of the factorization of $TL'T^{-1}$ from its form:

$$TL'T^{-1} = \begin{pmatrix} A & 0 \\ D & L_r \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ D & I \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ 0 & L_r \end{pmatrix}.$$

We note that $\begin{pmatrix} I & 0 \\ D & I \end{pmatrix}$ is a unit. Since L_r is an atom the product $\begin{pmatrix} I & 0 \\ D & I \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ 0 & L_r \end{pmatrix}$ is also an atom and a linear matrix, and it is the rightmost factor of $TL'T^{-1}$. Continuing thus with A now, we can factorize $TL'T^{-1}$ as a product $F_1' F_2' \cdots F_r'$ of r atoms, each of which is a linear matrix. It follows that $L = A_0 T^{-1} F_1' F_2' \cdots F_r' T$ is a complete factorization of L as a product of atomic linear matrices (both A_0 and T are scalar invertible matrices). ☐

Remark 4.7. *We note that Ronyai's algorithm [Rón90] for* INV($\mathbb{F}_q$) *is actually a deterministic polynomial-time* reduction *from* INV($\mathbb{F}_q$) *to univariate polynomial factorization over* $\mathbb{F}_q$*.*

Based on whether we want to work with right monic or left monic case we will express $f \oplus I_s$ in an appropriate form using Higman linearization and Theorem 3.3 as described in the equation below:

$$f \oplus I_s = \begin{cases} PU(L' \oplus I_t)SQ, & \text{in the right monic case} \\ PS(L' \oplus I_t)UQ, & \text{in the left monic case} \end{cases} \tag{4}$$

where $d + t = s + 1$, $L' \in \mathbb{F}\langle X \rangle^{d \times d}$ is a full and right (or left) monic linear matrix, P is upper triangular with all 1's diagonal, Q is lower triangular with all 1's diagonal, $U \in \mathbb{F}\langle X \rangle^{(d+t)\times(d+t)}$ is a unit, and $S \in \mathbb{F}^{(d+t)\times(d+t)}$ is an invertible scalar matrix.

Algorithm for FACT($\mathbb{F}_q$)

We are now ready to describe the polynomial factorization algorithm for commutatively nonzero polynomials in $\mathbb{F}\langle X \rangle$. Starting with the Higman linearization of the input polynomial $f \in \mathbb{F}\langle X \rangle$ as in Equation 4, by an application of the first parts of Theorems 3.3 and 4.6 we obtain the factorization $f \oplus I_s = PUF'_1F'_2 \cdots F'_rSQ$ using the structure in Equation 3.

Alternatively, by applying the second part of Theorem 3.3 we can compute a left monic linear matrix L' that is a stable associate of f and, applying the second part of Theorem 4.6 we can compute the factorization

$$f \oplus I_s = PS'F'_1F'_2 \cdots F'_rU'Q. \tag{5}$$

where each linear matrix F'_i is an atom, P is upper triangular with all 1's diagonal, Q is lower triangular with all 1's diagonal, U' is a unit and S' is a scalar invertible matrix. Equation 5 is the form we will use for the algorithm (we could equally well use the other factorization).

From the structure of the atomic block diagonal matrix $TL'T^{-1}$ in Equation 3 notice that the product $S'F'_1F'_2 \cdots F'_i$ is a linear matrix for each $1 \leq i < r$.

The next lemma presents an algorithm that is crucial for extracting the factors of f.

Lemma 4.8. *Let $C \in \mathbb{F}\langle X \rangle^{u \times d}$ be a linear matrix and $v \in \mathbb{F}\langle X \rangle^{d \times 1}$ be a column of polynomials such that $Cv = 0$. Each entry v_i of v is given by an algebraic branching program as input. Then, in polynomial time we can compute a invertible matrix $N \in \mathbb{F}\langle X \rangle^{d \times d}$ such that*

- *For $1 \leq i \leq d$ either the i^{th} column of CN is all zeros or the i^{th} row of $N^{-1}v$ is zero.*
- *Each entry of N is a polynomial of degree at most d^2 and is computed by a polynomial size ABP, and also each entry of N^{-1} is computed by a polynomial size ABP.*

Proof. We will describe the algorithm as a recursive procedure Trivialize that takes matrix C and column vector v as parameters and returns a matrix N as claimed in the statement.

Procedure Trivialize($C \in \mathbb{F}\langle X \rangle^{u \times d}, v \in \mathbb{F}\langle X \rangle^{d \times 1}$)

1. If $d = 1$ then (since $Cv = 0$ iff either $C = 0$ or $v = 0$) **return** the identity matrix.
2. If $d > 1$ then

3. write $C = C_0 + C_1$, where C_0 is a scalar matrix and C_1 is the degree 1 homogeneous part of C. Let k be the degree of the highest degree nonzero monomials in the polynomial vector v, and let m be a nonzero degree k monomial. Let $v(m) \in \mathbb{F}_q^{d\times 1}$ denote its (nonzero) coefficient in v. Then $Cv = 0$ imples $C_1 v(m) = 0$. Let $T_0 \in \mathbb{F}_q^{d\times d}$ be a scalar invertible matrix with first column $v(m)$ obtained by completing the basis.
   (a) If $C_0 v(m) = 0$ then the first column of CT_0 is zero.
   (b) Otherwise, CT_0 has first column as the nonzero scalar vector $Cv(m) = C_0 v(m)$. Suppose i^{th} entry of $Cv(m)$ is a nonzero scalar α. With column operations we can drive the i^{th} entry in all other columns of CT_0 to zero. Let the resulting matrix be CT_0T_1 (where the matrix T_1 is invertible as it is a product of elementary matrices corresponding to these column operations, each of which is of the form $\mathrm{Col}_i \leftarrow (\mathrm{Col}_i + \mathrm{Col}_1 \cdot \alpha_0 + \sum_i \alpha_i x_i))$. Notice that CT_0T_1 is still linear.
   (c) As $Cv = (CT_0T_1)(T_1^{-1}T_0^{-1}v)$, and in the i^{th} row of CT_0T_1 the only nonzero entry is α which is in its first column, we have that the first entry of $T_1^{-1}T_0^{-1}v$ is zero.
4. Let $C' \in \mathbb{F}\langle X\rangle^{u\times(d-1)}$ obtained by dropping the first column of CT_0T_1. Let $v' \in \mathbb{F}\langle X\rangle^{(d-1)\times 1}$ be obtained by dropping the first entry of $T_1^{-1}T_0^{-1}v$. Note that C' is still linear.
5. Recursively call Trivialize($C' \in \mathbb{F}\langle X\rangle^{u\times(d-1)}, v' \in \mathbb{F}\langle X\rangle^{(d-1)\times 1}$). and let the matrix returned by the call be $T_2 \in \mathbb{F}\langle X\rangle^{(d-1)\times(d-1)}$.
6. Putting it together, return the matrix $T_0T_1(I_1 \oplus T_2)$.

To complete the proof, we note that a highest degree monomial m such that $v(m) \neq 0$ is easy to compute in deterministic polynomial time if each v_i is given by an algebraic branching program using the PIT algorithm of Raz and Shpilka [RS05]. Notice that for the recursive call we need C' to be also a linear matrix and each entry of v' to have a small ABP. C' is linear because CT_0T_1 is a linear matrix since CT_0 is linear, its first column is scalar, and each column operation performed by T_1 is scaling the first column of CT_0 by a linear form and subtracting from another column of CT_0. Each entry of v' has a small ABP because T_0^{-1} is scalar and it is easy to see that the entries of T_1^{-1} have ABPs of polynomial size. Finally, we note that T_1 is a product of at most $d-1$ linear matrices (each corresponding to a column operation), and N is an iterated product of d such matrices. Hence, each entry of N as well as N^{-1} is a polynomial of degree at most d^2 and is computable by a small ABP.

□

Turning back to our algorithm for FACT($\mathbb{F}_q$), in the next lemma we design an efficient algorithm that will allow us to extract all the irreducible factors of f (given Equation 5).

Lemma 4.9 (Factor Extraction)**.** *Let $f \in \mathbb{F}\langle X\rangle$ be a polynomial and $G \in \mathbb{F}\langle X\rangle^{(d-1)\times(d-1)}$ be a unit such that*

$$\begin{pmatrix} f & u \\ 0 & G \end{pmatrix} = PCD, \tag{6}$$

such that

- *C is a full linear matrix that is a non-unit, P is upper triangular with all 1's diagonal, and $D \in \mathbb{F}\langle X\rangle^{d\times d}$ is a full non-unit matrix which is also an atom.*
- *The polynomial f, and the entries of u, G, P, D are all given as input by algebraic branching programs.*

Then we can compute in deterministic polynomial time a nontrivial factorization $f = g \cdot h$ of the polynomial f such that h is an irreducible polynomial.

Proof. Let

$$C = \begin{pmatrix} c_1 & c_3 \\ c_2 & c_4 \end{pmatrix} \text{ and } D = \begin{pmatrix} d_1 & d_3 \\ d_2 & d_4 \end{pmatrix},$$

written as 2×2 block matrices where c_1 and d_1 are 1×1 blocks. By dropping the first row of the matrix in the left hand side of Equation 6 and the first row of P we get

$$(0\ G) = (0\ P')CD,$$

where P' is also an upper triangular matrix with all 1's diagonal. Equating the first columns on both sides we have

$$\begin{aligned} 0 &= (0\ P')\begin{pmatrix} c_1 & c_3 \\ c_2 & c_4 \end{pmatrix}\begin{pmatrix} d_1 \\ d_2 \end{pmatrix}, \text{ which implies that} \\ 0 &= P'(c_2\ c_4)\begin{pmatrix} d_1 \\ d_2 \end{pmatrix}, \text{ and hence} \\ 0 &= (c_2\ c_4)\begin{pmatrix} d_1 \\ d_2 \end{pmatrix}, \text{ since } P' \text{ is invertible.} \end{aligned}$$

Since $(c_2\ c_4) \in \mathbb{F}\langle X\rangle^{(d-1)\times d}$ is a matrix with linear entries and $\begin{pmatrix} d_1 \\ d_2 \end{pmatrix} \in \mathbb{F}\langle X\rangle^{d\times 1}$ is a column vector of polynomials which are given by ABPs as input, we can apply the algorithm of Lemma 4.8 to compute a unit N such that its entries are all given by ABPs such that for $1 \le i \le d$, either the i^{th} column of $(c_2'\ c_4') = (c_2\ c_4)N$ is zero or the i^{th} row of $\begin{pmatrix} d_1' \\ d_2' \end{pmatrix} = N^{-1}\begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$ is zero.

Now the following argument is almost identical with the argument towards the end of the proof of the Theorem 3.6. We give it below for completeness. Since D is a full matrix, the matrix $N^{-1}D$ is also full which implies its first column $\begin{pmatrix} d_1' \\ d_2' \end{pmatrix}$ cannot be all zeros. So there is at least one nonzero entry in $\begin{pmatrix} d_1' \\ d_2' \end{pmatrix}$ and the corresponding column in $(c_2'\ c_4')$ is all zero. This implies there exist a permutation matrix Π such that the first column of $C(c_2'\ c_4')\Pi$ is all zero and first entry of $\Pi^{-1}\begin{pmatrix} d_1' \\ d_2' \end{pmatrix}$ is non zero.

Consider the matrices $C'' = CN\Pi = \begin{pmatrix} c_1'' & c_3'' \\ c_2'' & c_4'' \end{pmatrix}$ and $D'' = \Pi^{-1}N^{-1}D = \begin{pmatrix} d_1'' & d_3'' \\ d_2'' & d_4'' \end{pmatrix}$. We have

$$\begin{pmatrix} f & * \\ 0 & G' \end{pmatrix} = P^{-1}\begin{pmatrix} f & u \\ 0 & G \end{pmatrix} = \begin{pmatrix} c_1'' & c_3'' \\ c_2'' & c_4'' \end{pmatrix}\begin{pmatrix} d_1'' & d_3'' \\ d_2'' & d_4'' \end{pmatrix}$$

, where $G' = (P')^{-1}G$ is a unit, c_2'' is all zero column matrix and d_1'' is non-zero. Now observing $(2,1)^{th}$ matrix block in the above equation, we get d_2'' is all zero column. Hence, by looking at $(2,2)^{th}$ block in the above equation, we can see that c_4'' and d_4'' are units as G' is a unit. Clearly, we have $f = c_1'' \cdot d_1''$. Now, since C and D are non-units (by assumption), the matrices C'' and D'' are also non-units. Therefore, c_1'' is not a scalar for otherwise C'' would be a unit. Similarly, d_1'' is not a scalar. It follows that $f = c_1''d_1''$ is a nontrivial factorization of f.

Furthermore, since D is an atom by assumption and D'' is a stable associate of D, D'' is an atom. As $D'' = \begin{pmatrix} d_1'' & d_3'' \\ 0 & d_4'' \end{pmatrix}$ and d_4'' is invertible, we get $\begin{pmatrix} 1 & 0 \\ 0 & (d_4'')^{-1} \end{pmatrix} \cdot D'' = \begin{pmatrix} d_1'' & d_3'' \\ 0 & I_s \end{pmatrix}$. Now applying suitable row operations to the matrix $(1 \oplus (d_4'')^{-1})D''$ we can drive d_3'' to zero. So we have $U(1 \oplus (d_4'')^{-1})D'' = (d_1'' \oplus I_s)$ for a unit U. Hence d_1'' is an associate of D'' and therefore d_1'' is irreducible as D'' is an atom.

□

Finally, we describe the factorization algorithm for commutatively nonzero polynomials $f \in \mathbb{F}\langle X\rangle$ over finite fields $\mathbb{F}_q$.

Theorem 4.10. *Let $\mathbb{F}\langle X\rangle = \mathbb{F}_q\langle X\rangle$ and $f \in \mathbb{F}\langle X\rangle$ be a commutatively nonzero polynomial given by an algebraic branching program of size s as input instance of* FACT($\mathbb{F}_q$). *Then there is a* poly$(s, \log q)$ *time randomized algorithm that outputs a factorization $f = f_1 f_2 \cdots f_r$ such that each f_i is irreducible and is output as an algebraic branching program.*

Proof. Given f as input, we apply Higman linearization followed by the algorithm for LIN-FACT($\mathbb{F}_q$) described in Theorem 4.6 to obtain the factorization of $f \oplus I_s = PSS_1F_1F_2 \dots F_rS_2UQ$ where each linear matrix F_i is an atom, P is upper triangular with all 1's diagonal, Q is lower triangular with all 1's diagonal, U is a unit and S is a scalar invertible matrix, as given in Equation 5. We can now apply Lemma 4.9 to extract irreducible factors of f (one by one from the right).

For the first step, let $C = SS_1F_1F_2 \cdots F_{r-1}$ and $D = F_rS_2UQ$ in Lemma 4.9. The proof of Lemma 4.9 yields the matrix $N_r = N\Pi$ such that both matrices $C'' = PSS_1F_1F_2 \cdots F_{r-1}N_r$ and $D'' = N_r^{-1}F_rS_2UQ$ has the first column all zeros except the $(1,1)^{th}$ entries c_1'' and d_1'' which yields the nontrivial factorization $f = c_1''d_1''$, where $d_1'' = f_r$ is irreducible. Renaming c_1'' as g_r we have from the structure of C'':

$$\begin{pmatrix} g_r & * \\ 0 & G_r \end{pmatrix} = P(SS_1F_1F_2 \cdots F_{r-2})(F_{r-1}N_r).$$

Setting $C = SS_1F_1F_2 \cdots F_{r-2}$ and $D = F_{r-1}N_r$ in Lemma 4.9 we can compute the matrix N_{r-1} using which we will obtain the next factorization $g_r = g_{r-1}f_{r-1}$, where f_{r-1} is irreducible because the linear matrix F_{r-1} is an atom. Lemma 4.9 is applicable as all conditions are met by the matrices in the above equation (note that G_r will be a unit).

Continuing thus, at the i^{th} stage we will have $f = g_{r-i+1} f_{r-i+1} f_{r-i+2} \cdots f_r$ after obtaining the rightmost i irreducible factors by the above process. At this stage we will have

$$\begin{pmatrix} g_{r-i+1} & * \\ 0 & G_{r-i+1} \end{pmatrix} = P(SS_1 F_1 F_2 \cdots F_{r-i-1})(F_{r-i} N_{r-i+1}),$$

where G_{r-i+1} is a unit and all other conditions are met to apply Lemma 4.9.

Thus, after r stages we will obtain the complete factorization $f = f_1 f_2 \cdots f_r$. For the running time, it suffices to note that the matrix N computed in Lemma 4.9 is a product of degree at most d^2 many linear matrices (corresponding to the column operations). Thus, at the i^{th} of the above iteration, the sizes of the ABPs for the entries of N_{r-i+1} are independent of the stages. Hence, the overall running time is easily seen to be polynomial in s and $\log q$. □

Corollary 4.11. *If $f \in \mathbb{F}\langle X \rangle$ is commutatively nonzero polynomial given as input in sparse representation (as an $\mathbb{F}_q$-linear combination of its monomials) then in randomized polynomial time we can compute a factorization into irreducible factors in sparse representation.*

Proof. Let f be given as input in sparse representation. Suppos $\deg f = d$ and it is t-sparse. Then there are at most td^2 many monomials that can occur as a substring of the monomials of f. We can apply the randomized algorithm of Theorem 4.10 to obtain the factorization $f = f_1 f_2 \cdots f_r$, where each f_i is given by an ABP. Now, for each of the td^2 many candidate monomials of f_i we can find its coefficient in f_i in polynomial time (using the Raz-Shpilka algorithm [RS05]). Hence we can obtain the factorization $f = f'_1 f'_2 \cdots f'_r$, where each f'_i is a t-sparse polynomial. □

5 Factorization of Commutatively zero polynomials

In this section we will describe the general case of the factorization algorithm when the input polynomial $f \in \mathbb{F}\langle X \rangle$ is a commutatively zero polynomial. That is, f evaluates to zero on all scalar substitutions from $\mathbb{F}_q$ or any (commutative) extension field.

The factorization algorithm will follow the three broad steps described in Section 4 for the commutatively nonzero case: first, using Higman linearization and Theorem 3.3, transform the polynomial f to a stably associated linear matrix L that is full and left (or right) monic. Next, factorize the linear matrix L into atoms. Finally, recover the irreducible factors of f from the atomic factors of the linear matrix L using the factor extraction procedure described in Lemma 4.9.

The step that requires a new algorithm is factorizing a full and right (or left) monic linear matrix $L \in \mathbb{F}\langle X \rangle$ into atoms when f is commutatively zero, which means there is no scalar substitution $x_i \leftarrow \alpha_i, i \in [n]$ such that $L(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is invertible. Note that in this case we cannot apply the algorithm for factorizing a linear matrix as discussed in the proof of Theorem 4.6).

5.1 Factorization of full and monic linear matrices

Let $f \in \mathbb{F}\langle X \rangle$ be the input polynomial given by a size s formula and let $L \in \mathbb{F}\langle X \rangle^{d \times d}$ be a full, right monic linear matrix stably associated with f obtained via Higman linearization and an application of Theorem 3.3.

Recall, by Equation 4 we have $f \oplus I_s = PU(L \oplus I_t)SQ$ where, P, Q are respectively upper triangular and lower triangular units with diagonal entries 1, U is a unit and S is scalar invertible.

Let $L = A_0 + \sum_{i=1}^{n} A_n x_i \in \mathbb{F}\langle X\rangle^{d\times d}$ be the given full and right monic linear matrix. First, by Lemma 3.8, we will find a suitable scalar matrix n-tuple $\bar{M} = (M_1, M_2, \ldots, M_n)$, each $M_i \in \mathbb{F}_q^{\ell\times\ell}$ for $\ell \le 2d$, such that under the substitution $x_i \leftarrow M_i$ the matrix $L(\bar{M})$ is invertible.

For $1 \le i \le n$ let Y_i be an $\ell \times \ell$ matrix of distinct noncommuting variables y_{ijk}. We consider the dilated linear matrix

$$L' = A_0 \otimes I_\ell + \sum_{i=1}^{n} A_i \otimes (Y_i + M_i). \tag{7}$$

It is not hard to see that L' is full and L' is right monic as L is right monic. Additionally, its constant term is invertible. So, we can apply Theorem 4.6 to factorize L' as a product of two linear matrices, both non-units.

The following lemma [HKV20] has an important role in our algorithm for recovering the factorization for L from a factorization of L'.

Lemma 5.1. *[HKV20]*

Let $L \in \mathbb{F}\langle X\rangle^{d\times d}$ be a full linear matrix with $L = A_0 + A_1x_1 + \ldots + A_nx_n$ such that $A_i \neq 0$ for at least one i, $1 \le i \le n$ and $L' \in R^{d\ell\times d\ell}$ be a matrix obtained from L by substituting variable x_i by Y_i for $i \in [n]$, where Y_i is $\ell \times \ell$ matrix whose $(j,k)^{th}$ entry is a fresh noncommuting variable $y_{i,j,k}$ for $1 \le j, k \le \ell$. Then

1. *If L' is of the form $GL'H = \left(\begin{array}{c|c} A' & 0 \\ \hline D' & B' \end{array}\right)$, where A' is $d' \times d'$ matrix and B' is $d'' \times d''$ matrix for $0 < d', d''$, with $d' + d'' = d\ell$ and G, H are $d\ell \times d\ell$ invertible scalar matrices then there exist $d \times d$ invertible scalar matrices U, V such that $ULV = \left(\begin{array}{c|c} A & 0 \\ \hline D & B \end{array}\right)$, where A is $e' \times e'$ matrix and B is $e'' \times e''$ matrix for $0 < e', e''$, with $e' + e'' = d$.*
2. *Moreover, given L' explicitly along with its representation mentioned above, we can find the matrices U, V in deterministic polynomial time (in n, ℓ, d).*

Remark 5.2. *We give a self-contained complete proof of the above linear-algebraic lemma in the appendix for $\mathbb{F}_q$, because the proof given in [HKV20] is sketchy in parts with some details missing, and also their lemma is stated only for complex numbers and they are not concerned about computing the matrices U and V.*

Now, we can apply Lemma 5.1 to transform the factorization of L' to a factorization of L as a product of two linear matrices, both non-units. Repeating the above on both the factors of L we will get a complete atomic factorization of L. Formally, we prove the following.

Theorem 5.3. *On input a full and right (or left) monic linear matrix $L = A_0 + \sum_{i=1}^{n} A_i x_i$ where $A_i \in \mathbb{F}^{d\times d}$ for $i \in [n]$, there is a randomized polynomial time (poly(n,d)) algorithm to compute scalar invertible matrices S, S' such that SLS' has atomic block diagonal form.*

Proof. We present the algorithm only for right monic L; the left monic case has essentially the same solution.

If the input L is not full or right monic the algorithm can efficiently detect that and output "failure". If L is an atom the algorithm will output that L is an atom and set the matrices S and S' to I_d. Otherwise, the algorithm will compute invertible scalar matrices S and S' such that

$$SLS' = \begin{pmatrix} L_1 & 0 & 0 & \dots & 0 \\ * & L_2 & 0 & \dots & 0 \\ * & * & L_3 & \dots & 0 \\ & & & \ddots & \\ * & * & * & \dots & L_r \end{pmatrix}, \tag{8}$$

where the matrix on the right is in atomic block diagonal form, that is, each linear matrix L_i is an atom.

Procedure Factor(L).

1. Test if L has full noncommutative rank using the algorithm in [IQS17] or [GGdOW20]. Test if L is right monic by checking if the matrix $[A_1 A_2 \dots A_n]$ has full row rank (which is d). If L is not full and right monic the algorithm outputs "fail".

2. Assume L is full and right monic. Using Lemma 3.8, find smallest positive integer $\ell \leq 2d$ and $\ell \times \ell$ scalar matrices $M_i, i \in [n]$ with entries from $\mathbb{F}$ (or a small degree extension of $\mathbb{F}$) such that $W = L(\bar{M})$ is $d \cdot \ell \times d \cdot \ell$ invertible scalar matrix. Compute the dilated linear matrix L' in the y_{ijk} variables as in Equation 7 which can be rewritten as:

$$L' = A_0 \otimes I_\ell + \sum_{i=1}^{n} A_i \otimes M_i + \sum_{i=1}^{n} \sum_{j,k=1}^{\ell} (A_i \otimes E_{jk}) \cdot y_{ijk}.$$

   Let $L'' = W^{-1}L'$. Clearly $L''(\bar{0}) = I_{d\ell}$. Hence, by the algorithm of Theorem 4.6 we can either detect that L'' is an atom or factorize L''. If L'' is an atom then L is also an atom and the algorithm can output that and stop. Otherwise, L' is not an atom and by Theorem 4.6 we will obtain a basis change matrix T such that $TW^{-1}L'T^{-1} = TL''T^{-1} = \begin{pmatrix} C'' & 0 \\ * & D'' \end{pmatrix}$ where C'' and D'' are linear matrices of dimension $c'' \times c''$ and $d'' \times d''$ respectively, such that $c'' + d'' = d\ell$.

3. By linear shift of variables $y_{ijk} \leftarrow y_{ijk} - M_i(j,k)$ we obtain $\tilde{T}\tilde{L}\tilde{T}' = \begin{pmatrix} C' & 0 \\ * & D' \end{pmatrix}$ for some scalar invertible matrices $\tilde{T}, \tilde{T}'$ where $\tilde{L} = L(Y_1, \dots, Y_n)$.

4. Applying the algorithm of Lemma 5.1 to $\tilde{L}$, $\tilde{T}$, and $\tilde{T}'$, in deterministic polynomial time we obtain scalar invertible matrices $\tilde{S}, \tilde{S}'$ such that $\tilde{S}L\tilde{S}' = \begin{pmatrix} C & 0 \\ * & D \end{pmatrix}$ where C, D are square matrices of dimensions $e \times e$ and $g \times g$, respectively, such that $e + g = d$.

5. Recursively call Factor(C) and Factor(D). Let S_1, S_1' be the matrices returned by Factor(C) and S_2, S_2' be the matrices returned by Factor(D).

6. Let $S = (S_1 \oplus S_2)\tilde{S}$ and $S' = \tilde{S}'(S'_1 \oplus S'_2)$. Return the invertible scalar matrices S and S'. Note that at this stage SLS' has the desired atomic block diagonal form.

Next we give a brief argument for proving correctness of the above algorithm. Firstly, the algorithm declares L as an atom iff L is indeed an atom. To see this, we will prove L is not an atom iff L'' is not an atom. Forward direction is obvious. To prove the reverse direction of implication, let L'' is not an atom. Which implies $L' = WL''$ is not an atom. $\tilde{L}$ is a linear matrix obtained by substituting $M_i(j,k) = 0$ for all i, j, k in L'. Clearly, $\tilde{L}$ is not an atom as L' is not an atom. Using Lemma 5.1 it follows that L is not an atom. So we have established L is not a atom iff L'' is not an atom. So if input linear matrix L is an atom, the algorithm will correctly declare it to be an atom in step 2.

Now we argue that we will get correct atomic block diagonal form in the last step of the algorithm. Firstly, for giving recursive calls to the Factor procedure for the matrices C, D, we must have C, D to be right monic as stated in the claim below. This is proved by the same argument as in the proof of Theorem 3.9.

Claim 5.4. *Let $L \in \mathbb{F}\langle X\rangle^{d\times d}$ be a full and right monic linear matrix such that $P'LQ' = \begin{pmatrix} C & 0 \\ E & D \end{pmatrix}$ where C and D are linear matrices of dimensions $e \times e$, $g \times g$, respectively, such that $e + g = d$. Then both C, D are right monic.*

By recursive calls Factor(C) and Factor(D) obtain matrices S_1, S'_1, S_2, S'_2 such that $S_1CS'_1 = C'$ and $S_2DS'_2 = D'$ are in atomic block diagonal form. We can write $\tilde{S}L\tilde{S}'$ as

$$\begin{aligned}
&= \begin{pmatrix} C & 0 \\ E & D \end{pmatrix} \\
&= \begin{pmatrix} C & 0 \\ 0 & I_g \end{pmatrix}\begin{pmatrix} I_e & 0 \\ E & I_g \end{pmatrix}\begin{pmatrix} I_e & 0 \\ 0 & B \end{pmatrix} \\
&= (S_1^{-1} \oplus I_g)(C' \oplus I_g)({S'}_1^{-1} \oplus I_g)\begin{pmatrix} I_e & 0 \\ E & I_g \end{pmatrix}(I_e \oplus S_2^{-1})(I_e \oplus D')(I_e \oplus {S'}_2^{-1}) \\
&= (S_1^{-1} \oplus I_g)(C' \oplus I_g)(I_e \oplus {S'}_2^{-1})\begin{pmatrix} I_e & 0 \\ S_2ES'_1 & I_g \end{pmatrix}({S'}_1^{-1} \oplus I_g)(I_e \oplus D')(I_e \oplus {S'}_2^{-1}) \\
&= (S_1^{-1} \oplus I_g)(I_e \oplus S_2^{-1})(C' \oplus I_g)\begin{pmatrix} I_e & 0 \\ S_2ES'_1 & I_g \end{pmatrix}(I_e \oplus D')({S'}_1^{-1} \oplus I_g)(I_e \oplus {S'}_2^{-1}) \\
&= (S_1^{-1} \oplus I_g)(I_e \oplus S_2^{-1})\begin{pmatrix} C' & 0 \\ S_2ES'_1 & D' \end{pmatrix}({S'}_1^{-1} \oplus I_g)(I_e \oplus {S'}_2^{-1}) \\
&= (S_1^{-1} \oplus S_2^{-1})\begin{pmatrix} C' & 0 \\ S_2ES'_1 & D' \end{pmatrix}({S'}_1^{-1} \oplus {S'}_2^{-1}).
\end{aligned}$$

Thus we have

$$(S_1 \oplus S_2)\tilde{S}L\tilde{S}'(S'_1 \oplus S'_2) = \begin{pmatrix} C' & 0 \\ S_2ES'_1 & D' \end{pmatrix}.$$

As C' and D' are in atomic block diagonal form, it follows that $\begin{pmatrix} C' & 0 \\ S_2ES_1' & D' \end{pmatrix}$ is also in atomic block diagonal form. Letting $S = (S_1 \oplus S_2)\tilde{S}$ and $S' = \tilde{S}'(S_1' \oplus S_2')$, it follows that SLS' is in the desired atomic block diagonal form which proves the correctness of Factor procedure. In each call to the procedure (excluding the recursive calls) the algorithm takes $\text{poly}(n, d, \log_2 q)$ time. The total number of recursive calls overall is bounded by d. Hence, the overall running time is $\text{poly}(n, d, \log_2 q)$. This completes the proof of the theorem. □

For the factorization of f, we assume the stably associated full linear matrix L is left monic. After we obtain atomic block diagonal form as in Equation 8, we can factorize L into atomic factors by Theorem 4.6. Combined with Equation 5 we have

$$f \oplus I_s = PS'F_1'F_2' \cdots F_r'U'Q,$$

where each linear matrix F_i' is an atom, P is upper triangular with all 1's diagonal, Q is lower triangular with all 1's diagonal, and S' is scalar invertible and U' is a unit. Now, applying Lemma 4.9 and Theorem 4.10 we obtain the complete factorization of f into irreducible factors. This is summarized in the following.

Theorem 5.5. *Let $f \in \mathbb{F}\langle X\rangle$ be a polynomial given by an algebraic branching program as input instance of* $\text{FACT}(\mathbb{F}_q)$*. Then there is a* $\text{poly}(s, \log q, |X|)$ *time randomized algorithm that outputs a factorization $f = f_1f_2 \cdots f_r$ such that each f_i is irreducible and is output as an algebraic branching program.*

Analogous to Corollary 4.11, when the polynomial is given in a sparse representation, we have

Corollary 5.6. *If $f \in \mathbb{F}\langle X\rangle$ is a polynomial given as input in sparse representation (that is, an $\mathbb{F}_q$-linear combination of its monomials) then in randomized polynomial time we can compute a factorization into irreducible factors in sparse representation.*

5.2 Factorization over small finite fields

Finally, we briefly discuss the factorization problem over small finite fields. As explained in Section 1.2, the two steps in our factoring algorithm requiring randomization can be replaced with deterministic $\text{poly}(s, q, |X|)$ time computation. Furthermore, as explained in Section 1.2, the matrix shift $(M_1, M_2, \ldots, M_n)$ required for the Theorem 5.3 can be obtained in deterministic polynomial time such that the entries of the matrices M_i are from $\mathbb{F}_q$ for each i. Putting it together, it gives us a deterministic factorization algorithm for noncommutative polynomials that are input as arithmetic formulas over $\mathbb{F}_q$. In summary, we have the following.

Theorem 5.7. *Given as input a multivariate polynomial $f \in \mathbb{F}_q\langle X\rangle$ for a finite field $\mathbb{F}_q$ by a noncommutative algebraic branching program of size s, a factorization of f as a product $f = f_1f_2 \cdots f_r$ can be computed in deterministic time* $\text{poly}(s, q, |X|)$*, where each $f_i \in \mathbb{F}_q\langle X\rangle$ is an irreducible polynomial that is output as an algebraic branching program.*

6 Concluding Remarks

In this paper we present a randomized polynomial-time algorithm for the factorization of noncommutative polyomials *over finite fields* that are input as *algebraic branching programs*. The irreducible factors are output as algebraic branching programs.

Several open questions arise from our work. We mention two of them. The first question is the complexity of factorization over rationals of noncommutative polynomials given as ABPs or arithmetic formulas. Our approach involves the crucial use of Ronyai's algorithm for invariant subspace comptutation which turns out to be a hard problem over rationals. We believe a different approach may be required for the rational case.

The use of Higman linearization prevents us from generalizing this approach to noncommutative polynomials given as arithmetic circuits. We do not know any nontrivial complexity upper bound for the factorization problem for noncommutative polynomials given as arithmetic circuits.

Acknowledgements. We thank anonymous referees and Partha Mukhopadhyay for asking about extension of our earlier factorization algorithm for noncommutative formulas to algebraic branching programs.

References

[ACDM20] Vikraman Arvind, Abhranil Chatterjee, Rajit Datta, and Partha Mukhopadhyay. A special case of rational identity testing and the brešar-klep theorem. In Javier Esparza and Daniel Kráľ, editors, *45th International Symposium on Mathematical Foundations of Computer Science, MFCS 2020, August 24-28, 2020, Prague, Czech Republic*, volume 170 of *LIPIcs*, pages 10:1–10:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[AJ22] Vikraman Arvind and Pushkar S. Joglekar. On efficient noncommutative polynomial factorization via higman linearization. In Shachar Lovett, editor, *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA*, volume 234 of *LIPIcs*, pages 12:1–12:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[AJR18] V. Arvind, Pushkar S. Joglekar, and Gaurav Rattan. On the complexity of noncommutative polynomial factorization. *Inf. Comput.*, 262:22–39, 2018.

[AL50] S.A. Amitsur and J. Levitzki. Minimal identities for algebras. *Proceedings of the American Mathematical Society*, 4(2):449–463, 1950.

[Ami66] S.A Amitsur. Rational identities and applications to algebra and geometry. *Journal of Algebra*, 3(3):304–359, 1966.

[BHL17] Jason Bell, Albert Heinle, and Viktor Levandovskyy. On noncommutative finite factorization domains. *Transactions of the American Mathematical Society*, 369(4):2675–2695, 2017.

[BS15] Nicholas R. Baeth and Daniel Smertnig. Factorization theory: From commutative to noncommutative settings. *Journal of Algebra*, 441:475–551, 2015.

[Bur05] W. Burnside. On the condition of reducibility of any group of linear substitutions. *Proceedings of London Mathematical Society*, 3:430–434, 1905.

[BW05] Andrej Bogdanov and Hoeteck Wee. More on noncommutative polynomial identity testing. In *20th Annual IEEE Conference on Computational Complexity (CCC 2005), 11-15 June 2005, San Jose, CA, USA*, pages 92–99, 2005.

[Coh06] P. M. Cohn. *Free Ideal Rings and Localization in General Rings*. New Mathematical Monographs. Cambridge University Press, 2006.

[Coh11] P. M. Cohn. *Introduction To Ring Theory*. Springer, 2011.

[DL78] Richard A. DeMillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Inf. Process. Lett.*, 7(4):193–195, 1978.

[DM17] Harm Derksen and Visu Makam. Polynomial degree bounds for matrix semi-invariants. *Advances in Mathematics*, 310:44–63, 2017.

[For14] Michael A. Forbes. *Polynomial identity testing of read-once oblivious algebraic branching programs*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2014.

[FR85] Katalin Friedl and Lajos Rónyai. Polynomial time solutions of some problems in computational algebra. In Robert Sedgewick, editor, *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 153–162. ACM, 1985.

[GGdOW20] Ankit Garg, Leonid Gurvits, Rafael Mendes de Oliveira, and Avi Wigderson. Operator scaling: Theory and applications. *Found. Comput. Math.*, 20(2):223–290, 2020.

[Hig40] Graham Higman. The units of group-rings. *Proceedings of the London Mathematical Society*, s2-46(1):231–248, 1940.

[HKV18] J.W. Helton, Igor Klep, and Jurij Volčič. Geometry of free loci and factorization of noncommutative polynomials. *Advances in Mathematics*, 331:589–626, 2018.

[HKV20] J Helton, Igor Klep, and Jurij Volčič. Factorization of Noncommutative Polynomials and Nullstellensätze for the Free Algebra. *International Mathematics Research Notices*, 2022(1):343–372, 06 2020.

[HW15] Pavel Hrubes and Avi Wigderson. Non-commutative arithmetic circuits with division. *Theory Comput.*, 11:357–393, 2015.

[IQS17] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Non-commutative edmonds' problem and matrix semi-invariants. *Comput. Complex.*, 26(3):717–763, 2017.

[IQS18] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Comput. Complex.*, 27(4):561–593, 2018.

[Kal89] Erich Kaltofen. Factorization of polynomials given by straight-line programs. *Adv. Comput. Res.*, 5:375–412, 1989.

[KSS15] Swastik Kopparty, Shubhangi Saraf, and Amir Shpilka. Equivalence of polynomial identity testing and polynomial factorization. *Comput. Complex.*, 24(2):295–331, 2015.

[KT90] Erich Kaltofen and Barry M. Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *J. Symb. Comput.*, 9(3):301–320, 1990.

[Nis91] Noam Nisan. Lower bounds for non-commutative computation (extended abstract). In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 410–418, 1991.

[Rón90] Lajos Rónyai. Computing the structure of finite algebras. *J. Symb. Comput.*, 9(3):355–373, 1990.

[RS05] Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non-commutative models. *Computational Complexity*, 14(1):1–19, 2005.

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra (3. ed.)*. Cambridge University Press, 2013.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward W. Ng, editor, *Symbolic and Algebraic Computation, EUROSAM '79, An International Symposiumon Symbolic and Algebraic Computation, Marseille, France, June 1979, Proceedings*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, 1979.

A Appendix

A.1 Higman Linearization of Algebraic Branching Programs

In this section we present a proof of Theorem 2.9. More precisely, we give an efficient deterministic algorithm to compute Higman Linearization for a non-commutative polynomial given by an algebraic branching program. We obtain this by generalizing the Higman Linearization process (described in Theorem 2.8) to what we call Block-Higman linearization. We restate Theorem 2.9) and present its proof.

Theorem A.1 (Block Higman Linearization)**.** *Given as input an algebraic branching program of size s computing a noncommutative polynomial $f \in \mathbb{F}\langle X\rangle$, we can compute in deterministic polynomial time matrices $P, Q \in \mathbb{F}\langle X\rangle^{\ell\times\ell}$ and a linear matrix $L \in \mathbb{F}\langle X\rangle^{\ell\times\ell}$ such that*

$$P\left(\begin{array}{c|c} f & 0 \\ \hline 0 & I_{\ell-1} \end{array}\right) Q \;=\; L \tag{9}$$

with P upper triangular, Q lower triangular, and the diagonal entries of both P and Q are all 1's (hence, P and Q are both units in $\mathbb{F}\langle X\rangle^{\ell\times\ell}$). Futhermore, the algorithm computes the entries of matrices P and Q as algebraic branching programs. The entries of P^{-1} and Q^{-1} are also computable as algebraic branching programs.

Proof. Let $f \in \mathbb{F}\langle X\rangle$ be the input noncommutative polynomial of degree d computed by an ABP of size s and $d+1$ layers, where the i^{th} layer has say n_i nodes. Then we have linear matrices $A_1, A_2, \ldots, A_d$ such that

$$f = A_1 \cdot A_2 \cdots A_d,$$

where A_i is $n_i \times n_{i+1}$ for each i and $n_1 = n_{d+1} = 1$. Note that the $(j,k)^{th}$ entry of A_i is the linear form labeling the edge from j^{th} node in layer i to k^{th} node in layer $i+1$.

We will prove the following more general result, dropping the constraint that $n_1 = n_{d+1} = 1$. Suppose $A_1, A_2, \ldots, A_d$ are linear matrices of compatible dimensions (A_i is $n_i \times n_{i+1}$ for each i) such that the matrix product

$$M = A_1 \cdot A_2 \cdots A_d$$

is well defined. The algorithm we will describe will compute matrices P, Q, L such that

$$P\left(\begin{array}{c|c} M & 0 \\ \hline 0 & I_{\ell-1} \end{array}\right) Q \;=\; L \tag{10}$$

and P, Q, L have the properties as stated in the theorem.

The proof is by an easy induction on number d of linear matrices whose product is M. We set up this induction by describing a single step of Block-Higman linearization writing the input matrix $M = AB$, where $A = A_1 \cdot A_2 \cdots A_{d-1}$ and $B = A_d$ is a linear matrix.

So, let M be the $r \times t$ matrix where $M = A \cdot B$ with $A \in \mathbb{F}\langle X\rangle^{r\times s}$ and $B \in \mathbb{F}\langle X\rangle^{s\times t}$, and B is a linear matrix. We apply the following steps to M.

- Expand M to a $(r+s)\times(t+s)$ matrix of the following shape by adding s new rows and s new columns, with the bottom right diagonal block being I_s and the remaining entries zero to obtain the following:

$$\left[\begin{array}{c|c} M & 0 \\ \hline 0 & I_s \end{array}\right].$$

- Use suitable block row and column operations to transform the matrix as follows

$$\begin{pmatrix} AB & 0 \\ 0 & I_s \end{pmatrix} \to \begin{pmatrix} AB & A \\ 0 & I_s \end{pmatrix} \to \begin{pmatrix} 0 & A \\ -B & I_s \end{pmatrix}$$

  Here the first step is realized by computing the matrix product $A\cdot[0 \mid I_s]$ and adding it to the respective blocks of the first r rows. The second step is realized by computing the matrix product

$$\begin{pmatrix} A \\ I_s \end{pmatrix} \cdot (-B)$$

  and adding this to the respective blocks of the first t columns. These two steps are realized by left multiplication by $\left(\begin{array}{c|c} I_r & A \\ \hline 0 & I_s \end{array}\right)$ and right multiplication by $\left(\begin{array}{c|c} I_t & 0 \\ \hline -B & I_s \end{array}\right)$.

So we have

$$\begin{pmatrix} I_r & A \\ 0 & I_s \end{pmatrix}\begin{pmatrix} AB & 0 \\ 0 & I_s \end{pmatrix}\begin{pmatrix} I_t & 0 \\ -B & I_s \end{pmatrix} = \begin{pmatrix} 0 & A \\ -B & I_s \end{pmatrix}.$$

In the above, we note that the row operation matrix $\begin{pmatrix} I_r & A \\ 0 & I_s \end{pmatrix}$ is upper triangular with all diagonal entries 1 where as the column operation matrix $\begin{pmatrix} I_t & 0 \\ -B & I_s \end{pmatrix}$ is lower triangular with all diagonal entries 1.

Crucially, if $A = A_1 \cdot A_2 \cdots A_{d-1}$ and $B = A_d$, the resulting matrix has only A as the nonlinear block which is a product of $d-1$ linear matrices. We can now apply induction to the matrix A to obtain the Block-Higman linearization of M as claimed.

We describe the intermediate steps of the induction in more detail, in order to see the final shape of the linear matrix.

Let $M = A_1A_2\dots A_d$ where $A_i \in \mathbb{F}\langle X\rangle^{n_i\times n_{i+1}}$, are linear matrices. At the i^{th} step of the induction Block-Higman linearization transforms a matrix of the form $\begin{pmatrix} * & A_1A_2\dots A_{d-i} \\ * & * \end{pmatrix}$ into a matrix of the form $\begin{pmatrix} * & A_1A_2\dots A_{d-i-1} \\ * & * \end{pmatrix}$ where each $*$ indicates matrix blocks with linear entries. After $d-1$ steps of Block-Higman linearization we obtain a linear matrix which is an associate of M.

In more detail, let $M_0 = A_1A_2\dots A_d, P_0 = I_{n_1}$, $Q_0 = I_{n_{d+1}}$ and $t_0 = 0$. We have $P_0(M \oplus I_{t_0})Q_0 = M_0$. Inductively, assume that we have upper triangular matrix P_i with all diagonal entries 1 and a lower triangular matrix Q_i with all diagonal entries 1 such that

$$P_i \begin{pmatrix} M & 0 \\ 0 & I_{t_i} \end{pmatrix} Q_i = M_i.$$

Here, M_i is a polynomial matrix which has top right block equal to $A_1A_2\dots A_{d-i}$ and the other entries of M are linear and the entries of P_i and Q_i are all computable by ABPs. Let $t_{i+1} = t_i + n_{d-i}$. Clearly, $(P_i \oplus I_{n_{d-i}})(M \oplus I_{t_{i+1}})(Q_i \oplus I_{n_{d-i}}) = M_i \oplus I_{n_{d-i}}$. Let M_i' be a matrix obtained from M_i by replacing top right block by 0. Let M_{i+1} be a 2×2 block matrix with M_i' as top left block and the structure as shown below

$$M_{i+1} = \left(\begin{array}{c|c|c} & 0 & A_1A_2\dots A_{d-i-1} \\ \hline & & 0 \\ & & \vdots \\ & & 0 \\ \hline 0 \quad 0 \quad \dots \quad 0 \quad 0 & -A_{d-i} & I_{n_{d-i}} \end{array}\right),$$

where matrix blocks $-A_{d-i}$ and $A_1A_2\dots A_{d-i-1}$ align with top right 0 block in M_i'. Now we define suitable block row and column operations which transforms matrix $M_i \oplus I_{n_{d-i}}$ to M_{i+1}.

By applying the Block-Higman linearization step we will obtain

$$P'(M_i \oplus I_{n_{d-i}})Q' = M_{i+1},$$

where P' and Q' are upper and lower triangular matrices performing the block row and column operations and their entries are computable by ABPs. Letting $P_{i+1} = P'(P_i \oplus I_{n_{d-i}})$ and $Q_{i+1} = (Q_i \oplus I_{n_{d-i}})Q'$ we get

$$P_{i+1}(M \oplus I_{t_{i+1}})Q_{i+1} = M_{i+1}$$

where P_{i+1} and Q_{i+1} are upper and lower triangular matrices with diagonal entries 1, the top right block (consisting of top n_1 rows and last n_{d-i} columns) of M_{i+1} is $A_1A_2\dots A_{d-i-1}$ and all other entries of M_{i+1} are linear. Continuing thus, we obtain upper and lower triangular matrices P_{d-1} and Q_{d-1} with all diagonal entries 1 such that $P_{d-1}(M \oplus I_{t_{d-1}})Q_{d-1} = M_{d-1}$ which is a linear matrix. Moreover, it is easy to see that entries of P_{d-1} and Q_{d-1} are given by polynomial size ABPs (of $O(s^2)$ size to be precise).

Carefully observing the shapes of the matrices M_i we note that the final linearized matrix M_{d-1} has the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & A_1 \\ A_d & I_{n_d} & 0 & 0 & \dots & 0 & 0 \\ 0 & A_{d-1} & I_{n_{d-1}} & 0 & \dots & 0 & 0 \\ 0 & 0 & A_{d-2} & I_{n_{d-2}} & \dots & 0 & 0 \\ 0 & 0 & \dots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & 0 & 0 & \dots & A_2 & I_{n_2} \end{pmatrix}$$

M_{d-1} is a $d \times d$ block matrix with

- $n_1 \times n_2$ sized top right block in A_1.

- $(i,i)^{th}$ block is $I_{n_{d+2-i}}$ for $2 \le i \le d$.

- $(i, i-1)^{th}$ block is A_{d+2-i} for $2 \leq i \leq d$.

- all other entries are 0.

□

A.2 Missing proofs from Section 2

Proof of Theorem 3.9. Let $C \in \mathbb{F}\langle X\rangle^{d\times d}$ be a full and right monic linear matrix. Suppose Equation 2 holds for some invertible scalar matrices S, S'. Then we can write

$$SCS' = \begin{pmatrix} A & 0 \\ D & B \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ D & I \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ 0 & B \end{pmatrix}.$$

Since C is right monic and S, S' are invertible scalar matrices the linear matrix $SCS' = \begin{pmatrix} A & 0 \\ D & B \end{pmatrix}$ is also full and right monic. Writing it as

$$\begin{pmatrix} A & 0 \\ D & B \end{pmatrix} = \begin{pmatrix} A_0 & 0 \\ D_0 & B_0 \end{pmatrix} + \sum_{i=1}^{n} \begin{pmatrix} A_i & 0 \\ D_i & B_i \end{pmatrix} \cdot x_i,$$

it means the matrix

$$\left[\begin{array}{cc|cc|c|cc} A_1 & 0 & A_2 & 0 & & A_n & 0 \\ D_1 & B_1 & D_2 & B_2 & \dots & D_n & B_n \end{array}\right]$$

is full row rank. With suitable row operations applied to the above we can see that both $[A_1 A_2 \dots A_n]$ and $[B_1 B_2 \dots B_n]$ are full row rank. Therefore, both A and B are full right monic matrices hence they are nonunits by Lemma 3.2. Hence $A \oplus I$ and $B \oplus I$ are both non-units which implies that the factorization of SCS' is nontrivial and hence C is not an atom.

Conversely, suppose C is not an atom and $C = F \cdot G$ is a nontrivial factorization. That means both F and G are full and non-units. As C is a linear matrix, applying [Coh06, Lemma 5.8.7] we can assume that both F and G are linear matrices. Now, since F is a full linear matrix, by Theorem 3.3 (and Remark 3.4) there are a scalar invertible matrix S_1 and polynomial matrix U_1, which is a unit, such that $S_1 F U_1 = A \oplus I$ such that A is *left* monic. Therefore, we have

$$S_1 C = S_1 F U U^{-1} G = \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} G_1' & G_3' \\ G_2' & G_4' \end{pmatrix} = \begin{pmatrix} AG_1' & AG_3' \\ G_2' & G_4' \end{pmatrix}.$$

As $S_1 C$ is a linear matrix and A is a left monic linear matrix we can assume that G_1' and G_3' are scalar matrices. Since $S_1 C$ is full rank, it forces the matrix $[G_1' G_3']$ to be full row rank (say r, where A is $r \times r$). Therefore, there is an invertible scalar matrix S' such that $[G_1' G_3'] S' = [I_r 0]$. Putting it together, we get the factorization

$$SCS' = \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} \cdot \begin{pmatrix} I_r & 0 \\ G_2'' & G_4'' \end{pmatrix} = \begin{pmatrix} A & 0 \\ G_2'' & G_4'' \end{pmatrix}$$

as claimed by the theorem. □

A.3 Proof of Lemma 5.1

We present a self-contained proof of Lemma 5.1 of [HKV20].

Definition A.2. *Let $U, V \subseteq \mathbb{F}^D$ be subspaces of $\mathbb{F}^D$ and $d = \dim U$. Fix a basis $u_1, u_2, \ldots, u_\ell \in \mathbb{F}^D$ for $U \cap V$ and extend it to a basis $u_1, u_2, \ldots, u_\ell, u_{\ell+1}, \ldots, u_d$ for U. Further, let $u_1, u_2, ..., u_D$ be a basis for $\mathbb{F}^D$ obtained by extending the above basis for U. Then $U \backslash V$ is defined as span$(u_{\ell+1}, u_{\ell+2}, \ldots, u_d)$, i.e.*

$$U \setminus V = \{ \sum_{i=\ell+1}^{d} \alpha_i u_i | \alpha_i \in \mathbb{F} \text{ for } \ell < i \leq d\}$$

Clearly $\dim U \setminus V = \dim U - \dim U \cap V$. Notice that although the subspace $U \setminus V$ is basis dependent, the number $\dim U \setminus V$ is independent of the construction of $U \setminus V$.

Definition A.3. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_d\}$ be a collection of subspaces of $\mathbb{F}^D$. For each $i \in [d]$ define $\hat{U}_i^{(\mathcal{U})} = U_i \setminus (\sum_{k \neq i} U_k)$ as above with respect to fixed bases for the subspaces.*

We first prove a technical lemma, essentially using the inclusion-exclusion principle.

Lemma A.4. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_d\}$ be a collection of subspaces of $\mathbb{F}^D$ for $d \geq 1$. Then*

$$\sum_{i=1}^{d} \left[\dim U_i + \dim \hat{U}_i^{(\mathcal{U})}\right] \quad \geq \quad 2 \quad \cdot \quad \dim \sum_{i=1}^{d} U_i.$$

Proof. The proof will be by induction on d. The base case, $d = 1$, is obvious. Suppose it is is true for all $t < d$. I.e. for any subspace collection $\mathcal{V} = \{V_1, V_2, \ldots, V_t\}$ we have

$$\sum_{i=1}^{t} \left[\dim V_i + \dim \hat{V}_i^{(\mathcal{V})}\right] \quad \geq \quad 2 \quad \cdot \quad \dim \sum_{i=1}^{t} V_i.$$

Letting $V_i = U_i$ for $1 \leq i \leq d-2$ and $V_{d-1} = U_{d-1} + U_d$ in the above, we have

$$\sum_{i=1}^{d-1} \left[\dim V_i + \dim \hat{V}_i^{(\mathcal{V})}\right] \quad \geq \quad 2 \quad \cdot \quad \dim \sum_{i=1}^{d-1} V_i = 2 \cdot \dim \sum_{i=1}^{d} U_i.$$

For the induction we need to show that $\sum_{i=1}^{d-1}(\dim V_i + \dim \hat{V}_i^{(\mathcal{V})}) \leq \sum_{i=1}^{d}(\dim U_i + \dim \hat{U}_i^{(\mathcal{U})})$. Now,

$$\sum_{i=1}^{d-1} \ (\dim V_i + \dim \hat{V}_i^{(\mathcal{V})})$$

is

$$
\begin{aligned}
&= \dim V_{d-1} + \dim \hat{V}_{d-1}^{(\mathcal{V})} + \sum_{i=1}^{d-2} \left[\dim U_i + \dim(U_i \setminus (U_{d-1} + U_d + \sum_{k \neq i, k < d-1} U_k)) \right] \\
&= \dim V_{d-1} + \dim \hat{V}_{d-1}^{(\mathcal{V})} + \sum_{i=1}^{d-2} \left[\dim U_i + \dim(U_i \setminus \sum_{k \neq i, k \leq d} U_k) \right] \\
&= \dim V_{d-1} + \dim \hat{V}_{d-1}^{(\mathcal{V})} + \sum_{i=1}^{d-2} \left[\dim U_i + \dim \hat{U}_i^{(\mathcal{U})} \right] \\
&= \dim U_{d-1} + \dim U_d - dim(U_{d-1} \cap U_d) + \dim \hat{V}_{d-1}^{(\mathcal{V})} + \sum_{i=1}^{d-2} \left[\dim U_i + \dim \hat{U}_i^{(\mathcal{U})} \right] \\
&= \left[\sum_{i=1}^{d} \dim U_i \right] + \left[\sum_{i=1}^{d-2} \dim \hat{U}_i^{(\mathcal{U})} \right] + \dim \hat{V}_{d-1}^{(\mathcal{V})} - \dim(U_{d-1} \cap U_d).
\end{aligned}
$$

Hence, to complete the proof it suffices to show the following claim.

Claim A.5.

$$\dim \hat{V}_{d-1}^{(\mathcal{V})} \leq \dim \hat{U}_{d-1}^{(\mathcal{U})} + \dim \hat{U}_d^{(\mathcal{U})} + \dim(U_{d-1} \cap U_d)$$

Proof of Claim. Let $T = U_1 + U_2 + \ldots + U_{d-2}$. Let D, D_1, D_2, and D_3 denote dimensions of $T + U_{d-1} + U_d, U_{d-1}, U_d$, and T respectively.

We have

$$
\begin{aligned}
\dim \hat{V}_{d-1}^{(\mathcal{V})} &= \dim(U_{d-1} + U_d) - \dim((U_{d-1} + U_d) \cap T) \\
&= \dim(U_{d-1} + U_d) - \dim(U_{d-1} + U_d) - \dim(T) + \dim(U_{d-1} + U_d + T) \\
&= D - D_3
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
\dim \hat{U}_{d-1}^{(\mathcal{U})} &= \dim(U_{d-1}) - \dim(U_{d-1} \cap (T + U_d)) \\
&= D_1 + \dim(T + U_{d-1} + U_d) - \dim(U_{d-1}) - \dim(T + U_d) \\
&= D_1 + D - D_1 - \dim(T) - \dim(U_d) + \dim(T \cap U_d) \\
&= D - D_3 - D_2 + \dim(T \cap U_d).
\end{aligned}
$$

Likewise, we also have

$$\dim(\hat{U}_d^{(\mathcal{U})}) = D - D_3 - D_1 + \dim(T \cap U_{d-1}).$$

It is clear that the claim is equivalent to

$$D \geq D_1 + D_2 + D_3 - \dim(T \cap U_d) - \dim(T \cap U_{d-1}) - \dim(U_{d-1} \cap U_d)$$

which follows immediately from the Inclusion-Exclusion Principle. □

□

Now we will present a complete proof for Lemma 5.1 from [HKV20] where the proof is sketchy.

Proof of Lemma 5.1

Let $L = A_0 + \sum_{i=1}^{n} A_i x_i$ Where $A_i \in \mathbb{F}_q^{d\times d}$ for $i \in [n]$. So, $L' = A_0 \otimes I_\ell + \sum_{i=1}^{n} A_i \otimes Y_i$. From standard properties of the Kronecker product of matrices, there are a row permutation matrix R and a column permutation matrix C such that $L'' = RL'C = I_\ell \otimes A_0 + \sum_{i=1}^{n} Y_i \otimes A_i$. So $L'' = I_\ell \otimes A_0 + \sum_{i=1}^{n} \sum_{1\le j,k\le \ell} (E_{j,k} \otimes A_i)\ y_{i,j,k}$, where $E_{j,k}$ is a a matrix with $(j,k)^{th}$ entry one and rest all entries equal to zero.

We have $GL'H = \left(\begin{array}{c|c} A' & 0 \\ \hline D' & B' \end{array}\right)$ Where A' is $d' \times d'$ linear matrix for $d' > 0$, B' is $d'' \times d''$ linear matrix with $d' + d'' = d\ell$. Hence, $GR^{-1}L''C^{-1}H = \left(\begin{array}{c|c} A' & 0 \\ \hline D' & B' \end{array}\right)$. Let $GR^{-1} = P_0$ and $C^{-1}H = Q_0$. Let $[P_1 P_2 \ldots P_\ell]$ be the (full row rank) matrix obtained by picking the top d' rows of P_0 where each P_i is $d' \times d$ scalar matrix. Similarly let $[Q_1^T Q_2^T \ldots Q_\ell^T]^T$ be the (full column rank) matrix obtained by picking the rightmost d'' columns of Q_0 where each Q_i is $d \times d''$ scalar matrix. Clearly,

$$[P_1 P_2 \ldots P_\ell] L'' [Q_1^T Q_2^T \ldots Q_\ell^T]^T = 0,$$

which implies,

$$[P_1 P_2 \ldots P_\ell] \left[I_\ell \otimes A_0 + \sum_{i=1}^{n} \sum_{1\le j,k\le \ell} (E_{j,k} \otimes A_i)\ y_{i,j,k} \right] [Q_1^T Q_2^T \ldots Q_\ell^T]^T = 0.$$

Equating the coefficients of each $y_{i,j,k}$ to zero we get the following.

$$\sum_{i=1}^{\ell} P_i A_0 Q_i = 0. \tag{11}$$

$$P_j A_i Q_k = 0 \text{ for each } i > 0 \text{ and } 1 \le j,k \le \ell. \tag{12}$$

For each $i \in [\ell]$ the matrix P_i is a linear transformation from $\mathbb{F}^d$ to $\mathbb{F}^{d'}$. Let $U_i = \text{Range}(P_i) = \{P_i u | u \in \mathbb{F}^d\}$ for each i, and $\mathcal{U} = \{U_1, U_2, \ldots, U_\ell\}$. Let $T_i = \sum_{j\ne i} U_j$ for $i \in [\ell]$. Clearly, $U_1 + U_2 + \ldots + U_\ell = \mathbb{F}_q^{d'}$ as $[P_1 P_2 \ldots P_\ell]$ is a full row rank matrix. For $i \in [\ell]$, let $\hat{P}_i$ be a linear transformation from $\mathbb{F}^{d'}$ to $\mathbb{F}^{d'}$ defined as follows. Fix a basis $u_{i,1}, u_{i,2}, \ldots, u_{i,r_i}$ of the subspace $U_i \cap T_i$. Extend it to a basis $u_{i,1}, u_{i,2}, \ldots, u_{i,r_i}, u_{i,r_i+1}, \ldots, u_{i,k_i}$, $k_i \ge r$, for U_i. Further, extend this basis of U_i to a complete basis $u_{i,1}, u_{i,2}, \ldots, u_{i,d'}$, for $\mathbb{F}^{d'}$, where $d' \ge k_i$. For any vector $u = \sum_{j=1}^{d'} \alpha_j u_{i,j}$ in $\mathbb{F}^{d'}$ let $\hat{P}_i(u) = \sum_{j=r+1}^{k} \alpha_j u_{i,j}$. So, $\hat{P}_i(u)$ is the vector obtained by projecting to the subspace $U_i \setminus T_i$ (which is defined w.r.t. the above basis). Hence, $\hat{P}_i(u_{i,t}) = u_{i,t}$ for $r_i < t \le k_i$ and $\hat{P}_i(u_{i,t}) = 0$ otherwise. This defines a $d' \times d'$ matrix for each $\hat{P}_i$ for $i \in [\ell]$, which we also refer to as $\hat{P}_i$ by abuse of notation. From the Definition A.3, it follows that $\text{Range}(\hat{P}_i) = \hat{U}_i^{(\mathcal{U})}$, so $\text{rank}(P_i) = \dim \hat{U}_i^{(\mathcal{U})}$. Clearly, $\text{rank}(\hat{P}_i P_i) = \text{rank}(\hat{P}_i)$ for $i \in [\ell]$. Now, by Lemma A.4 applied to the collection $\mathcal{U} = \{U_1, U_2, \ldots, U_\ell\}$ we get

$$\sum_{i=1}^{\ell} \left[\text{rank}\, P_i \ + \ \text{rank}\, \hat{P}_i \right] \ \ge \ 2 \cdot \ \dim \sum_{i=1}^{\ell} \text{Range}(P_i) = 2d'.$$

Similarly, each $Q_i : \mathbb{F}^{d''} \to \mathbb{F}^d$ is a linear map. We can define the corresponding linear maps $\hat{Q}_i : \mathbb{F}^{d''} \to \mathbb{F}^{d''}$ and associated $d'' \times d''$ sized matrices and we will have $\operatorname{rank} Q_i\hat{Q}_i = \operatorname{rank} \hat{Q}_i$ for each i. Applying the above argument we will get

$$\sum_{i=1}^{\ell} \left[\operatorname{rank} Q_i \ + \ \operatorname{rank} \hat{Q}_i\right] \ \geq \ 2 \cdot \ \dim \sum_{i=1}^{\ell} \operatorname{Range}(Q_i) = 2d''.$$

Adding the two inequalities yields

$$\sum_{i=1}^{\ell} \left(\operatorname{rank} \hat{P}_i \ + \ \operatorname{rank} Q_i\right) \ + \left(\operatorname{rank} P_i \ + \ \operatorname{rank} \hat{Q}_i\right) \ \geq \ 2 \cdot \ (d' + d'') = 2d\ell. \tag{13}$$

From the Equation 13 we would like to prove the following Claim.

Claim A.6. *There exist index $i \in [\ell]$ such that $\operatorname{rank} \hat{P}_i \ + \ \operatorname{rank} Q_i \geq d$ and $\operatorname{rank} \hat{P}_i, \operatorname{rank} Q_i > 0$ or $\operatorname{rank} P_i \ + \ \operatorname{rank} \hat{Q}_i \geq d$ and $\operatorname{rank} P_i, \operatorname{rank} \hat{Q}_i > 0$.*

First we complete the proof of the Lemma 5.1 assuming the Claim A.6. Without loss of generality, let index $i = 1$ satisfies the Claim A.6 and further, let $\operatorname{rank} \hat{P}_1 + \operatorname{rank} Q_1 \geq d$ with $\operatorname{rank} \hat{P}_1, \operatorname{rank} Q_1 > 0$ (other case handled similarly).

Equation 11 implies that $\operatorname{Range}(P_1A_0Q_1) \subseteq T_1$, also clearly, $\operatorname{Range}(P_1A_0Q_1) \subseteq \operatorname{Range}(P_1) = U_1$. Which implies $\operatorname{Range}(P_1A_0Q_1) \subseteq U_1 \cap T_1$. Hence $\hat{P}_1P_1A_0Q_1 = 0$. Equation 12 implies that, $\hat{P}_1P_jA_iQ_k = 0$ for all $i \geq 1$ and $1 \leq j, k \leq \ell$. So we get $\hat{P}_1P_1LQ_1 = 0$. Now $\operatorname{rank}(\hat{P}_1P_1) = \operatorname{rank}(\hat{P}_1) \geq 1$, $\operatorname{rank}(Q_1) \geq 1$ and $\operatorname{rank}(\hat{P}_1P_1) + \operatorname{rank}(Q_1) \geq d$. It follows that there exist $0 < e' \leq \operatorname{rank}(\hat{P}_1P_1)$ and $0 < e'' \leq \operatorname{rank}(Q_1)$ with $e' + e'' = d$. By choosing e' linearly independent rows of $\hat{P}_1P_1$ and e'' linearly independent columns of Q_1 we obtain full row rank matrix $U' \in \mathbb{F}_q^{e' \times d}$ and a full column rank matrix $V' \in \mathbb{F}_q^{d \times e''}$ respectively. Now we extend U' to a $d \times d$ matrix U by adding any $d - e'$ linearly independent rows such that U is invertible. Similarly we extend V' to a $d \times d$ matrix V by adding any $d - e''$ linearly independent columns such that V is invertible. We clearly have $ULV = \left(\begin{array}{c|c} A & 0 \\ \hline D & B \end{array}\right)$ for some linear matrices A, D, B such that $A \in \mathbb{F}\langle X \rangle^{e' \times e'}$ and $B \in \mathbb{F}\langle X \rangle^{e'' \times e''}$ with $0 < e', e''$ and $e' + e'' = d$ as required. This completes the proof of Lemma 5.1.

Proof of Claim A.6.

Each P_i has d columns and each Q_i has d rows. Thus, $\operatorname{rank} P_i \leq d$ and $\operatorname{rank} Q_i \leq d$. Also, $\operatorname{rank} \hat{P}_i \leq \operatorname{rank} P_i$ and $\operatorname{rank} \hat{Q}_i \leq \operatorname{rank} Q_i$. Hence, $\operatorname{rank} \hat{P}_i + \operatorname{rank} Q_i \leq 2d$ and $\operatorname{rank} P_i + \operatorname{rank} \hat{Q}_i \leq 2d$ for each i.

It follows from Inequality 13 that if there is an i for which either $\operatorname{rank} \hat{P}_i + \operatorname{rank} Q_i < d$ or $\operatorname{rank} P_i + \operatorname{rank} \hat{Q}_i < d$ then there must be an index j such that either $\operatorname{rank} \hat{P}_j + \operatorname{rank} Q_j > d$ or $\operatorname{rank} P_j + \operatorname{rank} \hat{Q}_j > d$. Two cases arise:

1. for all $j \in [\ell]$, $\operatorname{rank} \hat{P}_j + \operatorname{rank} Q_j = d$ and $\operatorname{rank} P_j + \operatorname{rank} \hat{Q}_j = d$.

2. there is $j \in [\ell]$ with either $\operatorname{rank} \hat{P}_j + \operatorname{rank} Q_j > d$ or $\operatorname{rank} P_j + \operatorname{rank} \hat{Q}_j > d$.

Suppose the first case occurs. It has the following two subcases.

(a) for all $j \in [\ell]$, $\operatorname{rank} \hat{P}_j = 0$ or $\operatorname{rank} Q_j = 0$ and $\operatorname{rank} P_j = 0$ or $\operatorname{rank} \hat{Q}_j = 0$.

(b) there is $j \in [\ell]$ such that $\operatorname{rank} \hat{P}_j, \operatorname{rank} Q_j > 0$ or $\operatorname{rank} P_j, \operatorname{rank} \hat{Q}_j > 0$

First, consider Case 1(a). Note that $\operatorname{rank} \hat{P}_j = 0$ implies $\operatorname{rank} Q_j = d$. And $\operatorname{rank} Q_j = 0$ implies $\operatorname{rank} \hat{P}_j = d$, which implies $\operatorname{rank} P_j = d$. Thus, either $\operatorname{rank} P_j = d$ or $\operatorname{rank} Q_j = d$ for every j. Moreover, Case 1(a) also implies $\operatorname{rank} P_j, \operatorname{rank} Q_j \in \{0, d\}$ for each j.

Now as $[P_1 P_2 \ldots P_\ell]$ has full row rank and $[Q_1^T Q_2^T \ \ldots Q_\ell^T]^T$ has full column rank, Case 1(a) implies that there are indices $j, k \in [\ell]$ such that P_j and Q_k are both rank d matrices. As P_j is full column rank matrix, there is a $d \times d'$ matrix P'_j such that $P'_j P_j = I_d$. Similarly, there is a $d'' \times d$ matrix Q'_k such that $Q_k Q'_k = I_d$. Now from Equation 12 we know that $P_j A_i Q_k = 0$ for all i, $1 \leq i \leq n$. Hence $P'_j P_j A_i Q_k Q'_k = 0$ for all i, $1 \leq i \leq n$. Consequently, $A_i = 0$ for $1 \leq i \leq n$ which is a contradiction to the lemma statement. Hence case 1(a) cannot occur.

If case 1(b) or 2 holds then for some index $j \in [\ell]$ either $\operatorname{rank} \hat{P}_j + \operatorname{rank} Q_j \geq d$ with $\operatorname{rank} \hat{P}_j$, $\operatorname{rank} Q_j > 0$ or $\operatorname{rank} P_j + \operatorname{rank} \hat{Q}_j \geq d$ with $\operatorname{rank} P_j$, $\operatorname{rank} \hat{Q}_j > 0$. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il