# On the Complexity of "Superdetermined" Minrank Instances

Javier Verbel[1], John Baena[1], Daniel Cabarcas[1], Ray Perlner[2], and Daniel Smith-Tone[2,3]

[1] Universidad Nacional de Colombia, Colombia
{javerbelh,jbbaena,dcabarc}@unal.edu.co
[2] National Institute of Standards and Technology, USA
ray.perlner@nist.gov
[3] University of Louisville, USA
daniel-c.smith@louisville.edu

**Abstract.** The Minrank (MR) problem is a computational problem closely related to attacks on code- and multivariate-based schemes. In this paper we revisit the so-called Kipnis-Shamir (KS) approach to this problem. We extend previous complexity analysis by exposing non-trivial syzygies through the analysis of the Jacobian of the resulting system, with respect to a group of variables. We focus on a particular set of instances that yield a very overdetermined system which we refer to as "superdetermined". We provide a tighter complexity estimate for such instances and discuss its implications for the key recovery attack on some multivariate schemes. For example, in HFE the speedup is roughly a square root.

**Keywords:** Minrank problem · Multivariate · Cryptanalysis · HFE.

## 1 Introduction

The post-quantum cryptography initiative emerges in response to Shor's factoring algorithm [25], to identify quantum hard problems to support cryptographic constructions. This major endeavor has come to a climax in recent years with NIST's ongoing post-quantum "competition."

One central problem is the Minrank problem (MR). Its decisional version is, given $m$ matrices $M_1, M_2, \ldots, M_m \in \mathcal{M}_{n\times n}(\mathbb{F})$, and a target rank $r$, to determine whether there exists a linear combination of these matrices with rank at most $r$. It is important both in multivariate public key cryptography [4, 21, 23, 26], and in code-based cryptography [19]. Buss et al. first introduced the MR problem and proved it NP-complete [3]. In the context of cryptography, MR first appeared as part of an attack against the HFE cryptosystem by Kipnis and Shamir [21]. There are three well known approaches to solve the Minrank problem, namely, Kipnis-Shamir (KS), minors [16], and linear algebra search [20].

The complexity of the minors approach and of the linear algebra search are well understood. However, the complexity of the KS approach is not so clear. In [16], the authors assume that a generic instance of KS yields a "generic enough" bilinear system (see Section 2.2), and under this assumption, using the results in [17], they estimate the solving degree at $d = \min(m, r(n-r)) + 1$ and so the complexity of KS as $O\left(\binom{m+r(n-r)+d-1}{d}^{\omega}\right)$, with $2 \leq \omega \leq 3$. Experimental evidence shows that this estimate wildly overestimates the true solving degree [4].

An important technical contribution of this paper is to show that the assumption that the KS system is generic bilinear is unrealistic. The system is indeed bilinear in two sets of variables that we call the linear variables and the kernel variables. However, we expose the structure in the system beyond bilinearity. It can be seen as having a sequence of generic bilinear blocks. Such a structure implies that the Jacobians with respect to the linear and kernel variables have particular forms. This is important because left kernel vectors of the Jacobian are syzygies. Thus, through the Jacobian with respect to the linear variables, we show how to construct some non-trivial syzygies, yielding non-trivial degree falls.

The degree of these syzygies suggests a crucial distinction between two cases of the MR problem. If $m > nr$, these syzygies typically have degree $r + 2$. However, if $m < nr$, we can construct a number of lower degree syzygies. We refer to instances where $m < nr$ as "superdetermined." This property applies to several multivariate schemes and it is in contrast to instances of the minrank problem that occur in other contexts, like rank-based cryptography.

The exposed structure of the KS system leads to tighter complexity estimates for the superdetermined MR instances. Using the XL algorithm and multiplying only by monomials from kernel variables, the complexity of solving uniformly random instances of KS systems is $O\left((r\kappa)^{(d_{\mathrm{KS}}+2)\omega}\right)$, where $2 < \omega \leq 3$,

$$d_{\mathrm{KS}} = \min\left\{ d \mid \left[ \binom{r}{d} n > \binom{r}{d+1} m \right],\ 1 \leq d \leq r-1 \right\},$$

and $\kappa$ can be chosen so that $\max\left\{\frac{m}{n-r}, d_{\mathrm{KS}}+1\right\} \leq \kappa \leq n-r$. This is much lower than previous estimates. For example, if $m = n$ and $r < \sqrt{n}$, then $d_{\mathrm{KS}} \leq r/2+1$, and we can choose $\kappa = \sqrt{n}$, so that, $r\kappa < n$, and hence, our complexity estimate is $O(n^{(r/2)\omega})$, compared to $O(n^{r\omega})$ from previous estimates, c.f. [1].

Since a key recovery attack based on the MR problem can be performed on several multivariate schemes, we revise the complexity of the KS method for some multivariate schemes such as HFE, ZHFE, and HFEv-. The speedup in each case depends on the ratio of $m$ to $n$ and on the relation between $n$ and $r$. For example, in HFE the speedup is roughly a square root.

The paper is organized as follows. In Section 2 we present background material. In Section 3 we describe the structure of the KS system. In Section 4 we provide the main results of the paper, including the construction of the syzygies. In Section 5 we revise the complexity of the KS method based on the new findings. In Section 6 we provide some experimental data supporting the theoretical results. Finally, in Section 7 we discuss the implications of our findings for some multivariate schemes.

## 2 Preliminaries

### 2.1 Solving Multivariate Systems of Equations

Let $\mathbb{F}$ be a finite field, and consider the polynomial system $F = \mathbf{a}$, where $\mathbf{a}$ is an element in the image of $F = (f_1, \ldots, f_m) : \mathbb{F}^n \to \mathbb{F}^m$, and the $f_i$'s are multivariate polynomials in the unknowns $x_1, \ldots, x_n$, with coefficients in $\mathbb{F}$. The first effective algorithm for solving nonlinear multivariate systems did so by computing a Gröbner basis for the ideal generated by the equations [2]. Since the late 90s, however, far superior algorithms have been developed such as Faugère's F4 and F5 [14, 15], and the XL family of algorithms inspired by [22] and popularized in [6, 21].

The XL algorithm simply computes an echelon form of the Macaulay matrix in degree $d$ of $F$ for high enough $d$. This is the matrix whose columns represent the monomials of degree at most $d$ with rows representing each polynomial of degree less than or equal to $d$ of the $tf_i$, where $t$ is a monomial. It can be shown that there exists some degree $d$ such that this echelon form is a Gröbner basis of the ideal. The algorithms F4 and F5 are similar but more efficient in removing redundant rows a priori. The first fall degree $d_{\mathrm{ff}}$ is the smallest degree such that some polynomial drops in degree after echelonizing the Macaulay matrix. It is widely accepted that $d_{\mathrm{ff}}$ is a good parameter to measure the complexity of solving polynomial systems [10–13]. The reason is that often the solving degree is not much larger than the first fall degree. Our experiments confirm this is the case for KS systems, as shown below in Section 6.

### 2.2 Bilinear Systems

Consider two tuples of unknows $\mathbf{x} = (x_1, x_2, \ldots, x_{n_1})$ and $\mathbf{y} = (y_1, y_2, \ldots, y_{n_2})$. Let $\mathbb{F}[\mathbf{x}, \mathbf{y}]$ denote the ring of multivariate polynomials with coefficients in $\mathbb{F}$ and variables $x_1, x_2, \ldots, x_{n_1}, y_1, y_2, \ldots, y_{n_2}$. A *bilinear polynomial* $f(\mathbf{x}, \mathbf{y})$ is a quadratic polynomial in $\mathbb{F}[\mathbf{x}, \mathbf{y}]$ which is affine in each set of variables. If we can write $f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^\top A \mathbf{y}$ for some $A \in \mathcal{M}_{n_1 \times n_2}(\mathbb{F})$, we say $f$ is a *homogeneous bilinear polynomial.*

Throughout this work, sequences of polynomials are considered as column vectors of polynomials. Suppose $f_i \in \mathbb{F}[\mathbf{x}, \mathbf{y}]$ is a bilinear polynomial for $i = 1, 2, \ldots, m$. The sequence $\mathcal{F} = (f_1, f_2, \ldots, f_m)$ is called a *bilinear sequence* on $\mathbb{F}[\mathbf{x}, \mathbf{y}]$. In the particular case when each $f_i$ is also homogeneous, we say $\mathcal{F}$ is a *homogeneous bilinear sequence* on $\mathbb{F}[\mathbf{x}, \mathbf{y}]$.

**Definition 1.** *Given a sequence $\mathcal{F} = (f_1, f_2, \ldots, f_m)$ on $\mathbb{F}[\boldsymbol{x}, \boldsymbol{y}]$, the Jacobian of $\mathcal{F}$ with respect to the set $\boldsymbol{x}$, is given by $\mathsf{jac}_{\boldsymbol{x}}(\mathcal{F}) = \left[\frac{\partial f_i}{\partial x_j}\right]_{1 \le i \le m, 1 \le j \le n_1}$. Likewise we define $\mathsf{jac}_{\boldsymbol{y}}(\mathcal{F})$, the Jacobian of $\mathcal{F}$ with respect to the set $\boldsymbol{y}$.*

When $\mathcal{F}$ is a bilinear sequence, each entry of $\mathsf{jac}_{\mathbf{x}}(\mathcal{F})$ (*resp.* $\mathsf{jac}_{\mathbf{y}}(\mathcal{F})$) is a linear form in the $\mathbf{y}$ (*resp.* $\mathbf{x}$) variables. A *syzygy* of $\mathcal{F}$ is a sequence $\mathcal{G} = (g_1, g_2, \ldots, g_m) \in \mathbb{F}[\mathbf{x}, \mathbf{y}]^m$ such that $\sum_{i=1}^m g_i f_i = 0$.

**Proposition 1.** *Let $\mathcal{F} = (f_1, f_2, \ldots, f_m)$ be a homogeneous bilinear sequence on $\mathbb{F}[\boldsymbol{x}, \boldsymbol{y}]$. Suppose $\mathcal{G} = (g_1, g_2, \ldots, g_m)$ is a sequence on $\mathbb{F}[\boldsymbol{y}]$, then*

$$\sum_{i=1}^{m} g_i f_i = 0 \tag{1}$$

*if and only if $\mathcal{G}^\top$ belongs to the left-kernel of $\mathsf{jac}_{\boldsymbol{x}}(\mathcal{F})$.*

**Proposition 2.** *Suppose that $\mathcal{F}$ is a homogeneous bilinear sequence on $\mathbb{F}[\boldsymbol{x}, \boldsymbol{y}]$. If a sequence $\mathcal{G}$ on $\mathcal{F}[\boldsymbol{x}]$ is a syzygy of $\mathcal{F}$, then $\mathcal{G}$ is not a trivial syzygy* [4].

### 2.3 Minrank Problem

One complexity theoretic problem related to the hardness of solving certain multivariate systems is the MinRank (MR) problem. The computational MR problem can be stated as follows.

**Problem 1 (MinRank (Search Version))** *Given a positive integer $r$, and $m$ matrices $M_1, M_2, \ldots, M_m \in \mathcal{M}_{s \times t}(\mathbb{F})$, find $x_1, x_2, \ldots, x_m \in \mathbb{F}$ such that $\mathsf{Rank}\left(\sum_{\ell=1}^m x_\ell M_\ell\right) \leq r$.*

The decisional version of the MR problem is known to be $NP$-complete even if we insist that $s = t = n$, see [3], and seems difficult in practice. There are three main methods in the literature for solving the MR problem, Kipnis-Shamir modeling, minors modeling [1] and linear algebra search [20].

Introduced by Kipnis and Shamir in [21], the KS method stands on the following fact: if $p < n$, $M \in \mathcal{M}_{n \times n}(\mathbb{F})$, $K' \in \mathcal{M}_{n \times p}(\mathbb{F})$ has rank $p$ and $MK' = \mathbf{0}$, then $\mathsf{Rank}(M) \leq n - p$. Thus, the MR problem can be solved by finding $x_1, \ldots, x_m, k_1, \ldots, k_{r(n-r)} \in \mathbb{F}$ such that

$$\left(\sum_{\ell=1}^{m} x_\ell M_\ell\right) \begin{bmatrix} I_{n-r} \\ K^\top \end{bmatrix} = \mathbf{0}, \tag{2}$$

where

$$K = \begin{bmatrix} k_1 & k_2 & \cdots & k_r \\ \vdots & \vdots & \ddots & \vdots \\ k_{r(n-r-1)+1} & k_{r(n-r-1)+2} & \cdots & k_{r(n-r)} \end{bmatrix} \tag{3}$$

and $I_{n-r}$ is the identity matrix of size $n - r$. If there exists a matrix in the span of the $M_i$'s such that its column space is generated by its $r$ rightmost columns, then the system (2) has a solution. This system is bilinear in the

[4] For a formal definition of a trivial syzygy see [13].

variables $\mathbf{x} = (x_1, \ldots, x_m)$ and the unknown entries $\mathbf{k} = (k_1, k_2, \ldots, k_{r(n-r)})$ of $K$. Throughout this work we will refer to the first group as the *linear variables*, and to the second one as the *kernel variables*. Therefore, (2) can be seen as a bilinear system of $n(n-r)$ equations in $m + r(n-r)$ variables. The complexity of solving this kind of system has been studied by Faugère et al. in [16, 17]. They upper bound the complexity of KS modeling by that of solving a generic bilinear system with $n(n-r)$ equations, where one group of variables has $m$ elements and the other has $r(n-r)$ elements. In that case, the given bound is

$$O\left(\binom{m + r(n-r) + \min(m, r(n-r)) + 1}{\min(m, r(n-r)) + 1}^{\omega}\right),$$

where $2 \leq \omega \leq 3$ is the linear algebra constant.

## 3 The Structure of the KS System

In this section we describe the basic structure of the system given in (2). First, in Section 3.1, we show that such a matrix equation can be seen as a set of $n-r$ chained bilinear subsystems, where each subsystem has generic quadratic part and linear part involving only the $\mathbf{x}$ varibles. Then, in Section 3.2, we describe the Jacobian of the system with respect to the kernel variables. We show that if a KS instance $\mathcal{F}$ is chosen uniformly at random, then, with high probability, the syzygies of $\mathcal{F}$ that only involve linear variables have degree at least $r$.

### 3.1 KS and Bilinear System

Set $M = \sum_{\ell=1}^{m} x_\ell M_\ell$, where each $M_\ell \in \mathcal{M}_{n\times n}(\mathbb{F})$. Let $M_{(i,j)}$ and $M_{\ell,(i,j)}$ denote the $(i,j)$ entry of the matrices $M$ and $M_\ell$, respectively. Under this setting, the $(i,j)$ entry of $M \cdot \begin{bmatrix} I_{n-r} \; K \end{bmatrix}^\top$ is given by the polynomial

$$f_j^{(i)} = \sum_{t=1}^{r} M_{(i,n-r+t)} \cdot k_{(j-1)r+t} + M_{(i,j)} \in \mathbb{F}[\mathbf{x}, \mathbf{k}], \tag{4}$$

where $1 \leq i \leq n$, $1 \leq j \leq n-r$, and $k_{(t-1)r+j}$ is located at the $(t,j)$ entry of $K$. The sequence $\mathcal{F}$ formed by the $n(n-r)$ polynomials given in (4) is called a KS *sequence* with parameters $n, m, r$. The sequence $\mathcal{F}$ is bilinear in the sets of unknowns $\mathbf{x} = (x_1, \ldots, x_m)$ and $\mathbf{k} = (k_1, k_2, \ldots, k_{r(n-r)})$. Recall that we refer to $\mathbf{x}$ and $\mathbf{k}$ as the linear and kernel variables, respectively. We also denote as $\mathsf{KS}(n, m, r)$ the set of KS sequences with parameters $n, m, r$. A KS *system* is a system of the form $\mathcal{F} = \mathbf{0}$, where $\mathcal{F}$ is a KS sequence.

Even though a sequence $\mathcal{F} \in \mathsf{KS}(n, m, r)$ is bilinear, it is not a generic one. Notice that each polynomial $f_j^{(i)}$ only involves $r$ variables of the set $\mathbf{k}$ and its linear part only contains variables from $\mathbf{x}$. For $t = 1, 2, \ldots, n-r$, let $\mathcal{F}_t$ denote the subsequence of $\mathcal{F}$ given by $\mathcal{F}_t = (f_t^{(1)}, f_t^{(2)}, \ldots, f_t^{(n)})$. This sequence is bilinear in the set of variables $\mathbf{x}$ and $\mathbf{k}^{(t)} = (k_{(t-1)r+1}, k_{(t-1)r+2}, \ldots, k_{tr})$. Notice that the coefficient of every quadratic monomial in $\mathcal{F}$ can be any element in $\mathbb{F}$. On the contrary, the linear part of the polynomials in $\mathcal{F}$ only contains linear variables, so the coefficients of the kernel variables in the linear part of the polynomials in $\mathcal{F}$ are forced to be zero. Thus, a sequence $\mathcal{F} \in \mathsf{KS}(n, m, r)$ can be seen as $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_{n-r})$, where the quadratic part of $\mathcal{F}_t$ is generic (no restrictions at all) and the linear part is a generic linear form in the linear variables.

### 3.2 Jacobian with Respect to Kernel Variables

Let us begin by showing the structure of the Jacobian with respect to the kernel variables for KS sequences. Here we set $\mathcal{F}_t = (f_t^{(1)}, f_t^{(2)}, \ldots, f_t^{(n)})$, $f_t^{(i)}$, $M$ as in Section 3.1 and $\otimes$ will denote the Kronecker product.

**Lemma 1.** *Suppose* $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_{n-r}) \in \mathsf{KS}(n, m, r)$*. Let* $I_{n-r}$ *be the identity matrix of size* $n - r$*. Then for* $j \in \{1, 2, \ldots, n - r\}$*, we have that* $\mathsf{jac}_{\mathbf{k}^{(1)}}(\mathcal{F}_1) = \mathsf{jac}_{\mathbf{k}^{(j)}}(\mathcal{F}_j)$*, and* $\mathsf{jac}_{\mathbf{k}}(\mathcal{F}) = I_{n-r} \otimes \mathsf{jac}_{\mathbf{k}^{(1)}}(\mathcal{F}_1)$*.*

*Remark 1.* Assume $\mathcal{F}$ denotes the quadratic part of a sequence in $\mathsf{KS}(n, m, r)$. By Proposition 1 and Lemma 1, $\mathcal{F}$ has a degree $d$ syzygy $\mathcal{G} \in \mathbb{F}[\mathbf{x}]^{n(n-r)}$ if and only if $\mathcal{F}_1$ has a degree $d$ syzygy $\mathcal{G}_1 \in \mathbb{F}[\mathbf{x}]^n$. Explicitly, each syzygy $\mathcal{G}$ of $\mathcal{F}$ can be written as $(\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_{n-r})$, where each $\mathcal{G}_j$ is a syzygy of $\mathcal{F}_1$.

Now suppose that the matrices $M_1, M_2, \ldots, M_m \in \mathcal{M}_{n\times n}(\mathbb{F})$ are chosen uniformly at random. Each entry of the matrix $M = \sum_{i=1}^{m} x_i M_i$ is a uniformly chosen linear form in the linear variables. In particular, its $r$ rightmost columns are the Jacobian of a uniformly chosen homogeneous bilinear sequence. This is a bilinear sequence with $m + r$ variables and $n$ equations. Assume $\mathcal{F}_1$ is underdetermined ($n < m + r$) and that $r < n$. If Conjecture 1 in Section 4.2 of [17] is true, with high probability the left kernel of $\mathsf{jac}_{\mathbf{k}^{(1)}}(\mathcal{F}_1)$ is generated by

$$\text{Ker} := \left\{ \left( \mathsf{minor}(\tilde{M}_T, 1), -\mathsf{minor}(\tilde{M}_T, 2), \ldots, (-1)^n \mathsf{minor}(\tilde{M}_T, n) \right) \mid T \in \mathcal{T} \right\},$$

where $\tilde{M}_T = \begin{bmatrix} \tilde{M} \; T \end{bmatrix}$ with $\tilde{M} = \mathsf{jac}_{\mathbf{k}^{(1)}}(\mathcal{F}_1)$, $\mathsf{minor}(\tilde{M}_T, j)$ denotes the determinant of $\tilde{M}_T$ after removing its $j$-th row, and $\mathcal{T}$ is the set of $n \times (n - r - 1)$ matrices such that

- each column of $T$ has exactly a 1 and the rest of its entries are 0,
- each row of $T$ has at most a 1 and the remaining entries 0,
- if $i_j$ denotes the number of the row containing the only 1 of the $j-$th column and if $j < t$, then $i_j < i_t$.

Notice that Ker has $\binom{n}{r+1}$ elements. Each of them has exactly $r + 1$ nonzero components and every nonzero component is a different minor of $\tilde{M}$ of size $r$. Since each entry of $\tilde{M}$ is a homogeneous linear polynomial in the $\mathbf{x}$ variables, $\text{Ker} \subset \mathbb{F}[\mathbf{x}]_r^n$ [5]. Consequently, if Conjecture 1 in [17] is true, then we do not expect to find an element in Ker having degree less than $r$.

[5] $\mathbb{F}[\mathbf{x}]_r$ denotes the vector space formed by the degree $d$ homogeneous polynomials in $\mathbb{F}[\mathbf{x}]$.

The following theorem summarizes these results. We include a proof for completeness.

**Theorem 1.** *Suppose Conjecture 1 in [17] is true, $\mathcal{F} \in \mathsf{KS}(n, m, r)$ is chosen uniformly at random. Then, using only monomials in the linear variables in the XL algorithm, with high probability the first fall degree is $r + 2$.*

*Proof.* By Proposition 1 and Lemma 1, we only need to prove that with high probability there is not $\mathcal{G}_1 \in \mathbb{F}[\mathbf{x}]^n$ having degree less than $r$ and $\mathcal{G}_1^\top \mathsf{jac}_{\mathbf{k}^{(1)}}(\mathcal{F}_1) = 0$. Assuming that Conjecture 1 in [17] is true, if $\mathcal{F} \in \mathsf{KS}(n, m, r)$ is chosen uniformly at random, then with high probability Ker generates the left kernel of $\mathsf{jac}_{\mathbf{k}^{(1)}}(\mathcal{F}_1)$. Therefore, with high probability, each syzygy of $\mathcal{F}_1$, only involving $\mathbf{x}$ variables, has degree at least $r + 2$.

## 4 Jacobian with Respect to the Linear Variables

The Jacobian of a KS system with respect to the linear variables deserves a section of its own. We provide a detailed description here and describe non-trivial syzygies that arise from this structure. We show that if $m < nr$ non-trivial syzygies of the quadratic part of $\mathcal{F}$ can be explicitly built, having degree less than $r$. In Section 4.1 we use a small example to motivate the notation thereafter. We then provide a general construction in Section 4.2 for square matrices, and further generalize in Section 4.3 to non-square matrices and fewer kernel vectors.

Let us consider an MR instance with $m$ matrices $M_1, \dots, M_m \in \mathcal{M}_{n\times n}(\mathbb{F})$ and target rank $r$. Recall that the KS system is given by $\left(\sum_{i=1}^m x_i M_i\right) K' = \mathbf{0}$, where the kernel matrix is $K' = \begin{bmatrix} I_{n-r} \ K \end{bmatrix}^\top$ with $K$ as in (3). The Jacobian with respect to the linear variables of the corresponding sequence $\mathcal{F} \in \mathsf{KS}(n, m, r)$ can be written as $\mathsf{jac}_{\mathbf{x}}(\mathcal{F}) = (I_n \otimes K)\, L + C$, where $C \in \mathcal{M}_{n(n-r)\times m}(\mathbb{F})$, $L$ is an $nr \times m$ matrix whose rows $L_1, L_2, \dots, L_{rn}$ are given by the expression $L_{r(i-1)+j} = \begin{bmatrix} M_{1,(i,n-r+j)} \ M_{2,(i,n-r+j)} \ \dots \ M_{m,(i,n-r+j)} \end{bmatrix}$ for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, r$.

The approach we follow here to find syzygies of a KS sequence $\mathcal{F}$ is the same used in Section 3.2, i.e., we find elements in the left-kernel of the Jacobian of the quadratic part of $\mathcal{F}$, but now with respect to the linear variables. By Proposition 1, those kernel elements correspond to syzygies of the quadratic part of $\mathcal{F}$. In order to simplify the notation, throughout this section, we assume that the sequence $\mathcal{F} \in \mathsf{KS}(n, m, r)$ only contains its quadratic part. Under such assumption, the Jacobian with respect to the $\mathbf{x}$ variables of the sequence $\mathcal{F}$ is given by $\mathsf{jac}_{\mathbf{x}}(\mathcal{F}) = (I_n \otimes K)\, L$.

From now on $\ker_l(B)$ will denote the left-kernel of a matrix $B$. A naïve way to find elements in $\ker_l(\mathsf{jac}_{\mathbf{x}}(\mathcal{F}))$ is by finding elements in $\ker_l(I_n \otimes K)$. Those kernel elements have degree $r$ and can be built analogously as we did in Section 3.2 for $\mathsf{jac}_{\mathbf{k}}(\mathcal{F})$. A natural question is whether it is possible to get degree falls at a smaller degree from $\mathsf{jac}_{\mathbf{x}}(\mathcal{F})$. The answer to this question is affirmative under certain conditions. In Section 4.2 we show how it can be done for general sequences in $\mathsf{KS}(n, m, r)$, with $m < nr$. We now show a small example to introduce the general process.

### 4.1 A Small Example $n = 4, m = 4$ and $r = 2$

Here we show how to build degree one syzygies of a sequence $\mathcal{F} \in \mathsf{KS}(4,4,2)$, which involve only the kernel variables. In this particular case, the Jacobian $\mathsf{jac}_{\mathbf{x}}(\mathcal{F})$ is given by

$$\mathsf{jac}_{\mathbf{x}}(\mathcal{F}) = \left( \begin{bmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{bmatrix} \otimes \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} \right) \cdot L.$$

Suppose $(a_1, a_2, \dots, a_8) \in \ker_l(L)$, $\mathbf{v}_0 = (a_2, a_4, a_6, a_8) \otimes (-k_3, k_1)$ and $\mathbf{v}_1 = (a_1, a_3, a_5, a_7) \otimes (k_4, -k_2)$. Then $\mathbf{v}_0\,(I_4 \otimes K) = \det(K)\,[(0,1) \otimes (a_2, a_4, a_6, a_8)]$ and $\mathbf{v}_1\,(I_4 \otimes K) = \det(K)\,[(1,0) \otimes (a_1, a_3, a_5, a_7)]$. Thus

$$(\mathbf{v}_0 + \mathbf{v}_1)\mathsf{jac}_{\mathbf{x}}(\mathcal{F}) = \det(K)(a_1, a_2, \dots, a_8) \cdot L = \mathbf{0},$$

and $\mathbf{v}_0 + \mathbf{v}_1$ is a syzygy of $\mathcal{F}$ of degree one.

We just saw how to build a syzygy of degree one, namely $\mathbf{v}_0 + \mathbf{v}_1$. If we consider $\mathbf{b} \in \ker_l(L)$, linearly independent with $\mathbf{a} = (a_1, \dots, a_8)$, and repeat the process described above, then we end up with a degree one syzygy $\tilde{\mathbf{v}}_0 + \tilde{\mathbf{v}}_1$ linearly independent with $\mathbf{v}_0 + \mathbf{v}_1$.Indeed, notice that $\mathbf{v}_0$ and $\mathbf{v}_1$ do not share monomials componentwise, and similarly neither do $\tilde{\mathbf{v}}_0$ and $\tilde{\mathbf{v}}_1$. Thus, we have that

$$x(\mathbf{v}_0 + \mathbf{v}_1) + y(\tilde{\mathbf{v}}_0 + \tilde{\mathbf{v}}_1) = \mathbf{0} \text{ if and only if } x\mathbf{v}_0 + y\tilde{\mathbf{v}}_0 = 0 \text{ and } x\mathbf{v}_1 + y\tilde{\mathbf{v}}_1 = 0,$$

and the right-hand implication happens if and only if $x\mathbf{a} + y\mathbf{b} = 0$. Consequently, $\mathbf{v}_1 + \mathbf{v}_2$ and $\tilde{\mathbf{v}}_1 + \tilde{\mathbf{v}}_2$ are linearly independent if and only if $\mathbf{a}$ and $\mathbf{b}$ are.

As a consequence of the previous analysis, we can build a set of linearly independent degree one syzygies in $\mathcal{F}[\mathbf{k}]$ with as many elements as the dimension of $\ker_l(L)$. Thus, if $\mathcal{F} \in \mathsf{KS}(4,4,2)$ is chosen uniformly at random, so are the matrices $M_1, M_2, M_3, M_4$ used to build $\mathcal{F}$. In particular, $L$ is a uniformly random matrix of size $8 \times 4$, so with high probability, the left kernel of $L$ has dimension 4, which is the maximum number of linearly independent syzygies of degree one that we can construct as above.

### 4.2 First Degree Fall for Any $n, m, r$, with $m < rn$.

We now describe a general method to find syzygies of degree $d_{\mathrm{KS}}$ of a sequence $\mathcal{F} \in \mathsf{KS}(n, m, r)$, where $d_{\mathrm{KS}}$ is some particular integer less than $r$.

Let us begin by introducing the notation using throughout this section. Here $k_1, k_2, \dots, k_{r(n-r)}$ are the entries of the matrix $K$, as shown in (3). Given two vectors of integers $\mathbf{l} = (l_1 + 1, \dots, l_\ell + 1)$ and $\mathbf{c} = (c_1, \dots, c_\ell)$, where $1 \leq c_i \leq r$ and $1 \leq l_i + 1 \leq n - r$ for $i = 1, \dots, r$, we define $K_{\mathbf{l},\mathbf{c}}$ as

$$K_{\mathbf{l},\mathbf{c}} = \begin{vmatrix} k_{rl_1+c_1} & k_{rl_1+c_2} & \cdots & k_{rl_1+c_\ell} \\ k_{rl_2+c_1} & k_{rl_2+c_2} & \cdots & k_{rl_2+c_\ell} \\ \vdots & \vdots & \ddots & \vdots \\ k_{rl_\ell+c_1} & k_{rl_\ell+c_2} & \cdots & k_{rl_\ell+c_\ell} \end{vmatrix}.$$

Let $d$ be an integer such that $0 < d+1 \leq \min\{n-r, r\}$. We set $\mathcal{C}_d = \{(t_1, \ldots, t_d) \mid t_k \in \mathbb{N},\ 1 \leq t_k < t_{k+1} \leq r\}$ and $\mathcal{R}_d = \{(j_1+1, \ldots, j_{d+1}+1) \mid j_k \in \mathbb{N},\ 0 \leq j_k < j_{k+1} \leq n-r-1\}$. The sets $\mathcal{C}_d$, $\mathcal{R}_d$ represent, respectively, all possible sets of $d$ columns and sets of $d+1$ rows of $K$ in ascending order. For any $\mathbf{t} = (t_1, \ldots, t_d) \in \mathcal{C}_d$ and $\mathbf{j} = (j_1+1, \ldots, j_{d+1}+1) \in \mathcal{R}_d$, let $\mathbf{j}_s$ denote the vector resulting from removing the $s$-th entry from $\mathbf{j}$, and $V_{\mathbf{j}}^{\mathbf{t}}$ denote the column vector in $\mathbb{F}[\mathbf{k}]^{n-r}$ which has values $(-1)^1 K_{\mathbf{j}_1,\mathbf{t}}, \ldots, (-1)^{d+1} K_{\mathbf{j}_{d+1},\mathbf{t}}$ in positions numbered by $j_1+1, \ldots, j_{d+1}+1$, respectively, and zeros elsewhere. More precisely, $V_{\mathbf{j}}^{\mathbf{t}} = \sum_{i=1}^{d+1} (-1)^i K_{\mathbf{j}_i,\mathbf{t}}\ \mathbf{e}_{j_i+1}$, where $\mathbf{e}_i$ denotes the $i$-th standard basis vector of $\mathbb{F}^{n-r}$. Notice that if $\hat{\mathbf{e}}_1, \hat{\mathbf{e}}_2, \ldots, \hat{\mathbf{e}}_r$ are the canonical vectors in $\mathbb{F}^r$, then it can be shown that

$$\left(V_{\mathbf{j}}^{\mathbf{t}}\right)^{\top} K = \sum_{s \in \mathcal{S}_{\mathbf{t}}} K_{\mathbf{j},(\mathbf{t},s)}\ \hat{\mathbf{e}}_s^{\top}, \tag{5}$$

where $\mathcal{S}_{\mathbf{t}} := \{s \in \mathbb{N} \mid 1 \leq s \leq r,\ s \text{ is not an entry of } \mathbf{t}\}$. For $\mathbf{t} \in \mathcal{C}_d$ and $\mathbf{j} \in \mathcal{R}_d$, let $E_{\mathbf{j},\mathbf{t}}$ be the subspace of $\mathbb{F}[\mathbf{k}]_d^{n(n-r)}$ spanned by $\left\{\tilde{\mathbf{e}}_1 \otimes V_{\mathbf{j}}^{\mathbf{t}}, \ldots, \tilde{\mathbf{e}}_n \otimes V_{\mathbf{j}}^{\mathbf{t}}\right\}$, where $\tilde{\mathbf{e}}_i$ denotes the $i$-th standard vector basis of $\mathbb{F}^n$. It can be shown that if $\mathbf{j} \neq \mathbf{j}'$ or $\mathbf{t} \neq \mathbf{t}'$ then $E_{\mathbf{j},\mathbf{t}} \cap E_{\mathbf{j}',\mathbf{t}'} = \{\mathbf{0}\}$.

**Lemma 2.** *Suppose $\boldsymbol{j}$, $\boldsymbol{j}' \in \mathcal{R}_d$, and $\boldsymbol{t}, \boldsymbol{t}' \in \mathcal{C}_d$. If $\boldsymbol{j} \neq \boldsymbol{j}'$ or $\boldsymbol{t} \neq \boldsymbol{t}'$ then $E_{\boldsymbol{j},\boldsymbol{t}} \cap E_{\boldsymbol{j}',\boldsymbol{t}'} = \{\boldsymbol{0}\}$.*

*Proof.* First of all, note that if $\mathbf{e}'_\ell$ denotes the $\ell$-th vector in the standard basis of $\mathbb{F}^{n(n-r)}$, then the following set is a basis for the $\mathbb{F}$-vector space $\mathbb{F}[\mathbf{k}]_d^{n(n-r)}$

$$\mathcal{B} = \{\mathrm{m}\ \mathbf{e}'_\ell \mid \mathrm{m} \in \mathbb{F}[\mathbf{k}]_d \text{ a monomial and } \ell = 1, \ldots, n(n-r)\}.$$

In particular, any basis element $\tilde{\mathbf{e}}_s \otimes V_{\mathbf{j}}^{\mathbf{t}}$ of $E_{\mathbf{j},\mathbf{t}}$ can be seen as an $\mathbb{F}$-linear combination of elements in $\mathcal{B}$. Notice that if $\mathbf{j} = (j_1+1, j_2+2, \ldots, j_{d+1}+2)$, by definition we have $V_{\mathbf{j}}^{\mathbf{t}} = \sum_{i=1}^{d+1} (-1)^i K_{\mathbf{j}_i,\mathbf{t}}\ \mathbf{e}_{j_i+1}$, hence

$$\begin{aligned} \tilde{\mathbf{e}}_s \otimes V_{\mathbf{j}}^{\mathbf{t}} &= \sum_{i=1}^{d+1} (-1)^i K_{\mathbf{j}_i,\mathbf{t}}\ \left(\tilde{\mathbf{e}}_s \otimes \mathbf{e}_{j_i+1}\right) \\ &= \sum_{i=1}^{d+1} (-1)^i K_{\mathbf{j}_i,\mathbf{t}}\ \mathbf{e}'_{(s-1)(n-r)+j_i+1}. \end{aligned}$$

Let us set

$$\mathcal{B}_{\mathbf{j},\mathbf{t}}^s := \{\mathrm{m}\ \mathbf{e}'_{(s-1)(n-r)+j_i+1} \mid \mathrm{m} \text{ is a monomial of } K_{\mathbf{j}_i,\mathbf{t}} \text{ and } i = 1, \ldots, d+1\},$$

i.e., $\mathcal{B}_{\mathbf{j},\mathbf{t}}^s$ contains the basis vectors from $\mathcal{B}$ whose $\mathbb{F}$-linear combination produces $\tilde{\mathbf{e}}_s \otimes V_{\mathbf{j}}^{\mathbf{t}}$. For this reason

$$E_{\mathbf{j},\mathbf{t}} \subset \mathsf{Span}_{\mathbb{F}} \left\{ \bigcup_{s=1}^{n} \mathcal{B}_{\mathbf{j},\mathbf{t}}^s \right\}.$$

Finally we show that in any case, $\mathbf{t} \neq \mathbf{t}'$ or $\mathbf{j} \neq \mathbf{j}'$, we have

$$\left\{ \bigcup_{s=1}^{n} \mathcal{B}^{s}_{\mathbf{j},\mathbf{t}} \right\} \cap \left\{ \bigcup_{s=1}^{n} \mathcal{B}^{s}_{\mathbf{j}',\mathbf{t}'} \right\} = \emptyset. \tag{6}$$

In the first case, there is some integer $t$ which is a component of $\mathbf{t}$, but not a component of $\mathbf{t}'$. Because of the structure of $K$, it is clear that each monomial in the polynomial $K_{\mathbf{j}_i,\mathbf{t}}$ has a factor of the form $k_{2j+t}$. Since $t$ does not appear as a component in $\mathbf{t}'$, no monomial in $K_{\mathbf{j}'_i,\mathbf{t}'}$has a factor of the form $k_{2j'+t}$. Consequently, equation (6) holds.

In the other case, $\mathbf{j} \neq \mathbf{j}$’, there is at least one index $i$ for which $j_i + 1$ is a component of $\mathbf{j}$ and it is not a component of $\mathbf{j}'$. So each element in $\bigcup_{s=1}^{n} \mathcal{B}^{s}_{\mathbf{j},\mathbf{t}}$ has as a factor either a monomial of the form $\mathrm{m}k_{2j_i+t}$, for some $t$, or the vector $\mathbf{e}'_{(s-1)(n-r)+j_i+1}$ for some $s$, and no element with such factors belongs to $\bigcup_{s=1}^{n} \mathcal{B}^{s}_{\mathbf{j}',t'}$. Consequently, equation (6) holds.

Fix $\mathbf{t} = (t_1, \dots, t_d) \in \mathcal{C}_d$ and $s \in \mathcal{S}_{\mathbf{t}}$. Let $i$ be the only integer satisfying $t_i < s < t_{i+1}$ and $\sigma$ the permutation that sends $(t_1, \dots, t_i, s, t_{i+1}, \dots, t_d)$ to $(t_1, \dots, t_d, s)$. For each $s \in \{1, 2, \dots, r\}$ define $\mathsf{sgn}(\mathbf{t}, s)$ to be $\mathsf{sgn}(\sigma)$ if $s \in \mathcal{S}_{\mathbf{t}}$ and zero otherwise[6]. Notice that, if $\tilde{\mathbf{t}} := (t_1, \dots, t_i, s, t_{i+1}, \dots, t_d)$, then $K_{\mathbf{j},\tilde{\mathbf{t}}}$ is a minor of $K$ of size $d+1$. Moreover, for any $\mathbf{j} \in \mathcal{R}_d$ it holds that $\mathsf{sgn}(\mathbf{t}, s) \cdot K_{\mathbf{j},(\mathbf{t},s)}$ is equal to $K_{\mathbf{j},\tilde{\mathbf{t}}}$ if $s \in \mathcal{S}_{\mathbf{t}}$, or equal to 0 otherwise.

We now address the main theorem of this section. For some fixed $\mathbf{j} \in \mathcal{R}_d$ we establish a one-to-one correspondence between elements in the left-kernel of certain matrix $\tilde{B}_{\mathbf{j}}$ and certain elements in the left-kernel of $(I_n \otimes K)L$, where $K$ is as in (3) and $L \in \mathcal{M}_{rn \times m}(\mathbb{F})$, see Theorem 2 below.

Before stating the mentioned theorem, let us describe the matrix $\tilde{B}_{\mathbf{j}}$ for a given $\mathbf{j} \in \mathcal{R}_d$. This is a column block matrix of size $\binom{r}{d}n \times \binom{r}{d+1}m$, with blocks $B_{\mathbf{t}_1}, B_{\mathbf{t}_2}, \dots, B_{\mathbf{t}_\ell}$, where $\ell = \binom{r}{d}$ and each $B_{\mathbf{t}_i}$ is an $n \times \binom{r}{d+1}m$ matrix over $\mathbb{F}$. To define each block $B_{\mathbf{t}_i}$, we introduce one more notation. We denote by $\mathrm{MINORS}_{d+1}(K(\mathbf{j}))$ the set of minors of size $d+1$ of the matrix $K(\mathbf{j})$, which is simply the matrix whose rows are the rows of $K$ with indexes in $\mathbf{j}$. Let us fix an enumeration on that set of minors, say $\mathrm{MINORS}_{d+1}(K(\mathbf{j})) = \{\mathsf{m}_1, \mathsf{m}_2, \dots, \mathsf{m}_{\ell'}\}$, with $\ell' = \binom{r}{d+1}$. For each $\mathbf{t}_i \in \mathcal{C}_d$, the block $B_{\mathbf{t}_i}$ is also a block matrix of the form $B_{\mathbf{t}_i} = \left[B_{\mathbf{t}_i,1}\; B_{\mathbf{t}_i,2} \cdots B_{\mathbf{t}_i,\ell'}\right]$, where $B_{\mathbf{t}_i,k}$ is a matrix of size $n \times m$, for $k = 1, 2, \dots, \ell'$. A particular $B_{\mathbf{t}_i,k}$ is given by $B_{\mathbf{t}_i,k} := \mathsf{sgn}(\mathbf{t}_i, s) \left( L_s^\top \; L_{r+s}^\top \cdots L_{r(n-1)+s}^\top \right)^\top$, where $L_1, L_2, \dots, L_{rn}$ are the rows of $L$, if $s$ is the unique integer such that $\mathsf{sgn}(\mathbf{t}_i, s) K_{\mathbf{j},(\mathbf{t}_i,s)} = \mathsf{m}_k$. Otherwise, $B_{\mathbf{t}_i,k}$ is the $n \times m$ zero matrix.

From now on we set $\mathcal{C}_d = \{\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_\ell\}$.

**Theorem 2.** *Let $\mathbb{F}$ be a field, $L \in \mathcal{M}_{rn \times m}(\mathbb{F})$, $d$ be an integer such that $0 < d + 1 \leq \min\{n - r, r\}$, $\boldsymbol{j} \in \mathcal{R}_d$, and $\boldsymbol{a} \in \mathbb{F}^{\ell n}$. If $\boldsymbol{a}_{t_1}, \boldsymbol{a}_{t_2}, \dots, \boldsymbol{a}_{t_\ell} \in \mathbb{F}^n$ are*

[6] $\mathsf{sgn}(\sigma)$ denotes the sign of the permutation $\sigma$.

*such that $\boldsymbol{a} = (\boldsymbol{a}_{\boldsymbol{t}_1}, \boldsymbol{a}_{\boldsymbol{t}_2}, \dots, \boldsymbol{a}_{\boldsymbol{t}_\ell})$, then $\boldsymbol{a} \in \ker_l(\tilde{B}_{\boldsymbol{j}})$ if and only if $\sum_{k=1}^{\ell} \boldsymbol{a}_{\boldsymbol{t}_k} \otimes V_{\boldsymbol{j}}^{\boldsymbol{t}_k} \in \ker_l\left[(I_n \otimes K)L\right]$. Moreover, assume $A = \{\boldsymbol{a}^1, \dots, \boldsymbol{a}^h\}$ for some $1 \leq h \leq n|\mathcal{C}_d|$ and $\boldsymbol{a}^i := (\boldsymbol{a}^i_{\boldsymbol{t}_1}, \dots, \boldsymbol{a}^i_{\boldsymbol{t}_\ell})$, with $\boldsymbol{a}^i_{\boldsymbol{t}_k} \in \mathbb{F}^n$ for $i = 1, \dots, h$. Then, $\tilde{\mathcal{S}}_{\boldsymbol{j}} := \left\{\sum_{k=1}^{\ell} \boldsymbol{a}^i_{\boldsymbol{t}_k} \otimes V_{\boldsymbol{j}}^{\boldsymbol{t}_k} \mid i = 1, \dots, h\right\}$ is $\mathbb{F}$-linearly independent if and only if $A$ is $\mathbb{F}$-linearly independent.*

*Proof.* For each $\mathbf{t} \in \mathcal{C}_d$, we set $\mathbf{a}_\mathbf{t} = (a_{1,\mathbf{t}}, \dots, a_{n,\mathbf{t}}) \in \mathbb{F}^n$. So that $\mathbf{a}_\mathbf{t} = \sum_{i=1}^{n} a_{i,\mathbf{t}}\ \tilde{\mathbf{e}}_i$, where $\tilde{\mathbf{e}}_i$ denotes the $i$-th element in the standard basis of $\mathbb{F}^n$. By equation (5) we have

$$\begin{aligned}
\sum_{\mathbf{t}\in\mathcal{C}_d} \left(\mathbf{a}_\mathbf{t} \otimes V_\mathbf{j}^\mathbf{t}\right)^\top (I_n \otimes K)\, L &= \sum_{\mathbf{t}\in\mathcal{C}_d} \left(\mathbf{a}_\mathbf{t}^\top \otimes (V_\mathbf{j}^\mathbf{t})^\top K\right) L \\
&= \sum_{\mathbf{t}\in\mathcal{C}_d} \left(\mathbf{a}_\mathbf{t}^\top \otimes \left[\sum_{s\in\mathcal{S}_\mathbf{t}} K_{\mathbf{j},(\mathbf{t},s)}\ \hat{\mathbf{e}}_s^\top\right]\right) L \\
&= \sum_{\mathbf{t}\in\mathcal{C}_d} \left[\sum_{s\in\mathcal{S}_\mathbf{t}} K_{\mathbf{j},(\mathbf{t},s)} \sum_{i=1}^{n} a_{i\mathbf{t}}\, (\tilde{\mathbf{e}}_i \otimes \hat{\mathbf{e}}_s)^\top L\right] \\
&= \sum_{\substack{\mathbf{t}\in\mathcal{C}_d\\ s\in\mathcal{S}_\mathbf{t}}} \mathsf{sgn}(\mathbf{t}, s) \left[\mathbf{a}_\mathbf{t}^\top \begin{pmatrix} L_s \\ L_{r+s} \\ \vdots \\ L_{r(n-1)+s} \end{pmatrix}\right] \mathsf{sgn}(\mathbf{t}, s) K_{\mathbf{j},(\mathbf{t},s)},
\end{aligned}$$

where $L_1, \dots, L_{rn}$ are the rows of $L$. For each $\mathsf{m}_k \in \mathrm{MINORS}_{d+1}(K(\mathbf{j}))$ let $(\tilde{\mathbf{t}}_1, s_1), (\tilde{\mathbf{t}}_2, s_2), \dots, (\tilde{\mathbf{t}}_e, s_e)$ be the sequence of $(d+1)$-tuples with $\tilde{\mathbf{t}}_i \in \mathcal{C}_d$ and $s_i \in \mathcal{S}_{\tilde{\mathbf{t}}_i}$ such that $\mathsf{sgn}(\tilde{\mathbf{t}}_j, s_j) K_{(\tilde{\mathbf{t}}_j, s_j)} = \mathsf{m}_k$ for $j = 1, 2, \dots, e$. Thus

$$\begin{aligned}
\sum_{\mathbf{t}\in\mathcal{C}_d} \left(\mathbf{a}_\mathbf{t} \otimes V_\mathbf{j}^\mathbf{t}\right)^\top (I_n \otimes K)\, L &= \sum_{k=1}^{\ell'} \left[\sum_{j=1}^{e} \mathsf{sgn}(\tilde{\mathbf{t}}_j, s_j) \mathbf{a}_{\tilde{\mathbf{t}}_j}^\top \begin{pmatrix} L_{s_j} \\ L_{r+s_j} \\ \vdots \\ L_{r(n-1)+s_j} \end{pmatrix}\right] \mathsf{m}_k \\
&= \sum_{k=1}^{\ell'} \left(\sum_{\mathbf{t}\in\mathcal{C}_d} \mathbf{a}_\mathbf{t} \mathbf{B}_{\mathbf{t},k}\right) \mathsf{m}_k.
\end{aligned}$$

The last equality holds because any $\mathbf{t} \in \mathcal{C}_d - \{\tilde{\mathbf{t}}_1, \tilde{\mathbf{t}}_2, \dots, \tilde{\mathbf{t}}_e\}$ leads to a $\mathbf{B}_{\mathbf{t},k} = \mathbf{0}$. Since the minors of $K$ do not have monomials in common, $\mathbf{a} = (\mathbf{a}_{\mathbf{t}_1}, \dots, \mathbf{a}_{\mathbf{t}_\ell})$ is a vector such that $\sum_{i=1}^{\ell} \left(\mathbf{a}_{\mathbf{t}_i} \otimes V_\mathbf{j}^{\mathbf{t}_i}\right)^\top \in \ker_l\left[(I_n \otimes K)L\right]$ if and only if we have that $\sum_{i=1}^{\ell} \mathbf{a}_{\mathbf{t}_i} \mathbf{B}_{\mathbf{t}_i,k} = \mathbf{0}$ for each minor $\mathsf{m}_k$. Equivalently, if and only if

$$\sum_{i=1}^{\ell} \mathbf{a}_{\mathbf{t}_i} \left[\mathbf{B}_{\mathbf{t}_i,1}\ \mathbf{B}_{\mathbf{t}_i,2} \cdots\ \mathbf{B}_{\mathbf{t}_i,\ell'}\right] = \mathbf{0}, \quad \sum_{i=1}^{\ell} \mathbf{a}_{\mathbf{t}_i} \mathbf{B}_{\mathbf{t}_i} = \mathbf{0},$$

$$(\mathbf{a}_{\mathbf{t}_1}, \mathbf{a}_{\mathbf{t}_2}, \dots, \mathbf{a}_{\mathbf{t}_\ell}) \left[\mathbf{B}_{\mathbf{t}_1}^\top\ \mathbf{B}_{\mathbf{t}_2}^\top \cdots\ \mathbf{B}_{\mathbf{t}_\ell}^\top\right]^\top = \mathbf{0}, \quad \text{and } \mathbf{a}\tilde{B}_\mathbf{j} = \mathbf{0}.$$

Now we prove the last statement of the theorem. Suppose $\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^h \in \mathbb{F}^{\ell n}$ are linearly independent and $\mathbf{a}^i = (\mathbf{a}^i_{\mathbf{t}_1}, \mathbf{a}^i_{\mathbf{t}_2}, \dots, \mathbf{a}^i_{\mathbf{t}_\ell})$, for each $i = 1, 2, \dots, h$. Assume $x_1, x_2, \dots, x_h \in \mathbb{F}$ are such that $\sum_{i=1}^h x_i \left( \sum_{j=1}^{\ell} \mathbf{a}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}}^{\mathbf{t}_j} \right) = \mathbf{0}$. Since each $\mathbf{a}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}}^{\mathbf{t}_j} \in E_{\mathbf{j},\mathbf{t}_j}$, so does every $\sum_{i=1}^h x_i \left( \mathbf{a}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}}^{\mathbf{t}_j} \right)$. By Lemma 2 the previous equation holds if and only if $\sum_{i=1}^h x_i \left( \mathbf{a}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}}^{\mathbf{t}_j} \right) = \mathbf{0}$, for each $j = 1, 2, \dots, \ell$. Equivalently, $\sum_{i=1}^h x_i \mathbf{a}^i_{\mathbf{t}_j} = \mathbf{0}$ for each $j$. That is, $\sum_{i=1}^h x_i \mathbf{a}^i = \mathbf{0}$.

Remember that we are only considering the quadratic part of sequences $\mathcal{F} \in \mathsf{KS}(n, m, r)$, so that $\mathsf{jac}_{\mathbf{x}}(\mathcal{F}) = (I_n \otimes K)\, L$, where $K$ is given in (3). Consequently, the previous theorem shows a way to build syzygies of $\mathcal{F}$ (see Proposition 1). For a fixed $j \in \mathcal{R}_d$, Theorem 2 also says that we can build as many syzygies as the dimension of the left-kernel of the matrix $\tilde{B}_{\mathbf{j}}$. For a matrix $L \in \mathcal{M}_{rn \times m}(\mathbb{F})$ chosen uniformly at random, we conjecture that the probability that $\tilde{B}_{\mathbf{j}}$ is full rank is very high and it depends on the size of $\mathbb{F}$.

*Conjecture 1.* Suppose $\binom{r}{d} n > \binom{r}{d+1} m$, $d + 1 \leq \min\{n - r, r\}$, $m \leq rn$, and $\mathbf{j} \in \mathcal{R}_d$. If $L \in \mathcal{M}_{rn \times m}(\mathbb{F})$ is chosen uniformly at random, then with overwhelming probability in the size of $\mathbb{F}$, the rank of $\tilde{B}_{\mathbf{j}}$ is $\binom{r}{d+1} m$.

We experimentally tested this conjecture for values of $20 \leq n \leq 25$, $n - 3 \leq m \leq 2n$, $6 \leq r \leq 10$ and $|\mathbb{F}| = 13$; and for $8 \leq n \leq 16$, $2 \leq r \leq 8$, $n - 4 \leq m \leq rn$ and $|\mathbb{F}| = 2$. Assuming that Conjecture 1 is true, we have the following corollary.

**Corollary 1.** *Suppose $\binom{r}{d} n > \binom{r}{d+1} m$, $d + 1 \leq \min\{n - r, r\}$, $m < rn$, and $\boldsymbol{j} \in \mathcal{R}_d$. If $\mathcal{F} \in \mathsf{KS}(n, m, r)$ is chosen uniformly at random, and assuming Conjecture 1 holds, then with overwhelming probability, there is a set $\tilde{\mathcal{S}}_{\boldsymbol{j}}$ of $\binom{r}{d} n - \binom{r}{d+1} m$ syzygies of $\mathcal{F}$ of degree $d$. Moreover, $\tilde{\mathcal{S}}_{\boldsymbol{j}}$ is $\mathbb{F}$-linearly independent.*

*Proof.* Suppose $\mathcal{F} \in \mathsf{KS}(n, m, r)$ is chosen uniformly at random. Recall that $\mathsf{jac}_x(\mathcal{F}) = (I_n \otimes K) L$, so $L \in \mathcal{M}_{rn \times m}(\mathbb{F})$ can be seen as chosen uniformly at random as well. Let us set $A = \{\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^h\}$ and define $\tilde{\mathcal{S}}_{\mathbf{j}}$ and $\tilde{B}_{\mathbf{j}}$ as in Theorem 2. By this theorem, $A \subset \ker_l(\tilde{B}_{\mathbf{j}})$ is $\mathbb{F}$-linearly independent if and only if $\tilde{\mathcal{S}}_{\mathbf{j}} \subset \ker_l \left[ (I_n \otimes K) L \right]$ is linearly independent. By Conjecture 1, with overwhelming probability the dimension of $\ker_l(\tilde{B}_{\mathbf{j}})$ is $\binom{r}{d} n - \binom{r}{d+1} m$. Finally, by Proposition 1, each element in $\tilde{\mathcal{S}}_{\mathbf{j}}$ is a syzygy of $\mathcal{F}$.

It can be shown that for different $\mathbf{j}, \mathbf{j}' \in \mathcal{R}_d$, $\tilde{\mathcal{S}}_{\mathbf{j}} \cup \tilde{\mathcal{S}}'_{\mathbf{j}}$ is a linearly independent set of syzygies of $\mathcal{F}$.

**Proposition 3.** *Suppose $\boldsymbol{j}, \boldsymbol{j}'$ $\in \mathcal{R}_d$ are distinct and that $L \in \mathcal{M}_{rn \times m}(\mathbb{F})$. Let $A = \{\boldsymbol{a}^1, \dots, \boldsymbol{a}^{\ell_1}\}$ and $B = \{\boldsymbol{b}^1, \dots, \boldsymbol{b}^{\ell_2}\}$ be two sets not necessarily different, with $\boldsymbol{a}^i = (\boldsymbol{a}^i_{\boldsymbol{t}_1}, \boldsymbol{a}^i_{\boldsymbol{t}_2}, \dots, \boldsymbol{a}^i_{\boldsymbol{t}_{\ell'}})$ and $\boldsymbol{b}^i = (\boldsymbol{b}^i_{\boldsymbol{t}_1}, \boldsymbol{b}^i_{\boldsymbol{t}_2}, \dots, \boldsymbol{b}^i_{\boldsymbol{t}_\ell})$ as described in Theorem 2. If we set*

$$\tilde{\mathcal{S}}_{\boldsymbol{j}} = \left\{ \sum_{j=1}^{\ell} \boldsymbol{a}^i_{\boldsymbol{t}_j} \otimes V_{\boldsymbol{j}}^{\boldsymbol{t}_j} \mid i = 1, \dots, \ell_1 \right\}, \quad \tilde{\mathcal{S}}_{\boldsymbol{j}\,'} = \left\{ \sum_{j=1}^{\ell} \boldsymbol{b}^i_{\boldsymbol{t}_j} \otimes V_{\boldsymbol{j}'}^{\boldsymbol{t}_j} \mid i = 1, \dots, \ell_2 \right\},$$

*then $\mathcal{S}_{\mathbf{j}} \cup \mathcal{S}_{\mathbf{j}'}$ is a set of linearly independent vectors in* $\ker_l\left[(I_n \otimes K)L\right]$ *if and only if $A$ and $B$ are both linearly independent in* $\ker_l(L)$.

*Proof.* By Theorem 2 we have that $A, B \subset \ker_l(\tilde{B}_{\mathbf{j}})$ and are $\mathbb{F}$-linearly independent if and only if $\mathcal{S}_{\mathbf{j}}, \mathcal{S}_{\mathbf{j}\,'} \subset \ker_l\left[(I_n \otimes K)L\right]$ and are both $\mathbb{F}$-linearly independent. Suppose there are $x_1, x_2, \ldots, x_{\ell_1}, y_1, y_2, \ldots, y_{\ell_2} \in \mathbb{F}$ such that

$$\sum_{i=1}^{\ell_1} x_i \left( \sum_{j=1}^{\ell} \mathbf{a}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}}^{\mathbf{t}_j} \right) + \sum_{i=1}^{\ell_2} y_i \left( \sum_{j=1}^{\ell} \mathbf{b}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}'}^{\mathbf{t}_j} \right) = \mathbf{0}, \quad \text{i.e.,}$$

$$\sum_{j=1}^{\ell} \left[ \sum_{i=1}^{\ell_1} x_i \left( \mathbf{a}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}}^{\mathbf{t}_j} \right) + \sum_{i=1}^{\ell_2} y_i \left( \mathbf{b}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}'}^{\mathbf{t}_j} \right) \right] = \mathbf{0}.$$

Notice that each of the $2\ell$ sums in the previous equation belongs to a different $E_{\mathbf{j},\mathbf{t}}$ subspace. By Lemma 2, those subspaces have trivial intersection pairwise. Consequently, last equation holds if and only if each of those sums is zero, that is, for $j = 1, 2, \ldots, \ell$,

$$\sum_{i=1}^{\ell_1} x_i \left( \mathbf{a}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}}^{\mathbf{t}_j} \right) = \mathbf{0} \text{ and } \sum_{i=1}^{\ell_2} y_i \left( \mathbf{b}^i_{\mathbf{t}_j} \otimes V_{\mathbf{j}'}^{\mathbf{t}_j} \right) = \mathbf{0},$$

which is true if and only if

$$\sum_{i=1}^{\ell_1} x_i \mathbf{a}^i = \mathbf{0} \text{ and } \sum_{i=1}^{\ell_2} y_i \mathbf{b}^i = \mathbf{0}.$$

As a consequence and assuming that Conjecture 1 is true, we can calculate a number of degree falls that we know for sure will happen at degree $d+2$, for a particular $d < r$.

**Corollary 2.** *Suppose Conjecture 1 is true, $\binom{r}{d}n > \binom{r}{d+1}m$, $d+1 \leq \min\{n-r, r\}$ and $m < rn$. If $\mathcal{F} \in \mathsf{KS}(n, m, r)$ is chosen uniformly at random, then with overwhelming probability there is a set of*

$$\binom{n-r}{d+1}\left[\binom{r}{d}n - \binom{r}{d+1}m\right]$$

*linearly independent syzygies of $\mathcal{F}$ of degree $d$.*

### 4.3 Analysis for Non-Square MR and $\kappa$ Kernel Vectors

In this part we adapt the analysis performed in Section 4.2 to MR instances with non-square matrices. We also see how the results of that section are affected if we consider a KS system with only $\kappa$ kernel vectors.

Suppose $p, q, m, r, \kappa$ are integers such that $m < rp$ and $\frac{m}{p-r} < \kappa \leq q - r$. We can consider an MR instance with matrices $M_1, M_2, \ldots, M_m \in \mathcal{M}_{p\times q}(\mathbb{F})$ and target rank $r$. When we say that we are considering $\kappa$ kernel vectors in the KS modeling, what we mean is that we are dealing with the system

$$\left(\sum_{i=1}^{m} x_i M_i\right) K'_\kappa = \mathbf{0}_{p\times\kappa}, \tag{7}$$

where $K'_\kappa$ is the matrix consisting of the first $\kappa$ columns of $K'$, that is, $K'_\kappa = \left[\tilde{I}_\kappa\ K_\kappa\right]^\top$, $\tilde{I}_\kappa$ is formed by the first $\kappa$ rows of the identity matrix $I_{q-r}$ and

$$K_\kappa = \begin{bmatrix} k_1 & k_2 & \cdots & k_r \\ k_{r+1} & k_{r+2} & \cdots & k_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ k_{r(\kappa-1)+1} & k_{r(\kappa-1)+2} & \cdots & k_{r\kappa} \end{bmatrix}.$$

Let us set $\mathbf{k} = (k_1, k_2, \ldots, k_{r\kappa})$, and let $\mathsf{KS}_\kappa(p\times q, m, r)$ be the set of all sequences in $\mathbb{F}[\mathbf{x}, \mathbf{k}]$ that are formed by the entries of any matrix that has the shape of the one on the left-hand side of (7). For each $\mathcal{F} \in \mathsf{KS}_\kappa(p\times q, m, r)$ its Jacobian is given by

$$\mathsf{jac}_{\mathbf{x}}(\mathcal{F}) = (I_p \otimes K_\kappa)\, L + C, \tag{8}$$

where $C \in \mathcal{M}_{p\kappa\times m}(\mathbb{F})$, $L$ is an $rp\times m$ matrix with rows $L_1, L_2, \ldots, L_{rp}$ and $L_{r(i-1)+j} = \left[M_{1,(i,p-r+j)}\ M_{2,(i,p-r+j)}\ \ldots\ M_{m,(i,p-r+j)}\right]$ for $i = 1, 2, \ldots, p$ and $j = 1, 2, \ldots, r$.

Let $\mathcal{C}_d$ be like in Section 4.2 and $\mathcal{R}_{\kappa,d} := \{(j_1+1, \ldots, j_{d+1}+1) \mid j_k \in \mathbb{N},\ 0 \le j_k < j_{k+1} \le \kappa-1\}$. Provided an integer $d$, with $0 \le d \le \min\{\kappa-1, r-1\}$, and $\mathbf{j} \in \mathcal{R}_{\kappa,d}$, the matrix $\tilde{B}_{\mathbf{j}}$ is now of size $\binom{r}{d}p \times \binom{r}{d+1}m$. Such a matrix is constructed as in the square MR case, but setting $n = p$. The polynomial vector $V_{\mathbf{j}}^{\mathbf{t}}$ is defined like in the full kernel vector case, with the only difference that now it has length $\kappa$ instead of $q-r$. The proof of the following theorem is analogous to the proof of Theorem 2.

**Theorem 3.** *Let $\mathbb{F}$ be a field, $L \in \mathcal{M}_{rp\times m}(\mathbb{F})$, $d$ be an integer such that $0 < d+1 \le \min\{\kappa, r\}$, $\boldsymbol{j} \in \mathcal{R}_{\kappa,d}$, and $\boldsymbol{a} \in \mathbb{F}^{\ell p}$. If $\boldsymbol{a}_{\mathbf{t}_1}, \boldsymbol{a}_{\mathbf{t}_2}, \ldots, \boldsymbol{a}_{\mathbf{t}_\ell} \in \mathbb{F}^p$ are such that $\boldsymbol{a} = (\boldsymbol{a}_{\mathbf{t}_1}, \boldsymbol{a}_{\mathbf{t}_2}, \ldots, \boldsymbol{a}_{\mathbf{t}_\ell})$, then $\boldsymbol{a} \in \ker_l(\tilde{B}_{\boldsymbol{j}})$ if and only if $\sum_{k=1}^{\ell} \boldsymbol{a}^i_{\mathbf{t}_k} \otimes V_{\boldsymbol{j}}^{\boldsymbol{t}_k} \in \ker_l\left[(I_p \otimes K)L\right]$. Moreover, if $A = \{\boldsymbol{a}^1, \ldots, \boldsymbol{a}^h\}$ for some $1 \le h \le n|\mathcal{C}_d|$ and $\boldsymbol{a}^i := (\boldsymbol{a}^i_{\mathbf{t}_1}, \boldsymbol{a}^i_{\mathbf{t}_2}, \ldots, \boldsymbol{a}^i_{\mathbf{t}_\ell})$, with $\boldsymbol{a}^i_{\mathbf{t}_k} \in \mathbb{F}^p$ for $i = 1, \ldots, h$, then*

$$\tilde{\mathcal{S}}_{\boldsymbol{j}} := \left\{ \sum_{k=1}^{\ell} \boldsymbol{a}^i_{\mathbf{t}_k} \otimes V_{\boldsymbol{j}}^{\boldsymbol{t}_k} \mid i = 1, \ldots, h \right\}$$

*is $\mathbb{F}$- linearly independent if and only if $A$ is $\mathbb{F}$- linearly independent.*

If Conjecture 1 is true, we have the following two corollaries.

**Corollary 3.** *Suppose Conjecture 1 is true, $\binom{r}{d}p > \binom{r}{d+1}m$, $d+1 \le \min\{\kappa, r\}$, $m < rp$, and $\boldsymbol{j} \in \mathcal{R}_{\kappa,d}$. If $\mathcal{F} \in \mathsf{KS}_\kappa(p\times q, m, r)$ is chosen uniformly at random, then with overwhelming probability the rank of $\tilde{B}_{\boldsymbol{j}}$ is $\binom{r}{d+1}m$.*

*Proof.* Given $\mathbf{j} \in \mathcal{R}_{\kappa,d} \subset \mathcal{R}_d$, if Conjecture 1 is true, with high probability the rank of $\tilde{B}_{\mathbf{j}}$ is $\binom{r}{d+1}m$.

**Corollary 4.** *Suppose Conjecture 1 is true, $\binom{r}{d}p > \binom{r}{d+1}m$, $d+1 \leq \min\{\kappa, r\}$, $m < rp$, and $\boldsymbol{j} \in \mathcal{R}_{\kappa,d}$. If $\mathcal{F} \in \mathsf{KS}_\kappa(p \times q, m, r)$ is chosen uniformly at random, then with high probability there is a set $\tilde{\mathcal{S}}_{\boldsymbol{j}}$ of $\binom{r}{d}p - \binom{r}{d+1}m$ syzygies of $\mathcal{F}$ of degree $d$. Moreover, $\tilde{\mathcal{S}}_{\boldsymbol{j}}$ is $\mathbb{F}$-linearly independent.*

**Proposition 4.** *Let $\boldsymbol{j}, \boldsymbol{j}'$ be two different elements in $\mathcal{R}_{\kappa,d}$ and $L \in \mathcal{M}_{rp\times m}(\mathbb{F})$. Let $A = \{\boldsymbol{a}^1, \ldots, \boldsymbol{a}^{\ell_1}\}$, $B = \{\boldsymbol{b}^1, \ldots, \boldsymbol{b}^{\ell_2}\}$, $\tilde{\mathcal{S}}_{\boldsymbol{j}}$ and $\tilde{\mathcal{S}}_{\boldsymbol{j}'}$ be as in Proposition 3. Then, $\tilde{\mathcal{S}}_{\boldsymbol{j}} \cup \tilde{\mathcal{S}}_{\boldsymbol{j}'}$ is a set of linearly independent vectors in $\ker_l\left[(I_p \otimes K)L\right]$ if and only if $A$ and $B$ are both linearly independent in $\ker_l(L)$.*

Similarly to the square case and full kernel case, we expect to have the following result.

**Corollary 5.** *Suppose Conjecture 1 is true, $\binom{r}{d}p > \binom{r}{d+1}m$, $d+1 \leq \min\{\kappa, r\}$ and $m < rp$. If $\mathcal{F} \in \mathsf{KS}_\kappa(p \times q, m, r)$ is chosen uniformly at random, then with high probability there is a set with*

$$\binom{\kappa}{d+1}\left[\binom{r}{d}p - \binom{r}{d+1}m\right]$$

*linearly independent syzygies of $\mathcal{F}$ of degree $d$.*

## 5 Complexity of the KS Modeling Revisited

Proposition 4 and Corollary 5 (Corollary 2 for square matrices) naturally lead to a new algorithm to solve systems of the form $\mathcal{F} = \mathbf{0}$, where $\mathcal{F}$ is randomly chosen in $\mathsf{KS}_\kappa(p \times q, m, r)$, and $m < rp$. Let $p, q, m, r$ be positive integers. The following number

$$d_{\mathrm{KS}} = \min\left\{d \mid \left[\binom{r}{d}p > \binom{r}{d+1}m\right],\ 1 \leq d \leq r-1\right\} \tag{9}$$

is well defined if $m < rp$. Assuming $d_{\mathrm{KS}} + 1 \leq \kappa$, by Corollary 5, with high probability we can build degree drops from $d_{\mathrm{KS}} + 2$ to $d_{\mathrm{KS}} + 1$, for a randomly given $\mathcal{F} \in \mathsf{KS}_\kappa(p \times q, m, r)$. By Proposition 2, such degree falls are not produced by trivial syzygies. Thus $D_{\mathrm{KS}} := d_{\mathrm{KS}} + 2$ is an upper bound for the first fall degree $D_{\mathrm{ff}}$. Then, we construct the Macaulay matrix at degree $d_{\mathrm{KS}} + 1$, append the degree falls, and row reduce this augmented matrix. If there are not enough polynomials to solve, we continue the XL algorithm up to degree $d_{\mathrm{KS}} + 2, d_{\mathrm{KS}} + 3, \ldots$ until we solve the system.

Based on these observations, we now estimate the complexity of solving such a system, by means of the first fall degree $D_{\mathrm{ff}}$ of the system, which is the smallest degree needed so that the Macaulay matrix of the system of that degree exhibits a degree fall when reduced [9].

We can further improve the complexity by multiplying only by monomials from kernel variables $\mathbf{k}$ in the XL algorithm. It can be proved that for this particular kind of equations, the XL algorithm restricted in this manner, still finds a solution. This follows from the facts that the ideal generated by $\mathcal{F}$ is radical [18], that the system $\mathcal{F} = 0$ has a unique solution, and that each polynomial in $\mathcal{F}$ has only linear variables in its linear part.

Consequently, using the XL algorithm and multiplying only by monomials from kernel variables, the complexity of solving instances of KS that are chosen uniformly at random is

$$O\left(\binom{r\kappa + d_{KS} + 1}{d_{KS} + 2}^w\right) = O\left(\binom{r\kappa + D_{KS} - 1}{D_{KS}}^w\right) = O\left((r\kappa)^{D_{KS}w}\right),$$

where $2 < \omega \leq 3$ and $\kappa$ is the number of kernel vectors that we choose in order to keep the system overdetermined, that is, $\kappa \geq \frac{m}{p-r}$.

This is much lower than previous estimates. For example, if $m = p = q = n$ and $r < \sqrt{n}$, then $d_{\mathrm{KS}} \leq r/2 + 1$, and we can choose $\kappa = \sqrt{n}$, so that, $r\kappa < n$, and hence, our complexity estimate is $O(n^{(r/2)\omega})$, compared to $O(n^{r\omega})$ from previous estimates, c.f. [1].

## 6 Experimental Results

In this section we present some experimental data to confront our theoretical findings. The results are summarized in Tables 1 and 2.

Table 1 shows that for $\mathcal{F} \in \mathsf{KS}(n \times n, m, r)$, and different values of $r$, $D_{\mathrm{KS}} = d_{\mathrm{KS}} + 2$ is a tight bound on the first fall degree. It also shows that $D_{\mathrm{KS}}$ is not far from the solving degree, which the maximum degree reached during the Gröbner basis computation. The solving degree was exactly $D_{\mathrm{KS}}$ in most cases, and it was $D_{\mathrm{KS}} + 1$ in the worst case. Also, in Table 1 we can see that the KS system can be solved by using the XL algorithm multiplying only by kernel variables. This leads to much smaller matrices.

Table 2 addresses the question of how to choose $\kappa$. In Section 4.3, we showed that as long as $d_{\mathrm{KS}} + 1 \leq \kappa$, we would find nontrivial relations for a sequence $\mathcal{F} \in \mathsf{KS}_\kappa(n \times n, m, r)$ at degree $d_{\mathrm{KS}} + 2$. We also saw that if $\kappa \geq \frac{m}{n-r}$, the system is overdetermined, so we do not expect spurious solutions. In all the experiments presented in Table 2, we indeed obtained only true solutions. However, choosing the smallest possible $\kappa$ is not necessarily the best choice, because for very small $\kappa$ the solving degree increases. The experiments suggest there is an optimal $\kappa$ around $d_{\mathrm{KS}} + 2$. In Table 2, $d_{\mathrm{KS}} + 2 = 5$ for $r = 6$ or $r = 5$, and $d_{\mathrm{KS}} + 2 = 4$ when $r = 4$.

## 7 Implications in Multivariate Cryptography

A key recovery attack can be performed on several multivariate schemes by solving some MR problem instances [4, 7, 21, 23, 26]. In this section, we review

**Table 1.** Experimental result for KS method on uniformly chosen MR instances over $GF(13)$. For different values of $r$, a sequence $\mathcal{F} \in \mathsf{KS}(10\times 10, 10, r)$ is chosen considering $n-r$ kernel vectors. In each case $F4$ and a version of the XL algorithm, in which we only multiply by kernel variables, are run over $\mathcal{F}$. Measures of the first fall degree $D_{\mathrm{ff}}$, the solving degree $D_{\mathrm{slv}}$ and size of the largest matrix L.matrix. For each $r$ in the first column shows the F4 data and in the second one the XL data.

| $r$ | 2 | | 3 | | 4 | | 5 | | 6 | |
|---|---|---|---|---|---|---|---|---|---|---|
| $D_{\mathrm{KS}}$ | 3 | | 4 | | 4 | | 5 | | 5 | |
| | F4 | XL | F4 | XL | F4 | XL | F4 | XL | F4 | XL |
| $D_{\mathrm{ff}}$ | 3 | 3 | 4 | 4 | 4 | 4 | 5 | | 5 | |
| $D_{\mathrm{slv}}$ | 3 | 3 | 4 | 4 | 4 | | 5 | | | |
| L.matrix | 2217 | 1530 | 24582 | 20240 | 38586 | | 341495 | | $> 2035458$ | |

**Table 2.** Experimental results for the KS method on uniformly chosen MR instances over $GF(13)$. A sequence $F \in KS(12\times 12, 12, r)$ is chosen considering $\kappa$ kernel vectors. The variable $x_1$ is set to 1 in $F$. $F4$ is used to find the variety of the resulting system. Measures of the first fall degree $D_{\mathrm{ff}}$, the solving degree $D_{\mathrm{slv}}$, time and memory are presented.

| $r$ | $\kappa$ | $D_{\mathrm{ff}}$ | $D_{\mathrm{slv}}$ | Time [s] | Mem [MB] | $r$ | $\kappa$ | $D_{\mathrm{ff}}$ | $D_{\mathrm{slv}}$ | Time [s] | Mem [MB] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 6 | 4 | 5 | 20079 | 25547 | 4 | 8 | 4 | 4 | 58 | 194 |
| | 5 | 4 | 5 | 42858 | 20928 | | 7 | 4 | 4 | 38 | 128 |
| | 4 | 4 | 5 | 95768 | 34573 | | 6 | 4 | 4 | 21 | 107 |
| 5 | 7 | 4 | 4 | 756 | 1984 | | 5 | 4 | 4 | 13 | 104 |
| | 6 | 4 | 4 | 367 | 1199 | | 4 | 4 | 4 | 11 | 64 |
| | 5 | 4 | 4 | 377 | 758 | | 3 | 4 | 4 | 6 | 64 |
| | 4 | 4 | 4 | 108 | 352 | | 2 | 4 | 5 | 14 | 160 |
| | 3 | 5 | 5 | 795 | 1648 | | | | | | |

the complexity of the KS method for some of the most common multivariate schemes. We are not including Rainbow in this analysis, since the improvement that we are proposing for KS is still way slower than the linear algebra techniques used to perform the MR attack against this particular signature scheme [8].

**HFE:** A key recovery attack on the HFE encryption scheme with parameters $(n, D, |\mathbb{F}|)$ can be performed by solving a KS system $\mathcal{F} = \mathbf{0}$, where $\mathcal{F} \in \mathsf{KS}(n \times n, n, r)$ and $r = \lceil \log_{|\mathbb{F}|} D \rceil$. In this case, $d_{\mathrm{KS}} = \lceil \frac{r-1}{2} \rceil$ or $d_{\mathrm{KS}} = \frac{r-1}{2} + 1$, depending on whether $r-1$ is odd or even. The complexity of solving an MR instance with parameters $n \times n, n, r$, using $\kappa$ kernel vectors is

$$O\left(\binom{r\kappa + d_{\mathrm{KS}} + 1}{d_{\mathrm{KS}} + 2}^{w}\right),$$

where $d_{\mathrm{KS}} = \lceil \frac{r-1}{2} \rceil$ or $\frac{r-1}{2} + 1$.

For example, for the parameters $n = 128, D = 192, |\mathbb{F}| = 2$ analyzed in [1], we have $r = 8$, and $d_{\mathrm{KS}} = 4$. Using $\kappa = 10$ kernel vectors, we need to deal with a KS system of $n\kappa = 1280$ equations in $n + r\kappa = 208$ variables. Assuming $\omega = 2.4$, the complexity of solving such a system is $2^{69}$, which is way better than the $2^{108}$ complexity of the minors method approach estimated in [1] .

**ZHFE:** To perform a key recovery attack on the ZHFE encryption scheme with parameters $(n, D, |\mathbb{F}|)$, we need to solve a KS instance $\mathcal{F} = \mathbf{0}$, where $\mathcal{F} \in \mathsf{KS}(n \times n, 2n, r)$ and $r = \lceil \log_{|\mathbb{F}|} D \rceil + 1$, see [4]. In this case $d_{\mathrm{KS}}$ is either $\lceil \frac{2r-1}{3} \rceil$ or $\frac{2r-1}{3} + 1$.

For the proposed parameters $n = 55$, $D = 105$, $|\mathbb{F}| = 7$ [24], we have that $r = 4$ and $d_{\mathrm{KS}} = 3$. Thus, by considering $\kappa = 14$ kernel vectors, the estimated complexity is then $2^{63}$, with $\omega = 2.8$. This is better than the estimated $2^{76}$ with $\omega = 2.8$ provided in [4] based on the minors method.

**HFEv-:** In HFEv- with parameters $(|\mathbb{F}|, n, D, a, v)$ the system to solve is $\mathcal{F} = \mathbf{0}$, where $\mathcal{F} \in \mathsf{KS}((n + v) \times (n + v), n - a, r + a + v)$ [7] and $r = \lceil \log_{|\mathbb{F}|} D \rceil$ [23]. The parameter for complexity $d_{\mathrm{KS}}$ is given by $\left\lceil \frac{(r+a+v)(n-a)-(n+v)}{2n+v-a} \right\rceil$ or $\frac{(r+a+v)(n-a)-(n+v)}{2n+v-a} + 1$, depending if the value inside $\lceil \cdot \rceil$ is even or odd.

**GeMMS and Gui:** GeMMS and Gui are HFEv- based multivariate signature schemes proposed in the NIST's ongoing post-quantum "competition" [5, 23]. A key recovery attack to GeMMS or Gui with parameters $(|\mathbb{F}|, n, D, a, v, k)$ reduces to a key recovery attack to the underlying HFEv- instances with parameters $(|\mathbb{F}|, n, D, a, v)$. We use the sets of parameters proposed for the NIST's competition to analyze the complexity of such an attack and set $\omega = 2.3$, which is the one used in the Gui submission. The main improvement in the key recovery attack is derived from reducing the number of kernel vectors. For the parameter sets Gui-184(2,184,33,16,16,2), Gui-312(2,312,129,24,20,2) and Gui-448(2,448,513,32,28,2) we may set $\kappa = 18$, $\kappa = 25$ and $\kappa = 34$, respectively, producing key recovery complexities of $2^{281}$, $2^{429}$ and $2^{598}$ steps, respectively. For comparison, the estimates provided in [23] via minors modeling were $2^{323}$, $2^{480}$ and $2^{665}$, respectively. A similar effect applies to the GeMMS security estimates as well.

## 8 Acknowledgements

We would like to thank Daniel Escudero, Albrecht Petzoldt, Rusydi Makarim, and Karan Khathuria for useful discussions. The author Javier Verbel is supported by "Fondo Nacional de Financiamiento para la Ciencia, la Tecnología y la Innovación Francisco José de Caldas", Colciencias (Colombia). Some of the

[7] When $r + v + a$ is odd the target rank is $r + a + v - 1$

experiments were conducted on the Gauss Server, financed by “Proyecto Plan 150x150 Fomento de la cultura de evaluación continua a través del apoyo a planes de mejoramiento de los programas curriculares”.

## References

1. Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, 2013.
2. B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.*, 10(3):19–29, August 1976.
3. Jonathan F Buss, Gudmund S Frandsen, and Jeffrey O Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3):572 – 596, 1999.
4. Daniel Cabarcas, Daniel Smith-Tone, and Javier A. Verbel. Key recovery attack for zhfe. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography*, pages 289–308, Cham, 2017. Springer International Publishing.
5. A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. Gemss: A great multivariate short signature. NIST CSRC, 2017. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/GeMSS.zip.
6. N. Courtois, A. Klimov, J. Patarin, and A.Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. *EUROCRYPT 2000, LNCS*, 1807:392–407, 2000.
7. Nicolas T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem minrank. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 402–421, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.
8. J. Ding, M.S. Chen, A. Petzoldt, D. Schmidt, and B.Y. Yang. Rainbow. NIST CSRC, 2017. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/Rainbow.zip.
9. Jintai Ding and Timothy J. Hodges. Inverting HFE Systems is Quasi-Polynomial for All Fields. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 724–742. Springer Berlin Heidelberg, 2011.
10. Jintai Ding and Thorsten Kleinjung. Degree of regularity for hfe-. Cryptology ePrint Archive, Report 2011/570, 2011. https://eprint.iacr.org/2011/570.
11. Jintai Ding and Dieter Schmidt. *Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields*, pages 34–49. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
12. Jintai Ding and Bo-Yin Yang. Degree of regularity for hfev and hfev-. In Philippe Gaborit, editor, *Post-Quantum Cryptography*, pages 52–66, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
13. Vivien Dubois and Nicolas Gama. The degree of regularity of hfe systems. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010*, pages 557–576, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.
14. J. C. Faugere. A new efficient algorithm for computing grobner bases (f4). *Journal of Pure and Applied Algebra*, 139:61–88, 1999.

15. J. C. Faugere. A new efficient algorithm for computing grobner bases without reduction to zero (f5). *ISSAC 2002, ACM Press*, pages 75–83, 2002.
16. Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. *Symbolic and Algebraic Computation, International Symposium, ISSAC 2010, Munich, Germany, July 25-28, 2010, Proceedings*, pages 257–264, 2010.
17. Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Groebner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. *Journal of Symbolic Computation*, 46(4):406 – 437, 2011.
18. Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret. Cryptanalysis of minrank. In *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, pages 280–296, 2008.
19. P. Gaborit, O. Ruatta, and J. Schrek. On the complexity of the rank syndrome decoding problem. *IEEE Transactions on Information Theory*, 62(2):1006–1019, 2016.
20. Louis Goubin and Nicolas T. Courtois. *Cryptanalysis of the TTM Cryptosystem*, pages 44–57. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.
21. Aviad Kipnis and Adi Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In Michael Wiener, editor, *Advances in Cryptology – CRYPTO 99*, pages 19–30, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.
22. Daniel Lazard. Gröbner-bases, gaussian elimination and resolution of systems of algebraic equations. In *Computer Algebra, EUROCAL '83, European Computer Algebra Conference, London, England, March 28-30, 1983, Proceedings*, pages 146–156, 1983.
23. Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. Design principles for hfev- based multivariate signature schemes. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015*, pages 311–334, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.
24. Jaiberth Porras, John Baena, and Jintai Ding. Zhfe, a new multivariate public key encryption scheme. In Michele Mosca, editor, *Post-Quantum Cryptography*, pages 229–245, Cham, 2014. Springer International Publishing.
25. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.
26. Jeremy Vates and Daniel Smith-Tone. Key recovery attack for all parameters of hfe-. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography*, pages 272–288, Cham, 2017. Springer International Publishing.