Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology

Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer
INRIA, Paris-Rocquencourt Center, SALSA Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy-Kennedy
Case 169, 4, Place Jussieu, F-75252 Paris
{Jean-Charles.Faugere,Mohab.Safey,Pierre-Jean.Spaenlehauer}@lip6.fr

ABSTRACT

Computing loci of rank defects of linear matrices (also called the MinRank problem) is a fundamental NP-hard problem of linear algebra which has applications in Cryptology, in Error Correcting Codes and in Geometry. Given a square linear matrix (i.e. a matrix whose entries are k-variate linear forms) of size n and an integer r, the problem is to find points such that the evaluation of the matrix has rank less than $r+1$. The aim of the paper is to obtain the most efficient algorithm to solve this problem. To this end, we give the theoretical and practical complexity of computing Gröbner bases of two algebraic formulations of the MinRank problem. Both modelings lead to *structured algebraic systems*.

The first modeling, proposed by Kipnis and Shamir generates bi-homogeneous equations of bi-degree $(1,1)$. The second one is classically obtained by the vanishing of the $(r+1)$-minors of the given matrix, giving rise to a determinantal ideal. In both cases, under genericity assumptions on the entries of the considered matrix, we give new bounds on the degree of regularity of the considered ideal which allows us to estimate the complexity of the whole Gröbner bases computations. For instance, the *exact* degree of regularity of the determinantal ideal formulation of a generic well-defined MinRank problem is $r(n-r)+1$. We also give optimal degree bounds of the loci of rank defect which are reached under genericity assumptions; the new bounds are much lower than the standard multi-homogeneous Bézout bounds (or mixed volume of Newton polytopes).

As a by-product, we prove that the generic MinRank problem could be solved in polynomial time in n (when $n-r$ is fixed) as announced in a previous paper of Faugère, Levy-dit-Vehel and Perret. Moreover, using the determinantal ideal formulation, these results are used to break a cryptographic challenge (which was untractable so far) and allow us to evaluate precisely the security of the cryptosystem w.r.t. n, r and k. Our practical results suggest that, up to the software state of the art, this latter formulation is more adapted in the context of Gröbner bases computations.

Keywords

Polynomial systems solving, Gröbner bases, Degree of regularity, Multi-homogeneous ideals, Determinantal ideals, Multivariate Cryptography, Generalized nonlinear Eigenvalue problem.

1. INTRODUCTION

Computing the locus of rank defect of a linear matrix (also called the MinRank problem) is of first importance for a wide range of applications. For instance, the security of many multivariate cryptosystems is closely related to the difficulty of solving MinRank problems [19, 7]. In geometry, the degeneracy locus of a projection of an algebraic surface defined by quadratic equations is the locus of rank defect of its jacobian matrix (which is a linear matrix) (see for instance [1]). Also, decoding metric rank codes can be reduced to a MinRank problem [21].

For $(n,k,r)\in\mathbb{N}^3$, we define the square MinRank problem as follows: given a square linear matrix of size n with k variables (i.e. a matrix whose entries are k-variate polynomials of degree 1 over a field $\mathbb{K}$), the goal is to find the locus of the points such that the matrix has a rank less than $r+1$. This problem is difficult since deciding whether this locus is empty or not is NP-hard when $\mathbb{K}$ is a finite field [5]. When $k=1$ the MinRank problem can be reduced to the well known EigenValue problem. Therefore, the MinRank problem can be seen as a generalized nonlinear eigenvalue problem.

The ultimate objective of this paper is to find the most efficient method to solve this problem when the linear matrix is generic. In particular, we focus on two algebraic representations: the Kipnis-Shamir modeling [19] and the minors formulation.

Both representations are rather intuitive. For the Kipnis-Shamir modeling, the algebraic system is constructed by remarking that a matrix has a rank $\leq r$ if and only if there exist at least $n-r$ independent vectors in its kernel. Considering the coefficients of these vectors as variables gives rise to a quadratic system. On the other hand, the minors modeling is obtained by considering all the minors of size $r+1$ of the linear matrix (which simultaneously vanish on the solutions of the MinRank problem).

Previous work. Since the MinRank problem has many applications, it has been extensively studied during the past decades, and a lot of different approaches have been tried (see [7] for details). So far, the most successful method seemed to be the Kipnis-Shamir formulation [19], which has been analyzed in [14]. Indeed, when combined with the Algorithms F_5 [12] and FGLM [13], it can solve the challenges A and B proposed in [7]. However, the challenge C was remaining unbroken until now.

If $k=(n-r)^2$, then the number of solutions of a generic (n,k,r)-MinRank instance is finite and equal to the degree of the ideal I generated by the Kipnis-Shamir equations [14]. Since the solving strategy involves the FGLM Algorithm (whose complexity is $O(\deg(I)^3)$), it is crucial to have good estimates of $\deg(I)$. The algebraic system obtained by the Kipnis-Shamir formulation is multi-homogeneous, thus upper bounds can be obtained by the multi-homogeneous Bézout number [14] or by computing the mixed volume of the associated Newton polytope [10]. However, those bounds are not sharp.

Main results. The contributions of the paper are two-fold: theoretical and practical. Applying a Theorem from [15] to the Kipnis-Shamir modeling yields a bound on the degree of regularity of this system. From the viewpoint of the minors approach, we show that properties of the associated ideal are closely related to properties of determinantal ideals generated by minors of matrices whose entries are variables. More precisely, Lemma 1 brings out the relation between the ideal generated by the minors of a generic linear matrix and the ideal obtained by adding to a determinantal ideal n^2 generic linear forms. Thus properties known about determinantal ideals can be transferred to ideals corresponding to the minors modeling. In particular, this permits to establish explicit formulae for the exact degree of the ideal (Corollary 1) and for its Hilbert series (Theorem 3 and Theorem 4).

With this new information, the asymptotic complexity of solving the generic MinRank problem by both methods can be estimated, and it is shown (Section 4) that this complexity is polynomial in n when $k=(n-r)^2$ is constant. Surprisingly, using these new complexity estimates we found than the complexity bound of the minors approach is better than the complexity bound of the Kipnis-Shamir modeling.

Experiments were carried out with a view to checking the accuracy of the previous theoretical estimates. We apply those results to solve a cryptographic challenge based on MinRank which was untractable so far: experiments show that it is now possible to effectively break the challenge C from [7] by using the minors formulation and the F_5 Algorithm in only 2^{49} arithmetic operations in $\mathsf{GF}(65521)$.

Organization of the paper. After this short introduction, notations are introduced and the two modelings are formally defined. Some useful results are also recalled. Section 3 contains the main theoretical results and their proofs. Then, we derive complexity estimates of the cost of solving MinRank by using Gröbner bases Algorithms. Finally, we present in Section 5 experimental results.

Acknowledgements. We wish to thank Ioannis Z. Emiris and Tomohiko Mizutani who provided bounds obtained by computing the mixed volume of the Newton polytope of the Kipnis-Shamir formulation. We are also grateful to Ludovic Perret for his helpful comments and suggestions.

2. PRELIMINARIES

General notations. Let $\mathbb{K}$ be a field. Let k, n and r be three integers, with $r<n$ and let $\mathbf{a}=(a_{(1,1)}^{(0)},\ldots,a_{(n,n)}^{(k)})\in\mathbb{K}^{n^2(k+1)}$. Consider $\mathscr{M}\in\mathsf{M}_n(\mathbb{K}[x_1,\ldots,x_k])$ the $n\times n$ linear matrix

$$\mathscr{M}_{i,j}(x_1,\ldots,x_k)=a_{i,j}^{(0)}+\sum_{\ell=1}^{k}a_{i,j}^{(\ell)}x_\ell.$$

We called (n,k,r)-MinRank the problem of finding a point $(x_1,\ldots,x_k)$ in $\overline{\mathbb{K}}^k$ (where $\overline{\mathbb{K}}$ denotes the algebraic closure of $\mathbb{K}$) such that the rank of $\mathscr{M}(x_1,\ldots,x_k)$ is less than $r+1$.

In this paper, we focus on the generic case, i.e. when $\mathbf{a}$ is chosen "at random". If $k=(n-r)^2$ (resp. $k<(n-r)^2$), the problem admits a finite number of solutions (see [14]) and is called *well-defined* (resp. *over-defined*). Note that if the problem is under-defined ($k>(n-r)^2$), it can be reduced to the well-defined case by specializing $k-(n-r)^2$ variables to random values [14].

An interesting subclass of problems is the homogeneous MinRank problem, obtained when $a_{(i,j)}^{(0)}=0$ for all (i,j).

The Kipnis-Shamir formulation. $(x_1,\ldots,x_k)$ is solution of the (n,k,r)-MinRank problem if and only if there are at least $n-r$ independent vectors in the kernel of $\mathscr{M}(x_1,\ldots,x_k)$. Since we assumed that $\mathbf{a}$ is chosen at generic, we can suppose that a basis of the kernel can be written in systematic form [14]. Consider the following $n\times(n-r)$ matrix:

$$\mathscr{K}=\begin{pmatrix}1&0&\ldots&0\\0&1&\ldots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\ldots&1\\y_1^{(1)}&y_1^{(2)}&\ldots&y_1^{(n-r)}\\\vdots&\vdots&\ddots&\vdots\\y_r^{(1)}&y_r^{(2)}&\ldots&y_r^{(n-r)}\end{pmatrix}.$$

The Kipnis-Shamir modeling is constructed by considering the algebraic system $\mathscr{M}\cdot\mathscr{K}=0$. Indeed, if $(x_1,\ldots,x_k,y_1^{(1)},\ldots,y_r^{(n-r)})$ is a solution of the algebraic system, then $(x_1,\ldots,x_k)$ is solution of the corresponding MinRank problem.

On the one hand, this system can be seen as a multi-homogeneous system with the following partition of variables:

$$\{x_1,\ldots,x_k\}\cup\{y_1^{(1)},\ldots,y_r^{(1)}\}\cup\ldots\cup\{y_1^{(n-r)},\ldots,y_r^{(n-r)}\}.$$

On the other hand, it can also be considered as a bilinear system with the partition of variables $X\cup Y$.

The minors formulation. $(x_1,\ldots,x_k)$ is solution of a (n,k,r)-MinRank problem if and only if all minors of size $r+1$ of $\mathscr{M}$ simultaneously vanish on this point. Thus the minors modeling is obtained by considering the algebraic system of all minors of size $r+1$.

Solving strategy. For the well-defined problem, we use the following strategy (for both modelings): first compute a grevlex Gröbner basis of the ideal generated by the equations with the F_5 Algorithm [12], then compute a Gröbner basis for the lex ordering by using FGLM [13]. For applications in Cryptology, $\mathbb{K}$ is a finite field and it is often known that a solution of the problem lies in $\mathbb{K}^k$. Then it is possible to combine this approach with an exhaustive search over s variables. For every possible values of s variables, we solve the resulting over-determined $(n,(n-r)^2-s,r)$-MinRank problem.

Previous works. The strategy for solving well-defined MinRank problems involves the FGLM Algorithm. Its complexity is well known: $O(\deg(I)^3)$ arithmetic operations, where $\deg(I)$ is the degree of the ideal generated by the equations (this degree is the same for both modelings). Therefore, sharp bounds on $\deg(I)$ are required to estimate the complexity of this step. So far, bounds on this degree are obtained by considering the multi-homogeneous structure of the Kipnis-Shamir formulation. A bound can be obtained with the multi-homogeneous Bézout number: $\deg(I)\le\binom{n}{r}^{n-r}$ (see [14] for details). Newton polytope techniques [10] permits to achieve slightly sharper bounds, but requires heavier computations. However, the gap between known bounds and the real degree is big. For instance, for the $(6,9,3)$ problem, the degree of the ideal generated by either of the two modelings is 980, whereas the associated

Bézout number is 8000 [14], and the mixed volume bound of the associated Newton polytope is 7340[1].

To estimate the complexity of the computation of the grevlex Gröbner basis, upper bounds on the so-called *degree of regularity* of the ideal generated by the equations are required. This value is the highest degree encountered during a Gröbner basis calculation with respect to a graded monomial ordering. The complexity of the whole Gröbner basis computation can be estimated by $O(\mathsf{M}(\mathsf{d}_{\mathsf{reg}})^{\omega})$ [3, 2], where $\mathsf{M}(\mathsf{d}_{\mathsf{reg}})$ denotes the number of monomials of degree less than or equal to $\mathsf{d}_{\mathsf{reg}}$, and ω is the linear algebra constant ($2 \leq \omega \leq 3$). Recently, we showed in [15] a sharp bound on the degree of regularity of generic affine bilinear systems:

THEOREM 1. *[15, Theorem 6.1] For the grevlex ordering, the degree of regularity of a generic affine bilinear 0-dimensional system over $\mathbb{K}[X,Y]$ is upper bounded by $\min(\mathsf{card}(X), \mathsf{card}(Y)) + 1$.*

The Kipnis-Shamir algebraic modeling is a bilinear system, thus this bound can be applied: $\mathsf{d}_{\mathsf{reg}} \leq \min(k, (n-r)r) + 1$. In the case of well-defined instances, $k = (n-r)^2$ and thus $\mathsf{d}_{\mathsf{reg}} \leq \min((n-r)^2, (n-r)r) + 1$. In comparison, the classical Macaulay bound would yield an upper bound of $n(n-r)+1$ [20].

In [15, Section 6.1], we also proposed a variant of the F_5 Algorithm dedicated to multi-homogeneous systems, which could speed-up the computation of the Gröbner basis of the Kipnis-Shamir system. However, there is so far no efficient implementation of this algorithm.

Determinantal ideals. Properties of the minors modeling are strongly related to properties of *determinantal ideals* generated by minors of matrices whose entries are variables. In this paper, $\mathscr{D}$ denotes the ideal of $\mathbb{K}[v_{1,1}, \dots, v_{n,n}]$ generated by all minors of size $r+1$ of the following $n \times n$ matrix:

$$\begin{pmatrix} v_{1,1} & \dots & v_{1,n} \\ \vdots & \ddots & \vdots \\ v_{n,1} & \dots & v_{n,n} \end{pmatrix}.$$

Many results are known about the structure of the ideal $\mathscr{D}$.

THEOREM 2. *[6, page 679] The dimension of $\mathscr{D}$ is $(2n-r)r$, and its Hilbert series is*

$$\mathsf{HS}(t) = \frac{\det A(t)}{t^{\binom{r}{2}}(1-t)^{(2n-r)r}}.$$

The following Proposition is a consequence of the Thom-Porteous formula. This question has been discussed by Giambelli, Harris-Tu and Baker. A short proof of this formula can be found in [18, page 261].

PROPOSITION 1. *[18, page 261] The degree of the determinantal ideal $\mathscr{D}$ is*

$$\prod_{i=0}^{n-r-1} \frac{i!(n+i)!}{(n-1-i)!(n-r+i)!}$$

3. THEORETICAL ANALYSIS OF THE MINORS FORMULATION

Applications require efficient methods to solve the affine MinRank problem. However, we start by studying the homogeneous case. Indeed, the structure of the homogeneous problem is closely related to that of the affine case, and is easier to describe from a theoretical viewpoint.

[1]This value was provided to us by Ioannis Z. Emiris and Tomohiko Mizutani.

Notations Throughout this paper, $\mathfrak{a}$ denotes the set of kn^2 variables $\{\mathfrak{a}_{1,1}^{(1)}, \dots, \mathfrak{a}_{n,n}^{(k)}\}$, $\mathfrak{b}$ denotes the set of kn^2 variables $\{\mathfrak{b}_{1,1}^{(1)}, \dots, \mathfrak{b}_{n,n}^{(k)}\}$ and $\mathfrak{c}$ is the set of n^4 variables $\{\mathfrak{c}_{1,1}^{(1,1)}, \dots, \mathfrak{c}_{n,n}^{(n,n)}\}$. We consider the generic matrix $\mathscr{M} \in \mathsf{M}_n(\mathbb{K}(\mathfrak{a})[x_1, \dots, x_k])$ defined by

$$\mathscr{M}_{i,j} = \sum_{\ell=1}^{k} \mathfrak{a}_{i,j}^{(\ell)} x_\ell.$$

In the following, $\mathscr{I}$ denotes the ideal generated by all minors of size $r+1$ of $\mathscr{M}$. X (resp. V) denotes the set of variables $\{x_1, \dots, x_k\}$ (resp. $\{v_{1,1}, \dots, v_{n,n}\}$).

We would like to point out that the results of this section can be extended to the case where $\mathscr{M}$ is a non-square matrix.

3.1 The under-defined homogeneous case

In this part of the paper, we suppose that $k > (n-r)^2$. When $k \leq (n-r)^2$, the system is 0-dimensional and this case is discussed in Section 3.2.

DEFINITION 1.

- *We denote by $\widetilde{\mathscr{I}}$ the ideal of $\mathbb{L}[X,V]$ defined by*

$$\widetilde{\mathscr{I}} = \mathscr{I} + \left\langle v_{i,j} - \sum_{\ell=1}^{k} \mathfrak{a}_{i,j}^{(\ell)} x_\ell \right\rangle_{1 \leq i,j \leq n}.$$

- *For $\mathbf{a} = (a_{1,1}^{(1)}, \dots, a_{n,n}^{(k)}) \in \mathbb{K}^{n^2 k}$, the specialization morphism is denoted by $\varphi_{\mathbf{a}}$:*

$$\begin{array}{ccc} \mathbb{K}(\mathfrak{a}) & \to & \mathbb{K} \\ f(\mathfrak{a}_{1,1}^{(1)}, \dots, \mathfrak{a}_{n,n}^{(k)}) & \mapsto & f(a_{1,1}^{(1)}, \dots, a_{n,n}^{(k)}) \end{array}$$

- *$\widetilde{\mathscr{D}}$ denotes the ideal of $\mathbb{K}(\mathfrak{b}, \mathfrak{c})[X,V]$ defined by:*

$$\widetilde{\mathscr{D}} = \mathscr{D} + \langle g_{i,j} \rangle_{1 \leq i,j \leq n},$$

where $g_{i,j} = \sum_{\ell=1}^{k} \mathfrak{b}_{i,j}^{(\ell)} x_k + \sum_{1 \leq \ell_1, \ell_2 \leq n} \mathfrak{c}_{i,j}^{(\ell_1,\ell_2)} v_{\ell_1,\ell_2}$ are generic linear forms.

- *For $(\mathbf{b}, \mathbf{c}) \in \mathbb{K}^{n^2 k} \times \mathbb{K}^{n^4}$, $\psi_{\mathbf{b},\mathbf{c}}$ denotes the specialization morphism:*

$$\begin{array}{ccc} \mathbb{K}(\mathfrak{b}, \mathfrak{c}) & \to & \mathbb{K} \\ f(\mathfrak{b}, \mathfrak{c}) & \mapsto & f(\mathbf{b}, \mathbf{c}) \end{array}$$

The following Lemma is one of the main tools of this Section: it shows how to transfer properties of $\mathscr{D}$ to the ideal $\widetilde{\mathscr{I}}$ generated by the minors.

LEMMA 1. *Let $\mathscr{P}$ be a property which holds on some ideals of $\mathbb{K}[X,V]$. Suppose that there exists a nonempty Zariski open set $O_P \subset \mathbb{K}^{n^2 k} \times \mathbb{K}^{n^4}$ such that $\forall (\mathbf{b}, \mathbf{c}) \in O_P$, $\mathscr{P}$ is verified on $\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}})$. Then there exist nonempty Zariski open sets $O' \subset \mathbb{K}^{n^2 k} \times \mathbb{K}^{n^4}$ and $O'' \subset \mathbb{K}^{n^2 k}$ such that*

$$\{\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}}) : \mathbf{a} \in O''\} = \{\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}}) : (\mathbf{b}, \mathbf{c}) \in O'\}$$

and the property $\mathscr{P}$ holds for every ideal in this set.

PROOF. Let $\mathscr{F}$ denote the complementary of O_P in $\mathbb{K}^{n^2 k} \times \mathbb{K}^{n^4}$, and let $I \subset \mathbb{K}[X,V]$ denote the ideal of polynomials vanishing on

$\mathscr{F}$. Consider the following $n^2 \times (n^2+k)$ matrix:

$$\mathscr{C} = \begin{pmatrix} \mathfrak{c}_{1,1}^{(1,1)} & \dots & \mathfrak{c}_{1,1}^{(n,n)} & \mathfrak{b}_{1,1}^{(1)} & \dots & \mathfrak{b}_{1,1}^{(k)} \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathfrak{c}_{1,n}^{(1,1)} & \dots & \mathfrak{c}_{1,n}^{(n,n)} & \mathfrak{b}_{1,n}^{(1)} & \dots & \mathfrak{b}_{1,n}^{(k)} \\ \mathfrak{c}_{2,1}^{(1,1)} & \dots & \mathfrak{c}_{2,1}^{(n,n)} & \mathfrak{b}_{2,1}^{(1)} & \dots & \mathfrak{b}_{2,1}^{(k)} \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathfrak{c}_{n,n}^{(1,1)} & \dots & \mathfrak{c}_{n,n}^{(n,n)} & \mathfrak{b}_{n,n}^{(1)} & \dots & \mathfrak{b}_{n,n}^{(k)} \end{pmatrix}.$$

For $M \in \mathsf{GL}_{n^2}(\mathbb{K})$, let $I_M \subset \mathbb{K}[X,V]$ denote the ideal obtained by performing the linear change of variables $\mathscr{C}' = M \cdot \mathscr{C}$ and let $\mathscr{F}_M$ denote the variety of I_M. Since $\mathbb{K}[X,V]$ is Noetherian,

$$\bigcap_{M \in \mathsf{GL}_{n^2}(\mathbb{K})} \mathscr{F}_M$$

is a Zariski closed subset. Let $\widehat{O}$ be its complementary. Then $\widehat{O}$ is a nonempty Zariski open subset and $\forall (\mathbf{b},\mathbf{c}) \in \widehat{O}$, $\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}})$ verifies the property $\mathscr{P}$.

Let $h \in \mathbb{K}[\mathfrak{b},\mathfrak{c}]$ be the determinant of the $n^2 \times n^2$ matrix of the n^2 first columns of $\mathscr{C}$. The inequation $h(\mathfrak{b},\mathfrak{c}) \neq 0$ defines a nonempty Zariski open subset O_{det} of $\mathbb{K}^{n^2k} \times \mathbb{K}^{n^4}$. Let O' be equal to $\widehat{O} \cap O_{det}$. Then consider the vector $\mathbf{id} = (\mathsf{id}_{i,j}^{(\ell_1,\ell_2)})$ defined by

$$\mathsf{id}_{i,j}^{(\ell_1,\ell_2)} = \begin{cases} 1 \text{ if } (i,j) = (\ell_1,\ell_2) \\ 0 \text{ otherwise.} \end{cases}$$

Then let $O'' \subset \mathbb{K}^{n^2k}$ denote the set $\{\mathbf{a} : (\mathbf{a},\mathbf{id}) \in O'\}$. Then O'' is a nonempty Zariski open subset of $\mathbb{K}^{n^2k}$.

Let $(\mathbf{b},\mathbf{c})$ be in O'. Consequently, the $n^2 \times n^2$ matrix of the n^2 first columns of $\psi_{\mathbf{b},\mathbf{c}}(\mathscr{C})$ is invertible, and thus, by performing a linear combination of the generators, there exists $\mathbf{a} \in \mathbb{K}^{n^2k}$ such that

$$\begin{aligned} &\left\langle \textstyle\sum_{1 \le \ell_1,\ell_2 \le n} c_{i,j}^{(\ell_1,\ell_2)} v_{\ell_1,\ell_2} + \sum_{\ell=1}^{k} b_{i,j}^{(\ell)} x_k \right\rangle_{1 \le i,j \le n} \\ &= \left\langle v_{\ell_1,\ell_2} - \textstyle\sum_{\ell=1}^{k} a_{i,j}^{(\ell)} x_k \right\rangle_{1 \le i,j \le n}. \end{aligned}$$

Then remark that

$$\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}}) = \mathscr{D} + \left\langle v_{\ell_1,\ell_2} - \sum_{\ell=1}^{k} a_{i,j}^{(\ell)} x_k \right\rangle_{1 \le i,j \le n} = \varphi_{\mathbf{a}}(\widetilde{\mathscr{I}}).$$

This shows the inclusion

$$\{\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}}) : (\mathbf{b},\mathbf{c}) \in O'\} \subset \{\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}}) : \mathbf{a} \in O''\}.$$

Conversely, let $\mathbf{a}$ be in O''. By construction, $(\mathbf{a},\mathbf{id})$ is in O' and $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}}) = \psi_{\mathbf{a},\mathbf{id}}(\widetilde{\mathscr{D}})$. Thus $\{\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}}) : \mathbf{a} \in O''\} \subset \{\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}}) : (\mathbf{b},\mathbf{c}) \in O'\}$. $\square$

In order to prove results on $\varphi_{\mathbf{a}}(\mathscr{I})$ (for generic $\mathbf{a}$), we use the following strategy:

- ◦ deduce properties of $\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}})$ by adding to $\mathscr{D}$ generic linear forms;
- ◦ with Lemma 1, transfer those properties to $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}})$;
- ◦ finally, prove properties of $\varphi_{\mathbf{a}}(\mathscr{I})$ by eliminating the variables V.

From now on, we suppose that $n > 1$ and $\prec$ denotes the strict lexicographical ordering on $\mathbb{N}^2$: $(i_1,j_1) \prec (i_2,j_2)$ if and only if

$$\begin{cases} i_1 < i_2 \text{ or} \\ i_1 = i_2 \text{ and } j_1 < j_2. \end{cases}$$

We recall that $g_{i,j}$ denotes a generic linear form (see Definition 1).

PROPOSITION 2.
Let $\mathscr{D}_{\prec(i,j)}$ denote the ideal $\mathscr{D} + \langle g_{\ell_1,\ell_2} \rangle_{(\ell_1,\ell_2) \prec (i,j)} \subset \mathbb{K}[X,V]$. There exists a nonempty Zariski open subset $O \subset \mathbb{K}^{n^2k} \times \mathbb{K}^{n^4}$ such that, if $(\mathbf{b},\mathbf{c}) \in O$, then for all $(i,j) \in \{1,\dots,n\}^2$, $\psi_{\mathbf{b},\mathbf{c}}(g_{i,j})$ does not divide 0 in $\mathbb{K}[X,V]/\psi_{\mathbf{b},\mathbf{c}}(\mathscr{D}_{\prec(i,j)})$.

PROOF. It is proved in [4, Theorem 2.10 and Remark 2.12], that $\mathscr{D}$ is a prime ideal. Moreover $\dim(\mathscr{D}) \ge 2$ (Theorem 2), thus there exists a nonempty Zariski open subset $O_{1,1}$ such that if $(\mathbf{b},\mathbf{c}) \in O_{1,1}$, then $\psi_{\mathbf{b},\mathbf{c}}(g_{1,1})$ does not divide 0 in $\mathbb{K}[X,V]/\mathscr{D}$. Furthermore, since $\mathscr{D}$ is prime, $\mathsf{Spec}(\mathbb{K}[X,V]/\mathscr{D})$ is a reduced and irreducible scheme. According to [16, Corollary 3.4.14], cutting a reduced and irreducible scheme of dimension ≥ 2 by a generic hyperplane yields an irreducible and reduced scheme (it is a consequence of Bertini First Theorem). Therefore, there exists a nonempty Zariski open subset $O'_{1,1}$ such that if $(\mathbf{b},\mathbf{c}) \in O'_{1,1}$, then $\psi_{\mathbf{b},\mathbf{c}}(\mathscr{D} + g_{1,1})$ is also radical and irreducible, thus prime. By recurrence, there exists nonempty Zariski open sets $O_{i,j}$ and $O'_{i,j}$ such that, if $(\mathbf{b},\mathbf{c}) \in O_{i,j}$, then $\psi_{\mathbf{b},\mathbf{c}}(g_{i,j})$ does not divide 0 in $\mathbb{K}[X,V]/\mathscr{D}_{\prec(i,j)}$, and if $(\mathbf{b},\mathbf{c}) \in O'_{i,j}$, then $\psi_{\mathbf{b},\mathbf{c}}(\mathscr{D}_{\prec(i,j)} + g_{i,j})$ is prime. Finally,

$$O = \bigcap_{(i,j) \in \{1,\dots,n\}^2} O_{i,j}$$

is the wanted nonempty Zariski open subset. $\square$

REMARK. We would like to point out that the condition $k > (n-r)^2$ is crucial for the proof of Proposition 2: this proof relies on a Bertini Theorem [16, Theorem 3.4.10], which is only valid if the projective dimension is ≥ 2 (i.e. the Krull dimension is ≥ 3). A consequence of this Theorem is that if a prime homogeneous ideal has dimension $d \ge 3$, then adding $d-2$ generic linear forms yields a prime ideal of dimension 2 [16, Corollary 3.4.14]. Consequently, the maximum number of generic linear forms we can add such that each form does not divide zero in the previous quotient ring is $\dim(\mathscr{D}) + k - 1 = (2n-r)r + k - 1$. We need to add n^2 linear forms to define the generic MinRank problem and $(2n-r)r + k - 1 \ge n^2$ if and only if $k > (n-r)^2$.

COROLLARY 1. *There exists a nonempty Zariski open subset O_1 of $\mathbb{K}^{n^2k}$ such that if $\mathbf{a} \in O_1$, then the dimension of $\varphi_{\mathbf{a}}(I)$ is $k-(n-r)^2$ and its degree is*

$$\prod_{i=0}^{n-r-1} \frac{i!(n+i)!}{(n-1-i)!(n-r+i)!}.$$

PROOF. Consider $\mathscr{D}$ as an ideal of $\mathbb{K}[X,V]$. From Proposition 1, its degree is

$$\prod_{i=0}^{n-r-1} \frac{i!(n+i)!}{(n-1-i)!(n-r+i)!}.$$

From Theorem 2, the dimension of this ideal is $(2n-r)r+k$. According to Proposition 2, there exists a nonempty Zariski open subset O of $\mathbb{K}^{n^2k} \times \mathbb{K}^{n^4}$ such that, $\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}})$ has the same degree as $\mathscr{D}$ and its dimension is $k-(n-r)^2$ if $(\mathbf{b},\mathbf{c}) \in O$ (since adding to an ideal a linear form which is not a divisor or zero in the quotient ring does not change the degree and make the dimension decrease by 1).

Next, Lemma 1 shows that there exists a nonempty Zariski open subset $O_1 \subset \mathbb{K}^{n^2k}$, such that if $\mathbf{a} \in O_1$, then

$$\deg(\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}})) = \prod_{i=0}^{n-r-1} \frac{i!(n+i)!}{(n-1-i)!(n-r+i)!}.$$

Finally remark that in $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}})$, the variables V are linear combinations of the variables X. Thus

$$\begin{array}{rcl}\deg(\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}})) & = & \deg(\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}})\cap\mathbb{K}[X]) \\ & = & \varphi_{\mathbf{a}}(\mathscr{I}). \qquad \square\end{array}$$

The Hilbert series is a useful tool to describe homogeneous ideals of $\mathbb{K}[X]$. If $I\subset\mathbb{K}[X]$, it is defined as follows:

$$\mathsf{HS}(t)=\sum_{\ell\in\mathbb{N}}\dim(\mathbb{K}[X]_d/I_d)t^d,$$

where $\mathbb{K}[X]_d$ is the vector space of homogeneous polynomials of degree d and I_d denotes the vector space $I\cap\mathbb{K}[X]_d$.

Many information can be read on this series. For instance, the dimension, the degree and the degree of regularity can be computed once this series is known. More precisely, if $\mathsf{HS}(t)\in\mathbb{Z}[[t]]$ is the Hilbert series of an ideal $I\subset\mathbb{K}[X]$, then

- the smallest d such that $(1-t)^d\mathsf{HS}(t)$ is a polynomial is the dimension of I;
- if the dimension of I is 0, then the evaluation of the polynomial $\mathsf{HS}(t)$ in $t=1$ gives the degree of the ideal (where d is the dimension of I) and $\deg(\mathsf{HS}(t))+1$ is the degree of regularity of I.

Next Theorem provides an explicit formula for the Hilbert series of the ideal generated by the minors of a generic linear matrix in the homogeneous under-defined case:

THEOREM 3. *There exists a nonempty Zariski open subset O_2 of $\mathbb{K}^{n^2k}$ such that if $\mathbf{a}\in O_2$, then the Hilbert series of $\varphi_{\mathbf{a}}(I)$ is*

$$\mathsf{HS}(t)=\frac{\det A(t)}{t^{\binom{r}{2}}(1-t)^{k-(n-r)^2}},$$

where $A(t)$ is the $r\times r$ matrix defined by

$$A_{i,j}(t)=\sum_{\ell=0}^{n-\max(i,j)}\binom{n-i}{\ell}\binom{n-j}{\ell}t^\ell.$$

PROOF. In [6, Corollary 1], it is shown that the Hilbert series of $\mathscr{D}\subset\mathbb{K}[V]$ is

$$\mathsf{HS}(t)=\frac{\det A(t)}{t^{\binom{r}{2}}(1-t)^{(2n-r)r}}.$$

Thus the Hilbert Series of $\mathscr{D}$ as an ideal of $\mathbb{K}[X,V]$ is

$$\frac{\det A(t)}{t^{\binom{r}{2}}(1-t)^{(2n-r)r+\mathsf{card}(X)}}=\frac{\det A(t)}{t^{\binom{r}{2}}(1-t)^{(2n-r)r+k}}.$$

Let O be the Zariski open set defined in Proposition 2. Adding to an ideal a linear form which is not a divisor of zero in the quotient ring multiplies the Hilbert series by $(1-t)$. Thus, if $(\mathbf{b},\mathbf{c})\in O$, then the Hilbert series of $\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}})$ is

$$\frac{\det A(t)}{t^{\binom{r}{2}}(1-t)^{k-(n-r)^2}}.$$

Then, applying Lemma 1, the result can be transferred to $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}})$ (for $\mathbf{a}$ in a nonempty Zariski open set O_2). Let G be a Gröbner basis of $\varphi_{\mathbf{a}}(\mathscr{I})$. Then

$$G\cup\{v_{i,j}-\sum_{\ell=1}^{k}\mathfrak{a}_{i,j}^{(\ell)}x_\ell\}_{1\le i,j\le n}$$

is a Gröbner basis of $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}})$ for a grevlex ordering with $V>X$ (i.e. an grevlex ordering such that $v_{i,j}^{(\ell_1,\ell_2)}>x_\ell$ for all i,j,ℓ,ℓ_1,ℓ_2). Consequently, $\mathbb{K}[X]/\varphi_a(\mathscr{I})$ is isomorphic (as $\mathbb{K}$-vector spaces) to $\mathbb{K}[X,V]/\varphi_a(\widetilde{\mathscr{I}})$, thus the Hilbert series of $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}})$ is the same as the Hilbert series of $\varphi_{\mathbf{a}}(\mathscr{I})$. $\square$

3.2 The well-defined and over-determined cases

In this part, $k\le(n-r)^2$, and we still consider the homogeneous MinRank problem. First, we propose a variant of the Fröberg Conjecture [17], which describes the structure of the ideal obtained by adding to $\mathscr{D}$ more than $\dim(\mathscr{D})-1$ generic linear forms $g_{i,j}$ (as defined in Definition 1).

CONJECTURE 1. *We use the same notations as Proposition 2. Let $\mathscr{D}_{\prec(i,j),d}$ denote the vector space of homogeneous polynomials of degree d in $\mathscr{D}_{\prec(i,j)}$. Then there exists a nonempty Zariski open subset O_3 of $\mathbb{K}^{n^2k}\times\mathbb{K}^{n^4}$ such that, if $(\mathbf{b},\mathbf{c})\in O_3$, then $\forall(i,j)\in\{1,\dots,n\}^2,\forall d\in\mathbb{N}$, the linear application*

$$\begin{array}{ccc}\psi_{\mathbf{b},\mathbf{c}}(\mathscr{D}_{\prec(i,j),d}) & \longrightarrow & \psi_{\mathbf{b},\mathbf{c}}(\mathscr{D}_{\prec(i,j),d+1}) \\ f & \longmapsto & f\cdot\psi_{\mathbf{b},\mathbf{c}}(g_{i,j})\end{array}$$

is of maximal rank.

From now on, we use the following notation: for a series $S\in\mathbb{Z}[[t]]$, $[S]$ denotes the series obtained by truncating S at the first null or negative coefficient.

COROLLARY 2. *Under the same conditions as the Conjecture 1, if $(\mathbf{b},\mathbf{c})\in O_3$, then the Hilbert series of $\psi_{\mathbf{b},\mathbf{c}}(\mathscr{D}_{\prec(i,j)}+g_{i,j})$ is*

$$\left[(1-t)\mathsf{HS}_{\psi_{\mathbf{b},\mathbf{c}}(\mathscr{D}_{\prec(i,j)})}(t)\right],$$

PROOF. In order to simplify the notations, I denotes the ideal $\psi_{\mathbf{b},\mathbf{c}}(\mathscr{D}_{\prec(i,j)})$ and I_d denotes the set of polynomials of I of degree d. Let $\times\psi_{\mathbf{b},\mathbf{c}}(g_{i,j})$ denote the multiplication by $\psi_{\mathbf{b},\mathbf{c}}(g_{i,j})$ and let $\mathsf{ann}(\psi_{\mathbf{b},\mathbf{c}}(g_{i,j}))$ be the ideal $\{f\in\mathbb{K}[X,V]: f\psi_{\mathbf{b},\mathbf{c}}(g_{i,j})\in I\}$. Consider the following exact sequence:

$$\begin{array}{r}0\to\mathsf{ann}(\psi_{\mathbf{b},\mathbf{c}}(g_{i,j}))_d\to\mathbb{K}[X,V]_d/I_d\xrightarrow{\times\psi_{\mathbf{b},\mathbf{c}}(g_{i,j})}\mathbb{K}[X,V]_{d+1}/I_{d+1}\to\\ \to\mathbb{K}[X,V]_{d+1}/(I+\psi_{\mathbf{b},\mathbf{c}}(g_{i,j}))_{d+1}\to 0.\end{array}$$

According to Conjecture 1, the dimension of $\mathsf{ann}(\psi_{\mathbf{b},\mathbf{c}}(g_{i,j}))_d$ is equal to $\max(0,\dim(\mathbb{K}[X,V]_d/I_d)-\dim(\mathbb{K}[X,V]_{d+1}/I_{d+1}))$. It is well known that the alternate sum of the dimensions of an exact sequence of vector spaces is 0. Therefore,

$$\begin{array}{l}\dim(\mathbb{K}[X,V]_{d+1}/(I+\psi_{\mathbf{b},\mathbf{c}}(g_{i,j}))_{d+1})\\ =\max(\dim(\mathbb{K}[X,V]_{d+1}/I_{d+1})-\dim(\mathbb{K}[X,V]_d/I_d),0).\end{array}$$

Multiplying this equation by t^{d+1} and summing over $d\in\mathbb{N}$ yields the claimed relation between the Hilbert series. $\square$

THEOREM 4. *If $k<(n-r)^2$, then there exists a nonempty Zariski open subset O_4 of $\mathbb{K}^{n^2k}$ such that if $\mathbf{a}\in O_4$, then the Hilbert series of $\varphi_{\mathbf{a}}(I)$ is*

$$\mathsf{HS}(t)=\left[(1-t)^{(n-r)^2-k}\frac{\det A(t)}{t^{\binom{r}{2}}}\right],$$

where $A(t)$ is the $r\times r$ matrix defined by

$$A_{i,j}(t)=\sum_{\ell=0}^{n-\max(i,j)}\binom{n-i}{\ell}\binom{n-j}{\ell}t^\ell.$$

PROOF. Consider $\widehat{\mathscr{D}}$ the determinantal ideal on which we add only $(2n-r)r+k-1$ generic linear forms:

$$\widehat{\mathscr{D}} = \mathscr{D} + \left\langle \sum_{\ell=1}^{k} \mathfrak{b}_{i,j}^{(\ell)} x_k + \sum_{1\leq \ell_1,\ell_2 \leq n} \mathfrak{c}_{i,j}^{(\ell_1,\ell_2)} v_{\ell_1,\ell_2} \right\rangle_{(i,j)\in S}$$

where $S \subset \{1,\ldots,n\}^2$ and $\mathsf{card}(S) = (2n-r)r+k-1$. Now take $(\mathbf{b},\mathbf{c})$ in the nonempty Zariski open set $O_2 \cap O_3$, (O_2 is defined in Theorem 3, and O_3 is defined in Conjecture 1). Thus the Hilbert Series of $\psi_{\mathbf{b},\mathbf{c}}(\widehat{\mathscr{D}})$ is $\mathsf{HS}(t) = \frac{\det A(t)}{t^{\binom{r}{2}}(1-t)}$. Thus, adding the $n^2-(2n-r)r-k+1$ remaining linear forms, and applying Corollary 2 for each linear form, it is proved that the Hilbert series of $\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}})$ is $\left[(1-t)\left[(1-t)\left[\ldots(1-t)\left[\frac{\det A(t)}{t^{\binom{r}{2}}(1-t)}\right]\right]\right]\right]$. It is easy to prove that if $S \in \mathbb{Z}[[t]]$ is a series such that $S(0) \geq 1$ (which is the case when S is an Hilbert series of an homogeneous ideal), then $[(1-t)[S]] = [(1-t)S]$. Thus the Hilbert series of $\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{D}})$ can be rewritten as $\left[(1-t)^{(n-r)^2-k}\frac{\det A(t)}{t^{\binom{r}{2}}}\right]$.

Finally, by the same argument as in the proof of Theorem 3 (i.e. by using Lemma 1 and then eliminating the variables V), there exists a nonempty Zariski open set $O_4 \subset \mathbb{K}^{n^2k}$ such that, if $a \in O_4$, then the Hilbert Series of $\varphi_{\mathbf{a}}(\mathscr{I})$ is the same. ☐

The *degree of regularity* is a sharp indicator of the complexity of Gröbner basis algorithms. It is the highest degree of the polynomials occurring during the Gröbner basis computation. If I is a 0-dimensional homogeneous ideal, $\mathsf{d_{reg}}$ is precisely the lowest integer such that all monomials of degree $\mathsf{d_{reg}}$ are in I and can be read on the Hilbert series (which is a polynomial):

$$\mathsf{d_{reg}} = 1 + \deg(\mathsf{HS}(t)).$$

Most bounds of the complexity of Gröbner basis algorithms (for instance F_4 [11] or F_5 [12]) are exponential in the degree of regularity. Therefore it is crucial to obtain sharp estimates of d_{reg}.

COROLLARY 3. *Under the same conditions as Theorem 4, the degree of regularity of $\varphi_{\mathbf{a}}(\mathscr{I})$ is*

$$\deg\left(\left[(1-t)^{(n-r)^2-k}\frac{\det A(t)}{t^{\binom{r}{2}}}\right]\right)+1.$$

PROOF. The degree of regularity of a 0-dimensional homogeneous system is equal to the degree of the Hilbert series (given by Theorem 4) of the associated ideal plus 1. ☐

COROLLARY 4. *The degree of regularity of the ideal generated by the minor formulation of a generic well-defined MinRank problem (i.e. $k=(n-r)^2$) is bounded by $\mathsf{d_{reg}} \leq r(n-r)+1$.*

PROOF. According to Corollary 3,

$$\mathsf{d_{reg}} = \deg\left(\left[\frac{\det A(t)}{t^{\binom{r}{2}}}\right]\right)+1 = \deg\left(\frac{\det A(t)}{t^{\binom{r}{2}}}\right)+1.$$

On each row of the matrix $A(t)$, a polynomial with the highest degree is on the diagonal. Moreover, $\deg A_{i,i}(t) = n-i$. Thus

$$\deg(\det A(t)) \leq \sum_{i=1}^{r}(n-i) = nr - \frac{r(r+1)}{2}.$$

Finally $\mathsf{HS}(t) = \frac{\det(A(t))}{t^{\binom{r}{2}}}$, and

$$\begin{array}{rcl}\mathsf{d_{reg}} & = & \deg(\mathsf{HS}(\mathsf{t}))+1\\ & \leq & nr - \frac{r(r+1)}{2} - \frac{r(r-1)}{2} + 1\\ & = & r(n-r)+1. \end{array}$$ ☐

This bound is sharp in practice: if the MinRank instance is generic, then the degree of regularity of the ideal generated by the minors is exactly $r(n-r)+1$.

The affine well-defined and over-determined MinRank problem. In most applications, the MinRank problems occurring are affine. The analysis performed for the homogeneous MinRank problem permits to estimate the complexity of solving MinRank by the minors approach in the 0-dimensional affine case. Indeed, the maximal degree reached during the Gröbner basis computation is upper bounded by the degree of regularity of the ideal generated by the homogeneous parts of highest degree of the minors.

Therefore, the degree of regularity of the minors formulation of a generic affine (n,r,k)-MinRank problem is less or equal than the degree of regularity of the minors formulation of a generic homogeneous (n,r,k)-MinRank (given by Corollary 3). In practice, this bound is sharp: when the MinRank instance is generic, it is an equality.

4. ASYMPTOTIC COMPLEXITY ANALYSIS

In this Section, we estimate the costs of the Gröbner basis computations and of the Algorithm FGLM for generic well-defined ($k=(n-r)^2$) affine MinRank problems.

4.1 The Kipnis-Shamir formulation

The arithmetic complexity of the F_5 Algorithm [12] for computing a grevlex Gröbner basis can be estimated by $O(\mathsf{M}(\mathsf{d_{reg}})^{\omega})$ [2, 3], where $\mathsf{M}(\mathsf{d_{reg}})$ denotes the number of monomials of degree less than or equal to $\mathsf{d_{reg}}$ and ω is the linear algebra constant. According to Theorem 1, in the case of the Kipnis-Shamir modeling, $\mathsf{d_{reg}} \leq \min(k,(n-r)r)+1$. Consequently the complexity is upper bounded by $O\left(\binom{k+r(n-r)+\mathsf{d_{reg}}}{\mathsf{d_{reg}}}^{\omega}\right)$.

In applications, $r'=(n-r)$ is often constant, $k=(n-r)^2$, and we want to estimate the asymptotic complexity when n grows. According to Theorem 1, $\mathsf{d_{reg}} = r'^2+1$ when n is big enough.

A straightforward computation gives

$$\begin{array}{rcl}\binom{k+(n-r')r'+r'^2+1}{r'^2+1}^{\omega} & \underset{n\to\infty}{\sim} & \left(\frac{1}{(r'^2+1)!}\right)^{\omega}(k+nr')^{\omega(r'^2+1)}\\ & = & O(n^{\omega(r'^2+1)}).\end{array}$$

This estimate of the complexity is for standard Gröbner basis Algorithms F_4 and F_5 for homogeneous systems. In [15, Section 6.1], a variant of F_5 dedicated to multi-homogeneous is proposed. The key observation is that the multi-homogeneous structure of the system induces a structure in the matrices occurring in the F_4 and F_5 Algorithms. Consequently, those matrices can be decomposed into smaller matrices, whose row echelon forms can be computed independently. A consequence of this decomposition would be a speed-up and a reduction of the required memory. Since the Kipnis-Shamir modeling has a multi-homogeneous structure, this variant of F_5 could lead to practical improvements. However, so far there is no efficient implementation of this multi-homogeneous variant, and no precise complexity analysis.

4.2 The minors formulation

In this part, we estimate the asymptotic complexity of computing a grevlex Gröbner basis in the well-defined case ($k=(n-r)^2$). In particular, we fix $r'=(n-r)$, and we estimate the arithmetic complexity when n grows. As in Section 4.1, the complexity of the F_5 Algorithm can be estimated by $O(\mathsf{M}(\mathsf{d_{reg}})^{\omega})$.

According to Corollary 4, the complexity is then upper bounded by $O\left(\binom{k+r'(n-r')+1}{r'(n-r')+1}^{\omega}\right)$.

An equivalent when n grows is

$$\binom{k+r'(n-r')+1}{r'(n-r')+1}^{\omega} \underset{n\to\infty}{\sim} \left(\frac{1}{k!}\right)^{\omega}(k+r'n)^{\omega k} = O(n^{\omega r'^2}).$$

One remarks that – in the well-defined case – the complexity bound of the minors approach is slightly better than the complexity bound of the Kipnis-Shamir modeling.

4.3 Complexity of FGLM in the well-defined case

With both modelings, when a grevlex basis is computed in the well-defined case ($k=(n-r)^2$), a change of ordering is required to obtain the lexicographical basis which gives the solutions of the problem. Corollary 1 yields the degree of the ideal (with the Kipnis-Shamir modeling or with the minors modeling). The complexity of FGLM is $O(\deg(I)^3)$, thus we need the asymptotic behaviour of the degree to perform a complexity analysis.

When $r'=n-r$ is constant, applying Corollary 1, we get

$$\deg(I) = \prod_{i=0}^{r'-1}\frac{(n+i)!}{(n-1-i)!}\cdot\prod_{i=0}^{r'-1}\frac{i!}{(r'+i)!} \underset{n\to\infty}{\sim} n^{r'^2}\prod_{i=0}^{r'-1}\frac{i!}{(r'+i)!}.$$

Therefore, the asymptotic complexity of FGLM is $O(n^{3r'^2})$.

5. EXPERIMENTAL RESULTS AND APPLICATIONS

In this Section, $\mathbb{K}$ is the finite field $\mathsf{GF}(65521)$.

Workstation. Experimental results have been obtained with 24 Xeon quadricore processors 3.2 GHz, with 64 GB of RAM.

5.1 Computing the minors

The minors modeling raises questions about how to generate the equations. It is not clear how to compute efficiently all minors of size $r+1$ of a big matrix. For a $n\times n$ matrix, there are $\binom{n}{r+1}^2$ such minors, and each is a polynomial of degree $r+1$ in k variables. For instance, for an affine problem with $\mathbb{K}=\mathsf{GF}(65521)$, $n=11$, $k=9$ and $r=8$, it took 14 days on one CPU (with Maple). Fortunately, this computation can be parallelized: with 120 processes running simultaneously on 24 CPU, the computation lasted 12 hours. The size of the resulting algebraic system is 3466 MB.

For this computation, we used naive algorithms (each determinant was computed independently) but we believe that there is room for improvement by using more sophisticated algorithms.

5.2 The well-defined case

Here, $k=(n-r)^2$ and we consider the ground field $\mathbb{K}=\mathsf{GF}(65521)$. This set of parameters is used in a MinRank-based authentification scheme [7].

Generation of the instances. For $(n,k,r)\in\mathbb{N}^3$, we generate a $n\times n$ matrix $M=(M_{i,j})$ where the $M_{i,j}$ are affine linear forms in k variables: $M_{i,j}=a_{i,j}^{(0)}+\sum_{\ell=1}^{k}a_{i,j}^{(\ell)}x_\ell$, where the $a_{i,j}^{(\ell)}$ are chosen uniformly at random in $\mathsf{GF}(65521)$.

Interpretation of the results. Table 1 describes experimental results, for different values of the triplet (n,r,k). In particular, we consider sets of parameters used in Cryptology for a MinRank-based authentification scheme [7]. The complexity of solving the MinRank problem is then directly related to the security of this cryptosystem. The values in italic font were not computed, but are estimates of the complexity based on the theoretical results from the previous section.

The row "degree" provides the degree of the ideal (i.e. the number of solutions in the algebraic closure) and can be compared with

Chall.	**A**	**B**				**C**
	(6,9,3)	(7,9,4)	(8,9,5)	(9,9,6)	(10,9,7)	(11,9,8)
degree	**980**	**4116**	**14112**	**41580**	**108900**	259545
MH Bézout	8000	42875	175616	592704	1728000	4492125
	Minors					
F_5 time	**1.1s**	**37s**	**935s**	**18122s**	**229094s**	*2570396s*
F_5 mem	**488 MB**	**587 MB**	**1213 MB**	**5048 MB**	**25719MB**	
F_4 Magma	**4.6s**	**142.8s**	**3343.5s**	∞		
$\mathsf{d}_{\mathsf{reg}}$	**10**	**13**	**16**	**19**	**22**	*25*
Nb op.	**21.5**	**25.9**	**29.2**	**32.7**	**35.2**	*40.2*
FGLM time	**1.7s**	**97.2s**	DNF			
	Kipnis-Shamir					
F_5 time	**30s**	**3795s**	**328233s**	∞		
F_5 mem	**407 MB**	**3113 MB**	**58587 MB**			
F_4 Magma	**300s**	**48745s**	∞			
$\mathsf{d}_{\mathsf{reg}}$	**5**	**6**	**7**			
Nb op.	**30.5**	**37.1**	**43.4**	*50.4*	*57.4*	*64.4*
FGLM time	**35s**	**2580s**	∞			

Table 1: Authentification scheme parameters

the multi-homogeneous Bézout bound ("MH Bézout"). The row "F_5 time" (resp. "F_5 mem") gives the time (resp. the memory) needed to compute the grevlex Gröbner basis of the ideal under consideration. The computation is done with the F_5 Algorithm from the FGb package. We also give the time obtained for the same Gröbner basis computations with the implantation of F_4 in Magma2.16, so that experiments can be reproduced. "$\mathsf{d}_{\mathsf{reg}}$" gives the degree of regularity of the ideal. Finally "Nb op." indicates the logarithm (in base 2) of the exact number of arithmetic operations performed during the execution of the F_5 Algorithm, and "FGLM time" provides the running time of FGLM (from the FGb package).

Note that the degree of regularity of the ideal generated by the minors matches the value given in Corollary 4. Moreover, remark that the degree of the ideal is equal to the value provided by Corollary 1.

Looking at the logarithm of the number of arithmetic operations which is growing linearly, it seems clear that, for both formulations, the Gröbner basis computation is polynomial in n when $n-r$ is fixed, as announced in [14] and proved in this paper (Section 4).

We would like to emphasize that the FGLM step costs sometimes more than the DRL Gröbner basis computation. In order to avoid this cost, a possible strategy is to combine the minors approach with an exhaustive search over some variables.

5.3 Solving the challenge C of the Courtois authentification scheme

Solving the challenge C requires to find one solution of a generic affine $(11,9,8)$-MinRank problem which has a particularity: it is known that there is a solution $(x_1,\ldots,x_9)\in\mathsf{GF}(65521)^9$ in the ground field. Therefore we can combine the minor formulation with a partial exhaustive search. To this end, we specialize s variables and solve the corresponding over-determined $(11,9-s,8)$-MinRank problem for all specializations of the s variables. The degree of regularity of the over-determined systems can be estimated with Corollary 3, so the complexity of the complete computation can be approximated. For these systems, the degree of the ideal is 0 or 1. Consequently, a grevlex Gröbner basis is also a lex Gröbner basis and the FGLM Algorithm is no longer required.

Table 2 shows the experimental results for different values of s. The row "$\mathsf{d}_{\mathsf{reg}}$" gives the degree of regularity obtained for each specialization of the s variables. The row "Nb op." gives an estimate of the logarithm in base 2 of total number of operations needed

		$(n=11,k=9-s,r=8)$			
	s	3	2	1	0
Minors	F_5 time		**1594s**	**80255s**	*2570396s*
	F_5 mem		**2400 MB**	**29929 MB**	
	$\mathsf{d_{reg}}$		**10**	**13**	*25*
	Nb op.		**60**	**49.1**	*40.2*
KS	F_5 FGb	**57000s**	∞		
	F_5 mem	**10539 MB**			
	$\mathsf{d_{reg}}$	**7**			
	Nb op.	**88.6**			

Table 2: Challenge C of the Courtois authentification scheme.

to solve the challenge C. It is equal to $\log_2(65521^s \mathsf{OpF_5})$ where $\mathsf{OpF_5}$ is the number of arithmetic operations used by the F_5 Algorithm to solve one $(11, 9-s, 8)$-MinRank problem. The values in italic font were not effectively computed but are given as estimates based on practical and theoretical results.

First of all, we want to emphasize the fact that the degree of regularity of the ideal generated by the minors matches the one deduced from the generic Hilbert series (Corollary 3) in the over-determined case.

According to Table 2, the best practical choice seems to be $s = 1$. In practice, the 65521 computations of the over-determined systems can be parallelized, and the total number of required arithmetic operations ($2^{49.1}$) is quite practical. We estimate to 238 days the time needed to effectively solve this challenge on 64 quadri-core processors. Therefore, the authentification scheme cannot be considered secure anymore with the set of parameters $(n = 11, k = 9, r = 8)$.

Note that it may be possible to compute directly a Gröbner basis of the ideal generated by the minors ($s = 0$). By interpolating the practical results, we give a rough estimate of the complexity of this computation: it would take approximately 29 days (on one CPU). However, it is not clear how much memory would be required, and the FGLM step could be untractable since the degree of the ideal is 259545 (Corollary 1).

6. CONCLUSION

In this paper, we studied two formulations of the MinRank problem from the viewpoint of efficency and practical applications. In particular, the analysis of the ideals generated by the minors gave new information about the intrinsic structure of this problem.

Results from algebraic geometry about determinantal ideals permits to obtain the number of solutions for a generic MinRank problem when $k = (n-r)^2$. This value is important for the study of the complexity of the solving process since it has a direct impact on the complexity of FGLM.

We provided the Hilbert series and an explicit formula for the degree of regularity of the ideal generated by the minors. These information lead to a complexity analysis of the whole Gröbner basis computation. We also proposed a method to break the challenge C of the MinRank authentification scheme faster than any other known approaches. This method is feasible in practice since it requires only 2^{49} arithmetic operations.

Many interesting questions have arisen from this study. First, to be able to apply the minor approach on huge over-determined MinRank instances, algorithms for computing efficiently all the minors of size $r+1$ of a linear matrix are required. Another question is to find how the multi-homogeneous structure of the Kipnis-Shamir formulation can be used to speed-up the computations, and to evaluate precisely its cost. We derived a formula from [15] to bound the degree of regularity of the Kipnis-Shamir modeling. Although this bound is much sharper than any other known bounds, there is still a small gap between it and the real degree of regularity.

7. REFERENCES

[1] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and E. Schost. On the geometry of polar varieties. *Applicable Algebra in Engineering, Communication and Computing*, 21(1):33–83, 2010.

[2] M. Bardet, J. Faugère, and B. Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

[3] M. Bardet, J.-C. Faugère, B. Salvy, and B. Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *Proc. of MEGA*, 2005.

[4] W. Bruns and U. Vetter. *Determinantal rings*. Springer, 1988.

[5] J. Buss, G. Frandsen, and J. Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3):572–596, 1999.

[6] A. Conca and J. Herzog. On the Hilbert function of determinantal rings and their canonical module. *Proceedings of the American Mathematical Society*, pages 677–681, 1994.

[7] N. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. *Lecture notes in computer science*, pages 402–421, 2002.

[8] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Verlag, 1997.

[9] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Springer, 2004.

[10] I. Emiris and J. Canny. Efficient incremental algorithms for the sparse resultant and the mixed volume. *Journal of Symbolic Computation*, 20(2):117–149, 1995.

[11] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4), 1999. *Journal of Pure and Applied Algebra*, 139(1-3):61–88, 1999.

[12] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, page 83. ACM, 2002.

[13] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[14] J.-C. Faugère, F. Levy-dit Vehel, and L. Perret. Cryptanalysis of MinRank. In *Proceedings of the 28th Annual conference on Cryptology: Advances in Cryptology*, page 296. Springer, 2008.

[15] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. *arXiv:1001.4004v1 [cs.SC]*, 2010.

[16] H. Flenner, L. van Gastel, and W. Vogel. *Joins and intersections*, volume 291. Springer, 1991.

[17] R. Fröberg. An inequality for Hilbert series of graded algebras. 1985.

[18] W. Fulton. *Intersection theory*. Springer, 1984.

[19] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. *Lecture Notes in Computer Science*, pages 19–30, 1999.

[20] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *EUROCAL*, volume 162, pages 146–156. Springer, 1983.

[21] A.-V. Ourivski and T. Johansson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38(3):237–246, 2002.