THE COMPLEXITY OF MINRANK

ALESSIO CAMINATA AND ELISA GORLA

Abstract. In this note, we leverage the results of [6] to produce a concise and rigorous proof for the complexity of the generalized MinRank Problem in the under-defined and well-defined case. Our main theorem recovers and extends the main results of [9, 10].

1. Introduction

The MinRank Problem asks to find an element of low rank in a given space of matrices. In its classical formulation, one searches for a matrix whose rank is at most a chosen integer, in a vector space given via a system of generators.

(Classical) MinRank Problem. Let $\Bbbk$ be a field and let m, n, r, k be positive integers. Given as input k matrices $M_1, \ldots, M_k$ of size $m \times n$ with entries in $\Bbbk$, find $x_1, \ldots, x_k \in \Bbbk$ such that the corresponding linear combination satisfies

$$\operatorname{rank}\left(\sum_{i=1}^{k} x_i M_i\right) \leq r.$$

The entries of the matrix $M = \sum_{i=1}^{k} x_i M_i$ are linear polynomials in the variables $x_1, \ldots, x_k$. The following is a natural generalization of the MinRank Problem.

Generalized MinRank Problem. Let $\Bbbk$ be a field and let m, n, r, k be positive integers. Given as input a matrix M of size $m \times n$ with entries in $\Bbbk[x_1, \ldots, x_k]$, compute the set of points in $\Bbbk^k$ where the evaluation of M has rank at most r.

Both of these problems arise naturally within cryptography and coding theory, as well as in numerous other applications. Within multivariate cryptography, the MinRank Problem plays a central role in the cryptanalysis of several systems, including HFE and its variants [14, 1, 5, 18, 7], the TTM Cryptosystem [12], and the ABC Cryptosystem [16, 17]. Within coding theory, the problem of decoding a linear rank-metric code is always an instance of the MinRank Problem, and in some cases it can be modeled as a generalized MinRank Problem, where some entries of the matrix have degree greater than one, see e.g. [15, 11]. Further applications of the generalized MinRank Problem to nonlinear computational geometry, real geometry and optimization, and other problems in symbolic computation are discussed in the introduction of [10].

Following [14], we distinguish the following three situations.

Definition 1.1. A MinRank Problem is *under-defined* if $k > (n-r)(m-r)$, *well-defined* if $k = (n-r)(m-r)$, and *over-defined* if $k < (n-r)(m-r)$.

There are at least three ways of approaching the MinRank Problem: the Kipnis-Shamir modeling [14], the linear algebra search [12], and the minors modeling. We concentrate on the latter. The minors modeling relies on the following observation: A vector $(a_1, \ldots, a_k)$ is a

2010 *Mathematics Subject Classification.* Primary: 94A60, 13P10, 13P15, 13C40, 13P25.

Key words and phrases. MinRank Problem; minors; solving degree; Castelnuovo-Mumford regularity; Gröbner bases; multivariate cryptography; post-quantum cryptography.

We are grateful to an anonymous referee for a detailed reading and comments which helped us improve the clarity of the proof of the main theorem.

solution of the (classical or generalized) MinRank Problem for a matrix M if and only if all minors of size $r+1$ of M vanish at this point. Thus we can find the solutions of the generalized MinRank Problem by solving the polynomial system consisting of all minors of size $r+1$ of M. This is a system of multivariate polynomial equations $\mathcal{F} = \{f_1, \ldots, f_s\}$, so one may attempt to solve it by means of the usual Gröbner bases methods. The complexity of these methods is controlled by the *solving degree* of $\mathcal{F}$, that is the highest degree of polynomials appearing during the computation of a degree reverse lexicographic Gröbner basis of $\mathcal{F}$.

In this paper, we take another look at the complexity of solving the generalized MinRank Problem with the minors modeling. We focus on the under-defined and well-defined situations, which we treat with a unified approach. Notice that no fully provable, general results on the complexity of the over-defined case are currently available.

The results from [6], in combination with classical commutative algebra results, provide us with a simple provable estimate for the complexity of the homogeneous version of the generalized MinRank Problem. As a special case of our main result, we obtain a simple and concise proof of the main results from [9, 10], which avoids lengthy technical computations.

2. Main Results

We fix an infinite field $\Bbbk$ and positive integers m, n, r, k. Without loss of generality, we assume that $n \geq m$ and $r < m$. We focus on the MinRank Problem in the under-defined and well-defined case. We state the results in increasing order of generality.

Theorem 2.1 ([9], Corollary 4)**.** *The solving degree of the minors modeling of a generic classical well-defined square MinRank Problem ($m = n$ and $k = (n-r)^2$) is upper bounded by*

$$\text{solv. deg}(\mathcal{F}) \leq nr - r^2 + 1.$$

Theorem 2.2 ([10], Lemma 18, Corollary 19, Lemma 22, Corollary 23)**.** *Let M be an $m \times n$ matrix whose entries are generic homogeneous polynomials of degree d in $\Bbbk[x_1, \ldots, x_k]$ and assume $k \geq (m-r)(n-r)$. Let $\mathcal{F}$ be the polynomial system of the minors of size $r+1$ of M. Then the solving degree of $\mathcal{F}$ is upper bounded by*

$$\text{solv. deg}(\mathcal{F}) \leq (m-r)(nd - n + r) + 1.$$

The previous theorems recover the main results of [9, 10]. We obtain them as a consequence of our more general Theorem 2.3, by letting $m = n$ and $d_{i,j} = 1$ (Theorem 2.1), or $d_{i,j} = d$ (Theorem 2.2).

We consider an $m \times n$ matrix M, whose entry in position (i, j) is a polynomial of degree $d_{i,j}$ in $\Bbbk[x_1, \ldots, x_k]$, for all i, j. Up to permuting the rows of M, we may assume that $d_{1,1} \leq d_{2,1} \leq \cdots \leq d_{m,1}$. Moreover, assume that the following two conditions hold:

(1) $d_{i,j} > 0$ for all i, j.
(2) $d_{i,j} + d_{h,\ell} = d_{i,\ell} + d_{h,j}$ for all i, j, ℓ, h.

Finally, we assume that the entries of M are generic polynomials. One may think of this assumption as the coefficients of each polynomial being randomly chosen.

Theorem 2.3. *Let M be an $m \times n$ matrix as above and assume $k \geq (m-r)(n-r)$. Let $\mathcal{F}$ be the polynomial system of the minors of size $r+1$ of M. Then the solving degree of $\mathcal{F}$ is upper bounded by*

$$\text{solv. deg}(\mathcal{F}) \leq (m-r)\sum_{i=1}^{r} d_{i,i} + \sum_{i=r+1}^{m}\sum_{j=r+1}^{n} d_{i,j} - (m-r)(n-r) + 1.$$

Proof. Under our assumptions, the homogenizations of the $(r+1)$-minors of M are the $(r+1)$-minors of the matrix obtained from M by homogenizing its entries. Therefore, we may assume without loss of generality that the entries of M are generic homogeneous polynomials. The main result of [6, Section 3.3] implies that

$$\text{solv. deg}(\mathcal{F}) \leq \operatorname{reg} I,$$

where I is the ideal generated by the polynomials of $\mathcal{F}$ and $\operatorname{reg} I$ denotes the Castelnuovo-Mumford regularity of I. We can compute it as follows.

First, since the polynomials of M are generic and the matrix M is homogeneous, by combining Eagon-Northcott's Theorem [8, Theorem 3] with [4, Theorem 2.5] one obtains that the quotient ring $S = \Bbbk[x_1, \ldots, x_k]/I$ is Cohen-Macaulay and the ideal I has codimension $\operatorname{codim}(I) = (m-r)(n-r)$. Recall that the codimension of a homogeneous ideal in a polynomial ring $\Bbbk[x_1, \ldots, x_k]$ is the difference between k and the Krull dimension of the quotient of the polynomial ring by the ideal.

Now consider the quotient ring $T = \Bbbk[X]/I_{r+1}(X)$, where $X = (x_{i,j})$ is a matrix of size $m \times n$ whose entries are distinct variables, $\deg(x_{i,j}) = d_{i,j}$, $\Bbbk[X]$ is the polynomial ring over $\Bbbk$ with variables the entries of X, and $I_{r+1}(X)$ denotes the ideal generated by the minors of size $r+1$ of X. By [13, Corollary 4] $\operatorname{codim}(I_{r+1}(X)) = (m-r)(n-r)$, see also [3, Theorem 3.7.1].

Since $\operatorname{codim}(I) = \operatorname{codim}(I_{r+1}(X))$, by [4, Theorem 3.5] a minimal graded free resolution of S is obtained from a minimal graded free resolution of T by substituting $x_{i,j}$ with the entry of M in position (i, j), for all i and j. In particular

$$\operatorname{reg}_{\Bbbk[x_1,\ldots,x_k]}(S) = \operatorname{reg}_{\Bbbk[X]}(T),$$

where $\operatorname{reg}(S) = \operatorname{reg}(I) - 1$ and $\operatorname{reg}(T) = \operatorname{reg}(I_{r+1}(X)) - 1$. Moreover, since T is Cohen-Macaulay, we can express its regularity in terms of its a-invariant (see [3, Definition 3.6.13]) and of the codimension of $I_{r+1}(X)$. We have

$$\operatorname{reg}(T) = a(T) - a(\Bbbk[X]) - \operatorname{codim}(I_{r+1}(X)) = a(T) + \sum_{i=1}^{m}\sum_{j=1}^{n} d_{i,j} - (m-r)(n-r),$$

where a denotes the a-invariant, the first equality follows from [3, Examples 3.6.15 b)], and the second from [3, Examples 3.6.15 a)] and $\operatorname{codim}(I_{r+1}(X)) = (m-r)(n-r)$. By [2, Corollary 1.5]

$$a(T) = -r\sum_{i=1}^{m} d_{i,i} - \sum_{i=1}^{r}\sum_{j=m+1}^{n} d_{i,j},$$

where $d_{i,j} = e_i + f_j$ in the notation of [2]. Putting everything together we obtain

$$\begin{aligned}\operatorname{reg}(I) = \operatorname{reg}(S) + 1 &= a(T) + \sum_{i=1}^{m}\sum_{j=1}^{n} d_{i,j} - (m-r)(n-r) + 1 \\ &= (m-r)\sum_{i=1}^{r} d_{i,i} + \sum_{i=r+1}^{m}\sum_{j=r+1}^{n} d_{i,j} - (m-r)(n-r) + 1,\end{aligned}$$

which proves the statement. □

Remark 2.4. Theorem 2.3 analyzes the under-defined and well-defined situations. In the over-defined situation, assume that k is sufficiently small and that $d_{i,j} = 1$ for all i and j. Then the minors of size $r+1$ of M generate the maximal ideal to the power $r+1$. In particular,

$$\text{solv. deg}(\mathcal{F}) = r + 1.$$

Remark 2.5. The word "generic" used in the statements is a technical term from algebraic geometry, which means "there exists a nonempty open set" of polynomials for which the result holds. This is exactly the same use of generic as in [9, 10]. We stress that the genericity assumption is often essential to a type of approach that uses algebraic geometry. To the extent of our knowledge, this assumption appears also in all the previous works that use similar methods.

Usually one thinks of a generic property as a property that holds for "almost every point" of the ambient space. In order for this intuition to be true, however, one needs to work over an infinite field, or at least over a large enough field extension of $\Bbbk$ (if $\Bbbk$ is a finite field). In

fact, a nonempty open set over an infinite field may contain only a few points, or even no point, over a given finite subfield.

One may therefore be lead to think that theorems with a genericity assumption are of little use over finite fields. This is however not the case. In fact, if an open set is nonempty over the algebraic closure, then it will contain most points over a large enough (but finite) field extension of $\Bbbk$. Therefore, if we are willing to take a field extension, we have that a generic property holds for most points.

In addition, any open set is defined by a finite number of conditions. Whenever one can explicitly describe them, one can check whether any given point (including points over any finite field) satisfies them, which is equivalent to checking whether the point belongs to the open set. These conditions may always be expressed as a set of polynomial equations which should not all vanish on the point in question. Sometimes, when the polynomials are difficult to describe explicitly or involve a large number of terms, one may choose to describe the conditions as equivalent properties that can be checked directly. E.g., in the proof of Theorem 2.3, for any minor of the matrix M one can check whether the homogenization of the minor is equal to the corresponding minor of the matrix obtained from M by homogenizing its entries. This condition can be expressed also as a polynomial in the coefficients of the entries of M, namely the condition on the homogenization holds if and only if the polynomial does not vanish on the coefficients of the entries of M. In particular, whenever we are able to explicitly state the genericity conditions, one can directly check whether a given system of equations satisfies the genericity properties, independently of the field of definition (which can also have small cardinality).

In the next theorem we explicitly state the genericity conditions of Theorem 2.3, so that they can be checked directly over any finite field. This provides a version of Theorem 2.3 over finite fields.

Theorem 2.6. *Let $\Bbbk$ be a finite field. Let M be an $m \times n$ matrix whose entry in position (i, j) is a polynomial of degree $d_{i,j} > 0$ in $\Bbbk[x_1, \dots, x_k]$, for all i, j. Assume that $k \geq (m-r)(n-r)$, $d_{1,1} \leq d_{2,1} \leq \cdots \leq d_{m,1}$, and $d_{i,j} + d_{h,\ell} = d_{i,\ell} + d_{h,j}$ for all i, j, ℓ, h. Let $\mathcal{F}$ be the polynomial system of the minors of size $r+1$ of M. Let t be a new variable, let M^h be the matrix obtained from M by homogenizing its entries with respect to t, and let $J = I_{r+1}(M^h)$. Suppose that $\operatorname{codim}(J) = (m-r)(n-r)$, that $t \nmid 0$ modulo J, and that the homogenization with respect to t of each $(r+1)$-minor of M equals the corresponding $(r+1)$-minor of M^h. Then the solving degree of $\mathcal{F}$ is upper bounded by*

$$\text{solv. deg}(\mathcal{F}) \leq (m-r) \sum_{i=1}^{r} d_{i,i} + \sum_{i=r+1}^{m} \sum_{j=r+1}^{n} d_{i,j} - (m-r)(n-r) + 1.$$

References

[1] Luk Bettale, Jean-Charles Faugère, Ludovic Perret, *Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic*, Designs, Codes and Cryptography vol. 69, no. 1, 1–52, 2013.

[2] Winfried Bruns, Jürgen Herzog, *On the computation of a-invariants*, Manuscripta Mathematica vol. 77, pp. 201–213, 1992.

[3] Winfried Bruns, Jürgen Herzog, *Cohen-Macaulay rings. Revised edition*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, 1998.

[4] Winfried Bruns, Udo Vetter, *Determinantal Rings*, Lecture Notes in Mathematics, 1327, Springer-Verlag, Berlin, 1988.

[5] Daniel Cabarcas, Daniel Smith-Tone, Javier A. Verbel, *Key Recovery Attack for ZHFE*, Post-quantum cryptography, 289–308, Lecture Notes in Computer Science, 10346, Springer, Cham, 2017.

[6] Alessio Caminata, Elisa Gorla, *Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra*, preprint arXiv:1706.06319.

[7] Jintai Ding, Ray Perlner, Albrecht Petzoldt, Daniel Smith-Tone, *Improved cryptanalysis of HFEv$^-$ via projection*, Post-quantum cryptography, 375–395, Lecture Notes in Computer Science, 10786, Springer, Cham, 2018.

[8] John A. Eagon, Douglas G. Northcott, *Ideals Defined by Matrices and a Certain Complex Associated with Them*, Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, vol. 269, n. 1337, pp. 188–204 , 1962.
[9] Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer, *Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology*, Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ISSAC '10, pp. 257–264, Munich, Germany, 2010.
[10] Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer, *On the Complexity of the Generalized MinRank Problem*, Journal of Symbolic Computation, vol. 55, pp. 30–58, 2013.
[11] Elisa Gorla, Felice Manganiello, Joachim Rosenthal, *An algebraic approach for decoding spread codes*, Advances in Mathematics of Communications, vol. 6, n. 4, pp. 443–466, 2012.
[12] Louis Goubin, Nicolas T. Courtois, *Cryptanalysis of the TTM Cryptosystem*, Advances in Cryptology, Proceedings of ASIACRYPT 2000, Lecture Notes in Computer Science, vol. 1976, Springer-Verlag, pp. 44–57, 2000.
[13] Melvin Hochster, John A. Eagon, *Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci*, American Journal of Mathematics, vol. 93, n. 4, pp. 1020–1058, 1971.
[14] Aviad Kipnis, Adi Shamir, *Cryptanalysis of the HFE public key cryptosystem*, Advances in Cryptology, Proceedings of Crypto '99, LNCS no. 1666, Springer-Verlag, pp. 19–30, 1999.
[15] Felice Manganiello, Elisa Gorla, Joachim Rosenthal, *Spread codes and spread decoding in network coding*, Proceedings of the IEEE International Symposium on Information Theory – ISIT, 881–885, 2008.
[16] Dustin Moody, Ray Perlner, Daniel Smith-Tone, *An asymptotically optimal structural attack on the ABC multivariate encryption scheme*, Post-quantum cryptography, 180–196, Lecture Notes in Computer Science, 8772, Springer, Cham, 2014.
[17] Dustin Moody, Ray Perlner, Daniel Smith-Tone, *Improved attacks for characteristic-2 parameters of the cubic ABC simple matrix encryption scheme*, Post-quantum cryptography, 255–271, Lecture Notes in Computer Science, 10346, Springer, Cham, 2017.
[18] Jeremy Vates, Daniel Smith-Tone, *Key recovery attack for all parameters of HFE⁻*, Post-quantum cryptography, 272–288, Lecture Notes in Computer Science, 10346, Springer, Cham, 2017.

Alessio Caminata, Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, CH-2000 Neuchâtel, Switzerland
Email address: alessio.caminata@unine.ch

Elisa Gorla, Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, CH-2000 Neuchâtel, Switzerland
Email address: elisa.gorla@unine.ch