THE COMPLEXITY OF MINRANK

ALESSIO CAMINATA AND ELISA GORLA

Abstract. In this note, we leverage the results of [CG19] 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 [FSS10, FSS13].

1. Introduction

The MinRank Problem asks to find an element of least rank in a given space of matrices. In its classical formulation, one searches for a matrix of minimum rank 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 $M_1, \ldots, M_k$ 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 with entries in $\Bbbk[x_1, \ldots, x_k]$, compute the set of points in $\Bbbk^k$ at which 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 [KS99, BFP13, CSV17, VS17, DPPS18], the TTM Cryptosystem [GC00], and the ABC Cryptosystem [MPS14, MPS17]. Within coding theory, the problem of decoding a linear rank-metric code is an instance of the classical MinRank Problem.

Following [KS99], 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-determined* if $k < (n-r)(m-r)$.

There are at least two ways of approaching the MinRank Problem: the *Kipnis-Shamir modeling* introduced in [KS99] and the *minors modeling*. We concentrate on the second one.

The minors modeling relies on the following observation: A vector $(a_1, \ldots, a_k)$ is a solution of the (classic 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 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

---

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.

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.

In this paper, we take another look at the complexity of solving the MinRank Problem. 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-determined case are currently available.

The results from [CG19], 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. More generally, Theorem 2.5 holds in the situation when the minors of the matrix obtained by homogenizing the entries of M are the homogenization of the minors of M. As a special case of our main result, we obtain a simple and concise proof of the main results from [FSS10, FSS13], which avoids lengthy technical computations.

2. Main Results

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

Theorem 2.1. *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*

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

Theorem 2.2. *Let M be an $m \times n$ matrix whose entries are generic linear polynomials in $\Bbbk[x_1, \dots, x_k]$ 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*

$$\operatorname{solv.deg}(\mathcal{F}) \leq k - mn + mr - r^2 + 1.$$

Theorem 2.3. *Let M be an $m \times n$ matrix whose entries are generic homogeneous polynomials of degree d in $\Bbbk[x_1, \dots, x_k]$ 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*

$$\operatorname{solv.deg}(\mathcal{F}) \leq k - mn + mr + (1-d)rn - r^2 + 1.$$

Remark 2.4. 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 results hold. This is exactly the same use of generic as in [FSS10, FSS13].

The previous theorems recover the main results of [FSS10, FSS13]. We obtain them as a consequence of our more general Theorem 2.5, by letting $d_{i,j} = 1$ (Theorems 2.1 and 2.2) and $d_{i,j} = d$ (Theorem 2.3).

We consider an $m \times n$ matrix M, whose entry in position (i, j) is a polynomial of degree $d_{i,j}$ in $\Bbbk[x_1, \dots, x_k]$, for all i, j. Up to permuting rows and columns, 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 2.5. *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*

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

Proof. Notice that, because of the assumption on the degrees of the entries of M, 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 [CG19, Section 3.3] implies that

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

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, observe that since the polynomials of M are generic and the matrix M is homogeneous, the quotient ring $S = \Bbbk[x_1, \ldots, x_k]/I$ is Cohen-Macaulay of Krull dimension $\dim(S) = k - (m-r)(n-r)$ by Eagon-Northcott's Theorem [EN62]. Moreover by [BH98, Examples 3.6.15], we have $\operatorname{reg}(S) = a(S) + \dim(S)$, where $a(S)$ denotes the a-invariant of S. By [BH92, Corollary 1.5], this is given by

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

where $d_{i,j} = e_i + f_j$ in the notation of [BH92]. Finally, putting everything together we obtain

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

□

References

[BFP13] Luk Bettale, Jean-Charles Faugère, Ludovic Perret, *Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic*, Des. Codes Cryptogr. vol. 69, no. 1, 1–52, 2013.

[BH92] Winfried Bruns, Jürgen Herzog, *On the computation of a-invariants*, Manuscripta Mathematica vol. 77, pp. 201–213, 1992.

[BH98] Winfried Bruns, Jürgen Herzog, *Cohen-Macaulay rings. Revised edition*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, 1998.

[CSV17] Daniel Cabarcas, Daniel Smith-Tone, Javier A. Verbel, *Key Recovery Attack for ZHFE*, Post-quantum cryptography, 289–308, Lecture Notes in Comput. Sci., 10346, Springer, Cham, 2017.

[CG19] Alessio Caminata, Elisa Gorla, *Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra*, preprint arXiv:1706.06319.

[DPPS18] Jintai Ding, Ray Perlner, Albrecht Petzoldt, Daniel Smith-Tone, *Improved cryptanalysis of HFEv⁻ via projection*, Post-quantum cryptography, 375–395, Lecture Notes in Comput. Sci., 10786, Springer, Cham, 2018.

[EN62] 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.

[FSS10] 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.

[FSS13] 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.

[GC00] 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.

[KS99] 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.

[MPS14] 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 Comput. Sci., 8772, Springer, Cham, 2014.

[MPS17] 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 Comput. Sci., 10346, Springer, Cham, 2017.

[VS17] Jeremy Vates, Daniel Smith-Tone, *Key recovery attack for all parameters of HFE$^-$*, Post-quantum cryptography, 272–288, Lecture Notes in Comput. Sci., 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