From:	[redacted]
To:	Perlner, Ray A. (Fed)
Subject:	MinRank
Date:	Friday, July 21, 2017 11:50:16 AM
Attachments:	GCMR_RP_DCST_article.pdf

Here it is. The argument is just fine and correct as it is in the homogeneous case. (This is good since Hilbert regularity is only defined for homogeneous ideals.)

Cheers,
Daniel

The Generic Complexity of MinRank[*]

Ray Perlner[†] and Daniel Smith-Tone[‡]

Abstract. The MinRank problem is the basis for much of our understanding of the complexity of solving large systems of structured multivariate quadratic equations. In this article we derive an exact upper bound on the complexity of quite overdetermined instances of MinRank that doesn't depend on any heuristic. Such systems with a low MinRank are effectively the only ones possible in multivariate cryptography, thus the complexity bound has practical value.

Key words. MinRank, Hilbert Series, Hilbert Regularity, Rank Defect

AMS subject classifications. 68Q25, 96A60

1. Introduction.

The MinRank problem has emerged as a central technique in the resolution of large systems of structured multivariate equations. Examples of practical instances of systems of equations solvable by way of MinRank include many cryptanalyses of multivariate public key cryptosystems, see, for example, [6, 1, 8, 7, 9, 2, 5]. There is thus tremendous practical value to the effective computation of MinRank.

Previous work investigating the complexity of the MinRank problem includes [3]. The article addresses the general problem, but the most practically important case— practical in the sense that the result is relevant to cryptanalytic problems— is solved only under a conjecture related to the Fröberg conjecture of [4]. Furthermore, the calculation of the complexity is cumbersome, consuming much effort and space in articles such as [1, 2].

We define a category of overdefined MinRank instances, called *superdefined*. This category includes the vast majority of MinRank instances relevant to cryptanalyses of multivariate public key cryptosystems, and in particular, all of the examples cited above. We provide an explicit closed form upper bound on the complexity of superdefined instances of MinRank free from any qualifying assumptions or conjectures. In particular, we compute the exact Hilbert regularity of such MinRank systems. Thus, the complexity of such MinRank calculations can be derived in constant time.

2. The MinRank Problem.

Definition 1. *The MinRank problem with parameters (n, r, k) over a field $\mathbb{K}$ is the problem of constructing with input $\mathbf{M}_1, \ldots, \mathbf{M}_k \in \mathcal{M}_{n\times n}(\mathbb{K})$ a nonzero $\mathbb{K}$-linear combination satisfying:*

$$Rank\left(\sum_{i=1}^{k} a_i \mathbf{M}_i\right) \leq r.$$

The complexity of the MinRank problem in general is clearly bounded by the complexity in the case that the minimum rank of any nonzero $\mathbb{K}$-linear combination is exactly r; thus, we

---

[*]Submitted to the editors DATE.

[†]National Institute of Standards and Technology, Gaithersburg, MD (ray.perlner@nist.gov).

[‡]National Institute of Standards and Technology, Gaithersburg, MD & Department of Mathematics, University of Louisville, Louisville, KY (daniel.smith@nist.gov).

generally assume that the nonzero matrix of minimum rank in the span of the $\mathbf{M}_i$ has rank exactly r.

One may consider the matrix

$$\overline{\mathbf{M}} = \sum_{i=1}^{k} t_i \mathbf{M}_i,$$

whose entries are in $\mathbb{K}[T] = \mathbb{K}[t_1, \ldots, t_k]$. The Kipnis-Shamir modeling of this MinRank problem, see [6] constructs a basis for the right kernel of $\overline{\mathbf{M}}$ of the form

$$\mathbf{K} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & 1 \\ v_{1,1} & v_{1,2} & \cdots & v_{1,n-r} \\ \vdots & \vdots & \ddots & \vdots \\ v_{r,1} & v_{r,2} & \cdots & v_{r,n-r} \end{bmatrix}$$

using $r(n-r)$ new variables $v_{i,j}$. Then the relation $\overline{\mathbf{M}}\mathbf{K} = \mathbf{0}_{n\times n-r}$ produces $n(n-r)$ equations in $k + r(n-r)$ variables in the polynomial ring $\mathbb{K}[T, V] = \mathbb{K}[t_1, \ldots, t_k, v_{1,1}, \ldots, v_{r,n-r}]$. Under the condition that for no fixed nonzero $(t_1, \ldots, t_k)$ is the rank of $\overline{\mathbf{M}}$ less than r, the representation of $\mathbf{K}$ in column echelon form is unique, if existant; thus, the solution space is zero dimensional for all nonzero $(t_1, \ldots, t_k)$. We may therefore link the under and overdetermination of the MinRank problem to that of the corresponding Kipnis-Shamir modeling. Consequently, we define a MinRank problem to be *underdetermined* if $k > (n-r)^2$, *well-determined* if $k = (n-r)^2$ and *overdetermined* if $k < (n-r)^2$.

3. Minors Modeling in the General Case.

One approach to the solution of the MinRank problem is known as minors modeling. Let I be the ideal in $\mathbb{K}[T]$ generated by the $(r+1) \times (r+1)$ minors of $\overline{\mathbf{M}}$. Any element of $V(I) \cap \mathbb{K}^k$ is clearly a solution to the MinRank problem over $\mathbb{K}$.

The number of $(r+1) \times (r+1)$ minors in $\overline{\mathbf{M}}$ is $\binom{n}{r+1}^2$; however, since every minor is homogeneous of degree $r+1$ and there are only $\binom{k+r}{r+1}$ degree $r+1$ monomials, there can be at most

$$q = \min\left(\binom{k+r}{r+1}, \binom{n}{r+1}^2\right)$$

linearly independent generators of I. For MinRank instances with $(n-r)^2 < q$, these generators are algebraically dependent.

In the following, we focus on the overdetermined case $k < (n-r)^2$. In [3, Corollary 4], the Hilbert regularity of I is shown to be bounded by $r(n-r)+1$ via a derivation of the Hilbert Series of $\mathbb{K}[T]/I$ obtained with the aid of a variant of the Fröberg Conjecture. In many applications it has been shown that the regularity is $r+1$ via the same cumbersome analysis, see [1, 2], for example.

Among these overdetermined instances of MinRank is a special class, in which $q = \binom{k+r}{r+1}$. We refer to such instances as *superdetermined*. (If we consider the symmetric MinRank problem, in which the matrices are all symmetric, then we say that the instance is superdetermined if $\binom{k+r}{r+1} \leq \binom{n}{r+1}^2/2$). In particular, the instances of MinRank arising in cryptography, which we may always consider to be symmetric instances, are all superdetermined. This is due to the fact that the hard instances of multivariate quadratic systems of equations have a number of equations proportional to the number of variables whereas a system is superdetermined merely if the number of equations k is bounded by a quadratic function of the number of variables n, as proven in the following proposition.

Proposition 1. *A MinRank problem with parameters (n, r, k) over the field $\mathbb{K}$ is superdetermined if $k \leq \frac{(n-r)^2}{r+1} - r$.*

Proof. Let $k \leq \frac{(n-r)^2}{r+1} - r$. First, we note that

$$2(r+1)!^2\binom{k+r}{r+1} = 2(r+1)!(k+r)(k+r-1)\cdots k \leq 2(r+1)!(k+r)^{r+1}.$$

Next, since $2(r+1)! \leq (r+1)^{r+1}$ when $r \geq 1$, we have that

$$2(r+1)!^2\binom{k+r}{r+1} \leq \left[(r+1)(k+r)\right]^{r+1}.$$

Since $k \leq \frac{(n-r)^2}{r+1} - r$, then

$$(r+1)(k+r) \leq (n-r)^2,$$

and so

$$\left[(r+1)(k+r)\right]^{r+1} \leq (n-r)^{2(r+1)}$$

Since $(n-r)^{2(r+1)} < n^2(n-1)^2\cdots(n-r)^2 = (r+1)!^2\binom{n}{r+1}^2$, we obtain

$$2\binom{k+r}{r+1} < \binom{n}{r+1}^2.$$ ■

A generic superdetermined MinRank instance has a straightforward structure. We derive the exact Hilbert regularity for generic superdetermined systems.

Theorem 1. *Let $(\mathbf{M}_1, \ldots, \mathbf{M}_k)$ be a generic superdetermined instance of MinRank with parameters (n, r, k) over the field $\mathbb{K}$. Let $\overline{\mathbf{M}} = \sum_{i=1}^k t_i\mathbf{M}_i \in \mathcal{M}_{n\times n}(\mathbb{K}[T])$. Let I be the ideal generated by the $r+1 \times r+1$ minors of $\overline{\mathbf{M}}$. Then the Hilbert Series of $\mathbb{K}[T]/I$ is*

$$HS(t) = \sum_{d=0}^{r}\binom{k+d-1}{d}t^d.$$

Consequently, the Hilbert regularity of I is $r+1$.

Proof. Consider $\mathcal{A} = \mathbb{K}[T]$ as a graded algebra,

$$\mathcal{A} = \bigoplus_{d\geq 0}\mathcal{A}_d,$$

graded by total degree. Since there are $\binom{k+r}{r+1}$ monomials of total degree $r+1$ and the linear span of the minors of a generic superdetermined MinRank instance is $\binom{k+r}{r+1}$ dimensional, there is a set of $\binom{k+r}{r+1}$ minors of $\overline{\mathbf{M}}$ that forms a basis of $\mathcal{A}_{r+1}$. Thus the homogeneous ideal I can be written

$$I \approx \mathbf{0} \oplus \cdots \oplus \mathbf{0} \oplus \mathcal{A}_{r+1} \oplus \mathcal{A}_{r+2} \oplus \cdots .$$

Thus, the quotient $\mathbb{K}[T]/I$ as a graded algebra satisfies

$$\mathbb{K}[T]/I \approx \bigoplus_{d=0}^{r} \mathcal{A}_d.$$

Since $\dim_{\mathbb{K}}(\mathcal{A}_d) = \binom{k+d-1}{d}$ for $0 \leq d \leq r$— with the convention that $\binom{0}{0} = 1$— the Hilbert Series of $\mathbb{K}[T]/I$ is

$$HS(t) = \sum_{d=0}^{r} \binom{k+d-1}{d} t^d.$$

Since the Hilbert Series is a polynomial of degree r, the Hilbert regularity is $r+1$. ■

4. Relevance of the Superdetermined Case to Multivariate Cryptography.

The MinRank problem with parameters (n, r, k) typically occurs in cryptosystems where the public key is a system of k quadratic equations in n variables. While solving the MinRank problem typically leads to a key recovery, these cryptosystems can also be attacked by directly solving the system of k equations for the n variables, resulting in either a signature forgery or a plaintext recovery.

One strategy for solving this system of quadratic equations is to convert it into a system of degree-d equations and then linearly solve for all degree-d monomials in terms of lower degree polynomials. Multiplying each of the k quadratic equations by each of the $\binom{n+d-3}{d-2}$ linearly independent degree-$(d-2)$ monomials results in $k\binom{n+d-3}{d-2}$ equations. This method of solving succeeds with high probability when this number of equations exceeds the number of linearly independent degree-d monomials, $\binom{n+d-1}{d}$, due to the fact that nontrivial syzygies reduce the number of monomials required at degree d in proportion to the number of equations at degree d which are linearly dependent due to these syzygies. This inequality is satisfied when

$$k \geq \frac{(n+d-1)(n+d-2)}{d(d-1)}.$$

In order for the complexity of MinRank to be cryptographically interesting we require that the MinRank attack be no more expensive than the direct attack. This condition implies the inequality

$$\binom{n+d-1}{d} \geq \binom{k+r}{r+1}.$$

Since a system of equations where $k < n$ may be solved with high probability, by first guessing the value of $n-k$ variables and then directly solving, we may assume WLOG that $k \geq n$. Thus, minrank is only cryptographically interesting when $d \geq r+1$. In order for this to be true, we require:

$$k < \frac{(n+r-1)(n+r-2)}{r(r-1)}.$$

In combination with Proposition 1, this relation provides a sufficient condition on n and r for all cryptographically interesting instances of the MinRank problem with n variables and rank r to be superdetermined:

$$\frac{(n+r-1)(n+r-2)}{r(r-1)} \leq \frac{(n-r)^2}{r+1} - r.$$

Asymptotically, this condition is met for $1+\sqrt{2} < r < \frac{n}{2}$. There are no cryptographically interesting instances where $r \geq \frac{n}{2}$ since $d < \frac{5}{2}+\sqrt{n} < \frac{n}{2}+1$ for all but the very smallest values of n. The above considerations rule out cryptographically interesting, but not superdetermined, instances of MinRank with $r > 2$ and $n > 25$. For reference, multivariate systems used in cryptography typically have $n \geq 40$. A cryptosystem which could be attacked as a MinRank instance with $r = 2$ would have an attack complexity which is polynomial in the key size with degree less than or equal to $\frac{3\omega}{2}$, where ω is the linear algebra constant. For any reasonable security level, such a cryptosystem would be extremely inefficient. Thus, cryptographically significant instances of the MinRank problem are all superdetermined.

5. Conclusion.

The seminal article [3] directly addresses the complexity of the MinRank problem and provides a general but computationally tedious solution. Since the above work is most often cited in reference to applications in cryptography, it is reasonable to consider whether there is a better formula for cryptographically interesting instances.

We provide such a formula, requiring zero calculation. For multivariate cryptosystems for which the MinRank attack is the most efficient, the Hilbert regularity of the MinRank system is $r+1$ where the target rank is r. Thus the complexity of such MinRank instances is $\mathcal{O}(\binom{k+r+1}{r+1}^{\omega}) = \mathcal{O}(k^{(r+1)\omega})$, where ω is the linear algebra constant.

REFERENCES

[1] L. Bettale, J. Faugère, and L. Perret, *Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic*, Des. Codes Cryptography, 69 (2013), pp. 1–52, https://doi.org/10.1007/s10623-012-9617-2, http://dx.doi.org/10.1007/s10623-012-9617-2.

[2] D. Cabarcas, D. C. Smith-Tone, and J. Verbel, *An attack on zhfe*, PQCRYPTO 2017, LNCS, 10346 (2017).

[3] J. Faugère, M. S. E. Din, and P. Spaenlehauer, *Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology*, in Symbolic and Algebraic Computation, International Symposium, ISSAC 2010, Munich, Germany, July 25-28, 2010, Proceedings, W. Koepf, ed., ACM, 2010, pp. 257–264, https://doi.org/10.1145/1837934.1837984, http://doi.acm.org/10.1145/1837934.1837984.

[4] R. Fröberg, *An inequality for Hilbert series of graded algebras*, Math. Scand., 56 (1985), pp. 117–144.

[5] L. Goubin and N. Courtois, *Cryptanalysis of the ttm cryptosystem*, in ASIACRYPT, T. Okamoto, ed., vol. 1976 of Lecture Notes in Computer Science, Springer, 2000, pp. 44–57.

[6] A. Kipnis and A. Shamir, *Cryptanalysis of the HFE public key cryptosystem by relinearization*, Advances in Cryptology - CRYPTO 1999, Springer, 1666 (1999), p. 788.

[7] D. Moody, R. Perlner, and D. C. Smith-Tone, *Improved attacks for characteristic-2 parameters of the cubic abc simple matrix encryption scheme*, PQCRYPTO 2017, LNCS, 10346 (2017).

[8] D. Moody, R. A. Perlner, and D. Smith-Tone, *An asymptotically optimal structural attack on the ABC multivariate encryption scheme*, in Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings, M. Mosca, ed., vol. 8772 of Lecture Notes in Computer Science, Springer, 2014, pp. 180–196, https://doi.org/10.1007/978-3-319-11659-4_11, http://dx.doi.org/10.1007/978-3-319-11659-4_11.

[9] J. Vates and D. C. Smith-Tone, *Key recovery attack for all parameters of hfe-*, PQCRYPTO 2017, LNCS, 10346 (2017).