From: Perlner, Ray (Fed)
To: Smith-Tone, Daniel (Fed)
Subject: RE: MinRank Paper
Date: Friday, May 19, 2017 5:15:00 PM
Attachments: GCMR_RP_DCST.tex

Here are my edits. I added the requested paragraph. I decided not to duplicate the list of references for examples of MinRank attacks, since such a list appeared earlier in your intro. I did add to the list the attack on TTM (which is similar to the attack used to set parameters for Rainbow.)

I also reworded the last paragraph in section 2 for clarity and I added the word “nonzero’ to definition 1.

From: Smith-Tone, Daniel (Fed)
Sent: Thursday, May 18, 2017 5:29 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: MinRank Paper

Here are the files for the MinRank paper. I don’t think that it needs much more. I put a note for a paragraph that maybe you can add about the need for n~m. Maybe you can find a reference or two to make it look solid. Then, please check the math and make sure I’m not crazy. Then we can try to find a reasonable journal in algebraic geometry to send it to.

Cheers,
Daniel

```
\documentclass{article}

\usepackage{amssymb,amsmath,authblk,amsthm}
\usepackage{mathtools}
\usepackage{color}
\setcounter{tocdepth}{3}
\usepackage{graphicx}
\usepackage[all]{xy}
\usepackage{textcomp}

\usepackage{url}
\urldef{\mailsa}\path|daniel.smith@nist.gov|
\urldef{\mailsb}\path|ray.perlner@nist.gov|
\newcommand{\keywords}[1]{\par\addvspace\baselineskip
\noindent\keywordname\enspace\ignorespaces#1}


%==============Definitions=========================


\newcommand{\bdf}{\begin{definition}}
\newcommand{\edf}{\end{definition}}
\newcommand{\beq}{\begin{equation}}
\newcommand{\eeq}{\end{equation}}
\newcommand{\bsp}{\begin{split}}
\newcommand{\esp}{\end{split}}
\newtheorem{Thm}{Theorem}
\newtheorem{Def}{Definition}
\newtheorem{Lem}{Lemma}
\newtheorem{Cor}{Corollary}
\newtheorem{Rem}{Remark}
\newtheorem{Prop}{Proposition}
\newtheorem{Conj}{Conjecture}
\def\mathbi#1{\textbf{\em #1}}

\newcommand{\ff}{\mathbb{F}}
\newcommand{\kk}{\mathbb{K}}
\newcommand{\mv}{\mathcal{M}_V}


%==================End Definitions=====================

\begin{document}

\title{The Generic Complexity of MinRank}

\author[1]{Ray Perlner}
\author[1,2]{Daniel Smith-Tone}
\affil[1]{National Institute of Standards and Technology,\newline
Gaithersburg, Maryland, USA}
\affil[2]{Department of Mathematics, University of Louisville,\newline Louisville, Kentucky, USA}
\affil[ ]{\mailsb \ \ \mailsa}
```

\date{}

\providecommand{\Quiwords}[1]{\textbf{\textit{Keywords: }} #1}

\maketitle

\begin{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.
\end{abstract}
\Quiwords{MinRank, Hilbert Series, Hilbert Regularity, Rank Defect}

\section{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, \cite{KipnisShamir:relin,DBLP:journals/dcc/BettaleFP13,DBLP:conf/pqcrypto/MoodyPS14,DMRPDCST,JVDCST,DCDCSTJV, DBLP:conf/asiacrypt/GoubinC00}. There is thus tremendous practical value to the effective computation of MinRank.

Previous work investigating the complexity of the MinRank problem includes \cite{DBLP:conf/issac/FaugereDS10}. 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 Fr\"oberg conjecture of \cite{Froberg}.

We define a category of overdefined MinRank instances, called \emph{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.
%e.g. \cite{DBLP:conf/pqcrypto/TaoDTD13, Dingrainbow, DBLP:conf/ctrsa/PatarinCG01}.
%I decided that there was no point in citing examples of MinRank problems in multivariate cryptanalysis twice. I also added TTM/Rainbow as an example above.
We provide an 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.

\section{The MinRank Problem}

\begin{Def}
The MinRank problem with parameters (n,r,k) over a field $\kk$ is the problem of constructing with input $\mathbf{M}_1,\ldots,\mathbf{M}_k\in\mathcal{M}_{n\times n}(\kk)$ a nonzero $\kk$-linear combination satisfying:
\[
\mbox{Rank}\left(\sum_{i=1}^ka_i\mathbf{M}_i\right)\leq r.
\]
\end{Def}
The complexity of the MinRank problem in general is clearly bounded by the complexity in the case that the minimum rank of any nonzero $\kk$-linear combination is exactly r; thus, we 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
\[
\overline{\mathbf{M}}=\sum_{i=1}^kt_i\mathbf{M}_i,
\]

whose entries are in $\kk[T]=\kk[t_1,\ldots,t_k]$. The Kipnis-Shamir modeling of this MinRank problem, see \cite{KipnisShamir:relin} constructs a basis for the right kernel of $\overline{\mathbf{M}}$ of the form
\[
\mathbf{K}=\left[\begin{matrix}
1 & 0 & \cdots & 0\\
0 & 1 & \cdots & 0\\
\vdots & \vdots & \ddots & 1\\
v_{1,1} & v_{1,2} & \cdots & v_{1,n-r}\\
\vdots & \vdots & \ddots & \vdots\\
v_{r,1} & v_{r,2} & \cdots & v_{r,n-r}\\
\end{matrix}\right]
\]
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 $\kk[T,V]=\kk[t_1,\ldots,t_k,v_{1,1},\ldots,v_{r,n-r}]$. 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 \emph{underdetermined} if $k>(n-r)^2$, \emph{well-determined} if $k=(n-r)^2$ and \emph{overdetermined} if $k<(n-r)^2$.

\section{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 $\kk[T]$ generated by the $(r+1)\times (r+1)$ minors of $\overline{\mathbf{M}}$. Any element of $V(I)\cap\kk^k$ is clearly a solution to the MinRank problem over $\kk$.

The number of $(r+1)\times (r+1)$ minors in $\overline{\mathbf{M}}$ is ${n\choose r+1}^2$; however, since every minor is homogeneous of degree $r+1$ and there are only ${k+r\choose r+1}$ degree $r+1$ monomials, there can be at most
\[
q=\min\left({k+r\choose r+1},{n\choose r+1}^2\right)
\]
\emph{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 \cite[Corollary 4]{DBLP:conf/issac/FaugereDS10}, the Hilbert regularity of I is shown to be bounded by $r(n-r)+1$ via a derivation of the Hilbert Series of $\kk[T]/I$ obtained with the aid of a variant of the Fr\"oberg Conjecture. In many applications it has been shown that the regularity is $r+1$ via the same analysis, see \cite{DBLP:journals/dcc/BettaleFP13,DCDCSTJV}, for example.

Among these overdetermined instances of MinRank is a special class, in which $q={k+r\choose r+1}$. We refer to such instances as \emph{superdetermined}. (If we consider the symmetric MinRank problem, in which the matrices are all symmetric, then we say that the instance is superdetermined if ${k+r\choose r+1}\leq{n\choose r+1}/2$). 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.

\begin{Prop}
A MinRank problem with parameters (n,r,k) over the field $\kk$ is superdetermined if $k\leq\frac{(n-r)^2}{r+1}-r$.
\end{Prop}

\begin{proof}
Let $k\leq\frac{(n-r)^2}{r+1}-r$. First, we note that
\[
2(r+1)!^2{k+r\choose r+1}=2(r+1)!(k+r)(k+r-1)\cdots k\leq 2(r+1)!(k+r)^{r+1}.
\]
Next, since $2(r+1)!\leq(r+1)^{r+1}$ when $r\geq 1$, we have that
\[
2(r+1)!^2{k+r\choose r+1}\leq\left[(r+1)(k+r)\right]^{r+1}.
\]
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 $(n-r)^{2(r+1)}<n^2(n-1)^2\cdots(n-r)^2=(r+1)!^2{n\choose r+1}^2$,
we obtain
\[
2{k+r\choose r+1}<{n\choose r+1}^2.
\]
\end{proof}

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

\begin{Thm}
Let $(\mathbf{M}_1,\ldots,\mathbf{M}_k)$ be a generic superdetermined instance of MinRank with parameters (n,r,k) over the field $\kk$. Let $\overline{\mathbf{M}}=\sum_{i=1}^kt_i\mathbf{M}_i\in\mathcal{M}_{n\times n}(\kk[T])$. Let I be the ideal generated by the $r+1\times r+1$ minors of $\overline{\mathbf{M}}$. Then the Hilbert Series of $\kk[T]/I$ is
\[
HS(t)=\sum_{d=0}^r{k+d-1\choose d}t^d.
\]
Consequently, the Hilbert regularity of I is $r+1$.
\end{Thm}
\begin{proof}
Consider $\mathcal{A}=\kk[T]$ as a graded algebra,
\[
\mathcal{A}=\bigoplus_{d\geq 0}\mathcal{A}_d,
\]
graded by total degree. Since there are ${k+r\choose r+1}$ monomials of total degree $r+1$ and the linear span of the minors of a generic superdetermined MinRank instance is ${k+r\choose r+1}$ dimensional, there is a set of ${k+r\choose r+1}$ 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 $\kk[T]/I$ as a graded algebra satisfies
\[
\kk[T]/I\approx \bigoplus_{d=0}^r\mathcal{A}_d.
\]
Since $\text{dim}_{\kk}(\mathcal{A}_d)={k+d-1\choose d}$ for $0\leq d\leq r$--- with the convention that ${0\choose

0}=1$--- the Hilbert Series of $\kk[T]/I$ is
\[
HS(t)=\sum_{d=0}^r{k+d-1\choose d}t^d.
\]
Since the Hilbert Series is a polynomial of degree r, the Hilbert regularity is $r+1$.
\end{proof}

% ==
\bibliographystyle{plain}
\bibliography{References}

\end{document}