The (minimum) rank of typical fooling-set matrices

Mozhgan Pourmoradnasseri, Dirk Oliver Theis*

Institute of Computer Science of the University of Tartu
Ülikooli 17, 51014 Tartu, Estonia
{dotheis,mozhgan}@ut.ee

Abstract

A fooling-set matrix has nonzero diagonal, but at least one in every pair of diagonally opposite entries is 0. Dietzfelbinger et al. ’96 proved that the rank of such a matrix is at least $\sqrt{n}$. It is known that the bound is tight (up to a multiplicative constant).

We ask for the typical minimum rank of a fooling-set matrix: For a fooling-set zero-nonzero pattern chosen at random, is the minimum rank of a matrix with that zero-nonzero pattern over a field $F$ closer to its lower bound $\sqrt{n}$ or to its upper bound $n$? We study random patterns with a given density $p$, and prove an $\Omega(n)$ bound for the cases when
(a) $p$ tends to 0 quickly enough;
(b) $p$ tends to 0 slowly, and $|F| = O(1)$;
(c) $p \in (0,1]$ is a constant.

We have to leave open the case when $p \to 0$ slowly and $F$ is a large or infinite field (e.g., $F = \text{GF}(2^n)$, $F = \mathbb{R}$).

1 Introduction

Let $f : X \times Y \to \{0,1\}$ be a function. A fooling set of size $n$ is a family $(x_1, y_1), \ldots, (x_n, y_n) \in X \times Y$ such that $f(x, y) = 1$ for all $i$, and for $i \neq j$, at least one of $f(x_i, y_j)$ of $f(y_i, y_j)$ is 0.

Sizes of fooling sets are important lower bounds in Communication Complexity (see, e.g., [13, 12]) and the study of extended formulations (e.g., [4, 1]).

There is an a priori upper bound on the size of fooling sets due to Dietzfelbinger et al. [3], based on the rank of a matrix associated with $f$. Let $\overline{F}$ be an arbitrary field. The following is a slight generalization of the result in [3] (see the appendix for a proof).

Lemma 1. No fooling set in $f$ is larger than the square of $\min_A \text{rk}_F(A)$, where the minimum ranges over all $X \times Y$-matrices $A$ over $\overline{F}$ with $A_{x,y} = 0$ iff $f(x,y) = 0$.

It is known that, for fields $F$ with nonzero characteristic, this upper bound is asymptotically attained [6], and for all fields, it is attained up to a multiplicative constant [5]. These results, however, require sophisticated constructions. In this paper, we ask how useful that upper bound is for typical functions $f$.

Put differently, a fooling-set pattern of size $n$ is a matrix $R$ with entries in $\{0,1\} \subseteq \overline{F}$ with $R_{k,k} = 1$ for all $k$ and $R_{k,\ell}R_{\ell,k} = 0$ whenever $k \neq \ell$. We say that a fooling-set pattern of size $n$
has density \( p \in [0, 1] \), if it has exactly \( \binom{n}{2} p \) off-diagonal 1-entries. So, the density is roughly the quotient \( (|R| - n) / \binom{n}{2} \), where \(|\cdot|\) denotes the Hamming weight, i.e., the number of nonzero entries. The densest possible fooling-set pattern has \( \binom{n}{2} \) off-diagonal ones (density \( p = 1 \)).

For any field \( \mathbb{F} \) and \( y \in \mathbb{F} \), let \( \sigma(y) := 0 \), if \( y = 0 \), and \( \sigma(y) := 1 \), otherwise. For a matrix (or vector, in case \( n = 1 \)) \( M \in \mathbb{F}^{m \times n} \), define the zero-nonzero pattern of \( M \), \( \sigma(M) \), as the matrix in \( \{0, 1\}^{m \times n} \) which results from applying \( \sigma \) to every entry of \( M \).

This paper deals with the following question: *For a fooling-set pattern chosen at random, is the minimum rank of closer to its lower bound \( \sqrt{n} \) or to its trivial upper bound \( n \)?* The question turns out to be surprisingly difficult. We give partial results, but we must leave some cases open. The distributions we study are the following:

- \( Q(n) \) denotes a fooling-set pattern drawn uniformly at random from all fooling-set patterns of size \( n \);
- \( R(n, p) \) denotes a fooling-set patterns drawn uniformly at random from all fooling-set patterns of size \( n \) with density \( p \).

We allow that the density depends on the size of the matrix: \( p = p(n) \). From now on, \( Q = Q(n) \) and \( R = R(n, p) \) will denote these random fooling-set patterns.

Our first result is the following. As customary, we use the terminology “asymptotically almost surely, a.a.s.,” to stand for “with probability tending to 1 as \( n \) tends to infinity”.

**Theorem 2.** (a) For every field \( \mathbb{F} \), if \( p = O(1/n) \), then, a.a.s., the minimum rank of a matrix with zero-nonzero pattern \( R(n, p) \) is \( \Omega(1) \).

(b) Let \( \mathbb{F} \) be a finite field and \( F := |\mathbb{F}| \). (We allow \( F \) to grow with \( n \).) If \( 100 \max(1, \ln \ln F)/n \leq p \leq 1 \), then the minimum rank of a matrix over \( \mathbb{F} \) with zero-nonzero pattern \( R(n, p) \) is

\[
\Omega\left(\frac{\log(1/p)}{\log(1/p) + \log(F)^n}\right) = \Omega(n/\log(F)).
\]

(c) For every field \( \mathbb{F} \), if \( p \in [0, 1] \) is a constant, then the minimum rank of a matrix with zero-nonzero pattern \( R(n, p) \) is \( \Omega(1) \). (The same is true for zero-nonzero pattern \( Q(n) \).)

Since the constant in the big-\( \Omega \) in Theorem 2(c) tends to 0 with \( p \to 0 \), the proof technique used for constant \( p \) does not work for \( p = o(1) \); moreover, the bound in (b) does not give an \( \Omega(n) \) lower bound for infinite fields, or for large finite fields, e.g., \( GF(2^n) \). We conjecture that the bound is still true (see Lemma 4 for a lower bound):

**Conjecture 3.** For every field \( \mathbb{F} \) and for all \( p = p(n) \), the minimum rank of a fooling-set matrix with random zero-nonzero pattern \( R(n, p) \) is \( \Omega(n) \).

The bound in Theorem 2(b) is similar to that in [8], but it is better by roughly a factor of \( \log n \) if \( p \) is (constant or) slowly decreasing, e.g., \( p = 1/\log n \). (Their minrank definition gives a lower bound to fooling-set pattern minimum rank.)

The next three sections hold the proofs for Theorem 2.

**Acknowledgments.** The second author would like to thank Kaveh Khoshkhah for discussions on the subject.

## 2 Proof of Theorem 2(a)

It is quite easy to see (using, e.g., Turán’s theorem) that in the region \( p = O(1/n) \), \( R(n, p) \) contains a triangular submatrix with nonzero diagonal entries of order \( \Omega(n) \), thus lower bounding the rank over any field. Here, we prove the following stronger result, which also gives a lower bound (for arbitrary fields) for more slowly decreasing \( p \).
Lemma 4. For \( p(n) = d(n)/n = o(1) \), if \( d(n) > C \) for some constant \( C \), then zero-nonzero pattern \( R(n, p) \) contains a triangular submatrix with nonzero diagonal entries of size \( \Omega \left( \frac{\ln d}{d} \cdot n \right) \).

We prove the lemma by using the following theorem about the independence number of random graphs in the Erdős-Rényi model. Let \( G_{n, q} \) denote the random graph with vertex set \([n]\) where each edge is chosen independently with probability \( q \).

Theorem 5 (Theorem 7.4 in [11]). Let \( \epsilon > 0 \) be a constant, \( q = q(n) \), and define

\[
k_{\pm \epsilon} := \left[ \frac{2}{q} (\ln (nq) - \ln (nq) + 1 - \ln 2 \pm \epsilon) \right].
\]

There exists a constant \( C \), such that for \( C/n \leq q = q(n) \leq n^{-2} n \), a.a.s., the largest independent set in \( G_{n, q} \) has size between \( k_{-\epsilon} \) and \( k_{+\epsilon} \).

Proof of Lemma 4. Construct a graph \( G \) with vertex set \([n]\) from the fooling-set pattern matrix \( R(n, p) \) in the following way: There is an edge between vertices \( k \) and \( \ell \) with \( k > \ell \), if and only if \( M_{k, \ell} \neq 0 \). This gives a random graph \( G = G_{n, m, 1/2} \) which is constructed by first drawing uniformly at random a graph from all graphs with vertex set \([n]\) and exactly \( m \) edges, and then deleting each edge, independently, with probability \( 1/2 \). Using standard results in random graph theory (e.g., Lemma 1.3 and Theorem 1.4 in [7]), this random graph behaves similarly to the Erdős-Rényi graph with \( q := p/2 \). In particular, since \( G_{n, p/2} \) has an independent set of size \( \Omega(n) \), so does \( G_{n, m, 1/2} \).

It is easy to see that the independent sets in \( G \) are just the lower-triangular principal submatrices of \( R_{n, p} \).

As already mentioned, Theorem 2(a) is completed by noting that for \( p < C/n \), an easy application of Turán’s theorem (or ad-hoc methods) gives us an independent set of size \( \Omega(n) \).

3 Proof of Theorem 2(b)

Let \( \mathbb{F} \) be a finite field with \( F := |\mathbb{F}| \). As mentioned in Theorem 2, we allow \( F = F(n) \) to depend on \( n \). In this section, we need to bound some quantities away from others, and we do that generously.

Let us say that a tee shape is a set \( T = I \times [n] \cup [n] \times I \), for some \( I \subset [n] \). A tee matrix is a tee shape \( T \) together with a mapping \( N: T \to \mathbb{F} \) which satisfies

\[
N_{k, k} = 1 \text{ for all } k \in I, \quad N_{k, \ell} N_{\ell, k} = 0 \text{ for all } (k, \ell) \in I \times [n], k \neq \ell.
\]

The order of the tee shape/matrix is \( |I| \), and the rank of the tee matrix is the rank of the matrix \( N_{I \times I} \).

For a matrix \( M \) and a tee matrix \( N \) with tee shape \( T \), we say that \( M \) contains the tee matrix \( N \), if \( M_T = N \).

Lemma 6. Let \( M \) be a matrix with rank \( s := \text{rk } M \), which contains a tee matrix \( N \) of rank \( s \). Then \( M \) is the only matrix of rank \( s \) which contains \( N \).

In other words, the entries outside of the tee shape are uniquely determined by the entries inside the tee shape.

Proof. Let \( T = I \times [n] \cup [n] \times I \) be the tee shape of a tee matrix \( N \) contained in \( M \).

Since \( N_{I \times I} = M_{I \times I} \) and \( \text{rk } N_{I \times I} = s = \text{rk } M \), there is a row set \( I_1 \subset I \) of size \( s = \text{rk } M \) and a column set \( I_2 \subset I \) of size \( s \) such that \( \text{rk } M_{I_1 \times I_2} = s \). This implies that \( M \) is uniquely determined, among the matrices of rank \( s \), by \( M_{T'} \) with \( T' := I_1 \times [n] \cup [n] \times I_2 \subset T \). (Indeed,
since the rows of \( M_{t_1 \times [n]} \) are linearly independent and span the row space of \( M \), every row in \( M \) is a unique linear combination of the rows in \( M_{t_1 \times [n]} \); since the rows in \( M_{t_1 \times t_2} \) are linearly independent, this linear combination is uniquely determined by the rows of \( M_{[n] \times t_2} \).

Hence, \( M \) is the only matrix \( M' \) with \( \text{rk} M' = s \) and \( M'_{t_2} = M_{t_2} \). Trivially, then, \( M \) is the only matrix \( M' \) with \( \text{rk} M' = s \) and \( M'_{t_2} = M_{t_2} = N \). \( \square \)

**Lemma 7.** For \( r \leq n/5 \) and \( m \leq 2r(n - r)/3 \), there are at most

\[
O(1) \cdot \left( \frac{n}{2r} \right) \cdot \left( \frac{2r(n - r)}{m} \right) \cdot (2F)^m
\]

matrices of rank at most \( r \) over \( F \) which contain a tee matrix of order \( 2r \) with at most \( m \) nonzeros.

**Proof.** By the Lemma 6, the number of these matrices is upper bounded by the number of tee matrices (of all ranks) of order \( 2r \) with at most \( k \) nonzeros.

The tee shape is uniquely determined by the set \( I \subseteq [n] \). Hence, the number of tee shapes of order \( 2r \) is

\[
\binom{n}{2r}.
\]

The number of ways to choose the support a tee matrix. Suppose that the tee matrix has \( h \) nonzeros. Due to (1), \( h \) nonzeros must be chosen from \( \binom{2r}{2} + 2r(n - 2r) \leq 2r(n - r) \) opposite pairs. Since \( h < 2r(n - r)/2 \), we upper bound this by

\[
\binom{2r(n - r)}{h}.
\]

For each of the \( h \) opposite pairs, we have to pick one side, which gives a factor of \( 2^h \). Finally, picking, a number in \( F \) for each of the entries designated as nonzero gives a factor of \( (F - 1)^h \).

For summing over \( h = 0, \ldots, m \), first of all, remember that \( \sum_{i=0}^{(1-\varepsilon)j/2} \binom{j}{i} = O(1) \cdot \binom{j}{(1-\varepsilon)j/2} \) (e.g., Theorem 1.1 in [2], with \( p = 1/2, u := 1 + \varepsilon \)). Since \( m \leq 2r(n - r)/3 \), we conclude

\[
\sum_{h=0}^{m} \binom{2r(n - r)}{h} = O(1) \cdot \binom{2r(n - r)}{m}
\]

(with an absolute constant in the big-Oh). Hence, we find that the number of tee matrices (with fixed tee shape) is at most

\[
\sum_{h=0}^{m} \left( \binom{2r(n - r)}{h} \right)^2 (F - 1)^{h} \leq (2F)^m \sum_{h=0}^{m} \binom{2r(n - r)}{h} = O(1) \cdot (2F)^m \cdot \binom{2r(n - r)}{m}.
\]

Multiplying by \((*)\), the statement of the lemma follows. \( \square \)

**Lemma 8.** Let \( r \leq n/5 \). Every matrix \( M \) of rank at most \( r \) contains a tee matrix of order \( 2r \) and rank \( \text{rk} M \).

**Proof.** There is a row set \( I_1 \) of size \( s := \text{rk} M \) and a column set \( I_2 \) of size \( s \) such that \( \text{rk} M_{t_1 \times t_2} = s \). Take \( I \) be an arbitrary set of size \( 2r \) containing \( I_1 \cup I_2 \), and \( T := I \times [n] \cup [n] \times I \). Clearly, \( M \) contains the tee matrix \( N := M_T \), which is of order \( 2r \) and rank \( s = \text{rk} M \). \( \square \)

**Lemma 9.** Let \( 100 \max(1, \ln \ln F)/n \leq p \leq 1 \), and \( n/(1000 \max(1, \ln F)) \leq r \leq n/100 \). A.a.s., every tee shape of order \( 2r \) contained in the random matrix \( R(n, p) \) has fewer than \( 15pr(n - r) \) nonzeros.
Proof. We take the standard Chernoff-like bound for the hypergeometric distribution of the intersection of uniformly random $p \binom{n}{2}$-element subset (the diagonally opposite pairs of $R(n, p)$ which contain a 1-entry) of a $\binom{n}{2}$-element ground set (the total number of diagonally opposite pairs) with a fixed $2r(n-r)$-element subset (the opposite pairs in $T$) of the ground set. With $\lambda := 2r(n-r)$ (the expected size of the intersection), if $x \geq 7\lambda$, the probability that the intersection has at least $x$ elements is at most $e^{-x}$.

Hence, the probability that the support of a fixed tee shape of order $2r$ is greater than than $15pn(n-r) \geq 14pn(n-r)+r$ is at most

$$e^{-14pn(n-r)} \leq e^{-r(1.99 \max(1, \ln F))} \leq e^{-r(1000 \max(1, \ln F))}$$

Since the number of tee shapes is

$$\binom{n}{2r} \leq e^{r(1+\ln(n/r))} \leq e^{r(11+\ln \max(1, \ln F))} \leq e^{r(11+\max(1, \ln F))}$$

we conclude that the probability that a dense tee shape exists in $R(n, p)$ is at most $e^{-\Omega(r)}$. □

We are now ready for the main proof.

Proof of Theorem 2(b). Call a fooling-set matrix $M$ regular, if $M_{k,k} = 1$ for all $k$. The minimum rank over a fooling-set pattern is always attained by a regular matrix (divide every row by the corresponding diagonal element).

Consider the event that there is a regular matrix $M$ over $F$ with $\sigma(M) = R(n, p)$, and $rk M \leq r := n/(2000 \ln F)$. By Lemma 8, $M$ contains a tee matrix $N$ of order $2r$ and rank $rk M$. If the size of the support of $N$ is larger than $15pn(n-r)$, then we are in the situation of Lemma 9.

Otherwise, $M$ is one of the

$$O(1) \cdot \binom{n}{2r} \cdot \binom{2r(n-r)}{15pn(n-r)} \cdot (2F)^{15pn(n-r)}$$

matrices of Lemma 7.

Hence, the probability of said event is $o(1)$ (from Lemma 9) plus at most an $O(1)$ factor of the following (with $m := mn^2/2$ and $\phi := r/n$) a constant

$$\binom{n}{2r} \cdot \binom{2r(n-r)}{15pn(n-r)} \cdot (2F)^{15pn(n-r)} = \binom{n}{2r} \cdot \binom{2r(n-r)}{15pn(n-r)} \cdot (2F)^{15pn(n-r)}$$

$$= \binom{n}{2gn} \cdot \binom{4g(1-\phi)n^2/2}{30g(1-\phi)n^2/2} \cdot (2F)^{30g(1-\phi)n^2/2}$$

$$= \binom{n}{2gn} \cdot \binom{4g(1-\phi)n^2/2}{30g(1-\phi)n^2/2} \cdot (2F)^{30g(1-\phi)n^2/2}$$

$$= \binom{n}{2gn} \cdot \binom{4g(1-\phi)n^2/2}{30g(1-\phi)n^2/2} \cdot (2F)^{30g(1-\phi)n^2/2}$$

$$=: Q$$

Abbreviating $\alpha := 30g(1-\phi) < 30g$, denoting $H(t) := -t \ln t - (1-t) \ln(1-t)$, and using

$$\left(\frac{a}{ta}\right) = \Theta \left( (ta)^{-1/2} \right) e^{H(t)a} \text{, for } t \leq \frac{1}{2}$$

\[\text{(2)}\]
(for a large, “≤” holds instead of “= Θ”), we find (the $O(pm)$ exponent comes from replacing $\binom{n}{2}$ by $n^2/2$ in the denominator)

$$\left(\frac{n}{2^{\alpha n^2/2}}\right)^{30q(1-q)pn^2/2} \leq e^{H(1/2q)n-(\ln 2)(1-\alpha)pn^2/3}$$

$$\leq e^{H(1/2q)n-(\ln 2)(1-\alpha)pn^2/3} = e^{\alpha n(H(1/2q) - (\ln 2)(1-\alpha)pn/3)}$$

$$\leq e^{\alpha n(1/(2q) - (\ln 2)(1-\alpha))33(1-30q)} = o(1),$$

as $p n/2 \geq 30$ and $1 - \alpha > 1 - 30q$, and the expression in the parentheses is negative for all $q \in [0, 3/100]$.

For the rest of the fraction $Q$ above, using (2) again, we simplify

$$\left(4q(1-q) n^2/2 \right)^{30q(1-q)pn^2/2} \leq \left(\frac{\alpha n^2/2}{\alpha pn^2/2}\right)^{30q(1-q)pn^2/2} = \left(\frac{n^2/2}{pn^2/2}\right)^{30q(1-q)pn^2/2} = O(1) \cdot e^{n^2/2 \left((\alpha - 1)H(p) + \alpha \ln F\right)}.$$

Setting the expression in the parentheses to 0 and solving for $q$, we find

$$\alpha \geq \frac{\ln(1/p)}{\ln(1/p) + \ln F}$$

suffices for $Q = o(1)$; as $\alpha \leq q$, the same inequality with $\alpha$ replaced by $q$ is sufficient. This completes the proof of the theorem. \qed 

## 4 Proof of Theorem 2(c)

In this section, following the idea of [9], we apply a theorem of Ronyai, Babai, and Ganapathy [15] on the maximum number of zero-patterns of polynomials, which we now describe.

Let $f = (f_j)_{j=1,\ldots,h}$ be an $h$-tuple of polynomials in $n$ variables $x = (x_1, x_2, \ldots, x_n)$ over an arbitrary field $F$. In line with the definitions above, for $u \in F^n$, the zero-nonzero pattern of $f$ at $u$ is the vector $\sigma(f(u)) \in \{0,1\}^h$.

**Theorem 10** ([15]). If $h \geq n$ and each $f_j$ has degree at most $d$ then, for all $m$, the set

$$\left\{ y \in \{0,1\}^h \mid \|y\| \leq m \text{ and } y = \sigma(f(u)) \text{ for some } u \in F^n \right\} \leq \left(\frac{n+md}{n}\right).$$

In other words, the number of zero-nonzero patterns with Hamming weight at most $m$ is at most $\binom{n+md}{n}$.

As has been observed in [9], this theorem is implicit in the proof of Theorem 1.1 of [15] (for the sake of completeness, the proof is repeated in the appendix). It has been used in the context of minimum rank problems before (e.g., [14, 9]), but our use requires slightly more work.

Given positive integers $r < n$, let us say that a $G$-pattern is an $r \times n$ matrix whose entries are the symbols 0, 1, and *, with the following properties.

1. Every column contains at most one 1, and every column containing a 1 contains no *s.
2. In every row, the leftmost entry different from 0 is a 1, and every row contains at most one 1.
(3) Rows containing a 1 (i.e., not all-zero rows) have smaller row indices than rows containing no 1 (i.e., all-zero rows). In other words, the all-zero rows are at the bottom of $P$.

We say that an $r \times n$ matrix $Y$ has $G$-pattern $P$, if $Y_{j,\ell} = 0$ if $P_{j,\ell} = 0$, and $Y_{j,\ell} = 1$ if $P_{j,\ell} = \ast$. There is no restriction on the $Y_{j,\ell}$ for which $P_{j,\ell} = \ast$.

“G” stands for “Gaussian elimination using row operations”. We will need the following tree easy lemmas.

**Lemma 11.** Any $r \times n$ matrix $Y'$ can be transformed, by Gaussian elimination using only row operations, into a matrix $Y$ which has some G-pattern.

**Proof (sketch).** If $Y'$ has no nonzero entries, we are done. Otherwise start with the left-most column containing a nonzero entry, say $(j, \ell)$. Scale row $j$ that entry a 1, permute the row to the top, and add suitable multiples of it to the other rows to make every entry below the 1 vanish.

If all columns $1, \ldots, \ell$ have been treated such that column $\ell$ has a unique 1 in row, say $(j, \ell)$, consider the remaining matrix $\{j(\ell) + 1, \ldots r\} \times \{\ell + 1, \ldots, n\}$. If every entry is a 0, we are down. Otherwise, find the leftmost nonzero entry in the block; suppose it is in column $\ell'$ and row $j'$. Scale row $j'$ to make that entry a 1, permute row $j'$ to $j(\ell) + 1$, and add suitable multiples of it to all other rows $\{1, \ldots, r\} \setminus \{j(\ell) + 1\}$ to make every entry below the 1 vanish.

**Lemma 12.** For every $r \times n$ G-pattern matrix $P$, the number of $\ast$-entries in $P$ is at most $r(n - r/2)$.

**Proof (sketch).** The G-pattern matrix $P$ is uniquely determined by the set of columns containing a 1, which can be between 0 and $\phi n$. Hence, the number of $n \times \phi n$ G-pattern matrices is

$$O(1) \cdot \binom{n}{\phi n},$$

(with an absolute constant in the big-O).

**Lemma 13.** Let $\phi \in [0, 49/100]$. The number of $n \times \phi n$ G-pattern matrices is at most

$$O(1) \cdot \binom{n}{\phi n},$$

(with an absolute constant in the big-O).

**Proof (sketch).** A G-pattern matrix is uniquely determined by the set of columns containing a 1, which can be between 0 and $\phi n$. Hence, the number of $n \times \phi n$ G-pattern matrices is

$$\sum_{j=0}^{\phi n} \binom{n}{j}.$$

From here on, we do the usual tricks. As in the previous section, we use the helpful fact (Theorem 1.1 in [2]) that

$$(\ast) \leq \frac{1}{1 - \phi(1 - \phi)} \binom{n}{\phi n}.$$  

A swift calculation shows that $1/(1 - \phi(1 - \phi)) \leq 30$, which completes the proof.

We are now ready to complete the Proof of Theorem 2(c).
Proof of Theorem 2(c). Let $M$ be a fooling-set matrix of size $n$ and rank at most $r$. It can be factored as $M = XY$, for an $n \times r$ matrix $X$ and an $r \times n$ matrix $Y$. By Lemma 11, through applying row operations to $Y$ and corresponding column operations to $X$, we can assume that $Y$ has a G-pattern.

Now we use Theorem 10, for every G-pattern matrix $P$, the variables of the polynomials are

- $X_{k,j}$, where $(k, j)$ ranges over all pairs $\{1, \ldots, n\} \times \{1, \ldots, r\}$; and
- $Y_{j,\ell}$, where $(j, \ell)$ ranges over all pairs $\{1, \ldots, r\} \times \{1, \ldots, n\}$ with $P_{j,\ell} = *$.

The polynomials are: for every $(k, \ell) \in \{1, \ldots, n\}^2$, with $k \neq \ell$,

$$f_{k,\ell} = \sum_{P_{j,\ell}=1} X_{k,j} + \sum_{P_{j,\ell}=*} X_{k,j} Y_{j,\ell}.$$ 

Clearly, there are $n(n-1)$ polynomials; the number of variables is $2rn - r^2/2$, by Lemma 12 (and, if necessary, using “dummy” variables which have coefficient 0 always). The polynomials have degree at most 2.

By Theorem 10, we find that the number of zero-nonzero patterns with Hamming weight at most $m$ of fooling-set matrices with rank at most $r$ which result from this particular G-pattern matrix $P$ is at most

$$(2rn - r^2/2 + 2m)$$

Now, take a $\rho < 1/2$, and let $r := gn$. Summing over all G-pattern matrices $P$, and using Lemma 13, we find that the number of zero-nonzero patterns with Hamming weight at most $m$ of fooling-set matrices with rank at most $gn$ is at most an absolute constant times

$$\binom{n}{2} \frac{(2\rho - \rho^2/2)n^2 + 2m}{(2\rho - \rho^2/2)n^2}.$$ 

Now, take a constant $p \in [0,1]$, and let $m := \lfloor p(n^2/2) \rfloor$. The number of fooling-sets patterns of size $n$ with density $p$ is

$$\binom{n}{2} \frac{2^m}{2^{\alpha n^2}},$$

and hence, the probability that the minimum rank of a fooling-set matrix with zero-nonzero pattern $R(n,p)$ has rank at most $r$ is at most

$$\frac{n}{gn} \frac{(2\rho - \rho^2/2)n^2 + 2m}{(2\rho - \rho^2/2)n^2} \leq \binom{n}{2} \frac{(2\rho - \rho^2/2)n^2 + 2m n^2}{(2\rho - \rho^2/2)n^2} \binom{n}{2} \frac{(2\rho - \rho^2/2)n^2 + 2m n^2}{(2\rho - \rho^2/2)n^2} \binom{n}{2} \frac{(2\rho - \rho^2/2)n^2 + 2m n^2}{(2\rho - \rho^2/2)n^2} \binom{n}{2} \frac{(2\rho - \rho^2/2)n^2 + 2m n^2}{(2\rho - \rho^2/2)n^2} \binom{n}{2} \frac{(2\rho - \rho^2/2)n^2 + 2m n^2}{(2\rho - \rho^2/2)n^2}$$

We have set $\alpha := 2\rho - \rho^2/2$. As in the previous section, we use (2) to estimate this expression, and we obtain

$$\ln \left( \frac{n}{gn} \frac{\alpha n^2 + 2m n^2}{\alpha n^2} \right) = nH(\rho) + n^2 \left( \alpha H(\alpha/(\alpha + p)) - \frac{1}{2} H(p) - (\ln 2)p/2 \right) + O(\rho).$$

The dominant term is the one where $n$ appears quadratic. The expression $\frac{1}{2} H(p) + (\ln 2)p/2$ takes values in $[0,1]$. For every fixed $p$, the function $g: \alpha \mapsto \alpha H(\alpha/(\alpha + p))$ is strictly increasing on $[0,1/2]$ and satisfies $g(0) = 0$. Hence, for every given constant $p$, there exists an $\alpha$ for which the coefficient after the $n^2$ is negative.

(As indicated in the introduction, such an $\alpha$ must tend to 0 with $p \to 0$.)
References

[1] LeRoy B. Beasley, Hartmut Klauck, Troy Lee, and Dirk Oliver Theis. Communication complexity, linear optimization, and lower bounds for the nonnegative rank of matrices (dagstuhl seminar 13082). Dagstuhl Reports, 3(2):127–143, 2013.

[2] Béla Bollobás. Random graphs, volume 73 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, second edition, 2001.

[3] Martin Dietzfelbinger, Juraj Hromkovič, and Georg Schnitger. A comparison of two lower-bound methods for communication complexity. Theoret. Comput. Sci., 168(1):39–51, 1996. 19th International Symposium on Mathematical Foundations of Computer Science (Košice, 1994).

[4] Samuel Fiorini, Volker Kaibel, Kanstantin Pashkovich, and Dirk Oliver Theis. Combinatorial bounds on nonnegative rank and extended formulations. Discrete Math., 313(1):67–83, 2013.

[5] Mirjam Friesen, Aya Hamed, Troy Lee, and Dirk Oliver Theis. Fooling-sets and rank. European Journal of Combinatorics, 48:143–153, 2015.

[6] Mirjam Friesen and Dirk Oliver Theis. Fooling-sets and rank in nonzero characteristic. In Jaroslav Nešetřil and Marco Pellegrini, editors, The Seventh European Conference on Combinatorics, Graph Theory and Applications, volume 16 of CRM series, pages 383–390. CRM, 2013.

[7] Alan Frieze and Michal Karoński. Introduction to random graphs. Cambridge University Press, 2015.

[8] Alexander Golovnev, Oded Regev, and Omri Weinstein. The minrank of random graphs. arXiv preprint arXiv:1607.04842, 2016.

[9] H Tracy Hall, Leslie Hogben, Ryan Martin, and Bryan Shader. Expected values of parameters associated with the minimum rank of a graph. Linear Algebra and its Applications, 433(1):101–117, 2010.

[10] Ishay Haviv and Michael Langberg. On linear index coding for random graphs. In Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on, pages 2231–2235. IEEE, 2012.

[11] Svante Janson, Tomasz Łuczak, and Andrzej Rucinski. Random graphs. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience, New York, 2000.

[12] Hartmut Klauck and Ronald de Wolf. Fooling one-sided quantum protocols. In 30th International Symposium on Theoretical Aspects of Computer Science, 2013.

[13] Eyal Kushilevitz and Noam Nisan. Communication complexity. Cambridge University Press, Cambridge, 1997.

[14] Sudipta Mallik and Bryan L Shader. On graphs of minimum skew rank 4. Linear and Multilinear Algebra, 64(2):279–289, 2016.

[15] Lajos Rónyai, László Babai, and Murali Ganapathy. On the number of zero-patterns of a sequence of polynomials. Journal of the American Mathematical Society, 14(3):717–735, 2001.
A Proof of Lemma 1

Let \((x_1, y_1), \ldots, (x_n, y_n) \in X \times Y\) be a fooling set in \(f\), and let \(A\) be a matrix over \(F\) with \(A_{x,y} = 0\) iff \(f(x, y) = 0\). Consider the matrix \(B := A \otimes A^\top\). This matrix \(B\) contains a permutation matrix of size \(n\) as a submatrix: for \(i = 1, \ldots, n\), \(B(x_i, x_i), (y_i, y_i) = A_{x_i, y_i} A_{y_i, x_i} = 1\) but for \(i \neq j\), \(B(x_i, x_i), (y_j, y_j) = A_{x_i, y_j} A_{y_i, x_j} = 0\). Hence,

\[
n \leq \text{rk}(B) = \text{rk}(A)^2.
\]

\[\square\]

B Proof of Theorem 10

Since Theorem 10 is not explicitly proven in [15], we give here the slight modification of the proof of Theorem 1.1 from Theorem 10 which proves Theorem 10. The only difference between the following proof and that in [15] is where the proof below upper-bounds the degrees of the polynomials \(g_y\).

Proof of Theorem 10. Consider the set

\[S := \left\{ y \in \{0, 1\}^h \mid |y| \leq m \text{ and } y = \sigma(f(u)) \text{ for some } u \in F^n \right\} \]

For each such \(y\), let \(u_y \in F^n\) be such that \(\sigma(f(u_y)) = y\), and let

\[g_y := \prod_{j, y_j = 1} f_j.\]

Now define a square matrix \(A\) whose row- and column set is \(S\), and whose \((y, z)\) entry is \(g_y(u_z)\). We have

\[g_y(u_z) \neq 0 \iff z \geq y,
\]

with entry-wise comparison, and "\(1 > 0\)". Hence, if the rows and columns are arranged according to this partial ordering of \(S\), the matrix is upper triangular, with nonzero diagonal, so it has full rank, \(|S|\). This implies that the \(g_y, y \in S\), are linearly independent.

Since each \(g_y\) has degree at most \(|y| \cdot d \leq md\), and the space of polynomials in \(n\) variables with degree at most \(md\) has dimension \(\binom{n+md}{md}\), it follows that \(S\) has at most that many elements. \[\square\]