

# 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 is a square matrix with 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  $\sqrt{n}$ , for a matrix of order  $n$ .

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  $\mathbb{F}$  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  $|\mathbb{F}| = O(1)$ ; (c)  $p \in ]0, 1]$  is a constant. We leave open the case when  $p \rightarrow 0$  slowly and  $\mathbb{F}$  is a large (e.g.,  $\mathbb{F} = \text{GF}(2^n)$ ,  $\mathbb{F} = \mathbb{R}$ ).

## 1 Introduction

Let  $f: X \times Y \rightarrow \{0, 1\}$  be a function. A *fooling set* of size  $n$  is a family  $(x_1, y_1), \dots, (x_n, y_n) \in X \times Y$  such that  $f(x_i, y_i) = 1$  for all  $i$ , and for  $i \neq j$ , at least one of  $f(x_i, y_j)$  or  $f(y_i, y_j)$  is 0. Sizes of fooling sets are important lower bounds in Communication Complexity (see, e.g., [15, 14]) and the study of extended formulations (e.g., [5, 2]).

There is an *a priori* upper bound on the size of fooling sets due to Dietzfelbinger et al. [4], based on the rank of a matrix associated with  $f$ . Let  $\mathbb{F}$  be an arbitrary field. The following is a slight generalization of the result in [4] (see Chapter 5 of [17] for a proof).

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

It is known that, for fields  $\mathbb{F}$  with nonzero characteristic, this upper bound is asymptotically attained [7], and for all fields, it is attained up to a multiplicative constant [6]. 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  $\{0, 1\} \subseteq \mathbb{F}$  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  $n$

---

\*Supported by the Estonian Research Council, ETAG (*Eesti Teadusagentuur*), through PUT Exploratory Grant #620, and by the European Regional Development Fund through the Estonian Center of Excellence in Computer Science, EXCS.

has *density*  $p \in ]0, 1]$ , if it has exactly  $\lceil p \binom{n}{2} \rceil$  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)  $M \in \mathbb{F}^{m \times n}$ , 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 closer to its lower bound  $\sqrt{n}$  or to its trivial upper bound  $n$ ?*

The definition of *minimum rank* is implicit in Lemma 1. It differs from the definition used in the context of index coding [1] (which gives a lower bound). It is closer to the minimum rank of a graph [12], but there the matrix  $A$  has to be symmetric while the diagonal entries are unconstrained. Our research is in the same line as work on minimum ranks of other random matrix structures, e.g., [10, 11, 9].

Let  $R(n, p)$  denote a fooling-set pattern 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  $R = R(n, p)$  will denote this random fooling-set pattern. By standard arguments (e.g., [8]), this model behaves similarly to the one where the entries are chosen independently, but it has the advantage of making some arguments shorter.

Our main results are the following. (We use the customary terminology *asymptotically almost surely (a.a.s.)*, to mean “with probability tending to 1 as  $n \rightarrow \infty$ ”.)

**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  $\Omega(n)$ .*

(b) *Let  $\mathbb{F}$  be a finite field and  $F := |\mathbb{F}|$ . 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  $\Omega(n)$ .*

The bound in Theorem 2(b) is similar to that in [9], but it is better by roughly a factor of  $\log n$  if  $p$  is (constant or) slowly decreasing, e.g.,  $p = 1/\log n$ .

Since the constant in the big- $\Omega$  in Theorem 2(c) tends to 0 with  $p \rightarrow 0$ , 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.,  $\text{GF}(2^n)$ . We conjecture that the bound is still true. (See Lemma 4 for a  $o(n)$  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  $\Omega(n)$ .*

## 2 Proof of Theorem 2(a)

It is actually quite easy to see that in the region  $p = O(1/n)$ ,  $R(n, p)$  contains a principal 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  $p(n) = d(n)/n < \ln^{-2} n$ , if  $d(n) > C$  for some constant  $C$ , then the zero-nonzero pattern  $R(n, p)$  contains a triangular submatrix with nonzero diagonal entries of size*

$$\Omega\left(\frac{\ln d}{d} \cdot n\right).$$

From here, Theorem 2(a) follows by noting that for  $p \leq C/n$ , an easy application of Turán's theorem (or ad-hoc methods) gives us an independent set of size  $\Omega(n)$ .

We prove Lemma 4 by using the following theorem about the independence number of random graphs in the Erdős-Rényi model (Theorem 7.4 [13], simplified). Let  $G_{n,q}$  denote the random graph with vertex set  $[n]$  where each edge is chosen independently with probability  $q$ .

**Theorem 5.** *There exists a constant  $C$  such that for  $C/n \leq q = q(n) \leq \ln^{-2} n$ , a.a.s., the largest independent set in  $G_{n,q}$  has size  $2/q \cdot (\ln(qn) - O(\ln \ln(qn)))$ .*

*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 [8]), 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  $R_{n,p}$ . □

## 3 Proof of Theorem 2(b)

Let  $\mathbb{F}$  be a finite field with  $F := |\mathbb{F}|$ . 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  $N: T \rightarrow \mathbb{F}$  which

satisfies

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

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  $I_1 \subseteq I$  of size  $s = \text{rk } M$  and a column set  $I_2 \subseteq I$  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  $T' := I_1 \times [n] \cup [n] \times I_2 \subseteq T$ . (Indeed, since the rows of  $M_{I_1 \times [n]}$  are linearly independent and span the row space of  $M$ , every row in  $M$  is a unique linear combination of the rows in  $M_{I_1 \times [n]}$ ; since the rows in  $M_{I_1 \times I_2}$  are linearly independent, this linear combination is uniquely determined by the rows of  $M_{[n] \times I_2}$ .)

Hence,  $M$  is the only matrix  $M'$  with  $\text{rk } M' = s$  and  $M'_{T'} = M_{T'}$ . Trivially, then,  $M$  is the only matrix  $M'$  with  $\text{rk } M' = s$  and  $M'_T = M_T = N$ .  $\square$

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

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

*matrices of rank at most  $r$  over  $\mathbb{F}$  which contain a tee matrix of order  $2r$  with at most  $m$  nonzeros.*

*Proof.* By 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  $m$  nonzeros.

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

$$\binom{n}{2r}. \quad (*)$$

Now to the number of ways to choose the support the 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  $\mathbb{F}$  for each of the entries designated as nonzero gives a factor of  $(F-1)^h$ .

For summing over  $h = 0, \dots, m$ , first of all, remember that  $\sum_{i=0}^{(1-\varepsilon)j/2} \binom{j}{i} = O_\varepsilon(1) \cdot \binom{j}{(1-\varepsilon)j/2}$  (e.g., Theorem 1.1 in [3], 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

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

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  $\text{rk } M_{I_1 \times I_2} = s$ . 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.<sup>1</sup> With  $\lambda := p2r(n-r)$  (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

<sup>1</sup>Specifically, we use Theorem 2.10 applied to (2.11) in [13]

than  $15pr(n-r) \geq 14pr(n-r) + r$  is at most

$$e^{-14pr(n-r)} \leq e^{-r \cdot 14 \cdot 99 \cdot \max(1, \ln \ln F)} \leq e^{-r \cdot 1000 \cdot \max(1, \ln \ln F)}$$

Since the number of tee shapes is

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

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

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

Otherwise,  $M$  is one of the matrices of Lemma 7, of which there are

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

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

$$\begin{aligned} & \frac{\binom{n}{2r} \cdot \binom{2r(n-r)}{15pr(n-r)} \cdot (2F)^{15pr(n-r)}}{\binom{\binom{n}{2}}{p \binom{n}{2}} 2^{p \binom{n}{2}} 2^{-O(pn)}} = \frac{\binom{n}{2r} \cdot \binom{2r(n-r)}{15pr(n-r)} \cdot (2F)^{15pr(n-r)}}{\binom{n^2/2}{pn^2/2} 2^{pn^2/2 - O(pn)}} \\ & = \frac{\binom{n}{2\varrho n} \cdot \binom{4\varrho(1-\varrho)n^2/2}{30p\varrho(1-\varrho)n^2/2} \cdot (2F)^{30p\varrho(1-\varrho)n^2/2}}{\binom{n^2/2}{pn^2/2} 2^{pn^2/2 - O(pn)}} \\ & = \frac{\binom{n}{2\varrho n} \cdot \binom{4\varrho(1-\varrho)n^2/2}{30\varrho(1-\varrho)pn^2/2} \cdot (2F)^{30\varrho(1-\varrho)pn^2/2}}{\binom{n^2/2}{pn^2/2} 2^{pn^2/2 - O(pn)}} =: Q \end{aligned}$$

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

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

(for  $a$  large, “ $\leq$ ” holds instead of “ $= \Theta$ ”), we find (the  $O(pn)$  exponent comes from replacing  $\binom{n}{2}$  by  $n^2/2$  in the denominator)

$$\begin{aligned} \frac{\binom{n}{2\varrho n} 2^{30\varrho(1-\varrho)pn^2/2}}{2^{pn^2/2 - O(pn)}} &\leq e^{H(1/2\varrho)n - (\ln 2)(1-\alpha)pn^2/3} \\ &= e^{n(H(1/2\varrho) - (\ln 2)(1-\alpha)pn/3)} \\ &\leq e^{n(H(1/2\varrho) - (\ln 2)33(1-30\varrho))} \\ &= o(1), \end{aligned}$$

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

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

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

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

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

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

## 4 Proof of Theorem 2(c)

In this section, following the idea of [10], we apply a theorem of Ronyai, Babai, and Ganapathy [18] on the maximum number of zero-patterns of polynomials, which we now describe.

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

**Theorem 10** ([18]). *If  $h \geq n$  and each  $f_j$  has degree at most  $d$  then, for all  $m$ , the set*

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

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

As has been observed in [10], this theorem is implicit in the proof of Theorem 1.1 of [18] (see Chapter 5 of [17] for a proof of that exact statement). It has been used in the context of minimum rank problems before (e.g., [16, 10]), 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  $P_{j,\ell} = 1$ . There is no restriction on the  $Y_{j,\ell}$  for which  $P_{j,\ell} = *$ .

“G” stands for “Gaussian elimination using row operations”. We will need the following three 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.*

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

**Lemma 13.** *Let  $\varrho \in ]0, .49]$ . The number of  $n \times \varrho n$  G-pattern matrices is at most  $O(1) \cdot \binom{n}{\varrho n}$  (with an absolute constant in the big-O).*

We leave the proofs as advanced exercises to the reader (or see Chapter 5 of [17]). Now we 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 separately. For a fixed G-pattern matrix  $P$ , the variables of the polynomials are



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

The polynomials are: for every  $(k, \ell) \in [n]^2$ , with  $k \neq \ell$ ,

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

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

$$\binom{2rn - r^2/2 + 2m}{2rn - r^2/2}.$$

Now, take a  $\varrho < 1/2$ , and let  $r := \varrho n$ . Summing over all G-pattern matrices  $P$ , and using Lemma 13, we upper bound the number of zero-nonzero patterns with Hamming weight at most  $m$  of fooling-set matrices with rank at most  $\varrho n$ . On the other hand, take a constant  $p \in ]0, 1]$ , and let  $m := \lceil p \binom{n}{2} \rceil$ . The number of fooling-set patterns of size  $n$  with density  $p$  is

$$\binom{\binom{n}{2}}{m} 2^m. \tag{3}$$

Comparing these two bounds yields Theorem 2(c) using standard estimates, similar to those used in [10] (or see Chapter 5 of [17] for the details).  $\square$

## References

- [1] Ziv Bar-Yossef, Yitzhak Birk, TS Jayram, and Tomer Kol. Index coding with side information. *IEEE Transactions on Information Theory*, 57(3):1479–1494, 2011.
- [2] 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.
- [3] Béla Bollobás. *Random graphs*, volume 73 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2001.
- [4] 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).
- [5] 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.

- [6] Mirjam Friesen, Aya Hamed, Troy Lee, and Dirk Oliver Theis. Fooling-sets and rank. *European Journal of Combinatorics*, 48:143–153, 2015.
- [7] 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.
- [8] Alan Frieze and Michał Karoński. *Introduction to random graphs*. Cambridge University Press, 2015.
- [9] Alexander Golovnev, Oded Regev, and Omri Weinstein. The minrank of random graphs. *arXiv preprint arXiv:1607.04842*, 2016.
- [10] 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.
- [11] 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.
- [12] Leslie Hogben. Minimum rank problems. *Linear Algebra and its Applications*, 432(8):1961–1974, 2010.
- [13] Svante Janson, Tomasz Łuczak, and Andrzej Ruciński. *Random graphs*. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience, New York, 2000.
- [14] Hartmut Klauck and Ronald de Wolf. Fooling one-sided quantum protocols. In *30th International Symposium on Theoretical Aspects of Computer Science*, 2013.
- [15] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, Cambridge, 1997.
- [16] Sudipta Mallik and Bryan L Shader. On graphs of minimum skew rank 4. *Linear and Multilinear Algebra*, 64(2):279–289, 2016.
- [17] Mozghan Pourmoradnasseri. *Some Problems Related to Extensions of Polytopes*. PhD thesis, University of Tartu, Estonia, 2017. [http://ac.cs.ut.ee/files/Mozhgan\\_thesis.pdf](http://ac.cs.ut.ee/files/Mozhgan_thesis.pdf) (final draft).
- [18] 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.