Fooling-sets and rank

Friesen, Mirjam; Hamed, Aya; Lee, Troy; Oliver Theis, Dirk

2015

Friesen, M., Hamed, A., Lee, T., & Oliver Theis, D. (2015). Fooling-sets and rank. European journal of combinatorics, in press.

https://hdl.handle.net/10356/107304

https://doi.org/10.1016/j.ejc.2015.02.016

FOOLING-SETS AND RANK

MIRJAM FRIESEN[a], AYA HAMED[b], TROY LEE[c], AND DIRK OLIVER THEIS[d]

ABSTRACT. An $n \times n$ matrix M is called a *fooling-set matrix of size n* if its diagonal entries are nonzero and $M_{k,\ell}M_{\ell,k} = 0$ for every $k \neq \ell$. Dietzfelbinger, Hromkovič, and Schnitger (1996) showed that $n \leq (\mathrm{rk}\, M)^2$, regardless of over which field the rank is computed, and asked whether the exponent on $\mathrm{rk}\, M$ can be improved.
We settle this question. In characteristic zero, we construct an infinite family of rational fooling-set matrices with size $n = \binom{\mathrm{rk}\, M+1}{2}$. In nonzero characteristic, we construct an infinite family of matrices with $n = (1+o(1))(\mathrm{rk}\, M)^2$.

1. INTRODUCTION

An $n \times n$ matrix M over a field $\mathbb{k}$ is called a *fooling-set matrix of size n* if

$$M_{kk} \neq 0 \qquad \text{for all } k \text{ (its diagonal entries are all nonzero), and} \tag{1a}$$

$$M_{k,\ell}M_{\ell,k} = 0 \qquad \text{for all } k \neq \ell. \tag{1b}$$

Note that the definition depends only on the zero-nonzero pattern of M. The word "fooling set" originates from Communication Complexity, but the concept is used under different names in other contexts (see Section 2).

In Communication Complexity and Combinatorial Optimization fooling-set matrices are used to show lower bounds on other numerical properties of interest. To do this, one wants to find a large fooling-set (sub-)matrix contained in a given matrix A, where permutation of rows and columns is allowed. Since large fooling-set submatrices are typically difficult to identify (deciding whether a fooling-set submatrix of given size exists in a given matrix was recently shown to be NP-hard [Shi13]), it is desirable to upper-bound the size of a fooling-set matrix one may possibly hope for in terms of easily computable properties of A.

Dietzfelbinger, Hromkovič, and Schnitger ([DHS96, Thm. 1.4], or see [KN97, Lemma 4.15]; cf. [KdW12, FKPT13]) proved that the rank of a fooling-set matrix of size n is at least $\sqrt{n}$, i.e.,

$$n \leq (\mathrm{rk}_{\mathbb{k}}\, M)^2. \tag{2}$$

This bound follows as $\mathrm{rk}_{\mathbb{k}}\, I_n = \mathrm{rk}_{\mathbb{k}}\, M \circ M^T \leq (\mathrm{rk}_{\mathbb{k}}\, M)^2$, where I_n is the identity matrix of size n and $\circ$ denotes entrywise product. This inequality gives such an upper bound on the largest fooling-set submatrix in terms of the easily computable rank of A.

Dietzfelbinger et al. asked the question whether the exponent on the rank in the right-hand side of (2) can be improved or not [DHS96, Open Problem 2]. This problem is stated specifically for 0/1-matrices in their paper, mirroring the particular Communication Complexity situation studied there. Klauck and de Wolf [KdW12], however, gave applications and pointed out the importance for Communication Complexity of the question regarding general (i.e., not 0/1) matrices. For applications in Combinatorial Optimization, 0/1 matrices play no special role.

Date: Wed Jan 15 16:13:35 EET 2014

[a] Faculty of Mathematics, Otto von Guericke University Magdeburg, Germany
[b] Work done in part while visiting the Centre for Quantum Technologies, Singapore
[c] School of Physical and Mathematical Sciences, Nanyang Technological University and Centre for Quantum Technologies. This material is based on research supported in part by the Singapore National Research Foundation under NRF RF Award No. NRF-NRFF2013-13.
[d] Institute of Computer Science, University of Tartu, Estonia. dirk.oliver.theis@ut.ee.

Currently, the examples (attributed to M. Hühne in [DHS96]) of fooling-set matrices M with smallest rank are such that $n \approx (\mathrm{rk}_{\mathbb{F}_2} M)^{\log_4 6}$ ($\log_4 6 = 1.292\ldots$); for general matrices, Klauck and de Wolf [KdW12] have given examples with $n \approx (\mathrm{rk}_{\mathbb{Q}} M)^{\log_3 6}$ ($\log_3 6 = 1.63\ldots$).

In this paper, we settle this question. Firstly, for the case that $\mathbb{k}$ has nonzero characteristic, we prove that the inequality (2) is asymptotically tight. Notably, not only is the exponent on the rank in inequality (2) best possible, but so is the constant (one) in front of the rank. We do this by constructing an infinite family fooling-set matrices M over $\mathbb{k} = \mathbb{F}_p$ of size n, for with $n = (1+o(1))(\mathrm{rk}M)^2$. The construction is based on a periodic sequence involving binomial coefficients.[1]

Secondly, in characteristic zero, we prove that the inequality is best possible up to a multiplicative constant, by constructing, for infinitely many n, fooling-set matrices M over $\mathbb{k} = \mathbb{Q}$ of size n, with $n = \binom{\mathrm{rk}M+1}{2}$. This construction is inspired by the relations between binomial coefficients which used in the nonzero characteristic.

The method used in all the *earlier* examples mentioned above of fooling-set matrices with small rank was the following: One conjures up a single, small fooling-set matrix M^0 (of size, say, 6), determines its rank (say, 3), and then uses the tensor-powers of M^0 (which are fooling-set matrices, too). With these numerical values, from M^0, one obtains $\log_3 6$ as a lower bound on the exponent on the rank in (2).

Our constructions are departures from this approach. In the characteristic $k > 0$ case our matrices are circulant. For the characteristic $k = 0$ case, the matrices have a more complicated block structure, but each block is Toeplitz.

After the initial publication of our results, there has been exciting progress on the 0/1 case as well. Shigeta and Amano essentially resolve the original conjecture of Dietzfelbinger et al. giving a construction of a 0/1 fooling set matrix of size n and rank $n^{1/2+o(1)}$ [SA13]. Their construction is very different from the techniques we use here.

Organization of this paper. In the next section we will explain some of the connections of the fooling-set vs. rank problem with Combinatorial Optimization and Graph Theory concepts. In Section 4, we prove our result for nonzero characteristic, and in Section 5, we prove the result for characteristic zero.

In the final section, we discuss some consequences and point to some questions which remain open.

2. Some Remarks on the Importance of Fooling-Set Matrices

While the fooling-set size vs. rank problem is of interest in its own right as a minimum-rank type problem in Combinatorial Matrix Theory, fooling-set matrices are connected to other areas of Mathematics and Computer Science.

In Polytope Theory, given a polytope P, sizes of fooling-set submatrices of appropriately defined matrices provide lower bounds to the number of facets of any polytope Q which can be mapped onto P by a projective mapping. We sketch the connection (see [FKPT13] for the details).

Let P be a polytope. Let $A = A(P)$ be a matrix whose rows are indexed by the facets of P and whose columns are indexed by the vertices of P, and which satisfies $A_{F,v} = 0$, if $v \in F$, and $A_{F,v} \neq 0$, if $v \notin F$. The following was first observed by Yannakakis (see [FKPT13] for a direct proof).

Theorem 1 ([Yan91])**.** *If A has a fooling-set submatrix of size n, then every polytope Q which can be mapped onto P by a projective mapping has at least n facets.*

Since for any fooling-set submatrix of size n of A, the inequality

$$n \leq (\dim P + 1)^2. \tag{3}$$

[1] An extended abstract of this part of the current paper appeared in the EuroComb'13 proceedings [FT13].

follows from (2) (cf. [FKPT13]), the following variant of Dietzfelbinger et al.'s question is of pertinence in Polytope Theory: *Can the fooling-set size vs. dimension inequality* (3) *be improved for polytopes?* Our Theorem 5.1 below yields the following corollary.

Corollary 2. *For infinitely many d, there is a a polytope P of dimension d such that the matrix $A(P)$ contains a fooling-set submatrix of size $\Omega(\sqrt{d})$.*

We do not prove this corollary in this paper, because it would require a considerable amount of polytope theory overhead to arrive at the a comparatively easy consequence of Theorem 5.1. As a quick sketch, let the following suffice. From a given matrix A, one derives a pointed convex polyhedral cone by taking a rank factorization of A'. Intersecting the cone with a hyperplane gives the desired polytope P. The presence of rows/columns in A' which do not correspond to facets/vertices of P is not a problem by Proposition 5.4 in [FKPT13].

In **Combinatorial Optimization,** the polytope theoretic situation occurs for particular families of polytopes which arise from combinatorial optimization problems. Sizes of fooling-set matrices then yield lower bounds to the minimum sizes of Linear Programs for combinatorial optimization problems [Yan91]. See [FKPT13] for bounds based on fooling sets for a number of combinatorial optimization problems, including bipartite matching.

In the Polytope Theory / Combinatorial Optimization applications, we typically have $\mathbb{k} = \mathbb{Q}$, and the rank of the large matrix A is known. However, since the definition of a fooling-set matrix depends only on the zero-nonzero pattern, changing the field from $\mathbb{Q}$ to $\mathbb{k}'$ and replacing the nonzero rational entries of A by nonzero numbers in $\mathbb{k}'$ may yield a matrix with lower rank and hence a better upper bound on the size of a fooling-set matrix.

In Computational Complexity, fooling-set matrices provide lower bounds for the communication complexity of Boolean functions (see, e.g., [AB09, KN97, LS88, DHS96, KdW12]), and for the number of states of an automaton accepting a given language (e.g., [GH06]).

As an example from Communication Complexity where the "fooling-set method" can be seen to yield a poor lower bound is the inner product function

$$f(x,y) = \sum_{j=1}^{n} x_j y_j, \qquad \text{for } x,y \in \mathbb{Z}_2^n.$$

The rank of the associated $2^n \times 2^n$-matrix is n, hence, by (2), there is no fooling-set submatrix larger than n^2.

In Graph Theory, a fooling-set matrix (up to permutation of rows and columns) can be understood as the incidence matrix of a bipartite graph containing a perfect cross-free matching. Recall that a matching in a bipartite graph H is called *cross-free* if no two matching edges induce a C_4-subgraph of H.

Cross-free matchings are best known as a lower bound on the size of biclique coverings of graphs (e.g. [Daw03, JK09]). A *biclique covering* of a graph G is a collection of complete bipartite subgraphs of G such that each edge of G is contained in at least one of these bipartite subgraphs. If a cross-free matching of size n is contained as a subgraph in G, then at least n bicliques are needed to cover all edges of G. For some classes of graphs, this is a sharp lower bound on the biclique covering number [Daw03, ST11].

In Matrix Theory, the maximum size of a fooling-set submatrix is known under a couple of different names, e.g. as independence number [CR93, Lemma 2.4], or as intersection number. For some semirings, this number provides a lower bound for the factorization rank of the matrix over the semiring.

In each of these areas, fooling-set matrices are used as lower bounds. Upon embarking on a search for a big fooling-set matrix in a large, complicated matrix A, one is interested in an *a priori* upper bound on their sizes and thus the potential usefulness of the lower bound method.

3. Preliminaries

We will make use of binomial coefficients and a few of their standard properties. As multiple extensions of binomial coefficients to negative arguments are possible, we fix here the definition we use (following [KGP94]). For intgers n,k, let

$$\binom{n}{k} := \begin{cases} \dfrac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}, & \text{if } k \geq 0, \\ 0, & \text{if } k < 0. \end{cases}$$

Note that the *symmetry identity*

$$\binom{n}{k} = \binom{n}{n-k}, \qquad \text{for all } n \geq 0 \text{ and all integers } k,$$

and the *addition formula*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \qquad \text{for all integers } n,k,$$

hold.

4. Characteristic $p > 0$: Fooling-Set Matrices from Sequences

For a prime number p, we denote by $\mathbb{F}_p$ the finite field with p elements. The following is the accurate statement of our result.

Theorem 4.1. *For every prime number p, there is a family of fooling-set matrices $M^{(t)}$ over $\mathbb{F}_p$ of size $n^{(t)}$, $t = 1,2,3,\ldots$, such that $n^{(t)} \to \infty$, and*

$$\frac{n^{(t)}}{(\mathrm{rk}_{\mathbb{F}_p} M^{(t)})^2} \longrightarrow 1.$$

As noted above, we use linear recurring sequences. For every t, we construct an $n^{(t)}$-periodic function, which gives us a fooling-set matrix of size $n^{(t)}$.

We now describe that construction. Let p be a prime number and $r \geq 2$ an integer. Define the function $f\colon \mathbb{Z} \to \mathbb{F}_p$ by the recurrence relation

$$f(k+r) = -f(k) - f(k+1) \quad \text{for all } k \in \mathbb{Z} \tag{4a}$$

and the initial conditions

$$f(0) = 1, \text{ and } f(1) = \ldots = f(r-1) = 0. \tag{4b}$$

Fix an integer $n > r$. From the sequence, we define an $n \times n$ matrix as follows. For ease of notation, the matrix indices are taken to be in $\{0,\ldots,n-1\} \times \{0,\ldots,n-1\}$. We let

$$M_{k,\ell} := f(k-\ell). \tag{5}$$

It is fairly easy to see that $\mathrm{rk}\, M \leq r$.

Lemma 4.2. *The rank of M is at most r.*

Proof. From (4a), for $k \geq r$, we deduce the equation $M_{k,\star} = -M_{k-r,\star} - M_{k-r+1,\star}$. Hence, each of the rows $M_{k,\star}$, $k \geq r$, is a linear combination of the first r rows of M. □

It can be seen that the rank is, in fact, equal to r: The top-left $r \times r$ submatrix is non-singular because it is upper-triangular with nonzeros along the diagonal.

In the remainder of the section, we derive the fooling-set property. First, we reduce the fooling-set property (1) of M to a property of the function f.

Lemma 4.3. *The matrix M defined in (5) is a fooling-set matrix, if and only if,*

$$f(k)f(-k) = 0 \quad \textit{for all } k \in \{1,\ldots,n-1\}. \tag{6}$$

Proof. It is clear from (4b) and (5) that $M_{j,j} = f(0) = 1$ for all $j = 0,\dots,n-1$, so it remains to verify (1b). Since

$$M_{i,j}M_{j,i} = f(i-j)f(j-i) = f(i-j)f(-(i-j)),$$

if $f(k)f(-k) = 0$ for all $k = 1,\dots,n-1$, then $M_{i,j}M_{j,i}$ is zero whenever $i \neq j$. This proves (1b). □

Given appropriate conditions on r and n (depending on p), this condition on f can indeed be verified:

Lemma 4.4. *For all integers $t \geq 1$, if we let $r := p^t + 1$ and $n := r(r-1)+1$, then $f(k)f(-k) = 0$ for all $k \in \mathbb{Z} \setminus n\mathbb{Z}$.*

Combining the above three lemmas, we can complete the proof of Theorem 4.1.

Proof of Theorem 4.1. Let p be a prime number. For every integer $t \geq 1$, let $r := p^t + 1$ and $n^{(t)} := r(r-1)+1$, and define the matrix $M^{(t)} := M$ over $\mathbb{F}_p$ as in (5). By Lemma 4.2, the rank of $M^{(t)}$ is at most r, and from Lemmas 4.3 and 4.4 we conclude that $M^{(t)}$ is a fooling-set matrix. Hence, we have

$$1 \geq \frac{n^{(t)}}{\mathrm{rk}_{\mathbb{F}_p}(M^{(t)})^2} \geq \frac{r^2-r+1}{r^2} \geq 1 - p^{-t}/4 \xrightarrow{t\to\infty} 1,$$

where the left-most inequality is from (2). □

To prove Lemma 4.4, we need two more lemmas. The first one states that in every section $\{jr,\dots,(j+1)r-1\}$, $j = 0,1,\dots$, there is a block of zeros whose length decreases with j.

Lemma 4.5. *For $j = 0,\dots,r-2$, we have*

$$f(jr+i) = 0 \quad \text{for } i = 1,\dots,r-1-j. \tag{7}$$

Proof. Equation (7) is true for $j = 0$ by (4b). Suppose (7) holds for some $j < r-2$. Then $f((j+1)r+i) = 0$ for $i = 1,\dots,r-1-(j+1)$, because, by (4a),

$$f((j+1)r+i) = f(jr+i+r) = -f(jr+i) - f(jr+(i+1)) = -0-0$$

holds. □

Every function on $\mathbb{Z}$ with values in a finite field which is defined by a (reversible) linear recurrence relation is periodic (cf. e.g. [LN94]). The second lemma establishes that a specific number n is a period of f as defined in (4).

Lemma 4.6. *If $r = p^t + 1$ for some integer $t \geq 1$, then $n := r(r-1)+1$ is a period of the function f.*

Proof. In this proof, for convenience, we identify $\mathbb{F}_p$ with the integers modulo p.

Consider $h(j,i) := f((j+1)r-i)$ for $i,j \in \mathbb{Z}$. We have to show that

$$h(r-1,0) = 0. \tag{8a}$$

$$h(r-1,1) = \dots = h(r-1,r-2) = 0, \text{ and} \tag{8b}$$

$$h(r-1,r-1) = 1. \tag{8c}$$

We will first prove the following claims.

Claim (a). For all $i,j \in \mathbb{Z}$,

$$h(j+1,i) = -h(j,i) - h(j,i-1).$$

Claim (b). For $j = 0,\dots,r-3$

$$h(j,-1) = 0,\ h(j,j+1) = 0.$$

Claim (c). For $j = 0, \dots, r-2$ and $0 \le i \le j$

$$h(j,i) = (-1)^{j+1} \binom{j}{i} \mod p.$$

Before we prove the claims, we show how they imply (8). Recalling the well-known fact that

$$\binom{p^t}{i} = 0 \mod p$$

for every integer $t \ge 1$ and for all $i = 1, \dots, p^t - 1$ (cf. e.g. [LN94]), the equations (8b) follow by applying Claims a and c with $j := r-2$: For $i = 1, \dots, r-2 = p^t - 1$, since

$$h(r-1,i) = -h(r-2,i) - h(r-2,i-1) = \\ = -(-1)^{r-1} \binom{r-2}{i} - (-1)^{r-1} \binom{r-2}{i-1} \mod p,$$

it follows that

$$\begin{aligned} h(r-1,i) &= -\binom{r-1}{i} && \mod p \\ &= -\binom{p^t}{i} && \mod p \\ &= 0 && \mod p. \end{aligned}$$

To prove (8c), we infer from the claims that

$$h(r-1,r-1) = -h(r-2,r-1) - h(r-2,r-2) = \\ - f((r-1)r - r + 1) - (-1)^{r-1} \binom{r-2}{r-2} = \\ - f((r-2)r+1) - (-1)^p = 1,$$

where the last equation follows from Lemma 4.5 and the fact that $-(-1)^p = 1$ even for $p = 2$. Finally, for (8a), we conclude that

$$h(r-1,0) = -h(r-2,0) - h(r-2,-1) = \\ - (-1)^{r-1} \binom{r-2}{0} - f(r^2 - (r-1)) = -(-1)^p - h(r-1,r-1) = \\ - (-1)^p - 1 = 0,$$

where the last-but-one equation follows from (8c).

Proof of Claim (a). This is a straightforward computation. For all j, i, we compute

$$h(j+1,i) = f((j+2)r - i) = \\ f((j+1)r - i + r) = -f((j+1)r - i) - f((j+1)r - (i-1)) = \\ - h(j,i) - h(j,i-1).$$

□

Proof of Claim (b). This claim follows from Lemma 4.5. We have

$$h(j,-1) = f((j+1)r + 1) = 0 \qquad \text{for } j = 0, \dots, r-3,$$

and

$$h(j,j+1) = f((j+1)r - j - 1) = f(jr + r - 1 - j) = 0 \qquad \text{for } j = 0, \dots, r-2.$$

□

Proof of Claim (c). Since $h(0,0) = -1$, Claim (c), follows from Claims (a) and (b). □

This completes the proof of Lemma 4.6. □

Remark 4.7. As seen in the proof, not surprisingly, our recurrence relation (4a) produces binomial coefficients.

However, it would be interesting to know whether there are other linear recurrence relations, $f(k+r)=\sum_{j=0}^{r-1}\alpha_j f(k+j)$, which define circulant fooling-set matrices with the appropriate relation between size and rank. Since all such sequences are periodic, only the conclusion of Lemma 4.4 must be satisfied, and the period must be asymptotic to r^2.

Lemmas 4.5 and 4.6 allow us to prove Lemma 4.4.

Proof of Lemma 4.4. We need to show $f(k)f(-k)=0$ whenever $n\nmid k$. By Lemma 4.6, this is equivalent to showing $f(k)f(n-k)=0$ for $k=1,\dots,n-1$. Given such a k, let j,i be such that $k=jr+i$ and $0\le i\le r-1$.

If $i\le r-1-j$, then $f(k)=0$ by Lemma 4.5, and we are done. If, on the other hand, $i>r-1-j$, then

$$n-k=r^2-r+1-jr-i=(r-1-(j+1))r+(r-i+1),$$

and $r-i+1\le j+1$, so, by Lemma 4.5, we have $f(n-k)=0$. □

5. Characteristic Zero: Fooling-Set Matrices from Binomial Coefficients

We now prove the result in characteristic zero.

Theorem 5.1. *For each $r\ge 1$, there is a fooling-set matrix $M^{(r)}$ over $\mathbb{Q}$ of size $\binom{r+1}{2}$ and rank r.*

The entries of $M^{(r)}$ are binomial coefficients, up to sign. As in the previous section, the low rank property will follow from the binomial addition identity. Whereas the matrix in the previous section is circulant, this matrix has a more complicated block structure but each block is Toeplitz.

We now describe the construction of the matrices $M^{(r)}$. To get some feeling for these matrices, here are the first few examples

$$M^{(1)}=\begin{pmatrix}1\end{pmatrix},\ M^{(2)}=\begin{pmatrix}1&0&1\\-1&1&0\\0&1&1\end{pmatrix},\ M^{(3)}=\begin{pmatrix}1&0&0&1&-1&1\\-1&1&0&0&1&0\\1&-1&1&-1&0&0\\0&1&0&1&0&1\\0&0&1&-1&1&0\\0&1&1&0&1&1\end{pmatrix}.$$

The recursive structure of $M^{(r)}$ can be seen from these examples[2]. In general, the top left $r\times r$ principal submatrix of $M^{(r)}$ will be lower triangular with ones of alternating sign, and the bottom right $\binom{r}{2}$-sized principal submatrix will be $M^{(r-1)}$.

We now give the details of the construction. First we define, for each integer t, a function $f_t\colon \mathbb{N}\times\mathbb{N}\to\mathbb{Z}$ (with $\mathbb{N}:=\{1,2,3,\dots\}$). These functions will be used in the construction. They can be thought of as infinite matrices, and we will use the notation $f_t^{r,s}$ to specify the $r\times s$ matrix

$$\left(f_t^{r,s}\right)_{i,j}:=f_t(i,j),\qquad \text{for } i=1,\dots,r \text{ and } j=1,\dots,s.$$

[2]If the reader wants to see larger examples, Matlab code to construct $M^{(r)}$ can be found at https://github.com/troyjlee/hadamard_factorization.

Let $t \in \mathbb{Z}$ and $i, j \in \mathbb{N}$. The function f_t is defined as

$$f_t(i,j) := \begin{cases} \binom{t-1}{j-i-1}, & \text{if } t > 0, \\ (-1)^{j-i}\binom{-t-1+j-i}{-t-1}, & \text{if } t \leq 0 \text{ and } i < j, \\ (-1)^{i-j-t}\binom{i-j-1}{-t}, & \text{if } t \leq 0 \text{ and } i \geq j. \end{cases}$$

Note that in each case, $f_t(i,j)$ depends on the difference $i-j$ only, thus each f_t is Toeplitz. When $t > 0$, we see that $f_t(i,j) = 0$ whenever $i \geq j$ meaning that these f_t are upper triangular. When $t = 0$, the definition simplifies to $f_0(i,j) = \binom{-1}{i-j}$, thus f_0 is lower triangular with ones on the main diagonal.

To get a better idea where the f_t come from, consider an extended Pascal's triangle where the upper and lower indices begin from -1. In the following table, the entries are binomial coefficients where upper indices label the rows, lower indices label the columns.

	-1	0	1	2	3	4
-1	0	1	-1	1	-1	1
0	0	1	0	0	0	0
1	0	1	1	0	0	0
2	0	1	2	1	0	0
3	0	1	3	3	1	0
4	0	1	4	6	4	1

The matrix f_t for $t > 0$ is the infinite Toeplitz matrix whose first row is given by the row of Pascal's triangle indexed by $t-1$, and whose first column is all zero. For $t < 0$, up to signs, f_t is the infinite Toeplitz matrix whose first column is given by the column of Pascal's triangle indexed by $-t$ and whose first row is given by the $-t-1$ column of Pascal's triangle, starting from the row indexed by $-t-1$.

Using the f_t we can now construct the fooling-set matrices $M^{(r)}$. For $r \geq 1$, let $M^{(r)}$ be a matrix of size $\binom{r+1}{2}$ defined as

$$M^{(r)} = \begin{pmatrix} f_0^{r,r} & f_{-1}^{r,r-1} & f_{-2}^{r,r-2} & \cdots & f_{-r+1}^{r,1} \\ f_1^{r-1,r} & f_0^{r-1,r-1} & f_{-1}^{r-1,r-2} & & f_{-r+2}^{r-1,1} \\ f_2^{r-2,r} & f_1^{r-2,r-1} & f_0^{r-2,r-2} & & f_{-r+3}^{r-2,1} \\ \vdots & & & \ddots & \vdots \\ f_{r-1}^{1,r} & f_{r-2}^{1,r-1} & \cdots & \cdots & f_0^{1,1} \end{pmatrix}$$

The size of $M^{(r)}$ is clearly $\binom{r+1}{2}$. That $M^{(r)}$ is a fooling-set matrix and has rank r will be shown in the next lemmas.

We first show that $M^{(r)}$ is a fooling-set matrix. This follows from the fact that f_0 is lower triangular and that in the above extended Pascal's triangle for $t > 0$ the row indexed by $t-1$ and column indexed by t are disjoint.

Lemma 5.2. *$M^{(r)}$ is a fooling-set matrix.*

Proof. The diagonal entries of $M^{(r)}$ are 1 as desired. To show that $M^{(r)}(i,j)M^{(r)}(j,i) = 0$ for $i \neq j$, it suffices to show that $f_t(i,j)f_{-t}(j,i) = 0$ for each t. This clearly holds for $t = 0$ as f_0 is lower triangular. Now suppose $t > 0$. If $i \geq j$ then $f_t(i,j) = 0$ thus in this case we are also fine. In the case $j > i$ we have

$$|f_t(i,j)||f_{-t}(j,i)| = \binom{t-1}{j-i-1}\binom{j-i-1}{t} = 0.$$

The second term is zero for $j-i \leq t$ while the first term is zero for $j-i \geq t+1$, thus the product is always zero. □

In fact, $M^{(r)}$ has the stronger property that exactly one of $M^{(r)}(i,j), M^{(r)}(j,i)$ is zero for $i \neq j$.

We now come to the rank of $M^{(r)}$. The following claim is the key to prove $\mathrm{rk}(M^{(r)}) \leq r$.

Lemma 5.3. *For any $t \in \mathbb{Z}$ and $i, j \in \mathbb{N}$*

$$f_t(i,j) = f_{t-1}(i,j) + f_{t-1}(i+1,j).$$

Proof. We break the proof into three cases depending on the value of t.
Case 1: $t > 1$. This case follows from the binomial addition formula

$$\begin{aligned} f_t(i,j) = \binom{t-1}{j-i-1} &= \binom{t-2}{j-i-1} + \binom{t-2}{j-i-2} \\ &= f_{t-1}(i,j) + f_{t-1}(i+1,j) \ . \end{aligned}$$

Case 2: $t = 1$. In this case we use the symmetry identity together with binomial addition formula.

$$\begin{aligned} f_1(i,j) = \binom{0}{j-i-1} = \binom{0}{i-j+1} &= \binom{-1}{i-j} + \binom{-1}{i-j+1} \\ &= f_0(i,j) + f_0(i+1,j) \ . \end{aligned}$$

Case 3: $t \leq 0$. First consider the case $i \geq j$. Then again by the binomial addition formula

$$\begin{aligned} f_t(i,j) &= (-1)^{i-j-t} \binom{i-j-1}{-t} \\ &= (-1)^{i-j-t} \left(-\binom{i-j-1}{-t+1} + \binom{i-j}{-t+1} \right) \\ &= (-1)^{i-j-t+1} \binom{i-j-1}{-t+1} + (-1)^{i-j-t+2} \binom{i-j}{-t+1} \\ &= f_{t-1}(i,j) + f_{t-1}(i+1,j) \ . \end{aligned}$$

Finally, consider the case $i < j$. This case requires some care as it could be that $i+1 = j$. For $t < 0$, however, notice that the two formulas defining f_t agree when $i = j$. The first gives $(-1)^{j-i}$ and the second $(-1)^{i-j-t}(-1)^{-t} = (-1)^{j-i}$. Thus when $t < 0$ and $i = j$ the two formulas in the definition are consistent. As we are in Case 3, we are safe expressing $f_{t-1}(i+1,j)$ using the formula for $i < j$ as $t \leq 0$.

$$\begin{aligned} f_t(i,j) &= (-1)^{j-i} \binom{-t-1+j-i}{-t-1} \\ &= (-1)^{j-i} \left(\binom{-t+j-i}{-t} - \binom{-t+j-i-1}{-t} \right) \\ &= (-1)^{j-i} \binom{-t+j-i}{-t} + (-1)^{j-i-1} \binom{-t+j-i-1}{-t} \\ &= f_{t-1}(i,j) + f_{t-1}(i+1,j) \ . \end{aligned}$$

□

Lemma 5.4. *The rank of $M^{(r)}$ is r.*

Proof. The rank of $M^{(r)}$ is at least r, because the submatrix $f_0^{r,r}$ has rank r.

Lemma 5.3 shows that all rows of $M^{(r)}$ can be expressed as linear combinations of the first r rows, thus also $\mathrm{rk}(M^{(r)}) \leq r$. □

Putting it all together, Theorem 5.1 is obtained from Lemma 5.2 and Lemma 5.4.

6. Conclusion

We conclude by discussing some questions which remain open.

First of all, in characteristic zero, it would be interesting to know whether inequality (2) is asymptotically tight, or, more generally:

Question 6.1. *What is smallest constant C such that $n \leq C\,(\mathrm{rk}_{\mathbb{k}} M)^2$ for all $n \times n$ fooling-set matrices M over a field $\mathbb{k}$ of characteristic zero?*

There is a possibility that, in characteristic zero, the minimum achievable rank on the right hand side of inequality (2) may depend not only on the characteristic, but on the field $\mathbb{k}$ itself. Indeed, there are examples of zero-nonzero patterns for which the minimum rank of a matrix with that zero-nonzero pattern differs between $\mathbb{k} = \mathbb{Q}$ and $\mathbb{k} = \mathbb{R}$, see e.g. [KBR08].

Secondly, while the construction in Section 4 for nonzero characteristic gives circulant matrices, the matrices in Section 5 are not circulant.

Question 6.2. *Can the exponent on the rank in the inequality (2) be improved for circulant fooling-set matrices over $\mathbb{k}$ with characteristic zero?*

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational complexity*. Cambridge University Press, Cambridge, 2009. A modern approach.

[CR93] Joel E. Cohen and Uriel G. Rothblum. Nonnegative ranks, decompositions, and factorizations of nonnegative matrices. *Linear Algebra Appl.*, 190:149–168, 1993.

[Daw03] Milind Dawande. A notion of cross-perfect bipartite graphs. *Inform. Process. Lett.*, 88(4):143–147, 2003.

[DHS96] 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).

[FKPT13] Samuel Fiorini, Volker Kaibel, Kanstantin Pashkovich, and Dirk Oliver Theis. Combinatorial bounds on nonnegative rank and extended formulations. arXiv:1111.0444) (to appear in *Discrete Math.*), 2013+.

[FT13] 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.

[GH06] Hermann Gruber and Markus Holzer. Finding lower bounds for nondeterministic state complexity is hard (extended abstract). In *Developments in language theory*, volume 4036 of *Lecture Notes in Comput. Sci.*, pages 363–374. Springer, Berlin, 2006.

[JK09] S. Jukna and A. S. Kulikov. On covering graphs by complete bipartite subgraphs. *Discrete Math.*, 309(10):3399–3403, 2009.

[KBR08] Swastik Kopparty and K. P. S. Bhaskara Rao. The minimum rank problem: a counterexample. *Linear Algebra Appl.*, 428(7):1761–1765, 2008.

[KdW12] Hartmut Klauck and Ronald de Wolf. Fooling one-sided quantum protocols. arXiv:1204.4619, 2012.

[KGP94] Donald Knuth, Ronald Graham, and Oren Patashnik. *Concrete Mathematics*. Addison-Wesley, 1994.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, Cambridge, 1997.

[LN94] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, first edition, 1994.

[LS88] L. Lovász and M. Saks. Möbius functions and communication complexity. In *Proc. 29th IEEE FOCS*, pages 81–90. IEEE, 1988.

[SA13] M. Shigeta and K. Amano. Ordered biclique partitions and communication complexity problems. Technical Report arXiv:1311.6192, arXiv, 2013.

[Shi13] Yaroslav Shitov. On the complexity of Boolean matrix ranks. *Linear Algebra and Its Applications*, 439:2500–2502, 2013.

[ST11] José A. Soto and Claudio Telha. Jump number of two-directional orthogonal ray graphs. In *Integer programming and combinatorial optimization*, volume 6655 of *Lecture Notes in Comput. Sci.*, pages 389–403. Springer, Heidelberg, 2011.

[Yan91] Mihalis Yannakakis. Expressing combinatorial optimization problems by linear programs. *J. Comput. System Sci.*, 43(3):441–466, 1991.