A Note on Explicit Ramsey Graphs and Modular Sieves

Vince Grolmusz
Department of Computer Science
Eötvös University, H-1117 Budapest
HUNGARY
E-mail: grolmusz@cs.elte.hu

Abstract

In a previous work [4] we found a relation between the ranks of co-diagonal matrices (matrices with 0's in their diagonal and non-zeroes elsewhere) and the quality of explicit Ramsey-graph constructions. We also gave there a construction based on the BBR-polynomial of Barrington, Beigel and Rudich [1]. In the present work we give another construction for low-rank co-diagonal matrices, based on a modular sieve formula.

Keywords: composite modulus, explicit Ramsey-graph constructions, matrices over rings, co-diagonal matrices, modular sieve

1 Introduction

Constructing large graphs with small homogeneous vertex sets is a long-standing challenge for combinatorists. The seminal paper of Erdős [2] proved the existence of an $O(2^{t/2})$-vertex graph without a t-vertex clique or a t-vertex independent set, but the best construction to date — due to Frankl and Wilson [3] — gives a graph with

$$\exp\left((\frac{1}{4}-\varepsilon)\frac{(\log t)^2}{\log\log t}\right)$$

vertices. We proved matching bounds in [5], with a method generalizable to explicit Ramsey-colorings with more than two colors.

In the paper [4] we have found a relation between low-rank co-diagonal matrices and Ramsey-graphs.

Definition 1 ([4]) *Let R be a ring and let n be a positive integer. We say, that the $n \times n$ matrix $A = \{a_{ij}\}$ is a co-diagonal matrix over R, if $a_{ij} \in R,\ i,j = 1,2,\ldots,n$ and $a_{ii} = 0, a_{ij} \neq 0$, for all $i,j = 1,2,\ldots,n,\ i \neq j$.*

We say, that A is an upper co-triangle matrix over R, if $a_{ij} \in R,\ i,j = 1,2,\ldots,n$ and $a_{ii} = 0, a_{ij} \neq 0$, for all $1 \leq i < j \leq n$. A is a lower co-triangle matrix over R, if $a_{ij} \in R,\ i,j = 1,2,\ldots,n$ and $a_{ii} = 0, a_{ij} \neq 0$, for all $1 \leq j < i \leq n$. A matrix is co-triangle, if it is either lower- or upper co-triangle.

To formalize the connection between Ramsey-graphs and matrices, we also need the definition of the rank of a matrix over a ring; (see e.g., [6]).

Definition 2 *Let R be a ring and let n be a positive integer. We say, that the $n \times n$ matrix A over R has rank 0, if all of the elements of A are 0. Otherwise, the rank over the ring R of matrix A is the smallest r, such that A can be written as*

$$A = BC$$

over R, where B is an $n \times r$ and C is an $r \times n$ matrix. The rank of A over R is denoted by $\mathrm{rank}_R(A)$.

The following theorem establishes the connection between the low-rank co-triangle (or co-diagonal) matrices and Ramsey-graphs; the proof of that theorem is constructive: that means, that if a matrix is given constructively, then the Ramsey-graph is also given constructively.

Theorem 3 ([4]) *Let $A = \{a_{ij}\}$ be an $n \times n$ co-triangle matrix over $R = Z_6$, with $r = \mathrm{rank}_{Z_6}(A)$. Then there exists an n-vertex graph G, containing neither a clique of size $r+2$ nor an anti-clique of size*

$$\binom{r+1}{2} + 2.$$

□

In [4] we have given an explicit construction for a $\mathrm{rank}_{Z_6}(A) \leq 2^{c\sqrt{\log n(\log\log n)}}$-matrix of size $n \times n$, using the BBR-polynomial of Barrington, Beigel and Rudich [1]. An easy computation shows that this matrix-construction together with Theorem 3 imply an explicit Ramsey-graph with homogeneous sets of the same logarithmic order of magnitude as the result of Frankl and Wilson [3]. Now we give another construction for low mod 6 rank co-diagonal matrices using modular sieves. This construction is our main result here.

2 Our Construction

2.1 A logarithmic-rank co-diagonal matrix

The first step in the construction is a co-diagonal matrix suitable for large moduli. The next step is the modification of that construction for small composite moduli, say 6. The basic idea is to construct an $n \times n$ co-diagonal matrix A by a sum of a small number of rank-1 0-1 matrices.

Then A will have a small rank, because of the following easy lemma from [4]:

Lemma 4 ([4]) *Let R be a ring and let A and A' be two $n \times n$ matrices. Then* $\mathrm{rank}_R(A + A') \leq \mathrm{rank}_R(A) + \mathrm{rank}_R(A')$.

□

Consequently, if we get a co-diagonal matrix as a sum of – say – z rank-1 matrices, then its rank is at most z.

For simplicity, we identify these rank-1 0-1 matrices by the positions of the entries, containing 1. For example, $W = \{(i.j) : i \in I, j \in J\}$ denotes an $n \times n$ 0-1 matrix $\{w_{ij}\}$, where $w_{ij} = 1 \iff i \in I, j \in J$.

First, let us see a construction for a $2\lceil\log(n+1)\rceil$-rank co-diagonal matrix. Let us consider the following $n \times n$ rank-1 matrices:

$$U_t = \{(i,j) : i_t = 0, j_t = 1\}; \quad V_t = \{(i,j) : i_t = 1, j_t = 0\}$$

where i_t and j_t denotes the t^{th} bit in the binary form of $1 \leq i \leq n$ and $1 \leq j \leq n$, respectively, and let

$$A = \sum_{t=1}^{\lceil\log(n+1)\rceil} (U_t + V_t).$$

Clearly, both U_t and V_t are rank-1 0-1 matrices, their combined number is $2\lceil\log(n+1)\rceil$, and the 1's in them cover all the off-diagonal elements of A.

Consequently, the rank of A is at most $2\lceil\log(n+1)\rceil$. It is also obvious, that entry a_{ij} of matrix A is covered $H_2(i,j)$-times, where $H_2(i,j)$ stands for the Hamming-distance of the binary forms of i and j. Consequently, the entries of A are less than or equal to $\lceil\log(n+1)\rceil$.

For our results, we need a somewhat different initial cover. For the definition of this cover, let us represent the indices not in binary, but rather in N-ary form, for $N=\lceil\log n\rceil$. That is, for $1\le i,j\le n$, let i_t, j_t be the N-ary digits of i and j, respectively. Let $g=\lceil\log_N(n+1)\rceil$. Then let us define for $t=1,2,\ldots,g$, and $\ell=0,1,\ldots,N-1$:

$$U_t^\ell=\{(i,j): i_t=\ell, j_t\neq\ell\},$$

and let

$$\hat{A}=\sum_{\substack{t\in\{1,2,\ldots,g\}\\ \ell\in\underline{N}}} U_t^\ell,$$

where $\underline{N}$ denotes the set $\{0,1,\ldots,N-1\}$. Then any non-diagonal element will be covered by $H_N(i,j)$-times, where $H_N(i,j)$ stands for the Hamming-distance of the N-ary forms of i and j, that is, at most g-times.

Clearly, for large enough n, $g\ge 6$, so the cover by the sets U_t^ℓ will not define a co-diagonal matrix modulo 6; the entries, where the Hamming-distance is a multiple of 6, will be covered only 0 times mod 6.

One possible remedy to this problem is getting rid of the multiple covers, using a sieve-formula.

Let us recall, that we identify the rank-1 0-1 matrices by the positions of the entries, containing 1. Consequently, for any $I\subset\{1,2,\ldots,g\}$, and for any $(\ell_1,\ell_2,\ldots,\ell_{|I|})\in\underline{N}^{|I|}$, matrix $\bigcap_{t\in I}U_t^{\ell_t}$ denotes the rank-1 0-1 matrix with 1's exactly in the positions (i,j), where for *all* $t\in I$: $i_t=\ell_t\neq j_t$ are satisfied. Now let us consider the following sieve:

$$B=\sum_{I\subset\{1,2,\ldots,g\}}(-1)^{|I|+1}\left(\sum_{(\ell_1,\ell_2,\ldots,\ell_{|I|})\in\underline{N}^{|I|}}\ \bigcap_{t\in I}U_t^{\ell_t}\right). \qquad (1)$$

Note, that $B=\{b_{ij}\}$ is an $n\times n$ matrix.

If the entries of $\hat{A}$ are denoted by $\hat{a}_{ij}$, then for any $i\neq j$ if $\hat{a}_{ij}=s$, that is, the position (i,j) is covered s-times, then

$$b_{ij} = \binom{s}{1} - \binom{s}{2} + \cdots \pm \binom{s}{s} = 1, \tag{2}$$

and $b_{ii} = 0$, for all i's. So, clearly, B is a special co-diagonal matrix of the form

$$J - I,$$

where J is the all-1, and I is the identity-matrix of size $n \times n$. However, the rank of B is too high for any use in Theorem 3.

2.2 The Modular Sieve

Now we will cut the tail of the sieve of (1), getting a sum-matrix of low rank modulo 6. The method is similar to the construction of the BBR polynomial [1].

Let μ be the smallest integer that $2^\mu > \sqrt{g}$, and let ν be the smallest integer that $3^\nu > \sqrt{g}$.

Let us consider now the following two $n \times n$ matrices, defined with sieves:

$$C = \sum_{\substack{I \subset \{1,2,\ldots,g\} \\ |I| < 2^\mu}} (-1)^{|I|+1} \left(\sum_{(\ell_1,\ell_2,\ldots,\ell_{|I|}) \in \underline{N}^{|I|}} \bigcap_{t \in I} U_t^{\ell_t} \right), \tag{3}$$

and

$$D = \sum_{\substack{I \subset \{1,2,\ldots,g\} \\ |I| < 3^\nu}} (-1)^{|I|+1} \left(\sum_{(\ell_1,\ell_2,\ldots,\ell_{|I|}) \in \underline{N}^{|I|}} \bigcap_{t \in I} U_t^{\ell_t} \right). \tag{4}$$

Now we can state our main Lemma:

Lemma 5 *The matrix $3C + 4D$ is co-diagonal modulo 6, and its rank over Z_6 is* $\exp(O(\sqrt{\log n \log\log n}))$.

Proof.

For the entries c_{ij} of the matrix C we can give a similar formula that was given in (2). Again, let i and j be chosen so that $\hat{a}_{ij} = s$, then there are two cases.

Case 1: $s < 2^\mu$.

$$c_{ij} = \binom{s}{1} - \binom{s}{2} + \cdots \pm \binom{s}{s} = 1. \tag{5}$$

In Case 1 there are no problems, for an arbitrary modulus, c_{ij} is non-0.

Case 2: $s \geq 2^\mu$.

$$c_{ij} = \binom{s}{1} - \binom{s}{2} + \cdots + \binom{s}{2^\mu - 1}. \tag{6}$$

At this point we need a simple Lemma, its proof can be found e.g. in [5].

Lemma 6 *Let p be a prime, k, j, e non-negative integers, $e \geq 1$. For any $k < p^e$,*

$$\binom{j+p^e}{k} \equiv \binom{j}{k} \pmod{p}.$$

□

Now we deal with Case 2. Let $s' = s \bmod 2^\mu$, that is, $0 \leq s' < 2^\mu$, $s' \equiv s \pmod{2^\mu}$. From (6):

$$c_{ij} \equiv \binom{s'}{1} - \binom{s'}{2} + \cdots + \binom{s'}{s'} \pmod{2}, \tag{7}$$

That means that $c_{ij} \equiv 0 \pmod 2$ if $s = H_N(i,j)$ is a multiple of 2^μ and it is 1 modulo 2 otherwise.

An analogous proof shows for $D = \{d_{ij}\}$ of (4) that $d_{ij} \equiv 0 \pmod 3$ if $s = H_N(i,j)$ is a multiple of 3^ν and it is 1 modulo 3 otherwise.

Note, that $2^\mu 3^\nu > g = \lceil \log_N (n+1) \rceil$, that is, it is larger than the maximum Hamming-distance between any i and j, for any fixed $i \neq j$. So $c_{ij} \equiv 0 \pmod 2$ and $d_{ij} \equiv 0 \pmod 3$ cannot hold simultaneously. Consequently, the matrix $3C + 4D$ will be co-diagonal modulo 6, and its rank is at most the combined number of the rank-1 matrices in equations (3) and (4), that is $\exp\left(\sqrt{\log n \log\log n}\right)$.□

References

[1] D. A. M. Barrington, R. Beigel, and S. Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Comput. Complexity*, 4:367–382, 1994. Appeared also in *Proc. 24th Ann. ACM Symp. Theor. Comput.*, 1992.

[2] P. Erdős. Some remarks on the theory of graphs. *Bull. A.M.S.*, 53:292–294, 1947.

[3] P. Frankl and R. M. Wilson. Intersection theorems with geometric consequences. *Combinatorica*, 1(4):357–368, 1981.

[4] V. Grolmusz. Low-rank co-diagonal matrices and Ramsey graphs. *The Electronic Journal of Combinatorics*, 7:R15, 2000. www.combinatorics.org.

[5] V. Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20:73–88, 2000.

[6] C. Meinel and S. Waack. The Möbius function, variations ranks, and $\theta(n)$–bounds on the modular communication complexity of the undirected graph connectivity problem. Technical Report TR94-022, ECCC, 1994.