Low Rank Co-Diagonal Matrices and Ramsey Graphs

Vince Grolmusz
Department of Computer Science
Eötvös University, H-1053 Budapest
HUNGARY
E-mail: grolmusz@cs.elte.hu
Submitted: March 7, 2000. Accepted: March 12, 2000

Abstract

We examine $n \times n$ matrices over Z_m, with 0's in the diagonal and nonzeros elsewhere. If m is a prime, then such matrices have large rank (i.e., $n^{1/(p-1)} - O(1)$). If m is a non-prime-power integer, then we show that their rank can be much smaller. For $m = 6$ we construct a matrix of rank $\exp(c\sqrt{\log n \log\log n})$. We also show, that explicit constructions of such low rank matrices imply explicit constructions of Ramsey graphs.

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

1 Introduction

In this work we examine matrices over a ring R, such that the diagonal elements of the matrix are all 0's, but the elements off the diagonal are not zero (we shall call these matrices co-diagonal over R). We define the rank of a matrix over a ring, and show that low rank co-diagonal matrices over Z_6 naturally correspond to graphs with small homogenous vertex sets (i.e., cliques and anti-cliques). Consequently, explicitly constructible low rank co-diagonal matrices over Z_6 imply explicit Ramsey graph constructions. Our best construction reproduces the logarithmic order of magnitude of the Ramsey-graph of *Frankl* and *Wilson* [5], continuing the sequence of results on new explicit Ramsey graph constructions of *Alon* [1] and *Grolmusz* [6]. Our present result, analogously to the constructions of [6] and [1], can be generalized to more than one color.

Our results give a recipe for constructing explicit Ramsey graphs from explicit low rank co-diagonal matrices over Z_6, analogously to the way that our results gave a method for constructing explicit Ramsey graphs from certain low degree polynomials over Z_6 in [6]. In this sense, our results may lead to improved Ramsey graph constructions, if lower rank co-diagonal matrix constructions exist.

Definition 1 *Let R be a ring and let n be a positive integer. We say, that $n \times n$ 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.

We will also need the definition of the rank of a matrix with elements in a ring. The following definition is a generalization of the matrix rank over fields to matrices over rings:

Definition 2 *Let R be a ring and let n be a positive integer. We say, that $n \times n$ 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 $\mathrm{rank}_R(A)$.

It is easy to see, that this definition of the matrix rank coincides with the usual matrix-rank over R, when R is a field. The following property of the usual matrix rank also holds:

Lemma 3 *Let R be a ring and let A and A' be two $n \times n$ matrices. Then* $\mathrm{rank}_R(A + A') \leq \mathrm{rank}_R(A) + \mathrm{rank}_R(A')$.

Proof: Let $A = BC$ and $A' = B'C'$, where B is an $n \times r$ and C is an $r \times n$ matrix, while B' is an $n \times r'$ and C' is an $r' \times n$ matrix. Then $A + A'$ can be given as $B''C''$, where B'' is an $n \times (r + r')$ matrix, formed from the union of the columns of B and B', and C'' is an $(r + r') \times n$ matrix, formed from the union of rows of C and C'. □

The following theorem shows, that for any prime p, the co-triangle (and, consequently, the co-diagonal) matrices over the p-element field have large rank:

Theorem 4 *Let p be a prime, and let A be an $n \times n$ co-triangle matrix over GF_p. Then*

$$\mathrm{rank}_{\mathrm{GF}_p}(A) \geq n^{1/(p-1)} - p.$$

Proof: We may assume that A is a lower co-triangle matrix. Let $r = \text{rank}_{\text{GF}_p}(A)$, and let $B = \{b_{ij}\}$ be an $n \times r$, $C = \{c_{ij}\}$ be an $r \times n$ matrix over GF_p, such that:

$$A = BC. \tag{1}$$

For $i = 1, 2, \ldots, n$ let us consider the following polynomials:

$$P_i(x_1, x_2, \ldots, x_r) = \sum_{k=1}^{r} b_{ik} x_j. \tag{2}$$

From (1),

$$P_i(c_{1j}, c_{2j}, \ldots, c_{rj}) = \begin{cases} 0, & \text{if } i = j, \\ \neq 0, & \text{if } i > j. \end{cases}$$

Consequently, by the triangle criterion [2], polynomials

$$Q_i(x_1, x_2, \ldots, x_r) = 1 - P_i^{p-1}(x_1, x_2, \ldots, x_r),$$

for $i = 1, 2, \ldots, n$, form a linearly independent set in the vector space of dimension

$$\binom{r+p-2}{p-1} + 1$$

of polynomials of form $Q + \alpha$, where Q is an r-variable homogeneous polynomial of degree $p - 1$ and $\alpha \in \text{GF}_p$. (To prove this without the triangle criterion of [2], one should observe that Q_k is zero on column i of matrix C for $i < k$, and it is 1 for column k of C; so Q_i cannot be given as a linear combination of some Q_{k_j}'s, each $k_j > i$.) Consequently,

$$n \leq \binom{r+p-2}{p-1} + 1 \leq (r+p)^{p-1}. \tag{3}$$

□

We are interested in the following question:

Question. *Let $R = Z_m$, what is the minimum rank of an $n \times n$ co-triangle (or co-diagonal) matrix over R?*

If $m = p$ a prime, then by Theorem 4 we have that the rank should be at least $n^{1/p-1} - p$. What can we say for non-prime m's?

The main motivation of this question is the following theorem:

Theorem 5 *Let $A = \{a_{ij}\}$ be an $n \times n$ co-triangle matrix over $R = Z_6$, with $r = \text{rank}_{Z_6}(A)$. Then there exists an n-vertex graph G, containing neither a clique of size $r + 2$ nor an anti-clique of size*

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

Proof: Suppose, that A is a lower co-triangle matrix. If the Z_6 rank of A is r, then both the GF_2 and GF_3 ranks of A are at most r. Let $V = \{v_1, v_2, \ldots, v_n\}$. For any $i > j$, let us connect v_i and v_j with an edge, if a_{ij} is odd. Then any clique of size t will correspond to a $t \times t$ lower co-triangle minor over GF_2, so from (3),

$$t \leq r + 1.$$

Any anti-clique of size t will correspond to a $t \times t$ lower co-triangle minor over GF_3, so from (3),

$$t \leq \binom{r+1}{2} + 1. \tag{4}$$

□

From Theorem 5 one can get a lower bound for the rank, using estimations for the Ramsey numbers. Our original bound was significantly improved by *Noga Alon*, who allowed us to include his proof here.

Theorem 6 *Let $A = \{a_{ij}\}$ be an $n \times n$ co-triangle matrix over $R = Z_6$. Then*

$$\text{rank}_{Z_6}(A) \geq \frac{\log n}{2 \log \log n} - 2.$$

Proof: By the result of *Ramsey* [7] and *Erdős* and *Szekeres* [4], every n-vertex graph has either a clique on k, or an anti-clique on ℓ vertices, if

$$n \geq \binom{k+\ell-2}{k-1}.$$

If we set $k = \lfloor \frac{1}{2} \frac{\log n}{\log \log n} \rfloor$, and $\ell = \lfloor \log^2 n \rfloor$, then we get from Theorem 5, that both $r + 2 \leq k$ and $\binom{r+1}{2} + 2 \leq \ell$ cannot be satisfied, and this completes the proof. □

The proof of Theorem 5 also proves

Theorem 7 *Suppose, that there exists an explicitly constructible $n \times n$ co-triangle matrix $A = \{a_{ij}\}$ over $R = Z_6$, with $r = \text{rank}_{Z_6}(A)$. Then one can explicitly construct an n-vertex Ramsey-graph, without homogenous vertex-sets of size*

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

□

Our main result is that there do exist explicitly constructible low-rank co-diagonal matrices over Z_6, implying explicit Ramsey-graph constructions.

Theorem 8 *There exists a $c > 0$ such that for all positive integer n, there exists an explicitly constructible $n \times n$ co-diagonal matrix $A = \{a_{ij}\}$ over $R = Z_6$, with*

$$\mathrm{rank}_{Z_6}(A) \le 2^{c\sqrt{\log n \log\log n}}.$$

Theorem 8 together with Theorem 5, gives an explicit Ramsey-graph construction on n vertices, without a homogeneous vertex-set of size $2^{c'\sqrt{\log n \log\log n}}$, for some $c' > 0$, or in other words, an explicit Ramsey-graph construction on

$$2^{\frac{c'' \log^2 t}{\log\log t}}$$

vertices, without homogeneous vertex-set of size t, for some $c'' > 0$. This bound was first proven by *Frankl* and *Wilson* [5] with a larger (better) constant than our c'', using the famous Frankl-Wilson theorem [5]. We also gave a construction, using the BBR polynomial [3] and also the Frankl-Wilson theorem in [6].

A generalization of our main result for ring Z_m, where m has more than two prime divisors:

Theorem 9 *For any $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\ell^{\alpha_\ell}$, where the p_i's are distinct primes, there exists a $c = c_m > 0$ such that for all positive integer n, there exists an explicitly constructible $n \times n$ co-diagonal matrix $A = \{a_{ij}\}$ over $R = Z_m$, with*

$$\mathrm{rank}_{Z_m}(A) \le 2^{c\sqrt[\ell]{\log n (\log\log n)^{\ell-1}}}.$$

2 Constructing Low Rank mod 6 Co-Diagonal Matrices

In this section we prove Theorems 8 and 9.

Our main tool is the following theorem (choosing $m = 6$ and $\ell = 2$):

Theorem 10 (Barrington, Beigel, Rudich[3]) *Given $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\ell^{\alpha_\ell}$ where the p_i are distinct primes, then there exists an explicitly constructible multi-linear polynomial P with integer coefficients, with k variables, and of degree $O(k^{1/\ell})$ which satisfies for $x \in \{0,1\}^k$, that $P(x) = 0$ over Z_m iff $x = (0, 0, \ldots, 0)$.*

□

Let k be the smallest integer such that $n \le k^k$. Let $B = \{0, 1, 2, \ldots, k-1\}$. Let us define $\delta : B \times B \to \{0, 1\}$ as follows:

$$\delta(u, v) = \begin{cases} 1, & \text{if } u = v, \\ 0 & \text{otherwise.} \end{cases}$$

Then matrix $\bar{A}$ is defined as follows: both the rows and the columns of $\bar{A}$ correspond to the elements of the set B^k. The entry of matrix $\bar{A}$ in the intersection of a row, corresponding to $u = (u_1, u_2, \ldots, u_k) \in B^k$ and of a column, corresponding to $v = (v_1, v_2, \ldots, v_k) \in B^k$ is the number:

$$P(1 - \delta(u_1, v_1), 1 - \delta(u_2, v_2), \ldots, 1 - \delta(u_k, v_k)). \tag{5}$$

If $u = v$, then all of the $\delta(u_i, v_i)$'s are 1, so the value of P is 0. So the diagonal of $\bar{A}$ is all-0, but no other elements of the matrix are 0 over Z_6, consequently, $\bar{A}$ is co-diagonal over Z_6.

Multi-linear polynomial P has degree $O(\sqrt{k})$, so (5) can be written as the sum of

$$\binom{k}{\leq c\lfloor\sqrt{k}\rfloor} = \sum_{i=0}^{c\lfloor\sqrt{k}\rfloor} \binom{k}{i} < k^{c\sqrt{k}} \tag{6}$$

monomials of the form:

$$a_{i1,i2,\ldots,is}\delta(u_{i1}, v_{i1})\delta(u_{i2}, v_{i2}), \ldots \delta(u_{is}, v_{is}), \tag{7}$$

where c is positive, (in fact, $c < 3$ is also satisfied), $a_{i1,i2,\ldots,is}$ is an integer between 0 and 5, and $s \leq c\sqrt{k}$.

Since the (u, v) entry of $\bar{A}$ is the value (5), and (5) can be written as the sum of monomials in (7), matrix $\bar{A}$ can be written as the sum of matrices $D_{i1,i2,\ldots,is}$, where the entry of matrix $D_{i1,i2,\ldots,is}$ in the intersection of a row, corresponding to $u = (u_1, u_2, \ldots, u_k) \in B^k$ and of a column, corresponding to $v = (v_1, v_2, \ldots, v_k) \in B^k$ is equal to the value of (7).

It is easy to verify that $D_{i1,i2,\ldots,is}$ can be written into the following form (applying the same, suitable permutation to the rows and columns):

$$D_{i1,i2,\ldots,is} = a_{i1,i2,\ldots,is} \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 & 1 \end{pmatrix}$$

Let us observe, that the number of all-1 square minors, covering the diagonal is k^s. Then, from Lemma 3 the rank of $D_{i1,i2,\ldots,is}$ is k^s, $s \le c\sqrt{k}$. It follows from this and from (6), that the rank of $\bar{A}$ is at most $k^{2c\sqrt{k}}$.

Let matrix A be defined as the $n \times n$ upper left minor of matrix $\bar{A}$. Obviously, A is also a co-diagonal matrix, and its rank is at most $k^{2c\sqrt{k}}$. Due to the choice of k the statement follows. □

The proof of Theorem 9 follows the same steps as the proof of Theorem 8. If m has ℓ prime divisors, then polynomial P has degree $O(k^{1/\ell})$, so matrix $D_{i1,i2,\ldots,is}$ has rank at most k^s, $s \le ck^{1/\ell}$, and co-diagonal matrix A has rank at most $k^{2ck^{1/\ell}}$, and this proves the theorem.

Acknowledgment. The author is grateful to *Noga Alon* for his comments and for his significant improvement of Theorem 6, and to *Laci Babai* for the discussions on this topic .

References

[1] N. Alon. The Shannon capacity of a union. *Combinatorica*, 18:301–310, 1998.

[2] L. Babai and P. Frankl. *Linear algebra methods in combinatorics*. Department of Computer Science, The University of Chicago, September 1992. preliminary version.

[3] 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.

[4] P. Erdős and G. Szekeres. A combinatorial problem in geometry. *Composition Math.*, 2:464–470, 1935.

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

[6] V. Grolmusz. Superpolynomial size set systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20:1–14, 2000. Conference version appeared in Proc. COCOON'97, LNCS 1276.

[7] F. P. Ramsey. On a problem of formal logic. *Proc. London Math. Soc.*, 30:264–286, 1930.