Explicit Construction of Ramsey-type Graphs

Victor Yenwen Chen victor@cs.utexas.edu
Supervised by Dr. Zuckerman
University of Texas at Austin

May 2004

Abstract

We survey some recent constructions of Ramsey-type graphs, large graphs with small clique and independent set sizes. Then continuing the works of Grolmusz, we construct matrices over the ring Z_{pq}, where p and q are distinct primes, such that the diagonal entries are 0 modulo pq and the off diagonal entries are nonzero modulo pq. These matrices lead to a construction of Ramsey graphs. Our work simplifies Grolmusz's construction while still matching the best known constructive asymptotic bound.

1 Introduction

Randomization is extremely useful in many areas in computer science. Many algorithms become much simpler in both conception and implementation with access to randomness. However, it is not clear whether there are good random sources in nature, and furthermore, computers do not have access to truly random bits. It becomes natural to investigate the power of randomness - whether access to random bits can be removed or reduced without loss of efficiency.

The main focus of this area of study, termed derandomization, is to convert an existing randomized algorithm into an efficient, deterministic one. A pseudorandom generator, a deterministic algorithm that takes a short random string and stretches its length to fool polynomial time algorithms, is a useful tool in derandomization, and its constructibility has received attention from various researchers. Constructibility is defined as the existence of an efficient, deterministic algorithm to construct the object. The construction of pseudorandom generators is closely related to the constructions of many objects with combinatorial properties, such as error-correcting codes, expander graphs, and extractors. Thus, problems in derandomization can often be expressed as problems in explicit constructions. These combinatorial objects also have many applications in computer science, such as networking, algorithmic design, and complexity theory.

One famous problem in the area of explicit construction is the construction of Ramsey graphs. A Ramsey graph is a large graph with small clique and independent set sizes. More formally, the Ramsey number $n = R(k,t)$ is defined as the smallest number n such that any graph on n vertices contains a clique of size k or an independent set of size t. It is well known that this number is finite and so is well-defined [24]. The problem of determining a lower bound for the number is equivalent to proving that some graph on n vertices has no clique of size k and no independent set of size t. In one of the early uses of the probabilistic method, Erdős [11] showed that $R(k,k) = \Omega(2^{k/2})$. In other words, there exist Ramsey graphs with $\Omega(2^{k/2})$ vertices having cliques and independent sets of size strictly less than k. His proof is probabilistic and in fact shows that most graphs on $\Omega(2^{k/2})$ vertices exhibit this random-like property. This implies a very simple randomized algorithm to generate a Ramsey graph. The algorithm simply flips a fair coin for each pair of vertices to decide whether they are connected or not. However, the proof merely demonstrates the existence of such a graph with high probability without providing a construction. Our goal in exhibiting Ramsey graphs is in a sense a derandomization of the simple randomized algorithm. Trivially, we may search through the sample space of all graphs on n vertices and test whether each graph has a clique or an independent set of size at least $2\log n$.

However, this brute force approach is not efficient. Even if we use a reduced sample space, querying whether a graph has a clique or an independent set of a given size is nontrivial. The best known construction is due to Frankl and Wilson [15] who constructed graphs on

$$k^{\Omega(\frac{\log k}{\log\log k})}$$

vertices with the maximum size of a clique and an independent set less than

k. The constructive bound is much weaker than the probabilistic bound, and it remains open to show explicitly that $R(k,k)$ is exponential in terms of k.

In this paper, we survey some recent constructions of Ramsey graphs. Then continuing the works of Grolmusz, we construct matrices over the ring Z_{pq}, where p and q are distinct primes, such that the diagonal entries are 0 modulo pq and the off diagonal entries are nonzero modulo pq. These matrices lead to a construction of Ramsey graphs. Our work simplifies Grolmusz's construction while still matching the best known constructive asymptotic bound.

Our paper is organized as follows. In the first section, we survey some known results on the off diagonal number $R(3,t)$, and we shall see that these smaller Ramsey numbers are also difficult to estimate explicitly. The rest of the paper is devoted to the diagonal number $R(k,k)$. In the next two sections, we shall discuss the classical Frankl-Wilson construction and then Alon's work extending their result. Then in the last section, we shall present Grolmusz's work and our result.

2 The Ramsey Number R(3,t)

Various researchers over the years have studied the off diagonal Ramsey number $R(3,t)$. Ajtai, Komlós, and Szemerédi [1] showed that $R(3,t) = O(t^2/\log t)$. Improving Erdős's bound [12] $R(3,t) = \Omega((t/\log t)^2)$, Kim [19] demonstrated that the upper bound is tight up to a constant factor, namely $R(3,t) = \Theta(t^2/\log t)$. However, these lower bound proofs are probabilistic, and it presents a challenge to construct triangle-free graphs with the size of an independent set bounded by t while the number of vertices approach nearly quadratic in t.

Erdős [13] provided the first construction with graphs on

$$\Omega(t^{(2\log 2)/3(\log 3 - \log 2)}) = \Omega(t^{1.13})$$

vertices. Building on the works of Cleve and Dagum [9], Chung, Cleve, and Dagum [8] presented another construction with graphs on

$$\Omega(t^{\log 6/\log 4}) = \Omega(t^{1.29})$$

vertices. Alon, using ideas from coding theory, showed a construction with graphs on $\Omega(t^{4/3})$ vertices in [3] and subsequently improved it to $\Omega(t^{3/2})$ in

[2]. The latter is the best known constructive lower bound for $R(3,t)$. More recently, Codenotti, Pudlák, and Resta [10] gave a simpler construction that matches Alon's bound. Both constructions are presented in this section.

2.1 Projective Plane Approach

The construction due to Codenotti, Pudlák, and Resta [10] involves finite projective planes (see e.g. page 157 in [21] or Chapter 19 in [25]). For a prime power q, a projective plane of order q consists of a set of q^2+q+1 points and a set of q^2+q+1 lines. Each line has exactly $q+1$ points, each point is on exactly $q+1$ lines, and two points uniquely determine a line.

Theorem 1. *For every m, there is an explicitly constructible square matrix M of size $O(m^{3/2})$ which has ones on the diagonal, rank(M) $\leq m$, and the associated graph of nonzero entries does not contain a transitive triangle (edges a to b, b to c, and a to c).*

Before presenting the proof, we first show how Theorem 1 can provide a constructive lower bound for $R(3,t)$. Construct a matrix M of size n as specified in Theorem 1. Make it symmetric by copying the entries above the diagonal into their corresponding entries below the diagonal. Call the new matrix M' and its associated graph H'. Since H has no transitive triangle, H' cannot have a triangle. If H' has an independent set S of size k, it will correspond to a k by k minor in M', which is I_k. In M, the corresponding minor will have zeros above the the diagonal of ones, so the minor has rank k, which is bounded by $O(n^{2/3})$. This shows $R(3,t)=\Omega(t^{3/2})$ constructively.

Proof. (of Theorem 1) The idea is to construct a graph G with a superlinear number of edges such that G has no cycle of length less than 6. Then from G, construct an oriented graph H so that its vertices correspond to edges of G. The absence of small cycles in G should prohibit a transitive triangle (edges a to b, b to c, and a to c) from occurring in H, and then we can associate a matrix M with H such that M has low rank.

One such G with the desired properties is the incidence graph of a projective plane (a bipartite graph whose vertices correspond to the points and lines of the plane, and each edge connects a line to an incident point). Let $m := |V(G)| = O(n^2)$. $|E(G)| = O(m^{3/2})$, and G has no cycle of length less than 6 (else, we have two lines sharing two points, a contradiction).

For the oriented graph H, let

$$V(H) = E(G) = \{(P, L) : \text{point } P \text{ on line } L\}, \text{ and}$$

$$((P_1, L_1), (P_2, L_2)) \in E(H) \text{ iff } P_1 \neq P_2, L_1 \neq L_2, \text{ and } P_1 \text{ is on } L_2.$$

H cannot have a transitive triangle. Otherwise, for some points P_1, P_2, P_3 and lines L_1, L_2, L_3, we have edges $((P_1, L_1), (P_2, L_2))$, $((P_2, L_2), (P_3, L_3))$, and $((P_1, L_1), (P_3, L_3))$. This implies that in graph G, there exists a 4-cycle, namely $P_1 - L_2 - P_2 - L_3 - P_1$, which is a contradiction.

Associate a matrix M with H as follows. Index both rows and columns of M by $V(H)$. For row (P, L), assign a vector whose coordinates are in $V(G)$ and has a -1 on the coordinate P, 1 on the coordinate L, and 0 everywhere else. For column (P, L), assign a vector whose coordinates are in $V(G)$ and has a 1 on each incident point of L (except P), 1 on L, and 0 everywhere else. Define M_{ij} to be the inner product of v and w, where v is the vector associated with row i and w is the vector associated with column j.

Claim: $M_{ii} = 1$, and for off-diagonal entries, M_{ij} is -1 on entries corresponding to edges of H and 0 otherwise.

Proof. Let v be the associated vector of row (P, L) and w be the associated vector of column (P', L'). v has two nonzero coordinates at P and L. If $i = j$, w has a 0 at P and a 1 at L, so $M_{ij} = \langle v, w \rangle = 1$. Suppose $i \neq j$. We have $M_{ij} = -1$ iff w has a 1 at coordinate P and a 0 at coordinate L. This is true iff $L' \neq L$, $P \neq P'$, and P is on line L', which is the definition of an edge in H. We have $M_{ij} = 0$ iff the coordinates P and L in w are both 0 or 1, and neither case can occur if H has the edge $((P, L), (P', L'))$. This implies that H is the associated graph of M with nonzero elements. □

It remains to show that the rank of M is bounded by m. The key observation is that any linear combination of the vectors associated to the rows of M gives rise to a linear combination of the corresponding rows. To see this, let x be a linear relation of some vectors $\{z\}$ associated to the rows, i.e., $x = \sum_z \alpha_z z$. Suppose y is a vector associated to a column of M. The entry M_{xy} is equal to $\langle x, y \rangle = \sum_z \alpha_z \langle z, y \rangle$. Hence, the rows corresponding to $\{z\}$ are also dependent.

The vectors have length m, so at most m of them can be linearly independent, and therefore at most m rows are linearly independent. Since prime powers occur frequently, we conclude such M is constructible for every sufficiently large m. □

The construction requires a graph with a superlinear number of edges and has no cycle of length 4. If a graph G has no 4-cycle, it has no $K_{2,2}$ as a bipartite subgraph. Then by Zarankiewicz's problem (see [20] or page 25 in [21]), $|E(G)| = O(|V(G)|^{3/2})$. So our choice of the incidence graph of a projective plane is best possible.

2.2 Dual of a BCH Code

A Cayley graph $G = (V, E)$ consists of a finite group H and a generating set $S \subset H$ such that $V = H$ and $E = \{(h, h+s) : h \in H, s \in S\}$. We impose the additional requirement that $s \in S$ iff $s^{-1} \in S$ for G to be undirected. It is not known if there are Cayley graphs that are good diagonal Ramsey graphs, but Cayley graphs can be used to prove constructive lower bound for the number $R(3, t)$ [2].

Alon's idea is to take a parity check matrix of a linear code with sufficient minimum distance to obtain the triangle-free property in the graph. For a positive integer k, let $\mathbb{F}_k = GF(2^k)$ denote the finite field with 2^k elements, and the elements are represented as binary vectors. Let α be a primitive element in $\mathbb{F}_k$. Consider the following $3k$ by $2^k - 1$ matrix over $\mathbb{F}_2$:

$$A = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^k-2} \\ 1 & \alpha^3 & (\alpha^2)^3 & \cdots & (\alpha^{2^k-2})^3 \\ 1 & \alpha^5 & (\alpha^2)^5 & \cdots & (\alpha^{2^k-2})^5 \end{pmatrix},$$

which is the parity check matrix of a binary BCH code C of designed distance 7 (see e.g., Chapter 9 in [22]).

Now we define a Cayley graph $G = (V, E)$. Let $n = |V| = 2^{3k}$ where 3 does not divide k. Let $V = H$ be the additive group $\mathbb{F}_2^{3k}$. Define W_0 to be the set of all nonzero elements $\alpha \in F_k$ such that the leftmost bit of α^7 is 0, and let W_1 be the set of all nonzero elements $\alpha \in F_k$ such that the leftmost bit of α^7 is 1. Let (a, b, c) denote the concatenation of the three vectors a, b, and c. The generating set S is $U_0 + U_1 = \{u_o + u_1 : u_0 \in U_0, u_1 \in U_1\}$, where $U_i = \{(w_i, w_i^3, w_i^5) : w_i \in W_i\}$ for $i = 0, 1$.

Note that since 3 does not divide k and $\text{ord}_7 2 = 3$, 7 cannot divide $2^k - 1$. So for all $\alpha \neq 1 \in F_k, \alpha^7 \neq 1$. This implies that the map $x \to x^7$ is injective, and therefore, W_0 and W_1 form a partition of F_k. As a consequence, the set of all columns of A is the union of U_0 and U_1. Now we prove some properties of G using ideas from coding theory.

Proposition 1. *G is $d := 2^{k-1}(2^{k-1}-1)$ regular.*

Proof. The BCH code C has minimum distance at least 7, so every set of six columns of A is linearly independent over $GF(2)$ (BCH code is linear, and the minimum distance of a linear code is the minimum weight of the codewords in the code). This implies that all the sums $(u_0 + u_1)$, where $u_0 \in U_0$ and $u_1 \in U_1$, are distinct. Hence, $d = |S| = |U_0||U_1| = 2^{k-1}(2^{k-1}-1)$. □

Note that C only needs to have minimum distance at least 5 for the previous proposition. We need C to have minimum distance at least 7 for the following lemma.

Lemma 1. *G is triangle-free.*

Proof. Suppose G has a triangle, which is also a 3-cycle. Since G is Cayley, there exists $g \in H$ and distinct $s_1, s_2, s_3 \in S$ such that $(g, g+s_1, g+s_1+s_2)$ is a 3-cycle with $s_1+s_2+s_3 = 0$. Write $s_1 = a_0+a_1$, $s_2 = b_0+b_1$, and $s_3 = c_0+c_1$, where $a_0, b_0, c_0 \in U_0$ and $a_1, b_1, c_1 \in U_1$. Then $a_0 + a_1 + b_0 + b_1 + c_0 + c_1 = 0$. These are also column vectors of A. Since the code C has minimum distance at least 7, these six vectors must be linearly independent, contradicting that their sum is 0. □

To bound the maximum size of an independent set in G, we employ spectral techniques to analyze the eigenvalues of the adjacency matrix A_G of G. We first state a known result (see e.g. page 435 in [25] for a proof).

Fact 1. *For a d-regular graph G, the maximum size of an independent set in G is bounded above by*

$$\frac{-n\lambda_n}{\lambda_1 - \lambda_n},$$

where $n = |V(G)|$ and $d = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ are the eigenvalues.

It suffices to bound the smallest eigenvalue of our graph G.

Theorem 2. *For every eigenvalue λ of A_G,*

$$-9 \cdot 2^k - 3 \cdot 2^{k/2} - 1/4 \leq \lambda.$$

Proof. It is known that the eigenvalues of a Cayley graph of an Abelian group can be computed in terms of the characters of the group. To see this, for $r, a \in \mathbb{F}_2^{3k}$, r fixed, let $\chi_r(a) = (-1)^{r \cdot a}$, which is multiplicative, i.e., $\chi_r(a+b) = \chi_r(a)\chi_r(b)$. Let $v \in \{-1,1\}^{2^{3k}}$ be such that v_i is equal to χ_r applied to the ith string in $\mathbb{F}_2^{3k}$. Then

$$\begin{aligned}(A_G v)_i = \sum_{b:(i,b)\in E(G)} \chi_r(b) &= \sum_{s \in S} \chi_r(i+s) \\ &= \sum_{s\in S} \chi_r(i)\chi_r(s) \\ &= \left(\sum_{s\in S} \chi_r(s)\right) v_i.\end{aligned}$$

Hence, v is an eigenvector with eigenvalue

$$\lambda_r = \sum_{s\in S} \chi_r(s) = (\sum_{u_o \in U_0} \chi_r(u_o))(\sum_{u_1\in U_1} \chi_r(u_1)),$$

since $S = U_0 + U_1$.

Now recall that A is the parity check matrix of code C. Consider $w := r \cdot A$. For $j = 0, 1$, define vectors w_{U_j} to be the restriction of w to U_j. Let $\#_0(w)$ be the number of 0 in the vector w and $\#_1(w)$ to be the number of 1 in w. Then

$$\sum_{u_j \in U_j} \chi_r(u_j) = \sum_{u_j\in U_j} (-1)^{r\cdot u_j} = \#_0(w_{U_j}) - \#_1(w_{U_j})$$

Write $wt(w_{U_0}) = x$ and $wt(w_{U_1}) = y$. Then $\lambda_r = (2^{k-1} - 1 - 2x)(2^{k-1} - 2y)$.

Now we prove a lower bound for λ_r. Since w is a linear combination of the rows of A, which corresponds to a codeword in the dual code of C, this provides a way to bound the eigenvalue in terms of the Hamming weight of w. The AM-GM Inequality asserts that for real numbers a and b, $ab \leq (a+b)^2/4$. Substituting $a = (2^{k-1} - 1 - 2x)$ and $b = -(2^{k-1} - 2y)$, we have

$$\lambda_r \geq -(1 + 2(x-y))^2/4.$$

We will use the Carlitz-Uchiyama bound (see e.g. page 280 in [22]) to bound $x - y$.

Theorem 3. *Suppose C is a binary BCH code of length 2^{m-1} with designed distance $2t+1$, where $2t-1 < 2^{\lceil m/2 \rceil}+1$. Then for all nonzero vectors $c \in C^{\perp}$,*

$$2^{m-1} - (t-1)2^{m/2} \leq wt(c) \leq 2^{m-1} + (t-1)2^{m/2}.$$

Consider the following matrix in binary,

$$A' = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^k-2} \\ 1 & \alpha^3 & (\alpha^2)^3 & \cdots & (\alpha^{2^k-2})^3 \\ 1 & \alpha^5 & (\alpha^2)^5 & \cdots & (\alpha^{2^k-2})^5 \\ 1 & \alpha^7 & (\alpha^2)^7 & \cdots & (\alpha^{2^k-2})^7 \end{pmatrix},$$

where α is a primitive element of $\mathbb{F}_k$. Similar to A, A' is also the parity check matrix of a BCH code C' with designed distance 9.

Let p be the characteristic vector of W_1. Now let $r' \in \{0,1\}^{4k}$ be the vector r appended by the vector [1,0,...,0]. Then $r' \cdot A' = w + p$, and $w + p$ is a codeword in the dual of C' with Hamming weight $x + 2^{k-1} - y$, which is nonzero. By the Carlitz-Uchiyama bound, $2^{k-1} - 3 \cdot 2^{k/2} \leq x + 2^{k-1} - y$, which implies $\lambda_r \geq -9 \cdot 2^k - 3 \cdot 2^{k/2} - 1/4$, and thus completing the proof. □

With the lower bound on the smallest eigenvalue, we conclude that the graph G has independent sets of size at most

$$n \frac{36 \cdot 2^k + 12 \cdot 2^{k/2} + 1}{2^k(2^k-2) + 36 \cdot 2^k + 12 \cdot 2^{k/2} + 1} = O(n^{2/3}).$$

Our graph is also triangle-free. Hence, this shows $R(3,t) = \Omega(t^{3/2})$ explicitly.

3 Frankl-Wilson Construction

We now consider the diagonal Ramsey number $R(k,k)$ and survey several known constructive lower bound. For years, the only construction known is trivial – construct $k-1$ disjoint cliques of size $k-1$, which yields $R(k,k) = \Omega(k^2)$. In [23], Nagy showed $R(k,k) = \Omega(k^3)$. Building on the works of Frankl [14], Frankl and Wilson [15] made a breakthrough and constructed graphs with a superpolynomial number of vertices with respect to k. The following theorem regarding the size of a set system with restricted intersection modulo a prime p is the main tool involved. The original proof used higher incidence matrices, but Alon, Babai, and Suzuki [5] employed multivariate polynomials in a vector space with small dimension to bound the size. We state a weaker result without proof since the essential proof concept is illustrated in the next section.

Theorem 4. *Suppose u_0, u_1, …,u_s are distinct residues modulo a prime p. Let $\mathcal{F}$ be a family of k-element subsets of $\{1, 2, \ldots, n\}$. Suppose $k \equiv u_0$ mod p, and for every distinct A, $B \in \mathcal{F}$, $|A \cap B| \equiv u_i$ mod p for some $1 \leq i \leq s$. Then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$.*

Frankl and Wilson also showed a stronger bound $|\mathcal{F}| \leq \binom{n}{s}$ if $\mathcal{F}$ is k-uniform, but this makes no difference in the asymptotic bound in the following theorem.

Theorem 5. *There exists an explicitly constructible family of graphs $\{G_n\}$, where G_n is a graph on n vertices such that the cliques and the independent sets have size less than*

$$2^{O(\sqrt{\log n \log\log n})}.$$

Proof. Let p be a prime and consider the set $S = \{1, 2, \ldots, p^3\}$. Define a graph G such that its vertices are subsets of S with size $p^2 - 1$, and $(A, B) \in E(G)$ iff $|A \cap B| \not\equiv -1 \pmod{p}$. A clique corresponds to a family $\{A_1, \ldots, A_\ell\}$ such that for all $i \neq j$, $|A_i \cap A_j| \not\equiv -1 \pmod{p}$. Since each subset has size congruent to -1 modulo p, ℓ is bounded by

$$\sum_{i=0}^{p-1} \binom{p^3}{i} = p^{O(p)}.$$

An independent set of size t corresponds to a family $\{B_1, \ldots, B_t\}$ such that for all $i \neq j$, $|B_i \cap B_j| \in \{p-1, 2p-1, \ldots, p(p-1)-1\}$. Pick a prime q larger than $p^2 - 1$. Then $p-1, 2p-1, \ldots, p(p-1)-1, p^2-1$ are all distinct residues modulo q. By Theorem 4, $t \leq \sum_{i=0}^{p-1} \binom{p^3}{i} = p^{O(p)}$.

Note that $n = |V(G)| = \binom{p^3}{p^2-1} = p^{O(p^2)}$. By the density of primes, for every n, we can choose up to constants p so that $n < \binom{p^3}{p^2-1}$. Then we can construct a graph on $\binom{p^3}{p^2-1}$ vertices and then obtain a subgraph of G with n vertices. Hence, the size of a clique or an independent set in G is bounded by $2^{O(\sqrt{\log n \log\log n})}$. Simple computation shows that this is equivalent to stating that G has $t^{\Omega(\log t/\log\log t)}$ vertices while cliques and independent sets have size less than t. □

4 Alon's Extension

Suppose the edges of a complete graph are either red or blue. Theorem 4 asserts that it is possible to color the edges such that the size of a monochromatic (either red or blue) clique is small (think of the blue edges in the complete graph as non-edges before the coloring transformation). Then we can investigate the case when complete graphs are colored with ℓ colors and hope for similar results. Using more than one prime, Alon in [4] extended Frankl and Wilson's results.

Definition 1. *Let G=(V,E) be a graph and $\mathcal{F}$ be a subspace of the space of polynomial in r variables over a field F. We say that G has a representation over $\mathcal{F}$ if for each $v \in V$, we can assign a polynomial $f_v \in \mathcal{F}$ and $c_v \in F^r$ such that the following conditions hold:*
(1) For all $v \in V$, $f_v(c_v) \neq 0$.
(2) For all distinct, nonadjacent $u, v \in V$, $f_v(c_u) = 0$.

Lemma 2. *If a graph G=(V,E) has a representation over $\mathcal{F}$, then the size of an independent set in G is bounded above by dim($\mathcal{F}$).*

Proof. Let $\{f_v(x_1, \ldots, x_r) : v \in V\}$ and $\{c_v : v \in V\}$ be a representation, and let S be an independent set in G. Then the polynomials in $\{f_v : v \in S\}$ are linearly independent. To see this, suppose $\sum_{v \in S} \alpha_v f_v = 0$. If $u \in S$, evaluate this sum of polynomials on u, and we can conclude that $\alpha_u = 0$. Hence, $|S|$ is bounded by the dimension of $\mathcal{F}$. □

Note that the representation of a graph is defined with bounding the dimension of the space $\mathcal{F}$ in mind. This will then bound the size of a monochromatic clique in a graph from above.

Theorem 6. *For every fixed integer $\ell \geq 2$, we can construct a family of ℓ-colored graphs on*

$$k^{\frac{(1+o(1))(\log k)^{\ell-1}}{\ell^{\ell}(\log \log k)^{\ell-1}}}$$

vertices with no monochromatic cliques of size k.

Proof. Extending Frankl and Wilson's construction, let $\mathcal{P} = \{p_1, \ldots, p_\ell\}$ be a set of ℓ consecutive large primes. Define $s := p_1 p_2 \ldots p_\ell - 1$ and let $r = p_\ell^{p_\ell + 1}$. Construct a complete graph G whose vertices are subsets of $\{1, \ldots, r\}$ with size s. Define the color of edge (A, B) as

$$\min\{i \in \{1, \ldots, \ell\} : |A \cap B| \not\equiv -1 (\text{mod } p_i)\}.$$

Since $|A \cap B| < p_1 \dots p_\ell - 1$, $|A \cap B| \not\equiv -1 \pmod{p_i}$ for some i. So our coloring is well-defined.

Let G_i be the subgraph of G by removing the edges with color i. A monochromatic clique of color i in G corresponds to an independent set of G_i. Now we show that G_i has a representation over the space of multilinear polynomials of degree at most $p_i - 1$ in r variables over $GF(p_i)$. For each vertex A, assign the polynomial

$$P_A(x_1, \dots, x_r) = \prod_{i=0}^{p_i-2} [\sum_{j \in A} x_j - i],$$

and let its characteristic vector $c_A \in \{0,1\}^r \subseteq (GF(p_i))^r$. Then $P_A(c_A) = \prod_{i=0}^{p_i-2}[|A| - i]$, which is not congruent to 0 modulo p_i since $|A| \equiv -1 \bmod p_i$. For nonadjacent vertices A and B, $P_A(c_B) = \prod_{i=0}^{p_i-2}[|A \cap B| - i]$, which is congruent to 0 modulo p_i since $|A \cap B| \not\equiv -1$ modulo p_i by construction. These polynomials are multilinear; we can use the relations $x_i^2 = x_i$ and make appropriate substitutions since the characteristic vectors are binary.

A basis of the space these polynomials reside in consists of monomials of degree at most $p_i - 1$, so the dimension is precisely $\sum_{i=0}^{p_i-1} \binom{r}{i}$. By the preceding lemma, this implies that a monochromatic clique in G has size less than $k = r^{O(p_\ell)}$. We have the parameters $r = p_\ell^{p_\ell+1}$ and $s = p_1 \dots p_\ell - 1$. And by direct calculation and the density of primes, the number of vertices in G is

$$\binom{r}{s} = k^{\frac{(1+o(1))(\log k)^{\ell-1}}{\ell^\ell (\log \log k)^{\ell-1}}},$$

completing the proof. □

Recall that in Frankl and Wilson's construction, two vertices A and B in G are connected iff $|A \cap B| \not\equiv -1 \pmod{p}$. We sketch how the proof above can be modified to obtain Frankl and Wilson's construction. Set $r = p^3 - 1$ and $s = p^2 - 1$. G has a representation over the space of multilinear polynomials of degree at most $p - 1$ with r variables over the reals. For each vertex A, assign the polynomial

$$Q_A(x_1, \dots, x_r) = \prod_{i=1}^{p-1} [(\sum_{j \in A} x_j) - (p^2 - 1 - ip)]$$

and its characteristic vector c_A. Then $Q_A(c_A) = \prod_{i=1}^{p-1} \neq 0$. Since $|A \cap B| \in \{p-1, 2p-1, \dots, p(p-1)-1\}$, there must be an $i \in \{1, \dots, p-1\}$ such that

$|A \cap B| - (p^2 - 1 - ip) = 0$. The dimension of the space of these polynomials bounds the size of an independent set in G. Similarly, the complement of G has a representation over the field $GF(p)$ as described in the preceding proof, and the dimension of this space bounds the size of a clique in G.

5 Grolmusz's Work and Our Result

In Theorem 4, Frankl and Wilson showed that when m is a fixed prime, a set system with pairwise intersection modulo m has a polynomial upper bound, viewing m as a constant. In the same paper, they also proved that the upper bound holds when m is a fixed prime power and $s = m - 1$ (the number of distinct intersection size residues). They asked whether a polynomial upper bound exists if m is a fixed non-prime power or when $s = m - 1$. Grolmusz in [16] demonstrated an explicit family of superpolynomial size set system if m is a fixed non-prime power and $s = m - 1$. His set systems also provided a novel construction of Ramsey graphs matching the asymptotic bound by Frankl and Wilson, and his construction can be generalized to multicolors that matches Alon's bound.

Grolmusz's works involved certain low degree polynomials (call them BBR, due to Barrington, Beigel, and Rudich [7]). He used these polynomials to construct co-diagonal matrices (defined below) over the ring Z_6. These matrices in turn lead to the construction of his superpolynomial set systems. In [17], Grolmusz constructed good Ramsey graphs directly from low rank co-diagonal matrices over Z_6, and in [18], he provided another proof that these matrices have small rank. We shall describe the connection between Ramsey graphs and these matrices, but first let us define some basic terminologies.

5.1

Definition 2. *Let R be a ring and n be a positive integer. $A = \{a_{ij}\}$ is a co-diagonal matrix over R if for $i, j \in \{1, 2, \ldots, n\}, a_{ij}$ is nonzero in R if $i \neq j$ and zero if $i = j$.*
We say that matrix A is upper co-triangular over R if the diagonal entries are zero and the entries above the diagonal are nonzero in R. A lower co-triangular matrix is similarly defined. A matrix is co-triangular if it is either lower or upper co-triangular.

Definition 3. *The rank over the ring R of matrix A is the smallest number 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. If all entries in A are zero, it has rank 0.*

When R is a field, this is a well-known equivalent definition of the rank of a matrix. Grolmusz suggested using this definition for a ring since inverses do not necessarily exist. The following easy property still holds under this definition of rank.

Proposition 2. $rk_R(A + A') \leq rk_R(A) + rk_R(A')$.

Proof. Suppose $A = BC$ and $A' = B'C'$, where B is an $n \times r$, C is an $r \times n$, B' is an $n \times r'$, and C' is an $r' \times n$ matrix. Define new matrices B'' and C'' where the columns of B'' are formed from the union of the columns of B and B', and the rows of C'' are from the union of the rows of C and C'. Then $A + A' = B''C''$, and $rk_R(A + A') \leq r + r'$. □

Since we need to construct co-triangular matrices with small rank, it is useful to have a lower bound in mind.

Proposition 3. *If A is an $n \times n$ co-triangular matrix over R, then $rk_R(A) \geq \log_m n$, where $|R| = m$.*

Proof. Write $A = BC$, where B is an $n \times r$ matrix and C is a $r \times n$ matrix. A is co-triangular implies that all columns in A are different. Therefore, all columns in C are different. Consequently, $n \leq m^r$. □

There is a stronger lower bound modulo a prime. The following theorem implies that a co-triangular matrix has large rank over GF_p, more specifically, $r \geq n^{1/(p-1)} - p$.

Theorem 7. *Let p be a prime and A be an $n \times n$ co-triangular matrix over GF_p. Let $r = rk_{GF_p}(A)$. Then $n \leq \binom{r+p-2}{p-1} + 1$.*

Proof. If we have a set of polynomials f_i and points x_i such that $f_i(x_i) \neq 0$ and $f_i(x_j) = 0$ for $i > j$, then the polynomials are linearly independent. (see e.g. page 176 in [21], and the argument is also similar to the proof of Lemma 2). Then the number of polynomials is bounded by the dimension of the vector space in which they reside. Note that if we define a matrix such that entry (i, j) is equal to $f_i(x_j)$, then the matrix is triangular, the

”complement” of a co-triangular matrix. So our goal is use a co-triangular matrix to define polynomials satisfying the above mentioned criterion.

Suppose A is lower co-triangular, and $A = BC$, where $B = \{b_{ij}\}$ is an n by r matrix and $C = \{c_{ij}\}$ an r by n matrix over GF_p. For $i \in [n]$, define functions $P_i(x_1, \ldots, x_r) = \sum_{k=1}^{r} b_{ik} x_k$. Then

$$P_i(c_{1j}, \ldots, c_{rj}) = \begin{cases} 0 \bmod p & i = j \\ 1, \ldots, p-1 \bmod p & i > j. \end{cases}$$

Consider the polynomials $Q_i(x_1, \ldots, x_r) = 1 - P_i^{p-1}(x_1, \ldots, x_r)$. By Fermat's Little Theorem,

$$Q_i(c_{1j}, \ldots, c_{rj}) = \begin{cases} 1 \bmod p & \text{if } i = j \\ 0 \bmod p & \text{if } i > j. \end{cases}$$

The Q_i are linearly independent. Each Q_i is a degree $p-1$, r-variable polynomial. Since $Q_i - 1$ is homogeneous, a basis for the vector space these n polynomials reside in is

$$\{1\} \cup \{x_1^{\alpha_1} \ldots x_r^{\alpha_r} : \sum_{i=1}^{r} \alpha_i = p-1, \alpha_i \geq 0\}.$$

Hence, $n \leq \binom{r+p-2}{p-1} + 1$. □

In contrast to the prime case, a co-triangular matrix over Z_m where m is composite can have low rank. We are interested in the construction of such a matrix as the following theorem demonstrates the relation between good Ramsey graphs with low rank co-diagonal matrix over the ring Z_6.

Theorem 8. *Let A be an n by n co-diagonal matrix over $R = Z_6$ with $r = rk_R(A)$. Then there exists an explicit graph on n vertices such that a clique has size at most $r+1$ and an independent set has size at most $\binom{r+1}{2}+1$.*

Proof. Substitute $p = 2$ and $q = 3$ in Theorem 9. □

Theorem 9. *Let p and q be two distinct primes, and let A be an n by n co-diagonal matrix over $R = Z_{pq}$ with $r = rk_R(A)$. Then there exists an explicit graph on n vertices such that a clique has size at most $\binom{r+p-2}{p-1} + 1$ and an independent set has size at most $\binom{r+q-2}{q-1} + 1$.*

Proof. Note the rank of A over GF_p and GF_q is still bounded by the rank of A over Z_{pq}. Let $V(G) = \{v_1, \ldots, v_n\}$. For $i > j$, $\{(v_i, v_j)\} \in E(G)$ iff $a_{ij} \neq 0 \mod p$.

A t-clique corresponds to a $t \times t$ minor of A, which is co-triangular over GF_p. Hence, $t \leq \binom{r+p-2}{p-1} + 1$. A k-independent set corresponds to a $k \times k$ minor of A, whose off diagonal entries are 0 mod p. They can be p, 2p,...,$(q-1)p$ (cannot be 0 since A is co-triangular), and none of them is congruent to 0 modulo q. Hence, the corresponding minor is co-triangular over GF_q, and $k \leq \binom{r+q-2}{q-1} + 1$. □

It suffices to construct a co-diagonal matrix over Z_6 with low rank.

Theorem 10. *For all $n > 0$, there exists an explicitly constructible $n \times n$ co-diagonal matrix $A = \{a_{ij}\}$ over $R = Z_6$ with*

$$r = rk_{Z_6}(A) = 2^{O(\sqrt{\log n \log\log n})}.$$

Proof. Grolmusz's construction relies on results due to Barrington, Beigel, and Rudich [7], which we state without proof here.

Theorem 11. *Given $m = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}$ with $\ell > 1$, where the p_i are distinct primes, there exists an explicitly constructible multilinear polynomial P with integer coefficients, k variables, degree $O(k^{1/\ell})$, such that for all $\vec{x} \in \{0,1\}^k, P(\vec{x}) = 0$ over Z_m iff $\vec{x} = \vec{0}$.*

Choose the smallest integer k such that $n \leq k^k$. Construct a BBR polynomial P with $m = 6$ and $\ell = 2$ and with degree $O(\sqrt{k})$. Now define a $k^k \times k^k$ matrix A as follows. Associate each row u and column u with a vector of length k representing u in base k. For row $u = (u_1, \ldots, u_k)$ and column $v = (v_1, \ldots, v_k)$, where u_i and v_j are elements in $\{0, 1, \ldots, k-1\}$, define

$$a_{uv} = P(1 - \delta(u_1, v_1), \ldots, 1 - \delta(u_k, v_k)),$$

where

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

If $u = v$, then $a_{uv} = P(0, \ldots, 0) \equiv 0 \pmod 6$. If $u \neq v$, then there is some i such that $u_i \neq v_i$. So a_{uv} is the evaluation of P on a nonzero vector, which is nonzero modulo 6. Hence, A is co-diagonal modulo 6.

To bound r, we write A as the sum of matrices with smaller rank and use Proposition 2. Since P has degree $c\sqrt{k}$ for some constant c, P is the sum of monomials of the form

$$a_{i_1,i_2,\ldots,i_s}\delta(u_{i_1},v_{i_1})\delta(u_{i_2},vi_2)\cdots\delta(u_{i_s},v_{i_s}),$$

where $a_{i_1,i_2,\ldots,i_s} \in \{0,1,\ldots,5\}$ and $s \leq c\sqrt{k}$.

For each monomial $\delta(u_{i_1},v_{i_1})\cdots\delta(u_{i_s},v_{i_s})$ in P, define matrix $C_{i_1,\ldots,i_s} = \{c_{uv}\}$ such that $c_{uv} = \delta(u_{i_1},v_{i_1})\cdots\delta(u_{i_s},v_{i_s})$. Then

$$A = \sum_{s\leq c\sqrt{k},i_1,\ldots,i_s\in[k]} a_{i_1,\ldots,i_s}C_{i_1,\ldots,i_s}.$$

The number of monomials in P is at most $\sum_{i=0}^{c\sqrt{k}}\binom{k}{i} < k^{c_2\sqrt{k}}$ for some constant c_2. Now we need to bound the rank of each matrix $C_{i_1,\ldots,i_s}$.

Observe that entries in $C_{i_1,\ldots,i_s}$ are either zero or one. Furthermore, the number of ones in each row and column is exactly k^{k-s}. To see this, fix a row u. In the expression $\delta(u_{i_1},v_{i_1})\ldots\delta(u_{i_s},v_{i_s})$, the u_{i_j} are fixed. There are k^{k-s} ways to choose values for the $k-s$ v_{i_j} not in the expression while the remaining v_{i_j} must match up with the u_{i_j} for the expression to be one. Then it is not hard to see that we can permute the rows and columns in $C_{i_1,\ldots,i_s}$ so that it can be written in the form

$$a_{i_1,\ldots,i_s}\begin{pmatrix} J & 0 & 0 & \ldots & 0 \\ 0 & J & 0 & \ldots & 0 \\ 0 & 0 & J & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & J \end{pmatrix}$$

where each J is a k^{k-s} by k^{k-s} all ones matrix. Then the rank of this matrix over Z_6 is equal to the number of J blocks, which is k^s.

Hence, putting everything together, we have

$$rk_{Z_6}(A) \leq \sum_{i_1,\ldots,i_s} rk_{Z_6}(C_{i_1,\ldots,i_s}) < k^{c_2\sqrt{k}}k^s = k^{O(\sqrt{k})}.$$

Now, take the $n \times n$ upper leftmost minor of A. This is still co-diagonal over Z_6, has size n, and has rank $2^{O(\sqrt{\log n \log\log n})}$ by our choice of k. □

Grolmusz's construction can be generalized to low rank matrices over Z_m.

Corollary 1. *For $m = p_\ell^{\alpha_\ell} \dots p_\ell^{\alpha_\ell}$ and $\ell > 1$, there exists an explicitly constructible $n \times n$ co-diagonal matrix A over Z_m with*

$$r = rk_{Z_m}(A) = 2^{O(\sqrt[\ell]{\log n (\log \log n)^{\ell - 1}})}.$$

Proof. The proof follows the same steps as above. P has degree $O(k^{1/\ell})$, $C_{i_1,\dots,i_s}$ has rank $k^{O(\sqrt[\ell]{k})}$ over Z_m, and A has rank $k^{O(\sqrt[\ell]{k})}$ □

Corollary 2. *There exists an explicitly constructible family of graphs on n vertices such that the cliques and independent sets have size at most*

$$2^{O(\sqrt{\log n \log \log n})}.$$

Proof. We have constructed co-diagonal matrices over Z_6 with rank r. By Theorem 8, graphs on n vertices have cliques and independent sets of size $O(r^2)$. So the statement follows. □

5.2 Co-Diagonal over Z_{pq}

We describe our result in this section. Grolmusz examined co-diagonal matrices over the ring Z_6. We generalize his idea to Z_{pq}, where p and q are distinct primes. While Theorem 9 provides a worse bound on the size of a monochromatic clique than Theorem 8, it is much easier to construct a low rank co-diagonal matrix over a larger ring. In fact, the rank of the matrix is much smaller, and therefore, this tradeoff allows us to obtain the same asymptotic bound for $R(k, k)$. Over the ring Z_{pq}, we can simply force the off diagonal entries to be drawn from $\{1, \dots, pq - 1\}$ and avoid modulo arithmetic and the usage of the BBR polynomials. Our constructions are in part inspired by the explicit matrices introduced in Theorem 1.

Lemma 3. *There exists an explicitly constructible family of graphs $\{G_N\}$, where G_N is a graph on N vertices such that the size of cliques and independent set is at most $2^{O(\sqrt{\log N} \log \log N)}$.*

Proof. Let n be the smallest integer such that $N \leq \binom{n}{k}$, where $k = \lfloor n/2 \rfloor + 1$. Let A be a $\binom{n}{k}$ by $\binom{n}{k}$ matrix. Associate each row with a unique binary vector of length n with weight k, and each column i is associated with the vector associated with row i. Define A_{ij} to be the inner product of x and y, where x is the vector associated with row i, and y is the vector associated with column j.

$A_{ii} = \langle x, x \rangle = k$. Now consider A_{ij}, where $i \neq j$, and let x and y be the associated vectors for row i and column j, respectively. Clearly $A_{ij} < k$, since there must be a coordinate where x and y differ. Furthermore, by the Pigeonhole Principle, there must be a coordinate where x and y both have a 1, so $A_{ij} > 0$.

Now consider the top $N \times N$ upper leftmost minor of A and call it A'. Take the ring $R = Z_{pq}$, where p and q are distinct primes and $pq = k$. Then A' is co-diagonal over R. $rk_{Z_{pq}}(A') \leq n$ since A can be written as $A = BC$, where the rows of B are the vectors associated with the rows of A', and the columns of C are the vectors associated with the columns of A'. B is N by n and C is n by N. Hence, A' has size $N = \binom{n}{n/2+1} = O(2^n/\sqrt{n})$ and rank $r = O(\log N)$ over R.

From Theorem 9, matrix A gives rise to a graph with clique and independent sets of size at most $t < (r+q)^q$, assuming $p < q$. Our construction has the parameters $pq = n$ and $n = O(\log N)$. Taking p and q close, we have

$$t = (\log N + \sqrt{\log N})^{O(\sqrt{\log N})} = (\log N)^{O(\sqrt{\log N})} = 2^{O(\sqrt{\log N} \log\log N)}.$$

The matrix has size N. Each coefficient requires $\log n = \log\log N$ bits. Each dot product takes $n = \log N$ operations, and examining each entry modulo p or q is also efficient. So our construction takes time polynomial in N. □

This provides an alternate construction of these co-diagonal matrices though the asymptotic bound is worse than the best known result. However, we can improve the bound by increasing the range of the associated row and column vectors.

Define $U = U_1 \times U_2 \times \ldots \times U_k$, where each U_i is a set of n elements, and the U_i are disjoint. Consider a matrix A such that its rows and columns are indexed by elements in U. For row or column $(u_1, \ldots, u_k)$, let $x \in \{0,1\}^{kn}$ be its characteristic vector, i.e.,

$$x_a = \begin{cases} 1 & \text{if } a = u_1 \text{ or } u_2 \ldots \text{or } u_k \\ 0 & \text{otherwise} \end{cases}$$

Define $A_{ij} = \langle x, 1-y \rangle$, where x is the characteristic vector of row i and y is the characteristic vector of column j. Note that $A_{ii} =< x, 1-x >= 0$. For $i \neq j$, there exists a coordinate where x and y differ, so without loss of generality, x has a 1 in coordinate u_1 whereas y has a 0. Since there are no zero characteristic vectors, we can conclude $A_{ij} > 0$. Note for each characteristic vector x, it has exactly k ones, so $A_{ij} \leq k$.

Let $k = pq - 1$, where p and q are distinct primes. Then A is co-diagonal over $R = Z_{pq}$. A has size n^k and rank $r = kn$ over the ring R. From this explicit family of matrices, we have the following:

Theorem 12. *The co-diagonal matrix A implies an explicit graph on N vertices with clique and independent set sizes bounded by $2^{O(\sqrt{\log N \log\log N})}$.*

Proof. From Theorem 9 and assuming $p < q$, we have $t < (r+q)^q$, where t is the size of the largest clique or independent set. Our construction has the parameters $r = kn$, $pq - 1 = k$, and $N = n^k$. Choosing $k = n$, we have

$$t = (kn + \sqrt{k})^{O(\sqrt{k})} = (n^2 + \sqrt{n})^{O(\sqrt{n})} = 2^{O(\sqrt{n}\log n)} = 2^{O(\sqrt{\log N \log\log N})}.$$

□

A theorem by Bollobás in extremal set theory illustrates why our choice of k is best possible. The theorem asserts that if $A_1, \dots, A_m$ are sets of size a and $B_1, \dots, B_m$ are sets of size b such that $A_i \cap B_j = \emptyset$ iff $i = j$, then $m \le \binom{a+b}{a}$. (Numerous proofs are known; see e.g. [21]). In our construction, the row vectors x_i correspond to sets of size k, and the column vectors $1 - y_j$ correspond to sets of size $kn - k$, where the sets corresponding to x_i and $1 - y_j$ satisfy the property described above. So the size of the matrix is at most $(kn)^{O(k)}$. On the other hand, the maximum size of a monochromatic clique has a factor of $\sqrt{k}$ in the exponent because k is the product of two large primes.

5.3 multicolor

Naturally, we can generalize the previous construction to ℓ colors for a complete graph on N vertices over Z_m where m has ℓ prime divisors. Grolmusz did not describe the easy generalization, but we provide details here for completeness.

Here is how we can modify the construction. Instead of setting $k = pq$, let $k = p_1 \dots p_\ell - 1$, where p_i are consecutive primes such that $k = O(n^c)$ for some constant c. Then the matrix A defined in Theorem 12 is co-diagonal over $R = Z_{p_1 \dots p_\ell}$ with rank kn. Define a graph G such that $V(G)$ is the set of rows of A, and for $i > j$, define the color of the edge $\{(i,j)\} \in E(G)$ as

$$\min\{\ell : p_\ell \text{ does not divide } a_{ij}\}.$$

The coloring is well defined since the off-diagonal entries in A are not divisible by $p_1 \dots p_\ell$. A monochromatic clique of color i of size t corresponds to a t by t minor of A. This minor is co-triangular over GF_{p_i}. So by Theorem 8,

$$\begin{aligned} t &\leq \binom{r+p_i-2}{p_i-1}+1 \\ &< (r+p_i)^{p_i} \\ &= n^{O(\sqrt[\ell]{n})} \\ &= 2^{O(\log n \sqrt[\ell]{n})} \\ &= 2^{O(\sqrt[\ell]{\log N (\log\log N)^{\ell-1}})}. \end{aligned}$$

This shows that

Corollary 3. *We can explicitly construct a family of complete graphs $\{K_N\}$, where K_N is a ℓ-colored complete graph on N vertices such that the monochromatic cliques have size at most*

$$2^{O(\sqrt[\ell]{\log N (\log\log N)^{\ell-1}})}.$$

6 Acknowledgments

I sincerely thank my advisor Prof. Zuckerman for his support and encouragement throughout this research project. I have learned greatly from him in both classes and discussions in his office. I would also like to thank Prof. Gál for valuable comments on the writeup.

References

[1] M. Ajtai, J. Komlós and E. Szemerédi, *A note on Ramsey numbers*, J. Combinatorial Theory Ser. A **29** (1980), 354-360.

[2] N. Alon, *Explicit Ramsey graphs and orthonormal labelings*, Electronic Journal of Combinatorics **1** (1994), R12.

[3] N. Alon, *Tough Ramsey graphs without short cycles*, J. Algebraic Combinatorics **4** (1995), 189-195.

[4] N. Alon, *The Shannon Capacity of a union*, Combinatorica **18** (1998), 301-310.

[5] N. Alon, L. Babai, and H. Suzuki, *Multilinear polynomials and Frankl-Ray-Chaudhuri-Wilson type intersection theorems*, J. Combinatorial Theory Ser. A **58** (1991), 165-180.

[6] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics, with Applications to Geometry and Computer Science*, Preliminary version 2, University of Chicago, 1992.

[7] D. A. M. Barrington, R. Beigel and S. Rudich, *Representing Boolean functions as polynomials modulo composite numbers*, Comput. Complexity **4** (1994), 367-382.

[8] F.R.K. Chung, R. Cleve and P. Dagum, *A note on constructive lower bounds for the Ramsey numbers $R(3,t)$*, J. Combinatorial Theory Ser. B **57** (1993), 150-155.

[9] R. Cleve and P. Dagum, *A constructive $\Omega(t^{1.26})$ lower bound for the Ramsey number $R(3,t)$*, Inter. Comp. Sci. Inst. Tech. Rep. TR-89-009, 1989.

[10] B. Codenotti, P. Pudlák and G. Resta, *Some structural properties of low rank matrices related to computational complexity*, Theoretical Computer Sci. **235** (2000), 89-107.

[11] P. Erdős, *Some remarks on the theory of graphs*, Bulletin of the Amer. Math. Soc. **53** (1947), 292-294.

[12] P. Erdős, *Graph Theory and Probability, II*, Canad. J. Math. **13** (1961), 346-352.

[13] P. Erdős, *On the construction of certain graphs*, J. Combinatorial Theory **17** (1966), 149-153.

[14] P. Frankl, *A constructive lower bound for Ramsey numbers*, Ars. Combin. **3** (1977), 125-127.

[15] P. Frankl and R. Wilson, *Intersection theorems with geometric consequences*, Combinatorica **1** (1981), 357-368.

[16] V. Grolmusz, *Superpolynomial Size Set-system with restricted intersections mod 6 and explicit Ramsey graphs*, Combinatorica **20** (2000), 1-14.

[17] V. Grolmusz, *Low-rank co-diagonal matrices and Ramsey graphs*, Electronic Journal of Combinatorics **7** (2000), R15.

[18] V. Grolmusz, *A note on explicit Ramsey graphs and modular sieves*, to appear in Combinatorics, Probability, and Computing.

[19] J. H. Kim, *The Ramsey number R(3,t) has order of magnitude* $t^2/\log t$, Random Structures & Algorithms **7** (1995), 173-207.

[20] T. Kővari, V.T. Sós, P. Turán, *On a problem of K. Zarankiewicz*, Colloquium Math., **3** (1954), 50-57.

[21] S. Jukna, *Extremal Combinatorics, with Applications in Computer Science*, Springer, 2000.

[22] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

[23] Z. Nagy, *A certain constructive estimate of the Ramsey number*, Matematikai Lapok **23** (1972), 301-302. (Hungarian)

[24] F. P. Ramsey, *On a problem of formal logic*, Proc. London Math. Soc. 2nd series **30** (1930), 264-286.

[25] J. van Lint and R. Wilson, *A Course in Combinatorics*, 2nd edition, Cambridge Univ. Press, Cambridge, 2001.