Constructive Ramsey theory

Gábor Hegedűs

Abstract

Explicit construction of Ramsey graphs has remained a challenging open problem for a long time. Frankl–Wilson [8], Alon [1] and Grolmusz [11] gave the best explicit constructions of graphs on 2^n vertices with no clique or independent set of size $c^{\sqrt{n \log n}}$. We present here simpler constructions using L-intersecting families, codes and permutations. In the proof we use the polynomial subspace method.

We describe also an explicit construction which, for some fixed absolute constant $c > 0$, produces for every integer $s > 1$ and all $m < s^s$, a graph on at least $m^{c\frac{\log s}{\log \log s}}$ vertices containing neither a clique of size s nor an independent set of size m.

1 Introduction

First we introduce some notation. Let n be a positive integer and $[n]$ stand for the set $\{1, 2, \dots, n\}$.

Let X be a set, $k > 0$ be a positive integer. We denote by $\binom{X}{k}$ the family of all k element subsets of X.

Let $s > 0$ be a fix integer and $k_i > 0$ be arbitrary integers for $1 \leq i \leq s$. The Ramsey number $R(k_1, \dots, k_s)$ is the smallest integer n such that in any s-coloring of the edges of a complete graph on n vertices K_n, there exists an $1 \leq i \leq s$ such that there is a homogeneouos K_{k_i} in the i^{th} color (i.e. a complete subgraph on k_i vertices all of whose edges are colored with the i^{th} color). In [13] F. P. Ramsey showed that $R(k_1, \dots, k_s)$ is finite for any s integers $k_1, \dots, k_s$. P. Erdős in [7] obtained by probabilistic arguments the following non–constructive lower bound for the diagonal Ramsey numbers $R(k, k)$:

Theorem 1.1 *If* $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$, *then* $R(k,k) > n$. *Thus* $R(k,k) > \lfloor 2^{k/2} \rfloor$ *for all* $k \geq 3$. □

One of the striking applications of the Frankl–Wilson theorem [8] for prime moduli was an explicit construction of graphs of size $\exp(\frac{c \log^2 k}{\log \log k})$ without homogeneous complete subgraph K_k. These are the largest explicit Ramsey–graphs known to date. V. Grolmusz in [10] gave an alternative construction of explicit Ramsey graphs of the same logarithmic order of magnitude. This construction is easily extandable to the case of several colors.

V. Grolmusz proved the following Theorem:

Theorem 1.2 *For* $r \geq 2$, $t \geq 3$, *there exists an explicitly constructible* $r-$*coloring of the edges of the complete graph on* $\exp(c_r \frac{(\log t)^r}{(\log \log t)^{r-1}})$ *vertices such that no color contains a complete graph on* t *vertices. Here* $c_r = c/p_r^{2r} \approx c(r \ln r)^{-2r}$, *where* p_r *is the* r^{th} *prime, and* $c > 0$ *is an absolute constant.* □

N. Alon in [1] obtained also an other explicit construction of Ramsey graphs. He used this construction disproving a conjecture of Shannon about Shannon capacity.

In these notes we give simpler Ramsey graph constructions using L-intersecting families, codes and permutations.

In [2] N. Alon and P. Pudlák obtained explicit constructions for the off-diagonal Ramsey numbers $R(m,s)$, where s is fixed and m tends to infinity. They proved the following result.

Theorem 1.3 *There exists an* $\epsilon > 0$ *and an explicit construction of graphs such that for every* s *and every sufficiently large* m *the construction produces a graph on at least* $m^{\epsilon\sqrt{\log s/\log\log s}}$ *vertices containing neither a clique of size* s *nor and independent set of size* m. *This shows, constructively, that* $R(s,m) > m^{\epsilon\sqrt{\log s/\log\log s}}$. □

Our main result improves their construction in the case $m < s^s$:

Theorem 1.4 *There exists an absolute constant $c > 0$ and an explicit construction of graphs such that for every s and every m with $m < s^s$ the construction produces a graph on at least $m^{c\log s/\log\log s}$ vertices containig neither a clique of size s nor an independent set of size m. This shows, constructively, that*

$$R(s,m) > m^{c\log s/\log\log s}.$$

2 L-intersecting families

Let $q = p^\alpha$, $\alpha \geq 1$ be a fixed prime power. Suppose that $1 < q < n$. Define

$$\mathcal{F}(q,\ell) := \{A \subseteq [n] : \ |A| \equiv \ell \pmod q\}.$$

Since

$$\cup_{\ell=0}^{q-1}\mathcal{F}(q,\ell) \tag{1}$$

gives a disjoint decomposition of $2^{[n]}$, hence there exists an $0 \leq \ell \leq q-1$ such that $|\mathcal{F}(q,\ell)| \geq \frac{2^n}{q}$.

Let $\mathcal{A} := \mathcal{F}(q,\ell)$ and define a 2-colored complete graph with vertex set $\mathcal{A}$. Let K be a complete graph with vertex set $\mathcal{A}$. We color an edge $\{U,V\}$ by blue iff $|U \cap V| \equiv \ell \pmod q$, and red otherwise.

Theorem 2.1 *Let ℓ be an integer and $q = p^\alpha$, $\alpha \geq 1$, a prime power. Suppose that $2(q-1) \leq n$. Assume that $\mathcal{F} = \{A_1, \ldots, A_m\}$ is a family of subsets of $[n]$ such that*

$$(a)\ |A_i| \equiv \ell \ (mod\ q)\ for\ i = 1, \ldots, m$$

$$(b)\ |A_i \cap A_j| \not\equiv \ell \ (mod\ q)\ for\ 1 \leq i,j \leq m,\ i \neq j.$$

Then

$$m \leq \binom{n}{q-1}.$$

Theorem 2.2 *(Deza–Frankl–Singhi) Let ℓ be an integer and $q = p^\alpha$, $\alpha \geq 1$, a prime power. Assume that $\mathcal{G} = \{A_1, \ldots, A_m\}$ is a family of subsets of $[n]$ such that*

$$(a)\ |A_i| \equiv \ell \ (mod\ q)\ for\ i = 1, \ldots, m$$

and

$$(b)\ |A_i \cap A_j| \equiv \ell \ (mod\ q)\ for\ 1 \leq i,j \leq m,\ i \neq j.$$

Then

$$m \leq \sum_{i=0}^{\lfloor \frac{n}{q} \rfloor} \binom{n}{i}.$$

□

Suppose that K contains a homogeneous red complete graph C of r vertices. Then the sets, corresponding to the vertices of C, give a family $\mathcal{F}$ of r sets, such that the size of each set is congruent with r modulo ℓ, but the size of the intersection of any two elements of this set-system is not congruent with ℓ modulo q. Consequently, by Theorem 2.1,

$$r \leq \binom{n}{q-1}. \tag{2}$$

□

Now suppose that K contains a homogeneous blue complete graph D of k vertices. Then the sets, corresponding to the vertices of D, give a family $\mathcal{G}$ of k sets, such that the size of each set and the size of the intersection of any two elements are congruent with ℓ modulo q. Theorem 2.2 yields to the bound

$$k \leq \sum_{i=0}^{\lfloor \frac{n}{q} \rfloor} \binom{n}{i}. \tag{3}$$

If $q = 2$, then we can apply the following Lemma:

Lemma 2.3 *Let $\mathcal{G} = \{A_1, \ldots, A_m\}$ be a family of subsets of $[n]$ such that*

$$(a)\ |A_i| \equiv 0 \text{ (mod 2) for } i = 1, \ldots, m$$

and

$$(b)\ |A_i \cap A_j| \equiv 0 \text{ (mod 2) for } 1 \leq i, j \leq m,\ i \neq j.$$

Then

$$m \leq 2^{\lfloor n/2 \rfloor}.$$

Then Lemma 2.3 gives that if K contains a homogeneous blue complete graph D of k vertices, then $k \leq 2^{\lfloor n/2 \rfloor}$, hence this gives a constructive proof of the bound $R(n, 2^{\lfloor n/2 \rfloor}) > 2^{n-1}$.

3 Codes

Let p be a prime, $r > 1$ be an integer, $n := p^r - 1$. Let $\mathcal{A} := 2^{[n]}$ be an arbitrary down–set. Define an r-colored complete graph with vertex set $\mathcal{A}$.

Let K be a complete graph with vertex set $\mathcal{A}$.

An r-coloring of the edges of K by colors $0, 1, \dots, r-1$:

an edge $\{U, V\}$, $U, V \in \mathcal{A}$, has color k iff $|U \triangle V| \equiv 0 \pmod{p^k}$ and $|U \triangle V| \not\equiv 0 \pmod{p^{k+1}}$.

Theorem 3.1 *Let $0 \le k < r$ be integers, p be a prime, $n := p^r - 1$. Assume that $\mathcal{G} = \{A_1, \dots, A_m\} \subseteq \mathcal{A}$ is a family of subsets of $[n]$ such that*

$$(a)\ |A_i \triangle A_j| \equiv 0 \ (mod\ p^k)\ for\ 1 \le i, j \le m,\ i \ne j \tag{4}$$

and

$$(b)\ |A_i \triangle A_j| \not\equiv 0 \ (mod\ p^{k+1})\ for\ 1 \le i, j \le m,\ i \ne j. \tag{5}$$

Then

$$m \le |\mathcal{A} \cap \binom{n}{\le p-1}|.$$

Proof.

Let $v_j = (v_{j1}, \dots, v_{jn}) \in \mathcal{A} \subseteq \{0,1\}^n$ denote the characteristic vector of A_j. Consider the polynomials:

$$F_j(x_1, \dots, x_n) := \prod_{\ell=1}^{p-1} (\sum_{i=1}^{n} ((1 - v_{ji})x_i + (1 - x_i)v_{ji}) - \ell p^k \in \mathbb{Q}[x_1, \dots, x_n] \tag{6}$$

and denote by $\overline{F_j}$ the reduction of F_j by a deglex Gröbner basis for the ideal $I := I(V(\mathcal{A}))$. Clearly $F_j(v) = \overline{F_j}(v)$ for each $v \in \mathcal{A}$. It is easy to verify that

$$\overline{F_j}(v_j) = F_j(v_j) = \prod_{\ell=1}^{p-1} |A_j \triangle A_j| - \ell p^k = p^{k(p-1)} \cdot (\prod_{\ell=1}^{p-1} (-\ell)).$$

Then clearly

$$\overline{F_j}(v_j) \equiv 0 \pmod{p^{k(p-1)}},$$

but

$$\overline{F_j}(v_j) \not\equiv 0 \pmod{p^{k(p-1)+1}}.$$

If $i \neq j$, then

$$\overline{F_j}(v_i) = F_j(v_i) = \prod_{\ell=1}^{p-1}(|A_i \triangle A_j| - \ell p^k) = \prod_{\ell=1}^{p-1} p^k(\frac{|A_i \triangle A_j|}{p^k} - \ell)$$

$$= p^{k(p-1)} \prod_{\ell=1}^{p-1}(\frac{|A_i \triangle A_j|}{p^k} - \ell).$$

Since $|A_i \triangle A_j| \not\equiv 0 \pmod{p^{k+1}}$, hence there exists $1 \leq \ell \leq p-1$ such that

$$\frac{|A_i \triangle A_j|}{p^k} \equiv \ell \pmod{p},$$

therefore

$$\prod_{\ell=1}^{p-1}(\frac{|A_i \triangle A_j|}{p^k} - \ell) \equiv 0 \pmod{p}$$

i.e.,

$$\overline{F_j}(v_i) \equiv 0 \ (\mathrm{mod}\ p^{k(p-1)+1})$$

for each $j \neq i$.

We need for the following observation.

Proposition 3.2 *Let A be an $m \times m$ matrix with integer entries. If some prime power $q = p^\alpha$ divides each off-diagonal entry but it does not divide any of the diagonal entries then A is nonsingular.* □

We thus found that the $m \times m$ matrix $F := (F_j(v_i))_{1 \leq i,j \leq m}$ is nonsingular by Proposition 3.2, because $p^{p(k-1)+1}$ divides each off-diagonal entry but it does not divide any of the diagonal entries of F. From Proposition 2.7 of [4] (Determinant Criterion) it follows that the polynomials $\overline{F_1}, \ldots, \overline{F_m}$ are linearly independent functions over $\mathbb{Q}$.

Moreover, being reduced polynomials with respect to a Gröbner basis, the $\overline{F_i}$ are linear combination of standard monomials for I and $\deg(\overline{F_i}) \leq p-1$, because $\deg(F_i) = p-1$ and the deglex reductions can not increase the degree. Since $\mathcal{A}$ was a down–set, hence $\mathrm{Sm}(\prec_{deg}, \mathcal{A}) = \mathcal{A}$. We infer that the linearly independent polynomials $\{\overline{F_1}, \ldots, \overline{F_m}\}$ are in the $\mathbb{Q}$-space spanned by $\{x_A : \ A \in \mathcal{A}\}$, and hence

$$m \leq |\mathcal{A} \cap \binom{n}{\leq p-1}|,$$

which was to be proved. □

Suppose that K contains a homogeneous complete graph C_k of ℓ_k vertices in color k. Then the sets, corresponding to the vertices of C_k, give a family $\mathcal{F}_k$ of ℓ_k sets with the properties (a) and (b). Consequently, by the previous Theorem,

$$\ell_k \leq \sum_{i=0}^{p-1} \binom{n}{i}.$$

Hence we obtain the constructive bound:

$$R(\underbrace{\sum_{i=0}^{p-1} \binom{p^r-1}{i}, \ldots, \sum_{i=0}^{p-1} \binom{p^r-1}{i}}_{r}) > 2^{p^r-1}.$$

4 Generalized metric spaces

Definition 4.1 *We say that a pair $(\mathcal{F}, d)$ is a* generalized metric space*, where $d : \mathcal{F} \times \mathcal{F} \to \mathbb{Z}$ is a function with the properties:*

$$(i)\ d(f,f) = 0 \text{ for each } f \in \mathcal{F},$$

$$(ii)\ d(f,g) \in \mathbb{N} \text{ for each } f, g \in \mathcal{F}$$

and

$$(iii)\ d(f,g) = d(g,f) \text{ for each } f, g \in \mathcal{F}.$$

Construction:

Let p be a prime, $r > 1$ be an integer, $n := p^r - 1$. Suppose that $(\mathcal{F}, d)$ is a bounded generalized metric space and $d(f,g) \leq n$ for each $f, g \in \mathcal{F}$.

We define an r-colored complete graph with vertex set $\mathcal{F}$.

Let K be a complete graph with vertex set $\mathcal{F}$.

We give an explicit r-coloring of the edges of K by colors $0, 1, \ldots, r-1$: an edge $\{f, g\}$, $f, g \in \mathcal{F}$, has color k iff $d(f,g) \equiv 0 \pmod{p^k}$ and $d(f,g) \not\equiv 0 \pmod{p^{k+1}}$.

Examples

(1) Let $\mathcal{F} := \binom{[m]}{n}$ and $d(f,g) := n - |f \cap g|$ for each $f, g \in \mathcal{F}$. Clearly $(\mathcal{F}, d)$ is a generalized metric space and $d(f,g) \leq n$ for each $f, g \in \mathcal{F}$.

An edge $\{f, g\}$, $f, g \in \mathcal{F}$ has color k iff $|f \cap g| \equiv -1 \pmod{p^k}$ and $|f \cap g| \not\equiv -1 \pmod{p^{k+1}}$.

(2) Let $A := \{0, 1, \ldots, q-1\} \subseteq \mathbb{Q}$. The Hamming distance $d_H(a, b)$ between two words $\underline{a} = (a_1, \ldots, a_n)$ and $\underline{b} = (b_1, \ldots, b_n)$ in A^n is the number of coordinates i, $1 \leq i \leq n$, with $a_i \neq b_i$. Let $\mathcal{F} := A^n$ and define $d(a, b) := d_H(a, b)$.

Clearly $(\mathcal{F}, d)$ is a generalized metric space and $d(f, g) \leq n$ for each $f, g \in \mathcal{F}$.

An edge $\{f, g\}$, $f, g \in \mathcal{F}$, has color k iff $d_H(f, g) \equiv 0 \pmod{p^k}$ and $d_H(f, g) \not\equiv 0 \pmod{p^{k+1}}$.

(3) Let $\mathcal{P}_n$ denote the set of all permutations

$$\mathcal{P}_n = \{f : [n] \to [n] : \quad f \text{ is a bijection }\}.$$

Let $\mathrm{Fix}(f) \in \mathbb{N}$ denote the number of fixpoints of a permutation. Then

$$d(f, g) := n - \mathrm{Fix}(f \cdot g^{-1})$$

is the Hamming distance of f and g for each $f, g \in \mathcal{P}_n$, $f \neq g$.

Clearly $(\mathcal{F}, d)$ is a generalized metric space and $d(f, g) \leq n$ for each $f, g \in \mathcal{F}$.

An edge $\{f, g\}$, $f, g \in \mathcal{F}$ has color k iff $\mathrm{Fix}(f \cdot g^{-1}) \equiv -1 \pmod{p^k}$ and $\mathrm{Fix}(f \cdot g^{-1}) \not\equiv -1 \pmod{p^{k+1}}$.

Definition 4.2 *Let $(\mathcal{F}, d)$ be a generalized metric space. A* polynomial representation *of $\mathcal{F}$ over a field $\mathbb{F}$ is an assignment of a polynomial*

$$P_f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$$

and a vector $w_f \in \mathbb{F}^n$ to $f \in \mathcal{F}$ such that

$$P_f(w_g) = d(f, g) \textit{ for each } f, g \in \mathcal{F}.$$

We say that a generalized metric space $(\mathcal{F}, d)$ is representable with polynomials over a finite alphabet $A \subseteq \mathbb{F}$ if $\{w_f : \ f \in \mathcal{F}\} \subseteq A^n \subseteq \mathbb{F}^n$.

Examples

(1) $\mathcal{F} := \binom{[m]}{n}$. Let $f \in \mathcal{F}$, define $w_f := v_f = (v_1, \ldots, v_n) \in \{0, 1\}^m \subseteq \mathbb{Q}^m$ the characteristic vector of f and

$$P_f(x_1, \ldots, x_m) := n - \sum_{i=1}^{m} v_i x_i \in \mathbb{Q}[x_1, \ldots, x_m].$$

Then $P_f(v_g) = n - |f \cap g| = d(f,g)$. Clearly $A = \{0,1\}$.

(2) $\mathcal{F} := A^n$. By Lagrange interpolation, for each integer $a \in A$ there exists an $\epsilon(a,x) \in \mathbb{Q}[x]$ polynomial such that

$$\epsilon(a,b) := \begin{cases} 0 & \text{if } b = a \\ 1 & \text{if } b \neq a \end{cases}$$

for all $b \in A$. Let $f = (f_1, \ldots, f_n) \in A^n$, then $w_f := f \in A^n$ and define

$$P_f(x_1, \ldots, x_n) := \sum_{i=1}^{n} \epsilon(f_i, x_i) \in \mathbb{Q}[x_1, \ldots, x_n].$$

Clearly

$$P_f(g) = \sum_{i=1}^{n} \epsilon_i(f_i, g_i) = d_H(f,g) = d(f,g)$$

for each $f, g \in \mathcal{F}$.

(3) $\mathcal{F} = \mathcal{P}_n$. We assign for each $f \in \mathcal{P}_n$ an $n \times n$ permutation matrix $A_f \in \mathrm{Mat}(\mathbb{Q}, n)$ with the following rule:

$$A_f[i,j] := \begin{cases} 1 & \text{if } f(i) = j \\ 0 & \text{otherwise,} \end{cases}$$

where $1 \leq i, j \leq n$. We can consider also this matrix $A_f \in \mathrm{Mat}(\mathbb{Q}, n)$ as a vector $v_f \in \{0,1\}^{n^2} \subseteq \mathbb{Q}^{n^2}$.

By the definition of the matrix A_f,

$$\mathrm{Tr}(A_f) = \mathrm{Fix}(f),$$

and clearly A is a group homomorphism from $\mathcal{P}_n$ to $\mathrm{Mat}(\mathbb{Q}, n)$:

$$A_f \cdot A_g = A_{f \cdot g}.$$

Consider the following polynomial in the variables $(x_{11}, \ldots, x_{nn})$:

$$P_f(x_{11}, \ldots, x_{nn}) := n - \sum_{i=1}^{n} \sum_{j=1}^{n} A_{f^{-1}}[i,j] \cdot x_{ji} \in \mathbb{Q}[x_{11}, \ldots, x_{nn}]. \qquad (7)$$

Then it is easy to see that

$$\begin{aligned} P_f(v_g) &= n - \mathrm{Tr}(A_{f^{-1}} \cdot A_g) = n - \mathrm{Tr}(A_{f^{-1} \cdot g}) \\ &= n - \mathrm{Fix}(f^{-1} \cdot g) = d_H(f,g) = d(f,g) \qquad (8) \end{aligned}$$

for each $f, g \in \mathcal{P}_n$.

Define $A := \{0,1\}$.

Theorem 4.3 *Let $(\mathcal{G}, d)$ be a generalized metric space and $\{(P_g, w_g) : \ g \in \mathcal{G}\}$ be a polynomial representation of $(\mathcal{G}, d)$ with codes over the alphabet $A \subseteq \mathbb{Q}$. Assume that $\mathcal{F} = \{f_1, \dots, f_m\}$ is a subfamily of $\mathcal{G}$ such that*

$$(a)\ d(f_i, f_j) \equiv 0 \ (mod\ p^k)\ for\ 1 \le i, j \le m, \ i \neq j$$

and

$$(b)\ d(f_i, f_j) \not\equiv 0 \ (mod\ p^{k+1})\ for\ 1 \le i, j \le m, \ i \neq j$$

Define

$$Q_f := \prod_{\ell=1}^{p-1} (P_f - \ell \cdot p^k) \in \mathbb{Q}[x_1, \dots, x_n]$$

and let $\overline{Q_f}$ denote the reduction of Q_f via the polynomials $\{\prod_{a \in A}(x_i - a) : \ 1 \le i \le n\}$. Then

$$m \le dim_{\mathbb{Q}}(\{\overline{Q_f} : \ f \in \mathcal{F}\}).$$

Proof.

It is enough to show, that $\{\overline{Q_f} : \ f \in \mathcal{F}\}$ are linearly independent polynomials over $\mathbb{Q}$.

Since

$$\overline{Q_f}(v_f) = Q_f(v_f) = \prod_{\ell=1}^{p-1}(P_f(v_f) - \ell \cdot p^k) = \prod_{\ell=1}^{p-1}(d(f, f) - \ell \cdot p^k) = p^{k(p-1)} \cdot (\prod_{\ell=1}^{p-1}(-\ell)), \tag{9}$$

hence

$$Q_f(v_f) \equiv 0 \ (\text{mod } p^{k(p-1)}), \tag{10}$$

but

$$Q_f(v_f) \not\equiv 0 \ (\text{mod } p^{k(p-1)+1}). \tag{11}$$

If $f \neq g$, then

$$Q_f(v_g) = \prod_{\ell=1}^{p-1}(P_f(v_g) - \ell \cdot p^k) = \prod_{\ell=1}^{p-1}(d(f, g) - \ell \cdot p^k) = \tag{12}$$

$$= \prod_{\ell=1}^{p-1} p^k \cdot (\frac{d(f, g)}{p^k} - \ell) = p^{k(p-1)} \cdot \prod_{\ell=1}^{p-1}(\frac{d(f, g)}{p^k} - \ell). \tag{13}$$

Since $d(f,g) \not\equiv 0 \pmod{p^{k+1}}$, hence there exists an $1 \le \ell \le p-1$ such that

$$\frac{d(f,g)}{p^k} \equiv \ell \pmod{p}.$$

This means that

$$\prod_{\ell=1}^{p-1} (\frac{d(f,g)}{p^k} - \ell) \equiv 0 \pmod{p},$$

i.e.,

$$\overline{Q_f}(v_g) = Q_f(v_g) \equiv 0 \text{ (mod } p^{k(p-1)+1}) \tag{14}$$

for each $f \neq g$.

We need for the following observation.

Proposition 4.4 *Let A be an $m \times m$ matrix with integer entries. If some prime power $q = p^\alpha$ divides each off-diagonal entry but it does not divide any of the diagonal entries then A is nonsingular.* □

We thus found that the $m \times m$ matrix $Q := (\overline{Q_j}(v_i))_{1 \le i,j \le m}$ is nonsingular by Proposition 4.4, because $p^{p(k-1)+1}$ divides each off-diagonal entry but it does not divide any of the diagonal entries of Q. From Proposition 2.7 of [4] (Determinant Criterion) it follows that the polynomials $\{\overline{Q_f} : \ f \in \mathcal{F}\}$ are linearly independent functions over $\mathbb{Q}$. □

Suppose that K contains a homogeneous complete graph C_k of ℓ_k vertices in color k. Then the elements, corresponding to the vertices of C_k, give a family $\mathcal{F}_k$ of ℓ_k elements with the properties (a) and (b). Consequently, by the previous Theorem,

$$\ell_k \le \dim_{\mathbb{Q}}\{\overline{Q_f} : \ f \in \mathcal{F}\}.$$

Examples

(1) Clearly $\overline{Q_f}$ are multilinear polynomials of degree at most $p-1$, since P_f were linear polynomials, therefore $\dim_{\mathbb{Q}}\{\overline{Q_f} : \ f \in \mathcal{F}\} \le \sum_{i=0}^{p-1} \binom{m}{i}$.

Hence we get the following constructive bound:

$$R(\underbrace{\sum_{i=0}^{p-1} \binom{m}{i}, \dots, \sum_{i=0}^{p-1} \binom{m}{i}}_{r}) > \binom{m}{p^r - 1}.$$

(2) As a polynomial in the variables $x_1, \dots, x_n$, $\overline{Q_f}$ has the property that each term is a monomial in which at most $p-1$ distinct indeterminates x_i enter. As functions from A^n to the field $\mathbb{Q}$, all $\overline{Q_f}$, $f \in \mathcal{F}$ lie in the span of the $\sum_{i=0}^{p-1}(q-1)^i\binom{n}{i}$ monomial functions in which at most $p-1$ distinct variables x_i enter and the exponent of each x_i is at most $q-1$. This is because if any indeterminate x_j occurs in term of $Q_f(x)$ with exponent $e > q-1$, we can reduce it modulo $\prod_{a\in A}(x_j - a)$, that is, we can replace x_j^e by a polynomial in x_j of degree less then q that represent the same function on A. Hence $\dim_{\mathbb{Q}}\{\overline{Q_f} :\ f \in \mathcal{F}\} \leq \sum_{i=0}^{p-1}(q-1)^i\binom{n}{i}$.

Thus yields to the constructive bound:

$$R(\underbrace{\sum_{i=0}^{p-1}(q-1)^i\binom{n}{i}, \dots, \sum_{i=0}^{p-1}(q-1)^i\binom{n}{i}}_{r}) > q^n.$$

(3) Finally, $\overline{Q_f}$ are again multilinear polynomials of degree at most $p-1$, since P_f were linear polynomials, therefore $\dim_{\mathbb{Q}}\{\overline{Q_f} :\ f \in \mathcal{F}\} \leq \sum_{i=0}^{p-1}\binom{n^2}{i}$.

Hence we obtain the constructive bound:

$$R(\underbrace{\sum_{i=0}^{p-1}\binom{n^2}{i}, \dots, \sum_{i=0}^{p-1}\binom{n^2}{i}}_{r}) > n!.$$

We give now a construction, which gives natural lower bounds for the off–diagonal Ramsey numbers $R(m,s)$, $m < s^s$.

Construction 2

Let p be a prime, $\alpha \geq 1$, $n := p^\alpha - 1$.

Suppose that $(\mathcal{F}, d)$ is a bounded generalized metric space and $d(f,g) \leq n$ for each $f, g \in \mathcal{F}$.

We define an 2-colored complete graph with vertex set $\mathcal{F}$.

Let K be a complete graph with vertex set $\mathcal{F}$.

We give an explicit 2-coloring of the edges of K by colors red and blue:

an edge $\{f,g\}$, $f, g \in \mathcal{F}$, has color blue iff $d(f,g) \equiv 0 \pmod{p}$ and red otherwise.

Suppose that K contains a homogeneous red complete graph R of r vertices. Then the elements, corresponding to the vertices of R, give a family $\mathcal{F}$ of r elements such that $d(f,g) \not\equiv 0 \pmod{p}$ for each $f, g \in \mathcal{F}$.

Examples

(1) By Theorem 4.3, $\overline{Q_f}$ are multilinear polynomials of degree at most $p-1$, since P_f were linear polynomials, therefore $r \leq \sum_{i=0}^{p-1} \binom{m}{i}$.

(2) The polynomials $\overline{Q_f}$ has the property that each term is a monomial in which at most $p-1$ distinct indeterminates x_i enter, and the exponent of each x_i is at most $q-1$. Hence $r \leq \sum_{i=0}^{p-1}(q-1)^i \binom{n}{i}$.

(3) Finally, $\overline{Q_f}$ are multilinear polynomials of degree at most $p-1$, since P_f were linear polynomials, therefore $r \leq \sum_{i=0}^{p-1} \binom{n^2}{i}$.

Suppose that K contains a homogeneous blue complete graph B of b vertices. Then the elements, corresponding to the vertices of B, give a family $\mathcal{G}$ of b elements such that $d(f,g) \equiv 0 \pmod{p}$ for each $f, g \in \mathcal{G}$.

Examples

(1) By Theorem 4.3, $\overline{Q_f}$ are multilinear polynomials of degree at most $p^{\alpha-1}-1$, since P_f were linear polynomials, therefore $b \leq \sum_{i=0}^{p^{\alpha-1}-1} \binom{m}{i}$.

(2) Each term of the polynomials $\overline{Q_f}$ is a monomial in which at most $p-1$ distinct indeterminates x_i enter, and the exponent of each x_i is at most $q-1$. Hence $b \leq \sum_{i=0}^{p^{\alpha-1}-1}(q-1)^i \binom{n}{i}$.

(3) Finally, $\overline{Q_f}$ are multilinear polynomials of degree at most $p-1$, since P_f were linear polynomials, therefore $b \leq \sum_{i=0}^{p^{\alpha-1}-1} \binom{n^2}{i}$.

Hence we obtain the following result.

Theorem 4.5 *There exists an explicit construction of graphs such that for every s and every m with $m < s^s$ the construction produces a graph on at least $m^{c \log s/ \log\log s}$ vertices containig neither a clique of size s nor an independent set of size m. This shows, constructively, that*

$$R(s,m) > m^{c \log s/ \log\log s}.$$

References

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

[2] N. Alon, P. Pudlák, Constructive Lower Bounds for off-diagonal Ramsey Numbers, *Israel J. of Math.* **122** (2001) 243–251.

[3] N. Alon, M. Krivelevich, Constructive bounds for a Ramsey-type problem, *Graphs and Combinatorics* **13** (1997), 217–225.

[4] L. Babai, P. Frankl, *Linear algebra methods in combinatorics,* September 1992.

[5] L. Babai, H. Snevily, R. M. Wilson, A New Proof of Several Inequalities on Codes and Sets, *J. of Comb. Theory A* **71** 146–153 (1995)

[6] P. J. Cameron, Metric and geometric properties of sets of permutations, pp. 39–53 in *Algebraic, Extremal and Metric Combinatorics*, London Math. Soc. Lecture Notes **131**, Cambridge University Press, 1988

[7] P. Erdős, Some Remarks on the Theory of Graphs, *Bulletin of the American Mathematical Society*, **53** 292–294 (1947)

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

[9] P. Gopalan, Constructing Ramsey Graphs from Boolean Function Representations, *Elect. Colloquium on Comput. Complexity*, Report No. 143 (2005)

[10] V. Grolmusz, Low Rank Co-Diagonal Matrices and Ramsey Graphs, *Electronic J. of Comb.* Vol. 7, (2000), No. 1., R15

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

[12] V. Grolmusz, A Note on Explicit Ramsey Graphs and Modular Sieves, *Combin. Prob. and Computing* Vol. 12., (2003) 565–569.

[13] F. P. Ramsey, On a problem of formal logic, *Proc. London Math. Soc.* **30** (2), 264–286 (1929)