AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **64(2)** (2016), Pages 347–353

A bound for s-distance permutation families and explicit Ramsey graphs

Gábor Hegedüs

Óbuda University
Antal Bejczy Center for Intelligent Robotics
Kiscelli utca 82, Budapest, H-1032
Hungary
hegedus.gabor@nik.uni-obuda.hu

Abstract

Cameron gave an upper bound for the size of any s-distance family of permutations. We prove a modulo p version of Cameron's result. In the proof we use the polynomial subspace method. As an application we describe here an explicit construction which produces for every integer $m > 1$ a graph on at least $m^{(1+o(1))\frac{2}{9}\frac{\log m}{\log\log m}}$ vertices containing neither a clique of size m 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 $\{1, 2, \ldots, n\}$.

Let S_n denote the complete group of permutations. Let $\pi \in S_n$ be any permutation, then

$$\mathrm{Fix}(\pi) := \{i \in [n] : \ \pi(i) = i\}$$

denotes the set of fix-points of π.

If $\mathcal{F} \subseteq S_n$ is any family of permutations, then define the *distance set* of $\mathcal{F}$ as

$$L(\mathcal{F}) := \{n - |\mathrm{Fix}(\pi^{-1}\tau)| : \ \pi, \tau \in \mathcal{F}, \pi \neq \tau\}.$$

It is immediate from the definition that $0 \notin L(\mathcal{F})$. We say that $\mathcal{F} \subseteq S_n$ is an s-distance family of permutations, if $s = |L(\mathcal{F})|$.

Cameron proved in [8] the following remarkable result.

Theorem 1.1 *Let $\mathcal{F}$ be an s-distance family of permutations of S_n, then*

$$|\mathcal{F}| \leq \sum_{\chi \in \mathrm{Irr}(S_n), \dim(\chi) \leq s} \chi(1)^2, \tag{1}$$

where $\mathrm{Irr}(S_n)$ is the set of irreducible characters of S_n.

Remark. Cameron showed that for fixed s and large n, the order of magnitude of the bound $\sum_{\chi\in \mathrm{Irr}(S_n),\dim(\chi)\leq s}\chi(1)^2$ is asymptotically

$$\frac{p(s)n^{2s}}{(s!)^2}, \tag{2}$$

where $p(s)$ is the number of partition of s.

Remark. An (n,d)-permutation code is a subset C of S_n such that the Hamming distance between any two distinct elements of C is at least equal to d. These codes were the main motivation for the investigation of the upper bounds for the size of s-distance families of permutations. Blake proposed first these codes in 1974 in [7] as error-correcting codes for powerline communications (see [7]). This application motivated the study of the largest possible size that a permutation code with fixed parameters (n,d) can have.

Cameron obtained also in [8] the following upper bound from Ray-Chaudhuri and Wilson's Theorem (see [16]). We use this upper bound in our explicit Ramsey construction.

Theorem 1.2 *Let $\mathcal{F}$ be an s-distance family of permutations of S_n, then*

$$|\mathcal{F}|\leq \binom{n^2}{s}. \tag{3}$$

Our main result is the following modulo p version of Cameron's Theorem 1.2.

Let $\mathcal{F}$ be a permutation family of S_n. and $1<m<n$ be an integer. We say that $\mathcal{F}$ is a *modulo m s-distance family* if there exists an $S\subseteq[m-1]=\{1,2,\ldots,m-1\}$, $|S|=s$ subset such that for each $\ell\in L(\mathcal{F})$ there exists a $t\in S$ with $\ell\equiv t \pmod m$. Specially it follows from the definition that if $\mathcal{F}$ is a modulo m s-distance family, then

$$\{km:\ k\in\mathbb{Z}\}\cap L(\mathcal{F})=\emptyset.$$

Theorem 1.3 *Let p be a prime. Let $\mathcal{F}$ be a modulo p s-distance family. Then*

$$|\mathcal{F}|\leq \sum_{i=0}^{s}\binom{n^2}{i}. \tag{4}$$

Let $s>0$ be a fixed integer and $k_i>0$ be arbitrary integers for $1\leq i\leq s$. The Ramsey number $R(k_1,\ldots,k_s)$ 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 homogeneous 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). Ramsey showed in [15] that $R(k_1,\ldots,k_s)$ is finite for any s integers $k_1,\ldots,k_s$. Erdős in [9] obtained by probabilistic arguments the following non-constructive lower bound for the diagonal Ramsey numbers $R(n,n)$:

Theorem 1.4 *If* $\binom{m}{n} \cdot 2^{1-\binom{n}{2}} < 1$, *then* $R(n,n) > m$. *Thus* $R(n,n) > \lfloor 2^{n/2} \rfloor$ *for all* $n \geq 3$.

One of the most striking applications of the Frankl-Wilson theorem [10] for prime moduli was an explicit construction of graphs of size $\exp((1+o(1))\frac{1}{4}\log^2 k/\log\log k)$ without homogeneous complete subgraph K_k. Grolmusz in [12] gave an alternative construction of explicit Ramsey graphs of the same logarithmic order of magnitude. This construction is easily extendable to the case of several colors.

Grolmusz proved the following Theorem in [12].

Theorem 1.5 *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.*

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

Barak, Rao, Shaltiel and Widgerson in [6, Theorem 1.4] obtained the largest explicit Ramsey-graphs known to date.

Theorem 1.6 *Let* $C > 1$ *be a fixed positive number. Then there exists an explicit construction of graphs such that the construction produces a graph on at least* $m^{(\log m)^C}$ *vertices containing neither a clique of size* m *nor an independent set of size* m.

Their construction is quite complicated. As an application of our Theorem 1.3, we give here a simpler explicit Ramsey construction based on permutation families.

Theorem 1.7 *Let* p *be a prime. For* $m := \max(\binom{p^4}{p}, \sum_{i=0}^{p-1}\binom{p^4}{i})$ *there exists an explicit construction of graphs such that the construction produces a graph on at least* $m^{(1+o(1))\frac{2}{9}\frac{\log m}{\log\log m}}$ *vertices containing neither a clique of size* m *nor an independent set of size* m.

2 The proof

We assign for each $\pi \in S_n$ an $n \times n$ permutation matrix $A_\pi \in \mathrm{Mat}(\mathbb{Q}, n)$ over $\mathbb{Q}$ with the following rule:

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

where $1 \leq i, j \leq n$.

We can consider also this matrix $A_\pi \in \mathrm{Mat}(\mathbb{R}, n)$ as a vector $\mathbf{v}(\pi) \in \{0,1\}^{n^2} \subseteq \mathbb{R}^{n^2}$. Here $\mathbf{v}(\pi)_{i,j} := A_\pi[i,j]$ for each $1 \leq i, j \leq n$. This means that we defined $\mathbf{v}(\pi)$ as a concatenation of the rows of the matrix A.

Clearly

$$\mathrm{Tr}(A_\pi) = |\mathrm{Fix}(\pi)|, \tag{5}$$

by the definition of the matrix A_π and A is a group homomorphism from S_n to the matrix group $\mathrm{GL}(\mathbb{R}, n)$:

$$A_\pi \cdot A_\tau = A_{\pi\cdot\tau}.$$

We recall here for the reader's convenience the following criterion (see [4, Proposition 5.7]).

Proposition 2.1 *(Determinant Criterion) Let $\mathbb{F}$ denote an arbitrary field. Let $f_i : \Omega \to \mathbb{F}$ be functions for each $i = 1, \ldots, m$ and $\mathbf{v}_i \in \Omega$ elements such that the $m \times m$ matrix $B = (f_i(\mathbf{v}_j))_{i,j=1}^m$ is nonsingular. Then $f_1, \ldots, f_m$ are linearly independent functions of the space $\mathbb{F}^\Omega$.*

The following simple observation is a key ingredient in our proof (see [4, Proposition 5.16]). Recall that a polynomial is *multilinear* if it has degree at most one in each variable.

Proposition 2.2 *(Multilinearization) Let $\mathbb{F}$ denote an arbitrary field and $\Omega := \{0,1\}^n \subseteq \mathbb{F}^n$. If $f \in \mathbb{F}[x_1, \ldots, x_n]$ is an arbitrary polynomial of degree at most s then there exists a unique multilinear polynomial $g \in \mathbb{F}[x_1, \ldots, x_n]$ of degree at most s such that*

$$f(\mathbf{v}) = g(\mathbf{v})$$

for each $\mathbf{v} \in \{0,1\}^n$.

This is clear since we can use the identity $x_i^2 = x_i$ valid over $\Omega = \{0,1\}^n$.

The proof of Theorem 1.3:

Let $\mathbb{K} := \mathbb{F}_p[x_{1,1}, \ldots, x_{n,n}]$ denote the polynomial ring in the variables $x_{i,j}$, $1 \leq i, j, \leq n$ over the finite field $\mathbb{F}_p$.

For each $\pi \in \mathcal{F}$ consider the polynomial

$$P_\pi(x_{1,1}, \ldots x_{n,n}) := n - \sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{v}(\pi^{-1})_{i,j} \cdot x_{j,i} \in \mathbb{K}.$$

Let $\tau, \pi \in S_n$ be two fixed permutations. Then $\mathbf{v}(\tau) = (\mathbf{v}_{1,1}, \ldots \mathbf{v}_{n,n}) \in \{0,1\}^{n^2}$ and clearly

$$P_\pi(\mathbf{v}_{1,1}, \ldots \mathbf{v}_{n,n}) = n - \sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{v}(\pi^{-1})_{i,j} \cdot \mathbf{v}_{j,i} =$$

$$= n - Tr(A_{\pi^{-1}} A_\tau) = n - Tr(A_{\pi^{-1}\cdot\tau}) = n - |\mathrm{Fix}(\pi^{-1} \cdot \tau)|.$$

Since $\mathcal{F}$ is a modulo p s-distance family, there exists an $S \subseteq [m-1]$, $|S| = s$ subset such that for each $\ell \in L(\mathcal{F})$ there exists a $t \in S$ with $\ell \equiv t \pmod m$.

Define

$$Q_\pi(x_{1,1},\dots x_{n,n}) := \prod_{s\in S}(P_\pi(x_{1,1},\dots x_{n,n}) - s) \in \mathbb{K}.$$

Let R_π denote the unique multilinearization of Q_π. Clearly $\deg(R_\pi) \le \deg(Q_\pi) \le s$, because $|S| = s$.

Now we prove that the set of polynomials $\{R_\pi : \pi \in \mathcal{F}\}$ are linearly independent over $\mathbb{F}_p$.

1. Let $\pi \neq \tau \in \mathcal{F}$ be two different permutations. Let $\mathbf{v}(\tau) = (\mathbf{v}_{1,1},\dots \mathbf{v}_{n,n}) \in \{0,1\}^{n^2}$. Then

$$R_\pi(\mathbf{v}_\tau) = Q_\pi(\mathbf{v}_\tau) = \prod_{s\in S}(P_\pi(\mathbf{v}_{1,1},\dots \mathbf{v}_{n,n}) - s) =$$

$$= \prod_{s\in S}(n - |\mathrm{Fix}(\pi^{-1}\cdot\tau)| - s).$$

But $\mathcal{F}$ is a modulo p s-distance family, hence for each $\ell \in L(\mathcal{F})$ there exists a $t \in S$ with $\ell \equiv t \pmod p$). Clearly $n - |\mathrm{Fix}(\pi^{-1}\cdot\tau)| \in L(\mathcal{F})$ by definition of $L(\mathcal{F})$, hence

$$\prod_{s\in S}(n - |\mathrm{Fix}(\pi^{-1}\cdot\tau)| - s) \equiv 0 \pmod p$$

Consequently

$$R_\pi(\mathbf{v}_\tau) \equiv 0 \pmod p.$$

2. On the other hand,

$$R_\pi(\mathbf{v}_\pi) = \prod_{s\in S}(-s),$$

and since $S \subseteq [p-1]$, hence

$$R_\pi(\mathbf{v}_\pi) \not\equiv 0 \pmod p.$$

From Proposition 2.1 follows immediately that the set of polynomials $\{R_\pi : \pi \in \mathcal{F}\}$ are linearly independent over $\mathbb{F}_p$. But $\{R_\pi : \pi \in \mathcal{F}\}$ are multilinear polynomials and $\deg(R_\pi) \le s$, hence $|\mathcal{F}| \le \sum_{i=0}^{s}\binom{n^2}{i}$. □

3 The construction

In the following we prove Theorem 1.7.

Let p denote a fixed prime number. Let $n := p^2$ and $t := n!$.

We define a 2-colored complete graph with vertex set S_n. Let K_t denote the complete graph with vertex set S_n. Let π, τ be two fixed, distinct permutations. We

color an edge $\{\pi, \tau\} \in E(K_t)$ by blue iff $n - |\mathrm{Fix}(\pi^{-1} \cdot \tau)| \equiv 0 \pmod{p}$, and red otherwise.

Suppose that K_t contains a homogeneous red complete subgraph C on r vertices. Then the permutations, corresponding to the vertices of C, give a family $\mathcal{F}$ of r permutations, such that $n - |\mathrm{Fix}(\pi^{-1} \cdot \tau)| \not\equiv 0 \pmod{p}$ for all $\pi, \tau \in \mathcal{F}$, $\pi \neq \tau$. Hence $\mathcal{F}$ is a modulo p $(p-1)$-distance family with $S = [p-1]$. Consequently, by Theorem 1.3,

$$r \leq \sum_{i=0}^{p-1} \binom{n^2}{i}. \tag{6}$$

But $\sum_{i=0}^{p-1} \binom{n^2}{i}$ is asymptotically $n^{\frac{3\sqrt{n}}{2}}$ by the choice of n and p.

Now suppose that K_t contains a homogeneous blue complete subgraph D on k vertices. Then the permutations, corresponding to the vertices of D, give a permutation family $\mathcal{G}$ of k permutations, such that $n - |\mathrm{Fix}(\pi^{-1} \cdot \tau)| \equiv 0 \pmod{p}$ for all $\pi, \tau \in \mathcal{G}$, $\pi \neq \tau$. Hence $\mathcal{G}$ is a p-distance permutation family, where $L(\mathcal{G}) := \{kp : \ 1 \leq k \leq p\}$.

Consequently Theorem 1.2 yields to the bound

$$k \leq \binom{n^2}{p}. \tag{7}$$

But $\binom{n^2}{p}$ is asymptotically $n^{\frac{3\sqrt{n}}{2}}$ by the choice of n and p.

But $t = n!$, hence Theorem 1.7 follows from an easy computation using the bounds (6) and (7).

References

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

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

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

[4] L. Babai and P. Frankl, *Linear algebra methods in combinatorics with applications to geometry and computer science*, manuscript, Dept. Comp. Sci., University of Chicago, 1992.

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

[6] B. Barak, A. Rao, R. Shaltiel and A. Wigderson, 2-source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl-Wilson construction, *Proc. 38th annual ACM symposium on Theory of Computing*, ACM (2006), 671–680. 2006.

[7] I. F. Blake, Permutation codes for discrete channels, *IEEE Trans. Inf. Theory* **20**(1) (1974), 138–140.

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

[9] P. Erdős, Some Remarks on the Theory of Graphs, *Bull. Amer. Math. Soc.* **53** (1947), 292–294.

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

[11] P. Gopalan, Constructing Ramsey Graphs from Boolean Function Representations, *Elect. Coll. Comput. Compl.*, Report No. 143, (2005).

[12] V. Grolmusz, Low Rank Co-Diagonal Matrices and Ramsey Graphs, *Electr. J. Combin.* 7 (2000), No. 1., R15.

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

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

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

[16] D. K. Ray-Chaudhuri and R. M. Wilson, On t-designs, *Osaka J. Math.* **12** (3) (1975), 737–744.

(Received 8 Apr 2015; revised 8 Oct 2015)