AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **77(2)** (2020), Pages 180–183

Difference sets and power residues

Gábor Hegedűs

Óbuda University
Bécsi út 96/B, Budapest, H-1037
Hungary
hegedus.gabor@nik.uni-obuda.hu

Abstract

Let $q \geq 3$ be a fixed prime power and $n \geq 1$ be an integer. Let $K \subseteq \mathbb{F}_q$ denote a fixed subset with $0 \in K$. Let $A \subseteq (\mathbb{F}_q)^n$ be an arbitrary subset such that $\{\mathbf{a}-\mathbf{b}: \ \mathbf{a},\mathbf{b} \in A, \mathbf{a} \neq \mathbf{b}\} \cap K^n = \emptyset$. We prove the exponential upper bound $|A| \leq (q-|K|+1)^n$. We use the linear algebra bound method in our proof.

1 Introduction

Let p denote a prime with $p \equiv 1 \pmod 4$. The Paley graph of order p is a graph $G(p)$ on p vertices (here we associate each vertex with an element of $\mathbb{F}_p$), where (i,j) is an edge if $i-j$ is a quadratic residue modulo p. Let $\omega(p)$ denote the clique number of the Paley graph of order p. It is a challenging open problem to determine $\omega(p)$.

Until now the best known upper bound is $\omega(p) \leq \sqrt{p}-1$ for infinitely many primes p (see [2] Theorem 2.1).

It is well-known that the Paley graph is a self-complementary graph; hence $\alpha(G(p)) = \omega(p)$. Here we denote by $\alpha(G)$ the independence number of the graph G.

We can consider the following reformulation of this problem: Let $Q(2)$ denote the set of quadratic residues in $\mathbb{F}_p$. How large can a set $A \subseteq \mathbb{F}_p$ be, given that

$$\{a-b: \ a,b \in A, a \neq b\} \subseteq \mathbb{F}_p \setminus Q(2)\,?$$

We investigate here the following generalization of this problem to elementary p-groups. Let $p \geq 3$ be a prime, $k \geq 2$ be a fixed integer and let $Q(k)$ denote the set of kth power residues modulo p (i.e. $Q(k) = \{b \in \mathbb{F}_p : \text{ there exists } x \in \mathbb{F}_p \text{ with } x^k \equiv b \pmod p\}$. Clearly $0 \in Q(k)$. Let $n \geq 1$ be a fixed integer. How large can a set $A \subseteq (\mathbb{F}_p)^n$ be given that

$$\{\mathbf{a}-\mathbf{b}: \ \mathbf{a},\mathbf{b} \in A, \mathbf{a} \neq \mathbf{b}\} \subseteq (\mathbb{F}_p)^n \setminus (Q(k))^n?$$

Matolcsi and Ruzsa investigated the following version of this question in [3]:

Let G denote a finite abelian group and let $B \subseteq G$ be a fixed standard set (i.e. $B=-B$ and $0 \in B$). Consider the number

$$\Delta(B) := \max\{|A|: \ A \subseteq G, (A-A) \cap B = \{0\}\}.$$

ISSN: 2202-3518

How large can $\Delta(B)$ be for a fixed symmetric set?

We state here our main results.

Theorem 1.1 *Let $q \geq 3$ be a fixed prime power and let $n \geq 1$ be a fixed integer. Let $K \subseteq \mathbb{F}_q$ be a fixed subset with $0 \in K$. Define $t := |K|$. Suppose that $A \subseteq (\mathbb{F}_q)^n$ is a subset such that*

$$|A| > (q-t+1)^n.$$

Then there exist $\mathbf{a}_1, \mathbf{a}_2 \in A$, $\mathbf{a}_1 \neq \mathbf{a}_2$, such that $\mathbf{a}_1 - \mathbf{a}_2 \in K^n$.

Remark. We think the bound $(q-t+1)^n$ is not optimal in general. The only obvious case, when our bound is sharp, is the following: Let $K := \mathbb{F}_q$. Then $t = q$ and clearly if $A \subseteq (\mathbb{F}_q)^n$ is an arbitrary subset with $|A| > 1$, then there exist $\mathbf{a}_1, \mathbf{a}_2 \in A$, $\mathbf{a}_1 \neq \mathbf{a}_2$ such that $\mathbf{a}_1 - \mathbf{a}_2 \in K^n = (\mathbb{F}_q)^n$.

On the other hand let $n = 1$, q be a prime and consider the subset $K := \{0, 1\}$. Then it is easy to verify that if $A \subseteq \mathbb{F}_q$ is an arbitrary subset with $|A| > \lceil \frac{q}{2} \rceil$, then there exist $a_1, a_2 \in A$, $a_1 \neq a_2$, such that $a_1 - a_2 \in K = \{0, 1\}$.

Our proof technique is the usual linear algebra bound method (see [1] Chapter 2). Finally we point out an important special case of Theorem 1.1.

Corollary 1.2 *Let $q \geq 3$ be a prime, $k \geq 2$ be a fixed integer and let $Q(k) \subseteq \mathbb{F}_q$ denote the set of kth power residues modulo q. Let $n \geq 1$ be a fixed integer. Define $d := gcd(k, q-1)$. Suppose that $A \subseteq (\mathbb{F}_q)^n$ is a subset such that*

$$|A| > \Big(\frac{(q-1)(d-1)}{d} + 1\Big)^n. \tag{1}$$

Then there exist $\mathbf{a}_1, \mathbf{a}_2 \in A$, $\mathbf{a}_1 \neq \mathbf{a}_2$, such that $\mathbf{a}_1 - \mathbf{a}_2 \in (Q(k))^n$.

2 Proof

We can prove our main result using the linear algebra bound method and the Determinant Criterion (see [1] Proposition 2.7). We recall here for the reader's convenience the Determinant Criterion.

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

Proof. We use an indirect argument. Suppose that $B = (f_i(\mathbf{v}_j))_{i,j=1}^m$ is a non-singular matrix, but there exists a *nontrivial* linear combination $\sum_{i=1}^m \lambda_i f_i$ between the functions f_i. If we substitute $\mathbf{v}_j$ for each j, then we obtain a nontrivial linear combination between the rows of B (with the same coefficients λ_i). This contradicts the non-singularity of B. $\square$

Proof of Theorem 1.1:

Indirectly, suppose that there exists a subset $A \subseteq (\mathbb{F}_q)^n$ such that

$$|A| > (q-t+1)^n$$

and

$$\{\mathbf{a}-\mathbf{b} :\ \mathbf{a},\mathbf{b} \in A, \mathbf{a} \neq \mathbf{b}\} \subseteq (\mathbb{F}_q)^n \setminus K^n. \tag{2}$$

Define $N := \mathbb{F}_q \setminus K$. Then $|N| = q-t$.

Consider the polynomial

$$Q(x_1,\ldots,x_n) := \prod_{1\le i\le n} \prod_{\alpha\in N} (x_i - \alpha) \in \mathbb{F}_q[x_1,\ldots,x_n].$$

Then clearly

$$\deg(Q) = n|N| = n(q-t).$$

If we expand

$$Q = \sum_{\alpha\in\mathbb{N}^n, c_\alpha\neq 0} c_\alpha x^\alpha,$$

as a linear combination of monomials x^α (here x^α denotes the monomial $x_1^{\alpha_1}\ldots x_n^{\alpha_n}$, where $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$), then it follows from the definition of Q that $0 \le \alpha_i \le |N| = q-t$ for each i.

On the other hand $Q(\mathbf{0}) = \prod_{1\le i\le n}\prod_{\alpha\in N}(-\alpha) \neq 0$, because $0 \notin N$. But it follows from the inclusion (2) that $Q(\mathbf{a}_1 - \mathbf{a}_2) = 0$ for each $\mathbf{a}_1,\mathbf{a}_2 \in A$, $\mathbf{a}_1 \neq \mathbf{a}_2$: namely if $\mathbf{a}_1,\mathbf{a}_2 \in A$, $\mathbf{a}_1 \neq \mathbf{a}_2$, then it follows from the inclusion (2) that $\mathbf{a}_1 - \mathbf{a}_2 \in (\mathbb{F}_q)^n \setminus K^n$ and consequently there exists an index $1 \le i \le n$ such that $(\mathbf{a}_1 - \mathbf{a}_2)_i \notin K$. Hence $(\mathbf{a}_1 - \mathbf{a}_2)_i \in N$ and the definition of Q implies that $Q(\mathbf{a}_1 - \mathbf{a}_2) = 0$.

Consider the polynomials

$$P_{\mathbf{a}}(\mathbf{x}) := Q(\mathbf{a} - \mathbf{x}) \in \mathbb{F}_q[\mathbf{x}]$$

for each $\mathbf{a} \in A$. Then it follows from Proposition 2.1 that $\{P_{\mathbf{a}} :\ \mathbf{a} \in A\}$ are linearly independent polynomials. Namely, the matrix $B := (P_{\mathbf{a}}(\mathbf{b}))_{\mathbf{a},\mathbf{b}\in A}$ is a diagonal matrix, where each diagonal entry is nonzero.

On the other hand, if we expand $P_{\mathbf{a}}$ as a linear combination of monomials, then all monomials appearing in this linear combination are contained in the set of monomials

$$\{x_1^{\alpha_1}\ldots x_n^{\alpha_n} :\ 0 \le \alpha_i \le |N| \text{ for each } i\}.$$

Consequently

$$|A| \le (|N|+1)^n = (q-t+1)^n,$$

a contradiction. $\square$

References

[1] L. Babai and P. Frankl, *Linear algebra methods in combinatorics*, University of Chicago, preprint September 1992.

[2] C. Bachoc, I. Z. Ruzsa and M. Matolcsi, Squares and difference sets in finite fields, *Integers: Electr. J. Combin. Number Theory* **13** (2013), 5pp.

[3] M. Matolcsi and I. Z. Ruzsa, Difference sets and positive exponential sums I. General properties, *J. Fourier Anal. and Appl.* **20(1)** (2014), 17–41.

(Received 14 Mar 2019; revised 10 Mar 2020)