Mathematica Slovaca

Angelina Y. M. Chin

Maximal sum-free sets and block designs

Mathematica Slovaca, Vol. 51 (2001), No. 3, 295--299

Persistent URL: http://dml.cz/dmlcz/136809

Math. Slovaca, **51** (2001), No. 3, 295–299

Mathematica
Slovaca

MAXIMAL SUM-FREE SETS AND BLOCK DESIGNS

Angelina Y. M. Chin

(*Communicated by Pavol Zlatoš*)

ABSTRACT. Let G be a finite additive group and S a non-empty subset of G. S is said to be a *sum-free* set of G if $(S+S) \cap S = \emptyset$. If S is a sum-free set of G and $|S'| \leq |S|$ for every other sum-free set S' of G, then S is said to be a *maximal* sum-free set of G. In this paper it is shown that if G is the cyclic group C_{p^n} where p is an odd prime congruent to 2 modulo 3 and $n \geq 1$, the maximal sum-free sets of G form a block design.

1. Introduction

Let G be a finite additive group and S a non-empty subset of G. We say that S is a *sum-free* set of G if $(S+S) \cap S = \emptyset$. If S is a sum-free set of G and $|S'| \leq |S|$ for every other sum-free set S' of G, then S is said to be a *maximal* sum-free set of G. For a given group G, we shall denote by $\lambda(G)$ the cardinality of a maximal sum-free set of G.

We say that S is in *arithmetic progression* with *difference* d if $S = \{a,\ a+d,\ a+2d,\ \dots,\ a+kd\}$ for some $a, d \in G$ and some integer $k > 0$.

Let V be a set with v elements. A collection $\{B_1, \dots, B_b\}$ of subsets of V is called a *block design* if each of the subsets B_i has k elements and each element $x \in V$ is in r of the subsets B_i, $1 \leq i \leq b$. The b subsets $B_1, \dots, B_b$ of V are called *blocks* and the number r is called the *replication number* of the design. If a block design has parameters v, b, r and k, then we say that it is a (v,b,r,k)-design. In this paper we show that if G is the cyclic group C_{p^n} where p is an odd prime congruent to 2 modulo 3 and $n \geq 1$, the maximal sum-free sets of G form a block design. We first look at an elementary property of sum-free sets in Section 2. The case where $p \equiv 2 \pmod 3$ will be considered in Section 3.

2000 Mathematics Subject Classification: Primary 20F99, 20K99, 05B05.
Key words: sum-free, block design.

2. An elementary property of sum-free sets

Let G be the cyclic group C_{p^n} of order p^n where p is a prime and $n \geq 1$. Let $S = \{a_1, \ldots, a_m\}$ be a sum-free set of G. If $S' = \{ka_1, \ldots, ka_m\}$ where k is a positive integer such that $k \not\equiv 0 \pmod{p}$, then S' is called the *kth product set* of S and we write $S' = kS$. It is clear that $|S'| = |S|$ if S' is the kth product set of S for some positive integer k. The proof of the following is straightforward and shall be omitted.

PROPOSITION 1. *Let G be the cyclic group C_{p^n} of order p^n where p is a prime and $n \geq 1$. If S is a sum-free set of G, so is its kth product set, where k is a positive integer relatively prime to p.*

3. The case $p \equiv 2 \pmod 3$

PROPOSITION 2. *Let G be the cyclic group C_{p^n} of order p^n where $p = 3k+2$ is an odd prime and $n \geq 1$. Then*

$$S = \{(1+3j) + pr : \ j = 0, 1, \ldots, k; \ r = 0, 1, \ldots, p^{n-1} - 1\}$$

is a maximal sum-free set of G.

Proof. Suppose that there exist $j_1, j_2 \in \{0, 1, \ldots, k\}$ and $r_1, r_2 \in \{0, 1, \ldots \ldots, p^{n-1} - 1\}$ such that

$$\big((1+3j_1) + pr_1\big) + \big((1+3j_2) + pr_2\big) \equiv \big((1+3j) + pr\big) \pmod{p^n}$$

for some $j \in \{0, 1, \ldots, k\}$ and $r \in \{0, 1, \ldots, p^{n-1} - 1\}$. Then

$$2 + 3(j_1 + j_2) + p(r_1 + r_2) \equiv (1 + 3j) + pr \pmod{p^n}.$$

It follows that $1 + 3(j_1 + j_2 - j) + p(r_1 + r_2 - r) \equiv 0 \pmod{p^n}$. Note that (by taking ordinary addition, that is, not the "modulo addition") we have

$$\begin{aligned} \max\{1 + 3(j_1 + j_2 - j) + p(r_1 + r_2 - r)\} &= 1 + 3(2k) + p(2p^{n-1} - 2) \\ &= 2p^n - 3 < 2p^n \end{aligned}$$

and

$$\begin{aligned} \min\{1 + 3(j_1 + j_2 - j) + p(r_1 + r_2 - r)\} &= 1 - 3k + p[-(p^{n-1} - 1)] \\ &= -p^n + 3 > -p^n. \end{aligned}$$

Therefore

$$1 + 3(j_1 + j_2 - j) + p(r_1 + r_2 - r) = 0 \tag{1}$$

or

$$1 + 3(j_1 + j_2 - j) + p(r_1 + r_2 - r) = p^n . \qquad (2)$$

If (1) occurred, then $1 + 3(j_1 + j_2 - j)$ would be divisible by p. But this is not possible since $p = 3k+2$ and $j_1, j_2, j \in \{0, 1, \dots, k\}$. Similarly, (2) cannot occur since $1 + 3(j_1 + j_2 - j)$ would be divisible by p otherwise. We thus have that $\mathcal{S}$ is a sum-free set. Since $|\mathcal{S}| = p^{n-1}(k+1) = p^{n-1}(\frac{p+1}{3})$, it follows from [2; Theorem 2] or [4; Theorem 3] that $\mathcal{S}$ is a maximal sum-free set of G. □

By [4; Theorem 5] we have that if $\mathcal{S}$ is a maximal sum-free set of the cyclic group C_{p^n} where $p \equiv 2 \pmod 3$ is an odd prime, then $\mathcal{S}$ is a union of cosets of H where H is the subgroup of C_{p^n} of order p^{n-1}. Since $\lambda(C_{p^n}) = p^{n-1}(\frac{p+1}{3})$ and $|H| = p^{n-1}$, it is clear that

$$\mathcal{S} = (H + g_1) \cup (H + g_2) \cup \cdots \cup (H + g_{\frac{p+1}{3}})$$

for some $g_1, \dots, g_{\frac{p+1}{3}} \in C_{p^n}$. Clearly $\{g_1, \dots, g_{\frac{p+1}{3}}\}$ must be sum-free. Such a sum-free set can be obtained by considering the maximal sum-free sets of C_p. By [3; Theorem 2], C_p has $\frac{p-1}{2}$ maximal sum-free sets. Since H is unique, C_{p^n} also has $\frac{p-1}{2}$ maximal sum-free sets.

PROPOSITION 3. *Let $p = 3k + 2$ be an odd prime. Then the sets*

$$\mathcal{S}_t = \{3j + t : \ j = 0, t, 2t, \dots, kt\}, \qquad t = 1, \dots, \frac{p-1}{2},$$

are the maximal sum-free sets of C_p.

Proof. By Proposition 2 we know that $\mathcal{S}_1$ is a maximal sum-free set of C_p. Note that $\mathcal{S}_t = t\mathcal{S}_1$; hence it follows from Proposition 1 that $\mathcal{S}_t$, $t = 2, \dots, \frac{p-1}{2}$, are also maximal sum-free sets. It is clear that each $\mathcal{S}_t$ is in arithmetic progression with difference $3t$. Note that if $\mathcal{S}_{t_1} = \mathcal{S}_{t_2}$ for some $t_1, t_2 \in \{1, \dots, \frac{p-1}{2}\}$, then $t_1 \equiv t_2 + 3t_2 i \pmod p$ and $t_2 \equiv t_1 + 3t_1 j \pmod p$ for some $i, j \in \{0, 1, \dots, k\}$. It follows that $t_1 \equiv (1 + 3j + 3i + 9ij)t_1 \pmod p$, that is, $3(j + i + 3ij) \equiv 0 \pmod p$. But since p is of the form $3k + 2$, this is not possible unless $i = j = 0$, that is, $t_1 = t_2$. Therefore, $\mathcal{S}_1, \dots, \mathcal{S}_{\frac{p-1}{2}}$ must all be different and are the maximal sum-free sets of C_p. (One can easily check that $(\frac{p+1}{2} + j)\mathcal{S}_1 = (\frac{p-1}{2} - j)\mathcal{S}_1$ for $j = 0, 1, \dots, \frac{p-3}{2}$.) □

For ease of exposition, we shall refer to the element $3j + t$ of $\mathcal{S}_t$ (where $\mathcal{S}_t$ is as defined in Proposition 3) as the element in the $(\frac{j}{t} + 1)$st-tuple of $\mathcal{S}_t$.

PROPOSITION 4. *Let $p = 3k + 2$ be an odd prime. Then each i, $i = 1, \dots$ $\dots, p - 1$, appears in the same number of maximal sum-free sets of C_p. This number is given by $\frac{p+1}{6}$.*

Proof. Note that

$$\big(3(i-1)t+t\big)+\big(3(k-i+1)t+t\big)=(3k+2)t=pt\equiv 0 \pmod p$$

for $i=1,\dots,k+1$. Therefore each of the sets $\mathcal{S}_1,\mathcal{S}_2,\dots,\mathcal{S}_{\frac{p-1}{2}}$ is an inverse of itself with the inverse of the element in the ith tuple being the element in the $(k-i+2)$th tuple ($i=1,\dots,k+1$). Now consider $3j+1$ for some fixed $j\in\{0,1,\dots,k\}$. We wish to show that

$$t(3j+1)\not\equiv -t'(3j+1) \pmod p$$

for any $t,t'\in\{1,\dots,\frac{p-1}{2}\}$. Suppose on the contrary that

$$t(3j+1)\equiv -t'(3j+1) \pmod p$$

for some $t,t'\in\{1,\dots,\frac{p-1}{2}\}$. Then

$$(3j+1)(t+t')\equiv 0 \pmod p.$$

Since p is a prime number, so $p\mid(3j+1)$ or $p\mid(t+t')$. But $\max\{3j+1\}=p-1<p$ and $\max\{t+t'\}=p-1<p$. We thus have a contradiction and therefore $t(3j+1)\not\equiv -t'(3j+1) \pmod p$ for any $t,t'\in\{1,\dots,\frac{p-1}{2}\}$. It follows that

$$\Big\{(3j+1),2(3j+1),\dots,(\tfrac{p-1}{2})(3j+1),\\ -(3j+1),-2(3j+1),\dots,-(\tfrac{p-1}{2})(3j+1)\Big\}$$

must be equal to $\mathcal{C}_p\setminus\{0\}$. That is, the collection of all the elements in the $(j+1)$st and $(k-j+1)$st tuples of $\mathcal{S}_1,\mathcal{S}_2,\dots,\mathcal{S}_{\frac{p-1}{2}}$ is just $\mathcal{C}_p\setminus\{0\}$. Therefore each i, $i\neq 0$, appears in the same number of maximal sum-free sets. This number is clearly given by $\frac{1}{2}\lambda(\mathcal{C}_p)=\frac{p+1}{6}$. □

PROPOSITION 5. *Let G be the cyclic group $\mathcal{C}_{p^n}$ where $p\equiv 2 \pmod 3$ is an odd prime and $n\geq 1$. Then each i, $i=1,\dots,p^n-1$, $i\not\equiv 0 \pmod p$, appears in the same number of maximal sum-free sets of G. This number is given by $\frac{p+1}{6}$.*

Proof. Let $\mathcal{S}$ be a maximal sum-free set of G. Then

$$\mathcal{S}=(H+g_1)\cup\dots\cup(H+g_{\frac{p+1}{3}})$$

where $H=\langle p\rangle$ is the subgroup of G of order p^{n-1} and $\{g_1,\dots,g_{\frac{p+1}{3}}\}=\mathcal{S}_t$ for some $t=1,\dots,\frac{p-1}{2}$ ($\mathcal{S}_t$ is as defined in Proposition 3). Since $g_j\neq 0$ for any $j=1,\dots,\frac{p+1}{3}$, so the elements of H will never appear in any of the maximal sum-free sets of G. By Proposition 4 and by symmetry, we have that each i, $i=1,\dots,p^n-1$, $i\not\equiv 0 \pmod p$, will appear in $\frac{p+1}{6}$ of the maximal sum-free sets of G. □

THEOREM 6. *Let G be the cyclic group C_{p^n} where $p \equiv 2 \pmod 3$ is an odd prime and $n \geq 1$. Then the maximal sum-free sets of G form a $\left(p^n - p^{n-1}, \frac{p-1}{2}, \frac{p+1}{6}, p^{n-1}\left(\frac{p+1}{3}\right)\right)$-design.*

Proof. First we note by Proposition 2 that the number k' of elements in each maximal sum-free set of G is $p^{n-1}\left(\frac{p+1}{3}\right)$. We also have from the discussion preceding Proposition 3 that the number b of maximal sum-free sets of G is $\frac{p-1}{2}$. From the proof of Proposition 5 we know that none of the elements $p, 2p, \dots, (p^{n-1}-1)p$ will appear in the maximal sum-free sets of G. Hence, the number v of distinct elements of G appearing in the maximal sum-free sets of G is $p^n - p^{n-1}$. By Proposition 5 we also know that each of the integers $i \in G$, $i \not\equiv 0 \pmod p$, appears in exactly $\frac{p+1}{6}$ of the maximal sum-free sets of G. We thus have that the maximal sum-free sets of G form the asserted block design. □

4. Other cases

We remark here that if p is a prime not congruent to 2 modulo 3 and $n \geq 1$, the maximal sum-free sets of the cyclic group C_{p^n} also form a block design. For example, in the case where $p = 3$, the maximal sum-free sets of C_{3^n} where $n \geq 1$ form a symmetric $(3^n - 1, 3^n - 1, 3^{n-1}, 3^{n-1})$-design. The proof for this and for the case where $p \equiv 1 \pmod 3$ use different arguments from the ones in this paper and are given in [1].

REFERENCES

[1] CHIN, A. Y. M.: *On maximal sum-free sets of certain cyclic groups and block designs* (Submitted).

[2] DIANANDA, P. H.—YAP, H. P.: *Maximal sum-free sets of elements of finite groups*, Proc. Japan Acad. **45** (1969), 1–5.

[3] YAP, H. P.: *The number of maximal sum-free sets in C_p*, Nanta Math. **2** (1968), 68–71.

[4] YAP, H. P.: *Maximal sum-free sets of group elements*, J. London Math. Soc. **44** (1969), 131–136.

Received August 20, 1999
Revised February 16, 2000

Institute of Math. Sciences
Faculty of Science
University of Malaya
50603 Kuala Lumpur
MALAYSIA

E-mail: acym@mnt.math.um.edu.my