Canad. Math. Bull. Vol. 14 (1), 1971

MAXIMAL SUM-FREE SETS IN ELEMENTARY ABELIAN p-GROUPS

BY
A. H. RHEMTULLA[1] AND ANNE PENFOLD STREET[2]

1. **Introduction.** Given an additive group G and nonempty subsets S, T of G, let $S+T$ denote the set $\{s+t \mid s \in S, t \in T\}$, $\bar{S}$ the complement of S in G and $|S|$ the cardinality of S. We call S a *sum-free set* in G if $(S+S) \subseteq \bar{S}$. If, in addition, $|S| \geq |T|$ for every sum-free set T in G, then we call S a *maximal sum-free set* in G. We denote by $\lambda(G)$ the cardinality of a maximal sum-free set in G.

In a previous paper [3], we showed that if G is an elementary abelian p-group, where $p=3k+1$ and $|G|=p^n$, then $\lambda(G)=kp^{n-1}$. We also showed that if $G=Z_p$, the group of order p, then any maximal sum-free set S of G can be mapped, under some automorphism of G, to one of the following sets:

$$A = \{k, k+2, \ldots, 2k-1, 2k+1\};$$

$$B = \{k, \ldots, 2k-1\};$$

$$C = \{k+1, \ldots, 2k\}.$$

Maximal sum-free sets in elementary abelian q-groups, where q is prime, $q \equiv 2(3)$, have been characterized by Diananda and Yap [1]. Here we characterize the maximal sum-free sets S in an elementary abelian p-group G. if $|G| = p^n$, then exactly one of the $(p^n-1)/(p-1)$ maximal subgroups of G does not intersect S and each of the remaining maximal subgroups intersects S in a set of order kp^{n-2}, which by [3] is the largest possible intersection since S is sum-free. More precisely, we prove the following:

THEOREM. *Let G be an elementary abelian p-group, $|G|=p^n$, $p=3k+1$, $p>7$ and let S be a maximal sum-free set in G. If G is denoted by*

$$G = \{(i_1, \ldots, i_n) \mid i_j \in Z_p, j = 1, \ldots, n\}$$

then, under some automorphism of G, S can be mapped to one of the following $(2n+1)$ sets:

$$A_n^n = \{(i_1, \ldots, i_n) \mid i_n \in A\};$$

$$A_{n-r}^n = \{(i_1, \ldots, i_n) \mid \text{not all } i_1, \ldots, i_r = 0, i_n \in C\}$$
$$\cup \{(0, \ldots, 0, i_{r+1}, \ldots, i_n) \mid i_n \in A\} \quad \text{for } r = 1, \ldots, n-1;$$

Received by the editors May 20, 1970.

(1) The preparation of this paper was partially supported by the National Research Council of Canada Grant No. A-5299.

(2) Izaac Walton Killam Post-Doctoral Fellow.

https://doi.org/10.4153/CMB-1971-014-2 Published online by Cambridge University Press

$$B_n^n = \{(i_1, \ldots, i_n) \mid i_n \in B\};$$

$$\begin{aligned} B_{n-r}^n = \{(i_1, \ldots, i_n) \mid \text{not all } i_1, \ldots, i_r = 0, i_n \in C\} \\ \cup \{(0, \ldots, 0, i_{r+1}, \ldots, i_n) \mid i_n \in B\} \quad \text{for } r = 1, \ldots, n-1; \end{aligned}$$

$$C^n = \{(i_1, \ldots, i_n) \mid i_n \in C\} = A_0^n = B_0^n.$$

Note. If $p=7$ then $k=2$ and sets of type A do not occur. A similar proof shows that, in an elementary abelian 7-group of order 7^n, there are $(n+1)$ nonisomorphic maximal sum-free sets, namely B_{n-r}^n, $r = 0, 1, \ldots, n-1$ and C^n.

DEFINITION. Let G be a group, H a subgroup of G and S a maximal sum-free set in G. Then S is said to *avoid* H if and only if $S \cap H = \phi$ and to *cover* H if and only if $S \cap H$ is a maximal sum-free set in H.

In this terminology, any maximal sum-free set S of an elementary abelian group G avoids precisely one maximal subgroup of G and covers all the rest.

2. **Proofs.** We first establish the following results which we need in proving the theorem.

LEMMA 1. *Let $S \subseteq Z_p$ be a maximal sum-free set isomorphic to C and suppose that*

$$S \subseteq \left\{\frac{k}{2}+1, \ldots, \frac{5k}{2}\right\}.$$

Then either

$$S = C \quad \text{or} \quad S = \left\{\frac{k}{2}+1, \ldots, k, 2k+1, \ldots, \frac{5k}{2}\right\} = C'.$$

Proof. We may assume without loss of generality that $S = \{x, x+d, \ldots, x+(k-1)\,d\}$ for some $x \in Z_p$, $d \leq 3k/2$. Since $S = -S$, we have

$$2x+(k-1)\,d = 0$$

and hence

$$x = (k+1)d \quad \text{or equivalently} \quad 3x = 2d. \tag{1}$$

We have two cases to consider: (a) If

$$\frac{k}{2}+1 \leq x < x+d < \cdots < x+(k-1)d \leq \frac{5k}{2}, \tag{2}$$

then $(k-1)d \leq 2k-1$ and $d=1$ or 2. If $d=2$, then by (1), $x=2k+2$ and S is not contained in the given set; if $d=1$, then $S=C$.

(b) If (2) is not satisfied then for some l, $1 \leq l \leq k-1$, we have

$$x+ld \leq \frac{5k}{2} \quad \text{and} \quad \frac{k}{2}+1 \leq x+(l+1)d$$

so that

$$k+2 \leq d \leq \frac{3k}{2}. \tag{3}$$

https://doi.org/10.4153/CMB-1971-014-2 Published online by Cambridge University Press

If, for some $s \in S$, $k+1 \leq s \leq 3k/2$ then, by (3),

$$s-d \in \left\{\frac{5k}{2}+2, \ldots, 3k, 0, 1, \ldots, \frac{k}{2}-2\right\};$$

hence $s-d \notin S$ and $s=x$, the first element of the arithmetic progression. Now $k+1 \leq x \leq 3k/2$ implies that $2 \leq 3x \leq 3k/2-1$ but, by (3), $2k+4 \leq 2d \leq 3k$. Hence $3x \neq 2d$, contradicting (1). Therefore $S \cap C = \phi$ and $S = C'$.

LEMMA 2. *Let* $\phi \neq X \subseteq Z_p$ and $X+X \subseteq X$. *Then either* $X=\{0\}$ *or* $X=Z_p$.

Proof. By the Cauchy–Davenport theorem [2],

$$|X+X| \geq \min(p, 2|X|-1).$$

If $p \leq 2|X|-1$, then $X+X=Z_p$ and $X=Z_p$. If $2|X|-1<p$, then $2|X|-1 \leq |X|$, so that $|X| \leq 1$. Since $X \neq \phi$, we have $|X|=1$, $X+X=X$ and $X=\{0\}$.

Proof of the theorem. A routine computation shows that A^n_{n-r}, B^n_{n-r} and C^n are maximal sum-free sets. To prove no other maximal sum-free sets exist, we consider first the case when $|G|=p^2$ and then generalize.

(1) Let $G=\langle x_1, x_2 \mid px_i=0, i=1,2; x_1+x_2=x_2+x_1\rangle$ and let $X_i=\langle x_i\rangle$. Since $|G|=p^2$, $|S|=kp$ and hence S covers at least $(2k+2)$ of the $(p+1)$ subgroups of order p. We may assume without loss of generality that $|X_2 \cap S|=k$. We denote by S_i the subset of X_2 such that $S_i+ix_1=S \cap (X_2+ix_1)$ for $i=0,\ldots,p-1$.

We make repeated use of the sum-freeness of S in the form

$$(S_i+S_j) \cap S_{i+j} = \phi \tag{4}$$

and in particular

$$(S_0+S_i) \cap S_i = \phi. \tag{5}$$

Since $|S_0|=k$, we find from (5) and the Cauchy–Davenport theorem that $|S_i| \leq k+1$. By Vosper's theorem [2], if S_0 and S_i are not in arithmetic progression with the same common difference, then $|S_i| \leq k$; since $|S|=kp$, we must have $|S_i|=k$ for all i. If S_0 and S_i are in arithmetic progression with the same common difference and if $|S_i|=k+1$ for some i then, since S is sum-free, S_0 is isomorphic to C.

(a) Suppose that at least one proper subgroup of G intersects S in a set isomorphic to A. Without loss of generality we assume this subgroup to be X_2 and choose its generator x_2 so that $S_0=A$. By (5),

$$S_i \subseteq \{\alpha_i, \ldots, \alpha_i+k-1, \alpha_i+k+1\}$$

for some $\alpha_i \in X_2$ and not both of α_i+1, $\alpha_i+k+1 \in S_i$. Since $|S_i|=k$ for all i, we know that for each i, $S_i=\alpha_i-k+A$ or $S_i=\alpha_i-k-1+C$.

(i) If, for some i, $S_i=\alpha_i-k+A$, then we choose x_1, the other generator of G,

https://doi.org/10.4153/CMB-1971-014-2 Published online by Cambridge University Press

so that $S_1=A$. Then $S_1+S_1=\bar{A}$ and, by (4), $S_2=A$. By induction, $S_i=A$ for all i and $S=A_2^2$.

(ii) If, for all i, $S_i=\alpha_i-k-1+C$, then we choose x_1 so that $S_1=C$. Note that S_i and consequently (S_i+S_j) are in arithmetic progression with common difference 1 for all i, j. From this fact and (4), we have:

(6) $$\alpha_i+\alpha_{-i} = 2k+2 \quad \text{and in particular} \quad \alpha_{-1} = k+1;$$

(7) $$\alpha_{(p+1)/2} = k+1 \quad \text{or} \quad -\frac{k}{2} \quad \text{or} \quad -\frac{k}{2}+1;$$

(8) $$\alpha_{i+1} = \alpha_i-1 \quad \text{or} \quad \alpha_i \quad \text{or} \quad \alpha_i+1.$$

Suppose that $\alpha_{(p+1)/2}=-k/2$ and consider the movement of α_i as i runs from $(p+1)/2$ to $p-1$. By (6), in these $(3k/2-1)$ steps, α_i must either decrease from $(5k/2+1)$ by $3k/2$ or increase from $(5k/2+1)$ by $(3k/2+1)$. But by (8), α_i can increase or decrease by at most 1 at each step. Hence $\alpha_{(p+1)/2}\neq -k/2$. A similar argument shows that $\alpha_{(p+1)/2}\neq -k/2+1$ and hence, by (6) and (7),

(9) $$\alpha_{(p+1)/2} = \alpha_{(p-1)/2} = k+1.$$

By (6), (8), and (9), α_i differs from α_0 by at most $(3k-2)/4$; hence if $\alpha_i<k+1$, then $k \in S_i$.

Now let $X=\{i \in \langle x_1\rangle \mid (i, k) \in S\}=\{i \in \langle x_1\rangle \mid \alpha_i<k+1\}$. By (4), if $i, j \in X$, then $i+j \in X$. Hence $X+X \subseteq X$. But $0 \in X$, $1 \notin X$, so by Lemma 2, $X=\{0\}$. A similar argument shows that only S_0 contains an element greater than $2k$. Hence $S_i=C$ for all $i\neq 0$ and $S=A_1^2$.

(b) Suppose that no proper subgroup of G intersects S in a set isomorphic to A but that at least one proper subgroup intersects S in a set isomorphic to B. We assume this subgroup to be X_2 and choose x_2 so that $S_0=B$. By (5), $S_i \subseteq \{\alpha_i, \ldots, \alpha_i+k-1\}$ for all i, for some $\alpha_i \in X_2$. Since $|S|=kp$ we have $S=\alpha_i-k+B$ for all i; we choose x_1 so that $S_1=B+1=C$.

By (4), $\alpha_i+\alpha_{-i}=2k$ or $2k+1$ or $2k+2$ and in particular

(10) $$\alpha_{-1} = k-1 \quad \text{or} \quad k \quad \text{or} \quad k+1.$$

Also

(11) $$\alpha_{i+1} = \alpha_i-1 \quad \text{or} \quad \alpha_i \quad \text{or} \quad \alpha_i+1.$$

(i) If $\alpha_{-1}=k-1$, then by (4),

(12) $$\alpha_{i-1} = \alpha_i-3 \quad \text{or} \quad \alpha_i-2 \quad \text{or} \quad \alpha_i-1.$$

By (11) and (12), $\alpha_{i+1}=\alpha_i+1$ for all i. The automorphism of G which maps (i_1, i_2) to (i_1, i_2-i_1) maps S to B_2^2.

(ii) If $\alpha_{-1}=k$, then by (4),

(13) $$\alpha_{i-1} = \alpha_i-2 \quad \text{or} \quad \alpha_i-1 \quad \text{or} \quad \alpha_i.$$

https://doi.org/10.4153/CMB-1971-014-2 Published online by Cambridge University Press

By (11) and (13),

$$\alpha_{i+1} = \alpha_i \quad \text{or} \quad \alpha_i+1 \quad \text{for all } i. \tag{14}$$

Consider the movement of α_i as i runs from 1 to $(p-1)$. In these $(p-2)$ steps, α_i must increase by $(p-1)$, but by (14) α_i may increase by, at most, 1 at each step. Hence $\alpha_{-1} \neq k$.

(iii) If $\alpha_{-1}=k+1$, then a repetition of the argument of (a(ii)) shows that (7), (8), and (9) hold, that if $\alpha_i<k+1$, then $k \in S_i$ and that $k \in S_i$ only if $i=0$. Similarly, if we let $Y=\{i \in \langle x_1\rangle \mid \alpha_i>k+1\}$ then $Y+Y \subseteq Y$, $Y \neq Z_p$, $Y \neq \{0\}$, and by Lemma 2, $Y=\phi$. Hence $S_i=C$ for all $i \neq 0$ and $S=B_1^2$.

(c) Finally, suppose that every subgroup of G covered by S intersects S in a set isomorphic to C.

(i) If there exists a proper subgroup, covered by S and having at least one coset which contains $(k+1)$ elements of S, then we assume this subgroup to be X_2 and choose x_2 so that $S_0=C$. By (5), $S_i \subseteq \{\alpha_i, \ldots, \alpha_i+k\}$ for all i and we choose x_1 so that $S_1=\{k+1, \ldots, 2k+1\}$.

By the proof of Theorem 1(a) [3], S avoids $\langle x_1\rangle$. Hence S must cover every other subgroup of order p in G. But S intersects each such subgroup in a set isomorphic to C, implying that $S=-S$. This, combined with the previous proof in [3], shows that α_i (and similarly the right-hand end-point of S_i) can move by, at most, $k/2$ in either direction. Since $\alpha_1=k+1$ and the right-hand end-point of S_{-1} is $2k$, we have

$$S_i \subseteq \left\{\frac{k}{2}+1, \ldots, \frac{5k}{2}\right\} \quad \text{for all } i.$$

Hence for every subgroup $\langle(\rho, 1)\rangle$, the second coordinates of $\langle(\rho, 1) \cap S\rangle$ belong to $C \cup C'$. Since all these subgroups are covered by S, Lemma 1 shows that, for any given ρ, the second coordinates of the intersection are either C or C'. Let

$$T_j = \{i \in \langle x_1\rangle \mid (i, j) \in S\} = \{i \in \langle x_1\rangle \mid j \in S_i\}.$$

Then $|T_j|=a, j \in C'$ and $|T_j|=b, j \in C$. If $a>0$, $b>0$, then by (4), in particular,

$$T_{k/2+1}+T_{k/2+1} \cap T_{k+2} = \phi.$$

Hence by the Cauchy–Davenport theorem, $2a+b \leq p+1$. Similarly, $2b+a \leq p+1$ so that $a+b \leq 2(p+1)/3$. But $a+b=p$. Hence $a=0$ or $b=0$; we may assume that $a=0$ and for each $\langle(\rho, 1)\rangle$, the second coordinates of its intersection with S form the set C.

This contradicts our statement that $(1, 2k+1) \in S$. Hence every coset of every proper subgroup covered by S contains exactly k elements of S.

(ii) Now let X_2 be any subgroup of order p covered by S and choose its generator

x_2 so that $S_0 = C$. Then $S_i \subseteq \{\alpha_i, \ldots, \alpha_i+k\}$ for all i, for some $\alpha_i \in X_1$ and, since $|S_i| = k$, four types of sets may occur:

$$S_i = \{\alpha_i, \ldots, \alpha_i+k-1\} \in P;$$

$$S_i = \{\alpha_i, \alpha_i+2, \ldots, \alpha_i+k\} \in Q_1;$$

$$S_i = \{\alpha_i, \ldots, \alpha_i+k-2, \alpha_i+k\} \in Q_2;$$

$$S_i = \{\alpha_i, \ldots, \alpha_i+l, \alpha_i+l+2, \ldots, \alpha_i+k\} \in R, \quad 2 \leq l \leq k-2.$$

If a set of type R occurs, choose x_1 so that

$$S_1 = \{k+1, \ldots, k+1+l, k+3+l, \ldots, 2k+1\} \text{ for some } l, \quad 2 \leq l \leq k-2.$$

By (4), we find that $\alpha_2 = k+2$, $\alpha_{i+1} = \alpha_i$ or α_i+1 and $\alpha_{-1} = k$ or $k+1$. Since α_i can never decrease, in the $(p-3)$ steps as i runs from 2 to $(p-1)$, α_i must increase from $(k+2)$ by $(p-2)$ or $(p-1)$. But α_i can increase by, at most, 1 at each step. Hence no set of type R can occur.

If a set of type Q_2 occurs, choose x_1 so that

$$S_1 = \{k+1, \ldots, 2k-1, 2k+1\}.$$

By (4), we find that $\alpha_{-1} = k$ or $k+1$, $\alpha_{(p+1)/2} = k$ or $k+1$ or $-k/2+1$, $\alpha_{i+1} = \alpha_i - 1$ or α_i or α_i+1, and if $\alpha_{i+1} = \alpha_i - 1$ then $\alpha_{i+2} = \alpha_i$. A similar argument to that of (a(ii)) shows that $\alpha_i = k$ or $k+1$ for all i.

Hence S avoids $\langle x_1 \rangle$. Therefore S covers every other proper subgroup and intersects each of them in a set isomorphic to C and contained in $\{k, \ldots, 2k+1\}$. Hence by Lemma 1, every subgroup except $\langle x_1 \rangle$ intersects S in the set C, contradicting our statement that $(1, 2k+1) \in S$. Hence no set of type Q_2 (and similarly Q_1) can occur.

We now know that every coset of X_2 intersects S in a set of type P and we choose x_1 so that $S_1 = C$. By (4), we find that $\alpha_{-1} = k$ or $k+1$ or $k+2$, and

$$\alpha_{i+1} = \alpha_i - 1 \quad \text{or} \quad \alpha_i \quad \text{or} \quad \alpha_i + 1. \tag{15}$$

If $\alpha_{-1} = k$, then by (4) again,

$$\alpha_{i+1} = \alpha_i \quad \text{or} \quad \alpha_i + 1. \tag{16}$$

If $\alpha_{-1} = k+2$, then

$$\alpha_{i+1} = \alpha_i - 1 \quad \text{or} \quad \alpha_i. \tag{17}$$

If $\alpha_{-1} = k$, then by (16), in the $(p-2)$ steps as i runs from 1 to $(p-1)$, α_i must increase by $(p-1)$. But α_i may increase by, at most, 1 at each step. Hence $\alpha_{-1} \neq k$. A similar argument using (17) shows that $\alpha_{-1} \neq k+2$.

Hence $\alpha_{-1} = k+1$, and by (4) we have $\alpha_{(p+1)/2} = -k/2$ or $-k/2+1$ or $k+1$. An argument similar to that of (a(ii)) shows that $\alpha_i = k+1$ and hence $S_i = C$ for all i. Therefore $S = C^2$.

(2) Now let G be an elementary abelian group of order p^n.

(a) We show first that any maximal sum-free set S in G avoids exactly one maximal subgroup of G.

Since by [3], $|S|=kp^{n-1}$, G has at least one subgroup of order p which is covered by S. Let X be any such subgroup and let Y be the subgroup complementing X in G. Then $|Y|=p^{n-1}$ and $Y=\bigcup_{i=1}^{\rho} Y_i$, where Y_i is a subgroup of order p and $\rho=(p^{n-1}-1)/p-1$. Now

$$|S| = kp^{n-1} = \sum_{i=1}^{\rho} |(X+Y_i)\cap S|-(\rho-1)k.$$

But

$$|(X+Y_i)\cap S| \leq kp \quad \text{for all } i = 1,\ldots,\rho$$

and

$$\sum_{i=1}^{\rho} |(X+Y_i)\cap S| = kp^{n-1}+(\rho-1)k = kp\rho.$$

Hence

$$|(X+Y_i)\cap S| = kp \quad \text{for all } i = 1,\ldots,\rho.$$

From the proof of (1), there exists a subgroup Z_i of order p such that $Z_i < X+Y_i$ and S avoids Z_i, for each $i=1,\ldots,\rho$. These ρ subgroups are distinct for if $Z_i=Z_j$, then

$$X+Y_i = X+Z_i = X+Z_j = X+Y_j \quad \text{and} \quad i=j.$$

Hence S avoids ρ of the $(p^n-1)/p-1$ subgroups of order p in G, and since $|S|=kp^{n-1}$, S covers the p^{n-1} remaining subgroups of order p, which we denote by X_i, $i=1,\ldots,p^{n-1}$.

Suppose that for some h, i, j with $1\leq h\leq p^{n-1}$, $1\leq i,j\leq p$, we have $X_h<Z_i+Z_j$. Then we repeat the proof, choosing X_h as our subgroup X which is covered by S, and show that $|(Z_i+Z_j)\cap S|=kp$. But since S avoids both Z_i and Z_j, $|(Z_i+Z_j)\cap S|\leq k(p-1)$. Hence for any $i,j=1,\ldots,\rho$ we have $Z_i+Z_j\subseteq \bigcup_{l=1}^{\rho} Z_l$.

Now $|\bigcup_{l=1}^{\rho} Z_l|=p^{n-1}$ and $\bigcup_{l=1}^{\rho} Z_l$ is a subgroup. For if $z_1, z_2\in\bigcup_{l=1}^{\rho} Z_l$ then either $z_1, z_2\in Z_i$ and $z_1+z_2\in Z_i\subseteq\bigcup_{l=1}^{\rho} Z_l$ or $z_1\in Z_i$, $z_2\in Z_j$ and $z_1+z_2\in Z_i+Z_j \subseteq\bigcup_{l=1}^{\rho} Z_l$. Hence S avoids a maximal subgroup of G.

(b) We now suppose that in elementary abelian p-groups of orders p^{n-1} or less, the maximal sum-free sets have been characterized. By (1) we see that if H, K are subgroups of order p in G, of order p^n, then it is impossible to have $S\cap H=A$ and $S\cap K=B$. Hence two cases arise:

(i) Subgroups of order p intersect S in sets A or C. If no subgroup of order p intersects S in A, then $S=C^n$. If exactly one subgroup of order p intersects S in A, then $S=A_1^n$. If two subgroups of order p intersect S in A, then the subgroup of order p^2 which they generate intersects S in A_2^2 so that altogether p subgroups of order p intersect S in A and $S=A_2^n$. By induction, if the subgroups of order p intersecting S in A generate a subgroup of order p^r, then p^{r-1} subgroups of order p intersect S in A and $S=A_r^n$. In each case, since S avoids a maximal subgroup of

G, S is determined up to automorphism by the order of the subgroup generated by all those subgroups of order p which intersect S in A. Hence $(n+1)$ sets are possible.

(ii) Subgroups of order p intersect S in sets B or C. An argument similar to (i) shows that again $(n+1)$ sets are possible, namely C^n, $B_1^n, \ldots, B_n^n$.

Since C^n occurs in both cases, we have altogether $(2n+1)$ nonisomorphic sets.

References

1. P. H. Diananda and H. P. Yap, *Maximal sum-free sets of elements of finite groups*, Proc. Japan Acad., **45** (1969), 1–5.

2. H. B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Interscience, New York, 1965.

3. A. H. Rhemtulla and A. P. Street, *Maximal sum-free sets in finite abelian groups*, Bull. Austral. Math. Soc., **2** (1970), 289–297.

University of Alberta,
Edmonton, Alberta

https://doi.org/10.4153/CMB-1971-014-2 Published online by Cambridge University Press