BULL. AUSTRAL. MATH. SOC. MOS 0522, (2030, 2025, 2040)
VOL. 2 (1970), 289-297.

Maximal sum-free sets in finite abelian groups

A. H. Rhemtulla and Anne Penfold Street

A subset S of an additive group G is called a maximal sum-free set in G if $(S+S) \cap S = \emptyset$ and $|S| \geq |T|$ for every sum-free set T in G. It is shown that if G is an elementary abelian p-group of order p^n, where $p = 3k \pm 1$, then a maximal sum-free set in G has kp^{n-1} elements. The maximal sum-free sets in Z_p are characterized to within automorphism.

Given an additive group G and non-empty subsets S, T of G, let $S + T$ denote the set $\{s+t;\ s \in S,\ t \in T\}$, $\overline{S}$ the complement of S in G and $|S|$ the cardinality of S. We call S a *sum-free set* in G if $(S+S) \subseteq \overline{S}$. 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.

If G is a finite abelian group, then according to [2], $2|G|/7 \leq \lambda(G) \leq |G|/2$. Both these bounds can be attained since $\lambda(Z_7) = 2$, $\lambda(Z_2) = 1$, where Z_n denotes the cyclic group of order n. Exact values of $\lambda(G)$ were given by Diananda and Yap [1] for $|G|$ divisible by 3 or by at least one prime $q \equiv 2\ (3)$. When every prime divisor of $|G|$ is a prime $p \equiv 1\ (3)$ then, by [1],

$$(1) \qquad |G|(m-1)/3m \leq \lambda(G) \leq (|G|-1)/3\ ,$$

Received 13 February 1970. The preparation of this paper was partly supported by the National Research Council of Canada grant No. A-5299. The second author is Izaac Walton Killam Post-Doctoral Fellow.

where m is the exponent of G. If G is cyclic, $\lambda(G)$ attains its upper bound. It was shown in [1] that $\lambda(G)$ attains its lower bound when G is the direct sum of two cyclic groups of order 7. Here we prove the following:

THEOREM 1. *If G is an elementary abelian p-group, $|G| = p^n$, $p = 3k + 1$, then $\lambda(G) = kp^{n-1}$.*

In [6], Yap characterized all the maximal sum-free sets in Z_p, where p is prime and $p \equiv 2\ (3)$. Here we do the same when $p \equiv 1\ (3)$ in the following:

THEOREM 2. *Let $G = Z_p$ where $p = 3k + 1$ is prime. Then any maximal sum-free set S may be mapped, under some automorphism of G, to one of the following:*

(i) $\{k+1, k+2, \ldots, 2k\}$;
(ii) $\{k, k+1, \ldots, 2k-1\}$;
(iii) $\{k, k+2, k+3, \ldots, 2k-1, 2k+1\}$.

DEFINITIONS. Following Vosper [4], [5], we shall call a set $A \subseteq Z_n$ a *standard set* if the elements of A are in arithmetic progression. If $A, B \subseteq Z_n$ are standard sets with the same common difference, then (A, B) is a *standard pair*.

Proof of Theorem 1. We first consider the case when $|G| = p^2$ and then generalize.

(a) Let $G = \langle x_1, x_2; px_i = 0, i = 1, 2; x_1 + x_2 = x_2 + x_1\rangle$.

Let X_i denote $\langle x_i\rangle$ and let S be a maximal sum-free set in G.

G has $(p+1)$ subgroups of order p, none of which contains more than k elements of S by (1). But $\lambda(G) \geq kp$ and the union of these $(p+1)$ subgroups is the whole of G; hence at least one of these subgroups contains k elements of S. We assume this subgroup to be X_1.

So $G = \bigcup_{i=0}^{p-1} (X_1+ix_2)$, and we denote by S_i the subset of X_1 such

https://doi.org/10.1017/S000497270004199X Published online by Cambridge University Press

that $S_i + ix_2 = S \cap (X_1+ix_2)$. In particular $|S_0| = k$. If $|S_i| \le k$ for every $i = 1, \ldots, p-1$, then $|S| \le kp$. But $|S| \ge kp$ by (1) and the theorem follows.

So suppose $|S_i| > k$ for some i . We may choose x_2 so that $|S_1| > k$. Since S is sum-free,

(2) $$\left(S_i+S_j\right) \cap S_{i+j} = \emptyset$$

and, in particular,

(3) $$\left(S_0+S_i\right) \cap S_i = \emptyset .$$

Hence

(4) $$|S_0+S_1| \le p - |S_1| .$$

By the Cauchy-Davenport theorem [3],

(5) $$|S_0| + |S_1| - 1 \le |S_0+S_1| .$$

By (4) and (5), $2|S_1| \le p + 1 - |S_0|$ so that $|S_1| \le k+1$. Since we assumed $|S_1| > k$, we must have $|S_1| = k+1$. If $\left(S_0, S_1\right)$ is not a standard pair, then by Vosper's Theorem [4], [5], $|S_0+S_1| \ge |S_0| + |S_1| = 2k+1$. But by (4), $|S_0+S_1| \le 2k$, a contradiction. Hence $\left(S_0, S_1\right)$ is a standard pair with difference d and without loss of generality, we may assume that $d = 1$.

Since S_0 is sum-free, we have three possibilities: $S_0 = \{k, \ldots, 2k-1\}$ or $\{k+1, \ldots, 2k\}$ or $\{k+2, \ldots, 2k+1\}$. Since $S_1 = \{l, l+1, \ldots, l+k\}$ for some $l \in X_1$, neither k nor $2k + 1$ belongs to S_0 . Hence

(6) $$S_0 = \{k+1+r;\ \ r = 0, 1, \ldots, k-1\}$$

and we may choose x_2 so that

$$S_1 = \{k+1+r;\ \ r = 0, 1, \ldots, k\} .$$

Since S is sum-free, (3) bounds the range of each S_i ; more

https://doi.org/10.1017/S000497270004199X Published online by Cambridge University Press

precisely, for each i there exists $\alpha_i \in S_i$ such that

$$S_i \subseteq \{\alpha_i+r;\ \ r = 0, 1, \ldots, k\} .$$

We call S_i a small-range set if for some $m_i > 0$, we have

$$S_i \subseteq \{\alpha_i+r;\ \ r = 0, 1, \ldots, k-1-m_i\}$$

and $\alpha_i+k-1-m_i \in S_i$. Similarly we call S_i a normal-range set if $S_i \subseteq \{\alpha_i+r;\ \ r = 0, \ldots, k-1\}$ and $\alpha_i+k-1 \in S_i$, and a big-range set if $S_i \subseteq \{\alpha_i+r;\ \ r = 0, \ldots, k\}$ and $\alpha_i+k \in S_i$. By (2) we have

(7) $$S_{i+1} \subseteq \{\alpha_i-m_i+r;\ \ r = 0, 1, \ldots, k+m_i\}$$

when S_i is a small-range set;

(8) $$S_{i+1} \subseteq \{\alpha_i+r;\ \ r = 0, \ldots, k\}$$

when S_i is a normal-range set;

(9) $$S_{i+1} \subseteq \{\alpha_i+1+r;\ \ r = 0, \ldots, k-1\}$$

when S_i is a big-range set.

Now consider the movement of α_i for $i = 1, 2, \ldots, p-1$. If S_i is a big-range set then, by (9), $\alpha_{i+1} > \alpha_i$. If S_i is a normal-range set then, by (8), $\alpha_{i+1} \geq \alpha_i$. If S_i is a small-range set then, by (7), $\alpha_{i+1} \geq \alpha_i-m_i$. In this last case, α_{i+1} may be at most m_i steps closer to 0 than α_i is. But then the contribution of S_i to S is m_i elements fewer than the average contribution of k elements. Since $|S| \geq kp$, we must make up these m_i elements, one each from m_i of the big-range sets. But by (2) and the Cauchy-Davenport theorem, the cosets containing big-range sets themselves form a sum-free set in G/X_1, so that there are at most k big-range sets. Hence $m = \sum_{i=0}^{p-1} m_i \leq k$, and $\alpha_i \geq k+1-m$ for all $i = 1, \ldots, p-1$, where $k+1 = \alpha_0$ by (6). Hence

$\alpha_i \geq 1$ for all i. A similar argument, using the relation $(S_i - S_1) \cap S_{i-1} = \emptyset$ in place of (2), shows that the right hand end-point of S_i never exceeds $p-1$ for all i. Hence $0 \notin S_i$, $S \cap X_2 = \emptyset$ and $|S| \leq kp$.

(b) Now let G be an elementary abelian group of order p^n. Then G has $(p^n-1)/(p-1)$ subgroups of order p, none of which contains more than k elements of a maximal sum-free set S. But $\lambda(G) \geq kp^{n-1} > (k-1)(p^n-1)/(p-1)$ so that at least one of these subgroups contains k elements of S, and we denote this subgroup by X. Let Y denote the subgroup complementing X in G. Thus Y is an elementary abelian group of order p^{n-1} and has $(p^{n-1}-1)/(p-1) = \rho$ subgroups Y_i of order p.

Now $|S \cap X| = k$ and, by (a), $|S \cap (X+Y_i)| \leq kp$ for all i. Thus

$$\begin{aligned}|S| &= \sum_{i=1}^{\rho} |S \cap (X+Y_i)| - (\rho-1)k \\ &\leq \rho kp - (\rho-1)k \\ &= \rho k(p-1) + k \\ &= kp^{n-1} .\end{aligned}$$

This completes the proof of the Theorem.

We now establish the following result which we need in the proof of Theorem 2.

LEMMA. *Let $G = Z_n$ and let S be a sum-free set in G satisfying*

(10) $$|S| = k, \quad \overline{S} = S + S \quad \text{and} \quad S = -S$$

where $n = 3k+1$. Then

I $(S+g) \cap S = \emptyset$ *if and only if* $g \in S$;

II *if* $|(S+g) \cap S| = 1$ *for some* $g \in G$, *then* $|(S+g^*) \cap S| \geq k-3$ *where* $g^* = 3g/2$ *and* $\pm g/2 \in S$;

III *if* $|(S+g) \cap S| = \lambda > 1$ *for some* $g \in G$, *then there exists* $g^* \in G$ *such that* $|(S+g^*) \cap S| \geq k-(\lambda+1)$.

https://doi.org/10.1017/S000497270004199X Published online by Cambridge University Press

Proof. Part I is trivial. To show II, let $|(S+g) \cap S| = 1$ for some $g \in G$. Then there exist $s_1, s_2 \in S$ such that $s_1+g = s_2$. But $S = -S$, hence $-s_2+g = -s_1 \in S$ so that $s_2 = -s_1$ and $g = -2s_1$. Now $S \cap (S-s_1) = (S-s_1) \cap (S-2s_1) = (S-2s_1) \cap (S-3s_1) = \emptyset$ and $|S \cap (S-2s_1)| = |(S-3s_1) \cap (S-s_1)| = 1$ so that $|S \cap (S-3s_1)| \geq k-3$. Take $g^* = -3s_1$ to complete the proof of II.

By hypothesis of III, there exist $s_1, s_2 \in S$ such that $s_1+g, s_2+g \in S$ and $s_1 \neq s_2$. Hence

$$\emptyset = (S+s_1) \cap S = (S+s_2) \cap S = (S+g+s_1) \cap S$$
$$= (S+g+s_2) \cap S = (S+g+s_1) \cap (S+g) = (S+g+s_2) \cap (S+g) .$$

Thus $|(S+g+s_1) \cap (S+g+s_2)| \geq k - (\lambda+1)$, with equality only in the case when $S \cup (S+g) \cup (S+g+s_1) \cup (S+g+s_2) = G$. Choose $g^* = s_1 - s_2$ to complete the proof.

Proof of Theorem 2. If S is a standard set then, by taking an automorphism of G if necessary, we can assume the common difference to be 1. This gives two possibilities for S, namely *(i)* and *(ii)* of the theorem.

If S is not a standard set, then by Vosper's Theorem $|S-S| \geq 2|S|$ whence $|S-S| = 2k$ or $2k+1$. Since S is sum-free,

(11) $$S \cap (S+S) = S \cap (S-S) = (-S) \cap (S-S) = \emptyset .$$

If $|S-S| = 2k+1$, then $S \cup (S-S) = G$ and by (11), $S = -S$. We now show that the case $|S-S| = 2k$ does not arise. If $|S-S| = 2k$, then $S \cup (S-S) = \overline{\{g\}}$, for some $g \in G$ and $-S \subseteq S \cup \{g\}$. Two cases are possible:

(A) $S = -S$. Then $S+S = S-S$ and since $0 \in S-S$, $g \neq 0$ so that $-g \in S+S$. Thus for some $s_1, s_2 \in S$, $-g = s_1+s_2$. This implies that $g = -s_1-s_2 \in S+S$, a contradiction;

(B) $-S \subseteq S \cup \{g\}$ and $g \in -S$. Then $|S \cup (-S)| = |S| + 1$ and $|S \cap (-S)| = 2|S| - |S| - 1 = |S| - 1$, an odd number. But this is a contradiction since $0 \notin S$.

We may now assume that the maximal sum-free set S satisfies the conditions in (10). If for some $g \in G$, $|(S+g) \cap S| = 1$, then by II of the lemma $|(S+3g/2) \cap S| \geq k-3$. Map $3g/2$ to 1 so that $g = k+1$.

https://doi.org/10.1017/S000497270004199X Published online by Cambridge University Press

Now $|(S+1) \cap S| \neq k-1$ since S is not a standard set. If $|(S+1) \cap S| = k-2$, then obviously $S = \{\pm k/2, \pm(1+k/2), \ldots, \pm(k-1)\}$ which maps under automorphism to the set *(iii)* in the statement of the theorem. If $|(S+1) \cap S| = k-3$, then
$S = \{\alpha, \ldots, \alpha+\rho-1, k+\rho+1, \ldots, 2k-\rho, 3k+2-\alpha-\rho, \ldots, 3k+1-\alpha\}$, where $\alpha \leq k$ and $1 \leq \rho < k/2$. But $-g/2 = k \in S$ and $g = k+1 \notin S$ by the lemma. Hence $\alpha+\rho-1 = k$ and
$S = \{k+1-\rho, \ldots, k, k+\rho+1, \ldots, 2k-\rho, 2k+1, \ldots, 2k+\rho\}$. But $(k+1-\rho) + (k+\rho+1) = 2k+2 \in \bar{S}$. Hence $\rho = 1$ and S is the set *(iii)* of the statement of the theorem.

We are now left with the case where S satisfies the conditions in (10) and $|(S+g) \cap S| \neq 1$ for any $g \in G$. By taking an automorphism of G if necessary, assume that $|(S+1) \cap S|$ is maximal. We list the elements of S as follows:

(12) $$S = \{\alpha_1, \ldots, \alpha_1+l_1, \alpha_2, \ldots, \alpha_2+l_2, \ldots, \alpha_h, \ldots, \alpha_h+l_h\}$$

where $0 < \alpha_1 \leq \alpha_1+l_1 < \alpha_2-1 < \alpha_2+l_2 < \ldots < \alpha_h-1 < \alpha_h+l_h < p$, and $\alpha_i, \ldots, \alpha_i+l_i$ denotes a string of (l_i+1) consecutive elements of S. By (10),

(13) $$\alpha_{h-i} + l_{h-i} = p - \alpha_{i+1} \quad \text{for all } i = 0, \ldots, h-1 .$$

Also

(14) $$|(S+1) \cap S| = k - h \geq |(S+g) \cap S| \quad \text{for all } g \in G .$$

Hence h is minimal in (12). We show that $h = 2$.

Let $X = \{\alpha_1, \alpha_2, \ldots, \alpha_h\}$ and let
$Y = \{\alpha_1+l_1+1, \ldots, \alpha_h+l_h+1\} = \{1-\alpha_1, \ldots, 1-\alpha_h\} = 1 - X$ by (13). For any $i = 1, \ldots, h$, $\alpha_i-1 \in \bar{S}$ so that by (14) and the lemma, $|(S+\alpha_i-1) \cap S| \geq h-1$. But for any $s_1, s_2 \in S$, $s_1+\alpha_i-1 = s_2$ implies that $s_1 \in X$, $s_2 \in -X$ and $s_1+\alpha_i \in Y$. Hence

(15) $$h \geq |(X+\alpha_i) \cap Y| \geq h - 1 \quad \text{for all } i = 1, \ldots, h .$$

Also

https://doi.org/10.1017/S000497270004199X Published online by Cambridge University Press

(16) $$|X+X| \geq 2h - 1 .$$

Since $|Y| = h$, $X + X$ contains at least $(h-1)$ elements which do not belong to Y. By (15) $X + \alpha_i$ contains at most one element which does not belong to Y. Thus for at least $(h-2)$ values of $i = 1, 2, \ldots, h$, $2\alpha_i \notin Y$. But $2\alpha_i \notin Y$ implies that $1-\alpha_i \notin X+\alpha_i$ since $Y = 1-X$.

Hence for at least $(h-2)$ values of i,

$$\{\alpha_1+\alpha_i, \ldots, \alpha_{i-1}+\alpha_i, \alpha_{i+1}+\alpha_i, \ldots, \alpha_h+\alpha_i\} = (X+\alpha_i) \cap Y$$
$$= \{1-\alpha_1, \ldots, 1-\alpha_{i-1}, 1-\alpha_{i+1}, \ldots, 1-\alpha_h\} ,$$

and summing on both sides of this equation,

(17) $$(h-3)\alpha_i \equiv h - 1 - 2 \sum_{j=1}^{h} \alpha_j \ (p) .$$

Hence $h \leq 3$. But $h > 1$ since S is not a standard set. If $h = 3$, we can list the elements of S as follows:

$$S = \{\alpha, \ldots, \alpha+\rho-1, k+\rho+1, \ldots, 2k-\rho, 3k+2-\alpha-\rho, \ldots, 3k+1-\alpha\} ,$$

where $\alpha \leq k$ and $\rho < k/2$. From (17) we have
$0 \equiv 3-1-2(\alpha+k+\rho+1-(\alpha+\rho-1))\ (p)$ or $1 \equiv k+2\ (p)$ which is not possible.
Hence conclude that $h = 2$ and obviously
$S = \{\pm k/2, \pm(1+k/2), \ldots, \pm(k-1)\}$ which maps under automorphism to the set *(iii)* in the statement of the theorem.

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] P. Erdös, "Extremal problems in number theory", *Proc. Sympos. Pure Math.* 8, 181-189. (Amer. Math. Soc., Providence, R.I., 1965).

[3] Henry B. Mann, *Addition theorems: The addition theorems of group theory and number theory* (Interscience Tracts in Pure and Applied Mathematics, Number 18; John Wiley & Sons, New York, London, Sydney, 1965).

https://doi.org/10.1017/S000497270004199X Published online by Cambridge University Press

[4] A.G. Vosper, "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* 31 (1956), 200-205.

[5] A.G. Vosper, "Addendum to 'The critical pairs of subsets of a group of prime order' ", *J. London Math. Soc.* 31 (1956), 280-282.

[6] H.P. Yap, "The number of maximal sum-free sets in C_p", *Nanta Math.* 2 (1968), 68-71.

The University of Alberta,
Edmonton,
Alberta, Canada.