1. *Maximal Sum-Free Sets of Elements of Finite Groups*

By Palahenedi Hewage DIANANDA and Hian Poh YAP
Department of Mathematics, University of Singapore, Singapore

(Comm. by Zyoiti SUETUNA, M. J. A., Jan. 13, 1969)

1. *Introduction.* Let G be an additive group. If S and T are non-empty subsets of G, we write $S \pm T$ for $\{s \pm t ; s \in S, t \in T\}$ respectively, $|S|$ for the cardinal of S and $\bar{S}$ for the complement of S in G. We abbreviate $\{f\}$, where $f \in G$ to f. We say that S is sum-free in G if S and $S+S$ have no common element and that S is maximal sum-free in G if S is sum-free in G and $|S| \geqq |T|$ for every T sum-free in G. We denote by $\lambda(G)$ the cardinal of a maximal sum-free set in G. We say that S is in arithmetic progression with the difference d if $S=\{s, s+d, s+2d, \cdots, s+nd\}$ for some s and $d \in G$ and some integer $n \geqq 0$.

In [3] Yap obtained certain results concerning $\lambda(G)$ for abelian G. The main purpose of this paper is to generalize and to improve, where possible, his results.

2. *Abelian groups.* Throughout this section G is an abelian group. We use the following theorem [2; p. 6] due to M. Kneser:

Theorem 1. *Let A and B be finite non-empty subsets of G. Then a subgroup H of G exists such that $A+B+H=A+B$ and $|A+B| \geqq |A+H|+|B+H|-|H|$.*

Suppose that S is a maximal sum-free set in G. Then a subgroup H of G exists such that

$$S+S+H=S+S \quad \text{and} \quad |S+S| \geqq 2|S+H|-|H|. \tag{1}$$

Lemma 1. *$S+H$ is also a sum-free set in G.*

Proof. Otherwise, $S+H$ and $(S+H)+(S+H)=S+S$ have a common element. Thus $s+h=s_1+s_2$ for some s, s_1 and $s_2 \in S$ and some $h \in H$. Hence $s=s_1+s_2-h \in S+S+H=S+S$. This is not possible since S is sum-free in G.

It now follows that $S+H=S$ since S is maximal sum-free in G. Thus we have

Lemma 2. *S is a union of cosets of H in G.*

Hence $|H|$ is a divisor of $|S|$. Now $|G| \geqq |S|+|S+S| \geqq 3|S| - |H|$, from (1). Hence

$$|S| \leqq |H| \left[\frac{1}{3}\left(\frac{|G|}{|H|}+1\right)\right],$$

where $[x]$ denotes the integer part of x. Thus

$$\lambda(G) \leqq \max_{d \mid |G|} \frac{|G|}{d}\left[\frac{1}{3}(d+1)\right], \tag{3}$$

if G is finite. Clearly

$$\frac{1}{d}\left[\frac{1}{3}(d+1)\right]=\begin{cases}\frac{1}{3}\left(1+\frac{1}{d}\right) & \text{if } d\equiv 2 \pmod 3,\\ \frac{1}{3} & \text{if } d\equiv 0 \pmod 3,\\ \frac{1}{3}\left(1-\frac{1}{d}\right) & \text{if } d\equiv 1 \pmod 3.\end{cases} \tag{4}$$

We consider the following cases:

Case 1. $|G|$ has at least one prime factor $\equiv 2 \pmod 3$.

Case 2. $|G|$ has no prime factor $\equiv 2 \pmod 3$ but has 3 as a factor.

Case 3. $|G|$ has every prime factor and thus every factor $\equiv 1 \pmod 3$.

It is seen that these three cases are exhaustive and mutually exclusive. We thus have, from (3) and (4),

Lemma 3.

$$\lambda(G) \leqq \begin{cases}\frac{1}{3}|G|\left(1+\frac{1}{p}\right) & \textit{in Case } 1, & (5)\\ \frac{1}{3}|G| & \textit{in Case } 2, & (6)\\ \frac{1}{3}\left(|G|-1\right) & \textit{in Case } 3, & (7)\end{cases}$$

where, in Case 1, p *is the least prime factor* $\equiv 2 \pmod 3$ *of* $|G|$.

We note that this lemma implies Theorems 2, 7, 10 and 11 of [3].

Theorem 2. *In Case* 1, $\lambda(G)=(1/3)|G|(1+(1/p))$ *and, if S is a maximal sum-free set in G, then S is a union of cosets of some subgroup H of order $|G|/p$ of G, S/H is in arithmetic progression and* $S \cup (S+S)=G$.

Proof. Clearly G has a subgroup K of order $|G|/p$ and an element g of order p such that $G=K \cup (K+g) \cup (K+2g) \cup \cdots \cdots \cup (K+(p-1)g)$. It is easy to see that $T=(K+g) \cup (K+4g) \cup (K+7g) \cup \cdots \cup (K+(p-1)g)$ is sum-free in G and $|T|=(1/3)|G|(1+(1/p))$. Hence, from (5), T is maximal sum-free in G and $\lambda(G)=(1/3)|G|(1+(1/p))$.

Now let S be maximal sum-free in G. Then

$$|S|=\frac{1}{3}|G|\left(1+\frac{1}{p}\right). \tag{8}$$

Let H be a subgroup of G, satisfying (1). Then (2) is also satisfied and we have $|H|=|G|/p$. By Lemma 2, S is a union of cosets of H in G. From (1) and (8), $|S|+|S+S| \geqq |G|$. Since S is sum-free in G, we have equality in the above and $S \cup (S+S)=G$. Further, $|S+S|$

$=2|S|-|H|$ and so $|(S/H)+(S/H)|=2|S/H|-1$, where S/H is a subset of the factor group G/H of order p. That S/H is in arithmetic progression follows from the following theorem [2; pp. 3–4] due to A. G. Vosper:

Theorem 3. *Let $C=A+B$, where A and B are non-empty subsets of G of prime order p. Then either $|C|\geqq|A|+|B|$ or one of the following holds*: (i) $C=G$, (ii) $|C|=p-1$ *and* $\bar{B}=f-A$, *where* $\bar{C}=f$, (iii) *A and B are in arithmetic progression with the same difference*, (iv) $|A|=1$ *or* $|B|=1$.

We note that Theorem 2 generalizes Theorems 3, 4 and 5 of [3].

Theorem 4. *In Case* 2, $\lambda(G)=|G|/3$ *and, if S is a maximal sum-free set in G, then S is a union of cosets of some subgroup H of order $|G|/3m$, where m is an integer such that $3m\,|\,|G|$, and one of the following holds*: (i) $|S+S|=2|S|-|H|$, (ii) $|S+S|=2|S|$ *and* $S\cup(S+S)=G$.

Proof. Clearly G has a subgroup K of order $|G|/3$ and an element g of order 3 such that $G=K\cup(K+g)\cup(K+2g)$. It is easy to see that $T=K+g$ is sum-free in G and $|T|=|G|/3$. Hence, from (6), T is maximal sum-free in G and $\lambda(G)=|G|/3$.

Now let S be maximal sum-free in G. Then $|S|=|G|/3$. Let H be a subgroup of G satisfying (1). Then, by Lemma 2, S is a union of cosets of H and $|H|=|G|/3m$, where m is an integer and $3m\,|\,|G|$. From (1), $|S+S|\geqq2|S|-|H|$. Thus $|S+S|=2|S|-|H|$ or $2|S|$ since, S being sum-free, $|S|+|S+S|\leqq|G|$. Clearly $S\cup(S+S)=G$ if $|S+S|=2|S|$.

We note that Theorem 4 generalizes Theorems 8 and 9 of [3].

Theorem 5. *In Case* 3, $(1/3)|G|(1-(1/m))\leqq\lambda(G)\leqq(1/3)(|G|-1)$, *where m is the maximal order of an element of G.*

Proof. Suppose that G has an element g of order m. Then G clearly has a subgroup K of order $|G|/m$ such that $G=K\cup(K+g)\cup(K+2g)\cup\cdots\cup(K+(m-1)g)$. It is easy to see that $T=(K+2g)\cup(K+5g)\cup(K+8g)\cup\cdots\cup(K+(m-2)g)$ is sum-free in G and $|T|=\frac{m-1}{3}\frac{|G|}{m}$. The theorem now follows since (7) also is true.

We note that if G is cyclic then $|G|=m$ and the above theorem yields Theorem 6 of [3]. We make the following conjecture:

In Case 3, $\lambda(G)=\frac{1}{3}|G|\left(1-\frac{1}{m}\right)$, *where m is as in Theorem* 5.

This is true if G is cyclic. We can prove this conjecture for $G=C_7\times C_7$ also, where each C_7 is a cyclic group of order 7. An outline of the proof follows:

We use the following theorem [2; p. 3] due to A. Cauchy and H. Davenport:

Theorem 6. *If A and B are non-empty subsets of a group G of prime order then $A+B=G$ or $|A+B|\geqq|A|+|B|-1$.*

$G=C_7\times C_7$ has eight subgroups $K_1, K_2, \cdots, K_8$ of order 7. Their union is G and $K_i\cap K_j=0$ $(i\neq j)$. Let S be a maximal sum-free set in G. Then $0\notin S$; by Theorem 5, $|S|\geqq 14$ and, by Theorem 6, $|S\cap K_i|\leqq 2$ for every i. Thus the $S\cap K_i$ are disjoint and $|S\cap K_j|=2$ for some j. Let the cosets of K_j be $H_i=ia+K_j$ $(i=0, 1, \cdots, 6)$. Clearly $H_{7+i}=(7+i)a+K_j=H_i$. Let $S_i=S\cap H_i$. Then $|S|=|S_0|+(|S_1|+|S_2|+|S_4|)+(|S_3|+|S_6|+|S_5|)\leqq 14$ and thus $|S|=14$ if

$$|S_i|+|S_{2i}|+|S_{4i}|\leqq 6 \quad (i=1, 2, \cdots, 6). \tag{9}$$

Clearly, for all i and j,

$$(S_i+S_j)\cap S_{i+j}=\varnothing \quad \text{and} \quad (S_i+S_j)\cup S_{i+j}\subset H_{i+j}. \tag{10}$$

Since $|S_0|=2$, from (10) and Theorem 6, $|S_i|\leqq 3$ for every i. If $|S_i|\leqq 2$ for every i then (9) is satisfied. If $|S_i|=3$ for some i $(1\leqq i\leqq 6)$ then, since $|S_0|=2$, from (10) and Theorems 6 and 3, we have that S_i is in arithmetic progression. Thus $S_i=ia+b+\{-d, 0, d\}$ for some $d\,(\neq 0)$ and $b\in K_j$. Hence, from (10), $S_{2i}\subset 2ia+2b+\{-3d, 3d\}$. Since $S_{8i}=S_i$ and $|S_i|=3$ it follows that $|S_{4i}|\leqq 2$. Since also $|S_{2i}|\leqq 2$, (9) follows if we prove that $|S_i|=3$ and $|S_{2i}|=2$ imply that $|S_{4i}|\leqq 1$. If $|S_{2i}|=2$ then $S_{2i}=2ia+2b+\{-3d, 3d\}$. Thus, from (10), $S_{4i}\subset 4ia+4b+\{-3d, -2d, 2d, 3d\}$. Since $S_{8i}=S_i$, it follows from (10) that S_{4i} can have at most one element, namely $4ia+4b\pm 2d$. Thus (9) follows. Hence $\lambda(G)=|S|=14$.

3. *Non-abelian groups.* Hitherto we have considered abelian groups only. In this section we prove some results for groups G which are not necessarily abelian.

We first note that if $S=s+H=H+s$, where $s\in G$ and H is a subgroup of G then $|S+S|=|S|$. A converse of this is contained in the following generalization of Theorem 1 of [3].

Theorem 7. *If S is a finite subset of G and $|S+S|=|S|$ then there is a finite subgroup H of G such that $S+H=S=H+S$ and $S-S=H=-S+S$.*

Proof. Let s_1 and $s_2\in S$, $H_1=-s_1+S$ and $H_2=S-s_2$. Then $|H_1+H_2|=|S+S|=|S|=|H_1|=|H_2|<\infty$. But $0\in H_1\cap H_2$ and thus $H_1+H_2\supset H_1\cup H_2$. Hence $H_1+H_2=H_1=H_2$. Thus there is a finite subgroup $H=H_1$ of G such that S is both a left and a right coset of H. Thus $H=-s+S=S-s$ for every $s\in S$, and the theorem clearly follows.

Corollary. *Let $|G|=2m$. Then $\lambda(G)=m$ if and only if G has a subgroup of order m.*

It follows that if G is abelian and $|G|=2m$ then $\lambda(G)=m$. This is a consequence of Theorem 2 also.

We now prove, for non-abelian G, the following theorem, which, by Theorem 4, is true for abelian G:

Theorem 8. *Let* $|G|=3p$, *where* p *is a prime* $\equiv 1 \pmod 3$. *Then* $\lambda(G)=p$.

Proof. If G is non-abelian then G has generators a and b such that $3a=0=pb$ and $b+a=a+rb$, where $r^2+r+1\equiv 0 \pmod p$ [1; p. 51]. Let $H_0=\{0, b, 2b, \cdots, (p-1)b\}$, $H_1=a+H_0$, $H_2=2a+H_0$. Then H_1 is sum-free in G and so $\lambda(G)\geqq p$. Let S be a sum-free set in G and $S_i=S\cap H_i$. By Theorem 5, $|S_0|\leqq k$, where $p=3k+1$. Thus $|S_1|+|S_2|\geqq 2k+1$ and we assume, as we may, that $|S_1|\geqq k+1$. Let $S_1=a+\{t_1b, t_2b, \cdots, t_nb\}$. Then $S_1+S_2=2a+\{rt_1b, rt_2b, \cdots, rt_nb\}+\{t_1b, t_2b, \cdots, t_nb\}$. Thus, by Theorem 6, $|S_1+S_1|\geqq 2|S_1|-1$. Now $(S_1+S_1)\cap S_2=\varnothing$ and $(S_1+S_1)\cup S_2\subset H_2$. Hence $p\geqq 2|S_1|-1+|S_2|\geqq k+|S_1|+|S_2|\geqq |S_0|+|S_1|+|S_2|=|S|$. Thus $\lambda(G)=p$.

References

[1] Marshall Hall, Jr.: The Theory of Groups. Macmillan Co., New York (1959).

[2] H. B. Mann: Addition Theorems. Interscience Publ., New York etc. (1965).

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