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

By Palahenedi Hewage Diananda and Hian Poh Yap<br>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 sumfree 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 $S=\{s, s+d, s+2 d, \cdots, s+n d\}$ 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

$$
\begin{equation*}
S+S+H=S+S \quad \text { and } \quad|S+S| \geqq 2|S+H|-|H| \tag{1}
\end{equation*}
$$

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

$$
\begin{equation*}
\lambda(G) \leqq \max _{d| | G \mid} \frac{|G|}{d}\left[\frac{1}{3}(d+1)\right], \tag{3}
\end{equation*}
$$

if $G$ is finite. Clearly

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

We consider the following cases:
Case 1. $|G|$ has at least one prime factor $\equiv 2(\bmod 3)$.
Case 2. $|G|$ has no prime factor $\equiv 2(\bmod 3)$ but has 3 as a factor.
Case 3. $|G|$ has every prime factor and thus every factor $\equiv 1$ $(\bmod 3)$.

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

Lemma 3.

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

where, in Case $1, p$ is the least prime factor $\equiv 2(\bmod 3)$ 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 $G=K \cup(K+g) \cup(K+2 g) \cup \ldots$ $\cdots \cup(K+(p-1) g)$. It is easy to see that $T=(K+g) \cup(K+4 g) \cup(K+7 g)$ $\cup \cdots \cup(K+(p-1) g)$ 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

$$
\begin{equation*}
|S|=\frac{1}{3}|G|\left(1+\frac{1}{p}\right) \tag{8}
\end{equation*}
$$

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 sumfree set in $G$, then $S$ is a union of cosets of some subgroup $H$ of order $|G| / 3 m$, where $m$ is an integer such that $3 m||G|$, 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 $G=K \cup(K+g) \cup(K+2 g)$. 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 $|H|=|G| / 3 m$, where $m$ is an integer and $3 m||G|$. From (1), $|S+S| \geqq 2|S|-|H|$. 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 $G=K \cup(K+g)$ $\cup(K+2 g) \cup \cdots \cup(K+(m-1) g)$. It is easy to see that $T=(K+2 g)$ $\cup(K+5 g) \cup(K+8 g) \cup \cdots \cup(K+(m-2) g)$ 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 $6,\left|S \cap K_{i}\right|$ $\leqq 2$ for every $i$. Thus the $S \cap K_{i}$ are disjoint and $\left|S \cap K_{j}\right|=2$ for some $j$. Let the cosets of $K_{j}$ be $H_{i}=i a+K_{j}(i=0,1, \cdots, 6)$. Clearly $H_{7+i}$ $=(7+i) a+K_{j}=H_{i}$. Let $S_{i}=S \cap H_{i}$. Then $|S|=\left|S_{0}\right|+\left(\left|S_{1}\right|+\left|S_{2}\right|+\left|S_{4}\right|\right)$ $+\left(\left|S_{3}\right|+\left|S_{6}\right|+\left|S_{5}\right|\right) \leqq 14$ and thus $|S|=14$ if

$$
\begin{equation*}
\left|S_{i}\right|+\left|S_{2 i}\right|+\left|S_{4 i}\right| \leqq 6 \quad(i=1,2, \cdots, 6) \tag{9}
\end{equation*}
$$

Clearly, for all $i$ and $j$,

$$
\begin{equation*}
\left(S_{i}+S_{j}\right) \cap S_{i+j}=\varnothing \quad \text { and } \quad\left(S_{i}+S_{j}\right) \cup S_{i+j} \subset H_{i+j} \tag{10}
\end{equation*}
$$

Since $\left|S_{0}\right|=2$, from (10) and Theorem 6, $\left|S_{i}\right| \leqq 3$ for every $i$. If $\left|S_{i}\right|$ $\leqq 2$ for every $i$ then ( 9 ) is satisfied. If $\left|S_{i}\right|=3$ for some $i(1 \leqq i \leqq 6)$ then, since $\left|S_{0}\right|=2$, from (10) and Theorems 6 and 3, we have that $S_{i}$ is in arithmetic progression. Thus $S_{i}=i a+b+\{-d, 0, d\}$ for some $d(\neq 0)$ and $b \in K_{j}$. Hence, from (10), $S_{2 i} \subset 2 i a+2 b+\{-3 d, 3 d\}$. Since $S_{8 i}=S_{i}$ and $\left|S_{i}\right|=3$ it follows that $\left|S_{4 i}\right| \leqq 2$. Since also $\left|S_{2 i}\right| \leqq 2$, (9) follows if we prove that $\left|S_{i}\right|=3$ and $\left|S_{2 i}\right|=2$ imply that $\left|S_{4 i}\right| \leqq 1$. If $\left|S_{2 i}\right|=2$ then $S_{2 i}=2 i a+2 b+\{-3 d, 3 d\}$. Thus, from (10), $S_{4 i} \subset 4 i a+4 b$ $+\{-3 d,-2 d, 2 d, 3 d\}$. Since $S_{8 i}=S_{i}$, it follows from (10) that $S_{4 i}$ can have at most one element, namely $4 i a+4 b \pm 2 d$. 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 $\left|H_{1}+H_{2}\right|=|S+S|=|S|=\left|H_{1}\right|=\left|H_{2}\right|<\infty$. 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 $|G|=2 m$. Then $\lambda(G)=m$ if and only if $G$ has a subgroup of order $m$.

It follows that if $G$ is abelian and $|G|=2 m$ 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 $|G|=3 p$, where $p$ is a prime $\equiv 1(\bmod 3)$. Then $\lambda(G)=p$.

Proof. If $G$ is non-abelian then $G$ has generators $a$ and $b$ such that $3 a=0=p b$ and $b+a=a+r b$, where $r^{2}+r+1 \equiv 0(\bmod p)[1 ; p .51]$. Let $H_{0}=\{0, b, 2 b, \cdots,(p-1) b\}, H_{1}=a+H_{0}, H_{2}=2 a+H_{0}$. 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, $\left|S_{0}\right| \leqq k$, where $p=3 k+1$. Thus $\left|S_{1}\right|+\left|S_{2}\right|$ $\geqq 2 k+1$ and we assume, as we may, that $\left|S_{1}\right| \geqq k+1$. Let $S_{1}=a$ $+\left\{t_{1} b, t_{2} b, \cdots, t_{n} b\right\}$. Then $S_{1}+S_{2}=2 a+\left\{r t_{1} b, r t_{2} b, \cdots, r t_{n} b\right\}+\left\{t_{1} b, t_{2} b\right.$, $\left.\cdots, t_{n} b\right\}$. Thus, by Theorem $6,\left|S_{1}+S_{1}\right| \geqq 2\left|S_{1}\right|-1$. Now ( $S_{1}+S_{1}$ ) $\cap$ $S_{2}=\varnothing$ and $\left(S_{1}+S_{1}\right) \cup S_{2} \subset H_{2}$. Hence $p \geqq 2\left|S_{1}\right|-1+\left|S_{2}\right| \geqq k+\left|S_{1}\right|+\left|S_{2}\right|$ $\geqq\left|S_{0}\right|+\left|S_{1}\right|+\left|S_{2}\right|=|S|$. 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).

