Hart, Sarah. (2009) **Small maximal sum-free sets**

Electronic Journal of Combinatorics 16, (1) (2009)

Small maximal sum-free sets

Michael Giudici[1]*and Sarah Hart[2]

[1]School of Mathematics and Statistics
The University of Western Australia
35 Stirling Highway
Crawley, WA 6009
AUSTRALIA
giudici@maths.uwa.edu.au

[2]School of Economics, Mathematics and Statistics
Birkbeck College
Malet Street, London, WC1E 7HX
United Kingdom
s.hart@bbk.ac.uk

Abstract

Let G be a group and $S \subseteq G$. If $xy \notin S$ for any $x, y \in S$, then S is called *sum-free*. We show that if S is maximal by inclusion and no proper subset generates $\langle S \rangle$ then $|S| \leq 2$. We determine all groups with a maximal (by inclusion) sum-free set of size at most 2 and all of size 3 where there exists $a \in S$ such that $a \notin \langle S \setminus \{a\} \rangle$.

1 Introduction

Let G be a group, S a subset of G. Then S is *sum-free* if $ab \notin S$ for all $a, b \in S$. If H is a subgroup of G then Ha is a sum-free set for any $a \notin H$. We say S is *maximal sum-free* if S is sum-free and not properly contained in any other sum-free set. Some papers have used *locally maximal* for this concept and maximal to mean maximal by cardinality (for example [11, 12]).

Most work on sum-free sets has been done in the abelian group case, particularly for $\mathbb{Z}$ and $\mathbb{Z}_n$. This includes studying the number of sum-free sets in the integers (for example [2, 3]) and the density and number of sum-free sets in abelian groups (for example [4]). sum-free sets are also closely related to the widely studied concept of caps in finite geometry. A *k-cap* in the projective space $\mathrm{PG}(n, q)$ is a collection of k points with no three collinear (see [5]). Maximal (by inclusion) caps are known as *complete* caps. When $q = 2$ caps are equivalent to sum-free sets of $\mathbb{Z}_2^{n+1}$ and complete caps are equivalent to maximal sum-free sets.

Much less is known for nonabelian groups. Kedlaya [8] has shown that there exists a constant c such that the largest sum-free set in a group of order n has size at least $cn^{11/14}$. See also [9]. Petrosyan [10] has determined the asymptotic behaviour of the number of sum-free sets in groups of even order. sum-free sets were also studied in [1] where the authors ask what is the minimum size of a maximal

*The first author was supported by an Australian Postdoctoral Fellowship during the writing of this paper.

sum-free set in a group of order n? Kedlaya claims [9, Theorem 3] that for a maximal sum-free set S of size k in a group G of order n we have $k \geq \sqrt{n/3} - 1$. However, the proof forgets that $G \backslash S$ can contain elements whose square lies in S. From this he deduces that $3k \geq n - k$, which is not correct as the unique involution of Q_8 is maximal sum-free and provides a counterexample. However, we are unable to find a counterexample to the actual statement of the theorem.

In this paper we investigate the smallest maximal sum-free sets in arbitrary groups. In particular we are interested in determining the possibilities for G given the existence of a maximal sum-free set of size k for small values of k. In Section 2 we establish some general results; for example Proposition 2.5 states that for a maximal sum-free set S of a group G, $H = \langle S \rangle$ is a normal subgroup of G. In addition, G/H is either trivial or an elementary abelian 2-group. In Section 3 we show that if S is a maximal sum-free set and $\langle S \rangle$ is not generated by any proper subset of S then $|S| \leq 2$ (Theorem 3.4). We then determine all groups with a maximal sum-free set of size 1 or 2.

Theorem 1.1 *Let S be a maximal sum-free set of size k in a group G.*

- *If $k = 1$ then $G = C_2, C_3, C_4$ or Q_8, and S consists of an element of prime order in G.*
- *If $k = 2$ then G and S are as in Tables 1, 2, or 3, or $G = \langle x \rangle \cong C_8$ and $S = \{x^2, x^6\}$, or $G \cong Q_{12} = \langle g, h : g^6 = 1, g^3 = h^2, hg = g^{-1}h \rangle$ and $S = \{g^3, g^2\}$.*

Finally Section 4 is devoted to maximal sum-free sets of size 3. We classify all such sets S for which not every proper subset of S generates $\langle S \rangle$ (Theorem 4.5).

For a set $S \subseteq G$, we define the following sets:

$$\begin{aligned} S^2 &= \{a^2 : a \in S\}; \\ S^{-1} &= \{a^{-1} : a \in S\}; \\ SS &= \{ab : a, b \in S, a \neq b\}; \\ SS^{-1} &= \{ab^{-1} : a, b \in S, a \neq b\}; \\ S^{-1}S &= \{a^{-1}b : a, b \in S, a \neq b\}; \\ \sqrt{S} &= \{x \in G : x^2 \in S\}. \end{aligned}$$

For a single element set $\{a\}$ we usually write $\sqrt{a}$ instead of $\sqrt{\{a\}}$.

Finally, let $T = \{1\} \cup S \cup S^2 \cup SS \cup SS^{-1} \cup S^{-1}S$. If $|S| = k$, a simple calculation shows that $|T| \leq 3k^2 - k + 1$.

Note that S is sum-free if $S \cap (S^2 \cup SS) = \varnothing$, and S is maximal if in addition $G = T \cup \sqrt{S}$.

From now on, assume S is maximal sum-free in G and let $H = \langle S \rangle$.

2 General results

Lemma 2.1 *Suppose $S \cap S^{-1} = \varnothing$. Then $G = T \cup T^{-1}$.*

Proof Let $x \in \sqrt{S}$. Then $(x^{-1})^2 = (x^2)^{-1} \in S^{-1}$. By hypothesis, $x^{-1} \notin \sqrt{S}$. Since $G = T \cup \sqrt{S}$, $x^{-1} \in T$. Therefore $x \in T^{-1}$. Hence $G = T \cup \sqrt{S} \subseteq T \cup T^{-1}$. Since G is a group, we must have $G = T \cup T^{-1}$. □

Corollary 2.2 *Suppose $S \cap S^{-1} = \varnothing$. Then $|G| \leq 4k^2 + 1$.*

Proof Note that $(SS^{-1})^{-1} = SS^{-1}$. So $T \cup T^{-1} = \{1\} \cup S \cup S^2 \cup SS \cup SS^{-1} \cup S^{-1}S \cup S^{-1} \cup S^{-2} \cup (SS)^{-1}$. By Lemma 2.1, $|G| \leq 1 + 4k + 4k(k-1) = 4k^2 + 1$. □

Proposition 2.3 *Suppose $a \in S$ such that $a \notin \langle S \setminus \{a\} \rangle$. Then either $o(a) \in \{2, 3\}$ or $o(a)$ is even, greater than 4 and $a^{-2} \in S$.*

Proof Assume that $a \notin \langle S \setminus \{a\} \rangle$ and $o(a) \geq 4$. Consider a^{-1}. Then $a^{-1} \in T$ or $\sqrt{S}$. If $a^{-1} \in \sqrt{S}$ then $a^{-2} \in S$. If on the other hand, $a^{-1} \in T$ then $a^{-1} = bc$ for some $b, c \in S \cup S^{-1}$. Since $a^{-1} \notin \langle S \setminus \{a\} \rangle$, exactly one of $b, c \in \{a, a^{-1}\}$. Thus $a^{-1} \in \{a, a^2, ab^{\pm 1}, b^{\pm 1}a, a^{-1}b, ba^{-1}\}$ for some $b \in S \setminus \{a\}$. Since a has order at least 4, it follows that $b \in \{a^2, a^{-2}\}$. However, S is sum-free and so $b = a^{-2}$. Thus if $a^{-1} \in T$ or $\sqrt{S}$ we have that $a^{-2} \in S$. But if $o(a)$ is odd, $a \in \langle a^{-2} \rangle$, a contradiction. Hence $o(a)$ is even. If $o(a) = 4$, then $a^{-2} = a^2 \in S^2$, a contradiction. Therefore $o(a)$ is even, greater than 4 and $a^{-2} \in S$. □

Corollary 2.4 *Let S be maximal sum-free in $H = \langle S \rangle$. Then either $H = \langle S \backslash \{b\} \rangle$ for some $b \in S$ or $o(a) \leq 3$ for all $a \in S$.*

Proof Suppose that for all $b \in S$, $H \neq \langle S \setminus \{b\} \rangle$. Suppose for a contradiction that there exists $a \in S$ such that $o(a) \geq 4$. Then by Proposition 2.3, $a^{-2} \in S$. If $a^{-2} = b$ for $b \neq a$, then $b \in \langle a \rangle$, contradicting the fact that $b \notin \langle S \setminus \{b\} \rangle$. Thus $a^{-2} = a$ and hence $o(a) = 3$, another contradiction. Hence the result. □

Proposition 2.5 *Let S be a maximal sum-free set in G and let $H = \langle S \rangle$. Then H is a normal subgroup of G. In addition, G/H is either trivial or an elementary abelian 2-group.*

Proof Suppose $x \in G \setminus H$ and $h \in H$. Since $T \subseteq H$ and $G = T \cup \sqrt{S}$, the elements xh and x both lie in $\sqrt{S}$. Write $(xh)^2 = s_1$, $x^2 = s_2$. Then

$$\begin{aligned} xhxh &= s_1 \\ xhx &= s_1 h^{-1} \\ xhx^{-1}x^2 &= s_1 h^{-1} \\ xhx^{-1} &= s_1 h^{-1} s_2^{-1} \in H. \end{aligned}$$

Hence $H \trianglelefteq G$. Furthermore, for all $x \in G$, $x^2 \in H$. Thus each element of G/H has order dividing 2. Therefore G/H is either trivial or an elementary abelian 2-group. □

Proposition 2.6 *Let $a \in S$, and $A = S \setminus \{a\}$. Then either $a \in \langle A \rangle$; $a^2 \in \langle A \rangle$ and $o(a) > 4$; or A is maximal sum-free in $\langle A \rangle$ of size $k - 1$.*

Proof Suppose that $a \notin \langle A \rangle$ and that A is not maximal sum-free in $\langle A \rangle$. Then there exists $z \in \langle A \rangle \setminus S$ with $A \cup \{z\}$ sum-free. Write $B = A \cup \{z\}$. Then $B \cup \{a\} = S \cup \{z\}$ is not sum-free, because S is maximal. That is, the addition of a to B results in a non-sum-free set. Therefore $a \in B^2 \cup BB \cup BB^{-1} \cup B^{-1}B \cup \sqrt{B} \subseteq \langle A \rangle \cup \sqrt{B}$. Since $a \notin \langle A \rangle$, we get $a \in \sqrt{B}$. That is,

$a^2 \in B \subseteq \langle A \rangle \setminus \{1\}$. If $o(a) = 3$ then $a^2 \in \langle A \rangle$ if and only is $a \in \langle A \rangle$. Thus by Proposition 2.3, $o(a) > 4$ and the result follows. $\square$

Define $\hat{S} = \{s \in S : \sqrt{s} \setminus H \neq \varnothing\}$.

Proposition 2.7 *Every element s of $\hat{S}$ has even order, and moreover all odd powers of s lie in S.*

Proof Let $s \in \hat{S}$ and suppose $x \in \sqrt{s} \setminus H$. Consider x^k for k odd. Suppose for a contradiction that $s^k \notin S$. Then $(x^k)^2 = s^k \notin S$, so $x^k \notin \sqrt{S}$. Hence $x^k \in T \subseteq H$. But $x^k = s^{(k-1)/2}x$. Therefore $x = s^{(1-k)/2}x^k \in H$, a contradiction. Thus $s^k \in S$ for all odd k. Clearly if $o(s)$ is odd this implies $1 \in S$ which is impossible. Therefore $o(s)$ is even and all odd powers of s lie in S. $\square$

Proposition 2.8 *Suppose H is not an elementary abelian 2-group. If $|\hat{S}| = 1$, then $|G| = 2|H|$.*

Proof Suppose $\hat{S} = \{s\}$. Let $h \in H$ with $o(h) > 2$. Let $x, y \in \sqrt{s} \setminus H$. Since $G = H \cup \sqrt{s}$ we have $xh \in \sqrt{s} \setminus H$. So $xhxh = x^2$, which forces $x^{-1}hx = h^{-1}$. Similarly $y^{-1}hy = h^{-1}$. But now $(xy)^{-1}h(xy) = h \neq h^{-1}$. So $xy \notin \sqrt{s}$ and so $xy \in H$. Since G/H is an elementary abelian 2-group (Proposition 2.5) it follows that $|G/H| = 2$. $\square$

Proposition 2.9 *Suppose $\hat{S} = \{s, s^{m_1}, \ldots, s^{m_t}\}$ for some $s \in S$. Then $|G|$ divides $4|H|$.*

Proof By Proposition 2.7, each m_i is odd. Let $x \in G \backslash H$. Then $\{x, xs\} \subseteq \sqrt{\hat{S}}$ and by Proposition 2.7, $(xs)^2$ and x^2 are both odd powers of s. Thus $sx = xx^{-2}s^j$ for some even integer j and so $sx = xs^r$ for some odd integer r. It follows that for any odd integer i there exists an odd integer l such that $s^i x = xs^l$.

Suppose that yH and xH are distinct non-trivial cosets of H. Then $xy \notin H$ and so $(xy)^2 \in \hat{S}$ and so $(xy)^2 = s^r$ for some odd integer r. Thus $yx = xx^{-2}s^r y^{-2}y$ and since x^{-2} and y^{-2} are both odd powers of s it follows that $yx = xys^r$ for some odd integer r.

Finally suppose xH, yH and zH are distinct non-trivial cosets of H. Then

$$\begin{aligned}
(xyz)^2 &= xyzxyz = xyxzs^{r_1}yz && \text{where } zx = xzs^{r_1} \text{ with } r_1 \text{ odd} \\
&= xxys^{r_2}zs^{r_1}yz && \text{where } yx = xys^{r_2} \text{ with } r_2 \text{ odd} \\
&= x^2s^{r_3}yzs^{r_1}yz && \text{where } ys^{r_2} = s^{r_3}y \text{ with } r_3 \text{ odd} \\
&= x^2s^{r_3}s^{r_4}(yz)^2 && \text{where } (yz)s^{r_1} = s^{r_4}(yz) \text{ with } r_4 \text{ odd} \\
&= s^j && \text{for some even integer } j
\end{aligned}$$

Therefore $xyz \in H$, and hence $xHyH = zH$. Therefore by Proposition 2.5 either $G = H$, $G/H \cong C_2$ or $G/H \cong C_2 \times C_2$. Thus $|G|$ divides $4|H|$. $\square$

Proposition 2.10 $|G| \leq 2|T| \cdot |H|$.

Proof Suppose $G \neq H$. Then for some $a \in S$, there exists $x \in \sqrt{a}$ with $x \notin H$. Let $y \in C_G(x)$. If $y = \sqrt{b}$ for some $b \in S$, then $(xy)^2 = x^2y^2 = ab \notin S$. Therefore $xy \in T$. Hence $C_G(x) \subseteq T \cup x^{-1}T$ and so $|C_G(x)| \leq 2|T|$. Moreover, since G/H is abelian by Proposition 2.5, $x^G \subseteq xH$. Now $|G| = |C_G(x)| \cdot |x^G|$ gives the stated bound. $\square$

3 Maximal sum-free sets of size at most 2

First we determine all groups with a maximal sum-free set of size 1.

Theorem 3.1 *Let S be a maximal sum-free set of size 1 in the group G. Then $G = C_2, C_3, C_4$ or Q_8. In each case S is an element of prime order in G.*

Proof Let $S = \{a\}$. Suppose that $o(a) > 3$. Since $\{a, a^3\}$ is not sum-free it follows that $a^6 = a$ and so $o(a) = 5$. However, in this case $\{a, a^4\}$ is sum-free and so $o(a) = 2$ or 3. By Proposition 2.7, if $o(a) = 3$, then $G = H \cong C_3$. Suppose $o(a) = 2$. Then every $x \in G \backslash \langle a \rangle$ has order 4 and $\langle a \rangle$ is the unique subgroup of G of order 2. By Proposition 2.9, G has order 2, 4 or 8 and so $G = C_2, C_4$ or Q_8. Each of these possibilities does yield a maximal sum-free set. □

We now begin our investigation of maximal sum-free sets of size 2.

Proposition 3.2 *Let $S = \{a, b\}$ be a maximal sum-free set in the group G. Then either $H = \langle S \rangle$ is cyclic or $2 \in \{o(a), o(b)\} \subseteq \{2, 3\}$.*

Proof Assume H is not cyclic. By Corollary 2.4, $\{o(a), o(b)\} \subseteq \{2, 3\}$. We must eliminate the possibility that $o(a) = o(b) = 3$. Suppose this occurs. Then $S \cap S^{-1} = \varnothing$, so by Lemma 2.1, $H = T \cup T^{-1}$. Now

$$T \cup T^{-1} = \{1, a, b, a^2, b^2, ab, ba, ab^{-1}, a^{-1}b, ba^{-1}, b^{-1}a, b^{-1}a^{-1}, a^{-1}b^{-1}\}.$$

Thus $|H| \leq 13$ and of course 3 divides $|H|$. If H has even order, then there exists an involution $\sigma \in H$. The only possibility is $\sigma = a^i b^j$ for some nonzero i and j. But then $a^i b^j = \sigma = \sigma^{-1} = b^{3-j} a^{3-i}$. In addition $a^i b^j a^i b^j = 1$ implies $b^j a^i b^j a^i = 1$, so $b^j a^i = a^{3-i} b^{3-j}$. This means two pairs in $T \cup T^{-1}$ are actually equal. So $|H| \leq 11$. Hence $|H| \in \{3, 6, 9\}$. A quick check reveals that none of these cases results in a maximal sum-free set with $o(a) = o(b) = 2$. Thus at least one of a and b has order 2. □

Proposition 3.3 *Suppose S is a maximal sum-free set of order 2 in $H = \langle S \rangle$.*

1. *If S contains no involutions, then $H = \langle a \rangle$ where $a \in S$ and the possibilities for S are as in Table 1.*

$\langle a \rangle$	S
C_4	$\{a, a^{-1}\}$
C_5	$\{a, a^{-1}\}$
C_6	$\{a, a^4\}$
C_7	$\{a, a^{-1}\}$, $\{a, a^3\}$, $\{a, a^5\}$
C_8	$\{a, a^6\}$

Table 1: Maximal sum-free sets with no involution

2. *If S contains an involution a, then $S = \{a, b\}$ and the possibilities for H are given in Table 2.*

H	$S = \{a, b\}$
$C_2 \times C_2$	a, b any pair of involutions
C_6	a the unique involution and b any element of order 3
D_6	a any involution and b any element of order 3.

Table 2: Maximal sum-free sets with an involution

Note that D_n is the dihedral group of order n.

Proof Suppose that H is cyclic and $b = a^k$ for some k. Then

$$T = \{1, a, a^2, a^{k-1}, a^k, a^{k+1}, a^{2k}, a^{1-k}\}.$$

Since an element of a cyclic group has as most two square roots, we also have $|\sqrt{S}| \leq 4$. Since S is maximal in H we have $H = T \cup \sqrt{S}$ and so $|H| \leq |T| + 4 \leq 12$. The cyclic groups of order up to 12 were checked by hand. Those containing no involution are listed in Table 1 , and the only maximal sum-free sets of order two containing a generator involutions are the ones given in Table 1. The only example where S contains an involution is the C_6 example given in Table 2.

Suppose S contains no involution. Then by Proposition 3.2, H is cyclic and we have already dealt with this possibility. Thus the list given in Table 1 is complete.

Suppose S contains an involution a. If H is cyclic then the only possibility is $H = C_6$ as mentioned above. So assume H is not cyclic. By Proposition 3.2, $o(b) \in \{2, 3\}$. Consider bab^{-1}. Now $o(bab^{-1}) = 2$, so $bab^{-1} \in T = \{1, a, b, b^2, ab, ba, ab^2, b^2a\}$. Working through each possibility leads to two outcomes; either $ba = ab$ or $ba = ab^{-1}$. If $o(b) = 2$, we get a maximal sum-free set in $C_2 \times C_2$; if $o(b) = 3$ we get a maximal sum-free set in either $C_2 \times C_3$ (which we have already seen) or D_6, as shown in Table 2. These are the only possibilities. □

Theorem 3.4 *Suppose S is a maximal sum-free set in G such that no proper subset of S generates $H = \langle S \rangle$. Then $|S| \leq 2$.*

Proof Suppose $k > 2$ and no proper subset of S generates H. By Proposition 2.4 every element of S has order 2 or 3. Proposition 2.6 then implies that every proper subset A of S is maximal sum-free in $\langle A \rangle$. In particular, for all $a, b \in S$, we have that $\{a, b\}$ is maximal sum-free in $\langle a, b \rangle$. Thus $\langle a, b \rangle$ is not cyclic and by Proposition 3.3, at least one of a, b is an involution and either $ba = ab$ or $o(b) = 3$ and $ba = ab^{-1}$. Hence all but at most one element of S is an involution and all the involutions commute. Let A consist of all the involutions of S. Then $\langle A \rangle \cong C_2^l$ where $l = |A|$. But, writing $A = \{a_1, \ldots, a_l\}$, if $l > 2$ the set $\{a_1, \ldots, a_l, a_1a_2a_3\}$ is sum-free. Thus A is not maximal sum-free in $\langle A \rangle$, a contradiction. Therefore S contains at most two involutions. Since $|S| \geq 3$, the only case remaining is $S = \{a, b, c\}$, where a, b are involutions, c has order 3 and $ab = ba$. Now either $ac = ca$ or $ca = ac^{-1}$, and similarly for cb. So every element of $H = \langle S \rangle$ can be written $a^i b^j c^l$ where $i, j = 0$ or 1 and l is 0, 1 or 2. Hence $|H|$ divides 12. Since $a \notin \langle b, c \rangle$, in fact $|H| = 12$. If $ca = ac^{-1}$ and $cb = bc^{-1}$ then there are 9 involutions in H. No group of order 12 contains 9 involutions [6], pg 239. Therefore we can assume that $ca = ac$. Hence $a \in Z(H)$. Consider abc. Now $abc \notin T = \{1\} \cup S \cup S^2 \cup SS \cup SS^{-1} \cup S^{-1}S$, because we know H has order 12 and for this to occur, abc cannot have an alternative expression involving just one or two of a, b and c. But $(abc)^2 = (bc)^2 \in \{1, c^2\}$. Hence $abc \notin \sqrt{S}$. Therefore $H \neq T \cup \sqrt{S}$. This contradicts S being maximal sum-free in H and so $k \leq 2$. □

Proposition 3.5 *Suppose S is maximal sum-free set of size 2 in G such that S contains no involutions. Then either $G = H$ with the possibilities as in Proposition 3.3(1), or $G = C_8 = \langle x \rangle$ and $S = \{x^2, x^6\}$.*

Proof If S is maximal sum-free in G, then S must certainly be maximal in $H = \langle S \rangle$. Therefore S and H are as described in Proposition 3.3(1). Suppose that $G \neq H$. Then $\hat{S} = \{s \in S : \sqrt{s} \backslash H \neq \varnothing\}$ is nonempty and by Proposition 2.7, given $a \in \hat{S}$, a has even order and all odd powers of a must be in S. Since $|S| = 2$ and a is not an involution, it follows that a has order 4, and then S is forced to be $\{a, a^{-1}\}$ as S contains all odd powers of a. Since $\hat{S} \subseteq \{a, a^{-1}\}$, Proposition 2.9 implies that G has order 8 or 16. Every element x of $\sqrt{S}$ has order 8. If G had order 16, since $G = H \cup \sqrt{S}$, it would have to contain one involution, two elements of order 4 and 12 elements of order 8. There are no groups of this form (see [6] pg 239). If $|G| = 8$ then G is cyclic. Therefore $G = \langle x \rangle \cong C_8$ and $S = \{x^2, x^6\}$. □

Proposition 3.6 *Suppose S is maximal sum-free of size 2 and S contains exactly one involution. Then one of the following holds.*

1. $G = H \cong C_6$;
2. $G = H \cong D_6$;
3. $G \cong Q_{12} = \langle g, h : g^6 = 1, g^3 = h^2, hg = g^{-1}h \rangle$ *and* $S = \{g^3, g^2\}$ *or* $\{g^3, g^4\}$.

Proof By Proposition 3.3(2), writing $S = \{a, b\}$, we have $a^2 = b^3 = 1$ and either $H = C_6$ or D_6. By Propositions 2.7 and 2.8, either $G = H$ or $\hat{S} = \{a\}$ and $|G| = 12$. Suppose $|G| = 12$. Then since $G = H \cup \sqrt{S}$ and the elements of $\sqrt{S}$ not in H all square to a, it follows that G has six elements of order 4. The only such group is Q_{12} (see [6, p 239]), which has a unique involution. Thus $H = C_6$ and there are two possibilities for S: a is the unique involution and b is any element of order 3. Writing $Q_{12} = \langle g, h : g^6 = 1, g^3 = h^2, hg = g^{-1}h \rangle$ gives $S = \{g^3, g^2\}$ or $\{g^3, g^4\}$. This completes the proof. □

Proposition 3.7 *Suppose S is maximal sum-free of size 2 and contains 2 involutions. Then G, S is given by Table 3.*

G	$S = \{a, b\}$
$C_2 \times C_2$	any 2 involutions
$C_4 \times C_2 \cong \langle x, y : x^4 = y^2 = 1, xy = yx \rangle$	$\{x^2, y\}$, $\{x^2, x^2y\}$
$C_2 \times Q_8 = \langle b \rangle \times Q_8$	$\{a, b\}$ or $\{a, ab\}$ where $a \in Q_8, a^2 = 1$.
$\langle g, h : g^4 = 1 = h^4, hg = g^{-1}h \rangle$	$\{g^2, h^2\}$

Table 3: Maximal sum-free sets with 2 involutions

Proof We have $S = \{a, b\}$ where $a^2 = 1, b^2 = 1$ and $ab = ba$ by Proposition 3.3. Since $G = H \cup \sqrt{S}$, either $G = H \cong C_2 \times C_2$ or $\sqrt{S} \backslash H = \varnothing$. Let $g \in G \backslash H$. Without loss, $g \in \sqrt{a}$. Then $gb \in G \backslash H$ and since $(gb)^2 \neq b$ it follows that $(gb)^2 = a$. Thus $gb = gb$ and so $S \subseteq C_G(g)$. By symmetry, $S \subseteq Z(G)$.

Suppose $x, y \in \sqrt{S} \backslash H$ with $y \notin xH$. Then $xy \notin H$ and so $xy \in \sqrt{S}$. Thus $xyxy = s$ for some $s \in S$, and hence $yx = xyx^2y^2s$. At least two of x^2, y^2, s are the same and thus cancel. Hence $yx = xys'$ for some $s' \in S$. Now suppose x_1H, x_2H, x_3H are three distinct non-trivial cosets of H. Then $(x_1x_2x_3)^2 = x_1x_2x_3x_1x_2x_3 = x_1^2(x_2x_3)^2 s_1 s_2$ for some $s_i \in S$. Therefore $(x_1x_2x_3)^2 \in \{1, ab\}$, forcing $x_1x_2x_3 \in H$ and hence $(x_1H)(x_2H) = x_3H$. In other words the factor group G/H has order 2 or 4. Hence $|G| \in \{8, 16\}$. Furthermore G has exactly 3 elements of order 2, with the remaining non-trivial elements having order 4. If G has order 8, then in addition G must be abelian, as $G = H \cup xH$ and $H \subseteq Z(G)$. The only possibility is $G = \langle x, y : x^4 = y^2 = 1, xy = yx\rangle \cong C_4 \times C_2$, with $S = \{x^2, y\}$ or $\{x^2, x^2y\}$.

If G has order 16, then $G = H \cup xH \cup yH \cup xyH$ for $x \in \sqrt{a}$ and $y \in \sqrt{S}$. Since $xy \neq yx$, G is not abelian, and in fact $Z(G) \cong C_2 \times C_2$. Along with information we have about the orders of the elements, and groups of order 16 (see [6, p 239]), there are only two non-abelian groups of order 16 with 3 involutions and centre $C_2 \times C_2$, namely $C_2 \times Q_8$ and $K = \langle g, h : g^4 = 1 = h^4, hg = g^{-1}h\rangle$ as given in the statement of this proposition. Both these groups provide maximal sum-free sets of size 2. For $C_2 \times Q_8$, a is the unique involution of Q_8 and b is an involution outside Q_8. For K we get $S = \{g^2, h^2\}$. (note that $g^2 = h^2$ is impossible as this would result in K having fewer than 16 elements. So we may assume $g \in \sqrt{a}$ and $h \in \sqrt{b}$.) This completes the analysis. □

4 Maximal sum-free sets of size 3

Theorem 3.4 tells us that if no proper subset of S generates H, then $k \leq 2$. Here, in Theorem 4.5, we classify all the maximal sum-free sets S of size 3 for which not every proper subset of S generates H. In other words, there exists $a \in S$ such that $a \notin \langle S \setminus \{a\}\rangle$.

Theorem 4.1 *Up to isomorphism, the only instances of maximal sum-free sets S of size 3 of a group G where $|G| \leq 37$ are given in Table 4 overleaf.*

Proof The maximal sum-free sets of size 3 for groups of order up to 37 were checked using the computer algebra package GAP [7], using the 'AllSmallGroups' command. As can be seen from the final column, the set or sets listed are not necessarily the only such sets in the group. One set is listed for each type. So for example if $G \cong C_9$ then for some generator g of G, either $S = \{g, g^3, g^8\}$ or $S = \{g, g^4, g^7\}$. □

Corollary 4.2 *If S is maximal sum-free set of size 3 in G and $S \cap S^{-1} = \varnothing$, then (G, S) is one of the possibilities listed in Table 4.*

For the rest of the section, assume S is maximal sum-free set of size 3 in G, with $a \in S$ such that $a \notin \langle S \setminus \{a\}\rangle$.

The next two results are needed for the proof of Theorem 4.5.

Proposition 4.3 *Suppose $o(a) = 2$. Then $|G| \leq 32$.*

Proof Write $S = \{a, b, c\}$. By Proposition 2.6, $\{b, c\}$ is maximal sum-free in $\langle b, c\rangle$. The possibilities for $\{b, c\}$ are given in Proposition 3.3.

First, consider the case where $\langle b, c\rangle$ is cyclic, so $S = \{a, b, b^i\}$ for some i and by Proposition 3.3, $o(b) \in \{4, 5, 6, 7, 8\}$. Now $b^{-1}ab$ is an involution, so must lie in T. Given that $a \notin \langle b\rangle$, we get $b^{-1}ab \in \{a, ab, ba, b^{-i}a, b^ia\}$. Note that we don't need to consider ab^{-i} or ab^i, since if these are involutions, then $ab^{-i} = b^ia$ and $ab^i = b^{-i}a$.

G		S	H	# maximal sum-free sets of size 3 in G
$\langle g : g^6 = 1\rangle$	$\cong C_6$	$\{g, g^3, g^5\}$	$\cong C_6$	1
$\langle g, h : g^3 = h^2 = 1, hgh = g^{-1}\rangle$	$\cong D_6$	$\{h, gh, g^2h\}$	$\cong D_6$	1
$\langle g : g^8 = 1\rangle$	$\cong C_8$	$\{g, g^{-1}, g^4\}$	$\cong C_8$	2
$\langle g, h : g^4 = h^2 = 1, hgh^{-1} = g^{-1}\rangle$	$\cong D_8$	$\{h, gh, g^2\}$	$\cong D_8$	4
$\langle g : g^9 = 1\rangle$	$\cong C_9$	$\{g, g^3, g^8\}, \{g, g^4, g^7\}$	$\cong C_9$	8
$\langle g, h : g^3 = h^3 = 1, gh = hg\rangle$	$\cong C_3 \times C_3$	$\{g, h, g^2h^2\}$	$\cong C_3 \times C_3$	8
$\langle g : g^{10} = 1\rangle$	$\cong C_{10}$	$\{g^2, g^5, g^8\}, \{g, g^5, g^8\}$	$\cong C_{10}$	6
$\langle g : g^{11} = 1\rangle$	$\cong C_{11}$	$\{g, g^3, g^5\}$	$\cong C_{11}$	10
$\langle g : g^{12} = 1\rangle$	$\cong C_{12}$	$\{g^2, g^6, g^{10}\}$	$\cong C_6$	1
		$\{g, g^6, g^{10}\}, \{g, g^3, g^8\}$	$\cong C_{12}$	8
$\langle g, h : g^6 = 1, g^3 = h^2, hgh^{-1} = g^{-1}\rangle$	$\cong Q_{12}$	$\{g, g^3, g^5\}$	$\cong C_6$	1
Alternating group of degree 4	$=$ Alt(4)	$\{x, y, z : x^2 = y^2 = z^3 = 1\}$	$\cong$ Alt(4)	48
		$\{x, z, xzx : x^2 = z^3 = 1\}$		
		$\{x, z, zxz : x^2 = z^3 = 1\}$		
$\langle g : g^{13} = 1\rangle$	$\cong C_{13}$	$\{g, g^3, g^9\}, \{g, g^6, g^{10}\}$	$\cong C_{13}$	16
$\langle g : g^{15} = 1\rangle$	$\cong C_{15}$	$\{g, g^6, g^{11}\}$	$\cong C_{15}$	4
$\langle g, h : g^4 = h^4 = 1, gh = hg\rangle$	$\cong C_4 \times C_4$	$\{g, h, g^{-1}h^{-1}\}$	$\cong C_4 \times C_4$	16
$\langle g, h : g^8 = 1, g^4 = h^2, hgh^{-1} = g^{-1}\rangle$	$\cong Q_{16}$	$\{g, g^4, g^{-1}\}$	$\cong C_8$	2
$\langle g, h : g^8 = h^2 = 1, hgh^{-1} = y^3\rangle$	(order 16)	$\{g, g^6, g^3h\}$	$\cong G$	8
$\langle g, h : g^{10} = 1, g^5 = h^2, hgh^{-1} = g^{-1}\rangle$	$\cong Q_{20}$	$\{g, g^5, g^8\}, \{g^2, g^5, g^8\}$	$\cong C_{10}$	6
$\langle g, h : g^3 = h^7 = 1, ghg^{-1} = h^2\rangle$	$\cong 7:3$	$\{gh, gh^{-1}, g^{-1}\}$	$\cong 7:3$	42
$\langle x : x^3 = 1\rangle \times \langle g, h : g^4 = 1, g^2 = h^2, hgh^{-1} = g^{-1}\rangle$	$\cong C_3 \times Q_8$	$\{g^2, xg^2, x^2g^2\}$	$\cong C_6$	1
$\langle g, h : g^{12} = 1, g^6 = h^2, hgh^{-1} = g^{-1}\rangle$	$\cong Q_{24}$	$\{g^2, g^6, g^{10}\}$	$\cong C_6$	1
		$\{g, g^6, g^{10}\}$	$\cong C_{12}$	4

Table 4: Maximal sum-free sets in groups of order up to 37

Now $b^{-1}ab = ab$ is impossible. The other four possibilities imply that $ab = b^j a$ for some j. Hence every element of H can be written $b^l a^\varepsilon$ for $0 \leq l < o(b)$ and $\varepsilon \in \{0, 1\}$. Therefore $|H| \leq 2o(b)$ and since $a \notin \langle b \rangle$ we have $|H| = 2o(b)$. Suppose then that $o(b) = 4$. Consider ab^2. By Proposition 3.3(1), $i = 3$, so $ab^2 \notin T$, and hence $ab^2 \in \sqrt{S}$. But $(ab^2)^2 = ab^2ab^2 = b^{2j}a^2b^2 \in \{1, b^2\} \notin S$, a contradiction. Therefore $o(b) \neq 4$. By considering the remaining possible orders of b and values of i given in Proposition 3.3, Proposition 2.7 implies that $\hat{S} \subseteq \{a\}$. Therefore, by Proposition 2.8, $|G| \leq 2|H| = 4o(b) \leq 32$.

We have shown that if $\langle b, c \rangle$ is cyclic then $|G| \leq 32$. It remains to consider the case $\langle b, c \rangle$ is not cyclic. Then by Corollary 2.4, we may assume $o(b) = 2$ and $o(c) \in \{2, 3\}$. In addition Proposition 3.3 implies that $\langle b, c \rangle$ is either abelian or isomorphic to D_6. Now by Proposition 2.6, either $c \in \langle a, b \rangle$ or $\{a, b\}$ is maximal sum-free in $\langle a, b \rangle$. For a contradiction, assume the latter case holds. Since a and b are both involutions, the only possibility is that $\langle a, b \rangle = C_2 \times C_2$, and in particular $ab = ba$. We also know that either $bc = cb$ or $cb = bc^{-1}$, and similarly either $ac = ca$ or $ca = ac^{-1}$. Therefore we can express any element of H as $a^i b^j c^l$ for $i, j \in \{0, 1\}$, $l = 0, 1$ or 2. If $abc \in T$, then $abc = a^i b^j c^l$ for some $\{i, j, l\}$ with $0 \in \{i, j, l\}$. If $l = 0$ or $l = 2$ then $c \in \langle a, b \rangle$, contrary to assumption. If $l = 1$ then $0 \in \{i, j\}$, forcing $a = 1$ or $b = 1$, another contradiction. Thus $abc \notin T$. However $(abc)^2 \in \{1, c^2\} \notin S$ so $abc \notin \sqrt{S}$, a contradiction. Therefore $c \in \langle a, b \rangle$. Since a and b are both involutions, $\langle a, b \rangle = H$ is dihedral. Now a and b lie in the non-trivial coset of the cyclic subgroup $\langle ab \rangle$ of index 2 in H. This coset is sum-free, so if c also lies in the coset, then $H \cong D_6$, as S is maximal. However we would then have $a \in \langle b, c \rangle$, which is impossible (we are assuming that $a \notin \langle S \setminus \{a\} \rangle$). Hence $c = (ab)^i$ for some i. The fact that $\{a, b, c\}$ and $\{a, b, aba\}$ are sum-free but $\{a, b, aba, c\}$ is not forces $c \in \{abab, baba\}$. Hence $H \cong D_8$ or $H \cong D_{12}$. However in D_{12}, $(ab)^3 = cab$ is an involution not contained in T, which is impossible. Therefore $H = \langle a, b \rangle \cong D_8$, where $(ab)^4 = 1$ and $c = (ab)^2$. Suppose $x \in \sqrt{a}$. Then $(bxb)^2 = bab \notin S$. Thus $bxb \in T$ and hence $x \in H$. Therefore $\sqrt{a} \subseteq H$ and similarly $\sqrt{b} \subseteq H$. Hence $\hat{S} \subseteq \{c\}$ and therefore, by Proposition 2.8, $|G| \leq 16$. We have now shown that in all cases where $o(a) = 2$, $|G| \leq 32$. □

Proposition 4.4 *Suppose $S = \{a, b, b^{-1}\}$ for some b, and $o(a) = 3$. Then $|G| \leq 21$.*

Proof By Proposition 2.6, $\{b, b^{-1}\}$ is maximal sum-free in $\langle b \rangle$. Hence by Proposition 3.3, $o(b) \in \{4, 5, 7\}$. Here

$$T = \{1, b, b^{-1}, b^2, b^{-2}, a, a^2, ab, ba, b^{-1}a, ab^{-1}, a^{-1}b, ba^{-1}, b^{-1}a^{-1}, a^{-1}b^{-1}\}.$$

Let $x \in G$ and suppose $o(x) = 3^i$ for some $i \geq 1$. If $x \in \sqrt{a}$ then $x^2 = a$, so $x = x^4 = a^2 \in T$. Hence the elements of order 3^i lie in T. Therefore G contains between 2 and 10 elements of 3-power order. Also note that $o(ba) = o(ab) = o(a^{-1}b^{-1}) = o(b^{-1}a^{-1})$ and $o(b^{-1}a) = o(ab^{-1}) = o(a^{-1}b) = o(ba^{-1})$. Now the Sylow 3-subgroups must have order 3 or 9. By Sylow's Theorem either there are 1 or 4 Sylow subgroups of order 3, or there is a unique Sylow 3-subgroup of order 9. If the Sylow 3-subgroup is C_9, then there are six elements of order 9, forcing $o(ab) = 9 = o(ab^{-1})$, and at least two of the eight elements $\{ab, ba, b^{-1}a, ab^{-1}, a^{-1}b, ba^{-1}, b^{-1}a^{-1}, a^{-1}b^{-1}\}$ to be equal. It is easy to check that this is impossible. If the Sylow 3-subgroup is $C_3 \times C_3$, or there are four Sylow 3-subgroups of order 3, then there are eight elements of order 3, which means again that at least two of the eight elements above are equal, a contradiction. Hence there is a unique Sylow 3-subgroup of order 3, which implies $\langle a \rangle$ is normal. Hence $b^{-1}ab = a^{\pm 1}$. That is, $ab = ba^{\pm 1}$. Therefore every element of $H = \langle S \rangle$ can be written $b^i a^j$ for $0 \leq i < o(b)$ and $0 \leq j < 3$. So $|H| \leq 3o(b)$ and as $a \notin \langle b \rangle$ we have $|H| = 3o(b)$. Suppose that $o(b) = 4$. Then $|H| = 12$. Now $ab^2 \notin T$, so $ab^2 \in \sqrt{S}$. But $(ab^2)^2 = ab^2ab^2 = ab^4a^{\pm 2} \in \{1, a^{-1}\}$, a contradiction. Hence $o(b) \neq 4$, so $o(b)$ is odd. Now Proposition 2.7 implies that $H = G$. Hence $|G| \leq 21$. □

Theorem 4.5 *The only examples of maximal sum-free sets S of size 3 for which not every proper subset of S generates H are those given in Table 5.*

G		S	H	# sets
$\langle g,h : g^4 = h^2 = 1, hgh^{-1} = g^{-1}\rangle$	$\cong D_8$	$\{h, gh, g^2\}$	$\cong D_8$	4
$\langle g : g^{10} = 1\rangle$	$\cong C_{10}$	$\{g^5, g^2, g^8\}$	$\cong C_{10}$	2
$\langle g : g^{12} = 1\rangle$	$\cong C_{12}$	$\{g, g^6, g^{10}\}$	$\cong C_{12}$	4
Alternating group of degree 4	$\cong \mathrm{Alt}(4)$	$\{z, x, y : x^2 = y^2 = z^3 = 1\}$	$\cong \mathrm{Alt}(4)$	24
$\langle g,h : g^{10} = 1, g^5 = h^2, hgh^{-1} = g^{-1}\rangle$	$\cong Q_{20}$	$\{g^5, g^2, g^8\}$	$\cong C_{10}$	2
$\langle g,h : g^{12} = 1, g^6 = h^2, hgh^{-1} = g^{-1}\rangle$	$\cong Q_{24}$	$\{g, g^6, g^{10}\}$	$\cong C_{12}$	4

Table 5: Maximal sum-free sets of size 3

Proof We will show that $|G| \le 37$. By Proposition 2.3, either $o(a) \in \{2, 3\}$ or $o(a)$ is even, greater than 4 and $a^{-2} \in S$. If $o(a) = 2$, then Proposition 4.3 implies $|G| \le 32$. If $o(a) = 3$, then either $S \cap S^{-1} = \varnothing$ or $S = \{a, b, b^{-1}\}$. By Corollary 2.2 and Proposition 4.4, $|G| \le 37$. It remains to consider the case where $o(a)$ is even, greater than 4 and $a^{-2} \in S$. Write $S = \{a, a^{-2}, b\}$. It is easy to check that $S \cap S^{-1} = \varnothing$ in this case. Therefore, again, $|G| \le 37$. By Theorem 3.4, (G, S) is one of the pairs given in Table 4. However in some of these cases, every proper subset of S generates H. Table 5 lists the examples for which not every proper subset of S generates H. In each case the first element of S as listed in the table is not contained in the span of the other two elements. □

Note We have checked, using GAP, all groups of order up to 100 and found no further examples of maximal sum-free sets of size 3.

References

[1] László Babai and Vera T. Sós, Sidon sets in groups and induced subgraphs of Cayley graphs. European J. Combin. 6 (1985), 101–114.

[2] P. J. Cameron, P. Erdös, P. On the number of sets of integers with various properties. Number theory (Banff, AB, 1988), 61–79, de Gruyter, Berlin, 1990.

[3] Ben Green, The Cameron-Erdös conjecture. Bull. London Math. Soc. 36 (2004), 769–778.

[4] Ben Green and Imre Z. Ruzsa, Sum-free sets in abelian groups. Israel J. Math. 147 (2005), 157–188.

[5] J. W. P. Hirschfeld and J. A. Thas, General Galois geometries. Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1991.

[6] John F. Humphreys *A Course in Group Theory*, Oxford University Press, 1996.

[7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4; 2006. (http://www.gap-system.org)

[8] Kiran S. Kedlaya, Large product-free subsets of finite groups. J. Combin. Theory Ser. A 77 (1997), 339–343.

[9] Kiran S. Kedlaya, Product-free subsets of groups. Amer. Math. Monthly 105 (1998), 900–906

[10] T. G. Petrosyan, On the number of product-free sets in groups of even order. (Russian) Diskret. Mat. 17 (2005), no. 1, 89–101; translation in Discrete Math. Appl. 15 (2005), no. 1, 47–58.

[11] A. P. Street and E. G. Whitehead Jr., Group Ramsey theory. J. Combinatorial Theory Ser. A 17 (1974), 219–226.

[12] W. D. Wallis, A. P. Street and J. Seberry Wallis, Combinatorics: Room squares, sum-free sets, Hadamard matrices. Lecture Notes in Mathematics, Vol. 292. Springer-Verlag, Berlin-New York, 1972.