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

Submitted: Nov 23, 2007; Accepted: Apr 25, 2009; Published: May 11, 2009
Mathematics Subject Classification: 20D60

Abstract

Let G be a group and S a non-empty subset of G. If $ab \notin S$ for any $a, b \in S$, 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 non-empty subset of G. Then S is *sum-free* if $ab \notin S$ for all $a, b \in S$. For example, if H is a subgroup of G then Hg is a sum-free set for any $g \notin H$. We say S is *maximal sum-free* if S is sum-free and not properly contained in any other sum-free set. Some authors have used *locally maximal* for this concept and maximal to mean maximal by cardinality (for example [12, 13]).

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

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, 4]) and the density and number of sum-free sets in abelian groups (for example [5]). 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 [6]). 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, where sometimes the term *product-free* is used instead of sum-free. Kedlaya [9] has shown that there exists a constant c such that the largest sum-free set in a group G of order n has size at least $cn^{11/14}$. See also [10]. On the other hand Gowers [3, Theorem 3.3] has recently proved that if the smallest nontrivial representation of G is of dimension k then G has no sum-free sets of size greater than $k^{-1/3}n$. Petrosyan [11] 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 sum-free set in a group of order n? Kedlaya claims [10, 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 set out the notation used in the paper. In Section 3 we establish some general results; for example Proposition 3.2 states that for a maximal sum-free set S of a group G, $\langle S \rangle$ is a normal subgroup of G. In addition, $G/\langle S \rangle$ is either trivial or an elementary abelian 2-group. In Section 4 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 4.4). We also determine all groups with a maximal sum-free set of size 1 or 2. (In Theorem 1.1, C_n is the cyclic group of order n and Q_8 is the quaternion group.)

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

- *If $k = 1$ then $G \cong C_2, C_3, C_4$ 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 5 is devoted to maximal sum-free sets of size 3. We classify all such sets S for which not every subset of size 2 in S generates $\langle S \rangle$ (Theorem 5.6).

2 Notation

In this section we establish the notation to be used in the rest of the paper. For subsets A, B of a group G, we use the standard notation AB for the product of A and B. That is,

$$AB = \{ab : a \in A, b \in B\}.$$

By definition, a nonempty set $S \subseteq G$ is sum-free if and only if $S \cap SS = \varnothing$. In order to investigate maximal sum-free sets we introduce some further notation.

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

$$\begin{aligned}
S^2 &= \{a^2 : a \in S\}; \\
S^{-1} &= \{a^{-1} : a \in S\}; \\
\sqrt{S} &= \{x \in G : x^2 \in S\}; \\
T(S) &= S \cup SS \cup SS^{-1} \cup S^{-1}S; \\
\hat{S} &= \{s \in S : \sqrt{\{s\}} \not\subset \langle S \rangle\}
\end{aligned}$$

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

We will show (Lemma 3.1) that a sum-free set $S \subseteq G$ is maximal sum-free in G if and only if $G = T(S) \cup \sqrt{S}$. The size of $T(S)$ is easy to bound (see Lemma 3.3). In general, this is far from being the case for $|\sqrt{S}|$.

For an element $g \in G$, the order of g is denoted $o(g)$. The centraliser of g in G is denoted by $C_G(g)$ and the conjugacy class containing g by g^G.

For positive integers n, C_n is the cyclic group of order n, D_{2n} is the dihedral group of order $2n$ and A_n is the alternating group of degree n. Finally, Q_{4n} is the generalized quaternion group of order $4n$. That is, $Q_{4n} = \langle g, h : g^{2n} = 1, g^n = h^2, hg = g^{-1}h \rangle$.

3 Preliminary Results

Our first result illustrates the importance of the set $T(S)$.

Lemma 3.1 *Suppose S is a sum-free set in the group G. Then S is maximal sum-free if and only if $G = T(S) \cup \sqrt{S}$.*

Proof Let S be sum-free in G. Suppose that $G = T(S) \cup \sqrt{S}$. Let $g \in G \setminus S$ and consider the set $U = S \cup \{g\}$. Suppose $g \in T(S) = S \cup SS \cup SS^{-1} \cup S^{-1}S$. If $g \in SS \subset UU$, then U is clearly not sum-free. If $g \in SS^{-1}$, then $g = st^{-1}$ for some $s, t \in S$. Hence $gt = s$ and again U is not sum-free. Similarly if $g \in S^{-1}S$, then U is not sum-free. Suppose $g \in \sqrt{S}$. Then $g^2 \in S$ and hence $UU \cap U \neq \varnothing$, so again U is not sum-free. Therefore S is not properly contained in any sum-free set, so by definition S is a maximal sum-free set.

For the reverse implication, suppose that S is a maximal sum-free set in G. Then for all $g \in G \setminus S$, the set $V = S \cup \{g\}$ is not sum-free. That is, $V \cap VV$ is nonempty. Now $VV = gS \cup Sg \cup \{g^2\} \cup SS$. Suppose $g \in V \cap VV$. No sum-free set can contain the identity element, so $g \notin gS$ and $g \notin Sg$. Therefore either $g \in SS$ or $g = 1$. Since $ss^{-1} = 1$ for all $s \in S$, we deduce that $g \in SS \cup SS^{-1}$. On the other hand, suppose there exists $s \in S \cap VV$. Now $S \cap SS = \varnothing$. Thus either $s = gt$ or $s = tg$ for some $t \in S$, or $s = g^2$. That is, $g \in SS^{-1} \cup S^{-1}S \cup \sqrt{S}$. In summary, $V \cap VV \neq \varnothing$ forces $g \in SS \cup SS^{-1} \cup S^{-1}S \cup \sqrt{S}$. This holds for all $g \in G \setminus S$. Since $T(S) = S \cup SS \cup SS^{-1} \cup S^{-1}S$, we obtain $G = T(S) \cup \sqrt{S}$. □

As a stepping-stone to classifying the groups G that can contain a given maximal sum-free set S, we often start by considering the subgroup generated by S. The structure of the quotient $G/\langle S \rangle$ given in the next result is a useful restriction on the possibilities for G.

Proposition 3.2 *Let S be a maximal sum-free set in G. Then $\langle S \rangle$ is a normal subgroup of G. In addition, $G/\langle S \rangle$ is either trivial or an elementary abelian 2-group.*

Proof Suppose $x \in G \setminus \langle S \rangle$ and $h \in \langle S \rangle$. By Lemma 3.1, $G = T(S) \cup \sqrt{S}$. Thus, since $T(S) \subseteq \langle S \rangle$, the elements xh and x both lie in $\sqrt{S}$. That is, there are elements s_1 and s_2 of S such that $(xh)^2 = s_1$ and $x^2 = s_2$. Then

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

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

Proposition 3.2 allows us to bound $|G|$ in terms of $|\langle S \rangle|$. We first require a lemma bounding the size of $|T(S)|$.

Lemma 3.3 *Suppose $S \subseteq G$ with $|S| = k$. Then $|T(S)| \leq 3k^2 - k + 1$.*

Proof Recall that $T(S) = S \cup SS \cup SS^{-1} \cup S^{-1}S$. Since $aa^{-1} = a^{-1}a = 1$ for all $a \in S$, we need only count one of the $2k$ such products. Thus

$$|T(S)| \leq |S| + |SS| + |SS^{-1}| + |S^{-1}S| - 2k + 1 \leq k + 3k^2 - 2k + 1 = 3k^2 - k + 1.$$

□

Theorem 3.4 *Suppose S is maximal sum-free in G. Then $|G| \leq 2|T(S)| \cdot |\langle S \rangle|$.*

Proof Suppose $G \neq \langle S \rangle$. By Lemma 3.1 and the fact that $T(S) \subseteq \langle S \rangle$, for some $a \in S$ there exists $x \in \sqrt{a}$ with $x \notin \langle S \rangle$. Let $y \in C_G(x)$. If $y \in \sqrt{b}$ for some $b \in S$, then $(xy)^2 = x^2y^2 = ab \notin S$. Therefore $xy \in T(S)$. Hence $C_G(x) \subseteq T(S) \cup x^{-1}T(S)$ and so $|C_G(x)| \leq 2|T(S)|$. Moreover, since $G/\langle S \rangle$ is abelian by Proposition 3.2, $x^G \subseteq x\langle S \rangle$. Now $|G| = |C_G(x)| \cdot |x^G|$ gives the stated bound. □

The bound in Theorem 3.4 is sharp. For example it is attained in the case where S consists of the unique involution in the quaternion group Q_8.

Corollary 3.5 is an immediate consequence of Lemma 3.3 and Theorem 3.4.

Corollary 3.5 *Suppose S is maximal sum-free in G with $|S| = k$. Then $|G| \leq 2(3k^2 - k+1)|\langle S\rangle|$.*

In the rest of this section, we gather together some preliminary results which will be of use to us later.

The next three results look more carefully at $\hat{S} = \{s \in S : \sqrt{s} \not\subset \langle S\rangle\}$ in order to obtain improved bounds on $|G|$ in certain special cases. Proposition 3.7 is needed in the proof of Proposition 3.8, but also gives constraints on the elements of $\hat{S}$ which in several instances can be used to show that $\hat{S} = \varnothing$ and hence that $G = \langle S\rangle$.

Proposition 3.6 *Suppose S is maximal sum-free in G and that $\langle S\rangle$ is not an elementary abelian 2-group. If $|\hat{S}| = 1$, then $|G| = 2|\langle S\rangle|$.*

Proof Suppose $\hat{S} = \{s\}$. Let $h \in \langle S\rangle$ with $o(h) > 2$. Let $x, y \in G \setminus \langle S\rangle$. It follows from Lemma 3.1 that $G = \langle S\rangle \cup \sqrt{s}$. Hence $\{x, y, xh, yh\} \subseteq \sqrt{s} \setminus \langle S\rangle$. 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 $xy \notin \sqrt{s} \setminus \langle S\rangle$, and consequently $xy \in \langle S\rangle$. Since $G/\langle S\rangle$ is an elementary abelian 2-group (Proposition 3.2) it follows that $|G/\langle S\rangle| = 2$. □

Proposition 3.7 *Suppose S is maximal sum-free in G. Then every element s of $\hat{S}$ has even order. Moreover all odd powers of s lie in S.*

Proof Let $s \in \hat{S}$ and suppose $x \in \sqrt{s} \setminus \langle S\rangle$. 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 (Lemma 3.1) $x^k \in T(S) \subseteq \langle S\rangle$. But $x^k = s^{(k-1)/2}x$. Therefore $x = s^{(1-k)/2}x^k \in \langle S\rangle$, 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. □

Proposition 3.8 *Suppose S is maximal sum-free in G. If there exist $s \in S$ and integers $m_1, \ldots, m_t$ such that $\hat{S} = \{s, s^{m_1}, \ldots, s^{m_t}\}$, then $|G|$ divides $4|\langle S\rangle|$.*

Proof By Proposition 3.7, each odd power of s lies in S. If any m_i were even, then $s^{m_i-1} \in S$ and hence $s^{m_i} = ss^{m_i-1} \in SS \cap S$, a contradiction. Therefore each m_i is odd. Let $x \in G\setminus\langle S\rangle$. Then by Lemma 3.1 $\{x, xs\} \subseteq \sqrt{\hat{S}}$. Thus for some odd integers j and m, we have $(xs)^2 = s^j$ and $x^2 = s^m$. Rearranging $xsxs = s^j$ gives $sx = xs^{-m+j-1}$. Because $-m+j-1$ is odd, it follows that for any odd integer i there exists an odd integer l such that $s^i x = xs^l$.

Suppose that $y\langle S\rangle$ and $x\langle S\rangle$ are distinct non-trivial cosets of $\langle S\rangle$. Then $xy \notin \langle S\rangle$ and so $(xy)^2 \in \hat{S}$, meaning that $(xy)^2 = s^{m_i}$ for some odd integer m_i. Thus $yx = xx^{-2}s^{m_i}y^{-2}y$. 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 $x\langle S\rangle, y\langle S\rangle$ and $z\langle S\rangle$ are distinct non-trivial cosets of $\langle S\rangle$. Then

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

Therefore $xyz \in \langle S\rangle$, and hence $x\langle S\rangle y\langle S\rangle z\langle S\rangle = \langle S\rangle$. Now Proposition 3.2 implies that either $G = \langle S\rangle$, $G/\langle S\rangle \cong C_2$ or $G/\langle S\rangle \cong C_2 \times C_2$. Thus $|G|$ divides $4|\langle S\rangle|$. □

Given that $|T(S)|$ can be bounded in terms of $|S|$, the following lemma provides us with a quick bound for $|G|$ in the special case when $S \cap S^{-1} = \varnothing$.

Lemma 3.9 *Suppose S is maximal sum-free in G. If $S \cap S^{-1} = \varnothing$, then $G = T(S) \cup T(S)^{-1}$.*

Proof Let $x \in \sqrt{S}$. Then $(x^{-1})^2 = (x^2)^{-1} \in S^{-1}$. By hypothesis, $x^{-1} \notin \sqrt{S}$. Since $G = T(S) \cup \sqrt{S}$ by Lemma 3.1, $x^{-1} \in T(S)$. Therefore $x \in T(S)^{-1}$. Hence $G = T(S) \cup \sqrt{S} \subseteq T(S) \cup T(S)^{-1}$ and so $G = T(S) \cup T(S)^{-1}$. □

Corollary 3.10 *Suppose S is maximal sum-free in G with $|S| = k$. If $S \cap S^{-1} = \varnothing$, then $|G| \leq 4k^2 + 1$.*

Proof Note that $(SS^{-1})^{-1} = SS^{-1}$ and $(S^{-1}S)^{-1} = S^{-1}S$. So $T(S) \cup T(S)^{-1} = T(S) \cup S^{-1} \cup (SS)^{-1}$. By Lemma 3.3, $|T(S)| \leq 3k^2 - k + 1$. Hence $|T(S) \cup T(S)^{-1}| \leq 4k^2 + 1$. The result now follows from Lemma 3.9. □

Corollary 3.10 will be used repeatedly in subsequent sections. For example, it shows that a maximal sum-free set of size one either consists of an involution or is contained in a group of order at most 5.

The final three results in this section deal with the situation where a maximal sum-free set S contains one or more elements a with the property that $a \notin \langle S \setminus \{a\}\rangle$. We show that there are strong restrictions on the possible orders of such elements. These results enable us to show in Theorem 4.4 that if no proper subset of S generates $\langle S\rangle$, then $|S| \leq 2$.

Proposition 3.11 *Let S be maximal sum-free in G. Suppose $a \in S$ is 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 $o(a) \geq 4$. We first show that $a^{-2} \in S$. This follows immediately if $a^{-1} \in \sqrt{S}$. So suppose that $a^{-1} \notin \sqrt{S}$. Then the fact that $G = T(S) \cup \sqrt{S}$ (Lemma 3.1) implies $a^{-1} \in T(S)$. That is, $a^{-1} = bc$ for some $b, c \in S \cup S^{-1}$. Since $a^{-1} \notin \langle S\setminus\{a\}\rangle$, at least one of $b, c \in \{a, a^{-1}\}$. Thus $a^{-1} \in \{a^{\pm 2}, ab^{\pm 1}, b^{\pm 1}a, a^{-1}b, ba^{-1}\}$ 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 $b = a^{-2}$. That is, $a^{-2} \in S$. It remains to show that $o(a)$ is even and greater than 4. If $o(a)$ were odd, then $a \in \langle a^{-2}\rangle \subseteq \langle S \setminus \{a\}\rangle$, a contradiction. Hence $o(a)$ is even. If $o(a) = 4$, then $a^{-2} = a^2 \in S \cap SS$, another contradiction. Therefore $o(a)$ is even, greater than 4 and $a^{-2} \in S$. □

Corollary 3.12 *Let S be maximal sum-free in $\langle S\rangle$. Then either $\langle S\rangle = \langle S\backslash\{b\}\rangle$ for some $b \in S$ or $o(a) \leq 3$ for all $a \in S$.*

Proof Suppose that for all $b \in S$, $\langle S\rangle \neq \langle S \setminus \{b\}\rangle$. Suppose for a contradiction that there exists $a \in S$ such that $o(a) \geq 4$. Then by Proposition 3.11, $a^{-2} \in S$. 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. $\square$

Proposition 3.13 *Suppose S is maximal sum-free in G. Let $a \in S$, and write $A = S \setminus \{a\}$. Then either $a \in \langle A\rangle$; or $a^2 \in \langle A\rangle$ and $o(a) > 4$; or A is maximal sum-free in $\langle A\rangle$.*

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 $a \in BB \cup BB^{-1} \cup B^{-1}B \cup \sqrt{B} \subseteq \langle A\rangle \cup \sqrt{B}$. 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 if $a \in \langle A\rangle$. Therefore $o(a) \geq 4$. By Proposition 3.11, $o(a) > 4$ and the result follows. $\square$

4 Maximal sum-free sets of size at most 2

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

Theorem 4.1 *Let S be a maximal sum-free set of size 1 in the group G. Then $G \cong C_2, C_3, C_4$ or Q_8. In each case S consists of an element of prime order in G.*

Proof Let $S = \{a\}$. If a is not an involution, then $S \cap S^{-1} = \varnothing$. Hence, by Corollary 3.10, $|G| \leq 5$. A quick check shows that the only example is $G \cong C_3$. Suppose $o(a) = 2$. Then, by Lemma 3.1, 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 3.8, G has order 2, 4 or 8 and so $G \cong C_2, C_4$ or Q_8. Each of these possibilities does yield a maximal sum-free set. $\square$

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

Proposition 4.2 *Let $S = \{a, b\}$ be a maximal sum-free set of size 2 in the group G. Then either $\langle S\rangle = \langle a\rangle$, $\langle S\rangle = \langle b\rangle$, or $2 \in \{o(a), o(b)\} \subseteq \{2, 3\}$.*

Proof Assume $\langle S\rangle$ is not generated by a or b. By Corollary 3.12, $\{o(a), o(b)\} \subseteq \{2, 3\}$. We must eliminate the possibility that $o(a) = o(b) = 3$. Suppose this occurs. Then $S \cap S^{-1} = \varnothing$, so by Lemma 3.9, $G = T(S) \cup T(S)^{-1}$. Now

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

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

We are now in a position to classify the groups containing a maximal sum-free set S of size 2 which also generates the group.

Proposition 4.3 *Suppose S is a maximal sum-free set of order 2 in $\langle S \rangle$.*

1. *If S contains no involutions, then $\langle S \rangle = \langle a \rangle$ for some $a \in S$ 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 $\langle S \rangle$ are given in Table 2.*

$\langle S \rangle$	$S = \{a, b\}$
$C_2 \times C_2$	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

Proof Let $S = \{a, b\}$. Suppose first that $b = a^k$ for some k. Then

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

Because $\langle S \rangle = \langle a \rangle$ is cyclic, each element of $\langle S \rangle$ has at most two square roots. Thus $|\sqrt{S}| \leq 4$. Since S is maximal sum-free in $\langle S \rangle$ Lemma 3.1 implies $\langle S \rangle = T(S) \cup \sqrt{S}$ and so $|\langle S \rangle| \leq |T(S)| + 4 \leq 12$. The cyclic groups of order up to 12 were checked by hand. The only maximal sum-free sets of order two containing a generator and no 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. (By symmetry, the same reasoning applies to the situation $a \in \langle b \rangle$.)

Suppose S contains no involution. Then by Proposition 4.2, $\langle S\rangle$ is generated by either a or b and we have already dealt with this possibility. Thus the list given in Table 1 is complete.

Suppose S contains an involution a. By Proposition 4.2, either $\langle S\rangle = \langle b\rangle$, or $o(b) \in \{2,3\}$. If $\langle S\rangle = \langle b\rangle$, then the only possibility is $\langle S\rangle = C_6$ as mentioned above. So assume $o(b) \in \{2,3\}$, and consider the element bab^{-1}. Now $o(bab^{-1}) = 2$, so $bab^{-1} \notin \sqrt{S}$. Therefore, by Lemma 3.1, $bab^{-1} \in T(S) = \{1, a, b, b^2, ab, ba, ab^{-1}, b^{-1}a\}$. 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_6 or D_6, as shown in Table 2. These are the only possibilities. $\square$

Proposition 4.3 allows us to prove Theorem 4.4, which concerns groups containing maximal sum-free sets S with the property that no proper subset of S generates $\langle S\rangle$. We show that such sets have size at most 2. Thus all examples can be found from a classification of groups containing a maximal sum-free set of size 1 or 2.

Theorem 4.4 *Suppose S is a maximal sum-free set in G such that no proper subset of S generates $\langle S\rangle$. Then $|S| \leq 2$.*

Proof Suppose $|S| \geq 3$ and no proper subset of S generates $\langle S\rangle$. By Corollary 3.12 every element of S has order 2 or 3. Proposition 3.13 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 $\langle a, b\rangle$. The possibilities for $\{a, b\}$ and $\langle a, b\rangle$ are given in Proposition 4.3. Since the orders of a and b are at most 3, $\langle a, b\rangle$ cannot be generated by a or b. Therefore 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 and b are involutions, c has order 3 and $ab = ba$. Moreover either $ca = ac$ or $ca = ac^{-1}$, and either $cb = bc$ or $cb = bc^{-1}$. So every element of $\langle S\rangle$ can be written $a^ib^jc^l$ where $i, j = 0$ or 1 and l is 0, 1 or 2. Hence $|\langle S\rangle|$ divides 12. Since $a \notin \langle b, c\rangle$, in fact $|\langle S\rangle| = 12$. If $ca = ac^{-1}$ and $cb = bc^{-1}$ then there are 9 involutions in $\langle S\rangle$. No group of order 12 contains 9 involutions (see for example [7], pg 239). Therefore we can assume that $ca = ac$. Hence $a \in Z(\langle S\rangle)$. Consider abc. Now $abc \notin T(S) = S \cup SS \cup SS^{-1} \cup S^{-1}S$, because we know $\langle S\rangle$ 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 $abc \notin \sqrt{S}$, which means $\langle S\rangle \neq T(S) \cup \sqrt{S}$. But now Lemma 3.1 implies S is not maximal sum-free in $\langle S\rangle$, a contradiction. Therefore our initial assumption, that $|S| \geq 3$, was false. Hence $|S| \leq 2$. $\square$

The last three results in this section complete the classification of groups containing maximal sum-free sets S of size 2. They deal with the cases where S contains zero, one or two involutions respectively.

Proposition 4.5 *Suppose S is a maximal sum-free set of size 2 in G such that S contains no involutions. Then either $G = \langle S \rangle$ with the possibilities as in Proposition 4.3(1), or there exists $x \in G$ with $G = \langle x \rangle \cong C_8$ and $S = \{x^2, x^6\}$.*

Proof If S is maximal sum-free in G, then S must certainly be maximal in $\langle S \rangle$. Therefore S and $\langle S \rangle$ are as described in Proposition 4.3(1). Suppose that $G \neq \langle S \rangle$. Then, by Lemma 3.1, $\hat{S}$ is nonempty. Furthermore, by Proposition 3.7, each element a of $\hat{S}$ has even order and all odd powers of a are 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 $\{a, a^{-1}\}$, so $\langle S \rangle \cong C_4$. Since $\hat{S} \subseteq \{a, a^{-1}\}$, Proposition 3.8 implies that G has order 8 or 16. Every element of $\sqrt{S}$ has order 8. If G had order 16, since $G = \langle S \rangle \cup \sqrt{S}$, 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 [7] pg 239). Therefore $|G| = 8$ and so G is cyclic. This case does yield a maximal sum-free set. Given any $x \in \sqrt{S}$ we have $G = \langle x \rangle \cong C_8$ and $S = \{x^2, x^6\}$. $\square$

Proposition 4.6 *Suppose that S is maximal sum-free of size 2 in G and that S contains exactly one involution. Then one of the following holds.*

1. *$G = \langle S \rangle \cong C_6$;*
2. *$G = \langle S \rangle \cong D_6$;*
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 Since S is maximal sum-free in G, S is also maximal in $\langle S \rangle$. By Proposition 4.3(2), writing $S = \{a, b\}$, we have $a^2 = b^3 = 1$ and either $\langle S \rangle = C_6$ or D_6. By Propositions 3.6 and 3.7, either $G = \langle S \rangle$ or $\hat{S} = \{a\}$ and $|G| = 12$. If $G = \langle S \rangle$, then we are done. Suppose $|G| = 12$. Then since $G = \langle S \rangle \cup \sqrt{S}$ and the elements of $\sqrt{S}$ not in $\langle S \rangle$ all square to a, it follows that G has six elements of order 4. The only such group is Q_{12} (see [7, p 239]), which has a unique involution and two elements of order 3, meaning there are two possibilities for S. 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. $\square$

Proposition 4.7 *Suppose that S is maximal sum-free of size 2 in G and that S contains 2 involutions. Then (G, S) is one of the pairs given in Table 3.*

G	S
$C_2 \times C_2$	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 Since S is maximal sum-free in G, S is also maximal in $\langle S\rangle$. We may write $S = \{a, b\}$ where $a^2 = 1, b^2 = 1$ and $ab = ba$ by Proposition 4.3. Since by Lemma 3.1 $G = \langle S\rangle \cup \sqrt{S}$, either $G = \langle S\rangle \cong C_2 \times C_2$ or $\sqrt{S}\backslash\langle S\rangle \neq \varnothing$. Suppose there exists $g \in \sqrt{S}\backslash\langle S\rangle = G\backslash\langle S\rangle$. Without loss of generality, $g \in \sqrt{a}$. Then $gb \in G\backslash\langle S\rangle$ and since $(gb)^2 \neq b$ it follows that $(gb)^2 = a = g^2$. Thus $gb = bg$ and so $S \subseteq C_G(g)$. Consequently $S \subseteq Z(G)$.

Suppose $x, y \in \sqrt{S}\backslash\langle S\rangle$ with $y \notin x\langle S\rangle$. Then $xy \notin \langle S\rangle$ and so $xy \in \sqrt{S}$. Thus $xyxy = s$ for some $s \in S$. Rearranging gives $yx = x^{-1}sy^{-1} = xx^2syy^2$, since $o(x) = o(y) = 4$. Now x^2 and y^2, as elements of S, are central in G 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 $x_1\langle S\rangle, x_2\langle S\rangle, x_3\langle S\rangle$ are three distinct non-trivial cosets of $\langle S\rangle$. Then $(x_1x_2x_3)^2 = x_1x_2x_3x_1x_2x_3 = x_1^2(x_2x_3)^2s_1s_2$ for some $s_i \in S$. At least two of x_1^2, $(x_2x_3)^2$, s_1 and s_2 are the same and thus cancel. Therefore $(x_1x_2x_3)^2 \in \{1, ab\}$, forcing $x_1x_2x_3 \in \langle S\rangle$ and hence by Proposition 3.2 $(x_1\langle S\rangle)(x_2\langle S\rangle) = x_3\langle S\rangle$. In other words the factor group $G/\langle S\rangle$ 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 $G = \langle S\rangle \cup x\langle S\rangle$ and $\langle S\rangle \subseteq Z(G)$. 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 $G = \langle S\rangle \cup x\langle S\rangle \cup y\langle S\rangle \cup xy\langle S\rangle$ for $x \in \sqrt{a}$ and $y \in \sqrt{S}$. Note that $xy \neq yx$, since $xy = yx$ implies $(xy)^2 = x^2y^2 \in \{1, ab\}$, and so $xy \in G \setminus (\langle S\rangle \cup \sqrt{S})$, contradicting Lemma 3.1. Hence G is not abelian; in fact $Z(G) = \langle S\rangle \cong C_2 \times C_2$. There are only two non-abelian groups of order 16 with 3 involutions and centre $C_2 \times C_2$ (see [7], pg 239), 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 Proposition 4.7. Both these groups contain 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. □

5 Maximal sum-free sets of size 3

Theorem 4.4 tells us that if S is maximal sum-free and no proper subset of S generates $\langle S\rangle$, then $|S| \leq 2$. In this section our goal is to prove Theorem 5.6, in which we classify all the maximal sum-free sets S of size 3 for which at least one two-element subset does not generate $\langle S\rangle$. In other words, those S for which there exists $a \in S$ such that $a \notin \langle S \setminus \{a\}\rangle$. In view of Corollary 3.10, it is natural to look for sum-free sets of size $k = 3$ in groups of order up to $4k^2 + 1 = 37$. Maximal sum-free sets of size 3 might still possibly exist in groups of order more than 37 but we conjecture that they do not; see the end of the section.

Theorem 5.1 *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 5.*

Proof The maximal sum-free sets of size 3 for groups of order up to 37 were checked using the computer algebra package GAP [8], using the 'AllSmallGroups' command. As can be seen from the final column of Table 5, there may be more than one set in the group of the form given. One set is listed for each form. So for example if $G \cong C_9$ then for some generator g of G, either $S = \{g, g^3, g^8\}$ or $S = \{g, g^4, g^7\}$. $\square$

Corollary 5.2 is an immediate consequence of Theorem 5.1 and Corollary 3.10.

Corollary 5.2 *If S is a 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 5.*

Theorem 5.1 also allows us to bound $|\langle S\rangle|$ in the case of maximal sum-free sets S of size three for which $\langle S\rangle$ is cyclic. The bound is required in the proof of Theorem 5.6.

Corollary 5.3 *Suppose S is maximal sum-free set of size 3 in $\langle S\rangle$. If $\langle S\rangle$ is cyclic, then $|\langle S\rangle| \leq 15$.*

Proof Using the fact that $\langle S\rangle$ is abelian, we see that $T(S) = S \cup SS \cup SS^{-1}$ and hence that $|T(S)| \leq 21$. Since $\langle S\rangle$ is cyclic, each element has at most two square roots. Therefore $|\sqrt{S} \cap \langle S\rangle| \leq 6$. Hence, by Lemma 3.1, $|\langle S\rangle| \leq 27$. From Table 5 we see that the largest possibility that actually occurs is C_{15}. Hence $|\langle S\rangle| \leq 15$. $\square$

For the rest of the section we concentrate on the case where S is a 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 5.6.

Proposition 5.4 *Suppose S is maximal sum-free of size 3 in G and a is an element of S for which $a \notin \langle S \setminus \{a\}\rangle$. If $o(a) = 2$, then $|G| \leq 32$.*

Proof Write $S = \{a, b, c\}$. By Proposition 3.13, $\{b, c\}$ is maximal sum-free in $\langle b, c\rangle$. The possibilities for $\{b, c\}$ are given in Proposition 4.3.

First, consider the case where $c \in \langle b\rangle$, so $S = \{a, b, b^i\}$ for some i and by Proposition 4.3, $o(b) \in \{4, 5, 6, 7, 8\}$. Now $b^{-1}ab$ is an involution, so cannot lie in $\sqrt{S}$. Thus by Lemma 3.1, $b^{-1}ab \in T(S)$. Given that $a \notin \langle b\rangle$, we get $b^{-1}ab \in \{a, ab, ba, b^{-i}a, b^i a\}$. Note that we do not need to consider ab^{-i} or ab^i, since if these are involutions, then $ab^{-i} = b^i a$ and $ab^i = b^{-i}a$.

Now $b^{-1}ab = ab$ is impossible. The other four possibilities imply that $ab = b^j a$ for some integer j. Hence every element of $\langle S\rangle$ can be written $b^l a^\varepsilon$ for $0 \leq l < o(b)$ and $\varepsilon \in \{0, 1\}$. Therefore $|\langle S\rangle| \leq 2o(b)$ and since $a \notin \langle b\rangle$ we have $|\langle S\rangle| = 2o(b)$. Suppose first that $o(b) = 4$ and consider ab^2. By Proposition 4.3(1), $c = b^{-1}$, so $ab^2 \notin T(S)$, 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 $o(b) \geq 5$. Now Proposition 3.7 states that all elements s of $\hat{S}$ have even order and moreover that all odd powers of s lie in S. Considering the remaining possible orders of b and corresponding values of i given in Proposition 4.3 we quickly see that $\hat{S} \subseteq \{a\}$. Therefore, by Proposition 3.6, $|G| \leq 2|\langle S\rangle| = 4o(b) \leq 32$.

We have shown that if $c \in \langle b \rangle$, then $|G| \leq 32$. By symmetry if $b \in \langle c \rangle$, then $|G| \leq 32$. It remains to consider the case $\langle b \rangle \neq \langle b, c \rangle \neq \langle c \rangle$. Then, by Proposition 4.2, we may assume $o(b) = 2$ and $o(c) \in \{2, 3\}$. Proposition 4.3 implies that $\langle b, c \rangle$ is either abelian or isomorphic to D_6. Furthermore by Theorem 4.4, at least one proper subset of S generates $\langle S \rangle$. So either $b \in \langle a, c \rangle$ or $c \in \langle a, b \rangle$. If $o(c) = o(b) = 2$, then without loss of generality, $c \in \langle a, b \rangle$. Therefore we may assume that either $c \in \langle a, b \rangle$ or both $o(c) = 3$ and $c \notin \langle a, b \rangle$.

For a contradiction, assume that $o(c) = 3$ and $c \notin \langle a, b \rangle$. Then $b \in \langle a, c \rangle$. Moreover, by Proposition 3.13, $\{a, b\}$ is maximal sum-free in $\langle a, b \rangle$. Since a and b are both involutions, we must have $\langle a, b \rangle \cong C_2 \times C_2$, and in particular $ab = ba$. We also know, from the fact that $\{b, c\}$ is maximal sum-free in $\langle b, c \rangle$, that either $bc = cb$ or $cb = bc^{-1}$. A quick calculation shows that

$$T(S) = \{1, a, b, c, c^2, ab, bc, cb, bc^{-1}, c^{-1}b, ac, ca, ac^{-1}, ca^{-1}\}.$$

Let $x \in G$ and suppose that $o(x) = 3^i$ for some $i \geq 1$. If $x \in T(S)$, then $x \in \{c, c^2, ac, ca, ac^{-1}, ca^{-1}\}$. Otherwise $x \in \sqrt{S}$ by Lemma 3.1. But then since $o(a) = o(b) = 2$ we must have $x^2 = c$, forcing $x = x^4 = c^2 \in T(S)$. Therefore there are at most 6 non-trivial elements of Sylow 3-subgroups of G. By Sylow's Theorems, the number of Sylow subgroups is either 1 or at least 4. An elementary counting argument shows that there is a unique Sylow 3-subgroup of order 3, namely $\langle c \rangle$. This subgroup is therefore normal and hence either $ac = ca$ or $ac = c^{-1}a$. But then $|\langle a, c \rangle| = 6$. But the subgroup $\langle a, b \rangle$ of $\langle a, c \rangle$ has order 4, a contradiction.

It now remains to deal with the case $c \in \langle a, b \rangle$. Since a and b are both involutions, $\langle a, b \rangle = \langle S \rangle$ is dihedral. Now a and b lie in the non-trivial coset of the cyclic subgroup $\langle ab \rangle$ of index 2 in $\langle S \rangle$. This coset is sum-free, so if c also lies in the coset, then the fact that S is maximal forces $|\langle ab \rangle| = 3$. That is, $\langle S \rangle \cong D_6$. However we would then have $a = bcb \in \langle b, c \rangle$, contrary to our hypothesis. Hence $c = (ab)^i$ for some $i > 1$. The fact that $\{a, b, c\}$ and $\{a, b, aba\}$ are sum-free but $\{a, b, aba, c\}$ is not forces $c \in \{abab, baba\}$. Recalling that $o(c) \leq 3$, we have $\langle S \rangle \cong D_8$ or $\langle S \rangle \cong D_{12}$. However in D_{12}, $(ab)^3 \in \{abc, bac\}$ is an involution not contained in $T(S)$, which is impossible by Lemma 3.1. Therefore $\langle S \rangle = \langle a, b \rangle \cong D_8$, where $(ab)^4 = 1$ and $c = (ab)^2$. Suppose $x \in \sqrt{a}$. Then $(bxb)^2 = bab \notin S$. Thus $bxb \in T(S)$ and hence $x \in \langle S \rangle$. Therefore $\sqrt{a} \subseteq \langle S \rangle$ and similarly $\sqrt{b} \subseteq \langle S \rangle$. Hence $\hat{S} \subseteq \{c\}$ and therefore, by Proposition 3.6, $|G| \leq 16$. We have now shown that in all cases where $o(a) = 2$, $|G| \leq 32$. □

Proposition 5.5 *Suppose S is maximal sum-free of size 3 in G and a is an element of S for which $a \notin \langle S \setminus \{a\} \rangle$. If $o(a) = 3$ and $S = \{a, b, b^{-1}\}$ for some $b \in G$, then $|G| \leq 21$.*

Proof By Proposition 3.13, $\{b, b^{-1}\}$ is maximal sum-free in $\langle b \rangle$. Hence by Proposition 4.3, $o(b) \in \{4, 5, 7\}$. Here

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

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 $x = x^4 = a^2 \in T(S)$. Hence the elements of order 3^i lie in $T(S)$. 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 $o(b^{-1}a) = o(ab^{-1}) = o(a^{-1}b) = o(ba^{-1})$. Let

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

Now the Sylow 3-subgroups must have order 3 or 9. By Sylow's Theorems 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 $|U| = 6$. However if any pair of elements in U is equal then it is easy to check that either $a \in \langle b\rangle$ or $|U| \leq 4$, a contradiction. 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, including a and a^2, which means again that $|U| = 6$, which is impossible. 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 $\langle S\rangle$ can be written $b^i a^j$ for $0 \leq i < o(b)$ and $0 \leq j < 3$. So $|\langle S\rangle| \leq 3o(b)$ and as $a \notin \langle b\rangle$ we have $|\langle S\rangle| = 3o(b)$. Suppose that $o(b) = 4$. Then $|\langle S\rangle| = 12$. Now $ab^2 \notin T(S)$, so (by Lemma 3.1) $ab^2 \in \sqrt{S}$. But $(ab^2)^2 = ab^2ab^2 = ab^{-2}ab^2 \in \{1, a^2\}$, a contradiction. Hence $o(b) \neq 4$, so $o(b)$ is odd. Now Proposition 3.7 implies that $\langle S\rangle = G$. Hence $|G| \leq 21$. □

Theorem 5.6 *The only examples of maximal sum-free sets S of size 3 for which not every proper two-element subset of S generates $\langle S\rangle$ are those given in Table 4.*

G		S	$\langle S\rangle$	$\#S$
$\langle g, h : g^4 = h^2 = 1, hgh^{-1} = g^{-1}\rangle$	$\cong D_8$	$\{h, gh, g^2\}$	$\cong D_8$	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	$\cong A_4$	$\{z, x, y : x^2 = y^2 = z^3 = 1\}$	$\cong A_4$	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 4: Maximal sum-free sets $S = \{a_1, a_2, a_3\}$ with $a_1 \notin \langle a_2, a_3\rangle$.

Proof Suppose S is maximal sum-free in G, that $|S| = 3$ and that not every proper two-element subset of S generates $\langle S\rangle$. Then there exists $a \in S$ for which $a \notin \langle S \setminus \{a\}\rangle$. We will show that $|G| \leq 37$. By Proposition 3.11, 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 5.4 implies $|G| \leq 32$. If $o(a) = 3$, then either $S \cap S^{-1} = \varnothing$ or $S = \{a, b, b^{-1}\}$. By Corollary 3.10 and Proposition 5.5, $|G| \leq 37$. It remains to consider the case where $o(a)$ is even, greater than 4 and $a^{-2} \in S$. Then $S = \{a, a^{-2}, b\}$ for some $b \in G$. If $S \cap S^{-1} = \varnothing$, then by Corollary 3.10, $|G| \leq 37$. So suppose $S \cap S^{-1}$ is non-empty. Now $S^{-1} = \{a^{-1}, a^2, b^{-1}\}$. Clearly $a^{-1} \notin S$, since this would imply $a^{-2} \in S \cap SS$, contradicting the fact that S is sum-free. Similarly $a^2 \notin S$. Therefore $b = b^{-1}$. If $b \notin \langle a\rangle$, then by Proposition 5.4, $|G| \leq 32$. So suppose $b \in \langle a\rangle$. Then $\langle S\rangle$ is cyclic, so by Corollary 5.3, $|\langle S\rangle| \leq 15$. Next we consider $\hat{S}$. By

Proposition 3.7, if $a \in \hat{S}$ then every odd power of a lies in S. In particular, $a^{-1} \in S$, a contradiction. Similarly $a^{-2} \in \hat{S}$ implies $a^2 \in S$, another contradiction. Hence $|\hat{S}| \leq 1$. Thus either $G = \langle S \rangle$ or, by Proposition 3.6, $|G| = 2|\langle S \rangle|$. In either case $|G| \leq 2 \cdot 15 = 30$. Therefore, again, $|G| \leq 37$. By Theorem 5.1, (G, S) is one of the pairs given in Table 5. However in some of these cases, every proper subset of S generates $\langle S \rangle$. Table 4 lists the examples for which not every proper subset of S generates $\langle S \rangle$. In each case the first element of S as listed in the table is not contained in the span of the other two elements. □

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. We are led to the following conjecture.

Conjecture 5.7 *If G is a group of order greater than 24 than G does not contain a maximal sum-free set of size 3.*

If G is a group of order greater than 24 with a maximal sum-free set S of size 3 then by Theorem 5.6, $\langle S \rangle = \langle a, b \rangle$ for any $a, b \in S$. Corollary 5.3 implies that $\langle S \rangle$ is not cyclic and so if $a \in S$ is of order at least 3 then $a^{-1} \notin S$. Corollary 5.2 then implies that S contains an involution.

Acknowledgements: The authors would like to thank the referee whose comments and suggestions greatly improved the quality of the paper.

G		S	$\langle S\rangle$	#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	$= A_4$	$\{x, y, z : x^2 = y^2 = z^3 = 1\}$	$= A_4$	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
$\langle g, h : g^3 = h^7 = 1, ghg^{-1} = h^2\rangle$	$\cong C_7 \rtimes C_3$	$\{gh, gh^{-1}, g^{-1}\}$	$\cong C_7 \rtimes C_3$	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 5: Maximal sum-free sets in groups of order up to 37

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. Erdős, *On the number of sets of integers with various properties*, Number theory (Banff, AB, 1988), 61–79, de Gruyter, Berlin, 1990.

[3] W. T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. 17 (2008), no. 3, 363–387.

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

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

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

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

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

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

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

[11] 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.

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

[13] 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.