Journal der mathematischen Ablehnungen
Paper No.28 (2013)

Subsets of finite groups exhibiting additive regularity

Robert S. Coulter[1] and Todd Gutekunst[2]

[1]Department of Mathematical Sciences, University of Delaware, Newark, DE, 19716, USA.
[2]Department of Mathematics, King's College, Wilkes-Barre, PA, 18711, USA.

AMS Subject class: 05E15

Keywords: sum set, additive regularity, difference set, Frobenius group

Abstract

In this article we aim to develop from first principles a theory of sum sets and partial sum sets, which are defined analogously to difference sets and partial difference sets. We obtain non-existence results and characterisations. In particular, we show that any sum set must exhibit higher-order regularity and that an abelian sum set is necessarily a reversible difference set. We next develop several general construction techniques under the hypothesis that the over-riding group contains a normal subgroup of order 2. Finally, by exploiting properties of dihedral groups and Frobenius groups, several infinite classes of sum sets and partial sum sets are introduced.

§ 1. Introduction

In [1], the authors used versions of additive regularity of subsets of groups to obtain new results on skew Hadamard difference sets. For instance, by exploiting the additive regularity of skew Hadamard difference sets we were able to completely categorise their full multiplier group, see [1], Theorem 4.2. Motivated, in part, by these results, in this article we treat sum sets and partial sum sets as combinatorial objects in their own right. Moreover, in keeping with the "keep it simple" philosophy we adopted in [1], we approach our topic with the intention of using as little heavy machinery as possible. For example, we find we are able to manage without character theory, though we readily acknowledge that, in one or two places, such theory may allow shorter, if possibly less illuminating, proofs.

Let G be a finite group, and let S be a subset of G. We shall be interested in counting the number of ways an element of G can be generated as "a product in S" (that is, as the product of two elements of S). If S is an arbitrary subset, then we should expect some elements of G to be generated more often than others. Indeed, some elements may be generated very often while others are not generated at all. If, however, the number of ways of generating elements of G takes very few values, we say the subset S possesses *additive regularity*. To make this concept more precise, we make the following definition.

Definition 1.1. *Let G be a group of order v and let S be a subset of G with $|S| = k$. We say S is a (v, k, λ, μ)* **partial sum set** *if every nonidentity element in S can be written in precisely λ ways as a product in S while every nonidentity element not in S can be written in precisely μ ways as a product in S. If $\lambda = \mu$, then S is called a (v, k, μ)* **sum set**. *The numbers (v, k, λ, μ) are the* **parameters** *of S.*

Readers familiar with (v, k, λ) difference sets will note how similar the definition of a sum set is to that of a difference set, and it is because of this similarity that we choose to speak of "sum sets" instead of "product sets". The use of the term "difference set" is historical, as the earliest investigations of difference sets focused entirely on cyclic groups, where additive notation is natural. The name was maintained, even when mathematicians began constructing examples in arbitrary groups.

Sum sets as presently defined were previously studied in [5] and [7] as particular examples of "addition sets". Proper acknowledgement is made wherever the current work coincides with these papers' results.

It is easily checked that the set-theoretic complement of a sum set is a sum set. Specifically, if $S \subset G$ is a (v, k, μ) sum set, then $G \setminus S$ is a $(v, v-k, v-2k+\mu)$ sum set. Hence we restrict our attention to sum sets of size $k \leq \frac{v}{2}$.

Note the empty set is a $(v, 0, 0)$ sum set. Also, if $g \in G$, then the singleton $\{g\}$ is a $(v, 1, 0)$ sum set if and only if $o(g) \leq 2$. These sum sets and their complements are deemed trivial examples. Henceforth all sum sets are understood to be nontrivial.

The parameters (v, k, μ) of a sum set must satisfy

$$k^2 = \mu(v-1) + |S \cap S^{(-1)}|, \tag{1}$$

where $S^{(-1)} = \{s^{-1} : s \in S\}$. Any triple of nonnegative integers (v, k, μ) with $v > k > \mu$ induce a unique value for $|S \cap S^{(-1)}|$ with respect to (1). If that value is between 0 and k, we say the triple (v, k, μ) are *admissible parameters* for a sum set. Of course, if (v, k, μ) is admissible, it is not necessarily true that there exists a sum set with these parameters. In what follows, the quantity $|S \cap S^{(-1)}| - \mu$ appears frequently enough to warrant its own symbol, so we define $n := |S \cap S^{(-1)}| - \mu$.

The primary goal of this paper is to offer a foundation for a comprehensive theory of sum sets. The theory is built upon the dual goals of providing theoretical construction techniques which encompass all known examples while simultaneously deriving nonexistence results to explain why there are no other examples. Some of the theory is based on results from [1], and we recall the relevant results in Section 2. Nonexistence results are obtained in Sections 3 and 4, where we also derive from first principles a theoretical basis for the study of sum sets. Some general constructions are given in Section 5, which we then use to construct several infinite families of sum sets in Sections 6 and 7.

§ 2. Special subsets

In [1], the authors introduce the notion of *special subsets* and use them to explore the additive properties of skew Hadamard difference sets. These special subsets provide a useful mechanism for studying sum sets, so we now recall some basic facts about them.

Let S be a subset of G. If $S = S^{(-1)}$ we say S is *reversible*. If $S \cap S^{(-1)} = \varnothing$ we say S is *skew*. A a skew subset of G not properly contained in any other skew subset of G is called a *maximal skew set*. If $v = o(G)$ is odd, then any maximal skew set in G has size $\frac{v-1}{2}$. For any $a \in G$, the *special subsets* of S with respect to a are

$$\begin{aligned}
\mathcal{A}_{a,S} &= \{x \in S : a = xy^{-1} \text{ for some } y \in S\},\\
\mathcal{B}_{a,S} &= \{y \in S : a = xy^{-1} \text{ for some } x \in S\},\\
\mathcal{C}_{a,S} &= \{x \in S : a = xy \text{ for some } y \in S\}.
\end{aligned}$$

The cardinality $|\mathcal{A}_{a,S}|$ counts the number of ways to write a as a quotient in S, so in this context S is a difference set set if and only if $|\mathcal{A}_{a,S}|$ is constant for all nonidentity elements $a \in G$. Similarly S is a sum set if and only if $|\mathcal{C}_{a,S}|$ is constant for all nonidentity elements $a \in G$. The following lemma is a summary of Lemmas 2.1, 2.2, and 2.4 in [1].

Lemma 2.1. *Let S be a subset of the group G.*

(i) $\mathcal{A}_{a,S} \cap \mathcal{C}_{a,S} = \varnothing$ for all $a \in G$ if and only if S is skew.

(ii) $\mathcal{A}_{a,S} = \mathcal{C}_{a,S}$ for all $a \in G$ if and only if S is reversible.

(iii) Suppose G has odd order v, and suppose S is a maximal skew set in G. Then

$$|\mathcal{A}_{a,S}| + |\mathcal{C}_{a,S}| = \begin{cases} \frac{v-3}{2} & \text{if } a \in S, \\ \frac{v-1}{2} & \text{if } a \notin S. \end{cases}$$

It is natural to ask whether a difference set may also be a sum set or a partial sum set. The former question is completely answered, and in the latter case we know of one family of difference sets that are also partial sum sets.

Theorem 2.2. *Let G be a group of order v, and let $S \subset G$. Then any two of the following statements imply the third.*

(i) S is a (v, k, λ) difference set.

(ii) S is a (v, k, μ) sum set.

(iii) $S = S^{(-1)}$.

In particular, a (v, k, λ) difference set S is also a sum set if and only if $S = S^{(-1)}$.

Proof. Suppose (i) and (ii) hold. Then the integers (v, k, λ) satisfy

$$k^2 = \lambda(v-1) + k,$$

as S is a difference set. At the same time, the integers (v, k, μ) must satisfy

$$k^2 = \mu(v-1) + |S \cap S^{(-1)}|,$$

as S is a sum set. If $\mu = \lambda$, then $k = |S \cap S^{(-1)}|$ and so $S = S^{(-1)}$. If $\mu \neq \lambda$, then combining these two equations we have

$$(\mu - \lambda)(v-1) = k - |S \cap S^{(-1)}|.$$

Now $0 \leq |S \cap S^{(-1)}| \leq k$, so $0 \leq k - |S \cap S^{(-1)}| \leq k$. Since $v-1$ divides $k - |S \cap S^{(-1)}|$ and $k \leq v/2$, we must have $k - |S \cap S^{(-1)}| = 0$. Hence $|S \cap S^{(-1)}| = k$, so $S = S^{(-1)}$.

If (i) and (iii) hold, then S is reversible, so by Lemma 2.1, $|\mathcal{C}_{a,S}| = |\mathcal{A}_{a,S}|$ for all nonidentity elements $a \in G$. Hence S is a sum set with $\mu = \lambda$. Similarly, if (ii) and (iii) hold, then by Lemma 2.1 S is a difference set with $\lambda = \mu$.

The final statement, which also follows from Corollary 2.5 in [7], is now clear. □

The next theorem appears as Theorem 3.1 in [1].

Theorem 2.3. *A (v, k, λ) skew Hadamard difference set is a $(v, k, \lambda, \lambda+1)$ partial sum set.*

§ 3. Nonexistence and restriction of admissible parameters

We begin with a basic observation regarding sum sets in an arbitrary group G. Whenever a sum set contains a pair of commuting elements, their product is generated at least twice. More formally, we have the following:

Lemma 3.1. *If a (v, k, μ) sum set $S \subset G$ contains a pair of commuting elements, then $\mu \geq 2$. In particular, if G is abelian, then μ is even.*

Proof. The first claim is obvious. Suppose G is abelian, and suppose $S \subset G$ is a (v, k, μ) sum set with μ odd. Form all possible products of two distinct elements of S. In doing so, each element of G is generated some even number of times. To satisfy μ odd, there must then be at least one element $s \in S$ for each nonidentity $g \in G$ such that $s^2 = g$. This is possible only if $|S| \geq v - 1$, so S is a trivial sum set. □

This simple lemma is enough to restrict a large class of groups from admitting sum sets.

Theorem 3.2. *An abelian group of odd order admits no sum sets.*

Proof. Let G be an abelian group of order v, with v odd. Suppose S is a (v, k, μ) sum set in G. Since 2 does not divide v, the elements x^2 with $x \in S$ are all distinct. It follows that the number of ways to write any such element as a product in S must be odd, contradicting the fact that μ must be even. □

The results established thus far allow us to reject certain admissible parameters (v, k, μ), or at least to rule out certain groups of order v from admitting sum sets. To extend our ability to restrict parameters, we now consider how the existence of normal subgroups can affect whether a group may admit sum sets. In particular, we consider how S may be partitioned by the cosets of a normal subgroup.

Suppose G is a group admitting a $(o(G), k, \mu)$ sum set S. Further suppose that N is a normal subgroup of G. Let H be a group isomorphic to the quotient group G/N and label the cosets of N in G by N_α, $\alpha \in H$, so that $N_\alpha N_\beta = N_{\alpha\beta}$. For each $\alpha \in H$, set $X_\alpha = |S \cap N_\alpha|$. Note that

$$\sum_{\alpha \in H} X_\alpha = k. \tag{2}$$

As S is a sum set, any nonidentity element $g \in G$ is generated μ times as a product in S. Suppose $g \in N_\beta$ and $g = ab$ for some elements $a, b \in S$. If $a \in N_\alpha$, then we must have $b \in N_{\alpha^{-1}\beta}$. Now if $\beta \neq 1$, then $1 \notin N_\beta$. Hence, every element of N_β is generated precisely μ times as a product in S. But if $\beta = 1$, then each nonidentity element of N_1 is generated μ times as a product in S while 1 is generated $|S \cap S^{-1}|$ times. Thus,

$$\sum_{\alpha \in H} X_\alpha X_{\alpha^{-1}\beta} = \begin{cases} \mu o(N) & \text{if } \beta \neq 1, \\ \mu o(N) + |S \cap S^{(-1)}| - \mu & \text{if } \beta = 1. \end{cases} \tag{3}$$

We may rewrite (1) as

$$|S \cap S^{(-1)}| - \mu = k^2 - \mu v.$$

Noting $n = |S \cap S^{(-1)}| - \mu$ $(= k^2 - \mu v)$, (3) has the following equivalent formulation:

$$\sum_{\alpha \in H} X_\alpha X_{\alpha^{-1}\beta} = \begin{cases} \mu o(N) & \text{if } \beta \neq 1, \\ \mu o(N) + n & \text{if } \beta = 1. \end{cases} \tag{4}$$

We note that as β varies over H, (4) yields a system of $o(H)$ equations that effectively partitions (1). The sum of their left-hand sides is

$$\left(\sum_{\alpha \in H} X_\alpha \right)^2,$$

which is simply k^2 by (2). Their right-hand sides, meanwhile, sum to $\mu o(N) i_G(N) + n$, which equals $\mu(o(G) - 1) + |S \cap S^{(-1)}|$.

The following is a consequence of (4):

Lemma 3.3. *Let G be a group with $N \lhd G$ and $S \subset G$ a sum set. If the center of G/N contains some element which is not a square of any element in G/N, then $\mu o(N)$ must be even.*

Proof. Set $H = G/N$ as above, and suppose $\beta \in Z(H)$ is not a square; i.e. the equation $x^2 = \beta$ has no solution in H. Clearly $\beta \neq 1$. As $\beta \in Z(H)$,

$$N_\alpha N_{\alpha^{-1}\beta} = N_{\alpha^{-1}\beta} N_\alpha = N_\beta$$

for each $\alpha \in H$. Correspondingly, whenever the term $X_\alpha X_{\alpha^{-1}\beta}$ appears on the left-hand side of (4), so too does the (equal) term $X_{\alpha^{-1}\beta} X_\alpha$. Moreover, since β is not a square, no term of the form X_γ^2 appears on the left-hand side of (4). It follows that the left-hand side of (4) is divisible by 2, proving the claim. □

We now consider the possible values of X_α. That is, if a nonsimple group admits a sum set S, how may that sum set be distributed over the cosets of some normal subgroup N? We consider the situation where the intersection sizes X_α take only two values. That is, suppose $M \subseteq H$ such that

$$X_\alpha = \begin{cases} m & \text{if } \alpha \in M, \\ l & \text{if } \alpha \notin M. \end{cases}$$

With only two values for X_α, (2) reduces to

$$m|M| + l(o(H) - |M|) = k.$$

We will count $\sum_{\alpha \in H} X_\alpha X_{\alpha^{-1}\beta}$ in a different way and compare the result to (4). Before counting, it will be useful to define the set $M_\beta = \{\beta\gamma^{-1} : \gamma \in M\}$. Note that for any $\beta \in H$, $\alpha \in M_\beta$ if and only if $\alpha^{-1}\beta \in M$. In particular, $M \cap M_\beta = \mathcal{C}_{\beta,M}$. We have

$$\begin{aligned}
\sum_{\alpha \in H} X_\alpha X_{\alpha^{-1}\beta} &= \sum_{\alpha \in M} m X_{\alpha^{-1}\beta} + \sum_{\alpha \notin M} l X_{\alpha^{-1}\beta} \\
&= \sum_{\alpha \in M \cap M_\beta} m^2 + \sum_{\alpha \in M \setminus M_\beta} ml + \sum_{\alpha \in M_\beta \setminus M} lm + \sum_{\alpha \in H \setminus (M \cup M_\beta)} l^2 \\
&= |\mathcal{C}_{\beta,M}| m^2 + 2(|M| - |\mathcal{C}_{\beta,M}|) ml + (o(H) - 2|M| + |\mathcal{C}_{\beta,M}|) l^2 \\
&= |\mathcal{C}_{\beta,M}| (m-l)^2 + 2|M| ml + o(H) l^2 - 2|M| l^2 \\
&= |\mathcal{C}_{\beta,M}| (m-l)^2 + 2[k + |M| l - o(H) l] l + o(H) l^2 - 2|M| l^2 \\
&= |\mathcal{C}_{\beta,M}| (m-l)^2 + 2kl - o(H) l^2
\end{aligned}$$

Combined with (4), we have

$$|\mathcal{C}_{\beta,M}| (m-l)^2 + 2kl - o(H) l^2 = \begin{cases} \mu o(N) & \text{if } \beta \neq 1, \\ \mu o(N) + n & \text{if } \beta = 1. \end{cases} \tag{5}$$

Equation 5 has several immediate implications, which we summarize in a theorem.

Theorem 3.4.

(i) $|\mathcal{C}_{\beta,M}| = \omega$ *is constant for all* $\beta \neq 1$. *Hence,* M *is a* $(o(H), |M|, \omega)$ *sum set in* H. *In particular,* M *is a subgroup of* H *if and only if* $M = \{1\}$ *or* $M = H$.

(ii) $n = (|\mathcal{C}_{1,M}| - \omega)(m-l)^2$.

(iii) If $M = \{1\}$, *then*

$$l = \frac{k \pm \sqrt{n}}{o(H)}.$$

In particular n *must be a square. Moreover, the parameters of the complementary sum set satisfy the same equation with the opposite sign chosen.*

(iv) If $M = H$, then $n = 0$ and $m = \frac{\mu o(N)}{k}$.

Proof. That M is a $(o(H), |M|, \omega)$ sum set in H is clear. Hence, M is a subgroup of H only if M is a trivial subgroup, i.e. $M = \{1\}$ or $M = H$, in which case M is a trivial sum set as well. This proves the first claim.

To prove the second claim, simply subtract (5) with $\beta = 1$ from the same equation with $\beta \neq 1$.

For the third claim, note the condition $M = \{1\}$ is equivalent to $|\mathcal{C}_{\beta,M}| = 0$ for all $\beta \neq 1$. Substituting into (5), we get

$$2kl - o(H)l^2 = \mu o(N).$$

Solving this quadratic for l yields the claimed result. That n must be a square is clear since l must be an integer. Considering the complement easily verifies the remainder of the third claim.

Finally, suppose $M = H$. Then we must have $m = l$, so the first term in (5) vanishes, rendering the left-hand side independent of β. It follows that $n = 0$. Hence, for any $\beta \in H$ we have

$$2km - o(H)m^2 = \mu o(N).$$

But we also have $k = o(H)m$, and substituting yields $km = \mu o(N)$. The last claim follows. □

On the surface, the most tantalizing outcome of Theorem 3.4 is that even distribution of a sum set over the cosets of a normal subgroup induces a sum set in the corresponding quotient group. The sum sets in the quotient group may be trivial, however, though even then we can deduce much about the original sum set in G.

Consider a group G which has a normal subgroup N of index 2. As there are only two cosets of N in G, any sum set S in G must intersect the cosets of N in at most two values. Regardless of how S is distributed among the cosets, the corresponding sum set in the quotient group will be trivial (as the quotient group has order 2). Nonetheless, the fact that there can be at most two intersection sizes of S with cosets of N leads to a restriction of the possible parameters of any sum set in G:

Theorem 3.5. *Suppose S is a (v, k, μ) sum set in G. If G has a normal subgroup N of index 2, then n is a square. In particular, if k is odd, then n must be a nonzero square.*

Proof. Let $G/N = \{N_1, N_\beta\}$, so $H = \{1, \beta\}$. If $X_1 = X_\beta$, then necessarily $X_1 = X_\beta = \frac{k}{2}$ and $n = 0$. If $X_1 \neq X_\beta$, then without loss of generality $M = \{1\}$, hence n is a square. If k is odd, then the first conclusion is impossible, and the second conclusion is possible only if n is nonzero. □

It should be noted Sumner and Butson [7] prove that the parameter n is necessarily a square, though possibly $n = 0$. We include the above somewhat weaker result as it follows very naturally and directly from our discussion.

We may obtain similar results under the assumption that G has a normal subgroup of index 3. If a sum set intersects the three cosets of this subgroup in at most 2 distinct amounts, then Theorem 3.4 applies. If the sum set intersects the cosets in three distinct amounts, we obtain the following.

Theorem 3.6. *Suppose S is a (v, k, μ) sum set in G, and suppose G possesses a normal subgroup N of index 3. If S intersects the cosets of N in G in three distinct values, then 3 divides k, $|S \cap N| = \frac{k}{3}$, and $n = -3x^2$ for some integer $x \neq 0$.*

Proof. Since N has index 3 in G, $H = \{1, h, h^2\}$, the cyclic group of order 3. Applying (4) to the cases $\beta = h$ and $\beta = h^2$, we obtain

$$X_{h^2}^2 + 2X_1X_h = \mu o(N),$$
$$X_h^2 + 2X_1X_{h^2} = \mu o(N),$$

respectively. Combined, these equations yield

$$X_h^2 - X_{h^2}^2 = 2X_1(X_h - X_{h^2}).$$

By assumption $X_h \neq X_{h^2}$ so we may divide by $X_h - X_{h^2}$ to obtain

$$X_h + X_{h^2} = 2X_1.$$

But we also know $X_1 + X_h + X_{h^2} = k$, hence $|S \cap N| = X_1 = \frac{k}{3}$.

Set $X_h = \frac{k}{3} + x$ for some integer $x \neq 0$ so that $X_{h^2} = \frac{k}{3} - x$. Substituting these values for X_h and X_{h^2} into $X_{h^2}^2 + 2X_1X_h = \mu o(N)$, we obtain

$$\mu o(N) - \frac{k^2}{3} = x^2,$$

which is equivalent to the final claim. □

§ 4. Higher-order regularity and Abelian Sum Sets

Whenever we have said an element a can be generated "as a product in S", it has been implied there exist elements $x, y \in S$ such that $a = xy$. In other words, we have only considered the notion of writing an element as the product of two elements of our set S. One might wonder whether our notion of additive regularity can be extended to include sets for which every nonidentity element of the ambient group can be expressed some constant number of times as a product of three (or four, or five, etc...) elements of the set. Intuitively, we refer to this extended notion as "higher-order regularity."

In what follows, we demonstrate that additive regularity implies higher-order regularity. Specifically, if S is a sum set in the group G, then the number of ways to write elements of G as the product of j elements of S – for any $j \geq 2$ – is predictable and (almost) constant. This fact, interestingly, proves to be the key to characterizing abelian sum sets.

The calculations that follow are most easily carried out in the integral group ring $\mathbb{Z}G$. This ring consists of all formal sums

$$\sum_{g \in G} a_g g$$

with $a_g \in \mathbb{Z}$. For each element $g \in G$ there is a corresponding element $1g \in \mathbb{Z}G$, though for simplicity we identify $1g$ with g. Similarly, for any $a_1 \in \mathbb{Z}$ write $a_1 1 \in \mathbb{Z}G$ simply as a_1. Each subset of $S \subseteq G$ corresponds to a group ring element $\sum_{g \in S} g$, which we write simply as S. Reusing notation in this fashion is convenient because we will often be able to use facts about the group ring element $S \in \mathbb{Z}G$ to deduce facts about the subset $S \subset G$.

Addition in $\mathbb{Z}G$ is defined component-wise:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

If we define $(ag)(bh) = (ab)(gh)$ for $a, b \in \mathbb{Z}$ and $g, h \in G$, then we can extend this rule via the standard distributive laws to define multiplication in $\mathbb{Z}G$. Expressions such as X^t, where $X \in \mathbb{Z}G$ and $t \in \mathbb{N}$ are then understood to mean multiplication of X with itself t times.

Finally, for any $X = \sum_{g \in G} a_g g \in \mathbb{Z}G$ and any integer t, define $X^{(t)} = \sum_{g \in G} a_g g^t$. Note that $X^{(t)} \neq X^t$ in general! This notation has the potential to create confusion, since if $S \subseteq G$, then we may use the same notation to define the *set* $S^{(t)} = \{s^t : s \in S\}$. In this instance, the elements appearing in the *set* $S^{(t)}$ will be precisely those elements whose coefficient in the *group ring element* $S^{(t)}$ is nonzero. However, if there exist r distinct elements in G whose t^{th} powers equal some element g, then the coefficient of g in the group ring element $S^{(t)}$ will be r, while of course g will appear but once in the set $S^{(t)}$. Note that when t is relatively prime to the order of G, there is no potential for ambiguity. So, for example, if $S \subseteq G$ we may write $S^{(-1)}$ to mean both the set of inverses of S and the group ring element $\sum_{s \in S} s^{-1}$ without fear of confusion.

Lemma 4.1. *If S is a (v,k,μ) sum set, then for any $m \geq 1$,*

$$S^{2m} = \frac{1}{v}(k^{2m} - n^m)G + n^m.$$

Proof. We induct on m. When $m = 1$, the equation reduces to $S^2 = \mu G + n$, which is correct. Now assume the result holds for some $m \geq 1$ and consider $S^{2(m+1)}$:

$$\begin{aligned} S^{2(m+1)} = S^{2m}S^2 &= (\frac{1}{v}(k^{2m} - n^m)G + n^m)(\mu G + n) \\ &= \frac{\mu}{v}(k^{2m} - n^m)vG + \frac{n}{v}(k^{2m} - n^m)G + \mu n^m G + n^{m+1} \\ &= \frac{1}{v}[(k^{2m} - n^m)(\mu v + n) + (k^2 - n)n^m]G + n^{m+1} \\ &= \frac{1}{v}[(k^{2m} - n^m)k^2 + (k^2 - n)n^m]G + n^{m+1} \\ &= \frac{1}{v}(k^{2m+2} - n^{m+1})G + n^{m+1}. \end{aligned}$$

This completes the induction. □

Since in $\mathbb{Z}G$, $GS = SG = |S|G$ for any subset S, we also have

Corollary 4.2. *If S is a (v,k,μ) sum set, then for any $m \geq 1$,*

$$S^{2m+1} = \frac{k}{v}(k^{2m} - n^m)G + n^m S.$$

These results are aesthetically satisfying, for they imply that additive regularity at a base level is enough to ensure regularity at all higher levels. However, the corollary has a rather surprising consequence in the case where G is abelian. This consequence – that every abelian sum set satisfies $S = S^{(-1)}$ – is the main result of this section. To prove it, we will need the following well-known fact about arithmetic in $\mathbb{Z}G$ when G is abelian:

Lemma 4.3 ([4] Lemma 3.3)**.** *Let p be a prime. If G is abelian, then for any $S \in \mathbb{Z}G$,*

$$S^p \equiv S^{(p)} \bmod p.$$

We will also use the fact that for any odd prime p, a natural number j relatively prime to p is a quadratic residue modulo p if and only if $j^{(p-1)/2} \equiv 1 \bmod p$.

The outline of the proof is as follows: first we prove that if S is an abelian sum set, then $n \neq 0$. Next, we show $n \neq 0$ implies n is a square. From there, we are able to deduce that $S^{(p)} = S$ for infinitely many primes p, which leads to the result.

Theorem 4.4. *If S is a (v,k,μ) sum set in an abelian group G, then S is reversible.*

Proof. Suppose S is a (v,k,μ) sum set with $n = 0$. Then $k^2 = \mu v$. For any odd prime p, Corollary 4.2 says

$$S^p = \left(\frac{k}{v}\right) k^{p-1}G = \mu k^{p-2}G.$$

Hence by Lemma 4.3, we have

$$\mu k^{p-2}G \equiv S^{(p)} \bmod p.$$

Provided p is relatively prime to both μ and k this is impossible, because the group ring element $\mu k^{p-2}G$ contains some nonzero constant number of copies of each element of G, while $S^{(p)}$ can not do this. Hence,

$n \neq 0$. Next, suppose n is not a square. Then there must exist some odd prime $p > v$ such that $n^{(p-1)/2} \equiv -1 \bmod p$ ([3], Chapter 5, Theorem 3). Thus,

$$\begin{aligned} vS^p &= kG(k^{p-1} - n^{\frac{p-1}{2}}) + vn^{\frac{p-1}{2}}S \\ &\equiv kG(1-(-1)) + v(-1)S \bmod p \\ &\equiv 2kG - vS \bmod p. \end{aligned}$$

Now $p > v$ implies that $p > k$, so p can not divide $2k$. Thus every element of $G \setminus S$ appears in the expression $2kG - vS$, taken modulo p. Also, as $n \neq 0$, we know $2k \neq v$. It follows that every element of G appears in the expression $2kG - vS$, taken modulo p. But by Lemma 4.3, we know that

$$2kG - vS \equiv vS^{(p)} \bmod p.$$

As before, this is impossible, so we conclude that if S is a sum set in an abelian group, then n must be a square.

If n is a square, then n is a square modulo p for any prime p. Consequently, if $p > v$,

$$\begin{aligned} S^p &= \frac{k}{v}G(k^{p-1} - n^{\frac{p-1}{2}}) + n^{\frac{p-1}{2}}S \\ &\equiv \frac{k}{v}G(1-1) + (1)S \bmod p \\ &\equiv S \bmod p. \end{aligned}$$

Lemma 4.3 now says that $S^{(p)} \equiv S \bmod p$ for any prime $p > v$. But clearly this is possible only if $S^{(p)} = S$.

Now we are ready to show that $S = S^{(-1)}$. Let $x \in S$. By Dirichlet's Theorem on arithmetic progressions, there exists a prime $p > v$ such that $p \equiv -1 \bmod o(x)$. We know $S^{(p)} = S$, so $x^p = x^{-1} \in S$. The proof is complete. □

In the case where G is nonabelian, we can not deduce so much. One reason is that Lemma 4.3, which was our primary tool in proving Theorem 4.4, does not apply. Although nonabelian sum sets exhibit the same higher-order regularity as abelian sum sets, it is unclear whether this fact can be exploited to gain as much information about the structure of nonabelian sum sets.

We have already seen in Theorem 4.4 that every abelian sum set is necessarily reversible. Thus, we now have

Corollary 4.5. *An abelian sum set is a reversible difference set. In particular, there are no cyclic sum sets.*

Proof. A reversible sum set is necessarily a difference set, by Theorem 2.2, so the first result is obvious. The second result, first obtained by Lam [5], now follows immediately as there are no reversible cyclic difference sets [6]. □

§ 5. General Constructions

In Section 3 we saw how the existence of normal subgroups of small index can affect the possible structure of sum sets. Here we look at the opposite end of the spectrum – normal subgroups of order 2. While normal subgroups of small index proved useful in developing nonexistence results for sum sets, normal subgroups of small order allow for simple, generic construction techniques for sum sets.

If $N = \{1, z\}$ is a normal subgroup of G, then $z \in Z(G)$. Clearly any sum set $S \subset G$ meets each coset of N in either 0, 1, or 2 elements. We highlight two possible situations which will be of importance to us.

Definition 5.1. *Let $N \lhd G$, $o(N) = 2$, and let $S \subset G$ be a sum set. We say S is* **type 1 with respect to** *N if it does not intersect N but intersects each other coset of N in either 0 or 1 element. We say S is* **type 2 with respect to** *N if it intersects N in one element and intersects each other coset of N in either 0 or 2 elements.*

The motivation for these definitions will become apparent as we develop techniques for constructing sum sets.

If S is a sum set, then the translate $Sg = \{sg : s \in S\}$ is generally not a sum set. However, if z is a central involution, then we can write $a = xy$ as a product in S if and only if we can write $a = (xz)(yz)$ in Sz. Thus, if z is a central involution, then Sz is a sum set with the same parameters as S. We can say slightly more in the case where S is either type 1 or type 2 with respect to the normal subgroup $N = \{1, z\}$.

Lemma 5.2. *Let S be a sum set in G and suppose G possesses a normal subgroup $N = \{1, z\}$. If S is type 1 with respect to N, then Sz is also a type 1 sum set, necessarily disjoint from S. If S is type 2 with respect to N, then Sz is also a type 2 sum set, and Sz differs from S in precisely one element.*

Proof. That Sz is a sum set is clear from the preceeding discussion. Multiplying the elements of G by z fixes all cosets of N. Thus S and Sz intersect the same cosets of N. If S is type 1, S and Sz intersect those cosets in distinct elements, by definition. If S is type 2, then Sz contains the same nontrivial cosets of N as S, while if S contains 1, then Sz contains z. If S contains z, then Sz contains 1. □

We now present a technique for constructing type 2 sum sets. Essentially, the process involves "lifting" a partial sum set P in the group K to a partial sum set in the group $G = K \times \{1, z\}$, which can then be completed to a sum set by adjoining either 1 or z.

Theorem 5.3. *Let P be a $(v, k, \beta - 1, \beta)$ partial sum set in K not containing 1. Then $S = P \cup Pz$ is a $(2v, 2k, 2\beta - 2, 2\beta)$ partial sum set in $G = K \times \{1, z\}$ if and only if $|P \cap P^{(-1)}| = \beta$. Consequently, when $|P \cap P^{(-1)}| = \beta$, $S \cup \{1\}$ and $S \cup \{z\}$ are both $(2v, 2k + 1, 2\beta)$ type 2 sum sets in G with respect to $N = \{1, z\}$.*

Proof. It is clear that $|S| = 2k$, so we need only prove that S exhibits the claimed additive regularity.

Consider any element $a \in G \setminus N$. Either $a \in K$ or $a = bz$ for some $b \in K$. We prove the number of ways to write a as a product in S is twice the number of ways to write a as a product in P.

First suppose $a \in K$ and let $a = xy$ be a representation for a as a product in P. Then $a = xy$ is also a representation for a as a product in S as $P \subset S$. In addition, $a = (xz)(yz)$ is a representation for a as a product in S. Conversely, whenever we can write $a = xy$ as a product in S it must be the case that both x and y are in P or both are in Pz. Hence,

$$|\mathcal{C}_{a,S}| = 2|\mathcal{C}_{a,P}| = \begin{cases} 2\beta - 2 & \text{if } a \in S, \\ 2\beta & \text{if } a \notin S. \end{cases}$$

Now suppose $a = bz$ for some $b \in K$. Whenever $b = xy$ is a representation for b as a product in P, $a = (xz)y$ and $a = x(yz)$ are representations for b as a product in S. Conversely, whenever we can write $b = xy$ as a product in S, we must have precisely one of x or y in P and the other in Pz. Hence,

$$|\mathcal{C}_{a,S}| = 2|\mathcal{C}_{b,P}| = \begin{cases} 2\beta - 2 & \text{if } a \in S, \\ 2\beta & \text{if } a \notin S. \end{cases}$$

Thus, with the exception of z, all nonidentity elements of G are represented as products in S in the number of ways claimed. Note $z \notin S$ so we require z to be represented as a product in S in precisely 2β ways. Suppose $z = xy$ where $x, y \in S$. If $x \in P$, then $y = x^{-1}z \in Pz$, so necessarily $x^{-1} \in P$. Hence the number of ways to write $z = xy$ where $x, y \in S$ and $x \in P$ is precisely $|P \cap P^{(-1)}|$. Similarly if $x \notin P$, then we must have $y \in P$ and $x = y^{-1}z$. Again, the number of ways to write $z = xy$ in this situation is $|P \cap P^{(-1)}|$. Thus z can be written as a product in S in precisely $2|P \cap P^{(-1)}|$ ways, so S is a $(2v, 2k, 2\beta - 2, 2\beta)$ partial sum set if and only if $|P \cap P^{(-1)}| = \beta$.

Finally if S is a $(2v, 2k, 2\beta - 2, 2\beta)$ partial sum set, then adjoining 1 to S increases the number of ways to write each element of S as a product in S by 2 while not affecting the number of ways to write elements not in S as products in S. Hence $S \cup \{1\}$ is a $(2v, 2k + 1, 2\beta)$ sum set which is clearly type 2 with respect to N. By Lemma 5.2, $S \cup \{z\} = (S \cup \{1\})z$ is also a type 2 $(2v, 2k + 1, 2\beta)$ sum set. □

This lifting process can be reversed in the sense that if S is a type 2 sum set in G with respect to the normal subgroup N, then there exists a partial sum set P in the group G/N. Hence there is a 2-to-1 correspondence between type 2 sum sets in groups of order $2v$ and partial sum sets with particular parameters in groups of order v.

Theorem 5.4. *Let S be a $(2v, 2k+1, 2\beta)$ sum set in G, type 2 with respect to the normal subgroup $N = \{1, z\}$. Then $P = (S \setminus N)/N$ is a $(v, k, \beta - 1, \beta)$ partial sum set in G/N.*

Proof. If S is type 2, then S intersects N in one element, and $S \setminus N$ is a $(2v, 2k, 2\beta - 2, 2\beta)$ partial sum set. For any $a \in G \setminus N$, if $x \in \mathcal{C}_{a,S}$ then $xz \in \mathcal{C}_{a,S}$ as well. Under the canonical homomorphism $g \mapsto gN$, the elements x and xz are both mapped to xN. Hence, $|\mathcal{C}_{aN,P}| = \frac{1}{2}|\mathcal{C}_{a,S\setminus N}|$. The result follows. □

§ 6. Dihedral Constructions

The preceding constructions are of a general nature, and to apply them one must already be in possession of some additively regular set. Dihedral groups provide a wealth of additively regular sets and an easily exploitable group structure for constructing them. For any $a, b \in G$, we use the standard notation a^b for $b^{-1}ab$. Throughout this section, we use the presentation

$$D_j = \langle x, t \mid x^j = t^2 = 1, x^t = x^{-1} \rangle$$

to denote the dihedral group of order $2j$.

We present two constructions for sum sets in D_j with parameters $(2j, j-1, \frac{j-2}{2})$. These parameters imply j is even, so that $Z(D_j)$ has order 2. The first construction yields type 1 sum sets with respect to $Z(D_j)$ while the sum sets of the second construction are type 2 with respect to $Z(D_j)$.

Theorem 6.1. *Let $C_j = \langle x \rangle$ be the cyclic group of order j where $j \geq 4$ is even. Let M be a maximally skew set in C_j containing precisely one element from each coset of $\langle x^{\frac{j}{2}} \rangle$. Set $S = M \cup Mt \subset D_j$. Then $S \cup \{t\}$ and $S \cup \{x^{\frac{j}{2}}t\}$ are both $(2j, j-1, \frac{j-2}{2})$ type 1 sum sets with respect to $Z(D_j)$.*

Proof. Set $z = x^{\frac{j}{2}}$. Let M be a maximally skew set in C_j containing precisely one element from each coset of $\langle z \rangle$. As j is even, z is the unique involution in C_j. The remaining $j-2$ nonidentity elements each have inverses distinct from themselves, so $|M| = \frac{j-2}{2}$.

Fix some $y \in C_j$. For each $w \in M$, consider the element $w^{-1}y$. There are four possibilities:

1. $w^{-1}y = 1 \quad (\Leftrightarrow w = y)$,
2. $w^{-1}y = z \quad (\Leftrightarrow w = yz)$,
3. $w^{-1}y \in M$,
4. $w^{-1}y \in M^{(-1)}$.

If $y = 1$ or $y = z$, the first two cases are impossible. Hence every $w \in M$ is in either $\mathcal{C}_{1,M}$ or $\mathcal{A}_{1,M}$, and in either $\mathcal{C}_{z,M}$ or $\mathcal{A}_{z,M}$. As M is skew, $\mathcal{C}_{a,M} \cap \mathcal{A}_{a,M} = \emptyset$ for any $a \in C_j$. We therefore have

$$|\mathcal{C}_{1,M}| + |\mathcal{A}_{1,M}| = |\mathcal{C}_{z,M}| + |\mathcal{A}_{z,M}| = |M| = \frac{j-2}{2}. \tag{6}$$

If $y \notin \{1, z\}$, then either y or y^{-1} is in M. If $y \in M$, then $yz \notin M$ by construction, so case 2 does not occur. Similarly, if $y \notin M$, then $yz \in M$ so case 1 does not occur. In either situation we have

$$|\mathcal{C}_{y,M}| + |\mathcal{A}_{y,M}| = |M| - 1 = \frac{j-4}{2}. \tag{7}$$

Now we move from the group C_j to the group $D_j = C_j \cup C_j t$. Form the set $S = M \cup Mt$, and form all possible products ab in S. There are again four distinct situations:

1. $a \in M$, $b \in M$,
2. $a \in Mt$, $b \in Mt$,
3. $a \in Mt$, $b \in M$,
4. $a \in M$, $b \in Mt$.

Note in the first two cases, the product ab is in C_j, while in the latter two cases $ab \in C_j t$.

Multiplication in D_j obeys the rule $ty = y^{-1}t$, for any $y \in C_j$. So, for example, for $w_1, w_2 \in M$, $(w_1 t)w_2 = w_1(tw_2) = (w_1 w_2^{-1})t$, while $w_1(w_2 t) = (w_1 w_2)t$. Hence, the number of ways to write yt as a product in S is the sum of the number of ways to write y as a product in M and the number of ways to write y as a quotient in M. It follows from (6) and (7) that

$$|\mathcal{C}_{a,S}| = \begin{cases} \frac{j-2}{2} & \text{if } a \in \{1, t, z, zt\}, \\ \frac{j-4}{2} & \text{if } a \notin \{1, t, z, zt\}. \end{cases}$$

If we adjoin the element t to S, what new products can be generated? The set S contains none of the elements $\{1, t, z, zt\}$, so none of $\{t, z, zt\}$ gains any additional representations as products. The identity gains one additional representation, since $t^2 = 1$. If $a \in D_j$ is any element other than these four, then precisely one of at or $a^{-1}t$ is in S. If $at \in S$, then $(at)t = a$ is a new way to write a as a product in S. On the other hand, if $a^{-1}t \in S$ then $t(a^{-1}t) = a$ is a new way to write a as a product in S. Hence,

$$|\mathcal{C}_{a,S\cup\{t\}}| = \begin{cases} \frac{j}{2} & \text{if } a = 1, \\ \frac{j-2}{2} & \text{if } a \neq 1. \end{cases}$$

Thus, $S \cup \{t\}$ is a $(2j, j-1, \frac{j-2}{2})$ sum set in D_j. A similar argument shows adjoining zt to S produces a sum set with the same parameters. The construction guarantees that the resulting sum set misses the center of D_j while containing precisely one element from each nontrivial coset of $\{1, z\} = Z(D_j)$. Thus, these sum sets are type 1 with respect to $Z(D_j)$. □

While type 1 dihedral sum sets with parameters $(2j, j-1, \frac{j-2}{2})$ can be constructed in D_j for all even $j \geq 4$, there is an additional restriction for type 2 dihedral sum sets with these parameters:

Lemma 6.2. *A type 2 sum set with parameters $(2j, j-1, \frac{j-2}{2})$ may exist in D_j only if $j \equiv 2 \bmod 4$.*

Proof. If there exists a $(2j, j-1, \frac{j-2}{2})$ sum set in D_j, then j is necessarily even, so we may rewrite these parameters as $(4m, 2m-1, m-1)$. By Theorem 5.4, if there exists a type 2 dihedral sum set with parameters $(4m, 2m-1, m-1)$, then there must exist a $(2m, m-1, \frac{m-3}{2}, \frac{m-1}{2})$ partial sum set in $D_{2m}/Z(D_{2m})$. Consequently type 2 sum sets with these parameters may exist in D_{2m} only if m is odd, i.e. only if $j \equiv 2 \bmod 4$. □

In the case where m is odd, $D_{2m} \cong D_m \times Z(D_{2m})$. Hence $D_{2m}/Z(D_{2m}) \cong D_m$, so the problem of constructing type 2 dihedral sum sets in D_{2m} is equivalent to the problem of constructing partial sum sets in D_m with liftable parameters. We now show how one may construct these partial sum sets.

The procedure begins with a maximally skew set in a group G of odd order, which we "twist" into a partial sum set in the generalized dihedral group of G. That our starting set is skew guarantees (see Lemma 2.1) the partial sum set has parameters amenable to the lifting process described by Theorem 5.3. When the group in which we begin is cyclic of odd order m, then the twist yields a partial sum set in D_m which is then lifted to a sum set in D_{2m}.

Theorem 6.3. *Let G be a group of odd order m with M a maximal skew set in G. Then $S = M \cup Mt$ is a $(2m, m-1, \frac{m-3}{2}, \frac{m-1}{2})$ partial sum set in $DihG = G \rtimes \{1, t\}$. These partial sum sets can be lifted to $(4m, 2m-1, m-1)$ sum sets in $DihG \times C_2$.*

Proof. As $|M| = \frac{m-1}{2}$, $|S| = m-1$. Suppose $g = ab$ is a representation for $g \in G$ as a product in S. Then either $a, b \in M$ or $a, b \in Mt$. By definition there are $|\mathcal{C}_{g,M}|$ ways to write $g = ab$ as a product in M. If $a, b \in Mt$, then we have, for $w_1, w_2 \in M$,

$$g = (w_1 t)(w_2 t) = w_1(t w_2)t = w_1(w_2^{-1}t)t = w_1 w_2^{-1}.$$

Hence there are $|\mathcal{A}_{g,M}|$ ways to write g as a product in Mt. Combined, there are thus $|\mathcal{C}_{g,M}| + |\mathcal{A}_{g,M}|$ ways to write g as a product in S.

Similarly, if $y = gt$ for some $g \in G$, then the number of ways to write y as a product in S is $|\mathcal{C}_{g,M}| + |\mathcal{A}_{g,M}|$. Note $y \in S$ if and only if $g \in M$.

By Lemma 2.1, we have

$$|\mathcal{C}_{y,S}| = \begin{cases} \frac{m-3}{2} & \text{if } y \in S, \\ \frac{m-1}{2} & \text{if } y \notin S. \end{cases}$$

Thus, S is a $(2m, m-1, \frac{m-3}{2}, \frac{m-1}{2})$ partial sum set in $DihG$, as claimed. That M is skew implies $1 \notin M$ and $|S \cap S^{(-1)}| = |Mt| = \frac{m-1}{2}$. By Theorem 5.3, S can be lifted into a $(4m, 2m-1, m-1)$ sum set in $DihG \times C_2$. □

The partial sum set $S = M \cup Mt \subset DihG$ can also be used to construct sum sets in the group

$$D_j^* := \langle x, t \mid x^j = t^4 = 1, x^t = x^{-1} \rangle.$$

Note that this group is defined by a presentation very similar to the standard presentation for D_j, except the element t which acts by inversion on the cyclic group $\langle x \rangle$ has order 4 rather than order 2. It is easily seen that when j is odd, this group has center $Z(D_j^*) = \{1, t^2\}$, and $D_j^*/Z(D_j^*) \cong D_j$.

Suppose $S \subset D_j$ is a $(2j, j-1, \frac{j-3}{2}, \frac{j-1}{2})$ partial sum set as described in Theorem 6.3. Using the natural correspondence between D_j and $D_j^*/Z(D_j^*)$, define

$$S^* = \bigcup_{x \in S} xZ(D_j^*).$$

That S^* is a $(4j, 2j-2, j-3, j-1)$ partial sum set follows from an argument almost identical to that used in Theorem 5.3. Hence, adjoining either central element to S^* creates a $(4j, 2j-1, j-1)$ sum set in D_j^*. We summarize the preceding discussion as a theorem:

Theorem 6.4. *The group*

$$D_j^* = \langle x, t | x^j = t^4 = 1, x^t = x^{-1} \rangle$$

admits $(4j, 2j-1, j-1)$ *sum sets whenever* j *is odd. These sum sets are all type 2 with respect to the center* $\{1, t^2\}$ *of* D_j^*.

Sum sets in the groups D_j and D_j^* appear as Examples 6.3 and 6.4 in [7].

§ 7. Frobenius Constructions

We have seen how normal subgroups of a group G affect the possible size and shape of sum sets in G. In this section, we consider a family of groups that admits both sum sets and partial sum sets. Interestingly, these sum sets and partial sum sets are constructed with respect to subgroups which are not normal.

The groups in question are all Frobenius groups, so before proceeding with the constructions, we collect some relevant information about Frobenius groups. For a more detailed treatment see Gorenstein [2]. Let H be a subgroup of the group G. For any $g \in G$, we write H^g to represent the conjugate of H by g, i.e. $H^g = g^{-1}Hg$. If $N_G(H) = H$ and $H^{g_1} \cap H^{g_2} = \{1\}$ whenever H^{g_1} and H^{g_2} are distinct conjugates of H in G, then G is called a *Frobenius group* and the subgroup H is called a *Frobenius complement*. Note any conjugate of H also functions as a Frobenius complement in G.

If G is a Frobenius group, then G possesses a proper, nontrivial normal subgroup K, called the *Frobenius kernel* of G, such that $G = K \rtimes H$, where H is a Frobenius complement. It can be shown $C_G(b) \leq K$ for all nonidentity $b \in K$. Consequently, for any nonidentity $b \in K$ and $h_1, h_2 \in H$, we have $b^{h_1} = b^{h_2}$ if and only if $h_1 = h_2$. It follows $o(H) \leq o(K) - 1$ for any Frobenius group $K \rtimes H$, with equality if and only if H acts regularly (i.e. sharply transitively) on the nonidentity elements of K. This regular action is the key to our construction of additively regular sets in Frobenius groups.

Theorem 7.1. *Let $G = K \rtimes H$ be a Frobenius group where H acts regularly on the nonidentity elements of K. Then the union of any j nontrivial left cosets of H is a $(o(G), j\,o(H), j^2 - j, j^2)$ partial sum set. Any j nontrivial left cosets of H together with H is a $(o(G), (j+1)o(H), j^2 + o(H), j^2 + j)$ partial sum set.*

Proof. Whenever an arbitrary element $bh \in G$, with $b \in K$, $h \in H$, is expressed as a product in G, we have

$$\begin{aligned} bh &= (b_1h_1)(b_2h_2) \\ &= b_1(h_1b_2h_1^{-1})h_1h_2 \\ &= (b_1b_2^{h_1^{-1}})(h_1h_2). \end{aligned}$$

(Here, and throughout this proof, $b_i \in K$, $h_i \in H$.) Hence we require $b = b_1b_2^{h_1^{-1}}$ and $h = h_1h_2$.

Now $K \cap H = \{1\}$, so for $b_1, b_2 \in K$ we have $b_1H = b_2H$ if and only if $b_1 = b_2$. So the set of left cosets of H in G is the set $\{bH : b \in K\}$. Choose j nonidentity elements $b_1, \ldots, b_j \in K$, and set $S = b_1H \cup \cdots \cup b_jH$. We count the number of ways to write an arbitrary element of G as a product in S.

Let $bh \in G$, with $b \in K$, $h \in H$. For each $b_i \in K$ such that $b_iH \subset S$, consider the element $b_i^{-1}b$. Provided $b_i \neq b$, $b_i^{-1}b \neq 1$. As H acts regularly on the nonidentity elements of K, for any $b_l \in \{b_1, \ldots, b_j\}$ there is a unique $h_1 \in H$ such that

$$b_l^{h_1^{-1}} = b_i^{-1}b.$$

With h_1 now fixed, there is a unique $h_2 \in H$ such that $h = h_1h_2$. We have $b = b_ib_l^{h_1^{-1}}$ and $h = h_1h_2$, so $bh = (b_ih_1)(b_lh_2)$.

If $bh \in S$, then b is one of the elements $b_1, \ldots, b_j$, so there are $j - 1$ choices for b_i in the preceding argument, and then j choices for b_l. Hence bh can be written as a product in S in $(j-1)j = j^2 - j$ ways. If $bh \notin S$, then there are j choices for b_i, so bh can be written as a product in S in j^2 ways. Thus, S is a $(o(G), j\,o(H), j^2 - j, j^2)$ partial sum set.

Next we consider the set $S \cup H$. We have already counted the number of ways to write any element in G as a product in S, so now we must only consider writing an arbitrary element bh, with $b \in K$, $h \in H$, as a product $bh = h_i(b_lh_l)$ and as a product $bh = (b_ih_i)h_l$.

First suppose $bh \in S \cup H$. If $b = 1$, i.e. $bh = h \in H$, then from the previous argument there are j^2 ways to write h as a product in S. There are an additional $o(H)$ ways to write h as a product in H, and there is no way to write h as a product where one factor lives in H and the other does not. Hence, there are $j^2 + o(H)$ ways to write any $h \in H$ as a product in $S \cup H$.

If $b \neq 1$, then $bh = h_i(b_lh_l)$ if and only if $b = b_l^{h_i^{-1}}$ and $h = h_ih_l$. As before, the regular action of H on the nonidentity elements of K allows us to choose b_l freely from $b_1, \ldots, b_j$, whereupon h_i and hence h_l are uniquely determined. This contributes j additional ways to write $bh \in S$ as a product in $S \cup H$. Finally, to write bh as a product $(b_ih_i)h_l$ in $S \cup H$, then b must equal b_i, but h_i may be chosen freely and uniquely determines h_l. Hence $bh \in S$ can be written as a product in $S \cup H$ in $(j^2 - j) + j + o(H) = j^2 + o(H)$ ways, the same as the number of ways to write $h \in H$ as a product in $S \cup H$.

Now suppose $bh \notin S \cup H$. There are j^2 ways to write bh as a product in S. As previously argued, the regular action of H on nonidentity elements of K provides j ways to write $bh = h_i(b_lh_l)$ as a product in $S \cup H$. To write bh as a product $(b_ih_i)h_l$ we require $b = b_i$. But we are assuming $bh \notin S$, so $b \notin \{b_1, \ldots, b_j\}$. Hence it is impossible to write bh as a product $(b_ih_i)h_l$. Thus, the total number of ways to write $bh \notin S \cup H$ as a product in $S \cup H$ is $j^2 + j$. This completes the proof. □

To make use of Theorem 7.1, we first must possess a Frobenius group $K \rtimes H$ where H acts regularly on the nonidentity elements of K, or equivalently, where $o(H) = o(K) - 1$. A sufficient condition for the existence of such a group is that $o(K)$ is a prime power.

For any prime power q, the set of invertible affine transformations of the form $x \mapsto ax + b$ of the field $GF(q)$ forms a group Aff(q) of order $q(q-1)$. The set of maps for which $a = 1$ forms a normal subgroup K isomorphic to the additive group $EA(q)$ of the field, while those maps for which $b = 0$ form a subgroup H isomorphic to the field's multiplicative group C_{q-1}. It is easily checked that Aff(q) is Frobenius with kernel K and complement H, and that H acts regularly on K. Hence we may apply Theorem 7.1 to the group Aff(q). In particular, by fixing certain values of t, we can use the partial sum sets of Theorem 7.1 to construct sum sets in certain subgroups of Aff(q) and in extensions of Aff(q).

First, we consider a partial sum set $P \subset$ Aff(q) consisting of a single nontrivial left coset of H. By Theorem 7.1, P is a $(q(q-1), q-1, 0, 1)$ partial sum set. Note that every element not in P is generated precisely once as a product in P. In particular, simple counting shows that 1 must be generated precisely once as a product in P, so $|P \cap P^{(-1)}| = 1$. Hence P is amenable to the lifting procedure described in Theorem 5.3. That is, if $\{1, z\}$ is the cyclic group of order 2, then $P \cup Pz$ is a $(2q(q-1), 2(q-1), 0, 2)$ partial sum set in Aff(q) $\times \{1, z\}$. Adjoining either 1 or z to $P \cup Pz$ yields a $(2q(q-1), 2q-1, 2)$ sum set. We state this conclusion as a corollary to Theorems 5.3 and 7.1.

Corollary 7.2. *For any prime power q, there exist sum sets with parameters $(2q(q-1), 2q-1, 2)$ in the group Aff(q) $\times C_2$, where C_2 is the cyclic group of order 2.*

If $K \rtimes H$ is a Frobenius group and J is a nontrivial subgroup of H, then $K \rtimes J$ is a Frobenius group with kernel K and complement J (if J is the identity subgroup then $K \rtimes J \cong K$ is not Frobenius). The Frobenius group Aff(q) has complement $H \cong GF(q)^*$, so the subgroups of H correspond to divisors of $q-1$. If $d \mid (q-1)$, then the subgroup of H of order d is the cyclic group C_d of order d, so we write $EA(q) \rtimes C_d$ to denote the corresponding Frobenius subgroup of Aff(q). We now demonstrate the existence of sum sets in all Frobenius subgroups of Aff(q).

Theorem 7.3. *For any divisor $d \geq 2$ of $q-1$, the Frobenius group $EA(q) \rtimes C_d$ admits sum sets with parameters $(qd, 2q-1, \frac{4(q-1)}{d})$.*

Proof. The proof is similar to the proof of Theorem 7.1, so we adopt consistent notation. Let $K \cong EA(q)$ denote the Frobenius kernel of Aff(q), and let H denote the Frobenius complement. Let $d \geq 2$ be a divisor of $q-1$, and set $G = K \rtimes C_d$.

We begin by constructing a partial sum set in Aff(q). The induced action of $C_d < H$ on the nonidentity elements of K has $(q-1)/d$ orbits each of length d. Choose two elements from each orbit, say $b_1, b_2, \ldots, b_j$, where $j = 2(q-1)/d$. Set $S = b_1H \cup \cdots b_jH$. By Theorem 7.1, S is a partial sum set in Aff(q) with parameters

$$(q(q-1), j(q-1), j(q-1)[j(q-1)-1], j^2(q-1)^2)$$

We claim $S \cap G$ is a partial sum set in G.

Let $bh \in G$, with $b \in K$, $h \in H$. For each b_i such that $b_iH \subset S$, consider the element $b_i^{-1}b$. Provided b_i does not equal b, $b_i^{-1}b \neq 1$, so $b_i^{-1}b$ lives in one of the $(q-1)/d$ orbits of K induced by C_d. Let b_l be an element of this orbit satisfying $b_lH \subset S$. There is a unique $h_1 \in C_d$ such that

$$b_l^{h_1^{-1}} = b_i^{-1}b.$$

With h_1 now fixed there is a unique $h_2 \in C_d$ such that $h = h_1h_2$. We have $b = b_ib_l^{h_1^{-1}}$ and $h = h_1h_2$, so $bh = (b_ih_1)(b_lh_2)$.

If $bh \in S \cap G$, then b is one of the elements $b_1, \ldots, b_j$, so there are $j-1$ choices for b_i in the preceding argument. Since we chose precisely two elements from each orbit of the action of C_d on the nonidentity elements of K, there are two choices for b_l. Thus bh can be written as a product in $S \cap G$ in precisely $2(j-1)$ ways. If $bh \notin S \cap G$, then there are j choices for b_i, so bh can be written as a product in $S \cap G$ in $2j$ ways. Hence $S \cap G$ is a $(qd, 2(q-1), 2(j-1), 2j)$ partial sum set in G. Adjoining 1 to $S \cap G$ yields a $(qd, 2q-1, \frac{4(q-1)}{d})$ sum set. □

A few remarks about Theorem 7.3 are helpful. The key step in the proof is choosing precisely two elements from each orbit of the induced action of C_d on K. More generally, choosing some constant number of elements, say c, from each orbit will induce a partial sum set in the subgroup G, but unless $c = 2$ this partial sum set will not be completable to a sum set. If we do not choose some constant number of elements from each orbit, then $S \cap G$ will not be a partial sum set.

When q is odd, $d = 2$ is always a divisor of $q - 1$, but the resulting sum set in $EA(q) \rtimes C_2$ is a trivial $(2q, 2q - 1, 2q - 2)$ sum set. When $d = q - 1$ the resulting sum set is in Aff(q) itself, so we have the following corollary.

Corollary 7.4. *In the group Aff$(q) = EA(q) \rtimes C_{q-1}$, any two nonidentity cosets of C_{q-1} together with 1 form a $(q(q-1), 2q-1, 4)$ sum set.*

References

[1] R.S. Coulter and T. Gutekunst, *Special subsets of difference sets with particular emphasis on skew Hadamard difference sets*, Des. Codes Cryptogr. **53** (2009), 1–12.

[2] D. Gorenstein, *Finite Groups*, 3rd ed., Chelsea Publishing Company, New York, 1980.

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, vol. 158, Springer-Verlag, 1990.

[4] D. Jungnickel, *Difference sets*, Contemporary Design Theory, Wiley-Intersci. Ser. Discre Math. Optim., Wiley, New York, 1992, pp. 241–324.

[5] C.W.H. Lam, *A generalization of cyclic difference sets*, J. Combin. Theory Ser. A **19** (1975), 51–65.

[6] R.L. McFarland and S.L. Ma, *Abelian difference sets with multiplier minus one*, Arc. Math. (Basel) **54** (1990), 610–623.

[7] J.S. Sumner and A.T. Butson, *Addition sets in a finite group*, J. Combin. Theory Ser. A **32** (1982), 350–369.