

# MOST SUBSETS ARE BALANCED IN FINITE GROUPS

STEVEN J. MILLER AND KEVIN VISSUET

**ABSTRACT.** The sumset is one of the most basic and central objects in additive number theory. Many of the most important problems (such as Goldbach’s conjecture and Fermat’s Last theorem) can be formulated in terms of the sumset  $S + S = \{x + y : x, y \in S\}$  of a set of integers  $S$ . A finite set of integers  $A$  is sum-dominated if  $|A + A| > |A - A|$ . Though it was believed that the percentage of subsets of  $\{0, \dots, n\}$  that are sum-dominated tends to zero, in 2006 Martin and O’Bryant proved a very small positive percentage are sum-dominated if the sets are chosen uniformly at random (through work of Zhao we know this percentage is approximately  $4.5 \cdot 10^{-4}$ ). While most sets are difference-dominated in the integer case, this is not the case when we take subsets of many finite groups. We show that if we take subsets of larger and larger finite groups uniformly at random, then not only does the probability of a set being sum-dominated tend to zero but the probability that  $|A + A| = |A - A|$  tends to one, and hence a typical set is balanced in this case. The cause of this marked difference in behavior is that subsets of  $\{0, \dots, n\}$  have a fringe, whereas finite groups do not. We end with a detailed analysis of dihedral groups, where the results are in striking contrast to what occurs for subsets of integers. Specifically, even though almost all subsets of dihedral groups are balanced as the size grows, more sets are sum-dominated than difference-dominated.

## CONTENTS

1.	Introduction	2
2.	Subsets of Finite Groups	3
3.	Sum Dominated sets in Dihedral Groups	6
3.1.	Cyclic Group Preliminaries	6
3.2.	Dihedral Group Case	8
4.	Conclusion	9
	References	10

---

*Date:* August 9, 2013.

*2010 Mathematics Subject Classification.* 11B13, 11P99 (primary), 05B10, 11K99 (secondary).

*Key words and phrases.* More Sum Than Difference sets, sum-dominated and difference-dominated sets, MSTD, sumsets, finite Abelian groups, dihedral group.

The first named author was partially supported by NSF Grant DMS0970067, and the second named author was partially supported by NSF Grant DMS0850577. We thank the participants of the 2012 SMALL REU program, especially Ginny Hogan and Nicholas Triantafillou, as well as Kevin O’Bryant, for helpful discussions.

## 1. INTRODUCTION

Given a subset  $S$  of a group  $G$ , we define its sumset  $S + S$  and difference set  $S - S$  by

$$\begin{aligned} S + S &= \{a_i + a_j : a_i, a_j \in A\} \\ S - S &= \{a_i - a_j : a_i, a_j \in A\}, \end{aligned} \tag{1.1}$$

and let  $|X|$  denote the cardinality of  $X$ . Notice that we're writing the group action as addition, but are not assuming commutativity. If we were to write the action multiplicatively we would still call these the sumset and the difference set, instead of the product and quotient sets, to match the language from earlier work which studied subsets of the integers.

If  $|S + S| > |S - S|$  then  $S$  is sum-dominant or an MSTD (more sums than differences) set, while if  $|S + S| = |S - S|$  we say  $S$  is balanced and if  $|S + S| < |S - S|$  then  $S$  is difference-dominated. If we let the group  $G$  be the integers, then we expect that for a 'generic' set  $S$  we have  $|S - S| > |S + S|$ . This is because addition is commutative while subtraction is not, since a typical pair  $(x, y)$  contributes one sum and two differences.

Though MSTD sets are rare among all finite subsets of integers, they do exist. Examples of MSTD sets go back to the 1960s. Conway is credited with finding  $\{0, 2, 3, 4, 7, 11, 12, 14\}$ ; for other early examples see also Marica [Ma] and Freiman and Pigearev [FP]. Recently there has been much progress in finding infinite families, either through explicit constructions (see Hegarty [He] and Nathanson [Na1]), and existence arguments via non-constructive methods (see Ruzsa [Ru1, Ru2, Ru3] and Miller-Orosz-Scheinerman [MOS]). The main result in the subject is due to Martin and O'Bryant [MO], who proved a positive percentage of subsets of  $\{0, 1, \dots, N\}$  are sum-dominant, though the percentage is small (work of Zhao [Zh2] suggests it is around  $4.5 \cdot 10^{-4}$ ).

Almost all previous research on MSTD sets focused exclusively on subsets of the integers, though recently Zhao [Zh1] extended previous results of Nathanson [Na2], who showed that MSTD sets of integers can be constructed from MSTD sets in finite abelian groups. Zhao provides asymptotics for the number of MSTD sets in finite abelian groups. An immediate corollary of the main theorem in [Zh2] is that if  $\{G_n\}$  is a sequence of finite abelian groups with  $|G_n| \rightarrow \infty$  then the percentage of MSTD sets is almost surely 0. In this paper we not only extend this result to difference-dominated sets but to non-abelian finite groups as well.

**Theorem 1.1.** *Let  $\{G_n\}$  be a sequence of finite groups, not necessarily abelian, with  $|G_n| \rightarrow \infty$ . Let  $S_n$  be a uniformly chosen random subset of a  $G_n$ . Then  $\mathbb{P}(S_n + S_n = S_n - S_n = G) \rightarrow 1$  as  $n \rightarrow \infty$ . In other words, as the size of the finite group grows almost all subsets are balanced (with sumset and difference set the entire group).*

While Theorem 1.1 shows that in the limit almost all subsets of finite groups are balanced, it leaves open the relative behavior of sum-dominant and difference-dominant sets. Though the number of such sets are lower order and percentagewise tends to zero, are there more, equal or fewer sum-dominant or difference-dominant sets? For example, Figure 1 shows the result of numerical simulations for 10,000 clock groups  $\mathbb{Z}/n\mathbb{Z}$  for  $n \in \{10, \dots, 100\}$ .

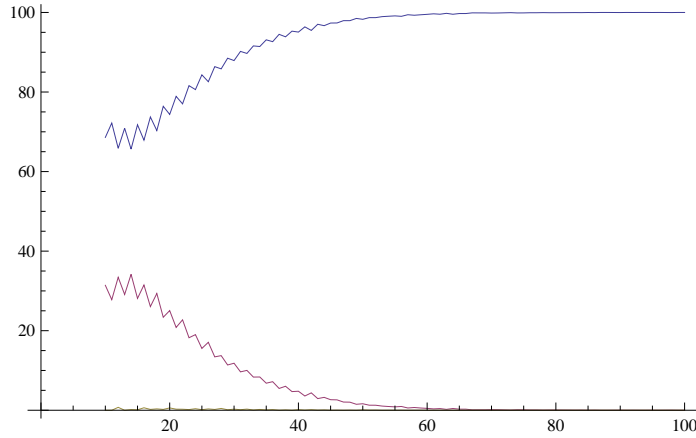


FIGURE 1. Numerical simulations on the number of balanced, difference-dominated and sum-dominated subsets of  $\mathbb{Z}/n\mathbb{Z}$  for  $n \in \{10, \dots, 100\}$ . For each  $n$  we uniformly chose 10,000 random subsets of  $\{1, \dots, n\}$ . Top plot is the percentage of balanced, middle is the percentage of difference-dominated, and bottom is the percentage of sum-dominated.

In Section 3.2 we explore this question for subsets of dihedral groups, and see very different behavior than in the integers. We conjecture that while almost all subsets of the dihedral group are balanced, there are more MSTD sets than there are difference-dominated sets, in sharp contrast to the prevalence of difference-dominated subsets of the integers.

The paper is organized as follows. We first prove our main result for all finite groups in §2. We then explore the MSTD sets of the dihedral group in §3. We end with some concluding remarks and suggestions for future research.

## 2. SUBSETS OF FINITE GROUPS

Martin and O’Bryant [MO] showed that although MSTD subsets of the integers are rare, they are a positive percentage of subsets. MSTD sets in finite groups are even rarer. We will prove that as the size of a finite group tends to infinity, the probability that a subset chosen uniformly at random is sum-dominant tends to zero. Somewhat surprisingly, this is also true for difference-dominated sets. This is very different than the integer case, where more than 99.99% of all subsets are difference-dominated.

The reason the integers behave differently than finite groups is that a subset of the integers contains fringe elements, which we now define. Let  $S$  be a subset of  $I_n := \{0, 1, \dots, n\}$  chosen uniformly at random. The elements of  $S$  near 0 and  $n$  are called the fringe elements. Interestingly the notion of nearness is independent of  $n$ ; the reason is that almost all possible elements of  $I_n + I_n$  and  $I_n - I_n$  are realized respectively by  $S + S$  and  $S - S$ ; Martin and O’Bryant [MO] prove that  $S + S$  and  $S - S$  miss on average 10 and 6 elements, while Lazarev, Miller and O’Bryant [LMO] prove the variance is bounded independent of  $n$ . Thus whether or not a set is sum-dominant is essentially controlled by the fringe elements of  $S$ , as the ‘middle’ is filled with probability 1 and the presence and absence of fringe elements control the extremes. In a finite group,

there are no fringe elements since each element can be written as  $|G|$  different sums and differences, and thus most elements appear in the sumset or difference set with high probability.

In the proof of Theorem 1.1 we reduce certain probabilities to products of Lucas numbers  $L(n)$ ; these satisfy the recurrence  $L(n+2) = L(n+1) + L(n)$  with initial conditions  $L(0) = 2$  and  $L(1) = 1$ . Note this is the same recurrence relation as the Fibonacci numbers  $F(n)$ , who differ from the Lucas numbers in that their initial conditions are  $F(0) = 0$  and  $F(1) = 1$ .

The following lemma is useful, and is in the spirit of calculations from [LMO]. The interpretation will be that the red vertices correspond to elements chosen to be in an  $S$ , and the condition that no neighboring vertices are both colored red will ensure that certain elements are not represented in  $S + S$ .

**Lemma 2.1.** *Let  $C_n = \{a_1, \dots, a_n\}$  denote a closed chain of  $n$  elements (so  $a_1$  is adjacent to  $a_2$  and  $a_n$ , and so on). If  $P(n)$  is the number of ways to color the vertices of  $C_n$  red or blue such that no two neighboring vertices are colored red, then  $P(n) = L(n)$ .*

*Proof.* We derive a recurrence formula for  $P(n)$ . We may draw  $C_n$  as a regular  $n$ -gon with the  $a_i$ 's as the vertices. Let  $A(n)$  denote the number of ways a line with  $n$  vertices  $a_1, a_2, \dots, a_n$  can be colored red or blue so that no two neighboring vertices are colored red. We have

$$P(n) = A(n-1) + A(n-3). \quad (2.1)$$

To see this, there are two cases. Consider the first vertex,  $a_1$ . If it is colored blue then we may ‘break’ the chain at  $a_1$  and the problem reduces to determining the number of ways to color  $n-1$  vertices on a line red or blue so that no two neighboring ones are both red; by definition this is  $A(n-1)$ . Alternatively, if  $a_1$  is colored red then  $a_2$  and  $a_n$  must both be colored blue, and thus we are left with coloring  $n-3$  vertices on a line so that no two consecutive vertices are both red; again, by definition this is just  $A(n-3)$ .

Thus the lemma is reduced to computing  $A(n)$ , which satisfies the Fibonacci-Lucas recurrence. To see this, consider  $n$  vertices on a line, with  $A(n)$  the number of ways to color these red and blue so that no neighbors are both colored red. If the first vertex is colored blue, then by definition there are  $A(n-1)$  ways to color the remaining vertices, while if the first vertex is colored red then the second must be colored blue, leaving  $A(n-2)$  ways to color the remaining vertices. Thus

$$A(n) = A(n-1) + A(n-2). \quad (2.2)$$

It is easy to see that  $A(1) = 2$  and  $A(2) = 3$ , which implies

$$A(n) = F(n+2), \quad (2.3)$$

where  $F(n)$  is the  $n^{\text{th}}$  Fibonacci number. As  $P(n) = A(n-1) + A(n-3)$ , we find

$$P(n) = F(n+1) + F(n-1). \quad (2.4)$$

As the  $n^{\text{th}}$  Lucas number satisfies

$$L(n) = F(n+1) + F(n-1) \quad (2.5)$$

(this can easily be proved directly, or see for example [BQ]), we find  $P(n) = L(n)$  as claimed.  $\square$

We now prove our main theorem.

*Proof of Theorem 1.1.* We start by showing that the probability a  $g \in G = \{g_1, g_2, \dots, g_n\}$  is in  $S + S$  approaches 1 exponentially fast. For  $g \in G$ , we have

$$\mathbb{P}(g \notin S + S) = \mathbb{P}(x \notin S \vee y \notin S \quad \forall x, y \in G \text{ s.t. } x + y = g). \quad (2.6)$$

To determine the probability that  $S + S$  is not all of  $G$  we will add the probabilities  $\mathbb{P}(g \notin S + S)$  for each  $g$ . Note these probabilities are not independent, as  $x \notin G$  affects the probability of several  $g$  being in  $S + S$ .

We concentrate on a fixed  $g$ . If  $x \in G$  then there exist a chain of elements  $\{x_1, x_2 \dots x_n\} = X \subseteq G$  such that

$$x + x_1 = x_2 + x_3 = \dots = x_{n-1} + x_n = x_n + x = g, \quad (2.7)$$

; clearly the pairs depend on  $g$ . Note that  $X$  also depends on the choice of  $x \in G$ . If we denote all distinct chains as  $X_1, \dots, X_n$  then these sets partition  $G$ . If  $S$  is a subset of  $G$ , for  $g$  not to be represented in  $S + S$  we need at least one element of each pair in each  $X_i$  to fail to be in  $S$ . The number of ways this can happen is  $\prod L(|X_i|)$ , where  $L(n)$  is the  $n^{\text{th}}$  Lucas number.

To see this equality we use a method similar to that used by Lazarev, Miller, and O'Bryant in [LMO]. Counting the number of subsets of  $X_i$  such that we never take two adjacent elements is equivalent to counting the number of ways the vertices of a regular polygon with  $|X_i| = n$  vertices can be colored with two colors (say red and blue) such that no two adjacent vertices are blue. Note that each subset  $S$  of vertices with this property is equivalent to a set where  $g \notin S + S$ , and since the  $X_i$  partition  $G$ , then by Lemma 2.1 the number of such colorings is  $\prod L(|X_i|)$ . Combining the independence of the  $X_i$  with Lemma 2.1, we conclude,

$$\mathbb{P}(g \notin S + S) = \frac{\prod L(|X_i|)}{2^{|G|}}. \quad (2.8)$$

For example, take the element  $a + b \in D_6 = \langle a, b | a + a + a, b + b, a + b + a + b \rangle$ , where  $D_6$  is the dihedral group with six elements. Here we have that

$$a + b = (a + b) + (a + a + a) = (a + a + a) + (a + b) \quad (2.9)$$

and

$$a + b = (a + a) + (a + a + b) = (a + a + b) + (a) = (a) + (b) = (b) + (a + a), \quad (2.10)$$

where plus denotes the group operation. The two chains we obtain are  $X_1 = \{a + b, a + a + a\}$  and  $X_2 = \{a + a, a + a + b, a, b\}$ . Letting  $S_{X_1} = S \cap X_1$  and  $S_{X_2} = S \cap X_2$  we have that

$$\begin{aligned} \mathbb{P}(a + b \notin S + S) &= \mathbb{P}(a + b \notin S_{X_1} + S_{X_1}) \mathbb{P}(a + b \notin S_{X_2} + S_{X_2}) \\ &= \left( \frac{L(2)}{2^2} \right) \left( \frac{L(4)}{2^4} \right), \end{aligned} \quad (2.11)$$

where the latter equality occurs because of Lemma 2.1.

Note that  $L(n) = \phi^n + (-\phi)^{-n}$  where  $\phi = \frac{1+\sqrt{5}}{2}$  is the golden ratio. As the  $X_i$ 's are disjoint, we obtain for each  $g \in G$  that

$$\mathbb{P}(g \notin S + S) = \frac{\prod L(|X_i|)}{2^{|G|}} \leq \frac{\prod 1.8^{|X_i|}}{2^{|G|}} = \left(\frac{1.8}{2}\right)^{|G|}. \quad (2.12)$$

As crude bounds suffice, we use the union bound to bound the contribution from each element in  $G$ , and find

$$\mathbb{P}(|S+S| < |G|) = \mathbb{P}(\cup_{g \in G} g \notin G) \leq \sum_{g \in S+S} \mathbb{P}(g \notin S+S) \leq |G| \left(\frac{1.8}{2}\right)^{|G|}. \quad (2.13)$$

As the size of the group approaches infinity, we have that  $\mathbb{P}(|S+S| < |G|)$  approaches zero. The same argument holds for  $S - S$  since there is a one to one bijection between group elements and their inverses. Thus most subsets are balanced.  $\square$

**Remark 2.2.** *The above arguments do not apply to subsets of the integers. The reason is due to the lack of a group structure. In particular, the result from equation (2.7) does not hold and different elements have different number of representations as a sum or a difference. For example, for the integers the number of pairs  $(x, y) \in \{0, \dots, n-1\}^2$  such that  $x + y = k$  is a triangular function of  $k$ , peaking when  $k = n-1$ . Thus whether or not small (near 0) or large (near  $2n-2$ )  $k$  are in the sumset is controlled by the fringe elements of our set. A similar result holds for differences, and thus if the fringe is carefully chosen then we can force our set to be sum-dominant or difference-dominant. Note such forcing arguments cannot happen with a group structure.*

Note that we used 1.8 as a very crude bound. While  $\prod L(|X_i|)$  is much closer to  $\phi^n$  then it is to  $1.8^n$ , since  $\phi^0$  is less than  $L(0)$ ,  $\phi^n$  does not provide an inequality for all  $n$ .

### 3. SUM DOMINATED SETS IN DIHEDRAL GROUPS

Although sum-dominated sets and difference-dominated sets are rare in arbitrarily large finite groups, we can compare the size of the number of sum-dominated subsets and difference-dominated subsets in any fixed finite group. In this section we first explore the sumset and difference set of cyclic groups. We then apply those results to give intuition on why in any dihedral group, there should be more sum-dominated sets than difference-dominated sets.

**3.1. Cyclic Group Preliminaries.** Before we look at the dihedral group, we explore two different cases in cyclic groups. In the first case we compute the probability of an element missing in the sumset and difference set. In the second case we compute the probability of missing an element in  $A + B$  where  $A$  and  $B$  are both subsets of  $\mathbb{Z}/n\mathbb{Z}$ .

**Lemma 3.1.** *Let  $S$  be a uniformly chosen random subset of  $\mathbb{Z}/n\mathbb{Z}$ . Then*

$$\mathbb{P}(k \notin S + S) = O\left((3/4)^{n/2}\right). \quad (3.1)$$

*Proof.* Let  $k \in \mathbb{Z}/n\mathbb{Z}$ . Since addition is commutative, all sets of pairs of elements that sum to  $k$  partition the group. Furthermore, the number of pairs of distinct elements in  $\mathbb{Z}/n\mathbb{Z}$  is equal to either  $n/2$ ,  $n/2 - 1$  or  $(n-1)/2$ . The number of distinct pairs depends

on the parity of  $n$  and  $k$ . From the independence of the pairs of elements that sum to  $k$ , we have

$$\mathbb{P}(k \notin S + S) = \prod_{0 \leq i \leq \lceil (n+1)/2 \rceil} \mathbb{P}(i \notin S \vee k - i \notin S). \quad (3.2)$$

Finally, since counting the number of distinct pairs is straightforward, we conclude

$$\mathbb{P}(k \notin S + S) = \begin{cases} (1/2)^2 (3/4)^{n/2-1} & k \text{ even and } n \text{ even} \\ (3/4)^{n/2} & k \text{ odd and } n \text{ even} \\ (1/2)(3/4)^{(n-1)/2} & n \text{ odd.} \end{cases} \quad (3.3)$$

The factor of  $1/2$  is due to the number of elements  $x \in \mathbb{Z}/n\mathbb{Z}$  such that  $x + x = k$ . Again, the number of these elements depends on the parity of  $n$  and  $k$ .  $\square$

**Lemma 3.2.** *Let  $S_1$  and  $S_2$  be uniformly chosen random subsets of  $\mathbb{Z}/n\mathbb{Z}$ . Then*

$$\mathbb{P}(k \notin S_1 + S_2) = (3/4)^n. \quad (3.4)$$

*Proof.* Let  $k \in \mathbb{Z}/n\mathbb{Z}$ . The claim follows immediately from the fact that

$$\mathbb{P}(k \notin S_1 + S_2) = \prod_{0 \leq i \leq n-1} \mathbb{P}(i \notin S_1 \vee k - i \notin S_2) \quad (3.5)$$

and the fact that these  $n$  products are mutually independent.  $\square$

**Lemma 3.3.** *Let  $S$  be a uniformly chosen random subset of  $\mathbb{Z}/n\mathbb{Z}$ . Then*

$$\mathbb{P}(k \notin S - S) = \frac{L(n/d)^d}{2^n} = O((\phi/2)^n), \quad (3.6)$$

where  $\gcd(k, n) = d$ ,  $L(n)$  is the  $n^{\text{th}}$  Lucas number, and  $\phi$  is the golden ratio.

*Proof.* Let  $k \in \mathbb{Z}/n\mathbb{Z}$ . Since the order of  $k$  in  $\mathbb{Z}/n\mathbb{Z}$  is equal to  $n/\gcd(n, k)$ , if we have a set  $\{x_1, x_2, \dots, x_m\}$  such that  $x_1 - x_2 = x_2 - x_3 = \dots = x_m - x_1 = k$  then  $m = n/\gcd(n, k)$ . These sets partition the group and thus, the number of subsets of  $\mathbb{Z}/n\mathbb{Z}$  that satisfy this property is  $\gcd(n, k)$ . Combining the fact that these sets have a pairwise trivial intersection with Lemma 2.1 we have

$$\mathbb{P}(k \notin S - S) = \frac{L(n/d)^d}{2^n}, \quad (3.7)$$

as desired.  $\square$

**Lemma 3.4.** *Let  $S_1$  and  $S_2$  be uniformly chosen random subsets of  $\mathbb{Z}/n\mathbb{Z}$ . Then*

$$\mathbb{P}(k \notin S_1 - S_2) = \left(\frac{3}{4}\right)^n. \quad (3.8)$$



*Proof.* The proof follows immediately from the following equalities:

$$\begin{aligned}
\mathbb{P}(k \notin S_1 - S_2) &= \prod_{x \in \mathbb{Z}/n\mathbb{Z}} \mathbb{P}(x \notin S_1 \cup x - k \notin S_2) \\
&= \prod_{x \in \mathbb{Z}/n\mathbb{Z}} (1 - \mathbb{P}(x \in S_1 \cap x - k \notin S_2)) \\
&= \prod_{x \in \mathbb{Z}/n\mathbb{Z}} (1 - \mathbb{P}(x \in S_1)\mathbb{P}(x - k \notin S_2)) \\
&= \left(\frac{3}{4}\right)^n.
\end{aligned} \tag{3.9}$$

□

**Proposition 3.5.** *Let  $S$  be uniformly chosen random subsets of  $\mathbb{Z}/n\mathbb{Z}$  then as  $n$  approaches infinity  $\mathbb{P}(|S + S| = |S - S| = n)$  approaches 1.*

*Proof.* This is immediate from the union bound and Lemmas 3.1, 3.2, 3.3 and 3.4. □

**3.2. Dihedral Group Case.** Let  $S$  be a subset of  $D_{2n} = \langle a, b | a^n, b^2, abab \rangle$  chosen uniformly at random. We first give a proof for the dihedral group subcase of Theorem 1.1 by using the previous lemmas. Before we do so we need two results. The first looks at the probability of a rotation element ( $k = a^i$ ) not being in the sumset. The second looks at the probability of a reflection element ( $k = a^i b$ ) not being in the sumset. We denote the set of all rotation elements by  $R$  and the set of all reflection elements by  $F$ .

**Lemma 3.6.** *Let  $S$  be a uniformly chosen random subset of  $D_{2n}$  and let  $k \in D_{2n}$  such that  $k = a^i$ . Then  $\mathbb{P}(k \notin S + S) \leq (3/4)^{n/2}(\phi/2)^n$  and  $\mathbb{P}(k \notin S - S) \leq (\phi/2)^{2n}$ .*

*Proof.* An element of the form  $a^i$  can be written as a product of two rotations,  $a^x a^y$  where  $x + y = i$ , or the product of two reflections,  $a^x b a^y b$  where  $x - y = i$ . Since the set of rotations and the set of reflections can be viewed as cyclic groups the proofs follow immediately from Lemmas 3.1 and 3.3. □

**Lemma 3.7.** *Let  $S$  be a uniformly chosen random subset of  $D_{2n}$  and let  $k \in D_{2n}$  such that  $k = a^i b$ . Then  $\mathbb{P}(k \notin S + S) \leq (3/4)^n$  and  $\mathbb{P}(k \notin S - S) \leq (3/4)^n$ .*

*Proof.* Since an element of the form  $a^i b$  can be written as a product of a rotation and a reflection the proof follows immediately from Lemma 3.2. □

**Theorem 3.8.** *Let  $S$  be a uniformly random subset of  $D_{2n}$ . Then, as  $n$  approaches infinity,  $\mathbb{P}(|S + S| = |S - S|)$  approaches 1.*

*Proof.* The proof follows immediately from applying the union bound to Lemmas 3.6 and 3.7. □

Note that by Theorem 1.1 we know that the percentage of sum-dominated and difference-dominated sets goes to zero at an exponential rate. However, if we look at any fixed  $D_{2n}$  we conjecture that the number of sum-dominated subsets is greater than the number of difference-dominated subsets. For the first few dihedral groups (up to  $D_{16}$ ) Figure 2 shows an exhaustive comparison of the subsets of  $D_{2n}$ . Figure 2 also includes a sample



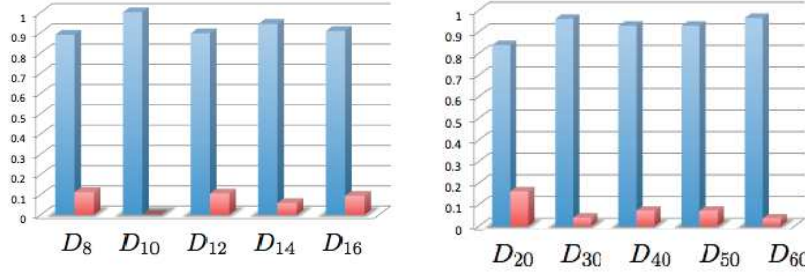


FIGURE 2. Relative number of sum-dominated sets (larger values) versus difference-dominated sets (lower values) in dihedral groups.

statistic for larger dihedral groups. Note that it is hard to continue a complete enumeration.

As Figure 2 suggests, sum-dominated sets are more likely to appear than difference-dominated sets. Let  $S = R \cup F$  where  $R$  is the set of rotations in  $S$  and  $F$  is the set of reflections in  $S$ . From Table 1 we note that the difference in what contributes to the sumsets and difference sets is  $R - R$  which contributes to the difference set and  $F - R$  and  $R + R$  which contributes to the sumset. It is due to this that there are more sum-dominated sets than difference-dominated sets.

Set	Rotations in the Set	Reflections in the Set
S	$R$	$F$
S+S	$R + R, F + F$	$R + F, -R + F$
S-S	$R - R, F + F$	$R + F$

TABLE 1. How elements contribute to the size of  $S + S$  versus  $S - S$ .

#### 4. CONCLUSION

We have shown that finite groups behave differently than the integers in the sense that almost all subsets are balanced. The reason is that finite groups do not have a fringe. As a result, in finite groups almost all sumsets and difference sets are equal to the entire group. The dihedral group case also hints at the importance of the size of the commutator subgroup and the number of order two elements. It is easy to see that the size of the sumset is greater when the commutator subgroup is small while the size of the difference set is lower due to the greater amount of order two elements.

A natural question to ask is what would happen if we no longer weight each subset equally. When each subset is chosen with uniform probability then the probability of the subset being balanced is equal to 1; however, in  $\mathbb{Z}/n\mathbb{Z}$ , if we take subsets of the first half of the group (i.e.,  $\bar{0}, \bar{1}, \dots, \bar{\lfloor \frac{n}{2} \rfloor}$ ) then the sumsets and difference sets behave like they would in  $\mathbb{Z}$ . Thus, the percentage of balanced groups is closer to 0. It would be interesting to explore where the phase transition occurs.

Another question to ask is what happens when we look at non-abelian infinite groups. One difficulty is how we approach subsets of infinite groups. For example, if we look at  $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$  we have two different ways to limit the size of the subset. One possibility is to

require  $S$  to be a subset of a finite subgroup. This would allow for an easier computation of the limiting behavior, though we would have to determine the probability it lives in each finite subgroup.

## REFERENCES

- [BQ] A. T. Benjamin and J. J. Quinn, *Proofs that Really Count: The Art of Combinatorial Proof*, the Mathematical Association of America, Washington, 2003.
- [FP] G. A. Freiman and V. P. Pigarev, *The relation between the invariants  $R$  and  $T$* , Number theoretic studins in the Markov Spectrum and in the structural theory of set addition (Russian), Kalinin GOs. Univ., Moscow, 1973, 172–174.
- [GO] G. Martin and K. O’Bryant, *Many sets have more sums than differences*, CRM Proceedings & Lecture Notes **43**, American Mathematical Society (Providence, RI, 2007), 287–305.
- [He] P. V. Hegarty, *Some explicit constructions of sets with more sums than differences* (2007), Acta Arithmetica **130** (2007), no. 1, 61–77.
- [ILMZ] G. Iyer, O. Lazarev, S. J. Miller and L. Zhang, *Finding and Counting MSTD sets* (2011), to appear in the conference in the conference proceedings of the 2011 Combinatorial and Additive Number Theory Conference.
- [LMO] O. Lazarev, S. J. Miller and K. O’Bryant, *Distribution of Missing Sums in Sumsets* (2013), Experimental Mathematics **22** (2013), no. 2, 132–156.
- [Ma] J. Marica, *On a conjecture of Conway*, Canad. Math. Bull. 12 (1969), 233–234.
- [MO] G. Martin and K. O’Bryant, *Many sets have more sums than differences*, Additive combinatorics, 287–305, CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI, 2007.
- [MOS] S. J. Miller, B. Orosz and D. Scheinerman, *Explicit constructions of infinite families of MSTD sets*, Journal of Number Theory **130** (2010), 1221–1233.
- [Na1] M. B. Nathanson, *Sets with more sums than differences*, Integers : Electronic Journal of Combinatorial Number Theory **7** (2007), Paper A5 (24pp).
- [Na2] M. B. Nathanson, *Problems in additive number theory. I*, Additive combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 263–270
- [Ru1] I. Z. Ruzsa, *On the cardinality of  $A + A$  and  $A - A$* , Combinatorics year (Keszthely, 1976), vol. 18, Coll. Math. Soc. J. Bolyai, North-Holland-Bolyai Tàrsulat, 1978, 933–938.
- [Ru2] I. Z. Ruzsa, *Sets of sums and differences*, Séminaire de Théorie des Nombres de Paris 1982–1983 (Boston), Birkhäuser, 1984, 267–273.
- [Ru3] I. Z. Ruzsa, *On the number of sums and differences*, Acta Math. Sci. Hungar. **59** (1992), 439–447.
- [Zh1] Y. Zhao, *Counting MSTD Sets in Finite Abelian Groups*, J. Number Theory **130** (2010), 2308–2322.
- [Zh2] Y. Zhao, *Sets Characterized by Missing Sums and Differences*, Journal of Number Theory **131** (2011), 2107–2134.

*E-mail address:* [sjml@williams.edu](mailto:sjml@williams.edu), [Steven.Miller.MC.96@aya.yale.edu](mailto:Steven.Miller.MC.96@aya.yale.edu)

DEPARTMENT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267

*E-mail address:* [kvissuet@ucsd.edu](mailto:kvissuet@ucsd.edu)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA SAN DIEGO, LA JOLLA, CA 91941