More Sums Than Differences Sets in Finite Non-Abelian Groups

John Haviland (havijw@umich.edu)
Phúc Lâm (plam6@u.rochester.edu)
John Lentfer (jlentfer@hmc.edu)
Joint work with Elena Kim, Fernando Trejos Suárez, and Steven J. Miller

Young Mathematicians Conference
Ohio State University
08/14/2020

Introduction

Definition

Given a finite subset S of a group G, written additively, we define its **sum set**

$$S + S := \{s_1 + s_2 : s_1, s_2 \in S\},$$

and **difference set**

$$S - S := \{s_1 - s_2 : s_1, s_2 \in S\}.$$

Definition

A finite set S is called **MSTD** ("more sums than differences") if

$$|S+S| > |S-S|,$$

MDTS ("more differences than sums") if

$$|S+S| < |S-S|,$$

and **balanced** if

$$|S+S| = |S-S|.$$

Major Results in $\mathbb{Z}$

Theorem (Martin, O'Bryant)

Let $P = \{0, 1, \ldots, n\}$. For $n \geq 14$, there exists $0 < c < 1$ such that at least $c \cdot 2^{n+1}$ of the subsets of P are MSTD, MDTS, and balanced respectively.

Theorem (Zhao)

The proportions of MSTD, MDTS, and balanced subsets of P all converge to limits as $n \to \infty$.

- Zhao proved: MSTD limit $> 4.28 \cdot 10^{-4}$
- Monte Carlo: MSTD limit $\approx 4.5 \cdot 10^{-4}$

MSTD in Integers vs. Finite Groups

- In finding MSTD subsets of $\{0, 1, \ldots, n\} \subseteq \mathbb{Z}$, we usually look at "fringes."

- However, we do not have that "fringe" structure in finite groups. That is because unlike in $\mathbb{Z}$, finite groups do not have an ordering that respects addition.
- For example, in $\mathbb{Z}/n\mathbb{Z}$, the sumset "wraps around" and overlaps itself, destroying the fringe structure.

MSTD in Finite Abelian Groups

Theorem (Zhao)

- *The number of MSTD subsets of* $\mathbb{Z}/n\mathbb{Z}$ *is*

$$\sim \begin{cases} 3^{n/2} & \text{odd } n \\ \frac{n\phi^n}{2} & \text{even } n \end{cases}$$

- *The number of MSTD subsets of* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *is*

$$\sim \begin{cases} 3^{n+1} & \text{odd } n \\ 3^{n} & \text{even } n \end{cases}$$

MSTD in Finite Groups

Theorem (Miller-Vissuet 2014)

Let $\{G_n\}$ be a family of finite groups, not necessarily abelian, such that $|G_n| \to \infty$. If S_n is a uniformly chosen random subset of G_n, then $\mathbb{P}(S_n + S_n = S_n - S_n = G_n) \to 1$ as $n \to \infty$.

Proof idea.

- Given $g \in G_n$, form a partition of the group with chains $X = \{x_1, \dots, x_\ell\}$ such that

$$x_1 + x_2 = x_2 + x_3 = \cdots = x_\ell + x_1 = g$$

- Show $\mathbb{P}(g \notin S_n + S_n)$ and $\mathbb{P}(g \notin S_n - S_n)$ are each

$$\frac{\prod_X L(|X|)}{2^{|G_n|}} \leq \frac{\prod_X 1.8^{|X|}}{2^{|G_n|}} \to 0 \text{ as } n \to \infty$$

The Dihedral Group

MSTD in D_{2n}

- Miller and Vissuet looked the Dihedral group D_{2n}
- Started by proving probabilistic results in $\mathbb{Z}/n\mathbb{Z}$

Theorem (Miller-Vissuet)

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

$$\mathbb{P}(k \notin S_1 + S_1) = O((3/4)^{n/2})$$
$$\mathbb{P}(k \notin S_1 - S_1) = O((\phi/2)^{n})$$
$$\mathbb{P}(k \notin S_1 + S_2) = (3/4)^{n}$$
$$\mathbb{P}(k \notin S_1 - S_2) = (3/4)^{n}.$$

From $\mathbb{Z}/n\mathbb{Z}$ to D_{2n}

- To apply these results in D_{2n}, decompose S into rotations and reflections: $S = R \cup F$

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

- $S+S$ has contributions from $R+R$ and $-R+F$
- $S-S$ has contributions from $R-R$

Conjecture

There are more MSTD than MDTS subsets of D_{2n}.

Exact Probabilities in $\mathbb{Z}/n\mathbb{Z}$

We can improve one of Miller and Vissuet's results:

Theorem (SMALL 2020)

Let $S \subseteq \mathbb{Z}/n\mathbb{Z}$. Then,

$$\mathbb{P}(k \notin S + S) = (3/4)^{n/2} \left(\frac{\sqrt{3} + 2}{6} \right).$$

Proof.

Find exact probabilities for given parity of k and n, then average. □

Expected Size of $|R+R|$ and $|-R+F|$

- For $S = R \cup F \subseteq D_{2n}$,

$$\mathbb{E}(|R+R|) = n\left(1 - (3/4)^{n/2}\frac{\sqrt{3}+2}{6}\right)$$

$$\mathbb{E}(|-R+F|) = n(1-(3/4)^{n/2})$$

- Thus,

$$\mathbb{E}(|R+R|+|-R+F|) = n\left(2 - (3/4)^{n/2}\frac{\sqrt{3}+8}{6}\right)$$

Comparing to $|R - R|$

- $R - R$ is all rotations, so $|R - R| \leq n$. So,

$$\mathbb{E}(|R - R|) \leq n.$$

- Comparing $|R - R|$ and $|R + R| + |-R + F|$,

$$\mathbb{E}(|R + R| + |-R + F|) \geq \mathbb{E}(|R - R|)$$

$$\Updownarrow$$

$$n\left(2 - (3/4)^{n/2}\frac{\sqrt{3} + 8}{6}\right) \geq n.$$

- This holds for $n > 3$.

Back to Sum and Difference Sets

- How can we use these results to show there are more MSTD than MDTS sets?
- $|R + R| + |-R + F| > |R - R|$ doesn't mean $|S + S| > |S - S|$
- For example, if $|S| > n$, then $S + S = S - S = D_{2n}$, but above still holds
- Have to consider overlap with $F + F$ and $R + F$ to get actual expected size of $|S + S| - |S - S|$

Cayley Tables for D_{2n}

Cayley Tables

A **Cayley Table** describes the structure of a finite group by showing all combinations of two group elements with the group operation.

Cayley Table for D_6:

$+$		rot.			ref.		
		1	r	r^2	s	rs	r^2s
rot.	1	1	r	r^2	s	rs	r^2s
	r	r	r^2	1	rs	r^2s	s
	r^2	r^2	1	r	r^2s	s	rs
ref.	s	s	r^2s	rs	1	r^2	r
	rs	rs	s	r^2s	r	1	r^2
	r^2s	r^2s	rs	s	r^2	r	1

Inverse Column Cayley Tables

An **Inverse Column Cayley Table** describes the structure of a finite group by showing all combinations of two group elements with the inverse of the group operation.

Inverse Column Cayley Table for D_6:

	$-$	rot.			ref.		
		1	r	r^2	s	rs	r^2s
rot.	1	1	r^2	r	s	rs	r^2s
	r	r	1	r^2	rs	r^2s	s
	r^2	r^2	r	1	r^2s	s	rs
ref.	s	s	rs	r^2s	1	r^2	r
	rs	rs	r^2s	s	r	1	r^2
	r^2s	r^2s	s	rs	r^2	r	1

Number of Asymmetric Elements

- We used $+$ and $-$ tables to find formulas for the number of asymmetric elements.
- The tables have small differences for n odd or even.
- For the $+$ table, the number of asymmetric elements is

$$2n\left(2\left\lfloor\frac{n+1}{2}\right\rfloor+n-\left\lfloor\frac{n}{2}\right\rfloor-3\right)$$

- For the $-$ table, the number of asymmetric elements is

$$4n(n-\left\lfloor\frac{n}{2}\right\rfloor-1)$$

Lemma (SMALL 2020)

There are more asymmetric elements in the $+$ table than the $-$ table for D_{2n} for $n \geq 3$.

Probability of a Subset Being MSTD or MDTS

- We want to find the probability of a subset A of D_{2n} being MSTD or MDTS.
- We can do this by conditioning on the size of A.
- We notice that if $|A| = 1$, then $|A + A| = |A - A| = 1$, so it is balanced.
- We also have the following lemma

Lemma (SMALL 2020)

If $|A| > n$, then $|A + A| = |A - A| = |D_{2n}|$.

Probability When $|A| = 2$

- When $|A| = 2$, there are three possibilities for the distribution of $|R|$ and $|F|$: $|R| = 2$ and $|F| = 0$, $|R| = 1$ and $|F| = 1$, and $|R| = 0$ and $|F| = 2$.
- By conditioning on these three, using the Law of Total Probability, we get the following expression:

$$
\begin{aligned}
&\mathbb{P}(|A+A| > |A-A| : |A| = 2) \\
&= \mathbb{P}(|A+A| > |A-A| : |A| = 2 \cap |R| = 2)\mathbb{P}(|R| = 2 : |A| = 2) \\
&+ \mathbb{P}(|A+A| > |A-A| : |A| = 2 \cap |R| = 1)\mathbb{P}(|R| = 1 : |A| = 2) \\
&+ \mathbb{P}(|A+A| > |A-A| : |A| = 2 \cap |R| = 0)\mathbb{P}(|R| = 0 : |A| = 2)
\end{aligned}
$$

Lemma (SMALL 2020)

$$\mathbb{P}(|A+A| > |A-A| : |A| = 2) > \mathbb{P}(|A+A| < |A-A| : |A| = 2)$$

Breaking Down Sets Based on Size

What can we say about sets of sizes between 3 and n?

Lemma (SMALL 2020)

For odd n, $\mathbb{P}(|A+A| < |A-A| : |A| = n) = 0$.

So for odd n, there are no MDTS subsets of size n of D_{2n}.

Injective Mappings

- Now that we know that for when $|A| = 2$, there are strictly more MSTD sets than MDTS sets, one possible proof method is to show that for each other value of $|A|$, there are just at least as many MSTD sets as MDTS sets
- One way to show this would be to consturct an injection from the MDTS sets to MSTD sets given $|A|$
- This would complete the proof of the main conjecture

Conclusion

Future Work

Our goal is to prove that there are more MSTD than MDTS sets in D_{2n}.

- Explore interaction between $R + R$, $R - R$, and $F + F$ in subsets of D_{2n}
- Extend Cayley Tables approach for $3 \leq |A| \leq n$.
- Construct an injective mapping from MDTS sets to MSTD sets (given a set size $|A|$).

Bibliography

- G. Martin and K. O'Bryant, *Many sets have more sums than differences*, Additive Combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, (2007), 287–305.
- S. J. Miller and K. Vissuet, *Most Subsets are Balanced in Finite Groups*, Combinatorial and Additive Number Theory: CANT 2011 and 2012 (Springer Proceedings in Mathematics & Statistics, M. Nathanson editor (2014), 147–157).
- M. B. Nathanson, *Sets with more sums than differences*, Integers : Electronic Journal of Combinatorial Number Theory **7** (2007), Paper A5 (24pp).
- Y. Zhao, *Sets Characterized by Missing Sums and Differences*, Journal of Number Theory **131** (2011), 2107–2134.

Acknowledgements

- Thank you! Any questions?
- This research was conducted as part of the 2020 SMALL REU program at Williams College. This work was supported by NSF Grants DMS1947438 and DMS1561945, Williams College, Yale University, and the University of Rochester.