Most Sets are Balanced in Finite Groups

Kevin Vissuet (UCSD) and Steven J. Miller (Williams College)

http://web.williams.edu/Mathematics/sjmiller/public_html/jmm2013.html/

General Contributed Paper Session
Research in Number Theory
Room 2, Upper Level, San Diego
Wednesday January 9, 2013, 8:45p.m.

Summary

- History
- Main Result and Proof
- Why the Dihedral Group is Special

Introduction

Statement

S finite set of integers, $|S|$ its size. Form

- Sumset: $S + S = \{a_i + a_j : a_j, a_j \in S\}$.
- Difference set: $S - S = \{a_i - a_j : a_j, a_j \in S\}$.

Statement

S finite set of integers, $|S|$ its size. Form

- Sumset: $S + S = \{a_i + a_j : a_j, a_j \in S\}$.
- Difference set: $S - S = \{a_i - a_j : a_j, a_j \in S\}$.

Definition

We say S is difference dominated if $|S - S| > |S + S|$, balanced if $|S - S| = |S + S|$ and sum dominated (or an MSTD set) if $|S + S| > |S - S|$.

Expect generic in $\mathbb{Z}$ set to be difference dominated:

- addition is commutative, subtraction isn't:
- Generic pair (x, y) gives 1 sum, 2 differences.

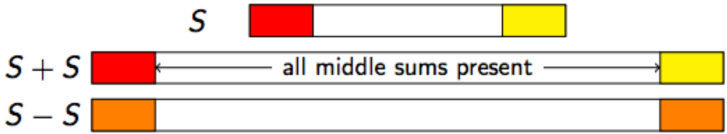
Expect generic in $\mathbb{Z}$ set to be difference dominated:

- addition is commutative, subtraction isn't:
- Generic pair (x, y) gives 1 sum, 2 differences.

Sum Dominated sets are rare but do occur.
Conway: $\{0, 2, 3, 4, 7, 11, 12, 14\}$

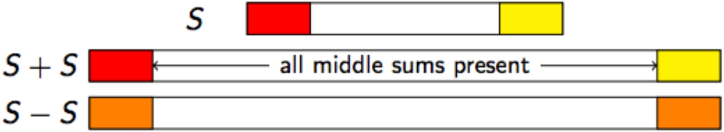
Intuition

- Key Idea: In the $\mathbb{Z}$ case, fringe matters most, middle sums and differences are present with high probability.



Intuition

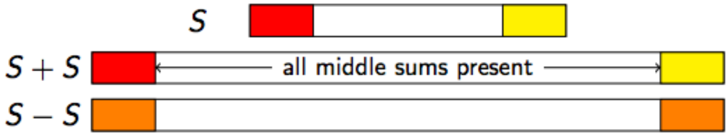
- Key Idea: In the $\mathbb{Z}$ case, fringe matters most, middle sums and differences are present with high probability.



- *If we choose the "fringe" of S cleverly, the middle of S will become largely irrelevant. - Martin, O'Bryant 2007*

Intuition

- Key Idea: In the $\mathbb{Z}$ case, fringe matters most, middle sums and differences are present with high probability.



- *If we choose the "fringe" of S cleverly, the middle of S will become largely irrelevant. - Martin, O'Bryant 2007*

- In a finite group there is no fringe. So the "largely irrelevant" is the only thing that can be relevant.

Main Result

Theorem

Let G be a group and let $S \subseteq G$. As $|G| \to \infty$
$\mathbb{P}(S + S = S - S = G) \to 1.$

Thus, as an immediate consequence, most set are balanced in finite groups.

Proof

Let $g \in G$.

We will first compute $\mathbb{P}(g \notin S + S)$.

Proof

Let $g \in G$.

We will first compute $\mathbb{P}(g \notin S + S)$.

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

Proof

Let $g \in G$.

We will first compute $\mathbb{P}(g \notin S + S)$.

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

This is not entirely trivial to compute since there are some slight dependency issues for example when we have $xy = zx = g$.

Proof Continued

Let $a_1a_2 = a_2a_3 = \cdots = a_{n-1}a_n = a_na_1 = g$ where $a_i \in G$

Proof Continued

Let $a_1a_2 = a_2a_3 = \cdots = a_{n-1}a_n = a_na_1 = g$ where $a_i \in G$

Claim: The number of subsets S of the "chain" elements $\{a_0, a_1, \ldots, a_n\}$ such that $g \notin S + S$ is the nth Lucas number.

Proof Continued

Let $a_1a_2 = a_2a_3 = \cdots = a_{n-1}a_n = a_na_1 = g$ where $a_i \in G$

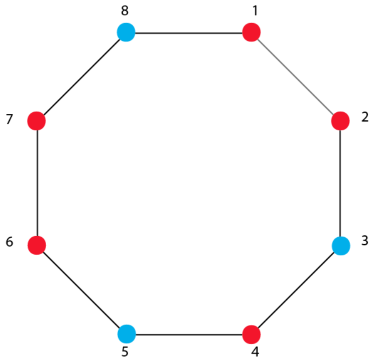
Claim: The number of subsets S of the "chain" elements $\{a_0, a_1, \ldots, a_n\}$ such that $g \notin S + S$ is the nth Lucas number.

To see this we look at a n-sided polygon.

The number of subsets such that $g \notin S + S$ is equal to the number of ways we can color the vertices of an n-polygon red or blue such that no two adjacent vertices are blue.

For example, here we have a possible coloring for a chain corresponding to $\bar{7} \in \mathbb{Z}/8\mathbb{Z}$.

Blue signifies that element is in S.



Let $n_1, n_2, \ldots, n_m$ be all the size of "chains" that we get for $g \in G$.

Let $n_1, n_2, \ldots, n_m$ be all the size of "chains" that we get for $g \in G$.

Since the "chains" partition the group we know that $\sum n_i = |G|$.

Let $n_1, n_2, \ldots, n_m$ be all the size of "chains" that we get for $g \in G$.

Since the "chains" partition the group we know that $\sum n_i = |G|$.

We also know that the n^{th} Lucas Number is given by $L(n) = \phi^n + (-1/\phi)^n$ where ϕ is the golden ratio.

Thus, the n^{th} lucas number can be bounded above by $L(n) < 1.8^n$.

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

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

$$\begin{aligned}\mathbb{P}(S+S \neq G) &= \mathbb{P}(\cup_{g\in G} g \notin S+S) \\ &\leq \sum_{g\in G} \mathbb{P}(g \notin S+S) \\ &\leq |G|(1.8/2)^{|G|}\end{aligned}$$

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

$$\begin{aligned}\mathbb{P}(S+S \neq G) &= \mathbb{P}(\cup_{g\in G} g \notin S+S) \\ &\leq \sum_{g\in G} \mathbb{P}(g \notin S+S) \\ &\leq |G|(1.8/2)^{|G|}\end{aligned}$$

So as $|G| \to \infty$ we have that $\mathbb{P}(S+S \neq G) = 0$. $\square$

Why the Dihedral Group is Special

Recall that in the integer case there exists many more difference dominated sets than sum dominated sets.

This is no longer necessarily the case in finite groups.

Recall that in the integer case there exists many more difference dominated sets than sum dominated sets.

This is no longer necessarily the case in finite groups.

Conjecture: For any Dihedral Group, there exists more sum dominated subsets than difference dominated subsets.

Some Intuition on Why This Should Be True

We know that a presentation for the dihedral group is D_{2n} is $\langle a, b | a^n = abab = b^2 = e \rangle$.

The thing to notice is that at least half the elements in D_{2n} are of order 2.

So for many elements $x = x^{-1}$

Some more intuition

Let $S \subseteq D_{2n}$

Some more intuition

Let $S \subseteq D_{2n}$

Let $S = R \cup F$ where R is the set of rotations in S and F is the set of flips in S.

Some more intuition

Let $S \subseteq D_{2n}$

Let $S = R \cup F$ where R is the set of rotations in S and F is the set of flips in S.

Set	Rotations in Set	Flips in Set
S	R	F
S+S	R+R, F+F	R+F, -R+F
S-S	R-R, F+F	R+F

Some more intuition

Let $S \subseteq D_{2n}$

Let $S = R \cup F$ where R is the set of rotations in S and F is the set of flips in S.

Set	Rotations in Set	Flips in Set
S	R	F
S+S	R+R, F+F	R+F, -R+F
S-S	R-R, F+F	R+F

Note that the difference in what contributes to the sumset and diffset is $R - R$ which contributes to the diffset and $-R + F$ and $R + R$ which contribute to the sunset.

Conclusion

Conclusion

A finite group acts different than the integers because a finite group does not have fringe elements.

Conclusion

A finite group acts different than the integers because a finite group does not have fringe elements.

However, if we let S be a random subset such that for each element in $g \in G$, $\mathbb{P}(g \in S) = 1/|G|$ then trivially $\mathbb{P}(S + S = G) < 1$.

Conclusion

A finite group acts different than the integers because a finite group does not have fringe elements.

However, if we let S be a random subset such that for each element in $g \in G$, $\mathbb{P}(g \in S) = 1/|G|$ then trivially $\mathbb{P}(S + S = G) < 1$.

So a question to ask is, with what constant probability does the phase transition occur.

Acknowledgements

We would like to thank the National Science Foundation for supporting our research through NSF Grant DMS0850577 and NSF Grant DMS0970067, as well as Williams College.

Bibliography

Bibliography

- G. Iyer, O. Lazarev, S.J. Miller, L. Zhang. *Generalized More Sums Than Differences Sets*. Journal of Number Theory. (132(2012),no 5, 1054–1073).
- O. Lazarev, S.J. Miller, K. O'Bryant. *Distribution of Missing Sums in Sumsets*. 2012.
- P. V. Hegarty and S. J. Miller, *When almost all sets are difference dominated*, Random Structures and Algorithms. **35** (2009), no. 1, 118–136.
- G. Martin, K. O'Bryant. *Many Sets Have More Sums Than Differences*, Additive Combinatorics, 287–305, 2007.