Weighted MPTQ Sums in Finite Groups

Yuval Amit[1] Lucas Chen[2] Devayani Pradhan[3]
Mentor: Steven J. Miller

SMALL REU, Williams College

[1]yuval.amit33@gmail.com, [2]lucasch@uchicago.edu, [3]pradhand@umich.edu

Combinatorial and Additive Number Theory Conference
July 13, 2026

Intro to MSTD

Given a set $A \subset \{0, \ldots, n\}$, we can ask when $|A + A| > |A - A|$.

Idea

$a + b = b + a$, but $a - b \neq b - a$.
$a + a \neq b + b$, but $a - a = b - b$.

Intro to MSTD

Given a set $A \subset \{0, \ldots, n\}$, we can ask when $|A + A| > |A - A|$.

Idea

$a + b = b + a$, but $a - b \neq b - a$.
$a + a \neq b + b$, but $a - a = b - b$.

- Martin and O'Bryant 2006 proved the proportion of subsets of $\{1, \ldots, n\}$ which are MSTD (more sums than differences) is bounded below by a constant.
- Zhao 2011 proved this constant is at least $4.28 \cdot 10^{-4}$.
- Nathanson 2006 detailed the history of the MSTD problem.

Question: What happens in (abelian) groups?

MSTD in Groups

Let G be a group and $A \subseteq G$. Define

$$AA := \{ x \cdot y \mid x, y \in A \},$$

and

$$AA^{-1} := \{ x \cdot y^{-1} \mid x, y \in A \}.$$

Definition

A subset $A \subseteq G$ is called

MPTQ if $|AA| - |AA^{-1}| > 0$.

MQTP if $|AA| - |AA^{-1}| < 0$.

Past Results on MSTD in Groups

- Miller and Vissuet 2014 showed that as a finite group gets arbitrarily large, the proportion of subsets that are balanced $(|A+A| = |A-A|)$ goes to 1
- Zhao 2010 works out asymptotic results for the number of MSTD sets in finite groups
- Miller and Vissuet 2014 conjectures that the dihedral groups are product-dominant.

Weighted Sum

Question: For a finite group G, are more subsets MPTQ or MQTP?

Weighted Sum

Question: For a finite group G, are more subsets MPTQ or MQTP?

Easier to understand:

Definition

For a group G, the **weighted sum** $W(G)$ is given by

$$W(G) := \sum_{A \subseteq G} \left(|AA| - |AA^{-1}| \right).$$

Weighted Sum

Question: For a finite group G, are more subsets MPTQ or MQTP?

Easier to understand:

Definition

For a group G, the **weighted sum** $W(G)$ is given by

$$W(G) := \sum_{A \subseteq G} \left(|AA| - |AA^{-1}| \right).$$

- $W(G)$ is *expected* to be positive (resp. negative) when G is product-dominant (resp. quotient-dominant).
- Martin and O'Bryant study this weighted sum as it describes the average magnitudes of $|AA|$ and $|AA^{-1}|$.

Results

Theorem

Let G be an abelian with $|G| \geq 6$. Then, $W(G) < 0$

Results

Theorem

Let G be an abelian with $|G| \geq 6$. Then, $W(G) < 0$

Theorem

Let G be the dihedral group on n vertices. For $n \geq 3$, $W(G) > 0$.

Results

Theorem

Let G be an abelian with $|G| \geq 6$. Then, $W(G) < 0$

Theorem

Let G be the dihedral group on n vertices. For $n \geq 3$, $W(G) > 0$.

Theorem

Let G be a finite group and $g \in G$. Then,

$$W(G) = \sum_{C_g} |C_g| \left(L_{|g|}^{n/|g|} - \prod_{m|(2|g|)} L_m^{c(m,g)} \right).$$

where the sum is taken over conjugacy classes.

First Step

Can rewrite

$$\begin{aligned} W(G) &= \sum_{A \subseteq G} \left(|AA| - |AA^{-1}|\right) \\ &= \sum_{A \subseteq G} \sum_{g \in G} \left(\mathbb{1}_{AA}(g) - \mathbb{1}_{AA^{-1}}(g)\right) \\ &= \sum_{g \in G} \sum_{A \subseteq G} \left(\mathbb{1}_{AA}(g) - \mathbb{1}_{AA^{-1}}(g)\right). \end{aligned}$$

First Step

Can rewrite

$$\begin{aligned} W(G) &= \sum_{A \subseteq G} \left(|AA| - |AA^{-1}|\right) \\ &= \sum_{A \subseteq G} \sum_{g \in G} \left(\mathbb{1}_{AA}(g) - \mathbb{1}_{AA^{-1}}(g)\right) \\ &= \sum_{g \in G} \sum_{A \subseteq G} \left(\mathbb{1}_{AA}(g) - \mathbb{1}_{AA^{-1}}(g)\right). \end{aligned}$$

Goal: Given $g \in G$, compute:

- $P(G, g) :=$ the number of $A \subseteq G$ such that $g \in AA$.
- $Q(G, g) :=$ the number of $A \subseteq G$ such that $g \in AA^{-1}$.

Then,

$$W(G) = \sum_{g \in G} (P(G, g) - Q(G, g)).$$

The Forbiddance Graph

We consider

$$\begin{aligned} P^c(G,g) &:= \left|\{A \subset G : g \notin AA\}\right|, \\ Q^c(G,g) &:= \left|\{A \subset G : g \notin AA^{-1}\}\right|. \end{aligned}$$

Definition (Zhao 2010)

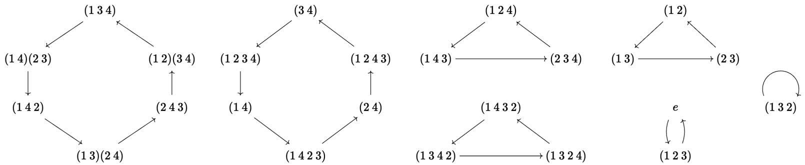
The **product** (resp. **quotient**) **forbiddance graph** has:

- Vertex set G
- A directed edge $x \to y$ whenever $xy = g$ (resp. $xy^{-1} = g$).

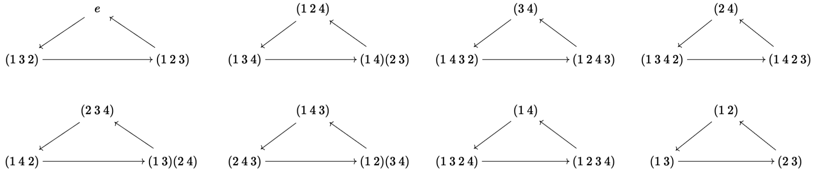
We denote this by $\Gamma^+(G,g)$ (resp. $\Gamma^-(G,g)$).

Forbiddance Graph Example

$\Gamma^{+}(S_4, (1\ 2\ 3))$:



$\Gamma^{-}(S_4, (1\ 2\ 3))$:



Independent Sets

Graph theory helps us understand products and quotients:

Lemma

For any $g \in G$, both $\Gamma^+(G, g)$ and $\Gamma^-(G, g)$ are composed of disjoint cycle graphs.

Independent Sets

Graph theory helps us understand products and quotients:

Lemma

For any $g \in G$, both $\Gamma^+(G,g)$ and $\Gamma^-(G,g)$ are composed of disjoint cycle graphs.

Definition

For a graph Γ, an **independent set** is a subgraph with no adjacent vertices.

Lemma

$$\begin{aligned} P^c(G,g) &= \#\ \textit{independent sets in}\ \Gamma^+(G,g), \\ Q^c(G,g) &= \#\ \textit{independent sets in}\ \Gamma^-(G,g). \end{aligned}$$

Lucas Numbers

Lemma

The number of independent sets of a cycle graph of length n is the n-th Lucas number L_n.

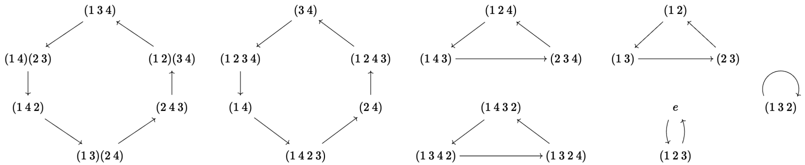
A variant of the Fibonacci numbers:

$$L_n := \begin{cases} 1 & n = 1 \\ 3 & n = 2 \\ L_{n-1} + L_{n-2} & n > 2 \end{cases}$$
$$= (\varphi)^n + (\widetilde{\varphi})^n,$$

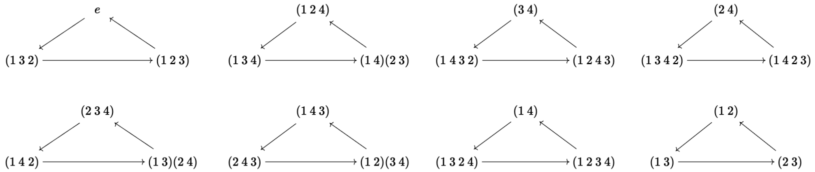
where $\varphi = \frac{1+\sqrt{5}}{2}$, $\widetilde{\varphi} = \frac{1-\sqrt{5}}{2}$.

Example Computation

$\Gamma^{+}(S_4, (1\,2\,3))$: $\#$ independent sets $= L_6^2 \cdot L_3^3 \cdot L_2 \cdot L_1$



$\Gamma^{-}(S_4, (1\,2\,3))$: $\#$ independent sets $= L_3^8$



Quotient Forbiddance

Lemma

For $g \in G$ with order ℓ,

$$Q^c(G, g) = L_\ell^{|G|/\ell}.$$

Quotient Forbiddance

Lemma

For $g \in G$ with order ℓ,

$$Q^c(G, g) = L_\ell^{|G|/\ell}.$$

Theorem

$$\sum_{A \subset G} |AA^{-1}| = \sum_{g \in G} \left(2^{|G|} - L_{|g|}^{|G|/|g|}\right).$$

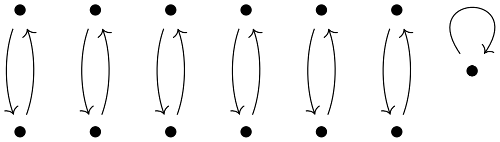
- The value of $Q(G, g)$ is dependent only on the order of g.
- The order of an element is invariant under conjugacy classes (more on this later).

Cyclic Groups

Theorem

Let $G = C_p$. If $g \in G$, then $P^c(G,g) = L_2^{(p-1)/2} = 3^{(p-1)/2}$.

$\Gamma^+(C_{13}, g)$ for any $g \in C_{13}$:

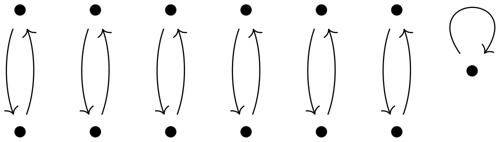


Cyclic Groups

Theorem

Let $G = C_p$. If $g \in G$, then $P^c(G, g) = L_2^{(p-1)/2} = 3^{(p-1)/2}$.

$\Gamma^+(C_{13}, g)$ for any $g \in C_{13}$:



Corollary

$$W(C_p) \sim (p-1)\varphi^p + 1 - p\sqrt{3}^{p-1}.$$

Finite Abelian Groups

Theorem

Suppose G is an abelian group. Then, $W(G) \leq 0$.

Proof Sketch:

Finite Abelian Groups

Theorem

Suppose G is an abelian group. Then, $W(G) \leq 0$.

Proof Sketch: Order of g always determines $Q(G,g)$. When G is abelian, it also determines $P(G,g)$.

$$W(G) = \sum_{g \in G} (P(G,g) - Q(G,g)) = \sum_{\ell \mid n} E(\ell)(P(G,g) - Q(G,g)).$$

where $E(\ell)$ is the number of elements of order ℓ.

Finite Abelian Groups

Theorem

Suppose G is an abelian group. Then, $W(G) \leq 0$.

Proof Sketch: Order of g always determines $Q(G,g)$. When G is abelian, it also determines $P(G,g)$.

$$W(G) = \sum_{g \in G} (P(G,g) - Q(G,g)) = \sum_{\ell \mid n} E(\ell)(P(G,g) - Q(G,g)).$$

where $E(\ell)$ is the number of elements of order ℓ.

- Show each term is either negative or is canceled out by another negative term.

Finite Abelian Groups

Theorem

Suppose G is an abelian group. Then, $W(G) \leq 0$.

Proof Sketch: Order of g always determines $Q(G, g)$. When G is abelian, it also determines $P(G, g)$.

$$W(G) = \sum_{g \in G} (P(G, g) - Q(G, g)) = \sum_{\ell \mid n} E(\ell)(P(G, g) - Q(G, g)).$$

where $E(\ell)$ is the number of elements of order ℓ.

- Show each term is either negative or is canceled out by another negative term.
- Relies on $L_n \sim \varphi^n$ as $n \to \infty$.

Finite Abelian Groups

Theorem

Suppose G is an abelian group. Then, $W(G) \leq 0$.

Proof Sketch: Order of g always determines $Q(G, g)$. When G is abelian, it also determines $P(G, g)$.

$$W(G) = \sum_{g \in G} (P(G, g) - Q(G, g)) = \sum_{\ell | n} E(\ell)(P(G, g) - Q(G, g)).$$

where $E(\ell)$ is the number of elements of order ℓ.

- Show each term is either negative or is canceled out by another negative term.
- Relies on $L_n \sim \varphi^n$ as $n \to \infty$.
  - Need $\varphi < \sqrt{3}$, as we compare $\sqrt{3}^n$ to φ^n.

Dihedral Groups (Non-Abelian)

Dihedral groups: Casework on rotations vs reflections
Example: Calculate the forbiddance sets for a rotation, ρ, in D_{12}.

For ρ of order ℓ, with $12/\ell$ odd, the product-quotient difference is $L_\ell^{12/\ell} - 3^{12/2} L_\ell^{12/\ell}$, with the following kinds of cycles in $\mathcal{PG}_\rho$:

$$\rho = \tau^k$$

$$\ldots \to \sigma\tau^{m-k} \longrightarrow \sigma\tau^m \longrightarrow \sigma\tau^{m+k} \to \ldots$$

$$\tau^m \longleftrightarrow \tau^{k-m}$$

Full computation of the formulas verifies weighted product dominance of dihedral groups.

Connections to Representation Theory

Definition

Let $p_g^1(x) := x^{-1}g$, (i.e. $x \cdot p_g^1(x) = g$).

Recursively, we let $p_g^d(x) = p_g^1(p_g^{d-1}(x))$.

Length of cycle containing x is the minimal $d \geq 1$ with $p_g^d(x) = x$.

Connections to Representation Theory

Definition

Let $p_g^1(x) := x^{-1}g$, (i.e. $x \cdot p_g^1(x) = g$).
Recursively, we let $p_g^d(x) = p_g^1(p_g^{d-1}(x))$.

Length of cycle containing x is the minimal $d \geq 1$ with $p_g^d(x) = x$.

Lemma

For $g \in G$ and $d \in \mathbb{N}$, the number of solutions to $p_g^d(x) = x$ is

$$T(d,g) := \begin{cases} \sum_\chi \nu_2(\chi)\chi(g^{-(d)}) & \text{if } d \text{ odd} \\ \sum_\chi |\chi(g^{d/2})|^2 & \text{if } d \text{ even} \end{cases}$$

- The sum is taken over all irreducible representations.
- Here, ν_2 denotes the second Frobenius-Schur indicator.
- Shows invariance of conjugacy class.

Cycle Formula

Lemma

Let $g \in G$. The number of m-length cycles of $\Gamma^+(G,g)$ is given by

$$c(m,g) \;:=\; \frac{1}{m}\sum_{d|m}\mu\left(\frac{m}{d}\right)T(d,g).$$

Cycle Formula

Lemma

Let $g \in G$. The number of m-length cycles of $\Gamma^+(G,g)$ is given by

$$c(m,g) \;:=\; \frac{1}{m}\sum_{d|m}\mu\left(\frac{m}{d}\right)T(d,g).$$

Theorem

Let G be a finite group and $g \in G$. Then,

$$W(G) \;=\; \sum_{C_g}|C_g|\left(L_{|g|}^{n/|g|} - \prod_{m|(2|g|)} L_m^{c(m,g)}\right).$$

where the sum is taken over conjugacy classes.

Cycle Formula

Lemma

Let $g \in G$. The number of m-length cycles of $\Gamma^+(G, g)$ is given by

$$c(m,g) \ := \ \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) T(d,g).$$

Theorem

Let G be a finite group and $g \in G$. Then,

$$W(G) \ = \ \sum_{C_g} |C_g| \left(L_{|g|}^{n/|g|} - \prod_{m|(2|g|)} L_m^{c(m,g)} \right).$$

where the sum is taken over conjugacy classes.

Advantages: Can quickly compute $W(G)$ for large groups.

Monster Group

For fun:

Question: For the monster group, $\mathbb{M}$, is $W(\mathbb{M})$ positive or negative?

Monster Group

For fun:

Question: For the monster group, $\mathbb{M}$, is $W(\mathbb{M})$ positive or negative?

- Compute prime factorizations of terms of sum.
- Compute magnitudes (term $\sim 10^{10^{53}}$).
- Identify and isolate leading terms.
- Recompute only leading terms (formula simplifies $\implies$ determine sign and magnitude).

Answer:

Monster Group

For fun:

Question: For the monster group, $\mathbb{M}$, is $W(\mathbb{M})$ positive or negative?

- Compute prime factorizations of terms of sum.
- Compute magnitudes (term $\sim 10^{10^{53}}$).
- Identify and isolate leading terms.
- Recompute only leading terms (formula simplifies $\implies$ determine sign and magnitude).

Answer:

$$W(\mathbb{M}) > 0$$

Monster Group

For fun:

Question: For the monster group, $\mathbb{M}$, is $W(\mathbb{M})$ positive or negative?

- Compute prime factorizations of terms of sum.
- Compute magnitudes (term $\sim 10^{10^{53}}$).
- Identify and isolate leading terms.
- Recompute only leading terms (formula simplifies $\implies$ determine sign and magnitude).

Answer:

$$W(\mathbb{M}) > 0$$

$$\log(W(\mathbb{M})) \approx 1.9276114377665424 \times 10^{53}$$

Future Work

Justify weighted dominance:

- Show $W(G) > 0 \implies G$ has more MPTQ than MQTP sets.
- Estimate proportion of subsets which are MPTQ/MQTP.

Future Work

Justify weighted dominance:

- Show $W(G) > 0 \implies G$ has more MPTQ than MQTP sets.
- Estimate proportion of subsets which are MPTQ/MQTP.

Compute $W(G)$ for more families:

- $W(N \rtimes H)$.
- Groups of Lie type.
- Compare similar families (dihedral vs. dicyclic).

Future Work

Justify weighted dominance:

- Show $W(G) > 0 \implies G$ has more MPTQ than MQTP sets.
- Estimate proportion of subsets which are MPTQ/MQTP.

Compute $W(G)$ for more families:

- $W(N \rtimes H)$.
- Groups of Lie type.
- Compare similar families (dihedral vs. dicyclic).

Extend to infinite groups:

- Covering ascending chains of subsets.
- Finitely generated groups, studying words with bounded length.
- Haar measure for infinite sets.

References

Ascoli, Ruben et al. (2022). *Sum and Difference Sets in Generalized Dihedral Groups*. arXiv: 2210.00669 [math.NT]. URL: https://arxiv.org/abs/2210.00669.

Fitch, Mark and Robert Jamison (Jan. 2000). "Minimum sum covers of small cyclic groups". In: *Congr. Numer.* 147. URL: https://www.researchgate.net/publication/228942670_Minimum_sum_covers_of_small_cyclic_groups.

Martin, Greg and Kevin O'Bryant (2006). *Many sets have more sums than differences*. arXiv: math/0608131 [math.NT]. URL: https://arxiv.org/abs/math/0608131.

Miller, Steven J. and Kevin Vissuet (2014). "Most Subsets Are Balanced in Finite Groups". In: *Combinatorial and Additive Number Theory*. Ed. by Melvyn B. Nathanson. New York, NY: Springer New York, pp. 147–157. ISBN: 978-1-4939-1601-6.

Nathanson, Melvyn B. (2006). *Problems in additive number theory, I*. arXiv: math/0604340 [math.NT]. URL: https://arxiv.org/abs/math/0604340.

Neetu, Anupriya Shetty, and B.R. Shankar (2025). "A Note on Sumsets and Difference Sets in Groups of Order 12". In: *Boletim da Sociedade Paranaense de Matematica* 43.3. Cited by: 0; All Open Access, Gold Open Access. DOI: 10.5269/bspm.78446. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-105030592611&doi=10.5269%2fbspm.78446&partnerID=40&md5=7d0c6e8d11bd9c50d334b9ce5138ab81.

Zhao, Yufei (2010). "Counting MSTD sets in finite abelian groups". In: *Journal of Number Theory* 130.10, pp. 2308–2322. ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2010.06.001. URL: https://www.sciencedirect.com/science/article/pii/S0022314X10001435.

— (2011). "Sets characterized by missing sums and differences". In: *Journal of Number Theory* 131.11, pp. 2107–2134. ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2011.05.003. URL: https://www.sciencedirect.com/science/article/pii/S0022314X11001430.

Thank You

Yuval Amit
University of Maryland
(yuval.amit33@gmail.com)

Lucas Chen
University of Chicago
(lucasch@uchicago.edu)

Devayani Pradhan
University of Michigan
(pradhand@umich.edu)

Supported by NSF, Williams College, Finnerty Fund, University of Chicago, University of Michigan