Product and Quotient Set Dominance in Finite Groups

YUVAL AMIT, LUCAS CHEN, CHRISTOPHER HOUSHOLDER, JOSHUA IM, JOSHUA KHAN, STEVEN J. MILLER, MATEO PALOMARES, AND DEVAYANI PRADHAN

ABSTRACT. A classic problem in additive number theory asks whether a given subset of integers has more sums or differences. This inquiry naturally extends to finite groups, where one compares the sizes of the product set AA and the quotient set AA^{-1} for a subset $A \subseteq G$. A finite group is considered product-dominant if it contains a higher proportion of subsets where $|AA| > |AA^{-1}|$, and quotient-dominant if the reverse is true. We establish statistical criteria to determine the dominance behavior of large finite groups by analyzing the moments of the random variable $d(A) := |AA| - |AA^{-1}|$. By translating product and quotient relationships into graph-theoretic constructions, we compute these moments through counting independent sets. Our main result demonstrates that for a growing sequence of finite groups G_k with center size Z_k and involution count T_k, the condition $Z_k = o(T_k)$ implies the groups are eventually product-dominant. Conversely, if $T_k \cdot \sqrt{3}^{R_k/Z_k} = o(Z_k)$ (where R_k denotes the number of elements whose square is central), the groups are eventually quotient-dominant. Using these asymptotic conditions, we resolve the Miller–Vissuet conjecture by proving that all dihedral groups D_n for $n \geq 3$ are product-dominant. Furthermore, we classify the dominance behavior of several major families of groups, proving that symmetric groups and non-abelian finite simple groups are product-dominant, while groups of odd order and certain abelian groups are quotient-dominant. Finally, for groups that fall outside our asymptotic conditions, we derive an explicit formula for the first moment utilizing the irreducible characters and conjugacy classes of the group.

CONTENTS

1. Introduction 2
1.1. Background 2
1.2. Main results 3
2. Proof of Theorem 1.3 5
3. The first moment M_1 6
4. The second moment M_2 12
5. Proof of Theorem 1.5 16
6. Proof of Conjecture 1.1 and other applications 20
6.1. Product-dominant groups 20
6.2. Quotient-dominant groups 22
7. Computing $M_1(G)$ by characters and conjugacy classes 24
8. Future work 27
Appendix A. Dihedral group computation 28
Acknowledgments 29
AI use 29

Date: October 7, 2026.

References 29

1. INTRODUCTION

1.1. **Background.** Given a subset $A \subseteq \{1, \ldots, n\}$, we may compare the sizes of the sumset

$$A + A := \{a + a' : a, a' \in A\} \tag{1.1}$$

and the difference set

$$A - A := \{a - a' : a, a' \in A\}. \tag{1.2}$$

The study of subsets with $|A + A| > |A - A|$ has long been of interest to additive number theorists (see [Nat06] for a history of the problem). In general, one expects to have $|A + A| < |A - A|$, as addition is commutative while subtraction is not. Sets with $|A + A| > |A - A|$ are called MSTD (more sums than differences) sets. While MSTD sets do exist (the smallest is attributed to J. H. Conway: $\{0, 2, 3, 4, 7, 11, 12, 14\}$), they typically make up only a small percentage of subsets of $\{1, \ldots, n\}$. However, Martin and O'Bryant [MO07] showed the surprising fact that if ρ_n is the proportion of subsets of $\{1, \ldots, n\}$ which are MSTD, then $\rho_n \geq 2 \cdot 10^{-7}$ for all $n \geq 15$. Explicit infinite families of MSTD sets have been constructed by Nathanson [Nat07], Hegarty [Heg07], Miller, Orosz, and Scheinerman [MOS10], and Zhao [Zha10a]. More recently, Herrmann [Her26] classified the small MSTD sets in arbitrary fields, showing in particular that no abelian group contains an MSTD set of size five. Hegarty and Miller [HM09] later showed that, under a natural model in which each element is chosen with a probability tending to zero, almost all sets are difference dominated.

A natural extension of the MSTD problem is found in studying the subsets of a finite group G. Given a subset $A \subseteq G$, we define the **product set** and **quotient set** as

$$AA := \{xy : x, y \in A\}, \tag{1.3}$$

$$AA^{-1} := \{xy^{-1} : x, y \in A\} \tag{1.4}$$

respectively. In a non-abelian group one could instead compare AA with the left quotient set $A^{-1}A$; the two quotient sets need not have the same size, and the possible differences between them are studied by Duvivier et al. [Duv+26]. We use the right quotient set AA^{-1}, and our work is largely independent of this choice. A subset $A \subseteq G$ is said to be **MPTQ** (more products than quotients) if $|AA| > |AA^{-1}|$, **MQTP** if $|AA| < |AA^{-1}|$, and **balanced** if $|AA| = |AA^{-1}|$. The situation for groups is different from that of $\{1, \ldots, n\}$ for two reasons.

(a) Unlike the interval $\{1, \ldots, n\}$, a group is closed under multiplication and inverses.

(b) The intuition about the commutativity of addition versus the non-commutativity of subtraction vanishes for non-abelian groups.

Product sets in non-commutative groups have also been studied from the perspective of growth, where the relevant question is how small $|AA|$ can be relative to $|A|$; see Tao [Tao08]. Nathanson [Nat06] studied product/quotient dominance in abelian groups to find methods that could be applied to the classical MSTD problem. He showed that MSTD sets in finite abelian groups could be lifted to construct infinite families of MSTD sets in the integers. Zhao [Zha10b] subsequently found an asymptotic formula for the proportion of MSTD sets in finite abelian groups, and showed that if $\{G_n\}$ is a sequence of finite abelian groups whose order goes to infinity, the proportion of subsets that are MSTD converges to zero; see also [Zha11] for the companion analysis of which sums and differences are missing. For the cyclic groups $\mathbb{Z}/n\mathbb{Z}$, Hemmady, Lott, and Miller [HLM17] determined when almost all subsets are difference dominated. Miller and Vissuet [MV14] generalized this to all finite groups by proving that, as the size of a finite group gets arbitrarily large, the proportion of subsets which are balanced converges to 1. Moreover, the probability that the product set and quotient set both equal the entire group G_n converges to 1.

Recent research has pivoted to studying the behavior of the small proportion of sets that remain unbalanced. This includes exploring how the structure of non-abelian groups affects the behavior of unbalanced sets. Notably, Miller and Vissuet [MV14] conjectured the following behavior of dihedral groups. We say that a group is product-dominant if it has more MPTQ sets than MQTP sets, and quotient-dominant if it has more MQTP than MPTQ sets.

Conjecture 1.1 (Miller–Vissuet). *All dihedral groups D_n for $n \geq 3$ are product-dominant.*

Note that D_n is balanced for $n = 1, 2$. Haviland et al. [Hav+21] and Ascoli et al. [Asc+22] studied generalized dihedral groups, providing strong evidence in favor of Conjecture 1.1. We continue along this line by characterizing when large finite groups are product- or quotient-dominant.

1.2. **Main results.** For a subset $A \subseteq G$, let

$$d(A) \;:=\; |AA| - |AA^{-1}|. \tag{1.5}$$

If $A \subseteq G$ is chosen uniformly at random, we aim to understand the distribution of the random variable $d(A)$. It is therefore natural to study the moments of $d(A)$.

Definition 1.2. *The r-th **raw moment** of $d(A)$ is defined by*

$$\mu_r(G) \;:=\; \frac{1}{2^{|G|}} \sum_{A \subseteq G} (d(A))^r. \tag{1.6}$$

For ease of notation, we write

$$M_r(G) \;:=\; \sum_{A \subseteq G} (d(A))^r \;=\; 2^{|G|} \mu_r(G). \tag{1.7}$$

*Another useful statistic is the number of subsets which are **balanced**, meaning $d(A) = 0$. Let*

$$B(G) \;:=\; \#\{A \subseteq G : d(A) = 0\}. \tag{1.8}$$

We occasionally write $M_r := M_r(G)$ and $B := B(G)$.

The statistical properties of moments (the first two moments in particular) and the number of balanced subsets can help us understand when a group is product- or quotient-dominant. This idea is captured by the following key theorem.

Theorem 1.3. *Let G be a finite group, and suppose*

$$\frac{M_1^2}{(2^{|G|} - B)M_2} > \frac{1}{2}. \tag{1.9}$$

Then

(i) $M_1 > 0 \implies G$ *is product-dominant,*

(ii) $M_1 < 0 \implies G$ *is quotient-dominant.*

Our main result uses Theorem 1.3 to determine whether sufficiently large groups, under certain assumptions, are product- or quotient-dominant.

Definition 1.4. *If $\{a_k\}, \{b_k\}$ are two sequences, we say $a_k = o(b_k)$ if $\lim_{k\to\infty} a_k/b_k = 0$.*

Theorem 1.5. *Let $\{G_k\}$ be a sequence of finite groups with $|G_k| \to \infty$. Let $Z(G_k)$ denote the center of G_k, and define*

$$T_k := \#\{g \in G_k : \mathrm{ord}(g) = 2\}, \tag{1.10}$$

$$Z_k := |Z(G_k)|, \tag{1.11}$$

$$R_k := \#\{g \in G_k : g^2 \in Z(G_k)\}. \tag{1.12}$$

Then, we have the following properties.

(i) If $Z_k = o(T_k)$, then G_k is product-dominant for sufficiently large k.

(ii) If $T_k \cdot \sqrt{3}^{R_k/Z_k} = o(Z_k)$, then G_k is quotient-dominant for sufficiently large k.

This establishes that in many cases, the size of the center and the number of order-two elements of a group are what most heavily influence its dominance behavior. There are many notable families of groups which satisfy the conditions in Theorem 1.5. Some of these groups are studied in Section 6, where we show that sufficiently large

- dihedral groups are product-dominant (Theorem 6.2),
- symmetric groups are product-dominant (Theorem 6.3),
- non-abelian finite simple groups are product-dominant (Theorem 6.4),
- groups of odd order are quotient-dominant (Theorem 6.5), and
- abelian groups with at least 6 squares and at least 171 elements[1] are quotient-dominant (Theorem 6.6).

For dihedral groups in particular, we evaluate precisely when "sufficiently large" occurs. Then, with manual computation we confirm all smaller dihedral groups to prove Conjecture 1.1. We also perform this threshold analysis on abelian groups.

[1]This threshold can be lowered. See Remark 6.7.

For groups that do not satisfy the conditions of Theorem 1.5 (dicyclic groups, for example), deeper study of the moments of $d(A)$ is needed. Computation of $M_1(G)$ in particular is important, as one must find whether (1.9) is satisfied, and if $M_1 > 0$ or $M_1 < 0$. In Theorems 7.5 and 7.6, we establish an explicit formula for $M_1(G)$ based on the irreducible characters and the conjugacy classes of G.

Finally, we discuss future work, and in particular we mention special cases where $M_1(G) > 0$ while G is quotient-dominant, or $M_1(G) < 0$ while G is product-dominant. Groups with these properties cannot be studied via the methods of Theorem 1.3, making them potentially necessary and interesting to classify.

The paper is organized as follows. Section 2 proves Theorem 1.3. Sections 3 and 4 express M_1 and M_2 in terms of independent sets of forbiddance graphs, and bounds those counts. Section 5 combines the bounds to prove Theorem 1.5. Section 6 applies Theorem 1.5 to dihedral, symmetric, simple, odd-order, and abelian groups. Section 7 derives a character-theoretic formula for $M_1(G)$, and Section 8 discusses open problems.

2. PROOF OF THEOREM 1.3

Theorem 1.3, which is restated below, is a purely statistical fact, but it turns out to be very effective for studying product/quotient-dominant behavior in finite groups.

Theorem 1.3. *Let G be a finite group, and suppose*

$$\frac{M_1^2}{(2^{|G|} - B)M_2} > \frac{1}{2}. \tag{1.9}$$

Then

(i) $M_1 > 0 \implies$ *G is product-dominant,*

(ii) $M_1 < 0 \implies$ *G is quotient-dominant.*

Proof. We prove statement (i), and the proof (ii) is nearly identical, hence omitted. To prove G is product-dominant, we must show

$$P(d(A) > 0) > P(d(A) < 0), \tag{2.1}$$

where P denotes the probability over a uniformly chosen random subset $A \subseteq G$. We use the shorthand $P(d < 0)$ and $P(d > 0)$. Let μ_1 be the expected value of $d(A)$ and σ^2 be the variance. Since $M_1 > 0$ implies $\mu_1 > 0$, Cantelli's inequality [Gho02] gives

$$P(d \leq 0) = P(d - \mu_1 \leq -\mu_1) \leq \frac{\sigma^2}{\sigma^2 + \mu_1^2}. \tag{2.2}$$

Hence

$$P(d > 0) = 1 - P(d \leq 0) \geq 1 - \frac{\sigma^2}{\sigma^2 + \mu_1^2}. \tag{2.3}$$

On the other hand, let $\beta := P(d = 0) = B/2^{|G|}$ be the proportion of balanced sets. Then,

$$P(d < 0) = 1 - P(d \geq 0) = 1 - P(d = 0) - P(d > 0)$$

$$= 1 - \beta - P(d > 0) \leq 1 - \beta - \left(1 - \frac{\sigma^2}{\sigma^2 + \mu_1^2}\right)$$
$$= \frac{\sigma^2}{\sigma^2 + \mu_1^2} - \beta. \tag{2.4}$$

Therefore, from (2.1) we see

$$1 - \frac{\sigma^2}{\sigma^2 + \mu_1^2} > \frac{\sigma^2}{\sigma^2 + \mu_1^2} - \beta \implies G \text{ is product-dominant.} \tag{2.5}$$

Now, we may simplify the expression in (2.5) by using the fact that $\sigma^2 + \mu_1^2 = \mu_2$ (see [Soc20], for example). This gives

$$\begin{aligned} 1 - \frac{\sigma^2}{\sigma^2 + \mu_1^2} > \frac{\sigma^2}{\sigma^2 + \mu_1^2} - \beta &\iff 1 + \beta > \frac{2\sigma^2}{\sigma^2 + \mu_1^2} \\ &\iff 1 + \beta > \frac{2\mu_2 - 2\mu_1^2}{\mu_2} \\ &\iff \frac{2\mu_1^2}{\mu_2} > 1 - \beta \\ &\iff \frac{2M_1^2}{M_2} > 2^{|G|} - B \\ &\iff \frac{M_1^2}{(2^{|G|} - B)M_2} > \frac{1}{2}, \end{aligned} \tag{2.6}$$

as desired. □

With Theorem 1.3 in mind, we aim to find sufficient lower bounds for M_1, and upper bounds for M_2 and $2^{|G|} - B$.

3. THE FIRST MOMENT M_1

To study $M_1(G)$, we express it with a graph-theoretic summation, following the work of [Zha10b]. For a set $S \subseteq G$, let $\mathbb{1}_S$ be the indicator function

$$\mathbb{1}_S(g) := \begin{cases} 1 & g \in S \\ 0 & g \notin S. \end{cases} \tag{3.1}$$

Then, we use the fact that

$$|S| = \sum_{g \in G} \mathbb{1}_S(g) \tag{3.2}$$

to obtain the equality

$$\begin{aligned} M_1(G) &= \sum_{A \subseteq G} d(A) = \sum_{A \subseteq G} \left(|AA| - |AA^{-1}|\right) \\ &= \sum_{A \subseteq G} \sum_{g \in G} (\mathbb{1}_{AA}(g) - \mathbb{1}_{AA^{-1}}(g)) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{g\in G}\sum_{A\subseteq G}\left(\mathbb{1}_{AA}(g)-\mathbb{1}_{AA^{-1}}(g)\right)\\
&= \sum_{g\in G}\Big[\#\{A\subseteq G : g\in AA\}-\#\{A\subseteq G : g\in AA^{-1}\}\Big]\\
&= \sum_{g\in G}\Big[\Big(2^{|G|}-\#\{A : g\notin AA\}\Big)-\Big(2^{|G|}-\#\{A : g\notin AA^{-1}\}\Big)\Big]\\
&= \sum_{g\in G}\Big[\#\{A : g\notin AA^{-1}\}-\#\{A : g\notin AA\}\Big]. \qquad (3.3)
\end{aligned}
$$

To compute the two cardinalities in (3.3), we turn to a graph-theoretic construction first explored in [Zha10b].

Definition 3.1. *Let G be a group. A **forbiddance graph** is a graph whose vertices are the elements of G, with an edge $x \to y$ whenever x and y satisfy a predetermined product or quotient relationship with respect to some fixed element(s) of G. In particular, for fixed $g \in G$, we define the forbiddance graphs $\mathcal{F}_P(g)$ and $\mathcal{F}_Q(g)$ by the following rules.*

$$\mathcal{F}_P(g) \text{ has } x \to y \text{ whenever } xy = g, \qquad (3.4)$$

$$\mathcal{F}_Q(g) \text{ has } x \to y \text{ whenever } xy^{-1} = g. \qquad (3.5)$$

Definition 3.2. *For a directed or undirected graph $\Gamma = (V, E)$, a set $A \subseteq V$ is said to be an **independent set** if there are no $x, y \in A$ (not necessarily distinct) joined by an edge. The number of independent sets of Γ is denoted $i(\Gamma)$.*

Example 3.3. *Let $G = S_4$ and $g = (1\,2\,3)$. Figure 1 depicts $\mathcal{F}_P(g)$, with an example independent set boxed and colored in red.*

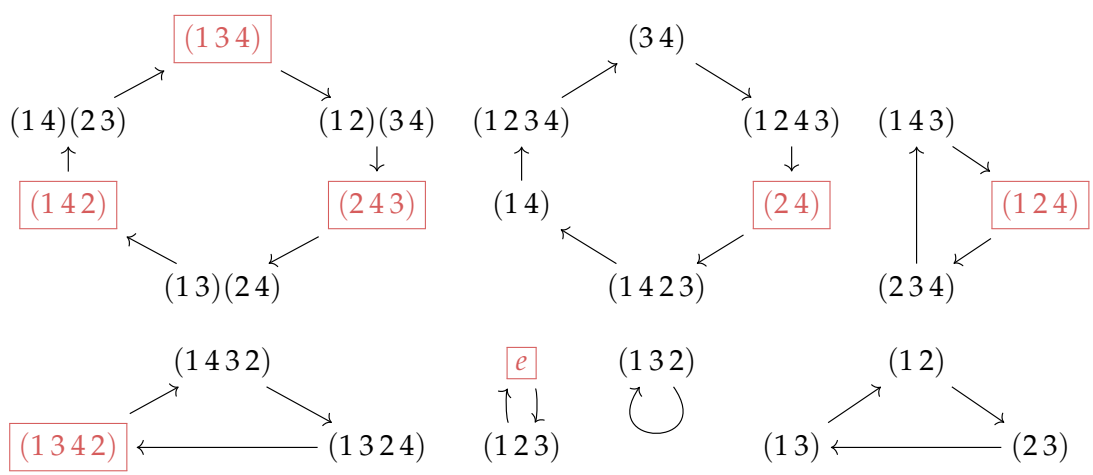

FIGURE 1. The forbiddance graph $\mathcal{F}_P((1\,2\,3))$ in S_4. The boxed red vertices form an independent set.

The number of independent sets of a graph is, in some cases, well understood (see [Zha09; Zha10b; Sah+19]). Therefore, graph-theoretic results on the number of independent sets can be applied to our problem via the following identities.

Remark 3.4. *For a finite group G, and $g \in G$,*

$$i(\mathcal{F}_P(g)) \;=\; \#\{A \subseteq G : g \notin AA\}, \tag{3.6}$$

$$i(\mathcal{F}_Q(g)) \;=\; \#\{A \subseteq G : g \notin AA^{-1}\}. \tag{3.7}$$

These equalities hold because a subset $A \subseteq G$ satisfies $g \notin AA$ (resp. $g \notin AA^{-1}$) exactly when A contains no x, y (not necessarily distinct) with $xy = g$ (resp. $xy^{-1} = g$); that is, exactly when A is an independent set of $\mathcal{F}_P(g)$ (resp. $\mathcal{F}_Q(g)$). We therefore obtain the following expression for $M_1(G)$.

Lemma 3.5. *For a finite group G, we have*

$$M_1(G) \;=\; \sum_{g \in G} \left(i(\mathcal{F}_Q(g)) - i(\mathcal{F}_P(g)) \right). \tag{3.8}$$

Proof. This follows from (3.3), (3.6), and (3.7). □

We now study a few properties of $\mathcal{F}_Q(g)$ and $\mathcal{F}_P(g)$ to aid our later analysis.

Lemma 3.6. *For any $g \in G$, both $\mathcal{F}_Q(g)$ and $\mathcal{F}_P(g)$ are disjoint unions of cycle graphs.*

Proof. For $x \in G$, define

$$q_g(x) \;:=\; q_g^{(1)}(x) \;:=\; g^{-1}x, \qquad q_g^{(n)}(x) \;:=\; q_g(q_g^{(n-1)}(x)), \tag{3.9}$$

$$p_g(x) \;:=\; p_g^{(1)}(x) \;:=\; x^{-1}g, \qquad p_g^{(n)}(x) \;:=\; p_g(p_g^{(n-1)}(x)). \tag{3.10}$$

Then $y = q_g(x)$ is the unique element satisfying $xy^{-1} = g$, and similarly $y = p_g(x)$ is the unique element satisfying $xy = g$. Thus, the forbiddance graph $\mathcal{F}_Q(g)$ locally around x looks like

$$x \;\to\; q_g^{(1)}(x) \;\to\; q_g^{(2)}(x) \;\to\; \cdots, \tag{3.11}$$

and this path must eventually loop back around to x, since q_g is a bijection and G is finite. The same holds for p_g. It follows that both forbiddance graphs are composed of disjoint cycles. □

The functions $q_g^{(n)}(x)$ and $p_g^{(n)}(x)$ play a central role later, so we record explicit formulas for them.

Lemma 3.7. *For any $n \geq 1$,*

$$q_g^{(n)}(x) \;=\; g^{-n}x. \tag{3.12}$$

Moreover,

$$p_g^{(2n-1)}(x) \;=\; g^{-n+1}x^{-1}g^{n}, \tag{3.13}$$

$$p_g^{(2n)}(x) \;=\; g^{-n}xg^{n}. \tag{3.14}$$

Proof. We proceed by induction. The base case for $q_g^{(1)}$ is by definition, and then

$$q_g^{(n)}(x) \;=\; q_g^{(1)}(q_g^{(n-1)}(x)) \;=\; g^{-1}(g^{-(n-1)}x) \;=\; g^{-n}x. \tag{3.15}$$

For p_g, the base case $p_g^{(1)}$ is by definition. Then

$$\begin{aligned} p_g^{(2n)}(x) &= p_g(p_g^{(2n-1)}(x)) = p_g(g^{-n+1}x^{-1}g^n) \\ &= (g^{-n+1}x^{-1}g^n)^{-1}g = g^{-n}xg^n, \end{aligned} \tag{3.16}$$

and

$$\begin{aligned} p_g^{(2n+1)}(x) &= p_g(p_g^{(2n)}(x)) = p_g(g^{-n}xg^n) \\ &= (g^{-n}xg^n)^{-1}g = g^{-n}x^{-1}g^{n+1}, \end{aligned} \tag{3.17}$$

as desired. □

Remark 3.8. *It is known that the number of independent sets of a cycle graph of length n is the nth Lucas number*[2] *L_n, where a cycle of length 1 is a single vertex with a loop and a cycle of length 2 is a single edge. Moreover, if $\Gamma := \Gamma_1 \sqcup \Gamma_2$ is the disjoint union of two component graphs, then*

$$i(\Gamma) = i(\Gamma_1) \cdot i(\Gamma_2). \tag{3.18}$$

See [Zha10b] for proofs. Thus, to find $i(\mathcal{F}_P(g))$ and $i(\mathcal{F}_Q(g))$, we must compute the lengths of their component cycles.

We first analyze $\mathcal{F}_Q(g)$ by restating [Zha10b, Lemma 3.3]. We also reprove it for completeness, as the proof is short and the strategy is important.

Lemma 3.9. *For a finite group G, and $g \in G$,*

$$i(\mathcal{F}_Q(g)) = L_{\operatorname{ord}(g)}^{|G|/\operatorname{ord}(g)}. \tag{3.19}$$

Proof. For any element $x \in G$, the length of the cycle in $\mathcal{F}_Q(g)$ containing x is precisely the minimal $\ell \geq 1$ such that $q_g^{(\ell)}(x) = x$. By Lemma 3.7, this equates to the minimal ℓ for which $g^{-\ell}x = x$, which is $\operatorname{ord}(g)$. Since every vertex in $\mathcal{F}_Q(g)$ is therefore contained in a cycle of length $\operatorname{ord}(g)$, it follows that $\mathcal{F}_Q(g)$ is precisely composed of $|G|/\operatorname{ord}(g)$ cycles of length $\operatorname{ord}(g)$, so the claim follows by Remark 3.8 and (3.18). □

To understand the behavior of $i(\mathcal{F}_Q(g))$ (and later $i(\mathcal{F}_P(g))$), we aim to know when it is maximized (i.e., what graph configurations yields the highest number of independent sets). For this, we have the following lemma.

Lemma 3.10. *Let N be a positive integer, and let $a_1, \ldots, a_j$ be positive integers with $a_i \neq 2$ for all i, and $a_1 + \cdots + a_j = N$. Then*

$$L_{a_1} \cdot L_{a_2} \cdots L_{a_j} \leq 7^{N/4}. \tag{3.20}$$

Proof. Let $\phi = (1+\sqrt{5})/2$ be the golden ratio. It is well known that

$$L_n = \phi^n + (1-\phi)^n, \tag{3.21}$$

[2] $L_1 = 1$, $L_2 = 3$, and $L_{n+2} = L_{n+1} + L_n$ for $n \geq 1$.

where notably $|1-\phi| < 1$, so $L_n \sim \phi^n$. Moreover, since $1-\phi < 0$, one sees that $L_n > \phi^n \iff n$ is even. Thus, as $L_4 = 7$, and $(1-\phi)^n < (1-\phi)^4$ for all $n > 4$, we get that

$$L_n \leq \left(7^{1/4}\right)^n \tag{3.22}$$

for all $n \geq 4$. This inequality also holds for L_1 and L_3. As $a_i \neq 2$ for all i, we have

$$\prod_{i=1}^{j} L_{a_i} \leq \prod_{i=1}^{j} 7^{a_i/4} = 7^{N/4}. \tag{3.23}$$

□

The exclusion of $a_i = 2$ is important here, as a graph with $N/2$ two-cycles has $L_2^{N/2} = \sqrt{3}^N$ independent sets, which is larger than $7^{N/4}$ (in the sense of little-o) since $7^{1/4} < \sqrt{3}$. We use this fact to show that, loosely speaking, group elements g with $\mathcal{F}_Q(g)$ or $\mathcal{F}_P(g)$ composed almost entirely of two-cycles have the greatest contribution in terms of number of independent sets.

Corollary 3.11. *Let G be a finite group of size N, and let T be the number of elements of G with order 2. Then*

$$T \cdot \sqrt{3}^N \leq \sum_{g \in G} i(\mathcal{F}_Q(g)) \leq T \cdot \sqrt{3}^N + (N-T) \cdot 7^{N/4}. \tag{3.24}$$

Proof. By Lemma 3.9,

$$\begin{aligned} \sum_{g \in G} i(\mathcal{F}_Q(g)) &= \sum_{g \in G} L_{\operatorname{ord}(g)}^{N/\operatorname{ord}(g)} \\ &= \sum_{\substack{g \in G \\ \operatorname{ord}(g)=2}} L_2^{N/2} + \sum_{\substack{g \in G \\ \operatorname{ord}(g)\neq 2}} L_{\operatorname{ord}(g)}^{N/\operatorname{ord}(g)} \\ &= T\sqrt{3}^N + \sum_{\substack{g \in G \\ \operatorname{ord}(g)\neq 2}} L_{\operatorname{ord}(g)}^{N/\operatorname{ord}(g)}. \end{aligned} \tag{3.25}$$

For each of the $N-T$ elements g with $\operatorname{ord}(g) \neq 2$, the graph $\mathcal{F}_Q(g)$ consists of $N/\operatorname{ord}(g)$ cycles of length $\operatorname{ord}(g) \neq 2$, and these lengths sum to N, so $L_{\operatorname{ord}(g)}^{N/\operatorname{ord}(g)} \leq 7^{N/4}$ by Lemma 3.10. The remaining summation is therefore at most $(N-T) \cdot 7^{N/4}$, and it is clearly non-negative, which gives both bounds in (3.24). □

Understanding $i(\mathcal{F}_P(g))$ is more difficult, since the length of the cycle containing $x \in G$ is the minimal $\ell \geq 1$ with $p_g^{(\ell)}(x) = x$, and by (3.13) and (3.14) this depends on both x and g in a less uniform way. However, the number of independent sets is still a product of Lucas numbers whose indices sum to $|G|$, as in Lemma 3.10. Since Corollary 3.11 demonstrated that the 2-cycles give the dominant contribution, we want to study the 2-cycles in $\mathcal{F}_P(g)$ as well.

Lemma 3.12. *Let G be a finite group of size N with center $Z(G)$. Let $Z := |Z(G)|$, and let*

$$R := \#\{x \in G : x^2 \in Z(G)\}. \tag{3.26}$$

Then

$$Z \cdot \sqrt{3}^{N-R/Z} \;\le\; \sum_{g\in G} i(\mathcal{F}_P(g)) \;\le\; Z \cdot \sqrt{3}^{N} + (N-Z)\cdot 1.68^N. \tag{3.27}$$

Moreover, for every $g \notin Z(G)$,

$$i(\mathcal{F}_P(g)) \;\le\; \left(3^{1/4}\cdot 7^{1/8}\right)^N \;<\; 1.68^N. \tag{3.28}$$

Proof. Suppose $g \in Z(G)$. By (3.14), $p_g^{(2)}(x) = g^{-1}xg$. Thus, as $gx = xg$, we know every $x \in G$ is contained in either a 1-cycle or a 2-cycle in $\mathcal{F}_P(g)$ by the proof of Lemma 3.6. In particular, x is contained in a 2-cycle if and only if $p_g^{(1)}(x) \neq x$, which is equivalent to $x^2 \neq g$. Let

$$r(g) \;:=\; \#\{x \in G : x^2 = g\}. \tag{3.29}$$

Then, the forbiddance graph $\mathcal{F}_P(g)$ is composed of $r(g)$ 1-cycles and $(N - r(g))/2$ two-cycles. Therefore, for any $g \in Z(G)$,

$$i(\mathcal{F}_P(g)) \;=\; L_1^{r(g)} \cdot L_2^{\frac{N-r(g)}{2}} \;=\; \sqrt{3}^{N-r(g)}. \tag{3.30}$$

On the other hand, suppose $g \notin Z(G)$. By (3.14), $p_g^{(2)}(x) = x$ if and only if $xg = gx$, so every vertex lying in a 2-cycle of $\mathcal{F}_P(g)$ belongs to the centralizer $C_G(g)$. Let k be the number of such vertices. As g is non-central, $C_G(g)$ is a proper subgroup of G, hence $k \le |C_G(g)| \le N/2$. The 2-cycles contribute $L_2^{k/2} = \sqrt{3}^k$ independent sets, while the remaining cycles have lengths different from 2 summing to $N - k$, so by Lemma 3.10 they contribute at most $7^{(N-k)/4}$. Since $\sqrt{3} > 7^{1/4}$, the resulting bound increases with k, and therefore

$$i(\mathcal{F}_P(g)) \;\le\; \sqrt{3}^k \cdot 7^{(N-k)/4} \;\le\; \sqrt{3}^{N/2}\cdot 7^{N/8} \;=\; \left(3^{1/4}\cdot 7^{1/8}\right)^N \;<\; 1.68^N, \tag{3.31}$$

which proves (3.28). Splitting the sum over the central and non-central elements of G now gives

$$\sum_{g\in G} i(\mathcal{F}_P(g)) \;=\; \sum_{g\in Z(G)} \sqrt{3}^{N-r(g)} + \sum_{g\notin Z(G)} i(\mathcal{F}_P(g)). \tag{3.32}$$

Since $\sqrt{3}^{N-r(g)} \le \sqrt{3}^N$, and since each of the $N - Z$ non-central elements contributes at most 1.68^N by (3.28), we have

$$\sum_{g\in G} i(\mathcal{F}_P(g)) \;\le\; Z\cdot\sqrt{3}^N + (N-Z)\cdot 1.68^N, \tag{3.33}$$

which is the second inequality in (3.27). To obtain the lower bound, we discard the non-negative second sum in (3.32) and observe that $f(x) := \sqrt{3}^{N-x}$ is a convex function. Therefore, by Jensen's inequality [Jen06; SS05],

$$\frac{1}{Z}\sum_{g\in Z(G)} \sqrt{3}^{N-r(g)} \;\ge\; \sqrt{3}^{N-(1/Z)\sum_{g\in Z(G)} r(g)} \;=\; \sqrt{3}^{N-R/Z}, \tag{3.34}$$

since $\sum_{g\in Z(G)} r(g) = R$. Thus, by (3.32),

$$\sum_{g\in G} i(\mathcal{F}_P(g)) \;\geq\; Z\cdot\sqrt{3}^{N-R/Z} \tag{3.35}$$

as desired. □

4. THE SECOND MOMENT M_2

Similar to the first moment, we reduce the study of the second moment to evaluating the number of independent sets of forbiddance graphs.

Definition 4.1. *We define three more forbiddance graphs as in Definition 3.1. Once again, the vertices of these graphs are the elements of G, and for fixed $g,h\in G$, we define*

$$\mathcal{F}_{PP}(g,h) \text{ has } x\to y \text{ whenever } xy=g \text{ or } xy=h, \tag{4.1}$$

$$\mathcal{F}_{QQ}(g,h) \text{ has } x\to y \text{ whenever } xy^{-1}=g \text{ or } xy^{-1}=h, \tag{4.2}$$

$$\mathcal{F}_{PQ}(g,h) \text{ has } x\to y \text{ whenever } xy=g \text{ or } xy^{-1}=h. \tag{4.3}$$

Remark 4.2. *Similar to before, the number of independent sets of these forbiddance graphs relates to cardinalities of subsets satisfying certain element exclusion properties. For a finite group G, and $g,h\in G$,*

$$i(\mathcal{F}_{PP}(g,h)) \;=\; \#\{A\subseteq G : g\notin AA, h\notin AA\}, \tag{4.4}$$

$$i(\mathcal{F}_{QQ}(g,h)) \;=\; \#\{A\subseteq G : g\notin AA^{-1}, h\notin AA^{-1}\}, \tag{4.5}$$

$$i(\mathcal{F}_{PQ}(g,h)) \;=\; \#\{A\subseteq G : g\notin AA, h\notin AA^{-1}\}. \tag{4.6}$$

Lemma 4.3. *Recall $M_2(G) := \sum_{A\subseteq G}(d(A))^2$. For any finite group G,*

$$M_2(G) \;=\; \sum_{g,h\in G}\left[i(\mathcal{F}_{PP}(g,h)) + i(\mathcal{F}_{QQ}(g,h)) - 2i(\mathcal{F}_{PQ}(g,h))\right]. \tag{4.7}$$

Proof. We proceed similarly to the first moment. Let $p(A) := |AA|$ and $q(A) := |AA^{-1}|$. Then

$$M_2(G) \;:=\; \sum_{A\subseteq G}(p(A)-q(A))^2 \;=\; \sum_{A\subseteq G}\left[p(A)^2+q(A)^2-2p(A)q(A)\right]. \tag{4.8}$$

Now, note that

$$p(A)^2 \;=\; \left(\sum_x \mathbb{1}_{AA}(x)\right)^2 = \sum_{g,h}\mathbb{1}_{AA}(g)\mathbb{1}_{AA}(h), \tag{4.9}$$

$$q(A)^2 \;=\; \left(\sum_x \mathbb{1}_{AA^{-1}}(x)\right)^2 = \sum_{g,h}\mathbb{1}_{AA^{-1}}(g)\mathbb{1}_{AA^{-1}}(h), \tag{4.10}$$

$$p(A)q(A) \;=\; \left(\sum_g \mathbb{1}_{AA}(g)\right)\left(\sum_h \mathbb{1}_{AA^{-1}}(h)\right) \;=\; \sum_{g,h}\mathbb{1}_{AA}(g)\mathbb{1}_{AA^{-1}}(h). \tag{4.11}$$

Thus, we rewrite (4.8) as

$$\sum_{A\subseteq G}\sum_{g,h}\left[\mathbb{1}_{AA}(g)\mathbb{1}_{AA}(h)+\mathbb{1}_{AA^{-1}}(g)\mathbb{1}_{AA^{-1}}(h)-2\cdot\mathbb{1}_{AA}(g)\mathbb{1}_{AA^{-1}}(h)\right]$$

$$= \sum_{g,h} \sum_{A \subseteq G} [\mathbb{1}_{AA}(g)\mathbb{1}_{AA}(h) + \mathbb{1}_{AA^{-1}}(g)\mathbb{1}_{AA^{-1}}(h) - 2 \cdot \mathbb{1}_{AA}(g)\mathbb{1}_{AA^{-1}}(h)]$$

$$= \sum_{g,h} \left[\#\{A : g,h \in AA\} + \#\{A : g,h \in AA^{-1}\} - 2\#\{A : g \in AA, h \in AA^{-1}\} \right]. \tag{4.12}$$

Now, to obtain the expressions in Remark 4.2, we use the inclusion–exclusion principle to obtain

$$\begin{aligned} \#\{A : g,h \in AA\} &= 2^{|G|} - \#\{A : g \notin AA \text{ or } h \notin AA\} \\ &= 2^{|G|} - \#\{A : g \notin AA\} - \#\{A : h \notin AA\} \\ &\quad + \#\{A : g \notin AA \text{ and } h \notin AA\} \\ &= 2^{|G|} - i(\mathcal{F}_P(g)) - i(\mathcal{F}_P(h)) + i(\mathcal{F}_{PP}(g,h)), \end{aligned} \tag{4.13}$$

and similarly

$$\#\{A : g,h \in AA^{-1}\} = 2^{|G|} - i(\mathcal{F}_Q(g)) - i(\mathcal{F}_Q(h)) + i(\mathcal{F}_{QQ}(g,h)), \tag{4.14}$$

$$\#\{A : g \in AA, h \in AA^{-1}\} = 2^{|G|} - i(\mathcal{F}_P(g)) - i(\mathcal{F}_Q(h)) + i(\mathcal{F}_{PQ}(g,h)). \tag{4.15}$$

Plugging these into (4.12) yields (after rearranging and canceling)

$$M_2(G) = \sum_{g,h} [i(\mathcal{F}_P(g)) - i(\mathcal{F}_P(h)) + i(\mathcal{F}_Q(h)) - i(\mathcal{F}_Q(g))] \tag{4.16}$$

$$+ \sum_{g,h} [i(\mathcal{F}_{PP}(g,h)) + i(\mathcal{F}_{QQ}(g,h)) - 2i(\mathcal{F}_{PQ}(g,h))]. \tag{4.17}$$

Notice that the entire sum in (4.16) cancels, and so we are left with

$$M_2(G) = \sum_{g,h} [i(\mathcal{F}_{PP}(g,h)) + i(\mathcal{F}_{QQ}(g,h)) - 2i(\mathcal{F}_{PQ}(g,h))], \tag{4.18}$$

as desired. □

We aim to find upper bounds for $M_2(G)$ to satisfy Theorem 1.3. From Lemma 4.3, we may rewrite $M_2(G)$ as

$$M_2(G) = \sum_{g \in G} [i(\mathcal{F}_P(g)) + i(\mathcal{F}_Q(g)) - 2i\,(\mathcal{F}_{PQ}(g,g))] \tag{4.19}$$

$$+ \sum_{g \neq h \in G} [i(\mathcal{F}_{PP}(g,h)) + i(\mathcal{F}_{QQ}(g,h)) - 2i(\mathcal{F}_{PQ}(g,h))]. \tag{4.20}$$

It suffices for our purposes to remove the negative terms from (4.19) and (4.20), so

$$M_2(G) \leq \sum_{g \in G} i(\mathcal{F}_P(g)) + \sum_{g \in G} i(\mathcal{F}_Q(g)) \tag{4.21}$$

$$+ \sum_{g \neq h \in G} i(\mathcal{F}_{PP}(g,h)) + \sum_{g \neq h \in G} i(\mathcal{F}_{QQ}(g,h)). \tag{4.22}$$

The behavior of the two sums in (4.21) was studied in Lemma 3.12 and Corollary 3.11. To bound the two sums in (4.22), we show that every term is exponentially smaller than $\sqrt{3}^N$. For this, we need a result by Sah, Sawhney, Stoner, and Zhao [Sah+19].

Theorem 4.4 ([Sah+19]). *Let $\Gamma = (V, E)$ be a simple, undirected graph with no isolated vertices. Let d_v be the degree of a vertex $v \in V$. Then*

$$i(\Gamma) \;\leq\; \prod_{uv \in E} \left(2^{d_u} + 2^{d_v} - 1\right)^{\frac{1}{d_u d_v}}. \tag{4.23}$$

Corollary 4.5. *Let $\Gamma = (V, E)$ be a simple, undirected graph with no isolated vertices such that $2 \leq d_v \leq 4$ for all $v \in V$. Then*

$$i(\Gamma) \;\leq\; 19^{|V|/6}. \tag{4.24}$$

Proof. To find an upper bound for the expression in (4.23), note that

$$\log\left(\prod_{uv \in E} \left(2^{d_u} + 2^{d_v} - 1\right)^{\frac{1}{d_u d_v}}\right) \;=\; \sum_{uv \in E} \frac{\log(2^{d_u} + 2^{d_v} - 1)}{d_u d_v}. \tag{4.25}$$

We wish to use the graph-theoretic identity

$$\sum_{uv \in E} \left(\frac{1}{d_u} + \frac{1}{d_v}\right) \;=\; |V|, \tag{4.26}$$

so we want the minimal constant c with

$$\frac{\log(2^{d_u} + 2^{d_v} - 1)}{d_u d_v} \;\leq\; c\left(\frac{1}{d_u} + \frac{1}{d_v}\right), \tag{4.27}$$

which is equivalent to

$$\frac{\log(2^{d_u} + 2^{d_v} - 1)}{d_u + d_v} \;\leq\; c. \tag{4.28}$$

Since $d_u, d_v \in \{2, 3, 4\}$, one can compute that the maximum of the left-hand side of (4.28) is attained at $\{d_u, d_v\} = \{2, 4\}$, so we set $c = \log(19)/6$. Then

$$\sum_{uv \in E} \frac{\log(2^{d_u} + 2^{d_v} - 1)}{d_u d_v} \;\leq\; \frac{\log(19)}{6} \sum_{uv \in E} \left(\frac{1}{d_u} + \frac{1}{d_v}\right) \;=\; \frac{\log(19)}{6}|V|, \tag{4.29}$$

hence

$$i(\Gamma) \;\leq\; \exp\left(\sum_{uv \in E} \frac{\log(2^{d_u} + 2^{d_v} - 1)}{d_u d_v}\right) \;\leq\; \exp\left(\frac{\log(19)}{6}|V|\right) \;=\; 19^{|V|/6}, \tag{4.30}$$

as desired. □

For the last lemma in this section, we need the number of independent sets of a path. The path Π_n with $n \geq 1$ vertices has F_{n+2} independent sets, where $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ are the Fibonacci numbers (see [Zha10b], for example).

Lemma 4.6. *For every $n \geq 1$,*

$$i(\Pi_n) \;=\; F_{n+2} \;\leq\; 2 \cdot 7^{(n-1)/4}. \tag{4.31}$$

Proof. For $n = 1$ and $n = 2$ we have $F_3 = 2 = 2 \cdot 7^0$ and $F_4 = 3 < 2 \cdot 7^{1/4}$. For $n \geq 3$, by induction,

$$F_{n+2} \;=\; F_{n+1} + F_n \;\leq\; 2 \cdot 7^{(n-2)/4} + 2 \cdot 7^{(n-3)/4}$$

$$= 2 \cdot 7^{(n-1)/4} \left(7^{-1/4} + 7^{-1/2}\right)$$
$$\leq 2 \cdot 7^{(n-1)/4}, \tag{4.32}$$

since $7^{-1/4} + 7^{-1/2} < 1$. □

Lemma 4.7. *Let G be a finite group of order N, and let $g \neq h \in G$. Then*

$$i(\mathcal{F}_{QQ}(g,h)) \leq 19^{N/6}, \tag{4.33}$$

$$i(\mathcal{F}_{PP}(g,h)) \leq \left(3^{1/4} \cdot 7^{1/8}\right)^N < 1.68^N. \tag{4.34}$$

Moreover, if $g, h \in Z(G)$, then

$$i(\mathcal{F}_{PP}(g,h)) \leq 7^{N/4}. \tag{4.35}$$

Proof. We first remark on three facts about independent sets. First, a self-adjacent vertex lies in no independent set, so deleting all self-adjacent vertices (and the edges attached to them) does not change the number of independent sets. Second, adding edges to a graph on a fixed vertex set can only decrease the number of independent sets. In particular, since $\mathcal{F}_P(g)$ and $\mathcal{F}_P(h)$ are subgraphs of $\mathcal{F}_{PP}(g,h)$ on the same vertex set,

$$i(\mathcal{F}_{PP}(g,h)) \leq \min\{i(\mathcal{F}_P(g)), i(\mathcal{F}_P(h))\}. \tag{4.36}$$

Third, for any directed graph $\mathcal{F}$, we define the underlying undirected graph Γ to have the same vertex set as $\mathcal{F}$, where each directed edge of $\mathcal{F}$ becomes an undirected edge, and two or more directed edges between the same pair of vertices are identified as a single undirected edge; see Figure 2.

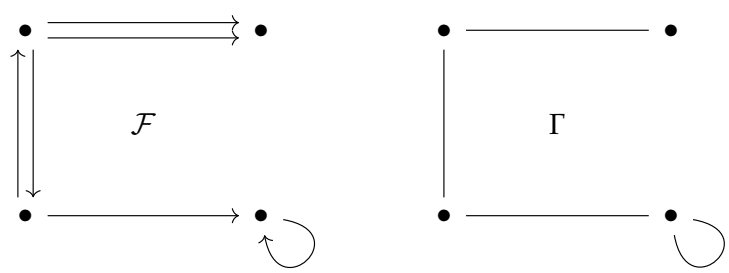

FIGURE 2. An example directed graph $\mathcal{F}$, and its underlying undirected graph Γ.

Then it is clear that $i(\mathcal{F}) = i(\Gamma)$. Moreover, if $\mathcal{F}$ has no self-adjacent vertices, then Γ is a simple, undirected graph.

We now prove (4.33). If $g = e$ or $h = e$, then every $x \in G$ is self-adjacent in $\mathcal{F}_{QQ}(g,h)$, since $xx^{-1} = e$, so $i(\mathcal{F}_{QQ}(g,h)) = 1$ and the claim follows trivially. Otherwise if $g, h \neq e$, then no vertex is self-adjacent. Let Γ_{QQ} denote the simple, undirected graph corresponding to $\mathcal{F}_{QQ}(g,h)$. The neighbors of x in Γ_{QQ} are the elements $\{g^{-1}x,\ h^{-1}x,\ gx,\ hx\}$. These are all different from x, and $g^{-1}x \neq h^{-1}x$, so every vertex has degree 2, 3, or 4. Thus (4.33) follows from Corollary 4.5.

To prove (4.34), we first assume $g \notin Z(G)$ (the case $h \notin Z(G)$ is identical). Then $i(\mathcal{F}_P(g)) \leq \left(3^{1/4} \cdot 7^{1/8}\right)^N$ by (3.28), and so (4.34) follows from (4.36).

Finally, suppose $g, h \in Z(G)$. We then get $xy = g$ if and only if $yx = g$, and the unique y with $xy = g$ is $p_g(x) := x^{-1}g$. The map p_g is an involution, since $p_g(p_g(x)) = g^{-1}xg = x$. Hence, in the underlying undirected graph Γ_{PP} of $\mathcal{F}_{PP}(g,h)$, the neighbors of x are exactly $p_g(x)$ and $p_h(x)$, and these are distinct because $g \neq h$. The vertex x is self-adjacent if and only if $x \in S := \{x \in G : x^2 \in \{g,h\}\}$. Let $s := |S|$, and let Γ' be the simple graph obtained from Γ_{PP} by deleting S, so that Γ' is simple, undirected, and $i(\mathcal{F}_{PP}(g,h)) = i(\Gamma')$.

Every vertex of Γ_{PP} outside S has exactly two neighbors, both different from itself, while every vertex in S has exactly one neighbor different from itself. In particular, Γ' has maximum degree at most 2, so it is a disjoint union of cycles of lengths $c_1, \ldots, c_a \geq 3$ and paths with $n_1, \ldots, n_b \geq 1$ vertices, where

$$\sum_i c_i + \sum_j n_j = N - s. \tag{4.37}$$

Consider a path component Π with n vertices. If $n > 1$, the endpoints of Π have degree 1 as vertices in Γ', but degree 2 as vertices in Γ_{PP}, so the neighbor each endpoint loses lies in S. If $n = 1$, then Π is a single vertex $x \notin S$, which has two distinct neighbors in Γ_{PP}, and both lie in S. In either case, each path component of Γ' accounts for two elements of S, and these elements are distinct for distinct path components, since every element of S has exactly one neighbor other than itself. Therefore $2b \leq s$. Therefore, by Lemma 3.10, Remark 3.8, and Lemma 4.6,

$$\begin{aligned} i(\mathcal{F}_{PP}(g,h)) \;=\; \prod_{i=1}^{a} L_{c_i} \cdot \prod_{j=1}^{b} F_{n_j+2} \;&\leq\; 7^{\sum_i c_i/4} \cdot \prod_{j=1}^{b} \left(2 \cdot 7^{(n_j-1)/4}\right) \\ &=\; 7^{(N-s)/4} \cdot \left(2 \cdot 7^{-1/4}\right)^b \\ &\leq\; 7^{(N-s)/4} \cdot \left(2 \cdot 7^{-1/4}\right)^{s/2} \\ &=\; 7^{N/4} \cdot \left(\sqrt{2} \cdot 7^{-3/8}\right)^s \;\leq\; 7^{N/4}, \end{aligned} \tag{4.38}$$

where we used $2 \cdot 7^{-1/4} > 1$ and $\sqrt{2} < 7^{3/8}$. This proves (4.35). Since $7^{1/4} < 3^{1/4} \cdot 7^{1/8}$, this also completes the proof of (4.34). □

5. PROOF OF THEOREM 1.5

We now combine the bounds on M_1 from Section 3 with the bounds on M_2 from Section 4 and apply Theorem 1.3 to prove Theorem 1.5.

Theorem 1.5. *Let $\{G_k\}$ be a sequence of finite groups with $|G_k| \to \infty$. Let $Z(G_k)$ denote the center of G_k, and define*

$$T_k \;:=\; \#\{g \in G_k : \mathrm{ord}(g) = 2\}, \tag{1.10}$$

$$Z_k \;:=\; |Z(G_k)|, \tag{1.11}$$

$$R_k \;:=\; \#\{g \in G_k : g^2 \in Z(G_k)\}. \tag{1.12}$$

Then, we have the following properties.

(i) If $Z_k = o(T_k)$, then G_k is product-dominant for sufficiently large k.

(ii) If $T_k \cdot \sqrt{3}^{R_k/Z_k} = o(Z_k)$, then G_k is quotient-dominant for sufficiently large k.

Proof. Let $N_k := |G_k|$. By Theorem 1.3, to prove that G_k is product- or quotient-dominant for sufficiently large k, it suffices to show that

$$\frac{1}{2} < \frac{(M_1(G_k))^2}{(2^{N_k} - B(G_k)) \cdot (M_2(G_k))} \tag{5.1}$$

for all sufficiently large k, and to determine the sign of $M_1(G_k)$.

Lemma 5.1. *Let*

$$P_k := \sum_{g \in G_k} i(\mathcal{F}_P(g)), \qquad Q_k := \sum_{g \in G_k} i(\mathcal{F}_Q(g)), \tag{5.2}$$

$$PP_k := \sum_{g \neq h \in G_k} i(\mathcal{F}_{PP}(g,h)), \qquad QQ_k := \sum_{g \neq h \in G_k} i(\mathcal{F}_{QQ}(g,h)). \tag{5.3}$$

Then

$$M_1(G_k) = Q_k - P_k, \tag{5.4}$$

$$M_2(G_k) \leq Q_k + P_k + QQ_k + PP_k, \tag{5.5}$$

$$2^{N_k} - B(G_k) \leq Q_k + P_k. \tag{5.6}$$

Proof. We immediately obtain (5.4) from Lemma 3.5, and (5.5) was shown in (4.21) and (4.22). Finally, (5.6) holds for any finite group G, as

$$\begin{aligned} 2^{|G|} - B(G) &= 2^{|G|} - \#\{A \subseteq G : d(A) = 0\} \\ &\leq 2^{|G|} - \#\{A : AA = AA^{-1} = G\} \\ &= \#\{A : \exists g \notin AA \text{ or } \exists h \notin AA^{-1}\} \\ &\leq \sum_{g \in G} \#\{A : g \notin AA \text{ or } g \notin AA^{-1}\} \\ &= \sum_{g \in G} (i(\mathcal{F}_P(g)) + i(\mathcal{F}_Q(g)) - i(\mathcal{F}_{PQ}(g,g))) \\ &\leq \sum_{g \in G} (i(\mathcal{F}_P(g)) + i(\mathcal{F}_Q(g))) . \end{aligned} \tag{5.7}$$

□

We reformulate the desired inequality in (5.1) as a statement about P_k, Q_k, PP_k, and QQ_k.

Lemma 5.2. *Let G be a finite group, and let P, Q, PP, QQ be as in Lemma 5.1, formed with G in place of G_k. Suppose $P \neq Q$, and set*

$$X := \max\{P, Q\}, \quad u := \frac{\min\{P, Q\}}{X}, \quad v := \frac{PP + QQ}{X}. \tag{5.8}$$

If

$$f(u,v) := u^2 - 6u + 1 - v(1+u) > 0, \tag{5.9}$$

then G is product-dominant when $Q > P$, and quotient-dominant when $P > Q$. Moreover, the following hold.

(i) The condition (5.9) is equivalent to

$$2(Q-P)^2 \;>\; (Q+P)\,(Q+P+PP+QQ)\,. \tag{5.10}$$

(ii) The function f is strictly decreasing in u on $[0,3)$ and in v on $[0,\infty)$. Hence, if $u \le u^+ < 3$ and $v \le v^+$, then $f(u,v) \ge f(u^+,v^+)$, so it suffices to verify (5.9) for any such upper bounds u^+ and v^+.

(iii) The condition (5.9) holds whenever $u \le 1$ and $6u + 2v < 1$.

Proof. By (5.4), we have

$$|M_1(G)| = |Q-P| = X(1-u), \tag{5.11}$$

$$2^{|G|} - B(G) \;\le\; Q+P \;=\; X(1+u), \tag{5.12}$$

$$M_2(G) \;\le\; Q+P+QQ+PP \;=\; X(1+u+v). \tag{5.13}$$

Thus,

$$\frac{(M_1(G))^2}{(2^{|G|}-B(G))\cdot M_2(G)} \;\ge\; \frac{X^2(1-u)^2}{X(1+u)\cdot X(1+u+v)} \;=\; \frac{(1-u)^2}{(1+u)(1+u+v)}. \tag{5.14}$$

Since $(1+u)(1+u+v) > 0$, we have

$$\begin{aligned} \frac{(1-u)^2}{(1+u)(1+u+v)} \;>\; \frac{1}{2} \;&\iff\; 2(1-u)^2 \;>\; (1+u)(1+u+v) \\ &\iff\; u^2 - 6u + 1 - v(1+u) \;>\; 0, \end{aligned} \tag{5.15}$$

so (5.9) gives (1.9). The conclusion now follows from Theorem 1.3, as $M_1(G) = Q - P$ is positive exactly when $Q > P$.

For (i), multiply (5.9) through by $X^2 > 0$ and use $X(1-u) = |Q-P|$, $X(1+u) = Q+P$, and $Xv = PP + QQ$, which turns $2(1-u)^2 > (1+u)(1+u+v)$ into (5.10). For (ii), let $u \in [0,3)$ and $v \in [0,\infty)$, so

$$\frac{\partial f}{\partial u} \;=\; 2u - 6 - v \;<\; 0, \qquad \frac{\partial f}{\partial v} \;=\; -(1+u) \;<\; 0. \tag{5.16}$$

For (iii), note that $u^2 \ge 0$ and $1 + u \le 2$, so $f(u,v) \ge 1 - 6u - 2v$. □

We next collect the bounds from Sections 3 and 4 in a common form. Let G be a finite group of order N, let T, Z, and R be as in Theorem 1.5 (formed with G in place of G_k), and let P, Q, PP, QQ be as in Lemma 5.1. Since $7^{1/4} < 1.68$, Corollary 3.11 and Lemma 3.12 give

$$T\sqrt{3}^{N} \;\le\; Q \;\le\; T\sqrt{3}^{N} + N\cdot 1.68^N, \tag{5.17}$$

$$Z\sqrt{3}^{N-R/Z} \;\le\; P \;\le\; Z\sqrt{3}^{N} + N\cdot 1.68^N. \tag{5.18}$$

Since the sums defining PP and QQ run over the $N(N-1)$ ordered pairs (g,h) with $g \neq h$, Lemma 4.7 and $19^{1/6} < 1.68$ give

$$PP + QQ \;\leq\; 2N(N-1)\cdot 1.68^N \;\leq\; 2N^2 \cdot 1.68^N. \tag{5.19}$$

Finally, as $1.68 < \sqrt{3}$, we remark that the quantity

$$\varepsilon(N) \;:=\; N^3 \left(\frac{1.68}{\sqrt{3}}\right)^N \tag{5.20}$$

satisfies $\varepsilon(N) \to 0$ as $N \to \infty$. The error terms obtained below are controlled by this $\varepsilon(N)$.

To prove statement (i) of the theorem, suppose $Z_k = o(T_k)$. As $Z_k \geq 1$ for every k, this forces $T_k \to \infty$; in particular $T_k \geq 1$ for all large k, so $Q_k \geq T_k\sqrt{3}^{N_k} > 0$ by (5.17). Dividing the upper bound in (5.18) by $T_k\sqrt{3}^{N_k}$ gives

$$\frac{P_k}{Q_k} \;\leq\; \frac{Z_k\sqrt{3}^{N_k} + N_k\cdot 1.68^{N_k}}{T_k\sqrt{3}^{N_k}} \;\leq\; \frac{Z_k}{T_k} + N_k\left(\frac{1.68}{\sqrt{3}}\right)^{N_k} \;\leq\; \frac{Z_k}{T_k} + \varepsilon(N_k), \tag{5.21}$$

and (5.19) gives

$$\frac{PP_k + QQ_k}{Q_k} \;\leq\; \frac{2N_k^2\cdot 1.68^{N_k}}{T_k\sqrt{3}^{N_k}} \;\leq\; 2\varepsilon(N_k). \tag{5.22}$$

The right-hand sides of (5.21) and (5.22) tend to 0, since $Z_k/T_k \to 0$ by assumption and $\varepsilon(N_k) \to 0$. Hence, for all sufficiently large k, we have $P_k < Q_k$ and

$$6\cdot\frac{P_k}{Q_k} + 2\cdot\frac{PP_k + QQ_k}{Q_k} \;<\; 1. \tag{5.23}$$

Applying Lemma 5.2 with $X = Q_k$, $u = P_k/Q_k$, and $v = (PP_k + QQ_k)/Q_k$, we conclude that G_k is product-dominant for all sufficiently large k.

Now, for case (ii) of the theorem, suppose $T_k \cdot \sqrt{3}^{R_k/Z_k} = o(Z_k)$, and set

$$W_k \;:=\; Z_k\sqrt{3}^{N_k - R_k/Z_k} \;\leq\; P_k, \tag{5.24}$$

the lower bound from (5.18). We first check that

$$\sqrt{3}^{R_k/Z_k} \;\leq\; N_k \tag{5.25}$$

for all sufficiently large k. If $T_k \geq 1$, then

$$\sqrt{3}^{R_k/Z_k} \;\leq\; T_k\sqrt{3}^{R_k/Z_k} \;<\; Z_k \;\leq\; N_k \tag{5.26}$$

for large k, by the assumption $T_k\sqrt{3}^{R_k/Z_k} = o(Z_k)$. If instead $T_k = 0$, then G_k has no element of order 2, and therefore has odd order by Cauchy's theorem. In that case, if $x^2 \in Z(G_k)$, then $\overline{x}^2 = \overline{e}$ in the quotient group $G_k/Z(G_k)$, which also has odd order, so $\overline{x} = \overline{e}$ and $x \in Z(G_k)$. Thus $R_k = Z_k$ and $\sqrt{3}^{R_k/Z_k} = \sqrt{3} \leq N_k$. This proves (5.25), and combining it with (5.24) yields

$$W_k \;\geq\; \frac{Z_k\sqrt{3}^{N_k}}{N_k} \;\geq\; \frac{\sqrt{3}^{N_k}}{N_k}. \tag{5.27}$$

Using (5.17), (5.24), and (5.27), we obtain

$$\frac{Q_k}{P_k} \le \frac{T_k\sqrt{3}^{N_k} + N_k \cdot 1.68^{N_k}}{W_k} \le \frac{T_k \cdot \sqrt{3}^{R_k/Z_k}}{Z_k} + N_k^2\left(\frac{1.68}{\sqrt{3}}\right)^{N_k} \le \frac{T_k \cdot \sqrt{3}^{R_k/Z_k}}{Z_k} + \varepsilon(N_k), \quad (5.28)$$

where the middle inequality uses $T_k\sqrt{3}^{N_k}/W_k = T_k\sqrt{3}^{R_k/Z_k}/Z_k$. Similarly, (5.19) and (5.27) give

$$\frac{PP_k + QQ_k}{P_k} \le \frac{2N_k^2 \cdot 1.68^{N_k}}{W_k} \le 2N_k^3\left(\frac{1.68}{\sqrt{3}}\right)^{N_k} = 2\varepsilon(N_k). \quad (5.29)$$

The right-hand sides of (5.28) and (5.29) tend to 0, since $T_k\sqrt{3}^{R_k/Z_k}/Z_k \to 0$ by assumption and $\varepsilon(N_k) \to 0$. Hence, for all sufficiently large k, we have $Q_k < P_k$ and

$$6 \cdot \frac{Q_k}{P_k} + 2 \cdot \frac{PP_k + QQ_k}{P_k} < 1. \quad (5.30)$$

Applying Lemma 5.2 with $X = P_k$, $u = Q_k/P_k$, and $v = (PP_k + QQ_k)/P_k$, we conclude that G_k is quotient-dominant for all sufficiently large k. □

6. PROOF OF CONJECTURE 1.1 AND OTHER APPLICATIONS

We now apply Theorem 1.5 to several families of groups. For dihedral and abelian groups, we also make the bounds of Section 5 explicit, which lets us handle all group orders rather than only sufficiently large ones.

6.1. **Product-dominant groups.** We begin by resolving Conjecture 1.1. Let D_k be the dihedral group of order $N = 2k$. Proving that D_k is product-dominant for sufficiently large k is quick: with Z_k, T_k as in Theorem 1.5, we have

$$Z_k = \begin{cases} 2 & k \text{ even}, \\ 1 & k \text{ odd}, \end{cases} \quad (6.1)$$

$$T_k = \begin{cases} k+1 & k \text{ even}, \\ k & k \text{ odd}, \end{cases} \quad (6.2)$$

so $Z_k = o(T_k)$ and Theorem 1.5 gives the desired result.

Now, we compute the threshold which we have been calling "sufficiently large", so that we can manually validate the conjecture for all smaller dihedral groups[3].

For dihedral groups, the general bound (4.34) is too weak to give a small explicit threshold (small enough for computation), so we first sharpen it.

Lemma 6.1. *Let D_k be the dihedral group of order $N = 2k$, with $k \ge 3$. Then for all $g \ne h \in D_k$,*

$$i(\mathcal{F}_{PP}(g,h)) \le \frac{9}{7} \cdot 19^{N/6}. \quad (6.3)$$

[3]From the perspective of Theorem 1.5, there's nothing particular special about dihedral groups. We apply this explicit threshold analysis as a proof-of-concept for our methodology, and to fully resolve Conjecture 1.1. Similar analysis can be applied to other families of groups, but for brevity we settle for "sufficiently large".

Proof. Write ρ for a rotation of order k, so the rotations form the cyclic subgroup $\langle\rho\rangle$ and every other element is a reflection. First suppose g or h is a reflection, say g. The centralizer of a reflection has order at most 4, so, as in the proof of Lemma 3.12, at most 4 vertices lie in 2-cycles of $\mathcal{F}_P(g)$ and

$$i(\mathcal{F}_{PP}(g,h)) \;\le\; i(\mathcal{F}_P(g)) \;\le\; \sqrt{3}^4 \cdot 7^{(N-4)/4} \;=\; \frac{9}{7}\cdot 7^{N/4} \;\le\; \frac{9}{7}\cdot 19^{N/6}. \tag{6.4}$$

Now suppose $g = \rho^a$ and $h = \rho^b$ are both rotations, with $a \neq b$ modulo k. A product xy is a rotation exactly when x and y are both rotations or both reflections, so $\mathcal{F}_{PP}(g,h)$ has no edges between rotations and reflections, and $i(\mathcal{F}_{PP}(g,h))$ is the product of the numbers of independent sets of the two induced subgraphs. The subgroup of rotations is abelian, so we are in the situation of the last part of the proof of Lemma 4.7 with G replaced by $\langle\rho\rangle$, hence the rotations contribute at most $7^{k/4}$.

On the reflections, a reflection x is joined to $xg,\ gx,\ xh,\ hx$, which are the reflections obtained from x by rotating through $\pm a$ and $\pm b$. If $a = 0$ or $b = 0$, every reflection is self-adjacent and contributes a factor of 1. Otherwise, the reflections form a simple graph with every degree in $\{2,3,4\}$, so they contribute at most $19^{k/6}$ by Corollary 4.5. Since $7^{1/4} < 19^{1/6}$, we conclude that

$$i(\mathcal{F}_{PP}(g,h)) \;\le\; 7^{k/4}\cdot 19^{k/6} \;\le\; 19^{k/3} \;=\; 19^{N/6}. \tag{6.5}$$

As $19^{N/6} \le \frac{9}{7}\cdot 19^{N/6}$, the bound in (6.4) is the larger of the two, so (6.3) holds in both cases. □

Theorem 6.2. *All dihedral groups D_n for $n \ge 3$ are product-dominant.*

Proof. Let D_k be the dihedral group of order $N_k := 2k$. We have

$$Z_k \;=\; \begin{cases} 2 & k \text{ even}, \\ 1 & k \text{ odd}, \end{cases} \tag{6.6}$$

and

$$T_k \;=\; \begin{cases} k+1 & k \text{ even}, \\ k & k \text{ odd}. \end{cases} \tag{6.7}$$

Let Q_k, P_k, QQ_k, PP_k be as in Lemma 5.1. As $7^{1/4} < 1.68$, Corollary 3.11 and Lemma 3.12 give

$$T_k\cdot\sqrt{3}^{N_k} \;\le\; Q_k \;\le\; T_k\cdot\sqrt{3}^{N_k} + (N_k - T_k)\cdot 1.68^{N_k}, \tag{6.8}$$

$$P_k \;\le\; Z_k\cdot\sqrt{3}^{N_k} + (N_k - Z_k)\cdot 1.68^{N_k}. \tag{6.9}$$

Furthermore, since the sums defining QQ_k and PP_k run over the $N_k(N_k-1)$ ordered pairs (g,h) with $g \neq h$, Lemmas 4.7 and 6.1 give

$$QQ_k \;\le\; N_k(N_k-1)\cdot 19^{N_k/6}, \tag{6.10}$$

$$PP_k \;\le\; \frac{9}{7}\cdot N_k(N_k-1)\cdot 19^{N_k/6}. \tag{6.11}$$

Let

$$U_k := (T_k + Z_k)\sqrt{3}^{N_k} + (2N_k - T_k - Z_k) \cdot 1.68^{N_k}. \tag{6.12}$$

Then $2^{N_k} - B(G_k) \leq Q_k + P_k \leq U_k$ and $M_2(G_k) \leq U_k + \frac{16}{7}N_k(N_k - 1) \cdot 19^{N_k/6}$. Hence, by Theorem 1.3 and Lemma 5.1, we want to find k_0 such that $k \geq k_0$ implies

$$\frac{\left[(T_k - Z_k)\sqrt{3}^{N_k} - (N_k - Z_k) \cdot 1.68^{N_k}\right]^2}{U_k\left(U_k + \frac{16}{7}N_k(N_k - 1) \cdot 19^{N_k/6}\right)} > \frac{1}{2}. \tag{6.13}$$

Recall that $N_k = 2k$. When k is even, the left-hand side of (6.13) evaluates to

$$\frac{\left[(k-1)3^k - (2k-2)1.68^{2k}\right]^2}{\left[(k+3)3^k + (3k-3)1.68^{2k}\right]\left[(k+3)3^k + (3k-3)1.68^{2k} + \frac{32}{7}k(2k-1)19^{k/3}\right]}. \tag{6.14}$$

One can check that this expression is strictly larger than $1/2$ for all even $k \geq 62$. When k is odd, the left-hand side of (6.13) evaluates to

$$\frac{\left[(k-1)3^k - (2k-1)1.68^{2k}\right]^2}{\left[(k+1)3^k + (3k-1)1.68^{2k}\right]\left[(k+1)3^k + (3k-1)1.68^{2k} + \frac{32}{7}k(2k-1)19^{k/3}\right]}. \tag{6.15}$$

One can check that this expression is strictly larger than $1/2$ for all odd $k \geq 61$. Thus, D_k is product-dominant for all $k \geq 61$, and we are left to check all $k \in \{3, \ldots, 60\}$ manually. The details of this computation are given in Appendix A. □

Theorem 6.3. *All sufficiently large symmetric groups are product-dominant.*

Proof. For symmetric groups $\{S_k\}$ with $k \geq 3$, we have $Z_k = 1$ and $T_k \geq \binom{k}{2}$, so $Z_k = o(T_k)$, and case (i) of Theorem 1.5 applies. □

Theorem 6.4. *All sufficiently large non-abelian finite simple groups are product-dominant.*

Proof. Let G be a non-abelian finite simple group. Then $Z = |Z(G)| = 1$, since $Z(G)$ is a normal subgroup of G and is proper because G is non-abelian. Moreover, by the Feit–Thompson theorem [FT63], G has even order, hence has an element g of order 2. Let $\mathcal{C}_g$ be the conjugacy class of g. Then, the action of G on $\mathcal{C}_g$ by conjugation induces a homomorphism $\varphi : G \to S(\mathcal{C}_g)$, where $S(\mathcal{C}_g)$ denotes the symmetric group on $\mathcal{C}_g$. If $\ker\varphi = G$, then $xgx^{-1} = g$ for all $x \in G$, hence $g \in Z(G)$ which cannot be the case. Therefore, $\ker\varphi$ is a proper normal subgroup of G, thus is trivial. So, G embeds in $S(\mathcal{C}_g)$, and $|G| \leq |\mathcal{C}_g|!$. Therefore, if $\{G_k\}$ is a sequence of non-abelian finite simple groups with $|G_k| \to \infty$, we must have an involution $g_k \in G_k$ for all k, and since $|G_k| \leq |\mathcal{C}_{g_k}|!$, we must have $|\mathcal{C}_{g_k}| \to \infty$. Finally, every element in the conjugacy class $\mathcal{C}_{g_k}$ must also have order 2, thus $T_k \geq |\mathcal{C}_{g_k}| \to \infty$, so it follows that $Z_k = 1 = o(T_k)$, and case (i) of Theorem 1.5 applies. □

6.2. **Quotient-dominant groups.**

Theorem 6.5. *All sufficiently large groups of odd order are quotient-dominant.*

Proof. Let $\{G_k\}$ be a sequence of groups of odd order. Then, $T_k = 0$ and $Z_k \geq 1$, so we immediately have

$$T_k \cdot \sqrt{3}^{R_k/Z_k} \;=\; 0 \;=\; o(Z_k), \tag{6.16}$$

and case (ii) of Theorem 1.5 applies. □

For finite abelian groups, due to their prevalence in relation to the classic MSTD problem (see [Nat06]), we go deeper to obtain more concrete results. In terms of the orders of their elements, abelian groups can vary greatly. For example, [PW14] showed that abelian groups of the form C_2^k are all balanced, but most other abelian groups are quotient-dominant, and in general abelian groups with many involutions are harder to analyze, as Z_k and T_k from Theorem 1.5 are then of similar size. Hence, a general classifying theorem is harder to obtain for abelian groups, but the following result gets closer to classification with some extra strategies.

Theorem 6.6. *Let G be a finite abelian group, written additively, let $2G := \{2g : g \in G\}$, and let $m := |2G|$. Suppose $m \geq 6$ and $|G| \geq 171$. Then, G is quotient-dominant.*

Proof. Let $N := |G|$, and let T be the number of elements of order 2. The kernel of the homomorphism $x \mapsto 2x$ consists of the identity and the T elements of order 2, so the first isomorphism theorem gives $N = m \cdot (T+1)$.

Let P and Q be as in Lemma 5.1 (formed with G instead of G_k). Since G is abelian, $Z(G) = G$, and the number $r(g)$ of square roots of g is $T+1$ if $g \in 2G$ and 0 otherwise. Hence, by (3.32) and Corollary 3.11,

$$P \;=\; (N-m)\sqrt{3}^N + m\sqrt{3}^{N-(T+1)} \;=\; mT\sqrt{3}^N + m\sqrt{3}^{N-(T+1)}, \tag{6.17}$$

$$Q \;\leq\; T\sqrt{3}^N + (N-T)7^{N/4}. \tag{6.18}$$

Let $Q^+ := T\sqrt{3}^N + (N-T)7^{N/4}$, so $Q \leq Q^+$. Since $m \geq 6$ and $5T + 6 \cdot 3^{-(T+1)/2} \geq 3$ for every $T \geq 0$, (6.17) and (6.18) give

$$M_1(G) \overset{(3.8)}{=} Q - P \;\leq\; Q^+ - P \;\leq\; \sqrt{3}^N \left(N(7/9)^{N/4} - 3\right) \;<\; 0, \tag{6.19}$$

where the last inequality holds as $N \geq 171$. Hence case (ii) of Theorem 1.3 applies. Since G is abelian, every pair g, h is central, so (4.35) gives $PP \leq N(N-1) \cdot 7^{N/4}$, while (4.33) gives $QQ \leq N(N-1) \cdot 19^{N/6}$ (here PP and QQ are as in Lemma 5.1, not to be confused with the products $P \cdot P$ and $Q \cdot Q$). Write $W := N(N-1)\left(19^{N/6} + 7^{N/4}\right)$, so that $PP + QQ \leq W$.

As $Q < P$, we may apply Lemma 5.2 with $X = P$, and the quantities u, v of that lemma satisfy

$$\frac{Q}{P} \;\leq\; \frac{Q^+}{P} \;=:\; u \qquad \text{and} \qquad \frac{PP + QQ}{P} \;\leq\; \frac{W}{P} \;=:\; v. \tag{6.20}$$

By Lemma 5.2(ii), it therefore suffices to prove that

$$f(u,v) \;=\; u^2 - 6u + 1 - v(1+u) \;>\; 0 \tag{6.21}$$

for these u and v. We find explicit upper bounds for u and v which depend only on N. If $T = 0$, then $m = N$ and $P = N\sqrt{3}^{N-1}$, so $u = \sqrt{3}\,(7/9)^{N/4}$ and $v = \sqrt{3}\,(N-1)\left((19/27)^{N/6} + (7/9)^{N/4}\right)$,

and both bounds below hold. If $T \geq 1$, we have

$$\begin{aligned} u &= \frac{T\sqrt{3}^N + (N-T)7^{N/4}}{(N-m)\sqrt{3}^N + m\sqrt{3}^{N-(T+1)}} \\ &\leq \frac{T\sqrt{3}^N + (N-T)7^{N/4}}{mT\sqrt{3}^N} \\ &= \frac{1}{m} + \frac{N-T}{mT}(7/9)^{N/4} \\ &\leq \frac{1}{6} + 2\left(\frac{7}{9}\right)^{N/4} \end{aligned} \tag{6.22}$$

as $(N-T)/(mT) < N/(mT) = (T+1)/T \leq 2$. Moreover,

$$\begin{aligned} v &= \frac{N(N-1)\left(19^{N/6} + 7^{N/4}\right)}{(N-m)\sqrt{3}^N + m\sqrt{3}^{N-(T+1)}} \\ &\leq \frac{N(N-1)\left(19^{N/6} + 7^{N/4}\right)}{mT\sqrt{3}^N} \\ &\leq 2(N-1)\left(\left(\frac{19}{27}\right)^{N/6} + \left(\frac{7}{9}\right)^{N/4}\right), \end{aligned} \tag{6.23}$$

since $N/(mT) = (T+1)/T \leq 2$. Thus,

$$f(u,v) \geq f\left(\frac{1}{6} + 2\left(\frac{7}{9}\right)^{N/4}, 2(N-1)\left(\left(\frac{19}{27}\right)^{N/6} + \left(\frac{7}{9}\right)^{N/4}\right)\right) =: h(N). \tag{6.24}$$

Finally, it is not hard to show that $h(N)$ is increasing for every $N \geq 12$, and numerical analysis shows that $h(N) > 0$ for all $N \geq 171$. □

Remark 6.7. *The threshold $N = 171$ can be lowered computationally in the same way as for dihedral groups, as described in Appendix A. However, due to the size of these groups, as well as the quantity with which they occur, it's unlikely that the present methods would resolve the rest of the abelian groups with $|2G| \geq 6$ and $|G| \leq 170$*

7. COMPUTING $M_1(G)$ BY CHARACTERS AND CONJUGACY CLASSES

We aim to find the length of the cycle containing a vertex x in $\mathcal{F}_P(g)$ in order to compute

$$\sum_{g \in G} i(\mathcal{F}_P(g)). \tag{7.1}$$

Definition 7.1. *Recall from Section 3 the definition of $p_g^{(n)}(x)$. For $g, x \in G$, let $\ell_{g,x}$ denote the minimal positive integer ℓ such that $p_g^{(\ell)}(x) = x$. Thus, the cycle containing x in $\mathcal{F}_P(g)$ has length $\ell_{g,x}$.*

Lemma 7.2. *If $p_g^{(d)}(x) = x$, then $\ell_{g,x} \mid d$.*

Proof. Write $\ell := \ell_{g,x}$ and $d = q\ell + s$ with $q \geq 0$ and $0 \leq s < \ell$. Since $p_g^{(\ell)}(x) = x$, applying this q times gives $p_g^{(q\ell)}(x) = x$, hence

$$x \;=\; p_g^{(d)}(x) \;=\; p_g^{(s)}\left(p_g^{(q\ell)}(x)\right) \;=\; p_g^{(s)}(x), \tag{7.2}$$

where $p_g^{(0)}$ denotes the identity map. By the minimality of ℓ, we must have $s = 0$, so $\ell \mid d$. □

Lemma 7.3. *For any $g, x \in G$, $\ell_{g,x}$ divides $2\,\mathrm{ord}(g)$.*

Proof. By Lemma 3.7,

$$p_g^{(2\,\mathrm{ord}(g))}(x) \;=\; g^{-\,\mathrm{ord}(g)} x g^{\mathrm{ord}(g)} \;=\; x, \tag{7.3}$$

so by Lemma 7.2 we have $\ell_{g,x} \mid 2\,\mathrm{ord}(g)$. □

To determine the minimal ℓ with $p_g^{(\ell)}(x) = x$, it helps to know how many $x \in G$ satisfy $p_g^{(d)}(x) = x$ for a fixed positive integer d. This can be computed with character theory, as the irreducible characters of a group provide counting formulas for the size of the centralizer of an element, and the number of square roots of an element.

Lemma 7.4. *For any $g \in G$, $d \in \mathbb{Z}^+$, let*

$$L(d, g) \;:=\; \#\left\{x \in G : p_g^{(d)}(x) = x\right\}. \tag{7.4}$$

Let $\chi_1, \ldots, \chi_n$ be the irreducible characters of G, and let ν be the Frobenius–Schur indicator

$$\nu(\chi) \;:=\; \frac{1}{|G|} \sum_{h \in G} \chi(h^2). \tag{7.5}$$

If $d = 2k$ is even, then

$$L(2k, g) \;=\; \left|C_G(g^k)\right| \;=\; \sum_{i=1}^{n} \left|\chi_i(g^k)\right|^2. \tag{7.6}$$

If $d = 2k+1$ is odd, then

$$L(2k+1, g) \;=\; \sum_{i=1}^{n} \nu(\chi_i) \cdot \chi_i(g^{-2k-1}). \tag{7.7}$$

Proof. Recall that $p_g^{(2k)}(x) = x \iff xg^k = g^k x$. Thus, $L(2k, g) = |C_G(g^k)|$. The second equality in (7.6) follows from the second orthogonality relation for characters.

When $d = 2k+1$ is odd, Lemma 3.7 gives

$$p_g^{(2k+1)}(x) \;=\; x \iff g^{-k} x^{-1} g^{k+1} \;=\; x. \tag{7.8}$$

Substituting $x = g^{k+1} y$ yields

$$\begin{aligned} p_g^{(d)}(x) = x \;&\iff\; g^{-k} y^{-1} g^{-(k+1)} g^{k+1} = g^{k+1} y \\ &\iff\; g^{-d} = y^2. \end{aligned} \tag{7.9}$$

Our substitution induces a bijection on G, hence the number of $y \in G$ satisfying $g^{-d} = y^2$ is precisely $L(d,g)$. The number of square roots of g^{-d} is known in general to be

$$\sum_{i=1}^{n} \nu(\chi_i) \cdot \chi_i(g^{-d}) \tag{7.10}$$

(see [Isa06] or [Row22], for example). This proves (7.7). □

Having counted the x satisfying $p_g^{(d)}(x) = x$, we apply the Möbius inversion formula (see [Wei]) to count the x for which d is the minimal positive integer with $p_g^{(d)}(x) = x$.

Theorem 7.5. *Fix $g \in G$. Let $c(m,g)$ be the number of m-length cycles in $\mathcal{F}_P(g)$. Then*

$$c(m,g) \;=\; \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) L(d,g). \tag{7.11}$$

Proof. Define

$$f(d) \;:=\; \#\{x \in G : \ell_{g,x} = d\}. \tag{7.12}$$

Then, by Lemma 7.2, we see that

$$L(m,g) \;=\; \sum_{d|m} f(d). \tag{7.13}$$

Thus, by the Möbius inversion formula, we have

$$f(m) \;=\; \sum_{d|m} \mu(m/d) \cdot L(d,g), \tag{7.14}$$

where μ is the Möbius function. This gives us the number of $x \in G$ contained in m-cycles in $\mathcal{F}_P(g)$. We divide by m to obtain the total number of m-length cycles. □

Theorem 7.6. *Let G be a finite group, let $\mathcal{C}_1, \ldots, \mathcal{C}_n$ be the distinct conjugacy classes of G, and let g_i be a representative for $\mathcal{C}_i$. Then*

$$M_1(G) \;=\; \sum_{i=1}^{n} |\mathcal{C}_i| \left(L_{\operatorname{ord} g_i}^{|G|/\operatorname{ord} g_i} - \prod_{m|(2\cdot \operatorname{ord} g_i)} L_m^{c(m,g_i)} \right). \tag{7.15}$$

Proof. By Lemma 3.5,

$$M_1(G) \;=\; \sum_{g \in G} \left(i(\mathcal{F}_Q(g)) - i(\mathcal{F}_P(g)) \right). \tag{7.16}$$

By the work done in Section 3 (namely Lemma 3.6, Remark 3.8, and Lemma 3.9), as well as the definition of $c(m,g)$ and Lemma 7.3, we see that

$$i(\mathcal{F}_Q(g)) - i(\mathcal{F}_P(g)) \;=\; L_{\operatorname{ord}(g)}^{|G|/\operatorname{ord}(g)} - \prod_{m|(2\cdot \operatorname{ord} g)} L_m^{c(m,g)}. \tag{7.17}$$

Moreover, from the computation leading to (3.3), recall that

$$i(\mathcal{F}_Q(g)) - i(\mathcal{F}_P(g)) \;=\; \#\{A \subseteq G : g \in AA\} - \#\{A \subseteq G : g \in AA^{-1}\}. \tag{7.18}$$

Now, for any $g \in G$, $A \subseteq G$, and any automorphism σ of G, note that

$$\begin{aligned} g \in AA &\iff g = xy \text{ for } x, y \in A \\ &\iff \sigma(g) = \sigma(x)\sigma(y) \text{ for } x, y \in A \\ &\iff \sigma(g) \in \sigma(A)\sigma(A). \end{aligned} \tag{7.19}$$

We obtain a similar equivalence for $g \in AA^{-1}$. Since $A \mapsto \sigma(A)$ is a bijection on the subsets of G, the expression in (7.18) takes the same value at g and at $\sigma(g)$. In particular, they are invariant under the action of conjugation, so it follows from (7.17) that

$$\begin{aligned} \sum_{g \in G} \left(i(\mathcal{F}_Q(g)) - i(\mathcal{F}_P(g))\right) &= \sum_{i=1}^{n} |\mathcal{C}_i| \left(i(\mathcal{F}_Q(g_i)) - i(\mathcal{F}_P(g_i))\right) \\ &= \sum_{i=1}^{n} |\mathcal{C}_i| \left(L_{\operatorname{ord} g_i}^{|G|/\operatorname{ord} g_i} - \prod_{m \mid (2 \cdot \operatorname{ord} g_i)} L_m^{c(m, g_i)} \right). \end{aligned} \tag{7.20}$$

□

Using Theorems 7.5 and 7.6, we obtain a simpler way to compute $M_1(G)$ for groups whose character theory and conjugacy classes are understood.

8. FUTURE WORK

Theorem 1.5 establishes the product/quotient-dominant behavior for many families of groups. However, the limitations of the theorem provide two natural paths for future work.

(1) For groups that satisfy the conditions of Theorem 1.5, such as those studied in Section 6, it may be of interest to quantify exactly when the key inequality in (1.9) is satisfied (as we do for dihedral groups in Theorem 6.2). Then, the product/quotient-dominant behavior can be manually computed so long as the remaining groups to check do not get too large.

(2) For groups which do not satisfy the conditions of Theorem 1.5, deeper analysis is required. In particular, these groups may not obtain the dominance of $\sqrt{3}^N$ terms in M_1, M_2, or $2^{|G|} - B$. For specific families like dicyclic (or generalized quaternion) groups, it is necessary to analyze the lower order terms to identify when (or if) (1.9) can be satisfied. For dicyclic groups, Mandal and Neetu [MN26] recently obtained exact and asymptotic counts of the MSTD, MDTS, and balanced subsets of sizes two and three, which suggests that the dominance behavior of these groups is delicate. For this, formulations like Theorems 7.5 and 7.6 could be useful.

On the topic of groups for which the conditions of Theorem 1.5 do not apply, we make the following remark.

Remark 8.1. *There exists a quotient-dominant group with $M_1(G) > 0$, namely the binary octahedral group (GAP ID (48,28)). Furthermore, there exists a product-dominant group with $M_1(G) < 0$, namely $C_6 \times S_3$ (GAP ID (36,12)). Therefore the method of proving dominance using the inequality in Theorem 1.3 does not work for all groups.*

It would be interesting to understand what exactly causes counterexamples such as these to occur.

Another natural direction may be to expand on the work of [Zha10b; Hav+21; Asc+22], by computing explicit asymptotic formulas on the proportion of subsets which are MPTQ or MQTP. One could also replace AA and AA^{-1} by more general words in A and A^{-1}, in the spirit of the generalized MSTD sets of Iyer, Lazarev, Miller, and Zhang [Iye+12].

Finally, for groups which are particularly resilient to the methodology of Theorem 1.3, it may be possible to apply more advanced statistical methods by taking higher moments of $d(A)$. These can be understood with forbiddance graphs as follows. For subsets $U, V \subseteq G$, define the generalized forbiddance graph $\mathcal{F}(U, V)$ to be the graph where the elements of U are forbidden "product-wise" and the elements of V are forbidden "quotient-wise". For example,

- $\mathcal{F}_P(g) = \mathcal{F}(\{g\}, \emptyset)$,
- $\mathcal{F}_{QQ}(g, h) = \mathcal{F}(\emptyset, \{g, h\})$,
- $\mathcal{F}_{PQ}(g, h) = \mathcal{F}(\{g\}, \{h\})$.

Then, one can show similarly to Lemma 4.3 that

$$M_r(G) := \sum_{A \subseteq G} d(A)^r = \sum_{j=0}^{r} \binom{r}{j} (-1)^{r-j} \sum_{\substack{g_1, \ldots, g_{r-j} \in G \\ h_1, \ldots, h_j \in G}} i(\mathcal{F}(\{g_1, \ldots, g_{r-j}\}, \{h_1, \ldots, h_j\})). \tag{8.1}$$

Using higher moments, it may be possible to obtain a stronger understanding of the distribution of $d(A)$.

APPENDIX A. DIHEDRAL GROUP COMPUTATION

We explain the computation involved, which can be found in [Ami26]. Generally speaking, naively computing whether a group is product- or quotient-dominant requires iterating over all 2^N subsets, which becomes very slow, very quickly. However, computing the number of independent sets of a graph can be faster: once a subset of the vertices is not independent, any superset cannot be independent either. Thus, we implement a depth-first search, which starts from the empty set and branches to larger subsets until non-independence is reached, at which point we backtrack. This is especially useful because, by [MV14], the proportion of subsets A with $AA = AA^{-1} = G$ converges to 1; such a subset is independent in no forbiddance graph, so the search prunes early and this algorithm becomes considerably more efficient than the naive one.

Furthermore, this algorithm can be pushed further if we already know the structure of the graphs we are studying. For instance, we know $\mathcal{F}_P$ and $\mathcal{F}_Q$ are disjoint unions of cycle graphs, so we need only count the lengths of the component cycles to compute the number of independent sets.

Theorem 6.2 used Theorem 1.3, along with our bounds on M_1, M_2, and $2^N - B$, to show that product dominance holds for sufficiently large k. Explicit computation of $M_1^2/(M_2 \cdot (2^N - B))$ shows that the desired inequality does hold for small N, when we use the actual values of M_1, M_2, and B.

- Up to 61, and far beyond it, computing M_1 is no problem, because the algorithm works extremely efficiently on graphs which it knows are disjoint cycle graphs, so Lemma 3.5 makes it easy.
- Computing M_2 is harder, as some of the graphs in Lemma 4.3 can take much longer to compute independent sets for. However, we have the upper bound from (5.5) and (5.19), which reduces computation of M_2 to the fast computations for $\mathcal{F}_P$ and $\mathcal{F}_Q$.
- Computing the number of balanced subsets is the hardest, as it cannot be directly expressed using independent sets of graphs; we only have the inequality (5.6), which allows us to bound $2^N - B$ with the fast computations for $\mathcal{F}_P$ and $\mathcal{F}_Q$.

With this in mind, starting from $k = 60$ and going down, we use the upper bounds for M_2 and $2^N - B$ for as long as they can satisfy (1.9). This works down through $k = 53$. Then, wanting to avoid having to compute B at all costs, we compute the exact value of M_2, continue using the upper bound for $2^N - B$, and this works down through $k = 31$ (and technically $k = 29$). With nowhere left to turn, we have to compute B explicitly for $k \in \{3, \dots, 30\}$. For the larger values of k this required multi-threaded code running on a computing cluster. The desired inequality of Theorem 1.3 indeed held for all $k \in \{3, \dots, 60\}$, completing the proof. Note that this need not have been the case, as a group G can be product-dominant without satisfying the inequality (1.9).

ACKNOWLEDGMENTS

This research was conducted at the 2026 SMALL REU, with funding from the National Science Foundation (NSF Grant DMS-2341670), Missouri State University, the University of Chicago, the University of Michigan, the University of Rochester, and Williams College. We also thank Atrey Desai for running necessary computations on the UMIACS Nexus Cluster.

AI use. Large language models such as ChatGPT, Claude, and Gemini were used to assist with

- finding and helping to resolve two flaws in earlier versions of the proof of Theorem 1.5,
- refining our proof methods for Lemmas 4.7, 5.2 and 6.1,
- searching the literature for applicable known methods, such as Jensen's inequality for (3.34), the results in [Sah+19] for Corollary 4.5, and the Möbius inversion formula for (7.14),
- optimizing the code in [Ami26].

The authors take full responsibility for the content of this paper.

REFERENCES

[Ami26] Yuval Amit. *MSTD Groups*. https://github.com/YuvalAmit2/MSTD_Groups.git. 2026.

[Asc+22] Ruben Ascoli, Justin Cheigh, Guilherme Zeus Dantas e Moura, Ryan Jeong, Andrew Keisling, Astrid Lilly, Steven J. Miller, Prakod Ngamlamai, and Matthew Phang. "Sum and Difference Sets in Generalized Dihedral Groups". In: *Combinatorics and Combinatorial Computing MCCCC34, Normal, IL, USA, October 21–23, 2022*. Ed. by Amin Bahmanian. Springer Proceedings in Mathematics & Statistics. Springer, 2022, pp. 1–30.

[Duv+26] Julian Duvivier, Xiaoyao Huang, Ava Kennon, Say-Yeon Kwon, Steven J. Miller, Arman Rysmakhanov, Pramana Saldin, and Ren Watson. "Comparing Left and Right Quotient Sets in Groups". In: *Integers* 26A (2026).

[FT63] Walter Feit and John G. Thompson. "Solvability of Groups of Odd Order". In: *Pacific Journal of Mathematics* 13 (1963), pp. 775–1029. ISSN: 0030-8730. URL: http://projecteuclid.org/euclid.pjm/1103053943.

[Gho02] B. K. Ghosh. "Probability Inequalities Related to Markov's Theorem". In: *The American Statistician* 56.3 (2002), pp. 186–190. DOI: 10.1198/000313002119. URL: https://www.tandfonline.com/doi/abs/10.1198/000313002119.

[Hav+21] Jack Haviland, Phúc Lâm, John Lentfer, Steven J. Miller, and Fernando Trejos Suárez. "More Sums Than Differences Sets in Finite Non-Abelian Groups". In: *Combinatorial and Additive Number Theory IV: CANT 2019 and 2020*. Springer. 2021, pp. 21–77.

[Heg07] Peter V. Hegarty. "Some explicit constructions of sets with more sums than differences". In: *Acta Arithmetica* 130 (2007), pp. 61–77. DOI: 10.4064/aa130-1-4.

[HM09] Peter V. Hegarty and Steven J. Miller. "When Almost All Sets Are Difference Dominated". In: *Random Structures & Algorithms* 35.1 (2009), pp. 118–136. DOI: 10.1002/rsa.20268. URL: https://doi.org/10.1002/rsa.20268.

[HLM17] Anand Hemmady, Adam Lott, and Steven J. Miller. "When Almost All Sets Are Difference Dominated in Z/nZ". In: *Integers* 17 (2017), A54. URL: https://api.semanticscholar.org/CorpusID:53617459.

[Her26] Yorick Herrmann. "A Classification of Small MSTD Sets in Arbitrary Fields". In: *arXiv preprint* (2026). arXiv: 2608.22189 [math.NT]. URL: https://arxiv.org/abs/2608.22189.

[Isa06] Martin Isaacs. *Character Theory of Finite Groups*. Providence, RI: AMS Chelsea Publishing, 2006. ISBN: 978-0821842294.

[Iye+12] Geoffrey Iyer, Oleg Lazarev, Steven J. Miller, and Liyang Zhang. "Generalized More Sums Than Differences Sets". In: *Journal of Number Theory* 132.5 (2012), pp. 1054–1073. DOI: 10.1016/j.jnt.2011.10.012. URL: https://doi.org/10.1016/j.jnt.2011.10.012.

[Jen06] J. L. W. V. Jensen. "Sur les Fonctions Convexes et les Inégalités entre les Valeurs Moyennes". In: *Acta Mathematica* 30.1 (1906), pp. 175–193. DOI: 10.1007/BF02418571. URL: https://doi.org/10.1007/BF02418571.

[MN26] Sagar Mandal and Neetu. "Exact and Asymptotic Counts of MSTD, MDTS, and Balanced Sets in Dicyclic Groups". In: *arXiv preprint* (2026). arXiv: 2602.09073 [math.NT]. URL: https://arxiv.org/abs/2602.09073.

[MO07] G. Martin and K. O'Bryant. "Many sets have more sums than differences". In: *Additive Combinatorics*. Vol. 43. CRM Proceedings & Lecture Notes. Providence, RI: American Mathematical Society, 2007, pp. 287–305.

[MOS10] Steven J. Miller, Brooke Orosz, and Daniel Scheinerman. "Explicit Constructions of Infinite Families of MSTD Sets". In: *Journal of Number Theory* 130.5 (2010), pp. 1221–

1233. DOI: 10.1016/j.jnt.2009.09.003. URL: https://doi.org/10.1016/j.jnt.2009.09.003.

[MV14] Steven J. Miller and Kevin Vissuet. "Most Subsets Are Balanced in Finite Groups". In: *Combinatorial and Additive Number Theory*. Ed. by Melvyn B. Nathanson. New York, NY: Springer New York, 2014, pp. 147–157. ISBN: 978-1-4939-1601-6.

[Nat07] M. B. Nathanson. "Sets with more sums than differences". In: *Integers* 7 (2007), A5.

[Nat06] Melvyn B. Nathanson. "Problems in Additive Number Theory, I". In: *arXiv preprint* (2006). arXiv: math/0604340 [math.NT]. URL: https://arxiv.org/abs/math/0604340.

[PW14] David Penman and Matthew Wells. "Sum-Dominant Sets and Restricted-Sum-Dominant Sets in Finite Abelian Groups". In: *Acta Arithmetica* 165 (Jan. 2014), pp. 361–383. DOI: 10.4064/aa165-4-6.

[Row22] Glenn Rowe. *Square Roots of Group Elements*. PhysicsPages. Aug. 2022. URL: https://physicspages.com/pdf/Group%20theory/Square%20roots%20of%20group%20elements.pdf.

[Sah+19] Ashwin Sah, Mehtaab Sawhney, David Stoner, and Yufei Zhao. "The Number of Independent Sets in an Irregular Graph". In: *Journal of Combinatorial Theory, Series B* 138 (Sept. 2019), pp. 172–195. ISSN: 0095-8956. DOI: 10.1016/j.jctb.2019.01.007. URL: http://dx.doi.org/10.1016/j.jctb.2019.01.007.

[Soc20] Joram Soch. *The Second Raw Moment Equals Squared Mean Plus Squared Standard Deviation*. The Book of Statistical Proofs. Oct. 2020. DOI: 10.5281/zenodo.4305949. URL: https://statproofbook.github.io/P/momraw-2nd.html.

[SS05] Elias M. Stein and Rami Shakarchi. *Real Analysis: Measure Theory, Integration, and Hilbert Spaces*. Vol. 3. Princeton Lectures in Analysis. Princeton, NJ: Princeton University Press, 2005. ISBN: 978-0-691-11386-9.

[Tao08] Terence Tao. "Product Set Estimates for Non-Commutative Groups". In: *Combinatorica* 28.5 (2008), pp. 547–594. DOI: 10.1007/s00493-008-2271-7. URL: https://doi.org/10.1007/s00493-008-2271-7.

[Wei] Eric W. Weisstein. *Möbius Inversion Formula*. MathWorld–A Wolfram Web Resource. URL: https://mathworld.wolfram.com/MoebiusInversionFormula.html.

[Zha09] Yufei Zhao. "The Number of Independent Sets in a Regular Graph". In: *Combinatorics, Probability and Computing* 19.2 (Nov. 2009), pp. 315–320. ISSN: 1469-2163. DOI: 10.1017/s0963548309990538. URL: http://dx.doi.org/10.1017/S0963548309990538.

[Zha10a] Yufei Zhao. "Constructing MSTD Sets Using Bidirectional Ballot Sequences". In: *Journal of Number Theory* 130.5 (2010), pp. 1212–1220. DOI: 10.1016/j.jnt.2009.11.005. URL: https://doi.org/10.1016/j.jnt.2009.11.005.

[Zha10b] Yufei Zhao. "Counting MSTD Sets in Finite Abelian Groups". In: *Journal of Number Theory* 130.10 (Oct. 2010), pp. 2308–2322. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2010.06.001. URL: http://dx.doi.org/10.1016/j.jnt.2010.06.001.

[Zha11] Yufei Zhao. "Sets Characterized by Missing Sums and Differences". In: *Journal of Number Theory* 131.11 (2011), pp. 2107–2134. DOI: 10.1016/j.jnt.2011.05.003. URL: https://doi.org/10.1016/j.jnt.2011.05.003.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK
Email address: yamit@umd.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CHICAGO
Email address: lucasch@uchicago.edu

DEPARTMENT OF MATHEMATICS, MISSOURI STATE UNIVERSITY
Email address: christopherlancehousholder@gmail.com

DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY
Email address: jri@tamu.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ROCHESTER
Email address: joshuakhan1307@gmail.com

DEPARTMENT OF MATHEMATICS, WILLIAMS COLLEGE
Email address: sjm1@williams.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN
Email address: mateop@umich.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN
Email address: pradhand@umich.edu