

COMPARING LEFT AND RIGHT QUOTIENT SETS IN GROUPS

Julian Duvivier*Department of Mathematics, Reed College, Portland, OR*
june@duvivier.us**Xiaoyao Huang***Department of Mathematics, University of Michigan, Ann Arbor, MI*
xyrushac@umich.edu**Ava Kennon***Department of Mathematics, Amherst College, Amherst, MA*
akennon26@amherst.edu**Say-Yeon Kwon***Department of Mathematics, Princeton University, Princeton, NJ*
sk9017@princeton.edu**Steven J. Miller***Department of Mathematics, Williams College, Williamstown, MA*
sjm1@williams.edu**Arman Rysmakhanov***Department of Mathematics, Williams College, Williamstown, MA*
ar21@williams.edu**Pramana Saldin***Department of Mathematics, University of Wisconsin, Madison, WI*
saldin@wisc.edu**Ren Watson***Department of Mathematics, University of Texas at Austin, Austin, TX*
renwatson@utexas.edu*Revised: February 24, 2026***Abstract**

For a finite subset A of a group G , we define the right quotient set and the left quotient set of A , respectively, as

$$AA^{-1} := \{a_1 a_2^{-1} : a_1, a_2 \in A\},$$

$$A^{-1}A := \{a_1^{-1} a_2 : a_1, a_2 \in A\}.$$

While the right and left quotient sets are equal if G is abelian, subtleties arise when G is a nonabelian group, where the cardinality difference $|AA^{-1}| - |A^{-1}A|$ may take on arbitrarily large values. Using the results of Martin and O’Bryant on the cardinality differences of sum sets and difference sets in \mathbb{Z} , we prove that in the infinite dihedral group, $D_\infty \cong \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, every integer difference is achievable. Further, we prove that in F_2 , the free group on 2 generators, an integer difference is achievable if and only if that integer is even, and we explicitly construct subsets of F_2 that achieve every even integer. We further determine the minimum cardinality of $A \subset G$ so that the difference between the cardinalities of the left and right quotient sets is nonzero, depending on the existence of order 2 elements in G . To prove these results, we construct difference graphs D_A and $D_{A^{-1}}$ which encode equality, respectively, in the right and left quotient sets. We observe a bijection from edges in D_A to edges in $D_{A^{-1}}$ and count connected components in order to obtain our results on cardinality differences $|AA^{-1}| - |A^{-1}A|$.

§1 Introduction

Note: This paper is dedicated with thanks to Carl Pomerance and Mel Nathanson. The genesis for this work came from conversations the fifth named author had at the Integers Conference in Georgia in 2025 on Results in Additive & Elementary Number Theory Inspired by Carl and Mel. His presentation described how much of his mentoring of students has been influenced by each, in particular problems in the orbit of MSTD sets (from Mel) and multiplicative and quotient structures (from Carl). This led to springboard problems for the SMALL 2025 REU, which led to the work below.

1.1. Background

Given a subset A of $[N] := \{1, \dots, N\}$, the sumset and difference sets are defined as

$$\begin{aligned} A + A &:= \{a_1 + a_2 : a_1, a_2 \in A\}, \\ A - A &:= \{a_1 - a_2 : a_1, a_2 \in A\}. \end{aligned}$$

A natural comparison arises between the cardinalities of the sum and difference sets. Our set A is said to be *sum dominated or MSTD* (more sums than differences) if $|A + A| > |A - A|$ and *difference dominated (MDTS)* if $|A - A| > |A + A|$. One might expect that the difference set would have a greater cardinality as addition is commutative in \mathbb{Z} while subtraction is not. In particular, if we consider a pair of distinct elements $a_1, a_2 \in A$, $a_1 - a_2$ and $a_2 - a_1$ are distinct elements in the difference set, while $a_1 + a_2 = a_2 + a_1$ is a single element in the sumset. However, it is possible to have a set that is sum dominated. The earliest example of a MSTD

set was discovered by Conway in 1960s: $\{0, 2, 3, 4, 7, 11, 12, 14\}$. Surprisingly, in contrast to the intuition that MSTD sets should form a vanishing proportion of subsets of $[N]$ as N grows large, in 2006 Martin and O’Bryant [11] proved that the proportion of subsets of $[N] \subseteq \mathbb{Z}$ which are MSTD does not vanish as $N \rightarrow \infty$. Since then, extensive research has expanded the classical MSTD problem to various settings, including higher dimensions and various families [6, 3, 2].

A natural extension of the study of MSTD sets among subsets of \mathbb{Z} is to ask the question for general groups. This has been investigated in previous work by [1, 13, 14, 17]. In this paper, the main groups of interest are the free group F_2 on two generators and the infinite dihedral group $D_\infty \cong \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Definition 1.1. *Let A be a set of generators with $|A| = n$. The free group on A , denoted $F(A)$ or F_n , is the group consisting of all reduced words over the alphabet $A \cup A^{-1} = \{x : x \in A\} \cup \{x^{-1} : x \in A\}$ under the operation of concatenation followed by reduction, where reduction means canceling adjacent inverse pairs.*

We now define sumsets and difference sets in general groups. Let $A \subset G$ be a finite subset of a group G equipped with the operation $\times : (x, y) \mapsto xy$ and the inverse map $*^{-1} : x \mapsto x^{-1}$. Although some authors use the terminology sumset and difference set in this context [1, 13, 14, 17], we refer to the *product set* and the *quotient set* of A , which are defined, respectively as

$$\begin{aligned} AA &:= \{xy : x, y \in A\}, \\ AA^{-1} &:= \{xy^{-1} : x, y \in A\}. \end{aligned}$$

More generally, let G be any group. Let $A = \{a_1, \dots, a_n\} \subseteq G$. Define $A^{-1} := \{a_1^{-1}, \dots, a_n^{-1}\}$. We consider the *right quotient set* and *left quotient set* of A , defined, respectively, by

$$\begin{aligned} AA^{-1} &:= \{a_i \cdot a_j^{-1} : a_i, a_j \in A\}, \\ A^{-1}A &:= \{a_i^{-1} \cdot a_j : a_i, a_j \in A\}. \end{aligned}$$

In the classical MSTD problem, one natural area of study has been the cardinality of the smallest MSTD set. Hegarty showed that the smallest such example in \mathbb{Z} has cardinality 8, and is unique up to affine translation [4]. Another natural question asks for the set of values that $|A + A| - |A - A|$ can attain across all $A \subset [N]$. Martin and O’Bryant proved, over finite subsets of \mathbb{Z} , that this difference achieves all integers [11].

Inspired by this, we consider similar questions about left and right quotient sets. First note that the problem of constructing a set A where $|AA^{-1}| > |A^{-1}A|$ is the same as the problem of $|AA^{-1}| < |A^{-1}A|$ (by replacing A with A^{-1}). Therefore, a more natural question to ask is the smallest A where the left and right quotient sets are not equal. Moreover, inspired by [11], we give results on what values $|AA^{-1}| - |A^{-1}A|$ can take as A ranges over finite subsets of a group G .

Example 1.2. While there has been some work done generalizing in an abelian group setting [13, 14, 18], our questions are only relevant for non-abelian groups. Indeed, if G is abelian, then all $A \subseteq G$ have $AA^{-1} = A^{-1}A$, so the only possible value of $|AA^{-1}| - |A^{-1}A|$ is 0.

1.2. Notation and Main Results

Theorem 1.3. Let G be a group with no elements of order 2.¹ Let $A \subseteq G$ be a finite subset. Then $|AA^{-1}| - |A^{-1}A|$ is even.

This result does not hold in the context of groups with elements of order 2. In fact, we can construct examples where odd values of $|AA^{-1}| - |A^{-1}A|$ are achieved.

Example 1.4. Let $G = D_\infty := \langle r, s \mid sr = r^{-1}s, s^2 = e \rangle$ be the infinite dihedral group. For every $n \in \mathbb{Z}$, there exists a subset $A_n \subseteq D_\infty$ such that $|A_n A_n^{-1}| - |A_n^{-1} A_n| = n$. Indeed, let $B \subseteq \mathbb{Z}$ be a finite subset to be determined later. Consider the subset

$$A := \{r^b : b \in B\} \cup \{sr^b : b \in B\} \subseteq D_\infty.$$

We see that

$$\begin{aligned} AA^{-1} &= \underbrace{\{r^{b-b'} : b, b' \in B\}}_{A_1} \sqcup \underbrace{\{sr^{b'-b} : b, b' \in B\}}_{A_2}, \\ A^{-1}A &= \underbrace{\{r^{b'-b} : b, b' \in B\}}_{A'_1} \sqcup \underbrace{\{sr^{b'+b} : b, b' \in B\}}_{A'_2}. \end{aligned}$$

Notice that $A_1 = A'_1$, and $|A_2| = |B - B|$ and $|A'_2| = |B + B|$. Therefore,

$$|AA^{-1}| - |A^{-1}A| = |B - B| - |B + B|.$$

By [11, Theorem 4], the latter difference ranges over every integer.

Considering in particular the free group $G = F_2$, we can construct examples where every even integer is achieved.

Theorem 1.5 (F_2 achieves all even possible differences). For all $n \in \mathbb{Z}$, there exists a set $A_n \subseteq F_2$ such that $|A_n A_n^{-1}| - |A_n^{-1} A_n| = 2n$.

The construction for the previous theorem uses a subset $A \subseteq F_2$ of cardinality 5 that satisfies $|AA^{-1}| \neq |A^{-1}A|$. The following theorem shows this construction is optimal with respect to the size of A for a more general class of groups.

¹While we use the language of “a group with no elements of order 2”, we remark that Tao refers to such a group as a “a 2-torsion-free group” in [15].

Theorem 1.6. *Let G be a group. Let $A \subseteq G$ be a finite subset and suppose that $|AA^{-1}| \neq |A^{-1}A|$. Then*

- *without any further assumptions, $|A| \geq 4$, and*
- *if G is a group with no elements of order 2, then $|A| \geq 5$.*

A brute force search on groups of small order show that the bound $|A| \geq 4$ is sharp (see Example 2.10). The main tool we use to prove this result is a graph associated to the left (and right) quotient sets, which we call the difference graph. The cardinalities of AA^{-1} and $A^{-1}A$ can be interpreted as the number of connected components on these graphs. Making use a bijection of edges between these graphs, we perform an argument based on the properties of this graph to prove that when $|A| \leq 3$ (resp. $|A| \leq 4$ when A has no elements of order 2), the number of connected components does not change under the bijection of edges.

§2 Left vs. Right Quotient Sets

2.1. Graph Construction

To prove our results, we define the *difference graph* D_A of a finite subset $A := \{a_1, a_2, \dots, a_n\} \subseteq G$. The graph $D_A = (V, E)$ is defined as follows.

1. The vertex set is given by $V := [n] \times [n]$.
2. The edge set $E(D_A)$ is given by the relation

$$(i, j) \sim (k, \ell) \text{ if and only if } a_i a_j^{-1} = a_k a_\ell^{-1}.$$

The difference graph is directed and *not* simple (we allow self-loops).

Similarly, for $D_{A^{-1}}$, we have the edge relation

$$(i, j) \sim (k, \ell) \text{ if and only if } a_i^{-1} a_j = a_k^{-1} a_\ell.$$

We first note the following basic facts about D_A .

Lemma 2.1 (Properties of D_A). *Let $i, j, k, \ell \in [n]$.*

1. $[(i, j), (k, \ell)] \in E(D_A)$ if and only if $[(j, i), (\ell, k)] \in E(D_A)$.
2. *The following types of edges are not present in $E(D_A)$.*
 - (a) $[(i, j), (k, k)]$, an edge connecting to the diagonal, provided that $i \neq j$.
 - (b) $[(i, j), (i, k)]$ (or $[(j, i), (k, i)]$, but this is handled by (1)), an edge connecting vertices on the same axis.

(c) If G has no elements of order 2, then no edge connects a vertex (i, j) to its symmetric pair (j, i) , provided that $j \neq i$.

3. $[(i, i), (j, j)] \in E(D_A)$.

4. If C is a connected component in D_A , then C is a clique.

Proof. (1) Suppose $a_i a_j^{-1} = a_k a_\ell^{-1}$. Then

$$a_j a_i^{-1} = (a_i a_j^{-1})^{-1} = (a_k a_\ell^{-1})^{-1} = a_\ell a_k^{-1}.$$

Hence, $[(j, i), (\ell, k)] \in E(D_A)$ and note the reverse follows.

(2a) Let $[(i, j), (k, k)] \in E(D_A)$ where $i \neq j$. Thus

$$a_i a_j^{-1} = a_k a_k^{-1} = e,$$

which implies $a_i = a_j$. But $i \neq j$, a contradiction.

(2b) Without loss of generality, take the edge $[(i, j), (i, k)]$. Then we have

$$a_i a_j^{-1} = a_i a_k^{-1},$$

which implies $a_j = a_k$.

(2c) Let $[(i, j), (j, i)] \in E(D_A)$ where $i \neq j$. Then,

$$a_i a_j^{-1} = a_j a_i^{-1} = (a_i a_j^{-1})^{-1},$$

which implies

$$(a_i a_j^{-1})^2 = e.$$

Because G has no elements of order 2, so $a_i a_j^{-1} = e$ and $a_i = a_j$, contradicting our assumption that $i \neq j$.

(3) Consider $a_i a_i^{-1} = e = a_j a_j^{-1}$, thus $[(i, i), (j, j)] \in E(D_A)$.

(4) This follows because equality is an equivalence relation. □

Remark 2.2. In light of Property (4), we refer to a connected component C in D_A consisting of k elements simply by indicating its vertices $C = (a_1, b_1)(a_2, b_2) \cdots (a_k, b_k)$.

Remark 2.3. Property (1) is the same as saying the “transpose” operation

$$\begin{aligned} T: E(D_A) &\rightarrow E(D_A) \\ [(i, j), (k, \ell)] &\mapsto [(j, i), (\ell, k)] \end{aligned}$$

is a graph automorphism.

Let $\mathcal{C}(D_A)$ be the set of connected components of D_A and $c(D_A) = |\mathcal{C}(D_A)|$ be the number of connected components. Note that $c(D_A) = |AA^{-1}|$ and $c(D_{A^{-1}}) = |A^{-1}A|$.

Using the fact that

$$a_i a_j^{-1} = a_k a_\ell^{-1} \text{ exactly when } a_k^{-1} a_i = a_\ell^{-1} a_j,$$

we obtain a bijection of edges between D_A and $D_{A^{-1}}$ as follows:

$$\begin{aligned} \phi: E(D_A) &\rightarrow E(D_{A^{-1}}) \\ [(i, j), (k, \ell)] &\mapsto [(k, i), (\ell, j)]. \end{aligned}$$

A priori, this map is only well-defined if we consider edges as directed (the reverse edge gets mapped to the transpose of the original edge) and allow loops (they get mapped to the diagonal). However, since T is an automorphism of D_A , we may take D_A to be undirected. This is a well-motivated map: its existence already tells us that the *additive energies* $\Lambda(A, A^{-1}) := \{\#(a_1, a_2, a_3, a_4) \in A^4 : a_1 a_2^{-1} = a_3 a_4^{-1}\}$ and $\Lambda(A^{-1}, A) := \{\#(a_1, a_2, a_3, a_4) \in A^4 : a_1^{-1} a_2 = a_3^{-1} a_4\}$ are equal in non-commutative groups (see [15]).

Example 2.4. *When $n = 5$, consider the example in Figure 1.*

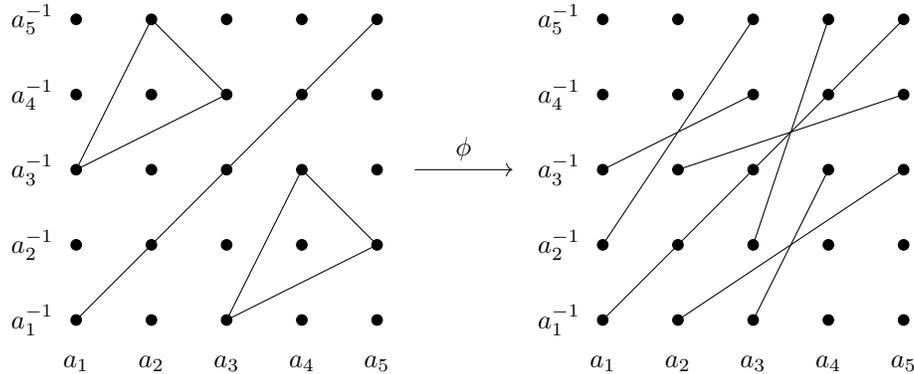


Figure 1: This example shows that the number of connected components in D_A changes after applying the map ϕ .

The former (left) graph prior to the mapping ϕ has 17 connected components, and the latter (right) graph after ϕ is applied has 15 connected components.

The first graph corresponds to

$$a_3 a_1^{-1} = a_4 a_3^{-1} = a_5 a_2^{-1}$$

being satisfied, and no other relations between words (other than the diagonal). The set

$$A := \{x, xz, y^{-1}, y^{-1}x^{-1}y^{-1}, y^{-1}z\} \subseteq F_3 = F(\{x, y, z\}) \quad (2.1)$$

satisfies this property, therefore giving us an example where $|AA^{-1}| \neq |A^{-1}A|$.

2.2. Possible Differences

The natural question that arises is: what are the possible differences between the cardinalities of the right and left quotient sets of $A \subset G$? In Example 1.4 we gave a construction on the infinite dihedral group D_∞ demonstrating the difference $|AA^{-1}| - |A^{-1}A|$ achieves every possible $n \in \mathbb{Z}$. Given the restriction that there are no elements of order 2 in our group, we can conclude that $|AA^{-1}| - |A^{-1}A|$ is even. The proof of Theorem 1.3 follows.

Proof of Theorem 1.3. It suffices to show that $c(D_A) - c(D_{A^{-1}})$ is even. We claim that $c(D_A)$ is odd. We divide $\mathcal{C}(D_A)$ into two disjoint classes.

1. The connected components that are fixed under T (i.e., $T(C) = C$), and
2. the connected components which are disjoint from their image under T ; that is, those connected components that are swapped with a distinct component under T .

Denote these sets, respectively, by \mathcal{C}_1 and \mathcal{C}_2 . Note that $|\mathcal{C}_2|$ is even as each component comes in pairs.

We claim that \mathcal{C}_1 contains only the diagonal (the diagonal is a connected component by Lemma 2.1 (3, 2a)). Indeed, if any other component C belongs to \mathcal{C}_1 , then there exists a vertex (i, j) with $i \neq j$ such that $[(i, j), (j, i)] \in C$, which contradicts Lemma 2.1 (2c). Therefore, there is exactly one component of \mathcal{C}_1 while the rest of the connected components come in symmetric pairs, so $|\mathcal{C}_1|$ is odd. Applying the same reasoning to $c(D_{A^{-1}})$ shows it is odd, so $c(D_A) - c(D_{A^{-1}})$ is even. \square

We now consider the set of possible differences in F_2 . In order to prove Theorem 1.5, we use the following.

Fact 2.5. *Let $m \geq 2$ be an integer. Then there exists an embedding $F_m \hookrightarrow F_2$.*

Proof. See, for example [9, Chapter I. Proposition 3.1.]. \square

Writing out this embedding explicitly allows us to describe a subset of F_2 where $|AA^{-1}| \neq |A^{-1}A|$. Indeed, take the set A given in (2.1) with the embedding $F_3 \hookrightarrow F_2$ by $x \mapsto x^2, y \mapsto xy, z \mapsto xy^{-1}$ to get the set

$$\{x^2, x^3y^{-1}, y^{-1}x^{-1}, y^{-1}x^{-3}y^{-1}x^{-1}, y^{-2}\} \subseteq F_2.$$

Proof of Theorem 1.5. Any set $A \subseteq \langle a \rangle \cong \mathbb{Z}$ with $a \in F_2$ yields the $n = 0$ case. By replacing A with A^{-1} , it suffices to prove the result for positive n . So, we construct

a family of sets $A_n \subseteq F_m$ for some $m \geq 2$ and then compose it with the embedding (2.5). The following set (described above) in $F_3 = F(\{x, y, z\})$ for $n = 1$

$$A = \{x, xz, y^{-1}, y^{-1}x^{-1}y^{-1}, y^{-1}z\},$$

$$A^{-1} = \{x^{-1}, z^{-1}x^{-1}, y, yxy, z^{-1}y\},$$

has

$$AA^{-1} = \{e, xz^{-1}x^{-1}, xy, xyxy, xz^{-1}y, xzx^{-1}, xzy, xzyxy, y^{-1}x^{-1}, y^{-1}z^{-1}x^{-1}, y^{-1}z^{-1}y, y^{-1}x^{-1}y^{-1}x^{-1}, y^{-1}x^{-1}y^{-1}z^{-1}x^{-1}, y^{-1}x^{-1}y^{-1}z^{-1}y, y^{-1}zx^{-1}, y^{-1}zy, y^{-1}zyxy\},$$

$$A^{-1}A = \{e, z, x^{-1}y^{-1}, x^{-1}y^{-1}x^{-1}y^{-1}, x^{-1}y^{-1}z, z^{-1}, z^{-1}x^{-1}y^{-1}, z^{-1}x^{-1}y^{-1}x^{-1}y^{-1}, z^{-1}x^{-1}y^{-1}z, yx, yxz, yxyx, yxyxz, z^{-1}yx, z^{-1}yxz\}.$$

Hence,

$$|AA^{-1}| - |A^{-1}A| = 17 - 15 = 2.$$

More generally for $n \geq 1$, A_n is constructed as a subset of $F_{3n} = F(\{x_1, y_1, z_1, \dots, x_n, y_n, z_n\})$ as follows. Let

$$A_n := \bigcup_{i=1}^n \{x_i, y_i^{-1}, y_i^{-1}x_i^{-1}y_i^{-1}, x_i z_i, y_i^{-1} z_i\}.$$

We claim

$$|A_n A_n^{-1}| - |A_n^{-1} A_n| = 2n.$$

Define $A_n^{(i)} = \{x_i, y_i^{-1}, y_i^{-1}x_i^{-1}y_i^{-1}, x_i z_i, y_i^{-1} z_i\}$ for $1 \leq i \leq n$. We have

$$A_n A_n^{-1} = \bigsqcup_{i=1}^n \bigsqcup_{j=1}^n A_n^{(i)} \left(A_n^{(j)}\right)^{-1},$$

$$A_n^{-1} A_n = \bigsqcup_{i=1}^n \bigsqcup_{j=1}^n \left(A_n^{(i)}\right)^{-1} A_n^{(j)}.$$

This implies²

$$|A_n A_n^{-1}| = \sum_{i=1}^n \sum_{j=1}^n \left|A_n^{(i)} \left(A_n^{(j)}\right)^{-1}\right|$$

$$= \sum_{i=1}^n \left|A_n^{(i)} \left(A_n^{(i)}\right)^{-1}\right| + \sum_{i=1}^n \sum_{\substack{j=1 \\ j \neq i}}^n \left|A_n^{(i)} \left(A_n^{(j)}\right)^{-1}\right|$$

$$= n \cdot |AA^{-1}| + n \cdot (n - 1) \cdot |A|^2,$$

²For $i \neq j$, the sets $A_n^{(i)}$ and $A_n^{(j)}$ are supported on disjoint sets of generators in F_{3k} , meaning any product of the form ab^{-1} or $a^{-1}b$ where $a \in A_n^{(i)}$ and $b \in A_n^{(j)}$ produces a word involving letters from distinct alphabets. Thus, all such products are distinct. However, if $i = j$, the words produced come from the same alphabet, which does not generate distinct products.

and

$$\begin{aligned} |A_n^{-1}A_n| &= \sum_{i=1}^n \sum_{j=1}^n \left| \left(A_n^{(i)} \right)^{-1} A_n^{(j)} \right| \\ &= \sum_{i=1}^n \left| \left(A_n^{(i)} \right)^{-1} A_n^{(i)} \right| + \sum_{i=1}^n \sum_{\substack{j=1 \\ j \neq i}}^n \left| \left(A_n^{(i)} \right)^{-1} A_n^{(j)} \right| \\ &= n \cdot |A^{-1}A| + n \cdot (n - 1) \cdot |A|^2. \end{aligned}$$

Therefore,

$$|A_n A_n^{-1}| - |A_n^{-1} A_n| = n \cdot (|AA^{-1}| - |A^{-1}A|) = 2n. \quad \square$$

Theorem 1.3 and Theorem 1.5 establish that every even integer arises in the difference between the left and right quotient set. Naturally, we may now ask how large such differences can be in terms of the cardinality of A . Define

$$M_n := \sup_{\substack{A \subseteq F_2 \\ |A|=n}} \left| |AA^{-1}| - |A^{-1}A| \right|.$$

Proposition 2.6. *We have $M_n = \Theta(n^2)$.*

Proof. We establish both an upper and lower bound. For the lower bound, observe that for any finite subset $A \subseteq F_2$ with $|A| = n$ it follows that $|AA^{-1}| \leq n^2$ and $|A^{-1}A| \leq n^2$. This implies $\left| |AA^{-1}| - |A^{-1}A| \right| \leq n^2$ thus $M_n \leq n^2$ so $M_n = O(n^2)$. For the lower bound, let

$$\begin{aligned} A_k &:= \{x^i : 1 \leq i \leq k\}, \\ B_k &:= \{x^i y : 1 \leq i \leq k\}, \\ C_k &:= A_k \cup B_k. \end{aligned}$$

Note that $|C_k| = 2k$ and thus let $n = 2k$. Next, we compute the size of the right quotient set:

$$\begin{aligned} C_k C_{k-1}^{-1} &= (A_k \cup B_k)(B_k^{-1} \cup A_k^{-1}) \\ &= (A_k B_k^{-1}) \cup (B_k B_k^{-1}) \cup (A_k A_k^{-1}) \cup (B_k A_k^{-1}). \end{aligned}$$

As $A_k A_k^{-1} = \{x^{i-j}\} = B_k B_k^{-1}$, this accounts for $2k - 1$ elements. As $A_k B_k^{-1} = \{x^i y^{-1} x^{-j}\}$, this adds k^2 elements, and lastly for $B_k A_k^{-1} = \{x^i y x^{-j}\}$, there are also k^2 elements. Thus,

$$|C_k C_k^{-1}| = 2k^2 + 2k - 1.$$

For the left quotient set, we obtain

$$\begin{aligned} C_k^{-1}C_k &= (B_k^{-1} \cup A_k^{-1})(A_k \cup B_k) \\ &= (B_k^{-1}A_k) \cup (B_k^{-1}B_k) \cup (A_k^{-1}A_k) \cup (A_k^{-1}B_k). \end{aligned}$$

As each of these four terms contribute $2k - 1$ elements,

$$|C_k^{-1}C_k| = 4(2k - 1) = 8k - 4.$$

Then, taking the difference between the left and right quotient set yields

$$\begin{aligned} ||C_k C_k^{-1}| - |C_k^{-1}C_k|| &= (2k^2 + 2k - 1) - (8k - 4) \\ &= 2k^2 - 6k + 1. \end{aligned}$$

Substituting $k = n/2$ gives $M_n \geq \frac{1}{2}n^2 - 3n + 1 = \Omega(n^2)$. Thus, $M_n = \Theta(n^2)$. \square

Remark 2.7. *The following remark is mentioned in [15, Remark 4.4.]. If $H \subseteq G$ is a finite subgroup of some group G and g is an element of G not in the normalizer of H , then the set $A := Hg \cup H$ has $A^{-1}A$ about the same size as H , but AA^{-1} can be possibly large. If we slightly modify this construction, letting H be a subset of G , then the proof of Proposition 2.6 is the case $H = \{x, x^2, \dots, x^k\}$ and $g = y$. Indeed, $|A^{-1}A| = O(|H|)$, but $|AA^{-1}| = O(|H|^2)$.*

2.3. Cardinality of A

The set A given in (2.1) is extremal in the sense that it is the smallest such set such that $|AA^{-1}| - |A^{-1}A|$ in F_2 . In fact, this holds for all groups with no elements of order 2, which we prove in Theorem 1.6.

Lemma 2.8. *Let G be a group with $A \subset G$ and $|A| = n$. Then D_A contains no connected component with more than n elements.*

Proof. Suppose, for contradiction, C was a connected component with more than n elements. By the pigeonhole principle, two vertices in C have the same first coordinate. Since C is a clique by Lemma 2.1 (4), this contradicts Lemma 2.1 (2b). \square

Lemma 2.9. *Let G be a group with $A \subseteq G$ and $|A| = 4$. If G does not have an element of order 2, then the number of connected components in D_A is equal to the number of connected components in $D_{A^{-1}}$.*

Proof. Suppose D_A contains a K_4 clique. Then, up to relabeling and transposition, this clique has the form $(1, 2)(2, 3)(3, 4)(4, 1)$. Indeed, given a K_4 of the form $(1, j_1)(2, j_2)(3, j_3)(4, j_4)$, we may assume $j_1 = 2$ and $j_2 = 3$ up to relabeling. This forces $j_4 = 1$ and $j_3 = 4$. This clique is impossible if G has no elements of order

2 since $a_1a_3^{-1} = (a_1a_2^{-1})(a_2a_3^{-1}) = (a_3a_4^{-1})(a_4a_1^{-1}) = a_3a_1^{-1}$ and this contradicts Lemma 2.1 (2c) given the assumption that G has no elements of order 2.

It remains to consider the case where the largest clique is a K_3 , which we call a triangle. Consider a triangle $\Delta = (\alpha_1, \beta_1)(\alpha_2, \beta_2)(\alpha_3, \beta_3)$. By Lemma 2.1 (2b), we know that the same number can appear at most twice in the coordinates $\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3$, and β_3 . Moreover the same number appears at most once for an α_i and at most once for a β_j , where $1 \leq i, j \leq 3$. Therefore, there are two cases to consider.

Case 1: There are 4 distinct elements in Δ . Because of the condition that there is no element of order 2 in G , there cannot be an edge between (i, j) and (j, i) . Therefore, up to relabeling, $\Delta = (1, 2)(2, 3)(3, 4)$. By elementary group operations, the edge $[(1, 3), (2, 4)]$ and its transpose are also in D_A . Hence, D_A and $D_{A^{-1}}$ look as in Figure 2. Therefore, in this case, the number of connected components stays the same.

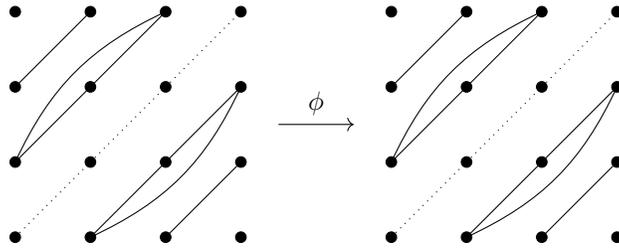


Figure 2: Up to relabeling, $\Delta = (1, 2)(2, 3)(3, 4)$ induces D_A and $D_{A^{-1}}$ above.

Additionally there may be a triangle $\Delta' = (3, 1)(4, 2)(1, 4)$ and its reflection under T . However, we can check that the image of this graph under ϕ is itself as in Figure 3 below.

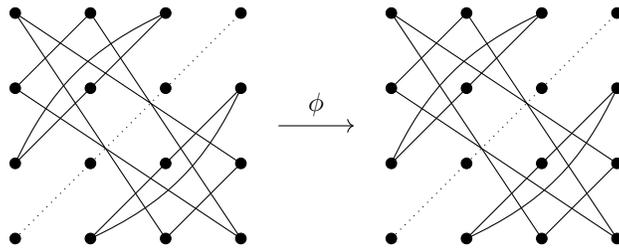


Figure 3: Up to relabeling, $\Delta' = (3, 1)(4, 2)(1, 4)$ induces D_A and $D_{A^{-1}}$ above.

Case 2: There are 3 distinct elements in Δ . The only possibility in this case is that up to relabelling, $\Delta = (1, 2)(2, 3)(3, 1)$. Notice that this triangle cannot be

part of a K_4 because $(4, 4)$ is not in the same connected component as Δ and every other coordinates will cause contradiction to Lemma 2.1 (2b). Then, D_A and $D_{A^{-1}}$ are as in Figure 4 below.

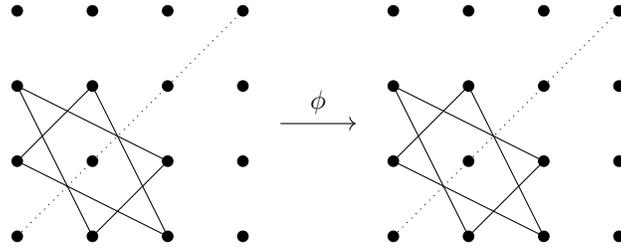


Figure 4: Up to relabeling, $\Delta = (1, 2)(2, 3)(3, 1)$ induces D_A and $D_{A^{-1}}$ above.

In the second case, we see it is impossible to place a second triangle without two vertices being on the same axis, violating Lemma 2.1 (2b). \square

Proof of Theorem 1.6. If $|AA^{-1}| \neq |A^{-1}A|$, then the number of connected components in D_A is different from $D_{A^{-1}}$. We claim at least one of D_A and $D_{A^{-1}}$ contains a clique of size 3 or greater off the main diagonal (a non-diagonal clique). Indeed, since ϕ is a bijection between the non-diagonal and self-loop edges, the number of connected components in D_A would be the same as $D_{A^{-1}}$ if there were no non-diagonal connected components of size 3 or greater.

Assume D_A has a non-diagonal clique of size 3 or greater. This is impossible if $|A| \in \{1, 2\}$ by Lemma 2.8. If $|A| = 3$, then the only possible triangles are $(1, 2)(3, 1)(2, 3)$ and $(2, 1)(1, 3)(3, 2)$. Since any D_A is invariant under transposition by T , if D_A has a triangle, then it has both. Any other edge would either (1) connect the triangles to the diagonal, which is forbidden, or (2) connect the triangle to each other, which creates a component with more 3 vertices, contradicting Lemma 2.8. Thus, with $|A| = 3$, D_A and $D_{A^{-1}}$ must have the same component counts. So, we have shown for any group G if $|A| \leq 3$ then $|AA^{-1}| = |A^{-1}A|$.

Notice how the above proof does not use Lemma 2.1 (2c), so it holds for any group, yielding the first part of the theorem.

Next, suppose that G has no elements of order 2. If $|A| = 4$, then Lemma 2.9 shows that ϕ preserves the number of connected components. Hence, we have shown if G is a group with no elements of order 2 and $|A| \leq 4$, then $|AA^{-1}| = |A^{-1}A|$. \square

Example 2.10. *If G has elements of order 2, then we may no longer use Lemma 2.1 (2c) in the previous statements. Indeed, we check with Sage [16] that the set*

$$A = \{(15)(26)(37)(48), (1256)(3874), (17)(35)(48), (18765432)\} \subseteq S_8,$$

which can be viewed as a subset of the quasidihedral group of order 16, has $|AA^{-1}| = 10$, but $|A^{-1}A| = 7$. This simultaneously shows we can have an odd difference in the left and right quotient sets and also that $|A| = 4$ can achieve a nonzero difference.

§3 Future Work

In a finite subset S of a group G , one may ask how many finite subsets $A \subseteq S$ have the left quotient set larger than the right quotient set. If S is symmetric (i.e., $w \in S$ if and only if $w^{-1} \in S$), this is equal to the number of finite subsets with right quotient set larger than left quotient set. Indeed, if $|A^{-1}A| > |AA^{-1}|$, then we can replace A with $B := A^{-1}$ to get $|B^{-1}B| < |BB^{-1}|$, and vice-versa. In particular, this implies that the quantity

$$\mathbb{E}[|A^{-1}A| - |AA^{-1}|] = 0,$$

where $A \subseteq S$ is chosen by including elements at random with probability $1/2$.

On the other hand, the second moment (i.e., the variance)

$$\text{Var}(|A^{-1}A| - |AA^{-1}|) = \mathbb{E}[(|A^{-1}A| - |AA^{-1}|)^2]$$

is nonzero for groups where $|AA^{-1}| \neq |A^{-1}A|$ for some finite subset $A \subseteq S$. If A is a subgroup then trivially one has the two cardinalities are the same, as in that case $A = A^{-1}$. Having to avoid such special cases is common; for example, there is non-Benford behavior if the support of certain random variables live in a coset of a group (see [10], in particular the discussion related to a result of Levy [7]).

We can cast this problem specifically to the free group.

Question 3.1. *Let $B_N \subseteq F_2$ be the set of words of length $\leq N$. With respect to the uniform probability measure on the subsets of B_N , what is $\text{Var}(|A^{-1}A| - |AA^{-1}|)$?*

A technique for studying the moments of $|AA^{-1}|$ and related quantities is the graph theoretic framework in [8]. This paper suggests that to study $\mathbb{P}(w_1, \dots, w_k \notin AA^{-1})$, we should look at the graph with vertex set S and edge relation $u \sim v$ if $uv^{-1} = w_m$ or $vu^{-1} = w_m$ for some $m = 1, \dots, k$. It would be interesting to find a structure which encapsulates both the the above graphs and the graphs D_A and $D_{A^{-1}}$ which we introduced.

There are still other unanswered questions about the values $|AA^{-1}| - |A^{-1}A|$ can take in various groups.

Question 3.2 (Answered in [12] and [5]). *What are the necessary and sufficient conditions on a group G so that there exists a finite subset $A \subseteq G$ such that $|A^{-1}A| \neq |AA^{-1}|$?*

Of course, G being non-abelian is a necessary condition for $|A^{-1}A| \neq |AA^{-1}|$. However, one can check that $|AA^{-1}| = |A^{-1}A|$ for all subsets A of the symmetric group S_3 . Hence, being non-abelian is not a sufficient condition. It is possible that $|AA^{-1}| = |A^{-1}A|$ is true for all $A \subseteq S_3$ only because S_3 is sufficiently small³

Question 3.3 (Answered in [12] and [5]). *Is there an infinite family of finite, non-isomorphic, non-abelian groups $\{G_i\}$ for which $|A^{-1}A| = |AA^{-1}|$ for all subsets A of G_i ?*

Remark 3.4. *Following the initial draft of this paper, the sixth author answered Questions 3.2 and 3.3 in the preprint [12]. Shortly following this preprint, the authors of the present paper were directed to [5] which answered the questions previously and independently. Both answer the question by providing a classification of groups G for which $|AA^{-1}| = |A^{-1}A|$ for all $A \subseteq G$. Question 3.3. is answered affirmatively with the Hamiltonian 2-groups $Q_8 \times (C_2)^n$ being the unique infinite family of groups where $|AA^{-1}| = |A^{-1}A|$ holds for all subsets. This classification appears as [5, Theorem 7.4.] for all finite and infinite groups and as [12, Theorem 1.1.] where the classification is only for finite groups. We are grateful to Liubomir Chiriac for pointing us to [5] after reading a previous draft of this paper.*

An alternative way to characterize groups where $|AA^{-1}| \neq |A^{-1}A|$ is possible would be to find a finite collection of difference graphs which serve as minimal counterexamples to the statement $|AA^{-1}| = |A^{-1}A|$ for all $A \subseteq G$. We conjecture that such a collection exists. That is to say, there should be a finite collection of graphs $\{H_1, \dots, H_k\}$ such that, if $|AA^{-1}| \neq |A^{-1}A|$ for some $A \subseteq G$, then there is some $B \subseteq G$ such that $D_B \cong H_i$ for some $i = 1, \dots, k$. A counterexample to our conjecture would be an infinite sequence of groups G_ℓ such that for any $N > 0$, there is some group G_m in the collection for which $|AA^{-1}| = |A^{-1}A|$ for all sets A of size $< N$, but $|AA^{-1}| \neq |A^{-1}A|$ for some A of size $\geq N$.

³As $|S_n| = n!$, the number of subsets is $2^{n!}$, which grows very rapidly; $2^{3!} = 64$, $2^{4!}$ is approximately $1.7 \cdot 10^7$, while $2^{5!}$ exceeds 10^{36} ; straightforward sampling cannot hope but to explore a very small percentage of possible A 's.

Acknowledgements.

The authors gratefully acknowledge the referee's careful reading of the manuscript and their constructive comments. The authors also thank Carl Pomerance and Mel Nathanson for stimulating discussions; the genesis of this work came from conversations the fifth-named author had with them at the Integers Conference in Georgia in 2025. This project took place at the SMALL REU program at Williams College and was funded by the Finnerty Fund from Williams College and the National Science Foundation (Grant DMS2241623). The authors are grateful for the support of Amherst College, Princeton University, the University of Michigan, the University of Wisconsin, and Williams College.

References

- [1] R. Ascoli, J. Cheigh, G. Z. Dantas e Moura, R. Jeong, A. Keisling, A. Lilly, S. J. Miller, P. Ngamlamai, and M. Phang, Sum and difference sets in generalized dihedral groups, preprint, [arXiv:2210.00669](https://arxiv.org/abs/2210.00669).
- [2] H. V. Chu, N. Luntzlara, S. J. Miller, and L. Shao, Infinite families of partitions into MSTD subsets, *Integers*, **19** (2019), #A60, 20 pp.
- [3] H. V. Chu, N. Luntzlara, S. J. Miller, and L. Shao, Generalizations of a curious family of MSTD sets hidden by interior blocks, *Integers* **20A** (2020), #A5, 19 pp.
- [4] P. V. Hegarty, Some explicit constructions of sets with more sums than differences, *Acta Arith.* **130** (1) (2007), 61–77.
- [5] M. Herzog, G. Kaplan, P. Longobardi, and M. Maj, Products of subsets of groups by their inverses, *Beitr. Algebra Geom.* **55** (2) (2014), 311–346.
- [6] E. Kim and S. J. Miller, Constructions of generalized MSTD sets in higher dimensions, *J. Number Theory* **235** (2022), 358–381.
- [7] P. Lévy, L'addition des variables aléatoires définies sur une circonférence, *Bull. Soc. Math. France* **67** (1939), 1–41.
- [8] O. Lazarev, S. J. Miller, and K. O'Bryant, Distribution of missing sums in sumsets, *Exp. Math.* **22** (2) (2013), 132–156.
- [9] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, Berlin, 2001.
- [10] S. J. Miller and M. Nigrini, The modulo 1 central limit theorem and Benford's law for products, *Int. J. Algebra* **2** (1–4) (2008), 119–130.
- [11] G. Martin and K. O'Bryant, Many sets have more sums than differences, in *Additive Combinatorics*, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007, 287–305.
- [12] H. Mouli and P. Saldin, Classification of finite groups with equal left and right quotient sets, preprint, [arXiv:2509.04717](https://arxiv.org/abs/2509.04717).
- [13] S. J. Miller and K. Vissuet, Most subsets are balanced in finite groups, in *Combinatorial and Additive Number Theory—CANT 2011 and 2012*, Springer Proc. Math. Stat., 101, Springer, New York, NY, 2014, 147–157.

- [14] M. B. Nathanson, Sets with more sums than differences, *Integers* **7** (2007), #A5, 24 pp.
- [15] T. Tao, Product set estimates for non-commutative groups, *Combinatorica* **28** (5) (2008), 547–594.
- [16] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.6)*, 2025. <https://www.sagemath.org>.
- [17] Y. Zhao, Counting MSTD sets in finite abelian groups, *J. Number Theory* **130** (10) (2010), 2308–2322.
- [18] Y. Zhao, Sets characterized by missing sums and differences, *J. Number Theory* **131** (11) (2011), 2107–2134