Left and Right Quotient Sets in Non-Abelian Groups

Xiaoyao Haung (xyrushac@umich.edu)
Pramana Saldin (saldin@wisc.edu)
Arman Rysmakhanov (ar21@williams.edu)

Joint work with June Duvivier, Ava Kennon, Say-Yeon Kwon, Ren Watson
Advised by Steven J. Miller (sjm1@williams.edu)

SMALL REU 2025
Yale, July 23, 2025

Background

Definitions

The famous More-Sums-Than-Differences (MSTD) problem asks if $|A + A| > |A - A|$ for $A \subseteq \mathbb{Z}$, where $A + A$ denotes the set of all distinct sums and $A - A$ is the set of all distinct differences formed by the elements of A.

Definitions

The famous More-Sums-Than-Differences (MSTD) problem asks if $|A+A| > |A-A|$ for $A \subseteq \mathbb{Z}$, where $A+A$ denotes the set of all distinct sums and $A-A$ is the set of all distinct differences formed by the elements of A.

In 2006, Martin and O'Bryant proved that a positive percentage of sets are sum-dominant. [MO06]

Related problem

What if A is non-commutative?
$AA^{-1} \neq A^{-1}A$.

Definitions

Definition

Right Quotient Set:

- $AA^{-1} := \{a_i \cdot a_j^{-1} : a_i, a_j \in A\}$

Left Quotient Set:

- $A^{-1}A := \{a_i^{-1} \cdot a_j : a_i, a_j \in A\}$

Free groups

Definition

Let $A = \{x, y\}$ be generators. $F(A) = F_2$ is the group of **words** on $\{x, y, x^{-1}, y^{-1}\}$.

Free groups

Definition

Let $A = \{x, y\}$ be generators. $F(A) = F_2$ is the group of **words** on $\{x, y, x^{-1}, y^{-1}\}$.

Example

For example,

$$x * x^2 = x^3$$

Free groups

Definition

Let $A = \{x, y\}$ be generators. $F(A) = F_2$ is the group of **words** on $\{x, y, x^{-1}, y^{-1}\}$.

Example

For example,

$$x * x^2 = x^3$$
$$x * x^{-1} = e$$

Free groups

Definition

Let $A = \{x, y\}$ be generators. $F(A) = F_2$ is the group of **words** on $\{x, y, x^{-1}, y^{-1}\}$.

Example

For example,

$$x * x^2 = x^3$$
$$x * x^{-1} = e$$
$$x * y = xy.$$

Graph of F_2

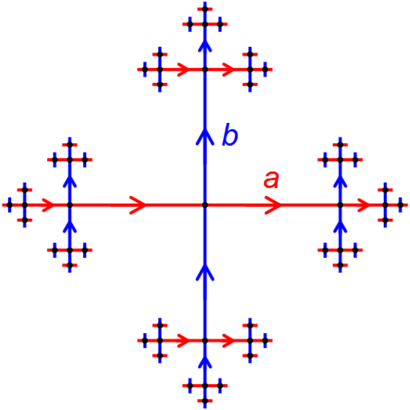


Figure: Visualization of group multiplication in F_2

Example (Quotient set example)

Example

	x	y
y^{-1}		
x^{-1}		

Table: “Multiplication table” of $A = \{x, y\}$ with $A^{-1} = \{x^{-1}, y^{-1}\}$

Definitions

Definition

A set $A \subseteq G$ is either

- **More Right Then Left (MRTL)**: $|AA^{-1}| > |A^{-1}A|$.
- **Balanced**: $|AA^{-1}| = |A^{-1}A|$.
- **More Left Then Right (MLTR)**: $|A^{-1}A| > |AA^{-1}|$.

Motivation

Question: What are the possible values of $|AA^{-1}| - |A^{-1}A|$ for finite subsets $A \subseteq G$?

Example

If G is abelian, then $AA^{-1} = A^{-1}A$. Thus, the only possible value of $|AA^{-1}| - |A^{-1}A|$ is 0.

History

Tao remarks

> *there is no relation between the size of AA^{-1} and $A^{-1}A$ in general. For instance, if H is a multiplicative set which is also a subgroup of G, and $A := (x \cdot H) \cup H$ for some x not in the normaliser of H, then AA^{-1} has about the same size as H, but $A^{-1}A$ can be much larger. [Tao11]*

The Difference Graph

Motivating example

	x	y
y^{-1}	xy^{-1}	e
x^{-1}	e	yx^{-1}

$$\xrightarrow{\text{graph structure}}$$

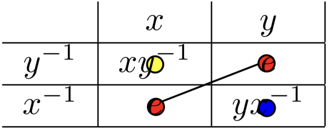


Figure: Associated to the "multiplication table" of $\{x, y\}$ is a graph.

Definition

Definition

Given a finite subset $A \subseteq G$ with $|A| = n$, the **difference graph** $D_A = (V, E)$ is defined as follows.

- Vertex set is $V := [n] \times [n]$
- Edge set is $E(D_A) := [(i, j), (k, \ell)] \iff a_i a_j^{-1} = a_k a_\ell^{-1}$

Definition

Definition

Given a finite subset $A \subseteq G$ with $|A| = n$, the **difference graph** $D_A = (V, E)$ is defined as follows.

- Vertex set is $V := [n] \times [n]$
- Edge set is $E(D_A) := [(i, j), (k, \ell)] \iff a_i a_j^{-1} = a_k a_\ell^{-1}$

Definition

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.

Definition

Definition

Given a finite subset $A \subseteq G$ with $|A| = n$, the **difference graph** $D_A = (V, E)$ is defined as follows.

- Vertex set is $V := [n] \times [n]$
- Edge set is $E(D_A) := [(i,j),(k,\ell)] \iff a_i a_j^{-1} = a_k a_\ell^{-1}$

Definition

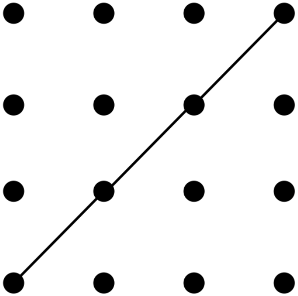
Let $\mathcal{C}(D_A)$ be the set of connected components of D_A and $c(D_A) = |\mathcal{C}(D_A)|$ be the number of connected components.

Note that $c(D_A) = |AA^{-1}|$.

Properties of D_A

$$\begin{array}{c|cccc}
 & a_1 & a_2 & a_3 & a_4 \\
a_4^{-1} & \bullet & \bullet & \bullet & \bullet \\
a_3^{-1} & \bullet & \bullet & \bullet & \bullet \\
a_2^{-1} & \bullet & \bullet & \bullet & \bullet \\
a_1^{-1} & \bullet & \bullet & \bullet & \bullet
\end{array}$$

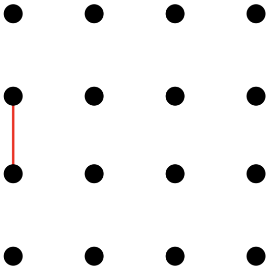
Properties of D_A



$$\longleftrightarrow \quad a_1 a_1^{-1} = a_2 a_2^{-1} = e$$

Figure: Diagonal edges are always present.

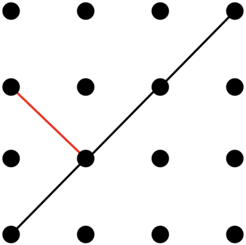
Properties of D_A



$$\longleftrightarrow a_1 a_2^{-1} = a_1 a_3^{-1} \implies a_2 = a_3$$

Figure: Any edge parallel to the x or y axis is not present.

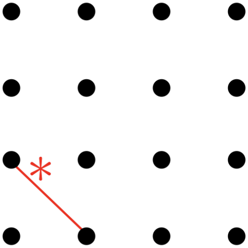
Properties of D_A



$$\longleftrightarrow \quad a_1 a_3^{-1} = a_2 a_2^{-1} = e \implies a_1 = a_3$$

Figure: No vertex connects to the diagonal.

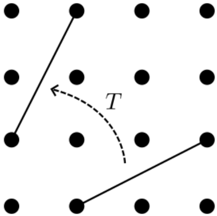
Properties of D_A



$$\longleftrightarrow \quad a_1 a_2^{-1} = a_2 a_1^{-1} \implies (a_1 a_2^{-1})^2 = e$$

Figure: **If** G **has no elements of order** 2, no vertex connects to its "transpose"

Properties of D_A



$$\longleftrightarrow \quad \begin{aligned} & a_2a_1^{-1} = a_4a_2^{-1} \\ & \implies a_1a_2^{-1} = (a_2a_1^{-1})^{-1} = (a_4a_2^{-1})^{-1} = a_2a_4^{-1} \end{aligned}$$

Figure: If any edge is present, its “transpose” is also present.

Properties of D_A

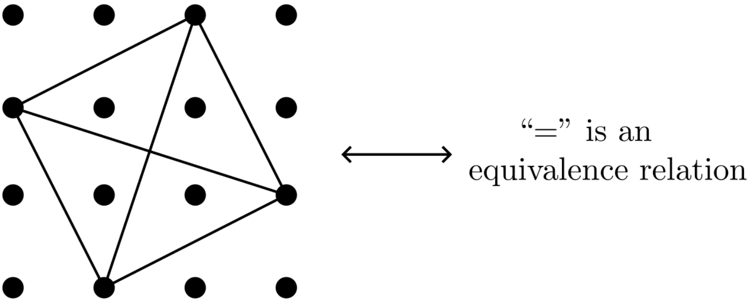


Figure: Connected components form a clique.

Summary of properties

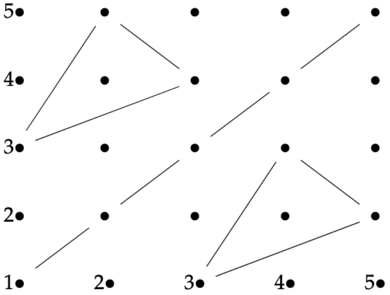
Lemma

Let $i, j, k, \ell \in [n]$.

1. *The following edges are forbidden in* $E(D_A)$*:*
    1. $[(i,j),(k,k)]$*: an edge connecting to the diagonal, provided that* $i \neq j$*.*
    2. $[(i,j),(i,k)]$ *(or* $[(j,i),(k,i)]$*, but this is the handled by (1)): an edge connecting vertices on the same axis.*
    3. ***If*** G ***has no elements of order*** 2*,* $[(i,j),(j,i)]$*: an edge connecting to its symmetric pair, provided that* $j \neq i$*.*
2. $[(i,i),(j,j)] \in E(D_A)$.
3. $[(i,j),(k,\ell)] \in E(D_A) \iff [(j,i),(\ell,k)] \in E(D_A)$.
4. *If* C *is a connected component in* D_A*, then* C *is a clique.*

Example

For $n = 5$, $A = \{x^2, (xy)^{-1}, (xy)^{-1}x(xy)^{-1}, x(xy^{-1}), (xy)^{-1}(xy^{-1})\} \subseteq F_2$ has the following difference graph:



Bijection of Edges

Using the fact:

$$a_i a_j^{-1} = a_k a_\ell^{-1} \iff a_k^{-1} a_i = a_\ell^{-1} a_j$$

We can obtain a **bijection of edges**

$$\phi\colon E(D_A) \to E(D_{A^{-1}})$$
$$[(i,j),(k,\ell)] \mapsto [(k,i),(\ell,j)].$$

Bijection of Edges

Using the fact:

$$a_i a_j^{-1} = a_k a_\ell^{-1} \iff a_k^{-1} a_i = a_\ell^{-1} a_j$$

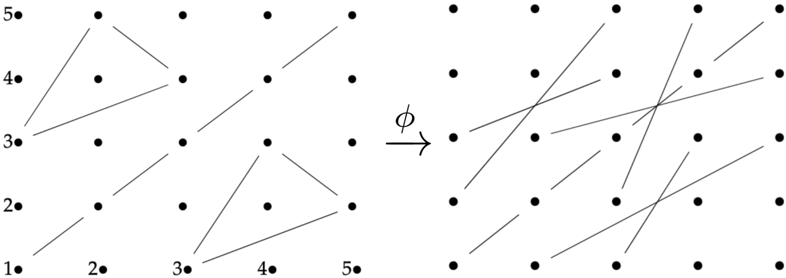
We can obtain a **bijection of edges**

$$\phi \colon E(D_A) \to E(D_{A^{-1}})$$
$$[(i,j),(k,\ell)] \mapsto [(k,i),(\ell,j)].$$

Remark

*Tao uses this to prove the **additive energies** $\Lambda(A, A^{-1})$ and $\Lambda(A^{-1}, A)$ are equal.*

Bijection of Edges Example



17 components 15 components

Figure: ϕ reduces the number of connected components

Nonzero Cardinality Difference

Nonzero Cardinality Difference

Theorem (SMALL 2025)

Let G be a group. Let $A \subseteq G$ be a finite subset. If $|AA^{-1}| \neq |A^{-1}A|$, then $|A| \geq 4$.

- Casework: $|A| = 1, 2, 3$.

No Elements of Order 2

Definition

Recall that a group G is said to have **no elements of order 2** if for every element $g \in G$ with $g \neq e$ we have $g^2 \neq e$.

An example is $\mathbb{Z}/3\mathbb{Z}$.

No Elements of Order 2

Theorem

Let G be a group with no elements of order 2. Let $A \subseteq G$ be a finite subset. Then $|AA^{-1}| - |A^{-1}A|$ is even.

No Elements of Order 2

Theorem

Let G be a group with no elements of order 2. Let $A \subseteq G$ be a finite subset. Then $|AA^{-1}| - |A^{-1}A|$ is even.

Proof sketch.

We prove a stronger result: $|AA^{-1}|$ is always odd.
A connected component is either (1) symmetric under transposition, or (2) is disjoint from its transpose. Only one component is in the first class: the diagonal. All other components come in pairs.

$$\underbrace{\text{odd}}_{(1)} + \underbrace{\text{even}}_{(2)} = \text{odd}. \qquad \square$$

No Elements of Order 2

Theorem

Let G be a group with no elements of order 2. Let $A \subseteq G$ be a finite subset. If $|AA^{-1}| \neq |A^{-1}A|$, then $|A| \geq \blacksquare$.

Guesses?

Hint: Without restriction, $|A| \geq 4$ (previous theorem).

No Elements of Order 2

Theorem

Let G be a group with no elements of order 2. Let $A \subseteq G$ be a finite subset. If $|AA^{-1}| \neq |A^{-1}A|$, then $|A| \geq 5$.

Lemma

Let $|A| = n$. Then D_A has no connected component (other then the diagonal) with more than n elements.

- By Contradiction.

Continuation

Lemma

Suppose $|A| = 4$. If group G does not have an element of order 2 and its largest possible cycle is K_4, then the number of connected components in D_A is equal to the number of connected components in $D_{A^{-1}}$.

- The difference graph is heavily used to this lemma.
- We do casework on triangles.
- ϕ leaves the number of connected components unchanged.

The Free Group on 2 Generators

The Free Group on 2 Generators

Theorem

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 Free Group on 2 Generators

Theorem

For all $n \in \mathbb{Z}$, there exists a set $A_n \subseteq F_2$ such that $|A_nA_n^{-1}| - |A_n^{-1}A_n| = 2n$.

The following set in F_3 with $n = 1$:

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

has

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

The Free Group on 2 Generators

Theorem

For all $n \in \mathbb{Z}$, there exists a set $A_n \subseteq F_2$ such that $|A_nA_n^{-1}| - |A_n^{-1}A_n| = 2n$.

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

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

We prove

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

The Infinite Dihedral Group

Definition

Definition

The **Infinite Dihedral group**, denoted D_∞ is defined as followed: $D_\infty := \langle r, s | s^2 = e, srs = r^{-1} \rangle$

- r: a generator representing translation
- s: a generator representing reflection

Key Properties:

- Non-abelian: $rs \neq sr$
- Has elements of order 2

The Infinite Dihedral Group

Theorem

For every $n \in \mathbb{Z}$, there exists a subset $A_n \subseteq D_\infty$ such that $|A_nA_n^{-1}| - |A_n^{-1}A_n| = n$

The Infinite Dihedral Group

Theorem

For every $n \in \mathbb{Z}$, there exists a subset $A_n \subseteq D_\infty$ such that $|A_n A_n^{-1}| - |A_n^{-1} A_n| = n$

Proof sketch.

D_∞ has two copies of $\mathbb{Z}$: $\langle r \rangle$ and $s\langle r \rangle$.

The Infinite Dihedral Group

Theorem

For every $n \in \mathbb{Z}$, there exists a subset $A_n \subseteq D_\infty$ such that $|A_n A_n^{-1}| - |A_n^{-1} A_n| = n$

Proof sketch.

D_∞ has two copies of $\mathbb{Z}$: $\langle r \rangle$ and $s\langle r \rangle$. Let $B \subseteq \mathbb{Z}$ be finite and let $A = \{r^b, sr^b : b \in B\}$. Then

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

A result of Martin and O'Bryant says this ranges over all $n \in \mathbb{Z}$. [MO06]. $\square$

Summary of Results

Results

Theorem (SMALL 2025)

Let G be a group. Let $A \subseteq G$ be a finite subset. If $|AA^{-1}| \neq |A^{-1}A|$, then $|A| \geq 4$.

Results

Theorem (SMALL 2025)

Let G be a group. Let $A \subseteq G$ be a finite subset. If $|AA^{-1}| \neq |A^{-1}A|$, then $|A| \geq 4$.

This is sharp: the quasidihedral group of order 16 has a subset of size 4 satisfying the above theorem.

Results

Theorem (SMALL 2025)

Let G be a group with no elements of order 2. Let $A \subseteq G$ be a finite subset. If $|AA^{-1}| \neq |A^{-1}A|$, then $|A| \geq 5$.

Results on possible values

Question: possible values of $|AA^{-1}| - |A^{-1}A|$?

Theorem

Let G be a group with no elements of order 2. Let $A \subseteq G$ be a finite subset. Then $|AA^{-1}| - |A^{-1}A|$ is even.

Acknowledgements

We are grateful to Professor Steven J. Miller for suggesting this problem and for his mentorship.

This research was supported by the National Science Foundation, under NSF Grant DMS2241623, Amherst College, Princeton University, the University of Wisconsin, the University of Michigan, and the Finnerty Fund.

References I

- Greg Martin and Kevin O'Bryant, *Many sets have more sums than differences*, 2006.
- Terence Tao, *Product set estimates for non-commutative groups*, 2011.