Left and Right Differences in Groups

June Duvivier[1], Xiaoyao Huang[2], Ava Kennon[3], Say-yeon Kwon[4], Steven J. Miller[5], Arman Rysmakhanov[5], Pramana Saldin[6], Ren Watson[7]

[1]Reed College, [2]University of Michigan, [3]Amherst College, [4]Princeton University, [5]Williams College, [6]University of Wisconsin, [7]The University of Texas at Austin

The Difference Graph

Let G be a nonabelian group. Let $A = \{a_1, \ldots, a_n\} \subseteq G$ and define $A^{-1} = \{a_1^{-1}, \ldots, a_n^{-1}\}$. We consider the **right** and **left difference sets**:

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

We are interested in the relative sizes of AA^{-1} and $A^{-1}A$. In particular, we looked at the possible values of $|AA^{-1}| - |A^{-1}A|$ for finite subsets $A \subseteq G$. If $|AA^{-1}| > |A^{-1}A|$, we say that A has more right quotients than left quotients or is more rights than lefts (MRTL). Conversely, if $|A^{-1}A| > |AA^{-1}|$, we say A is more lefts than rights (MLTR).

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 $E(D_A) := [(i,j),(k,\ell)] \iff a_i a_j^{-1} = a_k a_\ell^{-1}$

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**

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

Example:

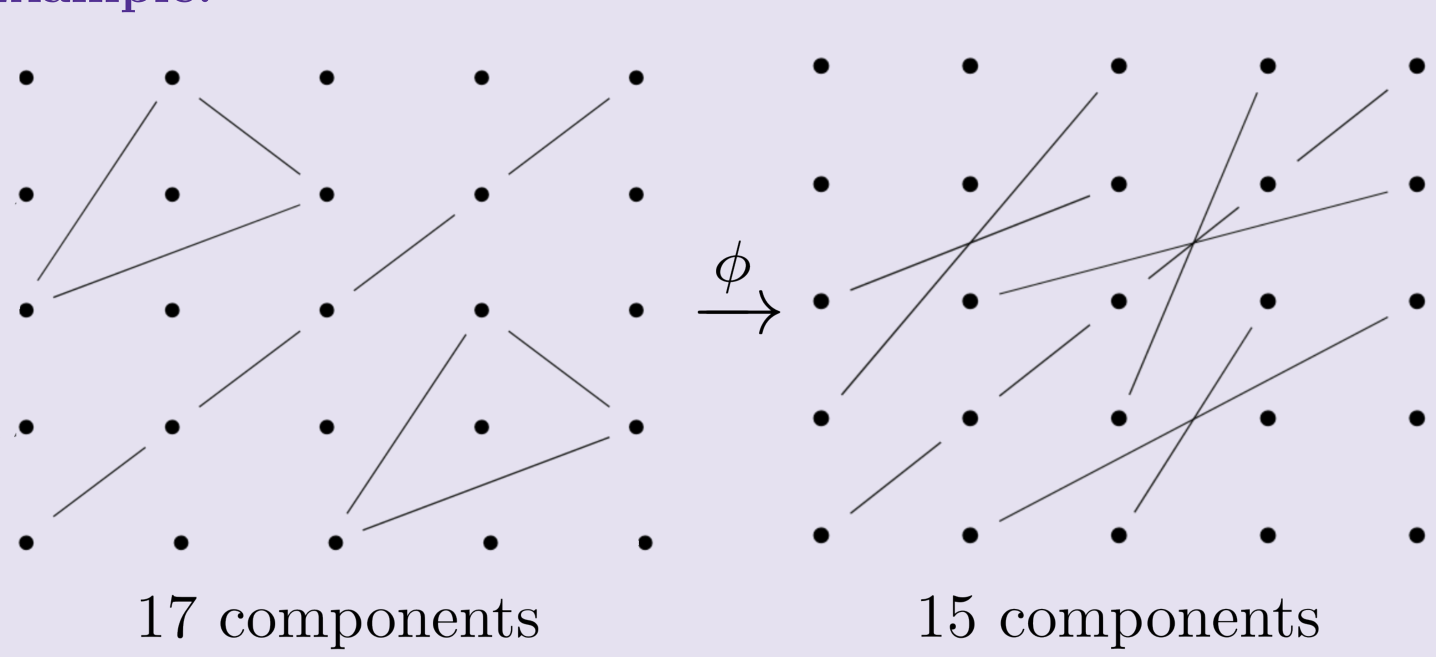


Figure 1: ϕ reduces the number of connected components

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, assuming that T is an automorphism of D_A, we may assume that the graph is undirected.

Cardinality of A

Theorem (Smallest MRTL Set)

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, $|A| \geq 4$
- If we further assume G is a group with no elements of order 2 then $|A| \geq 5$.

This is sharp for both cases: the quasidihedral group of order 16 has an MRTL subset of size 4 while F_2 has an MRTL subset of size 5. In order to prove this theorem two lemmas are needed.

Lemma 1 (DHKKMRSW): Let $|A| = n$. Then D_A has no connected component (other then the diagonal) with more than n elements.

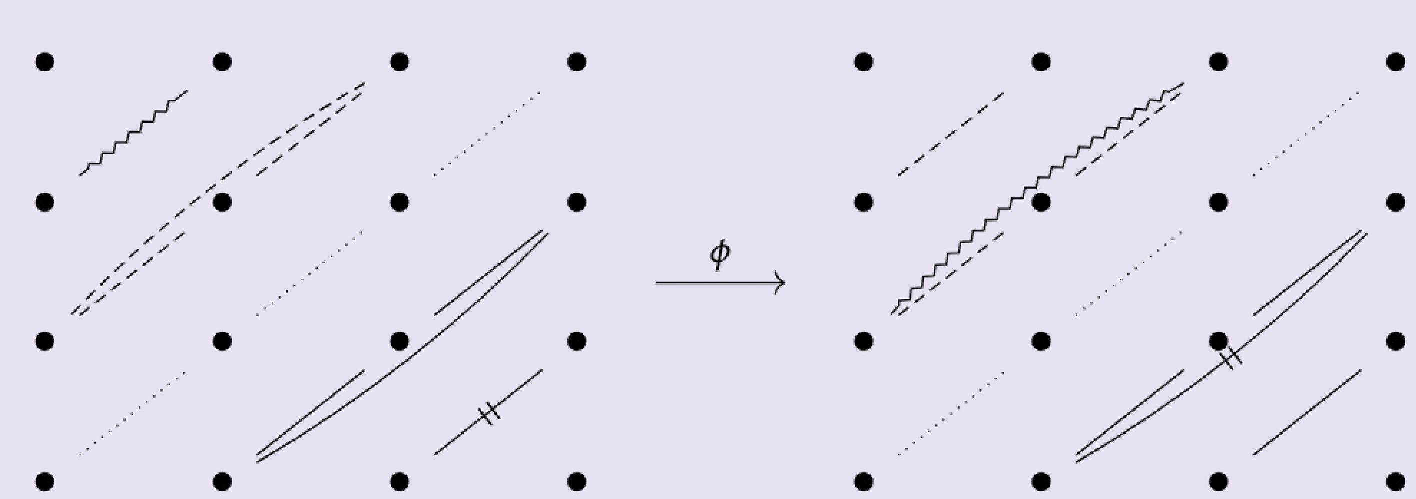
This Lemma is proven by contradiction which relies on the pigeonhole principle.

Lemma 2 (DHKKMRSW): Suppose $|A| = 4$. If group G does not have an element of order 2 and its largest possible cycle is C_4, then the number of connected components in D_A is equal to the number of connected components in $D_{A^{-1}}$.

Making use the 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. $|A| \leq 4$ for when A has no elements of order 2) it is impossible for the number of connected components to change under the bijection of edges. This is done through case work on triangles.

Sketch of Cases:

Case 1: There are 4 distinct elements in $\triangle$.



Case 2: There are 3 distinct elements in $\triangle$.

Possible Differences

Theorem (F_2 achieves all even 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 following set in F_3 with $n = 1$:

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

has

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

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:

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

We can then show

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

Future Directions

Our work suggests a number of natural questions about $|AA^{-1}| - |A^{-1}A|$ and related quantities.

1. What is the variance of $|AA^{-1}| - |A^{-1}A|$ for sets A consisting of words of length $\leq R$? (in various groups with presentations)
2. Can we extend our methods to
$$|A^{-1}AA^{-1}A| - |AA^{-1}AA^{-1}|?$$
and similar differences between sets of higher order?
3. What are the relative orderings of AAA, $A^{-1}AA$, and $AA^{-1}A$ for sets A consisting of words of length $\leq R$? (in various groups with presentations)

References

G. Martin, K. O'Bryant, *Many Sets Have More Sums Than Differences.* Additive combinatorics, 287–305, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.

T. Tao, *Product Set Estimates for Non-Commutative Groups.* Combinatorica (28 (2008), 547-594).

Acknowledgements

We are grateful to Professor Steven J. Miller 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.