Geometric group theory and computation

Collin Jung[1], Yeowoon Jung[1], Jake Regenwetter[1], Zhaohan Sun[1], and Heejoung Kim[2]

[1]*IGL-Frankel Scholars,* [2]*Department of Mathematics, University of Illinois at Urbana-Champaign*

1 Introduction

This is a project in geometric group theory, which is the study of groups by investigating connections between algebraic properties of groups and geometric properties of spaces. A group is a set of elements with an operation which combines any two elements to form another element. In this project, we investigated various examples of finite groups and infinite groups, such as the set of integers, special linear groups, and Braid groups. We then explored their geometrical representations, namely Cayley graphs. We also discussed an algorithmic problem in geometric group theory.

2 Groups

A group can be understood as a set that utilizes a specific binary operation to combine elements in the set to form other elements. A set is a collection of objects called elements, while a binary operation is a tool used to combine two elements.

Definition 1. Let G be a set and let $\cdot : G \times G \to G$ be a binary operation. The set G is a *group* if G satisfies the following four basic axioms:

1. A group G is closed under their operation; that is, any two elements a, b in a given group must produce an element $c = a \cdot b$ also in G.
2. Elements of G follows the associative property.
3. There exists an identity element e in G, which when combined with any other element using the group operation leaves them unchanged; thus $e \cdot a = a$.
4. An element a in a group possesses a unique inverse a^{-1} such that $a \cdot a^{-1} = e$.

2.1 Generating sets

Definition 2. Let G be a group. A subset $S \subset G$ is *a generating set* if all of its elements can be expressed as products of elements in S and their inverses.

Finding the generating set of a group is useful for understanding the structure of the group, as discovering a method to obtain any element in a group proves more helpful than simply knowing a large number of elements in the group.

Example 1. *The set of integers $\mathbb{Z}$ is a group uner addition $+$. For example, the whole set $\mathbb{Z}, \{-1, 1\}$, and $\{2, 3\}$ are generating sets of $(\mathbb{Z}, +)$.*

2.2 Subgroups

Definition 3. Let G be a group and let H be a subset of G. The subset H is a *subgroup* of G if H is a group with the same group operation whose elements are all in G,

Example 2. *$(\mathbb{Z}, +)$ is a group using the set of all integers and the binary operation addition. The set of all integers can be seen as the set of all multiples of 1. Looking at the set of all multiples of 2 with addition, $(2\mathbb{Z}, +)$, we can see that it is a valid group and a subgroup of $(\mathbb{Z}, +)$. We can thus produce an infinite number of subgroups within $(\mathbb{Z}, +)$ by finding sets of integers of multiple n.*

3 Examples of groups

3.1 Special linear groups

We define two different groups, namely the set of all linear transformations and the set of matrices with binary operations. We then explain how they relate to each other via an example.

Definition 4. A *linear transformation* is a function $T : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ that must follow these properties:

1. $T(x + y) = T(x) + T(y)$
2. $T(ax) = aT(x)$

for all elements $x, y \in \mathbb{Z} \times \mathbb{Z}$ and $a \in \mathbb{Z}$.

Definition 5. The *special linear group* $SL(2, \mathbb{Z})$ is a set of 2×2 matrices with determinant 1 under matrix multiplication, that is,

$$SL(2, \mathbb{Z}) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a, b, c, d \in \mathbb{Z}, ad - bc = 1 \},$$

where matrix multiplication for 2×2 matrices:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}.$$

In fact, $SL(2,\mathbb{Z})$ corresponds to the group of all linear transformations of $\mathbb{Z}^2$ that preserve oriented area. This can be seen in the following example.

Example 3. *Let $T : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ be a linear tansformation. Suppose that $T(1,0) = (1,0)$ and $T(0,1) = (1,1)$.*

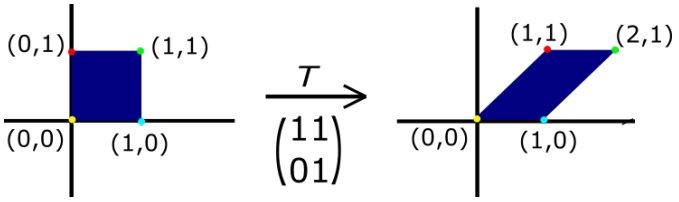


Figure 1 : A visualization of a linear transformation

We can consider T as $T(a,b) = \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}$ by using matrix multiplication. Then $T(1,0) = (1,0)$ and $T(0,1) = (1,1)$ because multiplying the corresponding matrix to each 2×1 matrix of the x,y coordinates gives $(1,0)$ and $(1,1)$. With this, it can be stated that for any point (a,b) within the plane, $T(a,b)$ is the same as multiplying each value of a to $T(1,0)$ and b to $T(0,1)$ and adding them together:

$$\begin{bmatrix}a\\ 0\end{bmatrix} + \begin{bmatrix}b\\ b\end{bmatrix} = \begin{bmatrix}a+b\\ b\end{bmatrix} \text{ or } (a+b,b).$$

The value and sign of the determinant reflects the change in area and orientation respectively. For this specific example, the determinant of the corresponding matrix of the linear transformation is 1. Since the determinant is 1, the transformation preserves the area of the original image. In other words, the area is simply changed by a scale of 1.

Also, there is no change in orientation. As shown in Figure 1, each of the points have a corresponding color: red, yellow, blue, or green. If one were to go counterclockwise from point to point in the first image (on the left in Figure 1) and record the order that the colors are in (for example, red, yellow, blue then green), the order of the colors will stay the same in the image resulting from the linear transformation (as shown in the right image in Figure 1). Therefore the area and orientation are preserved.

4 Algorithmic problem for groups

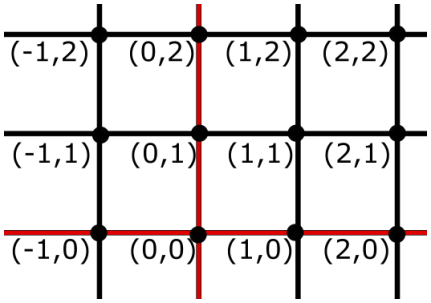
Question 1 (Word problem for a group)**.** *Let G be a group given by a finite presentation. Does there exist an algorithm which, for an arbitrary element g of G, determines whether or not g is the identity in G?*

Example 4. *The word problems for finite groups and $SL(2,\mathbb{Z})$ are solvable.*

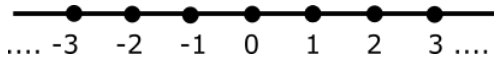
5 Cayley graphs

Definition 6. Let G be a group and let S be a generating set of G. A *Cayley Graph* is a visual representation of any group G where the elements of G serve as vertices, and edges are drawn between any two elements which are separated by one generator in S.

Example 5. *The Cayley graph of* $\mathbb{Z}^2$ *with respect to the generating set* $\{(1,0),(0,1),(-1,0),(0,-1)\}$*:*



Example 6. *The Cayley graph of* $\mathbb{Z}$ *with respect to the generating set* $\{-1,1\}$*:*



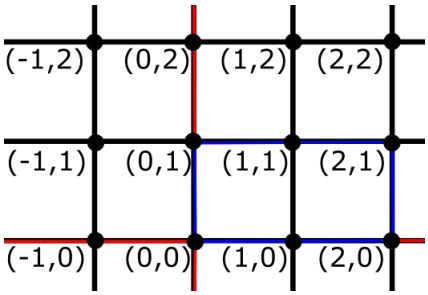
Cayley Graphs are useful for finding unique properties of groups, since they display the relations between elements well. An example of an important property which a Cayley graph can reveal is whether a group is free or not.

To have a free group, the group must not have any nontrivial representations of the identity element e of G. A nontrivial representation of e is any set of operations between the generators of G which will result in e, and is not algebraically simplifiable. An example of a simplifiable (trivial) representation of e is $A * A^{-1} * B * B^{-1}$. In this example, it is easy to just cancel the inverses ($A * A^{-1} = e$) to arrive at e.

While it may seem difficult to find any nontrivial representations of e of G, a Cayley graph makes the task fairly simple. A nontrivial representation of e can be identified as a loop that includes the identity element as one of its vertices. The loop can be seen as a sequence of generating elements which cannot be simplified algebraically, and eventually result in e.

Given all the information regarding the generating set and nontrivial representations of e in G, there is a concise way to notate all this information in what is called group presentation. The formatting of group presentation is as follows: $\langle$generating set | nontrivial representations of $e\rangle$.

Example 7. *In the Cayley graph of* $\mathbb{Z}^2$ *with a generating set* $\{(1,0),(0,1),\ (-1,0),(0,-1)\}$ *on the right figure, the blue loop staring at* $(0,0)$ *represents nontrivial representation of* $e=(0,0)$*, that is,* $(2,0)+(1,0)+(-2,0)+(0,-1)$*. Note that* $\mathbb{Z}^2$ *has a group presentation as* $\langle(1,0),(0,1),(-1,0),(0,-1)\,|\,(m,0)+(0,n)+(-m,0)+(0,-n)=(0,0)\rangle$



5.1 Braid groups

We define another interesting groups used in pure mathematics such as geometric topology and also in quantum physics.

Definition 7. A *Braid Group* B_n contains elements that are equivalence classes of n-braids and whose group operation is the composition of braids.

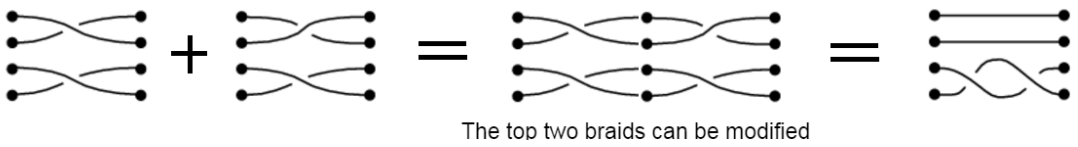
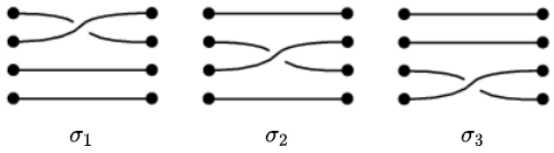


Figure 1: An example of a composition of two braids

Braid Groups are easier to understand through visuals because the process of composing a braid group through operations on a set of other braid groups is an intuitive process. Because of the unique composition of braid groups, problems regarding them can be solved using tools like Cayley graphs and algebraically.

Example 8. *B_4 is generated by the following three braids:*



The set of relations is $\{\sigma_1\sigma_3 = \sigma_3\sigma_1, \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2\, \sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3\}$.

We can check $g = \sigma_1\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2^1\sigma_1^{-1}\sigma_2^{-1} \in B_4$ the identity e algebraically or with the Cayley graph.

6 Future Directions

Question 2. *Let G be a particular group. Is there an algorithm which, for an element $g \in G$, determines g is the identity element in G?*

Question 3. *Suppose that we have such an algorithm. What is the complexity of the algorithm? Is the algorithm practical?*

Question 4. *There is a computer algebra system for computational discrete algebra named GAP. Can we implement such an algorithm into GAP?*

References

[1] Baumslag, Gilbert. Topics in combinatorial group theory. *Birkhäuser,* 2012.

[2] de La Harpe, Pierre. Topics in geometric group theory. *University of Chicago Press*, 2000.

[3] Lyndon, Roger C., and Paul E. Schupp. Combinatorial group theory. *Springer*, 2015.