LAGRANGE'S THEOREM

Sharon Donohoe and Ciara Hamilton†
†National University of Galway

INTRODUCTION

This poster will discuss one of the Lagrange's lasting legacies;
Lagrange's theorem on groups, as well as the developments it underwent to become the theorem we recognise today.

Lagrange's theorem is a well known result which is used in group theory and other fields in mathematics, it is defined as followed:
"Let G be a group of order n and H a subgroup of order m. Then m is a divisor for n"

WHO WAS LAGRANGE?

Joseph-Louis Lagrange was an Italian mathematician born in Turin in 1736.
By age 19, Lagrange had become a professor of mathematics Royal Artillery School in Turin.
Due to his prolific contributions to mathematics and physics, he soon became known as one of the greatest mathematicians in Europe.
Lagrange was born into a changing world in 18th century Italy.
Growing up he was surrounded by great developments in medicine, physics, and the natural sciences, pioneered by his fellow Italian scholars.
There is no doubt that Lagrange soon went on to become one of the defining academics of the age of enlightenment in Italy.

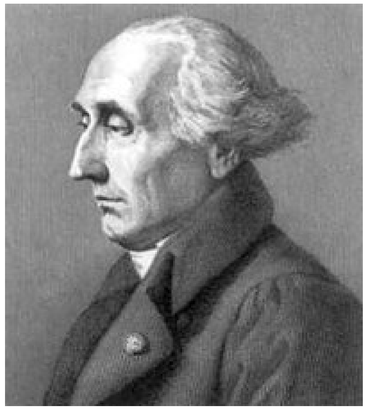


Fig. 1: Joseph-Louis Lagrange.

SOME IMPORTANT DEFINITIONS

GROUP: a non-empty set equipped with a binary operation that together satisfy the properties of closure, associativity, the identity property, and the inverse property.

SUBGROUP: Suppose G is a group under the operation *, and let H be a subset of G. Then H is a subgroup of G if H satisfies the four properties of a group under the operation of G.

ORDER: the order of a group is the number of elements in its set.

ORIGINAL THEOREM OF LAGRANGE

When Lagrange first proposed his theorem, group theory had not yet been defined.
The theorem was first developed in 1770 when Lagrange published workings on the theory of equations.
In this he aimed to derive a formula that could be used to solve a polynomial of 5 degrees or higher.
He reasoned that if solving the quadratic and cubic polynomials involved solving supplementary polynomials of a lower degree then the same might stand for a polynomial of the 5th degree.
This led to the original theorem which stated: If a function F(x1, x2, . . . , xn) of n variables is acted on by all n! possible permutations of the variables and these permuted functions take on only r distinct values then r is a division of n.
This original theorem is vastly different from the one we know today. As the study of group theory developed and changed so too did the theorem originally propose by Lagrange back in 1770.

DEVELOPMENTS ON HIS WORK

Many later developments were made on Lagrange's original work.
In 1799, Paolo Ruffini published a book in which he provided proof that the converse of Lagrange's Theorem does not hold.
In 1815, a paper by Cauchy tied together the prior developments made on Lagrange's Theorem. Cauchy provided a proof of the original theorem as well as a generalised version of Ruffini's theorem.
Cauchy later went on to prove that order of a subgroup Sn is a divisor of n!.
This was the first solid proof of Lagrange's theorem in the case of symmetric groups.
It wasn't until the twentieth century that the language of cosets was used to prove Lagrange's theorem.
Though it is hard to accredit anyone in particular with the first formal proof of the theorem, the coset approach is said to have been inspired by Galois.

Fig. 2: Austin Louis Cauchy

PROVING LAGRANGE'S THEOREM

In order to proof Lagrange's theorem we start with a subgroup H of the finite group G.
If we find that H = G then the theorem holds.But if H G then we choose an element x of G with x not being an element of H (xH).
Then the coset xH is disjoint from H and has |H| elements. If H xH = G then |G| = 2|H| and we are done.
If not, choose y 6 H xH and add the coset yH.Eventually we find that G is the union of k disjoint left cosets of H, and |G| = k|H|.

THE THEOREM EXPLAINED

In this case the term "divides" tells us that the order of subgroup H is a factor of the order of group G.
An example of the theorem in practice is the group S4. S4 has 4! (or 24) elements.
A subgroup of S4 could possibly have 1,2,3,4,6,8,12, or 24 elements as these are all factors of 24 (the order of S4).
The subgroup could not have, for example, 9 or 11 elements as these do not divide 24.
The converse of the theorem is not true.

APPLICATIONS OF LAGRANGE

Lagrange Theorem can be widely applied in mathematics's to prove other theorems.
This can be used to prove Euler's theorem and Fermat Theorem (an integer raised to a prime power leaves the same remainder as the integer itself when divided by the prime) and its generalization.
In addition to this we can use Lagrange to illustrate that there are infinitely many primes.
Lagrange's Theorems can be seen today used in the modern world of the digital payments system namely Cyptocurrencies (eg.Bitcoin).

THE FUTURE OF LAGRANGE

The Future of Lagrange lies in the hands of two very capable students of the School of Mathematics at NUI Galway.

References

Moravia, Sergio., 'An Outline of the Italian Enlightenment', in Comparative Literature Studies, vol. 6, no. 4 (1969), pp.380-409.

Roth, Richard L., 'The History of Lagrange's Theorem on Groups', in Mathematics Magazine, vol. 74, no. 2 (April 2001), pp. 99-108.

'Joseph-Louis Lagrange',Physics Today, (January 2017), https://physicstoday.scitation.org/do/10.1063/PT.5.031404/full/, accessed

Card Shuffling as a Group and the Faro Shuffle

Anna Golden, Emma Meaney, Lise Wall, Lydia Costello

Introduction

In this poster we look at card shuffling a deck of cards is as a group. First, we establish that shuffling is a group and that it is isomorphic to the group of permutations S_N where N is the number of cards in a deck, typically 52 in a standard deck. We then discuss a specific type of shuffle known as the Faro or Perfect Shuffle used by magicians and gamblers, that has interesting properties when considered as a group. We prove the Fundamental Theorem of Faro Shuffling. We discuss the generating set of shuffles. We give an example of a card trick that applies these concepts.

Why Is Card Shuffling a Group?

The set of all shuffles can be represented by the symmetric group S_N, where N is the number of cards in the deck.Let S be a card shuffle that acts on S_{52}, such that S:1,2,...,52 ↦ 1,2,...,52 (Let T, U also be shuffles on S_{52}). The shuffling function is a form of permutation. Card shuffling is a group because it satisfies the group axioms as follows:

- **Closure:** consider shuffles (permutations) S,T, then S ∘ T is also a shuffle (perform T, followed by S)
- **Identity:** This consists of the shuffle which leaves each element in it's original position. Let i(x) be the identity shuffle performed on x ∈ 1,2,...,52, then i(1)=1, i(2)=2,...,i(52)=52.
- **Inverse:** Each permutation S also has an inverse S^{-1} contained in the group, e.g if S(1)=52, $S^{-1}(52)$=1.
- **Associative Property:** For shuffles S,T,U it is true that:
  - S ∘ (T ∘ U) = (S ∘ T) ∘ U.

Faro/Perfect Shuffle

The Faro shuffle is a method of "perfectly" shuffling a deck of cards. A deck of cards is divided into two equal piles and then perfectly interwoven. There are two ways of doing this:

- **In Shuffle:** The In Shuffle leaves the top and bottom card second from top and bottom respectively.

$$\begin{pmatrix} 1 & 2 & 3 \dots 25 & 26 & 27 \dots 50 & 51 & 52 \\ 2 & 4 & 6 \dots 50 & 52 & 1 \dots 47 & 49 & 51 \end{pmatrix} \tag{1}$$

- **Out Shuffle:** The Out Shuffle leaves the top and bottom card in place.

$$\begin{pmatrix} 1 & 2 & 3 \dots 25 & 26 & 27 \dots 50 & 51 & 52 \\ 1 & 3 & 5 \dots 49 & 51 & 2 \dots 48 & 50 & 52 \end{pmatrix} \tag{2}$$

By doing a Faro shuffle on a memorized deck, one can always compute where a card in any given position will end up. What is perhaps more interesting is that Faro shuffles form a subgroup and will always return to the identity within a set number of shuffles. As we will see, for a deck of 52 cards, it will take exactly eight Faro Shuffles to return the cards to their original positions (i.e. $\text{Faro}^8 = id_{52}$).

The Fundamental Theorem of Faro Shuffling

Alex Elmsley found that a series of in and out shuffles can be used to bring the original top card (at position 0) to any desired position p in the deck. This can be achieved by expressing p in binary with 0 meaning an out shuffle and 1 meaning an in shuffle. For example to go from 0 to position 7 (where 7 = 111), perform in, in, in.

With a deck of $2n$ cards, r exists such that $2^{r-1} < 2n \leq 2^r$.
Where $0 < p < 2n-1$, let $t = \frac{(p+1)2^r}{2n}$.
For $p = 0$, set $t = 0$. For $p = 2n-1$, set $t = 2^r - 1$.
Express t in binary as $t = t_{r-1}t_{r-2}...t_1t_0$ with $t_i = 1$ or 0
Let s be correction terms where $s = 2nt - 2^r p = s_{r-1}s_{r-2}...s_1s_0$ with $s_i = 1$ or 0
The shuffling sequence is $t_{r-1} + s_{r-1}, t_{r-2} + s_{r-2}, ..., t_0 + s_0$

For example, if $2n = 52, p = 35$. Then $r = 6$, $t = \frac{36(64)}{52} = 44 = 101100$ and $s = 2288 - 2240 = 48 = 110000$.
Now the co-ordinate sum of 101100 and 110000 is 011100 which is out, in, in. We can ignore the final two shuffles as they do nothing to the top card.

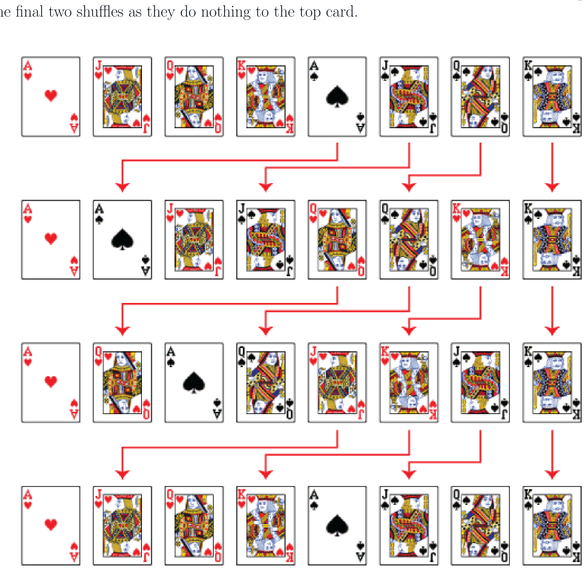


Fig. 1: For an 8-card deck, only three out-shuffles are required to restore the original order

The Generating Set of Shuffles

Starting with a randomly shuffled deck of 52 cards, any other shuffle of the deck can be reached by a combination of swapping the first two cards and putting the bottom card on top of the deck. In other words S_{52} is generated by the transposition (1 2) which swaps the first two cards in the deck and the 52-cycle (1 2 ... 52) which brings the bottom card of the deck to the top.
Proof:

Let x = (1 2 ... 52)

$x(1 \quad 2)x^{-1} = (2 \quad 3)$
$x(2 \quad 3)x^{-1} = (3 \quad 4)$
$\vdots$
$x(50 \quad 51)x^{-1} = (51 \quad 52)$
$\implies (i \quad i+1) \in \langle (1 \quad 2), x \rangle \quad \forall \quad 1 \leq i \leq 51$
$(2 \quad 3)(1 \quad 2)(2 \quad 3)^{-1} = (1 \quad 3)$
$(3 \quad 4)(1 \quad 3)(3 \quad 4)^{-1} = (1 \quad 4)$
$\vdots$
$(51 \quad 52)(1 \quad 51)(51 \quad 52)^{-1} = (1 \quad 52),$
$\implies (1 \quad i) \in \langle (1 \quad 2), x \rangle \quad \forall \quad 1 \leq i \leq 52$
For any $1 \leq i < j \leq 52$:
$(i \quad j) = (1 \quad i)(1 \quad j)(1 \quad i)^{-1} \in \langle (1 \quad 2), x \rangle.$

Therefore $\langle (1,2), x \rangle$ generates all transpositions in the group S_{52}, and so generates the group itself as every permutation is a product of transpositions.

A Card Trick to Try

Before you start memorise the card on the bottom of the deck. Ask your friend to pick a card out of the deck, look at it and put it on top of the deck without you seeing it. Then allow them to cut the deck as many times as they want. Spread the cards out face up and announce the chosen card which is the card in front the "bottom card" you had memorised.
Why does this work?
Under the action of cutting the cards the adjacency of pairs of cards is preserved. The group H is the subgroup of S_{52} generated by the 52 cycle (1 2 3... 51 52). The adjacency of pairs of cards is not changed by any action in H and so although H seems to be shuffling the cards, the chosen card will always remain in front of the original bottom card making it is easy to find the chosen card.

References

Conrad, K.,Generating Sets. University of Conneticut.https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf
C-for-dummies.com.2017.The Perfect Shuffle | C For Dummies Blog.[online]https://c-for-dummies.com/blog/?p=2519
Diaconis, P., Graham, R. and Kantor, W.(1983). The mathematics of perfect shuffles. Advances in Applied Mathematics, 4(2), pp.175-196.
Diaconis, P. and Graham, R.(2020). The Solutions To Elmsley'S Problem.https://statweb.stanford.edu/~cgates/PERSI/papers/pre-elmsley.pdf
Ensley, D. (1999). Invariants under Group Actions to Amaze Your Friends. Mathematics Magazine, [online] 72(5), p.383.https://www.maa.org/sites/default/files/269079545577.pdf
Quinlan, R. (2020), "The Axioms of a Group", *MA3343: Groups*, available: http://www.maths.nuigalway.ie/~rquinlan/groups/section1-2.pdf [accessed 11 Dec 2020]

Quantum Mechanics: The Stabilizer Formalism

Billy Ray

Introduction

The stabilizer formalism of quantum mechanics presents a novel way of describing the machinery of quantum mechanics using concepts from Group Theory. The stabilizer formalism uses the concepts of the stabilizer of a group and generators of a group in order to characterise quantum states and the result of operations on those states.

Quantum States

- Quantum states are represented as unit vectors in a complex vector space. The state is represented using a set of orthonormal basis vectors which span the space. Let $|0\rangle$ and $|1\rangle$ represent a basis of two orthonormal vectors in $\mathbb{C}^2$ such that:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

  Thus, a quantum state, $|\psi\rangle \in \mathbb{C}^2$, could have the form:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

- A quantum state in $\mathbb{C}^2$ is called a qubit state. The basis of quantum computing consists in manipulating qubit states through matrix-vector multiplication.

Multiple Qubit States

- The tensor product operation combines multiple qubits into a single composite system. The composite system of two qubits, $|\psi\rangle \otimes |\psi\rangle$, occupies the complex vector space $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$. Thus, a 2-qubit state can be represented using a set of four orthonormal basis vectors spanning the space $\mathbb{C}^4$.
- In general, a composite system of n qubits is defined in $\mathbb{C}_1^2 \otimes \mathbb{C}_2^2 \otimes ... \otimes \mathbb{C}_n^2 = \mathbb{C}^{2^n}$. An arbitrary n-qubit state can be represented using an orthonormal basis consisting of 2^n vectors which span the vector space $\mathbb{C}^{2^n}$.

The Pauli Group

- Operators are matrices which act on quantum states. Operators acting on separate qubit states are also combined using the tensor product operation. For two operators U_1 acting on a qubit $|\psi_1\rangle$ and U_2 acting on another qubit $|\psi_2\rangle$, the total action on the composite system is simply:

$$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (U_1 |\psi_1\rangle \otimes U_2 |\psi_2\rangle)$$

- For the qubit state, $|\psi\rangle \in \mathbb{C}^2$, there exist a special class of operators known as the Pauli matrices:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- A group under the operation of matrix multiplication, known as the Pauli group, G_1, can be defined using these operators with the multiplicative factors ± 1 and $\pm i$:

$$G_1 = \{\pm\mathbb{I}, \pm i\mathbb{I}, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

  The Pauli group generalizes to the n-qubit case, where each element of the Pauli group, G_n, is a distinct tensor product of n individual Pauli matrices with multiplicative factors ± 1 and $\pm i$[1].
- Every matrix in the group G_1 can be *generated* by the elements X,Y and Z:

$$G_1 = < X, Y, Z >$$

The Stabilizer Formalism

- Consider a subgroup S of G_n, and define the subspace V_s to be the set of n-qubit states which are fixed by every element of S. The set of vectors V_s is *stabilized* by S and the subgroup S forms the *stabilizer* of the subspace V_s, $Stab_{G_n}(V_s)$.
- The subgroup S can be defined in terms of its *generators*. To assess whether a particular n-qubit state belongs to the stabilized subspace, V_s, it suffices to check whether the vector is stabilized by the generators of S[1].

Arbitrary Operations

- Quantum operators are unitary, this means they satisfy the relation $UU^\dagger = U^\dagger U = \mathbb{I}$ where U is a unitary operator and $U^\dagger$ involves transposing U and complex conjugating all of the entries.
- Consider an arbitrary unitary operator, U, applied to the vector space V_s which is stabilized by the subgroup S. For any vector $|\psi\rangle \in V_s$ and matrix element $g \in S$ we find:

$$U|\psi\rangle = Ug|\psi\rangle = (UgU^\dagger)U|\psi\rangle$$

- The new vector $U|\psi\rangle$ is stabilized by $UgU^\dagger$. After applying the operator U to our entire vector space V_s, we can see that our new vector space UV_s has stabilizer $USU^\dagger = \{UgU^\dagger | g \in S\}$.
- If the stabilizer S has generators $< g_1, g_2, ..., g_n >$ then our new stabilizer, $USU^\dagger$, has generators $< Ug_1U^\dagger, Ug_2U^\dagger, ..., Ug_nU^\dagger >$.

Benefits of the Stabilizer Approach

- It can be shown that the Pauli Z gate stabilizes the $|0\rangle$ state i.e. $Z|0\rangle = |0\rangle$. Thus, an n-qubit state:

$$|\phi\rangle = (|0\rangle_1 \otimes |0\rangle_2 \otimes ... \otimes |0\rangle_n) = |0\rangle^{\otimes n} \in \mathbb{C}^n$$

  has a stabilizer with a single element, $S = \{Z_1 \otimes Z_2 \otimes ... \otimes Z_n\}$.
- Define a unitary operator, H, with the property $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Applying this operator to $|\phi\rangle$ gives:

$$H^{\otimes n}|\phi\rangle = H_1|0\rangle_1 \otimes ... \otimes H_n|0\rangle_n \in \mathbb{C}^{2^n}.$$

- However, the Pauli X gate stabilizes this resulting state:

$$X\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- This means our new state $H^{\otimes n}|\phi\rangle$ also has a single-element stabilizer, $S' = \{X_1 \otimes X_2 \otimes ... \otimes X_n\}$. Our stabilizer still has n terms, but the vector representation of our new state has 2^n terms! For 100 qubits, this is a $\approx 10^{28}$ improvement...
- A group-theoretic approach to simple quantum computations allows for classical simulations as we can keep the number of terms *linear* in n.

References

Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.

History of Lagranges Theorem

By Dylan Cassidy Killane and Cian Forde

National University of Ireland, Galway

Introduction

Joseph Louis Lagrange and his theorem are core principals to grouping theory. Through this informative poster we intend to examine the history of this theorem including:

- A brief history on the creator Joseph Louis Lagrange
- Why did he create this theorem?
- Other famous mathematicians' contributions to the theorem
- Examples of this theorem
- Applications of the theorem in today's world

Joseph Louis Lagrange - The Man Behind The Theorem

Joseph Louis Lagrange was born on the 25th of january 1736 in Turin. He studied at the University of Turin where his favourite subject was classical Latin having no great enthusiasm in mathematics and found Greek Geometry rather dull and in his later life is famously quoted as saying "If I had been rich, I probably would not have devoted myself to mathematics".[1] After having his interest in mathematics sparked by reading a paper published by Edmond Halley. From this he improved his stature in the world of mathematics with feats like solving the isoperimetrical problem at only 19 years of age. Then in 1766 he moved to Berlin to start work on his theorem of which is named after him, Lagrange's Theorem. Later in life he moved to France and became a naturalised frenchman. He would pass away in Paris in April 1813.

What was he trying to achieve?

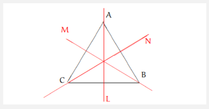
With formulas already existing for the quadratic, cube and quartic equations, Lagrange wanted to derive a formula for equations of degree five also known as quintic equations and more specifically for equations of nth degree. He saw that when solving more known polynomials such as quadratic and cubic resolvent polynomials of lesser degrees. From this he noted that the roots of the polynomial x1,x2,x3 and x4 could be permuted 24 times or (4!)

Other Famous Mathematician's Contributions

Augustin-Louis Cauchy contributed twice to Lagrange's theorem writing a paper on permutation groups before the idea of groups was even formalised and again in 1844, proving lagranges theorem for symmetric groups.
Camille Jordan added to Cauchy's work in 1861 by proving the theorem for finite permutation groups
Evariste Galois was the man who formalised the idea of groups in 1831 in a paper on solving solutions of permutation groups by radical

Examples of this Theorem

- Lagrange's Theorem: If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.
- Let D6 be the set of symmetries of the equilateral triangle, with rotations id, R120, R240 and reflections TL, TM and TN as shown.[2]



- Then H = id, TL is a subgroup of D6 of order 2, and left cosets of H in D6 determined by the six elements are:
  1. idH = id ∘ id, id ∘ TL = id, TL = H
  2. TLH = TL ∘ id, TL ∘ TL = TL, id = H again.
  3. R120H = R120 ∘ id, R120 ∘ TL = R120, TM.
  4. TMH = TM ∘ id, TM ∘ TL = TM, R120 = R120H again.
  5. R240H = R240 ∘ id, R240 ∘ TL = R240, TN
  6. TNH = TN ∘ id, TN ∘ TL = TN, R240 = R240H again.

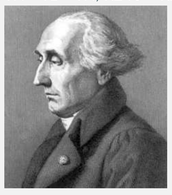


Figure: Joseph Louis Lagrange

Contributors To This Theorem



Figure: Cauchy(left), Galois(Centre), Jordan(right)

Application in Todays World

- It seems fair to state that Lagranges theorem is going to be used a lot more in the everyday life of a mathematician than that of say an electrician. If you are a mathematician however its applications are bountiful. For example, Lagranges theorem can be used to prove Euler's theorem as well as Fermat's little theorem aswell as its generalization.[3]
- It also has uses in cryptography.Due to its use in computing the power of an integer modulo a prime number. This shows the theorem to be applicable even in the general public's lives whether they know it or not as cyber-security plays such an important part in our lives.

Conclusion

Lagrange is such an interesting Mathematician to study to say the least. It seems bizzare that someone so intelligent and mathematically skilled had no great passion for his field of study. Inspite of this he has produced one of the most important theorem's used in Group theory to this day. It's core use in group theory will preserve Lagranges name in the minds of mathematicians for centuries to come.

References

[1] J. J. O'Connor and E. F. Robertson. Joseph louis lagrange. https://mathshistory.st-andrews.ac.uk/Biographies/Lagrange/, January 1999.

[2] Essential concepts of group theory. http://www.maths.nuigalway.ie/~rquinlan/groups/section2-1.pdf.

[3] Lagranges theorem (group theory) wikipedia. https://en.wikipedia.org/wiki/Lagrange%27s_theorem_(group_theory).

Frieze Groups

Thomas Hayes Cian Doheny Jack Flood

Introduction

Our chosen topic is frieze groups. Frieze groups are two-dimensional line groups, having repetition in only one direction. They are the distancing preserving transformations of a pattern.

What makes a frieze group

There are seven distinct frieze groups. All of them can be generated by translation, reflection (along the same axis) and a 180° rotation.
The seven Frieze groups are:

- The first frieze group F_1 was named by Conway as a HOP.
- The second frieze group, F_2, contains translation and glide reflection symmetries. According to Conway, F_2 is called a STEP.
- The third frieze group, F_3, contains translation and vertical reflection symmetries. Conway named F_3 a SIDLE.
- The fourth frieze group, F_4, contains translation and rotation (by a half-turn) symmetries. According to Conway, F_4 is called a SPINNING HOP.
- The fifth frieze group, F_5, contains translation, glide reflection and rotation (by a half-turn) symmetries. Conway calls F_5 a SPINNING SIDLE.
- The sixth frieze group, F_6, contains translation and horizontal reflection symmetries. Conway named F_6 a JUMP.
- Finally, the seventh frieze group, F_7, contains all symmetries (translation, horizontal vertical reflection, and rotation). According to Conway, F_7 is named a SPINNING JUMP.

[1]

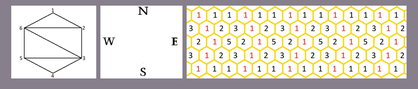
Background and History of frieze groups

Frieze patterns name originated from the architectural term of a frieze or a broad decorative band and were extremely popular in Ancient Greece. The patterns started off as simply patterns of lines repeated all the way around the building, with each set of lines spaced a particular distance away from the previous one. Later on the patterns became more intricate involving moldings or painting in each of the spaces where the lines used to be, but it would still be the same image repeated all the way around the structure. [2]

Frieze Pattern

Imagine some $n-gon$. Another way of looking at Frieze pattern is as a table of Natural numbers displayed in a lattice. Where the top and bottom rows are 1's, and the amount of rows is determined by $n-3$. To figure out the second row we triangulate the $n-gon$(hexagon in this example) any way we wish. Making some order out of the vertices(clockwise in this example), the number in the pattern corresponds to the amount of triangles adjacent to that vertex . The following rows are calculated by making unit diamonds with the above two rows labeling vertices in a compass fashion N,S,E,W.

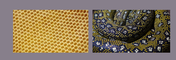
$$(W \times E) - (N \times S) = 1$$



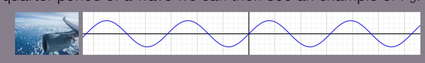
The example portrayed here is a special *Lightning bolt* example named due to the 'lightning bolt' of 1's

Examples of frieze groups in the real word

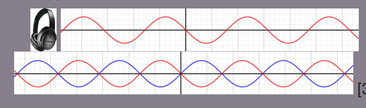
There are natural and man made friezes all around us. The honeycomb in a bees' nest (left) is an example of F_1 layered on top of each other. Snake skins have amazing intricate frieze patterns. This snake skin pattern (right) contains all symmetries. What Frieze groups can you spot in the honeycomb?



If we can think of a constant sound, like the engine on a plane, wave we can see examples of different frieze groups. If we take our first space as one period of a wave we can then see an example of F_1. If we take our second space as a quarter period of a wave we can then see an example of F_5.



An example of where we see similarities to Frieze groups are destructive sound waves, these are waves generated by headphones to cancel out background noise. Destructive waves looks like F_6 applied to the sound wave resulting in the inverted shape to cancel out noise(red graph). The resulting waves when added together(played together) should look like the final graph(red and blue) called total destructive interference.



[3]

References

URL: https://www.maa.org/sites/default/files/images/upload_library/4/vol1/architecture/Math/seven.html.

Tyler Landau. *Classifications of Frieze Groups and an Introduction to Crystallographic Groups*. 2019. URL: https://www.whitman.edu/documents/Academics/Mathematics/2019/Landau-Balof.pdf.

Numberphile. URL: https://www.youtube.com/watch?v=0mXz-NF-raY.

THE CONVERSE OF LAGRANGE'S THEOREM

Megan McGlinchey and Eoin Mulvihill

Group Theory MA3343

Introduction

Lagrange's Theorem can be regarded as one of the most central theorems of abstract algebra and considered by many "the most important theorem of group theory". However, the converse of this infamous theorem is undoubtedly false. This poster will explore why the converse fails as well as other methods of finding subgroups

Joseph Lagrange

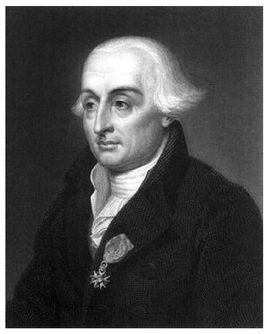


Fig. 1: Joseph Lagrange.

Giuseppe Luigi Lagrange was born in Turin, Italy on 25th January 1736. He made many significant contributions towards analysis, number theory and analytical and celestial mechanics although, sadly, did not prove his own theorem. In 1801 Gauss proved Lagrange's theorem for the multiplicative group of non-zero integers modulo p, $(\mathbb{Z}/p\mathbb{Z})$, in 1844 Cauchy proved the theorem for the symmetric group S_n and, finally, Jordan proved Lagrange's theorem for the case of any permutation group in 1861.

Applications of his work

Lagrange's Theorem displays some key properties that allow for further theorems such as Fermat's little theorem and Wilson's theorem to be proven as well as showing there to be infinitely many primes.

Converse of Lagrange's Theorem

Every divisor of the order of group G is the order of some subgroup H of G

Where the converse fails

The most basic example to demonstrate where the converse fails, is the alternating group A_4 of even permutations.

A_4={ ID,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(123),(132),(124),(142),(134),(143),(234),(243)}

$|A_4|$=12 , With the divisors of the group being {1,2,3,4,6,12}

Lets assume there exists a subgroup H, in A_4 with the order of $|H|$=6.
Let V be a non-cyclic subgroup of A_4 –> Known as the Klein four group.
V={ID,(12)(34),(13)(24),(14)(23)}

Let $K = H \cap V$, Since H and V are subgroups of A_4, then so to is K.
By Lagrange's Theorem, K's order divides both 6 and 4. So $|K|$=1 or $|K|$=2

If $|K|$=1, the map (h, v) -> $h.v$ defined from H x V to A_4 has a one to one relationship implying A_4 has 24 elements which we know is not true.
So $|K|$ = 2 where $h \in H$ and $v \in V$

The index $|A_4 : H|$=2 shows that there is exactly 2 distinct cosets and as such, we know H is a normal subgroup.
This implies $H = tHt^{-1}\ \forall t \in A_4$.

Take $v = (ab)(cd)$ and $t = (abc)$, where (a, b, c, d)= (1,2,3,4)
$tvt^{-1} = (bc)(ad) \neq (ab)(cd)$
$tvt^{-1} \neq v$
but V contains all disjoint transpositions so,
$tvt^{-1} \in V$ and $tvt^{-1} \in H$ So, $tvt^{-1} \in H \cap V = K$. Thus, we have demonstrated that there is a third element in K which contradicts our assumption that $|K|$=2 and so there is no subgroup of order 6.

Cauchy's Theorem

Cauchy's Theorem states that a group G whose order g is divisible by a prime number p contains an operator of order p.
Proof:
Suppose G is abelian and generated by a single operator S of order np. $S^n \neq 1$ although $(S^n)^p = 1$, showing that S^n is the required operator. If G is not generated by a single operator, we can examine a set of generating operators $\{S_1, S_2, ..., S_r\}$, which are all commutative. Since these operators are commutative there exists at least one generator for which the order is divisible by p, and some power of this generator must be the required operator of order p.

Fig. 2: Augustin-Louis Cauchy.

References

- Miller, G.A.. (1898). On an Extension of Sylow's Theorem. Bull. Amer. Math. Soc., vol. 4 p323
- https://mathshistory.st-andrews.ac.uk/Biographies/Lagrange/
- https://www.maa.org/sites/default/files/pdf/cms$_upload/On_the_Converse-Gallian34078.pdf$

- https://www.mathcounterexamples.net/converse-of-lagrange-theorem-does-not-hold/

- https://en.wikipedia.org/wiki/Lagrange

Group Theory

Applications of Non-Abelian Groups in Cryptography

Emma Corbett, Eoin McArdle & Gordon O'Connor
National University of Ireland, Galway

Introduction

Currently the majority of cryptographic schemes are based on commutative algebraic structures such as Abelian Groups. In terms of classical computing, these schemes are considered secure. This is because the problems which underpin their operation are considered 'hard' or intractable. This means that no solution can be found in reasonable time. For example it takes approx. $2.73 * 10^{61}$ years to crack AES-256 encryption using a home computer. However, recent advancements in quantum computing theory have shown that not all these problems are indeed intractable. The use of non-commutative algebraic structures such as non-abelian groups offer a possible solution to this security issue.

Abelian Groups in Cryptography

Abelian Platform Groups:

Many abelian groups can be used for cryptographic schemes. A simple example is the additive group $G = \mathbb{Z}/d\mathbb{Z}$. However, in practice much larger and complex groups are used. Groups of points on suitable elliptic curves are usually used. An elliptic curve is given by the equation $y^2 = x^3 + ax + b$.

Figure 1: Examples of an Elliptic Curves

Discrete Logarithm Problem (DLP):

The DLP is one of the main problems that current crypography relies on. It is described as follows where G is a cyclic group with generator g:

$$\textit{Let } G = \langle g \rangle$$

$$\textit{Given } h \in G \textit{ find } x \textit{ such that } g^x = h$$

- Currently the DLP problem is intractable using current computing methods for certain large groups of G.
- However, Shor's quantum algorithm has been shown to solve this problem in polynomial time, therefore making the DLP tractable even for complex, large groups such as elliptic curves.
- *Fig. 2* shows the difference between tractable problems (polynomial, linear, logarithmic) and intractable problems (exponential) in terms of time.

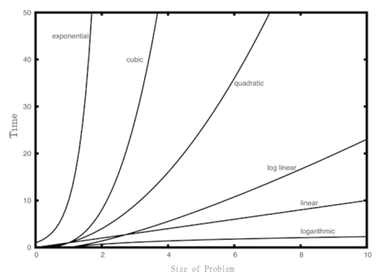


Figure 2: Time Complexity

Diffie-Hellman Key Exchange:

The Diffie-Hellman Key Exchange protocol is a fundamental method of establishing a secret shared key between two parties over an insecure connection. Suppose Alice and Bob wish to create a shared key, K using the cyclic group G where the order, d, and generator, g of G are publicly known:

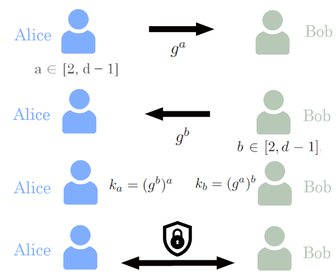


Figure 3: Diffie-Hellman Protocol

- From the above protocol we can clearly see that the Diffie Hellman Key Exchange relies on the DLP being intractable as do many other cryptographic protocols.
- This highlights the need for a more secure alternative for the quantum computing age.

Non-Abelian Platform Groups

The idea of using the complexity of non abelian (infinite) groups in cryptography dates back to the work of Wagner and Magyairk in 1985. A cryptographic platform group G must have several key requirements in order to tackle the conjugacy search problem:

- The group G must be well studied/understood.
- The word problem in G should have a linear/quadratic solution by a deterministic algorithm.
- There should be a way to disguise the elements of G so that they it is impossible to to recover individual elements from a product of elements just by inspection.
- G should be a group of super, polynomial growth. This insures that the number of elements in G of length n will grow faster than any polynomial in n.

Braid Groups:

Braid Groups were one of the first non-commutative groups to be suggested as a "good" suggestion as a cryptographic platform. There are many advantages and disadvantages of using braid groups in cryptography . It appears as if the conjugacy search problem in a braid group does not provide sufficient security unless keys are selected by narrow and yet to be determined subsets of the entire group.

A braid is obtained by laying down a number of parallel pieces if string and intertwining them without forgetting that they are essentially the same direction.

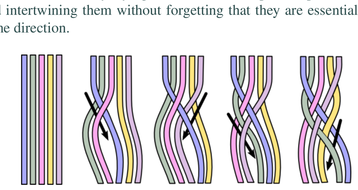


Figure 4: Five Strand Braid - Vertical direction

There are exactly $n-1$ crossing types for an n strand braid. $(x_1, ...x_{n-1})$.x_i is a positive crossing of of the ith and i +1st strands. the set $x_1, ...x_{n-1}$ generates B_n.Each crossing is subject to the relation

$$[x_i, x_j] = 1$$

for every i, j s.t $|i-j| > 1$ and

$$x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$$

That is , the braid group B_n is denoted :

$$B_n = \left\{ x_1, ...x_{n-1} \middle| \begin{array}{c} x_i x_j x_i = x_j x_i x_j \;\; if \;\; |i-j| = 1 \\ x_i x_j = x_j x_i \;\; if \;\; |i-j| > 1 \end{array} \right\}$$

Words and Normal Groups:

- A word is any written product of group elements and their inverses. For example if $x, y, z \in G$ then $xy,\ z^{-1}xzz,\ y^{-1}zxx^{-1}yz^{-1}$ are words in the set x,y,z.Two different words may evaluate to the same value in G
- A word is called reduced if it contains no string of the form $aa^{-1}, a \in$it's generating set
- Normal form for a free group G with generating set S is a choice of a reduced word in S for each element of G

Conjugacy Search Problem (CSP):

Let G be some platform group. For example:

$$G = B_n$$

Given words $x, y \in G$ find z such that:

$$y = zxz^{-1}$$

- It has been shown that for Braid groups and other suitable platform groups this problem is undecidable.
- This means that no algorithm can be designed such that leads to the conclusion whether z exists or not and therefore offer more security potential.

Non-Abelian Cryptographic Protocols

Many different protocols exist which rely on non-abelian platform groups to perform key exchanges, encryption/decryption and authentication. These protocols aim to provide greater security than their commutative equivalents.

Anshel–Anshel–Goldfeld Key Exchange:

- Is a non-abelian alternative to the Diffie-Hellman Key Exchange.
- Requires that the platform group used has easily computable normal forms. Because of this, braid groups are primarily used as the platform group for this protocol.

$$\textit{Let } G = B_n$$

$$a = (a_1, ..., a_k),\ b = (b_1, ..., b_m) \in G$$

$$a \textit{ and } b \textit{ are publicly known.}$$

Alice selects a word in a and computes its product A:

$$A = a_{i_1}^{\epsilon 1} ... a_{i_L}^{\epsilon L},\ a_{i_k} \in a,\ \epsilon_k = \pm 1$$

Bob selects a word in b and computes its product B:

$$B = b_{j_1}^{\delta 1} ... b_{j_L}^{\delta L},\ b_{j_k} \in b,\ \delta_k = \pm 1$$

Alice sends Bob the conjugates:

$$Ab_1A^{-1}, ..., Ab_mA^{-1}$$

Bob sends Alice the conjugates:

$$Ba_1B^{-1}, ..., Ba_kB^{-1}$$

Alice computes:

$$A^{-1}(Ba_{i_1}^{\epsilon 1}B^{-1})...(Ba_{i_L}^{\epsilon L}B^{-1}) = A^{-1}B^{-1}AB$$

Bob computes:

$$(Ab_{i_1}^{\epsilon 1}A^{-1})...(Ab_{i_L}^{\epsilon L}A^{-1})B = A^{-1}B^{-1}AB$$

Conclusion

Non-abelian cryptography clearly shows promise in resisting quantum computing attacks due to the CSP being undecidable for suitable platform groups. However, with their added complexity and relative lack of research they are not often implemented at present. With this said, they are one of the main candidates for the future of cryptography in the quantum computing age.

LAGRANGE'S THEOREM - A BRIEF INTRODUCTION AND HISTORY

Ryan McElhatton, Ruairi Dennehy, Enda Daly and Ross Trearty†

†National University of Ireland, Galway

Introduction to Lagrange's Theorem

This poster takes a look at mathematician Joseph Louis Lagrange, and his most famous work, 'Lagrange's Theorem'. Born in 1976, in Turin, Italy, Lagrange made huge contributions to the field of mathematics. One of his most important findings came in Group Theory where he proved a theorem that states if H is a subgroup of a finite group G, then, the size of H divides the size of G. We will take a look at Lagrange himself, his theorem, and some applications of the theorem.

Joesph Louis Lagrange

Giuseppe Luigi Lagrangia was born in Turin on the 25th of January 1736. He made for significant contributions to many areas of mathematics including analysis, number theory and mechanics. Areas in mathematics such as Lagrangian in mechanics and the Euler-Lagrange equation in calculus have been given his name as testament to his work. He passed away in Paris on the 10th of April 1813, aged 77.

The Theorem of Lagrange

Lagranges theorem states, If a function $f(x1, x2...xn)$ at $n!$ variables is acted on by all possible permutations of the variables and these permuted functions take only r distinct values then r is a division of $n!$.
Lagrange discovered this while he was trying to find an algebraic formula solution for a 5th degree polynomial and more generally for the nth degree polynomial where $n > 4$. He observed that the solution for quartic and cubic equations could be solved by finding an equation of a lower degree. These types of polynomials are known as resolvent polynomials. For this example we will write the roots as:

$$\frac{x_1x_2 + x_3x_4}{2}, \frac{x_1x_3 + x_2x_4}{2}, \frac{x_1x_4 + x_2 + x_3}{2}$$

where $x1, x2, x3, x4$ are roots of the original polynomial. In addition, he observed that all of the 4 roots are permuted in 4! = 24 ways and only these 3 values would occur. Lagrange then said that in order to solve a quintic equation, we would need a function which only takes 4 values when the variable is permuted permuted in $5! = 120$ ways.

Proof of Lagrange's Theorem

Theorem:
If *G* is a finite group of order *n* and *H* is a subgroup of G of order *k*, then k|n and $\frac{n}{k}$ is the number of distinct cosets of H in G

Proof:
To prove this theorem we start by considering the 3 lemmas outlined below.

- **Lemma 1:**If G is a group with subgroup H, then there is a one to one correspondence between H and any coset of H
- **Lemma 2:**If G is a group with subgroup H, then the left coset relation, $g_1 \sim g_2$ if and only if $g_1 \star H = g_2 \star H$ is an equivalence relation.
- **Lemma 3:**Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then A = B.

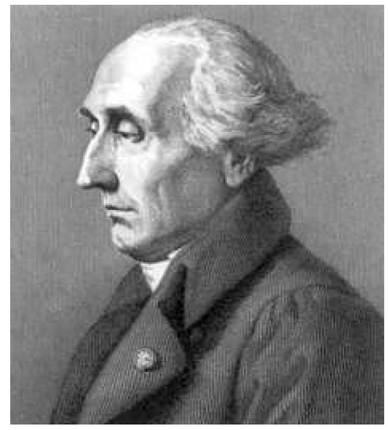


Fig. 1: Joespeh Louis Lagrange

Let $\sim$ be the left coset equivalence relation defined in Lemma 2.
It follows from Lemma 2 thatis an equivalence relation and by Lemma 3 any two distinct cosets of$\sim$are disjoint. Hence, we can write

$$G = (g_1 \star H) \cup (g_2 \star H) \cup \ldots \cup (g_n \star H)$$

where the $g_i \star$ H, i= 1,2,... are the disjoint left cosets of H guaranteed by Lemma 3. By Lemma 1, the cardinality of each of these cosets is the same as the order of H, and so

$$|G| = |g_1 \star H| + |g_2 \star H| + \ldots + |g \star H|$$
$$|G| = |H| + |H| + \ldots + |H|$$
$$|G| = n \star |H| = n \star k.$$

where k = the order of H
Q.E.D

Applications

Lagrange's theorem is often used to prove the special cases of Fermat's little theorem and its generalization, Euler's theorem, which were already known before Lagrange's theorem. Lagrange's theorem can also be used to show that there are an infinite number of primes. The theorem is also very important in the field of cryptography. With the rise of cryptocurrencies such as Bitcoin and our move towards a cashless society, work in cryptography is sure to be very important in the coming years. Bitcoin has recently reached its all time high of over 20,000 USD further proving our shift towards cryptocurrencies. Having a good knowledge of Lagrange's theorem may help you get into the world of cryptography!

Lagrange Fun Facts

Here are a few fun facts around Lagrange and his theorem

- Lagrange's interest in mathematics began by chance after reading a memoir by Edmond Halley
- In 1764, Lagrange was awarded a prize by the French Academy of Science for an essay on how apparent oscillation causes insignificant yet tangible changes in position of lunar features on the visible face of the moon. This essay included the famous equations we use today.

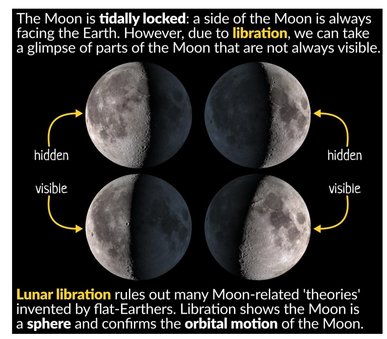


Fig. 2: The basis of one of Lagranges famous papers

- Lagrange, at Leonhard Euler's recommendation, was made Director of Mathematics at the Berlin Academy in 1766.
- Despite being both an academic, and a foreigner, Lagrange survived the French Revolution and Reign of Terror.

The Group of Symmetries of the Cube

Seán Tynan Luke Finn

Introduction

This is a poster about the group of symmetries of a cube. A cube is a 3D shape with 6 square faces, 8 vertices and 12 edges. There is a total of 48 symmetries of the cube. Comprising of 24 rotational symmetries and 24 reflections.

Reflection Symmetries

There are a total of 24 reflection symmetries of the cube and these are consisting of:

- 15 turn reflections.
- 9 plane reflections.

Turn Reflections

There are 3 axes which exists from the center of one face to the center of the opposite face and they can each be rotated 4 times. These degrees of rotation are 90°, 180° and 270°, not counting the identity. However since a 180° turn reflection is actually the antipodal symmetry, there are actually 6 turn reflections. Consisting of 3 each for the 90° and 270° rotations.

There are 4 axes which exists from a vertex to the diagonally opposing vertex and they can each be rotated 3 times. These degrees of rotation are 120° and 240°, not counting the identity. Therefore there are 8 of these turn reflections.

There are 6 axes which exists from the midpoint of one edge to the midpoint of the diagonally opposing edge and they can each be rotated twice. Again, not counting the identity, this degree of rotation is 180°. But since each of these 180° rotations are really the antipodal symmetry, there are no turn reflections for this axis either.

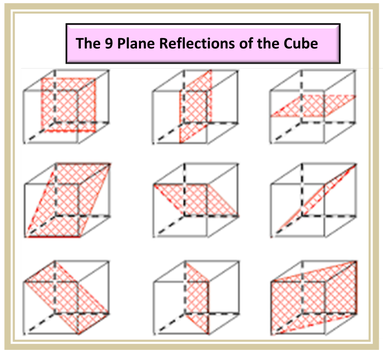
Finally we have the antipodal symmetry which was not counted in any of the above turn reflections. This is the 180° turn reflection. This is 1 turn reflection and combined with the previous 6 and 8 turn reflections stated above, brings the total to 15.

Plane Reflections

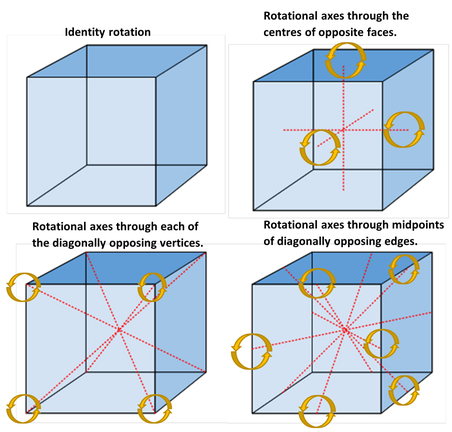
The cube has 9 reflection planes which are:

- 3 planes lie parallel to the side squares and go through the centre.
- 6 planes go through opposite edges and two body diagonals. They divide the cube into prisms.

Reflection Symmetries Graphic



Rotation Axes Graphics



Rotational Symmetries

There is a total of 24 rotational symmetries of the cube, all of which are anti-clockwise. These consist of:

- 9 rotations about lines through the centres of opposite faces.
  There is a total of 3 axes of rotation, each of which has 3 rotations. Consisting of 90°, 180°, 270°.
- 8 rotations about lines through diagonally opposing vertices.
  There is a total of 4 axes of rotation, each of which has 2 rotations. Consisting of 120°, 240°.
- 6 rotations about lines through midpoints of diagonally opposing edges.
  There is a total of 6 axes of rotation, each of which has 1 roation.
  This is the rotation through 180°.
- Identity which is a rotation 0° or 360° through any of these axes.

References

Rotation images - https://i0.wp.com/peterjamesthomas.com/wp-content/uploads/2016/08/rotational-group-of-a-cube.jpg?ssl=1
Reflections - http://jwilson.coe.uga.edu/EMAT6680Fa06/Sexton/NCTMThreeDimensionalGeometry/SymmetryofaCube.html

Rubik's Cubes & Group Theory

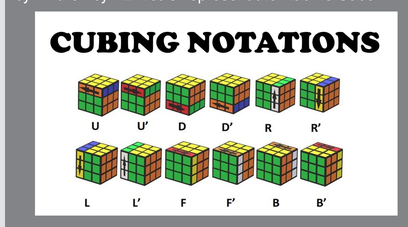
by Joshua Conneely

RUBIK'S CUBE

The Rubik's Cube is a 3-D combination puzzle invented in 1974 by Hungarian sculptor and professor of architecture Ernő Rubik. Although it reached it's peak popularity in the 1980's it is still widely know and used today.
Many "speedcubers" still use it and continue to improve on solve times.
The current world record for solving a cube is 3.47 seconds and is held by Yusheng Du.

How Group Theory and Rubik's Cube's Relate

All the possible rotations of a Rubik's Cube can be proven to be a group. First we need some notation for these rotations. Let $(R,\star)$ denote the group, where R is the set of all possible rotations, and $R_1 \star R_2$ is defined as rotating by R_1 then by R_2. Let G represent the Rubik's Cube.



U: Up, D: Down, L: Left, R: Right, F: Front, B: Back & ' is the inverse.

Proof that a Rubik's Cube is a group

Identity Element
Let R be any rotation, Let e be the Identity. Then
$e \star R = R$, $R \star e = R$
Therefore e is the Identity.

Closure
Let R_1 & $R_2 \in$ G.
For any $R_1 \star R_2$ it will produce a valid move, therefore $R_1 \star R2 \in G$. Thus is closed.

Inverse
Let R be any rotation in G, Let R' be the inverse to R. So $R \star R' = e$ and $R' \star R = e$, this shows that every rotation R has an inverse in G.

Associativity
Let R_1, R_2, $R_3 \in$ G.
$R_1 \star (R_2 \star R_3) = (R_1 \star R_2) \star R_3$
This is clearly true as for example, If you do the move $R \star (R \star U)$ its the exact same as $(R \star R) \star U$.
Therefore its associative and thus is a group.

How Group Theory Helps with Solving Rubik's Cubes

Group theory helps with solving cubes is by helping us find algorithms to solve them, as there is a very large number of permutations it is impossible to solve randomly so we need these algorithms.
These are made by looking at the commutativity of the group. The Rubik's Cube group is non-abelian ie, does not always commute
This property helps with solving them tremendously as we can devise algorithms to swap certain "cubies" (these are what the individual "cubes" are called), being able to swap these like this and not move the rest of the cubies is fundamental to solving a Rubik's cube.

Another way groups helps with solving a cube is with conjugates.
If R_1 and R_2 are two moves then the conjugate of R_1 is equal to $R_2R_1R'_2$
The conjugate has the same function as the original move R_1 but does the move in a different location.
This is very useful for cycling through cubies on an edge for example if you wanted to just move the top 3 corners a conjugate would be very useful here.

Other fact's

Number of permutations
The number of permutations possible for a Rubik's cube is a very large number.
First we need to take the 8 corner pieces so they can be arranged in 8! ways.
Then each corner piece can be arranged in 3^8 ways.
There are 12 edge pieces which can be arranged in 12! ways, then each of them has 2^{12} ways to be arranged.
But only $\frac{1}{3}$ of the permutations have the rotations of the corner cubies correct.
Only $\frac{1}{2}$ of the permutations have the same edge-flipping orientation as the original cube, and only $\frac{1}{2}$ of these have the correct cubie-rearrangement parity. So we end up with

$$\frac{(8!)(3^8)(12!)(2^{12})}{(2)(2)(3)} = 4.3x10^{19}$$

permutations.
God's Number
What is God's number, its the minimum amount of moves necessary to solve any Rubik's Cube from any state.
First we need to make a distinction between the half turn metric and the quarter turn metric.
A half turn is where any turn of 90, 180 or 270 degrees is one move Whereas a quarter turn any twist of the face is said to be a move.
God's Number is exactly 20 for the half turn metric, this was proved by Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge in 2010. It's 26 for the quarter turn metric, this was proved by Tomas Rokicki and Morley Davidson in 2014.
The superflip is the first position proven to require 20 moves (or 26 depending on which metric you prefer) the superflip is the position where all the corners are correct but all the edge pieces are flipped, the superflip actually commutes with every possible move.

NUI Galway
OÉ Gaillimh

School of Mathematics, Statistics and Applied Mathematics
Group Theory Poster Project
2020/2021

Frieze Groups and Mass Housing

Eoghan Breheny, Robert Deery, Ethan Goodfellow

MA3343 Group Theory Poster Project, 2020/2021

Introduction

There exists many philosophies among architects as to what constitutes good architecture. From the artistic vision down to the budget which funds it, dozens of factors are influencing what a structure will look like. With the rise of software such as autoCAD, which allows the modern architect to manipulate 2d geometry to design 3d models, a portal has been opened between what can and cannot be done with respect to exploring new ways in approaching architectural projects. Mass housing, in particular, has created a unique opportunity to combine structural design with group theory in new and interesting ways. We intend to show how group theory, in particular the application of frieze groups, can be employed to relieve the monotony of mass housing in a way that distinguishes each unit from its neighbour while maintaining the fundamental architectural properties of symmetry. This new approach towards repetitive architecture revitalises the stale aesthetics of mass housing, with methods that are precise, efficient and innovative. The thesis of this project is largely built on the work of Jin-Ho Park, as well as Alice V. James, Davd A. James, Loukas N. Kalisperis and Cornelie Leopold.

Principal Objectives

1. Introduce the concept of frieze groups.
2. Discuss the seven types of frieze groups.
3. Relate frieze groups as a solution to the issue of mass housing.

1 Frieze Groups

In design, a frieze is a pattern that regularly repeats along a given direction. Often, these friezes appear horizontally along a wall or bench. In group theory, we imagine that friezes are infinite; extending left and right. All friezes are constructed such that, if they are moved to the left or right by one unit, the overall appearance of the frieze is left unchanged. Also, there may be ways of rotating or reflecting friezes that leave its appearance unchanged. However not all friezes have this property. Each frieze belongs to a frieze group. The elements of the associated frieze group are the actions that leave the frieze's appearance unchanged. There are 5 actions that can be performed on friezes: (1) Translations r, (2) Vertical Mirror M_v, (3) Horizontal Mirror M_h, (4) Half Turn 1/2, and (5) Glide Reflections g. Using these actions we can construct the 7 standard frieze groups.

Mirrors		
Type 1:	XXXXX	*Horizontal & vertical mirrors & half turns (m_h, m_v, 1/2)*
Type 2:	VVVVV	*Vertical mirrors & half turns & glide reflections (m_v, 1/2, g)*
Type 3:	AAAAA	*Vertical mirrors & no half turn (m_v)*
Type 4:	EEEEEE	*Horizontal mirrors & no half turn (m_h)*
No Mirrors		
Type 5:	SSSSSS	*Half turns (1/2)*
Type 6:	qdqdqdq	*Glide reflections & no half turns (g)*
Type 7:	RRRRR	*Translation only*

Table 1: The seven standard frieze types.

2 Frieze Patterns in Pirgí

In 2004, a paper[1] publised by Alice V. James, Davd A. James and Loukas N. Kalisperis explored the façades of friezes in the village of Pirgí on the Greek island of Chios. The paper discovered a series of patterns which "are used to create a lively geometry, ranging from the straightforward to the complex, to give each house its distinctive identity, its own unique face to display to the world. While analyzing the frieze designs, the authors discovered that the frieze artists intuitively obey a unique set of color-reversing rules."

2.1 Notes

The paper offers three important findings: *(1)* that the geometries used in Pirgí obeyed the laws of frieze theory; *(2)* that all seven frieze types were used across the decorations of the village (see Figures 1-7); *(3)* and that frieze groups offers a unique way to establish a sense of diversity that works best when the structures are uniform and even identical.

2.2 Examples

Figure 1: Type 1, Horizontal and vertical mirrors, half turns ($m_h, m_v, 1/2$)

Figure 2: Type 2, Vertical mirrors, half turns, glide reflections ($m_v, 1/2, g$)

Figure 3: Type 3, Vertical mirrors and no half turns (bottom frieze) (m_v)

Figure 4: Type 4, Horizontal mirrors and no half turns (m_h)

Figure 5: Type 5, Half-turns and no mirrors (1/2)

Figure 6: Type 6, No mirrors, glide reflections (g)

Figure 7: Type 7, Translation only, marching right triangles

3 Modern Solutions to Modern Problems

Evidently, if you were to hold these examples up to a mathematical lens, you would undoubtedly find that these patterns are not exactly obeying the laws of group theory; this is primarily due to the fact that these façades were hand-painted and likely did not use strict measurements. However, an exact rendition of these patterns has been made infinitely easier since the conception of applications like autoCAD and ProE.

3.1 Mass Housing

As hinted in the introduction, the practice of architecture is subjective, in this project we consider the design of mass housing as the primary subject since it has more limitations (e.g. government funded, generally attached/semi-detached, relatively small units) and the crucial property of being repetitive. The fundamental application of frieze groups will be in making the façade of housing less repetitive by combining common elements in housing to subvert the generic, dissatisfying, monotonous traits typically associated with it in a cheap and efficient way.

3.2 The Work of Jin-Ho Park

In 2017, Jin-Ho Park published a paper, entitled "Subsymmetries for the Analysis and Design of Housing façades[2]," in which he sets forth an innovative approach in applying frieze groups (and combinations of their subsymmetries) to repetitive rows of housing. The application process involved using computer software to generate a 3-dimensional model of the streetscape. As mentioned already, not only does Park employ the concepts of freize theory but also introduces a "combinatorial" approach in which he combines different constituents of symmetry and subsymmetries. In his own words, "by using all or just some of the subsymmetry principles, the application results in a huge number of compositional possibilities."

3.3 Park's method

1. A series of 2-dimensional diagrams are created with respect to the frieze groups[3]. These are unique elements of the façade (not the fundamental building structure) such as doors, partial walls, windows, etc., as seen in Table 2 below:

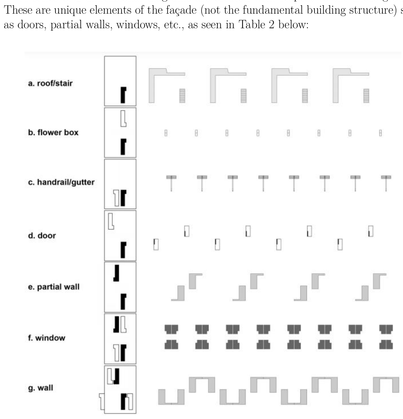


Table 2: Seven frieze groups with design elements: a detailed example of how the complete set of frieze groups is used to design the façade

2. These elements are then *uniformly* superimposed on each other without any variation in subsymmetries in Figure 8:

Figure 8: Final design where all elements are superimposed to form a housing façade

This creates a typical uniform housing façade. As Park notes, "Proper positioning of each symmetric element produces an orderly superimposed pattern of seven distinct symmetry operations. When overlaid together, separate building elements dissolve in a façade, having no meaning as separate rules of their juxtaposition in the entire façade, and making each underlying layer invisible."

3. Park then renders the façade elements in 3-d space, in which the underlying geometry is "not revealed," or subdued, due to its inherent asymmetrical design - offering a "dynamic look and aesthetic variety" regardless of the underlying uniform layout of subsymmetries.

Figure 9: Three-dimensional computer model is depicted on a streetscape

4. Finally, Park begins to vary the subsymmetries of the façade: "Depending on how different parts of elements are superimposed on the façade, the expression of the final design will be different, even though it may look as if various elements are permutated, shifted, and positioned. When combined with different colors and materials, dynamic views of the alternating façades are created... In addition, a few elements may be removed, or a few subsymmetry principles left unused, thereby destroying the overall symmetry of the façade." Park presents four unique iterations[4] of the same underlying principle in Figure 10:

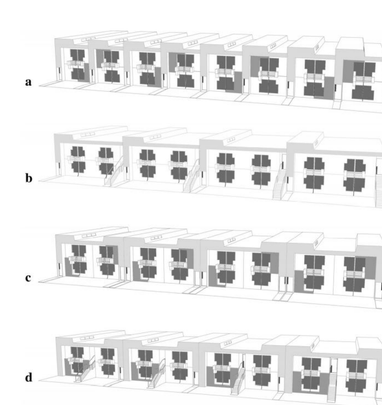


Figure 10: Four possible façade designs in that a few elements are removed or a few subsymmetry principles are not used. Although they appear similar, they are different from the ways that the principles are applied

4 Conclusion

- Group theory, and in particular the concept of frieze groups, has huge importance in structural and façade design.
- Although it has manifested in the past, modern technology now allows frieze patterns to be rendered with precision in complex and innovative ways.
- The first technological procedure for the technical application of frieze groups in architectural design was proposed (very recently) by Jin-Ho Park, whose method we have summarised and explored.
- This method can be universally applied to resolve the monotony of mass housing in a cheap, efficient way.

School of Mathematics, Statistics and Applied Mathematics
Group Theory Poster Project
2020/2021

References

[1] A. James, D. James, L. Kalisperis, A Unique Art Form: The Friezes of Pirgi (LEONARDO, Vol. 37, No. 3, 2004) p. 235.

[2] J. Park, Subsymmetries for the Analysis and Design of Housing Facades (Nexus Network Journal, 2017).

[3] *"In Fig. 9a, the pattern is shown rooted at the successive translation of asymmetric motifs by a distance: a wall and a stair. Figure 9b portrays a pattern of flower boxes. This example illustrates where a window is translated in the line of axis and then mirrored to generate the pattern. Paired, with corner elements, windows establish a rhythm across the units. In Fig. 9c, a gutter and a lanai handrail are mirrored with a subsequent translation. Figure 9d isolates the door and aligns it along a glide reflection. Here again, a decorative lighting element is attached to remove the symmetry of the door rectangle. The motifs in Fig. 9e are paired in a half turn. This forms a partial wall boundary of a unit of row houses. Figure 9f presents a window motif in Fig. 9b that is mirrored in a half-turn and reflected in an axis line. In Fig. 9g, a wall is half-turned and reflected in two mirrors at right angles. This forms the boundary configuration of all eight row house units. All the above generates a unique pattern in forming a fac¸ade of rows of houses."* J. Park, Subsymmetries for the Analysis and Design of Housing Facades (Nexus Network Journal, 2017).

[4] *"The first model of these (Fig. 12a) is a row of houses, where each unit has a clerestory window. The exterior stair is removed and the front door for each row house is placed on the ground level. The pattern for the slightly projecting wall is also changed. In this model, the Pma2 and P1a1 subsymmetries of the frieze groups are removed. In the second model (Fig. 12b), the projecting wall pattern is removed and the exterior stair is relocated. Two units are stacked together so that the two units appear to be a single building. In this model, the Pma2 and P112 subsymmetries of the frieze groups are removed. In the third model (Fig. 12c) each unit has its own roof but the forms reflect each other horizontally. The front door is relocated and the exterior stair is removed. In this model, the P1a1 and P111 subsymmetries of the frieze groups are removed. The fourth model (Fig. 12d) removes the projecting wall of the upper floor. The roof form is reflected and the exterior stair is translated. In this model, the Pma2, P112, and P111 subsymmetries of the frieze groups are removed."* J. Park, Subsymmetries for the Analysis and Design of Housing Facades (Nexus Network Journal, 2017).

[5] C. Leopold, Geometry Concepts in Architectural Design (ReseachGate).

[6] Wikipedia (2020) Group Theory, available: *https : //en.wikipedia.org/wiki/Group_theory* (accessed 18 November 2020).