Functional Analysis

Manish Kumar, Daniel Halmrast

University of California, Santa Barbara

Introduction

The core idea in functional analysis is to treat functions as 'points' or 'elements' in some sort of abstract space, so that instead of working with individual functions we work with the structure of the space (as the tradition in classical analysis), we deal with functions as points in a space endowed with some kind of overall structure. This viewpoint, was an integral step in the process of transferring familiar concepts in finite-dimensional Euclidean space to (typically infinite-dimensional) 'function spaces'.

Basics

We will be concerned with complex Hilbert spaces. A Hilbert space (H) is defined as a vector space over $\mathbb{C}$, with an inner product such that it is complete with respect to the inner product. Specifically we will be looking at the $L^2(X, \mu)$, this is the Hilbert space of the square integrable functions, with associated measure μ. Note the norm in L^2 is given by:

$$||f||_{L^2} = \int |f|^2 d\mu$$

This is the familiar state space of a quantum particle, contained in a region X.

Let $T : X \longrightarrow Y$ be a linear map between normed linear spaces. T is called a bounded linear operator if $\exists C$ such that

$$||Tx||_Y \leq C||x||_X$$

$\forall x \in X$. Now suppose $\mathscr{H}$ and $\mathscr{K}$ are hilbert spaces and $A : \mathscr{H} \longrightarrow \mathscr{K}$ a bounded linear operator. There is always a unique A^* such that:

$$\langle Ah, k\rangle_{\mathscr{K}} = \langle h, A^*k\rangle_{\mathscr{H}}$$

A^* is called the adjoint of A

Bounded Linear operators

In this section we will define spectrum on bounded linear operators. Let $T \in \mathscr{B}(X)$ ($T : X$ bounded), we say $\lambda \in \mathbb{C}$ is an eigenvalue, if for some x we have $Tx = \lambda x$.

Theorem: If $T \in \mathscr{B}(\mathscr{H})$ is self adjoint, then either $||T||$ or $-||T||$ is an eigenvalue. Note $||T|| = Sup(|\langle Tx, y\rangle| : ||x|| = ||y|| = 1)$. The eigenvalues are real and the eigenvectors for distinct eigenvalues are orthogonal.T is said compact if it is the limit of finite rank operators

Preliminary Spectral Theorem: Let T $\neq$ 0 be a self-adjoint, compact operator in $\mathscr{B}(\mathscr{H})$, there exists a finite or countably infinite set of eigenvectors g_n, with corresponding eigenvalues λn such that

$$Tx = \Sigma\lambda_n\langle x, g_n\rangle g_n$$

When we move from compact operators to Banach algebras, the concept of eigenvalue gets generalized to the spectrum.

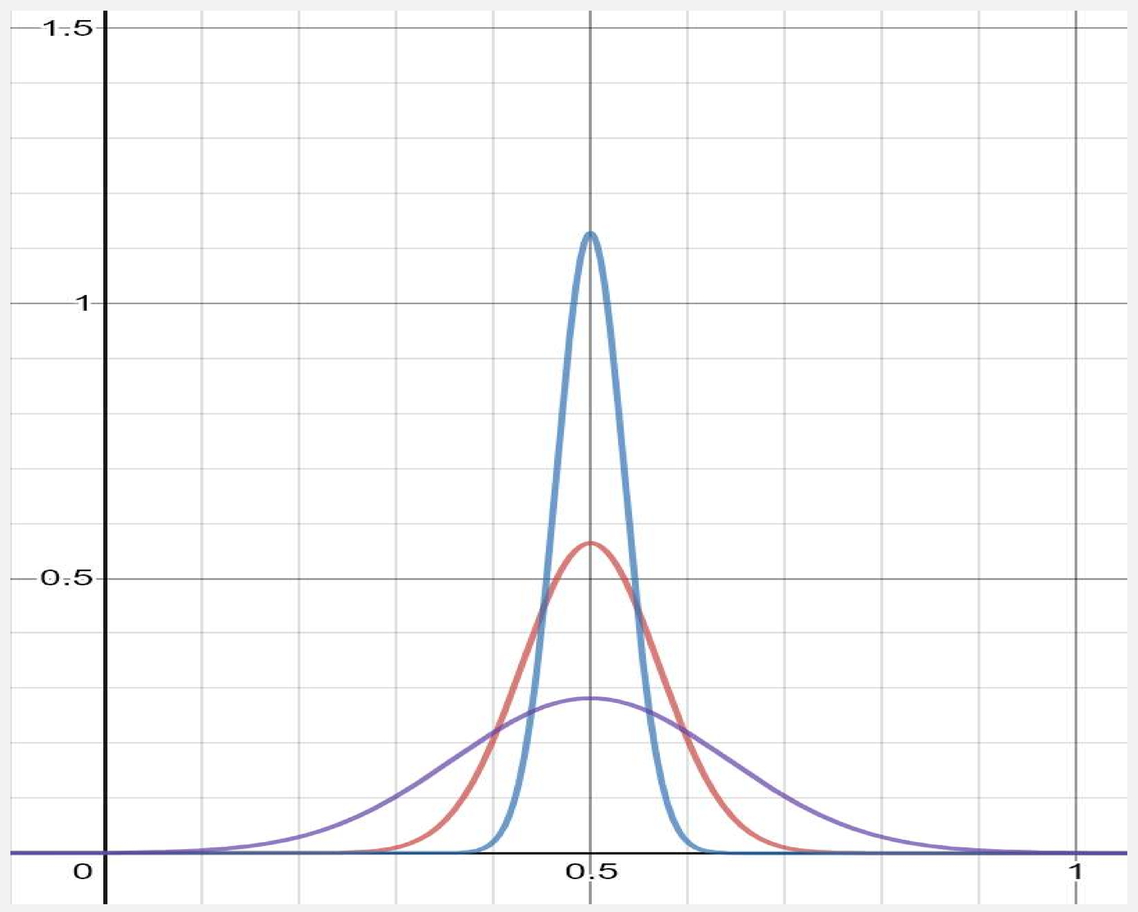


Figure: functions h_n approximating the eigenfunction for $\lambda = 0.5$

Spectrum

Spectrum of T: Let $T \in \mathscr{B}(X)$ be linear. The set of complex numbers λ such that $T - \lambda I$ is not invertible, is called the spectrum.

A bounded linear operator on a Hilbert space is invertible iff it is bounded below and has a dense range. So if either (or both) of those two conditions are not satisfied for $T - \lambda I$ then λ is in the spectrum. So we have:

Approximate point spectrum $\sigma_{ap}(x)$: $\{\lambda : T - \lambda I$ is not bounded below$\}$, this includes the eigenvalues.

Compression spectrum $\Gamma(x)$: $\{\lambda : T - I$ does not have a dense range$\}$

Spectral mapping theorem: Suppose $\mathscr{A}$ is a unital Banach algebra and $A \in \mathscr{A}$ and P is a polynomial. We have

$$\sigma(P(A)) = P(\sigma(A))$$

Our goal now is to generalize this to all continuous functions. For this we consider the set $\mathscr{M}_{\mathscr{A}}$ of *homomorphisms from $\mathscr{A}$ to $\mathbb{C}$ (in $\mathscr{B}(\mathscr{H})$ the * is just the adjoint).

Example:Position operator

Consider the operator M_x, multiplication by x. $M_x \in L^2[[0, 1]]$. Clearly, this operator has no eigenvalues, but it has approximate point spectrum $\sigma_{ap} = [0, 1]$. A key idea about $\lambda \in \sigma_{ap}(M_x)$ is that $(M_x - \lambda I)h_n \rightarrow 0$ for some sequence of normalized functions h_n. An example of such a sequence is :

$$h_n = \sqrt{\frac{n}{\pi}} e^{-n(x-\lambda)^2}$$

(If this did have a limit, it would be the delta function)

Gelfand Transform

If $\mathscr{A}$ is a commutative unital Banach algebra, then we can define a map:

$$\Gamma : \mathscr{A} \longrightarrow C(\mathscr{M}_{\mathscr{A}})$$

Theorem:If $\mathscr{A}$ is also a C^* algebra then Γ is a isometric-*isomorphism. Although we are limited by the commutativity requirement in the last theorem, we can generate a commutative C^* algebra, with $\{A, A^*, I\}$ for any $A \in \mathscr{A}$. The next result will be the central result of this poster, there is an isomorphism from $\mathscr{A}$ (which is a mysterious object) to $C(\sigma(A))$ (which are just continuous complex functions).

Theorem:Suppose $\mathscr{A}$ is some singly generated, commutative, unital C^* algebra with $\mathscr{A} = C^*(A)$ for some A which is necessarily normal. Then there is a unique * isomorphism between $\mathscr{A}$ and $C(\sigma(A))$, and maps A to the identity function on $\sigma(A)$.

Continuous spectral mapping

Theorem: Given a normal operator A as above, we have

$$\sigma(f(A)) = f(\sigma(A))$$

This theorem gives constraints on the spectra of operators based on their algebraic properties.

- $A^* = A$ iff $\sigma(A) \subset \mathbb{R}$
- $A^* = A^{-1}$ iff $\sigma(A) \subset \partial\mathbb{D}$
- $A^2 = A$ iff $\sigma(A) \subset \{0, 1\}$

References

[1] B. MacCluer.
Elementary Functional Analysis.
Springer, 1st edition, 2009.

Representation Theory

Anna Wade and Jasmine Gutierrez
Directed Reading Program, Mathematics
University of California, Santa Barbara

$$\begin{tikzcd} V \arrow[r, "\alpha"] \arrow[d, "\varphi(g)"'] & W \arrow[d, "\psi(g)"] \\ V \arrow[r, "\alpha"] & W \end{tikzcd}$$

Figure 1: Intertwiners of a representation/ between representations

Introduction

Representation Theory is a branch of mathematics that links Group Theory, Linear Algebra and Abstract Algebra. It was born in 1896 in the work of German mathematician F.G. Frobenius. Throughout the program we have been examining what it means to be a representation, sub representation, irreducible representation, and more

For some background, we start with the idea of Groups. In representation theory, we are trying to represent topics in abstract algebra with linear algebra. This way, it is more easily understood. A **representation of a group G** on a vector space V

1) A way for the group to act on a vector space

   $\phi : G \cdot V \to V$

   $(g,v) \mapsto g \cdot v$

   satisfying:

   $\forall v \in V, e \cdot v = v$; $\forall g \in G, \forall v_1,v_2 \in V, \forall c \in \mathbb{C}, g\cdot(cv_1 + v_2) = c\cdot g\cdot v_1 + g\cdot v_2$; $\forall g,h \in G, \forall v \in V, g\cdot(h\cdot v) = (g\cdot h)\cdot v$

2) A group homomorphism

   $\rho: G \to GL(v)$; $GL(v)$:{ invertible linear transformations $V \to V$}

   $\rho(g_1) \cdot \rho(g_2) = \rho(g_1,g_2)$

Examples of Groups:

- S_n = { invertible functions from a set of size n} : (1 3) (2 4)
  (1 2 3 4)
- $\mathbb{Z}/n\mathbb{Z}$ - group {[0],[1],...[n-1]} under addition modulo n

We start by introducing the concept of an **Associative Algebra**, which can be defined as a vector space V, where multiplication is defined by $a,b \to ab$, $a,b \in V$, and there is an identity element such that $1*a=a$ for all $a \in V$

Next we can define a **Representation** of an associative algebra is a vector space with a homomorphism $\rho \to \mathrm{End}V$ (a linear map preserving multiplication and unit)

A map $\rho: A \to \mathrm{End}V$

$\rho(a+b)=\rho(a)+\rho(b)$

$\rho(ab)=\rho(a)\rho(b)$

$\rho(c*a)=c*\rho(a)$, where c is a scalar

- **Subrepresentations:** of V is a subspace $U \subset V$ which is invariant under all the operators $\rho(a) : V \to V$, $a \in A$
- A representation is **irreducible** if it has not proper subrepresentations
  - Every representation has an irreducible subrepresentation

A map between representations is an **intertwiner** (Figure 1). It can be thought of as a linear map that commutes under the group operation. If both representations are irreducible, then an intertwiner only exists if the two representations are equivalent, which brings us to Schur's Lemma.

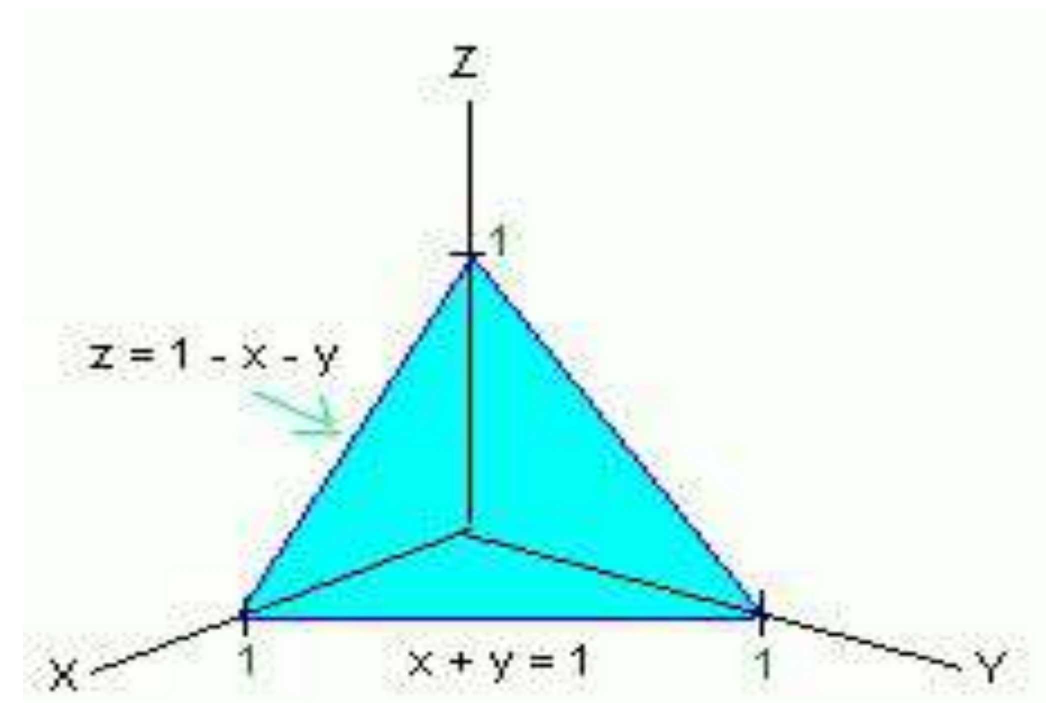


Figure 2: symmetries of space represented by a unit triangle

Schur's Lemma: Let V_1, V_2 be representations of an algebra A over any field F (which need not be algebraically closed)

Let $\phi : V_1 \to V_2$ be a non zero homomorphism of representations. then:

(i) if V_1 is irreducible, ϕ is injective

(ii) if V_2 is irreducible, ϕ is surjective

Thus, if both V_1 and V_2 are irreducible, ϕ is an isomorphism.

If we had a representation where every intertwiner was invertible, then it would be an irreducible representation.

Proof:

(i) The Kernel of ϕ is a subrepresentation of V_1. Since $\phi \neq 0$, the subrepresentation cannot be V_1. So be irreducibility of V_1, we have Kernel=0

(ii) The image of ϕ is a subrepresentation of V_2. Since $\phi \neq 0$, the subrepresentation cannot be 0. So be irreducibility of V_2, we have Image=V_2

Examples:

- D_2n- {symmetries of a n-gon} (groups representations model symmetries of space) (Figure 2)
- $\mathbb{Z}$ rep on $\mathbb{C}^2$
- **Group Algebra:** The group algebra A=k[G] of a group G is an example of algebras over k, where k is the field. k[G] is the set of all linear combinations of elements in G with coefficients in k. The group algebra respects addition, multiplication and scalar multiplication.

Completely Decomposable Representations: a semisimple representation of A (an algebra) is a direct sum of irreducible representations.

We can use Schur's Lemma to classify sub-representations in finite dimensional semisimple representations.

Objective

We want to "build" everything out of **irreducible representations**, but to do this we need the help of Maschke's Theorem.

Maschke's Theorem:

Let G be a finite* group and let k be a field whose characteristic does not divide |G|. Then:

(i) The algebra k[G] is semisimple

(ii) There is an isomorphism of algebras φ:k[G]→□$_i$EndV_i defined by g→□$_i$g|v_i where V_i are irreducible representations of G. In particular, this is an isomorphism of representation of G. In particular, this is an isomorphism of representations of G (where G acts on both sides by left multiplication). Hence, the regular representation k[G]decomposes into irreducibles as □$_i$ dim(V_i)V_i, and one has the "sum of the squares formula"

$|G|=\sum \dim(V_i)^2$

*note: it is important that G is a finite group because if G were infinite, we would have an infinite sum for |G|

Importance:

Through this theorem, we can take any finite dimensional group representation and decompose it into a direct sum of irreducible representations. In conclusion, Maschke's theorem shows how to generate semisimple Artinian rings.

Conclusion

While there is still much to learn in this field, we have touched base on some of the main building blocks of Representation Theory. This subject is important because it reduces problems in Abstract Algebra to Linear Algebra. The purpose of Representation Theory is to understand how a group G operates on a vector space V. Because of this, we have furthered our understanding of related topics including Group Theory and Linear Algebra. Group theory is applied to subjects such as, Mathematical Physics, Engineering, and Mathematical Chemistry.

Literature Cited

Introduction to Representation Theory -
Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, Elena Yudovina
With historical interludes by Slava Gerovitch

Acknowledgements

Thank you to Ashwin Trisal for his aid in both training and teaching. We greatly appreciate this opportunity to be mentored by you. We also thank the assistance of The Directed Reading Program for giving us this opportunity and for helping with media and supplies.

How to put your topological phase on a torus

Zishuo Zhao, Graduate Student Mentor: Colleen Delaney

UCSB

Motivation: topological quantum computing

The theoretical background of quantum computation with anyons is unitary modular tensor category (UMTC) theory and braid group representations. The theory of quantum computing with bilayer anyons and defects is given by representations from a unitary G-crossed braided fusion category (UGxBFC).

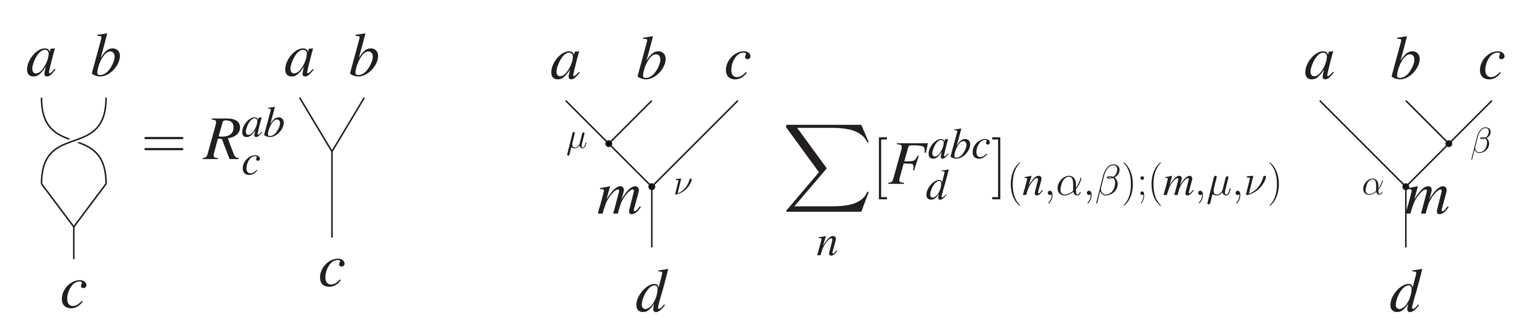
Quantum gates generated by exchange of anyons and defects come from representations of the n-strand braid group $\mathcal{B}_n$.

$$\mathcal{B}_n = \langle \sigma_1, \sigma_2, \dots \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| > 2\rangle$$

Background

In practice, we work with the algebraic data $\{N_c^{ab}, R_c^{ab}, F_d^{abc}\}$ for a UMTC $and\{N_Z^{XY}, R_Z^{XY}, F_W^{XYZ}, \mu, \eta\}$ for a UGxBFC [1].

$$a \otimes b = \bigoplus_c N_c^{ab}\, c$$



The modular data of a UMTC

The modular data are the matrices S, T

$S_{ab} = \frac{1}{\mathcal{D}}$ a b, and $T_{ab} = \theta_a\delta_{ab}$, where $\theta_a = \frac{1}{d_a}$ a $= \sum_c \frac{d_c}{d_a} R_c^{aa}$

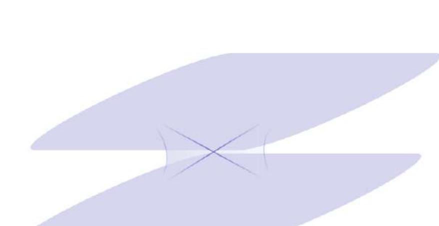
These matrices satisfy the relations below:

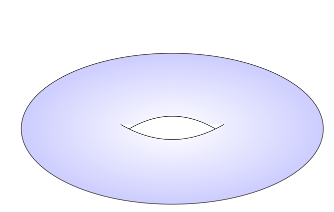
$$(ST)^3 = \Theta C \tag{1}$$
$$S^2 = C \tag{2}$$
$$C^2 = I_n \tag{3}$$

Bare bilayer defect data [3] $\qquad R_{c\boxtimes c^*}^{X_1X_1} = \theta_c \quad [F_{X_1}^{X_1X_1X_1}] = S$

Main idea: bilayer defects "create genus"

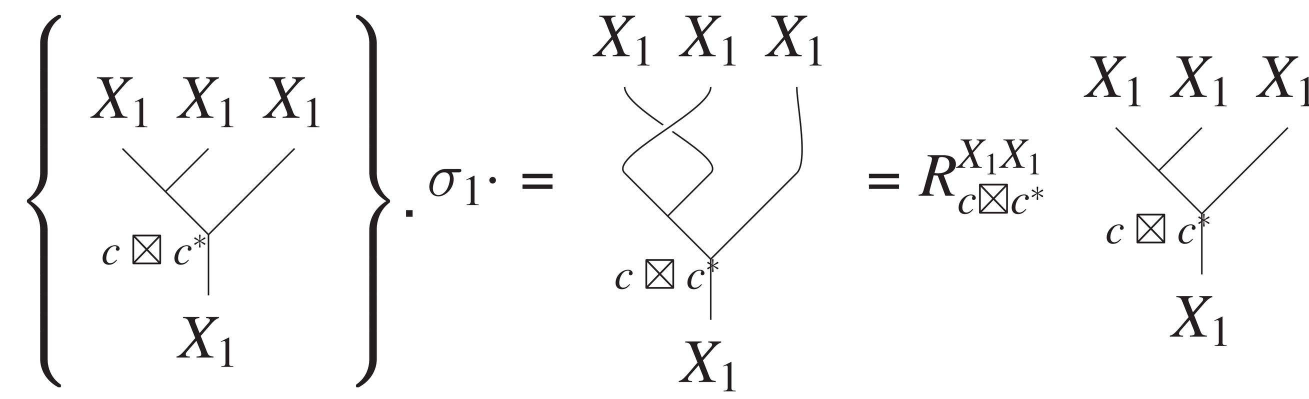
The physical interpretation of our result says that braiding 4 bilayer bare defects is equivalent to modular transformations of the monolayer vacuum states on a torus.



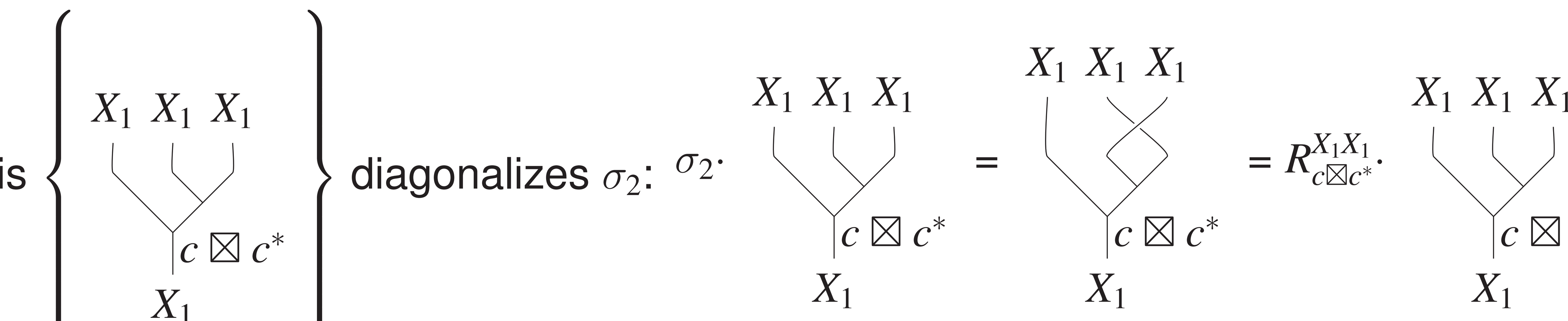


Quantum gates from braiding bilayer defects

Using the algebraic theory of bilayer defects [3], we compute the matrix representation of $\mathcal{B}_3$ on $V_{X_1}^{X_1^{\otimes 3}}$ with respect to the basis



The basis



Using the F matrix $F_{X_1}^{X_1X_1X_1}$ as the change of basis, we can write the matrix of $\sigma 2$ with respect to the left associated fusion trees as $(F_{X_1}^{X_1X_1X_1})^{-1}R(F_{X_1}^{X_1X_1X_1})$.

The image of the representation is then given by

$$\rho(\mathrm{B}_3) = \langle \rho(\sigma_1), \rho(\sigma_2)\rangle \simeq \langle T, S^{-1}TS\rangle$$

Proposition

Let $\mathfrak{C}$ be a UMTC. The image of the B_3 representation $V_{X_1}^{X_1^{\otimes}}$ coming from the GxBFC $(\mathfrak{C} \boxtimes \mathfrak{C})_{\mathbb{Z}_2}^{\times}$ is projectively equal to the image of the modular representation of $\mathfrak{C}$.

Proof.

It is clear that $\langle T, S^{-1}TS\rangle \subset \langle S, T\rangle$. For the other direction, since $(ST)^3 = \Theta C$,we have $(STS)(TST) = \Theta C$ Since $C^2 = I_n$, multiply C both sides gives us $(CSTS)(TST) = \Theta I_n$ (1).
Since $S^2 = C$, $S^{-1} = SC = CS$. Plug in to (1) we have $(S^{-1}TS)(TST) = \Theta I_n$, thus $(TST) = \Theta(S^{-1}TS)^{-1}$.
So we have $S = \Theta T^{-1}(S^{-1}TS)^{-1}T^{-1}$. Thus the two group are projectively equal. □

References

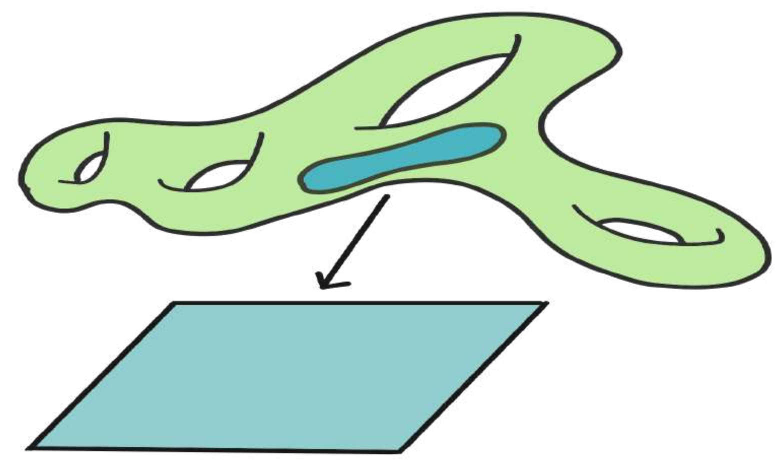
[1] M. Barkeshli, P. Bonderson, M. Cheng, Z. Wang. *Symmetry, defects, and gauging of topological phases.* arXiv preprint. 1410.4540v2. (2014).

[2] M. Barkeshli, C. M. Jian, X. L. Qi, *Genons, twist defects, and projective non-Abelian braiding statistics.* Phys. Rev. B, Vol. 87, No. 045130. (2013).

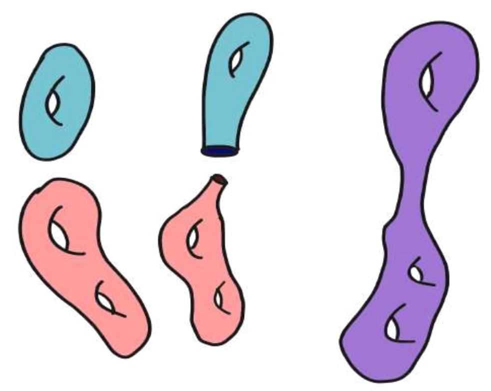
[3] C. Delaney. On the categorical approach to symmetry, topological order, and quantum information. Ph.D. Dissertation. (2019).

HYPERBOLIC SURFACES AND THE MODULAR GROUP

Surfaces



Definition (Surface): A surface is a metric space X, such that every point in X has a neighborhood that is homeomorphic to the plane. A surface is nonorientable if it contains a mobius band; and orientable otherwise.

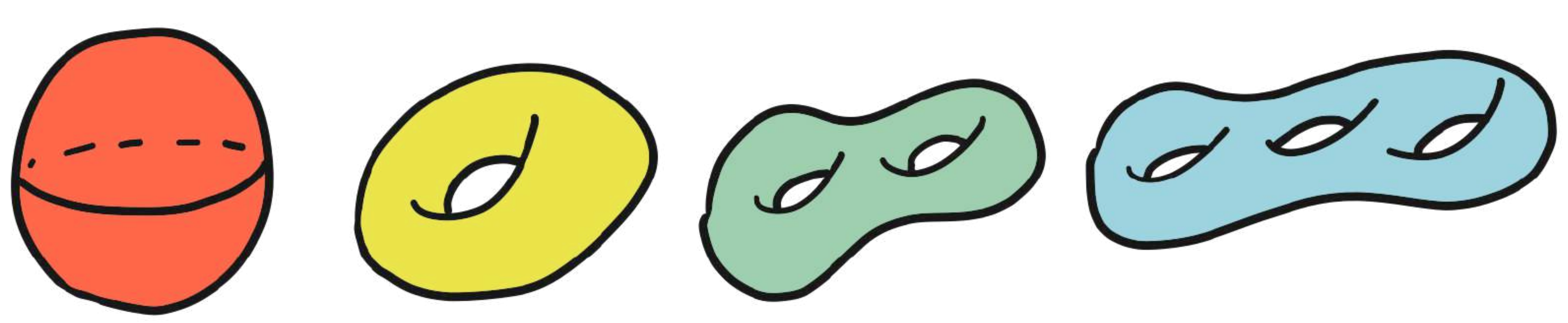


Definition (Connect Sum): The connect sum S#F of two surfaces S, F is obtained by removing a disk from each and identifying the boundaries by the gluing construction (below). A surface of genus g is surface from g connected sum operations of the torus.

Euler Characteristic: Suppose a surface of genus g is decomposed into polygons, then faces - edges + vertices = 2 - 2g

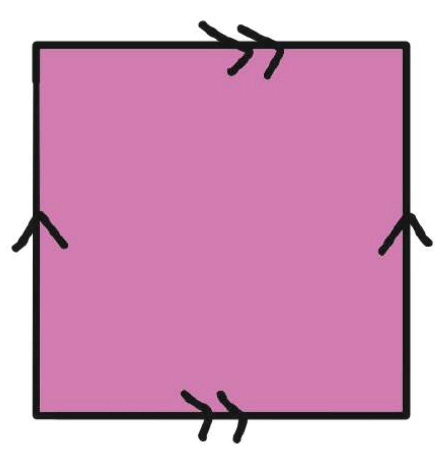
Classification

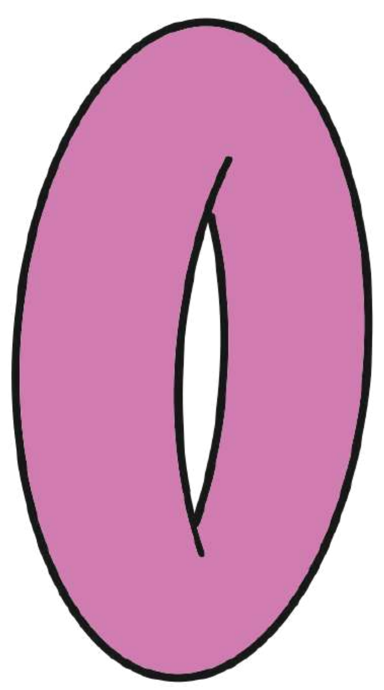
Every compact orientable surface is homeomorphic to the surface of genus g, for some g.



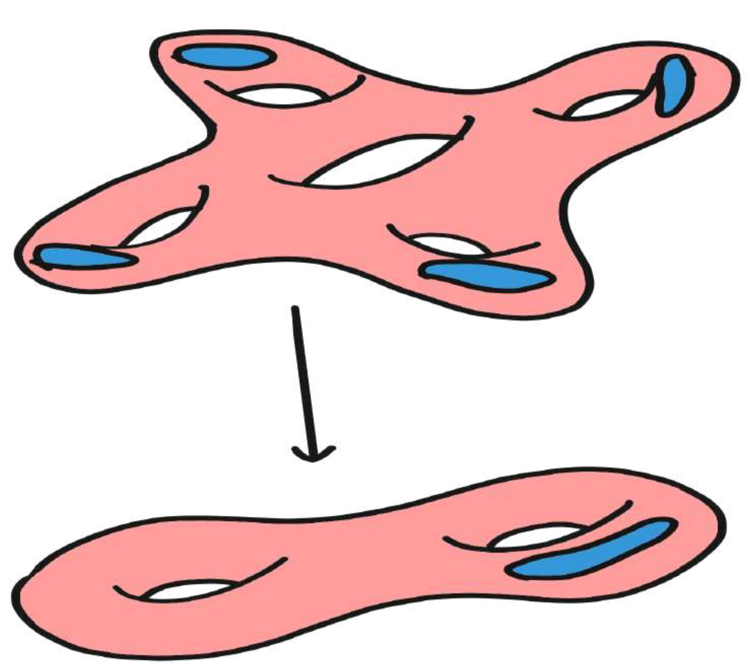
Gluings and Group Actions

One way of making surfaces is by gluing together the sides of a planar region, and giving the result the quotient topology. Another way of making a surface is taking the quotient of a nice (free, properly discontinuous) group action on the plane. This is equivalent to the gluing construction on a fundamental domain





Definition (Fundamental Domain): If G is a group acting on a space X, a fundamental domain for the action of G is a subset of X containing exactly one point of each orbit.



Covering Spaces

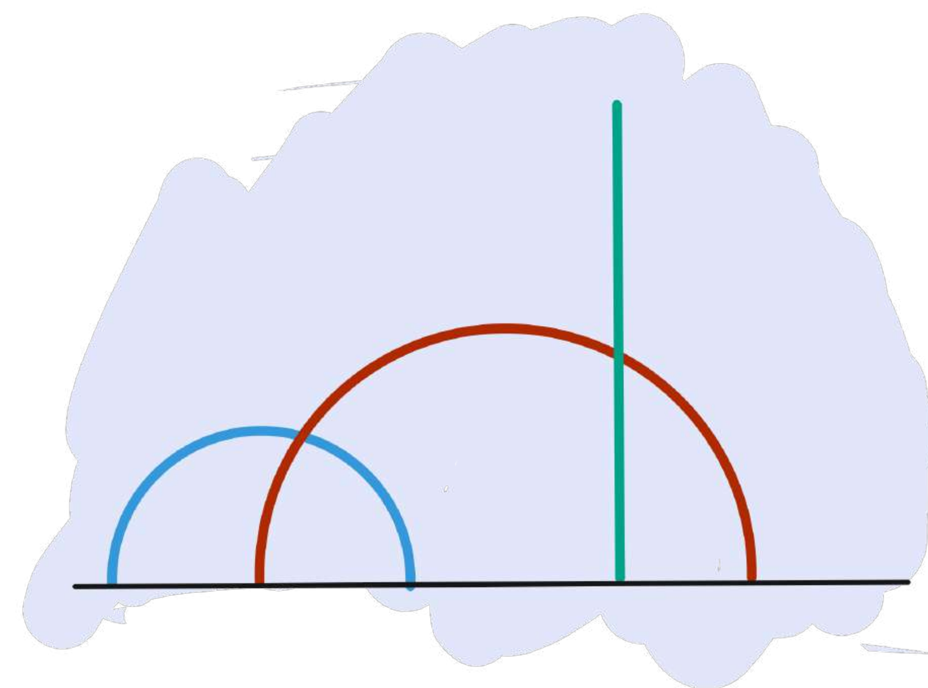
Definition: E:X -> X' is called a covering map if every point in X has a neighborhood that is evenly covered, and in X' is said to be a covering space of X. (U is evenly covered if the preimage consists of a countable disjoint union of sets homeomorphic to U)

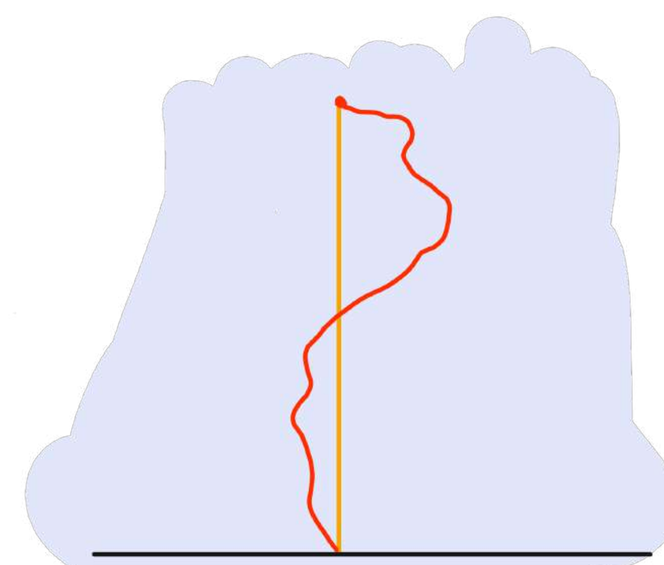
Hyperbolic Space

The upper half plane model $\mathbb{H}^2$, defined to be $\{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. In this model, the length of a curve γ is

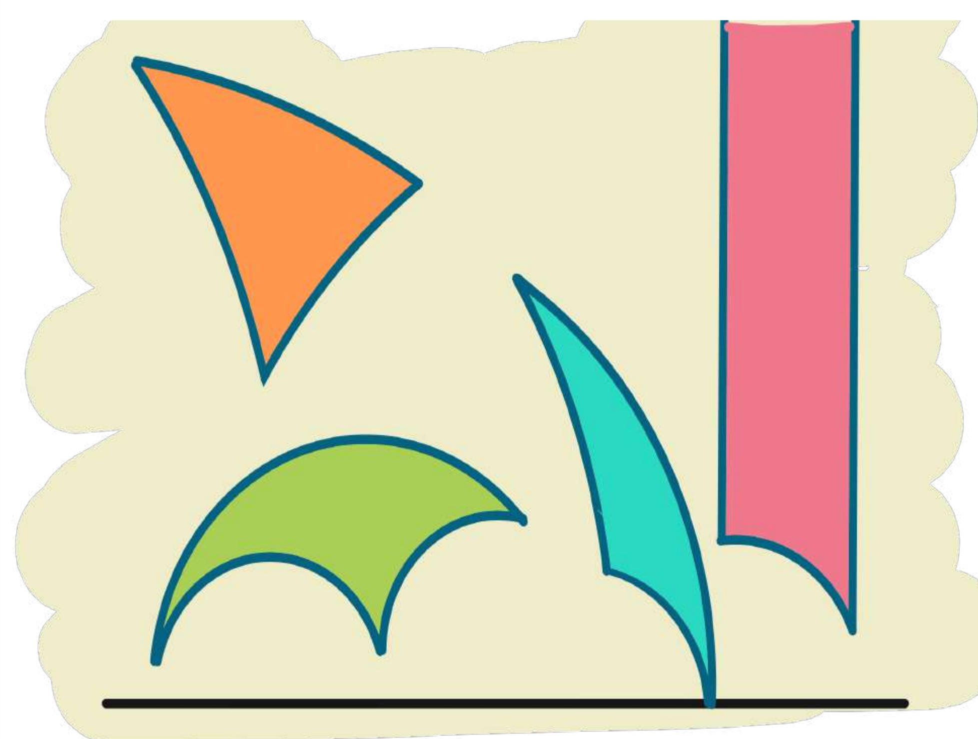
$$\mathrm{Length}(\gamma) = \int_\gamma \frac{ds}{y}$$

Definition(Geodesic): The shortest path between two points is a geodesic. The geodesics of the upper half plane model are vertical line segments or arcs of circles centered on the real axis.





Geodesic (orange) and non-geodesic (red)



Hyperbolic Triangles

A (geodesic) polygon is a simple closed path made from geodesic segments. A triangle is a geodesic polygon with 3 sides.

Angle sum and area relation of triangles: Let a,b,c be the inner angles of a triangle T, then Area(T) = pi - (a+b+c)

An *ideal vertex* of a hyperbolic triangle lies at infinity or on the real axis in this model.

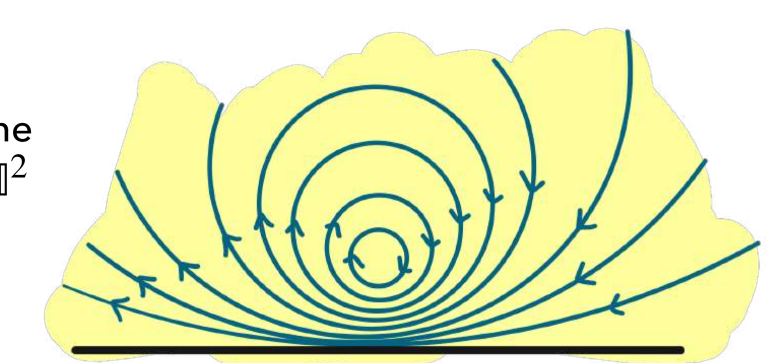
Isometries

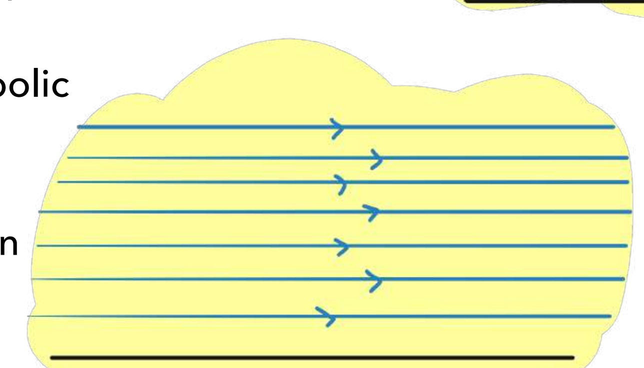
Isometries of Hyperbolic space are given by Mobius transformations of the upper half plane. There are three types of hyperbolic isometries: elliptic, parabolic and hyperbolic.

Definition: A Mobius transformation $f\colon \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ is a map of the form $f(z) = \dfrac{az+b}{cz+d}$ with $a,b,c,d \in \mathbb{C}$, $ad-bc \neq 0$

The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is associated to the Mobius transformation $f(z) = \frac{az+b}{cz+d}$. Any scalar multiple of this matrix represents the same Mobius transformation.

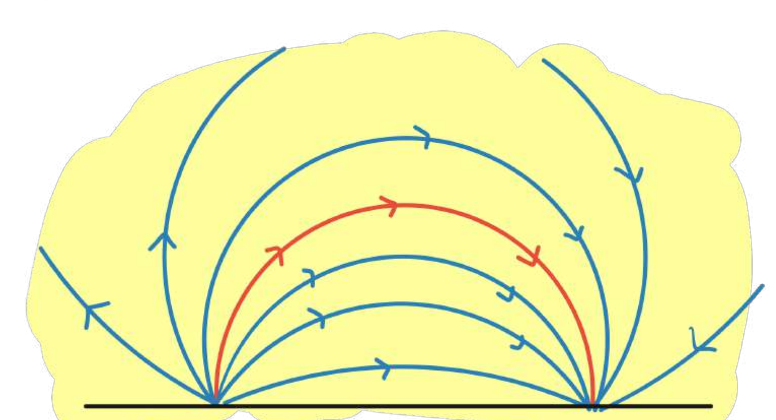
Elliptic: Has one fixed point in $\mathbb{H}^2$ not on the boundary.





Parabolic: Has one fixed point at infinity or on the boundary

Hyperbolic: Has two fixed points at infinity and/or on the boundary.



The Modular Group

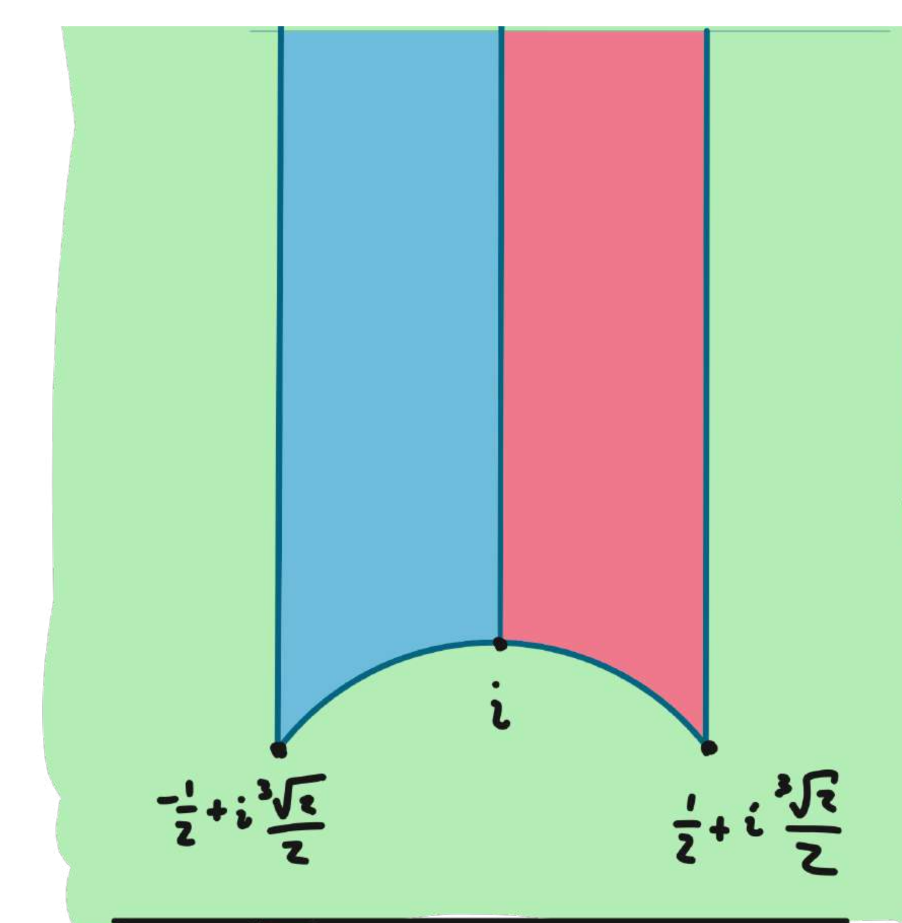
SL(2,Z) is the group of 2x2 matrices with integer entries and determinant 1. PSL(2,Z) is the quotient of SL(2,Z) by {I,-I}.

Generators: SL(2,Z) is generated by the matrices S, T below.

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Fundamental Domain for PSL(2,Z)

Half the fundamental domain of this surface can be found from the fixed points of S, T, and ST. These fixed points are at ∞ i, -½ + i (2)^(⅓)/2. After finding these fixed points the fundamental domain is the triangle with verticies ∞ , ½ + i (2)^(⅓)/2, -½ + i (2)^(⅓)/2 form the fundamental domain of the modular surface.



The Modular Surface

$$\mathbb{H}^2/\mathrm{PSL}(2,\mathbb{Z})$$

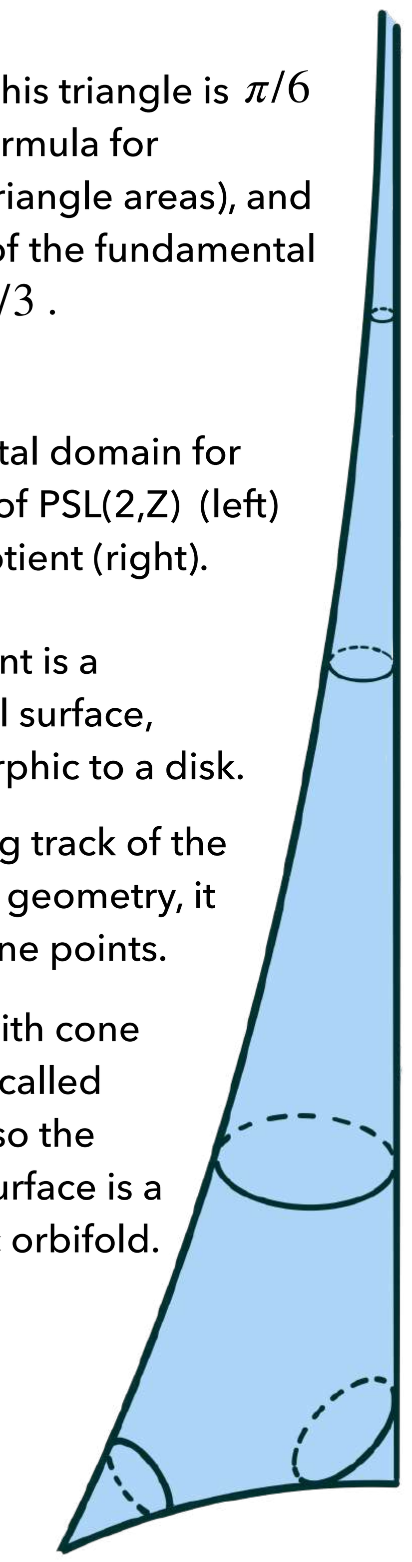
The area of this triangle is $\pi/6$ (using the formula for hyperbolic triangle areas), and so the area of the fundamental domain is $\pi/3$.

Fundamental domain for the action of PSL(2,Z) (left) and its quotient (right).

The quotient is a topological surface, homeomorphic to a disk.

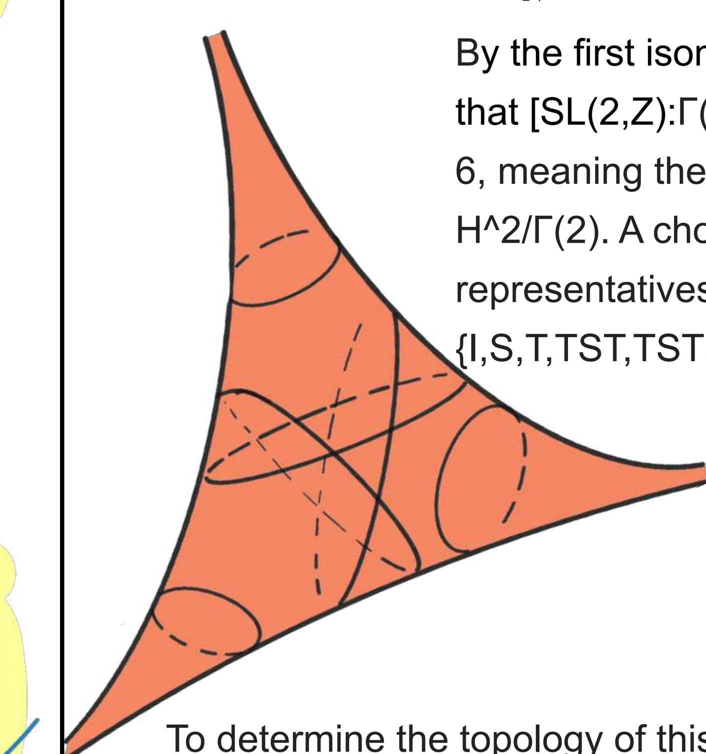
But keeping track of the hyperbolic geometry, it has two cone points.

Surfaces with cone points are called orbifolds, so the modular surface is a hyperbolic orbifold.



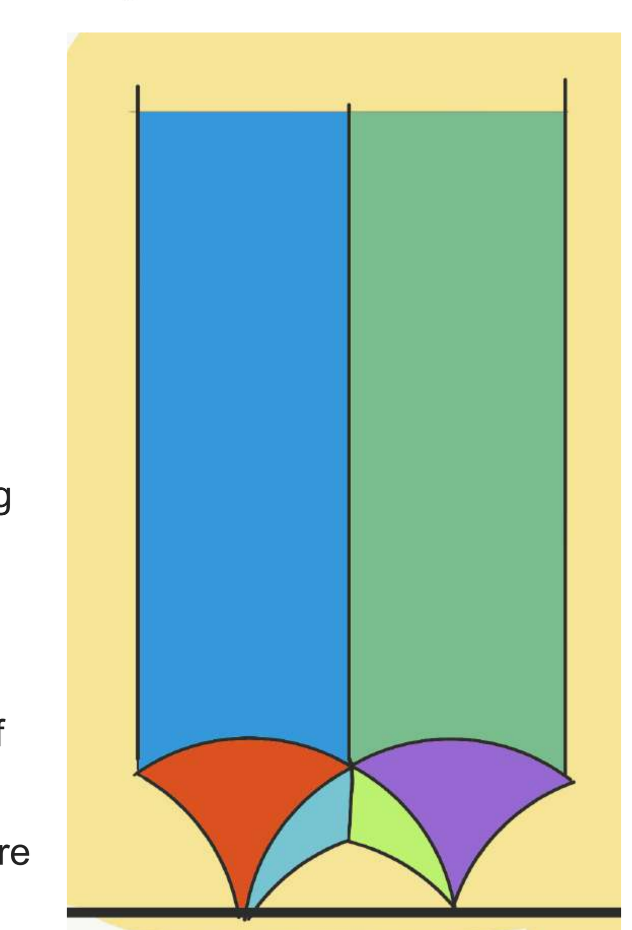
Congruence Covers

Definition: The Principal Congruence of Level N, Γ(N), is defined to be the kernel of $\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}_N)$



By the first isomorphism theorem that [SL(2,Z):Γ(2)] = |SL(2,Z_2)| = 6, meaning there are 6 cosets of H^2/Γ(2). A choice of 6 cosets representatives is {I,S,T,TST,TSTS,TS}

We construct a fundamental domain by 6 copies of the fundamental domain above, corresponding to these cosets.



To determine the topology of this surface, we compute the Euler characteristic (taking the infinity points to be vertices of the triangles). There are 6 faces, 9 edges, and 5 vertices. Then V-E+F= 2, which implies g = 0 so the surface is a sphere (with three punctures because of the ideal vertices)

Quandles

Ziqi Fu, Sherilyn Tamagawa†

Department of Mathematics, UCSB

Introduction

Quandles, introduced by David Joyce in 1982, are algebraic structures whose axioms encode the spatial movements of knots. The fundamental quandle of a classical oriented knot is a complete invariant up to reflection.

Preliminaries

What are knots?

A *knot* in $\mathbb{R}^3$ is a simple curve with no self-intersection. Two knots have the same *knot type* are *ambient isotopic*, meaning that one can be continuously deformed into another. In topological knot theory, different knots are distinguished up to ambient isotopy. Knots are studied using *knot diagrams*, projection of knots on a plane with broken understrands. Each knot can be *oriented* by assigning it a preferred direction of travel, which is indicated in the knot diagram using an arrow.

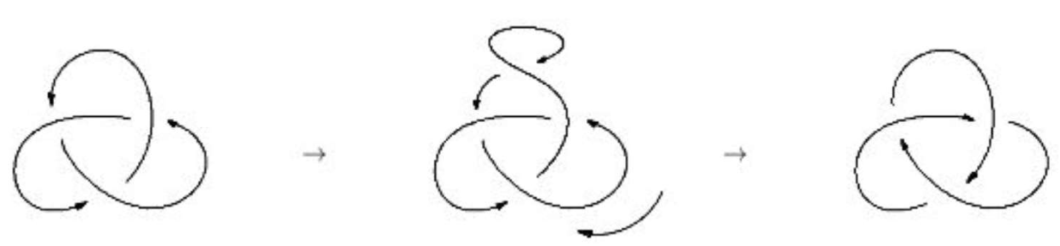


Figure 1: The oriented trefoil knot is ambient isotopic to its inverse

Knot Invariant

The fundamental question in knot theory is to determine whether two knot diagrams represent the same knot. Two knots are ambient isotopic if and only if they can be changed into the other by a finite sequence of *Reidemeister moves*.

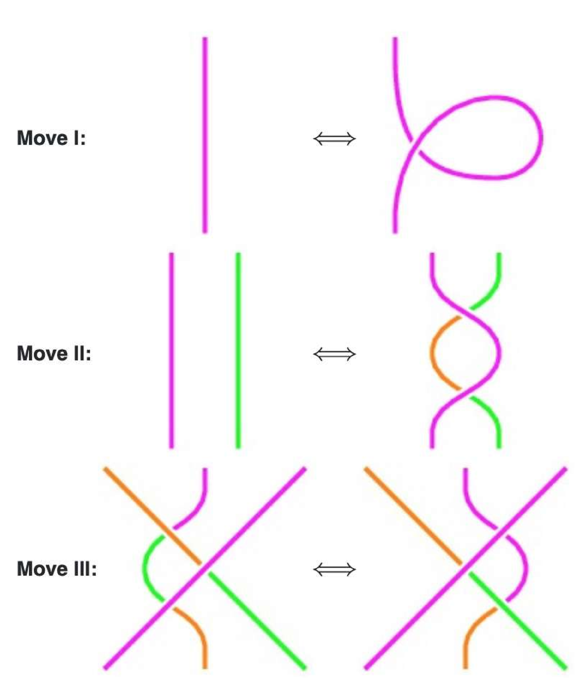


Figure 2: Reidemeister moves

A *knot invariant* is a function $f : \mathcal{K} \to X$ from the set of all knot diagrams to a set X such that for each Reidemeister move, $f(K_1) = f(K_2)$ where K_1 is the preimage of K_2.

Example

Tricolorability of a knot is a simple knot invariant. Each arc in the knot diagram is assigned with one color from a set of three. A tricoloring is *valid* if at every crossing it uses all three colors the same or all different. The number of valid triclorings of a knot diagram is an invariant.

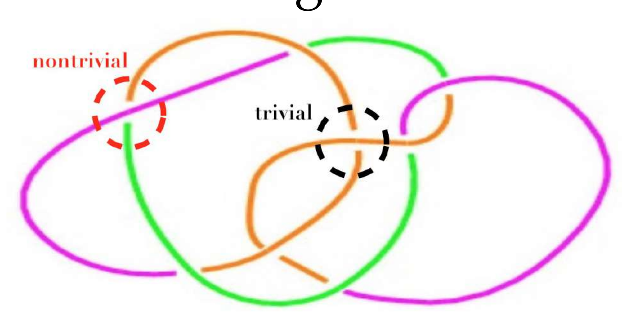


Figure 3: A valid tricoloring of a knot

Algebraic Structures

An algebraic structure is non-empty set X equipped with at least one closed binary *operation* $* : X \times X \to X$. Let $(X, *)$ and $(Y, \circ)$ be algebraic structures. X and Y are *homomorphic* if there exists a *homomorphism* $f : X \to Y$ such that it preserves all of the operations, i.e., $f(x * x') = f(x) \circ f(x')$. A bijective homomorphism is called an *isomorphism*.

Quandles

Definition. A ***quandle*** is a set X with a binary operation $\triangleright : X \times X \to X$ satisfying for all $x, y, z \in X$:

(i) $x \triangleright x = x$,

(ii) $f_y : X \to X$ defined by $f_y(x) = x \triangleright y$ is a bijection,

(iii) $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$.

The inverse of $f_y(x)$ is written as $x \triangleright^{-1} y$.

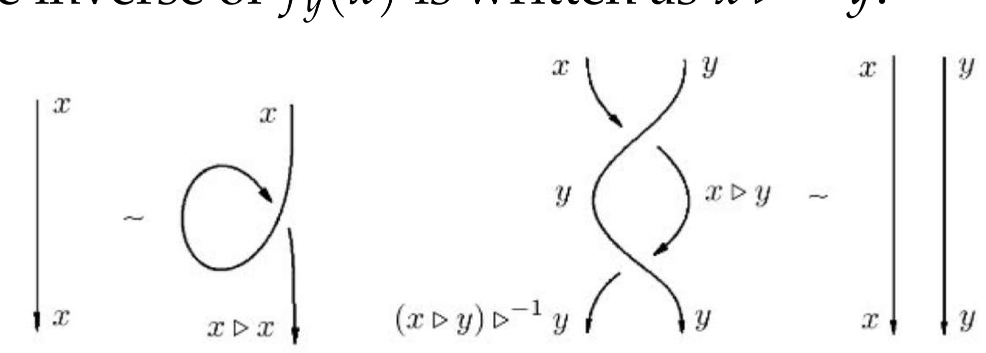
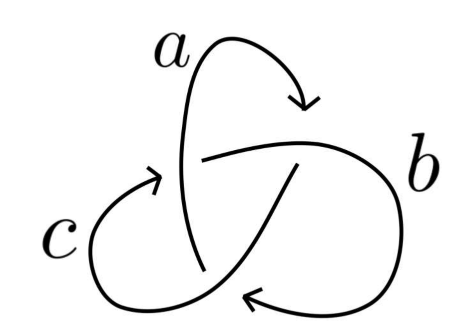


Figure 4: Axiom i and ii encoding the first two Reidemeister Moves

Fundamental Quandle

The *fundamental quandle*, or *knot quandle*, of an oriented knot is given by a representation with generators corresponding to arcs and quandle relations at crossings.

Example



$$\langle a, b, c \,|\, a \triangleright b = c, b \triangleright c = a, c \triangleright a = b \rangle.$$

Figure 5: Quandle of the oriented trefoil

Quandle Counting Invariant

Given a finite quandle X, we define the *counting invariant* $\Phi_X^{\mathbb{Z}}$ to be the number of quandle colorings of a knot diagram K. Formally put,

$$\Phi_X^{\mathbb{Z}} = |\mathrm{Hom}(\mathcal{K}(K), X)|,$$

with each homomorphism representing a valid quandle coloring of the diagram K. Since the fundamental quandle $\mathcal{K}(K)$ does not depend on the choice of the diagram of K, the set of all quandle homomorphisms is an invariant of the knot K.

Example

Take quandle $X = \mathbb{Z}_4$ with $x \triangleright y = 2y - x$. Let K be the oriented figure-8 whose knot quandle is

$$\langle x, y | y \triangleright (y \triangleright x) = x \triangleright y, x \triangleright (x \triangleright y) = y \triangleright x \rangle.$$

Calculation gives that $\Phi_X^{\mathbb{Z}} = 16$, meaning that we have a total of 16 different ways to color the figure-8 knot using quandle $X = \mathbb{Z}_4$.

$\triangleright$	0	1	2	3
0	0	2	0	2
1	3	1	3	1
2	2	0	2	0
3	1	3	1	3

Figure 6: Operation table of X

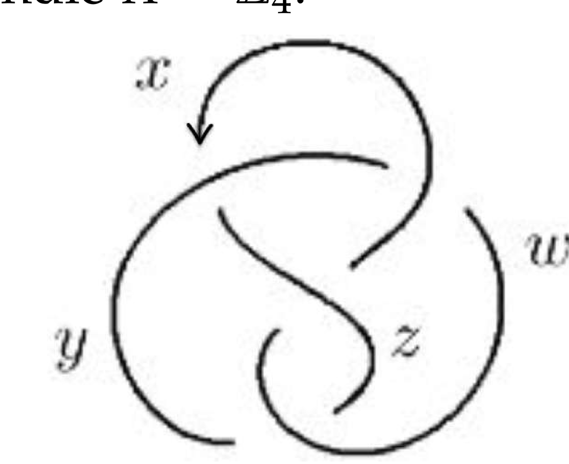


Figure 7: Oriented figure-8 knot

Virtual Knots

Classical knot theory is the study of the embeddings of curves in $\mathbb{R}^3$. Virtual knot theory, as a generalization, studies the embeddings of curves in *thickened* surfaces of arbitrary *genus*, up to the addition or removal of empty *handle*. Consider a virtual trefoil knot, which "almost" fits in a single *hyperplane* with a bit of thickness, it can be projected onto a plane by adding a new type of crossing called the *virtual crossing*. Note that these crossings do no exist because they live on the *bridge*, or *handle*, in the added dimension.

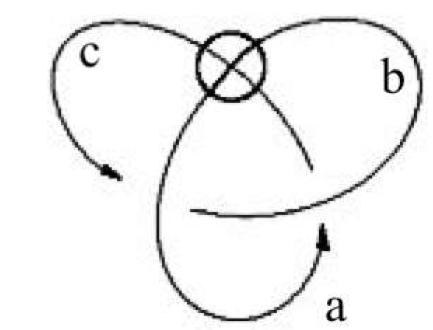


Figure 8: Virtual trefoil knot

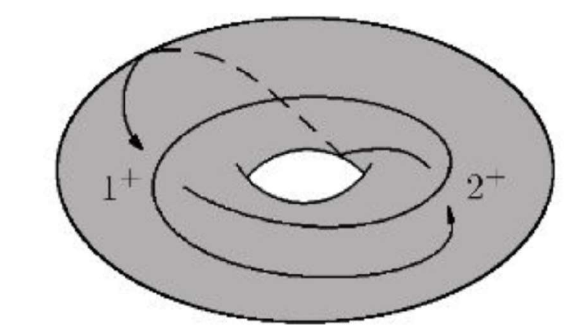


Figure 9: Trefoil knot on a torus

Another way to understand virtual knots is to draw them on a torus. The extra dimension needed by virtual knots is given by the torus' genus being greater than 0. We think of the virtual crossings as the result of flattening the torus onto a plane.

A virtual knot, formally put, is an equivalence class of virtual knot diagrams under the equivalence relation generated by classical and generalized virtual Reidemeister moves.

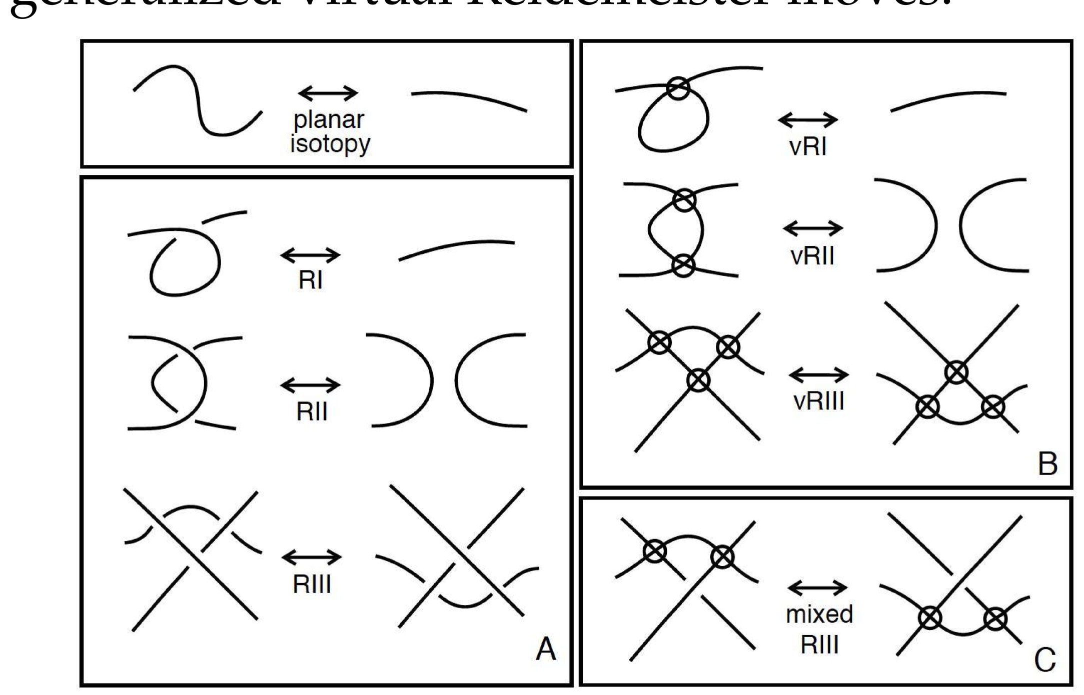


Figure 10: Generalized Reidemeister moves for virtual knots

References

1 Elhamdadi, M, and Nelson, S. (2015). Quandles: an introduction to the algebra of knots. *Amer. Math. Soc.*

2 Kauffman, L.H., et al.. (2014), Unsolved problems in virtual knot theory and combinatorial knot theory. *polish Acad. Sci. Inst. Math.*

3 Austin, D. Knot Quandaries Quelled by Quandles. Retrieved from http://www.ams.org/publicoutreach/feature-column/fc-2016-03

†Graduate mentor

Deep Learning: Image Classification Using Convolutional Neural Networks

Chau Tran, Troy Eggertsen, Nabil Hentabli

Department of Mathematics, University of California, Santa Barbara

Overview

- We use Convolutional Neural Networks (CNNs) to identify what object is in a given picture.
- By training this network architecture on a large dataset consisting of pre-labeled images, the network learns to identify objects through pattern recognition.
- Training and testing is done using CIFAR-10.

Neural Networks

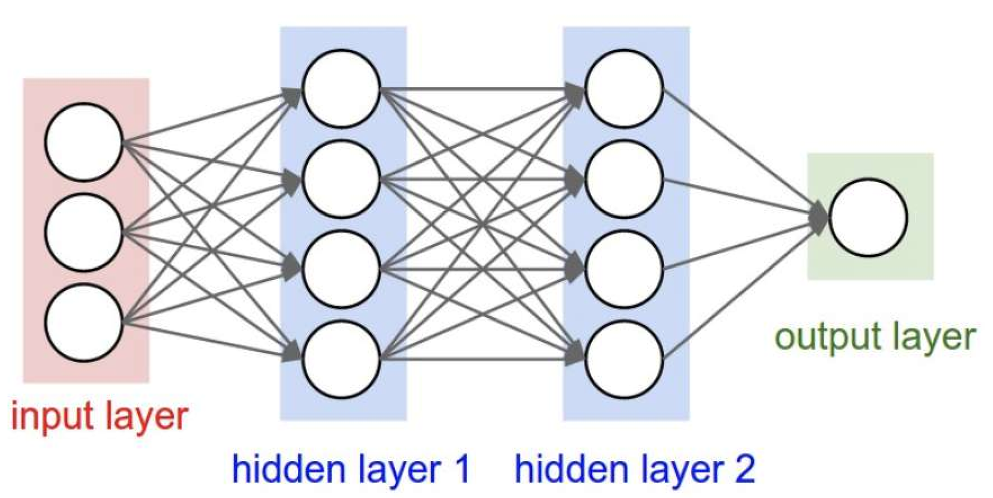


Fig. 1: Fully Connected Neural Network Architecture[5]

- Neural Networks are composed of a number of layers:
  - The input layer, in our case a three-dimensional tensor encoding an input image.
  - An arbitrarily large number of hidden layers that operate repeatedly on the outputs of the previous. layers via linear matrix multiplications and non-linear activation functions.
  - The output layer; for image classification problems, we use the softmax function to produce class confidence scores.

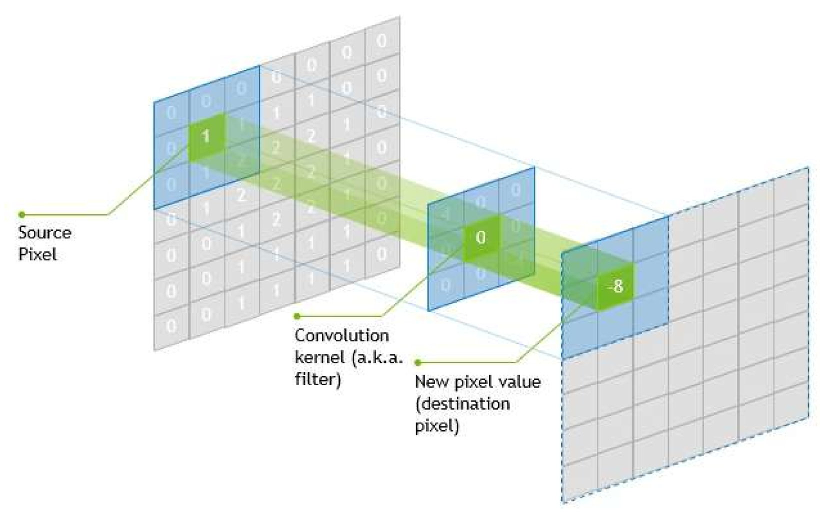


Fig. 2: Convolution [3]

- A CNN differs from standard Neural Network by containing a number of convolution layers before fully connected ones.
  - Fully connected layers are layers where every node in one layer is connected to all nodes in the next.
  - Convolution layers are better suited than standard layers for identifying information in spatial data; they do this by changing the dimensions of matrices as they go through the model.

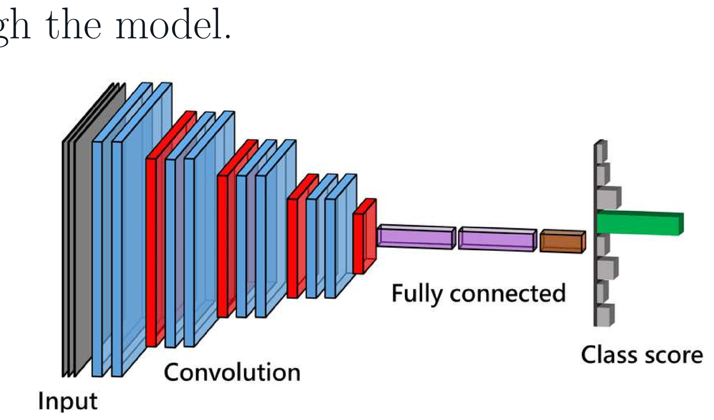


Fig. 3: Convolution Neural Network (CNN) [4]

Training

- During training, a model learns by going through each element of training data, evaluating its own output's accuracy against ground truth with a loss function, and then back-propagating changes to its algorithm based on calculated loss.
- Loss Function:

$$L = -\sum_{i=1}^{C} t_i log\left(\frac{e^{s_i}}{\sum_j^C e^{s_j}}\right)$$

C classes total; t_i, s_i are target and class score of class C_i

- Gradient-Based Optimization:

$$W = W - \lambda \nabla L$$

W are weighs; λ is the learning rate.

Image Classification

Image Classification: the task of assigning an input image one label from a fixed set of categories.

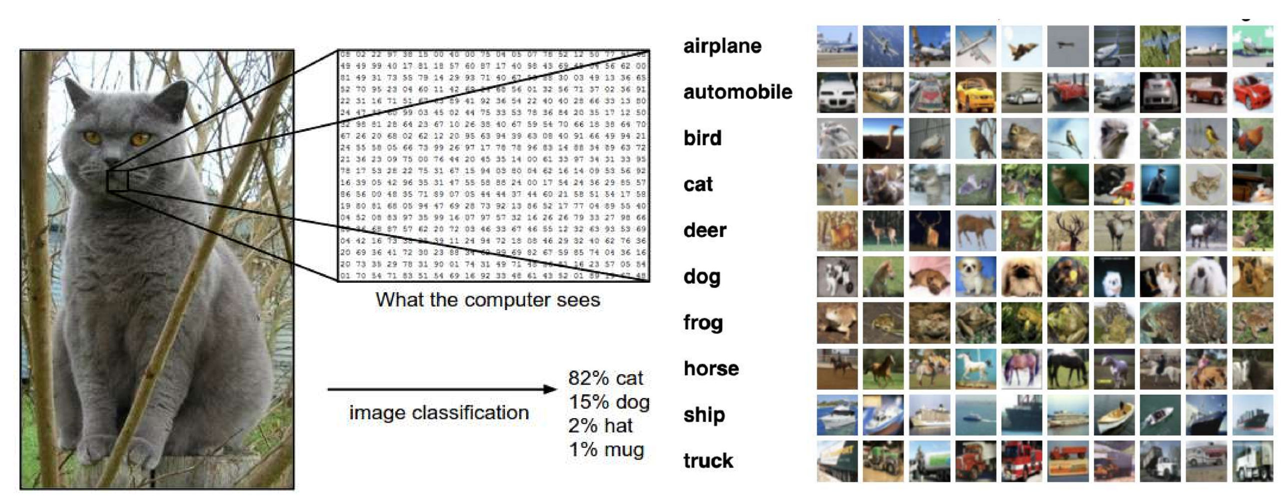


Fig. 4: **Left:**The task in Image Classification[5], **Right:** CIFAR-10 dataset[2]

Network Architectures

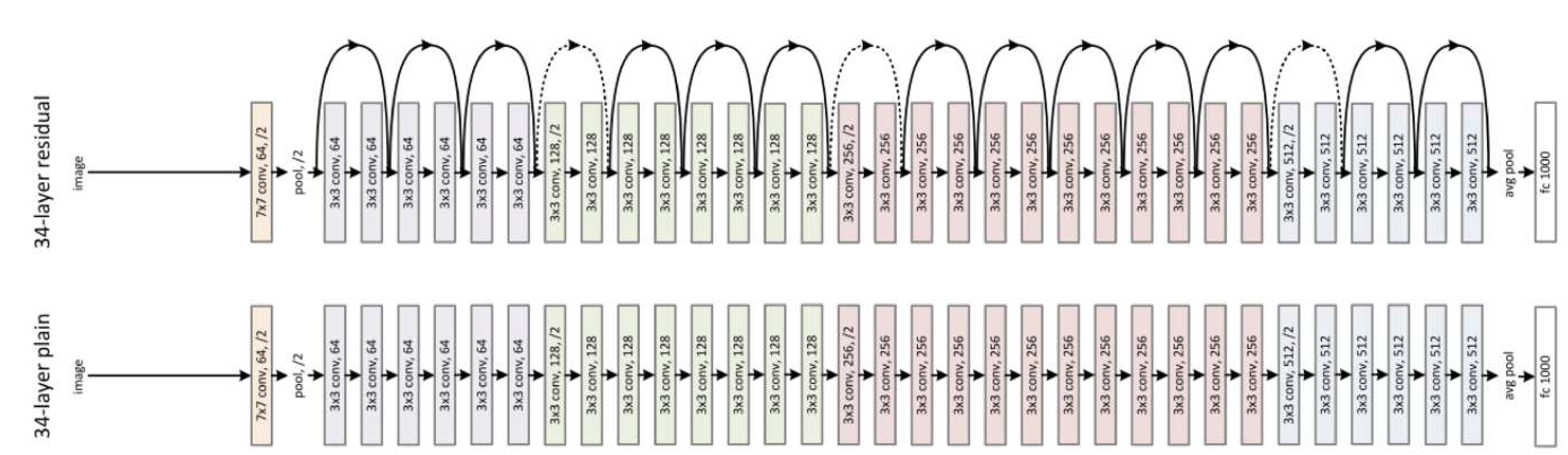


Fig. 5: Plain and Residual Network[1]

Residual Network is based on Plain Network with additional shortcut connections. The building block of the Residual Network is defined as:

$$y = \mathbf{F}(x, \{W_i\}) + x$$

Here x and y are the input and output vectors of the layers considered.

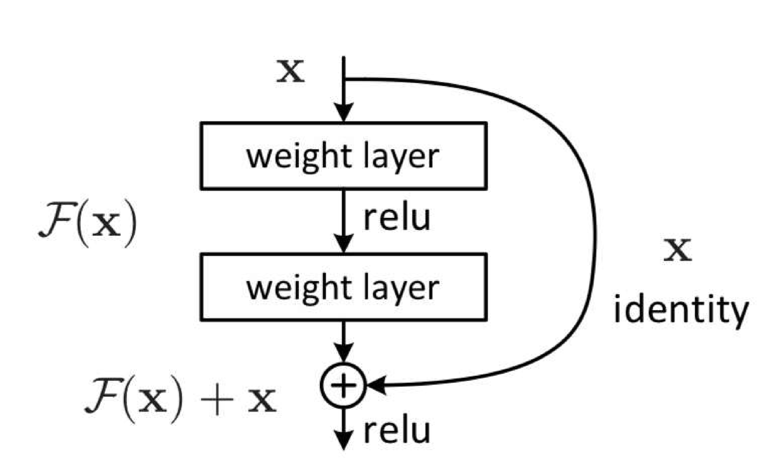


Fig. 6: Building Block of Residual Net[1]

Results

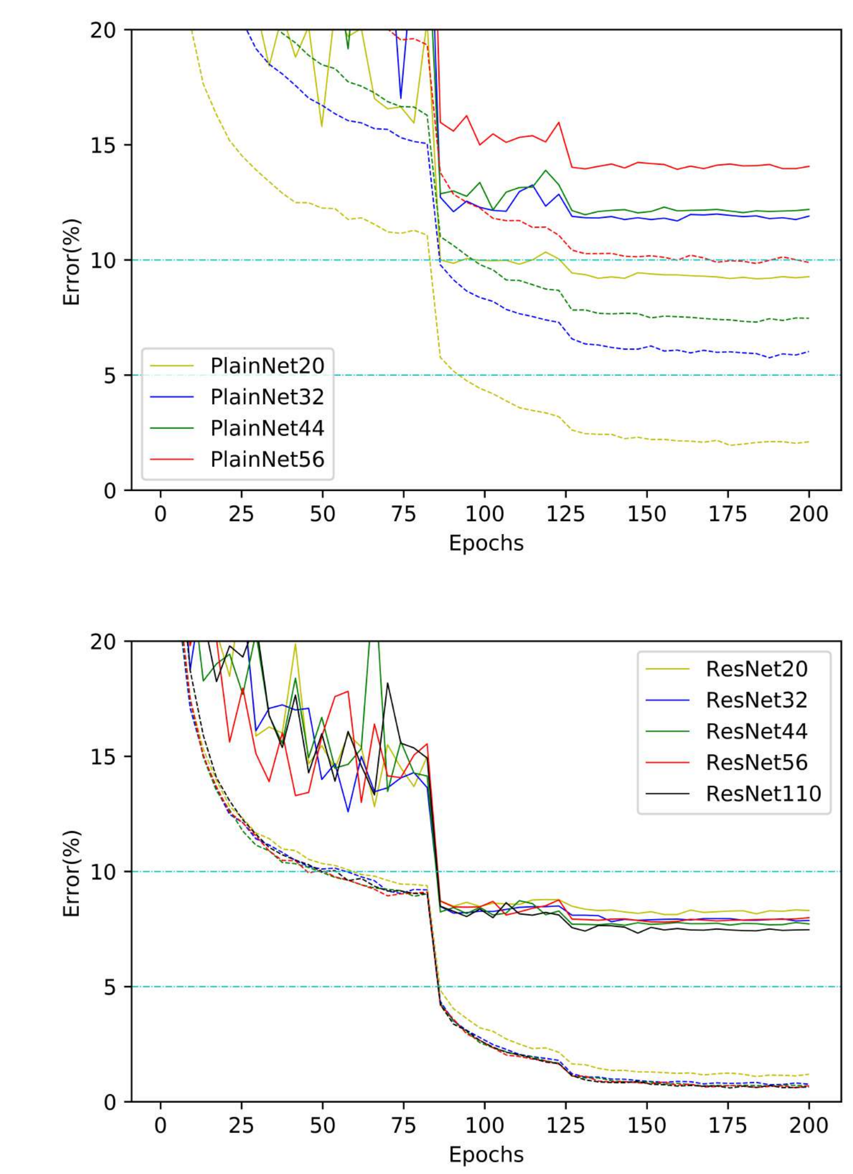


Fig. 7: Training on CIFAR-10. **DASHED** lines denote **trainning** errors, and **BOLD** lines denote **testing** errors. **Top**: Plain Networks. **Bottom**: Residual Networks

Comparison

Network	Training Error(%)	Testing Error(%)
20-layer ResNet	98.91	91.87
32-layer ResNet	99.28	92.18
44-layer ResNet	99.35	92.51
56-layer ResNet	99.39	92.26
110-layer ResNet	99.41	92.68
20-layer PlainNet	98.05	90.82
32-layer PlainNet	94.25	88.36
44-layer PlainNet	92.73	88.08
56-layer PlainNet	90.24	86.08

Acknowledgements

Jay Roberts and Kyle Mylonakis, our graduate advisers, for their help. UCSB Mathematics DRP for facilitating this opportunity.

References

[1] Kaiming He et al. *Deep Residual Learning for Image Recognition.* 2015. arXiv: `1512.03385 [cs.CV]`.

[2] Alex Krizhevsky. "Learning Multiple Layers of Features from Tiny Images". In: *University of Toronto* (May 2012).

[3] Nvidia. *Approaches to Object Detection.* URL: `https://www.slideshare.net/NVIDIATaiwan/nvidia-dli-approaches-to-object-detection`.

[4] Vladimir Puzyrev. "Deep learning electromagnetic inversion with convolutional neural networks". In: (Dec. 2018).

[5] Stanford. *Convolutional Neural Network for Visual Recognition.* URL: `http://cs231n.github.io`.

From Gluing Constructions to Hyperbolic Tessellations

Daniel Apsley

2019 Directed Reading Program
Department of Mathematics, University of California, Santa Barbara

Euclidean and Hyperbolic Space

Given two **metric spaces**, (X, d) and (X', d'), an **isometry** $\Phi : X \to X'$ is a bijective function such that

$$d'(\Phi(P), \Phi(Q)) = d(P, Q) \text{ for every } P, Q \in X.$$

The **euclidean plane** is the metric space composed of $\mathbb{R}^2$ equipped with the metric

$$d((x, y), (x', y')) = \sqrt{(x^2 - x'^2) + (y^2 - y'^2)}.$$

Hyperbolic space (in the Poincare disk model) is the set $\mathbb{B}^2 = \{z \in \mathbb{C} \mid |z| < 1\}$ equipped with the metric

$$d(z, z') = \inf\left\{\int_{t_0}^{t_1} \frac{2||\gamma'(t)||}{\mathrm{Im}(\gamma(t))(1 - |\gamma(t)|^2)}\, dt \mid \gamma(t_0) = z \text{ and } \gamma(t_1) = z'\right\}.$$

Gluing Maps and Quotient Spaces

One can visualize gluing maps by observing that gluing opposite edges of a square together (and allowing the paper to stretch and contract as needed) will create a torus as shown below. To make this kind of construction more rigorous, let (X, d) be a metric space and $\overline{X}$ be some *partition* of X. We say that $P, Q \in X$ are *glued together* (denoted $P \sim Q$) if P and Q are in the same element of $\overline{X}$. The elements of $\overline{X}$ will be denoted as $\overline{P}$ where $P \in \overline{P}$. Next, we would like to define a metric $\overline{d}$ on $\overline{X}$. To do this, define a **discrete walk** w between two points $\overline{P}, \overline{Q} \in \overline{X}$ as a finite sequence of points in X:

$$P = P_1, Q_1 \sim P_2, Q_2 \sim P_3, \ldots Q_{k-1} \sim P_k, Q_k = Q.$$

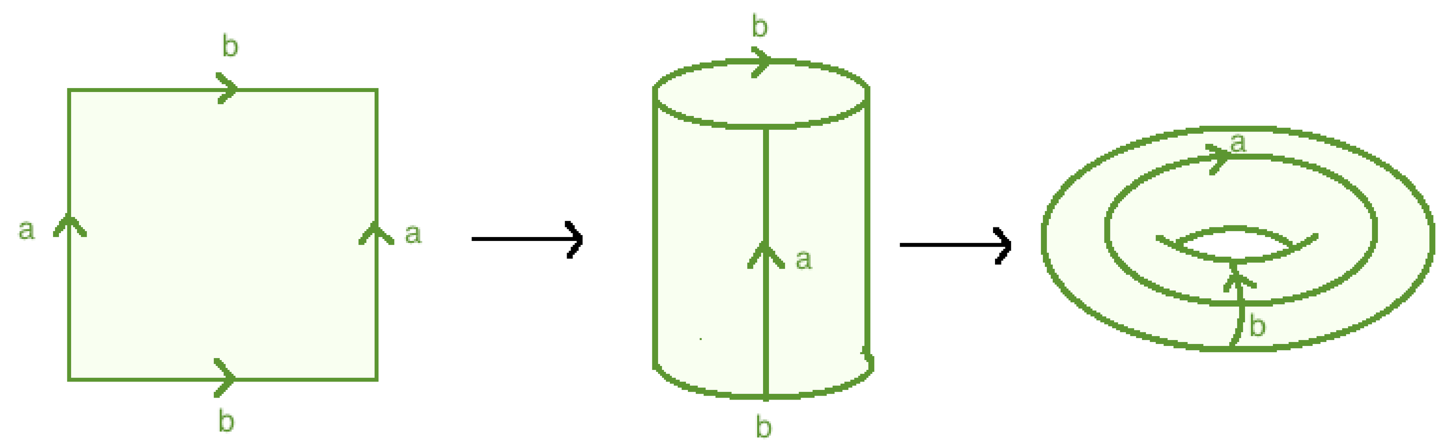
Next, we define the **length** of w to be the sum

$$l_d(w) = \sum_{i=0}^{k} d(P_i, Q_i).$$

Lastly, in order to make $(\overline{X}, \overline{d})$ a metric space, we can define $\overline{d} : \overline{X} \times \overline{X}$ to be

$$\overline{d}(\overline{P}, \overline{Q}) = \inf\{l_d(w) \mid w \text{ starts at } P \text{ and ends at } Q\}.$$

Given some arbitrary quotient space, it can be true that $\overline{d}(\overline{P}, \overline{Q}) = 0$ when $\overline{P} \neq \overline{Q}$ but in the following examples, it can be proven that this is not the case. In this way, we obtain the **quotient metric space** $(\overline{X}, \overline{d})$ of (X, d).



[2] This is how a torus can be seen as a gluing map where the letters show which sides are glued to which and the arrows show their orientation. What would the surface look like if you reversed one of the arrows?

A More Visual Example

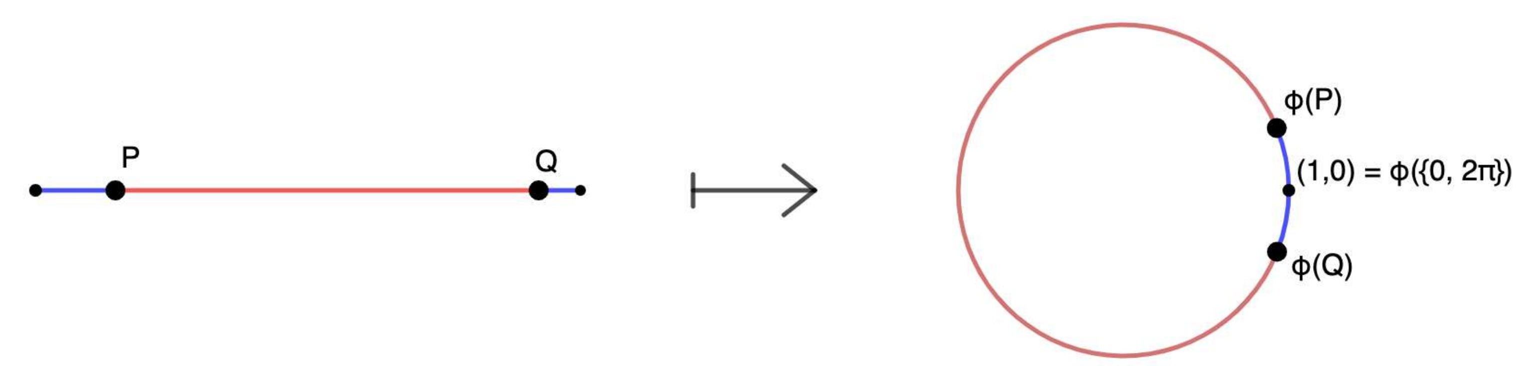
[1] Using the previous construction, we will produce a quotient space of the interval $[0, 2\pi]$ which is isometric to the unit circle S^1. Intuitively, as shown below, we can simply "wrap" the interval around the unit circle and glue the ends together. To make this rigorous, let our quotient space be

$$\overline{X} = \{\{P\} \mid P \in (0, 2\pi)\} \cup \{\{0, 2\pi\}\}$$

and let $\Phi : \overline{X} \to S^1$ be such that

$$\Phi(\overline{P}) = (\sin(P), \cos(P)).$$

The function Φ is bijective and well defined since $\Phi(\overline{2\pi}) = \Phi(\overline{0})$ and the rest of the points are singletons. All that needs to be checked is that Φ preserves distance. To see this, notice that the minimum distance on S^1 is the minimum of the two possible paths between them. Similarly, on the quotient, one can either measure the distance between the points in the interval using the discrete walk $P = P_1, Q_1 = Q$ or using the discrete walk $P = P_1, Q_1 \sim P_2, Q_2 = Q$ where $\overline{Q_1} = \overline{P_2} = \{0, \pi\}$. Therefore, the two objects are geometrically the same!



Clearly, the blue path is shorter but without taking the quotient of the space, the longer red path would represent the distance.

Polygons

A **geodesic** is a curve γ such that for every $P, Q \in \gamma$, it is the shortest curve connecting them. Intuitively, on the euclidean plane, the geodesics are all lines and line segments. In hyperbolic space, however, the geodesics are either lines which pass through the center of the disk or segments of circles which meet the boundary of the disk orthogonally.

A **polygon** X is a region in either $\mathbb{B}^2$ or $\mathbb{R}^2$ whose boundary is decomposed into finitely many geodesics $E_1, E_2, \ldots E_n$ called **edges** meeting only at their endpoints called **vertices**.

Glue the Edges of Polygons with Isometries

Let X be a hyperbolic or euclidean polygon. Then, we can pair the edges we want to glue together as follows: $\{E_1, E_2\}, \{E_3, E_4\}, \ldots, \{E_k, E_{k+1}\}$ and specify isometries $\Phi_{2i-1} : E_{2i-1} \to E_{2i}$ between the two edges in any pair. This is to ensure that the edges being glued together are the same size. Lastly, we will define $\overline{X}$ by the following properties:

- if P is in the interior of X, then it is glued to no other point and $\overline{P} = \{P\}$;
- if P is in an edge E_i and is not a vertex, then $\overline{P}$ consists of two points: P and $\Phi_i(P) \in E_{i\pm 1}$;
- if P is a vertex, then $\overline{P}$ consists of P and all the other vertices of the form $\Phi_{i_k} \circ \Phi_{i_{k-1}} \circ \cdots \circ \Phi_{i_1}(P)$ where $i_1, i_2, \ldots, i_k$ are such that $\Phi_{i_{l-1}} \circ \cdots \circ \Phi_{i_1} \in E_{i_j}$ for all j.

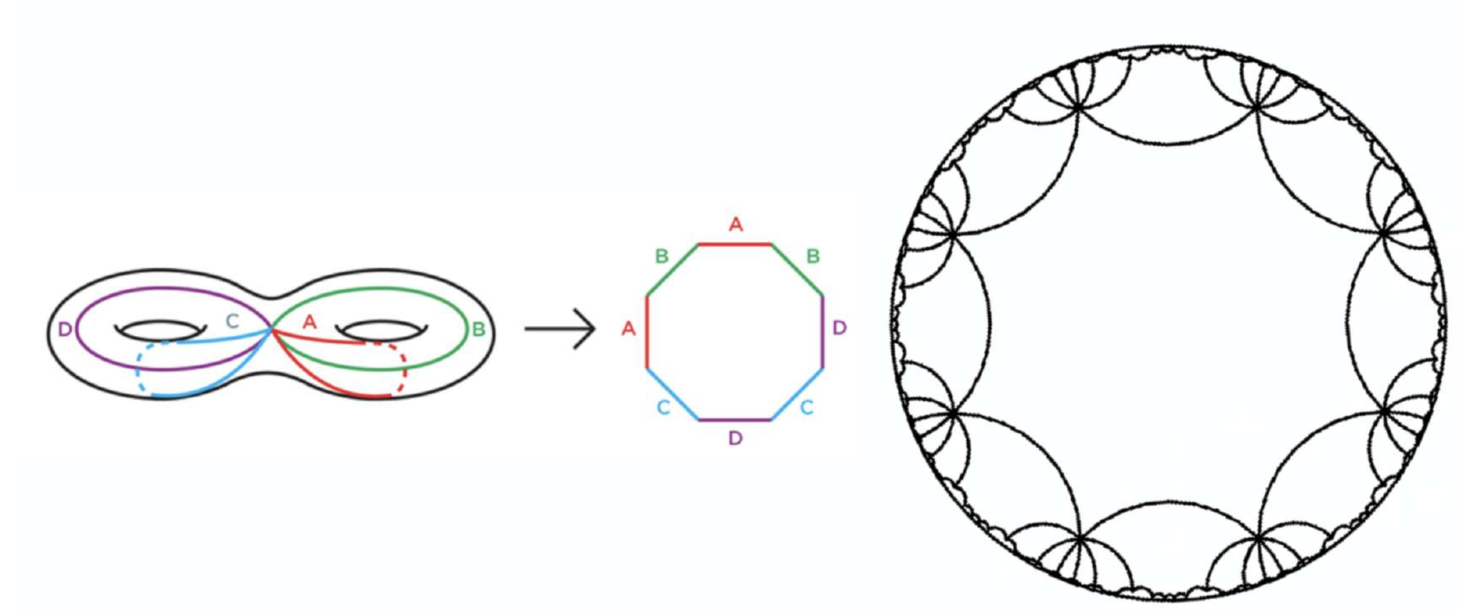
Tessellations

A **tessellation** of euclidean or hyperbolic space is a family of tiles $\{X_n\}_{n\in\mathbb{N}}$ such that

- each X_m is a connected Polygon in $\mathbb{B}^2$ or $\mathbb{R}^2$;
- any two X_n, X_m are isometric;
- the union of all the tiles is the whole space;
- any two X_n and X_m are either disjoint or their intersection only contains edges and vertices;
- for every point P on the plane, there exists a $\varepsilon > 0$ such that $B(P, \varepsilon)$ meets only finitely many tiles X_m.

Next, given a polygon X and its quotient space $\overline{X}$ with isometries Φ_k between pairs of edges as before, we define the **tiling group** Γ to be the set of all isometries of $\mathbb{R}^2$ or $\mathbb{B}^2$ which can be written as a finite composition $\Phi_l \circ \Phi_{l-1} \circ \cdots \circ \Phi_1$ of edge isometries. The connection between this group and tessellations is captured in the following theorem.

Theorem (Tessellation Theorem). *Let X be a Hyperbolic or Euclidean connected Polygon with gluing data as above. Also, suppose that for each vertex P of X, the angles of X at all vertices glued to P add up to $\frac{2\pi}{n}$ for some $n \in \mathbb{N}$. Lastly, assume that $\overline{X}$ is* ***complete****. Then, as Φ ranges over all elements of Γ, $\Phi(X)$ forms a tessellation.*



To see this theorem in action, observe that this gluing map is on a hyperbolic octagon with angles which add up to 2π. Because its quotient is the double torus which is compact and therefore, complete, the polygon can tessellate the plane using combinations of the isometries given by the colors in the diagram.

References

[1] F Bonahon. *Low-Dimensional Geometry.* Student Mathematical Library, 2009, p. 136.

[2] Mathonline. "Identifying Polygons and Their Quotient Spaces". In: (2012).

Lie Groups, Lie Algebras and Particle Physics

Transito-Bryan Gonzalez Graduate Mentor: Greg McGrath

Department of Mathematics University of California, Santa Barbara

Lie Groups, Matrix Lie Groups, Representations, and Lie Algebras

A **real Lie group** is a group G that is also a finite-dimensional real smooth manifold whose group operations are smooth maps.
A **matrix Lie Group** is any closed subgroup H of $GL(n, \mathbb{C})$. That is, for an arbitrary sequence $\{A_n\}$ of matrices in H,

$$\{A_n\} \to A$$

where $A \in H$ or A is not invertible.
A **representation** of a group G on a vector space V is defined as a homomorphism $\phi : G \to GL(V)$. For each $g \in G$, the representation assigns a linear map $\rho_g : V \to V$.
A **Lie Algebra** over a field F is an F-Vector space L, together with a bilinear map, the Lie bracket $[,] : L \times L \to L$ that satisfies the following conditions: $\forall X, Y, Z \in L$ and $\forall a, b \in F$,
$[,]$ is anti-symmetric,

$$[X, Y] = -[Y, X] \tag{1}$$

$[,]$ is bilinear,

$$[aX + bY, Z] = a[X, Z] + b[Y, Z] \tag{2}$$

$[,]$ satisfies the Jacobi identity,

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0 \tag{3}$$

A **Lie Algebra of a matrix Lie group** G, denoted by $\mathfrak{g}$, is the set of all matrices X such that e^{tX} is in G for all real numbers t, accompanied with a Lie bracket $[,] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$.
For the Lie Algebra of a matrix Lie Group, $[,]$ is defined to be the commutator of the matrices,

$$[X, Y] = XY - YX \tag{4}$$

which indeed satisfies the conditions of a Lie bracket.

Matrix Lie Groups in Physics

The Orthogonal and Special Orthogonal Groups

An $n \times n$ matrix A is said to be **orthogonal** if $A^T A = \mathbb{I}$, i.e $A^T = A^{-1}$.
Equivalently, the column vectors that make up A are orthonormal:

$$\sum_{i=1}^{n} A_{ij} Aik = \delta_{jk} \tag{5}$$

and equivalently, A preserves the inner product:

$$\langle x, y \rangle = \langle Ax, Ay \rangle \tag{6}$$

By the orthogonality of A, $det(A^T) = det(A)$ and so $det(A) = \pm 1$. Thus an orthogonal matrix is invertible.
Also by the orthogonality of A, $\langle A^{-1}x, A^{-1}y \rangle = \langle A(A^{-1}x), A(A^{-1}y) \rangle = \langle x, y \rangle$. The inverse of an orthogonal matrix is orthogonal.
Lastly, the product of two orthogonal matrices is also orthogonal. Then this set of $n \times x$ orthogonal matrices forms a group called the **orthogonal group** $O(n)$ which is a subgroup of $GL(n, \mathbb{C})$)
The **special orthogonal group** $SO(n)$ is defined to be a subgroup of $O(n)$ whose matrices have determinant 1. This is a matrix Lie group.

The Unitary and Special Unitary Groups

An $n \times n$ matrix A is said to be **unitary** if $A^\dagger A = \mathbb{I}$, i.e $A^\dagger = A^{-1}$.
Equivalently, the column vectors are orthonormal:

$$\sum_{i=1}^{n} \overline{A_{ij}} Aik = \delta_{jk} \tag{7}$$

and equivalently, A preserves the inner product:

$$\langle x, y \rangle = \langle Ax, Ay \rangle \tag{8}$$

Since A is unitary, $det(A^\dagger) = \overline{det(A)}$ and so $|det(A)| = 1$. Thus a unitary matrix is invertible.
Also since A is unitary, $\langle A^{-1}x, A^{-1}y \rangle = \langle A(A^{-1}x), A(A^{-1}y) \rangle = \langle x, y \rangle$. The inverse of a unitary matrix is unitary.
Lastly, the product of two unitary matrices is also unitary. Then this set of $n \times x$ unitary matrices forms a group called the **unitary group** $U(n)$ which is a subgroup of $GL(n, \mathbb{C})$
The **special unitary group** $SU(n)$ is defined to be a subgroup of $U(n)$ whose matrices have determinant 1. This is a matrix Lie group.

Isospin and SU(2)

Let's study the Isospin symmetry.
First, we define our operators. $a_p^\dagger$ and $a_n^\dagger$ are the creation operators for the proton and neutron respectively, and the corresponding annihilation operators are a_p and a_n. The possible bilinear products are:

$$\{a_p^\dagger a_n, a_n^\dagger a_p, a_p^\dagger a_p, a_n^\dagger a_n\} \tag{9}$$

From these, we may define the following operators:

$$B = a_p^\dagger a_p + a_n^\dagger a_n \tag{10}$$

$$\tau_+ = a_p^\dagger a_n \tag{11}$$

$$\tau_- = a_n^\dagger a_p \tag{12}$$

$$\tau_0 = \frac{1}{2}(a_p^\dagger a_p - a_n^\dagger a_n) \tag{13}$$

Which satisfy the commutation relations:

$$[\tau_0, \tau_+] = \tau_+ \tag{14}$$

$$[\tau_0, \tau_-] = -\tau_- \tag{15}$$

$$[\tau_+, \tau_-] = 2\tau_0 \tag{16}$$

The operators generate infinitesimal transformations such as:

$$\psi' = \{1 + i\epsilon(\tau_+ + \tau_-)\}\psi \tag{17}$$

These transformations change a proton or neutron into a linear combination of both states, hence the transformations occur in a two-dimensional Hilbert space. Furthermore, they are unitary. The group of interest is generated by our operators, $(10) - (13)$. However the unitary transformations generated by B are trivial. The remaining isospin operators generate a Lie group... SU(2)!

References

Heon Yoo, Joon. "LIE GROUPS, LIE ALGEBRAS, AND APPLICATIONS IN PHYSICS" The University of Chicago Mathematics REU 2015, 17 Sept. 2015. Web. 22 May 2019.

Lens Spaces

Wade Bloomquist and Emma Lennen
University of California, Santa Barbara

Our Problem

The important question we aim to tackle is telling whether two manifolds are the same or not. One way to do this is to look at the triangulations of the manifold. In our project, we focus on Lens Spaces. In particular, we work with an invariant that arises from triangulations of Lens Spaces using groups.

Simplicial Complexes

An n-simplex is simply the n-dimensional analog of a triangulation. In 0 dimensions, this is a point. In 1 dimension, this is a line. In 2 dimensions, this is just the classical triangle. In 3 dimensions, this is the tetrahedron. The way we construct these $n-$simplices is reliant that for each face of our simplex is an $n-1$ simplex. For example, in our traditional triangle, these faces are the line segments.

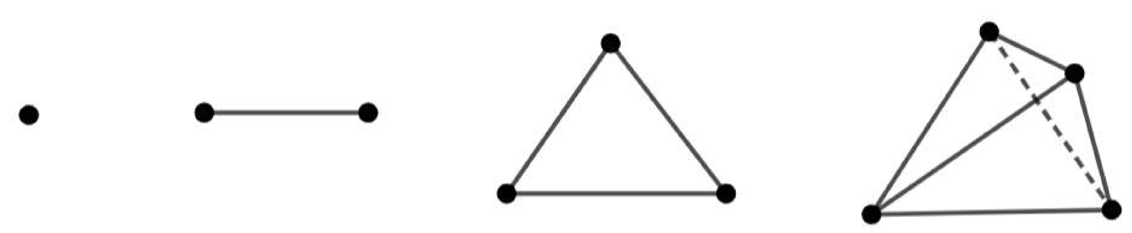


Fig. 1: 0-simplex, 1-simplex, 2-simplex, 3-simplex

Now what is a triangulation? We essentially map our simplices into our space in the obvious way. We see it visually.

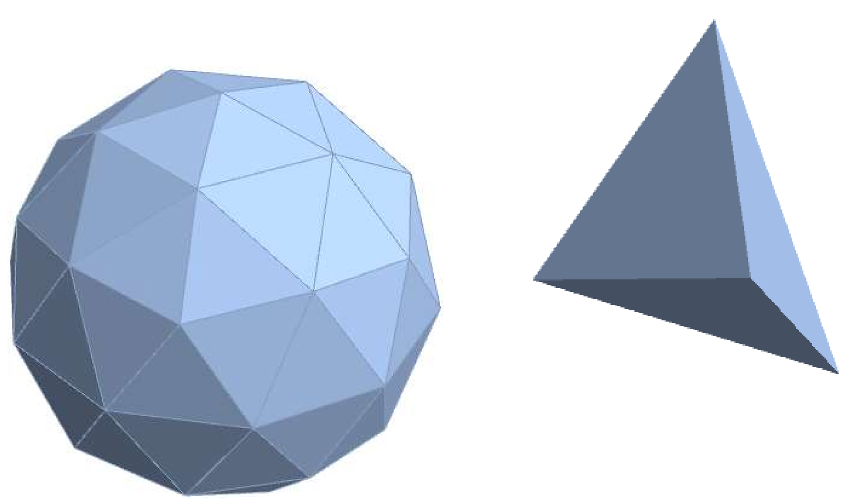


Fig. 2: Two possible triangulations of the 2-sphere

Pachner Moves

How do triangulations tell us anything about our manifold? Take any manifold M, then take any two triangulations, T_1, T_2, of M. Then T_1 and T_2 are related up to a finite number of Pachner moves. For $2-$manifolds, we can describe the moves as follows.

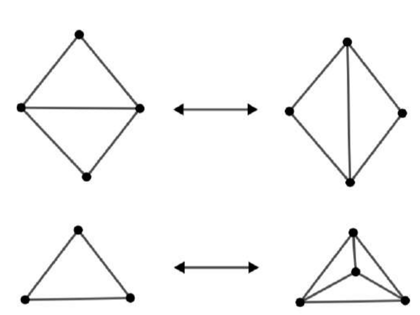


Fig. 3: The possible Pachner moves

If we have one of the configurations in our triangulation, we can change it to the corresponding configuration on the same vertices. Then in order to have an invariant of all our possible triangulations, we just need it to be invariant under Pachner moves. This kind of invariant can distinguish manifolds.

Lens Spaces

The manifold we focus on are Lens Spaces, denoted $L(p,q)$.

Definition 1. *$L(p,q)$ for coprime integers p,q is the quotienr of S^3 by $\mathbb{Z}/p-$actions. More precisely considering S^3 as the unit sphere in $\mathbb{C}^2$. The $\mathbb{Z}/p-$action on S^3 generated by the homeomorphism*

$$(z_1, z_2) \mapsto (e^{2\pi i/p} z_1, e^{2\pi i q/p} z_2)$$

is free. The resulting quotient space is the lens space $L(p,q)$.

What we are interested in is when $L(p_1,q_1)$ and $L(p_2,q_2)$ are equivalent based on an invariant that arises from triangulations. These spaces are nice to work with since they have already been classified as $L(p_1,q_1)$ and $L(p_2,q_2)$ are

1. homotopy equivalent if and only if $q_1 q_2 \equiv \pm n^2 \pmod{p_1}$ for some $n \in \mathbb{N}$
2. homeomorphic if and only if $q_1 \equiv \pm q_2^{\pm 1} \pmod{p_1}$

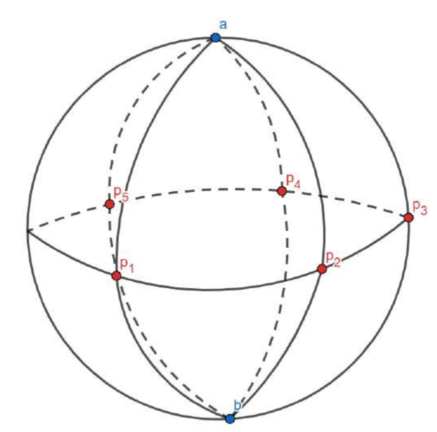


Fig. 4: $L(5,1)$ without twisting

In the picture above, p_i are the fifth roots of unity. They rotate by one roots over to each other. Points with a nonzero $y-$coordinate also rotate along that axis by $\exp(2\pi i/5)$.
The invariant we work with is called the **Dijkgraaf-Witten invariant**, which is reliant on a choice of abelian group G. The idea of how we obtain this invariant begins with a triangulation of the Lens Space. To each edge, we assign an element of G such that the sum of the elements on the edges of all faces is 0.
For each $i \leq p$, we can consider the tetrahedron. For any face, if we know two edges, this determines the third since the sum of them is 0. The if we know $g_{ab}, g_{cd}, g_{b,c}$ the whole tetrahedron is determined. The label in blue is determined by knowing $g_{c,d}$ and $g_{b,c}$.

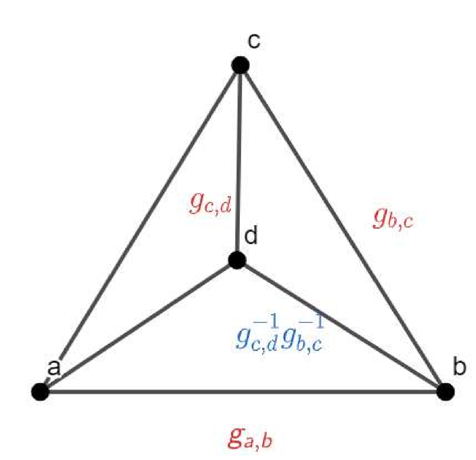


Fig. 5: Tetrahedron with elements

The idea of our invariant is them to take the sum of the product of the faces. Through some algebraic manipulations, we get that the Dijkgraaf-Witten invariant is

$$Z(L(p,q)) = \frac{1}{|G|} \sum_{g | g^p = 0} \prod_{j=1}^{p-1} \omega(g, g^j, g^b)$$

where $bq \equiv 1 \pmod{p}$ and ω is the cocycle. This cocycle is a condition that allows this to be an invariant of not only the triangulation but of the topological space because cocycle are invariant under Pachner moves.

Properties of the invariant

In particular, we work with $G = \mathbb{Z}/n\mathbb{Z}$ because the cocycle of a,b,c is

$$\omega^r(a,b,c) = \exp[(2i\pi/n^2 \overline{c}(\overline{a} + \overline{b} - \overline{a+b}))]$$

where $r = 0, ..., n-1$ and $\overline{x}$ denotes the integers representing x in $\{0, ..., n-1\}$.
When $\overline{x} + \overline{y} < N$, this is just 1. Otherwise, $\omega^r(a,b,c) = \exp(2\pi i r \overline{c}/n)$.
In fact, if $m = (n,p)$ and $a = \frac{rbp}{m}$, we can reduce $Z(L(p,q))$ to

$$Z(L(p,q)) = \frac{1}{n} \sum_{k=0}^{m-1} \exp(2i\pi a k^2/m)$$

This is the same as the Gauss sum of a and m.
This invariant cannot, unfortunately, distinguish between when two lens spaces are not homeomorphic, but are homotopic.

Theorem 1. *$L(p_1,q_1)$ and $L(p_2,q_2)$ with $p_1 < p_2$ can be distinguished using the Dijkgraaf-Witten invariant by $\mathbb{Z}/p_2\mathbb{Z}$ with $r = 0$.*

When $r = 0$, this formula is essentially the greatest common divisor of p_i and p_2, so when $p_1 \neq p_2$, this is different.

Theorem 2. *If $p \equiv 3 \pmod{4}$ for a prime p, then*

$$\pm i\sqrt{p}$$

depending on whether a is a square of $\mathbb{Z}/p\mathbb{Z}$

Theorem 3. *$L(p,1)$ and $L(p,2)$ are distinguished by $\mathbb{Z}/p\mathbb{Z}$ with $r = 1$ for $p \equiv 3 \pmod{4}$.*

Further Work

We have calculated the homotopy classes with fixed p and whether they are distinguished by the invariant for any n, r for up to $p = 70$. Some interesting results of this were that sometimes even when p is a prime, we require that $r > 1$. For example, the two homotopy classes of $p = 25$ can be distinguished by $n = 25$ and $r = 5, 10, 15, 20$, but not $r = 1, 2, 3, 4, 5$. A similar problem happens for $p = 36$ and $p = 64$.
One conjecture is that for any prime p, there exists r such that $\mathbb{Z}/p\mathbb{Z}$ distinguishes all of the homotopy classes.
Another stronger conjecture is that for any p, there exists an r and n combination such that $\mathbb{Z}/n\mathbb{Z}$ distinguishes all the homotopy classes of $L(p,q)$. It is important to note that $n = p$ does not always distinguish the homotopy classes.

Acknowledgements

We thank the University of California, Santa Barbara Directed Reading Program for their support.

References

1. Altschuler, Daniel, and Antoine Coste. "Invariants of Three-Manifolds from Finite Group Cohomology." Journal of Geometry and Physics, vol. 11, no. 1-4, 1993, pp. 191–203., doi:10.1016/0393-0440(93)90053-h.
2. Lickorish, W B R. "Simplicial Moves on Complexes and Manifolds." Proceedings of the Kirbyfest, 1999, doi:10.2140/gtm.1999.2.299.

Upper Half-Plane and Disk Model: Two Versions of Hyperbolic Space

Mentee: Erika McPhillips, Mentor: Carmen Galaz-Garcia

UCSB's Mathematics Directed Reading Program

Goal

Informally speaking, metric spaces are sets where we can measure the distance between points. We are familiar with the standard euclidean metric space; however, here we will explore the hyperbolic space and two of its models: the upper half-plane and the disk model. We will prove that there is an isometry between the two metric spaces.

Metric Spaces

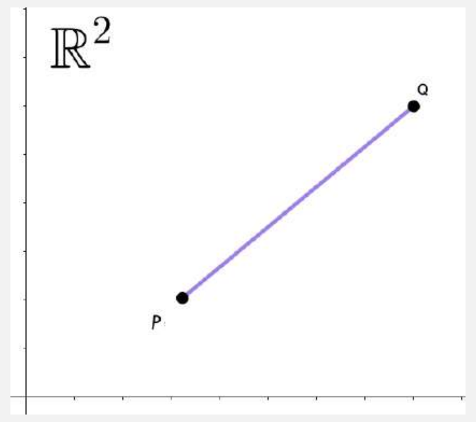
Definition: A metric space is a pair (X, d) where X is a set and d is a function $d : X \times X \longrightarrow \mathbb{R}$ such that

- $d(P, Q) \geq 0$ and $d(P, P) = 0$ for every P, Q;
- $d(P, Q) = 0$ if and only if $P = Q$;
- $d(Q, P) = d(P, Q)$ for every $P, Q \in X$;
- $d(P, R) \leq d(P, Q) + d(Q, R)$ for every $P, Q, R \in X$

Examples:

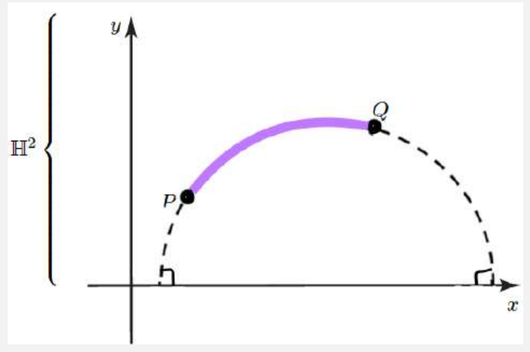
- **Euclidean Space**: $(\mathbb{R}^2, d_{euc})$

$$\mathbb{R}^2 = \{(x, y); x, y \in \mathbb{R}\}.$$

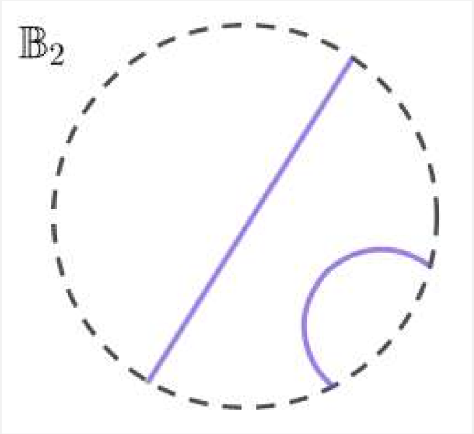


- **Upper half-plane**: The *Hyperbolic plane* $(\mathbb{H}^2, d_{hyp})$

$$\mathbb{H}^2 = \{(x, y) \in \mathbb{R}^2; y > 0\} = \{z \in \mathbb{C}; Im(z) > 0\}.$$



- **Disk model** for the hyperbolic plane $(\mathbb{B}^2, d_{\mathbb{B}^2})$. Here $\mathbb{B}^2$ is the open disk with radius 1 centered around 0 in the complex plane.



In all these spaces the distance is calculated by finding the infimum of the lengths of all piecewise differentiable curves between two points. For a smooth curve $\gamma(t)$, where $t \in [a, b]$, its lengths is

$$\int_a^b \| \gamma'(t) \| \, dt$$

where the norm of the tangent vector $\gamma'(t)$ at $\gamma(t)$ is different in, $\mathbb{R}^2$, $\mathbb{H}^2$, $\mathbb{B}^2$:

- **Euclidean norm** ($\| \vec{v} \|_{euc}$): is the length of a vector $\vec{v} = (a, b)$ in the euclidean plane
$$\| \vec{v} \|_{euc} = \sqrt{a^2 + b^2}.$$
- **Hyperbolic Norm** ($\| \vec{v} \|_{hyp}$): is the length of a vector in the hyperbolic plane based at the point $z \in \mathbb{H}^2 \subset \mathbb{C}$
$$\| \vec{v} \|_{hyp} = \frac{1}{Im(z)} \| \vec{v} \|_{euc}.$$
- **$\mathbb{B}^2$-norm** ($\| \vec{v} \|_{\mathbb{B}^2\ euc}$): length of a vector in the disk model based at the point $z \in \mathbb{B}^2$
$$\| \vec{v} \|_{\mathbb{B}^2} = \frac{2}{1 - |z|^2} \| \vec{v} \|_{euc}.$$

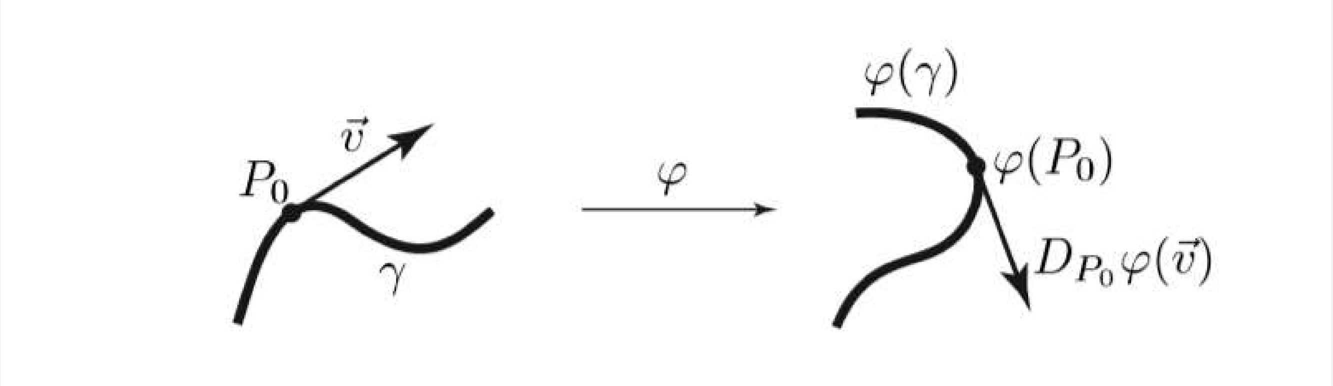
Isometries

Definition: An isometry between two metric spaces (X, d) and (X', d') is a bijection $\varphi : X \longrightarrow X'$ that respects distances:

$$d'(\varphi(P), \varphi(Q)) = d(P, Q)$$

for every $P, Q \in X$.

Differentiable map: If U is an open set in $\mathbb{R}^2$, $P_0 \in U$, and γ is a parameterized curve in U that passes through P_0, then the differentiable map $\varphi : U \longrightarrow \mathbb{R}^2$ will yield a new curve $\varphi(\gamma)$ in $\mathbb{R}^2$, that passes through $\varphi(P_0)$, and will be tangent to the vector $D_{P_0}\varphi(\vec{v})$.



Proposition: If $\varphi(z) = \frac{az+b}{cz+d}$, then

$$D_{z_0}\varphi(v) = \frac{ad - bc}{(cz_0 + d)^2} v.$$

Theorem

The map $\Phi(z) = \frac{-z+i}{z+i}$ induces an isometry from $(\mathbb{H}^2, d_{hyp})$ to $(\mathbb{B}^2, d_{\mathbb{B}^2})$.

Proof

When $z \in \mathbb{R}$, $|\Phi(z)| = 1$. This means Φ sends $\mathbb{R} \cup \{\infty\}$ to the unit circle. Next, Φ sends $\mathbb{H}^2$ to either the inside or outside of the unit circle in $\mathbb{C} \cup \{\infty\}$. Since $\Phi(i) = 0$, we know $\Phi(\mathbb{H}^2)$ is equivalent to the inside of the $\mathbb{B}^2$ unit circle.

Let $D_z\Phi : \mathbb{C} \longrightarrow \mathbb{C}$ be the differential of Φ at $z \in \mathbb{H}^2$. Then, by definition, a vector v based at z has $\mathbb{B}^2$-norm

$$\| D_z\Phi(v) \|_{\mathbb{B}^2} = \frac{2}{1 - |\Phi(z)|^2} \| D_z\Phi(v) \|_{euc}.$$

According to the previous proposition, $\| D_z\Phi(v) \|_{euc} = \left\| -\frac{2i}{(z+i)^2} v \right\|_{euc}$ because $a = -1$, $b = i$, $c = 1$, and $d = i$. Thus,

$$\begin{aligned}
\| D_z\Phi(v) \|_{\mathbb{B}^2} &= \frac{2}{1 - |\frac{-z+i}{z+i}|^2} \left\| -\frac{2i}{(z+i)^2} v \right\|_{euc} \\
&= \frac{4}{|z+i|^2 - |-z+i|^2} \| v \|_{euc} \\
&= \frac{4}{(z+i)(\bar{z}-i) - (-z+i)(-\bar{z}-i)} \| v \|_{euc} \\
&= \frac{2}{i(\bar{z}-z)} \| v \|_{euc}.
\end{aligned}$$

Since $i(\bar{z} - z)$ equals the y coordinate of $z = x + iy$, we get

$$\| D_z\Phi(v) \|_{\mathbb{B}^2} = \frac{1}{Im(z)} \| v \|_{euc}.$$

Finally, by the definition of the hyperbolic norm,

$$\| D_z\Phi(v) \|_{\mathbb{B}^2} = \| v \|_{hyp}.$$

Therefore, Φ sends a curve to a curve in $\mathbb{B}^2$ such that the lengths are equivalent in both the upper-half plane and the disk model. Thus, taking the infimum of these curves, $d_{\mathbb{B}^2}(\Phi(P), \Phi(Q)) = d_{hyp}(P, Q)\ \forall P, Q \in \mathbb{H}^2$. Which is the definition of an isometry. □

References

[1] F. Bonahon.
Low-Dimensional Geometry: From Euclidean Surfaces to Hyperbolic Knots.
American Mathematical Society, 1955.

Excursion into Ergodic Theory

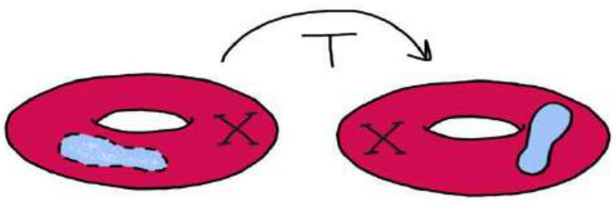
Samuel Alipour-fard, Justin Rogers

Why Ergodic Theory?

Ergodic Theory was born when Poincaré began addressing the motion of celestial bodies with measure-theoretic techniques. The tools Poincare developed for this problem have remarkably general applications. Although ergodic theory originated in the solution of a physical problem, it is now a fully-fledged branch of math with applications to many other subfields.

However, let us begin with the humble origins of ergodic theory in modelling physical systems. We model a **Dynamical System** as a triple **(X, μ, T)**, where (X, μ) is a finite measure space, and T is a is **measure-preserving** transformation: $\mu(T^{-1}(A)) = \mu(A)$ for measurable A.

T represents the evolution of our system across a small time step:



Poincaré Recurrence

Using our dynamical system, we say that **T is recurrent if time evolution brings almost every point near its initial position:**

T is recurrent

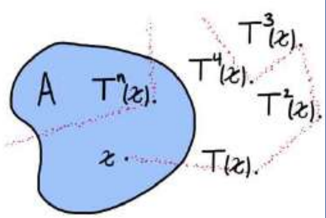
$\Leftrightarrow$

For any measurable set

$A \in$ X,

and almost every $x \in A$,

$\exists n > 0: T^n(x) \in A$



As Poincaré began studying celestial dynamics with measure theory, he stumbled upon a miraculous result:

Poincaré Recurrence Theorem:
A measure-preserving transformation T on a finite measure space (X, μ) is recurrent!

The proof is quite beautiful – you should check it out! (Silva p. 88)

Mixing It Up

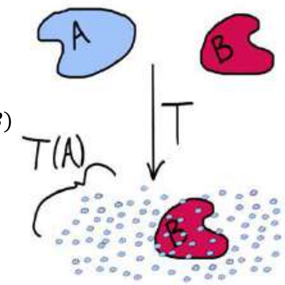
Going back to our dynamical system (X, μ, T), we say that **the map T is mixing if time evolution scrambles up the space:**

T is mixing

$\Leftrightarrow$

$$\lim_{n\to\infty} \mu(T^n(A) \cap B) = \mu(A)\mu(B)$$

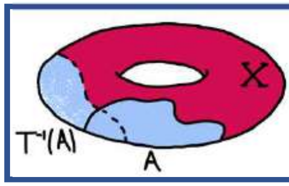
for all measurable A and B



This is a fun definition! If a random point x is in A, then this tells us about the probability that x is also in B. If T is mixing, applying T to x enough times will erase that information: for large n, the statements "x is in T^n(A)" and "x is in B" are independent.

What The Heck Is Ergodicity?

It's often too restrictive to require T to be mixing, so it's useful to define a larger class of maps: those with an "average mixing", or **ergodic** property.



T is ergodic

$\Leftrightarrow$

T^{-1}(A) = A implies

μ(A) = 0 or μ(A^c) = 0

Equivalently, we can say

T is ergodic $\Leftrightarrow$ $\lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} \mu(T^i(A) \cap B) = \mu(A)\mu(B)$

Here we applied a common analytical trick to the definition of mixing : we replace a sequence with its average values. The old sequences still converge, but we gain some new convergent sequences too!

The Big Kahuna

You may at first be a bit skeptical of ergodicity. We have given you some definitions and told you that they are important, but what can they do for you? It turns out they can be useful in a variety of applications. The key is the powerful and important

The Ergodic Theorem:

If a map T is ergodic, and f is a μ-integrable function then

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} f(T^i(x)) = \frac{1}{\mu(\mathrm{X})}\int_{\mathrm{X}} f(y)d\mu(y)$$

Read: "time averages equal space averages"

Applications

The Ergodic Theorem has some very powerful applications. Furstenberg used the ergodic theorem to produce a remarkably efficient proof of Szemeredi's theorem. The Green-Tao theorem extends his work in an important way.

Szemeredi's Theorem

Any subset of the natural numbers with positive upper density contains infinitely many arithmetic progressions of length k for all positive integers k.

Green-Tao Theorem

Let $\pi(N)$ denote the number of primes $\leq N$. If A is a subset of the prime numbers with $\limsup_{N\to\infty} \frac{|A\cap[1,N]|}{\pi(N)} > 0$, the set A contains infinitely many arithmetic progressions of length k for all positive integers k.

Ergodic theory has a miraculous ability to bring about results in fields that seem far from the dynamical systems Poincaré first considered. We hope that it will continue to spur new knowledge!

Acknowledgements and Citations

We thank the UCSB Math DRP for making this project possible.

[1] C. E. Silva. *Invitation to Ergodic Theory*. American Mathematical Society. 2007.
[2] https://www.reddit.com/r/math/comments/5mn0ou/expository_a_historical_introduction_to_ergodic/
[3] en.wikipedia.org
[4] https://terrytao.wordpress.com/2008/02/10/254a-lecture-10-the-furstenberg-correspondence-principle/

Local Waring's Problem

Geneva Schlafly with advisor Garo Sarajian

Problem

What is the smallest value s such that every residue class $a \pmod m$ can be represented by a sum of s k^{th} powers with at least one of the powers being coprime to m? In other words, given k, what is the minimum s such that we can write

$$x_1^k + \cdots + x_s^k \equiv a \pmod m$$

for each residue class a?

Is it true that $\lim_{k\to\infty} \Gamma(k) = \infty$, as conjectured in [1]? It has not even been known if $\liminf_{k\to\infty} \Gamma(k) \geq 4$.

Notation and Properties

- Let p be a prime and k, m, d be natural numbers with d even.
- Define $\gamma(k,m)$ as the smallest value s such that every residue class modulo m can be represented by a sum of s k^{th} powers with at least one of the powers coprime to m.
- Let $\Gamma(k)$ be the smallest value s such that for every m, every residue class modulo m can be represented by a sum of s k^{th} powers, that is,
$$\Gamma(k) := \max_{m\in\mathbb{N}} \gamma(k,m).$$
- If $k = xy$, then $\Gamma(k) \geq \Gamma(x)$.
- For $r \in \mathbb{N}$, $\Gamma(p^r) \geq r+1$.
- Let $\omega_n(k,m)$ denote the set of residue classes a_i modulo m that can be represented as the sum of n kth powers.
- If $dk+1$ is prime, then powers of k satisfy $x^d \equiv 0$ or 1 modulo $dk+1$. Moreover, $x^d \equiv 0$ has one solution and $x^d \equiv 1$ had d solutions.

Previous Results

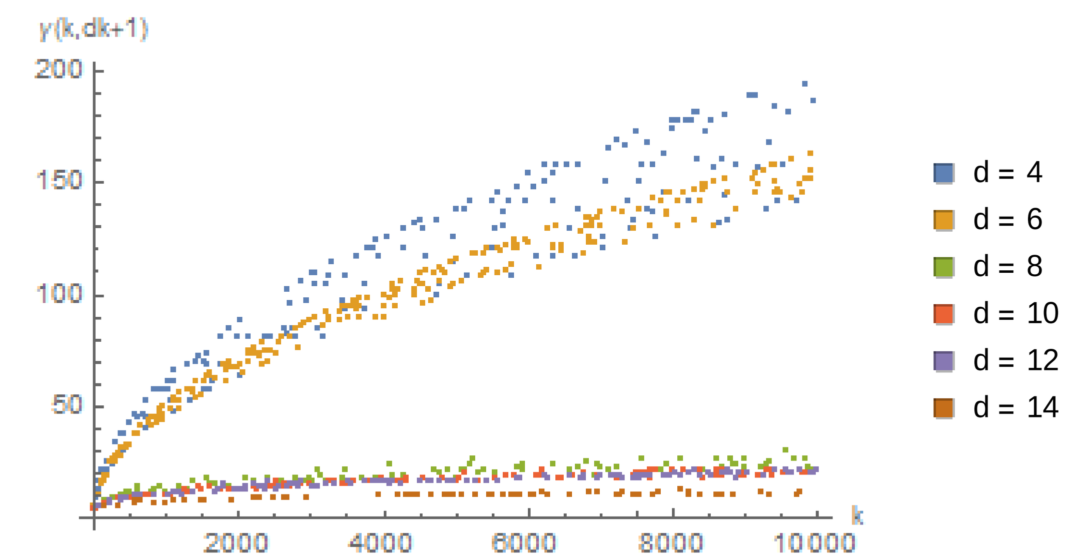
Hardy and Littlewood found the values of Γ when k is in the following classes:

1. If $k = 2^\alpha$, then $\Gamma(k) = 2^{\alpha+2}$.
2. If $k = 3\cdot 2^\alpha$, then $\Gamma(k) = 2^{\alpha+2}$.
3. If $k = p^\beta(p-1)$, then $\Gamma(k) = \frac{1}{2}p^\beta(p-1)$.
4. If $k = \frac{1}{2}p^\beta(\beta-1)$, then $\Gamma(k) = \frac{1}{2}(p^{\beta+1}-1)$.
5. If $k = p-1$, then $\Gamma(k) = p = k+1$.
6. If $k = \frac{1}{2}(p-1)$, then $\Gamma(k) = \frac{1}{2}(p-1) = k$.

Here $\alpha > 1, \beta > 0$, and the first four classes take priority. For k not in these classes, $\Gamma(k) \leq k$ They also showed that for any prime exponent k, $\Gamma(k)$ is equal to $\gamma(k,k^2)$ or $\gamma(k,dk+1)$ with $dk+1$ prime.

Trends for $\gamma(k,m)$

Consider modulo classes of the form $m = dk+1$. If we fix d, we can computationally determine $\gamma(k,dk+1)$ for a finite set of primes k.



Because $\Gamma(kk') \geq \Gamma(k)$, we only need to consider prime k to find a lower bound for $\Gamma(k)$. Frequently $\Gamma(k)$ is determined by the $\gamma(k,p)$ where p is the first smallest prime number of the form $dk+1$. For many primes k, $4k+1$ is also prime. If not, $6k+1$ is often prime. Observe $\Gamma(k)$ appears to be increasing.

Combinatorical Bound for ω_n

Each $\omega_n(k,m)$ includes $\omega_{n-1}(k,m)$. Hence, $\gamma(k,m)$ is equal to the smallest n such that $|\omega_n(k,m)| = m$. $\Gamma(k)$ relates to $\omega_n(k,m)$ over all m, but we only need to consider prime m of the form $dk+1$. So, $|\omega_1(k,dk+1)| = d+1$.

Analyzing growth of ω_n, we find an upper bound only dependent on n and d. As ω_n is $\omega_{n-1} \pm \omega_1$, the elements in ω_n, but not in ω_{n-1} are of the form $\pm a_{i_1} \pm a_{i_2} \pm \cdots \pm a_{i_n}$ where $a_i \neq 0$.

The number of distinct sums of this form is at most 2^n times the number of ways we can choose n numbers from a set of $d/2$ numbers, allowing repetition, which is $2^n\binom{d/2+n-1}{d/2-1}$. Including 0 and the new elements in each ω_j for $j < n$, we get the upper bound,

$$|\omega_n(k,dk+1)| \leq 1 + \sum_{j=1}^{n} 2^j \binom{d/2+j+1}{d/2-1}$$
$$\leq 1 + \frac{2^n}{(d/2-1)!}\sum_{j=1}^{n}\prod_{i=1}^{d/2-1}\left(\frac{d}{2}+j-i\right)$$
$$\leq 1 + \frac{2^n}{(d/2-1)!}\left[\frac{n^{d/2}}{d/2} + g(d)h(n,d)\right] =: f(n,d)$$

where the function $g(d)$ is a polynomial in d and $h(n,d)$ is a polynomial in n of degree $d/2-1$. So their product, $g(d)h(n,d)$, is $o((d/2-1)!)$.

Conclusions

Since $|\omega_n(k,m)| \leq m$, it holds that $dk+1 \leq f(n,d)$. So $d\to\infty$, i.e. $m\to\infty$, $f(n,d)\to\infty$ also. Notice if n is fixed, $f(n,d) \to 1$. Thus, n must tend toward ∞.

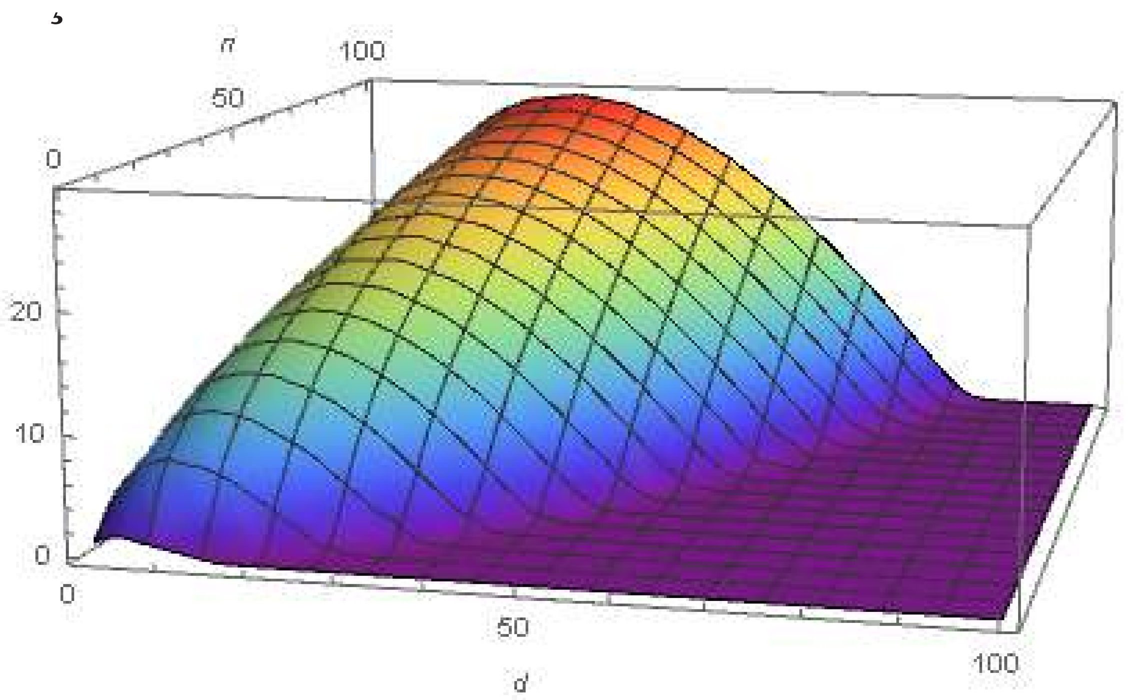
Given $M > 0$, there are only finitely many primes $p_1,\ldots p_l$ satisfying $\Gamma(p_i) < M$. Also, $\Gamma(p^r) \geq M$ for $r \geq M-1$. So, all k such that $\Gamma(k) < M$ are of the form $k = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_l^{\alpha_l}$ with $0 \leq \alpha_i \leq M-2$. Hence, there are only finitely many such k where $\Gamma(k) < M$.

Since $\gamma(k,dk+1)$ is the minimum n such that $|\omega_n(k,dk+1)| = dk+1$, each n has only finitely many pairs d,k satisfying $|\omega_n(k,dk+1)| = dk+1$. For each $n \leq M$, there are only finite number of k satisfying $f(n,d) \geq dk+1$.

Taking k large enough, we find $\omega_n(k,dk+1) < dk+1$ for all $n < M$ and all $d \in 2\mathbb{N}$. This implies that for large enough k and $dk+1$ prime, $\gamma(k,dk+1) > M$.

As $\Gamma(k) \geq \gamma(k,dk+1)$, we conclude

$$\lim_{k\to\infty}\Gamma(k) = \infty.$$



The graph above is of $\log(f(n,d))$, showing how n must continue to increase to allow $f(n,d)$ to increase.

References

[1] Hardy, G. H. and Littlewood, J. E. (1928), Some Problems of âĂIJPartitio NumerorumâĂİ (VIII): The Number $\Gamma(k)$ in Waring's Problem. Proceedings of the London Mathematical Society, s2-28: 518-542. doi:10.1112/plms/s2-28.1.518

Future Research

What is $\Gamma(k)$ where k is not in one of the known classes, such as $k = \frac{1}{4}(p-1)$? Given d, can we find bounds for $\gamma(k,dk+1)$ where $dk+1$ is prime?

How fast does $\Gamma(k)$ increase? Letting $G(k)$ denote the generalized $\Gamma(k)$, it is conjectured that $G(k) = \max\{\Gamma(k), k+1\}$.

Acknowledgements

This research was conducted as part of the Directed Reading Program at UC Santa Barbara. I would like to thank my advisor, Garo Sarajian, for all his guidance.

Isometries in the Hyperbolic Plane

Jennifer Rozenblit

Directed Reading Program, Department of Mathematics University of California, Santa Barbara

What is the Hyperbolic Plane?

The ***hyperbolic plane***, defined as the upper half plane, is

$$\mathbb{H}^2 = \{(x,y) \in \mathbb{R}^2 | y > 0\} \\ = \{z \in \mathbb{C} | Im(z) > 0\}$$

with metric $(ds)^2 = \frac{(dx)^2+(dy)^2}{y^2}$. An important characteristic of the Hyperbolic plane is that distance is preserved but looks different from Euclidean distance (explored below). As one gets closer to the x axis, perceived distance from the Euclidean standpoint looks increasingly smaller.

Metric on $\mathbb{H}^2$

In order to determine a distance function, we may look at the two types of geodesics that exist in this space. First, we can consider two vertically co-linear points $z_1 = x + iy_1$ and $z_2 = x + iy_2$, where $\gamma(t) = ((x(t), y(t)), t \in [a,b]$. The ***hyperbolic length*** of γ according to the hyperbolic metric is

$$l(\gamma) = \int_a^b \frac{\sqrt{x'(t)^2 + y'(t)^2}}{y(t)} dt \text{ or } \int_a^b ||\gamma'(t)|| dt$$

Through calculation we can see then that $\gamma(t) = log(y_2) - log(y_1)$. Thus we know that a line connecting two vertically colinear points will be a geodesic. Further, we may define ***distance*** as the distance between two points, a, b $\in \mathbb{H}^2$ as $inf\{l(\gamma)|\gamma$ is a path from a to b$\}$. We define a ***path*** to be, for points a,b $\in \mathbb{H}^2$, γ is a map such that $[0,1] \rightarrow \mathbb{H}^2$ such that γ is continuous, $\gamma(0) = a$, and $\gamma(1) = b$.
We may verify that this is a ***metric*** because the following are satisfied:

- $d(a,b) \geq 0$
- $d(a,b) = 0 \iff a = b$
- $d(a,b) = d(b,a)$; $d(a,b) \leq d(x,z) + d(z,y)$.

A ***geodesic*** is a path which minimizes the distance between two points. In $\mathbb{H}^2$ geodesics are vertical lines or half circles centered on the real axis.

Isometries

An ***isometry*** of $\mathbb{H}^2$ is a bijective map from $\mathbb{H}^2 \rightarrow \mathbb{H}^2$ that preserves the metric. The special linear group, $\mathrm{SL}_2(\mathbb{R})$, acts on $\mathbb{H}^2$ by isometries, given by

$$A \cdot z = \frac{az+b}{cz+d}$$

where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2\mathbb{R}$
We will name this map a ***fractional linear transformation*** or a ***Möbius tranformation*** $f_A : z \rightarrow \frac{az+b}{cz+d}$, where $a,b,c,d \in \mathbb{R}$ and $ad - bc = 1$. We can see that for any matrix A and its negative $-A$, the action of f_A and f_{-A} are the same. It turns out that we can identify the orientation preserving isometries with the projective special linear group

$$Isom^+\mathbb{H}^2 \cong \mathrm{SL}_2(\mathbb{R}) / \pm Id \\ \cong \mathrm{PSL}_2(\mathbb{R}).$$

Classification

Now we turn to the task of classifying these orientation preserving isometries. Orientation preserving isometries fall into three categories: ***elliptic***, ***parabolic***, and ***hyperbolic*** which will be explored in the next several sections. Their isometries can be categorized based on the number of points that they fix and their associated trace value (we will see how these are related). We know that for any $a, b \in \mathbb{H}^2$, there exists an isometry that maps a to b, and that isometries preserve geodesics. We note that for the matrix $X = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]$, the "absolute value" of the trace of X denoted $|Tr(X)| = |a+d|$. Thus, orientation preserving isometries for $\mathbb{H}^2$ fall into the three following categories:

- ***Elliptic:*** One point is fixed on $\mathbb{H}^2$, equivalently $|Tr(X)| < 2$
- ***Parabolic:*** One point is fixed on the boundary of $\mathbb{H}^2$, equivalently $|Tr(X)| = 2$
- ***Hyperbolic:*** Two points are fixed on the boundary of $\mathbb{H}^2$, equivalently $|Tr(X)| > 2$

Elliptic

Consider a fixed point $z \in \mathbb{H}^2$, and a geodesic γ passing through it. Let $f(\gamma)$ also pass through z with respect to some angle α with γ. Then, because f preserves angles, it will take any geodesic passing through z to another unique geodesic that preserves the angle α.
Thus, this is similar to a rotation in Euclidean Space, where its action on point z is based on the angle α that is created. As previously mentioned, $|Tr(X)| = |a+d| < 2$ in this case, corresponding to some $\lambda = e^{i\alpha}$ for some $\alpha \in \mathbb{R}$. Why is this the case? If we take i to be our fixed point, then we can see that $X(i) = \frac{ai+b}{ci+d} = i$. Through further calculation, we can see that $ad - bc = a^2 + b^2 = 1$, which is precisely true when $a = cos(\alpha), b = sin(\alpha)$ for some $\alpha \in [0, 2\pi)$. The elliptic isometry fixing i and rotating by α is then

$$X = \left[\begin{pmatrix} cos(\alpha) & sin(\alpha) \\ -sin(\alpha) & cos(\alpha) \end{pmatrix}\right].$$

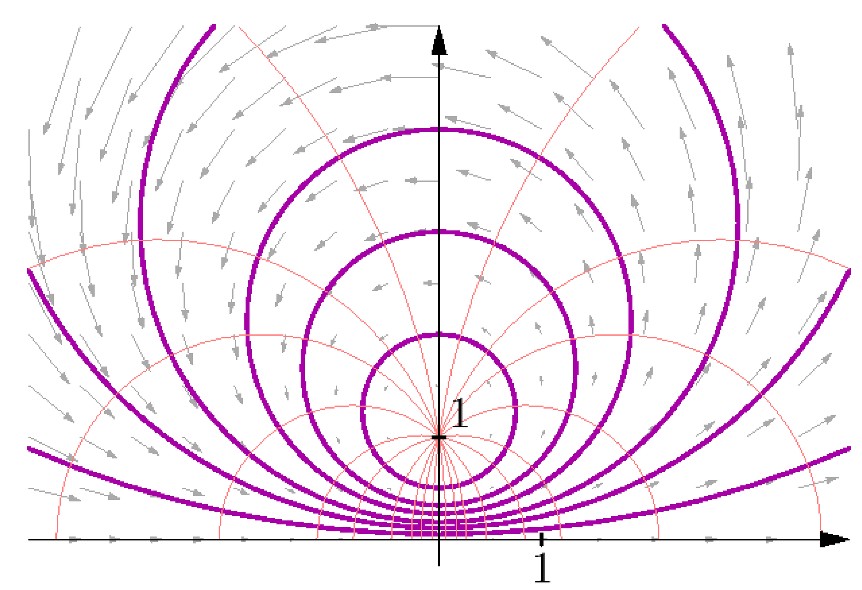


Figure 1. Elliptic isometry fixing the point (0,1), or $z = i$ [Cite: 3]

References

1. Katok, A. B., and Vaughn Climenhaga. Lectures on Surfaces: (Almost) Everything You Wanted to Know about Them. American Mathematical Society, Mathematics Advanced Study Semesters, 2008.

2. Chang, A., Snyder K. Isometries of the Hyperbolic Plane, University of Chicago, 2010.

3. Geometry of Möbius Transformations Color Illustrations, www1.maths.leeds.ac.uk/ kisilv/courses/color-figures/epal1-ws-fig.html.

I would like to sincerely thank Michelle Chu for her time and for answering my many questions, as well as Maribel Bueno and Daryl Cooper for their encouragement

Parabolic

For this situation, we will consider one fixed point on the ***ideal boundary*** $\mathbb{R} \cup \{\infty\}$ (meaning no points are fixed in the hyperbolic plane). In other words, parabolic transformations are similar to elliptic ones, except in this case the angle α that was previously preserved is lost as a distinct invariant. Parabolic isometries can also be referred to as *translations* $\gamma : z \rightarrow z + s$. Why does $|Tr(x)| = 2$ in this case? If the fixed point is at infinity, we will denote this as $z = \infty$, and $A(z) = \frac{az+b}{cz+d} = z$, which implies that $c = 0$, otherwise $\frac{a}{c} \neq \infty$. Thus, z can be re-written as $z = \frac{b}{d-a}$, where then $d = a$ for $z = \infty$. In other words, the matrix for parabolic transformations can be considered

$$X = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}.$$

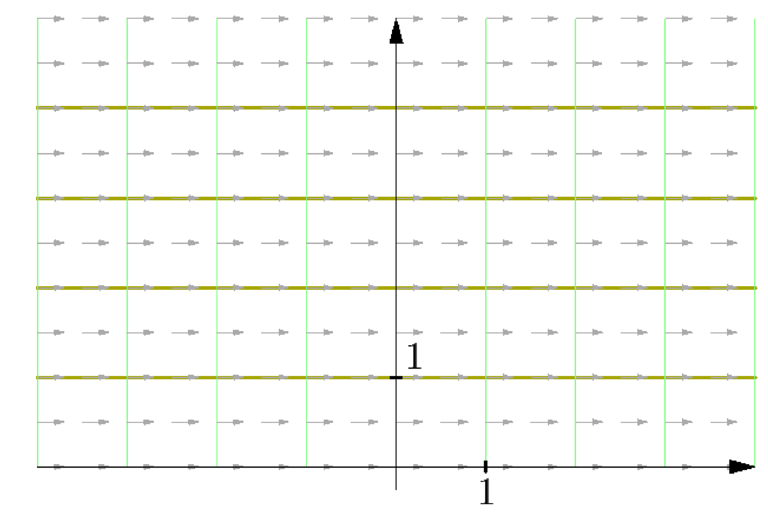


Figure 2. Parabolic isometry fixing $z = \infty$ [Cite:3]

Hyperbolic

In this case, we will fix two points w_1, w_2 at the ideal boundary, where without loss of generality, we will consider $w_1 < w_2$. As previously mentioned, $|Tr(x)| : |a+d| < 2$, but why does the number of fixed points correspond this trace value? If we let $w_1 = 0, w_2 = \infty$, then by plugging into our Möbius transformation, we can see that since $c = 0, b = 0$, and our matrix representation of hyperbolic transformations is

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \text{ or } \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \text{ since } |det(X)| = ad = 1.$$

Since in this case our points w_1, w_2 are fixed, and we know that there is a unique geodesic that takes on point to the other, f acts as a translation along this curve at some fixed distance, where the geodesic γ is the only geodesic invariant under this transformation.

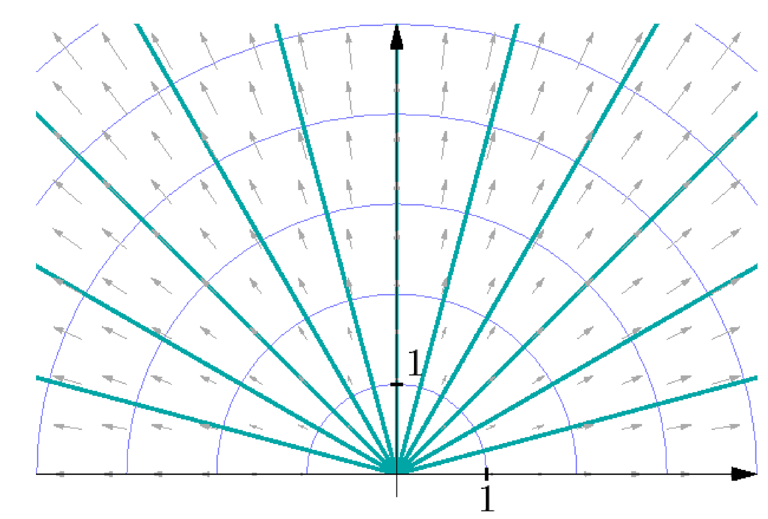


Figure 3.
Hyperbolic isometry fixing $z = 0$ and $z = \infty$ [Cite: 3].

Not Your Ordinary Knot: Knot Invariants

Emily Lopez and Iris Moininazeri

Mentors: Marcos Reyes and Jamie Vandeveer

Department of Mathematics, University of California, Santa Barbara

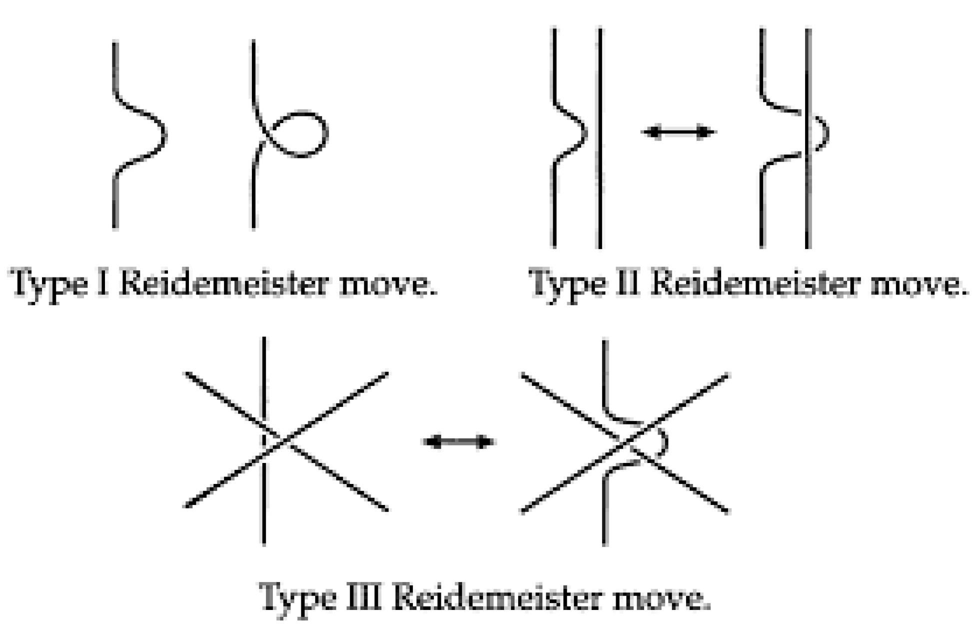
Background of Knot Theory

Knot Theory was originally created to tabulate distinguishable knots. Our goal is to be able to show there exists other knots distinguishable from the unknot. Knot Theory has applications in biology, chemistry, and physics including DNA and synthesis of knotted molecules. [See [1] for more details]

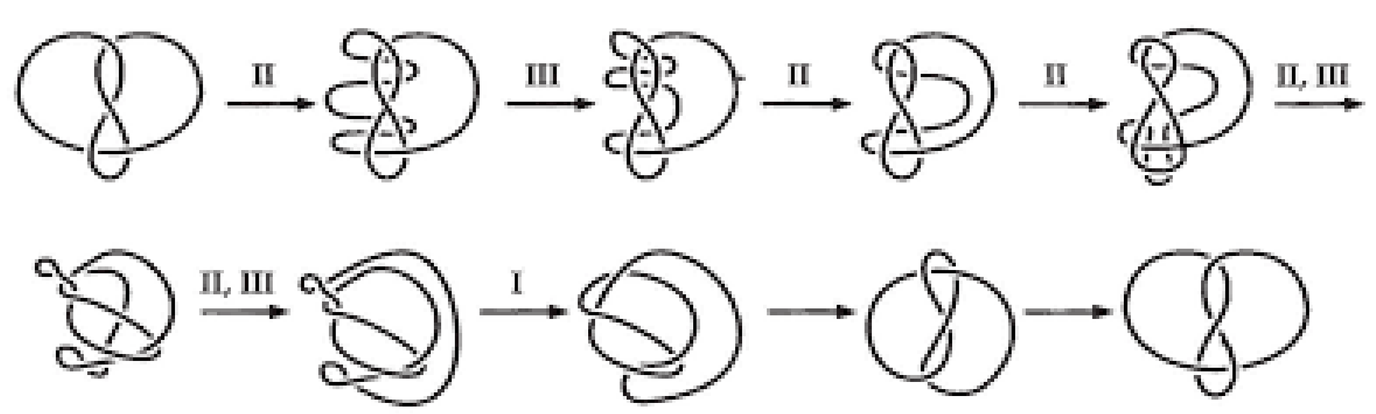
- A **knot** is a circle imbedded in $\mathbb{R}^3$.
- A **link** is a set of knotted loops tangled together.
- A **strand** is a piece of the link that goes from one undercrossing to another with only an overcrossing in between.
- A knot can be deformed to different projections. Two knots are said to be the same knot if one can be de-tangled to be a projection of the other.
- A **knot invariant** is a quantity defined for each knot which is the same for equivalent knots. This enables us to distinguish knots from one another.
- In this presentation, we provide a brief overview of knot invariants and their importance.

Reidemeister moves

- Different knot projections can be obtained through a series of the three **Reidemeister moves**



- **Example:** The figure 8 knot is equivalent to its mirror image.



- There is not a limit on the number of Reidemeister moves it can take to get from one knot projection to another, which makes it an ineffective way to determine whether two knots are distinct.

Tricolorability

- Tricolorability enables us to determine that there exists other knots that are not equivalent to the unknot.
- A projection of a knot is **tricolorable** if each strand in the projection can be colored one of three colors, so that at each crossing, either three different colors come together or three of the same color come together. At minimum two colors must be used in the coloring.

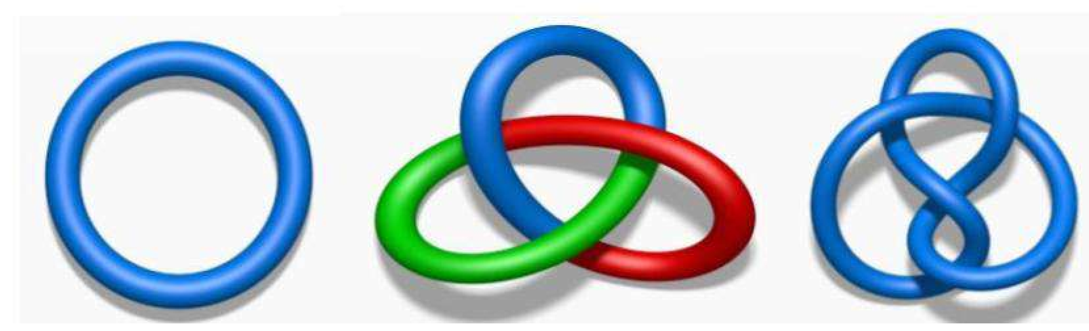


Fig. 1: Coloring of the Unknot, Trefoil knot, and Figure eight knot

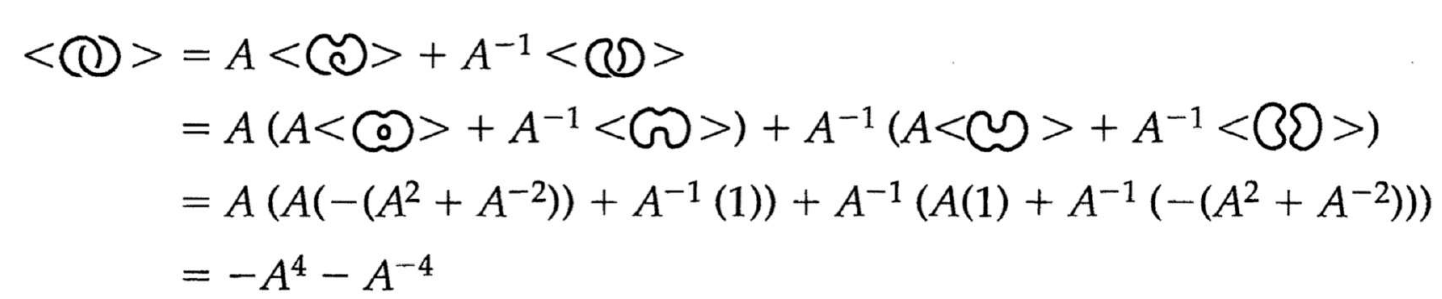
- Tricolorability fails to show that knots that are tricolorable (resp. non-tricolorable) are distinct. We seek for another invariant that provides stronger results.

Bracket Polynomials

- The goal is to be able to associate a polynomial to a knot, so that when the polynomial is computed, any two projections of a knot yield the same polynomial.
- The **Bracket polynomial** is obtained from the following rules, where $\langle K \rangle$ denotes the bracket polynomial for knot K.

1. $\langle \bigcirc \rangle = 1$
2. $\langle L \cup \bigcirc \rangle = (-A^2 - A^{-2})\langle L \rangle$
3. $\langle \times \rangle = A\,\langle \asymp \rangle + A^{-1}\,\langle)(\rangle$

- The bracket polynomial is not invariant under reidemeister move 1.
- **Example:** The bracket polynomial for the Hopf link is computed below.

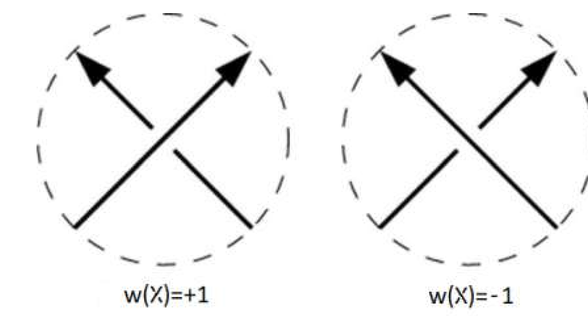


Jones Polynomial

- To obtain the Jones Polynomial we must first create the X polynomial that is invariant under all Reidemeister moves defined below:

$$X\langle L \rangle = (-A^3)^{-w(L)}\langle L \rangle$$

Where the writhe is the sum of $+1's$ or $-1's$ given to a crossing once an orientation is placed.



- The jones polynomial is obtained from the X polynomial by replacing each A with $t^{-1/4}$
- **Example:** We find the X polynomial for the trefoil knot:

  - First we find the writhe of the trefoil knot, which is 3. The bracket polynomial is

$$(A^{-7} - A^{-3} - A^5)$$

Therefore the X polynomial is

$$\begin{aligned} X\langle L \rangle &= (-A^3)^{-3}(A^{-7} - A^{-3} - A^5) \\ &= A^{-4} + A^{-12} - A^{-16}. \end{aligned}$$

and the corresponding Jones Polynomial is

$$-t^4 + t^3 + t^1$$

Acknowledgements

We would like to thank Marcos Reyes and Jamie Vandeveer for mentoring us and the UCSB Directed Reading Program for providing us this unique opportunity.

References

[1] Adam, C.C, .1994. The Knot Book. Amer. Math. Soc

Compactness in Topology: Tychonoff's Theorem

Hangqi Liang† Mentor: Micah Pedrick ‡

†Department of Mathematics University of California: Santa Barbara

The Study of Topology

Topology in some sense generalizes the properties in metric space. In the abstraction of concepts in analysis, we are allowed to talk about open sets, limits, convergence or other concepts in some spaces which might not be a metric space. In particular, one property we focus on in this poster is compactness.

Topological Space and Open Sets

Definition. Suppose X is a set. Then $\mathcal{J}$ is a **topology** on X if and only if $\mathcal{J}$ is a collection of subsets of X such that

1. $\emptyset \in \mathcal{J}$,
2. $X \in \mathcal{J}$,
3. if $U, V \in \mathcal{J}$, then $U \cap V \in J$, and
4. if $\{U_\alpha\}_{\alpha\in\Omega}$ is any collection of elements of $\mathcal{J}$, then $\bigcup\limits_{\alpha\in\Omega} U_\alpha \in \mathcal{J}$.

Definition. A **topological space** is an ordered pair $(X, \mathcal{J})$ such that X is a set and $\mathcal{J}$ is a Topology on X.

Definition. A set $U \subset X$ is called an open set in $(X, \mathcal{J})$ if and only if $U \in \mathcal{J}$.

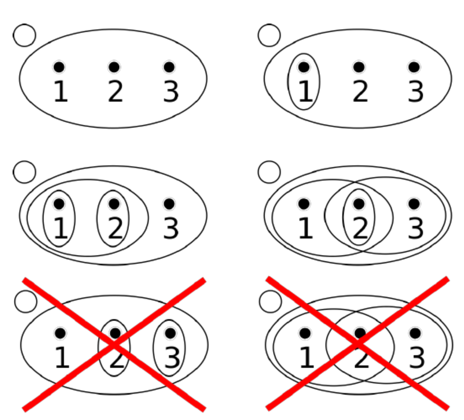


Fig. 1: Four examples which are Topologies and two which are not on the set 1,2,3

Another example of Topological space would be $(\mathbb{R}^n, \mathbb{R}^n_{std})$ for $\mathbb{R}^n_{std}$ is the set of open sets in $\mathbb{R}^n$ in the real analysis sense i.e. for every $E \in \mathbb{R}^n_{std}$ and every $x \in E$, x is an interior point of E. We also say $\mathbb{R}^n_{std}$ is the **standard topology** of $\mathbb{R}^n$.

Basis and Subbasis of a Topology

Similar to the idea of basis of a vector space, every elements of $\mathcal{J}$ is a union of elements in β if β is a **basis** of $\mathcal{J}$. Furthermore, if collection of all finite intersections of a set S is a basis, then S is a **subbasis**.

One example would be $\{(a.b) : a, b \in \mathbb{R}\}$ and $\{(a, \infty) : a \in \mathbb{R}\} \cup \{(-\infty, b) : b \in \mathbb{R}\}$ which are basis and subbaiss of $(\mathbb{R}, \mathbb{R}_{std})$ respectively.

Compactness in Topological Space

With the topological definition of open sets, we hence have our topological definition of compact sets.

Definition. A set $E \subset X$ is **compact** in $(X, \mathcal{J})$ if and only if every open cover of E has a finite cover.

Product Topology

With definition of topology given before, it is natural to induce the product topology of Cartesian product of topological spaces in the following way.

Definition. Suppose X and Y are topological spaces. The **product topology** of $X \times Y$ is the topology whose basis is all sets of the form $U \times V$ such that U is open in X and V is open in Y.

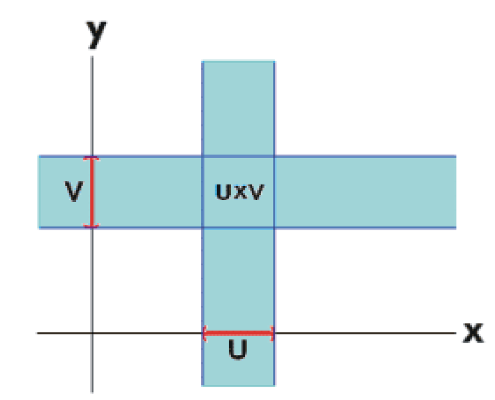


Fig. 2: An open set $U \times V$ in $X \times Y$

With all needed definitions introduced, we may finally see how powerful the topological approach to compactness is.

Alexander Subbasis Theorem

Theorem. Let S be a subbasis of X. Then X is compact if and only if every subbasic open cover has a finite cover.

Outline. Suppose the contradiction and use Zorn's lemma to find a maximal open cover Ω.Note that $S \cap \Omega$ is not an open cover and hence use maximality of Ω to construct a finite cover of Ω.

Proof. We will only prove the converse in this part. Assume that every subbasic cover has a finite cover and suppose the contradiction that X is not compact. Then by Zorn's lemma, there exists a maximal open cover Ω with no finite cover. Noticed that $\Omega \cap S$ cannot cover X by our assumption about subbasic cover. Let $x \in X - \bigcup\limits_{A\in\Omega\cap S} A$. This follows that $x \in U$ for some $U \in \Omega - S$ and there exists $S_1, .., S_n \in S$ such that $x \in \bigcap\limits_{i=1}^{n} S_i \subset U$. It is clear that $S_i \notin \Omega$. By maximal property of Ω, for every S_i, there exists $C^i_1, ..., C^i_{k_i} \in \Omega$ such that $\{S_i, C^i_1, ..., C^i_{k_i}\}$ covers X. This follows that $\{C^i_j\}^{n}_{i=1}{}^{k_i}_{j=1} \cup \{\bigcap\limits_{i=1}^{n} S_i\}$ is a finite cover of X. This implies that $\{C^i_j\}^{n}_{i=1}{}^{k_i}_{j=1} \cup \{U\}$ also covers X which is a contradiction.

Tychonoff's Theorem

Theorem. Any product of compact set is compact.

Proof. Let $X = \prod\limits_{\alpha\in\Omega} X_\alpha$ be a product of compact sets X_α. Let $\mathcal{O}_{\alpha,A} = \{f(\alpha) \in A\}$. Noticed that $S = \{\mathcal{O}_{\alpha,A} : \{f(\alpha) : \alpha \in \Omega$,A is open in $X_\alpha\}$. Suppose the contradiction that there exists a subbaic cover $\{\mathcal{O}_{\alpha,A}\}_{\alpha\in J, A\in X(\alpha)}$ of X with no finite cover for $J \subset \Omega$ and $X(\alpha)$ a collection of open sets in X_α. Note that for every α, $\{A\}_{A\in X(\alpha)}$ cannot cover X_α otherwise we will $\{A_1, .., A_n\} \subset X(\alpha)$ covering X_α which implies that $\{\mathcal{O}_{\alpha,A_1}\}^n_{i=1}$ covers X. This follows that $\beta_\alpha = \bigcap\limits_{A\in X(\alpha)} A^c$ is not empty. By axiom of choice, there exists $f \in X$ such that $f \in \prod\limits_{\alpha\in J} \beta_\alpha$. By the construction, $f \notin \{\mathcal{O}_{\alpha,A}\}_{\alpha\in J, A\in X(\alpha)}$ which is a contradiction.

Application

One result we may obtain from Tychonoff's Theorem is that for any $a, b \in \mathbb{R}$, $[a, b]^\infty$ is a compact set which is hard to prove using analysis approach. Another interesting result is that it simplifies the proof of Arzelà–Ascoli theorem.

Arzelà–Ascoli theorem. If $\mathcal{F}$ is a uniformly bounded and equicontinuous family of continuous real valued functions on $E \subset \mathbb{R}^n$, then every sequence $\{f_n\}$ in $\mathcal{F}$ has a subsequence converging uniformly to $f \in C(E, \mathbb{R})$.

Proof. Note that $\mathcal{F} \subset \prod\limits_{x\in D} [-M, M]$ for some $M < \infty$ as $\mathcal{F}$ is uniformly bounded. By Tychonoff's Theorem, $\prod\limits_{x\in D} [-M, M]$ is compact! This implies that a subsequence f_{n_k} must converge to $f \in \prod\limits_{x\in D} [-M, M]$ pointwise. Then by equicontinity of $\mathcal{F}$ we may conclude that f_{n_k} converge to f uniformly.

Remarks

Noticed the compactness implied by Tychonoff's Theorem is based on the product topology. We apply it directly in previous part as product topology of $\mathbb{R}^\infty$ is exactly $\mathbb{R}^\infty_{std}$. In other situation, one has to first figure out the relation between the product topology and specific topology of the product space.

Acknowledgements

This reading was supported by the Directed Reading Program of UCSB.

References

Michael Starbird and Francis Su, Topology Through Inquiry, AMS/MAA Texts, forthcoming, 2019.

Proving the Fundamental Theorem of Algebra Using Matrix Actions on $\mathbb{R}^n$

Brian Cheng

University of California Santa Barbara Directed Reading Program 2018-2019

Fundamental Theorem of Algebra

Every real polynomial can be expressed as the product of real linear and real quadratic factors.

This implies that every real, odd degree polynomial has at least one real linear factor, and therefore, at least one real root.

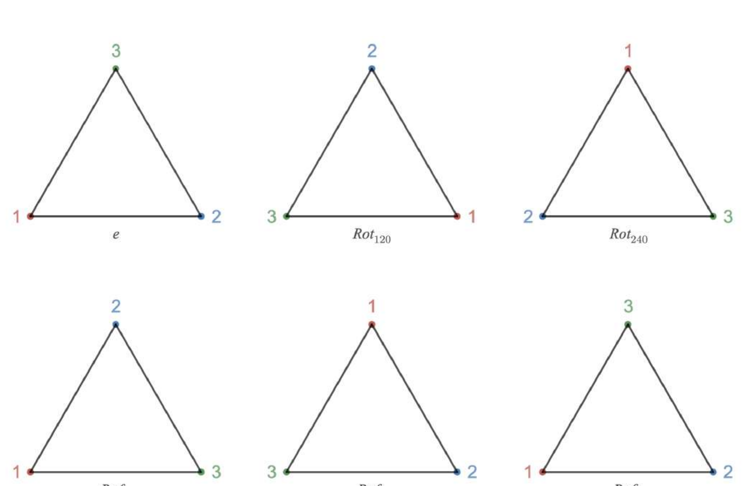
Groups

Definition: A group G is a set of elements together with a binary operation, $\cdot$, (called the group operation), that satisfy the following:

- Closure: If $a, b \in G$, then the product $a \cdot b \in G$.
- Associativity: For all $a, b, c \in G$,
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
- Identity: There exists an element $e \in G$ such that
$$e \cdot a = a \cdot e = a \text{ for all } a \in G.$$
- Inverses: For all $a \in G$, there exists an element $a^{-1} \in G$ such that
$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

Examples of Groups:

- The integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ form a group under addition.
- The nonzero integers modulo 5, $\mathbb{Z}_5 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ form a group under multiplication.
- The dihedral group D_3 is the symmetry group of the triangle and forms a group under composition.



- The general linear group forms a group under matrix multiplication
$$GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0 \right\}$$

Group Actions

Definition: A group G is said to act on a set X when there is a map $. : G \times X \to X$ such that the following conditions hold for all $x \in X$: (1) Let $e \in G$ be the identity. Then $e.x = x$. (2) For all $g, h \in G$, $g.(h.x) = (gh).x$

Examples of a Matrix Action: Consider the matrix $A = \begin{pmatrix} cos(\pi/2) & -sin(\pi/2) \\ sin(\pi/2) & cos(\pi/2) \end{pmatrix}$. Applying A to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ would map it to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Applying A to $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$ would then map it to $\begin{pmatrix} -3 \\ 2 \end{pmatrix}$.

Eigenvalues, Eigenvectors, Eigenspaces

Definition: Let A be a linear transformation represented by a matrix A. If there is a vector $X \in \mathbb{R}^n \neq 0$ such that $Ax = \lambda x$ for some scalar λ, then λ is called the eigenvalue of A with the corresponding eigenvector X. The union of the zero vector and the set of all eigenvectors corresponding to eigenvalues λ is a subspace of $\mathbb{R}^n$ known as the eigenspace of λ

Finding Eigenstuff: $A = \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix}$

$$Ax = \lambda x \to Ax - \lambda x = 0 \to (A - I\lambda)x = 0$$
$$det(A - \lambda I) = det \begin{pmatrix} -1-\lambda & 2 \\ 0 & -1-\lambda \end{pmatrix}$$
$$= (\lambda + 1)^2, \lambda = -1$$
$$\begin{pmatrix} -1-(-1) & 2 \\ 0 & -1-(-1) \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} == \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
$$x = x, y = 0$$
$$span = x \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

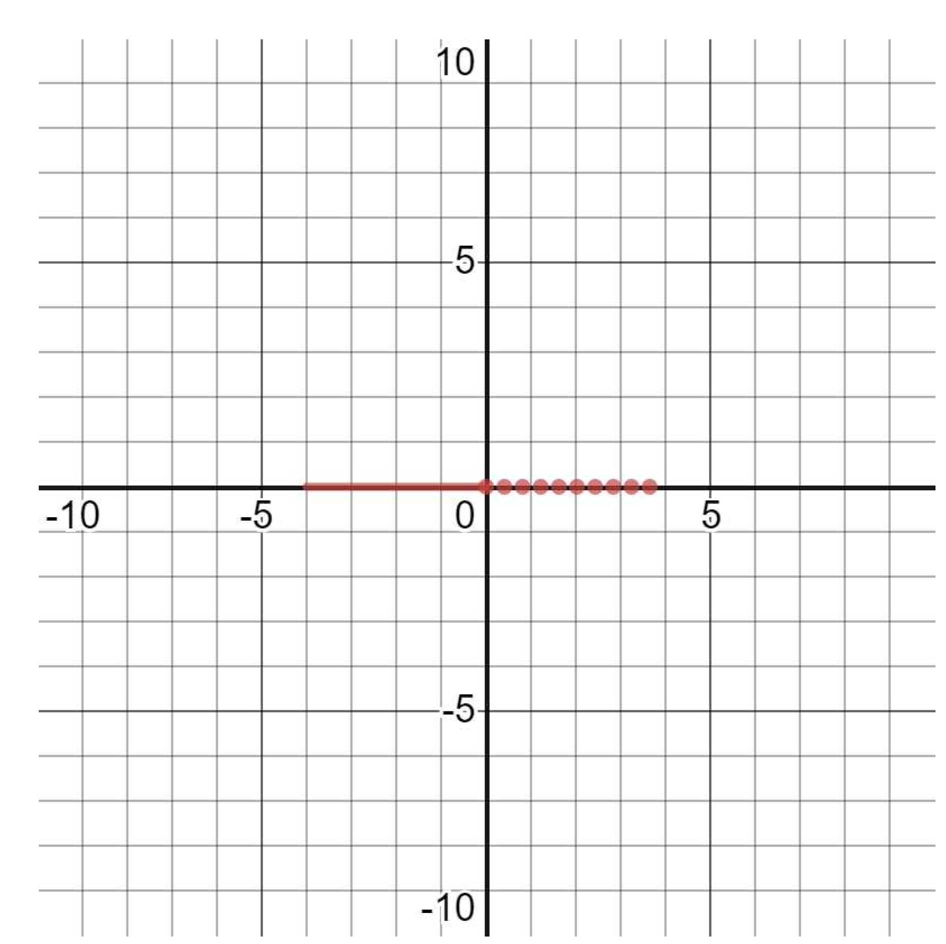
Eigenvalue: $\lambda = -1$, Eigenvector: $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

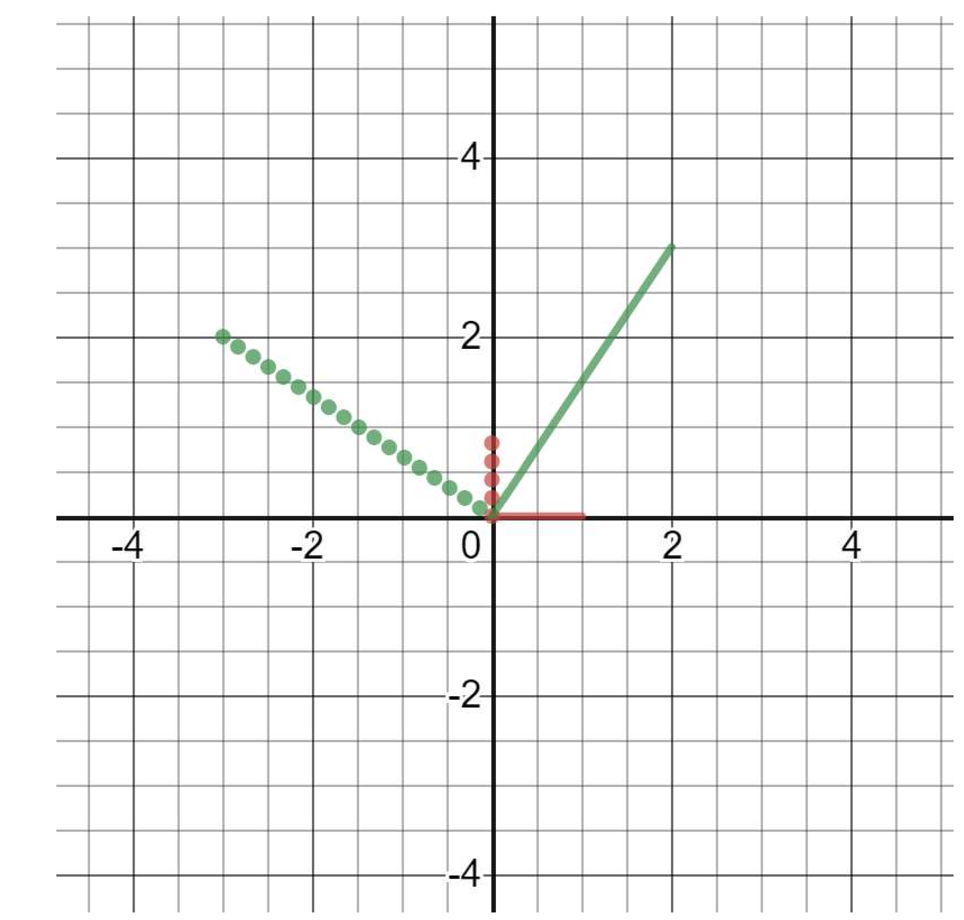
Eigenspace: $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Invariant Subspace

Definition: Suppose that $T: V \to V$ is a linear transformation and W is a subspace of V. Then suppose $T(w) \in W$ for every $w \in W$. Then W is an invariant subspace of V relative to T.

Take the matrix $A = \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix}$. If we apply the matrix to $\begin{pmatrix} -4 \\ 0 \end{pmatrix}$ (a scalar multiple of an eigenvector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ of matrix A), we get $\begin{pmatrix} 4 \\ 0 \end{pmatrix}$, which is also a scalar multiple of the eigenvector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. This means that the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is the invarient subspace of matrix A, which corresponds with the eigenspace of matrix A.





Question: Can you move a vector in $\mathbb{R}^3$ via a matrix action such that you have no invariant subspace?

Argument

No. One cannot move a vector in $\mathbb{R}^3$ via a matrix action such that there is no invariant subspace. Thus, there must exist at least one real invariant subspace, which implies there must be an eigenvector and eigenvalue that correspond to that invariant subspace. Since there exists a at least one eigenvalue, that means the the characteristic polynomial for the matrix action must have at least one real root.

Acknowledgements

- Meier, John, *Groups, Graphs and Trees*
- Wolfram MathWorld

The Generalized Ping Pong Lemma

Ryan Hayden† and Nic Brody‡

†Department of Mathematics, University of California, Santa Barbara
‡Department of Mathematics, University of California, Berkeley

Overview

Given a topological space X, one often wants to understand its fundamental group. The Seifert-van Kampen theorem provides a method for computing or understanding the fundamental group of X in terms of the fundamental groups of simpler pieces. The combinatorial group theory involved here leads to two notions - *that of an amalgamated free product, and that of an HNN extension.* These two constructions are generalized by the idea of a graph of groups, due to Serre.

Moreover, the theory of covering spaces gives a connection between fundamental groups and group actions. In particular, the fundamental group acts nicely on the universal cover of X.

Abstracting just to the setting of a group G acting on a simply connected space, we would like an analog of the Seifert-van Kampen theorem, so we can understand the relationship between the group action and the combinatorial decomposition mentioned above. The following combination theorems may be seen as generalizations of the Seifert-van Kampen theorem.

The Ping Pong Lemma for Free Groups

In [1], the Ping Pong Lemma for Free Groups (of rank 2) is given as follows:

Suppose a and b generate a group G that acts on a set X. If:

1. *X has disjoint nonempty subsets X_a and X_b, and*
2. *$a^k(X_b) \subset X_a$ and $b^k(X_a) \subset X_b$ for all nonzero powers k.*

then $G = \langle a, b\rangle$ is isomorphic to a free group of rank 2.

We also note that this lemma can easily be extended to free groups of higher rank.

Amalgamated Free Products

We now consider a slight generalization of the free product, known as a free product with amalgamation. An amalgamated free product is similar to a free product, however there is some "mixing" allowed between the two groups being combined. As in [2], we define the amalgamated free product as follows:

Let G_1,G_2 and H be groups. Then fix injective homomorphisms $\iota_{G_1} : H \longrightarrow G_1$ and $\iota_{G_2} : H \longrightarrow G_2$. Now, let N be the minimal normal subgroup of $G_1 \star G_2$ generated by all elements of the form $\iota_{G_1}(h)\iota_{G_2}(h)^{-1}$ for $h \in H$. Then, the free product of G_1 and G_2 amalgamated along H is

$$G_1 \star_H G_2 = (G_1 \star G_2)/N$$

Moreover, we can describe the amalgamated free product $G_1 \star_H G_2$ via group presentations: If $G_1 \cong \langle S_{G_1}|R_{G_1}\rangle$ and $G_2 \cong \langle S_{G_2}|R_{G_2}\rangle$, then

$$G_1 \star_H G_2 \cong \langle S_{G_1} \sqcup S_{G_2} | R_{G_1} \sqcup R_{G_2} \cup \{i_{G_1}(h) i_{G_2}(h)^{-1} | h \in H\}\rangle.$$

In other words, the free product with amalgamation can be thought of as the group obtained by "gluing" two groups along a subgroup of each. As such there is a natural connection between amalgamated free products and the Seifert-van Kampen theorem, which gives instructions for computing the fundamental group of a space obtained by "gluing" two spaces along a subspace in each.

The Ping Pong Lemma for Amalgamated Free Products

Suppose groups G_1 and G_2 each act faithfully on a set X and let $\phi_i : G_i \longrightarrow Aut(X)$ be the corresponding action map. If:

1. *For a group H, there exist injections $\iota_i : H \longrightarrow G_i$ such that $\phi_1\iota_1 = \phi_2\iota_2$*
2. *There exist disjoint, non-empty subsets X_1, $X_2 \subseteq X$ such that $g_1(X_2) \subseteq X_1$, $\forall g_1 \in G_1 \setminus \iota_1(H)$ and $g_2(X_1) \subseteq X_2$, $\forall g_2 \in G_2 \setminus \iota_2(H)$*
3. *H is not of index 2 in either G_1 or G_2 (ie: $[G_1 : H] \neq 2$ or $[G_2 : H] \neq 2$)*

Then the group generated by $\phi_1(G_1)$ and $\phi_2(G_2)$ is isomorphic to the free product of G_1 and G_2 amalgamated along H. In other words, $\langle\phi_1(G_1), \phi_2(G_2)\rangle = G_1 \star_H G_2$.

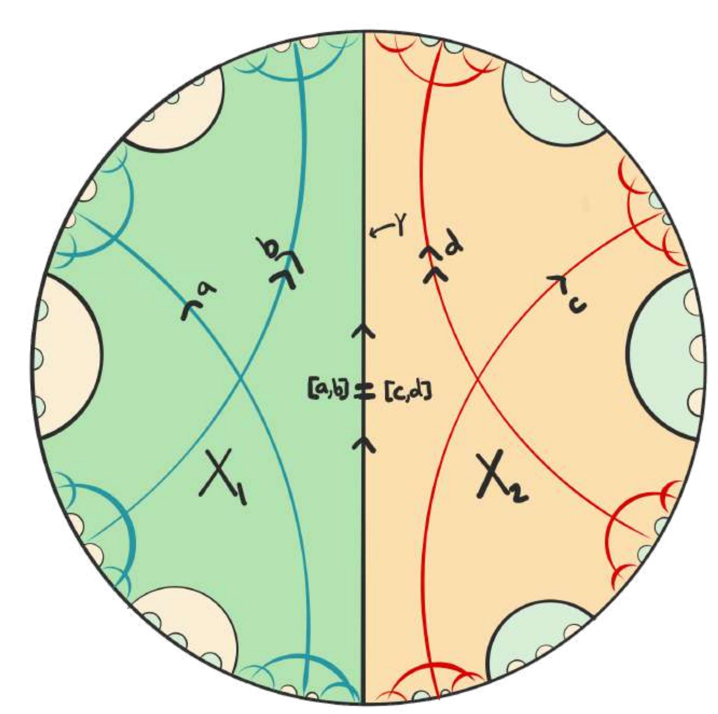


Fig. 1: Ping Pong in action

The proof is as follows:

Let $\phi : G_1 \star_H G_2 \longrightarrow Aut(X)$ where $\phi|_{G_i} = \phi_i$. First, note that $\langle\phi_1(G_1), \phi_2(G_2)\rangle \cong \phi(G_1 \star_H G_2)$, which is simply the copy in $Aut(X)$ of the free product of G_1 and G_2 amalgamated along H. Now, we want to show that the kernel of ϕ is trivial, so that we can then apply the first isomorphism theorem to show that $\langle\phi_1(G_1), \phi_2(G_2)\rangle \cong G_1 \star_H G_2$.

We first note that no element g of $\langle G_1, G_2\rangle$ of the form $g = g_1^{(1)} * g_1^{(2)} * g_2^{(1)} * \cdots * g_k^{(2)} * g_{k+1}^{(1)}$, for $g_j^{(i)} \in G_i \setminus \iota_i(H)$, is the identity since $g(X_2) \subseteq X_1$. In other words, for all such g, $g \neq 1$). We now note that every element of $G_1 \star_H G_2$ is conjugate to one of the above form (this is ensured by premise 3). As such, we observe that given any nontrivial, reduced word $w \in G_1 \star_H G_2$, $\exists z \in G_1 \star_H G_2$ which conjugates w to the form described above.

Thus, since G_1 and G_2 act faithfully, we have shown that no nontrivial reduced words in $G_1 \star_H G_2$ equal the identity. Moreover, since ϕ is a homomorphism, we know that no nontrivial reduced words in $\langle\phi_1(G_1), \phi_2(G_2)\rangle$ equal the identity. In other words, the kernel of ϕ is trivial ($ker\phi = 1$). Thus via the first isomorphism theorem, $G_1 \star_H G_2/\{1\} \cong \langle\phi_1(G_1), \phi_2(G_2)\rangle$. Hence, $G_1 \star_H G_2 \cong \langle\phi_1(G_1), \phi_2(G_2)\rangle$. As a result, we have proven that the group generated by $\phi_1(G_1)$ and $\phi_2(G_2)$ is isomorphic to the free product of G_1 and G_2 amalgamated along H.

HNN Extensions

The counter-notion of the Amalgamated Free Product is the HNN Extension, which we define as follows:

Let H and G be groups. Then fix injective homomorphisms $\iota_1 : H \longrightarrow G$, $\iota_2 : H \longrightarrow G$. Now, let $\langle t\rangle \cong \mathbb{Z}$. We then define N to be the minimal normal subgroup of $G \star \langle t\rangle$ generated by $\{t\iota_1(h)t^{-1}\iota_2(h)^{-1} | h \in H\}$. Then the HNN Extension of G relative to H is

$$G\star_H = (G \star \langle t\rangle)/N$$

As before, we can describe the HNN Extension of G relative to H via group presentations: If $G \cong \langle S_G|R_G\rangle$, then

$$G\star_H \cong \langle S_G, t | R_G, t\iota_1(h)t^{-1} = \iota_2(h)\rangle.$$

We also note that a combination theorem similar to those described above can be given for HNN extensions (ie: the Ping Pong Lemma for HNN Extensions).

Furthermore, we end by recalling the Seifert-van Kampen theorem and noting the relation between amalgamated free products and separating subspaces (where, as we noted earlier, we are essentially "gluing" two spaces along a shared subspace). Likewise, there is a similar relation between HNN extensions and non-separating subspaces.

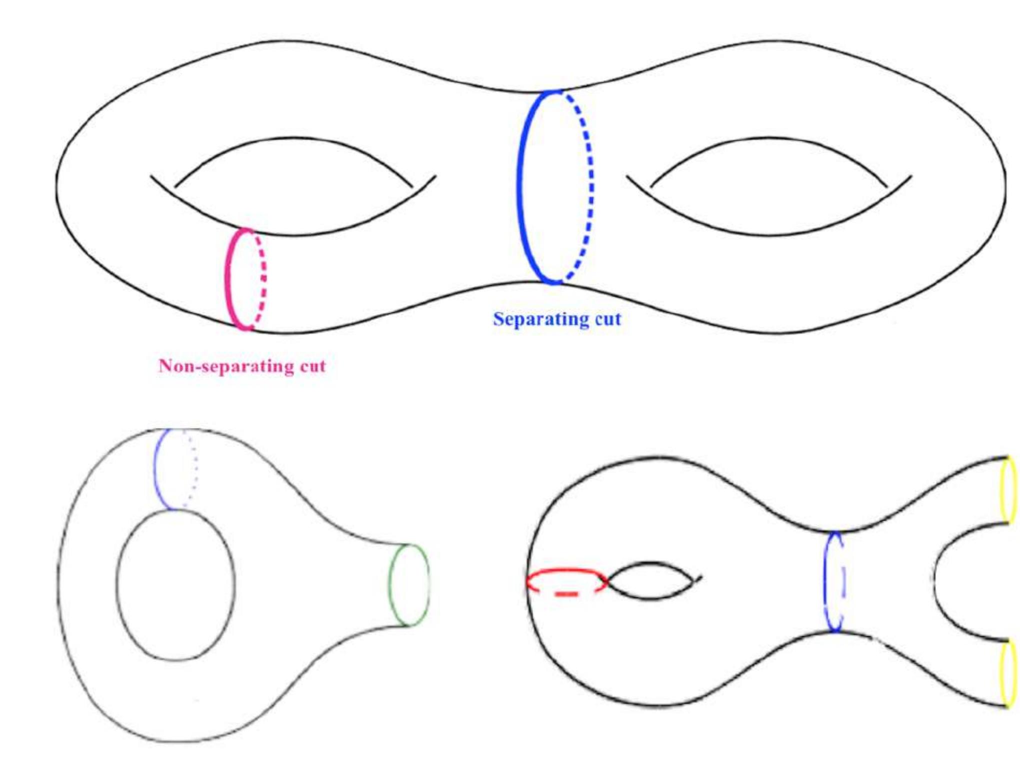


Fig. 2: Example of both a separating and a non-separating cut on a double torus

References

[1] M. Clay, D. Margalit and J. Mangahas. *The Ping Pong Lemma - Office Hours with a Geometric Group Theorist.* 2017, pgs. 85-105.

[2] M. Clay and D. Margalit. *Groups Acting on Trees - Office Hours with a Geometric Group Theorist.* 2017, pgs. 45-65.

Toric Varieties

Colbert Orta   Mentor: Sam Sehayek

Department of Mathematics UCSB

Background

- An **affine space** A^n is a set such that for $a = (a_1, ..., a_n) \in A^n, a_i \in k$ a field. For simplicity, we will usually let k= $\mathbb{C}$.
- An **affine variety** is a closed set $V \subset A^n$ that is the solution set to a set of polynomials $\{f_\alpha\}$.
- An **irreducible variety** is an affine variety X such that $X \neq X_1 \cup X_2$, where X_1, X_2 are closed proper subsets of X.
- A **normal variety** X is an irreducible affine variety where $k[X]$ is integrally closed.
- The **spectrum of a ring Spec(R)** is the set of all prime ideals in R. [1]

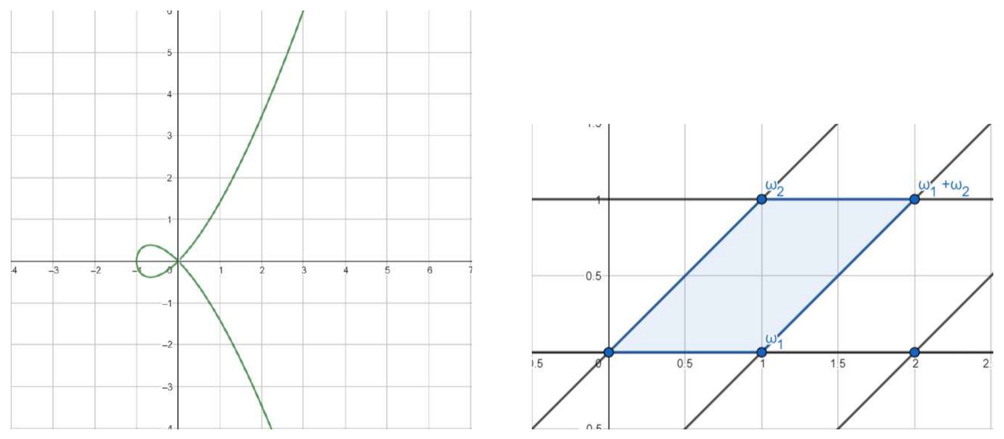


Figure 1: Left: This is the affine curve $V(y^2 - x^3 - x^2)$. Right: This is the parallelogram P_0 that shows opposite sides are congruent modulo L, the lattice.

The Complex Torus

A fundamental object in the study of Toric Varieties is the complex n- torus $\mathbf{T}^n = (\mathbb{C}^*)^n$, constructed as follows: [2]

- Define a lattice $L = \{\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\}$, where $\omega_1, \omega_2 \in \mathbb{C}$ are linearly independent over $\mathbb{R}$.
- Let $X = \mathbb{C}/L$. $\pi : \mathbb{C} \to X$ is a continuous, open mapping.
- Let $P_z = \{z + \lambda_1\omega_1 + \lambda_2\omega_2 | \lambda_i \in [0, 1]\} \subset X$. Each P_z is a compact and connected set.
- We find charts, ϕ_z to finalize the construction to show that this map is a complex manifold.
- P_z allows us to show that opposite sides are congruent modulo L, connecting this construction to the standard torus.

Toric Varieties

Toric Varieties and Properties

A **Toric Variety** is a normal variety X that contains a torus T as an open dense subset, together with an action T x $X \to X$ of T on X that extends the natural action of T on itself. [3]

We can also describe toric variety by their fans. A **fan** Δ is a set of rational strongly convex polyhedral cones σ in $N_{\mathbb{R}}$ such that 1) Each face of a cone in is also a cone in Δ, and 2) The intersection of two cones in Δ is a face of each.

We can construct a toric variety $X(\Delta)$ by gluing together disjoint **affine toric varieties,** irreducible affine varieties $U_\sigma = Spec(\mathbb{C}[S_\sigma])$, where $S_\sigma = \sigma^\wedge \cap M$. [4]

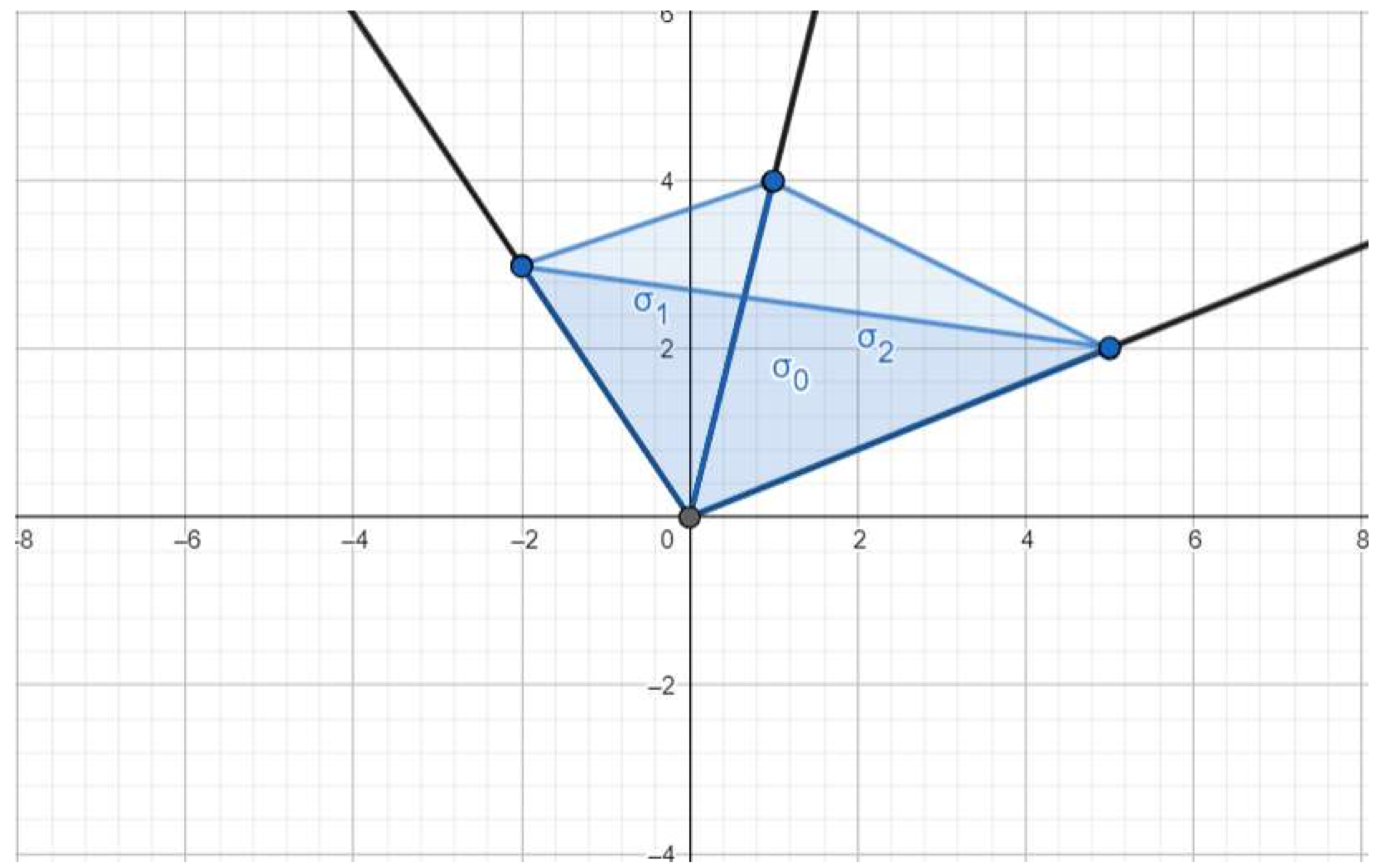


Figure 2: In the diagram above, each σ_i is a affine toric variety. Together, they create $X(\Delta)$.

Properties

Let X_Σ be the toric variety determined by a fan Σ in $_{\mathbb{R}}$. Then:

- X_Σ is complete $\iff$ Σ is complete.
- X_Σ is smooth $\iff$ every $\sigma \in \Sigma$ is a smooth cone.
- X_Σ is Cohen-Macaulay
- X_Σ has at worst rational singularities. [4]

Major Theorems

Using theorems from algebraic geometry, some significant results have been made in toric varieties:

- Riemann-Roch Theorem
- Serre-Duality Theorem
- Stanley's Theorem

Tropical Geometry

Since polyhedral geometry plays a significant role in toric variety theory, toric varieties have a close relationship with **Tropical Geometry**, a new field in algebraic geometry that focuses on the tropical semi-ring. The following is the tropicalization of a toric variety:

- **Definition:** Let Σ be a rational polyhedral fan in $N_{\mathbb{R}}$. For each cone $\sigma \in \Sigma$, we consider the $(n - dim(\sigma))-$dimensional vector space $N(\sigma) = N_{\mathbb{R}}/span(\sigma)$. As a set, the tropical toric variety X_Σ^{trop} is the disjoint union
$$X_\Sigma^{trop} = \sqcup N(\sigma).$$
We define a topology on X_Σ^{trop} by associating each $\sigma \in \Sigma$, the space $U_\sigma^{trop} = Hom(\sigma^\wedge \cap M, \mathbb{R})$ of semigroup homomorphisms from $(\sigma^\wedge \cap M, \mathbb{R})$to $(\mathbb{R}, \odot)$. [5]

References

[1] Igor R. Shafarevich.
Basic algebraic geometry 1: Varieties in projective space.
1(1):1–200, 2013.

[2] Rick Miranda.
Algebraic curves and riemann surfaces.
Graduate Studies in Mathematics, 5(5):1–30, 1995.

[3] William Fulton.
Introduction to toric varieties.
Annals of Mathematical Studies, 1(131):3–28, 1993.

[4] Henry K.Scheneck, David A.Cox, John B. Little.
Toric varieties.

[5] Diane Maclagan,Bernd Sturmfels.
Introduction to tropical geometry.
161(1):277–348, 2015.

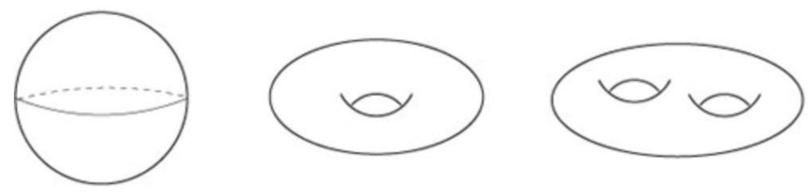
Methods for Solving Diophantine Equation

An Geometric Exploration of Number Theory

Yewen Sun

Mentor: Nadir Hajouji

yewen@ucsb.edu



Abstract

Thousands years ago, people started to think about Diophantine equation like $x^2 + y^2 = z^2$. To solve different kinds of Diophantine equation, the number theory developed quickly. In this paper, we try to review the technique to solve Diophantine equations, and some advanced math topics motivated those techniques.

Introduction

What kind of Diophantine equation is easy to solve? Apparently, equations like $x^2 = y^3$ are easy to find all integer solutions. As we can see, equations without addition are always friendly. For those equations, the unique factorization in $\mathbb{Z}$ makes sure that we can do prime decomposition.
When we meet a more complicated Diophantine equation, we have two ideas to solve it - to find a smaller ring in $\mathbb{Z}$, or to embed $\mathbb{Z}$ to a larger ring. The first is usually to consider the surjective homomorphism $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$. For example, we can solve $x^2 + 1 = 3y$ by consider $\mathbb{Z}/3\mathbb{Z}$. For a general homogeous quatric equation $aX^2 + bY^2 = cZ^2$, we have the Hasse Principle. We will talk about it later. For the second way, we need find a larger ring, and there are plenty of choices.

Ring Embedding

For the Mordell curve $y^2 + 2 = x^3$, Fermat changed it to $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$ and considered the embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-2}]$. Now we change the original equation to a equation without addition, and the ring is still a UFD! It is not hard to conclude $y + \sqrt{-2} = p^3$ and $y - \sqrt{-2} = q^3$, for some $p, q \in \mathbb{Z}[\sqrt{-2}]$. Then we solve the problem. Many mathematicians, like Euler, Gauss, Dirchlet, and Kummer all tried to use this idea to prove Fermat's last theorem - the insolubility in integer of the equation $x^n + y^n = z^n$. We actually only need to consider $x^p + y^p = z^p$ for odd prime p. It seems promising because the equation above is exactly

$$(x + y)(x + \zeta y)(x + \zeta^2 y)...(x + \zeta^{p-1} y) = z^p$$

where ζ is the pth root of unity. Thus, if $\mathbb{Z}[\zeta]$ is a UFD, it will be very profitable to help prove the Fermat's last theorem. (See [4]p.7-8).
However, it is not true that $\mathbb{Z}[\zeta]$ is always a UFD. When $p = 23$, it is not a UFD. (See [4]p.8.27) Years later, mathematicians like Dedekind, Kronecker, and Lasker try to find some generalization of unique factorization. Dedekind noticed that two principle ideals coincide if and only if their generators are associated, and the unique factorization is also unique up to unit multiples. He defined Dedekind domain (Noetherian normal domain of dimension 1). This kind of ring has unique factorization of ideals into prime ideals.
Around the same time, Kronecker took a different generalization. He is the first one to consider the polynomial ring $k[x]/f(x)$. Then the root of $f(x) = 0$ is the image of x in this ring. The research on zeros of polynomial developed into one of the most important fields of modern math - algebraic geometry, and it is closely related to number theory.

Quadratic Case - Hasse Principle

$x^2 + 1 = 3y$ has no solution in the subring $\mathbb{Z}/3\mathbb{Z}$, and $x^2 + 2 = y^2 + 8y$ has no solution in the subring $\mathbb{Z}/8\mathbb{Z}$, so we can solve these Diophantine equations. Hasse Principle is a generalization of it. It states as below:
Hasse Principle, also global-local principle: A homogeneous quadratic equation in several variables is solvable by integers, not all zero, if and only if it is solvable in real numbers and in p-adic numbers for each prime p.
p-adics and reals are both completion of $\mathbb{Q}$, so a global solution yields local solutions at each prime. The Hasse Principle asserts that the reverse can be done. Hasse Principle works well for quadratic forms, but in other cases it will fail. For example, the Mordell curve $y^2 = x^3 - 51$, Lind's equation $x^4 - 17y^4 = 2z^2$, and Selmer's famous homogeneous counterexample $3x^3 + 4y^3 + 5z^3 = 0$. (See [1],[3]) So people become interested in equations of higher degree.

Cubic case - Elliptic curve over $\mathbb{Q}$

For any cubic $f(u, v) = 0$, there is a birational equivalence between the cubic and a Weierstrass form, i.e. $y^2 = x^3 + ax^2 + bx + c$ in the projective plane[See [6]p.17-18]It is the elementary definition of an elliptic curve. How is the elliptic curve related to Diophantine equations? We give a fact here, that the Diophantine equation $x^3 + y^3 = 7z^3$ has an integer solution $(x, y, z) = (4381019, 9226981, 4989780)$. It is easy to check, but how do we construct it? It is directly related to the elliptic curve and the group law on it.

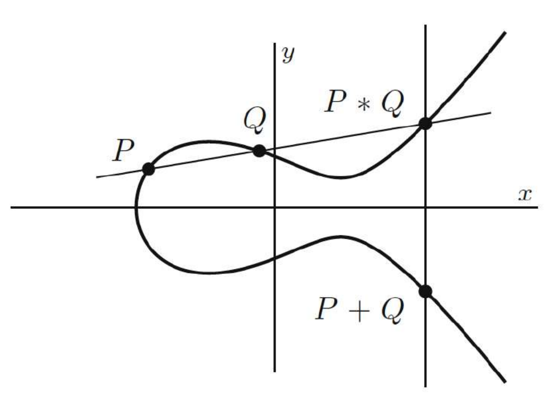


Figure 1: The group law

For points on the elliptic curve, we define a group law as above. Given the specific coordinates of P and Q, by using Vita's formula, it is not hard for us to calculate the coordinates of $P + Q$.
Back to the previous question, in order to find some peculiar rational solution of $x^3 + y^3 = 7$, we change it to the Weierstrass normal form $y^2 = x^3 - 21168$. Then we notice that $P = (x, y) = (\frac{4}{3}, \frac{5}{3})$ is a solution, so we can calculate points $2P, 3P$, etc. Then we can get many unusual solutions. However, the sequence $\{nP\}_{n=1}^{\infty}$ does not ensure that we have infinitely many solution. It is possible that the sequence will end somewhere. In other words, the P can be a torsion point. Thus, the research on torsion points will give us a lot of information.

Torsion Points

We are curious about two questions in general. The first is the easier one: given an elliptic curve, how do we find all of the torsion points. The second is for which n, there will be torsion points of order n for some elliptic curve?
The Nagell-Lutz Theorem answered the first question, and it is not hard to prove.
Nagell-Lutz Theorem: Let $y^2 = f(x) = x^3 + ax^2 + bx + c$ be a non-singular cubic curve with integer coefficients a, b, c and let$D$ be the discriminant of the cubic polynomial, if $P = (x, y)$ be a rational point of finite order. Then x and y are integers, and either $y = 0$, in which case P has order two, or else y divides D.
$y|D$ means we only check finitely many y. In some unfriendly cases the D will be large and it takes some time.
The second question is hard, and it takes many great mathematicians tens of years to solve it. Billing and Mahler [3] proved in 1940 that no elliptic curve has torision points of order 11. Thirty year later, Mazur finally found all 15 possible torsion groups. They are $\mathbb{Z}/n\mathbb{Z}$, where $1 \leq n \leq 10$ or $n = 12$; and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, where $1 \leq n \leq 4$.

Mordell Theorem and Heights

Mordell theorem states that the rational points on an elliptic curve is a finitely generated abelian group. The proof needs a very important technique called *height*. The definition is simple: for $x = \frac{m}{n} \in \mathbb{Q}$, define its height $H(x) = max\{|m|, |n|\}$. Roughly speaking, it is a way to measure the complexity of rationals. The proof of Mordell theorem(See [6]p.65-88) is too long to present here, but we can use a simple example to see how useful it is. Consider a special case of Fermat last theorem $x^4 + y^4 = z^4$, if $y \neq 0$, the equation can be rewritten as $(\frac{x^2 z}{y^3})^2 = (\frac{z^2}{y^2})^3 - \frac{z^2}{y^2}$, so we only need to show that any rational point (x, y) of the elliptic curve $y^2 = x^3 - x$ has $y = 0$. The proof goes like this: if we have a point x_0, y_0 with $y_0 \neq 0$, we can assume $x_0 > 1$ (since $(-1/x_0, y_0/x_0^2)$ is also a solution). Let $x_0' = \frac{x_0+1}{x_0-1}$, then $(x_0', 2y_0/(x_0 - 1)^2)$ is another solution with y-coordinate $\neq 0$. It is not hard to show $H(x_0') < H(x_0)$. However, infinite descent on H is apparently not possible, so we finish the proof.

Conclusion and Further development

The modern definition of the elliptic curve is a pair (E, O), where E is a nonsingular curve of genus one and $O \in E$. For example, the elliptic curve over $\mathbb{C}$ is $\mathbb{C}/\Lambda$ for some lattice Λ.

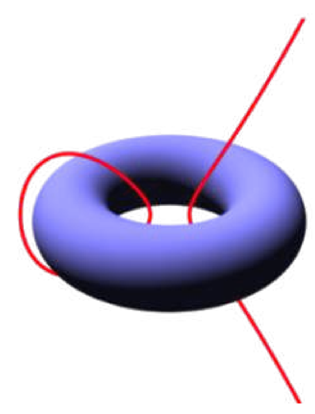


Figure 2: Elliptic curve over $\mathbb{C}$

Riemann-Roch theorem can show that every elliptic curve in this definition can be written as a plane cubic, and conversely every smooth Weierstrass plane cubic curve is an elliptic curve.(See [7]p.59)
Now let C be a non-singular algebraic curve of genus g over $\mathbb{Q}$.
When $g = 0$, it is a conic section. It is very easy to show that the number of rational points of C is 0 or infinity.
When $g = 1$, as we discussed above, the rational points form a finitely generated abelian group, i.e. $C(\mathbb{Q}) = \mathbb{Z}^r \oplus T$, and by Mazur's theorem, the structure of the torsion group T is very limited.
When $g > 2$, in 1983, one of the greatest mathematicians Gerd Faltings proved that C has only a finite number of rational points. His proof involves a large amount of advanced math techniques, especially from the modern algebraic geometry.

References

[1] W. Aitken and F. Lemmermeyer, Simple counterexamples to the local-global principle.
http://public.csusm.edu/aitken_html/m372/diophantine.pdf.

[2] M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley, 1969.

[3] G.Billing and K.Mahler , On exceptional points on cubic curves J. London Math. Soc. 15, (1940). 32 - 43.

[4] K. Conrad, Selmer's example.
https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf

[5] D. Eisenbud, Commutative algebra with a view toward algebraic geometry, Springer, New York, 1995

[6] D. Marcus , Number fields, Springer, New York, 2018

[7] J. Silverman , J. Tate, Rational Points on elliptic curves, Springer, New York, 1992

[8] J. Silverman , The arithmetic of elliptic curves, Springer, New York, 2000