Exploring the Jump From Pre to Post Quantum Cryptography

Fei Du and Carly Greutert, advised by Joel E. Pion
UC Santa Barbara Directed Reading Program (DRP)

Traditional Cryptography

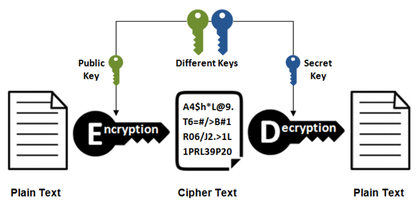
Symmetric encryption

1. Caesar Shift (50 BCE)
2. Vigenère (1553)
3. Enigma Machine (1920)

Asymmetric encryption

1. Rivest–Shamir–Adleman (1977)
2. Elliptic-Curve Cryptography (1985)

Asymmetric Encryption



Hidden Subgroup Problem (HSP)

Suppose there is a known group G and a function $f : G \to S$ where S is some finite set.
Suppose f has the property that there exists a subgroup $H \leq G$ such that f is constant within each coset, and distinct on different cosets: $f(g) = f(g') \iff gH = g'H$. This condition says f is well-defined on the set of left cosets G/H. Since H may be large, "finding H" typically means finding a **generating set** for H.

Discrete logarithm

Given a generator γ (people often use a prime number) of a cyclic multiplicative group C of size N.
This means that $C = \{\gamma^a | a \in \{0, ..., N-1\}\}$, and $A \in C$, can we find the unique $a \in \{0, 1, ..., N-1\}$ such that $\gamma^a = A$?

Classical computers need a lot of time to compute a from A (need time roughly exponential in $\log N$). Take $G = \mathbb{Z}_N \times \mathbb{Z}_N$ and define $f : G \to C$ by $f(x, y) = \gamma^x A^{-y}$. For group elements $g_1 = (x_1, y_1), g_2 = (x_2, y_2) \in G$ we have

$$f(g_1) = f(g_2) \iff \gamma^{x_1 - ay_1} = \gamma^{x_2 - ay_2} \iff (x_1 - x_2) = a(y_1 - y_2) \iff g_1 - g_2 \in \langle (a, 1) \rangle$$

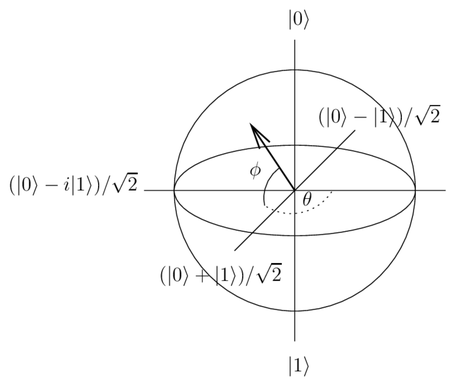
Let H be the subgroup of G generated by the element $(a, 1)$, then finding the generator of the hidden subgroup H gives us a.

The Abelian Case

If G is Abelian, the QFT operator shown on the right helps compute a generating set $\mathcal{L}$ for the period lattice

$$L = \{(x_1, ..., x_n) | \sum_{i=1}^{n} g_i^{x_i} \in H\}$$

Bloch Sphere Illustration



A geometric representation of a qubit

Quantum Fourier Transformation (QFT)

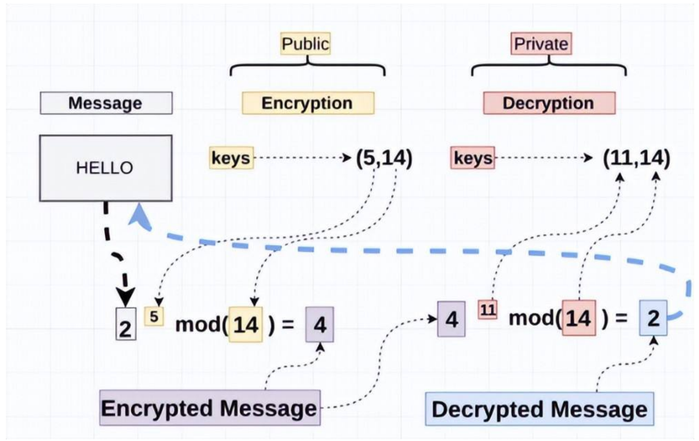
Suppose we have a group G, a set generating G, $\{g_1, ..., g_n\}$, a periodic function f on $\mathbb{Z}^n$ where there exists a normal subgroup H of G ($GHG^{-1} = H$), and an injective function g on the quotient group G/H such that

$$f(x_1, ..., x_n) = g(\sum_{i=1}^{n} g_i^{x_i} \bmod H)$$

The HSP then asks us to present a generating set of the largest such H and the relations between its elements. Define a 2^n dimensional Hilbert space as follows: $\mathcal{H}_n = \mathcal{H} \otimes \cdots \otimes \mathcal{H} = \mathbb{C} \oplus \mathbb{C} \otimes \cdots \otimes \mathbb{C} \oplus \mathbb{C}$. The QFT operator is then defined on an interval of length $N = 2^n$ below:

$$QFT_n : \mathcal{H}_n \longrightarrow \mathcal{H}_n : |x\rangle \longrightarrow 2^{\frac{-N}{2}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |y\rangle$$

RSA Illustration



1. Pick two prime numbers $p = 2$ and $q = 7$ and multiply them to get the modulus 14
2. Compute $L = \text{LCM}(p - 1, q - 1) = 6$ and choose the integer (public key) $e = 5$ such that $1 < e < L$ and $\text{GCD}(e, L) = 1$
3. Solve the private key $d = 11$ such that $d \cdot e = 1 (\text{MOD } L)$

RSA Algorithm

Step One (Key Generation): Choose two secret prime numbers, **p** and **q** (typically, p and q are very large to ensure your message is secure). Then, multiply them together to obtain **n**, the modulus for encryption/decryption. n is a part of the publicly available key.

Then, compute **L(n)**=lcm(L(p), L(q))=lcm(p-1, q-1), and keep L(n) a secret. We then choose a number **e** such that $1 < e < L(n)$ and gcd(e, L(n))=1 (i.e. e and L(n) are **relatively prime**). The integer e is then released as part of the public key. Note the size and length of e will determine how fast and secure the encryption is.

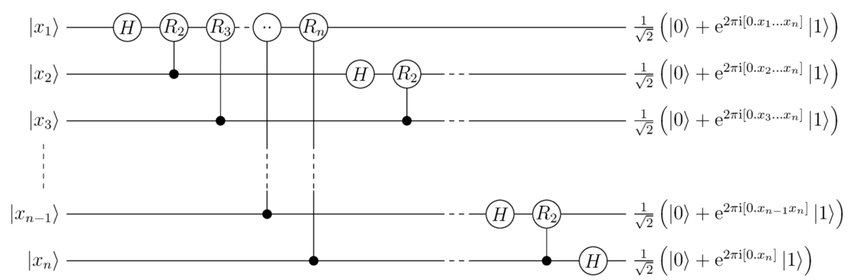
Finally, solve for **d** (the **modular multiplicative inverse** of e modulo L(n) in $d \equiv e^{-1} (\text{MOD } L(n))$. We know such an inverse exists since e and L(n) are coprime. This d will work as our **private key** component.

Step Two (Key Distribution): Suppose Alice is sending a message to Bob. Alice must know Bob's public key (n, e) to encrypt the message, and Bob must use his private key (d) to decrypt the message.

Step Three (Encryption): After Alice obtains Bob's public key, she can send a message M by converting it into an integer from **plain text** such that $(0 \leq M \leq n)$, $M \in \mathbb{Z}$. She computes the **cipher text (c)** by $c \equiv M^e \text{ MOD } n$. Alice then sends c to Bob.

Step Four (Decryption): Once Bob receives the cipher text, he can compute Alice's message M by solving $c^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{k(L(n))+1} \equiv M(M^{k(L(n))}) \equiv M(1) \equiv M \text{ MOD } n$.

QFT Illustration



Implementation of the discrete Fourier transform on $\mathbf{2^n}$ amplitudes into a quantum circuit consisting of only $\frac{\mathbf{n(n+1)}}{\mathbf{2}}$ Hadamard gates **H** (the gate that creates an equal superposition of the two basis states: $|0\rangle \longrightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |1\rangle \longrightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, so $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$) and controlled phase shift gates, $\boldsymbol{R_m} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^m}} \end{bmatrix}$, that modify the phase of the quantum state. Note **n** is the number of qubits.

Related Topics

- Elliptic Curve Cryptography (Pollard's p-1 and Lenstra's Factorization Algorithms)
- Classical Cryptosystems Not Yet Broken by the Quantum Algorithm (McEliece, NTRU, and Lattice-Based public key encryptions)
- Special Cases of the HSP (Pell's Equation, Non-abelian Groups, etc)
- Extended Euclidean Algorithm & Bezout's Identity

Acknowledgements and References

We would like to thank our wonderful advisor, Joel Pion, for his support and guidance through the intricate world of cryptography.
We would also like to thank the 2022 DRP program for giving us this opportunity to further our studies in a supportive environment.

[1] Bernstein, Daniel J., et al., editors. Post-Quantum Cryptography. Springer-Verlag , 2009.

[2] Ronald de Wolf. "Quantum Computing Lecture Notes, Extra Chapter".

The Bernstein Problem

Xingzhe Li, Graduate Mentor: Junrong Yan

Introduction

In minimal surface theory, the celebrated Bernstein problem is as follows: if the graph of a function on $\mathbb{R}^{n-1}$ is a minimal surface in $\mathbb{R}^n$, does this imply that the function is linear? This is proven to be true in dimensions at most 8 but false in dimensions at least 9. Bernstein solved $n = 3$ case at the beginning of 20th century. In 1962, Fleming gave a new proof by deducing it from the fact that all area-minimizing hypercones in $\mathbb{R}^3$ are flat. A few years later, De Giorgi solved $n = 4$ case and Almgren solved $n = 5$ case. In 1968, Simons showed that all area-minimizing hypercones in $\mathbb{R}^7$ are flat, thus extending the Bernstein theorem to dimension 8. Moreover, he gave examples of locally stable cones in $\mathbb{R}^8$, which were proven to be area-minimizing by Bombieri, De Giorgi, and Giusti in 1969. They also showed that there exists complete minimal graphs that are not hyperplanes for $n \geq 9$. Combined with the result of Simons, this gives a complete solution to Bernstein problem in $\mathbb{R}^n$.

Minimal Submanifolds

Let (M^n, g) be a Riemannian manifold with Levi-Civita connection ∇ and let Σ be a k-dimensional submanifold of M. If $X \in \mathfrak{X}(\Sigma)$, then let X^T and X^N denote the tangential and normal components, respectively. For $X, Y \in T_x\Sigma$, the vector-valued bilinear form A on Σ is given by

$$A(X, Y) = (\nabla_X Y)^N.$$

In literature, A is called the second fundamental form, and the trace of A at x is the mean curvature vector

$$H = \sum_{i=1}^{k} A(E_i, E_i),$$

where E_i is an orthonormal basis for $T_x\Sigma$. The normed squared of the second fundamental form at x is

$$|A|^2 = \sum_{i,j=1}^{k} |A(E_i, E_j)|^2.$$

An immersed submanifold $\Sigma^k \subset M^n$ is said to be minimal if the mean curvature H vanishes everywhere. This is equivalent to Σ^k being the critical point for the area functional. In particular, if $\Sigma \subset \mathbb{R}^3$ is a graph of C^2 function $u : \Omega \subset \mathbb{R}^2 \to \mathbb{R}$, then Σ satisfies the minimal surface equation

$$\operatorname{div}\left(\frac{\nabla u}{\sqrt{1 + |\nabla u|^2}}\right) = (1 + u_y^2)u_{xx} + (1 + u_x^2)u_{yy} - 2u_x u_y u_{xy} = 0.$$

Examples of embedded minimal surfaces in $\mathbb{R}^3$ include the helicoid $H = \{(t\cos s, t\sin s, s) | t, s \in \mathbb{R}\}$ and the catenoid $C = \{(x_1, x_2, x_3) | x_1^2 + x_2^2 = (\cosh x_3)^2\}$. By viewing H as the graph of function $u(x, y) = \arctan(y/x)$, one can check that the minimal surface equation holds.

Figure 1: The Helicoid

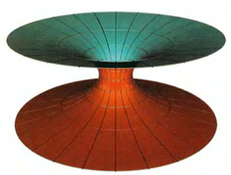


Figure 2: The Catenoid

References

[1] Tobius Holck Colding and William P. Minicozzi II. *A Course in Minimal Surfaces*. Volume 121 of Graduate studies in mathematics. American Mathematical Society, 2011.

[2] Xin Zhou. Lecture notes on minimal surfaces, 2021.

[3] Wendell H. Fleming. On the oriented plateau problem. *Rendiconti del Circolo Matematico di Palermo*, 11:69–90, 1962.

[4] James Simons. Minimal varieties in riemannian manifolds. *Annals of Mathematics*, 88:62–105, 1968.

[5] E. Giusti E. Bombieri, E. De Giorgi. Minimal cones and the bernstein problem. *Inventiones mathematicae*, 7:243–268, 1969.

The Second Variation Formula

Let $\Sigma^k \subset M^n$ be a minimal submanifold and let $F : \Sigma \times (-\epsilon, \epsilon) \to M$ be a variation of Σ with compact support and fixed boundary. In terms of local coordinates, we have the pullback metric $g_{ij}(t) = g(F_{x_i}, F_{x_j})$, the measure $\nu(t) = \sqrt{\det(g_{ij}(t))} \cdot \sqrt{\det(g^{ij}(0))}$, and the area formula

$$\operatorname{Vol}(F(\Sigma, t)) = \int \nu(t)\sqrt{\det(g_{ij}(0))}.$$

Since

$$\left.\frac{d^2}{dt^2}\right|_{t=0} \operatorname{Vol}(F(\Sigma, t)) = \int \nu''(0)\sqrt{\det(g_{ij}(0))},$$

it suffices to derive a formula for $\nu''(0)$ at some $x \in \Sigma$. Choose the normal coordinate system at x. By differentiating the first variation formula $2\nu'(t) = \operatorname{Tr}(g'_{ij}(t)g^{lm}(t))\nu(t)$, we obtain that

$$\begin{aligned} 2\nu''(0) &= \left.\frac{d}{dt}\right|_{t=0} (\operatorname{Tr}(g'_{ij}(t)g^{lm}(t))\nu(t)) \\ &= \left.\frac{d}{dt}\right|_{t=0} (\operatorname{Tr}(g'_{ij}(t)g^{lm}(t))) + \operatorname{Tr}(g'_{ij}(0)g^{lm}(0)) \cdot \frac{1}{2}\operatorname{Tr}(g'_{ij}(0)g^{lm}(0)) \\ &= \frac{1}{2}[\operatorname{Tr}(g'_{ij}(0))]^2 + \operatorname{Tr}(g''_{ij}(0)) - \operatorname{Tr}(g'_{ij}(0)g'_{lm}(0)). \end{aligned}$$

At the point x, we have

$$\begin{aligned} &|g'(0)|^2 = 4|\langle A(\cdot,\cdot), F_t\rangle|^2; \\ &\operatorname{Tr}(g''(0)) = 2|\langle A(\cdot,\cdot), F_t\rangle|^2 + 2|\nabla^N_\Sigma F_t|^2 + 2\operatorname{Tr}\langle R_M(\cdot, F_t)F_t, \cdot\rangle + 2\operatorname{div}_\Sigma(F_{tt}). \end{aligned}$$

Substituting $|g'(0)|^2$ and $\operatorname{Tr}(g''(0))$ inside yields that

$$\nu''(0) = -|\langle A(\cdot,\cdot), F_t\rangle|^2 + |\nabla^N_\Sigma F_t|^2 - \operatorname{Tr}_\Sigma\langle R_M(\cdot, F_t)\cdot, F_t\rangle + \operatorname{div}_\Sigma(F_{tt}) \text{ and}$$

$$\begin{aligned} \left.\frac{d^2}{dt^2}\right|_{t=0} \operatorname{Vol}(F(\Sigma, t)) &= -\int_\Sigma |\langle A(\cdot,\cdot), F_t\rangle|^2 + \int_\Sigma |\nabla^N_\Sigma F_t|^2 - \int_\Sigma \operatorname{Tr}_\Sigma\langle R_M(\cdot, F_t)\cdot, F_t\rangle \\ &= -\int_\Sigma \langle F_t, LF_t\rangle, \end{aligned}$$

where L is the stability operator introduced below.

The Stability Inequality

Suppose that Σ has a trivial normal bundle. By identifying a normal vector field $X = \eta N$ with η, we define the stability operator L as

$$L\eta = \Delta_\Sigma\eta + |A|^2\eta + \operatorname{Ric}_M(N, N)\eta.$$

In particular, if $M = \mathbb{R}^n$, then the Ricci tensor vanishes everywhere and

$$L\eta = \Delta_\Sigma\eta + |A|^2\eta.$$

We say that a minimal submanifold $\Sigma^k \subset M^n$ is stable if for all variations F with boundary fixed,

$$\left.\frac{d}{dt}\right|_{t=0} \operatorname{Vol}(F(\Sigma, t)) = -\int_\Sigma \langle F_t, LF_t\rangle \geq 0.$$

Intuitively, being stable means that the second derivative is positive and the graph is convex. Substituting the formula for L inside and applying the divergence theorem yield the stability inequality

$$\int_\Sigma (\inf_M \operatorname{Ric}_M + |A|^2)\eta^2 \leq \int_\Sigma |\nabla_\Sigma\eta|^2,$$

where $\Sigma^{n-1} \subset M^n$ is a stable minimal hypersurface with trivial normal bundle. In particular, if $M = \mathbb{R}^n$, then the stability inequality reduces to

$$\int_\Sigma |A|^2\eta^2 \leq \int_\Sigma |\nabla_\Sigma\eta|^2.$$

Acknowledgement

I would like to thank my mentor Junrong Yan for helping me develop the intuition for concepts in minimal surface theory and answering my numerous questions about proofs. I would also like to thank the organizer of 2022 UCSB DRP for running this fantastic program.

The Bernstein Theorems

The Bernstein theorem says that if $u : \mathbb{R}^{n-1} \to \mathbb{R}$ is an entire solution to the minimal surface equation and $n \leq 8$, then u is a linear function.

To see why it's true for $n \leq 6$, we make use of the L^p bound of $|A|^2$ for stable hypersurfaces along with the area bound. Let $\Sigma^{n-1} \subset \mathbb{R}^n$ be an orientable stable minimal hypersurface. For all $p \in [2, 2 + \sqrt{2/(n-1)}]$ and every nonnegative Lipschitz function ϕ with compact support, we have the estimate

$$\int_\Sigma |A|^{2p}\phi^{2p} \leq C(n, p)\int_\Sigma |\nabla\phi|^{2p}.$$

The proof is just a computation involving the stability inequality, the Cauchy-Schwarz inequality, the absorbing inequality $2xy \leq \epsilon x^2 + y^2/\epsilon$, and the Simons' inequality

$$|A|\Delta|A| + |A|^4 \geq \frac{2}{n-1}|\nabla|A||^2.$$

Suppose in addition that Σ is complete and

$$\sup_{R>0} \frac{\operatorname{Vol}(B_R \cap \Sigma)}{R^{n-1}} \leq V$$

for some $V < \infty$.

If we consider $2p = 4 + \sqrt{7/5} < 4 + \sqrt{8/(n-1)}$, then the above L^p bound of $|A|^2$ for the cutoff function

$$\phi(x) = \begin{cases} 1, & \text{if } |x| \leq r \\ 0, & \text{if } |x| \geq 2r \\ -\frac{1}{r}|x| + 2, & \text{otherwise} \end{cases}$$

implies that

$$\begin{aligned} \int_{B_r\cap\Sigma} |A|^{4+\sqrt{7/5}} &\leq C(n, p)r^{-4-\sqrt{7/5}} \operatorname{Vol}(B_{2r} \cap \Sigma) \\ &\leq C(n, p)2^{n-1}Vr^{n-5-\sqrt{7/5}} \to 0 \text{ as } r \to \infty. \end{aligned}$$

It follows that $|A|^2$ vanishes everywhere and Σ is flat.

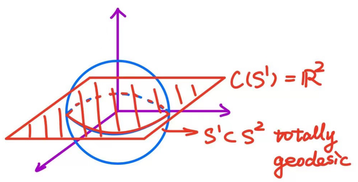
Now, if $u : \mathbb{R}^{n-1} \to \mathbb{R}$ solves the minimal surface equation entirely, then the area-minimizing property of a minimal graph (deduced from the monotonicity formula along with the calibration argument) gives an area bound and the previous argument shows that Σ is a hyperplane. Hence, u is a linear function and the Bernstein theorem holds for $n \leq 6$. For $6 < n \leq 8$, the proof relies on the fact that the hyperplanes are the only area-minimizing hypercones in $\mathbb{R}^n$ for $3 \leq n \leq 7$, which will be explained below.

Minimal Cones

Let N^{k-1} be a submanifold of $S^{n-1} \subset \mathbb{R}^n$. The cone over N is a smooth k-dimensional submanifold away from the origin

$$C(N) = \{x \in \mathbb{R}^n | x/|x| \in N\}.$$

It's immediate from definition that a cone is invariant under dilations about the origin. An example is given by the cone over the equator of S^2, which is just the horizontal plane. More generally, if S^{k-1} is a totally geodesic $(k-1)$-sphere in S^{n-1}, then $C(S^{k-1})$ is a k-dimensional plane through the origin in $\mathbb{R}^n$.



We mention two consequences of $N^{k-1} \subset S^{n-1}$ being a minimal submanifold. Let $\Delta x = (\Delta x_1, \ldots, \Delta x_n)$ denote the metric Laplacian on N. Since a submanifold $N^{k-1} \subset S^{n-1}$ is minimal if and only if Δx is normal to $S^{n-1} \subset \mathbb{R}^n$, we have $\Delta x = xf$ for some function f. As $|x|^2 = 1$, a simple calculation yields that

$$0 = \Delta|x|^2 = 2\langle x, \Delta x\rangle + 2|\nabla x|^2 = 2f + 2(k-1).$$

Hence, $f = 1 - k$ and the coordinate functions are eigenfunctions with eigenvalue $k - 1$. To obtain the other consequence, we observe that Δ_N and $\Delta_{C(N)}$ are related by the formula at $x \neq 0$:

$$\Delta_{C(N)}u = \frac{1}{r^2}\Delta_N u(\frac{1}{r}x) + (k-1)\frac{1}{r}\frac{\partial}{\partial r}u + \frac{\partial^2}{\partial r^2}u,$$

where $r = |x|$. Given x_i a coordinate function on $C(N)$, we may write it as $x_i = ru_i$ with x_i and u_i agreeing on $N \subset S^n$. By the chain rule, we know that

$$\begin{aligned} \Delta_{C(N)}x_i &= \frac{1}{r}\Delta_N u_i + u_i(k-1)\frac{1}{r}\frac{\partial}{\partial r}r + u_i\frac{\partial^2}{\partial r^2}r \\ &= -(k-1)\frac{1}{r}u_i + (k-1)\frac{1}{r}u_i = 0. \end{aligned}$$

Hence, every coordinate function is harmonic on $C(N)$ and $C(N) \subset \mathbb{R}^n$ is minimal.

Now, consider the Bernstein theorem for $n \leq 8$. Let Σ_u be the minimal graph of u and assume $x_0 \in \Sigma_u$. The monotonicity formula at x_0 yields that

$$\frac{\operatorname{Vol}(B_R(x_0) \cap \Sigma_u)}{R^{n-1}} - \frac{\operatorname{Vol}(B_r(x_0) \cap \Sigma_u)}{r^{n-1}} = \int_{(B_R(x_0)\setminus B_r(x_0))\cap\Sigma_u} \frac{|(x - x_0)^N|^2}{|x - x_0|^{n+1}}.$$

Let the density at infinity be

$$\Theta_\infty(x_0) = \lim_{r\to\infty} \Theta_r(x_0) = \lim_{r\to\infty} \frac{\operatorname{Vol}(B_r(x_0) \cap \Sigma_u)}{\omega_{n-1}r^{n-1}},$$

whose existence is guaranteed by the nondecreasing of $\Theta_r(x_0)$ as $r \to \infty$. Moreover, since $\Theta_0(x_0) \geq 1$, we have $\Theta_\infty(x_0) \geq 1$. If $\Theta_\infty(x_0) = 1$, then $\Theta_0(x_0) = 1$ and the monotonicity formula implies that

$$\lim_{\substack{r\to 0 \\ R\to\infty}} \int_{(B_R(x_0)\setminus B_r(x_0))\cap\Sigma_u} \frac{|(x - x_0)^N|^2}{|x - x_0|^{n+1}} = \Theta_\infty(x_0) - \Theta_0(x_0) = 1 - 1 = 0.$$

Hence, $x \in T_{x_0}\Sigma_u$ for all $x \in \Sigma_u$ and we obtain Σ_u as a cone. Blowing up Σ_u at x_0 gives

$$\Sigma_u = \lim_{r_n\to 0} \frac{1}{r_n}\Sigma_u = T_{x_0}\Sigma_u,$$

which implies that Σ_u is flat.

To prove the Bernstein theorem, we suppose that Σ_u is not a hyperplane. Then we have $\Theta_\infty > 1$. Blowing down Σ_u at 0 gives

$$\Sigma_\infty = \lim_{r_n\to 0} r_n\Sigma_u.$$

Based on the fact that

$$\Theta_r^{\Sigma_\infty}(x_0) = \lim_{n\to\infty} \frac{\operatorname{Vol}(r_n\Sigma_u \cap B_r(x_0))}{\omega_{n-1}r^{n-1}} = \lim_{n\to\infty} \frac{\operatorname{Vol}(\Sigma_u \cap B_{r/r_n}(x_0))}{\omega_{n-1}(r/r_n)^{n-1}} = \Theta_\infty(x_0),$$

we have $\Theta_r^{\Sigma_\infty} = \Theta_\infty$ for every $r > 0$. Since $r_j\Sigma_j$ is area-minimizing for every j, by stationary varifold theory or integral current theory, we deduce that Σ_∞ is also area-minimizing. As Σ_∞ has constant density, the monotonicity formula implies that Σ_∞ is a cone. However, by the splitting theorem of De Giorgi, there exists an area-minimizing hypercone with an isolated singularity, which contradicts with the fact that all area-minimizing hypercones in $\mathbb{R}^n$ for $3 \leq n \leq 7$ are flat.

The Bernstein problem is false for $n \geq 9$. In fact, there exists a singular area-minimizing cone in $\mathbb{R}^8$,

$$C_4 = \{(x_1, \ldots, x_8) | x_1^2 + \cdots + x_4^2 = x_5^2 + \cdots + x_8^2\}.$$

More generally, for $m \geq 4$, the cones

$$C_{2m} = \{(x_1, \ldots, x_{2m}) | x_1^2 + \cdots + x_m^2 = x_{m+1}^2 + \cdots + x_{2m}^2\}$$

are singular area-minimizing. Then, Fleming's result implies that there exists a nonlinear entire solution to the minimal surface equation.

Block Chain Mining and Game Theory

Eric Liu, Ryan Stofer, advised by Andre Martins Rodrigues

University of California, Santa Barbara

What is Block Chain?

Block chain is a public data structure used by crypto-currency networks, such as Bitcoin, to perform peer-to-peer transactions and decentralized governance. The block chain has the following four characteristics: it is a decentralized network, a tamperproof ledger, displays transparent transactions, and is trustless but has secure trading [1].

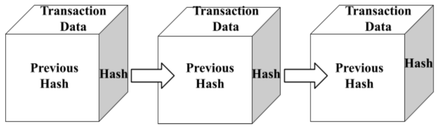


Fig. 1: Simple visualization of Bitcoin blockchain

Since any individual can join the public system and participate in the block chain, popular crypto-currencies, such as Bitcoin, employ a **proof of work** mechanism in order to secure all transactions and avoid potential attacks from hackers. Proof of work is performed by analyzing the exerting computing power made by participants when utilizing the block chain. When an individual (also known as a **miner**) has proven that they have exerted enough resources to the chain, they are then allowed to create a new **block** and are compensated with newly minted crypto-currency.

What are Mining Pools?

As for single miners, it may take an extremely long period to generate a new block because of the difficulty of the proof of work's protocol. Therefore, to decrease the uncertainty and make the revenue more predictable, miners form **mining pools** where all miners mine concurrently and share rewards with the whole mining pool when someone generates a new block.

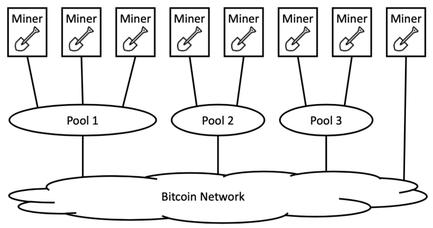


Fig. 2: Example of a Bitcoin system with 3 pools and 1 solo miner [1]

Mining pools are typically implemented as a **pool manager** and a group of miners, and the pool manager representing the whole pool joins the proof of work as a single miner[1]. The pool manager estimates the miners' power by accepting **partial proof of work** and allocates the revenue to miners according to the power they provided.

Game Theory and Nash Equilibrium

Game theory is a study of mathematical models of strategic interactions among rational players. In block chain, we can consider mining pools as rational players, since they always want to maximize their revenue. Through the game, each player will perform their own optimal strategy to maximize the profit, and strategies for mining pools will be discussed in the next section. A **non-cooperative game** is formed if players cannot collaborate or form alliance voluntarily.

One important concept of game theory is **Nash equilibrium** where the optimal outcome of a game is where there is no incentive to deviate from the initial strategy of each player. Therefore, Nash equilibrium is the most common way to define the solution of a non-cooperative game.

Pool Game

One of the classical attacks between mining pools is **pool block withholding attack**, where the attacking pool infiltrates other pools with attacking miners. Registered as miners in attacked pools, attacking miners only send partial proof of work and discards the full proof of work. Thus, the attacking miners can share the revenue obtained by other honest miners without contributing, which reduces the total revenue of the attacked pool. In addition, the total effective mining power in the block chain system will be reduced, decreasing the difficulty of the proof of work protocol.

Since a pool can potentially increase its revenue by attacking other pools, the strategies for each mining pool are to either attack other pools or mine honestly. The interaction between pools give rise to the **pool game** [1]. Since mining pools do not cooperate with other pools in our pool game model, the pool game is considered a non-cooperative game.

Attack between Two Pools

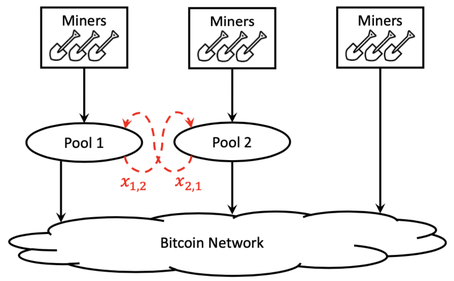


Fig. 3: Two pools attacking each other by infiltrating attacking miners [1]

We will begin the analysis with the case of two pools, pool 1 and 2. Let m_1 and m_2 denote the number of miners inside each pool and $x_{1,2}$ and $x_{2,1}$ denote the number of miners used by pool 1 to infiltrate pool 2 and the number of miners used by pool 2 to infiltrate pool 1 respectively. Then, the direct mining power of each pool is $m_1 - x_{1,2}$ and $m_2 - x_{2,1}$, and the effective mining power of the whole block chain is $m - x_{1,2} - x_{2,1}$ where m denotes all miners of the block chain.

Now, we define R_i as the direct mining rate of pool i which is the ratio between the direct mining power of pool i and the total effective mining power of the block chain. Therefore, the direct mining rate of two pools are:

$$R_1 = \frac{m_1 - x_{1,2}}{m - x_{1,2} - x_{2,1}}, \quad R_2 = \frac{m_2 - x_{2,1}}{m - x_{1,2} - x_{2,1}}$$

Then, we define r_i as the revenue density [2] of pool i which indicates the average revenue a miner can obtain inside pool i. We can obtain r_1 and r_2, based on the infiltration rate, by dividing the pool's revenue among all miners inside the pool:

$$r_1(x_{1,2}, x_{2,1}) = \frac{m_2 R_1 + x_{1,2}(R_1 + R_2)}{m_1 m_2 + m_1 x_{1,2} + m_2 x_{2,1}}, \quad r_2(x_{2,1}, x_{1,1}) = \frac{m_1 R_2 + x_{2,1}(R_1 + R_2)}{m_1 m_2 + m_1 x_{1,2} + m_2 x_{2,1}}$$

Since each pool will choose the optimal infiltration rate $x_{1,2}$ and $x_{2,1}$ that maximizes its revenue density, r_1 and r_2 will be maximized at single points in the range $0 \le x_{1,2} \le m_1$ and $0 \le x_{2,1} \le m_2$. We denote the optimal infiltration rate by $\bar{x}_{i,j} = \arg\max_{x_{i,j}} r_i$ and the corresponding revenue density $\bar{r}_i$ [1], where $i \neq j, i, j \in \{1, 2\}$ in this case.

Therefore, equilibrium can be achieved by finding pairs $x'_{1,2}$ and $x'_{2,1}$ such that

$$\begin{cases} \arg\max_{x_{1,2}} r_1(x_{1,2}, x'_{2,1}) = x'_{1,2} \\ \arg\max_{x_{2,1}} r_2(x'_{1,2}, x_{2,1}) = x'_{2,1} \end{cases}$$

under the constraints $0 < x'_{1,2} < m_1$ and $0 < x'_{2,1} < m_2$.

Two Pools Numerical Analysis and Equilibrium

Nash Equilibrium exists for $x_{1,2}, x_{2,1}$ when

$$\begin{cases} \frac{\delta r_1(x_{1,2}, x_{2,1})}{\delta x_{1,2}} = 0 \\ \frac{\delta r_2(x_{2,1}, x_{1,2})}{\delta x_{2,1}} = 0 \end{cases}$$

which is shown in the figure [1] below:

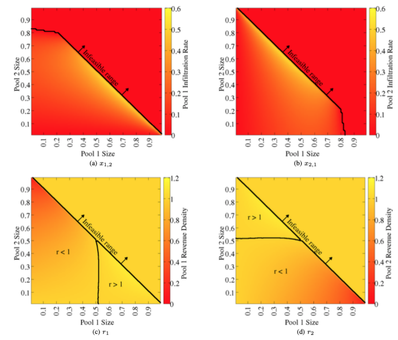


Fig. 4: Infiltration Rate and Revenue Graphs for 2 pools

We observe that only in extreme cases a pool does not attack its counterpart. Specifically, at equilibrium, a pool will refrain from attacking only if the other pool is larger than around 80% of the total mining power. Furthermore, we observe that a pool improves its revenue compared to the no-pool-attacks scenario only when it controls a strict majority of the total mining power. Thus, we see that the dominant strategy is to attack, regardless of what the other pool decides. The table below shows the Prisoner's Dilemma [1] for the Two Pools:

Pool 1 \ Pool 2	No Attack	Attack
No Attack	$(r_1 = 1, r_2 = 1)$	$(r_1 > 1, r_2 = \tilde{r}_2 < 1)$
Attack	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

Practicalities

Although the model presented is simplistic, there are many factors that can perturb our model due to the assumptions we have made. For instance, we assume that the infiltrating miners are loyal to the attacker. However, some of the pool's members may be disloyal infiltrators. To avoid such a risk, a pool needs a sufficient number of verified miners — miners that it knows to be loyal. In general, the optimal infiltration rate may be as high as 60% of the pool size, but this is only in extreme cases when pools are large [1]. For practical pool sizes, a pool may need up to 25% of its mining power for infiltration [1].

Furthermore, a pool may engage in an attack against another pool not to increase its absolute revenue, but to attract miners by temporarily increasing its revenue relative to a competing pool. Such sabotage attack does not transfer revenue from victim to attacker, and migrating miners will switch to less attacked pools, changing pool sizes and hence revenues until convergence. Thus, many requirements must be satisfied for our model to be accurate in practice.

References

[1] I. Eyal. "The Miner's dilemma". In: *2015 IEEE Symposium on Security and Privacy* (May 2015), pp. 89–103.

[2] C. Grunspan and R. Pérez-Marco. "On profitability of stubborn mining". In: *2010 Mathematics Subject Classification* (2010), pp. 1–16.

Algorithms to Generate Random Gentle Algebras

Brian Fan Max Heneghan Jose Landa

University of California, Santa Barbara

Representation Theory

Representation Theory is a branch of mathematics that allows us to take intricate objects and "represent" them with simpler objects. Moreover, these simpler objects correspond and link to elements of Linear Algebra and Abstract Algebra. This area of math studies these algebraic structures, specifically finite dimensional algebra. One of the most recognized class of algebras is the gentle algebras. To understand this class of algebras, it would be helpful to become familiar with several definitions.

Definitions

Throughout, K is a field. We will first talk about quivers and then move towards algebras. Quivers are important because every finite dimensional algebra can be associated with a quiver and quivers give us a visual way of representing complex aspects of algebras.

Quiver - A quiver $Q = (Q_0, Q_1, s, t)$ is a quadruple consisting of two sets: Q_0 (whose elements are called vertices) and Q_1 (whose elements are called arrows), and two maps s, t : $Q_1 \to Q_0$ which associate to each arrow $\alpha \in Q_1$ its source $s(\alpha) \in Q_0$ and its target $t(\alpha) \in Q_0$, respectively.

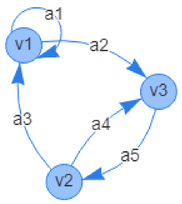


Figure 1. Example quiver Q, with $Q_0 = \{v1, v2, v3\}$ and $Q_1 = \{a1, a2, a3, a4, a5\}$

Adjacency Matrix - A square $n \times n$ matrix M which represents a quiver of n elements. The entry M_{ij} represents the number of arrows from vertex i to vertex j. If $M_{ij} = 0$, then there are no arrows from vertex i to vertex j. A non-zero entry on the diagonal of the matrix M (ie. $M_{ii} > 0$) represents an arrow(s) from vertex i to itself, and this is called a **loop**.

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Figure 2. Adjacency matrix for the quiver Q

K-Algebra - A K-algebra is a ring with identity, A, such that A has a K-vector space structure compatible with the multiplication of the ring. We say A is finite dimensional if the dimension of the K-vector space A is finite.

Path Algebra - Let Q be a quiver. The path algebra KQ of Q is the K-algebra whose underlying K-vector space has as its basis the set of all paths of length $l \geq 0$ in Q and such that the product of two paths $\alpha_1 ... \alpha_l$ and $\beta_1 ... \beta_k$ is equal to zero if $t(\alpha_l) \neq s(\beta_1)$ and is equal to the composed path $\alpha_1 ... \alpha_l \beta_1 ... \beta_k$ if $t(\alpha_l) = s(\beta_1)$.

Relations - Let Q be a quiver. A relation in Q with coefficients in K is a K-linear combination of paths of length at least two having the same source and target. Given a set of relations, let I be the ideal generated by these. Then KQ/I is the algebra bound by these relations.

Goal

A ***gentle algebra*** is a finite dimensional algebra

$$A = KQ/I$$

where Q is a quiver, KQ is a path algebra, and I is an ideal generated by paths of length 2 and satisfies:

1) At most 2 arrows enter and 2 leave each vertex of the quiver Q.

2) For each arrow $\beta \in Q_1$, there is at most one arrow $\gamma \in Q_1$ and at most one arrow $\alpha \in Q_1$ such that $\gamma\beta$ and $\beta\alpha$ are relations contained in I and at most one arrow $\gamma' \in Q_1$ and at most one arrow $\alpha' \in Q_1$ such that $\gamma'\beta$ and $\beta\alpha'$ are relations not contained in I.

The goal for our team was to develop an algorithmic code that enables the generation of gentle algebras. Adhering to the conditions for this class algebra were hard and generating them while maintaining their relations was even harder. Gentle algebras in Representation Theory are an interesting, pretty well-known type of algebra, and were considered to be a good challenge to test out examples.

Introducing GAP and QPA

Evidently, translating theoretical models into a coding language can prove to be a difficult feat, especially since for our project data inputs and outputs were both considered and desired respectfully. Thus, we used the programming language Groups, Algorithms, Programming (GAP) to construct our random generator for gentle algebras. Moreover, GAP has large data libraries that house many packages that contain functions implementing algebraic models written into the preceding programming language. The most frequented package used in GAP for our project was the Quivers and Path Algebras (QPA) package, which contains data structures for quivers and finite dimensional algebras.

Algorithms Mind-Map

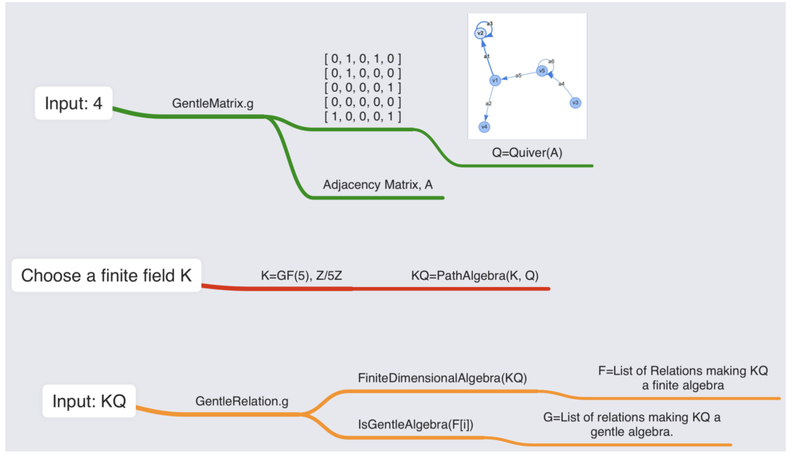


Figure 3. Example Algorithm for a Random 4 Vertices Quiver

Algorithm Explanations

Our approach to generate gentle algebra relations consists of three functions, allocated in "GentleMatrix.g", "FiniteDimensionalAlgebraRelation.g", and "GentleRelation.g". Due to the limitation of space, we have included our actual code works in the QR code below. Please scan it for detailed information.

(a) (b) (c) (d)

Figure 4. (a)-(b) GentleMatrix.g (c) FiniteDimensionalAlgebraRelation.g (d) GentleRelation.g

GentleMatrix.g

In this file, we are trying to generate an adjacency matrix that can be used to construct a gentle quiver which has at most two arrows entering and 2 leaving each vertex. The primary function in this file will take an integer n, which represents the number of vertices, as its input. To make the resulted adjacency matrix as random as possible, we utilize the built-in function **Random()** in GAP to create randomness. Moreover, to ensure our matrix can generate a special biserial quiver, we control the sum of entries in each row and column with an upper limit of 2.

FiniteDimensionalAlgebraRelation.g

In this file, we created a function called **FiniteDimensionalAlgebraRelation()** that takes a path algebra created by the adjacency matrix generated by the **GentleMatrix()** as its input and outputs a list of relations that can make this inputted path algebra finite dimensional. As said by the definition, every gentle algebra is finite dimensional, so the existence of this function helps us filter out all the relations that wouldn't make our path algebra finite. This function takes advantage of a built-in function called **IsFiniteDimensional()** in GAP's QPA package.

GentleRelation.g

In this file, we created a function called **GentleRelation()** that takes the path algebra created by the adjacency matrix generated by the **GentleMatrix()** as its input and outputs a list of relation that can make this inputted path algebra finite dimensional. In our algorithm, we employ the **FiniteDimensionalAlgebraRelation()** defined above and the built-in function **IsGentleAlgebra()** to filter out relations that can make the path algebra gentle.

Acknowledgement

We would like to extend our gratitude towards our advisor and mentor Andres Barei, whose research pertains in Representation Theory of Algebras. Also, it goes without saying, that we would like to thank the Directed Reading Program for allowing us to take part in this amazing opportunity.

References

[1] Assem, I., Simson, D., &; Skowroński Andrzej. (2006). Elements of the Representation Theory of Associative Algebras, Volume 1. Cambridge: Cambridge University Press.

[2] Geiß, C., &; Reiten, I. (2005). Gentle algebras are Gorenstein. Representations of Algebras and Related Topics, 129–133. doi:10.1090/fic/045/09

RSA Encryption

Anna Maximova and James McNeice

2022 Mathematics Directed Reading Program. Department of Mathematics, University of California, Santa Barbara

Why Public Key Cryptographic systems?

Consider the following situation: A message needs to be sent to someone over a public channel. As the channel is not secure, anyone can look at whatever you send to the other party. The question is, how do you send a message to the other party that without compromising the information contained in the message. This is the crux of the field of cryptography. Public Key systems come into play when there is no way to transmit a key safely. The solution is creating a system where all the necessary information to encrypt a message is available publicly, but decrypting the message is very difficult without some sort of key.

An Introduction To Number Theory

Modular Arithmetic

One of the most basic ideas in number theory is modular arithmetic, which is a system of arithmetic that centers around the remainder after repeated subtraction.

Consider a 12-hour clock. Suppose the hour hand points at 12 when no time has elapsed. When 3 hours pass, the hour hand will point at the 3. When 19 hours elapse, the hand will point at the 7 because the hand will cycle through the 12 hours and then restart its cycle to reach 7. Similarly when 25 hours elapse, the hand will point at the 1. We can represent this using the symbol for congruence $\equiv$ as follows:

$3 \equiv 3 \bmod 12$ $\qquad$ $19 \equiv 7 \bmod 12$ $\qquad$ $25 \equiv 1 \bmod 12$

So $a \equiv b \bmod (n)$ if and only if there exists an integer k such that $(a-b) = nk$.[3]

Modular Exponentiation

Suppose you were asked to find the smallest x such that $x \equiv 3^{173} \bmod 11$. We could multiply 3 by itself 173 times and then subtract 11 until we were left with a remainder between 0 and 11 but that would take too long and we're feeling a little lazy today. Luckily for us there is a very simple process we could employ to help us that relies on modular arithmetic: modular exponentiation. The process is relatively simple. First we find a few other congruences.

$3^1 \equiv 3 \bmod 11$ $\qquad$ $3^{16} \equiv 5^2 \equiv 3 \bmod 11$

$3^2 \equiv 9 \equiv 9 \bmod 11$ $\qquad$ $3^{32} \equiv 3^2 \equiv 9 \bmod 11$

$3^4 \equiv 9^2 \equiv 4 \bmod 11$ $\qquad$ $3^{64} \equiv 9^2 \equiv 4 \bmod 11$

$3^8 \equiv 4^2 \equiv 5 \bmod 11$ $\qquad$ $3^{128} \equiv 4^2 \equiv 5 \bmod 11$

Now we can use smaller powers to get to larger powers based on the fact that $x^m \cdot x^n = x^{m+n}$. So, $3^{173} \equiv 3^{(1+2+2+8+32+128)} \equiv 3 \cdot 9 \cdot 9 \cdot 9 \cdot 5 \equiv 1 \bmod 11$.

Chinese Remainder Theorem

Suppose gcd(m, n) = 1. Given integers a and b, there exists exactly one solution x mod (mn) to the simultaneous congruences: $x \equiv a \bmod (m)$ and $x \equiv b \bmod (n)$. [3]

Fermat's Little Theorem

If p is a prime and p does not divide a, then $a^{p-1} \equiv 1 \bmod (p)$. [3]

Intuition for RSA

Using the classic example in cryptography, suppose Bob wants to send a secret message over an unsecure channel to Alice such that if Eve (the eavesdropper) who is listening in on the channel isn't able to understand the message. Alice would create a lock and a key that only she possesses. She would send the unlocked lock to Bob who would use it to lock his message and send it back to Alice. Finally Alice would unlock the lock with her private key and read the message. Eve would only have information about the unlocked and locked lock and therefore theoretically would not be able to read the message.

RSA

RSA works by first choosing two large prime numbers, p and q, then multiplying them to make N, that is:

$$pq = N$$

This is the value that will serve as the modulus for encryption and decryption. At this point a message can be given a numeric representation, M, such that $0 \leq M \leq N-1$. We now choose some e with the following property

$$\gcd(e, (p-1)(q-1)) = 1$$

We now choose value d such that $ed \equiv 1 \mod (p-1)(q-1)$. The setup is now complete, and (n, e) are released as the public key. A message is encrypted by taking $a \equiv M^e \mod N$, and decrypted by taking $M = a^d \mod N$. [3].

Example [2]

Alice:

1. Chooses two primes: $p = 7$ and $q = 19$.
2. Calculates the product: $N = 7 \cdot 19 = 133$.
3. Calculates the totient: $\phi(N) = (p-1)(q-1) = 6 \cdot 18 = 108$.
4. Selects a public key: $e = 29$
5. Selects a private key: $d = 41$
6. Sends the public key: $(N, e) = (133, 29)$

Bob:

1. Chooses a message: $m_o = 99$.
2. Encrypts the message: $m_e = 99^{29} \bmod 133 = 92$.
3. Sends the encrypted message.

Alice:

1. Decrypts the message: $m_o = 92^{41} \bmod 133 = 99$

Note: The efficiency of RSA lies in the fact that it is significantly faster to multiply two numbers than it is to factor a number of the same size as their product. This means that even if an eavesdropper is able to read a message in its encrypted state, they are unable to understand its content because finding the value of d is difficult. Factoring can be made arbitrarily difficult by choosing sufficiently large numbers. For simplicity's sake, we used very small numbers in our example. However to make the encryption feasible and secure, the primes used are typically 1024 to 2048 bits long, approximately 300 to 600 digits long.

Attacks On RSA

Timing Attack

It was demonstrated in 1995 that by timing the process of decrypting multiple messages a malicious party is able to determine the key. This attack is worth mentioning because it does not attack the fundamental process of encryption[3]. Its more akin to having a storefront tightly locked up, and instead of picking the locks a thief throws a rock through the front window [3].

Fermat Attack

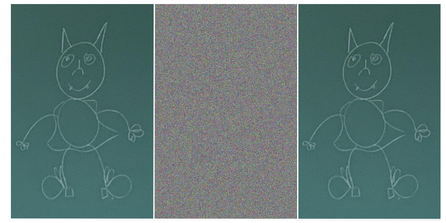
If the primes chosen for encryption are too close to each other then it has been demonstrated that an algorithm can factor N very efficiently. Using the fact that $N = a^2 - b^2 = (a-b)(a+b)$ we can tell that if we find a, b then $(a-b) = p$ and $(a+b) = q$. This is accomplished by taking $\lceil \sqrt{N} \rceil = a$, and determining if $b^2 = a^2 - N$ is an integer. If not, then increment a by one and try again until either a value of b is found, or until 100 or so values of a have been tried [1].

Shor's Algorithm

Shor's Algorithm is a quantum computing algorithm that shatters the security of RSA. It does this taking a 'bad' guess for two numbers that factor some given integer, and spitting out a 'good' guess [3].

Additional Applications of RSA

By coming up with a clever way to express some message many different forms of media can be transmitted via RSA, for instance:



Original Image | Encrypted Image | Decrypted Image

Acknowledgements

We would like to thank the organizers of the of the 2022 Directed Reading Program for the opportunity to learn about cryptography. We would also like to thank our mentor Charles Kulick for his incredible support and mentorship throughout this program.

References

[1] Hanno Böck. *Fermat Attack on RSA*. 2022. URL: https://fermatattack.secvuln.info/.

[2] Ed Harmoush. *RSA Example*. 2021. URL: https://www.practicalnetworking.net/series/cryptography/rsa-example/.

[3] W. Trappe and L.C. Washington. *Introduction to Cryptography: With Coding Theory*. Prentice Hall, 2002. ISBN: 9780130618146. URL: https://books.google.com/books?id=kVU%5C_AQAAIAAJ.

Algebraic Geometry and Moduli Spaces

Kai Yan, Graduate Mentor: Daniel Hamrast

Algebraic Varieties

An **affine algebraic variety** is the common zero set of a collection $\{F_i\}_{i\in I}$ of complex polynomials. In particular, the zero sets of homogeneous polynomials can be viewed as a **projective variety** in a quotient of $\mathbb{C}^{n+1}$ known as the projective space $\mathbb{P}^n$. These varieties form **Zariski topology**, where the open sets are the complement of the varieties. These varieties are completely determined by their **coordinate rings**, defined as $\mathbb{C}[V] = \mathbb{C}[x_1, ..., x_n]/\mathbb{I}(V)$, and conversey every reduced, finite type $\mathbb{C}$-algebra gives an affine/projective variety. The passage from a $\mathbb{C}$-algebra to its variety is denoted by $Spec$, which consists of all the prime ideals of the algebra.

Veronese Map

One useful relationship between projective spaces is the following: All homogeneous degree d polynomial in the polynomial ring $\mathbb{C}[x_0, ..., x_n]$ form a finite dimensional $\mathbb{C}-$vector space with the basis consisting of $\binom{d+n}{d}$ monomials: $x_0^{d_0}...x_n^{d_n}$ with $\sum d_i = d$. This motivates the **Veronese embedding** of the projective space $\mathbb{P}^n$ into $\mathbb{P}^m (m = \binom{d+n}{d} - 1)$, which is the morphism:

$$[x_0 : ... : x_n] \xrightarrow{\nu_d} [x_0^d : x_0^{d-1}x_1 : ... : x_n^d]$$

Five Points Determine a Conic

A conic in projective space $\mathbb{P}^2$ is the zero set of the polynomial:

$$F(x, y, z) = ax^2 + by^2 + cz^2 + dxy + exz + fyz$$

where the coefficients are not all 0. Hence each line through $\mathbb{C}^6$, denoted by $[a : b : c : d : e : f]$ uniquely determines a conic. Therefore we can identify sets of conics in $\mathbb{P}^2$ with points in $\mathbb{P}^5$, and we say that $\mathbb{P}^5$ parameterizes conics in $\mathbb{P}^2$. This is an example of a solution to a **moduli problem**, which I will talk about later.
Now consider a fixed point $[x_0 : y_0 : z_0]$ in $\mathbb{P}^2$, $F(x_0, y_0, z_0) = 0$ now defines a linear equation satisfied by a, b, c, d, e, f. Hence each point in $\mathbb{P}^2$ defines a hyperplane in $\mathbb{P}^5$ through F! Therefore five points(we require there can be no more than three collinear points) $p_1, p_2, p_3, p_4, p_5 \in \mathbb{P}^2$ determines five hyperplanes $H_1, ..., H_5 \subset \mathbb{P}^5$. The intersection of five linearly independent hyperplanes is nothing but a point in $\mathbb{P}^5$, since intersecting once reduce the dimension by one. So there is exactly one conic passing through five fixed point.

References

[1] Ravi Vakil. *THE RISING SEA, Foundations of Algebraic Geometry*. 2017.

[2] Pekka Kekalainen Karen E. Smith, Lauri Kahanpaa and William Traves. An invitation to algebraic geometry. 2000.

[3] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

Hilbert Polynomial

A **graded ring** is a ring that decomposes into direct sum of its subrings. The **Hilbert function** is defined on a graded ring $R = R_0 \oplus R_1 \oplus R_2 ... \oplus R_m$ by:

$$m \longrightarrow \dim R_m$$

Let $V \subset \mathbb{P}^n$ be a projective variety, whose coordinate ring is clearly a graded ring. In this way we can define the Hilbert function of a projective variety.
For large m Hilbert function agrees with a polynomial, called the **Hilbert polynomial**:

$$P(m) = e_0 m^d + ... + e_{d-1}m + e_d$$

with degree $d = \dim V$ and $e_0 = \frac{degV}{d!}$. $degV$ is the **degree** of V, which is defined to be the largest possible number of intersections between V and a codimension $\dim V$ linear subvariety of $\mathbb{P}^n$.

The Hilbert Scheme

Fixing an arbitrary polynomial P, the set of all subvarieties with P as its Hilbert polynomial naturally forms a variety, or more precicely, a **scheme**(a generalization of a variety) in its own right. We call this the **Hilbert scheme**. To contruct the Hilbert scheme, note that any projective variety $V \in \mathbb{P}^n$ is uniquely defined by a homogeneous radical ideal $I = \mathbb{I}(V) \subset \mathbb{C}[x_0, ..., x_n]$. Grothendieck showed that for any P, there exists a positive integer r(depending on P) such that for all ideals I defining a variety with Hilbert polynomial P, I is the radical of the subideal generated by its elements of degree r. Hence, to every Hilbert Polynomial P, one can associate a vector subspace $I_r \subset S_r$, where S_r is the vector space of all homogeneous polynomials of degree r. One can compute the dimension of the vector subspace I_r by:

$$d_r = \dim I_r = \dim S_r - \dim S_r/I_r = \binom{r+n}{r} - P(r)$$

In this way, a Hilbert polynomial, together with r, uniquely specifies a **Grassmannian** $G(\binom{r+n}{r}, d_r)$, which consists of all the d_r-dimensional vector subspaces of a $\binom{r+n}{r}$-dimensional vector space S_r. And a variety uniquely determines a single point in the Grassmannian. Therefore, the Hilbert scheme is a very good way to classify and parameterize subvarieties(or more generally, subschemes) of projective space.

Acknowledgement

I would like to thank my mentor Daniel Halmrast for helping me develop the intuition for concepts used in this poster as well as answering my questions. I would also like to thank the organizer of UCSB DRP for running this fantastic program.

Category, Natural Transformation and the Yoneda Lemma

If F, G are functors between categories $\mathcal{A}, \mathcal{B}$, then a **natural transformation** $\eta : F \implies G$ is a set of morphisms that satisfies:

- The natural transformation must associate a morphism $\eta_A : F(A) \longrightarrow G(A)$ to every object $A \in \mathcal{A}$. This morphism is called a **component** of A.
- For every morphism $f : A_1 \longrightarrow A_2$, we have:

  $$\eta_{A_2} \circ F(f) = G(f) \circ \eta_{A_1}$$

  In other words, the following diagram must commute:

$$\begin{array}{ccc} F(A_1) & \xrightarrow{\eta_{A_1}} & G(A_1) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(A_2) & \xrightarrow{\eta_{A_1}} & G(A_2) \end{array}$$

In category theory, one of the most important results regarding natural transformation is called the **Yoneda lemma**. Given a fixed category $\mathcal{A}$, each object $X \in \mathcal{A}$ naturally gives a functor h_X defined by:

$$h_X = Hom(-, X)$$

Hence for any objects $Y \in \mathcal{A}$, $h_X(Y) = Hom(Y, X)$, which is the set of all morphisms from Y to X. The Yoneda lemma states that the set of natural transformation between h_X and h_Y is isomorphic to the set of morphisms from Y to X. In other words:

$$Hom(h_x, h_y) \cong Hom(Y, X)$$

The Yoneda lemma allows us to completely determine any object by looking at the morphisms that maps into it. This is very powerful in the context of moduli problem, where the structure of the moduli space is not obvious.

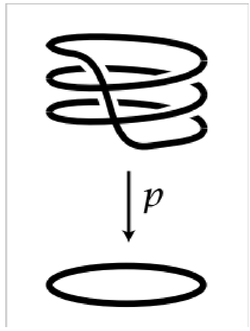
Hilbert functor and Moduli Space

In a more categorical term, the Hilbert scheme is a representation of a functor that sends topological spaces to sets. **Hilbert Functor** It can be defined as:

$$Hilb_X^d : Top \longrightarrow Sets$$

$$Hilb_X^d(Y) = \left\{ Z \subset X \times Y : \begin{array}{c} Z \xrightarrow{\pi_Y} Y \text{is finite and} \\ \text{locally free of rank } d \end{array} \right\}$$

In particular, π_y is analogous to a finite and locally free covering map:



To give a more concrete example, let X be a topological space. Consider the Hilbert functor $Hilb_X^1$. It sends any topological space Y to the set where the elements are topological subspaces $Z \subset X \times Y$ such that the projection from the Z to Y is a homeomorphism. Interestingly enough, $Hilb_X^1$ is in fact naturally isomorphic to the functor h_X and the components of the natural transformation map the set Z to the function $\pi_X \circ \pi_Y^{-1}$. If you let X be $\mathbb{R}$, then $Hilb_X^1$ simply sends any function $g : \mathbb{R} \longrightarrow \mathbb{R}$ to its graph.
Another example concerns the previously mentioned process of five points determining a conic.The Hilbert functor corresponding to a Hilbert polynomial $P(m)$ and subvarieties of $\mathbb{P}^n$ is denoted by: $Hilb_{\mathbb{P}^n}^{P(m)}$. Conics in $\mathbb{P}^2$ has Hilbert polynomial $2m + 1$ and degree 2. The veronese map of degree d associates the set of all degree d hypersurfaces in $\mathbb{P}^n$ with the set of all linear hyperplanes in $\mathbb{P}^M (M = \binom{d+n}{d} - 1)$, which is isomorphic to $\mathbb{P}^M$. Hence we have:

$$Hilb_{\mathbb{P}^2}^{2m+1} \cong h_{\mathbb{P}^5}$$

We say $\mathbb{P}^5$ **represents** the Hilbert functor $Hilb_{\mathbb{P}^n}^{2m+1}$.
These are the simple examples of **moduli spaces**, whose points represent algebraic subvarieties, or more generally subschemes, up to isomorphisms. In the language of moduli spaces, one can parameterize different classes of interesting geometric objects. More often than not, the moduli spaces themselves can have interesting structures beyond merely being a set of points representing classes of objects. And the Yoneda lemma is presicely the tool to study abstract objects like moduli spaces: one can probe the structure of moduli spaces by looking at how other topological spaces map into them. For instance, the map from $\mathbb{A}^1$ into any moduli spaces can give us information about their path connectedness. Hence, solving moduli problems not only helps one classify interesting objects, but give insight into how these classes relate to each other. This makes the study of moduli spaces a very active area in mathematics and physics.

Čech Cohomology!

Lawrence Wu Mentor: **Danning Lu**

University of California, Santa Barbara | 2022 Directed Reading Program

Abstract

In essence, this poster is a brief exploration into ideas from Sheaf Theory, specifically focusing on the Čech Cohomology. Firstly, we introduce the definition of a sheaf, as well as ways to construct sheaves. We then explore the Čech Cohomology, a powerful tool centered around intersections and open covers of a Topological Space.

What is a sheaf

We first must introduce some technical machinery before we discuss further topics.

Sheaves!

Let X be a topological space. A *sheaf of abelian groups on X* consists of:

(a) *a function $x \to \mathcal{F}_x$, assigning each $x \in X$ to some Abelian group $\mathcal{F}_x$.*

(b) *a topology on the set $\mathcal{F}$, the sum of the sets $\mathcal{F}_x$.*

If f is an element of $\mathcal{F}_x$, we put $\pi(f) = x$; we call the mapping of π the *projection* of $\mathcal{F}$ onto X; the family in $\mathcal{F} \times \mathcal{F}$ consisting of pairs (f, g) such that $\pi(f) = \pi(g)$ is denoted by $\mathcal{F} + \mathcal{F}$.

Furthermore, we impose two axioms on **(a)** and **(b)**.
(I) *for all $f \in \mathcal{F}$ there exist open neighborhoods of V of f and U of $\pi(f)$ to V is a homeomorphism of V and U.*

(II) *the mapping $f \to -f$ is a continuous mapping from $\mathcal{F}$ to $\mathcal{F}$, and the mapping $(f, g) \to f + g$ is a continuous mapping from $\mathcal{F} + \mathcal{F}$ to $\mathcal{F}$.*

Sections!

Let $\mathcal{F}$ be a sheaf, and let open $U \subseteq X$. We define a section of $\mathcal{F}$ over U as a continuous mapping $s : U \to \mathcal{F}$ such that $\pi \circ s$ coincides with the identity on U. The set of sections of $\mathcal{F}$ over U is denoted as $\Gamma(U, \mathcal{F})$ and is an abelian group.

Construction of Sheaves!

Suppose for all open $U \subset X$, we have an abelian group $\mathcal{F}_U$, and for all pairs of open subsets $U \subseteq V$ a homomorphism $\phi_U^V : \mathcal{F}_V \to \mathcal{F}_U$, satisfying the transitivity condition $\phi_U^V \circ \phi_U^W = \phi_U^W$. With these conditions, we can define $\mathcal{F}_x = \lim \mathcal{F}_U$ as the inductive limit of the system of open neighborhoods of x. Furthermore, let $t \in \mathcal{F}_U$ and denote $[t, U]$ as the set of $\phi_x^U(t)$ for x running over U. Now, we give $\mathcal{F}$ the topology generated by $[t, U]$. This guarantees that the system $(\Gamma(U, \mathcal{F}), \rho_U^V)$ is a sheaf, but it doesn't guarantee that it is isomorphic to $\mathcal{F}$.

Observe that $x \to \phi_x^U(t)$ is a section of $\mathcal{F}$ over U, which allows us to define the canonical morphism $\iota : \mathcal{F}_U \to \Gamma(U, \mathcal{F})$.

Proposition 1: $\iota : \mathcal{F}_V \to \Gamma(U, \mathcal{F})$ is injective if and only if the following condition holds:

If an element $t \in \mathcal{F}_U$ is such that there exists an open covering $\{U_i\}$ of U with $\phi_{U_i}^U = 0$.

Proposition 2: Let U be an open subset of X, and let $\iota : \mathcal{F}_V \to \Gamma(U, \mathcal{F})$ be injective for all open $V \subset U$. Then ι is surjective if and only if the following condition is satisfied:

For all open coverings $\{U_i\}$ of U, and all systems $\{t_i\}$, $t_i \in \mathcal{F}_{U_i}$ such that $\phi_{U_i \cap U_j}^{U_i}(t_i) = \phi_{U_i \cap U_j}^{U_j}(t_j)$ for all pairs (i, j), there exists a $t \in \mathcal{F}_U$ with $\phi_{U_i}^U(t) = t_i$ for all i.

Proposition 3: If $\mathcal{F}$ is a sheaf of abelian groups on X, the sheaf defined by the system $(\Gamma(U, \mathcal{F}), \rho_U^V)$ (with propositions 1,2) is canonically isomorphic with $\mathcal{F}$.

Some examples of sheaves

The definition of sheaves is undoubtedly daunting, but there are several examples that are relatively easy to grasp. Consider the following examples,

- Let X be some topological space. Let G be an abelian group, and set $\mathcal{F}_x = G$ for all $x \in X$. Now, our sheaf $\mathcal{F}$ can be identified as the $X \times G$ with the product topology of X and G, equipped with the discrete topology. This construction can be verified to be a sheaf, and is known as the *constant sheaf*.
- Let X be some topological space. Let $x \in X$, and let G be some abelian group. Let U be an open subset of X, we define $\mathcal{F}(U)$ as

$$\mathcal{F}(U) := \begin{cases} G & \text{if } x \in U \\ 0 & \text{if } x \notin U \end{cases}$$

  Indeed, we can construct a sheaf from $\mathcal{F}(U)$ and is known as the *skyscraper sheaf*.
- There are also more concrete examples we can talk about! For instance, we consider the topological space $\mathbb{C}$. Let $U \subset \mathbb{C}$ be an open subset of $\mathbb{C}$. We associate each U with the set of holomorphic functions $\mathcal{F}(U) := \mathcal{C}(U)$. Under a system of inclusion maps, it's easy to see that we in fact do yield a rather visual sheaf!

The Čech Cohomology

With some tools in our inventory, we can begin to talk about the Čech Cohomology! The full construction of the Čech Cohomology is quite long and technical, and the curious reader should turn their attention to Coherent Algebraic Sheaves.

Let $\mathcal{U} = \{U_i\}_{i \in I}$ be an open cover of X. If $s = (i_0, \ldots, i_p)$ is a finite sequence of elements in I, we put $U_s = U_{i_0} \cap \ldots U_{i_p}$. A p-cochain of $\mathcal{U}$ is a function f assigning every sequence s of $p+1$ elements of I to a section of $\mathcal{F}$ over U_s. Note that the p-cochains form an abelian group, denoted by $C^p(\mathcal{U}, \mathcal{F})$.

Let $S(I)$ be the simplex with I as its vertices. Let $K_p(I)$ be the free group with the set of simplexes of dimension p of $S(I)$ as its base. Now, we are beginning to delve into familiar territory. We define our boundary map $\partial : K_{p+1}(I) \to K_p(I)$ in the usual way,

$$\partial(i_0, \ldots, i_{p+1}) = \sum_{j=0}^{p+1} (-1)^j (i_0, \ldots, \hat{i}_j, \ldots, i_{p+1}).$$

Now, we define the coboundary operator ${}^t\partial : C^{p+1}(\mathcal{U}, \mathcal{F}) \to C^p(\mathcal{U}, \mathcal{F})$ as

$$({}^t\partial f)_{(i_0, \ldots, i_{p+1})} = \sum_{j=0}^{p+1} (-1)^j \rho_j (f_{i_0, \ldots, \hat{i}_j, \ldots, i_{p+1}}).$$

where $\rho_j : \Gamma(U_{i_0, \ldots, \hat{i}_j, \ldots, i_{p+1}}, \mathcal{F}) \to \Gamma(U_{i_0, \ldots, i_{p+1}}, \mathcal{F})$ denotes the restriction homomorphism.

With this, we can finally define the q-th cohomology group of the complex $C(\mathcal{U}, \mathcal{F})$ as $H^q(\mathcal{U}, \mathcal{F}) := \text{Ker}\,({}^t\partial_q)/\text{Im}\,({}^t\partial_{q-1})$. However, this is not enough to define the Čech Cohomology on X as our cohomology groups generally depend on our choice of $\mathcal{U}$. To combat this issue, we consider finer open covers of X.

A cover $\mathcal{U}$ is said to be finer than $\mathcal{V}$ if there exists a mapping $\tau : I \to J$, such that $U_i \subset V_{\tau(i)}$ for all $i \in I$. If $\mathcal{U}$ is finer than $\mathcal{V}$, there exists a canonical mapping $\sigma(\mathcal{U}, \mathcal{V})$ from $H^q(\mathcal{V}, \mathcal{F})$ to $H^q(\mathcal{U}, \mathcal{F})$.

Finally, we are ready to define the Čech Cohomology on X. Under refinement, the covers of X form a directed set, which allows us to set $H^q(X, \mathcal{F}) := \lim H^q(\mathcal{V}, \mathcal{F})$.

Čech Cohomology Isomorphic?

The construction of the Čech Cohomology is quite undeniably complicated. This begs the question, why exactly do we care about the Čech Cohomology? What exactly does Čech Cohomology bring to the table?

Firstly, the Čech Cohomology has many applications in Algebraic Geometry, which is a beautiful field in its own right. The curious reader should once again turn their attention towards the reference section.

In our construction of the Čech Cohomology, we are reminded of the construction of other Cohomologies. In some sense, the Čech Cohomology can be thought of as a generalization of both the Singular Cohomology and the de Rham Cohomology. While in general, the Čech Cohomology groups for an arbitrary space X is not isomorphic to either Cohomology groups, we can impose certain conditions such that they always coincide.

Proposition 4.

Let X be a paracompact topological space, and $\mathcal{F} = A$ a constant sheaf. Then the following is true,

$$\check{H}(X, \mathcal{F}) \cong H_{\text{Sing.}}(X, A).$$

Furthermore, since CW-complexes are paracompact, if X is homotopic equivalent to a CW-complex, then our two cohomology groups coincide.

Proposition 5.

Let X be a differential manifold, and $\mathcal{F} = \mathbb{R}$. Then the following holds,

$$\check{H}(X, \mathcal{F}) \cong H_{\text{de Rham}}(X, \mathbb{R}).$$

The proofs can be found in the references [2][3] respectively.

Acknowledgements

I would like to thank the Directed Reading Program for giving me this amazing opportunity to explore mathematics in such a hands-on fashion. I would also like to extend my gratitude to the many graduate students in the Mathematics Lab who helped me understand the material in a deeper level. Lastly, I would to like to give special thanks to my mentor, Danning Lu, who has been a terrific guide through this project. Without his boundless patience and wisdom, this project quite literally could not be possible.

References

[1] *Achinger, (1965). Faisceaux Algebriques Coherents [Coherent Algebraic Sheaves].*
[2] *Spanier, E. H. (1966). Algebraic topology. Springer.*
[3] *Bott, Raoul, and Loring W. Tu. Differential Forms in Algebraic Topology. Springer, 1995.*

UC SANTA BARBARA

An Introduction to Optimal Transport

Ayesha Usmani †

†Department of Mathematics, University of California, Santa Barbara

Introduction

As humans, we naturally aim to find the most efficient way to do things. Optimal Transport, as can be deduced by its name, is an area of study dedicated to finding the most efficient way to transport units from one location to another. Its origins can be traced back to French mathematician Gaspard Monge who, in the 1780s, considered a simple problem whereby a worker moves one pile of sand to create a new pile of a specific shape in another location. To do this while also using the least amount of effort, one must consider the local cost of moving each grain of sand from the original pile to the targeted pile and use this to find the minimum global cost. For the sake of simplicity, we will consider discrete optimal transport problems.

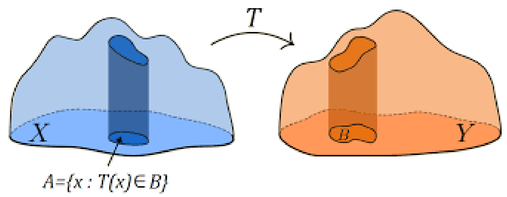


Figure 1. An example of the Monge problem - sand being moved from one location to another. Source: Matthew Thorpe, University of Cambridge.

Assignment Problem

A special case of the Monge Problem is the assignment problem.
Suppose we have equal masses contained in locations x_i that we wish to transfer to locations y_j. In this case, suppose that all the mass from any x_i must be transported to only one y_j.

$$\begin{array}{ccc} x_1 \bullet & & \bullet\ y_1 \\ x_2 \bullet & \xrightarrow[\text{permutation}]{\sigma} & \bullet\ y_2 \\ \vdots & & \vdots \\ x_n \bullet & & \bullet\ y_n \end{array}$$

The cost of transporting something from x_k to y_j is $C_{k,\sigma(k)}$. The optimal transport cost is

$$\min_{\sigma\in\text{Perm}(n)} \sum_{k=1}^{n} C_{k,\sigma(k)}.$$

There are two points of concern in this problem. Firstly, it does not allow the splitting of mass to transport multiple locations. Secondly, it does not have a unique solution, as you can see in Figure 1.

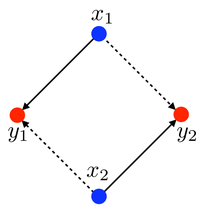


Figure 2. Notice that the cost of transporting mass from x_1 to y_1 and x_1 to y_2 is the same. Similarly, the cost of transporting mass from x_2 to y_1 and x_2 to y_2 is the same. Source: Gabriel Peyré.

Kantorovich Problem

In the 1940s, Soviet mathematician, Leonid Kantorovich, revisited Monge's problem but allowed for the splitting of mass, and admits a dual formulation. This problem also does not have a unique solution. Similar to the Monge problem, we wish to transfer mass from location x to location y.

$$\begin{array}{ccc} x_1 \bullet & & \bullet\ y_1 \\ x_2 \bullet & \xrightarrow{\sigma} & \bullet\ y_2 \\ \vdots & & \vdots \\ x_n \bullet & & \bullet\ y_m \end{array}$$

Here, it is possible for $m \neq n$, since it possible to send mass from one location to multiple destinations. Let $\sum_n$ denote a collection of n nonnegative numbers that add up to 1. We define a set of matrices

$$\mathbf{U}(\mathbf{a},\mathbf{b}) \stackrel{\text{def}}{=} \{\mathrm{P} \in \mathbb{R}_+^{n,m} : \mathrm{P}\mathbb{1}_m = a \text{ and } \mathrm{P}^T\mathbb{1}_n = b\}$$

where

$$\mathrm{P}\mathbb{1}_m = \sum_j (\mathrm{P}_{i,j})_i \in \mathbb{R}^n \text{ and } \mathrm{P}\mathbb{1}_n = \sum_i (\mathrm{P}_{i,j})_j \in \mathbb{R}^m.$$

Then the most efficient cost of transport in this case is

$$\mathbf{L}_{\mathbf{C}(\mathbf{a},\mathbf{b})} \stackrel{\text{def}}{=} \min_{\mathbf{P}\in\mathbf{U}(\mathbf{a},\mathbf{b})} \langle \mathbf{C}, \mathbf{P}\rangle \stackrel{\text{def}}{=} \sum_{i,j} \mathbf{C}_{i,j}\mathbf{P}_{i,j},$$

which is attained for transport plan P^*.

Lemma. The Kantorovich problem is more efficient than the Monge problem.

$$\mathbf{L}_{\mathbf{C}}(\mathbb{1}_n/n, \mathbb{1}_n/n) \leq \min_{\sigma\in\text{Perm(n)}} \langle \mathbf{C}, \mathbf{P}_\sigma\rangle$$

Theorem. If $m = n$ and $a = b = \frac{\mathbb{1}_n}{n}$, then there exists an optimal solution for the Kantorovich problem $\mathbb{P}_{\sigma^*}$, which is a permutation matrix associated to an optimal permutation $\sigma \in \text{Perm}(n)$.

Coffee Break!

To illustrate the Kantorovich problem, it helps to think of n warehouses that store coffee beans required by m coffee shops. Suppose each warehouse is indexed with an integer i and contains a_i units of the resource, while the coffee shops are indexed with integer j and require b_j units of the resource. To transport the raw materials, the warehouse manager can hire a transportation company that charges $\mathbf{C}_{i,j}$ to transport one unit from i to j. In order to get the most ideal deal, the manager must solve the Kantorovich problem to obtain a transportation plan $\mathbf{P}^*$. The total amount they would have to pay the transportation company would then be $\langle \mathbf{P}^*, \mathbf{C}\rangle$.

Kantorovich Dual Problem

Theorem. The Kantorovich problem admits the dual

$$\mathbf{L}_{\mathbf{C}}(\mathbf{a},\mathbf{b}) = \max_{(\mathbf{f},\mathbf{g})\in\mathbf{R}(\mathbf{C})} \langle \mathbf{f},\mathbf{a}\rangle + \langle \mathbf{g},\mathbf{b}\rangle$$

where the set of admissible dual variables is

$$\mathbf{R}(\mathbf{C}) \stackrel{\text{def}}{=} \{(\mathbf{f},\mathbf{g}) \in \mathbb{R}^n \times \mathbb{R}^m : \forall (i,j) \in [n]\times[m], \mathbf{f}\oplus\mathbf{g} \leq \mathbf{C}\}.$$

The Kantorovich problem is a linear minimization problem with convex constraints. Therefore, it admits a dual problem. Looking at the same example of warehouses and coffee, suppose the manager outsources the problem of solving for the ideal transportation plan to a third party. The third party vendor will suggest a price of

$$\langle f, g\rangle + \langle a, b\rangle$$

where fi is the cost to collect a unit of resource at each warehouse i, g_j is the cost to deliver a unit of resource to factory j. a_i is the total number of units at warehouse i and b_j is units required factory j. The vendor will try to make f and g as high as possible. The warehouse manager should check the recommended price by checking if $f_i + g_j \leq \mathbf{C}_{i,j}$. If this inequality fails, then the manager should reject the vendor's offer. The manager's own transport plans would be too expensive

$$\sum_{i,j} \mathbf{P}_{i,j}\mathbf{C}_{i,j} \geq \sum_{i,j} \mathbf{P}_{i,j}(\mathbf{f}_i + \mathbf{g}_j) = (\sum_i \mathbf{f}_i \sum_j \mathbf{P}_{i,j}) + (\sum_j \mathbf{g}_j \sum_i \mathbf{P}_{i,j}) = \langle \mathbf{f}, \mathbf{a}+\mathbf{g}, \mathbf{b}\rangle.$$

So, the manager should accept the vendor's offer while the vendor should seek prices $\mathbf{f}, \mathbf{g}$ that maximize $\langle \mathbf{f},\mathbf{a}\rangle + \langle \mathbf{g},\mathbf{b}\rangle$ but also satisfy $\mathbf{f}_i + \mathbf{g}_j \leq \mathbf{C}_{i,j}$.

The Auction Algorithm

One algorithm to solve the optimal assignment problem is the auction algorithm. Suppose you have an equal number of buyers and goods. The algorithm consists of distributing the goods in a way such that the maximum amount of satisfaction is reached by the buyers. Here, individual satisfaction isn't the goal. We instead aim to find the maximum satisfaction of the group as a whole.
Let a_{ij} denote the "happiness" person i receives from good j, let $j = \sigma(i)$ denote the good, where σ is some permutation of the goods among all of the buyers, and let p_j be the price of good j. All buyers are content with their purchases if the following condition is satisfied:

$$a_{i\sigma(i)} - p_{\sigma(i)} = \max_{j=1,\ldots,N}\{a_{ij} - p_j\}.$$

The way the algorithm works is we begin with a random injective map of buyers and goods. Then, we select a specific buyer such that the above condition does not hold, and we exchange the good they have with a good that brings them more satisfaction. Continue this process until we reach a point where buyers are indifferent with the good they possess and the second best option. The auction algorithm can be extended to solve optimal transport problems. It applies mostly to linear optimal transport problems such as network optimization, shortest path and max-flow problems.

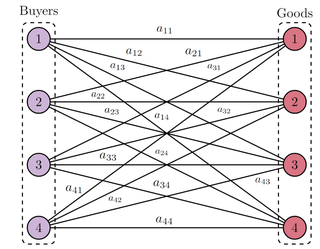


Figure 3. The Auction Algorithm. a_{ij} represents the satisfaction buyer i receives from good j.

Acknowledgements

I would like to thank the UCSB Directed Reading Program for giving me the opportunity to work on this project. I'm especially thankful to my mentor, Đorđe Nikolić, for his time and guidance throughout the past few months.

References

[1] Leonid V. Kantorovich. On translation of mass (in russian). Proceedings of the USSR Academy of Sciences, pages 199—201, 1942.

[2] Gaspard Monge. Mémoire sur la théorie des déblais et des remblais. De l'Imprimerie Royale, 1781.

[3] Gabriel Peyré and Marco Cuturi. Computational optimal transport. Foundations and Trends in Machine Learning, 11(5-6):355–607, 2019.

[4] Filippo Santambrogio. Optimal Transport for Applied Mathematicians, volume 87. Springer International Publishing, 2015.

Representation Theory (for Finite Groups)

Daniel Zhang [1]

[1]*University of California, Santa Barbara, Santa Barbara, CA*
UCSB Directed Reading Program 2022

Introduction

Representation theory is the study of how groups can act on vector spaces.

Definitions

A **representation** of a finite group G on a finite-dimensional vector space V is a homomorphism $\rho : G \to GL(V)$. We often refer to V as the representation and omit ρ.

A G**-linear map** between two representations V and W is a map $\varphi : V \to W$ where for all $g \in G$, $\rho_W(g) \circ \varphi = \varphi \circ \rho_V(g)$

Two representations are isomorphic if they are isomorphic as vector spaces by a G-linear isomorphism.

A **subrepresentation** W of V is a subspace W of V that is invariant under G.

An **irreducible** representation is a representation with no proper nonzero subspace invariant under G.

The **direct sum** $V \oplus W$ of two representations is a representation formed by taking the direct sums of their vector spaces with a group action defined by

$$g \cdot (v \oplus w) = (g \cdot v) \oplus (g \cdot w)$$

The **tensor product** $V \otimes W$ of two representations is a representation formed by taking tensor products of their vector spaces with a group action defined by

$$g \cdot (v \otimes w) = (g \cdot v, g \cdot w)$$

Properties of vector spaces such as $U \otimes (V \oplus W) = (U \otimes V) \oplus (U \otimes W)$ are also true for representations.

The **permutation representation** associated to a left action of G on a finite set X is a vector space with basis $\{e_g : g \in G\}$ with the left action

$$g \cdot \sum_{x \in G} a_x e_x = \sum_{x \in G} a_x e_{gx}$$

The **regular representation** of G is the permutation associated to the left action of G on itself.

Representations of S_3

Example (Trivial representation)

The trivial representation is the one-dimensional representation where the action of any group element is the identity.

Example (Alternating representation)

The alternating representation is the one-dimensional representation where the action of any permutation of even parity is the identity and the action of any permutation of odd parity is negation.

Example (Permutation representation on $\{1, 2, 3\}$)

This is the representation on a three dimensional vector space where the left action of $g \in S_3$ on the vector (z_1, z_2, z_3) is $g \cdot (z_1, z_2, z_3) = (z_{g^{-1}(1)}, z_{g^{-1}(2)}, z_{g^{-1}(3)})$

Example (Standard representation)

The permutation representation of S_3 acting on $\{1, 2, 3\}$ is not irreducible since it has an invariant subspace $\{(z_1, z_2, z_3) \in \mathbb{C}^3 : z_1 + z_2 + z_3 = 0\}$ The representation on this subspace is called the standard representation of S_3, and is irreducible.

The permutation representation on $\{1, 2, 3\}$ is the direct sum of the trivial representation and the standard representation. The trivial representation and standard representation are subrepresentations of the permutation representation on $\{1, 2, 3\}$.

Example (Regular representation of S_3)

This is the representation on a six-dimensional vector space with basis $\{e_h : h \in S_3\}$ where the left action of $g \in S_3$ is

$$g \sum_{h \in S_3} a_h e_h = \sum_{h \in G} a_h e_{gh}$$

Complete reducibility

If W is a subrepresentation of V, then there is a subspace W' of V invariant under G such that $V = W \oplus W'$. This can be shown by taking any projection onto W, averaging over all group elements, and looking at the kernel.

This means any representation can be recursively decomposed into a direct sum of irreducible representations. This means that if we find all irreducible representations of G, then any other representation can be written as a direct sum of those.

This decomposition is in some sense unique. Every representation V of G has a unique factorization $V = \oplus_i V_i^{\oplus a_i}$ where the V_i are irreducible representations of G. Each $V_i^{\oplus a_i}$ is uniquely determined, but the decomposition of $V_i^{\oplus a_i}$ into copies of V_i is not. A simple counterexample would be decomposing a 2-dimensional representation of the trivial group into 2 copies of the trivial representation.

Showing uniqueness requires the following lemma.

Theorem (Schur's lemma)

If $\varphi : V \to W$ is a G-module homomorphism between irreducible representations,

- *Either φ is an isomorphism or $\varphi = 0$*
- *If $V = W$, then φ is scalar multiplication by a constant.*

A consequence of Schur's lemma is that all irreducible representations of abelian groups are 1-dimensional.

Characters

A **character** of a representation V is a map $\chi_V : G \to \mathbb{C}$ defined by $\chi_V(g) = Tr(\rho(g))$.

χ_V is a class function, i.e. it is constant on conjugacy classes.

The character has the following nice properties, which make it convenient for computations:

$$\chi_{V \oplus W} = \chi_V + \chi_W$$
$$\chi_{V \otimes W} = \chi_V \cdot \chi_W$$
$$\chi_{V^*} = \overline{\chi_V}$$

We can define an inner product on characters

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\alpha(g)} \beta(g)$$

The characters of irreducible representations are orthonormal under this inner product.

The number of irreducible representations equals the number of conjugacy classes of G.

In other words, the characters of irreducible representations form an orthonormal basis on the space of class functions.

An irreducible representation V_i appears in V $\langle \chi_V, \chi_{V_i} \rangle$ times.

Since a representation is determined up to isomorphism by the number of copies of each irreducible representations it contains, this means a representation is determined up to isomorphism by its character.

If we know the character of a representation, it is very easy to check if it is irreducible: a representation is irreducible iff $\langle \chi_V, \chi_V \rangle = 1$.

Character tables

If we know all of a group's irreducible representations, we can decompose any representation with a known character into irreducible representations by taking inner products. It is convenient to summarize all this information about the group into a **character table**.

Since characters are constant on conjugacy classes, we only need its value on each conjugacy class. We also label each conjugacy class with how many elements it contains, since this is needed during inner product calculations. Character tables always have the same number of rows as columns.

Example (Character table for S_3)

	1	3	2
S_3	1	(1 2)	(1 2 3)
trivial U	1	1	1
alternating U'	1	-1	0
standard V	2	0	-1

We can check that these representations are irreducible because their inner product with themselves is 1. We know there are no other irreducible representations because S_3 only has three conjugacy classes.

Fixed-point formula

If V is a permutation representation of G acting on X, then $\chi_V(g)$ is the number of elements of X fixed by g. This is because if we write $\rho(g)$ as a matrix, the only nonzero diagonal entries are 1s where g fixes an element of X.

Example (Permutation representation of S_3 on $\{1, 2, 3\}$)

Let W be the permutation representation of S_3 on $\{1, 2, 3\}$.
The identity leaves all 3 elements fixed. A cycle of length 2 leaves 1 element fixed. A cycle of length 3 leaves no elements fixed.

$$\chi_W(1) = 3$$
$$\chi_W((1\,2)) = 1$$
$$\chi_W((1\,2\,3)) = 0$$

Now that we know the character, we can take inner products with irreducible representations to determine how many times each one occurs in W.

$$\langle \chi_W, \chi_U \rangle = \frac{1}{6}(1(3)(1) + 3(1)(1) + 2(0)(1)) = 1$$
$$\langle \chi_W, \chi_{U'} \rangle = \frac{1}{6}(1(3)(1) + 3(1)(-1) + 2(0)(1)) = 0$$
$$\langle \chi_W, \chi_V \rangle = \frac{1}{6}(1(3)(2) + 3(1)(0) + 2(0)(-1)) = 1$$

Hence, $W = U \oplus V$.

Irreducible representations of S_4

We can use the properties of characters to find all irreducible representations of S_4. Since S_4 has 5 conjugacy classes, it must have 5 irreducible represenations.

First, like S_3, S_4 has the trivial representation U, alternating representation U', and standard representation V. If we tensor the standard representation with the alternating representation, we get a distinct irreducible representation V'. We can verify this by computing its character by multiplying the characters for U' and V, and checking it is irreducible by taking its inner product with itself. The character of the remaining irreducible representation W must be orthogonal to all the other ones, and have inner product with itself equal to 1. The sign is determined since $\chi_W(1) = \dim W > 0$.

	1	6	8	6	3
S_4	1	(12)	(123)	(1234)	(12)(34)
U	1	1	1	1	1
U'	1	-1	1	-1	1
V	3	1	0	-1	-1
V'	3	-1	0	1	-1
W	2	0	-1	0	2

Acknowledgements

Thanks to the UCSB Directed Reading Program, and to Edward Chen for being my mentor.

References

[1] William Fulton; Joe Harris. *Representation Theory*. Springer, New York, NY, 2004.

Introduction to Quantum Computing

Sebastian Nunez and Shawn (Yeming) Xiao - Mentored by Greg McGrath

2022 Mathematics Directed Reading Program, University of California Santa Barbara

Introduction

Quantum computing is an emerging field and technology that uses the properties and behaviors of quantum mechanics to create more efficient computers. The main differentiation between classical and quantum computing is the possibility that quantum computing can challenge the weak church turing thesis. In classical computing all information exists in a simple "off" or "on" state, such as 0 or 1, state called "bits". Qubits do not have these restrictions and can exist in any probabilty of being 1 or 0. This means that the amount of information a systems can hold stored grows exponentially with additional qubits being added.

Mathematical Primer

- **Hilbert Spaces -** Hilbert spaces are special vector spaces denoted $\mathcal{H}$ that are necessary for the formulation of the notation of quantum computing. The Hilbert spaces that are relevant are finite-dimensional complex and will typically have a dimension 2^n.
- **Dirac Notation -** A quantum mechanic systems of vectors to represent the state of a qubit. Row vectors are named *kets* and are represented as $|\psi\rangle$ with ψ being the identifier of the ket. In a similar system column vectors are called *bras* and are represented as $\langle\phi|$.

$$\langle\psi| = \begin{bmatrix} a_1 & a_2 & \dots & a_n \end{bmatrix} \qquad |\phi\rangle = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

- **Orthonormal Basis -** Consider a Hilbert space $\mathcal{H}$ of dimension 2^n. A set of 2^n vectors $B = \{|b_m\rangle\} \subseteq \mathcal{H}$ is called an orthonormal basis for $\mathcal{H}$ if

$$\langle b_n|b_m\rangle = \delta_{n,m} \qquad \forall b_m, b_n \in B$$

and every $|\psi\rangle \in \mathcal{H}$ can be written as

$$|\psi\rangle = \sum_{b_n \in B} \psi_n |b_n\rangle \quad \text{for some } \psi_n \in \mathbb{C}$$

The set $\{\langle b_n|\}$ is the orthonormal basis for $\mathcal{H}^*$ called the dual space.

- **Operators -** An operator on a vector space $\mathcal{H}$ is a linear transformation $\mathbf{T} : \mathcal{H} \to \mathcal{H}$. It is useful to note that by constructing an orthonormal basis $B = \{|b_m\rangle\}$ for a vector space $\mathcal{H}$. Then every linear operator $\mathbf{T}$ on $\mathcal{H}$ can be written as

$$\mathbf{T} = \sum_{b_n, bm \in B} \mathbf{T}_{n,m} |b_n\rangle \langle b_m|$$

where $\mathbf{T}_{n,m} = \langle b_n| \mathbf{T} |b_m\rangle$ are matrix elements. Additionally, $|b_n\rangle \langle b_m|$ is the outer product.

- **Tensor Products -** The tensor product is a way of combining spaces, vectors, or operators together. Suppose $\mathcal{H}_1$ and $\mathcal{H}_2$ are Hilbert spaces of dimension *n* and *m* respectively. Then the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is a new, larger Hilbert space of dimension *n*×*m*. Very often the $\otimes$ symbol is left out of the tensor product notation and $|\psi\rangle \otimes |\phi\rangle$ becomes $|\psi\rangle |\phi\rangle$ or $|\psi\phi\rangle$.

Unitary - An operator $\mathbf{U}$ is unitary if

$$\mathbf{U}^\dagger = \mathbf{U}^{-1}$$

Hermitean - An operator $\mathbf{T}$ is Hermitean (or self-adjoint) if

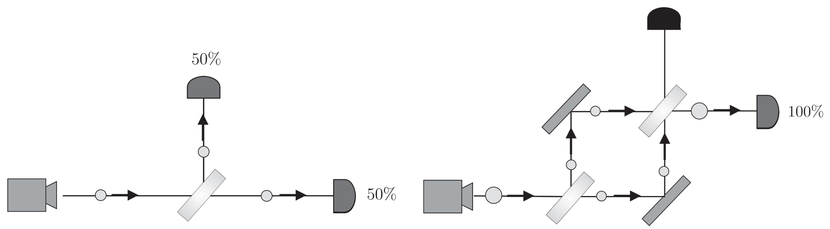
$$\mathbf{T}^\dagger = \mathbf{T}$$

Schmidt Decomposition Theorem

If $|\psi\rangle$ is a vector in a tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$, then there exists an orthonormal basis $\{|\phi_i^A\rangle\}$ for $\mathcal{H}_A$, and an orthonormal basis $\{|\phi_i^B\rangle\}$ for $\mathcal{H}_B$, and non-negative real numbers $\{p_i\}$ so that

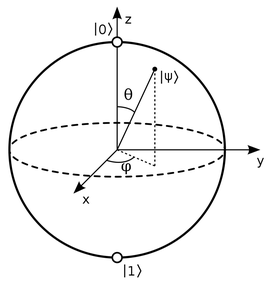
$$|\phi\rangle = \sum_i \sqrt{p_i} |\phi_i^A\rangle |\phi_i^B\rangle$$

Quantum Physics



Imagine that a beam of light is shot through a polished glass and two photon detectors are placed in the path of the reflect photons. After running the experiment on the left we observe that 50% of photons land in the path above and 50% of photons travel through to the right. This result is easily explained by classical mechanics as the polished glass randomly with a coin-flip to transmit or reflect the photons. On the right is the same setup with a few modifications to allow for an additional polished glass. Using our previous analysis we should expect that both photon sensors receive an equal distribution of photons. However, when performed the experiment on the right shows that 100% of photons travel to the right sensor. This non-intuitive behaviour occurs because of a unique property of quantum mechanics called *superposition*.

Superposition



Quantum bits exist in a superposition of states associated with weighted probabilities corresponding to the root of the likelihood of being observed in that state. A useful example quantum computing chooses is complex unit vector $|\Psi\rangle$ in a 2-dimensional Hilbert space.

$$|\Psi\rangle = \cos(\frac{\theta}{2}) |0\rangle + e^{i\Phi} \sin(\frac{\theta}{2}) |1\rangle$$

Where $e^{i\Phi}$ is a global phase factor and the kets $|0\rangle$ and $|1\rangle$ are the basis. When the qubit is measured such as the photon sensors in the experiment the superposition will "collapse" into the state $|0\rangle$ or $|1\rangle$. The state which the qubit collapses is determined by the state probabilities of $|0\rangle$ and $|1\rangle$.

Composite Systems and Measurements

The state space of the combined physical system is the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$ of the state spaces of the component subsystems. If the first system is in the state $|\psi_1\rangle$ and the second system is in the state $|\psi_2\rangle$, then the state of the combined system is

$$|\psi_1\rangle \otimes |\psi_2\rangle \,.$$

Importantly, qubits that can not be written as such are referred to as *entangled*.

For a given orthonormal basis $B = \{|\varphi_i\rangle\}$ of a state space $\mathcal{H}_A$ for a system *A*, it is possible to perform a *Von Neumman measurement* on system $\mathcal{H}_A$ with respect to the basis *B*, given a state

$$|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle \,,$$

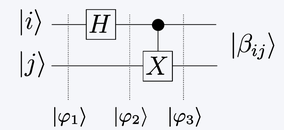
outputs a label *i* with a probability $|\alpha_i|^2$ and leaves the system in state $|\varphi_i\rangle$. Furthermore, given a state $|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle |\gamma_i\rangle$ fromm a bipartite state space $\mathcal{H}_A \otimes \mathcal{H}_B$ (the φ_i are orthonormal; the γ_i have a un it norm but are not necessarily orthogonal), then performing a Von Neumann measurement on system *A* will yield outcome *i* with a probability $|\alpha_i|^2$ and leave the bipartite system in state $|\varphi_i\rangle |\gamma_i\rangle$.

Quantum Circuits and Bell Basis

Quantum computing is performed on circuits that apply operators on a set of input qubits. The operators are called "gates" and are represented with a box spanning the qubits the operator acts on.

$$\mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \mathbf{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

The $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ gates are fundamental operators that correspond to a rotation of a qubit on one of the axis. Using them in combination can translate a qubit to any point on the Bloch sphere so they are referred to as a set of *universal gates*. The $\mathbf{H}$ gate is useful because it can take any qubit already collapsed and turn it into a superposition.



The Bell Basis is a constructed 2-qubit set of superpositions $\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\}$ that are necessary to generate many of the significant applications of quantum computing.

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

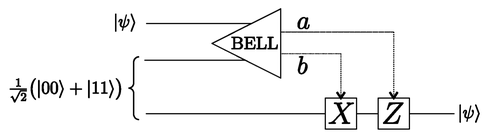
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Superdense Coding and Quantum Teleportation

Superdense coding allows for a qubit to send two classical pieces of information through a channel with only one qubit. The setup required is both ends of the channel to have the same initial $|\beta_{00}\rangle$ state. This is done through applying a combination of $\mathbf{Z}$ and $\mathbf{X}$ gates.

To send	Transformation
00	$\mathbf{I} \otimes \mathbf{I}$: $\|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \mapsto \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) = \|\beta_{00}\rangle$
01	$\mathbf{X} \otimes \mathbf{I}$: $\|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \mapsto \frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle) = \|\beta_{01}\rangle$
10	$\mathbf{Z} \otimes \mathbf{I}$: $\|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \mapsto \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle) = \|\beta_{10}\rangle$
11	$\mathbf{Z} \cdot \mathbf{X} \otimes \mathbf{I}$: $\|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \mapsto \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle) = \|\beta_{11}\rangle$

Quantum teleportation allows the abilty to send one qubit of information using only two *bits* of information.



Crucially, this is possible with neither party of the exchange knowing their own state.

References

[1] Michele Mosca Philip Kaye, Raymond Laflamme. An introduction to quantum computing. *Oxford University Press*, pages 1–270, 2007.

[2] Thomas G. Wong. Introduction to classical and quantum computing. *www.thomaswong.net*, pages 1–95, 2022.

Hyperbolic Geometry and the Farey Tessellation

Misha Kulshresta
University of California, Santa Barbara

What is Hyperbolic Geometry?

Hyperbolic geometry is a geometry in which Euclid's parallel postulate is rejected. Two-dimensional hyperbolic geometry can be modeled in two ways, the open half-plane and the disk model. We can define the open half-plane as follows:

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

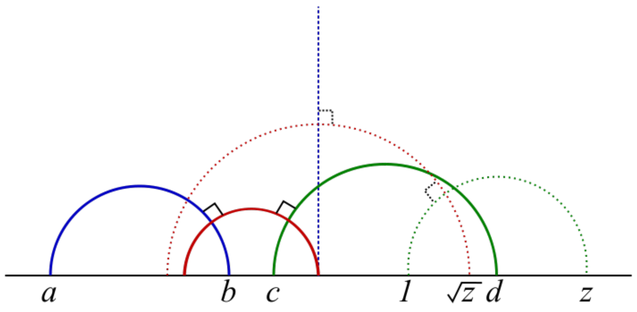


Fig. 1: An example of the half-plane model.

The vertical line here represents the imaginary axis, z. Each arc of Fig. 1 represents a *geodesic*, which can be defined as the curve which is the shortest distance between two points.

The *disk model* is represented by a disk of radius 1. It has a circle at infinity, such that as you get closer to the outer circle, you approach infinity. This model is additionally popular in mathematically-inspired art, as can be seen below in artist M.C. Escher's piece *Circle Limit 1*.

Fig. 2: M.C. Escher's Circle Limit 1.

The below definition will be useful in the following columns:
An *isometry* is a distance-preserving transformation between metric spaces (which includes both the euclidean and hyperbolic planes).

Tessellating

A *tessellation* of a surface (such as the euclidean or hyperbolic plane) is a family of tiles $X_n, n \in \mathbb{N}$, such that:
1. each tile X_m is a connected polygon on the surface.
2. any two X_m, X_n are isometric.
3. the X_m cover the whole surface, in the sense that their union is equal to this space.
4. the intersection of any two distinct tiles X_m and X_n consists only of vertices and edges of X_m, which are also vertices and edges of X_n.

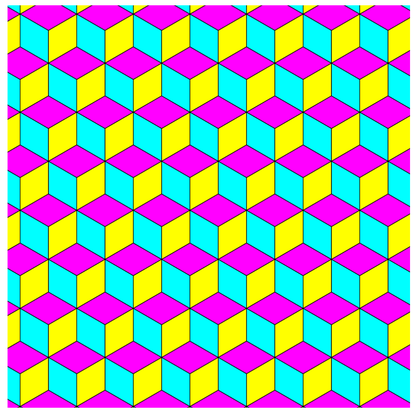


Fig. 3: A tessellation of the euclidean plane with isometric quadrilaterals.

The above diagram is classified as a p6m tessellation (primitive cell, 6-fold rotation, and mirrored), which is one of 17 wallpaper groups.

Tessellations of the hyperbolic plane follow the same rules. Isometries of the hyperbolic plane are not as immediately visible, but the diagram below does in fact satisfy point 2 from above.

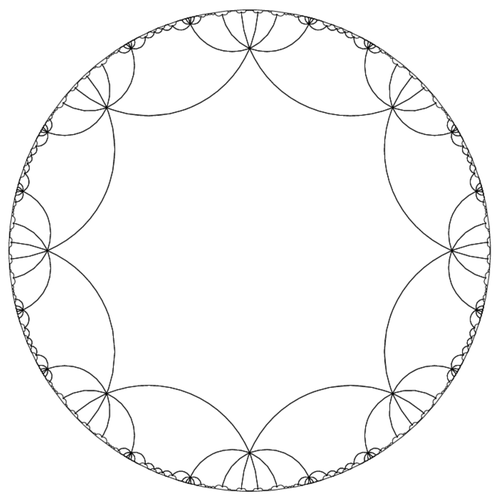


Fig. 4: An order-8 octagon tiling of the hyperbolic plane, resulting in a tessellation of the surface.

Farey Circle Packing

For every rational number $\frac{p}{q} \in \mathbb{Q}$ with p, q coprime and $q > 0$, draw in the plane $\mathbb{R}^2$ and the circle $C_{\frac{p}{q}}$ of diameter $\frac{1}{q^2}$ that is tangent to the x-axis at $(\frac{p}{q}, 0)$ and lies above this axis. These circles $C_{\frac{p}{q}}$ fit together to form a pattern of tangent circles with disjoint interiors as seen below.

$$\infty = \tfrac{1}{0}$$

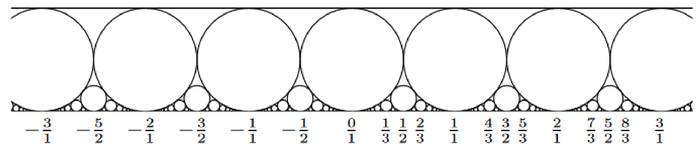


Fig. 5: Farey circle packing.

The Farey Tessellation

Suppose we erase the circles $C_{\frac{p}{q}}$ from the diagram, and instead connect the points $(\frac{p}{q}, 0)$ and $(\frac{p'}{q'}, 0)$ with a semi-circle centered on the x-axis where the circles $C_{\frac{p}{q}}$ and $C_{\frac{p'}{q'}}$ are tangent. The resulting set of hyperbolic geodesics form the *Farey Tessellation*.

$$\infty = \tfrac{1}{0}$$

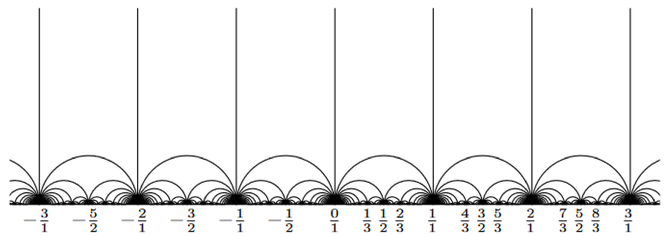


Fig. 6: The Farey tessellation of the hyperbolic plane.

Acknowledgements

A big thank you to Jaime Vandeveer for guiding me through this exciting adventure into hyperbolic geometry, and for making my participation in the Directed Reading Program possible!

References

Bonahon, Francis. *Low-Dimensional Geometry: From Euclidean Surfaces to Hyperbolic Knots.* American Mathematical Society, 2009.

Category Theory and Homological Algebra

Isaiah Martinez, Joseph Sullivan. Mentor: Jeremy Brightbill

2022 Mathematics Directed Reading Program.

Categories

A **category** $\mathcal{C}$ consists of the following data:

- a collection $\mathrm{Ob}(\mathcal{C})$ called the **objects** of $\mathcal{C}$,
- for each $A, B \in \mathrm{Ob}(\mathcal{C})$, a collection $\mathrm{Hom}_{\mathcal{C}}(A, B)$, called the **morphisms** from A to B,
- a morphism $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ for each $A \in \mathrm{Ob}(A)$
- for each $A, B, C \in \mathrm{Ob}(\mathcal{C})$, a function called **composition**,

$$\begin{aligned} \circ : \mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C) \\ f, g &\longmapsto g \circ f. \end{aligned}$$

with the axioms that composition is associative, and for each morphism $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$.

Example. We give three examples of categories.

- "Set" has sets as objects and set functions as morphisms.
- Let R be a ring. "$R-$Mod" has left R-modules as objects and R-module homomorphisms as morphisms.
- The category "Top" has topological spaces as objects and continuous maps as morphisms. "Haus" is the subcategory of "Top" consisting of Hausdorff spaces.

We give two more definitions—special types of morphism that generalize injective/surjective functions respectively.

- A **monomorphism** (mono) is a morphism $f : B \hookrightarrow C$ such that whenever morphisms $g, h : A \to B$ satisfy $f \circ g = f \circ h$, then $g = h$.
- An **epimorphism** (epi) is a morphism $f : A \twoheadrightarrow B$ such that whenever morphisms $g, h : B \to C$ satisfy $g \circ f = h \circ f$, then $g = h$.

Example. In the categories "Set" and "$R-$Mod", monos and epis are exactly injections and surjections. In "Haus", monos are still injections, but epis need not be surjective—they only need to have dense image.

Universal Properties

All objects live inside a category $\mathcal{C}$.

- An **initial object** is an object I such that for any object C, there exists a unique morphism $f : I \to C$.
- A **terminal object** is an object T such that for any object C, there exists a unique morphism $g : C \to T$.
- A **zero object** is an object 0 which is both initial and terminal.
- A **product** of a family $\{A_\lambda\}_{\lambda\in\Lambda}$ is a pair $(A, \{\pi_\lambda\}_{\lambda\in\Lambda})$ of an object A and morphisms $\pi_\lambda : A \to A_\lambda$ (called *projection morphisms*) such that for any object T and morphisms $\{f_\lambda : T \to A_\lambda\}_{\lambda\in\Lambda}$, there exists a unique $f : T \to A$ such that Figure 1 commutes (for each $\lambda \in \Lambda$).
- A **coproduct** of a family $\{B_\lambda\}_{\lambda\in\Lambda}$ is a pair $(B, \{\iota_\lambda\}_{\lambda\in\Lambda})$ of an object B and morphisms $\iota_\lambda : B_\lambda \to B$ (called *inclusion morphisms*) such that for any object T and morphisms $\{g_\lambda : B_\lambda \to T\}_{\lambda\in\Lambda}$, there exists a unique $g : B \to T$ such that Figure 2 commutes (for each $\lambda \in \Lambda$).

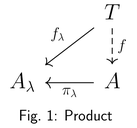


Fig. 1: Product

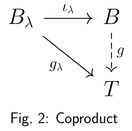


Fig. 2: Coproduct

Remark. In an arbitrary category objects satisfying these universal properties may not exist, but when they do exist, they are unique up to unique isomorphism.

Example. In "Set" ("Top" is similar),

- $\varnothing$ is initial.
- $\{*\}$ is terminal.
- There is no zero object.
- The product of $\{A_\lambda\}_{\lambda\in\Lambda}$ is the usual Cartesian product $\prod_{\lambda\in\Lambda} A_\lambda$ with componentwise projections.
- The coproduct of $\{B_\lambda\}_{\lambda\in\Lambda}$ is the *disjoint union* $\bigsqcup_{\lambda\in\Lambda} B_\lambda$ with inclusions.

Example. In "$R-$Mod",

- 0 is zero.
- The (finite) product and coproduct of $A_1, \ldots, A_n$ is $A_1 \oplus \cdots \oplus A_n$ with componentwise projections and inclusions.

Kernels and Cokernels

Let $\mathcal{C}$ be a category with zero object 0. We say a morphism $g : A \to B$ is 0 if g is the composition of the unique morphisms $A \to 0$ and $0 \to B$.

- A **kernel** of a morphism $f : A \to B$ is a pair (K, k) of an object K and a morphism $k : K \to A$ such that $f \circ k = 0$ and for any object K' and morphism $k' : K' \to A$ such that $f \circ k' = 0$, there exists a unique morphism $u : K' \to K$ such that Figure 3 commutes.
- A **cokernel** of a morphism $f : B \to A$ is a pair (Q, q) of an object Q and a morphism $q : A \to Q$ such that $q \circ f = 0$ and for any object Q' and morphism $q' : A \to Q'$ such that $q' \circ f = 0$, there exists a unique morphism $u : Q \to Q'$ such that Figure 4 commutes.

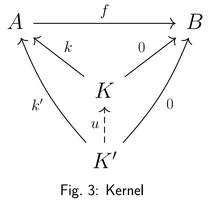


Fig. 3: Kernel

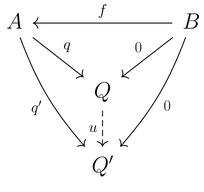


Fig. 4: Cokernel

- An **image** of a morphism $f : A \to B$ is a kernel of the cokernel of f.
- A **coimage** of a morphism $f : A \to B$ is a cokernel of the kernel of f.

Example. In the category $R-$Mod, a kernel of $f : A \to B$ is just $(\ker f, \iota)$, where ι is the inclusion of $\ker f \hookrightarrow A$. A cokernel of $f : A \to B$ is just $(B/\operatorname{im} f, \pi)$, where π is the quotient map $B \to B/\operatorname{im} f$.

Abelian Categories

- A **preadditive category** is a category $\mathcal{C}$ where all collections $\mathrm{Hom}_{\mathcal{C}}(A, B)$ are endowed with an abelian group structure, and all morphisms $f, g, h \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ satisfy
  - $f \circ (g + h) = (f \circ g) + (f \circ h)$
  - $(f + g) \circ h = (f \circ h) + (g \circ h)$.

  i.e., $\circ$ is biadditive.
- An **additive category** is a preadditive category that has all finite products and a zero object. In an additive category, all finite products are also coproducts.
- An **abelian category** is an additive category where
  - every morphism $f : A \to B$ has a kernel and cokernel.
  - every monomorphism is a kernel, and every epimorphism is a cokernel.
- An **exact sequence** is a sequence

$$\cdots \to X_{i-1} \xrightarrow{f_{i-1}} X_i \xrightarrow{f_i} X_{i+1} \to \cdots$$

of objects and morphisms in an abelian category $\mathcal{A}$ such that $\operatorname{im} f_i = \ker f_{i+1}$ for all i. In particular, $f_{i+1} \circ f_i = 0$.

Example. "$R-$Mod" is an abelian category. "Set" and "Top" are not abelian (they do not even have a zero object).

Proposition. Let $f : A \to B$ in an abelian category $\mathcal{A}$. Then, f is a mono iff $\ker f = 0$, and f is an epi iff $\operatorname{coker} f = 0$.

The Five Lemma

Theorem. (The Five Lemma) Let $\mathcal{A}$ be an abelian category. Consider the commutative diagram (Figure 5) of objects and morphisms in $\mathcal{A}$.

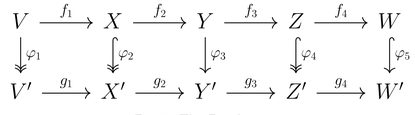


Fig. 5: The Five Lemma

Suppose both rows of the diagram are exact sequences. Additionally, suppose that φ_2 and φ_4 are isomorphisms (both an epimorphism and a monomorphism), φ_1 is an epimorphism, and φ_5 is a monomorphism. Then φ_3 must be an isomorphism.

Proof. For simplicity, we shall assume $\mathcal{A}$ is the category of R-modules. To prove that φ_3 is an isomorphism, it suffices to show that φ_3 is both injective and surjective.

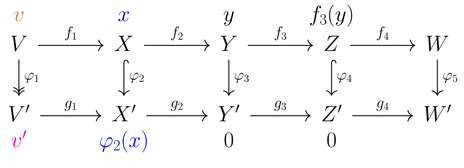


Fig. 6: Proof of Injectivity

To show injectivity of φ_3, we prove that $\ker(\varphi_3) = \{0\}$. Let $y \in \ker(\varphi_3)$, so that $\varphi_3(y) = 0 \in Y'$. Then $g_3(\varphi_3(y)) = g_3(0) = 0$. Since the diagram commutes, $\varphi_4(f_3(y)) = g_3(\varphi_3(y)) = 0$. Since φ_4 is injective, $\ker(\varphi_4) = \{0\}$. Thus $f_3(y) = 0$, so $y \in \ker(f_3)$. Exactness of the first row tells us that $\operatorname{im}(f_2) = \ker(f_3)$, so there exists an $x \in X$ such that $f_2(x) = y$. Now by commutativity of the diagram, we have

$$g_2(\varphi_2(x)) = \varphi_3(f_2(x)) = \varphi_3(y) = 0.$$

Thus $\varphi_2(x) \in \ker(g_2) = \operatorname{im}(g_1)$, so there exists $v' \in V'$ such that $g_1(v') = \varphi_2(x)$. Surjectivity of φ_1 implies that there exists a $v \in V$ such that $\varphi_1(v) = v'$. Then,

$$\varphi_2(f_1(v)) = g_1(\varphi_1(v)) = g_1(v') = \varphi_2(x).$$

By injectivity of φ_2, $f_1(v) = x$, so $f_2(f_1(v)) = f(x) = y$. By exactness, $f_2 \circ f_1$ is zero, so $y = 0$. Thus $\ker(\varphi_3) = \{0\}$, so φ_3 is injective.

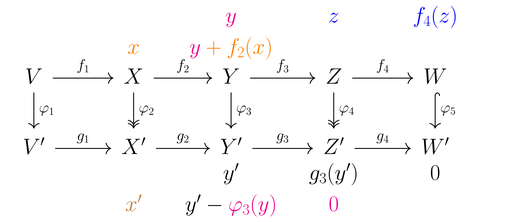


Fig. 7: Proof of Surjectivity

To prove φ_3 is surjective, let $y' \in Y'$. By surjectivity of φ_4 there exists $z \in Z$ such that $\varphi_4(z) = g_3(y')$. By exactness of the bottom row, $g_4 \circ g_3$ is zero. Then, by commutativity of the diagram,

$$0 = g_4(g_3(y')) = g_4(\varphi_4(z)) = \varphi_5(f_4(z)).$$

Thus $f_4(z) \in \ker(\varphi_5)$. Since φ_5 is injective, $f_4(z) = 0$. Thus, $z \in \ker(f_4) = \operatorname{im}(f_3)$, so there exists $y \in Y$ such that $f_3(y) = z$. Then,

$$g_3(\varphi_3(y)) = \varphi_4(f_3(y)) = \varphi_4(z) = g_3(y').$$

Thus $g_3(y' - \varphi_3(y)) = 0$ because g_3 is a homomorphism. Then $y' - \varphi_3(y) \in \ker(g_3) = \operatorname{im}(g_2)$ so there exists $x' \in X'$ such that $g_2(x') = y' - \varphi_3(y)$. Since φ_2 is surjective, there exists $x \in X$ such that $\varphi_2(x) = x'$. Then $\varphi_3(f_2(x)) = g_2(\varphi_2(x)) = g_2(x') = y' - \varphi_3(y)$. Therefore, $\varphi_3(f_2(x) + y) = \varphi_3(f_2(x)) + \varphi_3(y) = y' - \varphi_3(y) + \varphi_3(y) = y'$. Thus, every element of Y' has a nonempty preimage in Y, and therefore φ_3 is surjective.

□

References

(1) Francis Borceux. The Handbook of Categorical Algebra I: Basic Category Theory. Cambridge University Press, 1994.

(2) Thomas W. Hungerford. Algebra. Springer Science & Business Media, 2012.

(3) Samuel Petterson. Additive, abelian, and exact categories. 2016.

Application of Elliptic Curves to Fermat's Last Theorem

Elise Alvarez-Salazar, Caroline Baldan, and Kelly Stump

2022 Mathematics Directed Reading Program, University of California - Santa Barbara

Abstract

For this year's Directed Reading Program, we studied elliptic curves and methods for finding all their rational solutions. The three theorems about to be mentioned all tell us that the abelian group over $E(\mathbb{Q})$ has a rich group structure. Using this knowledge, we tackle the specific case of $n = 4$ of Fermat's Last Theorem.

Preliminary Information

Definition: An elliptic curve over $\mathbb{Q}$ is a smooth cubic projective curve E defined over $\mathbb{Q}$, with at least one rational point $\mathscr{O} \in E(\mathbb{Q})$ that we call the *origin*.

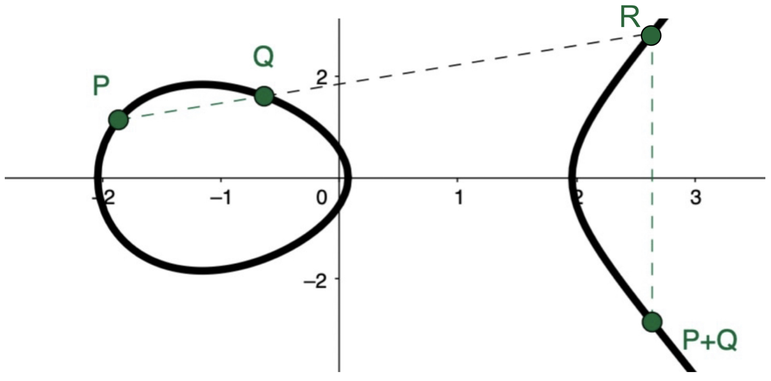
We will focus on elliptic curves of Weierstrass Form:

$$y^2 = x^3 + Ax + B \text{ where } A, B \in \mathbb{Z}$$

Defining P + Q

The operator for $E(\mathbb{Q})$ shall be defined as follows:

For $P, Q \in E(\mathbb{Q})$, where $P \neq Q$, we find the secant line which intersects both P and Q, $Y : y = ax + b$. Solving for the third point of intersection of Y with our curve E, labelled R, we see that $P + Q$ is the reflection of R over the x-axis.



For the case where $P = Q$, we consider the tangent line rather than the secant and a similar procedure follows to find $2P$. Note that every point has an inverse and our identity is the point at infinity, $\mathscr{O}$. Thus, we see that for this defined $+$ operator, we generate an abelian group on $E(\mathbb{Q})$.

Important Theorems

Mordell-Weil draws further conclusions about the previously created abelian group structure, stated below:

$E(\mathbb{Q})$ is a finitely generated abelian group. In other words, there are points $P_1, ..., P_n$ such that any other point $Q \in E(\mathbb{Q})$ can be expressed as a linear combination

$$Q = a_1P_1 + ... + a_nP_n$$

for some $a_i \in \mathbb{Z}$

From this theorem, and facts we know concerning finitely generated abelian groups, we find that:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}$$

Continuing on, we will refer to R_E as the *rank*. We can reach further conclusions about the group structure created over $E(\mathbb{Q})_{\text{torsion}}$ with Mazur's theorem stated in [**1**] as Thm 2.4.2.

Finding Rational Solutions

The natural continuation of the process of finding rational solutions for E is to next explore methods to calculate $E(\mathbb{Q})_{\text{torsion}}$ and $\mathbb{Z}^{R_E}$.

Specifically for calculating $E(\mathbb{Q})_{\text{torsion}}$, we have a theorem from Nagell-Lutz:

Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{Z}$ Then, every torsion point $P \neq \mathcal{O}$ of E satisfies:

(1) The coordinates of P are integers, i.e. $x(P), y(P) \in \mathbb{Z}$.
(2) If P is a point of order $n \geq 3$ then $4A^3 + 27B^2$ is divisible by $y(P)^2$.
(3) If P is of order 2 then $y(P) = 0$ and $x(P)^3 + Ax(P) + B = 0$.

We have come up with two methods from our readings for trying to calculate the rank. The first uses Theorem 2.6.4 in [**1**]. And the other possible solution is found in section 2.9 of [**1**].

Scan the following QR code to be taken to our algorithm that will find the torsion points of assorted elliptic curves:

Example of Finding Rational Solutions

Let us consider the elliptic curve $E : y^2 = x^3 - x$. Applying our code to E, we see that $(0, 0)$, $(1, 0)$, $(-1, 0)$ and the point at infinity make up $E(\mathbb{Q})_{\text{torsion}}$, where each non-identity element has order 2. We find that the discriminant $\Delta_E = 64$. Thus, the only prime of bad reduction to consider is $p = 2$. We determine that 2 is of multiplicative bad reduction. Thus, by Thm. 2.6.4 in [**1**], we see that

$$R_E \leq m + 2a - 1 = 0$$

Thus, $E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Fermat's Last Theorem (n = 4)

Problem Statement: Let $n = 4$. Are there any solutions to $a^n + b^n = c^n$ where $a, b, c \in \mathbb{Z}$ with $abc \neq 0$?

Solution: We claim that there are no non-trivial solutions. We are given the equation $a^4 + b^4 = c^4$, when $x = \frac{2(b^2+c^2)}{a^2}$ and $y = \frac{4b(b^2+c^2)}{a^3}$ are substituted in, we get the elliptic curve $E : y^2 = x^3 - 4x$.

Applying our given algorithm to this elliptic curve, we find that $E(\mathbb{Q})_{\text{torsion}} = \{(0, 0), (2, 0), (-2, 0), \mathscr{O}\}$. Note that these torsion points correspond to trivial solutions of $a^4 + b^4 = c^4$.

For the free part, an attempt to bound the rank proves insufficient as the prime of bad reduction is additive. Thus, we move onto use of the algorithm in 2.9 of [**1**] which tells us that the rank is 0. Thus, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}}$.

Acknowledgements

We would like to thank the DRP team for organizing this year's program. We would also like to thank our DRP Mentor, Marcos Reyes, for guiding us through our project. He was a wonderful resource while reading through our elliptic curve texts and taught us well.

References

[1] Á. Lozano-Robledo, *Elliptic Curves, Modular Forms and their L-functions*, American Mathematical Soc., 2011

[2] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 2015

Alexander Polynomial the Great

Alycia Doucette and Elizabeth Benda - Mentored by Melody Molander

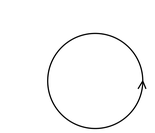
2022 Mathematics Directed Reading Program. University of California - Santa Barbara

Introduction

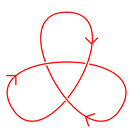
What is a **knot**? Simply speaking, a knot is a closed curve in space that does not intersect itself in any way. Knots have many applications to other fields of science and are fun for mathematicians to study. One of the main questions posed when studying knots is how to tell whether or not two different projections are the same knot. A tool that has developed as a way to distinguish two knots from each other is representing knots as polynomials. In this poster we will focus on one of the three major polynomial representations of knots, the Alexander polynomial.

Definitions

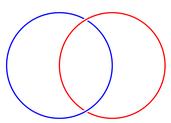
- **Projection:** A two-dimensional picture representation of a knot.
- **Orientation:** A direction in which you travel around the knot.
- **Crossing number:** The least number of crossings that occur in any projection of a particular knot.
- **Link:** A set of knotted loops tangled up together.
- **Unknot:** The unknot is also known as the trivial knot, and it looks as follows:



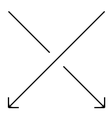
(a) Hi, I'm an oriented unknot!



(b) Hi, I'm an oriented trefoil!



(c) Hi, I'm a link!



(d) Hi, I'm a crossing!

The Alexander Polynomial

The Alexander polynomial was a method invented in 1928 as a way to represent knots and links as polynomial equations. It is an invariant for all representations of knots and links up to the same orientation. The Alexander polynomial is dependent on the orientation of the knot or link being assessed. The formula to compute the Alexander polynomial was refined by John Conway in 1969, and is now based on the following two rules:

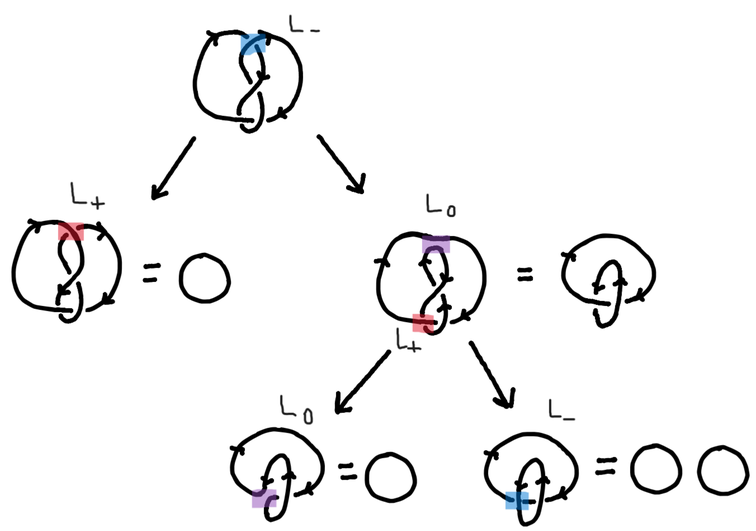
L_+ L_- L_0

$$\Delta(\bigcirc) = 1 \quad (1)$$

$$\Delta(L_+) - \Delta(L_-) + (t^{\frac{1}{2}} - t^{-\frac{1}{2}})\Delta(L_0) = 0 \quad (2)$$

The main tool used to compute the Alexander polynomial is called the **resolving tree**. The resolving tree is an easy way to break a knot down into a series of unknots and trivial links. In order to create the resolving tree, you choose one crossing of the knot, and determine whether it is an L_+, L_-, or L_0 crossing. From there, the chosen crossing is broken down into two new knots. These new knots are dependent on what type of crossing the original one is.

Resolving Tree of the Figure-Eight Knot



Alexander Polynomial of the Figure-Eight Knot

$$\Delta(L_+) - \Delta(L_-) + (t^{\frac{1}{2}} - t^{-\frac{1}{2}})\Delta(L_0) = 0$$

$$\Delta(L_+) = \Delta(\bigcirc) = 1$$

$$\Delta(L_0) = \Delta(\bigcirc \cup \bigcirc) - (t^{\frac{1}{2}} - t^{-\frac{1}{2}})\Delta(\bigcirc) = -(t^{\frac{1}{2}} - t^{-\frac{1}{2}})$$

$$\Rightarrow \Delta(L_-) = \Delta(L_+) + (t^{\frac{1}{2}} - t^{-\frac{1}{2}})\Delta(L_0) = 1 + (t^{\frac{1}{2}} - t^{-\frac{1}{2}})(-t^{\frac{1}{2}} + t^{-\frac{1}{2}})$$

$$= \boxed{3 - t - t^{-1}}$$

Since $3 - t - t^{-1} \neq 1$ we know that the figure-eight knot is not a projection of the unknot.

Other Polynomial Representations

The other polynomial representations we looked at were the Jones polynomial and the HOMFLY polynomial. The Jones polynomial, $V(t)$, is derived using three rules, and the base variable $t^{\frac{1}{2}}$. All prime knots with 9 or fewer crossings have a distinct Jones polynomial. The HOMFLY polynomial, unlike the other two, is multivariable. However, it does maintain a similar structure to that of the Alexander polynomial, using L_+, L_-, and L_0. Knots under both the HOMFLY and Jones polynomials are not affected by orientation, however, when computing the HOMFLY of a link, orientation between the two links does affect the result.

Consider the rules of the HOMFLY polynomial:

$$P(\bigcirc) = 1 \quad (1)$$

$$\alpha P(L_+) - \alpha^{-1} P(L_-) = z P(L_0) \quad (2)$$

The Alexander and Jones polynomials can be derived from the HOMFLY rules as follows:

$$\Delta(t) = P(\alpha = 1, z = t^{-\frac{1}{2}} - t^{\frac{1}{2}})$$

$$V(t) = P(\alpha = t^{-1}, z = t^{\frac{1}{2}} - t^{-\frac{1}{2}})$$

Conclusion

Each polynomial representation of knots has its own benefits and drawbacks. While the HOMFLY polynomial comes the closest to distinguishing between all knots and links, there is not currently any polynomial representation of knots that can completely distinguish all knots and links. Knots are the best!

References and Acknowledgements

It was fascinating to read and learn about how knots, simple strings in space, can be transformed into different polynomials. We would like to thank our graduate mentor Melody Molander, and the DRP, for creating this space for us to explore and grow our interests in mathematics.

Adams, Colin. The Knot Book. American Mathematical Society, 2004.

Introduction to Algebraic Number Theory

Robin Lee, Mr. Mulun Yin

University of California, Santa Barbara

UC SANTA BARBARA

Introduction

In this poster, we will overview the fundamentals of Algebraic Number Theory, focusing on the basic definitions of rings and fields, algebraic numbers, and algebraic integers.

Rings and Fields

As the most fundamental concept of Algebraic Number Theory, rings and fields are algebraic structures that contain two binary operations (addition and multiplication) with properties similar to those for integers $\mathbb{Z}$. In [1], we can define a **ring** as a non-empty set R with addition and multiplication. Assuming R is a ring, we mean it has the following characteristics:

- a set closed under addition $a+b \in R$ and multiplication $ab \in R$
- commutative under addition $a+b=b+a$
- associative under addition $a+(b+c)=(a+b)+c$ and multiplication $a(bc)=(ab)c$
- contains the additive identity $a+0=a, \forall a \in R$,for some $0 \in R$
- contains additive inverses: $\forall a \in R$, $\exists s \in R$ such that $a+s=0$
- contains the multiplicative identity $1*a=a*1=a, \forall a \in R$, for some $1 \in R$

Example of Rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$

An element of the ring $\mathbb{Z}[\sqrt{2}]$ is $a+b\sqrt{2}$ where $a,b \in \mathbb{Z}$.
An element of the ring $\mathbb{Z}[i]$ is $a+bi$ where $a,b \in \mathbb{Z}$.
An example of the ring's addition and multiplication properties is:
$(1+\sqrt{2})+(2+\sqrt{2})=3+2\sqrt{2}$, and
$(1+\sqrt{2})*(2+\sqrt{2})=2+2\sqrt{2}+\sqrt{2}+2=4+3\sqrt{2}$

Similar to rings, **fields** not only contain the same properties as a ring, but also contain multiplicative inverses (in addition to additive inverses) and is commutative under multiplication. In other words, a field F is a unique configuration of a commutative ring that contains at least two elements such that every non-zero element in F is both commutative under addition and multiplication. Furthermore, a field contains a multiplicative inverse.

Example of Fields: $\mathbb{Z}_n$ where n is a prime and positive integer, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$

An element of the field $\mathbb{Q}(\sqrt{2})$ is $a+b\sqrt{2}$ where $a,b \in \mathbb{Q}$.
An element of the field $\mathbb{Q}(i)$ is $a+bi$ where $a,b \in \mathbb{Q}$.

Algebraic Numbers and Minimal Polynomials

Diving deeper into our understanding of fields and rings, it is imperative we first overview an essential element to utilizing Algebraic Number Theory: Algebraic Numbers. According to [2], we can say that a complex number α is **algebraic** if it is the root of a polynomial with specifically integer coefficients, and **transcendental** if it is not. Furthermore, in the following proof, we can conclusively prove that there are only a countably large amount of Algebraic Numbers.
Given any polynomial with integer coefficients:

$$p(X)=C_0X^d+C_1X^{d-1}+\cdots+Cd=0.$$

with $C_i \in \mathbb{Z}$ and $C_0 \neq 0$, we can define the "height" $H(p)$ as:

$$H(p)=d+|C_0|+\cdots+|C_d| \in \mathbb{Z}$$

Such that given any $n \in \mathbb{Z}$, there are only finitely many such polynomials whose heights are $\leq n$. So, every polynomial with integer coefficients (which corresponds to an algebraic number) can thus be controlled by an integer, but $\mathbb{Z}$ is countably infinite—proving that Transcendental Numbers not only exist, but are also more prevalent than their Algebraic counterparts as $\mathbb{C}$ is uncountable.
Note: From the aforementioned properties, we can conclude that every rational $\frac{m}{n}$, where $m,n \in \mathbb{Z}$, is algebraic, since it is always a root of $nX-m=0$

With our definition of Algebraic Numbers established, we are able to quickly perceive the definition of the **Minimal Polynomial** of an algebraic number α. The minimal polynomial of α is a (unique) polynomial that consist of the following attributes: (1) coefficients are in $\mathbb{Q}$, (2) leading coefficient is 1 (monic), (3) smallest possible degree, and (4) α is a root.

Example of Minimal Polynomials: If $\alpha=\sqrt{2}$, then $f(x)=x^2-2$ is the minimal polynomial of $\sqrt{2}$, because all the coefficients in $f(x)$ are $\in \mathbb{Q}$, it is monic as the leading coefficient is 1, of the smallest degree (2), and α is a root. Similarly, the minimal polynomial of i is x^2+1.

Field of Algebraic Numbers

Utilizing our newfound knowledge of Algebraic Numbers and Minimal Polynomials, we can finally discuss the **Field of Algebraic Numbers**.

Let us define the set A of algebraic numbers. We actually know that set A is a field, but this will be proven later using field extension. Because it is a field, we can infer that it has the same properties as the ones we have mentioned in the "Rings and Fields" section. As such, if α and β are algebraic numbers, then so are the following:
$\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ where $\beta \neq 0$.

This is important, because for example, assume we want to find the minimal polynomial of $\sqrt{2}+\sqrt{3}$ to check using definition whether it's algebraic. This may be difficult to compute at first glance, but using our knowledge of the field of algebraic numbers, we already know $\sqrt{2}+\sqrt{3}$ is an algebraic number. Even though we did not find the minimal polynomial, we know this is algebraic, as both $\sqrt{2}$ and $\sqrt{3}$ are algebraic.

Field Extension

In our case, a field extension of $\mathbb{Q}$ can be defined as $\mathbb{Q}(\alpha)$, denoted by $\mathbb{Q}(\alpha)/\mathbb{Q}$, where $\mathbb{Q}(\alpha)$ is the smallest field containing $\mathbb{Q}$ and α (an algebraic number); there are a few examples in the Rings and Fields section. An element of $\mathbb{Q}(\alpha)$ is a polynomial with "variable" α (though α is fixed), with coefficients in $\mathbb{Q}$.

Note that we are able to combine two elements in $\mathbb{Q}(\alpha)$ as they are both polynomials and follow the usual rules for scalar multiplication and addition for polynomials. As such, $\mathbb{Q}(\alpha)$ is a vector space over $\mathbb{Q}$. Furthermore, the **degree of the field extension** is defined to be the dimension of the $\mathbb{Q}$ vector space $\mathbb{Q}(\alpha)$. Referring to $\mathbb{Q}(\sqrt{2})$, the dimension is 2, because we have a basis $\{1,\sqrt{2}\}$ that consists of 2 elements.

There exists a lemma that states α is algebraic if and only if the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ has a finite degree.

Using the aforementioned lemma, because α and β are algebraic, we know that $[\mathbb{Q}(\alpha):\mathbb{Q}]$ and $[\mathbb{Q}(\beta):\mathbb{Q}]$ are both finite. Thus, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$ must also be finite. As we can infer that $\alpha+\beta \in \mathbb{Q}(\alpha,\beta)$, this implies $\mathbb{Q}(\alpha+\beta) \subseteq \mathbb{Q}(\alpha,\beta)$ and $[\mathbb{Q}(\alpha+\beta):\mathbb{Q}]$ is finite. We know from the aforementioned lemma that α is algebraic if and only if the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ has a finite degree. Therefore, $\alpha+\beta$ must be algebraic. Note that in order to show algebraic numbers make a field, we just need to show that they are closed under the operations, since those axioms(say, associativity) are all inherited from C.
We can utilize this proof with $\alpha-\beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$(where $\beta \neq 0$), because they are all $\in \mathbb{Q}(\alpha,\beta)$. Hence, algebraic numbers form a field.

Example of Field Extension: The field extension $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}|a,b \in \mathbb{Q}\}$ and the degree is 2, and $\sqrt{2}$ is algebraic. We can test that $u+v$ and uv are still in the form $a+b\sqrt{2}$ where $a,b \in \mathbb{Q}$ when u,v are.

- $(a_1+_1 b\sqrt{2})+(a_2+b_2\sqrt{2})=(a_1+a_2)+(b_1+b_2)\sqrt{2}$
- $(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$

We define a **number field** K as an extension of $\mathbb{Q}$ of finite degree.

Integrality and the Ring of All Algebraic Integers

The **ring of all algebraic integers** I can be defined as an algebraic number α where the minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$. Thus, it is a subset of algebraic numbers, and in the following sections, we will prove that it forms a ring.

First and foremost, suppose α is a root of $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ where $a_i \in \mathbb{Q}$. Then, we have d = common multiple of denominators of a_i, then $d^n(\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0)=0$. Thus:

$d^n(\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0)=0$
$=>(d\alpha)^n+d\alpha_{n-1}(d\alpha)^{n-1}+\cdots+d^{n-1}a_1(d\alpha)+d^na_0=0$

Because $d\alpha$ is a root of the new equation, $x^n+da_{n-1}x^{n-1}+\cdots+d^{n-1}a_1x+d^na_0=0$. This means that $da_i \in \mathbb{Z}$, because we multiply a_i by its common denominator multiple and $a_i \in Q$. Thus, all the coefficients are integers and $d\alpha$ is an algebraic integer.

Therefore, $\forall \alpha \in A, \exists d \in \mathbb{Z}$ st $d\alpha \in I$,i.e., $d\alpha$ is an algebraic integer.

This means that every algebraic number α is an algebraic integer divided by an integer, which is analogous to a rational. Namely,

$$algebraic\ numbers=\frac{algebraic\ integers}{integers}$$

We define $\mathbb{Z}[\alpha]$ as the smallest ring containing $\mathbb{Z}$ and α, which is analogous to $\mathbb{Q}(\alpha)$. Similar to the lemma in the field extension, α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$ module. Now we are trying to prove that this a ring using this lemma.

Here R is a finitely generated $\mathbb{Z}$ module means every element in R can be written uniquely as a linear combination of fixed n elements. For example, every element in $\mathbb{Z}[i]$ is in the form $a+bi$ where $a,b \in \mathbb{Z}$. We will be able to show every element in $\mathbb{Z}[\alpha]$ is the root of a monic polynomial with coefficients $\in \mathbb{Z}$, i.e., they are all algebraic integers.

Analogous to the lemma in Field Extension, because α and β are algebraic integers, we know that $\mathbb{Z}[\alpha]$ is finitely generated and $\mathbb{Z}[\beta]$ is finitely generated. Thus, $\mathbb{Z}[\alpha,\beta]$ is finitely generated. Our previous proofs suggest that $\alpha+\beta \in \mathbb{Z}[\alpha,\beta]$, which means $\mathbb{Z}[\alpha+\beta] \subseteq \mathbb{Z}[\alpha,\beta]$ and $\mathbb{Z}[\alpha+\beta]$ is finitely generated. Therefore, $\alpha+\beta$ must be algebraic.
We can utilize this proof with $\alpha-\beta$, $\alpha\beta$, because they are all in $\mathbb{Z}[\alpha,\beta]$

Therefore, the set of all algebraic integers forms a ring.

Again, is $\sqrt{2}+\sqrt{3}$ an algebraic integer? We know the answer is yes, despite the fact that we didn't even compute it's minimal polynomial!

Integers in Number Fields

As a consequence, let us look at the **integers in a number field** K, which is by definition, $K \cap I$(namely, algebraic integers that are in K):

If we take $\alpha,\beta \in K \cap I$ (integers in K, as we just defined), then we can prove that their sum $\alpha+\beta \in K \cap I$.

Because they are in the intersections of K and I, $\alpha,\beta \in K$ and $\alpha,\beta \in I$. Furthermore, since I is a ring as proven above, $\alpha+\beta \in I$. Similarly, K is a field (closed under addition), so $\alpha+\beta \in K$.

Therefore, $\alpha+\beta \in K \cap I$. This is similar to $\alpha-\beta$ and $\alpha*\beta$, as both are in $K \cap I$.
In conclusion, $K \cap I$ forms a ring.

Example:
The integers in $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$
The integers in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$

Further Applications

With all these definitions, we could study number theory, say the theory of prime numbers, in a much broader context. Some familiar results about $\mathbb{Z}$ are still true in this new setting, but some are not (as an example, unique factorization of an integer into primes fail in general). These discoveries lead us to the modern algebraic number theory...
And yes, we are also able to show that the integers in a number field are always finitely generated—just as all the existing examples suggest.

References

[1] David R. Finston and Patrick J. Morandi. "Abstract Algebra: Structure and Application". In: (2010).

[2] Frazer Jarvis. "Algebraic Number Theory". In: (2010).

Elliptic Curve Cryptography

Rocky Beaty
Mentor: **Mychelle Parker**
University of California, Santa Barbara | 2022 Directed Reading Program
UC SANTA BARBARA
Department of Mathematics

What is an Elliptic Curve?

Definition 1 An *elliptic curve over a field K* is defined by an equation

$$E : y^2 = x^3 + ax + b \tag{1}$$

where $a, b \in K$ and $\Delta \neq 0$ where Δ is the *discriminant* of E and is defined as

$$\Delta = -16(4a^3 + 27b^2).$$

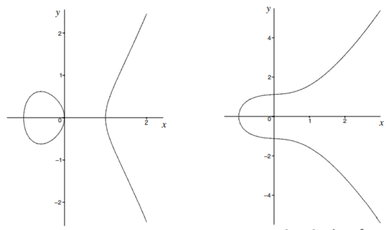
Note: There is a more general form of the equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

However, if the characteristic of $K \neq 2$ or 3, then the equation can be expressed as in (1). This assumption applies to all elliptic curves used in cryptography, and thus equation (1) is sufficient for us.

Definition 2 Let K be a field over which an elliptic curve is defined. Then the *K-rational* points, denoted $E(K)$, are all points on E with coordinates in K, along with the point at infinity denoted ∞. The *order* of the curve, $\#E(K)$, is the total number of points on the curve.

Elliptic curves can be defined over infinite fields such as $\mathbb{R}$ or $\mathbb{Q}$, or they can be defined over finite fields such as $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_q$. Consider the following graphs of various elliptic curves:



(a) $E_1 : y^2 = x^3 - x$

(b) $E_2 : y^2 = x^3 + \frac{1}{4}x + \frac{5}{4}$

Fig. 1: Elliptic Curves over $\mathbb{R}$. [1]

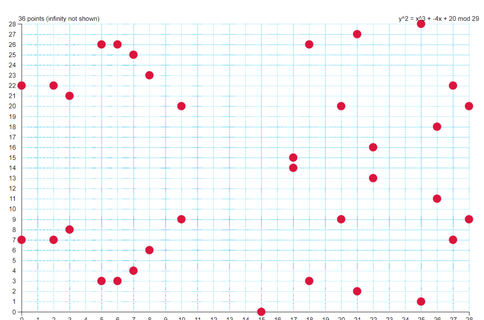
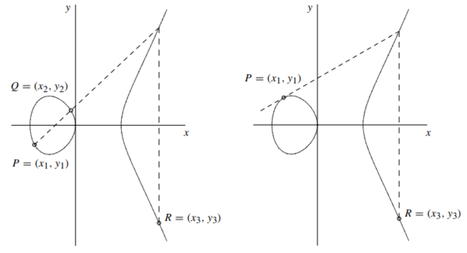


Fig. 2: Elliptic Curve over finite field $\mathbb{F}_{29}$. [2]

Group Law

There is a convenient way of defining an addition operation for two points in $E(K)$ to give a third point in $E(K)$. With this operation, the set of points in $E(K)$ forms an abelian group, where ∞ serves as the identity. The addition operation has a clear geometric interpretation. First, notice that any line will intersect an elliptic curve E at most 3 times. Given any two distinct points, $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, on E, then $P + Q = R = (x_3, y_3)$ is found by drawing a line through P and Q, find the third point this line intersects E. Then to obtain R reflect this point about the x-axis. Doubling a point P is the same, though the tangent line at the point P is used. Note: $P - Q$ is performed by taking $-Q = (x_2, -y_2) \in E(K)$.



(a) Addition: $P + Q = R$. (b) Doubling: $P + P = R$.

Fig. 3: Point Addition and Point Doubling. [1]

From this abelian group comes the basis for the scheme of elliptic curve cryptography.

What is Elliptic Curve Cryptography?

Elliptic Curve Cryptography (ECC) is a modern public-key cryptography technique based on the mathematics of elliptic curves over finite fields. ECC relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem.

Definition 3 The *elliptic curve discrete logarithm problem* (ECDLP) is: given an elliptic curve E defined over a finite field $\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ of order n, and a point $Q \in \langle P \rangle$, find the integer $l \in [0, n-1]$ such that $Q = lP$. The integer l is called the discrete logarithm of Q to the base P, denoted $l = \log_P Q$.

Simply put, the ECDLP is the problem of finding an integer n such that $Q = nP$. It exploits the fact that, as shown above, it is rather easy to double a point $P \in E(K)$ together, but it is thought to be very difficult to figure out how many times the point was doubled. The essential pieces of a secure ECC scheme are:

1. Elliptic Curve $E(\mathbb{F}_p)$ over finite field $\mathbb{F}_p$, p prime
2. P : generator - $P \in E(\mathbb{F}_p)$ *is a generator*
3. d : private key - $d \in \mathbb{Z}$ *is selected uniformly at random from the interval [1,n-1]*
4. Q : public key - *a point* $Q = dP \in E(\mathbb{F}_p)$
5. k : random integer - *used to increase security of encryption scheme*

In the ECC scheme, a sender's message is represented as a point M, and encrypted by adding it to kQ, where $Q = dP$ is the intended recipient's public key. The sender transmits the points $C_1 = kP, C_2 = M + kQ$ to the recipient who uses their private key d to compute

$$dC_1 = d(kP) = k(dP) = kQ$$

and can then easily recover $M = C_2 - kQ$. An attacker would have to find kQ, which is computationally infeasible using the public information.

Example

Note: It is possible to turn the geometric interpretation of point addition and point doubling into algebraic formulas by solving the cubic equations.
Let $K = \mathbb{F}_{97}$ and take

$$E : y^2 = x^3 + 2x + 3.$$

Consider $P = (3, 6)$, one can calculate the multiples of P using the mentioned algebraic formulas to obtain:

$$0P = \infty \;\; 1P = (3,6) \;\; 2P = (80,10) \;\; 3P = (80,87) \;\; 4P = (3,91)$$
$$5P = \infty \;\; 6P = (3,6) \;\; 7P = (80,10) \;\; 8P = (80,87) \;\; 9P = (3,91)$$

This pattern continues, so we see that $5P = \infty \implies P$ is a generator of order $n = 5$, and forms the *cyclic subgroup*

$$\langle P \rangle = \{\infty, P, 2P, 3P, 4P\}.$$

Now, consider the following problem. Let

$$P = (3,6),\ d = 3,\ Q = dP = 3P = (80,87),\ k = 9$$

and suppose the encoded message is $M = (24, 2)$. Using the algebraic formulas, one can calculate C_1 and C_2,

$$C_1 = kP = 9(3,6) = (3,91)$$

$$C_2 = M + kQ = (24,2) + 9(80,87) = (24,2) + (80,10) = (92,16).$$

The recipient receives C_1 and C_2, and then computes

$$dC_1 = d(kP) = k(dP) = kQ = (80,10)$$

so

$$M = C_2 - kQ = (92,16) - (80,10).$$

Notice that $-kQ = -(80,10) = (80,-10)$ where $-10 \equiv 87 \pmod{97}$ hence $-kQ = (80,87)$. So we get

$$M = (92,16) + (80,87) = (24,2)$$

as desired. An attacker wishing to recover M would likely know $E(\mathbb{F}_{97}), P, n, Q, C_1$ and C_2. However, even with this information it is computationally infeasible to compute kQ due to the cyclic nature of $\langle P \rangle$ and assuming k is sufficiently random.

Why ECC?

ECC is often preferred over RSA schemes because of the security and performance it offers using smaller key sizes. A common ECC key size of 256-bits is equivalent to a 3072-bit RSA key.

References

[1] *Elliptic Curves over Finite Fields*. `https://graui.de/code/elliptic2/`. Accessed: 2022-05-02.

[2] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Spring, 2004.

Algebraic Number Theory and Applications

Yanbo Cheng, Mychelle Parker
UC Santa Barbara

Motivations

It is known that a prime p can be written in the form $p = x^2+y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$. Since we can factorize such p in $\mathbb{Z}[i]$ as $p = (x+iy)(x-iy)$, it is natural to think of the prime elements in $\mathbb{Z}[i]$. We then want to relate the field $\mathbb{Q}(i)$ to $\mathbb{Z}[i]$, and a proposition was found that illustrates such relationship.
Proposition 1.

$$\mathbb{Z}[i] = \{x \in \mathbb{Q}(i) : x^2 + ax + b = 0 \text{ for some } a, b \in \mathbb{Z}\}$$

This proposition can be seen as a motivation to study the properties of algebraic integers of an algebraic number field.

Introduction

We first establish some basic principles of algebraic number theory.

Definition 2. An **algebraic number field** K is a finite extension of $\mathbb{Q}$. A element $\alpha \in K$ is called an **algebraic integer** if $f(\alpha) = 0$ for some monic polynomial $f(x) \in \mathbb{Z}[x]$.

Definition 3. Let $A \subseteq B$ be a ring extension. Then, $b \in B$ is **integral** over A if $f(b) = 0$ for some monic polynomial $f(x) \in A[x]$. We then define the **integral closure** to be the set $\overline{A} = \{b \in B : b \text{ integral over } A\}$. A is then called **integrally closed** if $A = \overline{A}$.

As in linear algebra, traces and norms play an important role in algebraic number theory. We thus give their definition.

Definition 4. For a finite field extension $L|K$. The **trace** of an element $\alpha \in L$ is the trace of the endomorphism $\psi : L \to L$, $\psi(x) = \alpha x$ where L is seen as a K-vector space. The **norm** pf α is then the determinant of ψ, that is:

$$Tr_{L|K}(\alpha) = Tr(\psi), \qquad N_{L|K}(\alpha) = \det(\psi)$$

There is an extra property in of traces and norms in a separable extension $L|K$ that uses field embeddings from L into an algebraic closure $\overline{K}$ of K.

Proposition 5. *Let $L|K$ be a separable extension, and define the set $\Sigma = \{\sigma : L \to \overline{K}$ a field embedding $\}$. Then we have:*

$$Tr_{L|K}(\alpha) = \sum_{\sigma \in \Sigma} \sigma(\alpha)$$

$$N_{L|K}(\alpha) = \prod_{\sigma \in \Sigma} \sigma(\alpha)$$

We then give the definition of a Dedekind domain, which is the main object that algebraic number theory studies.

Definition 6. A **Dedekind domain** is a neotherian, integrally closed integral domain in which every nonzero prime ideal is maximal.

The product and sum of ideals defined such that

$$\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

$$\mathfrak{ab} = \{\sum_{i \in I} a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, \forall i \in I\}$$

The importance of Dedekind domain is due to the fact that it gives unique prime factorization of prime ideals.

Dedekind domain

In this section, we denote $\mathcal{O}_K$ to be the ring of integers of an algebraic number field K. Such a ring has the following main properties:

Theorem 7. *$\mathcal{O}_K$ is a neotherian ring. It is integrally closed and every nontrivial prime ideal of $\mathcal{O}_K$ is a maximal ideal.*

Theorem 8. *Every ideal of $\mathfrak{a}$ of a Dedekind domain $\mathcal{O}$ that is nonzero and not the $\mathfrak{a} \neq \mathcal{O}$ admits a factorization in to nonzero prime ideal of $\mathcal{O}$:*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

This factorization is unique up to reordering.

We see that this is similar to a unique factorization domain in which every element admits a factorization into a product of a unit and irreducible elements which is unique up to association and reordering.
Then we can thus look at the properties of the extensions of Dedekind domains.
Let o be a Dedekind domain with field of fraction K, let $L|K$ be a field extension with integral closure $\mathcal{O}$. Then we can decompose prime ideals of o in $\mathcal{O}$

Theorem 9. *Let $\mathfrak{p}$ be a prime ideal of o, then*

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$$

with $f_i = [\mathcal{O}/\mathfrak{P}_i : o/p]$, we have the fundamental identity:

$$\sum_{i=1}^{n} f_i e_i = [L : K]$$

P-adic numbers

Now we introduce another topic, which are the p-adic numbers. We give two definitions of the p-adic integers $\mathbb{Z}_p$.

Definition 10. $\mathbb{Z}_p$ can be defined as the projective limit of if the rings $\mathbb{Z}/p^n\mathbb{Z}$, and thus

$$\mathbb{Z}_p = \lim_{n\leftarrow} \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_n \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : x_{n+1} \equiv x_n \mod p^n\}$$

We could also define $\mathbb{Z}_p$ through Cauchy sequences.
Define the p-adic absolute value $||_p$ as follows:
Let $a = \frac{b}{c}$, $b, c \in \mathbb{Z}$, we can find some integer n such that $a = p^n\frac{b'}{c'}$ where $(b'c', p) = 1$. Then we have $|a|_p = \frac{1}{p^n}$. We can thus define a metric using $||_p$ just like what we did using the normal absolute value $||$. Thus, we can define the p-adic numbers using Cauchy sequence with respect to the metric $||_p$. The induced metric on $\mathbb{Z}_p$ is $d(x, y) = |x - y|_p$ for $x, y \in \mathbb{Z}_p$.

Definition 11. Let R be the ring of Cauchy Sequence with respect to $||_p$, and m be the ideal of nullsequence, that is, the Cauchy sequences that converges to zero. Then we define the p-adic numbers $\mathbb{Q}_p$ as

$$\mathbb{Q}_p = R/m$$

Then, define the p-adic integers as

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

The Unit theorem

From Minkowski Theory, we derive the Dirichlet's Unit Theorem by studying the exact sequence:

$$1 \to \mu(K) \to \mathcal{O}_K^* \to \Gamma \to 0$$

Where $\mathcal{O}_K^*$ is the group of units and $\mu(K)$ is the roots of unity that lie in K, and Γ is the image $\lambda(\mathcal{O}_K^*)$ defined by

$$\lambda(a) = (log|\tau(a)|)_\tau \in [\prod_\tau \mathbb{R}]^+$$

Where τ run over the complex embeddings $\tau : K \to \mathbb{C}$.

Theorem 12. *The group of units $\mathcal{O}_K^*$ of $\mathcal{O}_K$ is the direct product of the finite group $\mu(K)$, which is the group of roots of unity are in K, and a free abelian group of rank $r + s - 1$. Where r is the number of real embeddings $\sigma : K \to \mathbb{R}$ and s is the number of pairs of complex conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$.*

This theorem give us a way to express any units u in $\mathcal{O}_K$ uniquely in the form

$$u = \xi u_1^{i_1} u_2^{i_2} \cdots u_{r+s-1}^{i_{r+s-1}}$$

where ξ is a root of unity and $u_1, u_2 \cdots$ are units of $\mathcal{O}_K$ that can be seen as a basis of the free abelian group mentioned above.

Applications

One of the applications of the Dirichlet's Unit Theorem is the solution of Pell's equations.

Corollary 13. *There exists infinily many pairs of solutions $x, y \in \mathbb{Z}$ to the equation*

$$x^2 + ny^2 = 1$$

with $n < 0$ not a perfect square and $n \in \mathbb{Z}$.

This is a direct application of the Dirichlet's Unit Theorem on the quadratic extension $K|\mathbb{Q}$, where $K = \mathbb{Q}(\sqrt{-n})$, and we use the fact that $r = 2$, $s = 0$, thus $r + s - 1 = 1$.
An application of the p-adic numbers is the following proposition:

Proposition 14. *Let $f(x_1, \cdots, x_n)$ be a polynomial with coefficients in integer. Then we have the equivalence:*

$$f(x_1, \cdots, x_n) \equiv 0 \mod p^n \text{ is solvable for all } n \geq 1$$
$$\iff f(x_1, \cdots, x_n) = 0 \text{ is solvable in p-adic integers}$$

Thus, the application of p-adic number also gives a way to solve problems in elementary number theory.

Acknowledgements

This is a poster of the Directed Reading Program in 2022. I would like to thank Mychelle Parker for being my mentor in this program.

References

Jürgen Neukirch, Algebraic Number Theory

Brouwer's Fixed Point Theorem with Application to Game Theory

Ruizhe Qian

Mentor: Pranav Arrepu

Introduction

We will prove Brouwer's Fixed Point Theorem by using fundamental groups. Then, we will show the application of Brouwer's Fixed Point Theorem to the game theory, namely the Nash Equilibrium.

Brouwer's Fixed Point Theorem in $\mathbb{R}$

Theorem (Brouwer's Fixed Point Theorem)**.** *Given that set $K \subset \mathbb{R}^n$ is compact and convex, and that function $f : K \to K$ is continuous, then there exists $c \in K$ such that $f(c) = c$.*

This is generalized statement of Brouwer's Fixed Point Theorem in $\mathbb{R}$. In this poster, we will explore the proof of a simple case, $D^2 \subset \mathbb{R}^2$. D^2 is homeomorphic to any closed and bounded compact subset of $\mathbb{R}^2$. But we will use the generalized version of this theorem to prove the existence of Nash equilibrium.

Algebraic Topology Preliminaries

We establish our theory from homotopy, an important equivalence relationship in topology,

Definition (Homotopy)**.** *[3] Two continuous maps $f_0, f_1 : X \to Y$ are said to be homotopic if there is a continuous map $F : X \times I \to Y$ such that $F(x, 0) = f_0(x)$ and $F(x, 1) = f_1(x)$. Then, we say $f_1(x) \simeq f_0(x)$*

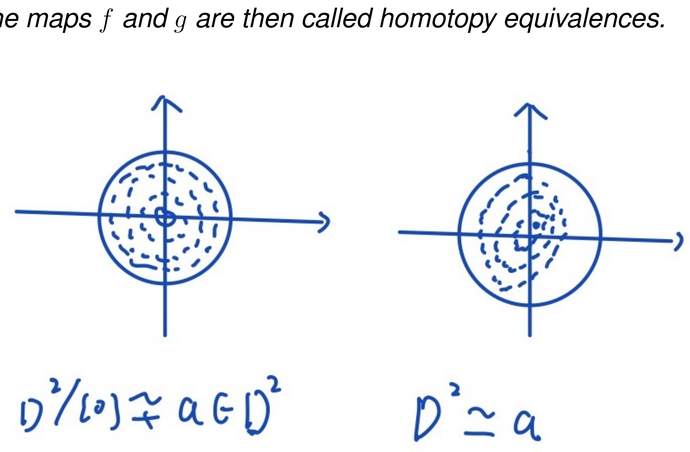
Definition (Homotopic Relative)**.** *Suppose that A is a subset of X and that f_0 and f_1 are two continuous functions from X to Y. We say f_0 and f_1 are homotopic relative to A if there is a homotopy $F : X \times I \to Y$ between f_0 and f_1 such that $F(a, t)$ does not depend on t for $a \in A$.*

Homotopy type, also known as homotopy equivalence, following from homotopy, is an important tool to classify topological space.

Definition (Homotopy Equivalence)**.** *Two spaces X and Y are homotopic equivalent if there exists continuous maps $f : X \to Y$ and $g : Y \to X$ such that*

$$g \circ f \simeq Id : X \to X$$
$$f \circ g \simeq Id : Y \to Y$$

The maps f and g are then called homotopy equivalences.



Spaces that are homotopy equivalent to a point are given a special name. The identity function of this space is homotopic to the constant map.

Definition (Contractible)**.** *A space X is said to be contractible if it is homotopy equivalent to a point.*

By using constant map and inclusion map, the following result can be easily derived.

Remark. *D^n is contractible and any convex subset of $\mathbb{R}^n$ is contractible.*

Consider that the cylinder, C and the circle S are a pair of homotopy equivalent spaces. Define $i : S \to C$ as the inclusion. This motivates the following definition.

Definition (Retraction)**.** *A subset A of a topological space X is called a retract of X if there is a continuous map $r : X \to A$ such that $r \circ i = Id : \quad A \to A$, where $i : A \to X$ is the inclusion map. The map r is called a retraction.*

Before we step into the definition of the fundamental group, we want to give the definition of some related concepts.

Definition (Path)**.** *A continuous mapping $f : [0, 1] \to X$ is called a path in X.*

Definition (Path Equivalent)**.** *Two path f, g in X are said to be equivalent if f and g are homotopic relative to $\{0, 1\}$. We write $f \sim g$*

Definition (Loop)**.** *A path is said to be closed if $f(0) = f(1)$. If $f(0) = f(1) = x$ then we say that f is based at x.*

Now, we have the definition of the fundamental group.

Definition (Fundamental Group)**.** *[1] The fundamental group of a space X will be defined so that its elements are loops in X starting and ending at a fixed basepoint $x \in X$ but two such loops are regarded as determining the same element of the fundamental group if one loop is homotopy equivalent to the other in space X. We denote this group as $\pi(X, x)$.*

We will explore the effect of continuous map between topological spaces $\psi : X \to Y$ has upon fundamental groups. Consider $\psi_* : \pi(X, x) \to \pi(Y, \psi(x))$ where $\psi_*[f] = [\psi f]$, f is a path in X.

Lemma. *ψ_* is a homomorphism of groups.*

Proof. $\psi_*([f][g]) = \psi_*([f * g] = [\psi(f * g)] = [\psi f * \psi g] = [\psi f][\psi g] = \psi_*[f]\psi_*[g]$. □

By proving this lemma, we can give ψ_* a name.

Definition (Induced Homomorphism)**.** *The homomorphism $\psi_* : \pi(X, x) \to \pi(Y, \psi(x))$ defined by $\psi_*[f] = [\psi f]$, where $\psi : X \to Y$ is a continuous map, is called the induced homomorphism.*

What if we have ψ as a homeomorphism?

Corollary. *If $\psi : X \to Y$ is a homeomorphism then $\psi_* : \pi(X, x) \to \pi(Y, \psi(x))$ is an isomorphism.*

The last piece of the puzzle is the fundamental group of the circle S^1, which turns out to be $\mathbb{Z}$. Let's consider a map e

$$\mathbb{R} \to S^1$$
$$t \to e^{2\pi i t}$$

Note that $e^{-1}(1) = \mathbb{Z} \subset \mathbb{R}$. If we are given $f : I \to S$ with $f(0) = f(1) = 1$, there is a unique map $\tilde{f} : I \to \mathbb{R}$ with $\tilde{f}(0) = 0$ and $e\tilde{f} = f$. $\tilde{f}$ is the lifting map of f. The integer $\tilde{f}(1) \in e^{-1}(1) = \mathbb{Z}$ is defined to be degree of f. If f_0 and f_1 are equivalent paths in S^1, then $\tilde{f}_0(1) = \tilde{f}_1(1)$. As a result, the function $\pi(S^1, 1) \to \mathbb{Z}$, where $[f] \mapsto degree(f)$, is isomorphism, which means the fundamental group of the circle is the set of integers.

Algebraic Proof for the Main Theorem

Proof. Suppose to the contrary that $x \neq f(x)$ for all $x \in D^2$. Then, we may define a function $\psi : D^2 \to S^1$ by setting $\psi(x)$ to be the point on S^1 obtained from the intersection of the line segment from $f(x)$ to x extended to meet S^1. We want to show ψ is continuous. Let's write ψ explicitely in coordinates, $y = \psi(x)$. The condition the ray meets the boundary is

$$|y + t(x - y)|^2 = 1.$$

It is a quadratic equation with the solution in

$$t_\pm = \frac{-2(x-y)y \pm \sqrt{4((x-y)y)^2 - 4|x-y|^2(|y|^2 - 1)}}{2|x-y|^2}$$

We only interested in the solution $y + t_+(x - y)$. Therefore, ϕ is continuous. Define $i : S^1 \to D^2$, denote the inclusion, then $\psi i = Id$ and we have the commutative diagram.

$$\begin{array}{ccc} S^1 & \xrightarrow{Id} & S^1 \\ & \searrow^{i} & \uparrow{\scriptstyle \psi} \\ & & D^2 \end{array}$$

This leads to another commutative diagram,

$$\begin{array}{ccc} \pi(S^1, 1) & \xrightarrow{Id} & \pi(S^1, 1) \\ & \searrow^{i_*} & \uparrow{\scriptstyle \psi_*} \\ & & \pi(D^2, 1) \end{array}$$

where ψ_* and i_* denote induced homomorphism. But $\pi(D^2, 1) = 0$ since D^2 is contractible, and so we get another commutative diagram due to isomorphism.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{Id} & \mathbb{Z} \\ & \searrow^{i_*\psi_*} & \uparrow \\ & & 0 \end{array}$$

This is impossible. Therefore, we prove the Brouwer's Fixed Point Theorem in two dimension. □

Game Theory Preliminaries

Now we move on to application to the game theory. We want to introduce the abstract notion of a normal form game, the following definitions are from [2]. We will use prisoner's dilemma to illustrate those definitions. In prisoner's dilemma, two prisoners are interrogated separately. If both of them confess, they get sentence for 3 years. If one confess, the other does not, the people who confess gets 1 years of sentence, the other gets 10 year. If both of them do not confess, they are innocent.

Definition (Normal-form game)**.** *A (finite, n-person) normal-form game is a tuple (N, A, O, μ, u), where*

- *N is a finite set of n players, indexed by i.*
- *$A = (A_1, \ldots, A_n)$, where A_i is a finite set of actions (or pure strategies; we will use the terms interchangeably) available to player i. Each vector $a = (a_1, \ldots, a_n) \in A$ is called an action profile (or pure strategy profile);*
- *O is a set of outcomes;*
- *$\mu : A \to O$ determines the outcomes as a function of the action profile; and*
- *$u = (u_1, \ldots, u_n)$ where $u_i : O \to \mathbb{R}$ is a real valued utility function for player i*

In prisoner's dilemma, $N = 2$. A is confess or not confess. O is what happens if both of prisoners confess, not confess and etc. In this way, μ and u is easy to understand. While players can select a single action to play, which is the pure strategy, they can also follow another type of strategy: randomizing over the set of available actions according to some probability distribution. Such strategy is called mixed strategy. We can define mixed strategy as follows. In prisoner's dilemma, mixed strategy can be like one person has 50% chance confessing 50% chance not confessing.

Definition (Mixed Strategy)**.** *Let $(N, (A_1, \ldots, A_n), O, \mu, u)$ be a normal form game, and for any set X let $\prod(X)$ be the set of all probability distributions over X. Then, the set of mixed strategies for player i is $S_i = \prod(A_i)$.*

Definition (Mixed Strategy Profile)**.** *The set of mixed strategy profiles is simply the Cartesian product of the individual mixed strategy sets, $S_1 \times \cdots \times S_n$.*

By $s_i(a_i)$ we denote the probability that an action a_i will be played under mixed strategy s_i. The subset of actions that are assigned positive probability by the mixed strategy s_i is called the support of s_i.

Definition (Support)**.** *The support of a mixed strategy s_i for a player i is the set of pure strategies $\{a_i | s_i(a_i) > 0\}$.*

Now, we want to introduce the concept of expected utility, a basic notion in decision theory,

Definition (Expected Utility of a Mixed Strategy)**.** *Given a normal form game (N, A, u), the expected utility u_i for player i of the mixed strategy profile $s = (s_1, \ldots, s_n)$ is defined as*

$$u_i(s) = \sum_{a \in A} u_i(a) \prod_{j=1}^{n} s_j(a_j)$$

Then, we want to look at games from an individual agent's point of view. This is going to lead us to the most influential concept in game theory, the Nash Equilibrium. Assume an agent knew how others were going to play, his strategy becomes simple. Define $s_{-i} = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$, a strategy profile s without i's strategy. We can write $s = (s_i, s_{-i})$. If the agents other than i were commit to play s_{-i}, a utility-maximizing agent I would face the problem of determining his best response.

Definition (Best Response)**.** *Player i's best response to the strategy profile s_{-i} is a mixed strategy $s_i^* \in S_i$ such that $u_i(s_i^*, s_{-1}) \geq u_i(s_i, s_{-i})$ for all strategies $s_i \in S_i$. Obviously, in prison's dilemma, confess is the best response.*

Finally, we will go to the most important definition, the Nah equilibrium. Its existence is one of the most well known application of Brouwer's Fixed Point Theorem.

Definition (Nash Equilibrium)**.** *A strategy profile $s = (s_1, \ldots, s_n)$ is a Nash equilibrium if for all agents i, s_i is a best response to s_{-i}*

When both prisoners confess, the game attain the Nash equilibrium.

Existence of Nash Equilibrium

Theorem (Nash 1951)**.** *Every game with a finite number of players and action profiles has at least one Nash equilibrium*

Proof. Given a strategy profile $s \in S$, for all $i \in N$ and $a_i \in A_i$ we define

$$\psi_{i,a_i}(s) = max\{0, u_i(a_i.s_{-i}) - u_i(s)\}$$

a function denoting the change of utility after each iteration of strategy. We then define the function $f : S \to S$ by $f(s) = s'$, where

$$s_i'(a_i) = \frac{s_i(a_i + \psi_{i,a_i}(s))}{\sum_{b_i \in A} s_i(b_i) + \psi_{i,b_i}(s)} = \frac{s_i(a_i + \psi_{i,a_i}(s))}{\sum_{b_i \in A} \psi_{i,b_i}(s) + 1}$$

Intuitively, this function maps a strategy profile s to a new strategy profile s' in which each agent's actions that are better responses to s receive increased probability mass.
The function f is continuous since each ψ_{i,a_i} is continuous. Since S is convex and compact and $f : S \to S$, by Brouwer's Fixed Point Theorem, f must have at least one fixed point.
First if s is a Nash equilibrium then all ψ's are 0, making s a fixed point of f.
Conversely, consider an arbitrary fixed point of f, s. If s is a fixed point, then $s'(a_i') = s(a_i')$. It follows that $\psi_{i,b_i}(s) = 0$, which only happens when no player can enhance their utility. Therefore, $s' = f(s)$ is the Nash equilibrium □

References

[1] Allen Hatcher. *Algebraic Topology*. 2001.

[2] Alber Xin Jiang and Kevin Leyton-Brown. "A Tutorial on the Proof of the Existence of Nash Equilibrium". In: (2007).

[3] Czes Kosniowski. *A First Course in Algebraic Topology*. Cambridge University Press, 1980.

A Bite-sized Introduction to Fluid Mechanics

Carlos Ortiz, advised by Pranav Arrepu

2022 Math Directed Reading Program, UC Santa Barbara

Introduction

The focus of fluid mechanics is the measurement of **observables** related to a fluid. Liquids and gases are examples of fluids, and their observables include temperature, pressure and density, to name a few. To approach this focus through first principles, the description of fluids is idealised by the notion of a *continuum*, which neglects the microscopic structure of fluids as separate molecules. "Infinitesimal" volume-elements of the fluid (called *fluid parcels*) are then understood to be large enough to contain many molecules, but small relative to the variation in the length-scale of the fluid properties. In this way, observables are understood to be averaged values over a fluid parcel. With this discussion, we are ready to form a mathematical approach to fluid theory.

To "Think" Eulerian or Lagrangian

There are two natural methods for studying fluid properties. In the **Lagrangian** approach, we follow a fluid parcel as it moves and measure the observables along the motion of the parcel. Suppose, at some initial time t_0, a fluid occupies an open set S_0 of $\mathbb{R}^n$. We could then label a *fluid particle* on the fluid (say with some dye) at the position $\mathbf{a} \in S_0$, and follow the particle over time. At some later time t, the fluid occupies the set S_t, and the particle's position is given by $\mathbf{X}(\mathbf{a}, t) \in S_t$. The Lagrangian coordinate $\mathbf{X}(\mathbf{a}, t)$ depends on the time as well as on the initial position to distinguish between fluid particles.

In the Eulerian approach, we instead consider a fixed point $\mathbf{x}$ in space and measure the fluid properties at this point as functions of time (being careful to ensure that $\mathbf{x}$ remains in S_t – otherwise no fluid is at the point!). An observable, q, is then a function of position and time: $q = q(\mathbf{x}, t)$.

Surely, there must be some relation between the two methods! In fact, the most obvious one is the concept of velocity: we have

$$\frac{\partial \mathbf{X}}{\partial t} = \mathbf{u}(\mathbf{X}(\mathbf{a}, t), t), \tag{1}$$

where $\mathbf{u}$ is the **flow velocity** in the Eulerian viewpoint at the Lagrangian coordinate $\mathbf{X}$. This follows merely by construction. But what about other observables? In the Lagrangian perspective, any observable attached to a fluid parcel just depends on the time explicitly. In the Eulerian viewpoint, however, the observables depend on time explicitly and implicitly through the position. By the Chain rule,

$$\frac{\mathrm{d}\, q(\mathbf{X}(\mathbf{a}, t), t)}{\mathrm{d}\, t} = \frac{\partial q}{\partial t} + \frac{\partial \mathbf{X}}{\partial t} \nabla q = \partial_t q + \mathbf{u} \cdot \nabla q. \tag{2}$$

The special operator

$$\frac{\mathrm{D}}{\mathrm{D}t} \equiv \frac{\partial}{\partial t} + \mathbf{u} \cdot \nabla, \tag{3}$$

is called the **material derivative**, and denotes the Lagrangian time derivative in Eulerian variables.

A Useful Identity: The Derivative of the Determinant of the Jacobian

One useful way to describe how fluid parcels transform is by the Jacobian $\mathbf{J}$. (For simplicity, I will work in three-dimensions, and I'll make heavy use of indicial notation and Einstein summation convention.) Recall in the Lagrangian viewpoint that a fluid moves from a set S_0 to S_t, which can be understood to occur via a map $M_t : S_0 \to S_t$. We now introduce the Jacobian of this map, whose elements are given by

$$\mathbf{J}_{ij} = \left.\frac{\partial x_i}{\partial a_j}\right|_t. \tag{4}$$

The determinant of the Jacobian can be written succinctly using the completely antisymmetric tensor, ϵ_{ijk}, as

$$J = \epsilon_{ijk} \mathbf{J}_{1i} \mathbf{J}_{2j} \mathbf{J}_{3k}. \tag{5}$$

With this, we can describe the deformation of a fluid parcel from $S_0 \to S_t$ by

$$\int_{S_t} \mathrm{d}^3\mathbf{x} = \int_{S_0} J \, \mathrm{d}^3\mathbf{a}. \tag{6}$$

We might be interested in observing how volume integrals like (6) change over time. This raises an interim problem: what is the material derivative of J? Well, by the product rule,

$$\frac{\mathrm{D}\, J}{\mathrm{D}\, t} = \epsilon_{ijk} \left(\frac{\mathrm{D}\, \mathbf{J}_{1i}}{\mathrm{D}\, t} \mathbf{J}_{2j} \mathbf{J}_{3k} + \mathbf{J}_{1i} \frac{\mathrm{D}\, \mathbf{J}_{2j}}{\mathrm{D}\, t} \mathbf{J}_{3k} + \mathbf{J}_{1i} \mathbf{J}_{2j} \frac{\mathrm{D}\, \mathbf{J}_{3k}}{\mathrm{D}\, t} \right). \tag{7}$$

Consider the derivative in the first term on (7):

$$\frac{\mathrm{D}\, \mathbf{J}_{1i}}{\mathrm{D}\, t} = \frac{\mathrm{D}}{\mathrm{D}\, t} \left(\frac{\partial x_1}{\partial a_i} \right) = \frac{\partial}{\partial a_i} \frac{\mathrm{D}\, x_1}{\mathrm{D}\, t} = \frac{\partial u_1}{\partial a_i} = \frac{\partial u_1}{\partial x_l} \frac{\partial x_l}{\partial a_i} = \frac{\partial u_1}{\partial x_l} \mathbf{J}_{li}. \tag{8}$$

We interchange the derivatives since the initial position $\mathbf{a}$ is time-independent. The first term of (7) now expands completely as

$$\epsilon_{ijk} \frac{\mathrm{D}\, \mathbf{J}_{1i}}{\mathrm{D}\, t} \mathbf{J}_{2j} \mathbf{J}_{3k} = \epsilon_{ijk} \frac{\partial u_1}{\partial x_l} \mathbf{J}_{li} \mathbf{J}_{2j} \mathbf{J}_{3k}. \tag{9}$$

For $l \neq 1$, $\epsilon_{ijk} = 0$ by definition since then $i = j$ or $i = k$. An analogous approach can be made for the other two terms of (7), admitting one final term by virtue of index repetition. Thus, reducing (7) gives

$$\frac{\mathrm{D}\, J}{\mathrm{D}t} = \epsilon_{ijk} \mathbf{J}_{1i} \mathbf{J}_{2j} \mathbf{J}_{3k} \left(\frac{\partial u_l}{\partial x_l} \right) = J(\nabla \cdot \mathbf{u}). \tag{10}$$

With this result, we can observe how a fluid property $q(\mathbf{X}(\mathbf{a}, t), t)$ changes with time over a fluid parcel:

$$\frac{\mathrm{D}}{\mathrm{D}\, t} \int_{S_t} q(\mathbf{X}(\mathbf{a}, t), t) \, \mathrm{d}^3\mathbf{x} = \frac{\mathrm{D}}{\mathrm{D}\, t} \int_{S_0} q J \, \mathrm{d}^3\mathbf{a} = \int_{S_0} \left(\frac{\mathrm{D}\, q}{\mathrm{D}\, t} J + q \frac{\mathrm{D}\, J}{\mathrm{D}\, t} \right) \mathrm{d}^3\mathbf{a} \tag{11}$$

$$= \int_{S_0} \left(\frac{\mathrm{D}\, q}{\mathrm{D}\, t} + q \nabla \cdot \mathbf{u} \right) J \, \mathrm{d}^3\mathbf{a} = \int_{S_t} \left(\frac{\mathrm{D}\, q}{\mathrm{D}\, t} + q \nabla \cdot \mathbf{u} \right) \mathrm{d}^3\mathbf{x} \tag{12}$$

$$\implies \frac{\mathrm{D}}{\mathrm{D}\, t} \int_{S_t} q(\mathbf{X}(\mathbf{a}, t), t) \, \mathrm{d}^3\mathbf{x} = \int_{S_t} \left(\frac{\mathrm{D}\, q}{\mathrm{D}\, t} + q \nabla \cdot \mathbf{u} \right) \mathrm{d}^3\mathbf{x}. \tag{13}$$

The result of equation (13) is known as the *Reynolds Transport Theorem*. When the observable $q = \rho(\mathbf{X}(\mathbf{a}, t), t)$, we have

$$\frac{\mathrm{D}}{\mathrm{D}\, t} \int_{S_t} \rho \, \mathrm{d}^3\mathbf{x} = \int_{S_t} \left(\frac{\mathrm{D}\, \rho}{\mathrm{D}\, t} + \rho \nabla \cdot \mathbf{u} \right) \mathrm{d}^3\mathbf{x}. \tag{14}$$

If we assume that mass is conserved, then (14) must be zero. The equation above must hold for all fluid parcels, which is only true if the integrand itself is zero:

$$\frac{\mathrm{D}\, \rho}{\mathrm{D}\, t} + \rho \nabla \cdot \mathbf{u} = 0. \tag{15}$$

The Euler Equations of Motion

The result (15) is known as the *continuity equation*, and, together with conservation of momentum, we can arrive at the so-called Euler equations. Newton's second law relates the material derivative of the momentum of a fluid to the net external force on the fluid. The net force per unit volume can be expressed generally as

$$F_i = f_i + \frac{\partial \sigma_{ij}}{\partial x_j}, \tag{16}$$

where σ_{ij} is the stress tensor and f_i is some external body force. Assuming an ideal fluid, the stress tensor is completely diagonal with $\sigma_{ij} = -p\delta_{ij}$, so that $\nabla \cdot \sigma = -\nabla p$, where p is the pressure exerted normal to the surface of the fluid. Hence, by Newton's second law,

$$\int_{S_t} \rho \frac{\mathrm{D}\, \mathbf{u}}{\mathrm{D}\, t} \, \mathrm{d}^3\mathbf{x} = \int_{S_t} \mathbf{f} \, \mathrm{d}^3\mathbf{x} + \int_{\partial S_t} (\boldsymbol{\sigma} \cdot \hat{n}) \, \mathrm{d}^2\mathbf{x}. \tag{17}$$

By the Divergence theorem, the far-right integral becomes $\int_{S_t} (\nabla \cdot \boldsymbol{\sigma}) \, \mathrm{d}^3\mathbf{x}$, so that

$$\int_{S_t} \rho \frac{\mathrm{D}\, \mathbf{u}}{\mathrm{D}\, t} \, \mathrm{d}^3\mathbf{x} = \int_{S_t} (\mathbf{f} + \nabla \cdot \boldsymbol{\sigma}) \, \mathrm{d}^3\mathbf{x} = \int_{S_t} (\mathbf{f} - \nabla p) \, \mathrm{d}^3\mathbf{x}. \tag{18}$$

Since this must hold for all such fluid parcels, we arrive at the second Euler equation:

$$\rho \frac{\mathrm{D}\, \mathbf{u}}{\mathrm{D}\, t} = \mathbf{f} - \nabla p. \tag{19}$$

The Navier-Stokes Equations of Motion for Viscous Fluids

The Euler equations assume stresses incident only normal to the surface of a fluid. Real fluids, however, are hardly as ideal. We can correct the equations of motion by modifying the stress tensor σ_{ij} to contain additional stresses unrelated to pressure. By Cauchy's Theorem (see [2]), one can prove that these non-pressure forces, represented by the *deviatoric tensor*, act linearly on the normal vector. Then we can split up the stress tensor into a sum of two terms: (i) the stresses normal to the surfaces of the fluid given by the pressure; and (ii) the stresses acting at arbitrary directions along the surface of the fluid. Mathematically, $\sigma_{ij} = -p\delta_{ij} + d_{ij}$, where d_{ij} denotes the deviatoric tensor. The implementation of this stress tensor to obtain the equations of motion is analogous to the method in obtaining the Euler equations. But before that, we need to first obtain the form of the deviatoric tensor.

By a physical argument, we find that the deviatoric, and hence the stress tensor, is symmetric. From Figure 1, one can see that the torque about the z-axis of a cube centered at the origin is $\alpha^3(\sigma_{21} - \sigma_{12})$, where α is the side-length of the cube. From elementary physics, we know that the moment of inertia of such a cube is of order α^4, so that the angular acceleration is proportional to $\alpha^{-1}(\sigma_{21} - \sigma_{12})$. In the limit of a fluid parcel $\alpha \to 0$, the angular acceleration remains finite only if $\sigma_{21} = \sigma_{12}$. A similar computation of the torque about the other axes allows one to conclude that the tensor is symmetric.

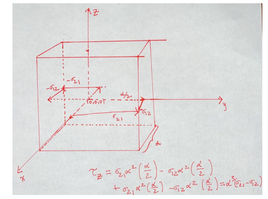


Figure 1.

For momentum to be conserved, the force on the fluid must be proportional to the gradient of the velocity. See the discussion on section 6.1 of [1]. As a result, the deviatoric tensor is a linear function of the deformation tensor $D_{ij} = (1/2)(\partial u_i/\partial x_j + \partial u_j/\partial x_i)$. This also means that d_{ij} and D_{ij} are simultaneously diagonalisable. By permuting the eigenvalues under rotations, the requirement that d_{ij} be isotropic forces the deviatoric tensor to take the form

$$d_{ij} = \lambda(\nabla \cdot \mathbf{u})\delta_{ij} + \mu \left(\frac{\partial u_i}{\partial x_j} + \frac{\partial u_j}{\partial x_i} \right). \tag{20}$$

With the full form of the deviatoric tensor, we can derive the equations of motion. By Newton's second law, we obtain (17) except now with our corrected stress tensor. The only new addition is the deviatoric tensor term $\int_{\partial S_t} (\mathbf{d} \cdot \hat{n}) \, \mathrm{d}^2\mathbf{x}$, which, by the Divergence theorem, becomes $\int_{S_t} (\nabla \cdot \mathbf{d}) \, \mathrm{d}^3\mathbf{x}$. Consider just one component (using index notation and Einstein summation convention):

$$(\nabla \cdot \mathbf{d})_i = \frac{\partial d_{ij}}{\partial x_j} = \lambda \delta_{ij} \frac{\partial}{\partial x_j} (\nabla \cdot \mathbf{u}) + \mu \frac{\partial}{\partial x_j} \frac{\partial u_j}{\partial x_i} + \mu \frac{\partial^2 u_i}{\partial x_j^2} \tag{21}$$

$$= \lambda \delta_{ij} \frac{\partial}{\partial x_j} (\nabla \cdot \mathbf{u}) + \mu \frac{\partial}{\partial x_i} \frac{\partial u_j}{\partial x_j} + \mu \nabla^2 u_i \tag{22}$$

$$= \lambda \left(\delta_{i1} \frac{\partial}{\partial x_1} + \delta_{i2} \frac{\partial}{\partial x_2} + \delta_{i3} \frac{\partial}{\partial x_3} \right) (\nabla \cdot \mathbf{u}) + \mu \frac{\partial}{\partial x_i} (\nabla \cdot \mathbf{u}) + \mu \nabla^2 u_i \tag{23}$$

Upon specifying the index i, the first and second terms of (23) are really the same thing, up to the viscosity coefficients λ and μ. From this, we obtain that

$$\nabla \cdot \mathbf{d} = (\lambda + \mu) \nabla (\nabla \cdot \mathbf{u}) + \mu \nabla^2 \mathbf{u}. \tag{24}$$

Returning to Newton's second law, we have

$$\int_{S_t} \rho \frac{\mathrm{D}\, \mathbf{u}}{\mathrm{D}\, t} \, \mathrm{d}^3\mathbf{x} = \int_{S_t} \left(\mathbf{f} - \nabla p + (\lambda + \mu) \nabla (\nabla \cdot \mathbf{u}) + \mu \nabla^2 \mathbf{u} \right) \mathrm{d}^3\mathbf{x}. \tag{25}$$

Since (25) must hold for any volume, it follows that

$$\rho \frac{\mathrm{D}\, \mathbf{u}}{\mathrm{D}\, t} = \mathbf{f} - \nabla p + (\lambda + \mu) \nabla (\nabla \cdot \mathbf{u}) + \mu \nabla^2 \mathbf{u}. \tag{26}$$

And so, we arrive at the *Navier-Stokes* equations for a viscous fluid!

References

[1] Stephen Childress. *An introduction to theoretical fluid mechanics*, volume 19. American Mathematical Soc., 2009.

[2] Alexandre Joel Chorin and Jerrold E Marsden. *A mathematical introduction to fluid mechanics*, volume 3. Springer, 1990.

[3] Jerrold E Marsden and Thomas JR Hughes. *Mathematical foundations of elasticity*. Courier Corporation, 1994.

Lebesgue Measure and Integration

Vardan Martirosyan Jordan Russo

University of California, Santa Barbara

Abstract and Background

Traditionally, the integral of a non-negative single valued function is defined to be the area under the smooth curve of the function, from a start point a to an end point b on the real number line. In undergraduate courses, this concept is formalized as the Riemman Integral. After proving numerous results and theorems relating to Riemman Integration, as well as extending it to multiple dimensions, it is shown that the Riemman Integral has some limitations: namely, there are severe issues when dealing with point-wise limits, and integrating sequences. To resolve these issues, the concept of the Lebesgue Measure and Lebesgue Integration is introduced at the end of undergraduate and the beginning of graduate courses. For our project, we studied the Lebesgue Measure and Lebesgue Integration from the textbook "Real Analysis" by H. Royden and P. Fitzpatrick.

Definitions

We first define several important terms:

- **Open, Non-Empty, and Bounded Sets** A *open* set is a set such that, for any point in the set, and any given distance, a point of the set can be found between the given point and distance. A *non-empty* set is a set that has at least one element contained within it. A *bounded* set is a set that is of a finite size.
- **Complement of a Set** Let E be a set of points. The *complement* of E, denoted by E^c, is the set of points that are not in E. We note that $E \cap E^c$, the intersection of E and it's complement, is the empty set $\emptyset$. Additionally, the union of E and E^c is all of the points U that are being looked at.

Length

Consider the extended real number line, which spans $\mathbb{R}$, the set of real numbers, combined with $-\infty$ and $+\infty$. Let I be an interval on the extended real number line. We define the **length of** I to be the difference of it's endpoints if it is bounded, and to be ∞ if it is unbounded. We call the length function a **set** function, which is a function that assigns an extended real number to each set in a collection of sets.

Outer Measure

Before being able to define the Lebesgue Measure, we first have to define a separate measure, called the **outer measure**. Let A be a set of real numbers. Consider the countable collections $\{I_k\}_{k=1}^{\infty}$ of nonempty, open, bounded intervals that cover A. For each collection, consider the sums of the lengths of the intervals within the collection. Since the lengths are forced to be positive numbers, each sum is uniquely defined independently of the order of the terms. We can then define the **outer measure** of A, $m^*(A)$, to be the infimum of all types of sums:

$$m^*(A) = \inf\left\{\sum_{k=1}^{\infty} l(I_k) | A \subseteq \cup_{k=1}^{\infty} I_k\right\} \tag{1}$$

Measurable Functions and the Lebesgue Measure

Let E be a set. We define E to be measurable if for any set A, we have the following to be true:

$$m^*(A) = m^*(A \cap E) + m^*(A \cap E^c) \tag{2}$$

All sets that satisfy the above equation make up a Borel sigma algebra. Then, the **Lebesgue Measure** is the restriction of the set function outer measure to this class of measurable sets. We denote the Lebesgue measure by m, and write that $m(E) = m^*(E)$. We note that the Lebesgue measure is not defined on all subsets of $\mathbb{R}$: only those that satisfy the above equation. (A proof of why not all subsets of $\mathbb{R}$ are measurable comes from Vitali's Theorem).

Properties of the Lebesgue Measure

There are several key properties that the Lebesgue Measure contains, which we will now describe:

- **The Measure of An Interval is it's Length** Let I be an arbitrary non-empty interval. Then, I is Lebesgue Measurable and:
$$m(I) = l(I) \tag{3}$$
where l is the 'set' length function described earlier.
- **Lebesgue Measure is Translation Invariant** Let E be a Lebesgue measurable set, and y be any number. Then, the translation of E by y, $E + y = \{x + y | x \in E\}$, is also Lebesgue measurable and:
$$m(E + y) = m(E) \tag{4}$$
We display a picture to illustrate this property:

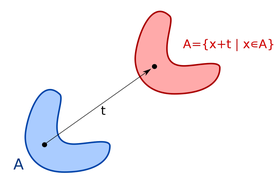


Figure 1. A picture displaying what translation invariance looks like. The picture comes from Wikipedia.

- **Lebesgue Measurable is Countably Additive Over Countable Disjoint Unions of Sets** Let $\{E_k\}_{k=1}^{\infty}$ be a countable disjoint collection of Lebesgue measurable sets. Then, we have that:
$$m(\cup_{k=1}^{\infty} E_k) = \sum_{k=1}^{\infty} m(E_k) \tag{5}$$
We note that one of the key differences between the outer measure defined earlier and the Lebesgue Measure is that in the equation above, the outer measure has sub-additive property, which is less powerful than the additive property stated above.

Lebesgue Measurable Functions

An extended real-valued function defined on a set E is said to be **Lebesgue measurable**, provided it's domain E is measurable, and it satisfies one of the following two conditions:

- For each real number c, the set $\{x \in E | f(x) > c\}$ is measurable.
- For each real number c, the set $\{x \in E | f(x) \geq c\}$ is measurable.

Characterizations and Properties of Measurable Functions

- A function f is measurable if and only if for each open set O, the inverse image of O under f is measurable.
- A real valued function that is continuous on it's measurable domain is measurable.
- A monotone function that is defined on an interval is measurable.
- Linear combinations, products, and compositions of finite measurable functions on the same set E are also measurable on the set E.
- A non-negative measurable function is the limit of a sequence of simple functions.

Lebesgue Integration

Characteristic Functions For any set A, we define the characteristic function of A on the real numbers, denoted by χ_A, as:

$$\chi_A(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases} \tag{6}$$

Simple Functions Let ϕ be a real valued function defined on a measurable set E. It is called a simple function if it is measurable and takes a finite number of values. Any simple function can be represented as a linear combination of characteristic functions:

$$\psi = \sum_{k=1}^{n} c_k \cdot \chi_{E_k}, \quad E_k = \{x \in E |\ \psi(x) = c_k\} \tag{7}$$

Integration of Simple Functions For a simple function ψ defined on a set E where $m(E) < \infty$, we defined the integral of ψ over E by:

$$\int_E \psi = \sum_{i=1}^{n} a_i \cdot m(E_i) \tag{8}$$

Lebesgue Integration For a bounded real-valued function f defined on a set E where $m(E) < \infty$, we define the lower and upper Lebesgue Integral, respectively, of f over E to be:

$$\sup\left\{\int_E \psi \;\middle|\; \psi \text{ simple},\ \psi \leq f \text{ on } E\right\} \quad \text{and} \quad \inf\left\{\int_E \phi \;\middle|\; \phi \text{ simple},\ f \leq \phi \text{ on } E\right\} \tag{9}$$

We say that f is **Lebesgue Integrable** over E when its lower and upper Lebesgue integrals over E are equal. We call the common value the **Lebesgue Integral** of f over E, and denote it by:

$$\int_E f \tag{10}$$

Advantages over the Riemman Integral

Monotone convergence Theorem Suppose we have a sequence of non-negative measurable functions $\{f_n\}$ on a measurable set X such that f_n converges pointwise to f almost everywhere and $f_1 \leq f_2 \leq \cdots \leq f_n$. The Monotone Convergence Theorem gives us the following property for Lebesgue integration:

$$\lim_{n\to\infty} \int_X f_n = \int_X \lim_{n\to\infty} f_n = \int_X f \tag{11}$$

Under the Riemman Integral, the ability to move the limit inside the integral requires uniform convergence, while under the Lebesgue Intregral, we only require pointwise convergence. We now give an example to illustrate the use of the Monotone Convergence Theorem. Let a_{ij} be an non-negative real valued sequence of numbers. Then, we have that:

$$\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_{ij} = \sum_{j=0}^{\infty}\sum_{i=0}^{\infty} a_{ij} \tag{12}$$

Acknowledgements

We would like to Pranav Arrepu for his guidance in helping us understand the material during this program. Additionally, we would like to thank the Directed Reading Program at UCSB for giving us the opportunity to participate in this program.

Sticking a 'PINN' in It: A Physics-Informed Neural Network Approach to PDEs

Yan Lashchev [1] Bill Nguyen [1] Mentor: Rafael Lainez Reyes [1]

[1]Department of Mathematics, University of California - Santa Barbara

UCSB

Abstract

Recent successes in neural networks have greatly encouraged their use in solving classical problems in applied mathematics, as the networks allow for rapid prototyping with usable estimations. This holds especially true in areas involving high dimensional partial differential equations (PDEs), such as quantum physics and fluid dynamics. Here, we present a neural network architecture, the physics-informed neural network (PINN), and implement a specific method, the continuous time approach.

Background

We describe the PINN approach for approximating the solution

$$u : [0,T] \times \mathcal{D} \to \mathbb{R} \quad (\star)$$

of an evolution equation

$$\partial_t u(t,x) + \mathcal{N}[u](t,x) = 0, \qquad (t,x) \in (0,T] \times \mathcal{D}, \tag{1a}$$
$$u(0,x) = u_0(x), \qquad x \in \mathcal{D}, \tag{1b}$$

where $\mathcal{N}$ is a differential operator acting on u, $\mathcal{D} \subset \mathbb{R}^d$ a bounded domain, T denotes the final time and $u_0 : \mathcal{D} \to \mathbb{R}$ the prescribed initial data. Based on the literature review conducted, we restrict our discussion to the Dirichlet case and define

$$u(t,x) = u_b(t,x), \quad (t,x) \in (0,T] \times \partial\mathcal{D}, \tag{1c}$$

where $\partial\mathcal{D}$ denotes the boundary of the domain $\mathcal{D}$ and $u_b : (0,T] \times \partial\mathcal{D} \to \mathbb{R}$ the given boundary data. The method constructs a neural network approximation $u_\theta(t,x) \approx u(t,x)$ of the solution of (1), where $u_\theta : [0,T] \times \mathcal{D} \to \mathbb{R}$ denotes a function realized by a neural network with parameters θ.

Continuous Time Approach

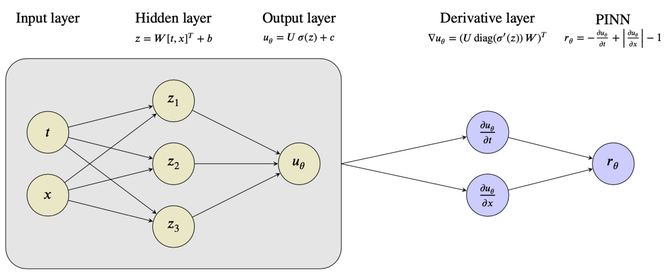


Figure 1) Neural network architecture of the PINN approach

The (strong) residual of a given neural network approximation of $(\star)$ with respect to the PINN approach above is

$$r_\theta(t,x) := \partial_t u_\theta(t,x) + \mathcal{N}\left[u_\theta\right](t,x) \tag{2}$$

These networks are compositions of alternating affine linear $W^\ell \cdot + b^\ell$ and nonlinear functions $\sigma^\ell(\cdot)$ called activations, i.e.,

$$u_\theta(z) := W^L \sigma^L \left(W^{L-1}\sigma^{L-1}\left(\cdots \sigma^1\left(W^0 z + b^0\right)\cdots\right) + b^{L-1}\right) + b^L,$$

where W^ℓ and b^ℓ are weight matrices and bias vectors, and $z = [t,x]^T$.

PINN Approach

For the solution of the PDE (1) now proceeds by minimization of the loss functional

$$\phi_\theta(X) := \phi_\theta^r\left(X^r\right) + \phi_\theta^0\left(X^0\right) + \phi_\theta^b\left(X^b\right), \tag{3}$$

where X denotes the collection of training data and the loss function ϕ_θ contains the following terms:

The Mean Squared Residual

$$\phi_\theta^r\left(X^r\right) := \frac{1}{N_r}\sum_{i=1}^{N_r}\left|r_\theta\left(t_i^r, x_i^r\right)\right|^2$$

in a number of collocation points $X^r := \left\{\left(t_i^r, x_i^r\right)\right\}_{i=1}^{N_r} \subset (0,T] \times \mathcal{D}$, where r_θ is the physics-informed neural network (2),

The Mean Squared Misfit *w.r.t* Initial and Boundary Conditions

$$\phi_\theta^0\left(X^0\right) := \frac{1}{N_0}\sum_{i=1}^{N_0}\left|u_\theta\left(t_i^0, x_i^0\right) - u_0\left(x_i^0\right)\right|^2 \quad \text{and} \quad \phi_\theta^b\left(X^b\right) := \frac{1}{N_b}\sum_{i=1}^{N_b}\left|u_\theta\left(t_i^b, x_i^b\right) - u_b\left(t_i^b, x_i^b\right)\right|^2$$

in a number of points $X^0 := \left\{\left(t_i^0, x_i^0\right)\right\}_{i=1}^{N_0} \subset \{0\} \times \mathcal{D}$ and $X^b := \left\{\left(t_i^b, x_i^b\right)\right\}_{i=1}^{N_b} \subset (0,T] \times \partial\mathcal{D}$, where u_θ is the neural network approximation of the solution $u : [0,T] \times \mathcal{D} \to \mathbb{R}$.

Example: Heat Equation

A classical problem in the domain of PDEs, the heat equation governs the temperature distribution of a rod of length l :

$$u_t = k u_{xx} \qquad (t,x) \in \mathbb{R}^+ \times (0,l)$$
$$u(t,0) = u(t,l) = 0 \qquad t \geq 0$$
$$u(0,x) = f(x) \qquad x \in (0,l).$$

If k, called the conductivity is a constant the rod is isotropic; if $k = k(x)$ it is anisotropic or heterogeneous medium.

Application

With respect to the fitting, we choose $k = 1, l = \pi$, and $f(x) = \sin(3x)$ for the demo of the PINN.

We assume that the collocation points X_r as well as the points for the initial time and boundary data X_0 and X_b are generated by random sampling from a uniform distribution.

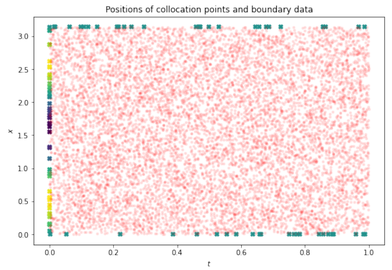
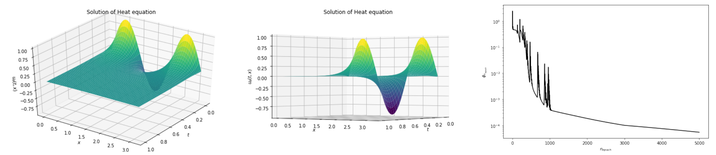


Figure 2) Plot of the collocation points ($N = 10,000$)

PINN Approximation and Evolution of Loss



(a) View 1 (b) View 2 (c) Loss

Test

The chosen problem can be solved via separation of variables. The idea is to assume the solution $u = u(t,x)$ can be written as

$$u(t,x) = F(t)G(x)$$

If we compute the corresponding partial derivatives and replace in the PDE, we get

$$\frac{F'(t)}{F(t)} = \frac{G''(x)}{G(x)}$$

The only way this equality is true for all t and x is if

$$F'(t) = \lambda F(t) \quad \text{and} \quad G''(x) = \lambda G(x)$$

The boundary condition becomes

$$G(0) = G(\pi) = 0$$

We can easily solve these ordinary differential equations. By considering the cases $\lambda > 0, \lambda = 0$ and $\lambda < 0$, we conclude $\lambda = -n^2, n \in \mathbb{N}$ and (up to constants)

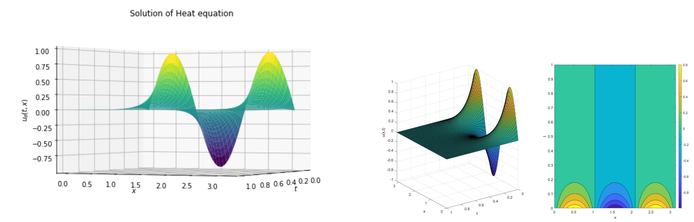
$$F(t) = \exp\left(-n^2 t\right) \quad \text{and} \quad G(x) = \sin(nx)$$

Since the equation is linear, by the principle of superposition $u(t,x) = \sum_{n=1}^{\infty} c_n \exp\left(-n^2 t\right)\sin(nx)$

Finally, since $u(0,x) = \sin(3x) = \sum_{n=1}^{\infty} c_n \sin(nx)$ with $c_3 = 1$ and $c_n = 0$ if $n \neq 3$. Hence,

$$u(t,x) = \exp(-9t)\sin(3x)$$

True Solution



(a) PINN (b) True Solution

References

[1] Jan Blechschmidt Oliver Ernst. Three ways to solve partial differential equations with neural networks — a review. *GAMM-Mitteilungen*, 44(2), 2021.

[2] Peter Olver. Introduction to partial differential equations. *Springer*, 2020.

Primitive Parking Functions and Non-Crossing Partitions

Yanru Liu, Mentored by **Sam Sehayek**

2022 Mathematics Direct Reading Program. University of California, Santa Barbara

Parking Functions

Imagine living on a one-way street that dead-ends with n parking spots available. You and your neighbors have n cars in total, and everyone has their preferred spot to park. Without reversing, does there exist a solution that everyone can park without collision? In mathematics, this real life dilemma is called the parking problem. Consider this set up:

- There are n cars and n parking spots on a straight street (n is a positive integer, $n \in \mathbb{Z}^+$; and i denotes the i-th spot, $i \in \{1, \cdots, n\}$)
- C_i is the i-th car to park, having preferred spot $\alpha_i \in \{1, \cdots, n\}$. More than one car can have the same preference.
- If the preferred spot had already been occupied, then the car will move forward and park in the next available spot. No backward movement allowed.

If all n cars can be parked under these conditions, then the preference list $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is a parking function.
Equivalently, an n-tuple of integers $\alpha = (\alpha_1, \cdots, \alpha_n)$ is a **parking function** if and only if $\beta_i \leq i$, where $\beta = \{\beta_1, \cdots, \beta_n\}$ is a reordering of α into weakly increasing order. i.e. $\beta_1 \leq \cdots \leq \beta_n$.
For n cars, how many parking functions are there?

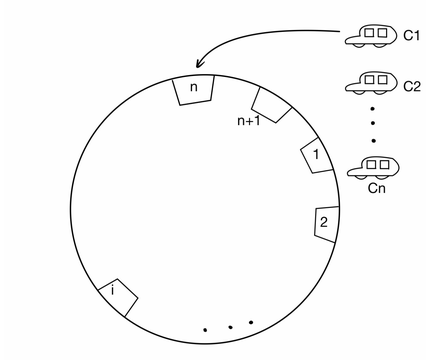


Fig. 1: Visual Representation of H.Pollack's Proof.

Regard the elements of the group $G = \mathbb{Z}/(n+1)\mathbb{Z}$ as being the integers $0, 1, \cdots, n$. Let H be the (cyclic) subgroup of order $n+1$ of the group G^n generated by $(1, 1, \cdots, 1)$. Each coset of H contains exactly one parking function. Let $f(n)$ be the number of parking functions of length n, hence we have

Theorem 1 (Konheim and Weiss, 1966)**.** *The number of parking functions of length n is*

$$f(n) = (n+1)^{n-1}.$$

Primitive Parking Functions

A parking function is called a **primitive parking function** if it is already in a weakly increasing order.
There is a well-known bijection between parking functions and labeled Dyke paths, wherein each distinct labeling of the same Dyke path corresponds to a permutation of the parking function. Thus, the primitive parking functions with length $n-1$ are in bijection with Dyke paths and can be enumerated by the n-th Catalan number:

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Non-Crossing Partitions

A **partition** of a finite set S is a collection $\{B_1, \cdots, B_k\}$ of nonempty subset $B_i \subseteq S$ s.t. $B_1 \cup \cdots \cup B_k = S$ and $B_i \cap B_j = \emptyset$ if $i \neq j$. And in our research of primitive parking functions, we especially care about a special one: the non-crossing partition. A **non-crossing partition** of set $\{1, \cdots, n\}$ is a partition $\{B_1, \cdots, B_k\}$ of $\{1, \cdots, n\}$ s.t. for $a < b < c < d$, $a, c \in B_i$, and $b, d \in B_j \Rightarrow i = j$.

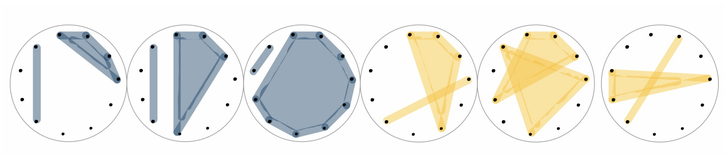


Fig. 2: Non-Crossing Partitions (Blue) & Crossing Partitions (Yellow) of $\{1, \cdots, 11\}$.

A **maximal chain** of non-crossing partitions of $\{1, \cdots, n+1\}$ is a sequence $\pi_0, \cdots, \pi_n$ of noncrossing partitions s.t. π_i is obtained from π_{i-1} by merging two blocks of π_{i-1} into a single block.
A maximal chain of $[n+1]$ has n merging steps. If we pick a label for each step, there are exactly n labels. Thus, it's possible for us to connect parking function with maximal chains.

Theorem 2. *There is a bijection between parking functions of length n and maximal chains of NC_{n+1}.*

Here is the algorithm: Let A and B be the two blocks we're going to merge at stage i, and A contains the smallest element in the disjoint union $A \cup B$. The label for this stage is the largest element in A which is smaller than all elements in B.

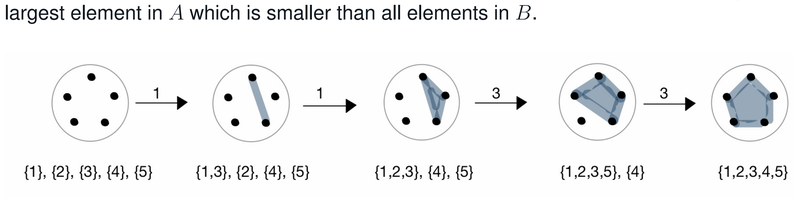


Fig. 3: One of the Maximal Chain of $\{1, \cdots, 5\}$ and Its Associated Parking Function $(1, 1, 3, 3)$.
(The top is 1 and the label goes in clockwise direction)

Every maximal chain is associating with a parking function, and only some of them are associating with the primitive ones.

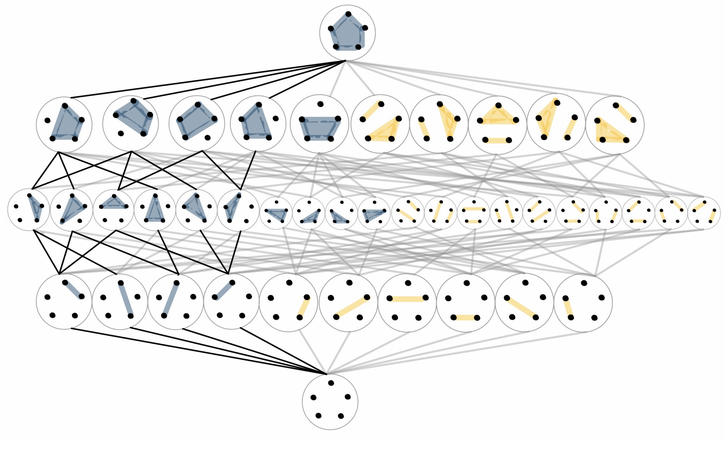


Fig. 4: Primitive Parking Functions with Length 4 (black) in the Maximal Chains of Noncrossing Partitions of $\{1, \cdots, 5\}$ (grey).

A New Proposition

For maximal chains corresponding to the primitive parking functions, do they form a certain pattern?

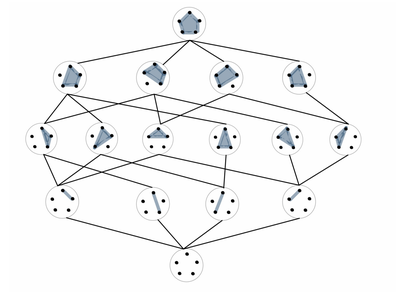
Lemma 3. *The chain starts by merging 1 with some other element.*

This lemma is trivial as the primitive parking function is always starting with 1, and only the merging between 1 and some other element gives the label 1.

Lemma 4. *The primitive parking functions are always adding one single block to the other block.*

This proposition can be verified via figure 4. From these lemmas, we can prove:

Proposition 5. *The subdiagram consisting only of nodes and edges from the primitive parking functions inside the non-crossing partition lattice is a coarsening of the Boolean lattice of size equal to the length of these parking functions.*



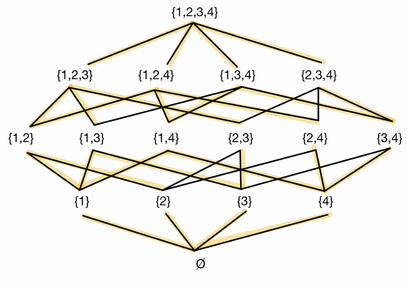


Fig. 6: Maximal Chains for Primitive Parking Functions of Length 4 (Up)
& Boolean Lattice of size 4 (Bottom).

In other words, maximal chains of primitive parking functions of length n are look just like the Boolean lattice of the same size with some relations removed.

Acknowledgements

I would like to thank my mentor Sam Sehayek, his knowledge and enthusiasm in mathematics deeply impressed me; he is such a good mentor and friend on my way of learning mathematics.

Reference

Richard P. Stanley. *Enumerative Combinatorics*. Cambridge Press, 1998.

A Brief Introduction to Network Theory

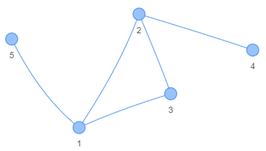
Ponokela DeMarzo

University of California, Santa Barbara

What is a Network?

A **network** is a collection of nodes where pairs of nodes may be connected by edges.

Networks can be visualized by drawing their graph structure, but they are also commonly represented by their adjacency matrix. The **adjacency matrix** for a network consisting of n nodes is an n x n matrix $\mathbf{A}$ with entries A_{ij} = the number of edges connecting node i and j.



$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Figure 1: The graph and adjacency matrix representations of the same network.

Edges can be **weighted**, where each edge is assigned a value that represents the "strength" of the connection, as well as **directed**, where a connection from node i to j does not imply a connection from j to i. Networks are also not limited to only one type of node; however, since many of the forms of analysis change, we will not be discussing them.

Node Centrality

A natural question arising from the gathered network data is determining the importance, or **centrality**, of each node. This can give us an idea of which nodes have more influence over a network. The four main centrality measures are defined below:

- **Degree Centrality:** This is perhaps the simplest measure of centrality, calculated by counting the number of edges attached to the node in question. In terms of the adjacency matrix $\mathbf{A}$, the degree centrality of a node i can be defined as follows:

$$k_i = \sum_j A_{ij}.$$

- **Eigenvector Centrality:** Unlike degree centrality, eigenvector centrality is primarily concerned with the *quality* of connections, not *quantity*. To measure centrality this way, the centrality of a node i will be proportional to the centrality of its neighbors, and thus is defined recursively like so:

$$x_i = \kappa^{-1} \sum_j A_{ij} x_j.$$

Rewritten in matrix notation, this equation becomes

$$\mathbf{x} = \kappa^{-1}\mathbf{A}\mathbf{x}, \text{ or } \mathbf{A}\mathbf{x} = \kappa\mathbf{x}.$$

In this form, it is clear that $\mathbf{x}$ is an eigenvector of $\mathbf{A}$; however, since there may be multiple eigenvectors, we generally define $\mathbf{x}$ and κ to be the leading eigenvector and eigenvalue.

- **Closeness:** This is a measure of the average distance from a node to other nodes. Suppose that d_{ij} is the shortest distance from node i to node j. Then the average distance from i to every other node is

$$\ell_i = \tfrac{1}{n-1} \sum_j d_{ij}.$$

Since we want to consider nodes that are on average closer to all other nodes as being more central, we define the closeness centrality as the inverse of ℓ_i so

$$C_i = \tfrac{1}{\ell_i} = \frac{n-1}{\left(\sum_j d_{ij}\right)}.$$

- **Betweenness:** This measures how often a given node lies on a shortest path between other nodes. Let n_{st}^i be the number of shortest paths from s to t that pass through i, and let g_{st} be the total number of shortest paths from s to t. We can then define the betweenness centrality of a node i as follows:

$$x_i = \tfrac{1}{n^2} \sum_{st} \tfrac{n_{st}^i}{g_{st}}.$$

A Social Network Example

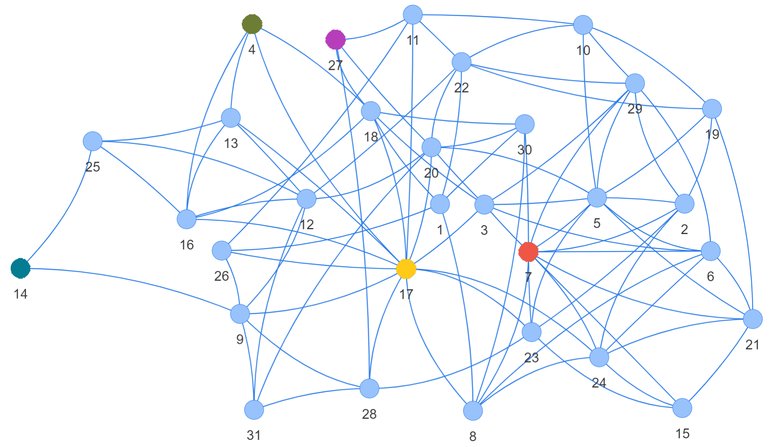


Figure 2: A social network constructed from anonymized friendship data collected by surveying a high school math classroom. The density of the network is 20.2% and the clustering coefficient is 37.2%. The largest core is a 4-core which includes all nodes except 14 and 25.

Network Analysis

Node	Degree	Eigenvector	Closeness	Betweenness	Local Clustering
1	5	0.1049	0.4615	0.0209	0.2
2	6	0.2153	0.4347	0.0116	0.4666
3	7	0.2595	0.5454	0.0525	0.4285
4	4	0.0911	0.4347	**0.0018**	**0.8333**
5	10	0.3201	0.5084	0.0657	0.3777
6	7	0.2605	0.4477	0.0107	0.5714
7	11	**0.3491**	0.4838	0.0573	0.3818
8	6	0.1972	0.4918	0.0285	0.4
9	6	0.0967	0.4687	0.0671	0.2666
10	5	0.1390	0.4347	0.0131	0.5
11	5	0.1054	0.4687	0.0324	0.2
12	7	0.1116	0.4838	0.0767	0.2857
13	5	0.0918	0.4477	0.0169	0.6
14	**2**	**0.0207**	**0.3370**	0.0021	**0**
15	4	0.1432	0.4	0.0019	0.6666
16	6	0.1111	0.4761	0.0297	0.5333
17	**13**	0.2783	**0.625**	**0.2732**	0.1538
18	7	0.1537	0.5	0.0474	0.2380
19	5	0.1485	0.4225	0.0156	0.4
20	8	0.2040	0.5555	0.0926	0.1428
21	6	0.2093	0.4285	0.0125	0.5333
22	7	0.1516	0.5084	0.0817	0.1904
23	6	0.2025	0.5084	0.0603	0.3333
24	7	0.2372	0.5	0.0573	0.4285
25	4	0.0481	0.375	0.0135	0.5
26	4	0.0840	0.4615	0.0137	0.3333
27	4	0.0815	0.4411	0.0102	**0**
28	5	0.1052	0.4687	0.0316	0.3
29	7	0.2432	0.4687	0.0247	0.4761
30	5	0.1447	0.4687	0.0171	0.3
31	4	0.0742	0.4285	0.0065	0.5

Table 1: The centrality and clustering measures for each node in Figure 2. The largest and smallest values in each column are bolded and the corresponding nodes are highlighted. Node 17 has the highest degree, closeness, and betweenness centralities, however, node 7 has the highest eigenvector centrality due to the importance of its neighbors (e.g., nodes 5 and 6). Node 4 has the highest clustering coefficient, indicating a tight-knit friend group, but has a low betweenness centrality because it is somewhat redundant in the network. Node 14 is the most isolated.

Why are Networks Useful?

Networks are a powerful analytical tool which are used across many different disciplines with a multitude of applications. Networks are an elegant representation of almost any system which consists of *objects* and *connections between those objects*, and when modeled this way, we can perform well-defined and meaningful calculations to analyze its structure.

There are four primary categories in which we can sort networks: technological, information, social, and biological. Technological networks are physical networks which are typically responsible for the transfer of data or materials, such as the Internet, waterlines, or commercial airline flights. Information networks can model the interaction of ideas, and are used to represent structures such as the World Wide Web or citation networks for academic papers. Social networks are used to model people and their interactions, such as friendships in a workplace or followers on social media. Even systems such as metabolic processes and food chains can be modeled by biological networks.

Network Structure

Beyond simply ranking nodes in accordance to their centralities, it also often important to be able to describe the overall structure of the network. Below are some basic, yet useful, measures of network structure:

- **Density:** In a simple network consisting of n nodes, we can calculate the maximum possible number of edges by counting the number of pairs of nodes given by $\binom{n}{2}$. The density of a network is the proportion of existing edges to the maximum possible edges.
- **k-cores:** A k-core is a connected set of nodes where each node is connected to at least k other nodes in the set.

Figure 3: The nodes 1-4 form a 3-core, and the nodes 1-5 form a 2-core.

- **k-components:** A k-component is a set of nodes where each node is reachable from each of the others by k node-independent paths.

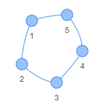


Figure 4: This network forms a 2-component.

- **Local Clustering Coefficient:** The local clustering coefficient is the proportion of the number of neighbors of a node i that are neighbors themselves. Visually, this can be thought of as the fraction of closed triangles out of all possible triangles with i as a vertex.

Figure 5: The local clustering coefficient of node 1 is $1/3$.

- **Clustering Coefficient:** This is a generalization of the local clustering coefficient to the whole network. For the whole network, it is the proportion of connected triples that are also closed triangles.

References

[1] Mark Newman.
Networks, Second Edition.
Oxford University Press, 2018.

Guided by

Sanjay Kumar
UCSB

Differential Forms and Maxwell's Equations

Samuel Zhang - Mentored by Yusen Xia

Department of Mathematics - University of California, Santa Barbara

Introduction

Differential manifolds are topological spaces that are locally homeomorphic to a vector space so that one may perform calculus on it, and a differential form allows one to define integrals over such manifolds. This poster is meant to revisit the Maxwell's Equations using such languages

Smooth Manifolds and Tangent Map

- A topological space M is called an *n-dimensional manifold* if $\forall p \in M$ there is a homeomorphism $F : U \to O$ such that $U \subset \mathbb{R}^n$ is non-empty and open, and $O \subset M$ is an open subset containing p. Such an F is called a *local parametrization* around p
- An n-dimensional manifold is called an *n-dimensional smooth manifold* if there is a collection of local parametrizations $F_\alpha : U_\alpha \to O_\alpha$ such that
  - $\cup U_\alpha = M$ (such parametrizations cover all of M)
  - Any transition map $F_\alpha^{-1} \circ F_\beta$ is smooth on their domain

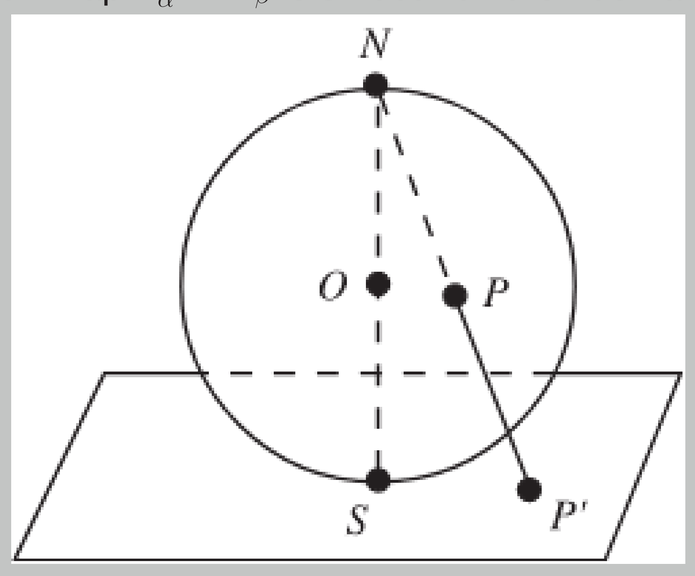


Figure 1:The stereographic projection of a sphere, which is a parametrization of a sphere except at the north pole. The sphere is an example of a 2-dimensional smooth manifold

- Given a smooth n-dimensional manifold M and a local parametrization $F : U \to M$, the *tangent space* at p is defined as $T_pM = span\{\frac{\partial}{\partial u_1}(p), ..., \frac{\partial}{\partial u_n}(p)\}$, with each $\frac{\partial}{\partial u_i}$ being the differential operator with respect to $F(u_1, ..., u_n)$ at p
- For a vector space V, define its *dual space* $V^* = \{T | T : V \to \mathbb{R}\}$
  - Moreover, V^* is a vector space itself. Given a basis of V as $\{e_1, ..., e_n\}$, a basis of V^* is $\{e^1, ..., e^n\}$ such that $e^i(e_j) = \delta_{ij}$
  - One can define the *cotangent space* of M at p as $T_p^*M = (T_pM)^*$ and any $v^* \in T_p^*M$ is called a *cotangent vector* of M at p. In the same fashion, one can express $T_p^*M = span\{du^1, ..., du^n\}$ such that $du^i[\frac{\partial}{\partial u_j}(p)] = \delta_{ij}$

Tensor Product and Wedge Product

- For V, W being two vector spaces, $T \in V^*$ and $S \in W^*$, the *tensor product* between T and S is defined as $T \otimes S : V \times W \to \mathbb{R}$ such that $(T \otimes S)(X, Y) = T(X)S(Y)$
- In the same setup, the *wedge product* is defined as $T \wedge S = T \otimes S - S \otimes T$
  - One can see that a wedge product is alternating; $T \wedge S = -S \wedge T$
  - Also noted that $T \wedge T = 0$

Differential Form

- Let M be a smooth manifold. The *smooth differential k-form* w on M is defined as $w : T_pM \times T_pM \times ... \times T_pM$(k times)$\to \mathbb{R}$ such that for any local parametrization $F : U \to M$, $w = \sum_{i_1,...,i_k=1}^n w_{i_1 i_2 ... i_k} du^{i_1} \wedge ... \wedge du^{i_k}$. The $w_{i_1 i_2 ... i_k}$'s are scalar functions locally defined in $F(U)$ and are called the *local components* of w
  - For example, in $\int_a^b f(x)dx$ the $f(x)dx$ is a differential 1-form

Exterior Derivative

- Given a smooth differential k-form w, its *exterior derivative* is defined as

$$dw = \sum_{i_1,...,i_k=1}^{n} dw_{i_1 i_2 ... i_k} \wedge du^{i_1} \wedge ... \wedge du^{i_k}$$
$$= \sum_{i_1,...,i_k=1}^{n} \sum_{j=1}^{n} \frac{\partial w_{i_1 i_2 ... i_k}}{\partial u_j} du^j \wedge du^{i_1} \wedge ... \wedge du^{i_k}$$

- Given smooth differential k-forms w, η on a smooth manifold M and a smooth scalar function f,
  - $d(w + \eta) = dw + d\eta$
  - $d(fw) = df \wedge w + d\eta$
  - $d^2w = d(dw) = 0$
- A connection between a differential form and exterior derivative in $\mathbb{R}^3$ and usual multivariable calculus is shown below:

Differential Form on $\mathbb{R}^3$	**Multivariable Calculus**
$f(x, y, z)$	$f(x, y, z)$
$w = Pdx + Qdy + Rdz$	$F = P\hat{i} + Q\hat{j} + R\hat{k}$
$\beta = Ady \wedge dz + Bdz \wedge dx + Cdx \wedge dy$	$G = A\hat{i} + B\hat{j} + C\hat{k}$
df	∇f
dw	$\nabla \times F$
$d\beta$	$\nabla \cdot G$
$d^2f = 0$	$\nabla \times \nabla f = 0$
$d^2w = 0$	$\nabla \cdot (\nabla \times F) = 0$

Revisit Maxwell's Equations

- The Maxwell's Equations can be written in differential equations as:

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\epsilon_0}$$
$$\nabla \cdot \mathbf{B} = 0$$
$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$$
$$\nabla \times \mathbf{B} = \mu_0 \mathbf{j} + \frac{1}{c^2}\frac{\partial \mathbf{E}}{\partial t}$$

- The first equation is the Gauss's law on electric field, the second equation is a statement that an magnetic monopole does not exist (it has been predicted in several models but not yet verified), the third equation is the law of electromagnetic induction, and the fourth equation is the Ampere's circuit law with Maxwell's correction
- Denote $(t, x, y, z) \in \mathbb{R}^4$ as (x_0, x_1, x_2, x_3) and take w be a k-form on $\mathbb{R}^4$ (here $k = 0, 1, 2, 3$ or 4). Define the *Hodge-star* map from a k-form to (4-k)-form such that $w \wedge *w = dt \wedge dx \wedge dy \wedge dz$, or $-dt \wedge dx \wedge dy \wedge dz$ if w contains a dt term (this is known as the volume form of the Minkowski spacetime)
- Express $\mathbf{E}, \mathbf{B}, \mathbf{J}$ as

$$\mathbf{E} = E_x dx + E_y dy + E_z dz$$
$$\mathbf{B} = B_x dy \wedge dz + B_y dz \wedge dx + B_z dx \wedge dy$$
$$\mathbf{J} = -(J_x dy + J_y dz \wedge dx + J_z dx \wedge dy) \wedge dt + \rho dx \wedge dy \wedge dz$$

Define $\mathbf{F} \equiv \mathbf{B} + \mathbf{E} \wedge dt$. Together with the Hodge-star map, one can rewrite the Maxwell's equations as:

$$d\mathbf{F} = 0$$
$$d(*\mathbf{F}) = \mathbf{J}$$

References

[1] T.H. Fong.
Differentiable Manifolds & Riemannian Geometry.
Hong Kong University of Science and Technology, 7th edition, 2021.

UNIVERSAL APPROXIMATION THEOREM

Xin Wang, Ruifan Wang

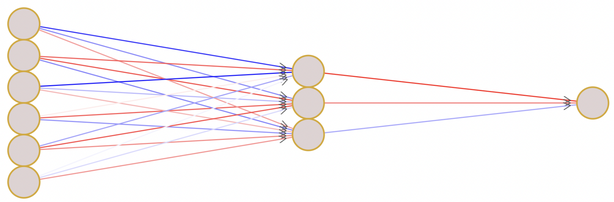
University of California, Santa Barbara

UC SANTA BARBARA

Multiplayer Feedforward Neural Networks

A neural network is the interconnection of unit models characterized by a threshold value θ, a univariate **activation function** $\sigma : R \to R$, and a vector of weights $w = w_1, ..., w_n$. Here, the value of n is determined by the dimension of the input-vector $x = x_1, ..., x_n$. When we feed x into a unit, it computes $\sigma(w \cdot x - \theta)$ and shoots the result to the next unit. A single hidden layer feedward neural network represents a $f : R^n \to R$ function

$$f(x) = \sum_{j=1}^{k} \beta_j \cdot \sigma(w_j \cdot x - \theta_j)$$



Input Layer $\in \mathbb{R}^6$ Hidden Layer $\in \mathbb{R}^3$ Output Layer $\in \mathbb{R}^1$

The most important application of neural networks is in machine learning, where neural networks are "trained" to approximate a function. Thus, a fundamental question for neural networks is whether they can approximate reasonable functions to an arbitrary degree of accuracy. This depends on the activation function σ and is the subject of many papers, including the paper studied for this project.

Nonpolynomial Activation Function

Leshno et al. proved in their paper "Multilayer Feedforward Networks With a Nonpolynomial Activation Function Can Approximate Any Function" [2] that, under modest assumptions, a broad class of activation functions are suitable for building neural networks to approximate continuous functions. We studied this paper to understand the mathematics underlying the result.

Definition (Notion of approximation)**.** We say that a set F of functions in $L^{\infty}_{loc}(R^n)$ is **dense** in $C(R^n)$ if for every function $g \in C(\mathbb{R}^n)$ and for every compact set $K \subset \mathbb{R}^n$, there exists a sequence of functions $f_j \in F$ such that

$$\lim_{j \to \infty} ||g - f_j||_{L^{\infty}(K)} = 0$$

Colloquially, $\{f_j\}$ approximates g "arbitrarily well."

Definition. The **admissible class of activation functions** which Leshno et al. denote by M is the set of locally bounded functions with a "small" number of discontinuities: if $\sigma \in M$ and K is the collection of discontinuities of σ, then $\overline{K}$ has zero Lebesgue measure.

Neural networks arise from the collection,

$$\Sigma_n = \text{span}\{\sigma(w \cdot x + \theta) : w \in \mathbb{R}^n, \theta \in \mathbb{R}\}$$

and the main result of the paper is that Σ_n is dense in $C(\mathbb{R}^n)$ if and only if σ is not an **algebraic polynomial**. This is a novel conclusion since the condition is very simple.

Reduced Case

There are two directions to prove, one of which is not difficult: *Σ_n is dense in $C(\mathbb{R}^n)$, then σ is not a polynomial.* The rest of the proof aims to show that if σ is not a polynomial, then Σ_n is dense in $C(\mathbb{R}^n)$. The proof relies on some analysis tricks, which we summarize here. Some common techniques to prove results like this are,

- Reduce the dimension of the space(s) considered.
- Prove the result for well-behaved functions first.
- Use a "smoothing" technique to deal with functions lacking regularity.

The complexity of the problem is reduced by showing first that if $\overline{\Sigma_1} = C(\mathbb{R})$, then $\overline{\Sigma_n} = C(\mathbb{R}^n)$. Then, Leshno et al. prove $\overline{\Sigma_1} = C(\mathbb{R})$ in the case that $\sigma \in C^{\infty}$.

To show $\overline{\Sigma_1} = C(\mathbb{R})$ when $\sigma \in C^{\infty}$, Leshno et al. show that $\overline{\Sigma_1}$ contains all polynomials. The result follows then as a consequence of Weierstrass's Theorem:

Theorem (Weierstrass's Theorem[3])**.** *If f is a continuous function on a compact set K, there exists a sequence of polynomials P_n such that*

$$\lim_{n \to \infty} P_n(x) = f(x)$$

uniformly on K.

It follows that $\overline{\Sigma_1}$ contains $C(K)$, where all $K \subset \mathbb{R}$. Hence, Σ_1 is dense in $C(\mathbb{R})$.

Generalized Case

From above steps, the "dense" argument can be easily achieved when σ is smooth. In this section, the author generalizes the problem to the entire class of admissible activation function by considering σ that is not smooth. The purpose of **convolution** $\sigma * \varphi$ is to deal with the *discontinuities* and points where σ *is not differentiable*. In a way, the convolution can overcome the limited differentiability of σ. We will discuss the merit of convolution in the next section.

By convolving σ with functions $\varphi \in C_0^{\infty}$, the general case follows as a consequence of the work for the reduced case: $\overline{\Sigma_1}$ is dense in $C(\mathbb{R})$ so long as $\sigma * \varphi$ is not a polynomial for some test function φ. The authors deal with this caveat using advanced techniques.

Basically, Leshno et al. must knows what is the condition that makes $\sigma * \varphi$ a polynomial for every test function φ. It turns out that this only occurs if σ is a polynomial almost everywhere, which rules out any strange conditions where $\sigma * \varphi$ is a polynomial for some $\varphi \in C_0^{\infty}$, yet σ is not a polynomial. Their key argument is to show that if $\sigma * \varphi$ is a polynomial for every test function φ, then the degree of $\sigma * \varphi$ is bounded by some m for every φ. From here, they conclude that since $\sigma * \varphi$ is a polynomial of degree at most m for every test function φ, andσ itself must be (almost everywhere) a polynomial of degree at most m.

Convolution Applied to a Specific Example

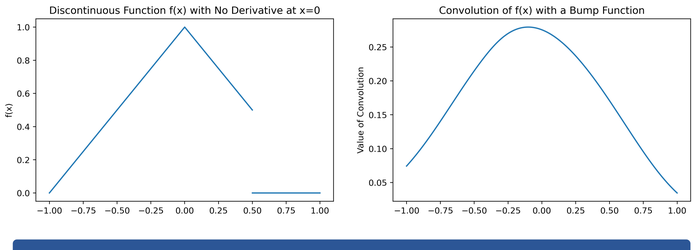
To illustrate the utility of the convolution, let $f(x) := 1 - |x|$ when $-1 \leq x \leq 1/2$ and 0 otherwise. Let $g(x)$ be a bump function, where $g(x) = e^{-1/(1-x^2)}$ for $|x| \leq 1$ and 0 otherwise. The convolution: $(f * g)(x)$, is defined as,

$$(f * g)(x) = \int_{-\infty}^{\infty} f(x - y)g(y)dy = \int_{-\infty}^{\infty} f(y)g(x - y)dy$$

The equality of the integrals above follows by a change of variables. Since f and g are supported on a compact set, we will write the convolution as,

$$(f * g)(x) = \int_{-1}^{1/2} (1 - |y|)e^{-1/(1-(x-y)^2)}dy$$

Then, we may use a numerical integrator to evaluate the convolution.
Here is a visual comparison between the discontinuous function $f(x)$ and the convolution of $f(x)$ with $g(x)$.



Remarks

In 1991, Hornik showed that the multilayer feed-ward architecture gives neural networks the potential of being universal approximators[1]. Leshno et al. led the study to a new dimension and discovered that a neural network does not need a continuous activation function to approximate some real-world functions in an arbitrary accuracy. This endows the neural network a biological interpretation because a real neuron is unlikely to have a continuous activation function. Later in the history, mathematicians extends the **Universal Approximation Theorem** by studying discontinuous functions, noncompact domains, and so on.

Acknowledgement

We especially appreciate our mentor Zach Wagner for enlightenment and two quarters of patient teaching for this project. We also thank every member contributed to the Directed Reading Program.

References

[1] Kurt Hornik. "Approximation capabilities of multilayer feedforward networks". In: *Neural Networks* 4.2 (1991), pp. 251–257.

[2] Moshe Leshno et al. "Multilayer feedforward networks with a nonpolynomial activation function can approximate any function". In: *Neural Networks* 6.6 (1993), pp. 861–867.

[3] Walter Rudin. *Principle of Mathematical Analysis*. McGraw-Hill, Inc., 1964, p. 159.

An Introduction to Cryptography

Lainey Watlington

University of California - Santa Barbara

The Beginnings of Cryptography

Cryptography is the study of methods of sending messages in a disguised form so that only the intended recipients can remove the disguise and read the message.

At the most basic level, a **cryptosystem** is the process of converting plaintext to a cyphertext using encryption and subsequently converting that cyphertext back to plaintext using decryption.

One of the earliest cryptosystems was created using **digraphs**, which map two characters in a message to a number. Let us consider the 27 letter alphabet which contains letters A-Z and a blank. Then, given any message, the following digraph can be used as an enciphering function where x and y are two characters which occur in succession in the message:

$$27x + y = C$$

The deciphering function is given by:

$$\begin{cases} C \mod 27 = x \\ C - x = y \end{cases}$$

Most early cryptosystems were based on a similar idea of using a rule, or a **key**, to shift the letters in a message to a different location. The idea was that only the person with the key would be able to decipher the message.

Breaking a Cryptosystem

Cryptosystems were developed in order to help protect sensitive information. In modern times, cryptography is widely used in the field of cybersecurity to protect people's

- passwords
- credit card information
- identity information
- other sensitive forms of data

In an increasingly digital world, cryptosystems have become extremely important in protecting this information.

Cryptanalysis is the science of "breaking" the code of cryptosystems. People do this in order to gain access to data that is not intended for them. This begs the question, "How does one break a cryptosystem?". To do so, one needs two types of information

1. The general nature, or the **structure** of the system
2. The specific choice of certain parameters connected with the given cryptosystem, like the shift parameter, also known as the **enciphering key**

An Example in Python

Let us extend the idea of a digraph to a cryptosystem which enciphers a message of length n from an alphabet of any size. Let N represent the size of the alphabet. Then, the enciphering function will be represented by

$$N^{n-1}x_1 + N^{n-2}x_2 + \cdots + Nx_{n-1} + x_{n-1} = C$$

The Python code for an enciphering transformation of this form is as follows:

```
def ngraph(base, message):
    message = str(message)
    length = len(message)
    sum = 0
    n = 1
    while (length-n) >= 0:
        sum = sum + (base**(n-1))*letternumber(message[length-n])
        n = n + 1
    return(sum)
```

The deciphering transformation will subtract $C \mod N$ from C n times and update C after each iteration. The Python code for a deciphering transformation of this form is:

```
def decipherngraph(base, number):
    n = 0
    string = ""
    if number == 0:
        string = "a"
    while number > 0:
        x = number%27
        number = int((number-x)/27)
        print(number)
        string = numberletter(x) + string

    return(string)
```

Primality and Factorization

Cryptosystems have evolved over time to prevent people from breaking them.

- The easier it is to guess the enciphering key of a cryptosystem, the easier it is to break the cryptosystem.
- So, methods of creating difficult to guess keys were developed

Public Key Cryptography: the enciphering and deciphering algorithms are publicly known, but the enciphering and deciphering keys are concealed. Gaining access to the keys allows you to break the system.

How do we create difficult to guess keys?

- **Factoring primes** is really difficult once we start dealing with very large numbers. So, if we multiply two large primes together, factoring them becomes almost impossible without having access to a key.
- The **discrete logarithm** problem is an idea based on the fact that if we know $y = b^x$, it is extremely difficult to solve for

$$x = \log_b y$$

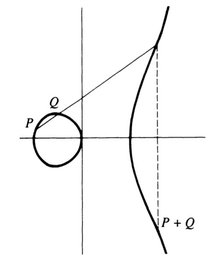
Fermat Factorization provides a way of "breaking" some public key cryptosystems. If two primes are close enough together, this algorithm allows one to efficiently calculate the two primes that have been multiplied together. This form of factorization is used to break RSA cryptosystems.

The Foundations of Modern Cryptography: Elliptic Curves

Elliptic Curve Cryptography

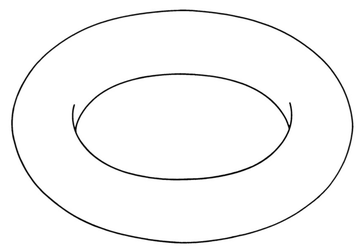
- An approach to public key cryptography which utilizes elliptic curves over finite fields to create keys.
- It is essentially impossible to find the discrete logarithm of a random element of an elliptic curve with respect to a publicly known base point.
- The larger the elliptic curve, the more secure the cryptosystem is since the discrete logarithm becomes more difficult to compute.

An Elliptic Curve Over the Real Numbers



- Elliptic curves over the reals form an abelian group. Thus, if we perform operations on two elements of the curve, we will end up with another element on the curve.

An Elliptic Curve Over the Complex Numbers



- Elliptic curves over the complex numbers form a torus.
- We can think of plotting elements of the curve over the integer lattice and then connecting all of the edges together.

Acknowledgements

Reference Material: "A Course in Number Theory and Cryptography" by Neal Koblitz

Thank you to the UCSB Directed Reading Program and to my mentor Katherine Merkl for making this project possible.

Isoperimetric Inequalities

Tyler Guo Mentor: Malik Tuerkoen

2022 Mathematics Directed Reading Program. University of California-Santa Barbara

Introduction

The classical isoperimetric problem is stated as follows: Among all closed curves in the plane of fixed perimeter, which curve (if any) maximizes the area of its enclosed region? This is equivalent to the problem: Among all closed curves in the plane enclosing a fixed area, which curve (if any) minimizes the perimeter? The problem can be extended to regions and surfaces in $\mathbb{R}^n$. In this poster, we show that a sphere has the smallest surface area with given volume by developing certain isoperimetric inequalities relating to the $\mathcal{L}^n$ measure of a sets and its perimeter.

Definitions

(1) For a function $u \in L^1(\Omega, \mathbb{R})$, we define

$$\mathrm{Var}(u, \Omega) := \sup\{\int_\Omega u \operatorname{div} \varphi \, dx : \varphi \in C_c^1(\Omega, \mathbb{R}^N), \|\varphi\|_\infty \le 1\}.$$

We say u has bounded variation in Ω if $\mathrm{Var}(u, \Omega) < \infty$.
Moreover, we let $BV(\Omega)$ denote the space of functions $u \in L^1(\Omega)$ which have bounded variation in Ω.
We also set

$$BV_{\mathrm{loc}}(\Omega) := \{u \in L^1_{\mathrm{loc}}(\Omega) : \mathrm{Var}(u, \Omega') < \infty \text{ for every } \Omega' \subset\subset \Omega\}.$$

(2) For a Lebesgue measurable subset E of $\mathbb{R}^N$. The perimeter of E in Ω is defined by

$$P(E, \Omega) := \mathrm{Var}(1_E, \Omega).$$

We say E has finite perimeter in Ω if $1_E \in BV(\Omega)$; E has locally finite perimeter in Ω if $1_E \in BV_{\mathrm{loc}}(\Omega)$.

Examples

(1) The distribution function

$$F_\mu : \mathbb{R} \to \mathbb{R}, \quad F_\mu(t) = \mu((-\infty, t])$$

of a probability measure μ on $\mathcal{B}(\mathbb{R})$ is a function of bounded variation in $\mathbb{R}$.

(2) Suppose $\Omega \subset \mathbb{R}^N$ is bounded and $u \in C^1(\overline{\Omega})$. Then $u \in BV(\Omega)$ and

$$\mathrm{Var}(u, \Omega) = \int_\Omega |\nabla u| \, dx.$$

(3) Let $Q_N := [0, 1]^N \subset \mathbb{R}^N$. Then Q has finite perimeter in $\mathbb{R}^N$ given by

$$P(Q_N) = 2N.$$

(4) Let $E \subset \mathbb{R}^N$ be a bounded open set with C^1-boundary. Then E has locally finite perimeter in Ω given by

$$P(E, \Omega) = \mathrm{vol}_{N-1}(\partial E \cap \Omega).$$

Gagliardo's Lemma

Let $N \ge 2$. For $x \in \mathbb{R}^N$, $j = 1, \dots, N$ let $\hat{x_j} := (x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_N)$. Moreover, let $f_1, \dots, f_N \in L^{N-1}(\mathbb{R}^{N-1})$ be given, and let $f : \mathbb{R}^N \to \mathbb{R}$ be defined by $f(x) = f_1(\hat{x_1}) \cdots f_N(\hat{x_N})$. Then

$$f \in L^1(\mathbb{R}^N) \text{ and } \|f\|_{L^1(\mathbb{R}^N)} \le \prod_{j=1}^N \|f_j\|_{L^{N-1}(\mathbb{R}^{N-1})}.$$

Non-optimal Isoperimetric Inequality

Let $N \ge 2$. Then we have

$$P(E) \ge 2\sqrt{N}|E|^{\frac{N-1}{N}}$$

for all measurable subsets $E \subset \mathbb{R}^N$ with $|E| < \infty$.

Proof of the theorem

The inequality holds trivially if $P(E) = \infty$. Suppose $P(E) < \infty$. We claim that for $u \in BV(\mathbb{R}^N)$, $N \ge 2$, we have

$$\|u\|_{L^{\frac{N}{N-1}}(\mathbb{R}^N)} \le \frac{1}{2\sqrt{N}} \mathrm{Var}(u, \mathbb{R}^N).$$

We obtain the inequality by applying this result to the function 1_E.
Proof of Claim: By standard approximation arguments, one can show that there exists a sequence (u_n) such that $u_n \in BV(\mathbb{R}^N) \cap C_c^1(\mathbb{R}^N)$ satisfying

$$\|u - u_n\|_1 \to 0, \quad \mathrm{Var}(u_n, \mathbb{R}^N) \to \mathrm{Var}(u, \mathbb{R}^N).$$

Hence it suffices to consider $u \in C_c^1(\mathbb{R}^N)$. Integration parallel to the j-th coordinate axis yields

$$|u(x)| \le \frac{1}{2} \int_{\mathbb{R}} |\partial_j u(x_1, \dots, x_{j-1}, t, x_{j+1}, \dots, x_N)| \, dt := v_j(\hat{x}_j)$$

for $x \in \mathbb{R}^N$, $j = 1, \dots, N$.

We then apply the Gagliardo's Lemma to $v_j^{\frac{1}{N-1}} \in L^{N-1}(\mathbb{R}^{N-1})$ and obtain

$$\int_{\mathbb{R}^N} |u(x)|^{\frac{N}{N-1}} dx \le \int_{\mathbb{R}^N} \prod_{j=1}^N v_j^{\frac{1}{N-1}}(\hat{x}_j) \, dx \le \prod_{j=1}^N \left\| v_j^{\frac{1}{N-1}} \right\|_{L^{N-1}(\mathbb{R}^{N-1})} = (\prod_{j=1}^N \|v_j\|_{L^1(\mathbb{R}^{N-1})})^{\frac{1}{N-1}}$$

$$\le (\frac{1}{N} \sum_{j=1}^N \|v_j\|_{L^1(\mathbb{R}^{N-1})})^{\frac{N}{N-1}} = (\frac{1}{2N} \int_{\mathbb{R}^N} [\sum_{j=1}^N |\partial_j u(x)|] \, dx)^{\frac{N}{N-1}} \le (\frac{1}{2\sqrt{N}} \int_{\mathbb{R}^N} |\nabla u| \, dx)^{\frac{N}{N-1}}.$$

□

Optimal Isoperimetric Inequality

For any measurable subset $E \subset \mathbb{R}^N$ with $|E| < \infty$ we have

$$P(E) \ge N\omega_N^{\frac{1}{N}} |E|^{\frac{N-1}{N}},$$

where ω_N denotes the volume of the unit ball in $\mathbb{R}^N$, and the equality occurs if and only if E is a ball.

Proof of the theorem

Suppose $P(E) < \infty$, we have $1_E \in BV(\mathbb{R}^N)$. Let $E^* = B_r(0)$, where r is chosen such that $|E| = |E^*|$. Then one can show there exists a sequence of sets (E_n) with $P(E_n) \le P(E)$ and $\|1_{E_n} - 1_{E^*}\|_1 \to 0$. By lower semicontinuity,

$$P(E^*) \le \liminf_{n\to\infty} P(E_n) = \liminf_{n\to\infty} \mathrm{Var}(1_{E_n}, \mathbb{R}^N) \le \mathrm{Var}(1_E, \mathbb{R}^N) = P(E).$$

Moreover,

$$P(E^*) = \mathrm{vol}_{N-1}(\partial E^*) = N\omega_N r^{N-1} = N\omega_N^{\frac{1}{N}} |E^*|^{\frac{N-1}{N}} = N\omega_N^{\frac{1}{N}} |E|^{\frac{N-1}{N}}.$$

□

Coarea Formula for BV functions

Let $f \in BV(\Omega)$ be a nonnegative function, and put

$$E_t := \{x \in \Omega : f(x) > t\} \quad \text{for } t \ge 0.$$

Then

$$\mathrm{Var}(f, \Omega) = \int_0^\infty P(E_t, \Omega) \, dt.$$

Optimal Functional Isoperimetric Inequality

For $f \in BV(\mathbb{R}^N)$ we have

$$\mathrm{Var}(f, \mathbb{R}^N) \ge N\omega_N^{\frac{1}{N}} \|f\|_{L^{\frac{N}{N-1}}}.$$

Proof of the theorem

Since

$$\|f\|_{L^{\frac{N}{N-1}}} \le \|f^+\|_{L^{\frac{N}{N-1}}} + \|f^-\|_{L^{\frac{N}{N-1}}},$$

and one can show that for $f \in BV(\mathbb{R}^N)$,

$$\mathrm{Var}(f, \mathbb{R}^N) = \mathrm{Var}(f^+, \mathbb{R}) + \mathrm{Var}(f^-, \mathbb{R}).$$

Hence it suffice to consider the case where f is nonnegative. In this case, the Coarea formula and the isoperimetric inequality yields

$$\mathrm{Var}(f, \mathbb{R}^N) = \int_0^\infty P(E_t) \, dt \ge N\omega_N^{\frac{1}{N}} \int_0^\infty |E_t|^{\frac{N-1}{N}} \, dt.$$

We now define

$$\chi : [0, \infty) \to \mathbb{R}, \quad \chi(t) = \|\min\{f, t\}\|_{L^{\frac{N}{N-1}}}.$$

Then χ is continuous, nondecreasing and hence a.e. differentiable. Moreover, for $t, h > 0$, we have

$$0 \le \chi(t + h) - \chi(t) \le \|\min\{f, t + h\} - \min\{f, t\}\|_{L^{\frac{N}{N-1}}} \le \|1_{E_t} h\|_{L^{\frac{N}{N-1}}} = h|E_t|^{\frac{N-1}{N}},$$

which implies that χ is locally Lipschitz continuous on $(0, \infty)$ with $\chi'(t) \le |E_t|^{\frac{N-1}{N}}$ for a.e. $t > 0$. Hence χ satisfies the assumptions of the Fundamental theorem of calculus . Since $0 = \chi(0) = \lim_{t\to 0^+} \chi(t)$, it follows that

$$\|f\|_{L^{\frac{N}{N-1}}} = \lim_{b\to\infty} [\chi(b) - \chi(\frac{1}{b})] = \lim_{b\to\infty} \int_{\frac{1}{b}}^b \chi'(t) \, dt \le \int_0^\infty |E_t|^{\frac{N-1}{N}} \, dt.$$

□

Acknowledgements

I would like to thank my mentor Malik Tuerkoen for his guidance and insight. I would also like to thank the organizers of the UCSB Directed Reading Program for this wonderful opportunity.

References

[1] Lawrence Craig Evans and Ronald F Gariepy. *Measure Theory and Fine Properties of Functions, Revised Edition*. CRC Press LLC, Oakville, 2015.