[DOT$^+$23]

Doing Math with Computers for Fun and Profit

Anakin

Hi, I'm Ryan!

- Junior in CS, on a mission to take all the CS theory courses
- I also do web dev :(
- Interests: randomized and streaming algorithms, (some) systems
- Will be presenting later this semester!

Section 1

REU

What is an REU?

- Research Experience for Undergraduates
- Get paid to do research in Math, CS, Engineering, Science, etc., over the summer
- See how other schools do things, meet new people
- Maybe even get a paper out of it!

How do I find them?

Save these slides for later!

- NSF List
- Math Programs
- This spreadsheet

How do I apply to them?

- Personal Statement
- 2 Letters of Rec
- Resume / CV
- Most deadlines are early – mid March
  - Start drafting in Winter Break

Tips & Tricks

- Most are government funded which means usually US citizens get funding.
  - It is possible for non-US citizens to get funding in some special cases.
- Get your letter writers to read your personal statement.
- There are other options outside of REUs (MSR, TTIC, EPFL, ETH Zürich, Max Planck, SCAMP, Independent Study, etc).
- Most people don't apply to enough REUs.

Any other questions?

Questions?

Section 2

Introduction to Group Theory

Groups and Group Actions

- A *group* is an object in the category of groups
- A *group action* is a functor from a 1-groupoid to the category of sets

What is a Group?

Groups are one of the most ubiquitous objects in all of math. They generalize structures with some sort of addition/multiplication.

Definition

A *group* is a set G with an operation $\_ \cdot \_ : G \times G \to G$ such that

- $\cdot$ is associative: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- There exists an identity e such that $g \cdot e = g = e \cdot g$
- Every element g has an inverse g^{-1} such that $g \cdot g^{-1} = e = g^{-1} \cdot g$

We will usually just write $x \cdot y$ as xy

Important Examples of Groups

Consider the set S_n of bijections $\sigma\colon [n] \to [n]$ where $[n] = \{ 1, \ldots, n \}$.
This forms a group with "multiplication" using composition

- Composing bijections with each other yields a bijection
- Identity: $\mathrm{id}(i) = i$ for all $1 \leq i \leq n$
- Inverses: σ has an inverse σ such that $\sigma \circ \sigma^{-1} = \mathrm{id}$

Important Examples of Groups

Recall that the integers mod p are $\mathbb{Z}_p = \{1, 2, \ldots, p\}$ with addition and multiplication done modulo p. Consider the set $\mathrm{GL}(n, p)$ of all $n \times n$ matrices with entries in $\mathbb{Z}_p$ with non-zero determinant. This forms a group with matrix multiplication

- Multiplying two matrices with non-zero determinant yields a matrix with non-zero determinant since $\det(AB) = \det(A) \cdot \det(B)$
- Identity: I_n with 1s on the diagonal and 0s elsewhere
- Inverses: Matrices have an inverse if and only if they have non-zero determinant, so each A has an inverse A^{-1} such that $A \times A^{-1} = I_n$

If you've taken Linear Algebra, these are just invertible linear transformations!

Group Isomorphism

Consider the following two groups:

$$G = \left\{ \mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \subseteq S_3$$

$$\mathbb{Z}_3 = \{ \qquad 0, \qquad 1, \qquad 2 \qquad \}$$

So G are some permutations with the operation of composition and $\mathbb{Z}_3$ are integers modulo 3 where the operation is addition but we keep the remainder after division by 3. So $2 + 2 \equiv 1 \pmod 3$.

Question: In what sense are these two groups the same group?

Answer: Mapping $\mathrm{id} \mapsto 0$, $\sigma \mapsto 1$, $\sigma^2 \mapsto 2$ preserve operations!

Notice that $\sigma \circ \sigma = \sigma^2$ and $1 + 1 \equiv 2 \pmod 3$.

Similarly, $\sigma \circ \sigma \circ \sigma = \mathrm{id}$ and $1 + 1 + 1 \equiv 0 \pmod 3$.

Group Actions

We want to study how a group G interacts with other sets. Let Ω be some set.

Definition

Then a *group action* is an operation $\_ \cdot \_ : G \times \Omega \to \Omega$ such that

- $e \cdot x = x$, for all $x \in \Omega$
- $g \cdot (h \cdot x) = (gh) \cdot x$, for all $g, h \in G$, and for all $x \in \Omega$

We write $G \curvearrowright \Omega$.

To prevent confusion with the group operation in G, we will keep the $\cdot$ when talking about actions.

Important Examples of Group Actions

Let $G = S_n$ and $\Omega = [n]$.

- Say $\sigma\colon [n] \to [n] \in S_n$ and $i \in [n]$. What would be a good choice of action $\sigma \cdot i$?
- $\sigma \cdot i \coloneqq \sigma(i)$

Now let G be a group of invertible linear transformations from a vector space $V \to V$.

- Say $T\colon V \to V \in G$ and $v \in V$. What would be a good choice of action $T \cdot v$?
- $T \cdot v \coloneqq T(v)$

Orbits and Stabilizers

We want to study the structure of $G \curvearrowright \Omega$.

Definition
The *orbit* of $\alpha \in \Omega$ is the set $G \cdot \alpha = \{ g \cdot \alpha \mid g \in G \}$

Every element of Ω belongs in some orbit. It turns out the orbits partition Ω.

Definition
The *stabilizer* of $\alpha \in \Omega$ is the set $G_\alpha = \{ g \in G \mid g \cdot \alpha = \alpha \}$

Exercise: Stabilizers are subgroups of G

Example

$$G = \left\{ \mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \right\} \subseteq S_4$$

This is the same group as before, but now 4 is a valid input and we don't do anything to it. Exercise: Check that this is a subgroup of S_4.

Consider $G \curvearrowright [4]$.

- $G \cdot 1 = \{ 1, 2, 3 \}$
- $G \cdot 4 = \{ 4 \}$
- $G_1 = \{ \mathrm{id} \}$
- $G_4 = G$

Group Classification

The *Group Classification Problem* is the problem of identifying groups satisfying some property "up to" isomorphism.

- This is one of the hardest problems in all of group theory.
- Even checking if two finite groups are isomorphic is difficult for computer.
- The classification of the finite simple groups took tens of thousands of pages written by over 100 authors between 1955 and 2004.

Rank

- Let G be some group of permutations in S_n and consider $G \curvearrowright [n]$ such that G only has one orbit.
- Let G_0 be the stabilizer of some element of $[n]$. It turns out it doesn't matter which one.

Definition

The *rank* of G is the number of orbits of $G_0 \curvearrowright [n]$.

This is a sort of measurement of the "reach" of stabilizer subgroups of G.

Section 3

Groups, Algorithms, and Programming

Structure

- Let G be some group of permutations in S_n and consider $G \curvearrowright [n]$ such that G only has one orbit.
- Let G_0 be the stabilizer of some element of Ω.
- Result 1: This is the same as considering $G_0 \curvearrowright V$ where G_0 is now a group of linear transformations and V is a vector space $\mathbb{F}_p^k$.
- $\#$ Orbits of $G_0 \curvearrowright [n] = \#$ Orbits of $G_0 \curvearrowright \mathbb{F}_p^k$.
- Result 2: G_0 must contain a certain subgroup E of order q^{2m+1}.

Making Change using Group Theory

So now we can consider $G_0 \curvearrowright \mathbb{F}_p^k$ and $E \subseteq G_0$ where $|E| = q^{2m+1}$. This gives us a nice set of parameters.

1. We find a value $B(p, k, q, m)$ such that $|G_0|$ divides B
2. A theorem in group theory tells us that the size of orbits of G_0 divides $|G_0|$, so they divide B
   - Let $d_1, \ldots, d_t$ be the divisors of B
3. We know there is one orbit of size 1 and the sizes of the other orbits must sum up to $p^k - 1$

Result 3: We can get a lower bound on rank by solving the *Change Making Problem* with coins $d_1, \ldots, d_t$ and target value $p^k - 1$.

Making Change using Group Theory

In the *Change-making Problem*, we are given coins from some set of denominations $d_1, \ldots, d_t$ and a target value T, we want to "make change" for T using as few coins as possible

- We have a fixed set of possible sizes of orbits and a target value $p^k - 1$
- We know the orbits partition this target value
- A worst case lower bound is the most efficient packing as possible
- Thus we want to solve the Change Making Problem with coins $d_1, \ldots, d_t$ and target value $p^k - 1$.

Inductively Making Change

Let *coins* $= [d_1, \ldots, d_n]$ be a sorted list of denominations of coins. Let $\textsc{NumCoins}(i, c)$ be the smallest possible number coins of denomination $[d_1, \ldots, d_c]$ needed make change for i

- If *coins* $= [1, 3, 5, 7]$ then $\textsc{NumCoins}(10, 1) = 10$ but $\textsc{NumCoins}(10, 4) = 2$

Inductively Making Change

Let $coins = [d_1, \ldots, d_n]$ be a sorted list of denominations of coins. Let $\textsc{NumCoins}(i, c)$ be the smallest possible number coins of denomination $[d_1, \ldots, d_c]$ needed make change for i.

$\textsc{NumCoins}(i, c) =$

$$\begin{cases} \infty & c = 0 \\ \textsc{NumCoins}(i, c-1) & i < coins[c] \\ 1 & i = coins[c] \\ \min\{\, \textsc{NumCoins}(i, c-1), 1 + \textsc{NumCoins}(i - coins[c], c) \,\} & \text{otherwise} \end{cases}$$

A (very high level) Overview of the Whole Paper

1. Define the parameters p, k, q, m
2. Do a bunch of pure math to get finite bounds on these parameters
3. Enumerate all possible sets of parameters and keep the ones that have a lower bound ≤ 6

A (very high level) Overview of the Whole Paper

For each set of valid parameters p, k, q, m. Let $N =$ the largest possible N such that $N \curvearrowright \mathbb{F}_p^k$

1. Check if the subgroup E with $|E| = q^{2m+1}$ is contained in N (HARD!)
2. Check if N has rank ≤ 6
3. Enumerate all possible subgroups of N (HARD!)
4. Repeat for each subgroup

How?

- All of this was done in a programming language called GAP: Groups, Algorithms, and Programming
- GAP is just one of many computational algebra systems
  - SageMath (Built on top of Python
  - Mathmatica
  - Magma (popular in Cryptography)
  - Macauley2 (Created at UIUC!)
- Hard computations were done on AWS.
- These techniques extend to higher ranks but computational resources are a large issue.

More Details?

- Check out the paper (linked on my website anakin-dey.com)
- Come to the Undergraduate Math Seminar (details coming soon)
- Ask me in the Discord!

Questions?

Algebra is the offer made by the devil to the mathematician...All you need to do, is give me your soul: give up geometry

— Michael Atiyah (1979)

Bibliography

Anakin Dey, Kolton O'Neal, Duc Van Khanh Tran, Camron Upshur, and Yong Yang.

Classifying primitive solvable permutation groups of rank 5 and 6, 2023.