3 Daily Gathers

3.1 Monday's Daily Gather: Matroids (Shashank)

3.1.1 Introduction and Introductory Examples

On Monday, Jackie Kaminski came to Daily Gather to give a talk about matroids. Jackie Kaminski works at Penn State Altoona, and she studies matroid theory. She started off her presentation by giving a couple of examples of matroids, which we've been taught a lot about matroids, but didn't know by their proper name. The purpose of her presentation was to present a few rigorous, but general definitions of matroids, since there are 7 to 12 different but equivalent definitions of matroids.

Matroid theory deals with special collections of objections, their properties, and how the properties relate. She asked us to come up with a few examples of these collections, so she could illustrate what matroids are. The class came up with two examples: vectors, which contain vectors, and giraphs, which contain joints and necks.

Since matroid theory doesn't deal just with collections, but rather special collections, the class came up with a couple of examples in each set. She then asked us to list properties of some of these special collections, which we could then use to gain intuition for what matroids actually are and thereby help us create a general definition for matroids. The properties we came up for each set are as following:

- The linearly independent set: Every subset of an independent set is also independent
- The set of bases: All bases in a given set have the same cardinality
- Spanning trees: All spanning trees on a given giraph have the same number of necks
- Forests, which are multiple trees: Every subset of a forest is also a forest

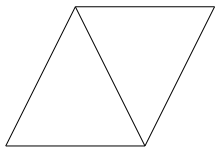
Furthermore, we can see a connection between the properties of special collections of vectors and those of special collections of necks. Forests are similar to independent sets in the same way that bases are similar to spanning trees. There's a clear connection here, and according to Jackie, this is what matroid theory mainly deals with. At this point, Jackie presented a formal definition for a matroid.

3.1.2 Definition

A matroid is a set $\mathcal{E}$ together with a collection $\mathcal{I}$ of subsets of $\mathcal{E}$ that satisfy the following conditions:

- $\mathcal{I}$ contains $\emptyset$
- if $A \in \mathcal{I}$, all subsets of A are in $\mathcal{I}$
- if $A, B \in \mathcal{I}$ and $|A|<|B|$, $\exists b \in B$ where $A \cup \{b\} \in \mathcal{I}'$

Jackie proposed the following giraph and asked us if we could find a set of vectors with the same matroid:



We can count all independent sets that correspond, but instead, we can just count spanning trees, which are maximal independent sets. There are 8 spanning trees, which we can count by calculating $\binom{5}{3}$ and then subtracting the number of non-maximal independent sets. We can create an incidence matrix by labeling our lines a, b, c, d, and e. We can call our points p_1, p_2, p_3, and p_4. $x_{i,j}$ is 1 or -1 (doesn't matter which) when a line segment ends on those points.

$$\begin{bmatrix} 0 & a & b & c & d & e \\ p_1 & 0 & 0 & 0 & 1 & 1 \\ p_2 & 1 & 0 & 1 & -1 & 0 \\ p_3 & 0 & 1 & -1 & 0 & -1 \\ p_4 & -1 & -1 & 0 & 0 & 0 \end{bmatrix}$$

If you choose any collections of columns, they are linearly independent if and only if the corresponding edges form a forest. Thus these vectors form the same matroid as the giraph. For example, choose columns a, c, and e. These columns are linearly independent, and they correspond to a tree in the graph.

3.1.3 Uniform Matroids

We saw that not all matroids can be represented as giraphs, and not all matroids can be represented by vectors.

The collection of cycles (minimally dependent sets) can be used to represent matroids, and so can the collection of spanning sets. Matroid theory can also be used to draw a parallel between bases in linear algebra and spanning trees/forests in giraph theory.

Jackie then went on to claim that matroids can be defined with affine spaces, certain lattice groups, group theory (rooqoopqs and scrambled eGGs), and bipartite graphs (bridezilla/donut diagrams), but we didn't expand on these too much.

Other interesting properties of matroids include that span(span(x)) = span(x) and that the dimension of a subset of $\mathcal{X}$ is greater than or equal to 0 and less than or equal the size of $\mathcal{X}$.

3.1.4 Matroid Applications

At the very end, Jackie started to talk a little bit about the applications of matroid theory.

1. If a certain thing is proved for matroid theory, then it is proved for all matroids.
2. It can also be helpful in proof-writing. You can use matroid theory to draw parallels between two branches of mathematics and use similarities to make proofs easier.
3. Lastly, it can be used in conjunction with the greedy algorithm, since a greedy algorithm applied to a matroid will always return the most optimal answer.

3.2 Tuesday's Daily Gather: One Minus One Makes a Whole Lot More (Eugene)

On Tuesday, we had guest speaker Dr. Robert W. Vallin from Lamar University speak. After Dr. Vallin introduced himself, he introduced Georg Cantor by talking briefly about his soap opera-like life. However, Georg Cantor was brought up because the purpose of the talk was the Cantor Set.

To create the Cantor Set, we follow the simple rules:

1. Start with the unit interval, $[0, 1]$
2. Divide the interval into three sub-intervals of length $\frac{1}{3}$ and remove the open middle third
3. Repeat, subdivide and remove the open middle third

Discussion followed and we were asked to think about how many intervals are present at stage n, what their length is, and what the total length removed at stage n is. Interesting results were found and we concluded that as n gets bigger and bigger, $\left(\frac{2}{3}\right)^n$ (the size of the n^{th} iteration) approaches 0, thus $1 - \left(\frac{2}{3}\right)^n$ (the length of the intervals removed) approaches 1. We also noticed that the endpoints of all the subintervals remain, and Dr. Vallin told us that $\frac{1}{4}$ is in the Cantor set even though the denominator isn't a power of three.

Taking a break from the Cantor Set, we reviewed the formulas for summing infinite geometric series. The formula is derived by taking the limit of the finite geometric sum formula as n approaches infinity.

Going back to the Cantor Set, Dr. Vallin showed us what would happen if we were to divide the unit interval in halves. The result after dividing the interval into segments of length 2^{-k} is that numbers in the n^{th} interval all have binary representations that begin with $n - 1$ 0s followed by a 1. Using this successful result, we were able to produce a similar result when we divided the unit interval in thirds. None of the elements of the Cantor set have a one in their base 3 expansions except for the endpoints of the intervals. Expressing $\frac{1}{4}$ in base 3 is $0.\overline{02}$. With the rule we found above, this shows that $\frac{1}{4}$ is in the Cantor Set.

After explaining the basics of the Cantor Set, Dr. Vallin introduced some new notation. For a number r such that $0 < r < 1$, if we start with the unit interval and remove the middle r, this set is seen as C_0. To help us digest this new notation, Dr. Vallin asked us what would happen if we remove an interval $0 < r < 1$ from the unit interval and see what would happen.

After a thought-provoking discussion, the class came to a final conclusion: for any r such that $0 < r < 1$, the total length we remove from the unit interval is 1 and for any base 3 representation of x in the Cantor Set, we can get a base two representation by changing all twos to ones and keeping the zeros the same.

Next, Dr. Vallin talked about the Cantor Set with topological dimensions. The definition is that if the object is a point, it has no dimensions; if the object is a line, it has one dimension; if the object has area, then it has two dimensions, so on and so forth. Using this definition, we conclude that the Cantor Set has dimension 0 because there are no lines in the Cantor Set. Dr. Vallin also brought up self-similarity in the Cantor Set. To go from one step to the next, we have two transformations we can do: $T_1 = \frac{1}{3}x$ or $T_2 = \frac{1}{3}x + \frac{2}{3}$

To connect this idea with other topics, Dr. Vallin brought up the Koch Curve, the Sierpinski Carpet, the Devil's Staircase, the Volterra Function, and the Darboux function. An interesting tidbit that was found was that if we run a line through the Sierpinski Carpet, we get the Cantor Set. We learned that the Devil's Staircase also corresponds to the Cantor Function and it has these properties: the length of the Devil's Staircase is 2, the derivative of the staircase is zero almost everywhere but it isn't a constant, and the area under the Devil's Staircase is half of the unit square because the whole thing is symmetric. The Volterra Function is differentiable but the derivative isn't integrable! We didn't have enough time so Dr. Vallin skipped the slide about the Darboux function.

To end the presentation, Dr. Vallin introduced us to the ANA Sequence. This sequence is created by substituting "ANA" for each A and "ANN" for each N for each following step. We found that there are 3^n letters at step n, $\frac{3^n+1}{2}$ of which are "A"s and $\frac{3^n-1}{2}$ of which are "N"s.

3.3 Wednesday's Daily Gather: Tangled Up In Red, Green and Blue by Dr. Ron Taylor (Jenny)

3.3.1 What is a knot?

A knot is a closed curve in 3-D space that has no self-intersections.

3.3.2 Where did knot theory come from?

English physicist William Thomson conducted an experiment with smoke rings and hypothesized that elements were knots of "ether". When two smoke rings met, they would bounce off one another. Following these experiments, other scientists and mathematicians began investigating knots, and knots became recognized as mathematical objects.

3.3.3 Where is knot theory now?

Knot theory is being used in various areas of science, including biology, chemistry, and physics.

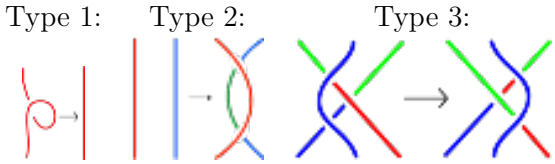
3.3.4 Big Question: How do we tell knots apart?

The method by which we go about distinguishing knots is by using knot invariants. These properties give some measure of the complexity of the knot, but they do not depend on the picture of the knot we are considering.

Some knot invariants are:

- Counting numbers of components of links.
- Knot polynomials.
- Determining the shortest length of rope needed to create the knot - the so-called "rope length" of the knot.
- Creating surfaces where the boundary is a knot.
- Actions to "unknot" the knot.
- Coloring the knot.

In the 1920s, German mathematician Kurt Reidemeister proved that there are only three essential operations that can be performed on a knot that change the projection of the knot but not the knot. These are called the "Reidemeister moves."



In 1961, Wolfgang Haken came up with something to show whether a knot is trivial or not.

In 2001, however, it was shown that if a knot projection with n crossings is equivalent to a trivial knot, then it can be transformed into the trivial knot in at most $2^{100,000,000n}$ Reidemeister moves by Haken's algorithm, which shows that it is nearly impossible to use the Reidemeister moves to show that a knot is equivalent to a trivial knot.

3.3.5 Colorability

We focused on colorability as our knot invariant.

3.3.6 Tricoloration

Definition: A knot is tricolorable if it has a projection that can be colored with three colors subject to the following:

1. At least two colors are used.
2. At each crossing, either all three strands are the same color or each of the three strands is a different color.

3.3.7 Theorem 1: Tricoloration is a knot invariant.

Proof: We considered the three Reidemeister moves independently and showed for each one that tricolorability still holds before and after the move.

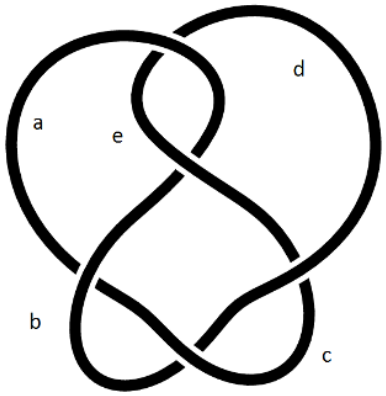
3.3.8 Generalized Colorability

Definition: Given an odd prime number p, a knot is called p-colorable if it has a projection whose strands can be labeled with the colors $\{0, 1, 2, ..., p-1\}$ subject to the following:

1. At least two colors are used.
2. If a crossing is labeled with x as the overpass and y and z as the two underpasses, then $y + z \equiv 2x \mod p$.

3.3.9 Determining Coloring Numbers

For what colors is the 5_2 knot p-colorable?



From this diagram, we get the following system of equations:

$$\begin{aligned} a + c &\equiv 2b \mod p \\ c + e &\equiv 2d \mod p \\ d + b &\equiv 2c \mod p \\ b + a &\equiv 2e \mod p \\ e + d &\equiv 2a \mod p \end{aligned}$$

We can then write this as a matrix:

$$\begin{bmatrix} 1 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 1 & -2 & 1 & 0 \\ 1 & 1 & 0 & 0 & -2 \\ -2 & 0 & 0 & 1 & 1 \end{bmatrix}$$

We can force a particular value to be 0, so let's make $e = 0$. We can also eliminate a row, since we have more rows and columns and can always find a solution. Then we get:

$$\begin{bmatrix} 1 & -2 & 1 & 0 \\ 0 & 0 & 1 & -2 \\ 0 & 1 & -2 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

We then find the determinant of the matrix to get that $det(M'_{5_2}) = 7$, meaning that 5_2 is 7-colorable.

3.4 Thursday's Daily Gather (Max)

3.4.1 Sudoku

Adam started with wanting to convince us that he knows the solution to the sudoku puzzle on the board without showing us the solution. There are 81 cards on the table with the solution covered.

Adam takes the first row and shuffles them, shows that they are the numbers 1 through 9. Doing this to every row, column, and box proves to us that the puzzle has a solution but is not repeatable so we can not prove that Adam knows a solution to anyone else.

3.4.2 Interactive Proof

Interactive Proofs take the form of a conversation between Merlin and Arthur. Merlin knows something and wants to prove it to Arthur. Arthur can only do things that are polynomial time while Merlin can do pretty much anything. We would like Arthur to accept true statements and to reject false ones.

Example: Merlin could send a proof of the Riemann Hypothesis to Arthur and Arthur could accept it.

Randomness could also be integrated under the conditions of Correctness: Accepts valid things with very high probability, and Soundness: Merlin can always convince us of true things.

On top of this an interactive proof is a Zero Knowledge Proof if it has the property that if the statement is true, Arthur learns nothing else.

3.4.3 Zero Knowledge Proof Examples

Merlin (or Adam in this case) could prove that he knows where Waldo is on a sheet by covering it up with a paper with a hole in it that covers everything but Waldo. With this information however, we still don't know where Waldo is.

If we want Merlin to prove to us that Graphs G_0 and G_1 are non-isomorphic we could choose either G_0 or G_1 at random and choose a random permutation of the vertices $\phi : V \to V$ then generate a graph $G_2 = G_i$ permuted by ϕ and then ask Merlin to

identify which graph the presented one is isomorphic to. If G_0 and G_1 are isomorphic then Merlin would not be able to the difference and so would mess up with probability 1/2. Because of this the question can be posed many times to check that Merlin can't lie about whether or not the graphs are non-isomorphic.

Commitment: I put a number in a box and give it to you but keep the key that I could give you later.

Properties:

- Hiding: Without key, one can't open the box.
- Binding: Given box, only one thing is inside, so Merlin can't provide 2 keys that open the box to different values.

Graph 3-coloring

Take a graph G. Colored with the colors T, F, and 2. Commit to the color of each vertex in its own individual box. Arthur can make a query about one edge and then unlock the boxes and check whether the colors differ.

Assuming that Merlin does not have a valid coloring the chance that he gets away with it after k queries is at least $(1 - 1/n^2)^k$ which is roughly $1/e^{(k/n^2)}$. Because of this it is possible to check with reasonable certainty whether Merlin knows a valid coloring without actually gaining knowledge about such a coloring after n^3 queries.

Zero knowledge proofs are useful for proving things like identity (being able to three-color the graph, an NP-coloring reduce to NP-complete) so this zero-knowledge protocol could be used to ensure someone's identity without revealing it.

3.4.4 Breadth of Interactive and Zero knowledge proofs

NP is roughly all the proofs that be checked in polynomial time. IP includes NP.

IP = PSPACE, the set of problems that can be solved on a computer with polynomial memory.

Arthur, running in polynomial time, can be convinced of any proof from a computer with polynomial memory but exponential computing ability. ZKP includes P since Arthur can solve it already. Assuming cryptography is secure ZKP includes NP and ZKP = IP.

3.5 Friday's Daily Gather: Building Bridges with Bernadette (Joel)

On Friday, Amanda Matson from Clarke University introduced us to a particular plane called Gaussland. In this coordinate plane, the x-axis was $\mathbb{Z}$, and the y-axis was $\mathbb{Z} \times \sqrt{-5}$. All numbers in consideration were lattice points of Gaussland, like $2 + 3\sqrt{-5}$. The rules for addition and multiplication of these numbers behave as expected.

Now there is a certain Bernadette rather concerned with the factorizations of an arbitrary number in Gaussland. Take, for example, 5 to demonstrate the curiosities of Gaussland; normally, we expect 5 to be prime, but in Gaussland, we have $5 = \sqrt{-5} \times \left(-\sqrt{-5}\right)$. A number like 6 has two different factorizations, unlike in the normal integers, for $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. In this situation, we would consider the archipelago of factorizations of numbers to be a few islands consisting of their distinct factorizations (We ignore trivial repeats like making two factors negative) and build bridges between islands based on their max number of non-repeated factors (More on this later).

This said, we split into groups to answer a few questions:

- When is a number "prime" in Gaussland?
- Can an archipelago have more than 2 islands?
- (As a followup to the previous) Given a number, can you construct an archipelago with exactly that many islands?

The second question was rather quickly answered by an example:

$$36 = 2^2 \times 3^2 = 2 \times 3 \times (1+\sqrt{-5})(1-\sqrt{-5}) = 2^2 \times (2+\sqrt{-5})(2-\sqrt{-5}) = (1+\sqrt{-5})^2(1-\sqrt{-5})^2$$

.

This led to some investigation and some conjectures:

- A prime p is reducible if $p = a^2 + 5b^2$
  Factor into $(a + b\sqrt{-5})(a - b\sqrt{-5})$.
- Prime p must be a congruent to a square mod 5 (0, 1, or 4) in order to be expressible as $a^2 + 5b^2$.
  $a^2 + 5b^2 = p \Rightarrow p \equiv a^2 \mod 5$
- The function $f(a + b\sqrt{-5}) = a^2 + 5b^2$ is multiplicative. Proof by trivial algebra.
- Any $a + b\sqrt{-5}$ is irreducible if $a^2 + 5b^2 = p$, a prime, or if $\nexists c = a_1^2 + 5b_1^2$ and $d = a_2^2 + 5b_2^2$ s.t. $cd = p$.
  The proof was not outlined in class.

We can also compile a table to simplify the process of finding factorizations:

	0	1	2	3	4	5	6
0	0	5	20	45	80	125	180
1	1	6	21	46	81	126	181
2	4	9	24	49	84	129	184
3	9	14	29	54	89	134	189
4	16	21	36	61	96	141	196
5	25	30	45	70	105	150	205
6	36	41	56	81	116	161	216

Can we actually find an archipelago of size 3?

Of course, try 18:

$$18 = 2 \times 3^2 = 2 \times (2 + \sqrt{-5})(2 - \sqrt{-5}) = 3 \times (1 + \sqrt{-5})(1 - \sqrt{-5})$$

.

We then moved on (due to time constraints) to bridge-building.

Each pair of islands in the archipelago is connected by an edge/bridge that is weighted according to how many uncommon factors the two islands share. Out of these edges, we try to find the minimum weight spanning tree, and the largest degree of in this spanning tree is known as the Catenary degree. For example, the Catenary degree for 36 in $\mathbb{Z} \times [\sqrt{-5}]$ is 2. A cool theorem to consider is that the Catenary degree in $\mathbb{Z} \times [\sqrt{-5}]$ for all numbers is either 0 or 2. The field of mathematics that Amanda introduced to us is called factorization theory.

4 Out of Context

4.1 Hum Bout: Myth of Equilateral Love

Quotable MathILonian of the Week: AI Max Engelstein

"Your abs will have fingers."

"Well if you prove it, you won't have to worry about proving it."

"The time of the meek is over! The time of the Justin is beginning!"

"That was mean. Now I gotta call my mom."

"Two parabolas enter, one tangent leaves!"

"Like cereal, we don't like choices in origami."

"Maxtropolis has very enlightened citizens."

"It's like a wall-seeking projectile from a turtle."

"Constantin drew this point, but he didn't give it a name. That's sad, so I'll give it a name. I'm naming it after my grandfather. I'll call it (0, 1). It's a family name."

"The crown giveth and the crown taketh away. Now that I have this crown, I'm amazing at math."

"Back when I was at a program like this, they only had 360 degrees, so life was much easier. Since then, they've invented more degrees."

4.1.1 Quotes From Daily Gather Lecturers

"Span span equals span." -Jackie Kaminski

"I'm going to put 'dot dot dot' in a snarky way like it's obvious." -Robert Vallin

"We don't have to throw it down a well, we can throw it off a bridge." -Adam Sealfon