12 A teaser for "Graph Theory and Additive Combinatorics"

For this last lecture, titled "triangles and equations," we're going to be previewing 18.217, "Graph Theory and Additive Combinatorics," being taught next fall. (This was a class Professor Zhao taught in Fall 2017 as well!)

12.1 A glance at Fermat's last theorem

Like many other mathematicians of the time, Schur thought about Fermat's Last Theorem, which looks for solutions

$$X^n + Y^n + Z^n, n \geq 3.$$

He considered the following idea: why not reduce this mod p? If we can show that for infinitely many different primes, there are no solutions mod p, then it must not have any solutions in the integers. Unfortunately, this doesn't work, and he proved it doesn't work. Instead, we got the following result:

Theorem 12.1 (FLT mod p)
For all n, the equation

$$X^n + Y^n = Z^n \bmod p$$

has a nontrivial solution (where p does not divide XYZ) for all sufficiently large p.

In fact, Schur proved a more combinatorial Ramsey-type result:

Theorem 12.2 (Schur)
For all r, there exists an integer N such that if we color $\{1, \cdots, N\}$ with r colors, then there exists a monochromatic solution to $X + Y = Z$.

The modern way to view this is that we can reduce to Ramsey's theorem.

Proof. Given a coloring of $\phi : [n] \to [r]$, we color a complete graph K_{n+1} with vertices $[N+1]$ by coloring an edge (i, j) with colors $\phi(|i-j|)$. By Ramsey's theorem, if N is sufficiently large, there exists a monochromatic triangle (think of this as using Pigeonhole principle). Then if those vertices are $i \leq j \leq k$, then

$$\phi(k-i), \phi(k-j), \phi(j-i)$$

are all the same color, and now we've found a monochromatic $X + Y = Z$: let $x = j - i, y = k - j, z = k - i$. □

So this is a connection between a number-theoretic problem and the corresponding graph-theory problem.

Fact 12.3
This implies FLT mod p: let H be the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ consisting of nth powers $\{a^n : a \in (\mathbb{Z}/p\mathbb{Z})*\}$. Then partition the numbers $\{1, 2, \cdots, (p-1)\}$ into H-cosets: this uses at most n colors. If p is sufficiently large in terms of n, Schur's theorem tells us that there exists some coset with a monochromatic solution: if the coset is aH, then

$$aX^n + aY^n = aZ^n \bmod p;$$

multiply by the multiplicative inverse of a to get the result.

This is a "baby example" of what is called additive combinatorics, which also goes under the name of "combinatorial number theory." Usually, number theory is about multiplying primes together: here, we care more about combinatorial properties of the numbers. Let's do a few more examples.

12.2 Turán's theorem and more

The question here is to find the **maximum number of edges in an n-vertex triangle-free graph.** The answer is that we want a completely bipartite graph $K_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil}$.

Well, the analogous problem in graph theory is to find the maximum subset of $[N]$ without a solution $x + y = z$. Picking odd numbers, or picking the numbers greater than $\frac{N}{2}$, gives half (rounded up) of the total subset. We can't do better, because we can let M be the maximum element in our subset: then both x and $M - x$ can't appear in our set, so we can have at most half density.

Here's a way to make that question a bit harder:

Problem 12.4

What's the maximum size subset of $[N]$ without a solution $x + y = 2z$ (where x, y, z aren't all equal)? In other words, we want a three-term arithmetic progression?

This problem is hard to answer, and it's even hard to find good guesses. One thing we can do is try this greedily: add 1 and 2, and then successively add numbers if they don't create 3-term arithmetic progressions. This gives only the numbers with digits 1 and 2 in base-3 representation, and it has density $N^{\log_3 2}$, since we pick 2^k of the first 3^k positive integers.

This is nowhere near the best, though: there exists an $N^{1-o(1)}$ construction, which we won't discuss here. On the other hand, due to Roth, we also know that the size is sublinear: we cannot get a positive proportion of $[N]$.

$$N^{1-o(1)} \leq \text{size of subset} \leq o(N).$$

This is probably Roth's second most important result, and it's driven a lot of research in additive combinatorics.

But now, what's the analogous question for the 3-term AP problem in graph theory?

Problem 12.5

What's the maximum number of edges in an n-vertex graph, where every edge is contained in a unique triangle?

Analogously, the answer here is

$$n^{2-o(1)} \leq \text{number of edges} \leq o(n^2).$$

Let's show the lower bound:

Proposition 12.6

We can find a graph with $n^{2-o(1)}$ edges where every edge is contained in a unique triangle.

Solution. Let's say $A \subset [\mathbb{Z}/N\mathbb{Z}]$ is a subset without three-term arithmetic progressions, where N is odd (just to avoid technicalities). Then we can actually construct a graph where every edge is contained in a unique triangle: we have three vertex sets, $X = Y = Z = \mathbb{Z}/n\mathbb{Z}$, and we put an edge between $x \in X$ and $y \in Y$ if $y - x \in A$, an edge between $y \in Y$ and $z \in Z$ if $z - y \in A$, and an edge between $x \in X$ and $z \in Z$ if $\frac{z-x}{2} \in A$.

What are the triangles in this graph? Note that $y-x, z-y, \frac{z-x}{2}$ form an arithmetic progression, but A doesn't have any 3-APs except for the trivial ones: x, x, x. So every edge here lies in exactly one triangle! This same construction also proves that the upper bound of the graph theory version implies the upper bound in the AP-subset problem. □

We haven't discussed how to prove any of the bounds, but we'll do that in the course next semester. A lot of interesting tools are used to achieve this, and generalizations and extensions have blossomed into a new field.

12.3 A generalization: more modern approaches

Theorem 12.7 (van der Waerden)
For all r and k, there exists N such that if $[N]$ is colored with r colors, then there is a monochromatic k-term arithmetic progression.

Erdös and Turán believed that the real reason for van der Waerden's theorem is not because we use k colors, but because one of our color classes has positive density. This led them to a conjecture in 1936 that was only resolved by Szemerédi in 1975, resulting in the following landmark theorem:

Theorem 12.8
For every δ, there exists N such that every subset $A \subset [N]$ with $|A| \geq \delta N$ contains a k-term arithmetic progression.

The proof is difficult and involved enough that we won't even prove it next semester. But this theorem has been looked at from other directions, and this has led to some success: the results can also be shown with ergodic theory, and this turns out to be more general in some sense. In addition, a Fourier analytic approach (by Roth) also works, but it doesn't work for 4-term arithmetic progressions. (We may have also heard of the "Hardy-Littlewood circle method.") Recently, a newer approach was found that generalizes Roth's proof to "higher-order Fourier analysis."

Remark. *Normal Fourier analysis considers correlations of a function with an exponential phase*

$$\mathbb{E}[f(x)e^{i\alpha x}].$$

In contrast, quadratic Fourier analysis looks at correlations with quadratic exponential phases:

$$\mathbb{E}[f(x)e^{i\alpha x^2}],$$

and these turn out to be essential when studying four-term arithmetic progressions.

12.4 A principle about approaching complicated problems

One last idea that developed out of Szemerédi's theorem is the "regularity lemma." Each of these approaches has its own tools, but overall, there are some connections. The idea here is **structure versus randomness**, or **signal versus noise**: the idea is that a system should be able to be written down as a piece that is structured, plus a "pseudo-random piece."

Example 12.9

If we want to understand 3-term arithmetic progressions in $[N]$, we may want to instead consider functions $f : \mathbb{Z}/n \to \mathbb{R}$. These can be written via the Fourier inversion formula

$$f(x) = \sum_r \hat{f}(r)\omega^{rx},$$

where ω is an Nth root of unity. The coefficients $\hat{f}(r) = \mathbb{E}[f(x)\omega^{-rx}]$ are generally not large (in some sense), so we can write out our sum as a sum of parts where $|\hat{f}(r)|$ is large (structured, few of them) and where $|\hat{f}(r)|$ is small (looks pseudorandom).

Example 12.10

If we start with a symmetric matrix $A \in \mathbb{R}^{n\times n}$, we can decompose it in terms of its spectrum:

$$A = \sum_i \lambda_i v_i v_i^T.$$

We can again separate this into terms where the eigenvalues are large versus small.

For graph theory, there's a similar notion: we can always start by representing a graph by its adjacency matrix, but there's also more combinatorial ways to do this. This leads us to a powerful tool in graph theory:

Theorem 12.11 (Szemerédi's regularity lemma)

Informally, every graph can be decomposed into a bounded number of vertex parts (in terms of some error), so that almost all pairs of parts look "pseudorandom."

In other words, we can think of two vertex parts as being essentially defined by edge densities. Then the "structure" part of this is the density we assign, and the "randomness" is the rest of the graph.

This is a powerful tool: it actually allows us to prove the $o(n^2)$ result for Problem 12.5.

12.5 Graph limits

Let's say we have a sequence of graphs $G_1, G_2, \cdots$ and ask the question of "do these graphs converge?" If we say that $G_n = G\left(n, \frac{1}{2}\right)$, we can say that the sequence converges to a limit, which is some constant function $\frac{1}{2}$. (In other words, we don't care about the specific edges, but only global macroscopic pictures.)

Definition 12.12

A sequence of graphs $(G_n)_n$ **converges** if for all graphs F, the density $t(F, G_n)$ converges to some constant c_F as $n \to \infty$.

This is a very local property, but how exactly do we represent this convergence?

Definition 12.13

A **graphon** is a symmetric, measurable function $W : [0,1]^2 \to [0,1]$.

We can think of our graphs as adjacency matrices: they'll have a bunch of 0s and 1s. Think of the 1s as black squares and the 0s as white squares: as $n \to \infty$, and our eyesight becomes poor, we see a grayscale image.

This isn't **quite** correct yet: for example, what's the limit of $K_{n/2,n/2}$? This can either look like a blown up version of $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, or it can look like a checkerboard! The latter begins to look a lot like $\frac{1}{2}$, but the former is the actually correct answer. So there's some subtleties that we're skipping over.

Here's some more motivation: let's say I want to maximize $x - x^3$ for $x \in [0, 1]$, but I only know about rational numbers. We can still say the answer, but it's a lot more contrived: we have to take some sequence of rationals to get to the answer.

Well, instead, let's say we want to minimize the 4-cycle density in a graph with edge density $\frac{1}{2}$. This is similar to the path of length 3 problem: the answer is to take a sequence of pseudorandom graphs with edge density $\frac{1}{2}$ and number of vertices going to ∞. That's kind of annoying to say, though: is there a nicer way to state the limit? The beauty of using graph limits is that we can just say our answer as $W = \frac{1}{2}$.

Proving these things exist requires Szemerédi's regularity lemma to represent graphs: this allows us to view graphs with this structure versus randomness decomposition. It's a nice fact, by the way, that every sequence of graphs contains at least one graph limit.

12.6 A few open problems

In 18.217, we'll discuss the structure of set addition: let $A + A$ be the set of all numbers $\{a + b : a, b \in A\}$. We can ask questions like "what is the size of $A + A$ if $|A| = n$?" In the integers, the minimum is attained for $A = [n]$, and the maximium is attained with random large numbers: this gives

$$2n - 1 \le |A + A| \le \binom{n+1}{2}.$$

But now, what can we say about A if $A + A$ is small? For example, are there any properties that we know if $|A + A| \le 100|A|$?

This means our set is not too random, or else we'd have quadratic pairwise sums. So there's some arithmetic structure in A:

Theorem 12.14 (Freiman)
A must be contained in a "small" **generalized arithmetic progression**; that is, numbers of the form $a + c_1 d_1 + c_2 d_2 + \cdots + c_k d_k$.

But there's still open problems around this theorem. In particular, the following is considered one of the most important conjectures in the field:

Conjecture 12.15 (Polynomial Freiman-Ruzsa conjecture)
There are two equivalent forms of this: we'll only state this over $\mathbb{F}_2^n$.

- Let $A \subset \mathbb{F}_2^n$ be a subset with small doubling: $|A + A| \le K|A|$. Then there exists a subspace V where $|V| \le |A|$, such that $|V \cap A| \ge K^{-O(1)}|A|$.
- Given a function $\mathbb{F}_2^n \to \mathbb{F}_2^n$ which is "almost linear" – $(f(x + y) - f(x) - f(y))$ takes on at most K values – then there exists a **linear** function $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $f(x) - g(x)$ takes on at most $K^{O(1)}$ different values.

In the second statement, it's easy to show that we can get 2^K: we just have g agree with f on a basis! Then all errors need to lie in the subspace spanned by $f(x+y)-f(x)-f(y)$. The best result that is known is a quasi-polynomial bound: we have $e^{(\log k)^{O(1)}}$.

Finally, let's consider both addition and multiplication together: much like we define $A+A = \{a+b : a, b \in A\}$, define $AA = \{ab : a, b \in A\}$. Then $|A+A|$ and $|AA|$ can separately be made linear, but there's a conjecture that this can't happen simultaneously:

Conjecture 12.16

Suppose $|A| = n$. Then

$$\max\{|A|+|A|, |AA|\} \geq n^{2-o(1)}.$$

Recent improvements have gotten us from $n^{4/3-o(1)}$ to $n^{4/3+c}$ for a small constant $c > 0$, which is still very far from what we think is the truth. This is another example of the connections between graph theory and additive combinatorics: earlier on, we saw the Szemerédi-Trotter theorem about incidences between points and lines, and it turns out we can connect the earlier material here as well. The idea is that slopes of lines involve both addition and multiplication, so encoding that information into this problem here allows us to use point-line incidences to deduce results about sums and products.

18.218 Probabilistic Method in Combinatorics

Spring 2019