Roth's theorem on arithmetic progressions

Darren Yao

Abstract

In this paper, we introduce Roth's theorem on the existence of 3-term arithmetic progressions and provide a graph-theoretic proof. We also discuss some generalizations of Roth's theorem.

1 Introduction

Additive combinatorics, also known as combinatorial number theory, is a field of mathematics concerned with sets and sequences of integers, and similarly related problems involving lattice points, sets in commutative groups, and so forth. One particularly important set of problems involves the existence of nontrivial arithmetic progressions in subsets of the positive integers.

First, we introduce Roth's theorem on arithmetic progressions, which states that any subset of the positive integers with positive upper density must contain a 3-term arithmetic progression. Roth's theorem can be proved in several ways, including Varnavides's theorem, Fourier analysis, and graph theory. In this paper, we present the graph-theoretic proof using Szemerédi's regularity lemma.

The main observation is that 3-term arithmetic progressions are equivalent to triangles in a certain graph. We first show that a graph can be partitioned in a "regular" way. Then, we bound the number of triangles and use this to make the graph triangle-free. Finally, we create a graph from an upper-bounded set of integers, and bound the number of edges in the graph in two different ways, which completes the proof.

We will also briefly present several other theorems and conjectures that can be seen as extensions of Roth's theorem.

2 Roth's theorem

In this section, we prove Roth's theorem on arithmetic progressions. We will follow the proof techniques of Yufei Zhao's Graph Theory and Additive Combinatorics [Zha19], which will be our main reference for this section.

Definition 2.1. Let A be a subset of the positive integers. Then, A has *positive upper density* if

$$\limsup_{N\to\infty} \frac{A \cap \{1, \ldots, N\}}{N} > 0.$$

Theorem 2.2 (Roth's theorem)**.** *Any subset S of the positive integers with positive upper density contains a 3-term arithmetic progression.*

We'll start by introducing some important concepts from graph theory, since this proof makes use of certain properties of triangle-free graphs.

Definition 2.3. For two sets of vertices X and Y in a graph G, let $e(X,Y)$ be the number of edges between X and Y. Then let the *edge density* $d(X,Y)$ be defined as

$$d(X,Y) = \frac{e(X,Y)}{|X||Y|}.$$

Informally, the edge density is the proportion of pairs of vertices from opposite sets where an edge exists.

Definition 2.4. Given a graph G and vertex sets $X, Y \subseteq G$, we say (X,Y) is an *ε-regular pair* if for all $A \subseteq X, B \subseteq Y$ with $|A| \geq \varepsilon|X|, |B| \geq \varepsilon|Y|$, then

$$|d(A,B) - d(X,Y)| \leq \varepsilon.$$

Definition 2.5. Given a graph G, a partition of its vertices into sets $\{V_1, \ldots, V_k\}$ is an *ε-regular partition* if

$$\sum_{\substack{1 \leq i,j \leq k, \\ (V_i,V_j) \text{ not } \varepsilon\text{-regular}}} |V_i||V_j| \leq \varepsilon|V(G)|^2.$$

Essentially, a partition is ε-regular if the sum of "irregularities" of pairs that fail to be ε-regular is less than $\varepsilon|V(G)|^2$.

With all the necessary definitions in place, we now introduce Szemerédi's regularity lemma, which we'll state without proof. Szemerédi's regularity lemma proves the existence of a certain type of graph partition with a bounded number of components. This allows us to approximate large graphs with a much simpler model.

Theorem 2.6 (Szemerédi's regularity lemma)**.** *For every $\varepsilon > 0$, there exists a constant M such that every graph has an ε-regular partition into at most M components.*

We'll also introduce the triangle counting lemma, which will become important in a bit.

Theorem 2.7 (Triangle counting lemma)**.** *Let G be a graph and X, Y, Z be subsets of the vertices of G such that $(X,Y), (Y,Z), (Z,X)$ are all ε-regular pairs for some $\varepsilon > 0$. If $d(X,Y), d(Y,Z), d(Z,X) \geq 2\varepsilon$, then the number of triples $(x,y,z) \in X \times Y \times Z$ such that x, y, z form a triangle in G is at least*

$$(1-2\varepsilon)(d(X,Y)-\varepsilon)(d(Y,Z)-\varepsilon)(d(Z,X)-\varepsilon)|X||Y||Z|.$$

The next component is the triangle removal lemma, which bounds the maximum number of vertices that need to be removed to make a graph triangle-free.

Theorem 2.8 (Triangle removal lemma)**.** *For all $\varepsilon > 0$, there exists $\delta > 0$ such that any graph G on n vertices with less than or equal to δn^3 triangles can be made triangle-free by removing at most εn^2 edges.*

Proof. First, we take a $(\varepsilon/4)$-regular partition of G, and number its vertex sets $V_1, \ldots, V_M$. We then proceed by disconnecting components that fail to be well-behaved. More formally, we remove all edges between pairs of components (V_i, V_j) that satisfy any of the following conditions:

(a) the pair (V_i, V_j) fails to be ε-regular,

(b) the pair is not dense enough: $d(V_i, V_j) < \varepsilon/2$, or

(c) one component is too small: either V_i or V_j has at most $(\varepsilon/4M)n$ vertices.

Let's examine the maximum number of edges that can be removed under each condition:

(a) By ε-regularity of the partition from Definition 2.5, we have

$$\sum_{\substack{1\le i,j\le k \\ (V_i,V_j) \text{ not } \varepsilon/4\text{-regular}}} |V_i||V_j| \le \frac{\varepsilon}{4}n^2.$$

(b) By the definition of edge density, we have

$$\sum_{\substack{1\le i,j\le k \\ d(V_i,V_j)<\varepsilon/2}} d(V_i,V_j)|V_i||V_j| \le \frac{\varepsilon}{2}\sum_{i,j}|V_i||V_j| = \frac{\varepsilon}{2}n^2.$$

(c) In each "small" component V_i, each vertex v is adjacent to at most $(\varepsilon/4M)n$ vertices in each small component. There are at most M small components, and n vertices in total, so the number of edges removed under this condition is at most

$$n \cdot \frac{\varepsilon}{4M}n \cdot M = \frac{\varepsilon}{4}n^2.$$

Summing over these three cases, at most εn^2 edges are removed. Now, suppose for the sake of contradiction that after removing these edges, there still exists a triangle in the graph. Now take (not necessarily distinct) vertex components V_i, V_j, V_k such that each component contains one vertex of this triangle. Because of the removals of components (a) and (b), V_i, V_j, V_k satisfies the hypotheses of Theorem 2.7. Then, Theorem 2.7 states that the number of triangles remaining in the graph is at least

$$\left(1-\frac{\varepsilon}{2}\right)\left(\frac{\varepsilon}{4}\right)^3|V_i||V_j||V_k|.$$

But we also have a bound on the size of the components; by (c), each of them must have at least $(\varepsilon/4M)n$ vertices, so the above expression reduces to

$$\left(1-\frac{\varepsilon}{2}\right)\left(\frac{\varepsilon}{4}\right)^3\left(\frac{\varepsilon}{4M}\right)^3 n^3.$$

Taking

$$0 < \delta < \frac{1}{6}\left(1-\frac{\varepsilon}{2}\right)\left(\frac{\varepsilon}{4}\right)^3\left(\frac{\varepsilon}{4M}\right)^3$$

yields a contradiction, because the hypothesis of the theorem states that the original graph has fewer than δn^3 triangles, but Theorem 2.7 states that we have more triangles than allowed. This completes the proof. ■

Corollary 2.9. *A graph G on n vertices in which every edge lies in a unique triangle has $o(n^2)$ edges.*

Proof. Let m be the number of edges in G, then G has $m/3$ triangles. Since $m < n^2$, we have that G has $o(n^3)$ triangles. By the triangle removal lemma, we can remove $o(n^2)$ edges to make the graph triangle-free. However, we need to remove one edge to cut each triangle, so we must remove at least $m/3$ edges. Setting these equal to each other, we have $m = o(n^2)$, as desired. ■

With all of our intermediate results in place, we are ready to prove Roth's theorem on arithmetic progressions.

Proof of Theorem 2.2. Let $A = S \cap \{1, 2, \ldots, N\}$. We will show that if S has no 3-term arithmetic progressions, then A has $o(N)$ elements, which means that S has zero upper density. Let $M = 2N+1$, now we look at A as a subset of $\mathbb{Z}/M\mathbb{Z}$. Then, we can construct a tripartite graph G whose components X, Y, Z are each copies of $\mathbb{Z}/M\mathbb{Z}$. Edges exist as follows:

- For $x \in X$ and $y \in Y$, x and y are connected by an edge if $y - x \in A$.
- For $y \in Y$ and $z \in Z$, y and z are connected by an edge if $z - y \in A$.
- For $z \in Z$ and $x \in X$, z and x are connected by an edge if $\frac{z-x}{2} \in A$. This is modular division, which is well-defined because M is odd.

If x, y, z form a triangle, then $y - x, \frac{z-x}{2}, z - y$ must all be congruent modulo M. This means that x, y, z must be an arithmetic progression in $\mathbb{Z}/M\mathbb{Z}$. Now, note that given two elements of $\mathbb{Z}/M\mathbb{Z}$ (an edge in G), there is exactly one valid way to choose a third element of $\mathbb{Z}/M\mathbb{Z}$ to form an arithmetic progression (a triangle in the G). Hence, each edge lies in exactly one triangle. In this construction, there are $3M|A|$ edges. By Corollary 2.9, G has $o(M^2)$ edges. Since the number of edges in G is $3M|A| = o(M^2)$, and $M = 2N + 1$, by dividing out an M on each side we can conclude that $|A|$ is $o(N)$. ■

3 Generalizations of Roth's theorem

Now that we've proved Roth's theorem, in this section we look at some of its generalizations and extensions.

Roth's theorem is actually the specific $n = 3$ case of Szemerédi's theorem, which generalizes Roth's theorem to arithmetic progressions that are arbitrarily long.

Theorem 3.1 (Szemerédi's theorem)**.** *For any integer k, any subset of the positive integers with positive upper density contains an arithmetic progression of length k.*

Remark 3.2. Szemerédi's theorem has many proofs, the three most important being Szemerédi's original 1975 proof using pure combinatorics [Sze75], Furstenberg's 1977 proof using ergodic theory [Fur82], and Gowers's 2001 proof using Fourier analysis and combinatorics [Gow01]. Unfortunately, the proofs are too long and too difficult for this paper.

A further generalization is Erdős's conjecture on arithmetic progressions, which remains an open problem.

Definition 3.3. A set $A = \{a_1, a_2, a_3, \ldots\}$ of positive integers is called a *large set* if the sum $\sum_i \frac{1}{a_i}$ diverges.

Conjecture 3.4 (Erdos's conjecture on arithmetic progressions)**.** *For any integer k, any large set A contains an arithmetic progression of length k.*

Another related theorem that can be seen as a generalization of Szemerédi's theorem is the Green-Tao theorem [GT08]. The Green-Tao theorem looks at the subset of primes within the integers, instead of looking at subsets of positive upper density.

Theorem 3.5 (Green–Tao)**.** *For any integer k, the prime numbers contain infinitely many arithmetic progressions of length k.*

References

[Fur82] Hillel Furstenberg. The ergodic theoretical proof of szemerédi's theorem. *Bulletin (New Series) of the American Mathematical Society*, 7:1–26, 1982.

[Gow01] William Timothy Gowers. A new proof of szemerédi's theorem. *Geometric and Functional Analysis*, 11:465–588, 2001.

[GT08] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167:481–547, 2008.

[Sze75] Endre Szemerédi. On sets of integers containing k elements in arithmetic progression. *Acta Arithmetica*, 27:199–245, 1975.

[Zha19] Yufei Zhao. *Graph Theory and Additive Combinatorics*. Massachusetts Institute of Technology, 2019.