

1. LECTURE 1. PROOF OF ROTH'S THEOREM.

Theorem 1. (Szemerédi) *There exists $N_0(\rho, k)$ so that, if $N \geq N_0(\rho, k)$, any $S \subset [1, N]$ with $|S| > \rho N$ contains a k -term arithmetic progression.*

Why is this result hard? It seems to be true for two different reasons, depending on whether S looks random or quasi-periodic. To see a suggestion of that, note that a random subset of $[1, N]$ of density $1/2$ and the set of even numbers have quite different numbers of arithmetic progressions.

The difficult part is decomposing a general set S into the two types of parts. All known proofs proceed by establishing, at some level, such a dichotomy. Today we prove $k = 3$: Roth's theorem.

By an *arithmetic progression of length N* we mean a subset of \mathbb{Z} of the form $a, a + b, \dots, a + (N - 1)b$. It is *nontrivial* if $b \neq 0$.

It is enough to prove the following:

Lemma 1. *Suppose ρ, S, N are as in the statement. There exists $N_0(\rho)$ so that, for $N \geq N_0(\rho)$, either:*

- (1) *S contains a nontrivial three-term arithmetic progression*
- (2) *There exists an arithmetic progression J of length $\geq N^{1/3}$ so that $\frac{|S \cap J|}{|J|} \geq \rho + \rho^3/10$.*

In latter classes we will see how this is a special case of a much deeper dichotomy.

For $f : \mathbb{Z} \rightarrow \mathbb{C}$, let $\hat{f} : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$ be the Fourier transform. It is defined as $\hat{f}(\alpha) = \sum_n f(n)e(n\alpha)$. Here $e(\alpha) := e^{2\pi i\alpha}$.

Let us begin by observing that for three functions $f_1, f_2, f_3 : \mathbb{Z} \rightarrow \mathbb{C}$, we have:

$$(1) \quad \sum_{x+y=2z} f_1(x)f_2(y)f_3(z) = \int_{\alpha} \hat{f}_1(\alpha)\hat{f}_3(\alpha)\hat{f}_2(-2\alpha)$$

In other terms, we can detect three-term arithmetic progressions by Fourier analysis on \mathbb{Z} . At this point it is interesting to ponder what the analog of (1) for four-term arithmetic progressions would be. The answer to this is not known explicitly, but in a certain sense an analog is implicit in the “nilmanifolds” theorem.

Apply it to $f_1 = f_3 = 1_S, f_2 = 1_S - \rho 1_{[1, N]}$. Let AP_3 be the number of three-term APs in S . Then $\sum_{x+z=2y} f_1(x)f_2(y)f_3(z) = AP_3 - \rho \sum'_{x, z \in S} 1$, where we sum only over pairs (x, z) for which $x + z$ is *even*. Since the latter number is $\geq |S|^2/2$ (why?) we see that if there are no nontrivial APs in S , we have

$$\left| \int \widehat{1_S}(\alpha)^2 \hat{f}_2(-2\alpha) \right| \geq \rho^3 N^2/2 - N$$

Because the L^2 -norm of $\widehat{1_S}(\alpha)$ is $\leq N$, we conclude that there exists α_0 so that – for N large enough –

$$(2) \quad |\hat{f}_2(\alpha_0)| \geq \rho^3 N/4$$

Our goal is to pass from this to the existence of a long arithmetic progression J so that $S \cap J$ has higher density than S . Roughly, (2) asserts that S correlates highly with a level set of the function $n \mapsto e(n\alpha_0)$. But that level set is a union of short arithmetic progressions.

Let J be an arithmetic progression of length L contained in $[1, M]$ so that $|e(n\alpha_0) - 1| \leq \epsilon$ for $n \in J$. We shall construct in a moment with

$$(3) \quad L \geq N^{1/3}, M \leq N^{9/10}, \epsilon \leq N^{-1/10}.$$

$$\left| \sum_{n \in \mathbb{Z}} \sum_{p \in J} f_2(n+p) e((n+p)\alpha_0) \right| \geq \rho^3 LN/4$$

The sum over n can be restricted to $[1-M, N]$; so:

$$\frac{1}{M+N} \sum_{n=1-M}^N \left| \sum_{p \in J} f_2(n_0+p) e(p\alpha_0) \right| \geq \frac{\rho^3 LN}{4(M+N)}$$

Consider, for $1-M \leq n \leq N$, the quantities $\rho_n = \frac{1}{L} \sum_{p \in J} f_2(n_0+p)$, i.e. “the normalized density of S along $n+J$.” They have average zero, i.e. $\sum_n \rho_n = 0$. But the average of $|\rho_n|$ is bounded below by the above statement:

$$\frac{1}{M+N} \sum_{n=1-M}^N |\rho_n| \geq \frac{\rho^3 N}{4(M+N)} - \epsilon$$

So there exists n_0 for which $\rho_{n_0} \geq \frac{\rho^3 N}{8(M+N)} - \epsilon$.

In fact (this point was not addressed in the lecture) we may choose n_0 so that $n_0 + J \subset [1, N]$. In effect, the “endpoints” $1-M \leq n \leq 0$ and $N \leq n \leq N+M$ do not affect the average significantly, because M is very small relative to N .

In other terms,

$$\frac{1}{L} \sum_{p \in J} 1_S(n_0+p) \geq \frac{\rho^3 N}{8(M+N)} + (\rho - \epsilon)$$

The claimed result follows in view of (3). It remains only to find the arithmetic progression J . By the pigeonhole principle, the first $[N^{1/2}]$ multiples of α_0 , considered modulo 1, contain a multiple $k_0\alpha_0$ whose distance to 0 in the circle \mathbb{R}/\mathbb{Z} is $\leq N^{-1/2}$. We take J to be $\{0, k_0, 2k_0, \dots, [N^{1/3} + 1]k_0\}$. It is easy to see that has the properties (3) for N big enough.

1.1. Complements: bounds, abelian groups. One can ask about the correct bounds.

A lovely example of Behrend shows that there exists $S \subset [1, N]$ with size $|S| > N \exp(-c\sqrt{\log N})$ containing no three-term AP. It is obtained from the fact that a sphere in \mathbb{R}^k contains no three co-linear points.

The above proof shows that if $|S| > N(\log \log N)^{-C}$ for a suitable constant C , then S contains a three-term AP. Being careful gives $C = 1$. The problem is that we passed to the very small subinterval J , discarding most of our knowledge about S . Refined arguments give the bound $N(\log N)^{-C}$ for a suitable constant C . We do not know here how to obtain $C = 1$. The best known bound is Bourgain which is slightly better than $C = 1/2$. The analogue of Roth’s theorem holds in a finite abelian group. Consider, in particular, the case of $S \subset (\mathbb{Z}/3)^k$. It is known that if $|S| \gg 3^k/k$, then S contains a three-term arithmetic progression. But here our knowledge is particularly poor: as far as we know there exists $\rho < 3$ so that any set of size $\geq \rho^k$ contains a three-term AP. This seems to be a very interesting problem.