Fourier analytic proof of Roth's theorem on 3-term arithmetic progressions

Sayantan Khan

July 2016

The fact that the integral

$$\int_{-\pi}^{\pi} e^{inx} dx$$

is 1 only when n is 0 and for other integral values of n, it is 0, can be very useful. It is this very observation that forms the backbone of a general class of techniques in number theory called the *circle method*. In a nutshell, this method lets one *count*, by integrating an appropriately picked function over the unit circle, hence the name.

Roth's theorem is question about existence of three term APs, but like many existence problems, it can be resolved by counting, and making sure your count doesn't end at 0. Formally, the theorem states that given a number $\delta > 0$, called the density, there exists a large enough N such that any subset of $\{0, 1, 2, 3, \ldots, N-1\}$ with a size greater than δN contains a three term arithmetic progression. The key idea in the proof is to count the number of triples x, y, z such that $x + z - 2y$ is 0. And this is where the circle method comes in, transforming a combinatorial problem into a problem in analysis.

1 Sketch of proof

The key idea in the proof of Roth's theorem is that for a given $0 < \delta < 1$, and a large enough N, if a subset A of $[N]$[1], which has size δN does not have a three term AP, then there exists a progression B_1 in $[N]$ such that the density of A in B_1 is greater than δ. Clearly, $A \cap B_1$ won't contain a three term AP either, so one iterates the argument again and again to get a sequence of nested sub progressions $B_1, B_2, \ldots B_k$ such that the density of A in B_k is at least 1. But that would mean $B_k = A$, and if $|B_k| \geq 3$, we'll have a contradiction. So one picks a large enough N such that $|B_k| \geq 3$, and that leads to the contradiction. Which means A must have had a three term AP.

[1] $[N]$ is shorthand for the set $\{0, 1, 2, 3 \ldots, N-1\}$

2 Fourier analysis on finite cyclic groups

Let's begin by endowing the set $[N]$ some additional structure, namely identifying it with the group $\mathbb{Z}/N\mathbb{Z}$. Furthermore, with the counting measure $\mathbb{Z}/N\mathbb{Z}$, we can integrate functions from $\mathbb{Z}/N\mathbb{Z}$ to $\mathbb{C}$. And with the discrete metric, we have the topology on the space; we can finally do some analysis.

Consider the set of functions from $\mathbb{Z}/N\mathbb{Z}$ to $\mathbb{C}$. This clearly forms a Hilbert space, with the inner product being

$$\begin{aligned}\langle f, g\rangle &= \frac{1}{N}\int_{\mathbb{Z}/N\mathbb{Z}} f(x)\overline{g(x)}dx \\ &= \frac{1}{N}\sum_{k=0}^{N-1} f(k)\overline{g(k)}\end{aligned}$$

The next step would be to determine an orthonormal basis for the Hilbert space. It turns out that the set of homomorphisms from $\mathbb{Z}/N\mathbb{Z}$ to $\mathbb{C}$ does form an orthonormal basis for the space. Define h_r to be the following homomorphism

$$h_r(k) = e^{\frac{2\pi i}{N}rk}$$

Notice that

$$\frac{1}{N}\int_{\mathbb{Z}/N\mathbb{Z}} h_r(x)dx = \begin{cases}1 & \text{if } r = 0\\ 0 & \text{if } r \neq 0\end{cases}$$

The r^{th} Fourier coefficient of f is defined as

$$\begin{aligned}\widehat{f}(r) &= \langle f, h_r\rangle \\ &= \frac{1}{N}\sum_{k=0}^{N-1} f(k)e^{-\frac{2\pi i}{N}rk}\end{aligned}$$

Hence, for any function f

$$f(x) = \widehat{f}(0)h_0(x) + \widehat{f}(1)h_1(x) + \ldots + \widehat{f}(N-1)h_{N-1}(x)$$

3 Counting progressions in $[N]$[1]

Note: We'll call (x, y, z) a progression in $\mathbb{Z}/N\mathbb{Z}$ when $x + z = 2y$ in the group $\mathbb{Z}/N\mathbb{Z}$, and we'll call it a progression in $[N]$ when $x + y = 2z$ in $\mathbb{Z}$.

Consider a subset A of $[N]$ of size δN. Identify A as a subset of $\mathbb{Z}/N\mathbb{Z}$ as well. We are looking for three term APs, or triples (x, y, z) such that $x + z - 2y = 0$ in $\mathbb{Z}/N\mathbb{Z}$. The number of such triples will be given by

$$\begin{aligned}S_0 &= \sum_{x,y,z\in A}\frac{1}{N}\int_{\mathbb{Z}/N\mathbb{Z}} h_{x+z-2y}(x)dx \\ &= \sum_{x,y,z\in[N]}\frac{1}{N}\sum_{k=0}^{N-1}\mathbb{1}_A(x)\mathbb{1}_A(y)\mathbb{1}_A(z)e^{-\frac{2\pi i}{N}k(x+z-2y)} \\ &= N^2\sum_{k=0}^{N-1}\widehat{\mathbb{1}_A}(k)^2\widehat{\mathbb{1}_A}(-2k)\end{aligned}$$

where $\mathbb{1}_A$ is the indicator function of A. This counts the number of three term APs in the group $\mathbb{Z}/N\mathbb{Z}$. But all the progressions in $\mathbb{Z}/N\mathbb{Z}$ need not be progressions in $[N]$. But if we know that x and y belong to $\left[\frac{N}{3}, \frac{2N}{3}\right]$, and $x + z - 2y = 0$ in the group, then x, y, z form an AP in $[N]$. Define the set M_A to be $\left[\frac{N}{3}, \frac{2N}{3}\right] \cap A$. Then, a lower bound for the number of three term APs in $[N]$ is given by

$$\begin{aligned}
S &= \sum_{x,y \in M_A} \sum_{z \in A} \frac{1}{N} \int_{\mathbb{Z}/N\mathbb{Z}} h_{x+z-2y}(x)dx \\
&= N^2 \sum_{k=0}^{N-1} \widehat{\mathbb{1}_A}(k)\widehat{\mathbb{1}_{M_A}}(k)\widehat{\mathbb{1}_{M_A}}(-2k) \\
&= N^2 \left(\widehat{\mathbb{1}_A}(0)\widehat{\mathbb{1}_{M_A}}(0)\widehat{\mathbb{1}_{M_A}}(0) + \sum_{k=1}^{N-1} \widehat{\mathbb{1}_A}(k)\widehat{\mathbb{1}_{M_A}}(k)\widehat{\mathbb{1}_{M_A}}(-2k) \right) \\
&= \delta|M_A|^2 + N^2 \sum_{k=1}^{N-1} \widehat{\mathbb{1}_A}(k)\widehat{\mathbb{1}_{M_A}}(k)\widehat{\mathbb{1}_{M_A}}(-2k)
\end{aligned}$$

We want to show that $[N]$ contains at least one three term AP. But the expression for S also counts triples like (x, x, x), which we don't want to count as APs. A contains $|A|$ such triples. Hence we'd like S to be greater than $|A|$ to show the existence of an AP. We have the following lemma

Lemma 3.1. *If N is odd, $\widehat{\mathbb{1}_A}(k) < \varepsilon$ for all $k \neq 0$, where $\varepsilon = \frac{\delta^2}{8}$, and $|M_A| \geq \frac{\delta N}{4}$, then $S \geq \frac{\delta^3 N^2}{32}$.*

Proof. We know that

$$S = \delta|M_A|^2 + N^2 \sum_{k=1}^{N-1} \widehat{\mathbb{1}_A}(k)\widehat{\mathbb{1}_{M_A}}(k)\widehat{\mathbb{1}_{M_A}}(-2k)$$

We can bound the second term in the sum using Cauchy-Schwarz inequality and Plancherel's identity.

$$\begin{aligned}
\left| \sum_{k=1}^{N-1} \widehat{\mathbb{1}_A}(k)\widehat{\mathbb{1}_{M_A}}(k)\widehat{\mathbb{1}_{M_A}}(-2k) \right| &\leq \varepsilon \sum_{k=1}^{N-1} \left| \widehat{\mathbb{1}_{M_A}}(k)\widehat{\mathbb{1}_{M_A}}(-2k) \right| \\
&\leq \varepsilon \left(\sum_{k=1}^{N-1} \left| \widehat{\mathbb{1}_A}(k) \right|^2 \right)^{\frac{1}{2}} \left(\sum_{k=1}^{N-1} \left| \widehat{\mathbb{1}_A}(-2k) \right|^2 \right)^{\frac{1}{2}} \\
&= \varepsilon \left(\sum_{k=1}^{N-1} \left| \widehat{\mathbb{1}_A}(k) \right|^2 \right) \\
&= \varepsilon \left(\sum_{k=1}^{N-1} |\mathbb{1}_A(k)|^2 \right) \\
&= \varepsilon |M_A|
\end{aligned}$$

From this, we get that

$$S \geq \delta|M_A|^2 - \varepsilon N^2 |M_A|$$

Since $|M_A| \geq \frac{\delta N}{4}$, and $\varepsilon = \frac{\delta^2}{8}$, we get

$$S \geq \frac{\delta^3 N^2}{32}$$

□

This lemma shows that if we pick an $N > \frac{32}{\delta^2}$, any subset A which satisfies the hypotheses of the lemma will contain a 3-AP.

4 Density incrementation

Now consider the contrapositive of lemma 3.1. It says that if a subset A of $[N]$ does not contain a 3-AP, then one of the following conditions must hold

1. For some non-zero k, $\widehat{\mathbb{1}_A}(k) > \varepsilon$, where $\varepsilon = \frac{\delta^2}{8}$.
2. $|M_A| < \frac{\delta N}{4}$.

We don't consider the third condition where N could be less than $\frac{32}{\delta^2}$ because we can make N as large as we want. Consider the second condition. If the density of A in $\left[\frac{N}{3}, \frac{2N}{3}\right]$ is less than $\frac{\delta N}{4}$, then by the pigeonhole principle, A has a density greater than $\delta + \frac{\delta}{8}$ in either $\left[0, \frac{N}{3}\right]$ or $\left[\frac{2N}{3}, N\right]$. To put it more generally, there exists an AP Z in $[N]$ of length greater than or equal to $\frac{N}{3}$ such that the density of A in Z is $\delta + \frac{\delta}{8}$, which is greater than the original density. Specifically, the progression Z in this case is either the interval $\left[0, \frac{N}{3}\right]$ or $\left[\frac{2N}{3}, N\right]$.

We will show even when $\widehat{\mathbb{1}_A}(k) > \varepsilon$ for some non-zero k, there exists a sufficiently long progression in $[N]$ such that the density of A in that subprogression is greater than δ.

Lemma 4.1. *If $\widehat{\mathbb{1}_A}(r) > \gamma$ for some $r \neq 0$, then there exists a $\mathbb{Z}/N\mathbb{Z}$ subprogression B of length at least $\frac{\sqrt{N}}{8}$ such that $|A \cap B| \geq \left(\delta + \frac{\gamma}{4}\right)|B|$.*

Proof. Consider the pairs of points

$$(0,0), (1,r), (2,2r), \ldots, (N-1, (N-1)r)$$

These points lie in the square $[0, N] \times [0, N]$. Divide this square into $\lfloor\sqrt{N}\rfloor^2$ squares (where $\lfloor x \rfloor$ is the greatest integer *less* than x) of side length $l = \frac{N}{\lfloor\sqrt{N}\rfloor}$. Since there are less than N squares, two of the points must lie in the same square. That means for some $d \leq l$

$$rd \leq l \pmod{N}$$

Let B' be an AP of length $\left\lfloor \frac{\lfloor N \rfloor}{2\pi} \right\rfloor$ in $\mathbb{Z}/N\mathbb{Z}$

$$\ldots, -3d, -2d, -d, 0, d, 2d, 3d, \ldots$$

Since $|B'|d$ is less than $|B'|l$, which in turn is less than $\frac{N}{2\pi}$, which means that it can be written as a union of two disjoint APs in $[N]$.

Consider the following inequality:

$$\begin{aligned}
\left|N\widehat{\mathbb{1}}_{B'}(r) - |B'|\right| &= \left|\sum_{\mathbb{Z}/N\mathbb{Z}} \mathbb{1}_{B'}(x)\left(e^{-\frac{2\pi i}{N}rx} - 1\right)\right| \\
&= \left|\sum_{|x|\leq\frac{1}{2}|B'|}\left(e^{-\frac{2\pi i}{N}rdx} - 1\right)\right| \\
&\leq \sum_{|x|\leq\frac{1}{2}|B'|}\left|e^{-\frac{2\pi i}{N}rdx} - 1\right| \\
&\leq 2\sum_{x=0}^{\frac{|B'|}{2}}\frac{2\pi}{N}rdx \\
&\leq \frac{4\pi l}{N}\sum_{x=0}^{\frac{|B'|}{2}}x \\
&\leq |B'|\frac{|B'|\pi l}{N} \\
&\leq \frac{|B'|}{2}
\end{aligned}$$

This means

$$\left|N\widehat{\mathbb{1}_B}(r)\right| \geq \frac{|B'|}{2}$$

The required progression, in which the density of A will be greater than $\left(\delta + \frac{\gamma}{4}\right)$, will be a translation of B', i.e. $B = B' + c$ for some constant c.

Define f_A to be the balanced indicator of A, i.e.

$$f_A(k) = \mathbb{1}_A(k) - \delta$$

Notice that the mean of f_A over $[N]$ is 0. Furthermore, if

$$\sum_{k=0}^{N-1} f_A(k)\mathbb{1}_B(k) \geq \kappa|B|$$

then

$$|A \cap B| \geq (\delta + \kappa)\,|B|$$

and vice versa. Here's why.

$$\begin{aligned}
\sum_{k=0}^{N-1} f_A(k)\mathbb{1}_B(k) &= \sum_{k\in B} f_A(k) \\
&= (1-\delta)|A\cap B| - \delta(|B| - |A\cap B|) \\
&= |A\cap B| - \delta|B|
\end{aligned}$$

$|A \cap B| - \delta|B|$ will be greater than $\kappa|B|$ iff $|A \cap B| > (\delta + \kappa)|B|$. Now our problem reduces to determining for what c, $\sum_{k=0}^{N-1} f_A(k)\mathbb{1}_{B'}(k-c)$ is greater than or equal to $\frac{\gamma}{4}|B'|$. Define $G(c)$ to be

$$G(c) = \sum_{k=0}^{N-1} f_A(k)\mathbb{1}_{B'}(k-c)$$

The Fourier transform of G is the following:

$$\widehat{G}(r) = N\widehat{f_A}(r)\widehat{\mathbb{1}_{B'}}(r)$$

And we know that

$$\sum_{[N]} |G(c)| \geq \left|\widehat{G}(r)\right| \geq \frac{1}{2}\gamma N|B'|$$

And since the mean of G over $[N]$ is 0

$$\sum_{[N]} G(c) + |G(c)| \geq \frac{1}{2}\gamma N|B'|$$

For some c_0

$$G(c_0) + |G(c_0)| \geq \frac{1}{2}\gamma|B'|$$

Hence, $G(c_0) \geq \frac{1}{4}\gamma$

The progression $B = B' + c_0$ is the one that satisfies our requirements. □

Lemma 4.2. *If $[N]$ has a $\mathbb{Z}/N\mathbb{Z}$ progression B of length $\frac{\sqrt{N}}{8}$, such that the density of A in B is greater than or equal to $\delta + \frac{\gamma}{4}$, and it is a union of two disjoint $[N]$ progressions, then there exists a progression P in $[N]$ such that $|P| \geq \frac{\gamma}{8}|B|$ such that A has density $\delta + \frac{\gamma}{8}$ in P.*

Proof. Write B as $P_1 \sqcup P_2$, where P_1 and P_2 are disjoint $[N]$ progressions, and $|P_1| \leq |P_2|$. If $|P_1| \leq \frac{\gamma}{8}|B|$, then

$$\begin{aligned}
|A \cap P_2| &\geq |A \cap B| - |P_1| \\
&\geq \left(\delta + \frac{\gamma}{4}\right)|B| - P_1 \\
&\geq \left(\delta + \frac{\gamma}{8}\right)|B| \\
&\geq \left(\delta + \frac{\gamma}{8}\right)|P_2|
\end{aligned}$$

One the other hand, if $|P_1| > \frac{\gamma}{8}$, then one of A must have density $\delta + \frac{\gamma}{4}$ on one of P_1 or P_2. □

With the previous lemmas, we can finally state in full the density incrementation theorem.

Theorem 4.3. *Given $0 < \delta < 1$, and $N > \frac{32}{\delta^2}$, and a subset A of $[N]$ of size δN, if for some non-zero k, $\widehat{\mathbb{1}_A}(k) > \frac{\delta^2}{8}$ or $\left|\left[\frac{N}{3}, \frac{2N}{3}\right] \cap A\right| < \frac{\delta N}{4}$, then there exists a progression in $[N]$ of length at least $\frac{\delta^2\sqrt{N}}{512}$ such that the density of A in the progression is at least $\delta + \frac{\delta^2}{64}$.*

Proof. Follows from lemmas 4.1 and 4.2. □

5 Iterating the density incrementation argument

The final step in the proof of Roth's theorem is to increment the density until one reaches a sub progression in which A has density 1. If the length of that sub progression is greater than 3, then we're done. After each iteration, the density grows by at least $\frac{\delta^2}{64}$, hence after $k = \frac{64}{\delta^2}(1-\delta)$ steps, the density will be at least 1. We just need to pick a large enough N such that the sub progression after k steps has at least 3 elements. We want

$$\frac{\delta^{2k} N^{\frac{1}{2^k}}}{512^k} \geq 3$$

$$N \geq 3^{2^k} \left(\frac{512}{\delta^2}\right)^{2^k \cdot k}$$

Substituting the given value of k, we get our lower bound on N, and that completes the proof.

References

[1] Mustazee Rahman, *Roth's theorem on 3-term arithmetic progressions*, `http://wiki.math.toronto.edu/TorontoMathWiki/images/2/2d/Expo_paper.pdf`.