AN OLD NEW PROOF OF ROTH'S THEOREM

Endre Szemerédi

In 1953 Roth [3] proved that for any fixed $\delta > 0$, if N is sufficiently large and A is any subset of $\{1, 2, \dots, N\}$ of size $\geq \delta N$ then A contains a non-trivial 3-term arithmetic progression. In the 1980s I came up with an alternate proof that is in some aspects a little simpler but which I did not publish. This school gives me another opportunity to present this approach.

We suppose that $A \subset \{1, 2, \dots, N\}$ with $|A| = \delta N$ (where $|A| \geq 1000\sqrt{N}$), and that A does not contain a non-trivial 3-term arithmetic progression, As usual we define $e(t) = \mathrm{e}^{2i\pi t}$ and

$$\hat{A}(\alpha) = \sum_{a \in A} e(a\alpha).$$

The number of solutions to $a + c = 2b$ with $a, b, c \in A$ is given by

$$|A| = \sum_{a,b,c \in A} \int_0^1 e(\alpha(a + c - 2b)) d\alpha = \int_0^1 \hat{A}(\alpha)^2 \hat{A}(-2\alpha) d\alpha \tag{1}$$

(the $|A|$ comes from the solutions with $a = b = c$). We will partition $\mathbb{R}/\mathbb{Z}$ into the arcs $I_j := [\frac{2j-1}{2MN}, \frac{2j+1}{2MN})$ for $j = 0, 1, \dots, NM - 1$ where M is the smallest integer $\geq 2\pi/\delta\eta$, with $\eta = 10^{-6}$. For real number t denote by $\|t\|$ the distance from t to the nearest integer. Note that $|e(t) - 1| = 2|\sin(\pi t)| = 2|\sin(\pi\|t\|)| \leq 2\pi\|t\|$. Hence if $\alpha \in I_j$, that is $\alpha = \frac{j}{MN} + \beta$ where $|\beta| \leq 1/2MN$, then

$$|\hat{A}(j/MN) - \hat{A}(\alpha)| \leq \sum_{a \in A} |e(a\beta) - 1| \leq \sum_{a \in A} 2\pi\|a\beta\| \leq |A| 2\pi N/2MN \leq \eta\delta^2 N/2. \tag{2}$$

Let J be the set of integers in $[0, MN)$ for which $|\hat{A}(j/MN)| \geq \eta\delta^2 N$; and then define the *major arc*, $\mathcal{M}$ to be the union of the I_j with $j \in J$. From (2) we deduce that

$$|\hat{A}(\alpha)| \geq \eta\delta^2 N/2 \quad \text{if } \alpha \in \mathcal{M}; \qquad \text{and } \ |\hat{A}(\alpha)| \leq 3\eta\delta^2 N/2 \quad \text{if } \alpha \notin \mathcal{M}.$$

From the second of these inequalities we deduce that

$$\left| \int_{\substack{0 \\ \alpha \notin \mathcal{M}}}^1 \hat{A}(\alpha)^2 \hat{A}(-2\alpha) d\alpha \right| \leq \max_{\alpha \notin \mathcal{M}} |\hat{A}(\alpha)| \cdot \int_0^1 |\hat{A}(\alpha)| \cdot |\hat{A}(-2\alpha)| d\alpha$$

$$\leq \frac{3}{2}\eta\delta^2 N \left(\int_0^1 |\hat{A}(\alpha)|^2 d\alpha \ \int_0^1 |\hat{A}(-2\alpha)|^2 d\alpha \right)^{1/2} = \frac{3}{2}\eta\delta^3 N^2 \tag{3}$$

by Parseval's identity that $\int_0^1 |\hat{A}(\alpha)|^2 d\alpha = |A|$. From the first of the inequalities we have that

$$\delta N = |A| = \int_0^1 |\hat{A}(\alpha)|^2 d\alpha \geq \int_{\alpha\in\mathcal{M}} |\hat{A}(\alpha)|^2 d\alpha \geq |\mathcal{M}|(\eta\delta^2 N/2)^2,$$

so that $|\mathcal{M}| \leq 4/(\eta^2\delta^3 N)$; and thus $k := |J| \leq 4M/\eta^2\delta^3 \lesssim 8\pi/\delta^4\eta^3$. (Here we use the notation "$\lesssim$" (and later "$\sim$") instead of "$\leq$" (and later "$=$", respectively), when there may be other terms that are negligible compared to the main term.)

We now claim that there exists a positive integer $q \leq Q$ for which

$$\left\| \frac{qj}{MN} \right\| \leq Q^{-1/k} \quad \text{for each } j \in J. \tag{4}$$

To see this consider the vectors w_i in $(\mathbb{R}/\mathbb{Z})^k$ with coordinates indexed by $j \in J$, where the jth coordinate is $ij/mn \pmod 1$. If we cut the space up into the Q k-dimensional minicubes given by cutting up each dimension into sides of length $Q^{-1/k}$, then at least two of the vectors from $w_0, w_1, \ldots, w_Q$ belong to the same minicube, by the pigeonhole principle. If these vectors are w_h and w_i with $0 \leq h < i \leq Q$ then let $q = i - h$ so that (4) holds as claimed.

Take $L = [N^{1/3k}/8M]$ and $Q = (8LM)^k$, so that $Q \leq N^{1/3}$. If $\alpha \in I_j$ with $j \in J$ then $\|q\alpha\| \leq \|qj/MN\| + \|q/2MN\| \leq Q^{-1/k} + Q/2MN$, and thus if ℓ is an integer for which $|\ell| \leq 4L$ then $\|\alpha q\ell\| \leq 4L(Q^{-1/k} + Q/2MN) \leq 1/M$, since $4LQ \leq Q^{1+1/k} \leq N^{2/3}$ as well. Therefore

$$\begin{aligned}
&\left| \int_0^1 \hat{A}(\alpha)^2 \hat{A}(-2\alpha) e(\alpha q\ell) d\alpha - \int_0^1 \hat{A}(\alpha)^2 \hat{A}(-2\alpha) d\alpha \right| \\
&\qquad \leq 2\pi \int_{\alpha\in\mathcal{M}} |\hat{A}(\alpha)|^2 \cdot |\hat{A}(-2\alpha)| \cdot \|\alpha q\ell\| d\alpha + 2\int_{\alpha\notin\mathcal{M}} |\hat{A}(\alpha)|^2 \cdot |\hat{A}(-2\alpha)| d\alpha \\
&\qquad \leq 2\pi\delta^2 N^2 \max_{\alpha\in\mathcal{M}} \|\alpha q\ell\| + 3\eta\delta^3 N^2 \leq 4\eta\delta^3 N^2
\end{aligned}$$

by (3). We deduce that for any $|r|, |s|, |t| \leq L$ (taking $\ell = r + t - 2s$ above) we have

$$\#\{a, b, c \in A : \ (a + rq) + (c + tq) = 2(b + sq)\} \leq 5\eta\delta^3 N^2, \tag{5}$$

using (1), since $\delta N \geq \sqrt{N/\eta}$ by assumption.

This suggests that for most 3–term arithmetic progressions of integers $u + w = 2v$ there cannot be many $a = u - rq, b = v - sq, c = w - tq \in A$, which seems implausible if A is reasonably distributed in segments of residue classes mod q. To show this define

$$\kappa(n) = \#\{r : \ |r| \leq L, \ n - rq \in A\}.$$

One expects that $\kappa(n)$ is roughly $\delta(2L + 1)$ for most integers n. We will now prove that most integers belong to

$$B = \left\{ n : \ 1 \leq n \leq N, \kappa(n) > \frac{\delta}{8}(2L + 1) \right\}$$

unless $\kappa(n)$ is surprisingly large for some n. Let $A(m) = 1$ if $m \in A$, and $= 0$ otherwise. Note that

$$\sum_{n=1}^{N} \kappa(n) = \sum_{n=1}^{N} \sum_{r=-L}^{L} A(n-rq) = \sum_{a\in A} \#\{r : |r| \le L,\ 1 \le a + rq \le N\}$$
$$\ge (2L+1)\#\{a \in A : Lq < a < N - Lq\} \ge (2L+1)(\delta N - 2Lq).$$

Now assume that each $\kappa(n) \le \frac{9\delta}{8}(2L+1)$ so that

$$\sum_{n=1}^{N} \kappa(n) \le |B|\frac{9\delta}{8}(2L+1) + (N - |B|)\frac{\delta}{8}(2L+1).$$

We can combine the last two inequalities to obtain $|B| \ge 7N/8 + O(N^{2/3})$. On the other hand, by (5) we have, writing $a = u - rq,\ b = v - sq,\ c = w - tq$,

$$5\eta\delta^3 N^2(2L+1)^3 \ge \sum_{|r|,|s|,|t|\le L} \#\{a, b, c \in A :\ (a + rq) + (c + tq) = 2(b + sq)\}$$
$$= \sum_{u+w=2v} \kappa(u)\kappa(v)\kappa(w) \ge \sum_{\substack{u+w=2v\\ u,v,w\in B}} \kappa(u)\kappa(v)\kappa(w)$$
$$\ge \left(\frac{\delta}{8}(2L+1)\right)^3 \#\{u, v, w \in B :\ u + w = 2v\};$$

that is

$$\#\{u, v, w \in B :\ u + w = 2v\} \le 5 \cdot 8^3\eta N^2 < N^2/300. \tag{6}$$

We can bound $\#\{u, v, w \in B :\ u + w = 2v\}$ from below by taking all $\sim N^2/4$ solutions to $u + w = 2v$ with $1 \le u, v, w \le N$, and then subtracting, for each $u \notin B$ the number of v for which $1 \le 2v - u \le N$ (that is $(N - |B|) \times N/2$) and similarly for w, and then subtracting, for each $v \notin B$ the number of $u, w \in B$ for which $u+w \in B$ (which is no more than $(N - |B|) \times |B|$). Thus

$$\#\{u, v, w \in B :\ u + w = 2v\} \gtrsim N^2/4 - (N^2 - |B|^2) \gtrsim N^2/64$$

as $|B| \gtrsim 7N/8$, which contradicts (6). Therefore the assumption is false, so that there exists n with $\kappa(n) > \frac{9\delta}{8}(2L+1)$.

We deduce that the set

$$A_0 := \{r + L + 1 :\ n - rq \in A\} \subset \{1, \ldots, 2L + 1\}$$

has $\ge \frac{9}{8}\delta(2L+1)$ elements, but no 3-term arithmetic progression. Let $N_1 := [N^{\delta^4/10^{20}}]$, which is smaller than $2L+1$. Select the subinterval $[s+1, s+N]$ of $[1, 2L+1]$ containing the most elements of A_0, so that

$$A_1 := \{j :\ 1 \le j \le N \text{ and } s + j \in A_0\}$$

does not contain any non-trivial 3-term arithmetic progressions, and has $\gtrsim \frac{9}{8}\delta N_1$ elements. We have therefore proved the following:

If A is a subset of $\{1, 2, \ldots, N\}$, with δN elements, which does not contain a non-trivial 3-term arithmetic progression, then there exists a subset A_1 of $\{1, 2, \ldots, N_1\}$, with $\gtrsim \frac{9}{8}\delta N_1$ elements, which does not contain a non-trivial 3-term arithmetic progression.

Suppose that $\delta \geq \delta_g = (8/9)^g$. If we iterate the above result j times then we have a subset $A_j \subset \{1, 2, \ldots, N_j\}$ containing $\delta_{g-j} N_j$ elements, no three of which form an arithmetic progression, where $N_j \sim N^{\eta_j}$ with $\eta_j := (8/9)^{2((2g+1)j-j^2)}/10^{20j}$. Therefore A_g contains all the integers up to N_g and so must contain many three term arithmetic progressions, a contradiction, provided N_g is sufficiently large. This will be the case if $\eta_g \gg 1/\log N$ which follows provided $g < (\log\log N/(2\log(9/8)))^{1/2} + O(1)$. Hence we may take any

$$\delta \gg 1/\exp(c\sqrt{\log\log N})$$

where $c = \sqrt{\frac{1}{2}\log\frac{9}{8}}$. One can optimize our argument to slightly increase the value of c.

We have therefore proved the following result:

Theorem. *There exists a constant $c > 0$ such that if A is a subset of $\{1, 2, \ldots, N\}$ with N sufficiently large, where A contains at least*

$$N/\exp(c\sqrt{\log\log N})$$

elements, then A contains a non-trivial three-term arithmetic progression.

Stronger results are proved in [1], [2] and [4].

Acknowledgements: This article was written by Antal Balog and Andrew Granville, based on the lecture given by the author at the school.

References

1. J. Bourgain, *On triples in arithmetic progressions*, GAFA **9** (1999), 107–156.
2. D.R. Heath-Brown, *Integer sets containing no arithmetic progressions*, JLMS **35** (1987), 385–394.
3. K.F. Roth, *On certain sets of integers*, JLMS **28** (1953), 104–109.
4. E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math Hungar **56** (1990), 155–158.