ROTH'S THEOREM

In this note, we apply circle method to integer sequences having no three terms in an arithmetic progression.

1. Introduction

In 1927 Van der Warden proved that if $r,\ l$ are positive integers and $n \geq n_0(r,l)$, then the set $\{1,2,\cdots,n\}$ if partitioned in anyway into r subsets, one of these subsets contains l terms in an arithmetic progression (a.p.).

Erdos and Turan (1936) conjectured that if $\mathcal{A}$ is any integer sequence of positive (asymptotic) upper density, i.e.,

$$\overline{d}(\mathcal{A}) := \limsup_{n\to\infty} \frac{1}{n} \sum_{\substack{a\in\mathcal{A}\\ a\leq n}} 1 \ > 0,$$

then $\mathcal{A}$ contains arbitrarily long a.p.'s. Alternatively, one may state the conjecture as follows:

If there exists an l such that $\mathcal{A}$ contains
no l terms in an a.p., then $d(\mathcal{A}) = 0$.

For $l = 3$, this is due to Roth (1952). For $l \geq 4$, this is due to Szemerédi (1969, 1975) and Fürstenberg and Katznelson (1979) using ergodic theory . An alternate statement of Roth's theorem is as follows:

For every positive integers l and r, there exists a constant $n(l,r)$ such that if $n_0 \geq n(l,r)$ and $\{1,2,\cdots,n_0\} \subset \cup C_1 \cup C_2 \cup \cdots \cup C_r$, then some set C_i contains an arithmetic sequence of length l.

Gowers (1998) gave a proof of this statement, with an upper bound on $n(l,r)$, for the case $l = 4$ (mentioned in his Fields Medal citation; Lepowsky et al. 1999) which improves upon Szemeredi's result of (1975) .

2. Proof of roth's theorem

Let $M^{(l)}(n)$ denote the largest number of integers in $[1,n]$ having among them no l terms of arithmetic progression. Define

$$\mu^{(l)}(n) = \frac{M^{(l)}(n)}{n}.$$

We have, trivially,

$$M^{(l)}(n+m) \le M^{(l)}(n) + M^{(l)}(m). \tag{1}$$

Lemma 1. *For $n,\ m \in \mathbb{Z}$, we have the following:*

(a) *If $m \le n$, then $\mu^{(l)}(n) \le 2\mu^{(l)}(m)$.*
(b) *If $m|n$, then $\mu^{(l)}(n) \le \mu^{(l)}(m)$.*
(c) $\lim_{n\to\infty} \mu^{(l)}(n) = \mu^{(l)}$ *exists.*

Proof. (a) Suppose $m \le n$ and let $n = qm + r,\ 0 \le r < m,\ q \ge 1$. Applying the triangular inequality (1) repeatedly, we obtain

$$M^{(l)}(n) \ \le \ qM^{(l)}(m) + M^{(l)}(r) \ \le \ (q+1)M^{(l)}(m).$$

And now, dividing by $n = qm + r$,

$$\begin{aligned} \mu^{(l)}(n) \ &\le \ \frac{(q+1)m}{qm+r}\mu^{(l)}(m) = \mu^{(l)}(m) + \frac{m-r}{qm+r}\mu^{(l)}(m) \\ &\le \ \left(1+\frac{1}{q}\right)\ \mu^{(l)}(m). \end{aligned}$$

In particular, $\mu^{(l)}(n) \ \le \ 2\mu^{(l)}(m)$.

(b) If $m \mid n$, then $r = 0$, and this gives $\mu^{(l)}(n) \le \mu^{(l)}(m)$.

(c) Finally, keeping m fixed, let $n \to \infty$. Then $q \to \infty$ and we get from (b)

$$\limsup_{n\to\infty} \mu^{(l)}(n) \ \le \ \mu^{(l)}(m).$$

Now letting $m \to \infty$,

$$\limsup_{n\to\infty} \mu^{(l)}(n) \ \le \liminf_{m\to\infty} \mu^{(l)}(m).$$

□

We shall prove

Roth's Theorem. (1952)

$$\mu^{(3)} = 0.$$

More precisely,

$$\mu^{(3)} \ll \frac{1}{\log\log n}.$$

Remarks. (1) Szemerédi, Heath-Brown gave the estimate

$$\mu^{(3)}(n) \ll \frac{1}{(\log n)^{3/10}},$$

and for $l \ge 4$, that $\mu^{(l)} = 0$.

Write $\mu,\ \mu(n),\ M(n)$ for $\mu^{(3)},\ \mu^{(3)}(n)$, and $M^{(3)}(n)$ respectively from now on. Let $\mathcal{M}$ denote the maximal set in $[1,n]$ having no three terms in a.p. so that $|\mathcal{M}| = M(n)$. We observe that if $m_1,\ m_2$, and m_3 are any three elements of the set $\mathcal{M}$, then the diaphantine equation

$$m_1 + m_2 = 2m_3$$

has only the trivial solution $m_1 = m_2 = m_3$. So if we define $f(\alpha) = \sum_{m\in\mathcal{M}} e(m\alpha)$, then

$$\int_0^1 f(\alpha)^2 f(-2\alpha)\ d\alpha = M(n).$$

Write $f(\alpha) = \sum_{r=1}^{n} \kappa(r)e(\alpha r)$, where $\kappa(r)$ is the indicator function of $\mathcal{M}$. We attempt to approximate $f(\alpha)$ by means of

$$v(\alpha) = \mu(m)\sum_{r=1}^{n} e(\alpha r),$$

where $m \leq n$, are still to be chosen. Introduce the "error" function

$$E(\alpha) := v(\alpha) - f(\alpha) = \sum_{r=1}^{n} c(r)\ e(\alpha r),$$

where $c(r) = \mu(m) - \kappa(r)$. As a first step in showing that $E(\alpha)$ is small for suitably chosen m, we smooth $E(\alpha)$ by first multiplying by $F(\alpha q)$, where

$$F(\alpha) := \sum_{s=0}^{m-1} e(-\alpha s),$$

and $n\ >\ qm$. We have

$$F(\alpha q)E(\alpha) = \sum_{s=0}^{m-1}\sum_{r=1}^{n} c(r)\ e\left(\alpha(r-qs)\right)$$

and changing variable r to $r - qs = h$, we get

$$\begin{aligned} F(\alpha q)E(\alpha) &= \sum_{s=1}^{m-1}\ \sum_{h=1-qs}^{n-qs} c\left(h+qs\right)\ e(\alpha h) \\ &= \sum_{s=0}^{m-1}\sum_{h=1}^{n-qm} c\left(h+qs\right) e(\alpha h) - R(\alpha), \end{aligned}$$

where

$$|R(\alpha)| \leq q\ m\cdot m, \tag{2}$$

because we have omitted $qs + (qm - qs)$ terms, each ≤ 1, from the inner sum. Thus,

$$F(\alpha q)E(\alpha) = \sum_{h=1}^{n-qm} \sigma(h)e(\alpha h) - R(\alpha), \tag{3}$$

where

$$\sigma(h) = \sum_{s=0}^{m-1} c(h + qs).$$

Lemma 2. *If $qm < n$, then $\sigma(h) \geq 0$ for $h = 1, 2, \ldots, n - mq$.*

Proof. We have

$$\begin{aligned}
\sigma(h) &= \sum_{s=0}^{m-1} \{\mu(m) - \kappa(h + qs)\} \\
&= \mu(m)m - \sum_{s=0}^{m-1} \kappa(h + qs) \\
&= M(m) - \kappa,
\end{aligned}$$

say. Here κ is the number of elements of $\mathcal{M}$ among the integers

$$\{h, h + q, h + 2q, \cdots, h + (m - 1)q\}.$$

Let us write these as

$$\{h + qs_i,\ i = 1, 2, \ldots, \kappa\}.$$

Since no three of these are in a.p. the same is true of the set

$$\{s_i,\ i = 1, 2, \ldots, \kappa\}$$

and the same is true for

$$\{1 + s_i,\ i = 1, 2, \ldots, \kappa\}\ \subset [1, M].$$

But this tells us that $\kappa \leq M(m)$.

□

Lemma 3. *Suppose $n > 2m^2$. Then for every $\alpha \in \mathbb{R}$,*

$$|E(\alpha)| < \frac{\pi}{2}\, n\ (\mu(m) - \mu(n)) + 7m^2.$$

Proof. As usual, there exist a and q with $(a, q) = 1$, such that

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{2mq}, \quad 1 \leq q \leq 2m,$$

i.e., $\left|\alpha - \frac{a}{q}\right| \le \frac{1}{2m}$, and so $F(\alpha q) = F(\beta)$, where $\beta = \alpha q - a$. But

$$|F(\beta)| = \left|\frac{\sin(\pi\beta m)}{\sin(\pi\beta)}\right|.$$

Since $\pi|\beta| \le \frac{\pi}{2m}$, we have

$$|F(\beta)| \ \ge \ \frac{\sin(\pi|\beta|m)}{\pi|\beta|} \ \ge \ \frac{2}{\pi}\cdot\frac{\pi\beta m}{\pi\beta} = \frac{2m}{\pi}.$$

Hence

$$\begin{aligned}\frac{2m}{\pi}\ |E(\alpha)| \le \ |F(\alpha q)E(\alpha)| \ &\le \ \sum_{h=1}^{n-mq}\sigma(h) + |R(\alpha)| \\ &= F(0)E(0) + R(0) + |R(\alpha)|.\end{aligned}$$

Whence

$$\begin{aligned}|E(\alpha)| &\le \ \frac{\pi}{2m}\left\{mE(0) + 2qm^2\right\} \\ &= \frac{\pi}{2}\ E(0) + \pi q m,\end{aligned}$$

and

$$\begin{aligned}E(0) &= v(0) - f(0) = n\mu(m) - M(m) \\ &= n\left(\mu(m) - \mu(n)\right).\end{aligned}$$

Therefore,

$$|E(\alpha)| \le \ \frac{\pi}{2}\ m\left(\mu(m) - \mu(n)\right) + \pi q m \ \le \ \frac{\pi}{2}\ m\left(\mu(m) - \mu(n)\right) + 7m^2.$$

□

Recall that

$$M(n) = \int_0^1 f^2(\alpha) f(-2\alpha)\ d\alpha$$

and we now write this as

$$\begin{aligned}M(n) &= \int_0^1 f^2(\alpha)v(-2\alpha)\ d\alpha - \int_0^1 f^2(\alpha)E(-2\alpha)\ d\alpha \\ &= I - \int_0^1 f^2(\alpha)E(-2\alpha)\ d\alpha,\end{aligned}$$

say. Now,

$$\begin{aligned}I &= \mu(m)\int_0^1 \left(\sum_{a\in\mathcal{M}} e(\alpha a)\right)^2 \sum_{r=1}^{n} e(-2\alpha r) d\alpha \\ &= \mu(m)\ \sum_{a\in\mathcal{M}}\ \sum_{b\in\mathcal{M}}\sum_{r=1}^{n}\int_0^1 e\left(\alpha(a+b-2r)\right)\ d\alpha,\end{aligned}$$

where the inner-most integral is

$$= \begin{cases} 1, & a+b \equiv 0 \mod 2 \\ 0, & \text{otherwise,} \end{cases}$$

and hence,

$$I \;=\; \mu(m) \sum_{\substack{a\in\mathcal{M},\ b\in\mathcal{M} \\ a+b\equiv 0 \mod 2}} 1 \;=\; \mu(m)(M_1^2+M_2^2),$$

where we let M_1 denote number of even elements in $\mathcal{M}$, and M_2 the number of odd elements in $\mathcal{M}$, so that $M_1+M_2 = M(n)$. But $M(n)^2(M_1+M_2)^2 \le 2(M_1^2+M_2^2)$, and so

$$I \;\ge\; \frac{\mu(m)}{2}\, M(n)^2.$$

Thus,

$$\begin{aligned} |M(n)-I| &\le \int_0^1 |f(\alpha)|^2\, |E(-2\alpha)|\ d\alpha \\ &\le \left\{\frac{\pi}{2}\, n\,(\mu(m)-\mu(n)) + 7m^2\right\} \int_0^1 |f(\alpha)|^2\ d\alpha \\ &= M(n)\ \left\{\frac{\pi}{2}\, n\,(\mu(m)-\mu(n)) + 7m^2\right\}, \end{aligned}$$

if n is greater than $2m^2$. On the other hand,

$$|M(n)-I| \ge I - M(n) \ge \frac{\mu(m)}{2}\, M(n)^2 \ - M(n)$$

so that

$$\frac{\mu(m)}{2}\, M(n)^2 - M(n) \le M(n) \left\{\frac{\pi}{2} n\,(\mu(m)-\mu(n)) + 7m^2\right\},$$

and

$$\frac{\mu(m)}{2}\, M(n)^2 \le 1 + \frac{\pi}{2} n\,(\mu(m)-\mu(n)) + 7m^2,$$

and therefore,

$$\mu(m)\mu(n) \;\le\; \pi\,(\mu(m)-\mu(n)) + \frac{16m^2}{n}, \quad 2m^2 < n. \tag{4}$$

Letting $n \to \infty$, while keeping m fixed,

$$\mu(m)\mu \le \pi(\mu(m)-\mu),$$

and letting $m \to \infty$, we arrive at $\mu^2 \le 0$, i.e., $\mu = 0$. This proves the weak form of Roth's theorem.

To prove the second assertion, we start from (4). Choose $n = 2^{3^k}$, $m = 2^{3^{k-1}}$. Then $m^3 = n$, and so $m^2/n = 1/m < 1/2$, if $k \ge 2$. For simplicity, write

$\lambda(k) = \mu(2^{3^k})$. By Lemma 1 (b), we have $\lambda(k) \geq l(k-1)$. Now we rewrite the inequality (4),

$$\lambda(k-1)\lambda(k) \leq \pi(\lambda(k-1) - \lambda(k)) + \frac{16}{2^{3^{k-1}}}$$

or

$$1 \leq \pi\left(\frac{1}{\lambda(k)} - \frac{1}{\lambda(k-1)}\right) + \frac{16}{2^{3^{k-1}}} \cdot \frac{1}{\lambda(k)^2}.$$

Sum this inequality from $k = l+1$ to $k = 2l$ to get

$$l \leq \pi\left(\frac{1}{\lambda(2l)} - \frac{1}{\lambda(1)}\right) + 16 \sum_{k=l+1}^{2l} \frac{1}{2^{3^{k-1}}\lambda(k)^2},$$

or

$$l \leq \frac{\pi}{\lambda(2l)} + 16\, \frac{l}{2^{3^l}\lambda(2l)^2},$$

or

$$\lambda(2l) \leq \frac{\pi}{\lambda(2l)} \leq \frac{\pi}{l} + \frac{16}{2^{3^l}\lambda(2l)}.$$

If $\lambda(2l) \leq \frac{1}{l}$, we are done. If not, then

$$\lambda(2l) \leq \frac{\pi}{l} + \frac{16l}{2^{3^l}}.$$

But

$$\frac{16l}{2^{3^l}} \leq \frac{1}{2l}$$

if $2 \cdot 16l^2 \leq 2^{3^l}$, and this is true for $l \geq 2$. Therefore, in any case $\lambda(2l) \leq 4/l$, and thus $\lambda(2l) \leq 8/(2l)$ for $l \geq 2$, i.e., $\lambda(l) \leq 8/l,\ l \geq 4$. Finally, suppose n satisfies

$$2^{3^l} \leq n < 2^{3^{l+1}}, \quad 3^l \leq \frac{\log n}{\log 2} < 3^{l+1}.$$

Then if $m \leq n$, $\mu(n) \leq 2\mu(m)$, so

$$\mu(n) \leq 2\mu(m) = 2\mu(2^{3^l}) = 2\lambda(l) \leq \frac{16}{l}.$$

Since

$$l \leq \frac{\log\left(\frac{\log n}{\log 2}\right)}{\log 3} < l+1,$$

we have

$$\begin{aligned}\mu(n) &\leq \frac{16}{n} \\ &\leq \frac{16}{\frac{\log\left(\frac{\log n}{\log 2}\right)}{\log 3} - 1} \leq \frac{16}{\log\left(\frac{\log n}{\log 2}\right) - 1} \\ &= \frac{16}{\log(\log n) - \log\log 2 - 1} \leq \frac{2 \cdot 16}{\log\log n},\end{aligned}$$

if $n \geq n_0$. Therefore, we have the asserted upper bound

$$\mu(n) \ll \frac{1}{\log\log n} .$$