

ROTH'S THEOREM ON ARITHMETIC PROGRESSIONS

ADAM LOTT

ABSTRACT. The goal of this paper is to present a self-contained exposition of Roth's

Remark 1.2. *Lower density can be defined in the same way, with \liminf replacing \limsup*

For the remainder of the paper, we focus our attention on Roth's original theorem.

Theorem 1.3 (Roth). *Let A be a subset of \mathbb{Z} with positive upper density. Then A contains a three term arithmetic progression.*

The theorem is often phrased in the following equivalent form, which is easier to work with.

Theorem 1.4 (Roth, finitary form). *For every $\epsilon > 0$, there exists an $N_0(\epsilon)$ such that for every $N \geq N_0$ and every $A \subseteq \{1, 2, \dots, N\}$ with $\#A \geq \epsilon N$, A contains a three term arithmetic progression.*

1.2. **Notation.** We denote by \mathbb{Z}_N the additive cyclic group $\mathbb{Z}/N\mathbb{Z}$. Throughout the paper, we identify sets with their characteristic functions in the sense that for any set S , we define the function $S(x) := 1$ if $x \in S$ and $S(x) := 0$ if

(b) *Pointwise estimate.* For any $m \in \mathbb{Z}_N$, we have

$$|f(m)| \leq N^{-1} \sum_{x \in \mathbb{Z}_N} |f(x)|. \quad (2.6)$$

(c) *Plancherel's identity.*

$$\sum_{m \in \mathbb{Z}_N} |f(m)|^2 = N^{-1} \sum_{x \in \mathbb{Z}_N} |f(x)|^2. \quad (2.7)$$

(d) *Convolution identity.* For $f, g : \mathbb{Z}_N \rightarrow \mathbb{C}$, define the convolution

$$(f * g)(x) := \sum_{y \in \mathbb{Z}_N} f(y)g(x - y). \quad (2.8)$$

Then for any m ,

$$(f * g)(m) = Nf(m)g(m). \quad (2.9)$$

Proof.

(a) We have, by Proposition 2.1,

$$\sum_m (xm)f(m) = N^{-1} \sum_{m,y} (xm) (-ym)f(y) \quad (2.10)$$

$$= N^{-1} \sum_y f(y) \sum_m (m(x - y)) \quad (2.11)$$

$$= f(x). \quad (2.12)$$

(b) By the triangle inequality,

$$\sum_x |f(m)| \leq N^{-1} \sum_x |(-xm)f(x)| = N^{-1} \sum_x |f(x)|. \quad (2.13)$$

(c) We have

$$\sum_m |f(m)|^2 = N^{-2} \sum_{m,x,y} (-xm)f(x) \overline{(-ym)f(y)} \quad (2.14)$$

$$= N^{-2} \sum_{x,y} f(x) \overline{f(y)} \sum_m (m(y - x)) \quad (2.15)$$

$$= N^{-1}$$

$$= Nf(m)g(m). \quad (2.21)$$

3. PROOF OF ROTH'S THEOREM

The general strategy of the proof is as follows. If the Fourier coefficients $|A(m)|$ are small for all $m \neq 0$

$$= N^{-1}(\#B)^2(\#A) + N^2 \sum_{m=0} B(m)B(-2m)A(m) \quad (3.6)$$

$$= N^{-1}(\#B)^2(\#A) + E. \quad (3.7)$$

At this point, we may assume that $\#B \leq \#A/5$. If this is not the case, then either $A \subset [0, N/3]$ or $A \subset [2N/3, N-1]$ must have size at least $2(\#A)/5$ and hence has relative density at least $6/5 > 1$ in its ambient progression. Thus the density increment argument kicks in (i.e., we may replace A by $A \cap [0, N/3]$ and $[N]$ by $[N/3]$ and repeat the same argument).

3.1. Small Fourier coefficients. When all of the nonzero Fourier coefficients $|A(m)|$ are small, we can use (3.7) to establish the existence of a three-term progression directly.

Theorem 3.1. *If $|A(m)| < \epsilon^2/10$ for all $m \neq 0$, then A contains a three term arithmetic progression.*

Proof. We prove this by showing that the error term E in (3.7) is small. By the Cauchy-Schwartz inequality and Plancherel's identity, we have

$$|E| \leq N^2 \max_m |A(m)|$$

3.2. **Large Fourier coefficients.** If A has a large Fourier coefficient, then the estimate given by (3.7) is not useful, so we must use the additional arithmetic information that the large Fourier coefficient encodes. In this section, it will be convenient to work with the so-called balanced function $f(x) := A(x) - \frac{\#A}{N}$. We quickly describe the important properties of f .

Proposition 3.2. *The balanced function f possesses the following properties.*

- (a) $\sum_x f(x) = 0$.
- (b) $f(m) = A(m)$ for all $m = 0$ and $f(0) = 0$.

Proof. We have

$$f(x) = A(x) - \frac{\#A}{N} = 0$$

and

$$f(m) = A(m) - \frac{\#A}{N} \quad (-mx)f(x) = N^{-1} \sum_x (-mx)A(x) - \frac{\#A}{N} \sum_x (-mx)$$

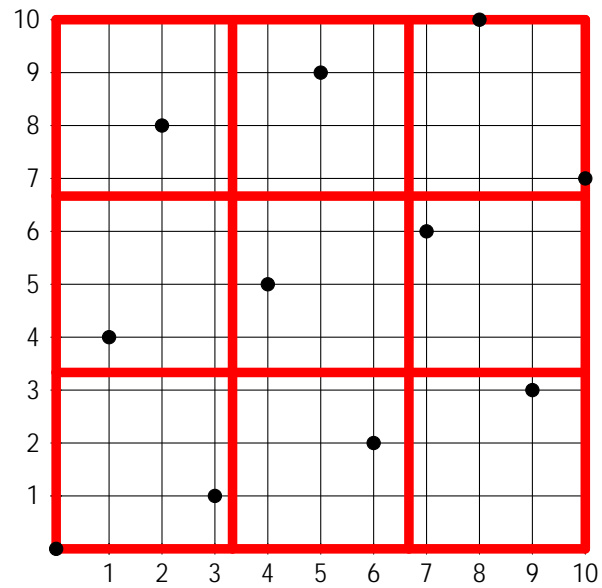


FIGURE 1. An example of the above construction with $N = 11$, $r = 4$, $\overline{N-1} = 3$. Notice that there are two points in the bottom left and top right boxes.

Let $d = p - q$. Let P be the progression $\{\dots, -d, 0, d, 2d, \dots\}$.

balanced function of A . Note that G has mean value zero because

$$G(x) = \frac{1}{x} \sum_{x,y} f(y)P(x-y) = \frac{1}{y} \sum_{x,y} f(y)P(x-y) = \frac{1}{y} (\#P) f(y) = 0. \quad (3.20)$$

3.3. Completing the proof via density increment argument. Suppose A is a subset of $[N]$ containing no 3APs. By Theorem 3.1, this implies that for some $r = 0$, $|A(r)| \geq \delta^2/10$. Then by Theorem 3.3 with $\delta = \delta^2/10$, there exists an arithmetic progression P_1 such that $\#P_1 \geq (\delta^2/640) \overline{N}$ and $\#(A \cap P_1) \geq (\delta + \delta^2/80)(\#P_1)$. Let $A_1 = A \cap P_1$

Proof. We have

$$|G(a)|^2 = \sum_{x,y \in \mathbb{Z}_p} (ax^2) \overline{(ay^2)} = \sum_{x,y \in \mathbb{Z}_p} (a(x^2 - y^2)). \quad (4.14)$$

The change of variables $t = x - y$, $u = x + y$ is bijective and $tu = x^2 - y^2$, so we have

$$|G(a)|^2 = \sum_{t,u \in \mathbb{Z}_p} (atu) \quad (4.15)$$

$$= \sum_{r \in \mathbb{Z}_p} \sum_{\substack{t,u \\ tu=r}} (ar) \quad (4.16)$$

$$= \sum_{r \in \mathbb{Z}_p} (ar)m(r) \quad (4.17)$$

where $m(r) := \#\{(t, u) \in \mathbb{Z}_p^2 : tu = r\}$. We know $tu = 0$ if and only if $t = 0$ or $u = 0$, so $m(0) = 2p - 1$. If $r \neq 0$, then t can be any nonzero element and u is determined, so $m(r) = p - 1$. Hence

$$|G(a)$$

Since $\#E_p = (p + 1)/2$, we have

$$p^{-1} \text{ ———}$$

$$= N^{-3} \sum_{\substack{a,b,c,d \\ a+d=b+c}} f(a)f(d)$$

$$= N^{-3} \sum_{x, h_1, h_2} (f(x) + f(x + h_1) + f(x + h_2))$$

$$N^{1/2} \int_y f(y) \int_z |f(z)|^2 \int_x f(x-y) f(x-z) \int_z f(x-y) f(x-z) \quad (5.27)$$

$$N^{1/2} N^{1/2} \int_y f(y) \int_{x,z,t} f(x-y) f(x-z) f(t-y) f(t-z) \quad (5.28)$$

$$N^{3/4} \int_y |f(y)|^2 \int_{x,z,t} f(x-y) f(x-z) f(t-y) f(t-z) \quad (5.29)$$

$$N^{3/4} N^{1/4} \int_{x,y,z,t} f(x-y) f(x-z) f(t-y) f(t-z) \quad (5.30)$$

$$= N \int_{a+b=c+d} f(a) f(b) f(c) f(d)$$

[Sz1] E. Szemerédi.