Notes on Roth’s Theorem

Jacques Verstraëte
Department of Mathematics
University of California, San Diego
La Jolla, CA, 92093.
E-mail: jacques@ucsd.edu.

1 Introduction

This is a simple exposition of Roth’s Theorem stating that a set of positive density has a three-term arithmetic progression. For convenience, a three-ap consists of distinct integers $a, b, c$ such that $a + b = 2c$. Let $r(N)$ denote the maximum size of a set $A \subset [N]$ containing no three-ap. A construction of Behrend (1946) shows for some $c > 0$ that

$$r(N) \gg \frac{N}{e^{c\sqrt{\log N}}}$$

whereas Roth’s Theorem (1952) shows $r(N) \ll N / \log \log N$ for some $C > 0$. While Behrend’s construction remains the densest known construction of a set in $[N]$ with no three-ap, Roth’s Theorem has been improved, culminating in the current record due to Bourgain (1999) giving

$$r(N) \ll \frac{N \sqrt{\log \log N}}{\sqrt{\log N}}.$$ 

It seems that the current methods available are unable to determine arithmetic progressions in the primes based purely on density considerations.

2 Behrend’s Construction

2.1 Using $p$-adic expansion

One way to construct a dense set with no three-aps is to fix a positive integer $p$ and to consider all integers of the form

$$f(a_1, a_2, \ldots, a_r) = a_1 + a_2 p + \cdots + a_r p^r$$
with the property that each \( a_i \) comes from a set which has no three ap in \( \mathbb{Z}_p \) and in addition \( 0 \leq a_i < p/2 \). This is the \( p \)-adic expansion of integers in a set \( A \subset [N] \) where

\[
N = \sum_{i=0}^{r} (p-1)p^i = p^{r+1} - 1.
\]

For then

\[
f(a_1, a_2, \ldots, a_r) + f(b_1, b_2, \ldots, b_r) = 2f(c_1, c_2, \ldots, c_r)
\]

implies \( a_i + b_i = 2c_i \) in \( \mathbb{Z}_p \) for all \( i : 1 \leq i \leq r \), but the choice of the \( a_i, b_i, c_i < p/2 \) means \( a_i = b_i = c_i \) and therefore \( f(a) = f(b) = f(c) \). On a Putnam exam, students were asked to construct a long three-ap in [2006], and this is achieved by taking \( p = 3 \) in the above construction, which gives a set of size roughly \( N^{\log_3 2} \). The function \( f \) is a special example of what is known as a Freiman homomorphism. Behrend’s construction has a similar flavor.

### 2.2 Details of Behrend’s construction

To describe Behrend’s construction, let \( X_s \) denote the sphere of radius \( s \) in \( d \)-dimensional Euclidean space. This comprises all vectors \( (x_1, x_2, \ldots, x_d) \) whose sum of squares is \( s^2 \). Let \( Y = [r]^d \) denote the portion of the \( d \)-dimensional integer lattice whose points have co-ordinates from \([r]\). Then

\[
\sum_{s^2 \in [d, dr^2]} |X_s \cap Y| = r^d.
\]

By the pigeonhole principle, there exists \( s^2 \in [d, dr^2] \) such that

\[
|X_s \cap Y| \geq \frac{1}{d} r^{d-2}.
\]

Let \( X = X_s \cap Y \). Consider the map \( \phi : Y \mapsto \mathbb{Z} \) defined by

\[
\phi(x_1, x_2, \ldots, x_d) = x_1 + x_2(2r + 1) + \cdots + x_d(2r + 1)^{d-1}.
\]

Let \( A = \phi(X) \). Then \( \phi \) constitutes the \((2r + 1)\)-adic representation of the elements of \( A \) and \( A \subset [N] \) where

\[
N = \max_{x \in X} \phi(x) < (2r + 1)^d.
\]

Since the \((2r + 1)\)-adic representation of any integer is unique, \( \phi \) is a bijection and \(|A| = |X|\). The second reason for considering the \((2r + 1)\)-adic representation is that \( \phi^{-1}(2c) = 2\phi^{-1}(c) \) for \( c \in A \) so if \( a + b = 2c \) with \( a, b, c \in A \) then \( x + y = 2z \) for some
$x, y, z \in X$, and this is impossible unless $x = y = z$, by the triangle inequality. Finally we note

$$|A| \geq \frac{1}{d} r^{d-2} \gg \frac{1}{d^2} N^{1-2/d}.$$  

Selecting $d = \sqrt{2 \log_2 N}$ so that $N^{2/d}$ is roughly $2^d$, we easily obtain

$$|A| \gg \frac{N}{e^{2\sqrt{\log N}}}.$$  

The constant 2 can be improved a bit, but the exponent of order $\sqrt{\log N}$ seems to be a barrier in this construction. In fact, Szemerédi (personal communication) believes that this construction might represent the true order of magnitude of $r(N)$.

3 Roth’s Theorem

It is convenient in what follows to refer to an arithmetic progression modulo $N$ as a $\mathbb{Z}_N$-progression and an arithmetic progression in $\mathbb{Z}$ as a $\mathbb{Z}$-progression. The density of $A$ on a finite set $S$ is defined by $|A|/|S|$.

Roth’s Theorem. Any set of density at least $800/\sqrt{\log \log N}$ in $[N]$ has a three-ap.

There are two basic ingredients one can identify in the proof of Roth’s Theorem, which are a prototype for many other theorems on the density of sets of integers without certain arithmetic configurations. We treat a set $A \subset [N]$ is a subset of $\mathbb{Z}_N$. The idea is to show that if $A$ has no three-ap, then $A$ is biased on a $\mathbb{Z}$-progression $P$ of length about $N^{1/2}$ – in the sense that $A$ has significantly increased density on $P$. Since $P$ is affinely equivalent to $[N]$ – a three-ap in $A \cap P$ is a three-ap in $A$ – we can repeat the argument and pass to a $\mathbb{Z}$-progression of length roughly $N^{1/4}$ in $P$ on which $A$ is biased. Repeating the argument again, if the density of $A$ reaches 1 in less than about $\log_2 \log_2 N$ steps, then we have found a $\mathbb{Z}$-progression $P$ with $|P| > 2$ and $|A \cap P| = |P|$, giving a three-ap in $A$.

3.1 A large Fourier coefficient

It is typical in discrete Fourier analysis to use the absence of an arithmetic structure in a set to show that the Fourier transform of the characteristic function of the set has an unusually large value. Here, unusually large can be quantified by looking at the transform of a random set with the same density. More precisely, let $A$ denote the
Fourier transform of the characteristic function of a set \( A \subset \mathbb{Z}_N \). To find the progression \( P \) promised before relies on showing that \( A \) has a large Fourier coefficient if \( A \) has no three-ap:

**Lemma 1** Let \( A, B \subset \mathbb{Z}_N \) with \( |A| = \alpha N \) and \( |B| = \beta N \). If there is no three-ap across \( A \times B \times B \), then for some \( r \neq 0 \),

\[
|\hat{A}(r)| > \alpha \beta N - 1.
\]

**Proof.** The number of three-aps across \( A \times B \times B \) is exactly

\[
\frac{1}{N} \sum_{r \in \mathbb{Z}_N} \sum_{a,b,c \in \mathbb{Z}_N} A(a)B(b)B(c)\omega^{r(a+b-2c)} - |B|.
\]

Using the inverse formula, this is zero if

\[
\sum_{r \in \mathbb{Z}_N} \hat{A}(r)\hat{B}(r)\hat{B}(-2r) = \beta N^2.
\]

The first term of the sum is \( \alpha \beta^2 N^3 \). Therefore we obtain using the triangle inequality that

\[
\alpha \beta^2 N^3 - \beta N^2 \leq \max_{r \neq 0} |\hat{A}(r)| \sum_{r \neq 0} |\hat{B}(-2r)||\hat{B}(r)|.
\]

Applying Cauchy-Schwarz and then Parseval’s Identity to the sum,

\[
\sum_{r \neq 0} |\hat{B}(-2r)||\hat{B}(r)| < \beta N^2.
\]

Therefore

\[
|\hat{A}(r)| > \alpha \beta N - 1.
\]

This completes the proof.

This lemma actually gives a lot more: it says that if there are not at least quadratically many three-aps across \( A \times B \times B \) – which is what we would expect if the sets were random sets with the same density – then \( A \) must have a large Fourier coefficient.

### 3.2 Bias on a long progression

Using Lemma 1, we find a long \( \mathbb{Z}_N \)-progression \( P \subset \mathbb{Z}_N \) on which \( A \) has increased density in the following manner.
Lemma 2 Let $\alpha > 0$ and let $A \subset \mathbb{Z}_N$ have density $\alpha$ and $|\hat{A}(r)| \geq 3\gamma N$ for some $r \neq 0$. Then there is a $\mathbb{Z}_N$-progression $P$ with $|P| \geq \gamma N$ and $|A \cap P| \geq (\alpha + \gamma)|P|$.

Proof. For convenience, assume $n = 1/\gamma$ is an integer. Rather than working with $B(x)$ we work with $f(x) = A(x) - \alpha$. This is convenient since $\sum_{x \in \mathbb{Z}_N} f(x) = 0$ and $\hat{f} \equiv \hat{A}$.

Cut the unit circle in the complex plane into arcs $I_1, I_2, \ldots, I_n$ of equal lengths, and define the progressions $P_k = \{x \in \mathbb{Z}_N : \omega^{rx} \in I_k\}$ for $k \in [n]$. Note these are actually progressions, since $r$ is relatively prime to $N$, and so the progressions all have common difference $r^{-1}$. We claim that some $P_k$ is the required arithmetic progression. We have by the triangle inequality

$$3\gamma N \leq |\hat{f}(r)| \leq \sum_{k=1}^{n} \sum_{x \in P_k} |f(x)\omega^{rx}|.$$ 

Writing

$$\omega^{rx} = \omega^{rx} - \omega^{rx_k} + \omega^{rx_k}$$

where $x_k \in P_k$ is arbitrary, and noting $|\omega^{rx} - \omega^{rx_k}| \leq \gamma$ for all $x \in P_k$, we get

$$2\gamma N \leq \sum_{k=1}^{n} \sum_{x \in P_k} |f(x)|.$$ 

By the pigeonhole principle, there exists $k$ such that

$$\sum_{x \in P_k} f(x) \geq \gamma|P_k|$$

which is to say $|A \cap P_k| \geq (\alpha + \gamma)|P_k|$. Then $P = P_k$ is the required progression. \hfill \blacksquare

Note that the progression $P$ produced by the last lemma is in general not affinely equivalent to $[N]$, so the above lemma is not enough for the iterative approach to Roth’s Theorem. We have to find a long $\mathbb{Z}$-progression in $P$ on which $A$ has increased density, and this is achieved as follows:

Lemma 3 Let $P$ be a $\mathbb{Z}_N$-progression and suppose $A \subset \mathbb{Z}_N$ satisfies $|A \cap P| \geq \delta|P|$. Then there exists a $\mathbb{Z}$-progression $Q \subset P$ with $|Q| > 0.01\delta^2|P|^{1/2}$ such that

$$|A \cap Q| \geq \delta(1 - 0.05\delta)|Q|.$$ 

Proof. It is straightforward to see that $P$ has a partition into at most $3|P|^{1/2}$ $\mathbb{Z}$-progressions. Remove from $P$ the union of all the $\mathbb{Z}$-progressions of length less than $0.01\delta^2|P|^{1/2}$, so that we are left with a collection of $\mathbb{Z}$-progressions of length at least $0.01\delta^2|P|^{1/2}$ on which the average density of $A$ is at least $\delta - 0.03\delta^2 > \delta - 0.05\delta^2$. It follows that at least one of these $\mathbb{Z}$-progressions $Q$ satisfies the requirements of the lemma. \hfill \blacksquare
3.3 An iterated function

The proof of the following little lemma is left as an exercise. Here we write $f^k$ to denote the $k$-fold iterate of a function $f$, where $k \in \mathbb{N}$.

**Lemma 4** Let $\alpha, c \in (0, 1)$ and let $f(\alpha) = \alpha(1 + c\alpha)$. If $k \leq \lceil 2/c\alpha \rceil$, then

$$f^k(\alpha) > 1.$$ 

3.4 Proof of Roth’s Theorem

By the distribution of primes, it is enough to prove $r(N) \leq 400N/\log \log N$ when $N$ is prime. Suppose $A = A_0 \subset [N]$ has density $\alpha = 4000/\log \log N$. We show that if $A$ contains no three-ap, then there is a $\mathbb{Z}$-progression $Q \subset [N]$ such that $|Q| \geq 0.0001\alpha^3N^{1/2}$ and

$$|A \cap Q| \geq f(\alpha)|Q|$$

where $f(\alpha) = \alpha(1 + 0.01\alpha)$. Since $Q$ is affinely equivalent to $[N]$, we can repeat the argument in $Q$. By the last lemma, after $k = \lceil 200/\alpha \rceil$ repetitions, we obtain a $\mathbb{Z}$-progression $Q_k$ such that $|A \cap Q_k| \geq f^k(\alpha)|Q_k| > |Q_k|$, which is a contradiction provided $Q_k$ is non-empty. Now $Q_k$ is non-empty, since we calculate

$$|Q_k| > (0.01\alpha)^6N^{1/2k} > (\log \log N)^{-6e^{\sqrt{\log N}}}.$$ 

We now show how to find $Q$. We may assume $B = A \cap (N/3, 2N/3)$ has $|B| \geq 0.32\alpha N$ otherwise $Q = [0, N/3]$ or $Q = [2N/3, N]$ is the required $\mathbb{Z}$-progression, where $A$ has relative density at least $f(\alpha)$ with room to spare. Applying the first lemma to $B$, and noting that a three-ap across $A \times B \times B$ is a three-ap in the integers, for some $r \neq 0$ we obtain

$$|\hat{A}(r)| > 0.31\alpha^2N - 1 > 0.3\alpha^2N$$

since $N$ is sufficiently large. By Lemma 2 and Lemma 3, with the appropriate parameters $\gamma$ and $\delta$, pass to a $\mathbb{Z}$-progression $Q$ such that

$$|Q| \geq 0.0001\alpha^3N^{1/2} \quad \text{and} \quad |A \cap Q| \geq f(\alpha)|Q|.$$ 

Thus $Q$ is the progression we required.
4 The genus of an equation

We might ask how dense a set can we have in $[N]$ with no non-trivial solutions to

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0$$

where $a_i \in \mathbb{Z}$ are constants. It is important to define what the word non-trivial means.

We discuss the case where the sum of the $a_i$ is zero, which includes the case of arithmetic progressions. A zero-sum partition of $\{1, 2, \ldots, k\}$ is a partition $(P_1, P_2, \ldots, P_r)$ such that for every $s \in [r], \sum_{i \in P_s} a_i = 0$. A solution $(x_1, x_2, \ldots, x_k)$ to the equation above is trivial if there is a zero-sum partition $(P_1, P_2, \ldots, P_r)$ such that for every $s \in [r], \sum_{i \in P_s} x_i = 0$. Clearly, trivial solutions cannot be avoided in a non-empty set $A \subset [N]$ – for instance the solution with all $x_i$ equal is trivial and appears in every set. Ruzsa (1995) defines the genus of such an equation to be the size of the finest zero-sum partition. It is not hard to show that if $A \subset [N]$ has no non-trivial solutions to an equation of genus $\gamma$, then $|A| \ll N^{1/\gamma}$. Let $r_E(N)$ be the size of a largest set in $[N]$ with only trivial solutions to a given equation $E$. Ruzsa’s main question is to prove or disprove that

$$\lim_{N \to \infty} \frac{\log r_E(N)}{\log N} = \frac{1}{\gamma(E)}$$

where $\gamma(E)$ is the genus of equation $E$. This is open in most cases; Behrend’s construction clearly shows this holds when the equation represents a three-ap, and for certain other equations it is also known to hold. Perhaps the simplest open example is the equation

$$x_1 + 3x_2 = 2x_3 + 2x_4$$

which has genus 1. Roth’s Theorem can be adapted easily to show that a set in $[N]$ with no solution to that equation has size at most roughly $N/\log \log N$. It would be extremely remarkable if one could show that an upper bound of order $N^\theta$ holds with $\theta < 1$ as $N \to \infty$; Ruzsa asks specifically if there is a set of size $N^{1-o(1)}$ with no non-trivial solutions to that equation.