PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 3, March 2009, Pages 805–809
S 0002-9939(08)09594-4
Article electronically published on November 4, 2008

A NEW PROOF OF ROTH'S THEOREM ON ARITHMETIC PROGRESSIONS

ERNIE CROOT AND OLOF SISASK

(Communicated by Michael T. Lacey)

Abstract. We present a proof of Roth's theorem that follows a slightly different structure to the usual proofs, in that there is not much iteration. Although our proof works using a type of density increment argument (which is typical of most proofs of Roth's theorem), we do not pass to a progression related to the large Fourier coefficients of our set (as most other proofs of Roth do). Furthermore, in our proof, the density increment is achieved through an application of a quantitative version of Varnavides's theorem, which is perhaps unexpected.

1. Introduction

Given an integer $N \geqslant 1$, let $r_3(N)$ denote the size of any largest subset S of $[N] := \{1, ..., N\}$ for which there are no solutions to

$$x + y = 2z,\ x, y, z \in S,\ x \neq y;$$

in other words, S has no non-trivial three-term arithmetic progressions.

In the present paper we give a proof of Roth's theorem [4] that, although iterative, uses a more benign type of iteration than most proofs.

Theorem 1.1. *We have that* $r_3(N) = o(N)$.

Roughly, we achieve this by showing that $r_3(N)/N$ is asymptotically decreasing. We will do this by starting with a set $S \subseteq [N]$, $|S| = r_3(N)$, such that S has no three-term progressions, and then convolving it with a measure on a carefully chosen three-term arithmetic progression $\{0, x, 2x\}$. The set T where this convolution is positive will be significantly larger than S, yet will have very few three-term arithmetic progressions. We will thus be able to deduce, using a quantitative version of a theorem of Varnavides [8], that $r_3(N)/N$ is much smaller than $r_3(M)/M$ for some $M = (\log N)^{1/16-o(1)}$. It is easy to see that this implies that $r_3(N) = o(N)$. Alas, the upper bound that our method will produce for $r_3(N)$ is quite poor and is of the quality $r_3(N) \ll N/\log_*(N)$, which nonetheless is the sort of bound produced by the "triangle-deletion" proof of Roth's theorem [5].

Received by the editors January 17, 2008.
2000 *Mathematics Subject Classification.* Primary 05D99.
The first author was funded by NSF grant DMS-0500863.
The second author was funded by an EPSRC DTG through the University of Bristol, and he would like to thank the University of Cambridge for its kind hospitality while this work was carried out.

Many of the other proofs of Roth's theorem, in particular [1], [3], [6], and [7], make use of similar convolution ideas;[1] however, none of these methods convolve with such a short progression as ours (three terms only), and none use the result of Varnavides to achieve a density increment. Furthermore, it seems that our method can be generalized to any context where: (1) the number of three-term progressions in a set depends only on a small number of Fourier coefficients, and (2) one has a quantitative version of Varnavides's theorem. This might prove especially useful in certain contexts, because the particular sets on which our method achieves a density increment (via Varnavides) are unrelated to the particular additive characters where the Fourier transform of S is "large".[2]

2. Notation

We shall require a modicum of notation: given a function $f : \mathbb{F}_p \to [0,1]$, we write

$$\Lambda(f) := \mathbb{E}_{x,d\in\mathbb{F}_p} f(x)f(x+d)f(x+2d)$$

(where $\mathbb{E}$ represents an averaged sum; thus the $\mathbb{E}$ above represents $p^{-2}\sum$). Thus Λ gives an average of f over three-term arithmetic progressions; when f is the indicator function of a set A, this is just the number of progressions in A divided by p^2. We shall make use of the Fourier transform $\widehat{f} : \mathbb{F}_p \to \mathbb{C}$ of a function f, given by

$$\widehat{f}(r) := \mathbb{E}_{x\in\mathbb{F}_p} f(x)e^{2\pi i r x/p},$$

as well as the easily verified Parseval's identity

$$\sum_{r\in\mathbb{F}_p} |\widehat{f}(r)|^2 = \mathbb{E}_x |f(x)|^2.$$

It is also easy to check that

$$\Lambda(f) = \sum_{r\in\mathbb{F}_p} \widehat{f}(r)^2 \widehat{f}(-2r). \tag{2.1}$$

Given a set $T \subseteq \mathbb{F}_p$, we shall furthermore use the notation

$$\Lambda(T) \ := \ \Lambda(1_T).$$

Finally, the notation $\|t\|_{\mathbb{T}}$ will be used to denote the distance from t to the nearest integer.

3. Proof of Theorem 1.1

Let

$$\kappa := \limsup_{N\to\infty} r_3(N)/N.$$

We shall show that $\kappa = 0$, which will prove the theorem.

Let $N \geqslant 2$ be an integer, and then let p be a prime number satisfying

$$2N < p < 4N.$$

[1] In the case of Szemerédi's argument [7], the convolution is disguised, but after the dust has settled, one will see that he convolves with a measure on a very long arithmetic progression. In the case of [3] and [6], the arguments can be directly expressed in terms of convolution with a measure supported on a long arithmetic progression.

[2] That is, the progression to which we pass with each iteration is unrelated to the additive characters where $\widehat{1_S}$ is "large".

The fact that such a p exists is of course the content of Bertrand's postulate.

Let $S \subset [N]$ be a set free of three-term progressions with $|S| = r_3(N)$. Thinking of S as a subset of $\mathbb{F}_p$ in the obvious way, we shall write $f = 1_S : \mathbb{F}_p \to \{0, 1\}$ for the indicator function of S. Let

$$R := \{r \in \mathbb{F}_p : |\widehat{f}(r)| \geqslant (2 \log\log p / \log p)^{1/2}\}.$$

By Parseval's identity, this set of large Fourier coefficients cannot be too big; certainly,

$$|R| \leqslant \log p / 2 \log\log p.$$

We may therefore dilate these points of R to be contained in a short part of $\mathbb{F}_p$. Indeed, by Dirichlet's box principle there is an integer dilate x satisfying

$$0 < x < p^{1-1/(|R|+1)} \leqslant p/\log p,$$

such that for all $r \in R$ we have

$$\|xr/p\|_{\mathbb{T}} \leqslant p^{-1/(|R|+1)} \leqslant 1/\log p. \tag{3.1}$$

Taking such an x, define

$$B := \{0, x, 2x\},$$

and define h to be the normalised indicator function for B, given by

$$h(n) := p 1_B(n)/3.$$

Then convolve f with h to produce the new function

$$g(n) := (f * h)(n) = (f(n) + f(n - x) + f(n - 2x))/3.$$

Since

$$\widehat{f}(r) - \widehat{g}(r) = \widehat{f}(r)(1 - \widehat{h}(r)),$$

it is easy to check using (3.1) that for all $r \in \mathbb{F}_p$,

$$|\widehat{f}(r) - \widehat{g}(r)| \ll (\log\log p / \log p)^{1/2}.$$

From this, along with the Cauchy-Schwarz inequality, Parseval's identity, and equation (2.1), one can quickly deduce that

$$|\Lambda(f) - \Lambda(g)| \ll (\log\log p / \log p)^{1/2},$$

and therefore since $\Lambda(f) \ll 1/p$ (because S is free of three-term arithmetic progressions), we deduce

$$\Lambda(g) \ll (\log\log p / \log p)^{1/2}. \tag{3.2}$$

Define

$$T := \{n \in \mathbb{F}_p : g(n) > 0\},$$

and note that from (3.2), along with the obvious fact that $\Lambda(T) \ll \Lambda(g)$, we have

$$\Lambda(T) \ll (\log\log p / \log p)^{1/2}. \tag{3.3}$$

Furthermore, since S is free of three-term progressions even in $\mathbb{F}_p$, we must have that $g(n) \leqslant 2/3$ for all $n \in \mathbb{F}_p$. Thus $1_T(n) \geqslant 3g(n)/2$ for all n, immediately implying that $|T| \geqslant 3|S|/2$. The set T would thus serve our purposes if it were not for the fact that it is not necessarily contained in $[N]$. However, since $x \leqslant p/\log p$, we certainly have the inclusion $T \subset [N + 2p/\log p]$. So, if we let T' be those elements of T lying in $[N]$, then

$$|T'| = |T| - O(N/\log N) \text{ and } \Lambda(T') \leqslant \Lambda(T).$$

Hence, for N large enough,

$$|T'| \geqslant 4|S|/3$$

(unless of course $r_3(N) = O(N/\log N)$, but then we would be happy anyway).

We have now created a set T', significantly larger than S but with only a few more three-term progressions. The following lemma, a quantitative version of Varnavides's theorem, will help us make use of this information. The notation $T_3(X)$ denotes the number of three-term progressions $a, a+d, a+2d$ with $d \geqslant 1$ in a set X of integers.

Lemma 3.1. *For any $1 \leqslant M \leqslant N$, and for any set $A \subseteq [N]$, we have*

$$T_3(A) \geqslant \left(\frac{|A|/N - (r_3(M)+1)/M}{M^4}\right) N^2.$$

Before we prove this, let us see how we can use it to finish the proof of our main theorem. Set $M := \lfloor (\log p/\log\log p)^{1/16} \rfloor$ and apply the lemma to our set T' to obtain the estimate

$$\Lambda(T') \gg \frac{4|S|/3N - (r_3(M)+1)/M}{M^4}.$$

Comparing this to (3.3) (recalling that $\Lambda(T') \leqslant \Lambda(T)$), we conclude that

$$r_3(N)/N = |S|/N \leqslant 3r_3(M)/(4M) + O((\log\log N/\log N)^{1/4}).$$

Thus $r_3(N)/N$ is asymptotically decreasing to 0, whence $\kappa = 0$.

Proof of Lemma 3.1. The result will follow from an averaging procedure essentially contained in [2]. We include the proof here since our formulation is slightly different: we are working over $[N]$ rather than $\mathbb{F}_p$, and so we have to take into account the inhomogeneity of $[N]$.

Let k be a positive integer. Let $\mathcal{B}$ denote the collection of length M arithmetic progressions contained in $[N]$ with common difference at most k, and let $\mathcal{B}_d$ denote the subcollection consisting of such arithmetic progressions with common difference d. Throughout this proof we restrict ourselves to progressions with positive common difference.

We first claim that any 3AP (three-term arithmetic progression) in $[N]$ can occur in at most $M^2/4$ progressions in $\mathcal{B}$. To see this, note that if a 3AP has common difference d, then it can occur in at most $M-2$ progressions of length M with common difference d. Similarly, the 3AP can occur in at most $M - 2d/n$ M-APs with difference n provided n divides d and $n \geqslant 2d/(M-1)$, and in no other M-APs. Thus the 3AP can occur in no more than

$$\sum_{1 \leqslant m \leqslant (M-1)/2} (M-2m) \leqslant M^2/4$$

members of $\mathcal{B}$, as claimed. It follows immediately that

$$T_3(A) \geqslant \frac{4}{M^2} \sum_{B \in \mathcal{B}} T_3(A \cap B). \tag{3.4}$$

Now if B is an arithmetic progression of length M and $|A \cap B| > r_3(M)$, then by definition we have $T_3(A \cap B) \geqslant 1$. In view of (3.4) our aim shall therefore be to estimate the number of such sets B; we shall do this by looking at progressions of fixed common differences. Indeed, for a fixed common difference d, every element in the interval $I_d := [(M-1)d+1, N-(M-1)d]$ is contained in precisely M progressions in $\mathcal{B}_d$, and so

$$\sum_{B\in\mathcal{B}} |A\cap B| = \sum_{d\leqslant k}\sum_{a\in A}\sum_{B\in\mathcal{B}_d} 1_B(a) \geqslant M\sum_{d\leqslant k}|A\cap I_d|.$$

Since $|A\cap I_d| \geqslant |A| - 2(M-1)d$, this quantity is at least $Mk(|A|-2Mk)$. Now let $\mathcal{C}\subset\mathcal{B}$ be the set of progressions B for which $|A\cap B| > r_3(M)$. We then have

$$\sum_{B\in\mathcal{B}} |A\cap B| \leqslant M|\mathcal{C}| + r_3(M)|\mathcal{B}\setminus\mathcal{C}|,$$

from which it follows that

$$|\mathcal{C}| \geqslant k(|A|-2Mk) - |\mathcal{B}|r_3(M)/M.$$

Since $|\mathcal{B}_d| = N-(M-1)d$ for each d, the total number of progressions $|\mathcal{B}|$ is at most Nk. Choosing $k = \lfloor N/2M^2\rfloor$ we conclude that there must be at least

$$|\mathcal{C}| \geqslant \left(\frac{|A|/N - r_3(M)/M - 1/M}{4M^2}\right)N^2$$

sets B for which $|A\cap B| > r_3(M)$. The result thus follows from (3.4). $\square$

4. Acknowledgment

We would like to thank Ben Green for pointing out that we can take B to be a three-term progression for our argument; in a previous draft we took B to be a 20-term arithmetic progression, due to a small inefficiency in one part of our proof.

References

[1] J. Bourgain, *On triples in arithmetic progression*, Geom. and Funct. Anal. **9** (1999), 968-984. MR1726234 (2001h:11132)

[2] E. Croot, *The structure of critical sets for $\mathbb{F}_p$ arithmetic progressions*, preprint.

[3] D.R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. **35** (1987), 385-394. MR889362 (88g:11005)

[4] K.F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104-109. MR0051853 (14:536g)

[5] I. Z. Ruzsa and E. Szemerédi, *Triple systems with no six points carrying three triangles*, Combinatorics, Vol. II, pp. 939-945, Colloq. Math. Soc. János Bolyai, 18, North-Holland, Amsterdam-New York, 1978. MR519318 (80c:05116)

[6] E. Szemerédi, *An old new proof of Roth's theorem*, Montreal Conference Proceedings on Additive Combinatorics, CRM Proc. Lecture Notes, vol. 43, pp. 51–54, Amer. Math. Soc., Providence, RI, 2007. MR2359467

[7] ———, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. **56** (1990), 155-158. MR1100788 (92c:11100)

[8] P. Varnavides, *On certain sets of positive density*, J. London Math. Soc. **34** (1959), 358-360. MR0106865 (21:5595)

Department of Mathematics, Georgia Institute of Technology, 103 Skiles, Atlanta, Georgia 30332

E-mail address: `ecroot@math.gatech.edu`

Department of Mathematics, University of Bristol, Bristol BS8 1TW, England

E-mail address: `O.Sisask@dpmms.cam.ac.uk`