Mémoire de Master 2 Mathématiques

Roth's Theorem on Arithmetic Progressions

Ramdinmawia

Supervisor: Gautami Bhowmik, June 2011

Université des Sciences et Technologies de Lille 1
Laboratoire Paul Painlevé

Contents

1 The First Proof

1.1 Introduction

This method here is based on Iosevich [2].

Here the main idea revolves around the estimation of the Fourier coefficients of the characteristic function of a subset of $[1, N]$ assumed to contain no nontrivial arithmetic progressions.

1.2 Statement of the theorem and some definitions

We first make a formal statement of Roth's theorem.

Roth's Theorem: *If B is a subset of the positive integers of positive upper density, i.e., if*

$$\limsup_{n\to\infty} \frac{|B \cap [1, n]|}{n} > 0, \tag{1.2.1}$$

then B contains a nontrivial arithmetic progression of length 3.

Definition 1: A real-valued function f defined on a subset of the positive integers $\mathbb{N}$ will be called *subadditive* if

$$f(m + n) \leq f(m) + f(n)$$

for all m and n in the domain of f.

We have a useful lemma about subadditve functions on subsets of $\mathbb{N}$, called Fekete's Lemma, which we prove below for completeness.

Lemma 1. ***Fekete's Lemma:*** Let f be a subadditive function on the set of the positive integers. Then the limit

$$\lim_{n\to\infty} \frac{f(n)}{n}$$

exists and is equal to

$$\inf_{n\geq 1} \frac{f(n)}{n}.$$

Proof of Fekete's Lemma: Let us write

$$l := \inf_{n\geq 1} \frac{f(n)}{n};$$

let $\epsilon > 0$. There exists $K \in \mathbb{N}$ such that

$$|\frac{f(K)}{K} - l| < \frac{\epsilon}{2}.$$

Let L be large enough to guarantee that $\frac{f(r)}{KL} < \frac{\epsilon}{2}$ for $r < K$.
Let $n \geq KL$. Then there exist nonnegative integers q, r such that $n = Kq + r$, where $r < K$. Clearly $q \geq L$. Also

$$\begin{aligned} \frac{f(n)}{n} &\leq \frac{f(Kq)}{Kq+r} + \frac{f(r)}{Kq+r} \\ &\leq \frac{qf(K)}{Kq} + \frac{f(Kq)}{Kq} \\ &= \frac{f(K)}{K} + \frac{f(Kq)}{Kq} \\ &< l + \frac{\epsilon}{2} + \frac{\epsilon}{2} \\ &= l + \epsilon, \end{aligned}$$

which shows that $|\frac{f(n)}{n} - l| < \epsilon$ for $n \geq KL$; this means $l = \lim_{n\to\infty} \frac{f(n)}{n}$. ▲

Definition 2: Let n be a positive integer. We define $A(n)$ to be the largest number of integers that can be chosen from $\{1, ..., n\}$ such that no 3-term arithmetic progression is formed (as in the introduction).

We shall show the *subadditivity* of the function A:

$$A(m+n) \leq A(m) + A(n) \tag{1.2.2}$$

Suppose m and n are positive integers. Let $\{a_1, ..., a_k\}$ be a subset of $\{1, ..., m+n\}$ which does not contain any nontrivial arithmetic progression. Let $a_{i_1}, ..., a_{i_r}$ be those a_i which do not exceed m, and let $a_{j_1}, ..., a_{j_s}$ be those which exceed m, so that

$r + s = k$. Then $\{a_{i_1}, ..., a_{i_r}\}$ and $\{a_{j_1} - n, ..., a_{j_s} - n\}$ are respectively subsets of $\{1, ...m\}$ and $\{1, ..., n\}$ which do not contain any nontrivial arithmetic progressions (note that if a set $\{a, b, c, ...\}$ of integers does not contain any nontrivial 3-term arithmetic progressions, then the set $\{a + n, b + n, c + n, ...\}$ also does not contain any nontrivial 3-term arithmetic progressions). Hence

$$r \leq A(m)$$

and

$$s \leq A(n)$$

by definition of A. So

$$k = r + s \leq A(m) + A(n)$$

showing that

$$A(m + n) \leq A(m) + A(n). \blacktriangle$$

Therefore by Fekete's lemma, the limit

$$\lim_{n\to\infty} \frac{A(n)}{n}$$

exists, and is equal to $\inf_{n\geq 1} \frac{A(n)}{n}$. Call this limit l. Then obviously, $0 \leq l \leq \frac{A(n)}{n} < 1$ for all n.

1.3 One observation

It is easy to see that Roth's theorem will be true if we can prove that $l = 0$. Indeed, suppose $l = 0$. Let $\epsilon = \frac{1}{2}\delta^+(B)$ which is > 0 by assumption. Since

$$\delta^+(S) = \limsup_{n\to\infty} \frac{|B \cap [1, n]|}{n}$$

and$\epsilon > 0$ we can choose a positive integer N such that

$$\delta^+(B) < \frac{|B \cap [1, n]|}{n} + \epsilon.$$

for all $n \geq N$. This gives that $\Big|B \cap [1, n]\Big| > n\epsilon$ for $n \geq N$. As $l = 0$ we can find $n \geq N$ such that $A(n) < n\epsilon$.

Since $\Big|B \cap [1, n]\Big| > n\epsilon$ and $A(n) < n\epsilon$ we see that that $B \cap [1, n]$ and hence B must contain a nontrivial 3-term aritmetic progression. And this is what Roth's Theorem says.

So now what we have to prove is: $l = 0$.

1.4 Start of the proof

We suppose, by way of contradiction, that $l > 0$. Let $\epsilon := \frac{l^2}{25}$, which is a positive number.

Let m be big enough to guarantee that

$$l \leq \frac{A(n)}{n} < l + \epsilon \tag{1.4.1}$$

for all $n \geq 2m + 1$.

Let us choose $N \geq 2m + 1$(we shall restrict N later, in fact many times).

Now $[1, 2N]$ has a subset S with $|S| \geq 2lN$ which does not contain any 3- term arithmetic progression. Let T be the set of even elements of S, and let us write

$$S = \{u_1, ..., u_s\}$$

and

$$T = \{2v_1, ..., 2v_t\}$$

Observe that

$$l \leq \frac{s}{2N} < l + \epsilon \tag{1.4.2}$$

$$t \leq N(l + \epsilon) \tag{1.4.3}$$

and, since the number of odd integers in S does not exceed $A(N)$,

$$t \geq A(2N) - A(N) \geq 2lN - N(l + \epsilon) = N(l - \epsilon) \tag{1.4.4}$$

We consider the *Fourier sums*

$$\hat{S}(\alpha) := \Sigma_{u \in S} e(\alpha u)$$

and

$$\hat{T}(\alpha) := \Sigma_{2v \in T} e(\alpha v)$$

for any real α, where $e(x) := e^{2\pi i x}$ for real x. From Equation 1.2.1

Let the symbol $\int dx$ denote the sum over $x = 0, \frac{1}{2N}, ..., \frac{2N-1}{2N}$, so that, for example,

$$\int e(x)dx = \{^{2N,\ if\ x=0}_{0,\ otherwise} \tag{1.4.5}$$

From this it is easy to deduce that

$$\int \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha = 2Nt \tag{1.4.6}$$

since we assumed that S does not contain any nontrivial arithmetic progressions of length 3. Also

$$2Nt \leq 2NN(l+\epsilon) \leq 3lN^2 \tag{1.4.7}$$

Now,

$$\hat{S}(0)\hat{T}(0)^2 = st^2 \geq 2lNN^2(l-\epsilon)^2 \geq l^3N^3 \tag{1.4.8}$$

and

$$|\hat{S}(0)\hat{T}(0)^2 \leq |\int \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha| + |\int_{\alpha\neq 0} \hat{S}(\alpha)\hat{T}(-\alpha) d\alpha| \tag{1.4.9}$$

which gives

$$l^3N^3 \leq 3lN^3 + y \tag{1.4.10}$$

where y represents the second integral on the right of eqEquation 1.4.5. Suppose for the moment that

$$|\hat{S}(\alpha)| \leq 6\epsilon N \tag{1.4.11}$$

for $\alpha \neq 0$. Then one gets

$$\begin{aligned} y &\leq 6\epsilon N \int |\hat{T}(-\alpha)^2| d\alpha \\ &= 6\epsilon N \Sigma_{j,k} \int e(\alpha(v_j - v_k)) d\alpha \\ &= 6\epsilon N \cdot 2Nt \end{aligned}$$

$$\leq 6\epsilon N \cdot 3lN^2 = 18\epsilon lN^3 \tag{1.4.12}$$

whence, from inequality Equation 1.4.9,

$$l^3N^3 \leq 3lN^3 + 18\epsilon N^3$$

which gives

$$\frac{7l^2}{25} \leq \frac{3}{N}$$

which is untenable for large N, giving the required contradiction.

So it remains to prove Equation 1.4.11.

1.5 The main estimate

In this section, we carry out a proof of inequality Equation 1.4.11, which is the main estimate of this theorem.

To this end, let M denote the largest interger less than $\sqrt{N}$, and let α be any nonzero real number. By the rational approximation (discussed earlier) we can choose integers p and q with $1 \leq q \leq M$ such that $|\alpha - \frac{p}{q}| \leq \frac{1}{qM}$. Write $\beta := \alpha - \frac{p}{q}$, so $|\beta| \leq \frac{1}{qM}$.

Now we have the elementary inequality

$$|\frac{e(x)+e(-x)}{2} - 1| = |\cos(x) - 1| \leq \frac{x^2}{2} \tag{1.5.1}$$

We shall prove Equation 1.4.11 by using the triangle inequality, with the help of an 'intermediate term'. In fact, we employ the sum $\frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m}e(\alpha(u+jq))$ as the intermediate term and show that both $\frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m}e(\alpha(u+jq))$ and $\hat{S}(\alpha) - \frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m}e(\alpha(u+jq))$ are small, which would obviously help us conclude that $\hat{S}(\alpha)$ is also small, in view of the triangle inequality.

Now, by a sequence of simple calculations,

$$\begin{aligned}
|\hat{S}(\alpha) - \frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m}e(\alpha(u+jq))| &= |\Sigma_{u\in S}e(\alpha u) - \frac{1}{2m+1}\Sigma_{|j|\leq m}e(\alpha(u+jq)) \\
&= |\Sigma_{u\in S}\frac{1}{2m+1}\Sigma_{|j|\leq m}[e(\alpha(u+jq) - e(\alpha u)]| \\
&= |\Sigma_{u\in S}\frac{1}{2m+1}\Sigma_{|j|\leq m}[e(j\beta q) - 1]| \\
&\leq \frac{2}{2m+1}\Sigma_{u\in S}|\Sigma_{j=1}^{m}[\frac{e(j\beta q)+e(-j\beta q)}{2} - 1]| \\
&\leq \frac{2}{2m+1}\Sigma_{u\in S}\Sigma_{j=1}^{m}\frac{(j\beta q)^2}{2} \\
&= \frac{(\beta q)^2}{2m+1}|S|\frac{m(m+1)(2m+1)}{6} \\
&= |S|\frac{(\beta q)^2}{6}m(m+1) \\
&< \frac{(\beta mq)^2}{2}|S| \\
&\leq \frac{m^2|S|}{2M^2}
\end{aligned}$$

$$\leq \frac{m^2}{2M^2}N \tag{1.5.2}$$

and this bounds $\hat{S}(\alpha) - \frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m}e(\alpha(u+jq))|$. So our next task is to give an upper bound for $\frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m}e(\alpha(u+jq))|$. We claim that

$$|\frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m}e(\alpha(u+jq)| \leq 5\epsilon N \tag{1.5.3}$$

Now for any integer u with $0 \leq u \leq 2N-1$ let $W_u := \{u+jq : |j| \leq m\}$ calculated mod $2N$. Observe that

$$\Sigma_{u\in S}\Sigma_{|j|\leq m}e(\alpha(u+jq)) = \Sigma_{r=0}^{2N-1}e(\alpha r)|W_r \cap S| \tag{1.5.4}$$

Note that for $mq \leq u \leq 2N - mq$, W_u is an arithmetic progression of length $2m+1$ in $[1, 2N]$. Therefore, since by assumption S does not contain any 3-term arithmetic progression, we obtain

$$\frac{|S \cap W_u|}{2m+1} < l + \epsilon \tag{1.5.5}$$

so for these $2N - 2mq$ values of u we have

$$0 \leq V_u < \epsilon \tag{1.5.6}$$

where we have written $V_u := \frac{1}{2m+1}|S \cap W_u| - l$ for all u with $0 \leq u \leq 2N$. For the other $2mq$ values of u we trivially have

$$V_u \leq 1 \tag{1.5.7}$$

Since every $a \in S$ occurs in exactly $2m+1$ of the sets W_u we have

$$\Sigma_{r=0}^{2N-1}|S \cap W_r| = (2m+1)|S| \tag{1.5.8}$$

which implies that the average of the V_r is

$$\frac{1}{2N}\Sigma_{r=0}^{2N-1}V_r = \frac{|S|}{2N} - l$$

which is ≥ 0 as $|S| \geq 2lN$. Therefore we have

$$\begin{aligned}\Sigma_{r=0}^{2N-1}|V_r| &\leq 2\Sigma_{r:V_r\geq 0} V_r \\ &\leq 2((2N-2mq)\epsilon + 2mq) \\ &\leq 4\epsilon N + 4mq \\ &\leq 4\epsilon N + 4mM\end{aligned}$$

$$\leq 5\epsilon N \tag{1.5.9}$$

for large N. This proves Equation 1.5.3.

Given the inequalities eqEquation 1.5.2 and eq Equation 1.5.9, we can complete the proof as follows.

We have, by the triangle inequality,

$$|\hat{S}(\alpha)| \leq |\hat{S}(\alpha) - \frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m} e(\alpha(u+jq))| + |\frac{1}{2m+1}\Sigma_{u\in S}\Sigma_{|j|\leq m} e(\alpha(u+jq))|$$

$$\leq \frac{m^2}{2M^2}N + 5\epsilon N$$

$$\leq 6\epsilon N$$

for large enough N which proves Equation 1.4.11 and hence completes the proof. ■

2 Roth's 1953 Proof

2.1 Introduction

In this chapter we give an exposition of Roth's 1953 proof. In fact, this version is stronger than the one proved in chapter 1. The proof is also longer and needs a much more delicate argument.

2.2 Statement and some remarks about the function A

Roth's Theorem(1953) *Let* (as in the previous chapter) $A(x)$ *denote the greatest number of positive integers that can be chosen from the set* $[1, x]$ *so that no three of them forms an arithmetic progression. Then*

$$\frac{A(x)}{x} = O(\frac{1}{\log\log x}).$$

We write $a(x) := \frac{A(x)}{x}$ so that the theorem may also be stated as

$$a(x) = O(\frac{1}{\log\log x}). \tag{2.2.1}$$

We note that $A(x)$ also denotes the greatest number of integers that can be chosen from any arithmetic progression of length x without forming any 3-term arithmetic progression.

Now it is obvious that

$$\frac{1}{n} \leq a(n) \leq 1 \; \forall n \in \mathbb{N} \tag{2.2.2}$$

Also using eq Equation 1.2.2 repeatedly we have

$$A(mn) \leq mA(n), \; A(m) \leq A(([\frac{m}{n}] + 1)n) \leq \frac{m+n}{n} A(n)$$

which give

$$a(mn) \leq a(n) \tag{2.2.3}$$

and

$$a(m) \leq (1 + \frac{n}{m})a(n) \tag{2.2.4}$$

respectively, for all positive integers m and n.

2.3 Some basic results

Let, as in the first proof, $S := \{u_1, ..., u_s\}$ be a subset of $[1, N]$ which contains no nontrivial arithmetic progression of length three.

We again consider the *Fourier sum*

$$\hat{S}(\alpha) := \Sigma_{u \in S} e(\alpha u)$$

for any real α.

Using the *Dirichlet Box Principle* again, we can find integers n, q with $1 \leq q \leq \sqrt{N}$ such that, putting $\beta = \alpha - \frac{n}{q}$

$$|\beta| \leq \frac{1}{q\sqrt{N}}.$$

For any $m < N$ write

$$T_m(\alpha) := \frac{a(m)}{q} \{\Sigma_{j=1}^{q} e(\frac{jn}{q})\}\{\Sigma_{k=1}^{N} e(\beta k)\}$$

so that $T_m(\alpha) = 0$ if $q > 1$, since $\Sigma_{j=1}^{q} e(\frac{jn}{q}) = 0$ for $q > 1$.

Proposition: *We have the asymptotic inequality*

$$|\hat{S}(\alpha) - T_m(\alpha)| < Na(m) - s + O(m\sqrt{N}) \tag{2.3.1}$$

For this we first prove the relation

$$\hat{S}(\alpha) = \frac{1}{mq} \Sigma_{j=1}^{q} \Sigma_{k=1}^{N} \Sigma_{k \leq u < k+mq, u \equiv j (\mod q)} e(\alpha u) + O(mq) \tag{2.3.2}$$

To prove this, first note that there exist mq integers k satisfying $k \leq u < k + mq$ for fixed m, q and u. In fact the only integers k satisfying this relation are

$$u - mq + 1, u - mq + 2, ..., u - 1, u$$

Also, for $mq \leq u < N - mq$ all these mq integers k lie in $[1, N]$, i.e., for $mq \leq u < N - mq$ one has $1 \leq k \leq N$. Hence for these mq values of u, the coefficient of

$e(\alpha u)$ in (29) reduces to $\frac{mq}{mq} = 1$. For the other values of u, that is, for $u < mq$ or $u \geq N - mq$, which are at most $(mq-1)+(N-(N-mq-1)) = 2mq$ in number, the error term $O(mq)$ gives the required compensation. This proves the above relation Equation 2.3.2.

Now consider the relation Equation 2.3.2. In the inner sum in Equation 2.3.2 we can write $u = Qq + j$ for some integer Q, since $u \equiv j \bmod q$. So

$$\begin{aligned} e(\alpha u) &= e((\beta + \frac{n}{q})u) \\ &= e(\frac{n}{q}(Qq + j))e(\beta u) \\ &= e(nQ)e(\frac{jn}{q})e(\beta u) \end{aligned}$$

Since in the inner sum $k \leq u < k + mq$ we may also write u as $k + v$ where $0 \leq v < mq$. So we can further express $e(\alpha u)$ as

$$\begin{aligned} e(\alpha u) &= e(nQ)e(\frac{jn}{q})e(\beta(k + v)) \\ &= e(\frac{jn}{q})e(\beta k)(e(nQ)e(\beta v)) \\ &\leq e(\frac{jn}{q})e(\beta k)(1 + nQ|\beta|v) \end{aligned}$$

so that

$$e(\alpha u) = e(\frac{jn}{q})e(\beta k) + O(mq|\beta|).$$

Also, we know that the number of terms in the inner sum is at most $A(m)$, using the statement made immediately after eq Equation 2.2.1. Hence the number of terms may be written as $A(m) - D(j,k,m,q)$ where $D(j,k,m,q) \geq 0$ is an integer depending on j, k, m and q. Hence

$$\begin{aligned} \hat{S}(\alpha) &= \frac{1}{mq}\Sigma_{j=1}^{q}\Sigma_{k=1}^{N}\Sigma_{k\leq u<k+mq,u\equiv j(\mod q)}e(\alpha u) + O(mq) \\ &= \frac{1}{mq}\Sigma_{j=1}^{q}\Sigma_{k=1}^{N}\Sigma_{k\leq u<k+mq,u\equiv j(\mathrm{mod}\ q)}\{e(\frac{jn}{q})e(\beta k) + O(mq|\beta|)\} + O(mq) \\ &= \frac{1}{mq}\Sigma_{j=1}^{q}e(\frac{jn}{q})\Sigma_{k=1}^{N}(A(m) - D(j,k,m,q))\{e(\beta k) + O(mq|\beta|)\} + O(mq) \\ &= \frac{A(m)}{m}\frac{1}{q}\Sigma_{j=1}^{q}e(\frac{jn}{q})\Sigma_{k=1}^{N}e(\beta k) + O(mNq|\beta|) \\ &- \{\frac{1}{mq}\Sigma_{j=1}^{q}e(\frac{jn}{q})\Sigma_{k=1}^{N}e(\beta k)D(j,k,m,q) + O(mNq|\beta|)\} + O(mq) \end{aligned}$$

i.e.,

$$\hat{S}(\alpha) = T_m(\alpha) - \frac{1}{mq}\Sigma_{j=1}^{q} e(\frac{jn}{q})\Sigma_{k=1}^{N} e(\beta k)D(j,k,m,q) + O(mNq|\beta|) + O(mq). \quad (2.3.3)$$

We can now prove Equation 2.3.1 To do this, we first estimate the sum $\Sigma_{j=1}^{q}\Sigma_{k=1}^{N} D(j,k,m,q)$. For this let us take $\alpha = 0$ in the functions on both sides of Equation 2.3.3. Then any q with $1 \leq q \leq \sqrt{N}$ and $n = 0$ will serve our purpose, in the sense that for these values of β, n, q one has $\left|\beta\right| = 0 \leq \frac{1}{q\sqrt{N}}$. We then have

$$\begin{aligned}
\hat{S}(0) &= T_m(0) - \frac{1}{mq}\Sigma_{j=1}^{q} e(0)\Sigma_{k=1}^{N} e(0)D(j,k,m,q) + O(0) + O(mq) \\
&= T_m(0) - \frac{1}{mq}\Sigma_{j=1}^{q}\Sigma_{k=1}^{N} D(j,k,m,q) + O(mq)
\end{aligned}$$

which gives

$$s = Na(m) - \frac{1}{mq}\Sigma_{j=1}^{q}\Sigma_{k=1}^{N} D(j,k,m,q) + O(mq)$$

which implies that for $\alpha = 0$,

$$\Sigma_{j=1}^{q}\Sigma_{k=1}^{N} D(j,k,m,q) = mNqa(m) - mqs + O(mq).$$

For $\alpha \neq 0$ we estimate as follows:

$$\begin{aligned}
|\hat{S}(\alpha) - T_m(\alpha)| &= |-\frac{1}{mq}\Sigma_{j=1}^{q} e(\frac{jn}{q})\Sigma_{k=1}^{N} e(\beta k)D(j,k,m,q) + O(mq) + O(mNq|\beta|)| \\
&< \frac{1}{mq}(mNqa(m) - mqs) + O(mq) + O(mNq|\beta|) \\
&= Na(m) - s + O(mq) + O(mNq|\beta|) \\
&\leq Na(m) - s + O(m\sqrt{N}) + O(mN\frac{1}{\sqrt{N}}) \\
&= Na(m) - s + O(m\sqrt{N})
\end{aligned}$$

which is Equation 2.3.1.

2.4 A functional inequality for $a(x)$ and its applications

2.4.1 Introduction

Let m be even, and let $2M = m^4$. Let $S = \{u_1, ..., u_s\}$ be a largest possible subset of $[1, 2M]$ which does not contain any nontrivial 3-term arithmetic progression, so that

$s = A(2M)$, and let $T = \{2v_1, ...2v_t\}$ be the set of all even elements of S. Observe that

$$s = 2Ma(2M) = 2Ma(m^4) \leq 2Ma(m) \tag{2.4.1}$$

$$t \leq A(M) = Na(M) \leq Ma(m) \tag{2.4.2}$$

and, as in (6),

$$t \geq A(2M) - A(M) \geq 2Ma(2M) - Ma(m). \tag{2.4.3}$$

The main aim of this section is to prove the asymptotic

$$a(m)^2 = O\left(\frac{a(m)^2}{\eta^2 M^2} + \{\eta M a(m) + 1\}\{a(m) - a(2M) + M^{-\frac{1}{4}}\} + \frac{a(m)}{\eta M}\right) \tag{2.4.4}$$

where η is a real number with $0 < \eta < \frac{1}{2}$.

2.4.2 Proof of the functional inequality

As in the previous proof, we again consider the Fourier sums

$$\hat{S}(\alpha) \ := \ \Sigma_{u\in S} e(\alpha u), \qquad \hat{T}(\alpha) := \Sigma_{2v\in T} e(\alpha v)$$

and two further sums

$$\sigma(\alpha) := a(m)\Sigma_{j=1}^{2M} e(\alpha j), \qquad \tau(\alpha) := a(m)\Sigma_{j=1}^{M} e(\alpha j).$$

Using Equation 2.4.1 and Equation 2.4.2, we have

$$\hat{S}(\alpha) = O(Ma(m)), \qquad \hat{T}(\alpha) = O(Ma(m)) \tag{2.4.5}$$

and it is obvious by definition that

$$\sigma(\alpha) = O(Ma(m)), \qquad \tau(\alpha) = O(Ma(m)). \tag{2.4.6}$$

In order to prove the above asymptotic Equation 2.4.4 we need the following succession of claims and propositions propositions.

Claim: Two asymptotics

$$\hat{S}(\alpha) - \sigma(\alpha) = O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}) \tag{2.4.7}$$

and

$$\hat{T}(\alpha) - \tau(\alpha) = O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}) \tag{2.4.8}$$

Let us assume this for the moment and use them for proving the ensuing propositions.

Proposition 1: Another asymptotics *For any α,*

$$\hat{S}(\alpha)\hat{T}(-\alpha)^2 - \sigma(\alpha)\tau(-\alpha)^2 = O(\{Ma(m)\}^2(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}).$$

Proposition 2: *If $\eta \in (0,1)$ and $0 < \eta < \alpha < 1-\eta$, we have*

$$\hat{S}(\alpha) = O(\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}).$$

Proposition 3: *The condition that S does not contain any nontrivial 3-term arithmetic progression can be expressed as*

$$\int_{-\eta}^{1-\eta} \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha = t.$$

Proposition 4: *For $0 < \eta < \frac{1}{2}$, we have*

$$\int_{\eta}^{1-\eta} \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha = O(\{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m)).$$

Proposition 5: *We have*

$$\int_{-\eta}^{\eta} \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha = \int_{-\eta}^{\eta} \sigma(\alpha)\tau(-\alpha)^2 d\alpha + O(\eta\{\frac{a(m)}{\eta}$$
$$+M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m)^2).$$

Proof of Proposition 5: Using Proposition 1, we can write

$$\hat{S}(\alpha)\hat{T}(-\alpha)^2 = \sigma(\alpha)\tau(\alpha)^2 + O(\{Ma(m)\}^2(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}).$$

Integrating this from $-\eta$ to η, the required equation results instantly. ■

Proposition 6: *We have the asymptotic formula*

$$\int_{-\eta}^{\eta} \sigma(\alpha)\tau(-\alpha)^2 d\alpha = \int_{-\frac{1}{2}}^{\frac{1}{2}} \sigma(\alpha)\tau(-\alpha)^2 d\alpha + O(\frac{a(m)^3}{\eta^2})$$

valid for $0 < \eta < \frac{1}{2}$.

Proposition 7: *We have*

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} \sigma(\alpha)\tau(-\alpha)^2 d\alpha = M^2 a(m)^3.$$

We will prove these results later. Let us first see how these can be used to prove the main aim of this section.

Proof of Equation 2.4.4

Given the above claim and the nine propositions above, we can prove the functional asymptotic as follows.

Using Proposition 6 we have

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} \sigma(\alpha)\tau(-\alpha)^2 d\alpha = \int_{-\eta}^{\eta} \sigma(\alpha)\tau(-\alpha)^2 d\alpha + O(\frac{a(m)^3}{\eta^2})$$

which, using Proposition 5, becomes

$$\int_{-\eta}^{\eta} \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha + O(\frac{a(m)^3}{\eta^2}) + O(\eta\{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m)^2)$$

which is equal to

$$\int_{-\eta}^{1-\eta} \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha - \int_{\eta}^{1-\eta} \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha + O(\frac{a(m)^3}{\eta^2}) + \\ O(\eta\{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m)^2).$$

Applying Proposition 3 and 4 respectively to the first and second integrals, we obtain

$$t + O\left(\{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m)\right) + \\ O(\frac{a(m)^3}{\eta^2}) + O(\eta\{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m)^2)$$

which may be written as

$$O\Bigg(Ma(m) + \{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m) + \frac{a(m)^3}{\eta^2} \\ + \eta\{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m)^2\Bigg)$$

(note that we have used the fact that $t \leq Ma(m)$, which is Equation 2.4.2). So, using Proposition 7,

$$\begin{aligned}
a(m)^2 &= O\Bigg(\frac{Ma(m)}{M^2a(m)} + \{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}\frac{Ma(m)}{M^2a(m)} \\
&+ \frac{a(m)^3}{\eta^2M^2a(m)} + \frac{\eta}{M^2a(m)}\{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}Ma(m)^2\Bigg)
\end{aligned}$$

$$\begin{aligned}
&= O\Bigg(\frac{1}{M} + \{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}\frac{1}{M} + \frac{a(m)^2}{\eta^2M^2} \\
&+ \frac{\eta}{Ma(m)}\{\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}}\}a(m)\Bigg) \\
&= O\Bigg(\frac{1}{M} + \{\frac{a(m)}{M\eta} + \{a(m) - a(2M)\} + M^{-\frac{1}{4}}\} + \frac{a(m)^2}{\eta^2M^2} \\
&+ \frac{1}{M} + \eta\{a(m) - a(2M)\} + M^{-\frac{1}{4}}\}\Bigg) \\
&= O\Bigg(\frac{a(m)}{M\eta} + a(m) - a(2M) + \frac{a(m)^2}{\eta^2M^2} \\
&+ \eta\{a(m) - a(2M)\} + M^{-\frac{1}{4}}\}\Bigg) \\
&= O\Bigg(\frac{a(m)}{\eta M} + \frac{a(m)^2}{\eta^2M^2} + (\eta Ma(m) + 1)\{a(m) - a(2M) + M^{-\frac{1}{4}}\}\Bigg)
\end{aligned}$$

which is the required asymptotics. ∎

2.4.3 Applications of the asymptotic

Before we prove the above chain of results, we first indicate how the asymptotic leads to the completion of the proof of Roth's theorem.

For this purpose, we have the following function $b(x)$ related to $a(x)$, defined in the following proposition.

Proposition 8: *If, for any positive integer x we define*

$$b(x) := a(2^{4^x}),$$

\then we have

$$b(x)^2 < c_1\Big\{b(x)\delta + b(x)^2\delta^2 + (\frac{b(x)}{\delta} + 1)\big(b(x) - b(x+1) + 2^{-4^x}\big)\Big\},$$

where $c_1$is an absolute constant and $\delta = \frac{1}{M\eta}$.

Proof of Proposition 8: Using the asymptotic Equation 2.4.4 we can write, by substituting $\delta = \frac{1}{\eta M}$

$$a(m)^2 = O(a(m)\delta + a(m)^2\delta^2 + (\frac{a(m)}{\delta} + 1)\{a(m) - a(2M) + \frac{1}{M^{\frac{1}{4}}}\})$$

$$= O(a(m)\delta + a(m)^2\delta^2 + (\frac{a(m)}{\delta} + 1)\{a(m) - a(m^4) + \frac{2^{\frac{1}{4}}}{m}\})$$

which is the same as saying that

$$a(m)^2 < c_1(a(m)\delta + a(m)^2\delta^2 + (\frac{a(m)}{\delta} + 1)\{a(m) - a(m^4) + \frac{1}{m}\})$$

for an absolute constant c_1. Now $b(x) = a(2^{4^x}) \implies b(x+1) = a(2^{4^{x+1}}) = a((2^{4^x})^4) = a(m^4)$ where $m = 2^{4^x}$ is even. Substituting these values in the above inequality one obtains

$$b(x)^2 < c_1(b(x)\delta + b(x)^2\delta^2 + (\frac{b(x)}{\delta} + 1)\{b(x) - b(x+1) + \frac{1}{2^{4^x}}\}). \blacksquare$$

We can clearly choose $c_1 > 1$ in the above inequality. Consequently we can choose $0 < \eta < \frac{1}{2}$ such that $c_1 = \frac{b(x)}{2\delta}$. This gives

$$c_1\{b(x)\delta + b(x)^2\delta^2\} \le b(x)^2\{\frac{1}{2} + \frac{1}{4c_1}\} < \frac{3}{4}b(x)^2.$$

Moreover, by the definition of δ and Equation 2.2.2,

$$\eta = \frac{1}{M\delta} = \frac{4c_1}{m^4 a(m)} < c_2\frac{1}{m^3},$$

where $c_2 = 4c_1$. This shows, since the constants c_1 and c_2 are absolute, that $0 < \eta < \frac{1}{2}$ is satisfied for large enough m. Hence from Proposition 9 we can write

$$b(x)^2 < \frac{3}{4}b(x)^2 + c_1((\frac{b(x)}{\delta} + 1)\{b(x) - b(x+1) + \frac{1}{2^{4^x}}\})$$

which gives

$$b(x)^2 < 4c_1((\frac{b(x)}{\delta} + 1)\{b(x) - b(x+1) + \frac{1}{2^{4^x}}\}),$$

and which, in turn, gives (using the fact that $c_1 = \frac{b(x)}{2\delta}$)

$$b(x)^2 < 4c_1((2c_1 + 1)\{b(x) - b(x+1) + \frac{1}{2^{4^x}}\})$$

$$= c_3\{b(x) - b(x+1) + \frac{1}{2^{4^x}}\}$$

for large enough x, say for $x > c_4$.

Now Equation 2.2.3 implies that b is a decreasing function. Therefore, for any positive integer k one has

$$\begin{aligned} kb(2k)^2 &\leq \Sigma_{j=k}^{2k-1} b(j)^2 < c_3 \Sigma_{j=k}^{2k-1}\{b(j) - b(j+1) + 2^{-4^j}\} \\ &= c_3(b(k) - b(2k)) + c_3 \Sigma_{j=k}^{2k-1} 2^{-4^j} \\ &< c_3(b(k) - b(2k)) + \frac{c_3 k}{2^{4^k}} \\ &< c_5\{b(k) - b(2k) + \frac{2c_5}{k}\}, \end{aligned}$$

for $k > c_4$, where c_5 is a constant.

We can now use these results to complete the proof of the theorem as follows.

Let $k > c_4$and suppose $2kb(2k) > 4c_5$. Then

$$2kb(2k) < \frac{1}{4c_5}\{2kb(2k)\} < k\{b(k) - b(2k) + \frac{2c_5}{k}\} < kb(k);$$

this clearly implies that if $2^r > 2^{r_0} > c_4$,

$$2^r b(2^r) \leq \max\{4c_5, 2^{r_0} b(2^{r_0})\}$$

whence

$$b(2^r) = O(2^{-r})$$

for large enough r.

We claim that this implies

$$b(x) = O(\frac{1}{x})$$

for large enough x.

Let x be large; in fact let $x > 2^{r_0} > c_4$. If x is a power of 2, we are done. So suppose it is not. Then we can choose k such that $2^k > x > 2^{k-1} \geq 2^{r_0}$. Since b is decreasing, then

$$O(2^{-k}) = b(2^k) \leq b(x) \leq b(2^{k-1}) = O(2^{-(k-1)});$$

since $O(2^{-k}) = 2^{-(k-1)}$ we have

$$b(x) = O(2^{-k}).$$

But since $2^{-k} \leq x^{-1}$ we have

$$b(x) = O(\frac{1}{x}),$$

which proves the claim.

Finally we have

$$a(x) = O(\frac{1}{\log\log x}).$$

We prove this as follows. Let x be any large integer. Then we can choose an integer y to satisfy

$$2^{4^y} < x \leq 2^{4^{y+1}}.$$

Using (27) we have

$$\begin{aligned} a(x) &\leq (1 + x^{-1}2^{4^y})a(2^{4^y}) \\ &\leq 2a(2^{4^y}) \\ &= 2b(y) \\ &= O(\frac{1}{y}); \end{aligned}$$

but since $2y < \log_2 \log_2 x \leq 2(y+1)$ and $\log_2 \log_2 x = \frac{\log \log_2 x}{\log 2} = \frac{\log \log x - \log \log 2}{\log 2}$ we clearly have

$$a(x) = O(\frac{1}{\log\log x}). \blacksquare\blacksquare\blacksquare$$

This is what we set out to prove.

It now remains to demonstrate the above chain of propositions

2.5 Proof of the claim (Two asymptotics, eqs Equation 2.4.7 and Equation 2.4.8)

2.5.1 Proof of Equation 2.4.7

2.5.1.1 Case I: $q = 1$

We let $N = 2M$ in Equation 2.3.1 and consider $\hat{S}(\alpha), \sigma(\alpha)$. Not that for this case

$$\begin{aligned}
T_m(\alpha) &= a(m)e(n)\Sigma_{j=1}^{2M} e(\beta j) \\
&= a(m)\Sigma_{j=1}^{2M} e(n + \beta j) \\
&= a(m)\Sigma_{j=1}^{2M} e(nj + \beta j) \\
&= a(m)\Sigma_{j=1}^{2M} e(\alpha j) \\
&= \sigma(\alpha)
\end{aligned}$$

so

$$|\hat{S}(\alpha) - \sigma(\alpha)| = |\hat{S}(\alpha) - T_m(\alpha)| < 2Ma(m) - s + O(m\sqrt{2M}) = 2Ma(m) - 2Ma(2M) + O(m\sqrt{M})$$

which gives that

$$\hat{S}(\alpha) - \sigma(\alpha) = O(2Ma(m) - 2Ma(2M) + m\sqrt{M})$$

$$= O(2Ma(m) - 2Ma(2M) + M^{\frac{3}{4}}) \tag{2.5.1}$$

using the fact that $2M = m^4$, whence $m = O(M^{\frac{1}{4}})$.

Next we consider $\hat{T}(\alpha), \tau(\alpha)$. For this we set $N = M$ in Equation 2.3.1. In that case we observe that

$$\begin{aligned}
T_m(\alpha) &= a(m)e(n)\Sigma_{k=1}^{M} e(\beta k) \\
&= a(m)\Sigma_{k=1}^{M} e((\beta + n)k) \\
&= a(m)\Sigma_{k=1}^{M} e(\alpha k) \\
&= \tau(\alpha).
\end{aligned}$$

Note that the *maximality* of the set S was not used at all in our bound Equation 2.3.1, so we can use the same bound for the present case; i.e.,

$$|\hat{T}(\alpha) - \tau(\alpha)| = O(Ma(m) - t + O(m\sqrt{M})$$

which, using Equation 2.4.3and the fact that $m = O(M^{\frac{1}{4}})$, reduces to

$$\begin{aligned} |\hat{T}(\alpha) - \tau(\alpha)| &= O(Ma(m) - \{2Ma(2M) - Ma(m)\} + O(M^{\frac{3}{4}}) \\ &= O(2Ma(m) - 2Ma(2M) + O(M^{\frac{3}{4}}) \\ &= O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}) \end{aligned}$$

which is what we wanted. ⊛

2.5.1.2 Case II: $q \neq 1$

First we have the following lemma

Lemma 1: *For any real α and any positive integer N, we have*

$$|\Sigma_{j=1}^{N} e(\alpha j)| \leq \min\{N, \frac{1}{2\left\|\alpha\right\|}\}$$

where $\left\|\alpha\right\|$ is the distance of the nearest integer from α.

Proof of Lemma 1: If for a fixed N, we denote $f_N(\alpha) := |\Sigma_{j=1}^{N} e(\alpha j)|, g_N(\alpha) := \min\{N, \frac{1}{2\left\|\alpha\right\|}\}$, we see that both f_N and g_N are even functions with period 1. So it is enough to prove the result for $0 \leq \alpha \leq \frac{1}{2}$.

Now

$$\Sigma_{j=1}^{N} e(\alpha j) = \frac{e(\alpha N) - 1}{e(\alpha) - 1} e(\alpha).$$

First of all, let us note that for $0 \leq \alpha \leq \frac{1}{2}$, we have the inequality

$$|e(\alpha) - 1| = 2\pi \sin(\pi\alpha) \geq 4\alpha = 4\left\|\alpha\right\|$$

where the inequality follows from *Jordan's inequality*

$$\frac{2x}{\pi} \leq \sin x \leq x$$

for $x \in [0, \frac{1}{2}]$, and the equality $\alpha = \left\|\alpha\right\|$ is obvious since $\alpha \in [0, \frac{1}{2}]$.

Let us suppose that $0 \leq \alpha \leq \frac{1}{2N}$. Then by the triangle inequality

$$\left|\Sigma_{j=1}^{N} e(\alpha j)\right| \leq N = \min\{N, \frac{1}{2\left\|\alpha\right\|}\}.$$

It remains to prove for $\frac{1}{2N} < \alpha \leq \frac{1}{2}$. In this case we have

$$\begin{aligned}
\left|\Sigma_{j=1}^{N} e(\alpha j)\right| &= \left|\frac{e(\alpha N)-1}{e(\alpha)-1} e(\alpha)\right| \\
&= \left|\frac{e(\alpha N)-1}{e(\alpha)-1}\right| \\
&\leq \frac{2}{4\left\|\alpha\right\|} \\
&= \frac{1}{2\left\|\alpha\right\|} \\
&= \min\{N, \frac{1}{2\left\|\alpha\right\|}\}
\end{aligned}$$

which completes the proof of the lemma. □

Using the lemma, we have, since $\frac{1}{\left\|\alpha\right\|} \geq 1$,

$$\begin{aligned}
\left|\Sigma_{j=1}^{N} e(\alpha j)\right| &\leq \min\{N, \frac{1}{2\left\|\alpha\right\|}\} \\
&\leq \min\{\frac{N}{\left\|\alpha\right\|}, \frac{1}{2\left\|\alpha\right\|}\}
\end{aligned}$$

which proves that

$$\Sigma_{j=1}^{N} e(\alpha j) = O(\frac{1}{\left\|\alpha\right\|}) \tag{2.5.2}$$

for all real α. ⊛

Lemma 2: *If $q \neq 1$ then $\alpha > \frac{1}{\sqrt{N}}$.*

Proof of Lemma 2: Now

$$\alpha = \frac{n}{q} + \beta,$$

so that if $q \neq 1$, then

$$\left\|\alpha\right\| = \frac{r}{q} \pm \beta,$$

where $1 < \left|r\right| \leq \left|n\right|$. Also, since $1 < q \leq \sqrt{N}$, one has

$$\left\|\alpha\right\| \geq \frac{r}{\sqrt{N}} \pm \beta,$$

from which, using the fact that $q|\beta| \leq \frac{1}{\sqrt{N}}$, it follows that

$$\left\|\alpha\right\| \geq \frac{r-1}{\sqrt{N}} > \frac{1}{\sqrt{N}},$$

which completes the proof of the lemma. □

Given these two lemmas, we can now complete the proof of the second case as follows.

Since $q > 1$, we have $T_m(\alpha) = 0$, so by Equation 2.3.1,

$$\hat{S}(\alpha) = \pm\left|\hat{S}(\alpha)\right| = \pm\left|\hat{S}(\alpha) - T_m(\alpha)\right| < Na(m) - s + O(m\sqrt{N}),$$

which means that

$$\begin{aligned}\hat{S}(\alpha) &= O(Ma(m) - \{2Ma(2M) - Ma(m)\} + M^{\frac{3}{4}}) \\ &= O(2Ma(m) - 2Ma(2M) + M^{\frac{3}{4}}).\end{aligned}$$

Also,

$$\sigma(\alpha) = a(m)\Sigma_{j=1}^{2N} e(\alpha j) = O(\frac{1}{\left\|\alpha\right\|})$$

using Lemma 1, and hence

$$\sigma(\alpha) = O(\sqrt{M})$$

using Lemma 2. So using the triangle inequality, we can write

$$\begin{aligned}|\hat{S}(\alpha) - \sigma(\alpha)| &\leq \left|\hat{S}(\alpha)\right| + \left|\sigma(\alpha)\right| \\ &\leq O(M(a(m) - a(2M)) + M^{\frac{3}{4}}) + O(\sqrt{M})\end{aligned}$$

which immediately gives that

$$\hat{S}(\alpha) - \sigma(\alpha) = O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}),$$

and our first claim Equation 2.4.7is proven.

2.5.2 Proof of Equation 2.4.8

We now proceed to Equation 2.4.8.

Here again, using the two lemmas succesively as in the above case, we can see that

$$\tau(\alpha) = O(\sqrt{M}).$$

Next, as in the paragraph immediately after eqEquation 2.5.1,

$$\hat{T}(\alpha) = \pm \left|\hat{T}(\alpha)\right| < Ma(m) - t + O(m\sqrt{M}),$$

which immediately leads to

$$\hat{T}(\alpha) = O(2Ma(m) - 2Ma(2M) + M^{\frac{3}{4}})$$

so that, as before,

$$\begin{aligned} \left|\hat{T}(\alpha) - \tau(\alpha)\right| &\leq \left|\hat{T}(\alpha)\right| + |\tau(\alpha)| \\ &= O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}) + O(\sqrt{M}) \\ &= O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}) \end{aligned}$$

which completes the proof of our claim. ■

The proof of our claim being finished, we must next demonstrate the propositions.

2.6 Proofs of the propositions

In this section we complete the proof of the theorem, by proving Proposition 1-Proposition 7.

Proof of Proposition 1: Using the triangle inequality, we get the inequality

$$\begin{aligned} \left|\hat{S}(\alpha)\hat{T}(-\alpha)^2 - \sigma(\alpha)\tau(-\alpha)^2\right| &= |\hat{S}(\alpha)\{\hat{T}(-\alpha)^2 - \tau(-\alpha)^2\} \\ &+ \tau(-\alpha)^2\{\hat{S}(\alpha) - \sigma(\alpha)\}| \\ &\leq |\hat{S}(\alpha)||\hat{T}(-\alpha) + \tau(-\alpha)||\hat{T}(-\alpha) - \tau(-\alpha)| \\ &+ |\tau(-\alpha)^2||\hat{S}(\alpha) - \sigma(\alpha)| \end{aligned}$$

to which we apply the bounds we have already obtained, namely (40), (41), (42) and (43) to get the asymptotics

$$\hat{S}(\alpha)\hat{T}(-\alpha)^2 - \sigma(\alpha)\tau(-\alpha)^2 = O(Ma(m))2O(Ma(m))O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}})$$
$$+O(Ma(m))^2 O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}),$$

which, by the rules of asymptotics, reduces immediately to

$$\hat{S}(\alpha)\hat{T}(-\alpha)^2 - \sigma(\alpha)\tau(\alpha)^2 = O(\{Ma(m)\}^2(M\{a(m) - a(2M)\} + M^{\frac{3}{4}})$$

which is what we wanted to show. ■

Proof of Proposition 2: We have proved (Equation 2.4.7) that

$$\hat{S}(\alpha) = \sigma(\alpha) + O(M\{a(m) - a(2M)\} + M^{\frac{3}{4}}).$$

Therefore it is enough to prove that for $0 < \eta < \alpha < 1 - \eta$ we have

$$\sigma(\alpha) = O(\frac{a(m)}{\eta}).$$

Now as $\alpha \in (0,1)$ we know that $\left\|\alpha\right\|$ is equal to either the distance of α from 0 or the distance of α from 1. But since $0 < \eta < \alpha < 1 - \eta$ it follows that $\left\|\alpha\right\| > \eta$. Hence

$$\begin{aligned} |\sigma(\alpha)| &= a(m)|\Sigma_{j=1}^{2M} e(\alpha j)| \\ &\leq a(m)\min\{2M, \frac{1}{2\left\|\alpha\right\|}\} \\ &\leq \frac{a(m)}{2\left\|\alpha\right\|} \\ &\leq \frac{a(m)}{2\eta} \end{aligned}$$

which proves the result. ■

Proof of Proposition 3: The integral $\int_{-\eta}^{1-\eta} \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha$ is equal to

$$\int_{\eta}^{1-\eta} \Sigma_{j=1}^{s} e(\alpha u_j)\{\Sigma_{k=1}^{t} e(-\alpha v_k)\}^2 d\alpha$$

$$= \Sigma_{i,j,k}^{s,t,t} \int_{-\eta}^{1-\eta} e(\alpha(u_i - v_j - v_k))d\alpha$$

and by changing the limits of integration, this is in turn equal to

$$\Sigma_{i,j,k}^{s,t,t} \int_0^1 e(\alpha(u_i - v_j - v_k))d\alpha.$$

But now,

$$\int_0^1 e(\alpha(u_i - v_j - v_k))d\alpha = \begin{cases} 1, & \text{if } u_i - v_j - v_k = 0 \\ 0, & \text{otherwise.} \end{cases}$$

From this it follows instantly that

$$\Sigma_{i,j,k}^{s,t,t} \int_0^1 e(\alpha(u_i - v_j - v_k))d\alpha = |\{(i,j,k) : u_i = v_j + v_k, 1 \le i \le s, 1 \le j,k \le t\}|$$

$$= t$$

as the quantity $|\{(i,j,k) : u_i = v_j + v_k, 1 \le i \le s, 1 \le j,k \le t\}|$ is exactly the number of 3-term arithmetic progressions, and since by assumption, this number is t. This proves the proposition (see Equation 2.4.2). ■

Proof of Proposition 4: We have

$$\begin{aligned} |\int_\eta^{1-\eta} \hat{S}(\alpha)\hat{T}(-\alpha)^2 d\alpha| &\le |\max_{\xi \in [\eta, 1-\eta]} |\hat{S}(\xi)| \int_\eta^{1-\eta} \hat{T}(-\alpha)^2 d\alpha| \\ &= O(\frac{a(m)}{\eta} + M\{a(m) - a(2M)\} + M^{\frac{3}{4}})| \int_\eta^{1-\eta} \hat{T}(-\alpha)^2 d\alpha| \qquad \text{(using Po} \end{aligned}$$

so it is enough to prove that

$$\int_\eta^{1-\eta} \hat{T}(-\alpha)^2 d\alpha = O(Ma(m)). \tag{2.6.1}$$

Now

$$\begin{aligned} |\int_\eta^{1-\eta} \hat{T}(-\alpha)^2 d\alpha| &\le |\int_\eta^{1-\eta} |\hat{T}(-\alpha)^2| d\alpha| \\ &= \left|\int_{1-\eta}^{\eta} |\hat{T}(\alpha)^2| d\alpha\right| \\ &\le \int_0^1 |\hat{T}(\alpha)^2| d\alpha \end{aligned}$$

since $\eta, 1-\eta \in [0,1]$. Now

$$\int_0^1 |\hat{T}(\alpha)^2| d\alpha = \Sigma_{j,k=1}^t \int_0^1 e(\alpha(v_j - v_k)) d\alpha$$

which, by the orthogonality of e and the fact that $\alpha \neq 0$, reduces immediately to t, which is, by Equation 2.4.2, $\leq Ma(m)$, completing the proof of the proposition. ■

Proof of Proposition 6: We split the integral $\int_{-\eta}^{\eta} \sigma(\alpha)\tau(-\alpha)^2 d\alpha$ as follows:

$$\int_{-\eta}^{\eta} \sigma(\alpha)\tau(-\alpha)^2 d\alpha = \int_{-\frac{1}{2}}^{\frac{1}{2}} \sigma(\alpha)\tau(-\alpha)^2 d\alpha - \Big\{ \int_{\eta}^{\frac{1}{2}} \sigma(\alpha)\tau(-\alpha)^2 d\alpha + \int_{-\frac{1}{2}}^{-\eta} \sigma(\alpha)\tau(-\alpha)^2 d\alpha \Big\}$$

which can be simplified as

$$\int_{-\eta}^{\eta} \sigma(\alpha)\tau(-\alpha)^2 d\alpha = \int_{-\frac{1}{2}}^{\frac{1}{2}} \sigma(\alpha)\tau(-\alpha)^2 d\alpha - \int_{\eta}^{\frac{1}{2}} \{\sigma(\alpha)\tau(-\alpha)^2 + \sigma(-\alpha)\tau(\alpha)^2\} d\alpha. \tag{2.6.2}$$

Consider now the latter integral

$$\int_{\eta}^{\frac{1}{2}} \{\sigma(\alpha)\tau(-\alpha)^2 + \sigma(-\alpha)\tau(\alpha)^2\} d\alpha$$

which is equal to

$$\int_{\eta}^{\frac{1}{2}} \{\sigma(\alpha)\tau(-\alpha)^2 + \overline{\sigma(\alpha)\tau(-\alpha)^2}\} d\alpha.$$

Taking the absolute value we get the following inequality

$$\Big| \int_{\eta}^{\frac{1}{2}} \{\sigma(\alpha)\tau(-\alpha)^2 d\alpha + \overline{\sigma(\alpha)\tau(-\alpha)^2}\} d\alpha \Big| \leq \int_{\eta}^{\frac{1}{2}} \{|\sigma(\alpha)\tau(-\alpha)^2| + |\overline{\sigma(\alpha)\tau(-\alpha)^2}|\} d\alpha$$

$$= 2\int_{\eta}^{\frac{1}{2}} |\sigma(\alpha)\tau(-\alpha)^2| d\alpha. \tag{2.6.3}$$

So we can now concentrate on tha integral $\int_{\eta}^{\frac{1}{2}} |\sigma(\alpha)\tau(-\alpha)^2| d\alpha$.

Since $0 < \eta < \frac{1}{2}$, we have $[\eta, \frac{1}{2}] \subset [\eta, 1-\eta]$. Then the argument of Proposition 2 proves that

$$\sigma(\alpha) = O(\frac{a(m)}{\eta}).$$

An almost exactly similar argument proves that

$$\tau(-\alpha) = O(\frac{a(m)}{\eta}).$$

Using these two bounds in Equation 2.6.3, we have

$$\Big|\int_{\eta}^{\frac{1}{2}}\{\sigma(\alpha)\tau(-\alpha)^2 d\alpha + \overline{\sigma(\alpha)\tau(-\alpha)^2}\}d\alpha\Big| = O((\eta - \frac{1}{2})\{\frac{a(m)}{\eta}\}^3)$$

$$= O(\frac{a(m)^3}{\eta^2})$$

and the proof of the proposition is complete with this. ■

Proof of Proposition 7: Expanding the integral using the definitions of $\sigma(\alpha)$ and $\tau(-\alpha)$ we have

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} \sigma(\alpha)\tau(-\alpha)^2 d\alpha = a(m)^3 \Sigma_{x=1}^{2M}\Sigma_{y=1}^{M}\Sigma_{z=1}^{M} \int_{-\frac{1}{2}}^{\frac{1}{2}} e(\alpha(x-y-z))d\alpha.$$

But now the integral $\int_{-\frac{1}{2}}^{\frac{1}{2}} e(\alpha(x-y-z))d\alpha$ is one or zero according as $x-y-z$ is zero or not. That is

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} e(\alpha(x-y-z))d\alpha = \begin{cases} 1, \text{ if } x-y-z=0 \\ 0, \text{ otherwise.} \end{cases}$$

Hence the integral $\Sigma_{x=1}^{2M}\Sigma_{y=1}^{M}\Sigma_{z=1}^{M} \int_{-\frac{1}{2}}^{\frac{1}{2}} e(\alpha(x-y-z))d\alpha$ counts the number of solutions of the equation

$$x = y + z$$

with $1 \leq x \leq 2M, 1 \leq y, z \leq M$ and this number is easily seen to be M^2. ■

3 A generalisation of Roth's theorem

3.1 Statement

Let A be a subset of the positive integers with

$$\lim_{n\to\infty} \frac{\left|A \cap [1,n]\right|}{n} > 0$$

Let $x_1, ..., x_k$ be nonzero integers with

$$x_1 + \cdots + x_k = 0.$$

Then there exist distinct $a_1, \cdots, a_k \in A$ such that

$$a_1 x_1 + \cdots + a_k x_k = 0.$$

Proof: We may assume without any loss that $gcd(x_1, x_2, \cdots, x_k) = 1$.
Such integers $a_1, \cdots, a_k$ will be said to form an **x-*progression***.
We will prove this in the form given below.
For each $N \in \mathbb{N}$ there is a density $\delta = \delta(N)$ such that if $A \subset [1, N]$ has density $\geq \delta$, then A contains distinct elements $a_1, \cdots, a_k$ such that

$$a_1 x_1 + \cdots + a_k x_k = 0. \tag{3.1.1}$$

3.2 Roth's Uniformity Lemma

We shall need the following Lemma of Roth.

Lemma 2. *: (Roth's Uniformity Lemma).* For all $1 \leq M \leq N$

$$\left\|\hat{1}_A - \delta \hat{1}_N\right\|_\infty \leq 2N(E_A(M) - \delta)) + 17M\sqrt{N} \tag{3.2.1}$$

where

$$E_A(M) = \frac{1}{M} \max\{\left|A \cap P\right| : P \in M - prog\}.$$

Here $M - prog$ denotes the set of all arithmetic progressions of length M in $\mathbb{Z}$.

Proof: Let us write

$$f := 1_A - \delta 1_N.$$

We have

$$\begin{aligned}
\hat{f}(\alpha) &= \sum_n f(n)e(-n\alpha) \\
&= \frac{1}{qM}\sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}} f(n)e(-\alpha n) \\
&= \frac{1}{qM}\sum_{m\in\mathbb{Z}}\sum_{n\in I_m} f(n)e(-\alpha n) \qquad (3.2.2)
\end{aligned}$$

where I_m is the interval $[m, m+qM[$ of length qM, and q is a positive integer. Note that each interval I_m can be partitioned into q disjoint intervals of length M each, namely

$$I_m = \bigsqcup_{r=1}^{q} I_m \cap \{x \in \mathbb{Z} : x \equiv r \ \mathtt{mod}\ q\}.$$

Now for any $a \in \mathbb{Z}$ if we put $\beta = \alpha - \frac{a}{q}$ then we have by the mean value theorem

$$e(\alpha n) = e(\alpha r/q)e(\beta m) + O_1(2\pi|\beta|qM)$$

where by $f = O_1(g)$ we mean $\left|f\right| \leq g$. Using this in 3.2.2 we get

$$\begin{aligned}
\hat{f}(\alpha) &= \frac{1}{qM}\sum_{r=1}^{q}\sum_{m\in\mathbb{Z}}\sum_{n\in I_m} f(n)e(\alpha r/q)e(\beta m) + O_1(2\pi|\beta|\sum_{r=1}^{q}\sum_{m\in\mathbb{Z}}\sum_{n\in I_m}|f(n)|) \\
&= \frac{1}{qM}\sum_{r=1}^{q} e(ar/q)\sum_{m\in\mathbb{Z}} e(\beta m)\sum_{n\in I_m\cap\overline{r}} f(n) + O_1(2\pi qM\left|\beta\right|\sum_{n\in\mathbb{Z}}\left|f(n)\right|)
\end{aligned}$$

Now, $f(n) = 1_A(n) - \delta 1_N(n)$, so that

$$\begin{aligned}
\sum_{n\in\mathbb{Z}}\left|f(n)\right| &= \sum_{n=1}^{N}\left|f(n)\right| \\
&= \left|A\right|(1-\delta) + (N - \left|A\right|)\delta \\
&= 2\delta(1-\delta)N \\
&\leq 2\delta N
\end{aligned}$$

so that we have the asymptotic

$$\hat{f}(\alpha) = \frac{1}{qM}\sum_{r=1}^{q} e(ar/q)\sum_{m\in\mathbb{Z}} e(\beta m)\sum_{n\in I_m\cap\overline{r}} f(n) + O_1(4\pi qM\left|\beta\right|\delta N). \qquad (3.2.3)$$

Now we simplify the first term on the right of 3.2.3. We know that $I_m \cap [1, N] = \emptyset$ unless $m \leq N$ and $I_m \neq \emptyset$, i.e., unless $1 - qM < m \leq N$. Therefore we can write

$$\sum_{r=1}^{q} e(ar/q) \sum_{m \in \mathbb{Z}} e(\beta m) \sum_{n \in I_m \cap \overline{r}} f(n) = \sum_{r=1}^{q} e(ar/q) \sum_{1-qM<m\leq N} e(\beta m) \sum_{n \in I_m \cap \overline{r}} f(n).$$

Now clearly for each choice of q, M there exists a non-negative integer $D(m, M, q, r)$ $(1 \leq r \leq q, 1 - qM < m \leq N$ such that

$$\begin{aligned}\sum_{n \in I_m \cap \overline{r}} f(n) &= ME_A(M) - D(m, M, q, r) - \delta \left|I_m \cap \overline{r} \cap [1, N]\right| \\ &= M(E_A(M) - \delta) + \delta \left|I_m \cap \overline{r} \backslash [1, N]\right| - D(m, M, q, r).\end{aligned}$$

Thus

$$\sum_{r=1}^{q} e(ar/q) \sum_{m \in \mathbb{Z}} e(\beta m) \sum_{n \in I_m \cap \overline{r}} f(n)$$

$$= \sum_{r=1}^{q} e(ar/q) \sum_{1-qM<m\leq N} e(\beta m) \Bigg(M(E_A(M) - \delta) + \delta \left|I_m \cap \overline{r} \backslash [1, N]\right| - D(m, M, q, r) \Bigg). \tag{3.2.4}$$

Taking $a = 0, \alpha = 0$ so that $\beta = 0$ 3.2.4 becomes

$$\sum_{r=1}^{q} \sum_{m \in \mathbb{Z}} \sum_{n \in I_m \cap \overline{r}} f(n) = qM \sum_{m \in \mathbb{Z}} f(m) = 0$$

which means that

$$\begin{aligned}\sum_{r=1}^{q} \sum_{1-qM<m\leq N} D(m, M, q, r) &= \sum_{r=1}^{q} \sum_{1-qM<m\leq N} (M(E_A(M) - \delta) + \delta \left|I_m \cap \overline{r} \backslash [1, N]\right| \\ &= qM(qM + N - 1)(E_A(M) - \delta) + \delta \sum_{r=1}^{q} \sum_{1-qM<m\leq N} \left|I_m \cap \overline{r} \backslash [1, N]\right| \qquad (3.2.5) \\ &= qM(qM + N - 1)(E_A(M) - \delta) + \delta \sum_{1-qM<m\leq N} \left|I_m \backslash [1, N]\right| \\ &= qM(qM + N - 1)(E_A(M) - \delta) + \delta qM(qM - 1) \\ &= qMN(E_A(M) - \delta) + qM(qM - 1)E_A(M)\end{aligned}$$

so

$$\begin{aligned}\frac{1}{qM} \sum_{r=1}^{q} \sum_{1-qM<m\leq N} D(m, M, q, r) &= N(E_A(M) - \delta) + (qM - 1)E_A(M) && (3.2.6) \\ &\leq N(E_A(M) - \delta) + qM. && (3.2.7)\end{aligned}$$

Now using the triangle inequality we have

$$\frac{1}{qM}|\sum_{r=0}^{q-1} e(ar/q) \sum_{1-qM<m\le N} e(\beta m)\Big(M(E_A(M)-\delta)+\delta\left|I_m\cap\overline{r}\backslash[1,N]\right| - D(m,M,q,r)\Big)|$$

$$\begin{aligned}
&\le \frac{\delta}{qM}\sum_{1-qM<m\le N}\left|I_m\backslash[1,N]\right| + \frac{1}{qM}\sum_{r=1}^{q}\sum_{1-qM<m\le N} D(m,M,q,r)\\
&\le \frac{\delta}{2}(qM-1)+N(E_A(M)-\delta)+qM\\
&\le N(E_A(M)-\delta)+2qM.
\end{aligned}$$

Using this in 3.2.4 we get

$$\begin{aligned}
&\frac{1}{qM}\sum_{r=0}^{q-1} e(ar/q)\sum_{m\in\mathbb{Z}} e(\beta m)\sum_{n\in I_m\cap\overline{r}} f(n)\\
&= \frac{E_A(M)-\delta}{q}\sum_{r=1}^{q} e(ar/q)\sum_{m\in\mathbb{Z}} e(\beta m) + O_1(N(E_A(M)-\delta)+2qM),
\end{aligned}$$

which gives

$$\hat{f}(\alpha) = \frac{E_A(M)-\delta}{q}\sum_{r=1}^{q} e(ar/q)\sum_{m\in\mathbb{Z}} e(\beta m)+O_1(4\pi\left|\beta\right|\delta qMN+N(E_A(M)-\delta)+2qM). \tag{3.2.8}$$

Now $\hat{f}(\alpha)=\hat{f}(\alpha+2\pi)$ so we may assume that $\alpha\in[-\frac{1}{2},\frac{1}{2}]$. This implies that the distance $\left\|\alpha\right\|$ of α from the nearest integer is equal to its absolute value$\left|\alpha\right|$.

Assume first that $\left\|\alpha\right\| > \frac{1}{\sqrt{N}}$. Then as we have done earlier we can find $a\in\mathbb{Z}$, $1\le q\le\sqrt{N}$ with $\gcd(a,q)=1$ such that

$$\left|\tfrac{a}{q}-\alpha\right| \le \frac{1}{q\sqrt{N}},$$

which together with $\left\|\alpha\right\| > N^{-\frac{1}{2}}$ obviously implies that $q>1$, whence

$$\sum_{r=1}^{q} e(ar/q)=0.$$

By 3.2.5 and 3.2.8 we get

$$\begin{aligned}
\left|\hat{f}(\alpha)\right| &\le N(E_A(M)-\delta)+qM(4\pi\left|\beta\right|N+2)\\
&\le 2N(E_A(M)-\delta)+qM(4\pi\left|\beta\right|N+3)\\
&\le 2N(E_A(M)-\delta)+16M\sqrt{N}.
\end{aligned} \tag{3.2.9}$$

Next for the case $\left\|\alpha\right\| \leq \frac{1}{\sqrt{N}}$. Taking $a=0, q=1$ in 3.2.8 we have

$$\hat{f}(\alpha) = (E_A(M)-\delta)\sum_{1-M<m\leq N} e(\alpha m) + O_1\Bigg(M(4\pi\left|\alpha\right|N+2) + N(E_A(M)-\delta)\Bigg).$$

Hence

$$\left|\hat{f}(\alpha)\right| \leq N\Bigg(\left|E_A(M)-\delta\right| + (E_A(M)-\delta)\Bigg) + M(4\pi\sqrt{N}+2).$$

For $E_A(M)-\delta \geq 0$ this gives

$$\left|\hat{f}(\alpha)\right| \leq 2(E_A(M)-\delta)) + M(4\pi\sqrt{N}+3), \tag{3.2.10}$$

whereas if $E_A(M)-\delta < 0$, by 3.2.5 $0 \leq N(E_A(M)-\delta)+M$ so that

$$\begin{aligned}\left|\hat{f}(\alpha)\right| &\leq M(4\pi\sqrt{N}+2)\\ &\leq 2N(E_A(M)-\delta) + M(4\pi\sqrt{N}+4).\end{aligned} \tag{3.2.11}$$

Since $4\pi\sqrt{N}+4 \leq 17\sqrt{N}$ we get the bound

$$\left|\hat{f}(\alpha)\right| \leq 2N(E_A(M)-\delta) + 17M\sqrt{N}$$

for all α, establishing the lemma.■

3.3 Proof of the theorem.

Suppose A has density δ in $[1,N]$. We define

$$f_i(\alpha) = \sum_{u\in A} e(-\alpha u x_i)$$

for $i=1,...,k$.
We also define

$$g_i(\alpha) = \sum_{1\leq u\leq N} e(-\alpha u x_i)$$

and

$$h_i = f_i - g_i,$$

for $i=1,...,k$.

Further let

$$K(B) = \#\{(a_1, \cdots, a_k) \in B \times \cdots \times B : a_1x_1 + a_kx_k = 0.$$

for any subset B of $[1, N]$. If $\left|B\right| = n$ we may write $K(n)$ instead of $K(B)$.
Then we have

$$\begin{aligned} \int f_1(\alpha)\cdots f_k(\alpha)d\alpha &= \int \sum_{a_i \in A} e(-\alpha(a_1x_1 + \cdots + a_kx_k))d\alpha \\ &= N \cdot K(A) \end{aligned}$$

since $\int e(r\alpha)d\alpha = 0 \iff r \neq 0$. Here we denote the sum over $\alpha = 0, \frac{1}{N}, \cdots, \frac{N-1}{N}$ by the symbol $\int d\alpha$. It is obvious that A contains nontrivial **x**-progressions iff

$$K(A) > \left|A\right|.$$

We have

$$K(A) = \delta^k K(N) + \frac{1}{N}\int (f_1(\alpha)\cdots f_k(\alpha) - \delta^k g_1(\alpha)\cdots g_k(\alpha))d\alpha. \tag{3.3.1}$$

Let us write

$$F_j = \prod_{i<j} f_i \prod_{i>j} \delta g_i$$

We then have

$$f_1 \cdots f_k - \delta^3 g_1 \cdots g_k = \sum_{i=1}^{k} F_i h_i,$$

so that

$$|\int (f_1(\alpha)\cdots f_k(\alpha) - \delta^k g_1(\alpha)\cdots g_k(\alpha))d\alpha| \leq \sum_{i=1}^{k} \left\|F_i\right\|_\infty \left\|h_i\right\|_1 \tag{3.3.2}$$

where$\|\|_\infty$ and $\left\|\cdot\right\|_1$ denote respectively the supremum norm and the ℓ^1-norm. That is

$$\begin{aligned} \left\|F\right\|_\infty &= \sup_{x\in A}\left|F(x)\right| \\ \left\|h\right\|_1 &= \int |h(x)|dx. \end{aligned}$$

Obviously,

$$\left\|f_i\right\|_\infty \leq \delta N$$

and

$$\left\|g_i\right\|_\infty \leq N.$$

We also observe that

$$\begin{aligned}\left\|f_i\right\|_2 &= (\int \left|f_i(\alpha)\right|^2 d\alpha)^{\frac{1}{2}} \\ &= (N \cdot \left|A\right|)^{\frac{1}{2}} \\ &= \delta^{\frac{1}{2}} N\end{aligned}$$

and similarly

$$\begin{aligned}\left\|g_i\right\| &= (\int \left|g_i(\alpha)\right|^2 d\alpha)^{\frac{1}{2}} \\ &= N\end{aligned}$$

which implies

$$\begin{aligned}\left\|\delta g_i\right\| &\leq \delta N \\ &\leq \delta^{\frac{1}{2}} N \\ &=\end{aligned}$$

We easily deduce from these that

$$\begin{aligned}\left\|F_i\right\|_1 &= (\delta^{\frac{1}{2}} N)^2 (\delta N)^{k-3} \\ &= (\delta N)^{k-2} N.\end{aligned}$$

Also, as $\|h_i\|_\infty = \|f_i - g_i\|_\infty = \left\|(\hat{1}_A - \delta \hat{1}_N)\right\|_\infty$ we have from Equation 3.3.2 that

$$|\int (f_1(\alpha) \cdots f_k(\alpha) - \delta^k g_1(\alpha) \cdots g_k(\alpha)) d\alpha| \leq kN(\delta N)^{k-2} \left\|\hat{1}_A - \delta \hat{1}_N\right\|_\infty.$$

We use this in Equation 3.3.1 to get

$$K(A) \geq \delta^k K(N) - k(\delta N)^{k-2} \left\|(\hat{1} - \delta \hat{1}_N)\right\|_\infty.$$

If we suppose that Equation 3.1.1 has only trivial solutions in A then we would have $K(A) = \delta N$ and this together with the last equation gives

$$\left\|(\hat{1}_A - \delta \hat{1}_N)\right\|_\infty \geq \frac{\delta^k K(N)}{k(\delta N)^{k-2}} - \frac{1}{k(\delta N)^{k-3}}. \tag{3.3.3}$$

We shall use Roth's Uniformity Lemma and the following Lemma to prove the above result.

Lemma 3. *: $K(N) \gg_{\mathbf{x}} N^{k-1}$.*

Proof of Lemma: We define

$$c_i = \frac{x_i}{-x_k} \qquad (1 \le i \le k)$$

and

$$C_+ = \sum_{c_i > 0} c_i, \quad C_- = -\sum_{c_i < 0} c_i.$$

Then $C_+ - C_- = 1$ and $C_+ > 0$. Write

$$I_N = [\frac{N}{2}, \frac{N}{2} + \frac{N}{2C_+}] \cap \mathbb{Z}.$$

We claim that

If $y_1, \cdots, y_{k-1} \in I_N$ then

$$c_1 y_1 + \cdots + c_{k-1} y_{k-1} \in]0, N].$$

To prove the claim we note that

$$\begin{aligned} c_1 y_1 + \cdots + c_{k-1} y_{k-1} &\ge \frac{C_+ N}{2} - C_- \left(\frac{N}{2} + \frac{N}{2C_+} \right) \\ &= \frac{N}{2C_+} > 0 \end{aligned}$$

and

$$c_1 y_1 + \cdots + c_{k-1} y_{k-1} \le \left(\frac{N}{2} + \frac{N}{2C_+} \right) C_+ - \frac{N}{2} C_- = N,$$

which proves the claim.

Next it is easy to see that:

For $\mathbf{n} = (n_1, \cdots, n_{k-1}) \in I_N^{k-1}$ the following conditions are equivalent:

- $c_1 n_1 + \cdots + c_{k-1} n_{k-1} \in \mathbb{Z}$.
- $n_1 x_1 + \cdots + n_{k-1} x_{k-1} \equiv 0 \bmod \left| x_k \right|$,

  and that the latter condition holds when $n_i \in \overline{r}$ for some $r \in [1, x_k]$. Now by the pigeon-hole principle, there exists an r such that

$$\left| I_N \cap \overline{r} \right| \ge \frac{\left| I_N \right|}{\left| x_k \right|}.$$

Therefore

$$\begin{aligned}
K(N) &= \left|\{\mathbf{n} \in [1,N]^k : n_1x_1 + \cdots + n_kx_k = 0\right| \\
&= \left|\{\mathbf{n} \in [1,N]^{k-1} : c_1n_1 + \cdots + c_{k-1}n_{k-1} \in [1,N]\}\right| \\
&\geq \left|\{\mathbf{n} \in I_N^{k-1} : c_1n_1 + \cdots + c_{k-1}x_{k-1} \in]0,N] \cap \mathbb{Z}\}\right| \\
&= \left|\{\mathbf{n} \in I_N^{k-1} : c_1n_1 + \cdots + c_{k-1}x_{k-1} \in \mathbb{Z}\right| \\
&\geq \left|I_N \cap \overline{r}\right|^{k-1} \\
&\geq \left(\frac{\left|I_N\right|}{\left|x_k\right|}\right)^{k-1}.
\end{aligned}$$

Now if $N \geq 6C_+$ then

$$\left|\left[\tfrac{N}{2}, \tfrac{N}{2} + \tfrac{N}{2C_+}\right] \cap \mathbb{Z}\right| \geq \frac{N}{2C_+} - 1 \geq \frac{N}{3C_+},$$

which means that for $N \geq 6C_+$ we have

$$\begin{aligned}
K(N) &\geq \left(\frac{N}{3C_+\left|x_k\right|}\right)^{k-1} \\
&= CN^{k-1}
\end{aligned}$$

where $C = (3C_+\left|x_k\right|)^{1-k}$. Write

$$C_0 = \left|x_1\right| + \cdots + \left|x_k\right|.$$

Then

$$C_+\left|x_k\right| \leq \left|x_1\right| + \cdots + \left|x_{k-1}\right| \leq C_0.$$

Also, as $\left|x_k\right| \geq 1$, we have $C_+ \leq C_0$. Therefore we can conclude that *for $N \geq 6C_0$ we have*

$$K(N) \geq \left(\frac{N}{3C_0}\right)^{k-1},$$

which completes the proof of the lemma. ■

We now complete the proof of the theorem.

Using 3.3.3 and the previous lemma, one has

$$\left\|\hat{1}_A - \delta\hat{1}_N\right\| \gg_{\mathbf{x}} N\delta^2 - \frac{1}{(\delta N)^{k-3}} \geq N\delta^2 - 1.$$

Choose N big enough, namely $N \gg_{\mathbf{x}} \delta^{-4}$ and put $N_0 = \left\lceil \sqrt[4]{N} \right\rceil$, the smallest positive integer greater than the fourth root of N. Then Roth's Uniformity Lemma gives

$$E_A(N_0) - \delta \gg_{\mathbf{x}} \left(\frac{\delta^2}{2} - 9N^{-\frac{1}{4}} \right) \gg_{\mathbf{x}} \delta^2.$$

Thus we may state

$$\boxed{N^{\frac{1}{4}} \gg_{\mathbf{x}} \delta^{-2} \implies E_A(N) - \delta \gg_{\mathbf{x}} \delta^2, \qquad (3.3.4)}$$

or, assuming the implied constants to be respectively η_0 and κ_0, we can state it as

$$\boxed{N^{\frac{1}{4}} \geq \eta_0 \delta^{-2} \implies E_A(N) - \delta \geq \kappa_0 \delta^2 \qquad (3.3.5)}$$

We now settle the theorem. We are supposing that $A \subset [1, N]$ has density $\delta > 0$ and contains no $\mathbf{x}$-progressions. If $N^{\frac{1}{4}} \geq \eta_0 \delta^{-2}$ then by 3.3.5 and Roth's Uniformity Lemma we can obtain a subset A_0 of $[1, N_0]$, where $N_0 = \lceil N^{\frac{1}{4}} \rceil$, of density $\delta_0 \geq \delta + \kappa_0 \delta^2$ which does not contain any $\mathbf{x}$-progression.

Again, if $N_0^{\frac{1}{4}} \geq \eta_0 \delta_0^{-2}$, we can iterate the previous step to obtain a subset A_1 of $[1, N_1]$, where $N_1 = \lceil N_0^{\frac{1}{4}} \rceil$, of density $\delta_1 \geq \delta_0 + \kappa_0 \delta_0^2$ which does not contain any $\mathbf{x}$-progression.

Now note that since $N_0 \geq N^{\frac{1}{4}}$ and $\delta_0 \geq \delta$, the condition for the second step (i.e., the condition $N_0 \geq \eta_0 \delta_0^{-2}$) is satisfied if $N^{\frac{1}{16}} \geq \eta_0 \delta^{-2}$ (note that we can choose η_0 to be ≥ 1).

We thus weaken to conclusion as follows: If $N^{\frac{1}{16}} \geq \eta_0 \delta^{-2}$, then there exists a subset A_1 of $[1, N_1]$ of density $\delta_1 \geq \delta + 2\kappa_0 \delta^2$ (observe that in fact we have earlier obtained a density $\delta_1 \geq \delta_0 + \kappa_0 \delta_0^2$, where the term on the right, $\delta_0 + \kappa_0 \delta_0^2$, is much greater than $\delta + 2\kappa_0 \delta^2$). Thus by iteration, we can state the following:

for any $n \in \mathbb{N}$, $N^{\frac{1}{4^n}} \geq \eta_0 \delta^{-2} \implies \exists A_n \subset [1, N_n]$ (where for $n = 1, 2, \cdots, N_n = \lceil N_{n-1}^{\frac{1}{4}} \rceil$ inductively) *of density* $\geq \delta + n\kappa_0\delta^2$ *which does not contain any* $\mathbf{x}$*-progression.*

Now take $n_1 = \lceil \frac{1}{\delta\kappa_0} \rceil$ and $M^{(1)} = N_{n_1}$. Then we have the following:

$N^{\frac{1}{4^{n_1}}} \geq \eta_0\delta^{-2}$ *implies there exists a subset* $A^{(1)}$ *of* $[1, M^{(1)}]$ *of density* $\geq \delta + n_1\kappa_0\delta^2 = \delta + \lceil \frac{1}{\delta\kappa_0} \rceil \kappa_0\delta^2 \geq \delta + \frac{1}{\delta\kappa_0}\kappa_0\delta^2 = 2\delta$.

We can iterate this sub-process: Take $n_2 = \lceil \frac{1}{2\delta\kappa_0} \rceil$, $M^{(2)} = N^{(1)}_{n_2}$ Then $N^{\frac{1}{4^{n_2}}} \geq \eta_0(2\delta)^{-2}$ *implies there exists a subset* $A^{(2)}$ *of* $[1, M^{(2)}]$ *of density* $\geq 2^2\delta$.

Observe that since $M^{(1)} \geq N^{\frac{1}{4^{n_1}}}$, then $N^{\frac{1}{4^{n_1+n_2}}} \geq \eta_0/(2\delta)^2 \implies N^{\frac{1}{4^{n_2}}} \geq \eta_0(2\delta)^{-2}$. In general, taking $n_k = \lceil \frac{1}{2^{k-1}\delta\kappa_0} \rceil$, $M^{(k+1)} = N^{(k)}_{n_{k+1}}$, we have:

for $N^{1/4^{n_1+\cdots+n_k}} \geq \eta_0 \frac{1}{(2\delta)^k}$*, there exists a subset* $A^{(k)}$ *of* $[1, M^{(k)}]$ *of density* $\geq 2^k\delta$ *and containing no* $\mathbf{x}$*-progression.*

But if we take $K = \lceil \frac{-\log\delta}{\log 2} \rceil$ then we get a subset $A^{(K)}$ of $[1, M^{(K)}]$ of density 1, containing no $\mathbf{x}$-progression, which is absurd. Thus the proof of the theorem is complete. $\blacksquare$.

Remerciements

Mes plus sincères remerciements vont à Mme Gautami Bhowmik pour tous ses efforts: d'abord pour l'obtention d'une bourse, et ensuite à travers les paperasseries administratives presque insupportables qu'entraîne le procédé d'obtention du visa français depuis l'Inde, et puis surtout pour tous ses encouragements et des discussions avec moi tout au long de mon travail. En même temps, je tiens également à remercier sincèrement le Professeur HK Mukerjee du NEHU pour ses conseils judicieux.

Je voudrais ensuite remercier les *Relations Internationales* pour le financement, et le Laboratoire Paul Painlevé, sans lesquels je n'aurais pas pu apprendre toutes les mathématiques élegantes que nous avons été appris ici dans les classes de Master 2.

Mes prochaines gratitudes sincères vont à tous les membres du jury qui ont pris leurs temps pour examiner la première version de ce mémoire, et qui ont daigné rester membres du jury lors de la soutenance.

Enfin, je tiens à exprimer ma sincère gratitude à mes amis Fanasina et Fabien, qui tout au long de mon travail me fournirent des matériaux dont j'eus besoin, et qui se sont toujours efforcés de me guider quand j'en ai besoin.

Bibliography

1. KF Roth, On certain sets of integers. *Journal of London Mathematical Society.* **28** (1953), 104-109.
2. Sean Prendiville, Roth's Theorem - An Exposition. November 13, 2008.
3. A Iosevich, Roth's theorem on arithmetic progressions. September 17, 2003.
4. R Graham, B Rothschild and J Spencer, *Ramsey Theory*, John Wiley and Sons, Inc (1990).
5. Terence Tao and Van H Vu, *Additive Combinatorics*, Cambridge University Press, 2006.
6. Melvyn B Nathanson, *Additive Number Theory* Inverse Problems and the Geometry of Sumsets, Springer (1996).
7. Andrew Granville, Melvyn B Nathanson, Jozsef Solymosi (*Editors*), *Additive Combinatorics,* CRM PROCEEDINGS & LECTURE NOTES, American Mathematical Society (2007).
8. GH Hardy and EM Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press (1962).
9. Tom M Apostol, *An Introduction to Analytic Number Theory*, Springer (1998).