On K. F. Roth's 'On Certain Sets of Integers'

David J. Wilson
Advised by Prof. D. Zeilberger

Masters Essay

Contents

List of Algorithms

Acknowledgements

This essay would not have been possible without the guidance and direction of Professor Doron Zeilberger. The bulk of the contents stemmed from a reading course with Professor Zeilberger where he helped me illuminate sections of the proof, influenced me with a strong work ethic and suggested the creation of an 'interactive' version of the paper. Giving his time selflessly, I am truly grateful for all of his help.

I am ever grateful to the UK–US Fulbright Commission, whose scholarship allowed me to study in the United States in the first place and through which I have met so many amazing people and visited many fascinating places.

I am also thankful to the Rutgers Mathematics Department for their support as I pursued my Masters.

Finally, I am eternally indebted to my family and friends for their support. In particular to my parents Margie and Kevin Wilson who have always encouraged me both academically and as a person. They give me all the strength and support I could need.

DJW

Chapter 1

Motivation and Aim

In this Masters Essay we shall inspect Roth's seminal paper on three-term arithmetic progressions in the integers, [12]. The aim is to fully understand the original proof, which is rather harsh in its brevity. All of the steps that Roth did not expand on will be re-proven independently and described with due clarity. This will all be done with the aid of symbolic computation and empirical evidence, and sample code for Maple is given in Appendix A.

We will follow Roth's exact method and have thus split his paper into six sections for ease of reference. If the reader would like a general feel of the proof they may read Section 2.7 which gives an overview of Roth's Method.

We will also look at methods of proof other than that which Roth employed, and the bounds that they provide. Finally, some generalizations of Roth's Theorem are given including Szeméredi's Theorem, the Green–Tao Theorem and the Erdős-Turán Conjecture.

Chapter 2

"On Certain Sets of Integers"

2.1 Main Result From "On Certain Sets of Integers" [12]

In [12] Roth looked at three term arithmetic sequences in certain sets of integers. He considered a function, called $A(x)$, that was the maximum size of a subset of $\{1, 2, \ldots, x\}$ that avoided three term arithmetic sequences. Having already proven the main result:

$$\frac{A(x)}{x} \longrightarrow 0 \qquad \text{as} \qquad x \longrightarrow \infty$$

Roth used the paper to proved a tighter aymptotic and so proved the following:

Theorem 1 (Roth's Theorem)**.**

$$\frac{A(x)}{x} = O\left(\frac{1}{\log\log x}\right)^{1} \tag{2.1}$$

2.2 Key Definitions (Section 1)

Notation 2. Throughout the paper a small Latin letter will denote a positive integer, unless otherwise stated. The main exceptions are h, which denotes any integer, and $c_1, c_2, \ldots$, which denote absolute constants (and any constants implied from O notation are also inherently absolute).

[1]The standard O notation is that $f(y) = O(g(y))$ if and only if there exists an absolute constant M such that for all sufficiently large y, $|f(y)| \leq M \cdot |g(y)|$.

We start with some basic definitions.

Definition 3. For any positive integer x, define the set

$$\langle x \rangle := \{1, 2, \ldots x\}$$

Definition 4. A subset $\{u_1, u_2, \ldots\}$ of the natural numbers $\mathbb{N}$ will be called an **$\mathcal{A}$-set** if no three elements are in arithmetic progression. If such a progression did exist, there would exist positive integers a and d and indices j,k,l such that

$$u_j = a; \qquad u_k = a + d; \qquad u_l = a + 2d;$$

and so they would satisfy the equation $u_j + u_k = u_l$. Indeed, if there exists a non-trivial solution of this equation (where j,k and l are distinct) then setting a to be u_j and d to be $u_k - u_j$ would exhibit an arithmetic progression of length three.

We see therefore that a set is a $\mathcal{A}$-set if and only if the only solution to $u_j + u_k = 2u_l$ is when $j = k = l$. Note, that if any two of j,k and l are equal then necessarily the third must also be identical, which simplifies matters.

Definition 5. We now define the function $A(x)$ as follows:

$$A(x) := \max \{|S| \mid S \subseteq \langle x \rangle, S \text{ an } \mathcal{A}\text{-set}\}.$$

We also define the function $a(x)$ as follows:

$$a(x) := \frac{A(x)}{x}.$$

We can therefore restate the main aim of the paper, Equation (2.1), as

$$a(x) = O\left(\frac{1}{\log \log x}\right). \tag{2.2}$$

2.3 'Obvious' Remarks (Section 2)

The first of Roth's obvious remarks is that the function $A(x)$ is equal to the greatest number of integers that can be selected from x consecutive terms of an arithmetic sequence that forms an $\mathcal{A}$-set. We prove this in the following lemma.

Lemma 6. *$A(x)$ is equal to the greatest number of integers that can be selected from x consecutive terms of an arithmetic progression to form an $\mathcal{A}$-set.*

Proof. This is easy to see as x consecutive terms in arithmetic progression:

$$\mathcal{A}_1 = \{a + b \cdot u_1, a + b \cdot u_2, \ldots, a + b \cdot u_x\}$$

correspond to x consecutive integers

$$\mathcal{A}_2 = \{u_1, u_2, \ldots, u_x\}$$

and as $(a+b\cdot u_k)-(a+b\cdot u_l) = b\cdot(u_k-u_l)$ we see that a three term sequence in $\mathcal{A}_1$ is arithmetic if and only if the corresponding three term sequence in $\mathcal{A}_2$ is arithmetic. □

Now we state a series of inequalities involving the $A(x)$ and $a(x)$ functions.

Lemma 7. *For any two positive integers x and y we have that*

$$A(x + y) \leq A(x) + A(y)$$

Proof. First we recall the definition of $A(x + y)$:

$$A(x + y) = \max\{|S| \mid S \subset \langle x + y\rangle, S \text{ a } \mathcal{A}\text{-set}\}$$

and similarly

$$A(x) = \max\{|S| \mid S \subset \langle x\rangle, S \text{ a } \mathcal{A}\text{-set}\}.$$

We now apply Lemma 6 to alter the definition of $A(y)$ to the following:

$$A(y) = \max\{|S| \mid S \subset \{x + 1, x + 2, \ldots, x + y\}, S \text{ a } \mathcal{A}\text{-set}\}. \tag{2.3}$$

Let $S_1 \subset \langle x+y\rangle$ be an $\mathcal{A}$-set such that $|S_1| = A(x+y)$. Now a subset of an $\mathcal{A}$-set is definitely still an $\mathcal{A}$-set (if a set contains no three-term arithmetic sequences, a subset cannot contain any either). We therefore see that $S_1 \cap \langle x\rangle$ is an $\mathcal{A}$-set and a subset of $\langle x\rangle$. To that extent, we have

$$|S_1 \cap \langle x\rangle| \leq A(x). \tag{2.4}$$

Similarly, we have $S_1 \cap \{x + 1, \ldots, x + y\}$ also an $\mathcal{A}$-set and a subset of $\{x + 1, \ldots, x + y\}$. From the definition of $A(y)$ given in (2.3) we see

$$|S_1 \cap \{x + 1, \ldots, x + y\}| \leq A(y). \tag{2.5}$$

Finally, combining (2.4) and (2.5) we get

$$\begin{aligned} A(x + y) &= |S_1| \\ &= |S_1 \cap \langle x\rangle| + |S_1 \cap \{x + 1, \ldots, x + y\}| \\ &\leq A(x) + A(y), \end{aligned}$$

as required.

□

As easy consequences to Lemma 7 we get the following corollaries.

Corollary 8. *For any positive integers x and y we have*

$$A(x \cdot y) \leq x \cdot A(y).$$

Proof. From Lemma 7 we have

$$A(x \cdot y) \leq A(y) + A((x-1) \cdot y),$$

and repeating x times we see

$$A(x \cdot y) \leq x \cdot A(y).$$

□

Corollary 9. *For any positive integers x and y we have*

$$A(x) \leq A\left(\left(\left[\frac{x}{y}\right]+1\right) \cdot y\right) \leq \frac{x+y}{y} \cdot A(y).$$

Proof. The first inequality follows as for any positive y we have

$$x \leq \left(\left[\frac{x}{y}\right]+1\right) \cdot y$$

and the function A is non-decreasing.

The second inequality is a direct consequence from Corollary 8, noting that

$$\left(\left[\frac{x}{y}\right]+1\right) \leq \frac{x+y}{y}.$$

□

We now use these corollaries to obtain some results regarding the function $a(x)$. Namely:

Corollary 10. *For any positive integers x and y we have*

$$a(x \cdot y) \leq a(y).$$

Proof. We simply utilize the definition of the function $a(x)$ and Corollary 8:

$$a(x \cdot y) = \frac{A(x \cdot y)}{x \cdot y} \leq \frac{x \cdot A(y)}{x \cdot y} = \frac{A(y)}{y} = a(y).$$

□

Corollary 11. *For any positive integers x and y we have:*

$$a(x) \leq \left(1 + \frac{y}{x}\right) \cdot a(y).$$

Proof. We use the definition of $a(x)$ along with Corollary 9:

$$\begin{aligned} a(x) = \frac{A(x)}{x} &\leq \frac{1}{x} \cdot \left(\frac{x+y}{y} \cdot A(y)\right) \\ &= \left(\frac{1}{y} + \frac{1}{x}\right) \cdot A(y) \\ &= \left(1 + \frac{y}{x}\right) \cdot \frac{A(y)}{y} = \left(1 + \frac{y}{x}\right) \cdot a(y). \end{aligned}$$

□

Finally, we have a truly trivial identity.

Lemma 12. *For any positive integer x we have*

$$\frac{1}{x} \leq a(x) \leq 1.$$

Proof. From the definition of $A(x)$ we see that $A(x)$ is the size of a non-empty subset of $\langle x \rangle$ and so

$$1 \leq A(x) \leq x.$$

But, by definition, $A(x) = x \cdot a(x)$ and so

$$1 \leq x \cdot a(x) \leq x$$

which give us (on division by positive x) our desired result:

$$\frac{1}{x} \leq a(x) \leq 1.$$

□

2.4 Some Number Theory (Section 3)

For this section we now fix $\{u_1, u_2, \ldots, u_U\}$ to be a maximal $\mathcal{A}$-set in $\langle M \rangle$, so that $A(M) = U$.

Definition 13. For any number θ define, for notational purposes, the function

$$e(\theta) = e^{2\pi i \theta}. \tag{2.6}$$

Denote by S the following exponential sum, where α is an arbitrary real number.

$$S = \sum_{k=1}^{U} e(\alpha \cdot u_k) = \sum_{k=1}^{U} e^{2\pi i \alpha u_k}.$$

We now use some basic number theory to show that for any α, with M fixed, we can find h, q and β such that

$$\alpha = \frac{h}{q} + \beta \tag{2.7}$$

and the constants satisfy the following conditions:

$$\begin{aligned} (h, q) &= 1, & (2.8)\\ q &\leq \sqrt{M}, & (2.9)\\ q \cdot |\beta| &\leq \frac{1}{\sqrt{M}}. & (2.10) \end{aligned}$$

This is the Dirichlet Approximation Theorem, restated as follows:

Theorem 14. *[15] Let α be a positive real number (α negative follows immediately) and $\widehat{M}$ a positive integer. Then there exists an integer q and an integer h with $0 < q < \widehat{M}$, for which*

$$-\frac{1}{\widehat{M}} < q \cdot \alpha - h < \frac{1}{\widehat{M}}. \tag{2.11}$$

Proof. This result follows, perhaps surprisingly, from the Pigeonhole Principle. That is, the fact that if you have l pigeonholes and strictly more than l pigeons, then at least one pigeonhole must contain more than one pigeon.

We consider the following numbers

$$\alpha_i = (i \cdot \alpha) - \lfloor i \cdot \alpha \rfloor, \qquad i = 0, 1, 2, \ldots, \widehat{M} \tag{2.12}$$

and note that each α_i (being the non-integral part of $i\alpha$) is contained in the interval $[0, 1)$.

We now split $[0,1)$ into $\widehat{M}$ subintervals

$$\left[\frac{r}{\widehat{M}}, \frac{r+1}{\widehat{M}}\right) \qquad r = 0, 1, \ldots, \widehat{M} - 1.$$

We now have $\widehat{M}$ subintervals and $\widehat{M}+1$ numbers, so by the pigeonhole principle there exists at least one subinterval containing two of the numbers, say α_k and α_j.

We therefore know that $-\frac{1}{\widehat{M}} < \alpha_k - \alpha_j < \frac{1}{\widehat{M}}$. Then we see that by using the definition of the α_i we have

$$-\frac{1}{\widehat{M}} < (k-j)\cdot\alpha - (\lfloor k\cdot\alpha\rfloor - \lfloor j\cdot\alpha\rfloor)$$

Repeating with $\alpha_j - \alpha_k$ and denoting $(\lfloor k\cdot\alpha\rfloor - \lfloor j\cdot\alpha\rfloor)$ by H we get

$$\begin{aligned} -\frac{1}{\widehat{M}} < &\quad (k-j)\cdot\alpha - H &< \frac{1}{\widehat{M}} \\ -\frac{1}{\widehat{M}} < &\quad (j-k)\cdot\alpha + H &< \frac{1}{\widehat{M}} \end{aligned}$$

Now to finish the proof, if $k > j$ put $q = k - j$ and $h = H$. If $k < j$ we set $q = j - k$ and $h = -H$. It follows from our construction that these choices satisfy the needed conditions.

□

Let $m < M$, and we now define

$$S' = \frac{a(m)}{q}\cdot\left(\sum_{r=1}^{q} e\left(\frac{r\cdot h}{q}\right)\right)\cdot\left(\sum_{n=1}^{M} e\left(\beta\cdot n\right)\right)$$

which obviously depends on m (and also M and α which we assume are fixed).

Lemma 15. *If $q > 1$ then $S' = 0$.*

Proof. If $q > 1$ then we look at the factor

$$\begin{aligned} \left(\sum_{r=1}^{q} e\left(\frac{r\cdot h}{q}\right)\right) &= \left(\sum_{r=1}^{q} e^{2\cdot\pi\cdot i\cdot\left(\frac{r\cdot h}{q}\right)}\right) \\ &= \left(\sum_{r=1}^{q}\left(e^{2\cdot\pi\cdot i\cdot\left(\frac{r}{q}\right)}\right)^{h}\right) \end{aligned}$$

Now as $(h,q) = 1$ we see that $r\cdot h$ modulo q produces all the integers from 0 to $q-1$ and so the sum (as $q \neq 1$) gives us 0.

□

For the rest of this section we aim to prove the following theorem, which will be essential later in our method.

Theorem 16. *The following inequality holds:*

$$|S - S'| < M \cdot a(m) - U + O\left(m \cdot \sqrt{M}\right) \tag{2.13}$$

(Recall that U is the size of our $\mathcal{A}$-set within $\langle M \rangle$ and that $m < M$).

We prove this through a series of lemmata.

Lemma 17. *We can rewrite S as:*

$$S = \frac{1}{m \cdot q} \cdot \sum_{r=1}^{q} \sum_{n=1}^{M} \sum_{\substack{n \le u_k < n + m \cdot q \\ u_k \equiv r (mod q)}} e(\alpha \cdot u_k) + O(m \cdot q) \tag{2.14}$$

Proof. First we note that for a fixed u_k, fixed m and fixed q then there are precisely $m \cdot q$ integers n satisfying

$$n \le u_k < n + m \cdot q,$$

namely, the set $\{u_k - (m \cdot q) + 1, u_k - (m \cdot q) + 2, \ldots, u_k - 1, u_k\}$.

Also if

$$m \cdot q \le u_k < M - m \cdot q$$

then it is clear that these values of n must lie in $[1, M]$.

Now, if $m \cdot q \le u_k < M - m \cdot q$ then from above the coefficient of $e(\alpha u_k)$ simplifies to $\frac{mq}{mq}$, that is, 1. This gives us the summation of exponential terms in Equation (2.14).

However, if $u_k < mq$ or $M - mq \le u_k \le M$ then there are at most $2mq$ terms to consider, which is compensated for, by the $O(mq)$ term.

□

Now we take (2.14) and rewrite it in to involve S'.

Lemma 18. *We will show that*

$$S = S' - \left(\frac{1}{mq} \sum_{r=1}^{q} e\left(\frac{rh}{q}\right) \sum_{n=1}^{M} e(\beta n) D(n, m, q, r) \right) + O(mq) + O(mqM|\beta|), \tag{2.15}$$

where $D(n, m, q, r) \ge 0$.

Proof. We begin by looking at the inner sum of the representation of S in (2.14). By the Dirichlet Box Principle in (2.7) we have

$$\begin{aligned} e(\alpha u_k) &= e\left(\left(\frac{h}{q}+\beta\right)u_k\right) \\ &= e\left(\frac{h}{q}u_k\right)e(\beta u_k). \end{aligned}$$

But we can now use the fact that all the terms in this inner sum obey

$$u_k \equiv r \mod q$$

to rewrite u_k as $Qq + r$ so that this becomes

$$\begin{aligned} e(\alpha u_k) &= e\left(\frac{h(Qq+r)}{q}\right)e(\beta u_k) \\ &= e(hQ)e\left(\frac{hr}{q}\right)e(\beta u_k). \end{aligned}$$

We now write u_k as $n + \eta$ where $0 \leq \eta < mq$ (as we are only dealing with terms such that $n \leq u_k < n + mq$)to simplify further:

$$\begin{aligned} e(\alpha u_k) &= e(hQ)e\left(\frac{hr}{q}\right)e(\beta(n+\eta)) \\ &= e(hQ)e\left(\frac{hr}{q}\right)e(\beta n)e(\beta\eta) \\ &= e\left(\frac{hr}{q}\right)\cdot e\left(\beta n\right)\cdot\left(e(hQ)\cdot e(\beta\eta)\right) \\ &\leq e\left(\frac{hr}{q}\right)\cdot e\left(\beta n\right)\cdot(1+hQ|\beta|\eta) \\ &= e\left(\frac{hr}{q}\right)\cdot e\left(\beta n\right)+O(mq|\beta|). \end{aligned}$$

We know that at most the number of terms in this inner section is $A(m)$ (as $A(m)$ also applies to arithmetic sequences). We can write this number as $A(m) - D(n, m, q, r)$ where $D \geq 0$.

We now replace each term in (2.14) with the above representation and so we can

rewrite S as follows:

$$\begin{aligned}
S &= \frac{1}{mq}\sum_{r=1}^{q}\sum_{n=1}^{M}\sum_{\substack{n\le u_k<n+mq\\ u_k\equiv r \mod q}} e(\alpha u_k)+O(mq)\\
&= \frac{1}{mq}\sum_{r=1}^{q}\sum_{n=1}^{M}\sum_{\substack{n\le u_k<n+mq\\ u_k\equiv r \mod q}} e\left(\frac{rh}{q}\right)e(\beta n)+O(mq|\beta|)+O(mq)\\
&= \frac{1}{mq}\sum_{r=1}^{q} e\left(\frac{rh}{q}\right)\sum_{n=1}^{M}\left(A(m)-D(n,m,q,r)\right)\left(e(\beta n)+O(mq|\beta|)\right)\\
&\qquad\qquad +O(mq)\\
&= \left(\frac{A(m)}{m}\cdot\frac{1}{q}\sum_{r=1}^{q} e\left(\frac{rh}{q}\right)\sum_{n=1}^{M} e(\beta n)+O(mqM|\beta|)\right)\\
&\quad -\left(\frac{1}{mq}\sum_{r=1}^{q} e\left(\frac{rh}{q}\right)\sum_{n=1}^{M} e(\beta n)D(n,m,q,r)+O(mqM|\beta|)\right)+O(mq)\\
&= S'-\left(\frac{1}{mq}\sum_{r=1}^{q} e\left(\frac{rh}{q}\right)\sum_{n=1}^{M} e(\beta n)D(n,m,q,r)\right)\\
&\qquad\qquad +O(mq)+O(mqM|\beta|)
\end{aligned}$$

as required.

□

We are now in a position to prove Theorem 16:

Theorem 19 (Referred to earlier as Theorem 16)**.** *The following inequality holds:*

$$|S-S'|<M\cdot a(m)-U+O\left(m\cdot\sqrt{M}\right) \tag{2.16}$$

(Recall that U is the size of our $\mathcal{A}$-set within $\langle M\rangle$ and $m<M$).

Proof. We start by setting β and h to be zero to make some estimations. This is allowed as we have not yet used that $(h,q)=1$. We are first going to estimate

$$\sum_{r=1}^{q}\sum_{n=1}^{M} D(n,m,q,r).$$

To do this we substitute $\beta = 0$ and $h = 0$ back into (2.15) to get

$$\begin{aligned} S &= S' - \frac{1}{mq}\sum_{r=1}^{q} e(0) \sum_{n=1}^{M} e(0) D(n,m,q,r) + O(mq) + O(0) \\ &= S' - \frac{1}{mq}\sum_{r=1}^{q}\sum_{n=1}^{M} D(n,m,q,r) + O(mq). \end{aligned} \tag{2.17}$$

But now, if β and h are 0, then so is α and so

$$S = \sum_{k=1}^{U} 1 = U,$$

and

$$\begin{aligned} S' &= \frac{a(m)}{q}\left(\sum_{r=1}^{q} e(0)\right)\left(\sum_{n=1}^{M} e(0)\right) \\ &= \frac{Ma(m)q}{q} = Ma(m) \end{aligned}$$

We can then substitute back into (2.17) to get

$$U = Ma(m) - \frac{1}{mq}\sum_{r=1}^{q}\sum_{n=1}^{M} D(n,m,q,r) + O(mq)$$

and so when h and β are zero we have:

$$\sum_{r=1}^{q}\sum_{n=1}^{M} D(n,m,q,r) = mMqa(m) - Umq + O(mq). \tag{2.18}$$

We are now going to use (2.15) and (2.18) to show (2.16). As α is positive, we can estimate as follows:

$$\begin{aligned} |S - S'| &= \left| -\left(\frac{1}{mq}\sum_{r=1}^{q} e\left(\frac{rh}{q}\right)\sum_{n=1}^{M} e(\beta n) D(n,m,q,r)\right) \right. \\ &\qquad \left. + O(mq) + O(mqM|\beta|)\right| \\ &< \frac{1}{mq}\left(mMqa(m) - Umq\right) + O(mq) + O(mqM|\beta|) \\ &= Ma(m) - U + O(mq) + O(Mmq|\beta|). \end{aligned}$$

and we use the fact that $q \leq M^{\frac{1}{2}}$ and $q|\beta| \leq M^{-\frac{1}{2}}$ and get

$$\begin{aligned} |S - S'| &< Ma(m) - U + O\left(mM^{\frac{1}{2}}\right) + O\left(MmM^{-\frac{1}{2}}\right) \\ &= Ma(m) - U + O\left(mM^{\frac{1}{2}}\right) \end{aligned}$$

which is what was required.

□

This theorem will be fundamental to our application of the Hardy-Littlewood Method, which is covered in the following section.

2.5 Adaptated Hardy-Littlewood Method (Section 4)

Let m now be an even integer and so we also have m^4 being even, and can find N such that $2N = m^4$.

Let $u_1, \ldots, u_U$ be a maximal $\mathcal{A}$-set from $\{1, \ldots .2N\}$ so we have

$$U = A(2N) = 2Na(2N).$$

Now let $2v_1, 2v_2, \ldots, 2v_V$ be the even integers among $\{u_1, u_2, \ldots, u_U\}$.

Lemma 20. *We show that*

$$U \leq 2Na(m)$$

and

$$V \leq A(N) \leq Na(m).$$

Proof. We use the fact that $a(xy) \leq a(y)$ to get

$$U = 2Na(2N) = 2Na(m^4) \leq 2Na(m).$$

Now the V numbers $2v_1, \ldots, 2v_V$ are selected from N possible even integers between 1 and $2N$ and so by definition

$$V \leq A(N) = Na(N)$$

but we know that $N = \frac{m^4}{2}$ which is larger than m for all $m \geq 2$, and so

$$V \leq Na\left(\frac{m^4}{2}\right) \leq Na(m).$$

□

Lemma 21. *We now show that*

$$V \geq A(2N) - A(N) \geq 2Na(2N) - Na(m).$$

Proof. The number of odd integers among the u_k certainly can't exceed $A(N)$ (by the equivalence of A under arithmetic progressions) and so

$$A(2N) \leq \max \text{ even} + \max \text{ odd} = V + A(N) \leq V + Na(m).$$

We can therefore conclude

$$V \geq A(2N) - A(N)$$

and

$$U = A(2N) \leq 2Na(2N)$$

and so

$$V \geq 2Na(2N) - A(N)$$

and

$$V \geq A(2N) - Na(m) = 2Na(2N) - Na(m)$$

□

Definition 22. We define the following key functions:

$$\begin{aligned} f_1(\alpha) &= \sum_{k=1}^{U} e(\alpha u_k) \\ f_2(\alpha) &= \sum_{k=1}^{V} e(\alpha v_k) \\ F_1(\alpha) &= a(m) \sum_{n=1}^{2N} e(\alpha n) \\ F_2(\alpha) &= a(m) \sum_{n=1}^{N} e(\alpha n). \end{aligned}$$

These are analogues of Fourier Transforms of indicator functions on the u_i and v_i. We want to estimate these functions so that later we can estimate integrals involving $f_1(\alpha)$, $f_2(\alpha)$, $F_1(\alpha)$ and $F_2(\alpha)$.

Lemma 23. *Our first estimate is that all the functions are of a similar order:*

$$\begin{aligned} f_1(\alpha) &= O(N \cdot a(m)); \\ f_2(\alpha) &= O(N \cdot a(m)); \\ F_1(\alpha) &= O(N \cdot a(m)); \\ F_2(\alpha) &= O(N \cdot a(m)). \end{aligned}$$

Proof. We use the fact that $U \leq 2Na(m)$ and $V \leq Na(m)$ to see that for $r = 1, 2$ we have

$$\begin{aligned} |f_r(\alpha)|, |F_r(\alpha)| &\leq 2 \cdot N \cdot a(m) \cdot \max_{k,n}\{e(\alpha u_k), e(\alpha n\} \\ &= 2 \cdot N \cdot a(m) \cdot \text{constant} \end{aligned}$$

so that

$$f_r(\alpha), F_r(\alpha) = O(N \cdot a(m)).$$

□

Lemma 24. *We now want to estimate the difference between these functions, showing that*

$$\begin{aligned} f_1(\alpha) - F_1(\alpha) &= O\left(N \cdot \{a(m) - a(2N)\} + N^{\frac{3}{4}}\right); \\ f_2(\alpha) - F_2(\alpha) &= O\left(N \cdot \{a(m) - a(2N)\} + N^{\frac{3}{4}}\right). \end{aligned}$$

Proof. We split into two cases, depending on whether q is equal to 1 or not. This splitting is motivated by q's effect on the exponential sum S'.

Case 1: $q = 1$

We let $M = 2N$ and consider $f_1(\alpha)$ and $F_1(\alpha)$. We know that $U = A(2N) = A(M)$ and so $f_1(\alpha) = S$. We also have the following for $F_1(\alpha)$:

$$\begin{aligned} F_1(\alpha) &= a(m) \cdot e(h) \cdot \sum_{n=1}^{2N} e(\beta n) \\ &= a(m) \cdot \sum_{n=1}^{M} e(h + \beta n) \\ &= a(m) \cdot \sum_{n=1}^{M} e(nh + \beta n) \\ &= a(m) \cdot \sum_{n=1}^{M} e(\alpha n) = S' \end{aligned}$$

as n and h are integers so $e(nh) = e(h)$ and $q = 1$ so $\alpha = h + \beta$.

We now consider (2.16) and find

$$\begin{aligned} |S - S'| &< 2Na(m) - U + O\left(m(2N)^{\frac{1}{2}}\right) \\ &= 2Na(m) - U + O\left(mN^{\frac{1}{2}}\right) \\ &= 2Na(m) - 2Na(2N) + O\left(mN^{\frac{1}{2}}\right). \end{aligned}$$

But then

$$\begin{aligned} f_1(\alpha) - F_1(\alpha) &= \pm|S - S'| \\ &= O\left(2Na(m) - 2Na(2N) + mN^{\frac{1}{2}}\right) \\ &= O\left(N\left\{a(m) - a(2N)\right\} + N^{\frac{3}{4}}\right), \end{aligned}$$

as required. Note that we use the fact that $m^4 = 2N$ and so $m = O\left(N^{\frac{1}{4}}\right)$.

We now need to consider $f_2(\alpha) - F_2(\alpha)$, and to do this we repeat much of the same argument as for $f_1(\alpha) - F_1(\alpha)$, but now set $M = N$.

Then, as $q = 1$ we have

$$S' = a(m)\sum_{n=1}^{M} e(\alpha n) = a(m)\sum_{n=1}^{N} e(\alpha n) = F_2(\alpha).$$

Now throughout Section 2.4 we assumed that S was defined on a maximal $\mathcal{A}$-set. But in fact S need not be maximal for Theorem 16 to hold (although it most definitely needs to be an $\mathcal{A}$-set); by the same argument as Theorem 16, if we set

$$S = \sum_{k=1}^{V} e(\alpha v_k); \tag{2.19}$$

then we have the bound

$$|S - S'| = O\left(M \cdot a(m) - V + O\left(m \cdot \sqrt{M}\right)\right).$$

But then we have

$$\begin{aligned} f_2(\alpha) - F_2(\alpha) &= \pm|S - S'| \\ &= O\left(M \cdot a(m) - V + O\left(m \cdot \sqrt{M}\right)\right) \\ &= O\left(N \cdot a(m) - V + O\left(m \cdot \sqrt{N}\right)\right). \end{aligned}$$

Now once again we know that $m^4 = 2N$ so that $m = O\left(N^{\frac{1}{4}}\right)$, and from Lemma 21 we have

$$V \geq 2Na(2N) - Na(m).$$

And so with some simple manipulation we have

$$\begin{aligned} f_2(\alpha) - F_2(\alpha) &= O\left(Na(m) - \{2Na(2N) - Na(m)\} + O\left(N^{\frac{3}{4}}\right)\right) \\ &= O\left(2Na(m) - 2Na(2N) + O\left(N^{\frac{3}{4}}\right)\right) \\ &= O\left(N\{a(m) - a(2N)\} + N^{\frac{3}{4}}\right); \end{aligned}$$

which was exactly what was needed.

Therefore the Lemma holds if in the Dirichlet expansion of α we can choose $q = 1$.

Case 2: $q \neq 1$

Before starting the proof for this case we need the following two lemmata and Jordan's Inequality:

Lemma 25. *[8] For any α and M,*

$$\sum_{n=1}^{M} e(\alpha n) = O\left(\frac{1}{\|\alpha\|}\right),$$

where $\|\alpha\|$ denotes the distance of α from the nearest integer

Proof. We first note that

$$e(\alpha n)e(\alpha m) = e(\alpha(m+n))$$

so the left hand side is the sum of a geometric series. We can therefore rewrite it in a closed form:

$$\sum_{n=1}^{M} e(\alpha n) = \frac{e(\alpha M) - 1}{e(\alpha) - 1} e(\alpha). \tag{2.20}$$

We wish to show that in fact for all α and M we have:

$$\left|\sum_{n=1}^{M} e(\alpha n)\right| \leq \min\left\{M, \frac{1}{2\|\alpha\|}\right\}. \tag{2.21}$$

But both sides of (2.21) are even and periodic with respect to α, with period 1. Therefore it is enough to prove the result true for $0 \leq \alpha \leq \frac{1}{2}$.

We first note that for $\alpha \in \left[0, \frac{1}{2}\right]$ we have

$$\begin{aligned} |e(\alpha) - 1| &= 2\pi \sin(\pi\alpha) \\ &\geq 4\alpha \qquad (2.22) \\ &= 4\|\alpha\| \qquad (2.23) \end{aligned}$$

where (2.23) follows from the fact that $0 \leq \alpha \leq \frac{1}{2}$ and so $\|\alpha\| = \alpha$. To obtain (2.22) we need Jordan's Inequality:

Lemma 26 (Jordan's Inequality)**.** *For any $x \in [0, \frac{\pi}{2}]$ the following inequality holds:*

$$\frac{2}{\pi} x \leq \sin(x) \leq x.$$

Proof. [10] It is sufficient to show that $\frac{\sin(x)}{x}$ decreases as x increases from 0 to $\frac{\pi}{2}$; as we know that

$$\lim_{x \to 0} \frac{\sin(x)}{x} = 1; \qquad \frac{\sin\left(\frac{\pi}{2}\right)}{\frac{\pi}{2}} = \frac{2}{\pi}.$$

We do this by showing the derivative of $\frac{\sin(x)}{x}$ is negative on the interval $(0, \frac{\pi}{2}]$. But

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{\sin(x)}{x}\right) = \frac{x\cos(x) - \sin(x)}{x^2}$$

and so it remains to show $x\cos(x) - \sin(x)$ is non-positive.

But we first note that at 0 we have

$$0 \cdot \cos(0) - \sin(0) = 0$$

and

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(x\cos(x) - \sin(x)\right) = \cos(x) - x\sin(x) - \cos(x) = -x\sin(x)$$

which is non-positive on our interval. Therefore $x\cos(x) - \sin(x) \leq 0$ and so the inequality is proven.

□

Returning to our proof, we let $\frac{1}{2M} \leq \alpha \leq \frac{1}{2}$. Applying (2.23) to (2.20) we obtain:

$$\begin{aligned}\left|\sum_{n=1}^{M} e(\alpha n)\right| &= \frac{|e(\alpha M) = 1|}{|e(\alpha) - 1|}|e(\alpha)| \\ &\leq \frac{2}{4\|\alpha\|} \cdot 1 = \frac{1}{2\|\alpha\|}.\end{aligned}$$

Now assume that $0 \leq \alpha \leq \frac{1}{2M}$, and apply the trivial bound to the sum (applying the triangle inequality):

$$\left|\sum_{n=1}^{M} e(\alpha n)\right| \leq \sum_{n=1}^{M} |e(\alpha n)| = M.$$

Finally we know that

$$0 < \|\alpha\| < 1, \qquad \text{so} \qquad \frac{1}{\|\alpha\|} > 1$$

and so

$$\begin{aligned}\left|\sum_{n=1}^{M} e(\alpha n)\right| &\leq \min\left(M, \frac{1}{2\|\alpha\|}\right) \\ &\leq \min\left(\frac{M}{\|\alpha\|}, \frac{1}{2\|\alpha\|}\right),\end{aligned}$$

and so we indeed have

$$\sum_{n=1}^{M} e(\alpha n) = O\left(\frac{1}{\|\alpha\|}\right).$$

□

Lemma 27. *If it is impossible to choose $q = 1$ in the Dirichlet Box Principle, then $\|\alpha\| > \frac{1}{\sqrt{M}}$.*

Proof. We start by noting that

$$\alpha = \frac{h}{q} + \beta$$

and so if $q \neq 1$ we must have

$$\|\alpha\| = \frac{k}{q} \pm \beta$$

where $1 < |k| \leq |h|$.

We also know from the Dirichlet Approximation Theorem that

$$q \leq \sqrt{M}$$

and so

$$\|\alpha\| \geq \frac{k}{\sqrt{M}} \pm \beta.$$

But we also know that $q|\beta| \leq \frac{1}{\sqrt{M}}$ and $|q > 1|$ so

$$\|\alpha\| \geq \frac{k-1}{\sqrt{M}} > \frac{1}{\sqrt{M}}.$$

□

Now we have the previous lemmata, we can prove the result for $q \neq 1$.

Combining Lemma 25 and Lemma 27 we have that if $q \neq 1$:

$$F_1(\alpha) = \sum_{n=1}^{M} e(\alpha n) = O\left(\sqrt{M}\right).$$

We also know that if $q > 1$ we must have $S' = 0$ (from Lemma 15) and so applying Theorem 16 (with $M = 2N$) we get

$$f_1(\alpha) = \pm \left| \sum_{k=1}^{U} e(\alpha u_k) \right| = \pm|S| < M \cdot a(m) - U + O\left(m \cdot \sqrt{M}\right).$$

and so

$$f_1(\alpha) = O\left(2Na(m) - 2Na(2N) + N^{\frac{3}{4}}\right).$$

Now we use a crude estimate by the triangle inequality

$$\begin{aligned} |f_1(\alpha) - F_1(\alpha)| &\leq |f_1(\alpha)| + |F_1(\alpha)| \\ &\leq O\left(N\left\{a(m) - a(2N\right\} + N^{\frac{3}{4}}\right) + O\left(\sqrt{N}\right). \end{aligned}$$

But we can easily compensate for the $O\left(\sqrt{N}\right)$ by the $N^{\frac{3}{4}}$ in the first asymptotic, and so we obtain

$$f_1(\alpha) - F_1(\alpha) = O\left(N\left\{a(m) - a(2N)\right\} + N^{\frac{3}{4}}\right)$$

and our first case for $q \neq 1$ is proven.

For $f_2(\alpha) - F_2(\alpha)$ we apply Lemma 25 and Lemma 27 to $F_2(\alpha)$ to get

$$F_2(\alpha) = O\left(\sqrt{N}\right). \tag{2.24}$$

We then apply Theorem 16 as above (but with $M = N$) to get

$$f_2(\alpha) = \pm\left|\sum_{k=1}^{V} e(\alpha v_k)\right| = \pm|S| < Na(m) - V + O(m\sqrt{N}).$$

We once again use the fact that $m = O\left(N^{\frac{1}{4}}\right)$ and Lemma 21 to simplify this to

$$f_2(\alpha) = O\left(2Na(m) - 2Na(2N) + N^{\frac{3}{4}}\right).$$

Now we use the triangle inequality as before to get

$$\begin{aligned} |f_2(\alpha) - F_2(\alpha)| &\leq |f_2(\alpha)| + |F_2(\alpha)| \\ &\leq O\left(N\left\{a(m) - a(2N\right\} + N^{\frac{3}{4}}\right) + O\left(\sqrt{N}\right). \end{aligned}$$

Therefore the Lemma is true when $q \neq 1$.

We have hence shown that for any α we have:

$$\begin{aligned} f_1(\alpha) - F_1(\alpha) &= O\left(N \cdot \left\{a(m) - a(2N)\right\} + N^{\frac{3}{4}}\right); \\ f_2(\alpha) - F_2(\alpha) &= O\left(N \cdot \left\{a(m) - a(2N)\right\} + N^{\frac{3}{4}}\right). \end{aligned}$$

□

We now note the following inequality from the previous results.

Lemma 28. *For any α we have*

$$f_1(\alpha){f_2}^2(-\alpha) - F_1(\alpha){F_2}^2(-\alpha) = O\left(\{Na(m)\}^2\left(N\{a(m)-a(2N)\}+N^{\frac{3}{4}}\right)\right).$$

Proof. We first note the following simple application of the triangle inequality:

$$\begin{aligned}\left|f_1\cdot{f_2}^2 - F_1\cdot{F_2}^2\right| &= \left|f_1\cdot\left({f_2}^2-{F_2}^2\right)+{F_2}^2\cdot(f_1-F_1)\right| \\ &\leq |f_1\cdot(f_2+F_2)\cdot(f_2-F_2)| + \left|{F_2}^2\cdot(f_1-F_1)\right|.\end{aligned}$$

We now apply this inequality with α and $-\alpha$:

$$\begin{aligned}|f_1(\alpha)f_2^2(-\alpha) - F_1(\alpha)F_2^2(-\alpha)| &\leq |f_1(\alpha)|\cdot|f_2(-\alpha)+F_2(-\alpha)|\cdot|f_2(-\alpha)-F_2(-\alpha)| \\ &\quad +|F_2(-\alpha)|^2\cdot|f_1(\alpha)-F_1(\alpha)|.\end{aligned}$$

We can apply Lemma 23 and Lemma 24 to bound the required quantity:

$$\begin{aligned}f_1(\alpha)f_2^2(-\alpha) - F_1(\alpha)F_2^2(-\alpha) &= O(Na(m))\cdot 2O(Na(m))\cdot O\left(N(a(m)-a(2N))+N^{\frac{3}{4}}\right) \\ &+ O(Na(m))^2\cdot O\left(N(a(m)-a(2N))+N^{\frac{3}{4}}\right).\end{aligned}$$

Simplifying by using linearity and product rules of asymptotics we obtain:

$$\begin{aligned}f_1(\alpha)f_2^2(-\alpha) - F_1(\alpha)F_2^2(-\alpha) &= O\left(2(Na(m))^2\cdot\left(N(a(m)-a(2N))+N^{\frac{3}{4}}\right)\right) \\ &= O\left((Na(m))^2\left\{N(a(m)-a(2N))+N^{\frac{3}{4}}\right\}\right)\end{aligned}$$

as required.

□

Lemma 29. *If $0<\eta<\alpha<1-\eta$ then we have*

$$f_1(\alpha) = O\left(\frac{a(m)}{\eta}+N\{a(m)-a(2N)\}+N^{\frac{3}{4}}\right). \tag{2.25}$$

Proof. We start by using Lemma 24 to write for any α

$$f_1(\alpha) = F_1(\alpha)+O\left(N\{a(m)-a(2N)\}+N^{\frac{3}{4}}\right).$$

Therefore if we can show that for $0 < \eta < \alpha < 1 - \eta$ we have

$$F_1(\alpha) = O\left(\frac{a(m)}{\eta}\right)$$

we will obtain (2.25).

But recalling the definition of $F_1(\alpha)$ (given in Definition 22) we have

$$F_1(\alpha) = a(m) \sum_{n=1}^{2N} e(\alpha n)$$

and appealing to Lemma 25 we can apply the following bound:

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

(where $\|\alpha\|$ denotes the distance from α to the nearest integer).

But $\alpha \in (0, 1)$ and so $\|\alpha\|$ is either the distance from α to 0 or 1. But as $0 < \eta < \alpha$, we know the distance from 0 to α is greater than η. Similarly, as $\alpha < 1 - \eta < 1$ we know the distance from 1 to α is also greater than η.

Hence $\|\alpha\| > \eta$ and we obtain

$$|F_1(\alpha)| = a(m) \left| \sum_{n=1}^{2N} e(\alpha n) \right| \leq \frac{a(m)}{2\|\alpha\|} < \frac{a(m)}{2\eta}$$

which gives us for $0 < \eta < \alpha < 1 - \eta$

$$F_1(\alpha) = O\left(\frac{a(m)}{\eta}\right)$$

as required.

□

We are now ready to apply the Hardy-Littlewood Method. This will involve restating a condition defining an $\mathcal{A}$-set as a condition on an integral involving f_1 and f_2. Recall from Definition 4 the fact that $u_1, u_2, \ldots, u_U$ form an $\mathcal{A}$-set implies that $u_h = v_k + v_l$ if and only if $k = l$ and $u_h = 2v_k$.

Theorem 30 (The Hardy-Littlewood Method)**.** *The condition that $u_h = v_k + v_l$ if and only if $k = l$ and $u_h = 2v_k$ can be expressed by*

$$\int_{-\eta}^{1-\eta} f_1(\alpha) {f_2}^2(-\alpha)\,\mathrm{d}\alpha = V \leq Na(m). \tag{2.26}$$

Proof. We now show the idea that shapes the Hardy-Littlewood Method: changing a condition on the solutions of an equation into a condition on a circle integral. Then we can work with the integral to prove the result regarding the equations.

Recall from Definition 22 that

$$f_1(\alpha) = \sum_{k=1}^{U} e(\alpha u_k) \qquad \text{and} \qquad f_2(\alpha) = \sum_{k=1}^{V} e(\alpha v_k)$$

and so our integral in question is

$$\int_{-\eta}^{1-\eta} \left(\sum_{j=1}^{U} e(\alpha u_j)\right)\left(\sum_{k=1}^{V} e(-\alpha v_k)\right)\left(\sum_{l=1}^{V} e(-\alpha v_l)\right)\,\mathrm{d}\alpha$$

which, after simplification from the linearity of integration and basic exponential laws of multiplication becomes

$$\sum_{j=1}^{U}\sum_{k=1}^{V}\sum_{l=1}^{V}\int_{-\eta}^{1-\eta} e\left(\alpha(u_j - v_k - v_l)\right)\,\mathrm{d}\alpha.$$

Now we note that our function e is periodic with period 1 and so we can make things a little simpler for ourselves and write the integrals as from 0 to 1 to end up with

$$\sum_{j=1}^{U}\sum_{k=1}^{V}\sum_{l=1}^{V}\int_{0}^{1} e\left(\alpha(u_j - v_k - v_l)\right)\,\mathrm{d}\alpha.$$

Now let us consider these integrals

$$\int_{0}^{1} e\left(\alpha(u_j - v_k - v_l)\right)\,\mathrm{d}\alpha$$

and to do this let j, k, l be fixed integers. By the orthogonality of e (and the fact that α is non-zero) we have

$$\int_{0}^{1} e\left(\alpha(u_j - v_k - v_l)\right)\,\mathrm{d}\alpha = \begin{cases} 1 & u_j - v_k - v_l = 0 \\ 0 & \text{o/wise} \end{cases}$$

and so this integral is non-zero if and only if $u_j = v_k + v_l$.

We can therefore go back to our sum of integrals to write it as follows:

$$\sum_{j=1}^{U}\sum_{k=1}^{V}\sum_{l=1}^{V}\int_0^1 e\left(\alpha(u_j - v_k - v_l)\right)\,\mathrm{d}\alpha = |\{j,k,l \mid u_j = u_k + u_l\}|$$

But for each k from 1 to V there exists a j_k between 1 and U such that

$$u_{j_k} = 2u_k$$

and so we have at least V integrals equal to 1 in the sum, and so

$$\sum_{j=1}^{U}\sum_{k=1}^{V}\sum_{l=1}^{V}\int_0^1 e\left(\alpha(u_j - v_k - v_l)\right)\,\mathrm{d}\alpha \geq V.$$

But if this sum is exactly V then this means that these are the only solutions to the equation $u_j = v_k + v_l$, which is exactly the condition we wanted.

Conversely, if the only solutions to $u_j = v_k + v_l$ is when $k = l$ then there are only V non-zero integrals and so

$$\sum_{j=1}^{U}\sum_{k=1}^{V}\sum_{l=1}^{V}\int_0^1 e\left(\alpha(u_j - v_k - v_l)\right)\,\mathrm{d}\alpha = V.$$

Hence these two conditions are equivalent, and the noted inequality was proven in Lemma 20.

□

We now suppose that $\eta = \eta(m)$ satisfies the condition

$$0 < \eta < \frac{1}{2}. \tag{2.27}$$

Lemma 31. *Assuming* (2.27) *we have*

$$\int_\eta^{1-\eta} f_1(\alpha){f_2}^2(-\alpha)\,\mathrm{d}\alpha = O\left(\left\{\frac{a(m)}{\eta} + N\left(a(m) - a(2N)\right) + N^{\frac{3}{4}}\right\} Na(m)\right).$$

Proof. We first bound the absolute value of the integral like so:

$$\left|\int_\eta^{1-\eta} f_1(\alpha){f_2}^2(-\alpha)\,\mathrm{d}\alpha\right| \leq \left|\left(\max_{\alpha\in[\eta,1-\eta]}|f_1(\alpha)|\right)\int_\eta^{1-\eta}{f_2}^2(-\alpha)\,\mathrm{d}\alpha\right|$$

and use Lemma 29 that for $0 < \eta < \alpha < 1 - \eta$

$$f_1(\alpha) = O\left(\frac{a(m)}{\eta} + N(a(m) - a(2N)) + N^{\frac{3}{4}}\right).$$

We are now going to look at the remaining integral and show that it is of order $O(Na(m))$. We first bound as follows:

$$\begin{aligned}\left|\int_{\eta}^{1-\eta} {f_2}^2(-\alpha)\,\mathrm{d}\alpha\right| &\leq \left|\int_{\eta}^{1-\eta} \left|{f_2}^2(-\alpha)\right|\,\mathrm{d}\alpha\right| \\ &= \left|\int_{1-\eta}^{\eta} \left|{f_2}^2(\alpha)\right|\,\mathrm{d}\alpha\right| \leq \int_0^1 \left|{f_2}^2(\alpha)\right|\,\mathrm{d}\alpha\end{aligned}$$

because $\eta, 1-\eta \in [0,1]$ and $|{f_2}^2(\alpha)| \geq 0$.

Now we only need to show

$$\int_0^1 |{f_2}^2(\alpha)|\,\mathrm{d}\alpha = V$$

after which we apply Lemma 20 (in particular $V \leq Na(m)$). Now recall from Definition 22 that

$$f_2(\alpha) = \sum_{k=1}^{V} e(\alpha v_k).$$

We now use the definition of the norm on complex numbers:

$$|f_2(\alpha)|^2 = f_2(\alpha)\overline{f_2(\alpha)}$$

and the linearity of conjugation to expand this as

$$|f_2(\alpha)|^2 = \left(\sum_{k=1}^{V} e(\alpha v_k)\right)\left(\sum_{l=1}^{V} \overline{e(\alpha v_l)}\right).$$

But for any $\gamma \in \mathbb{R}$ we have $\overline{e(\gamma)} = e(-\gamma)$ and so we can simplify further

$$|f_2(\alpha)|^2 = \left(\sum_{k=1}^{V} e(\alpha v_k)\right)\left(\sum_{l=1}^{V} e(-\alpha v_l)\right) = \sum_{k,l=1}^{V} e(\alpha(v_k - v_l)).$$

But by the orthogonality of e (and as $\alpha \neq 0$) we have

$$\int_0^1 e(\alpha(v_k - v_l))\,\mathrm{d}\alpha = \begin{cases} 1 & v_k - v_l = 0 \\ 0 & \text{o/wise} \end{cases}$$

and as the v_i are distinct $v_k - v_l = 0$ if and only if $k = l$. Hence we can write

$$\int_0^1 e(\alpha(v_k - v_l))\,\mathrm{d}\alpha = \delta_{k,l},$$

(here $\delta_{k,l}$ represents the Kronecker delta function).

Therefore

$$\begin{aligned}\int_0^1 |f_2(\alpha)|^2\,\mathrm{d}\alpha &= \sum_{k,l=1}^{V}\int_0^1 e(\alpha(v_k - v_l))\,\mathrm{d}\alpha \\ &= \sum_{k,l=1}^{V}\delta_{k,l} = V\end{aligned}$$

as we required. So the proof is complete.

□

Lemma 32. *We now apply Lemma 28 to get*

$$\begin{aligned}&\int_{-\eta}^{\eta} f_1(\alpha){f_2}^2(-\alpha)\,\mathrm{d}\alpha \\ &= \int_{-\eta}^{\eta} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha \;+\; O\left(\eta\left\{Na(m)\right\}^2\left(N\left\{a(m)-a(2N)\right\}+N^{\frac{3}{4}}\right)\right).\end{aligned}$$

Proof. We first recall Lemma 28 which states that for any α we have

$$f_1(\alpha){f_2}^2(-\alpha) - F_1(\alpha){F_2}^2(-\alpha) = O\left(\left\{Na(m)\right\}^2\left(N\left\{a(m)-a(2N)\right\}+N^{\frac{3}{4}}\right)\right).$$

We now simply integrate each term above from $-\eta$ to η. This produces the two integrals as required and we note that integrating the asymptotic notation, simply multiplies the contents of the asymptotic notation by 2η. That is, if

$$f(\alpha) = O(g(\alpha))$$

implies that

$$\int_{-\eta}^{\eta} f(\alpha)\,\mathrm{d}\alpha = O(2\eta g(\alpha)) = O(\eta g(\alpha)).$$

We can therefore integrate the asymptotic notation of Lemma 28 to get the required asymptotic in (2.28) and the Lemma is proven.

□

Lemma 33. *Finally we use Lemma 27 and* (2.27) *to get*

$$\int_{-\eta}^{\eta} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha = \int_{-\frac{1}{2}}^{\frac{1}{2}} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha + O\left(\frac{a^3(m)}{\eta^2}\right).$$

Proof. To start, we split the integral from $-\eta$ to η as follows:

$$\begin{aligned}\int_{-\eta}^{\eta} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha &= \int_{-\frac{1}{2}}^{\frac{1}{2}} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha \\ &\quad - \left\{\int_{\eta}^{\frac{1}{2}} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha + \int_{-\frac{1}{2}}^{-\eta} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha\right\}\end{aligned}$$

and we concern ourselves with the final pair of integrals.

First we note that these can be simplified to a single integral:

$$\int_{\eta}^{\frac{1}{2}} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha + \int_{-\frac{1}{2}}^{-\eta} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha = \int_{\eta}^{\frac{1}{2}} F_1(\alpha){F_2}^2(-\alpha) + F_1(-\alpha){F_2}^2(\alpha)\,\mathrm{d}\alpha.$$

But from the definition of F_i, and more specifically $e(\alpha n)$, we have

$$F_i(-\alpha) = \overline{F_i(\alpha)}$$

and so

$$\int_{\eta}^{\frac{1}{2}} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha + \int_{-\frac{1}{2}}^{-\eta} F_1(\alpha){F_2}^2(-\alpha)\,\mathrm{d}\alpha = \int_{\eta}^{\frac{1}{2}} F_1(\alpha){F_2}^2(-\alpha) + \overline{F_1(\alpha){F_2}^2(-\alpha)}\,\mathrm{d}\alpha.$$

We now bound the absolute value of this integral:

$$\begin{aligned}\left|\int_{\eta}^{\frac{1}{2}} F_1(\alpha){F_2}^2(-\alpha) + \overline{F_1(\alpha){F_2}^2(-\alpha)}\,\mathrm{d}\alpha\right| &\leq \int_{\eta}^{\frac{1}{2}} \left|F_1(\alpha){F_2}^2(-\alpha) + \overline{F_1(\alpha){F_2}^2(-\alpha)}\right|\,\mathrm{d}\alpha \\ &\leq \int_{\eta}^{\frac{1}{2}} \left|F_1(\alpha){F_2}^2(-\alpha)\right| + \left|\overline{F_1(\alpha){F_2}^2(-\alpha)}\right|\,\mathrm{d}\alpha.\end{aligned}$$

We now use the standard property that for any number $z \in \mathbb{C}$ we know that $|z| = |\overline{z}|$. We therefore see that our pair of integrals are in fact bounded by:

$$2\int_{\eta}^{\frac{1}{2}} \left|F_1(\alpha){F_2}^2(-\alpha)\right|\,\mathrm{d}\alpha.$$

We now turn our attention to bounding $\left|F_1(\alpha){F_2}^2(-\alpha)\right|$ for α in the interval $[\eta, \frac{1}{2}]$.

The first thing to note is that, as $0 < \eta < \frac{1}{2}$ (from (2.27)), we have

$$\left[\eta, \frac{1}{2}\right] \subset [\eta, 1-\eta].$$

We can therefore apply Lemma 27, just like we did in the proof of Lemma 29 to see that

$$F_1(\alpha) = O\left(\frac{a(m)}{\eta}\right).$$

But exactly the same argument holds for $F_2(-\alpha)$ (the only difference between the two proofs being a constant factor before applying asymptotic notation). So we get

$$F_2(-\alpha) = O\left(\frac{a(m)}{\eta}\right).$$

Hence we can combine these bounds to get

$$2\int_{\eta}^{\frac{1}{2}} \left|F_1(\alpha){F_2}^2(-\alpha)\right| \,\mathrm{d}\alpha = O\left(2\left(\frac{1}{2}-\eta\right)\frac{a^3(m)}{\eta^3}\right) = O\left(\frac{a^3(m)}{\eta^2}\right);$$

which immediately proves the Lemma.

□

We now prove a lemma regarding solutions to the equation $n = n' + n''$ under certain conditions, which will be used later to work with

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} F_1(\alpha)F_2^2(-\alpha)\,\mathrm{d}\alpha.$$

Lemma 34. *The number of solutions of the equation $n = n' + n''$ with integers n, n' and n'' satisfying $n \leq 2N$, $n' \leq N$ and $n'' \leq N$ is N^2.*

Proof. This is relatively straightforward. We want to count

$$n = n' + n''; \qquad n \leq 2N, \quad n' \leq N, \quad n'' \leq N;$$

and we do this by looking at the right hand side of the equation. For every choice of (n', n'') there is a unique $n \leq 2N$ satisfying the equation. We have N choices for n', and N choices for n'', and so a total of N^2 choices for (n', n'') and hence N^2 solutions to the equation.

□

Lemma 35. *We have*

$$\begin{aligned} a^2(m) &= \frac{1}{N^2 a(m)} \int_{-\frac{1}{2}}^{\frac{1}{2}} F_1(\alpha) {F_2}^2(-\alpha)\,\mathrm{d}\alpha \\ &= O\left(\frac{a^2(m)}{N^2\eta^2} + \{\eta N a(m)+1\}\left\{a(m) - a(2N) + \frac{1}{N^{\frac{1}{4}}}\right\} + \frac{a(m)}{N\eta}\right) \end{aligned}$$

Proof. We will use Theorem 30, Lemma 31, Lemma 32, Lemma 33 and Lemma 34 to prove the lemma.

To start, let us consider

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} F_1(\alpha) F_2^2(-\alpha)\,\mathrm{d}\alpha \tag{2.28}$$

We first shall see that this is in fact $a(m)^3$ times the number of solutions to $n = n' + n''$ with $n \leq 2N$ and $n', n'' \leq N$.

From the definitions of F_1 and F_2 we can rewrite the integral as:

$$a^3(m) \int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\sum_{n=1}^{2N} e(\alpha n)\right)\left(\sum_{n'=1}^{N} e(-\alpha n')\right)\left(\sum_{n''=1}^{N} e(-\alpha n'')\right)\,\mathrm{d}\alpha.$$

Upon expanding out the sums we get the integral:

$$a^3(m) \int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\sum_{n=1}^{2N}\sum_{n'=1}^{N}\sum_{n''=1}^{N} e\left((n-n'-n'')\alpha\right)\right)\,\mathrm{d}\alpha \tag{2.29}$$

We now use orthogonality and periodicity of the complex exponential function. If $n - n' - n'' = 0$ then the following occurs:

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} e((n-n'-n'')\alpha)\,\mathrm{d}\alpha = \int_{-\frac{1}{2}}^{\frac{1}{2}} 1\,\mathrm{d}\alpha = 1.$$

If, on the other hand we have $n - n' - n'' \in \mathbb{Z} \setminus \{0\}$, we get

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} e((n-n'-n'')\alpha)\,\mathrm{d}\alpha = 0.$$

This shows that the integral in (2.29) counts the solutions to the given equation and so (2.28) gives $a^3(m)$ times this number.

Now from Lemma 34, this number is N^2 and so

$$N^2 = \frac{1}{a^3(m)} \int_{-\frac{1}{2}}^{\frac{1}{2}} F_1(\alpha) F_2^2(-\alpha)\, \mathrm{d}\alpha,$$

and so

$$a^2(m) = \frac{1}{N^2 a(m)} \int_{-\frac{1}{2}}^{\frac{1}{2}} F_1(\alpha) F_2^2(-\alpha)\, \mathrm{d}\alpha, \tag{2.30}$$

as required.

We now make some estimates using asymptotics and the previous Lemmata and Theorems. To start we apply Lemma 33 to (2.30) to get

$$(2.30) = \frac{1}{N^2 a(m)} \left[\int_{-\eta}^{\eta} F_1(\alpha) F_2^2(-\alpha)\, \mathrm{d}\alpha + O\left(\frac{a^3(m)}{\eta^2} \right) \right]. \tag{2.31}$$

We now apply Lemma 32 to simplify (2.31) as follows:

$$\begin{aligned} (2.31) \quad = \quad & \frac{1}{N^2 a(m)} \left[\int_{-\eta}^{\eta} f_1(\alpha) f_2^2(-\alpha)\, \mathrm{d}\alpha + O\left(\frac{a^3(m)}{\eta^2} \right) \right. \\ & \left. + O\left(\eta \left\{ N a(m) \right\}^2 \left(N \left\{ a(m) - a(2N) \right\} + N^{\frac{3}{4}} \right) \right) \right]. \end{aligned} \tag{2.32}$$

We use linearity of integrals to rewrite (2.32) in the following way

$$\begin{aligned} (2.32) \quad = & \frac{1}{N^2 a(m)} \left[\int_{-\eta}^{1-\eta} f_1(\alpha) f_2^2(-\alpha)\, \mathrm{d}\alpha - \int_{\eta}^{1-\eta} f_1(\alpha) f_2^2(-\alpha)\, \mathrm{d}\alpha \right. \\ & \left. + O\left(\frac{a^3(m)}{\eta^2} \right) + O\left(\eta \left\{ N a(m) \right\}^2 \left(N \left\{ a(m) - a(2N) \right\} + N^{\frac{3}{4}} \right) \right) \right] \end{aligned} \tag{2.33}$$

which allows us to apply Theorem 30 to the first integral and Lemma 31 to the second integral in (2.33). In doing this we obtain

$$\begin{aligned} (2.33) \quad \leq \quad & \frac{1}{N^2 a(m)} \left[V + O\left(\left\{ \frac{a(m)}{\eta} + N(a(m) - a(2N)) + N^{\frac{3}{4}} \right\} N a(m) \right) \right. \\ & \left. + O\left(\frac{a^3(m)}{\eta^2} \right) + O\left(\eta \left\{ N a(m) \right\}^2 \left(N(a(m) - a(2N)) + N^{\frac{3}{4}} \right) \right) \right] \end{aligned} \tag{2.34}$$

We multiply through by the fraction and use the second part of Theorem 30 (which is in fact Lemma 20: $V \leq N a(m)$) to get

$$\begin{aligned} (2.34) \quad = \quad & O\left(\frac{N a(m)}{N^2 a(m)} + \frac{N a(m)}{N^2 a(m)} \left\{ \frac{a(m)}{\eta} + N(a(m) - a(2N)) + N^{\frac{3}{4}} \right\} \right. \\ & \left. + \frac{a^3(m)}{N^2 a(m) \eta^2} + \frac{\eta \left\{ N a(m) \right\}^2}{N^2 a(m)} \left\{ N(a(m) - a(2N)) + N^{\frac{3}{4}} \right\} \right) \end{aligned} \tag{2.35}$$

Expanding out we obtain

$$(2.35) = O\left(\frac{1}{N} + \frac{a(m)}{\eta N} + a(m) - a(2N) + N^{-\frac{1}{4}} + \frac{a^2(m)}{N^2\eta^2} + \eta N a^2(m) - \eta N a(m)a(2N) + \eta N a(m) N^{-\frac{1}{4}}\right) \quad (2.36)$$

and with some final simplifications (and noting that the first term is negligible compared to the $N^{-\frac{1}{4}}$ term) we get

$$(2.36) = O\left(\frac{a^2(m)}{N^2\eta^2} + \{\eta N a(m) + 1\}\left\{a(m) - a(2N) + N^{-\frac{1}{4}}\right\} + \frac{a(m)}{N\eta}\right)$$

as required.

□

Definition 36. For notational purposes we now write

$$\delta := \frac{1}{N\eta}. \quad (2.37)$$

We can therefore rewrite Lemma 35 as follows.

Lemma 37. *Recalling that $2N = m^4$ and using the definition of δ in (2.37) we have*

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

Where δ, which depends only on m, is subject only to the restriction that $0 < \eta < \frac{1}{2}$.

Proof. We start with Lemma 35 and substitute in δ to get

$$\begin{aligned} a^2(m) &= O\left(\frac{a^2(m)}{N^2\eta^2} + \{\eta N a(m) + 1\}\left\{a(m) - a(2N) + \frac{1}{N^{\frac{1}{4}}}\right\} + \frac{a(m)}{N\eta}\right) \\ &= O\left(a^2(m)\delta^2 + \left\{\frac{a(m)}{\delta} + 1\right\}\left\{a(m) - a(m^4) + \frac{\sqrt[4]{2}}{m}\right\} + a(m)\delta\right) \\ &< c_1\left\{a(m)\delta + a^2(m)\delta^2 + \left(\frac{a(m)}{\delta} + 1\right)\left(a(m) - a(m^4) + \frac{1}{m}\right)\right\} \end{aligned}$$

as required.

□

We now introduce some more notation.

Definition 38. We define $b(x)$ as follows:

$$m = 2^{4^x}, \qquad b(x) = a(m) = a\left(2^{4^x}\right).$$

for any positive integer x.

Then with this new notation we can rewrite Lemma 37.

Lemma 39. *With this new notation, Lemma 37 becomes*

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

Proof. We note from Definition 38 we have

$$\begin{aligned} b^2(x) &= a^2(m); \\ b(x+1) &= a\left(2^{4^{x+1}}\right) = a\left(\left(2^{4^x}\right)^4\right) = a(m^4). \end{aligned}$$

Then by simple substitution we obtain

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

as required. □

2.6 Deducing Asymptotic behaviour of $a(x)$ (Section 5)

We are now finally in a position to prove Theorem 1. We do this using Corollary 10, Corollary 11, Lemma 12 and Lemma 39.

We first note that we can choose c_1 to be strictly greater than 1, because it is an absolute constant defined by the O-notation.

Lemma 40. *We can write*

$$\delta = \frac{b(x)}{2c_1}$$

and then, noting from Lemma 12 that $b(x) \leq 1$ *we have*

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

Proof. We know that δ is $(N\eta)^{-1}$. We can pick any c_1 larger than an absolute lower bound $\widetilde{c_1} > 1$ defined by the asymptotic notation. As N and $b(x)$ are both very large and increasing, we can certainly assume $\widetilde{c_1} < \frac{b(x)N}{4}$ so that it is simple to pick a $c_1 > \widetilde{c}$ and $\eta < \frac{1}{2}$ such that

$$c_1 = \frac{b(x)N\eta}{2} = \frac{b(x)}{2\delta}.$$

Knowing that $\delta = \frac{b(x)}{2c_1}$ we also know that $b(x) = a(m)$ so that by Lemma 12 we have

$$\frac{1}{2^{4^x}} = \frac{1}{m} \leq b(x) \leq 1. \tag{2.38}$$

Now we rewrite the left hand side of the inequality in a simpler form

$$\begin{aligned} c_1 \left\{ b(x)\delta + b^2(x)\delta^2 \right\} &= \frac{b(x)}{2\delta} \left\{ b(x)\delta + b^2(x)\delta^2 \right\} \\ &= \frac{b^2(x)}{2} + b^2(x) \left(\frac{b(x)\delta}{2} \right). \end{aligned} \tag{2.39}$$

Now we know that from (2.38) that $b(x) < 1$ so that

$$b(x) < \frac{1}{b(x)}$$

and so

$$\frac{b(x)\delta}{2} < \frac{\delta}{2b(x)} = \frac{2\delta}{4b(x)} = \frac{1}{4c_1}.$$

Substituting back into (2.39) we get

$$\begin{aligned} (2.39) &\leq \frac{b^2(x)}{2} + b^2(x)\frac{1}{4c_1} \\ &= b^2(x) \left(\frac{1}{2} + \frac{1}{4c_1} \right). \end{aligned} \tag{2.40}$$

Finally, we have the trivial assumption that $c_1 > 1$ so that $\frac{1}{4c_1} < \frac{1}{4}$ and we have

$$(2.40) < \frac{3}{4}b^2(x);$$

which is what was required.

□

Lemma 41. *We now use the definition that $\delta = (N\eta)^{-1}$ and Lemma 12 to show*

$$\eta = \frac{1}{N\delta} = \frac{c_2}{m^4 a(m)} < \frac{c_2}{m^3}, \tag{2.41}$$

so that $0 < \eta < \frac{1}{2}$ for large x.

Proof. We start from Lemma 12, to get

$$1 \leq \frac{1}{a(m)} \leq m.$$

Now we simply do some algebraic manipulation:

$$\begin{aligned} \eta = \frac{1}{N\delta} &= \frac{2}{m^4} \cdot \frac{2c_1}{b(x)} \\ &= \frac{4c_1}{m^4 a(m)} \\ &\leq \frac{4c_1}{m^4} \cdot m = \frac{4c_1}{m^3}. \end{aligned}$$

We then simply define c_2 to be $4c_1$ and (2.41) follows. Finally, for large x, we have very large m and so η is small, and certainly between 0 and $\frac{1}{2}$.

□

Lemma 42. *We now use the previous lemmata to see that Lemma 39 implies*

$$b^2(x) < c_3 \left(b(x) - b(x+1) + \frac{1}{2^{4^x}} \right) \qquad \textit{for} \qquad x > c_4.$$

Proof. From Lemma 39 we have

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

We now use Lemma 40 to get

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

and so collecting the $b^2(x)$ terms we have

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

But from Lemma 40 we also have

$$\delta = \frac{b(x)}{2c_1}$$

and so our inequality becomes

$$\begin{aligned} b^2(x) &< 4c_1\left\{(2c_1+1)\left(b(x)-b(x+1)+\frac{1}{2^{4^x}}\right)\right\} \\ &= c_3\left(b(x)-b(x+1)+\frac{1}{2^{4^x}}\right). \end{aligned}$$

(where $c_3 = 8{c_1}^2 + 4c_1$) for large x, that is $x > c_4$ for some absolute constant c_4.

□

Lemma 43. *First, $b(x)$ is a decreasing function by Corollary 10. This gives, for all integers $P > c_4$, the following:*

$$Pb^2(2P) \le \sum_{x=P}^{2P-1} b^2(x) < c_5\left(b(P)-b(2P)+\frac{4c_5}{2P}\right).$$

Proof. First we show that $b(x)$ is indeed decreasing. From Corollary 10 we know that

$$a(m_1 \cdot m_2) \le a(m_1)$$

for any positive integers m_1 and m_2. But by definition $b(x) = a(m) = a(2^{4^x})$ so that

$$b(x+1) = a\left(2^{4^{x+1}}\right) = a\left(\left(2^{4^x}\right)^4\right) = a(m^4) \le a(m) = b(x)$$

and hence b is decreasing.

Now consider $Pb^2(2P)$, and write out the sum as P copies of $b^2(2P)$:

$$Pb^2(2P) = b^2(2P) + \cdots + b^2(2P);$$

and apply the fact that b is decreasing to bound each of these terms with $b^2(P)$, $b^2(P+1)$ and so forth up to $b^2(2P-1)$:

$$Pb^2(2P) \leq b^2(P) + \cdots b^2(2P-1) = \sum_{x=P}^{2P-1} b^2(x).$$

We are assuming that $P > c_4$, and so we can apply Lemma 42 to each of these terms and so bound $Pb^2(2P)$ as follows:

$$\begin{aligned} Pb^2(2P) &\leq \sum_{x=P}^{2P-1} c_3 \left(b(x) - b(x+1) + \frac{1}{2^{4^x}} \right) \\ &= c_3 \sum_{x=P}^{2P-1} (b(x) - b(x+1)) + c_3 \sum_{x=P}^{2P-1} \frac{1}{2^{4^x}}. \end{aligned} \tag{2.42}$$

The first thing to note about (2.42) is that the first sum is in fact telescoping. That is, the second term in each summand cancels out the first term in the consecutive summand, so that, on cancellation, we are left with simply the first and last terms:

$$\sum_{x=P}^{2P-1} (b(x) - b(x+1)) = b(P) - b(2P).$$

Therefore, as long as $c_5 > c_3$ we will have this first sum bounded by $c_5(b(P) - b(2P))$.

Now for any x in the second sum, we have $x \geq P \geq c_4$. We now use the fact that this implies

$$\frac{1}{2^{4^x}} \leq \frac{1}{2^{4^P}}.$$

So we have the second sum in (2.42) bounded as follows:

$$c_3 \sum_{x=P}^{2P-1} \frac{1}{2^{4^x}} \leq \frac{c_3 P}{2^{4^P}}.$$

We wish to show that this is bounded by $\frac{4c_5^2}{2P}$ and so this is equivalent to having

$$c_5 > \sqrt{\frac{c_3 P^2}{2 \cdot 2^{4^P}}} \qquad \forall P > c_4. \tag{2.43}$$

To find such a c_5 we use the obvious fact that $\frac{y^2}{2^{4^y}}$ is decreasing with integers $y > 0$. As $P > c_4$ we can therefore bound as follows:

$$\frac{P^2}{2^{4^P}} < \frac{{c_4}^2}{2^{4^{c_4}}}.$$

If we hence choose c_5 such that

$$c_5 > \sqrt{\frac{{c_4}^2 c_3}{2 \cdot 2^{4^{c_4}}}}$$

then (2.43) will hold.

Therefore we are left with the condition that if

$$c_5 > \max\left\{c_3, \sqrt{\frac{{c_4}^2 c_3}{2 \cdot 2^{4^{c_4}}}}\right\}$$

then we have

$$\begin{aligned} Pb^2(2P) &< c_3(b(P) - b(2P)) + \frac{c_3 P}{2^{4^P}} \\ &< c_5\left(b(P) - b(2P) + \frac{4c_5}{2P}\right); \end{aligned}$$

and so the Lemma holds.

□

Lemma 44. *Under the additional assumption that* $2Pb(2P) > 4c_5$*, as well as* $P > c_4$*, we get*

$$2Pb(2P) < \frac{1}{4c_5}\left\{2Pb(2P)\right\}^2 < P\left\{b(P) - b(2P) + \frac{4c_5}{2P}\right\} < Pb(P).$$

Proof. We start by looking at the additional assumption, and write it in the following alternative ways. First we can divide by the $4c_5$ factor to rewrite the assumption in the form

$$\frac{2Pb(2P)}{4c_5} > 1 \tag{2.44}$$

which will be useful for our first inequality.

The second form we will write it in simply involves canceling a factor of two and rearranging to get

$$2c_5 - Pb(2P) < 0 \tag{2.45}$$

which we will need in the final step.

So we start by using (2.44) to get

$$2Pb(2P) < \left(\frac{2Pb(2P)}{4c_5}\right) \cdot (2Pb(2P)) = \frac{1}{4c_5}\left\{2Pb(2P)\right\}^2. \tag{2.46}$$

Now we can cancel the factor of four and, as $P > c_4$, apply Lemma 43 to obtain:

$$\begin{aligned}(2.46) &= \frac{1}{c_5} P\left(Pb^2(2P)\right) \\ &< \frac{1}{c_5} P\left(c_5\left(b(P) - b(2P) + \frac{4c_5}{2P}\right)\right) \qquad (2.47)\end{aligned}$$

which we can simplify to obtain

$$\begin{aligned}(2.47) &= P\left(b(P) - b(2P) + \frac{4c_5}{2P}\right) \\ &= Pb(P) + 2c_5 - Pb(2P). \qquad (2.48)\end{aligned}$$

We can now apply (2.45) to remove the excess terms and finally obtain

$$(2.48) < Pb(P)$$

as we required.

□

Lemma 45. *We can apply a backward induction and see that if $c_4 < 2^{t_0} < 2^t$ then*

$$2^t b(2^t) \leq \max\left(4c_5, 2^{t_0} b\left(2^{t_0}\right)\right),$$

which gives

$$b(2^t) = O\left(\frac{1}{2^t}\right).$$

As $b(x)$ is a decreasing function, this gives us that for any x

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

Proof. Define

$$\zeta := \max\left(4c_5, 2^{t_0} b\left(2^{t_0}\right)\right).$$

The first thing we must do is choose a t_0 such that $2^{t_0} > c_4$. This is obviously possible, and we can choose c_5 such that

$$2^{t_0} b(2^{t_0}) \leq 4c_5$$

and so our base case of $t = t_0$ is satisfied.

Now let us assume the result is true for $t-1 \geq t_0$ so that

$$2^{t-1}b(2^{t-1}) \leq \zeta. \tag{2.49}$$

We wish to show the result then holds for t so let us assume that

$$2^t b(2^t) > \zeta; \tag{2.50}$$

and we will derive a contradiction.

We now show we can apply Lemma 44 with $P = 2^{t-1}$. First, as $P \geq 2^{t_0}b(2^{t_0}) > c_4$ we satisfy the first requirement that $P > c_4$. Now we look at (2.50) and see that

$$2Pb(2P) = 2^t b(2^t) > 4c_5 > c_5$$

so that our additional assumption holds.

The result of Lemma 44 gives the inequality

$$2Pb(2P) < Pb(P)$$

which becomes

$$2^t b(2^t) < 2^{t-1}b(2^{t-1}).$$

Finally we use (2.49) and (2.50) to get the string of inequalities:

$$\zeta < 2^t b(2^t) < 2^{t-1}b(2^{t-1}) \leq \zeta$$

which is clearly a contradiction and proves our induction.

So for large enough t we have

$$2^t b(2^t) \leq \zeta$$

and we get

$$b(2^t) \leq \frac{\zeta}{2^t} = O\left(\frac{1}{2^t}\right).$$

We are now going to generalize for numbers that are not powers of 2. For any large x there exists a k so that we have

$$2^{t_0} < 2^{k-1} < x < 2^k$$

and also that

$$\frac{1}{2^k} \leq \frac{1}{x} \leq \frac{1}{2^{k-1}}.$$

We know from Lemma 43 that $b(x)$ is decreasing, and so

$$O\left(\frac{1}{2^k}\right) = b(2^k) \leq b(x) \leq b(2^{k-1}) = O\left(\frac{1}{2^{k-1}}\right).$$

But $O(2^k) = O(2^{k-1})$ so

$$b(x) = O\left(\frac{1}{2^k}\right)$$

and $\frac{1}{x} \geq 2^{-k}$ so that we finally get

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

which was needed.

□

We can now finally prove our main result:

Theorem 46. *For any x we have*

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

Proof. For any large integer x we can choose an $\widehat{x}$ such that

$$2^{4^{\widehat{x}}} < x \leq 2^{4^{\widehat{x}+1}},$$

whence

$$2\widehat{x} < \log\log x < 2(\widehat{x}+1).$$

We can then use Corollary 11 to get

$$a(x) \leq 2a\left(2^{4^{\widehat{x}}}\right) = 2b(\widehat{x}).$$

Finally we use Lemma 45 with this inequality to get that

$$a(x) = O\left(\frac{1}{\widehat{x}}\right)$$

and so

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

□

2.7 Summary of Roth's Method

We have therefore proven Roth's Theorem, using the exact method he employed in his seminal paper. It is easy however to lose the general picture while working through such a meticulous proof.

Therefore we provide an overview summary as follows, which was inspired by Erdős masterful account [4].

We defined $A(x)$ to be the size of the largest subset of $\{1, 2, \ldots, x\}$ avoiding three-term arithmetic progressions (a maximal $\mathcal{A}$-set). We fix a $\mathcal{A}$-set, $\{u_1, \ldots, u_U\}$ in $\langle M \rangle$ and define, for an arbitrary real number α, the sum

$$S := \sum_{k=1}^{U} e(\alpha \cdot u_k),$$

which has obvious analogues to the Fourier transform.

We then split α up according to the Dirichlet Box Principle:

$$\alpha = \frac{h}{q} + \beta$$

where $(h, q) = 1$, $q \leq \sqrt{M}$ and $q|\beta| \leq \frac{1}{\sqrt{M}}$. For any $m < M$ we define another exponential sum:

$$S' := \frac{a(m)}{q} \sum_{r=1}^{q} e\left(\frac{rh}{q}\right) \sum_{n=1}^{M} e\left(\beta n\right).$$

We then derived a sequence of results and ended up proving the key inequality

$$|S - S'| < Ma(m) - U + O\left(m\sqrt{M}\right).$$

Now we wished to harness the power of the Hardy-Littlewood Method, and to do so we let m be even, and N such that $2N = m^4$. Now assuming that $u_1, \ldots u_U$ is a maximal $\mathcal{A}$-set we let $\{2v_1, \ldots, 2v_V\}$ be the even u_i.

We now work with the following four functions:

$$\begin{aligned} f_1(\alpha) &= \sum_{k=1}^{U} e(\alpha u_k); \\ f_2(\alpha) &= \sum_{k=1}^{V} e(\alpha v_k); \\ F_1(\alpha) &= a(m) \sum_{n=1}^{2N} e(\alpha n); \\ F_2(\alpha) &= a(m) \sum_{n=1}^{N} e(\alpha n); \end{aligned}$$

all of which are of the order $O(Na(m))$.

We start by getting a good (and definitely non-trivial) estimate on the differences of these functions:

$$\begin{aligned} f_1(\alpha) - F_1(\alpha) &= O\left(N\{a(m) - a(2N)\} + N^{\frac{3}{4}}\right); \\ f_2(\alpha) - F_2(\alpha) &= O\left(N\{a(m) - a(2N)\} + N^{\frac{3}{4}}\right); \end{aligned}$$

and the tighter bound on f_1 for $0 < \eta < \alpha < 1 - \eta$:

$$f_1(\alpha) = O\left(\frac{a(m)}{\eta} + N\{a(m) - a(2N)\} + N^{\frac{3}{4}}\right).$$

The reason for considering such functions was to inspect the integral:

$$\int_{-\eta}^{1-\eta} f_1(\alpha) f_2^2(-\alpha)\,\mathrm{d}\alpha \tag{2.51}$$

which is equal to V, due to $\{u_1, \ldots u_U\}$ being an $\mathcal{A}$-set.

The power of this equivalence is revealed when we bound this integral, under the assumption $\eta \in \left[0, \frac{1}{2}\right]$. After comparing to various integrals involving f_1, f_2, F_1, F_2 we arrive at the following asymptotic for a:

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

To simplify the remainder of the proof we then used the following notation:

$$\delta = \frac{1}{N\eta}; \qquad m = 2^{4^x}; \qquad b(x) = a(m) = a\left(2^{4^x}\right);$$

which simplified our asymptotic as

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

What followed in the final section was a series of inequalities involving $b(x)$. We ensured that $\eta \in \left[0, \frac{1}{2}\right]$ and saw that

$$b^2(x) < c_3 \left(b(x) - b(x+1) + \frac{1}{2^{4^x}} \right).$$

From this we used the fact that b was decreasing to see

$$Pb^2(2P) = O\left(b(P) - b(2P) + \frac{4c_5}{2P} \right)$$

and in fact for large enough P

$$2Pb(2P) < Pb(P).$$

But then it was relatively simple (at least compared to the rest of the proof) to show that in fact

$$b(\widehat{x}) = O\left(\frac{1}{\widehat{\widehat{x}}} \right); \tag{2.52}$$

which finally gives us

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

which was what we wished to prove.

Chapter 3

Other Methods of Proof

In this chapter we will discuss some alternative methods to prove Roth's Theorem, and obtain alternative bounds on $A(x)$.

Please note that this section is completely separate to Roth's proof. Although we will reference sections of Roth's paper we will not be restricting ourselves to Roth's paper. In general, the paper currently being discussed will dictate the chosen notation, with clarification given where necessary. Therefore $A(x)$ may be referred to as $r_3(x)$ (which has become standard notation in the literature) and so forth.

This is also not meant to be as deeply expository as Chapter 2. The aim for this section is to outline the proofs of some key papers dealing with Roth's Theorem and so invariably some steps will be missing. The reader can either work through these details independently or consult the relevant paper for further clarity.

3.1 Convoluting with a Measure on a Three-term Arithmetic Progression [3]

In [3] Croot and Sisask proved that

$$\limsup_{N\to\infty} \frac{r_3(N)}{N} = 0$$

by restricting their proof to dealing with a finite field $\mathbb{F}_p$. After selecting an appropriate prime p the rest of the proof bears some similarities to Roth's method. Although the restriction to $\mathbb{F}_p$ is beneficial in avoiding integrals, it does provide some new difficulties which are dealt with deftly.

3.1.1 Notation

The paper starts by defining a collection of notation, most importantly for any function $f : \mathbb{F}_p \to [0,1]$ the quantity

$$\Lambda(f) = \mathbb{E}_{x,d\in\mathbb{F}_p} f(x)f(x+d)f(x+2d) = \frac{1}{p^2}\sum_{x,d\in\mathbb{F}_p} f(x)f(x+d)f(x+2d).$$

For the most part, f will be taken to be an indicator function of a set $\mathbb{1}_A : \mathbb{F}_p \to \{0,1\}$. In this case we denote $\Lambda(A) = \Lambda(f)$ and this is the number of three term progressions in A divided by p^2.

We will also use the Fourier transform, $\widehat{f} : \mathbb{F}_p \to \mathbb{C}$ which is defined, in the finite field case, as

$$\widehat{f}(r) = \mathbb{E}_{x\in\mathbb{F}_p} f(x)e^{\frac{2\pi irx}{p}} = \frac{1}{p}\sum_{x\in\mathbb{F}_p} f(x)e\left(\frac{rx}{p}\right).$$

We relate a function and its Fourier coefficients by Parseval's identity

$$\sum_{r\in\mathbb{F}_p}\left|\widehat{f}(r)\right|^2 = \frac{1}{p}\sum_{x\in\mathbb{F}_p}|f(x)|^2; \tag{3.1}$$

which allows us to rewrite

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

This is analogous to the manipulation of the key integrals in Theorem 30 (The Hardy-Littlewood Method).

3.1.2 Method

We start our proof by selecting, for any integer $N \geq 2$ an appropriate prime p to restrict our work to $\mathbb{F}_p$. To do this we must utilize Bertrand's Postulate (which he postulated in 1845 and Chebyshev proved five years later):

Theorem 47 (Bertrand's Postulate)**.** *If $n > 3$ then there is always at least one prime p between n and $2n-2$.*

Applying Theorem 47 to $2N$ we see that for any integer $N \geq 2$ there is a prime in the interval $[2N, 4N]$. After picking such a prime we select an $\mathcal{A}$-set S with $|S| = r_3(N)$. We can then embed S in $\mathbb{F}_p$ and predictably let

$$f := \mathbb{1}_S : \mathbb{F}_p \to \{0,1\}.$$

We create a set of 'awkward' numbers, denoted R:

$$R := \left\{ r \in \mathbb{F}_p \mid \left|\widehat{f}(r)\right| \geq \left(\frac{2\log\log p}{\log p}\right)^{\frac{1}{2}} \right\}.$$

This bound may seem rather complicated and unexpected, but it appears as a repercussion of the imminent proof.

Knowing Parseval's identity, (3.1), we know that

$$\sum_{r\in\mathbb{F}_p} \left|\widehat{f}(r)\right|^2 = \frac{|S|}{p}$$

and so we must have

$$|R| \leq \frac{\log p}{2\log\log p}$$

otherwise we would have the following contradictory chain of inequalities

$$1 = \frac{\log p}{2\log\log p}\left(\sqrt{\frac{2\log\log p}{\log p}}\right)^2 \leq \sum_{r\in R}\left|\widehat{f}(r)\right|^2 \leq \sum_{r\in\mathbb{F}_p}\left|\widehat{f}(r)\right|^2 = \frac{|S|}{p} < 1.$$

We therefore dilate R to be only in a small portion of $\mathbb{F}_p$ by picking an x (using the Dirichlet Box Principle) with

$$0 < x < p^{1-\frac{1}{(|R|+1)}} \leq \frac{p}{\log p} \tag{3.2}$$

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

$$\left\|\frac{xr}{p}\right\|_{\mathbb{T}} \leq p^{-\frac{1}{(|R|+1)}} \leq \frac{1}{\log p}.$$

(here $\|\cdot\|_{\mathbb{T}}$ is identical to $\|\cdot\|$ defined in Chapter 2 — the distance to the nearest integer).

Once we have selected such an x we define

$$B := \{0, x, 2x\}, \qquad\qquad h(n) := \frac{p\mathbb{1}_B(n)}{3};$$

so that h is the normalized indicator function of B.

We then use finite convolution to define the function g:

$$\begin{aligned} g(n) &:= (f * h)(n) \\ &= \frac{1}{p} \sum_{y \in \mathbb{F}_p} f(n-y)h(y) \\ &= \frac{1}{p} \sum_{y \in \mathbb{F}_p} f(n-y)\mathbb{1}_B(y) \\ &= \frac{1}{3} \left(f(n) + f(n-x) + f(n-2x) \right). \end{aligned}$$

Because we picked x to dilate R, and R was conditioned on the size of $\widehat{f}(r)$, we get for all $r \in \mathbb{F}_p$

$$\left| \widehat{f}(r) - \widehat{g}(r) \right| = \left| \widehat{f}(r) \right| \cdot \left| 1 - \widehat{h}(r) \right| \ll \left(\frac{\log \log p}{\log p} \right)^{\frac{1}{2}}$$

and so

$$|\Lambda(f) - \Lambda(g)| \ll \left(\frac{\log \log p}{\log p} \right)^{\frac{1}{2}}.$$

Finally, to bound $\Lambda(g)$, we note that we chose S to be a $\mathcal{A}$-set and so $\Lambda(f) \ll \frac{1}{p}$ implying

$$\Lambda(g) \ll \left(\frac{\log \log p}{\log p} \right)^{\frac{1}{2}}.$$

We now select a superset of S that we define as

$$T := \{n \in \mathbb{F}_p \mid g(n) > 0\} = \{n \in \mathbb{F}_p \mid n, n-x, \text{ or } n-2x \in S\}$$

so that (because $\Lambda(T) \ll \Lambda(g)$) we have

$$\Lambda(T) \ll \left(\frac{\log \log p}{\log p} \right)^{\frac{1}{2}}.$$

Now S is a $\mathcal{A}$-set, so there is no n such that n, $n-x$ and $n-2x$ are all in S. Hence for all $n \in \mathbb{F}_p$ we must have $g(n) \leq \frac{2}{3}$. Rewriting as $\frac{3g(n)}{2} \leq 1$ we see that if n is in T we have

$$\frac{3g(n)}{2} \leq 1 = \mathbb{1}_T(n) \qquad (n \in T)$$

and if n is not in T we have $g(n) < 0$, whence

$$\frac{3g(n)}{2} \leq 0 = \mathbb{1}_T(n) \qquad (n \notin T).$$

We can combine these results into $\mathbb{1}_T(n) \geq \frac{3g(n)}{2}$ and so we get the useful bound

$$|T| \geq \frac{3|S|}{2}.$$

At first glance, this extension of the set S is useful and could possibly lead to the completion of the proof, if not for the fact that we can not know if T is contained in $\langle N \rangle$ (as needed) or not. But from our choice of x in (3.2) we do know that

$$T \subset \left[N + \frac{2p}{\log p} \right]$$

and so if we define

$$T' := T \cap [N]$$

we can deduce some facts about T'. First we have

$$|T'| = |T| - O\left(\frac{N}{\log N}\right), \qquad \Lambda(T') \leq \Lambda(T)$$

and so that for large enough N we have

$$|T'| \geq \frac{4|S|}{3}.$$

(The only exception would be if $r_3(N)$ was asymptotically $O\left(\frac{N}{\log N}\right)$ in which case there is no further result to prove).

Now this set T' is significantly larger than S but we will see that it only admits a few more 3-term arithmetic progressions. To do this we use a quantitative version of the following theorem of Varnavides:

Theorem 48 (Varnavides' Theorem [14])**.** *Let δ be any number satisfying $0 < \delta < 1$, and let $a_1, a_2, \ldots, a_m$ be any set of distinct positive integers not exceeding x. Suppose that*

$$m > \delta x \qquad \text{and} \qquad x > x_0(\delta)$$

where $x_0(\delta)$ sepends only on δ. Then the number of three term progressions of the a_i's is at least $C(\delta)x^2$, where $C(\delta)$ is a positive number depending only on δ.

The version we shall need is as follows:

Lemma 49. *For any $1 \leq M \leq N$ and $A \subseteq [N]$, if we denote by $T_3(A)$ to be the number of three-term arithmetic progressions $\{a, a+d, a+2d\}$ with $d \geq 1$ in A we have*

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

We will not reproduce the proof here as it is a reasonably straightforward combinatorial argument, however it is given in full in [3].

To conclude the proof we set

$$M := \left\lfloor \left(\frac{\log p}{\log \log p} \right)^{\frac{1}{16}} \right\rfloor$$

and apply Lemma 49 with $A = T'$. This gives us

$$\left(\frac{\log \log p}{\log p} \right)^{\frac{1}{2}} \gg \Lambda(T') \geq \frac{\frac{4|S|}{3N} - \frac{r_3(M)+1}{M}}{M^4}$$

so that

$$\frac{3}{4} M^4 \left(\frac{\log \log p}{\log p} \right)^{\frac{1}{2}} + \frac{3}{4} \frac{r_3(M)+1}{M} \geq \frac{r_3(N)}{N}$$

as $r_3(N) = |S|$. Simplifying further

$$\frac{r_3(N)}{N} \ll \frac{3}{4} r_3(M) + O\left(\left(\frac{\log \log N}{\log N} \right)^{\frac{1}{4}} \right)$$

and so $\frac{r_3(N)}{N}$ is asymptotically decreasing, and Roth's Theorem follows.

3.2 Improving Bounds by Considering Bohr Sets [2]

In his paper On Triples in Arithmetic Progression [2], Bourgain proved the best to date asymptotic on $a(x)$, namely

$$a(x) = O\left(\sqrt{\frac{\log \log x}{\log x}} \right).$$

To do this he followed a similar method to Roth (which he refers to as a combination of the circle method and density increment). What allows him to gain a better bound is not more careful analysis per se (although his work is impeccable) but the consideration of a different object: Bohr Sets.

Bohr sets have been used throughout Arithmetic Combinatorics and are defined as follows.

Definition 50. For given real numbers ϵ and M, and a vector $\vec{\theta} = (\theta_1, \ldots, \theta_d) \in \mathbb{T}^d$ we define the **Bohr Set** to be

$$\Lambda = \Lambda_{\vec{\theta},\epsilon,M} \left\{ n \in \mathbb{Z} \mid |n| \leq M \text{ and } \|n\theta_j\| < \epsilon \text{ for } j = 1, \ldots, d \right\}.$$

Bourgain works with the normalized indicator function (a probability measure) on Λ:

$$\lambda = \frac{1}{|\Lambda|} \mathbb{1}_\Lambda.$$

For two Bohr sets Λ' and Λ'' and set A we define λ' and λ'' as above, and define the following analogues of f_1, f_2, F_1 and F_2:

$$\begin{aligned} S'(x) &= \sum_n \lambda'(n) e(nx) \\ S''(x) &= \sum_n \lambda''(n) e(nx) \\ S'_A(x) &= \sum_{n \in A} \lambda'(n) e(nx) \\ S''_A(x) &= \sum_{n \in A} \lambda''(n) e(nx). \end{aligned}$$

Then letting $\lambda'(A) = S'_A(0)$ and $\lambda''(A) = S''_A(0)$, Bourgain compares the two integrals

$$\lambda'(A)^2 \lambda''(A) \int_{\mathbb{T}} S'(\alpha)^2 S''(-2\alpha)\, \mathrm{d}\alpha$$
$$\int_{\mathbb{T}} S'_A(\alpha)^2 S''_A(-2\alpha)\, \mathrm{d}\alpha$$

to obtain the required density increment. Then reanalysing Λ under a set of required conditions the stated asymptotic is obtained.

3.3 Lower Bound for $A(x)$ [1]

We now talk about bounding $A(x)$ below (rather than above). In his 1946 paper *On Sets Of Integers Which Contain No Three Terms In Arithmetical Progression* [1], Behrend showed a surprisingly simple construction of a set of integers avoiding three-term arithmetic progressions that gives one of the best current lower bounds.

Theorem 51. *[1]*
For any $\epsilon > 0$, for sufficiently large N we have

$$A(N) > N^{1-\frac{2\sqrt{2\log 2}+\epsilon}{\sqrt{\log N}}};$$

or equivalently

$$a(N) > N^{-\frac{2\sqrt{2\log 2}+\epsilon}{\sqrt{\log N}}}.$$

Proof. First, for integers $d \geq 2$, $n \geq 2$ and $k \leq n(d-1)^2$ we define the following set

$$S_k(n,d) = \left\{A = a_1 + a_2(2d-1) + \cdots a_n(2d-1)^{n-1} \mid 0 \leq a_i < d, \mathrm{norm}(A) = k\right\}$$

where we define

$$\mathrm{norm}(A) = \sqrt{a_1^2 + a_2^2 + \cdots a_n^2}.$$

Behrend first shows that $S_k(n,d)$ is three term progression-free. If there are three elements A, A' and A'' in $S_k(n,d)$ such that

$$A + A' = 2A'';$$

then we would have the following two norm calculations:

$$\begin{aligned} \mathrm{norm}(A + A') = \mathrm{norm}(2A'') &= 2\sqrt{k}; \\ \mathrm{norm}(A) + \mathrm{norm}(A') &= 2\sqrt{k}. \end{aligned}$$

But in the triangle inequality:

$$\mathrm{norm}(A + A') \leq \mathrm{norm}(A) + \mathrm{norm}(A');$$

equality only holds if the 'coefficients' of A and A' are proportional:

$$(a_1, a_2, \ldots, a_n) = \kappa \cdot (a_1', a_2', \ldots, a_n').$$

However, A and A' have identical norms, and so $\kappa = 1$ so that $A = A' = A''$.

Now there are d^n choices for A with each $a_i \in [0, d)$ and $n(d-1)^2 + 1$ possible choices for the integer k. Therefore, by the Pigeonhole Principle, for some $k = K$, the corresponding $S_k(n, d)$ must have:

$$|S_k(n,d)| \geq \frac{d^n}{n(d-1)^2+1} > \frac{d^{n-2}}{n}.$$

Now all the terms in $S_k(n, d)$ are smaller than $(2d-1)^n$ and so we get

$$A((2d-1)^n) > \frac{d^{n-2}}{n}.$$

Now for a given N we choose

$$n = \left\lfloor \sqrt{\frac{2\log N}{\log 2}} \right\rfloor$$

and a d such that

$$(2d-1)^n \leq N < (2d+1)^n.$$

Now it is basic algebraic manipulation to see

$$A(N) \geq A((2d-1)^n) > \frac{d^{n-2}}{n} > \frac{(N^{\frac{1}{n}}-1)^{n-2}}{n2^{n-2}} = \frac{N^{1-\frac{2}{n}}}{n2^{n-2}}(1-N^{-\frac{1}{n}})^{n-2}$$

so that for any $\epsilon > 0$, if N is sufficiently large

$$\begin{aligned} A(N) > N^{1-\frac{2}{n}} n 2^{n-1} &= N^{1-\frac{2}{n}-\frac{\log n}{\log N}-\frac{(n-1)\log 2}{\log N}} \\ &> N^{1-\frac{2\sqrt{2\log 2}+\epsilon}{\sqrt{\log N}}}. \end{aligned}$$

□

This bound has been improved on since Behrend's proof, namely by Elkin, Green, Wolf and Bryant, but none retain the beautiful simplicity of this construction.

Chapter 4

Generalisations of Roth's Method

We now discuss how Roth's method of proof generalises to other results. The most obvious extension of Roth's Theorem is Szeméredi's Theorem:

Theorem 52 (Szeméredi's Theorem)**.** *Let k be a positive integer and let $\delta > 0$. There exists a positive integer $N = N(k, \delta)$ such that for every subset of the set $\{1, 2, \ldots, N\}$ of size at least δN contains an arithmetic progression of length k.*

It is clear that Roth's Theorem is the first non-trivial case of Theorem 52: that is when $k = 3$. When Szemerédi proved this theorem in 1975 he used method unrelated to Roth's proof of $k = 3$ from 1952. He did produce a proof using a similar method for $k = 4$ but it seemed the general case would not succumb to this tactic.

However in 1998 Timothy Gowers produced a new proof for $k = 4$ using Roth's methods and three years later produced a proof of Theorem 52 using exponential sums like we have described earlier. We will concentrate on the simpler $k = 4$ case rather than the general proof. We will then look at Szemerédi's Theorem applied to the prime numbers (through work by Ben Green and Terence Tao) and end with an unproven conjecture of Erdős and Turán.

4.1 Gowers' Proof of Szeméredi's Theorem for $k = 4$

In 1998, Gower's published [5], which proved Szeméredi's Theorem when $k = 4$ using a generalization of Roth's method. This was certainly not the first proof of this theorem, Szeméredi's original proof had been published nearly 30 years prior, but it was the first proof that did not rely on Van der Waerden's Theorem or similar results in Ramsey Theory.

Why was this significant? Any result relying on Van der Waerden's Theorem inherits the, frankly, awful bounds related to it. Defining the **tower function**, T, inductively by

$$T(1) = 2; \qquad T(n+1) = 2^{T(n)};$$

we can then define the **ackermann function**, W, (or rather *an* ackermann function, as there are various definitions) by the following recursion:

$$W(1) = 2; \qquad W(n+1) = T(W(n));$$

Any proof of Szeméredi's Theorem utilizing Van der Waerden's Theorem gives, for a density $\delta > 0$, a bound of at least $W(\delta^{-1})$ on N, which grows at an alarming rate.

Gowers' attempt to prove Szeméredi's Theorem using Roth's method was therefore motivated by a hope to improve the bounds generated, along with the fact that Roth's argument is "very natural and beautiful" and that "it is curious that it should not have an obvious generalization."

Gowers was successful in both of these aims - ending up with a bound on N of $\exp\exp\exp(\delta^{-c})$ for some absolute constant c. In fact, this can be improved to a 'mere' double exponential $\exp\exp(\delta^{-c})$.

Gowers' idea was to apply Roth's density increment argument to a special class of sets of integers — quadratically uniform sets. To define this notion we must first define uniform sets.

Let A be a subset of $\langle N \rangle$ of size δN. We define the **balanced function** of A as

$$f_A(s) = \mathbb{1}_A - \delta \mathbb{1}_{\langle N \rangle} = \begin{cases} 1-\delta & s \in A \\ -\delta & s \notin A \end{cases}$$

which has the property that $\widehat{f_A}(0) = 0$, where $\widehat{f_A}$ is the Fourier transform.

For a given α, we say that this set A is α**-uniform** if

$$\sum_r \left|\widehat{f_A}(r)\right|^4 \leq \alpha N^4;$$

(which is also referred to as quasirandomness).

It turns out that Roth's method can be stated reasonably concisely in terms of α-uniform sets. For suitable α, if A is α-uniform then A contains approximately the expected number of three-term arithmetic progressions. If not, we can use density increments on A to show for N large enough it cannot avoid three-term progressions.

This concept of α-uniform is not applicable when looking at four-term arithmetic progressions, and so we define a stronger condition. For a given α, we say that A is a **quadratically α-uniform** set if

$$\sum_u \sum_v \left| \sum_s f_A(s)\overline{f_A(s-u)f_A(s-v)}f_A(s-u-v) \right|^2 \leq \alpha N^4.$$

This can be restated with the notation

$$\Delta(f;k)(s) = f(s)\overline{f(s-k)}$$

as the condition

$$\sum_k \sum_r \left| \widehat{\Delta(f_A;k)}(r) \right|^4 \leq \alpha N^5$$

which shows the similarity to the α-uniform definition.

It is precisely this definition that Gowers generalizes Roth's method for. This is highly non-trivial but results in the celebrated result that for four-term arithmetic progressions there exists an absolute constant c such that

$$\delta \leq \frac{1}{(\log\log N)^c}$$

for all N. This gives the bound

$$r_4(N) = O\left(\frac{N}{(\log\log N)^c}\right).$$

4.2 Gowers' Proof of Szeméredi's Theorem for general k

We will not discuss how Gowers generalizes this method in [6] to deal with Szemerédi's Theorem for any k, which is Theorem 52, as it is beyond the scope of this paper. However, his paper was a landmark proof in Arithmetic Combinatorics and contributed to the decision to award Gowers the Fields Medal in 1998.

4.3 Roth's Theorem on Prime Numbers

In 2004, Green revealed a proof of Roth's Theorem when applied to the prime numbers. Later, this would lead to the highly celebrated Green-Tao Theorem but we will concentrate, for the moment, on [7].

This paper is a masterpiece of modern arithmetic combinatorics, and to describe the method Green employs in any sort of detail is beyond the scope of this paper. However, we will see a very coarse sketch of Green's methodology by quoting a selection of theorems and lemmata from the paper.

Green and Tao, independently of Van der Corput, had already proven the following theorem.

Theorem 53. *The primes contain infinitely many three-term arithmetic progressions. Indeed, the primes contain arbitrarily long arithmetic progressions.*

Green then proves the following generalization:

Theorem 54. *Every subset of the prime numbers of positive upper density contains a three-term arithmetic progression.*

Although Green follows quite a different route to Roth, there are certainly similarities and a key step in Green's proof was to show the Hardy-Littlewood Majorant Property for the primes.

Theorem 55 (The Hardy–Littlewood Majorant Property of the Primes)**.** *Suppose $p \geq 2$ is real. Let $\mathcal{P}$ be the set of all prime numbers and let*

$$\mathcal{P}_N = \mathcal{P} \cap [1, N].$$

Let $\{a_n\}_{n\in\mathcal{P}_N}$ be any sequence of complex numbers with $|a_n| \leq 1$ for all n. Then, for a constant $C(p)$ depending only on p:

$$\left\| \sum_{n\in\mathcal{P}_N} a_n e(n\theta) \right\|_{L^p(\mathbb{T})} \leq C(p) \left\| \sum_{n\in\mathcal{P}_N} e(n\theta) \right\|_{L^p(\mathbb{T})}$$

In fact, Green solely uses this property with $p = \frac{5}{2}$ but, as always, it is preferable to state a more general result.

As with all proofs of, and stemming from, Roth's Theorem one of the key steps is deciding what kind of sets to analyse. For Green's argument we let $m \leq \log N$ be a positive integer and $0 \leq b \leq m-1$ be coprime to m. Then we define the set

$$\Lambda_{b,m,N} = \{n \leq N \mid nm + b \in \mathcal{P}\};$$

which we expect, by the Prime Number Theorem, to have size of around

$$|\Lambda_{b,m,N}| \approx \frac{mN}{\phi(m)\log N}.$$

Here $\phi(m)$ denotes Euler's totient function: the number of positive integers less than m and coprime to m.

We then define an approximately normalised indicator function

$$\lambda_{b,m,N}(n) = \frac{\phi(m)\log(nm+b)}{mN}\mathbb{1}_{\Lambda_{b,m,N}}(n)$$

so that

$$\sum_{n\in\Lambda_{b,m,N}} \lambda_{b,m,N}(n) \approx 1.$$

Green then considers a subset $A_0 \subseteq \mathcal{P}$ with **positive relative upper density** — there exists a positive constant α_0 such that for an infinite number of integers n we have

$$|A_0 \cap \mathcal{P}| \geq \frac{\alpha_0 n}{\log n}.$$

Lemma 56. *If $A_0 \subseteq \mathcal{P}$ is a subset with positive relative upper density that avoids three-term arithmetic progressions then there exists positive real α and an infinite number of primes N such that the following occurs: there exists $A \subseteq \{1,\dots,\lfloor\frac{N}{2}\rfloor\}$ and an integer $W \in \left[\frac{1}{8}\log\log N, \frac{1}{4}\log\log N\right]$ such that the following happens. A avoids three-term arithmetic progressions and if $m = \prod_{p\leq W} p$ there exists b such that $(b,m) = 1$ and*

$$\lambda_{b,m,N}(A) \geq \alpha.$$

Using slightly ambiguous notation, we let $a = A \cdot \lambda_{b,m,N}$ and see

$$\sum_{x,d} a(x)a(x+d)a(x+2d) \leq \frac{(\log N)^3}{N^2}$$

which forces α to be small. But Varnavide's Theorem (also used in Croot and Sisask's proof of Roth's Theorem) sets off a chain of implications resulting in a contradiction when

$$\alpha \geq \sqrt{\frac{\log\log\log\log\log N}{\log\log\log\log N}}$$

This is restated in the following theorem:

Theorem 57. *If A is a subset of $\mathcal{P}_N$ with cardinality*

$$|A| \geq \frac{C \cdot N}{\log N} \sqrt{\frac{\log\log\log\log\log N}{\log\log\log\log N}}$$

then A must contain a three-term arithmetic progression.

Green himself admits this bound is poor. He predicts the "probable truth" that in fact any subset of $\langle N \rangle$ with cardinality

$$\frac{N}{(\log N)^{1000}}$$

contains a three-term arithmetic progression.

4.4 The Green–Tao Theorem

To finish our generalizations, we state one of the most celebrated theorems in Arithmetic Combinatorics, and indeed one of the most impressive results in mathematics in the last decade. The Green–Tao Theorem, proven in 2004, extends Theorem 54 and we take the statement from [13].

Theorem 58 (The Green–Tao Theorem)**.** *Let $k \geq 1$ and $N > 1$. Denote by $\mathcal{P}$ the set of all prime numbers. Then*

$$r_k\left(\mathcal{P} \cap [1, N]\right) = o_{N\to\infty;k}\left(|\mathcal{P} \cap [1, N]|\right).$$

In particular, the primes contain arbitrarily long arithmetic progressions.

As with Gowers' proof of Szemerédi's Theorem, the proof is beyond our discussion. Needless to say their proof cemented Green and Tao's place in mathematical history, and undoubtedly influenced their election as Fellows of the Royal Society and the awarding of the Fields medal to Tao in 2006.

4.5 The Erdős–Turán Conjecture

To conclude our survey of results, we end with a conjecture of Erdős and Turán that has remained unsolved for 75 years.

Conjecture 59 (The Erdős–Turán Conjecture)**.** *Let $A \subset \mathbb{Z}^+$ be such that*

$$\sum_{n \in A} \frac{1}{n} = \infty.$$

Then A contains arbitrarily long proper arithmetic progressions.

This is unsolved, even for length three progressions. However the Green–Tao Theorem is a special case of the conjecture, due to the well known fact that

$$\sum_{p \in \mathcal{P}} \frac{1}{p} = \infty.$$

Whether the Erdős–Turán Conjecture will ever be proven remains to be seen; it does not seem an unreasonable statement, but it's difficulty is undisputed. This difficulty is reinforced by the fact that Erdős offered a \$3000 prize for anyone able to prove it; one of his highest prize sums (eclipsed only, to my knowledge, by two \$10,000 prizes: one for a tight asymptotic formula for $A(x)$ and the second for a conjecture showing "consecutive primes numbers are often far apart"). While it is unlikely that Roth's Method can be generalized to this statement, there is always hope that a fresh approach may yield substantial results.

Appendices

Appendix A

Code

In this appendix I provide the algorithms for the most important programs I used while studying Roth's Theorem. They will be reproduced in both pseudo-code and their original Maple code. They can all be found within a program file found at the author's website, or by emailing the author at david.john.wilson@me.com.

A.1 Three-term Arithmetic Progressions

This code takes a set of integers and checks whether there exists a three-term arithmetic sequence by a brute force method.

A.1.1 *GoodSubset*(s) Pseudo-code

In Algorithm 1 we present the pseudo-code. We consider the set s to be akin to a list in Maple, ordered under increasing numerical order, and s_i denotes the i^{th} entry in the set.

Require: $s \subseteq \{1, 2, \ldots, n\}$
1: **for** $i = 1$ to $|s| - 2$ **do**
2: **for** $j = i + 1$ to $|s| - 1$ **do**
3: **for** $k = j + 1$ to $|s|$ **do**
4: **if** $s_i + s_k = 2s_j$ **then**
5: **return** false **end**
6: **end if**
7: **end for**
8: **end for**
9: **end for**
10: **return** true **end**

Algorithm 1: *GoodSubset*(s) Algorithm

A.1.2 *GoodSubset*(s) Maple Code

In Algorithm 2 we present the equivalent Maple Code for Algorithm 1.

```
GoodSubset:=proc(s) local i,j,k,t:
t:=nops(s):

for i from 1 to t-2 do
  for j from i+1 to t-1 do
    for k from j+1 to t do
      if s[i]+s[k]=2*s[j] then
              RETURN(false):
      fi:
    od:
  od:
od:

RETURN(true):

end:
```

Algorithm 2: *GoodSubset*(s) Maple Code

A.2 $A(n)$ by Brute Force

The following code calculates A(n) using an inefficient brute force method and the $GoodSubset(s)$ procedure.

A.2.1 $A(n)$ Pseudo-code

Algorithm 3 provides the pseudo-code for calculating $A(n)$ by brute force.

Require: $n \geq 1$
1: S:={}
2: **for** $s \subseteq \{1, 2, \ldots, n\}$ **do**
3: **if** GoodSubset(s) **then**
4: $S \leftarrow S \cup \{|s|\}$
5: **end if**
6: **end for**
7: **return** $\max(S)$

Algorithm 3: $A(n)$ Algorithm

A.2.2 $A(n)$ Maple-code

In Algorithm 4 we present the equivalent Maple Code for Algorithm 3.

```
A:=proc(n) local T,S,i,l,s:

S:={}:
T:=combinat[powerset]({seq(i,i=1..n)}):

for i from 1 to 2^n do
  if GoodSubset(T[i]) then
    S:={op(S),T[i]}:
  fi:
od:

l:=seq(nops(s), s in S):

RETURN(max(l)):

end:
```

Algorithm 4: $A(n)$ Maple Code

A.3 $\mathcal{A}$-Sets by Recursive Methods

This code can be used to calculate $A(n)$ a little more efficiently by using recursive methods.

$RecursiveASet(n, k)$ produces all $\mathcal{A}$-sets of $\{1, 2, \ldots, n\}$ of size less than or equal to k. To then calculate $A(n)$ one needs only just look for the largest element of $RecursiveASet(n, n)$.

Although this method is much quicker in practice then using Algorithm 3/4 , it is memory intensive as it requires you to store the outputs of $RecursiveASet(n, j)$ for all $j < k$ (which is why the first line is the command **option remember**).

A.3.1 $RecursiveASet(n, k)$ Pseudo-code

Algorithm 5 provides the pseudo-code for $RecursiveASet(n, k)$.

Require: $n \geq 1$
Require: $1 \leq k \leq n$
1: **option remember**
2: **if** $n = 0$ or $k = 0$ **then**
3: **return** { } **end**
4: **end if**
5: $S := RecursiveASet(n - 1, k)$
6: $T := RecursiveASet(n - 1, k - 1)$
7: **for** $t \in T$ **do**
8: **if** $GoodSubset(t \cup \{n\})$ **then**
9: $S \leftarrow S \cup \{t \cup \{n\}\}$
10: **end if**
11: **end for**
12: **return** S **end**

Algorithm 5: $RecursiveASet(n, k)$ Algorithm

A.3.2 *RecursiveASet*(n, k) Maple Code

In Algorithm 6 we present the equivalent Maple Code for Algorithm 5.

```
RecursiveASet:=proc(n,k) local i,S,T:
option remember:

if n=0 or k=0 then
  RETURN({{}}):
fi:

S:=RecursiveASet(n-1,k):

T:=RecursiveASet(n-1,k-1):

for i from 1 to nops(T) do
  if GoodSubset(T[i]) then
    S:={op(S),T[i]}:
  fi:
od:

RETURN(S):

end:
```

Algorithm 6: *RecursiveASet*(n, k) Maple Code

A.4 Further Code

There is obviously scope for further programs related to Roth's Theorem. Included in the program file are programs to empirically test the main asymptotic in Theorem 1, calculate the Dirichlet constants in Theorem 14, check all the 'obvious' statements in section 2.3 and much more.

Bibliography

[1] F. A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci*, 32(12):331–332, 1946.

[2] J. Bourgain. On triples in arithmetic progression. *Geom. Funct. Anal.*, 9:968–984, 1999.

[3] Ernie Croot and Olof Sisask. A new proof of roth's theorem on arithmetic progressions. *Proceedings of the American Mathematical Society*, 137(3):805–809, March 2009.

[4] P. Erdős. Sur quelques ensembles d'entiers review. MathSciNet.

[5] W. T. Gowers. A new proof of szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.*, 8(3):529–551, 1998.

[6] W. T. Gowers. A new proof of szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001.

[7] Ben Green. Roth's theorem in the primes. *ArXiV*, (0302311v3), 2004.

[8] N. M. Korobov. *Exponential Sums and Their Applications*. Springer, 1992.

[9] Scott T Parsell. *Exponential Sums and Diophantine Problems*. PhD thesis, The University of Michigan, 1999.

[10] H. A. Priestley. *Introduction to Complex Analysis*. Oxford University Press, 2005.

[11] R.C.Vaughan. *The Hardy-Littlewood Method*. Cambridge University Press, second edition edition, 1997.

[12] K. F. Roth. On certain sets of integers. *J. London Math. Soc.*, s1-28(1):104–109, January 1953.

[13] Terence Tao and Van H. Vu. *Additive Combinatorics*. Number 105 in Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2010.

[14] P. Varnavides. On certain sets of positive density. *J. Lond. Math. Soc.*, 1959.

[15] John Woll. Dirichlet's approximation theorem, 2010.

Index