ROTH'S THEOREM: A SPECIAL CASE OF SZEMEREDI’S THEOREM

ROHAN SONI

Abstract. An arithmetic progression is a set of the form \{x, x + d, x + 2d, ..., x + (k - 1)d\} where \(x, d\) are natural numbers. Szemeredi’s theorem states that a set of the natural numbers that is "dense enough" contains arbitrarily long arithmetic progressions. Roth proved the case \(k = 3\), and provided a quantitative bound on the size of a set \(A \subset \{1, ..., N\}\) in terms of \(N\) that must contain a three-term progression. In this paper, we will prove this bound, and thus Roth’s theorem.

Contents
1. Introduction and Background 1
2. The Discrete Fourier Transform 2
3. The Density Increment Strategy 4
4. Bounding the Balanced Function via the Gowers \(U^2\)-norm 5
5. Analyzing the Balanced Function via Fourier Analysis 8
6. Applying the Pigeonhole Principle 9
Acknowledgments 11
References 11

1. Introduction and Background

Additive combinatorics is a field of mathematics that lies at the intersection of combinatorics, number theory and harmonic analysis. One of the central problems that has been driving the field forward since its inception involves describing conditions sufficient for a set of natural numbers to contain arithmetic progressions (a sequence \(x, x + d, x + 2d, ..., x + (k - 1)d\) where \(x, d \in \mathbb{N}\)) of arbitrary lengths. To that end, Erdős and Turán conjectured the following, which became Szemeredi’s theorem in his seminal 1975 paper [1].

Theorem 1.1 (Szemeredi’s theorem). We call \(A \subset \mathbb{N}\) a set of positive upper density if

\[
\limsup_{n \to \infty} \frac{|A \cap \{1, ..., n\}|}{n} > 0.
\]

A subset of the natural numbers with positive upper density contains a \(k\)-term arithmetic progression for all \(k \in \mathbb{N}\).

Roth’s theorem is the special case of Szemeredi’s theorem when \(k = 3\) [2]. In fact, Roth proved a quantitative bound in his proof of the theorem, which is stated below.
Theorem 1.2 (Roth’s theorem). There is an absolute constant $C$ such that any $A \subset \{1, \ldots, N\}$ with cardinality $\frac{CN}{(\log \log N)^{1/5}}$ contains a non-trivial three-term arithmetic progression.

In this paper, we will prove Roth’s theorem with the bound $\frac{CN}{(\log \log N)^{1/5}}$ instead of $\frac{CN}{(\log \log N)^3}$ [3]. The weaker bound offers an easier way to generalize the result to the general case of Szemerédi’s theorem.

2. The Discrete Fourier Transform

One of the most important tools utilized in the proof of Roth’s theorem is discrete Fourier analysis. The material in this section is largely adapted from [4] and [5].

Definition 2.1. Given the cyclic group $\mathbb{Z}/N\mathbb{Z}$, we define the (discrete) Fourier transform of the function $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ to be the function $\hat{f} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ such that

$$\hat{f}(n) := \mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) e^{-2\pi i nx/N} = \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) e^{-2\pi i nx/N}.$$ 

Remark 2.2. We use the expectation notation for notational convenience. Also for convenience, we will use $e(\theta) = e^{2\pi i \theta}$. So we have

$$\hat{f}(n) := \mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) e(-nx/N).$$

Definition 2.3. The convolution of $f, g : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ is the mapping

$$(f \ast g)(x) = \mathbb{E}_{y \in \mathbb{Z}/N\mathbb{Z}} f(y)g(x-y).$$

Remark 2.4. We let

$$||f||_2 = \left(\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} |f(x)|^2\right)^{1/2}$$

and

$$||f||_2 = \left(\sum_{h \in \mathbb{Z}/N\mathbb{Z}} |\hat{f}(h)|^2\right)^{1/2}.$$ 

We will prove some basic properties of the Fourier transform.

Lemma 2.5 (Orthogonality relation). Given $r, s \in \mathbb{Z}/N\mathbb{Z}$,

$$\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} e((r-s)x/N) = \begin{cases} 1, & \text{if } r = s \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $r = s$, $e((r-s)x/N) = e(0) = 1$. So we have $\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} e((r-s)x/N) = 1$.

If $r \neq s$, by the geometric series formula,

$$\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} e((r-s)x/N) = \frac{1}{N} \sum_{k=0}^{N-1} e((r-s)k/N) = \frac{1}{N} \frac{1 - e((r-s)/N)^N}{1 - e((r-s)/N)} = 0.$$ 

The final equality above follows since $e((r-s)/N)^N = 1$. 

\qed
Proposition 2.6 (Plancherel’s theorem). Given a function \( f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C} \),

\[
\| f \|_2 = \| f \|_2.
\]

Proof. By the definition of \( \| f \|_2 \),

\[
\| f \|_2^2 = \sum_{h \in \mathbb{Z}/N\mathbb{Z}} |\hat{f}(h)|^2
\]

\[
= \sum_{h \in \mathbb{Z}/N\mathbb{Z}} |\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)e(-hx/N)|^2
\]

\[
= \frac{1}{N^2} \sum_{h \in \mathbb{Z}/N\mathbb{Z}} \left( \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)e(-hx/N) \right) \left( \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \overline{f(x)}e(hx/N) \right)
\]

\[
= \frac{1}{N^2} \sum_{h \in \mathbb{Z}/N\mathbb{Z}} \sum_{x,x' \in \mathbb{Z}/N\mathbb{Z}} f(x)f(x')e(h(x' - x)/N)
\]

\[
= \frac{1}{N} \sum_{x,x' \in \mathbb{Z}/N\mathbb{Z}} f(x)f(x') \frac{1}{N} \sum_{h \in \mathbb{Z}/N\mathbb{Z}} e(h(x' - x)/N).
\]

Via Lemma 2.5, observe that

\[
\frac{1}{N} \sum_{h \in \mathbb{Z}/N\mathbb{Z}} e(h(x' - x)/N) = \mathbb{E}_{h \in \mathbb{Z}/N\mathbb{Z}} e(h(x' - x)/N) = \begin{cases} 1, & \text{if } x = x' \\ 0, & \text{otherwise} \end{cases}
\]

Then,

\[
\| f \|_2^2 = \frac{1}{N} \sum_{x,x' \in \mathbb{Z}/N\mathbb{Z}} f(x)f(x') \delta_{x,x'}
\]

\[
= \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} |f(x)|^2
\]

\[
= \| f \|_2^2.
\]

We then have the result. \( \square \)

Lemma 2.7. Given \( f, g : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C} \),

\[
(f * g)(h) = \hat{f}(h)\hat{g}(h).
\]
Proof. By the definition of convolution and the Fourier transform, we obtain the following chain of equalities, which gives us the result
\[
\hat{f}(h)\hat{g}(h) = (E_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)e(-hx/N))(E_{x \in \mathbb{Z}/N\mathbb{Z}} g(x)e(-hx/N))
\]
\[
= \frac{1}{N^2} \left( \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)e(-hx/N) \right) \left( \sum_{x \in \mathbb{Z}/N\mathbb{Z}} g(x)e(-hx/N) \right)
\]
\[
= \frac{1}{N^2} \sum_{x,x' \in \mathbb{Z}/N\mathbb{Z}} f(x)g(x')e(-h(x+x')/N)
\]
\[
= \frac{1}{N^2} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)g(y-x)e(-h(x+y-x)/N)
\]
\[
= \frac{1}{N} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} e(-h(x+y-x)/N) \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)g(y-x)
\]
\[
= E_{y \in \mathbb{Z}/N\mathbb{Z}} e(-hy/N) E_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)g(y-x)
\]
\[
= (f*g)(h).
\]
\[\square\]

3. The Density Increment Strategy

The goal of the paper is to prove the following proposition, which gives us Roth’s theorem as a direct consequence [6].

Proposition 3.1 (The density increment strategy). Suppose that 0 < \alpha < 1 and N > C\alpha^{-6}. Further assume that P \subset \mathbb{Z} is an arithmetic progression of length N and A \subset P has cardinality \alpha N. Then one of the following holds:

1) A contains at least \frac{1}{16}\alpha^3 N^2 non-trivial three-term arithmetic progressions.

2) There is an arithmetic progression P' of length N' \geq N^{1/3} such that given A' = A \cap P' and \alpha' = |A'|/|P'|, we have \alpha' > \alpha + C\alpha^6.

We will spend the whole paper proving this proposition. What follows is a proof that Roth’s theorem is a consequence of the Density Increment Strategy.

Let P_0 = \{1, ..., N\}, and A \subset P_0 have cardinality \alpha N, where 0 < \alpha < 1, with no non-trivial three-term progression. Then, there must be an arithmetic progression P_1 of length N_1 \geq N^{1/3} such that A_1 = A \cap P_1 has no non-trivial three-term progression (since it is a subset of A), and \alpha_1 = \frac{|A_1|}{|P_1|} > \alpha + C\alpha^6.

Continuing this pattern, we obtain progressions P_1, P_2, ... such that |P_i| \geq N^{(1/3)^i} and, given A_i = P_i \cap A, the densities \alpha_i = \frac{|A_i|}{|P_i|} satisfy \alpha_{i+1} > \alpha_i + C\alpha_i^6.

Since each step increases the density by at least C\alpha_i^6, \frac{C}{\alpha^6} steps will double the density, a further \frac{C}{\alpha^6} steps will double the density again. Ultimately, after \frac{C}{\alpha^6} steps, the density will exceed 1, which is impossible for any set.

Therefore, the hypothesis must be must be violated. The only condition that could be violated is |P_i| > C\alpha_i^{-C}, where i is the penultimate step before the density exceeds 1. Thus, i = \frac{C}{\alpha^6}. So, we see that |P_i| \leq C\alpha_i^{-C}. Since N^{(1/3)^i} \leq |P_i|,

N^{(1/3)^i} \leq C\alpha^{-C}.
We also know that $\alpha_i \geq \alpha$. Therefore,
\[ N^{(1/3)/C/\alpha^5} \leq C\alpha^{-C}. \]
Rearranging,
\[ \log \log N \leq \log \log(C\alpha^{-C}) + \frac{C}{\alpha^5} \leq \frac{C'}{\alpha^5}. \]
Rearranging once more, we get
\[ \alpha \leq \frac{C}{(\log \log N)^{1/5}}. \]
The contrapositive of this result is Roth's theorem.

4. Bounding the Balanced Function via the Gowers $U^2$-norm

Of course we have yet to prove that the Density Increment Strategy works. To do so, we want to use discrete Fourier analysis. However, this can only be performed on groups, not arbitrary finite sets. Suppose, then, that $P$ is an arithmetic progression of length $N$ with $A \subset P$ having size $\alpha N$. Instead, without loss of generality, we can consider $P = \{1, ..., N\}$. In order to work over groups, we define $G = \mathbb{Z}/N'\mathbb{Z}$, where $N' = 2N + 1$.

We can then consider $\hat{A} \subset \hat{P} = \{1, ..., N\}$ as subsets of $G = \{1, 2, ..., N'\}$.

If $G$ had size $M < 2N + 1$, $\{N, 2N, 3N\}$ (considered $\mod M$) could be a subset of $\hat{A}$. Defining the size of $G$ to be $N' = 2N + 1$ ensures that there are no "wraparound" arithmetic progressions in $\hat{A}$, since $2N$ cannot be in $\hat{A}$. Thus, if the elements of $\hat{A}$ correspond to $A$, they have the same number of three-term arithmetic progressions, since there are no "extra" arithmetic progressions in $\hat{A}$ considered as a subset of the group $G$.

By abuse of notation, we consider $A = \hat{A}$ henceforth.

To count the number of three-term arithmetic progressions, we will introduce the three-term progression operator $\Lambda$. Given functions $f_1, f_2, f_3 : \mathbb{Z}/N'\mathbb{Z} \to \mathbb{R}$, let
\[ \Lambda(f_1, f_2, f_3) = \mathbb{E}_{x, d \in \mathbb{Z}/N'\mathbb{Z}} f_1(x) f_2(x + d) f_3(x + 2d). \]

Let $1_A$ be the characteristic function of $A \subset \mathbb{Z}/N'\mathbb{Z}$. Then, $\Lambda(1_A, 1_A, 1_A)$ counts the number of three-term arithmetic progressions in $A$ up to a factor of $1/N'^2$.

The proof will involve a comparison with $\Lambda(\alpha 1_{[N]}, \alpha 1_{[N]}, \alpha 1_{[N]})$, where $1_{[N]}$ is the characteristic function of the set $\{1, ..., N\} \subset \mathbb{Z}/N'\mathbb{Z}$. To perform this comparison, we introduce the balanced function $f = 1_A - \alpha 1_{[N]}$.

By the linearity of expectation, we see that $\Lambda$ is multilinear (that is, it is linear in each variable). A simple computation then gives us the following:
\[ \Lambda(1_A, 1_A, 1_A) = \alpha^3 \Lambda(1_{[N]}, 1_{[N]}, 1_{[N]}) + \Lambda(f, \alpha 1_{[N]}, \alpha 1_{[N]}) + \Lambda(1_A, f, \alpha 1_{[N]}) + \Lambda(1_A, 1_A, f) \]
\[ = \alpha^3 \Lambda(1_{[N]}, 1_{[N]}, 1_{[N]}) + \Lambda(f, \alpha 1_{[N]}, \alpha 1_{[N]}) + \Lambda(\alpha 1_{[N]}, f, \alpha 1_{[N]}) + \Lambda(f, f, \alpha 1_{[N]}) \]
\[ + \Lambda(\alpha 1_{[N]}, \alpha 1_{[N]}, f) + \Lambda(f, \alpha 1_{[N]}, f) + \Lambda(\alpha 1_{[N]}, f, f) + \Lambda(f, f, f). \]

We can this consider $\Lambda(1_A, 1_A, 1_A)$ as the sum of $\alpha^3 \Lambda(1_{[N]}, 1_{[N]}, 1_{[N]})$ and seven other terms of the form $\Lambda(g_1, g_2, g_3)$ where at least one of $g_i = f$.

We are now ready to take our first step towards proving the Density Increment Strategy!
Lemma 4.1. Suppose \( N > C\alpha^{-C} \) and \( A \) contains fewer than \( \frac{1}{90}\alpha^3N^2 \) non-trivial three-term progressions. Then there are 1-bounded functions \( g_1, g_2, g_3 \) at least one of which is equal to \( f \) such that \( |\Lambda(g_1, g_2, g_3)| \geq \alpha^2 \).

Proof. To prove this lemma, we want to find a difference between a lower bound on \( \alpha^3\Lambda([N], [N], [N]) \) and an upper bound on the whole of \( \Lambda(1_A, 1_A, 1_A) \). The difference between the two must be "filled" by the sum of the seven terms of the form \( \Lambda(g_1, g_2, g_3) \).

Consider both \( x, d \leq N/3 \). Then, \( x, x + d, x + 2d \) all belong to \( \{1, ..., N\} \). Therefore, \( \{1, ..., N\} \) contains at least \( N^2/9 \) progressions. Since \( \Lambda([N], [N], [N]) \) tells us the number of arithmetic progressions divided by \( N^2 \),

\[
\alpha^3\Lambda([N], [N], [N]) \geq \frac{1}{9} \left( \frac{N}{N^2} \right)^2.
\]

We now obtain an upper bound on \( \Lambda(1_A, 1_A, 1_A) \). The number of non-trivial progressions is already bounded above by the hypothesis. The number of trivial arithmetic progressions in \( A \) is \( \alpha N \), the size of \( A \). Therefore,

\[
\Lambda(1_A, 1_A, 1_A) \leq \frac{1}{10} \alpha^3 \left( \frac{N}{N^2} \right)^2 + \frac{\alpha N}{N^2}.
\]

The second term in the upper bound is negligible, given that \( N > C\alpha^{-C} \) for sufficiently large \( C \). Consider it to be bounded above by \( \frac{1}{190} \alpha^3 \left( \frac{N}{N^2} \right)^2 \). Then,

\[
\Lambda(1_A, 1_A, 1_A) \leq \frac{2}{19} \alpha^3 \left( \frac{N}{N^2} \right)^2.
\]

Therefore, the sum of the seven terms of the form \( \Lambda(g_1, g_2, g_3) \) (where one of \( g_i = f \)) must have magnitude greater than \( \left( \frac{1}{9} - \frac{2}{19} \right) \alpha^3 \left( \frac{N}{N^2} \right)^2 \). Since \( N' \leq 3N \), \( \frac{1}{3N} \leq \frac{1}{N'} \).

Thus, the sum of the seven terms has magnitude greater than \( \left( \frac{1}{9} - \frac{2}{19} \right) \frac{1}{9} \alpha^3 \).

We see then that at least one of these seven terms must have magnitude greater than \( c\alpha^3 \) as claimed. □

In order to analyze the above property of \( f \) and \( \Lambda \), we introduce the Gowers \( U^2 \)-norm.

Definition 4.2. Given a function \( f : \mathbb{Z}/N \mathbb{Z} \to \mathbb{C} \), we define the Gowers \( U^2 \)-norm to be the functional

\[
\|f\|_{U^2} = \left( \mathbb{E}_{x, h_1, h_2 \in \mathbb{Z}/N \mathbb{Z}} f(x)f(x+h_1)f(x+h_2)f(x+h_1+h_2) \right)^{1/4}.
\]

Remark 4.3. The Gowers \( U^2 \)-norm is in fact a norm, however, this fact is not essential to the proof of Roth’s theorem [6]. Because of this, we will not prove that it is a norm in this paper.

To establish a relationship between the Gowers \( U^2 \)-norm and \( \Lambda \), we first have to prove the Cauchy-Schwarz inequality in a slightly obscure form.

Lemma 4.4 (Cauchy-Schwarz inequality). Given two finite sets \( X, Y \), let \( b : X \to \mathbb{C} \) be a 1-bounded function and \( F : X \times Y \to \mathbb{C} \) be any function. Then,

\[
\mathbb{E}_{x \in X, y \in Y} |b(x)F(x, y)|^2 \leq \mathbb{E}_{x \in X} \mathbb{E}_{y, y' \in Y} F(x, y) \overline{F(x, y')}.
\]
Proof. By the usual Cauchy-Schwarz inequality,
\[
\left| \sum_{x \in X} \alpha(x) \beta(x) \right|^2 \leq \left( \sum_{x \in X} |\alpha(x)|^2 \right) \left( \sum_{x \in X} |\beta(x)|^2 \right),
\]
where \( \alpha, \beta : X \to \mathbb{C} \) are any functions. To reformulate it in expectation notation, we divide both sides by \( |X|^2 \).
\[
|\mathbb{E}_{x \in X} \alpha(x) \beta(x)|^2 \leq (\mathbb{E}_{x \in X} |\alpha(x)|^2) (\mathbb{E}_{x \in X} |\beta(x)|^2).
\]
Then, to obtain the result, let \( \alpha(x) = b(x) \) and \( \beta(x) = \mathbb{E}_{y \in Y} F(x, y) \) and observe that \( |b(x)| \leq 1 \) for all \( x \) and
\[
|\mathbb{E}_{y \in Y} F(x, y)|^2 = (\mathbb{E}_{y \in Y} F(x, y)) (\mathbb{E}_{y \in Y} F(x, y)) = \mathbb{E}_{y, y' \in Y} F(x, y) F(x, y').
\]
\[\square\]

Lemma 4.5. Suppose \( f_1, f_2, f_3 : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C} \) are 1-bounded functions. Then,
\[
|\Lambda(f_1, f_2, f_3)| \leq ||f_i||_{U^2},
\]
for \( i = 1, 2, 3 \).

Proof. We will prove the result for \( i = 1 \). The other values of \( i \) follow without loss of generality.

First observe that \( 2x - y, x, y \) range over all three-term arithmetic progressions in \( \mathbb{Z}/N\mathbb{Z} \). Therefore,
\[
\Lambda(f_1, f_2, f_3) = \mathbb{E}_{x, y \in \mathbb{Z}/N\mathbb{Z}} f_1(2x - y) f_2(x) f_3(y).
\]
We then apply Lemma 4.4, which is valid because of the bound \( |f_2(x)| \leq 1 \), to obtain
\[
|\Lambda(f_1, f_2, f_3)|^2 \leq \mathbb{E}_{x, y \in \mathbb{Z}/N\mathbb{Z}} |\mathbb{E}_{y, y' \in \mathbb{Z}/N\mathbb{Z}} f_1(2x - y) f_1(2x - y') f_3(y) f_3(y')|
\]
Note that \( |f_3(y) f_3(y')| \leq 1 \), allowing us to apply Lemma 4.4 once more. We therefore have the inequality
\[
|\Lambda(f_1, f_2, f_3)|^4 \leq \mathbb{E}_{x, x' \in \mathbb{Z}/N\mathbb{Z}} |\mathbb{E}_{y, y' \in \mathbb{Z}/N\mathbb{Z}} f_1(2x - y) f_1(2x - y') f_3(2x' - y) f_3(2x' - y')|
\]
Since \( 2 \) does not divide \( N' \), \( 2x - y \) and \( 2x - 2x' \) attain all values over \( \mathbb{Z}/N'\mathbb{Z} \) exactly \( N \) times. Letting \( z = 2x - y, h_1 = y - y' \) and \( h_2 = 2x - 2x' \), we see that
\[
|\Lambda(f_1, f_2, f_3)|^4 \leq \mathbb{E}_{z, h_1, h_2 \in \mathbb{Z}/N\mathbb{Z}} f_1(z) f_1(z + h_1) f_1(z + h_2) f_1(z + h_1 + h_2),
\]
where the right-hand side is \( ||f_1||_{U^2}^4 \)
\[\square\]

Combining Lemma 4.1 and Lemma 4.5, we get the following lemma.

Lemma 4.6. Let \( \alpha \) be a real number such that \( 0 < \alpha < 1 \). Suppose \( N > C \alpha^{-3} \) and \( A \) is a subset of \( \{1, \ldots, N\} \) with cardinality \( \alpha N \) and less than \( \frac{1}{10} \alpha^3 N^2 \) three-term arithmetic progressions. Let \( f = 1_A - \alpha 1_{\{N\}} : \mathbb{Z}/N'\mathbb{Z} \) be the balanced function on \( A \). Then \( ||f||_{U^2} \geq \alpha^3 \).
5. Analyzing the Balanced Function via Fourier Analysis

To begin with, we prove a result connecting the Gowers $U^2$-norm with Fourier analysis.

**Lemma 5.1.** Given a function $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$, $\|f\|_{U^2} = \|f\|_4^2$, where $\|f\|_4 = \left(\sum_{h \in \mathbb{Z}/N\mathbb{Z}} |\hat{f}(h)|^4\right)^{1/4}$.

**Proof.** By Lemma 2.6, $\|f \ast f\|_2 = \|f \ast f\|_2$. By Lemma 2.7, $\|f \ast f\|_2 = \|\hat{f} \cdot \hat{f}\|_2$.

Since $\|\hat{f} \cdot \hat{f}\|_2 = \|f\|_2^4$, it is sufficient to prove that $\|f \ast f\|_2^2 = \|f\|_{U^2}^4$.

Observe that

$$\|f \ast f\|_2^2 = \mathbb{E}_y \mathbb{E}_x f(x) f(y - x)f(x')f(y - x').$$

Then, letting $z = x$, $h_1 = x' - x$, $h_2 = y - x' - x$,

$$\|f \ast f\|_2^2 = \mathbb{E}_z h_1, h_2 f(z + h_1)f(z + h_1)f(z + h_1 + h_2) = \|f\|_{U^2}^4.$$

□

**Theorem 5.2.** Suppose that $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$ is a 1-bounded function with $\|f\|_{U^2} \geq \delta$. Then there is some $h$ such that

$$\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)e(-hx/N) \geq \delta^2.$$

**Proof.** The conclusion is equivalent to $\max_{h \in \mathbb{Z}/N\mathbb{Z}} \hat{f}(h) \geq \delta^2$. We then have the following chain of inequalities.

$$\begin{align*}
\delta^4 &\leq \|f\|_{U^2}^4 \\
&= \|f\|_4^2 \\
&\leq \|f\|_2^4 \\
&\leq \|f\|_2^2 \left(\max_{h \in \mathbb{Z}/N\mathbb{Z}} \hat{f}(h)\right)^2 \\
&= \|f\|_2^2 \left(\max_{h \in \mathbb{Z}/N\mathbb{Z}} \hat{f}(h)\right)^2 \\
&\leq \left(\max_{h \in \mathbb{Z}/N\mathbb{Z}} \hat{f}(h)\right)^2.
\end{align*}$$

This gives us the result. □

Together with Lemma 4.6, this implies the following lemma, which does not involve a mention of $\mathbb{Z}/N'\mathbb{Z}$, since we do not have a need for a group structure anymore.

**Lemma 5.3.** Given $\alpha \in \mathbb{R}$ with $0 < \alpha < 1$, $N > C\alpha^{-C}$ and $A \subset \{1, ..., N\}$ with cardinality $\alpha N$. Suppose $A$ contains fewer than $\frac{1}{10} \alpha^3 N^2$ three-term arithmetic progressions and let $f = 1_A - \alpha$, which can now be considered as a function on $\{1, ..., N\}$. Then there is some $\theta \in [0, 1]$ such that

$$\left| \sum_{x=1}^N f(x)e(\theta x) \right| \geq c\alpha^6 N.$$
6. Applying the Pigeonhole Principle

At this point, to prove the Density Increment Strategy, we need to obtain a progression $P \subset \{1, ..., N\}$ of length at least $N^{1/3}$ where $|A \cap P|/|P| \geq \alpha + \epsilon$. It is sufficient to find a progression $P$ of length greater than $N^{1/3}$ such that

$$\sum_{x \in P} 1_A(x) - \alpha = \sum_{x \in P} f(x) = \epsilon|P|.$$  \hfill (6.1)

To do this, we want to partition $\{1, ..., N\}$ into a number of candidate progressions. We will need the following definition and lemma to do so.

**Definition 6.2.** Given $x \in \mathbb{R}$, let $\lfloor x \rfloor$ denote the largest integer less than or equal to $x$ and let $\langle x \rangle = x - \lfloor x \rfloor$, called the *integer part* and *fractional part* respectively.

**Lemma 6.3.** Take $\epsilon \in \mathbb{R}$ and $0 < \delta < 1$. Then there is a positive integer $d \leq 1/\delta$ such that $\langle x \rangle \leq \delta$.

**Proof.** Let $m = \lfloor 1/\delta \rfloor$. Then, by the pigeonhole principle, two of $0, \langle \epsilon \rangle, \langle 2\epsilon \rangle, ..., \langle m\epsilon \rangle$ are within $\delta$ of each other. Let these two be $n\epsilon$ and $n'\epsilon$. Then $d = \lfloor n - n' \rfloor$ proves the lemma. \hfill \Box

**Lemma 6.4.** Given $0 < \eta < 1$ and $\theta \in \mathbb{R}$, suppose that $N > CN^{-\epsilon}$. Then, it is possible to subdivide $\{1, ..., N\}$ into progressions $P_i$, $i = 1, ..., k$, each of length at least $N^{1/3}$, such that $\sup_{x, x' \in P_i} |e(\theta x) - e(\theta x')| \leq \eta$ for each $i$.

**Proof.** Let $\delta = \frac{1}{20} \eta N^{-1/3}$. Then, by Lemma 6.3 there exists a natural number $d$ such that $d \leq 1/\delta$ and $\langle d \rangle \leq \delta$.

If $N > CN^{-\epsilon}$, then

$$d \leq \frac{20N^{1/3}}{\eta} < CN^{1/6}N^{1/3} = C\sqrt{N}.$$  

Therefore, $d$ is at most $\sqrt{N}$. Let $P_k \subset \{1, ..., N\}$ be the progression $k, k + d, k + 2d, ...$ where $1 \leq k < d$. Then, each $P_k$ must have length at least $\frac{N}{\sqrt{N}} = \sqrt{N} > N^{1/3}$.

If $lN^{1/3} < |P_k| \leq (l + 1)N^{1/3}$ for some $l \geq 2$, then it is possible to break the progression up into $l$ progressions of which $l - 1$ have length $N^{1/3}$ and the last one has length $|P_k| - (l - 1)N^{1/3}$.

We have thus partitioned $\{1, ..., N\}$ into progressions with common difference $d$ and length between $N^{1/3}$ and $2N^{1/3}$. It is left to show that $\sup_{x, x' \in P} |e(\theta x) - e(\theta x')| \leq \eta$ for every such progression $P$.

Given such a progression $P$, of length at most $2N^{1/3}$, by the triangle inequality,

$$\sup_{x, x' \in P} |e(\theta x) - e(\theta x')| \leq \sum_{x \in P} |e(\theta(x + d)) - e(\theta x)|$$  

$$= \sum_{x \in P} |e(\theta x)||e(\theta d) - 1|$$  

$$= \sum_{x \in P} |e(\theta d) - 1|$$  

\hfill (6.5)  

$$\leq 2N^{1/3} |e(\theta d) - 1|.$$
We have the following equality
\[ |e(t) - 1| = \sqrt{(\cos(2\pi t) - 1) + \sin^2(2\pi t)} \]
\[ = \sqrt{\cos^2(2\pi t) - 2\cos(2\pi t) + 1 + \sin^2(2\pi t)} \]
\[ = \sqrt{2 - 2\cos(2\pi t)} \]
\[ = \sqrt{2 - 2 + 4\sin^2(\pi t)} \]
\[ = 2|\sin(\pi t)|. \]

Since \(|\sin(\pi t)|\) has period 1 and \(|\sin(\pi t)| \leq \pi t\) for \(0 \leq t \leq 1\),
\( (6.6) \quad |e(t) - 1| = 2|\sin(\pi t)| \leq 2\pi \langle t \rangle. \)

Then, combining (6.5) and (6.6), we see that,
\[ \sup_{x,x' \in P} |e(\theta x) - e(\theta x')| \leq 4N^{1/3}\pi(\theta d) \leq \eta \]
for all \(P\).

Our goal is to obtain (6.1) from Lemma 5.3. We will utilize Lemma 6.4 with \(\eta = \frac{\alpha N}{2}\). Consider \(P\) to be the progressions into which \(\{1, \ldots, N\}\) is partitioned by Lemma 6.4. Then, Lemma 5.3 implies
\[ \sum_i \left| \sum_{x \in P_i} f(x)e(\theta x) \right| \geq \alpha^6 \sum_i |P_i|. \]

By the triangle inequality and the fact is \(f\) is \(1\)-bounded, observe that
\[ \sum_i \left| \sum_{x \in P_i} f(x) \right| + \sum_i |P_i| \sup_{x,x' \in P_i} |e(\theta x) - e(\theta x')| \geq \sum_i \left| \sum_{x \in P_i} f(x)e(\theta x) \right| \geq \alpha^6 \sum_i |P_i|. \]

Then, by Lemma 6.4, \(\sum_i |P_i| \sup_{x,x' \in P_i} |e(\theta x) - e(\theta x')| \leq \sum_i |P_i| \frac{\alpha^6}{2}\). So,
\( (6.7) \quad \sum_i \left| \sum_{x \in P_i} f(x) \right| \geq \frac{\alpha^6}{2} \sum_i |P_i|. \)

Note that \(A\) has cardinality \(\alpha N\). Thus,
\( (6.8) \quad \sum_i \sum_{x \in P_i} f(x) = \sum_{x \in \{1, \ldots, N\}} f(x) = 0. \)

Then, adding (6.7) and (6.8) gives us
\[ \sum_i \sum_{x \in P_i} f(x) + \sum_i \left| \sum_{x \in P_i} f(x) \right| \geq \frac{\alpha^6}{2} \sum_i |P_i|. \]

Therefore by the pigeonhole principle, for some \(j\),
\[ \sum_{x \in P_j} f(x) + \left| \sum_{x \in P_j} f(x) \right| \geq \frac{\alpha^6}{2} |P_j|. \]
We immediately get
\[ \sum_{x \in P_j} f(x) \geq \frac{c\alpha^6}{4} |P_j|, \]
which proves the Density Increment Strategy and, therefore, Roth’s theorem.

ACKNOWLEDGMENTS

I would like to thank my mentor Iqra Altaf, for her help and kindness. I am also incredibly grateful to Professor May for allowing me to participate in the REU. I cannot think of a better way to spend a summer.

REFERENCES