Uniform Distribution and Roth's Theorem

Wang Yingnan

Shandong University

1. Uniform distribution mod one

In this talk, we mainly follow the discussion of Granville [1].

We begin by discussing Hermann Weyl's famous criterion for recognizing uniform distribution mod one.

Definition 1

A sequence of real numbers $a_1, a_2, \ldots$ is uniformly distributed mod one, if for all $0 \leq \alpha < \beta \leq 1$ we have

$$\#\{n \leq N : \ \alpha \leq \{a_n\} < \beta\} \sim (\beta - \alpha)N \qquad as \ \ N \to \infty.$$

In this talk, we mainly follow the discussion of Granville [1].

We begin by discussing Hermann Weyl's famous criterion for recognizing uniform distribution mod one.

Definition 1

A sequence of real numbers $a_1, a_2, \dots$ is uniformly distributed mod one, if for all $0 \le \alpha < \beta \le 1$ we have

$$\#\{n \le N : \ \alpha \le \{a_n\} < \beta\} \sim (\beta - \alpha)N \qquad as \ \ N \to \infty.$$

1. Uniform distribution mod one

In this talk, we mainly follow the discussion of Granville [1].

We begin by discussing Hermann Weyl's famous criterion for recognizing uniform distribution mod one.

Definition 1

A sequence of real numbers $a_1, a_2, \ldots$ *is uniformly distributed mod one, if for all* $0 \leq \alpha < \beta \leq 1$ *we have*

$$\#\{n \leq N : \ \alpha \leq \{a_n\} < \beta\} \sim (\beta - \alpha)N \qquad as \ \ N \to \infty.$$

Weyl's criterion

To determine whether a sequence of real numbers is uniformly distributed, we have the following famous criterion.

Theorem 1 (Weyl's criterion)

A sequence of real numbers $a_1, a_2, \ldots$ is uniformly distributed mod one, if and only if for every integer $b \neq 0$ we have

$$\sum_{n \leq N} e(ba_n) = o_b(N) \qquad as \quad N \to \infty. \tag{1}$$

Weyl's criterion

To determine whether a sequence of real numbers is uniformly distributed, we have the following famous criterion.

Theorem 1 (Weyl's criterion)

A sequence of real numbers $a_1, a_2, \ldots$ is uniformly distributed mod one, if and only if for every integer $b \neq 0$ we have

$$\sum_{n \leq N} e(ba_n) = o_b(N) \qquad as \;\; N \to \infty. \tag{1}$$

Weyl's criterion

In other words,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} e(ba_n) = 0.$$

Note that if $a_1, a_2, \ldots$ is uniformly distributed mod one, then $ka_1, ka_2, \ldots$ is uniformly distributed mod one for all $k \in \mathbb{Z}^*$.

In other words,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} e(ba_n) = 0.$$

Note that if $a_1, a_2, \ldots$ is uniformly distributed mod one, then $ka_1, ka_2, \ldots$ is uniformly distributed mod one for all $k \in \mathbb{Z}^*$.

Stronger theorem

In fact we can prove a stronger theorem as follows.

Theorem 2

The following statements are equivalent:

1. *A sequence of real numbers $a_1, a_2, \ldots$ is uniformly distributed mod one.*
2. *For every Riemann-integrable function f on $[0,1]$, we have*

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\}) = \int_0^1 f(x)dx.$$

3. *For every integer $b \neq 0$, we have*

$$\sum_{n\leq N} e(ba_n) = o_b(N) \qquad as \quad N \to \infty.$$

Stronger theorem

In fact we can prove a stronger theorem as follows.

Theorem 2

The following statements are equivalent:

1. *A sequence of real numbers* $a_1, a_2, \ldots$ *is uniformly distributed mod one.*
2. *For every Riemann-integrable function* f *on* $[0, 1]$, *we have*
$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{a_n\}) = \int_0^1 f(x)dx.$$
3. *For every integer* $b \neq 0$, *we have*
$$\sum_{n\leq N} e(ba_n) = o_b(N) \qquad as \;\; N \to \infty.$$

Stronger theorem

In fact we can prove a stronger theorem as follows.

Theorem 2

The following statements are equivalent:

1. *A sequence of real numbers* $a_1, a_2, \dots$ *is uniformly distributed mod one.*

2. *For every Riemann-integrable function* f *on* $[0,1]$*, we have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{a_n\}) = \int_0^1 f(x)dx.$$

3. *For every integer* $b \neq 0$*, we have*

$$\sum_{n\le N} e(ba_n) = o_b(N) \qquad as \quad N \to \infty.$$

Stronger theorem

In fact we can prove a stronger theorem as follows.

Theorem 2

The following statements are equivalent:

1. *A sequence of real numbers* $a_1, a_2, \ldots$ *is uniformly distributed mod one.*
2. *For every Riemann-integrable function* f *on* $[0,1]$*, we have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{a_n\}) = \int_0^1 f(x)dx.$$

3. *For every integer* $b \neq 0$*, we have*

$$\sum_{n\leq N} e(ba_n) = o_b(N) \qquad as \;\; N \to \infty.$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Suppose that the sequence $\{a_n\}$ is uniformly distributed mod one.

Fix $[\alpha, \beta) \subseteq [0, 1)$ and let $\chi_{[\alpha, \beta)}(x)$ denote the characteristic function of the interval $[\alpha, \beta)$. We may extend this function to $\mathbb{R}$ by periodicity (period 1) and still denote it by $\chi_{[\alpha, \beta)}(x)$.

Then, as a consequence of this definition, we find that

$$\#\{n \le N: \ \alpha \le \{a_n\} < \beta\} = \sum_{n=1}^{N} \chi_{[\alpha, \beta)}(a_n)$$

and

$$\frac{1}{N}\sum_{n=1}^{N} \chi_{[\alpha, \beta)}(a_n) \to \int_0^1 \chi_{[\alpha, \beta)}(x)dx, \qquad \text{as} \quad N \to \infty.$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Suppose that the sequence $\{a_n\}$ is uniformly distributed mod one.

Fix $[\alpha, \beta) \subseteq [0, 1)$ and let $\chi_{[\alpha, \beta)}(x)$ denote the characteristic function of the interval $[\alpha, \beta)$. We may extend this function to $\mathbb{R}$ by periodicity (period 1) and still denote it by $\chi_{[\alpha, \beta)}(x)$.

Then, as a consequence of this definition, we find that

$$\#\{n \le N : \ \alpha \le \{a_n\} < \beta\} = \sum_{n=1}^{N} \chi_{[\alpha, \beta)}(a_n)$$

and

$$\frac{1}{N}\sum_{n=1}^{N} \chi_{[\alpha, \beta)}(a_n) \to \int_0^1 \chi_{[\alpha, \beta)}(x)dx, \qquad \text{as} \quad N \to \infty.$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Suppose that the sequence $\{a_n\}$ is uniformly distributed mod one.

Fix $[\alpha,\, \beta) \subseteq [0,\, 1)$ and let $\chi_{[\alpha,\, \beta)}(x)$ denote the characteristic function of the interval $[\alpha,\, \beta)$. We may extend this function to $\mathbb{R}$ by periodicity (period 1) and still denote it by $\chi_{[\alpha,\, \beta)}(x)$.

Then, as a consequence of this definition, we find that

$$\#\{n \le N :\ \alpha \le \{a_n\} < \beta\} = \sum_{n=1}^{N} \chi_{[\alpha,\, \beta)}(a_n)$$

and

$$\frac{1}{N}\sum_{n=1}^{N} \chi_{[\alpha,\, \beta)}(a_n) \to \int_0^1 \chi_{[\alpha,\, \beta)}(x)dx, \qquad \text{as} \quad N \to \infty.$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Suppose that the sequence $\{a_n\}$ is uniformly distributed mod one.

Fix $[\alpha,\, \beta) \subseteq [0,\, 1)$ and let $\chi_{[\alpha,\, \beta)}(x)$ denote the characteristic function of the interval $[\alpha,\, \beta)$. We may extend this function to $\mathbb{R}$ by periodicity (period 1) and still denote it by $\chi_{[\alpha,\, \beta)}(x)$.

Then, as a consequence of this definition, we find that

$$\#\{n \le N:\ \alpha \le \{a_n\} < \beta\} = \sum_{n=1}^{N} \chi_{[\alpha,\, \beta)}(a_n)$$

and

$$\frac{1}{N}\sum_{n=1}^{N} \chi_{[\alpha,\, \beta)}(a_n) \to \int_0^1 \chi_{[\alpha,\, \beta)}(x)dx, \qquad \text{as} \quad N \to \infty.$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Since $f(x)$ is Riemann-integrable, $\forall \epsilon > 0$ there exists a partition of the interval $[0,1]$, $0 = x_0 < x_1 < \cdots < x_H = 1$, such that

$$\int_0^1 f(x)dx - \frac{\epsilon}{2} \le \int_0^1 f_L(x)dx \le \int_0^1 f(x)dx$$

and

$$\int_0^1 f(x)dx \le \int_0^1 f_U(x)dx \le \int_0^1 f(x)dx + \frac{\epsilon}{2},$$

where

$$f_L(x) = \inf_{x_{j-1} \le y \le x_j} f(y) \quad \text{for} \quad x \in [x_{j-1}, x_j)$$

and

$$f_U(x) = \sup_{x_{j-1} \le y \le x_j} f(y) \quad \text{for} \quad x \in [x_{j-1}, x_j).$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Since $f(x)$ is Riemann-integrable, $\forall \epsilon > 0$ there exists a partition of the interval $[0,1]$, $0 = x_0 < x_1 < \cdots < x_H = 1$, such that

$$\int_0^1 f(x)dx - \frac{\epsilon}{2} \leq \int_0^1 f_L(x)dx \leq \int_0^1 f(x)dx$$

and

$$\int_0^1 f(x)dx \leq \int_0^1 f_U(x)dx \leq \int_0^1 f(x)dx + \frac{\epsilon}{2},$$

where

$$f_L(x) = \inf_{x_{j-1} \leq y \leq x_j} f(y) \quad \text{for} \quad x \in [x_{j-1}, x_j)$$

and

$$f_U(x) = \sup_{x_{j-1} \leq y \leq x_j} f(y) \quad \text{for} \quad x \in [x_{j-1}, x_j).$$

Proof of Theorem 2: (1) $\Rightarrow$ (2)

Since $f(x)$ is Riemann-integrable, $\forall \epsilon > 0$ there exists a partition of the interval $[0,1]$, $0 = x_0 < x_1 < \cdots < x_H = 1$, such that

$$\int_0^1 f(x)dx - \frac{\epsilon}{2} \le \int_0^1 f_L(x)dx \le \int_0^1 f(x)dx$$

and

$$\int_0^1 f(x)dx \le \int_0^1 f_U(x)dx \le \int_0^1 f(x)dx + \frac{\epsilon}{2},$$

where

$$f_L(x) = \inf_{x_{j-1} \le y \le x_j} f(y) \quad \text{for} \quad x \in [x_{j-1}, x_j)$$

and

$$f_U(x) = \sup_{x_{j-1} \le y \le x_j} f(y) \quad \text{for} \quad x \in [x_{j-1}, x_j).$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Since $f(x)$ is Riemann-integrable, $\forall \epsilon > 0$ there exists a partition of the interval $[0, 1]$, $0 = x_0 < x_1 < \cdots < x_H = 1$, such that

$$\int_0^1 f(x)dx - \frac{\epsilon}{2} \leq \int_0^1 f_L(x)dx \leq \int_0^1 f(x)dx$$

and

$$\int_0^1 f(x)dx \leq \int_0^1 f_U(x)dx \leq \int_0^1 f(x)dx + \frac{\epsilon}{2},$$

where

$$f_L(x) = \inf_{x_{j-1} \leq y \leq x_j} f(y) \quad \text{for} \quad x \in [x_{j-1}, x_j)$$

and

$$f_U(x) = \sup_{x_{j-1} \leq y \leq x_j} f(y) \quad \text{for} \quad x \in [x_{j-1}, x_j).$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Obviously,

$$\sum_{n=1}^{N} f_L(\{a_n\}) \leq \sum_{n=1}^{N} f(\{a_n\}) \leq \sum_{n=1}^{N} f_U(\{a_n\}).$$

However,

$$\frac{1}{N}\sum_{n=1}^{N} f_L(\{a_n\}) \to \int_0^1 f_L(x)dx$$

because f_L is a finite linear combination of characteristic functions of intervals.

Similarly we have

$$\frac{1}{N}\sum_{n=1}^{N} f_U(\{a_n\}) \to \int_0^1 f_U(x)dx.$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Obviously,

$$\sum_{n=1}^{N} f_L(\{a_n\}) \leq \sum_{n=1}^{N} f(\{a_n\}) \leq \sum_{n=1}^{N} f_U(\{a_n\}).$$

However,

$$\frac{1}{N}\sum_{n=1}^{N} f_L(\{a_n\}) \to \int_0^1 f_L(x)dx$$

because f_L is a finite linear combination of characteristic functions of intervals.

Similarly we have

$$\frac{1}{N}\sum_{n=1}^{N} f_U(\{a_n\}) \to \int_0^1 f_U(x)dx.$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Obviously,

$$\sum_{n=1}^{N} f_L(\{a_n\}) \leq \sum_{n=1}^{N} f(\{a_n\}) \leq \sum_{n=1}^{N} f_U(\{a_n\}).$$

However,

$$\frac{1}{N}\sum_{n=1}^{N} f_L(\{a_n\}) \to \int_0^1 f_L(x)dx$$

because f_L is a finite linear combination of characteristic functions of intervals.

Similarly we have

$$\frac{1}{N}\sum_{n=1}^{N} f_U(\{a_n\}) \to \int_0^1 f_U(x)dx.$$

Therefore

$$\int_0^1 f(x)dx - \frac{\epsilon}{2} \le \int_0^1 f_L(x)dx \le \liminf_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\}),$$

and

$$\int_0^1 f(x)dx + \frac{\epsilon}{2} \ge \int_0^1 f_U(x)dx \ge \limsup_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\}).$$

Since this is true for every $\epsilon > 0$,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\})$$

exists and must be equal to

$$\int_0^1 f(x)dx.$$

Proof of Theorem 2: $(1) \Rightarrow (2)$

Therefore

$$\int_0^1 f(x)dx - \frac{\epsilon}{2} \leq \int_0^1 f_L(x)dx \leq \liminf_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\}),$$

and

$$\int_0^1 f(x)dx + \frac{\epsilon}{2} \geq \int_0^1 f_U(x)dx \geq \limsup_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\}).$$

Since this is true for every $\epsilon > 0$,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\})$$

exists and must be equal to

$$\int_0^1 f(x)dx.$$

Proof of Theorem 2: (1) $\Rightarrow$ (2)

Therefore

$$\int_0^1 f(x)dx - \frac{\epsilon}{2} \leq \int_0^1 f_L(x)dx \leq \liminf_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\}),$$

and

$$\int_0^1 f(x)dx + \frac{\epsilon}{2} \geq \int_0^1 f_U(x)dx \geq \limsup_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\}).$$

Since this is true for every $\epsilon > 0$,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{a_n\})$$

exists and must be equal to

$$\int_0^1 f(x)dx.$$

Proof of Theorem 2: $(2) \Rightarrow (3)$

This follows immediately by taking

$$f(x) = \cos(bx) \quad \text{and} \quad f(x) = \sin(bx)$$

respectively, where $b \in \mathbb{Z}^*$.

Proof of Theorem 2: $(3) \Rightarrow (1)$

What we want to show can be reformulated as the statement that

$$\frac{1}{N}\sum_{n=1}^{N}\chi_{[\alpha,\,\beta)}(a_n) \to \int_0^1 \chi_{[\alpha,\,\beta)}(x)dx \qquad \text{as} \quad N \to \infty.$$

Firstly we shall prove

Lemma 1

If f is continuous and periodic of period 1, and $\{a_n\}$ is a sequence of real numbers satisfying (1). Then

$$\frac{1}{N}\sum_{n=1}^{N} f(a_n) \to \int_0^1 f(x)dx \qquad as \quad N \to \infty.$$

Proof of Theorem 2: $(3) \Rightarrow (1)$

What we want to show can be reformulated as the statement that

$$\frac{1}{N}\sum_{n=1}^{N} \chi_{[\alpha,\,\beta)}(a_n) \to \int_0^1 \chi_{[\alpha,\,\beta)}(x)dx \qquad \text{as} \quad N \to \infty.$$

Firstly we shall prove

Lemma 1

If f is continuous and periodic of period 1, and $\{a_n\}$ is a sequence of real numbers satisfying (1). Then

$$\frac{1}{N}\sum_{n=1}^{N} f(a_n) \to \int_0^1 f(x)dx \qquad \text{as} \quad N \to \infty.$$

Proof of Theorem 2: proof of Lemma 1

We easily get that $f(x) = e(kx),\ \forall k \in \mathbb{Z}$, satisfies the lemma. So the lemma is also true for all trigonometric polynomials.

Let $\epsilon > 0$. If f is any continuous periodic function of period 1, we can choose a trigonometric polynomial P such that

$$\sup_{x\in\mathbb{R}} |\, f(x) - P(x)\,| < \frac{\epsilon}{3}.$$

(See Corollary 5.4 on page 54 in [3])

We easily get that $f(x) = e(kx),\ \forall k \in \mathbb{Z}$, satisfies the lemma. So the lemma is also true for all trigonometric polynomials.

Let $\epsilon > 0$. If f is any continuous periodic function of period 1, we can choose a trigonometric polynomial P such that

$$\sup_{x\in\mathbb{R}} |\, f(x) - P(x)\,| < \frac{\epsilon}{3}.$$

(See Corollary 5.4 on page 54 in [3])

Then for all large N, we have

$$I = \Big| \frac{1}{N} \sum_{n=1}^{N} P(a_n) - \int_0^1 P(x)dx \Big| < \frac{\epsilon}{3}.$$

Therefore

$$\begin{aligned} &\Big| \frac{1}{N} \sum_{n=1}^{N} f(a_n) - \int_0^1 f(x)dx \Big| \\ &\le \frac{1}{N} \sum_{n=1}^{N} \big| f(a_n) - P(a_n) \big| + I + \int_0^1 \big| P(x) - f(x) \big| dx \\ &< \epsilon. \end{aligned}$$

Proof of Theorem 2: proof of Lemma 1

Then for all large N, we have

$$I = \Big| \frac{1}{N} \sum_{n=1}^{N} P(a_n) - \int_0^1 P(x)dx \Big| < \frac{\epsilon}{3}.$$

Therefore

$$\begin{aligned} & \Big| \frac{1}{N} \sum_{n=1}^{N} f(a_n) - \int_0^1 f(x)dx \Big| \\ \leq & \frac{1}{N} \sum_{n=1}^{N} \big|f(a_n) - P(a_n)\big| + I + \int_0^1 \big|P(x) - f(x)\big|dx \\ < & \epsilon. \end{aligned}$$

Proof of Theorem 2: $(3) \Rightarrow (1)$

Choose two continuous periodic functions f_ϵ^+ and f_ϵ^- of period 1 such that

$$f_\epsilon^-(x) \leq \chi_{[\alpha,\, \beta)}(x) \leq f_\epsilon^+(x) \qquad \text{on} \;\; [0,\, 1);$$

both f_ϵ^+ and f_ϵ^- are bounded by 1 and agree with $\chi_{[\alpha,\, \beta)}(x)$ except in intervals of total length 2ϵ on $[0,\, 1)$.

Obviously,

$$\beta - \alpha - 2\epsilon \leq \int_0^1 f_\epsilon^-(x)dx$$

and

$$\int_0^1 f_\epsilon^+(x)dx \leq \beta - \alpha + 2\epsilon.$$

Proof of Theorem 2: $(3) \Rightarrow (1)$

Choose two continuous periodic functions f_ϵ^+ and f_ϵ^- of period 1 such that

$$f_\epsilon^-(x) \le \chi_{[\alpha,\,\beta)}(x) \le f_\epsilon^+(x) \qquad \text{on} \;\; [0,\,1);$$

both f_ϵ^+ and f_ϵ^- are bounded by 1 and agree with $\chi_{[\alpha,\,\beta)}(x)$ except in intervals of total length 2ϵ on $[0,\,1)$.

Obviously,

$$\beta - \alpha - 2\epsilon \le \int_0^1 f_\epsilon^-(x)dx$$

and

$$\int_0^1 f_\epsilon^+(x)dx \le \beta - \alpha + 2\epsilon.$$

Proof of Theorem 2: $(3) \Rightarrow (1)$

Write

$$S_N = \frac{1}{N} \sum_{n=1}^{N} \chi_{(\alpha,\,\beta)}(a_n).$$

Then we have

$$\frac{1}{N} \sum_{n=1}^{N} f_\epsilon^-(a_n) \le S_N \le \frac{1}{N} \sum_{n=1}^{N} f_\epsilon^+(a_n).$$

Therefore

$$\beta - \alpha - 2\epsilon \le \liminf_{N\to\infty} S_N, \qquad \limsup_{N\to\infty} S_N \le \beta - \alpha + 2\epsilon.$$

Since this is true for every $\epsilon > 0$, $\lim_{N\to\infty} S_N$ exists and must be equal to $\beta - \alpha$.

Proof of Theorem 2: $(3) \Rightarrow (1)$

Write

$$S_N = \frac{1}{N}\sum_{n=1}^{N}\chi_{(\alpha,\,\beta)}(a_n).$$

Then we have

$$\frac{1}{N}\sum_{n=1}^{N} f_\epsilon^-(a_n) \le S_N \le \frac{1}{N}\sum_{n=1}^{N} f_\epsilon^+(a_n).$$

Therefore

$$\beta - \alpha - 2\epsilon \le \liminf_{N\to\infty} S_N, \qquad \limsup_{N\to\infty} S_N \le \beta - \alpha + 2\epsilon.$$

Since this is true for every $\epsilon > 0$, $\lim_{N\to\infty} S_N$ exists and must be equal to $\beta - \alpha$.

Proof of Theorem 2: $(3) \Rightarrow (1)$

Write

$$S_N = \frac{1}{N} \sum_{n=1}^{N} \chi_{(\alpha,\,\beta)}(a_n).$$

Then we have

$$\frac{1}{N} \sum_{n=1}^{N} f_\epsilon^-(a_n) \leq S_N \leq \frac{1}{N} \sum_{n=1}^{N} f_\epsilon^+(a_n).$$

Therefore

$$\beta - \alpha - 2\epsilon \leq \liminf_{N\to\infty} S_N, \qquad \limsup_{N\to\infty} S_N \leq \beta - \alpha + 2\epsilon.$$

Since this is true for every $\epsilon > 0$, $\lim_{N\to\infty} S_N$ exists and must be equal to $\beta - \alpha$.

Proof of Theorem 2: $(3) \Rightarrow (1)$

Write

$$S_N = \frac{1}{N}\sum_{n=1}^{N} \chi_{(\alpha,\,\beta)}(a_n).$$

Then we have

$$\frac{1}{N}\sum_{n=1}^{N} f_\epsilon^-(a_n) \le S_N \le \frac{1}{N}\sum_{n=1}^{N} f_\epsilon^+(a_n).$$

Therefore

$$\beta - \alpha - 2\epsilon \le \liminf_{N\to\infty} S_N, \qquad \limsup_{N\to\infty} S_N \le \beta - \alpha + 2\epsilon.$$

Since this is true for every $\epsilon > 0$, $\lim_{N\to\infty} S_N$ exists and must be equal to $\beta - \alpha$.

Example 1

An famous example is that the sequence of α, 2α, 3α, $\ldots$ is uniformly distributed mod one if α is irrational.

Since $b\alpha$ is not an integer for $b \in \mathbb{Z}^*$, we have

$$\begin{aligned} \left| \frac{1}{N} \sum_{n=1}^{N} e(bn\alpha) \right| &= \left| \frac{1}{N} \frac{e(b\alpha)(1 - e(bN\alpha))}{1 - e(b\alpha)} \right| \\ &\leq \frac{2}{N \left| 1 - e(b\alpha) \right|} \\ &= o(1). \end{aligned}$$

By Weyl's criterion, we know that the sequence of α, 2α, 3α, $\ldots$ is uniformly distributed mod one.

Example 1

An famous example is that the sequence of $\alpha, 2\alpha, 3\alpha, \ldots$ is uniformly distributed mod one if α is irrational.

Since $b\alpha$ is not an integer for $b \in \mathbb{Z}^*$, we have

$$\left| \frac{1}{N} \sum_{n=1}^{N} e(bn\alpha) \right| = \left| \frac{1}{N} \frac{e(b\alpha)(1 - e(bN\alpha))}{1 - e(b\alpha)} \right| \leq \frac{2}{N|1 - e(b\alpha)|} = o(1).$$

By Weyl's criterion, we know that the sequence of $\alpha, 2\alpha, 3\alpha, \ldots$ is uniformly distributed mod one.

Example 1

An famous example is that the sequence of α, 2α, 3α, $\ldots$ is uniformly distributed mod one if α is irrational.

Since $b\alpha$ is not an integer for $b \in \mathbb{Z}^*$, we have

$$\Big|\frac{1}{N}\sum_{n=1}^{N} e(bn\alpha)\Big| = \Big|\frac{1}{N}\frac{e(b\alpha)(1-e(bN\alpha))}{1-e(b\alpha)}\Big| \le \frac{2}{N|1-e(b\alpha)|} = o(1).$$

By Weyl's criterion, we know that the sequence of α, 2α, 3α, $\ldots$ is uniformly distributed mod one.

Example 1

An famous example is that the sequence of $\alpha,\ 2\alpha,\ 3\alpha,\ \ldots$ is uniformly distributed mod one if α is irrational.

Since $b\alpha$ is not an integer for $b \in \mathbb{Z}^*$, we have

$$\begin{aligned} \Big|\, \frac{1}{N}\sum_{n=1}^{N} e(bn\alpha) \,\Big| &= \Big|\, \frac{1}{N}\frac{e(b\alpha)(1-e(bN\alpha))}{1-e(b\alpha)} \,\Big| \\ &\le \frac{2}{N|\,1-e(b\alpha)\,|} \\ &= o(1). \end{aligned}$$

By Weyl's criterion, we know that the sequence of $\alpha,\ 2\alpha,\ 3\alpha,\ \ldots$ is uniformly distributed mod one.

Example 2

We consider another interesting example about uniform distribution. Let

$$2^n = a_{k_n} 10^{k_n} + \cdots \quad \text{for all } n \in \mathbb{Z}^+$$

and

$$S_N(m) = \frac{1}{N} \# \{0 \leq n < N : \; a_{k_n} = m\} \quad \text{for } m = 1, 2, \ldots, 9.$$

We have

$$a_{k_n} = m \Longleftrightarrow m10^{k_n} \leq 2^n < (m+1)10^{k_n} \Longleftrightarrow$$
$$\log_{10} m + k_n \leq \frac{n}{\log_2 10} < \log_{10}(m+1) + k_n.$$

Example 2

We consider another interesting example about uniform distribution. Let

$$2^n = a_{k_n} 10^{k_n} + \cdots \quad \text{for all } n \in \mathbb{Z}^+$$

and

$$S_N(m) = \frac{1}{N} \# \{0 \le n < N : \ a_{k_n} = m\} \quad \text{for } m = 1, 2, \ldots, 9.$$

We have

$$a_{k_n} = m \Longleftrightarrow m 10^{k_n} \le 2^n < (m+1) 10^{k_n} \Longleftrightarrow$$

$$\log_{10} m + k_n \le \frac{n}{\log_2 10} < \log_{10}(m+1) + k_n.$$

Example 2

We consider another interesting example about uniform distribution. Let

$$2^n = a_{k_n} 10^{k_n} + \cdots \quad \text{for all } n \in \mathbb{Z}^+$$

and

$$S_N(m) = \frac{1}{N} \# \{0 \le n < N : \ a_{k_n} = m\} \quad \text{for } m = 1, 2, \ldots, 9.$$

We have

$$a_{k_n} = m \Longleftrightarrow m 10^{k_n} \le 2^n < (m+1) 10^{k_n} \Longleftrightarrow$$
$$\log_{10} m + k_n \le \frac{n}{\log_2 10} < \log_{10}(m+1) + k_n.$$

Example 2

Therefore

$$S_N(m) = \frac{1}{N}\#\left\{0 \le n < N:\ \log_{10} m \le \left\{\frac{n}{\log_2 10}\right\} < \log_{10}(m+1)\right\}.$$

Since $\log_2 10$ is irrational, we get

$$\lim_{N\to\infty} S_N(m) = \log_{10}(m+1) - \log_{10} m$$

by Weyl's criterion.

However, we can not determine whether some other interesting sequences are uniformly distributed mod one even today. The sequence $\left\{\left(\frac{3}{2}\right)^n\right\}$ is a very famous one of them.

Example 2

Therefore

$$S_N(m) = \frac{1}{N}\#\left\{0 \le n < N:\ \log_{10} m \le \left\{\frac{n}{\log_2 10}\right\} < \log_{10}(m+1)\right\}.$$

Since $\log_2 10$ is irrational, we get

$$\lim_{N\to\infty} S_N(m) = \log_{10}(m+1) - \log_{10} m$$

by Weyl's criterion.

However, we can not determine whether some other interesting sequences are uniformly distributed mod one even today. The sequence $\left\{\left(\frac{3}{2}\right)^n\right\}$ is a very famous one of them.

Example 2

Therefore

$$S_N(m) = \frac{1}{N}\#\left\{0 \le n < N:\ \log_{10} m \le \left\{\frac{n}{\log_2 10}\right\} < \log_{10}(m+1)\right\}.$$

Since $\log_2 10$ is irrational, we get

$$\lim_{N\to\infty} S_N(m) = \log_{10}(m+1) - \log_{10} m$$

by Weyl's criterion.

However, we can not determine whether some other interesting sequences are uniformly distributed mod one even today. The sequence $\left\{(\frac{3}{2})^n\right\}$ is a very famous one of them.

2. Uniform distribution mod N

For a given set A of residues mod N, define

$$\widehat{A}(b) := \sum_{n\in A} e(\frac{bn}{N}).$$

Let $(t)_N$ denote the least non-negative residue of $t \pmod N$. So

$$\frac{(t)_N}{N} = \left\{\frac{t}{N}\right\}.$$

The idea of uniform distribution mod N is surely something like: for all $0 \le \alpha < \beta \le 1$ and all $m \not\equiv 0 \pmod N$, we have

$$\#\{a \in A : \ \alpha N < (ma)_N \le \beta N\} \sim (\beta - \alpha)|A|. \tag{2}$$

For a given set A of residues mod N, define

$$\widehat{A}(b) := \sum_{n \in A} e(\frac{bn}{N}).$$

Let $(t)_N$ denote the least non-negative residue of $t \pmod N$. So

$$\frac{(t)_N}{N} = \left\{ \frac{t}{N} \right\}.$$

The idea of uniform distribution mod N is surely something like: for all $0 \le \alpha < \beta \le 1$ and all $m \not\equiv 0 \pmod N$, we have

$$\#\{a \in A : \ \alpha N < (ma)_N \le \beta N\} \sim (\beta - \alpha)|A|. \qquad (2)$$

For a given set A of residues mod N, define

$$\widehat{A}(b) := \sum_{n \in A} e(\frac{bn}{N}).$$

Let $(t)_N$ denote the least non-negative residue of $t \pmod N$. So

$$\frac{(t)_N}{N} = \left\{\frac{t}{N}\right\}.$$

The idea of uniform distribution mod N is surely something like: for all $0 \le \alpha < \beta \le 1$ and all $m \not\equiv 0 \pmod N$, we have

$$\#\{a \in A : \ \alpha N < (ma)_N \le \beta N\} \sim (\beta - \alpha)|A|. \tag{2}$$

Definition of Error(A)

One can only make sense of such a definition if $|A| \to \infty$ (since this is an asymptotic formula) but we are often interested in smaller sets A, indeed which are subsets of $\{1, 2, \ldots, N\}$. So we will work with something motivated by, but different from, (2).

Let us see how far we can go in proving an analogy to Weyl's criterion. For given subset A of the residues mod N, define

$$\text{Error}(A) := \max_{\substack{0 \le x < x+y \le N \\ m \not\equiv 0 \pmod N}} \left| \frac{\#\{a \in A : \ x < (ma)_N \le x+y\}}{|A|} - \frac{y}{N} \right|.$$

Definition of Error(A)

One can only make sense of such a definition if $|A| \to \infty$ (since this is an asymptotic formula) but we are often interested in smaller sets A, indeed which are subsets of $\{1, 2, \ldots, N\}$. So we will work with something motivated by, but different from, (2).

Let us see how far we can go in proving an analogy to Weyl's criterion. For given subset A of the residues mod N, define

$$\mathrm{Error}(A) := \max_{\substack{0 \le x < x+y \le N \\ m \not\equiv 0 (\mathrm{mod}\ N)}} \left| \frac{\#\{a \in A : \ x < (ma)_N \le x+y\}}{|A|} - \frac{y}{N} \right|.$$

Definition of Error(A)

One can only make sense of such a definition if $|A| \to \infty$ (since this is an asymptotic formula) but we are often interested in smaller sets A, indeed which are subsets of $\{1, 2, \ldots, N\}$. So we will work with something motivated by, but different from, (2).

Let us see how far we can go in proving an analogy to Weyl's criterion. For given subset A of the residues mod N, define

$$\mathrm{Error}(A) := \max_{\substack{0 \le x < x+y \le N \\ m \not\equiv 0 (\mathrm{mod}\, N)}} \left| \frac{\#\{a \in A : \ x < (ma)_N \le x + y\}}{|A|} - \frac{y}{N} \right|.$$

Theorem 3

Theorem 3

Suppose that N is prime. Fix $\delta > 0$. We have

1. *If $Error(A) \le \delta^2$, then for any $m \not\equiv 0 \,(mod\, N)$,*

$$\widehat{A}(m) \ll \delta |A|.$$

2. *If $|\widehat{A}(m)| \le \delta^2 |A|$ for all $m \not\equiv 0 \,(mod\, N)$, then*

$$Error(A) \ll \delta,$$

where

$$\delta \ll \frac{1}{\log \frac{N}{|A|}}.$$

Theorem 3

Suppose that N *is prime. Fix* $\delta > 0$. *We have*

1. *If* $Error(A) \leq \delta^2$, *then for any* $m \not\equiv 0 \,(mod\, N)$,

$$\widehat{A}(m) \ll \delta |A|.$$

2. *If* $|\widehat{A}(m)| \leq \delta^2 |A|$ *for all* $m \not\equiv 0 \,(mod\, N)$, *then*

$$Error(A) \ll \delta,$$

where

$$\delta \ll \frac{1}{\log \frac{N}{|A|}}.$$

Proof of Theorem 3: proof of (1)

For given integer $k > 1$, if $(ma)_N \in (x,\, x + \frac{N}{k}]$, then

$$e(\frac{ma}{N}) = e(\frac{x}{N} + \frac{\theta}{k})$$

$$= e(\frac{x}{N}) + e(\frac{x}{N})(e(\frac{\theta}{k}) - 1)$$

$$= e(\frac{x}{N}) + O(\frac{1}{k}),$$

here $\theta \in (0,\, 1]$.

For given integer $k > 1$, if $(ma)_N \in (x,\, x + \frac{N}{k}]$, then

$$\begin{aligned} e(\frac{ma}{N}) &= e(\frac{x}{N} + \frac{\theta}{k}) \\ &= e(\frac{x}{N}) + e(\frac{x}{N})(e(\frac{\theta}{k}) - 1) \\ &= e(\frac{x}{N}) + O(\frac{1}{k}), \end{aligned}$$

here $\theta \in (0,\, 1]$.

For given integer $k > 1$, if $(ma)_N \in (x,\ x + \frac{N}{k}]$, then

$$\begin{aligned} e(\frac{ma}{N}) &= e(\frac{x}{N} + \frac{\theta}{k}) \\ &= e(\frac{x}{N}) + e(\frac{x}{N})(e(\frac{\theta}{k}) - 1) \\ &= e(\frac{x}{N}) + O(\frac{1}{k}), \end{aligned}$$

here $\theta \in (0,\ 1]$.

Proof of Theorem 3: proof of (1)

Therefore

$$\widehat{A}(m) = \sum_{j=0}^{k-1} \sum_{\substack{a\in A \\ \frac{jN}{k} < (ma)_N \leq \frac{(j+1)N}{k}}} e(\frac{ma}{N})$$

$$= \sum_{j=0}^{k-1} \sum_{\substack{a\in A \\ \frac{jN}{k} < (ma)_N \leq \frac{(j+1)N}{k}}} (e(\frac{j}{k}) + O(\frac{1}{k}))$$

$$= \sum_{j=0}^{k-1} e(\frac{j}{k})(\frac{1}{k} + O(\mathrm{Error}(A)))|A| + O(\frac{|A|}{k})$$

$$= O(k|A|\,\mathrm{Error}(A)) + O(\frac{|A|}{k}).$$

The result follows taking $k \asymp \frac{1}{\delta}$.

Proof of Theorem 3: proof of (1)

Therefore

$$\widehat{A}(m) = \sum_{j=0}^{k-1} \sum_{\substack{a\in A \\ \frac{jN}{k} < (ma)_N \le \frac{(j+1)N}{k}}} e(\frac{ma}{N})$$

$$= \sum_{j=0}^{k-1} \sum_{\substack{a\in A \\ \frac{jN}{k} < (ma)_N \le \frac{(j+1)N}{k}}} \left(e(\frac{j}{k}) + O(\frac{1}{k})\right)$$

$$= \sum_{j=0}^{k-1} e(\frac{j}{k})(\frac{1}{k} + O(\mathrm{Error}(A)))|A| + O(\frac{|A|}{k})$$

$$= O(k|A|\,\mathrm{Error}(A)) + O(\frac{|A|}{k}).$$

The result follows taking $k \asymp \frac{1}{\delta}$.

Proof of Theorem 3: proof of (1)

Therefore

$$\widehat{A}(m) = \sum_{j=0}^{k-1} \sum_{\substack{a \in A \\ \frac{jN}{k} < (ma)_N \le \frac{(j+1)N}{k}}} e(\frac{ma}{N})$$

$$= \sum_{j=0}^{k-1} \sum_{\substack{a \in A \\ \frac{jN}{k} < (ma)_N \le \frac{(j+1)N}{k}}} \big(e(\frac{j}{k}) + O(\frac{1}{k})\big)$$

$$= \sum_{j=0}^{k-1} e(\frac{j}{k})\big(\frac{1}{k} + O(\mathrm{Error}(A))\big)|A| + O\big(\frac{|A|}{k}\big)$$

$$= O(k|A|\,\mathrm{Error}(A)) + O\big(\frac{|A|}{k}\big).$$

The result follows taking $k \asymp \frac{1}{\delta}$.

Proof of Theorem 3: proof of (1)

Therefore

$$\begin{aligned}
\widehat{A}(m) &= \sum_{j=0}^{k-1} \sum_{\substack{a\in A \\ \frac{jN}{k} < (ma)_N \le \frac{(j+1)N}{k}}} e(\frac{ma}{N}) \\
&= \sum_{j=0}^{k-1} \sum_{\substack{a\in A \\ \frac{jN}{k} < (ma)_N \le \frac{(j+1)N}{k}}} \left(e(\frac{j}{k}) + O(\frac{1}{k})\right) \\
&= \sum_{j=0}^{k-1} e(\frac{j}{k})\Big(\frac{1}{k} + O(\mathrm{Error}(A))\Big)|A| + O\Big(\frac{|A|}{k}\Big) \\
&= O(k|A|\,\mathrm{Error}(A)) + O\Big(\frac{|A|}{k}\Big).
\end{aligned}$$

The result follows taking $k \asymp \frac{1}{\delta}$.

Proof of Theorem 3: proof of (1)

Therefore

$$\begin{aligned}
\widehat{A}(m) &= \sum_{j=0}^{k-1} \sum_{\substack{a\in A \\ \frac{jN}{k} < (ma)_N \le \frac{(j+1)N}{k}}} e(\frac{ma}{N}) \\
&= \sum_{j=0}^{k-1} \sum_{\substack{a\in A \\ \frac{jN}{k} < (ma)_N \le \frac{(j+1)N}{k}}} (e(\frac{j}{k}) + O(\frac{1}{k})) \\
&= \sum_{j=0}^{k-1} e(\frac{j}{k})\Big(\frac{1}{k} + O(\mathrm{Error}(A))\Big)|A| + O\Big(\frac{|A|}{k}\Big) \\
&= O(k|A|\,\mathrm{Error}(A)) + O\Big(\frac{|A|}{k}\Big).
\end{aligned}$$

The result follows taking $k \asymp \frac{1}{\delta}$.

For integers x and y, we have

$$\sum_{\substack{a\in A\\ x<(ma)_N\le x+y}} 1=\sum_{j=1}^{y}\sum_{a\in A}\frac{1}{N}\sum_{r\in(\frac{-N}{2},\frac{N}{2}]} e(\frac{r(ma-x-j)}{N})$$

$$=\frac{1}{N}\sum_{r\in(\frac{-N}{2},\frac{N}{2}]} e(-\frac{rx}{N})\sum_{a\in A}e(\frac{rma}{N})\sum_{j=1}^{y}e(-\frac{rj}{N})$$

$$=\frac{y}{N}|A|+\frac{1}{N}\sum_{r\neq 0}e(-\frac{rx}{N})\widehat{A}(rm)\sum_{j=1}^{y}e(-\frac{rj}{N}).$$

For integers x and y, we have

$$\sum_{\substack{a\in A\\ x<(ma)_N\le x+y}} 1 = \sum_{j=1}^{y}\sum_{a\in A}\frac{1}{N}\sum_{r\in(\frac{-N}{2},\frac{N}{2}]} e(\frac{r(ma-x-j)}{N})$$

$$= \frac{1}{N}\sum_{r\in(\frac{-N}{2},\frac{N}{2}]} e(-\frac{rx}{N})\sum_{a\in A} e(\frac{rma}{N})\sum_{j=1}^{y} e(-\frac{rj}{N})$$

$$= \frac{y}{N}|A| + \frac{1}{N}\sum_{r\neq 0} e(-\frac{rx}{N})\widehat{A}(rm)\sum_{j=1}^{y} e(-\frac{rj}{N}).$$

Proof of Theorem 3: proof of (2)

For integers x and y, we have

$$\sum_{\substack{a\in A\\ x<(ma)_N\le x+y}} 1 = \sum_{j=1}^{y}\sum_{a\in A}\frac{1}{N}\sum_{r\in(\frac{-N}{2},\frac{N}{2}]} e(\frac{r(ma-x-j)}{N})$$

$$= \frac{1}{N}\sum_{r\in(\frac{-N}{2},\frac{N}{2}]} e(-\frac{rx}{N})\sum_{a\in A} e(\frac{rma}{N})\sum_{j=1}^{y} e(-\frac{rj}{N})$$

$$= \frac{y}{N}|A| + \frac{1}{N}\sum_{r\neq 0} e(-\frac{rx}{N})\widehat{A}(rm)\sum_{j=1}^{y} e(-\frac{rj}{N}).$$

Proof of Theorem 3: proof of (2)

Since

$$\Big|\sum_{j=1}^{y} e(-\frac{rj}{N})\Big| = \Big|\frac{1-e(-\frac{ry}{N})}{1-e(-\frac{r}{N})}\Big|$$

$$\le \frac{2}{|1-e(-\frac{r}{N})|} \ll \frac{1}{\|\frac{r}{N}\|} = \frac{N}{|r|},$$

and when $m \not\equiv 0 \pmod N$, $\forall M \in \mathbb{Z}$,

$$\sum_{r=M}^{M+N} |\widehat{A}(rm)|^2 = \sum_{r=M}^{M+N} \sum_{a\in A} e(\frac{rma}{N}) \sum_{b\in A} e(-\frac{rmb}{N})$$

$$= \sum_{a,b\in A} \sum_{r=M}^{M+N} e(\frac{rm(a-b)}{N})$$

$$= N|A|,$$

Proof of Theorem 3: proof of (2)

Since

$$\Big|\sum_{j=1}^{y} e(-\frac{rj}{N})\Big| = \Big|\frac{1-e(-\frac{ry}{N})}{1-e(-\frac{r}{N})}\Big|$$

$$\le \frac{2}{\left|1-e(-\frac{r}{N})\right|} \ll \frac{1}{\|\frac{r}{N}\|} = \frac{N}{|r|},$$

and when $m \not\equiv 0 \pmod N$, $\forall M \in \mathbb{Z}$,

$$\sum_{r=M}^{M+N} |\widehat{A}(rm)|^2 = \sum_{r=M}^{M+N} \sum_{a\in A} e(\frac{rma}{N}) \sum_{b\in A} e(-\frac{rmb}{N})$$

$$= \sum_{a,b\in A} \sum_{r=M}^{M+N} e(\frac{rm(a-b)}{N})$$

$$= N|A|,$$

Proof of Theorem 3: proof of (2)

Since

$$\Big|\sum_{j=1}^{y} e(-\frac{rj}{N})\Big| = \Big|\frac{1-e(-\frac{ry}{N})}{1-e(-\frac{r}{N})}\Big|$$

$$\leq \frac{2}{\big|1-e(-\frac{r}{N})\big|} \ll \frac{1}{\|\ \frac{r}{N}\ \|} = \frac{N}{|r|},$$

and when $m \not\equiv 0 \pmod N$, $\forall M \in \mathbb{Z}$,

$$\begin{aligned}\sum_{r=M}^{M+N} |\widehat{A}(rm)|^2 &= \sum_{r=M}^{M+N} \sum_{a\in A} e(\frac{rma}{N}) \sum_{b\in A} e(-\frac{rmb}{N}) \\ &= \sum_{a,b\in A} \sum_{r=M}^{M+N} e(\frac{rm(a-b)}{N}) \\ &= N|A|,\end{aligned}$$

Proof of Theorem 3: proof of (2)

Since

$$\Big|\sum_{j=1}^{y} e(-\frac{rj}{N})\Big| = \Big|\frac{1-e(-\frac{ry}{N})}{1-e(-\frac{r}{N})}\Big|$$

$$\le \frac{2}{\big|1-e(-\frac{r}{N})\big|} \ll \frac{1}{\parallel \frac{r}{N} \parallel} = \frac{N}{|r|},$$

and when $m \not\equiv 0 \pmod N$, $\forall M \in \mathbb{Z}$,

$$\sum_{r=M}^{M+N} |\widehat{A}(rm)|^2 = \sum_{r=M}^{M+N} \sum_{a\in A} e(\frac{rma}{N}) \sum_{b\in A} e(-\frac{rmb}{N})$$

$$= \sum_{a,b\in A} \sum_{r=M}^{M+N} e(\frac{rm(a-b)}{N})$$

$$= N|A|,$$

Proof of Theorem 3: proof of (2)

Since

$$\Big|\sum_{j=1}^{y} e(-\frac{rj}{N})\Big| = \Big|\frac{1-e(-\frac{ry}{N})}{1-e(-\frac{r}{N})}\Big|$$

$$\leq \frac{2}{\left|1-e(-\frac{r}{N})\right|} \ll \frac{1}{\| \frac{r}{N} \|} = \frac{N}{|r|},$$

and when $m \not\equiv 0 \pmod N$, $\forall M \in \mathbb{Z}$,

$$\begin{aligned}\sum_{r=M}^{M+N} |\widehat{A}(rm)|^2 &= \sum_{r=M}^{M+N} \sum_{a\in A} e(\frac{rma}{N}) \sum_{b\in A} e(-\frac{rmb}{N}) \\ &= \sum_{a,b\in A} \sum_{r=M}^{M+N} e(\frac{rm(a-b)}{N}) \\ &= N|A|,\end{aligned}$$

Proof of Theorem 3: proof of (2)

we have

$$\frac{1}{N}\sum_{r\neq 0} e(-\frac{rx}{N})\widehat{A}(rm)\sum_{j=1}^{y} e(-\frac{rj}{N}) \ll \sum_{r\neq 0}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\leq \sum_{0<|r|\leq R}\frac{|\widehat{A}(rm)|}{|r|} + \sum_{R<|r|\leq \frac{N}{2}}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\ll (\log R)\max_{s\neq 0}|\widehat{A}(s)| + \Big(\sum_{r\in(-\frac{N}{2},\frac{N}{2}]}|\widehat{A}(rm)|^2\Big)^{\frac{1}{2}}\Big(\sum_{R<|r|}\frac{1}{r^2}\Big)^{\frac{1}{2}}$$

$$\ll (\log R)\delta^2|A| + (\frac{|A|N}{R})^{\frac{1}{2}} \ll \delta|A|,$$

for $R \approx \frac{N}{\delta^2|A|}$.

Proof of Theorem 3: proof of (2)

we have

$$\frac{1}{N}\sum_{r\neq 0} e(-\frac{rx}{N})\widehat{A}(rm)\sum_{j=1}^{y} e(-\frac{rj}{N}) \ll \sum_{r\neq 0}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\leq \sum_{0<|r|\leq R}\frac{|\widehat{A}(rm)|}{|r|} + \sum_{R<|r|\leq \frac{N}{2}}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\ll (\log R)\max_{s\neq 0}|\widehat{A}(s)| + \Big(\sum_{r\in(-\frac{N}{2},\frac{N}{2}]}|\widehat{A}(rm)|^2\Big)^{\frac{1}{2}}\Big(\sum_{R<|r|}\frac{1}{r^2}\Big)^{\frac{1}{2}}$$

$$\ll (\log R)\delta^2|A| + (\frac{|A|N}{R})^{\frac{1}{2}} \ll \delta|A|,$$

for $R \approx \frac{N}{\delta^2|A|}$.

Proof of Theorem 3: proof of (2)

we have

$$\frac{1}{N}\sum_{r\neq 0} e(-\frac{rx}{N})\widehat{A}(rm)\sum_{j=1}^{y} e(-\frac{rj}{N}) \ll \sum_{r\neq 0}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\leq \sum_{0<|r|\leq R}\frac{|\widehat{A}(rm)|}{|r|} + \sum_{R<|r|\leq \frac{N}{2}}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\ll (\log R)\max_{s\neq 0}|\widehat{A}(s)| + \Big(\sum_{r\in(-\frac{N}{2},\frac{N}{2}]}|\widehat{A}(rm)|^2\Big)^{\frac{1}{2}}\Big(\sum_{R<|r|}\frac{1}{r^2}\Big)^{\frac{1}{2}}$$

$$\ll (\log R)\delta^2|A| + (\frac{|A|N}{R})^{\frac{1}{2}} \ll \delta|A|,$$

for $R \approx \frac{N}{\delta^2|A|}$.

Proof of Theorem 3: proof of (2)

we have

$$\frac{1}{N}\sum_{r\neq 0} e(-\frac{rx}{N})\widehat{A}(rm)\sum_{j=1}^{y} e(-\frac{rj}{N}) \ll \sum_{r\neq 0}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\leq \sum_{0<|r|\leq R}\frac{|\widehat{A}(rm)|}{|r|} + \sum_{R<|r|\leq \frac{N}{2}}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\ll (\log R)\max_{s\neq 0}|\widehat{A}(s)| + \Big(\sum_{r\in(-\frac{N}{2},\frac{N}{2}]}|\widehat{A}(rm)|^2\Big)^{\frac{1}{2}}\Big(\sum_{R<|r|}\frac{1}{r^2}\Big)^{\frac{1}{2}}$$

$$\ll (\log R)\delta^2|A| + (\frac{|A|N}{R})^{\frac{1}{2}} \ll \delta|A|,$$

for $R \approx \frac{N}{\delta^2|A|}$.

we have

$$\frac{1}{N}\sum_{r\neq 0} e(-\frac{rx}{N})\widehat{A}(rm)\sum_{j=1}^{y} e(-\frac{rj}{N}) \ll \sum_{r\neq 0}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\leq \sum_{0<|r|\leq R}\frac{|\widehat{A}(rm)|}{|r|} + \sum_{R<|r|\leq \frac{N}{2}}\frac{|\widehat{A}(rm)|}{|r|}$$

$$\ll (\log R)\max_{s\neq 0}|\widehat{A}(s)| + \Big(\sum_{r\in(-\frac{N}{2},\frac{N}{2}]}|\widehat{A}(rm)|^2\Big)^{\frac{1}{2}}\Big(\sum_{R<|r|}\frac{1}{r^2}\Big)^{\frac{1}{2}}$$

$$\ll (\log R)\delta^2|A| + (\frac{|A|N}{R})^{\frac{1}{2}} \ll \delta|A|,$$

for $R \approx \frac{N}{\delta^2|A|}$.

Remark 1

If we do not divide the sum

$$\sum_{r\neq 0} \frac{|\widehat{A}(rm)|}{|r|}$$

into two parts, then we can only get the result for $\delta \ll \frac{1}{\log N}$.

Analogy to Weyl's criterion

To obtain an analogy to Weyl's criterion, we think of an infinite sequence of pairs (A, N) with $N \to \infty$, where $|A| \gg N$. Then we have

Corollary 1

As $N \to \infty$ with $|A| \gg N$, we have that

$$Error(A) = o(1)$$

if and only if

$$\widehat{A}(m) = o(N)$$

for all $m \not\equiv 0 \,(mod\, N)$.

Analogy to Weyl's criterion

To obtain an analogy to Weyl's criterion, we think of an infinite sequence of pairs (A, N) with $N \to \infty$, where $|A| \gg N$. Then we have

Corollary 1

As $N \to \infty$ with $|A| \gg N$, we have that

$$Error(A) = o(1)$$

if and only if

$$\widehat{A}(m) = o(N)$$

for all $m \not\equiv 0\,(mod\, N)$.

Analogy to Weyl's criterion

One can therefore formulate an analogy to Weyl's criterion along the lines: the Fourier transforms of A are all small if and only if A and all of its dilates are uniformly distributed. (A dilate of A is the set $\{ma : a \in A\}$ for some $m \not\equiv 0 \pmod N$)

This idea is central to our recent understanding, in additive combinatorics, for proving that large sets contain 3-term arithmetic progressions (3-AP); and finding appropriate analogies to this is essential to our understanding when considering k-AP for $k \geq 3$.

Analogy to Weyl's criterion

One can therefore formulate an analogy to Weyl's criterion along the lines: the Fourier transforms of A are all small if and only if A and all of its dilates are uniformly distributed. (A dilate of A is the set $\{ma : a \in A\}$ for some $m \not\equiv 0 \pmod N$)

This idea is central to our recent understanding, in additive combinatorics, for proving that large sets contain 3-term arithmetic progressions (3-AP); and finding appropriate analogies to this is essential to our understanding when considering k-AP for $k \geq 3$.

Theorem 4

To give one example of how such a notion can be used, we ask whether a given set A of residues mod N contains a non-trivial 3-AP? In other words, we wish to find solutions to $a + b = 2c$ with a, b, $c \in A$ where $a \neq b$.

Theorem 4

If A is a subset of the residues mod N where N is odd, for which

$$|\widehat{A}(m)| < \frac{|A|^2}{N} - 1$$

whenever $m \not\equiv 0 \, (mod\, N)$, then A contains non-trivial 3-AP.

Theorem 4

To give one example of how such a notion can be used, we ask whether a given set A of residues mod N contains a non-trivial 3-AP? In other words, we wish to find solutions to $a + b = 2c$ with a, b, $c \in A$ where $a \neq b$.

Theorem 4

If A is a subset of the residues mod N where N is odd, for which

$$|\widehat{A}(m)| < \frac{|A|^2}{N} - 1$$

whenever $m \not\equiv 0 \, (mod \, N)$, then A contains non-trivial 3-AP.

The number of 3-AP in A is

$$\sum_{a,b,c\in A}\frac{1}{N}\sum_{r=0}^{N-1}e\left(\frac{r(a+b-2c)}{N}\right)=\frac{1}{N}\sum_{r=0}^{N-1}\widehat{A}(r)^2\widehat{A}(-2r).$$

The $r=0$ term gives $\frac{|A|^3}{N}$.

The number of 3-AP in A is

$$\sum_{a,b,c\in A}\frac{1}{N}\sum_{r=0}^{N-1}e(\frac{r(a+b-2c)}{N})=\frac{1}{N}\sum_{r=0}^{N-1}\widehat{A}(r)^2\widehat{A}(-2r).$$

The $r=0$ term gives $\frac{|A|^3}{N}$.

Proof of Theorem 4

The number of 3-AP in A is

$$\sum_{a,b,c\in A} \frac{1}{N}\sum_{r=0}^{N-1} e\left(\frac{r(a+b-2c)}{N}\right) = \frac{1}{N}\sum_{r=0}^{N-1} \widehat{A}(r)^2\widehat{A}(-2r).$$

The $r=0$ term gives $\frac{|A|^3}{N}$.

We regard the remaining terms as error terms, and bound them by their absolute values, giving a contribution (taking $m \equiv -2r \pmod{N}$)

$$\leq \frac{1}{N}\sum_{r=0}^{N-1} |\widehat{A}(r)|^2 \cdot \max_{m\neq 0} |\widehat{A}(m)| = |A| \max_{m\neq 0} |\widehat{A}(m)|.$$

There are $|A|$ trivial 3-AP, so we have established that A has non-trivial 3-AP when

$$\frac{|A|^3}{N} - |A| \max_{m\neq 0} |\widehat{A}(m)| > |A|.$$

Proof of Theorem 4

We regard the remaining terms as error terms, and bound them by their absolute values, giving a contribution (taking $m \equiv -2r \pmod N$)

$$\le \frac{1}{N}\sum_{r=0}^{N-1} |\widehat{A}(r)|^2 \cdot \max_{m\neq 0} |\widehat{A}(m)| = |A| \max_{m\neq 0} |\widehat{A}(m)|.$$

There are $|A|$ trivial 3-AP, so we have established that A has non-trivial 3-AP when

$$\frac{|A|^3}{N} - |A| \max_{m\neq 0} |\widehat{A}(m)| > |A|.$$

Generalization of Theorem 4

Rather more generally we can ask for solution to

$$ia + jb + kc \equiv l \pmod N, \tag{3}$$

where $(ijk,\, N) = 1$ with $a \in A$, $b \in B$, $c \in C$ and A, B, $C \subseteq \mathbb{Z}/N\mathbb{Z}$.

We count the above set as

$$\sum_{\substack{a\in A,\, b\in B\\ c\in C}} \frac{1}{N} \sum_{r=0}^{N-1} e\Big(\frac{r(ia+jb+kc-l)}{N}\Big)$$

$$= \frac{1}{N} \sum_{r=0}^{N-1} e\Big(\frac{-rl}{N}\Big) \widehat{A}(ir)\widehat{B}(jr)\widehat{C}(kr).$$

Generalization of Theorem 4

Rather more generally we can ask for solution to

$$ia + jb + kc \equiv l \pmod N, \tag{3}$$

where $(ijk,\, N) = 1$ with $a \in A$, $b \in B$, $c \in C$ and A, B, $C \subseteq \mathbb{Z}/N\mathbb{Z}$.

We count the above set as

$$\sum_{\substack{a \in A,\, b \in B \\ c \in C}} \frac{1}{N} \sum_{r=0}^{N-1} e\Big(\frac{r(ia + jb + kc - l)}{N}\Big)$$

$$= \frac{1}{N} \sum_{r=0}^{N-1} e\Big(\frac{-rl}{N}\Big) \widehat{A}(ir) \widehat{B}(jr) \widehat{C}(kr).$$

Generalization of Theorem 4

Rather more generally we can ask for solution to

$$ia + jb + kc \equiv l \pmod N, \tag{3}$$

where $(ijk,\, N) = 1$ with $a \in A$, $b \in B$, $c \in C$ and A, B, $C \subseteq \mathbb{Z}/N\mathbb{Z}$.

We count the above set as

$$\sum_{\substack{a\in A,\, b\in B\\ c\in C}} \frac{1}{N} \sum_{r=0}^{N-1} e\Big(\frac{r(ia + jb + kc - l)}{N}\Big)$$

$$= \frac{1}{N} \sum_{r=0}^{N-1} e\Big(\frac{-rl}{N}\Big) \widehat{A}(ir)\widehat{B}(jr)\widehat{C}(kr).$$

Generalization of Theorem 4

The $r = 0$ term contributes

$$\frac{1}{N}\widehat{A}(0)\widehat{B}(0)\widehat{C}(0) = \frac{|A||B||C|}{N}.$$

The total contribution of the other terms can be bounded above by

$$\begin{aligned}
&\frac{1}{N}\sum_{r\neq 0}|\widehat{A}(ir)||\widehat{B}(jr)||\widehat{C}(kr)| \\
\le\ &\frac{1}{N}\max_{m\neq 0}|\widehat{A}(m)|\sum_{r=0}^{N}|\widehat{B}(jr)||\widehat{C}(kr)| \\
\le\ &\frac{1}{N}\max_{m\neq 0}|\widehat{A}(m)|\Big(\sum_{t=0}^{N}|\widehat{B}(t)|^2\Big)^{\frac{1}{2}}\Big(\sum_{u=0}^{N}|\widehat{C}(u)|^2\Big)^{\frac{1}{2}}
\end{aligned}$$

Generalization of Theorem 4

The $r = 0$ term contributes

$$\frac{1}{N}\widehat{A}(0)\widehat{B}(0)\widehat{C}(0) = \frac{|A||B||C|}{N}.$$

The total contribution of the other terms can be bounded above by

$$\frac{1}{N}\sum_{r\neq 0}|\widehat{A}(ir)||\widehat{B}(jr)||\widehat{C}(kr)|$$

$$\leq \frac{1}{N}\max_{m\neq 0}|\widehat{A}(m)|\sum_{r=0}^{N}|\widehat{B}(jr)||\widehat{C}(kr)|$$

$$\leq \frac{1}{N}\max_{m\neq 0}|\widehat{A}(m)|\Big(\sum_{t=0}^{N}|\widehat{B}(t)|^2\Big)^{\frac{1}{2}}\Big(\sum_{u=0}^{N}|\widehat{C}(u)|^2\Big)^{\frac{1}{2}}$$

Generalization of Theorem 4

The $r = 0$ term contributes

$$\frac{1}{N}\widehat{A}(0)\widehat{B}(0)\widehat{C}(0) = \frac{|A||B||C|}{N}.$$

The total contribution of the other terms can be bounded above by

$$\frac{1}{N}\sum_{r\neq 0}|\widehat{A}(ir)||\widehat{B}(jr)||\widehat{C}(kr)|$$

$$\leq \frac{1}{N}\max_{m\neq 0}|\widehat{A}(m)|\sum_{r=0}^{N}|\widehat{B}(jr)||\widehat{C}(kr)|$$

$$\leq \frac{1}{N}\max_{m\neq 0}|\widehat{A}(m)|\left(\sum_{t=0}^{N}|\widehat{B}(t)|^2\right)^{\frac{1}{2}}\left(\sum_{u=0}^{N}|\widehat{C}(u)|^2\right)^{\frac{1}{2}}$$

Generalization of Theorem 4

The $r = 0$ term contributes

$$\frac{1}{N}\widehat{A}(0)\widehat{B}(0)\widehat{C}(0) = \frac{|A||B||C|}{N}.$$

The total contribution of the other terms can be bounded above by

$$\begin{aligned}
&\frac{1}{N}\sum_{r\neq 0}|\widehat{A}(ir)||\widehat{B}(jr)||\widehat{C}(kr)| \\
&\leq \frac{1}{N}\max_{m\neq 0}|\widehat{A}(m)|\sum_{r=0}^{N}|\widehat{B}(jr)||\widehat{C}(kr)| \\
&\leq \frac{1}{N}\max_{m\neq 0}|\widehat{A}(m)|\left(\sum_{t=0}^{N}|\widehat{B}(t)|^2\right)^{\frac{1}{2}}\left(\sum_{u=0}^{N}|\widehat{C}(u)|^2\right)^{\frac{1}{2}}
\end{aligned}$$

$$= \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)|(N|B| \cdot N|C|)^{\frac{1}{2}}$$

$$= (|B||C|)^{\frac{1}{2}} \max_{m \neq 0} |\widehat{A}(m)|,$$

using the Cauchy-Schwarz inequality.

Therefore there are $\geq \frac{|A||B||C|}{2N}$ solutions to (3) provided

$$|\widehat{A}(m)| \leq \frac{(|B||C|)^{\frac{1}{2}}}{2N} |A|, \quad (4)$$

for every $m \not\equiv 0 \pmod{N}$.

Generalization of Theorem 4

$$= \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| (N|B| \cdot N|C|)^{\frac{1}{2}}$$
$$= (|B||C|)^{\frac{1}{2}} \max_{m \neq 0} |\widehat{A}(m)|,$$

using the Cauchy-Schwarz inequality.

Therefore there are $\geq \frac{|A||B||C|}{2N}$ solutions to (3) provided

$$|\widehat{A}(m)| \leq \frac{(|B||C|)^{\frac{1}{2}}}{2N} |A|, \tag{4}$$

for every $m \not\equiv 0 \pmod{N}$.

Generalization of Theorem 4

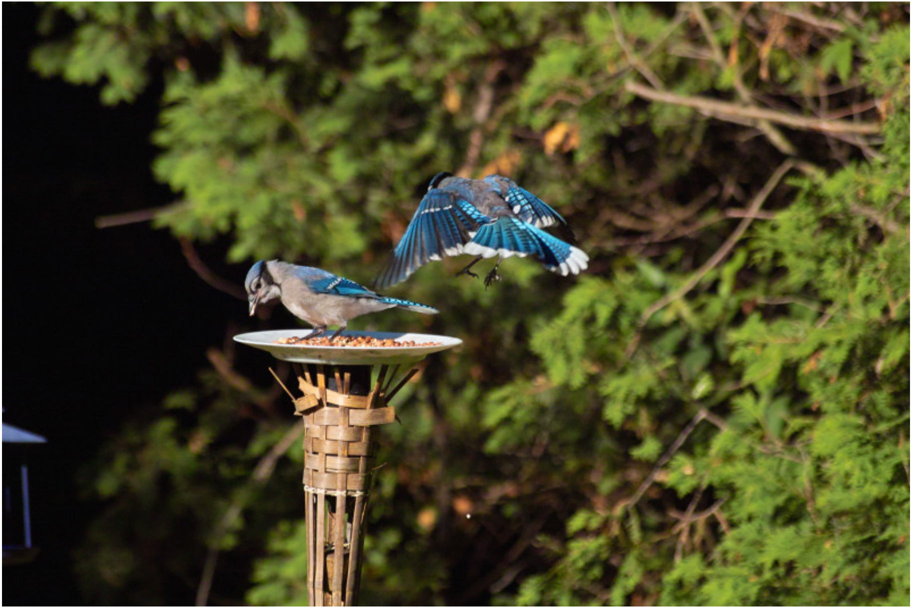
$$= \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| (N|B| \cdot N|C|)^{\frac{1}{2}}$$
$$= (|B||C|)^{\frac{1}{2}} \max_{m \neq 0} |\widehat{A}(m)|,$$

using the Cauchy-Schwarz inequality.

Therefore there are $\geq \frac{|A||B||C|}{2N}$ solutions to (3) provided

$$|\widehat{A}(m)| \leq \frac{(|B||C|)^{\frac{1}{2}}}{2N} |A|, \tag{4}$$

for every $m \not\equiv 0 \,(\mathrm{mod}\, N)$.



In 1953, Roth proved

Theorem 5 (Roth)

For any $\delta > 0$, if N is sufficiently large, then any subset A of $\{1, \ldots, N\}$ with more than δN elements contains a non-trivial 3-AP.

Proof of Roth's Theorem

To start our proof, we note that the result is easy for $\delta > \frac{2}{3}$ since then A must contain a subset of the form $\{a, a+1, a+2\}$.

For smaller δ, we shall prove that the theorem is true for δ, if it is true for $\delta(1+c\delta)$ for some $c > 0$. Then we can prove the theorem by induction.

Replace N by the smallest prime $\geq N$ which can be done with negligible change in our supposition.

Proof of Roth's Theorem

To start our proof, we note that the result is easy for $\delta > \frac{2}{3}$ since then A must contain a subset of the form $\{a,\, a+1,\, a+2\}$.

For smaller δ, we shall prove that the theorem is true for δ, if it is true for $\delta(1+c\delta)$ for some $c > 0$. Then we can prove the theorem by induction.

Replace N by the smallest prime $\geq N$ which can be done with negligible change in our supposition.

Proof of Roth's Theorem

To start our proof, we note that the result is easy for $\delta > \frac{2}{3}$ since then A must contain a subset of the form $\{a, a+1, a+2\}$.

For smaller δ, we shall prove that the theorem is true for δ, if it is true for $\delta(1 + c\delta)$ for some $c > 0$. Then we can prove the theorem by induction.

Replace N by the smallest prime $\geq N$ which can be done with negligible change in our supposition.

Proof of Roth's Theorem

If

$$\#\left\{a \in A : \ 0 < a < \frac{N}{3}\right\} \geq (1 + c\delta)\,\frac{|A|}{3}$$

or

$$\#\left\{a \in A : \ \frac{2N}{3} < a < N\right\} \geq (1 + c\delta)\,\frac{|A|}{3},$$

let

$$A_1 = \left\{a \in A : \ 0 < a < \frac{N}{3}\right\},$$
$$A_2 = \left\{a \in A : \ \frac{2N}{3} < a < N\right\}$$

and $N_1 = [\frac{N}{3}]$.

Proof of Roth's Theorem

If

$$\#\left\{a \in A:\ 0 < a < \frac{N}{3}\right\} \geq (1 + c\delta)\,\frac{|A|}{3}$$

or

$$\#\left\{a \in A:\ \frac{2N}{3} < a < N\right\} \geq (1 + c\delta)\,\frac{|A|}{3},$$

let

$$A_1 = \left\{a \in A:\ 0 < a < \frac{N}{3}\right\},$$
$$A_2 = \left\{a \in A:\ \frac{2N}{3} < a < N\right\}$$

and $N_1 = [\frac{N}{3}]$.

Proof of Roth's Theorem

Then

$$|A_i| \geq \delta(1 + c\delta)|N_1|,$$

so A_i has a non-trivial 3-AP and A has one, here $i = 1, 2$.

Otherwise, let

$$B = \left\{ a \in A : \frac{N}{3} < a < \frac{2N}{3} \right\},$$

so that

$$|B| > (1 - 2c\delta)\frac{|A|}{3}.$$

Proof of Roth's Theorem

Then

$$|A_i| \geq \delta(1 + c\delta)|N_1|,$$

so A_i has a non-trivial 3-AP and A has one, here $i = 1, 2$.

Otherwise, let

$$B = \left\{ a \in A : \frac{N}{3} < a < \frac{2N}{3} \right\},$$

so that

$$|B| > (1 - 2c\delta)\frac{|A|}{3}.$$

Proof of Roth's Theorem

Then

$$|A_i| \geq \delta(1 + c\delta)|N_1|,$$

so A_i has a non-trivial 3-AP and A has one, here $i = 1, 2$.

Otherwise, let

$$B = \left\{ a \in A : \ \frac{N}{3} < a < \frac{2N}{3} \right\},$$

so that

$$|B| > (1 - 2c\delta)\,\frac{|A|}{3}.$$

Then

$$|A_i| \geq \delta(1 + c\delta)|N_1|,$$

so A_i has a non-trivial 3-AP and A has one, here $i = 1,\ 2$.

Otherwise, let

$$B = \left\{ a \in A : \ \frac{N}{3} < a < \frac{2N}{3} \right\},$$

so that

$$|B| > (1 - 2c\delta)\,\frac{|A|}{3}.$$

Proof of Roth's Theorem

Suppose that A has no non-trivial 3-AP.

We are interested in solutions to $a + b \equiv 2c \pmod{N}$ with $a \in A$ and $b, c \in B$, which is the equation (3) with $i = j = 1$, $k = -2$, $l = 0$.

Note that if $b, c \in B$, then $0 < 2c - b < N$ and so $a + b = 2c$. We must have $a = b = c$. Now we know that every solution of (3) is a solution of equation $a + b = 2c$ so that it is an authentic 3-AP.

Proof of Roth's Theorem

Suppose that A has no non-trivial 3-AP.

We are interested in solutions to $a+b\equiv 2c \pmod N$ with $a\in A$ and $b,\, c\in B$, which is the equation (3) with $i=j=1$, $k=-2$, $l=0$.

Note that if $b,\, c\in B$, then $0<2c-b<N$ and so $a+b=2c$. We must have $a=b=c$. Now we know that every solution of (3) is a solution of equation $a+b=2c$ so that it is an authentic 3-AP.

Proof of Roth's Theorem

Suppose that A has no non-trivial 3-AP.

We are interested in solutions to $a + b \equiv 2c \pmod{N}$ with $a \in A$ and $b,\, c \in B$, which is the equation (3) with $i = j = 1$, $k = -2$, $l = 0$.

Note that if $b,\, c \in B$, then $0 < 2c - b < N$ and so $a + b = 2c$. We must have $a = b = c$. Now we know that every solution of (3) is a solution of equation $a + b = 2c$ so that it is an authentic 3-AP.

Proof of Roth's Theorem

Therefore there exists $m \not\equiv 0 \pmod N$ such that

$$|\widehat{A}(m)| > \delta(1 - 2c\delta)\,\frac{|A|}{6},$$

else we have a non-trivial solution to (3) by (4).

Now A is not uniformly distributed mod N. In particular, we have Error(A)$\gg \delta^2$ by Theorem 3.

In other words, there is some dilate of A and some long interval which does not contain the expected number of elements of the dilate of A. In fact it is out by a constant factor.

Proof of Roth's Theorem

Therefore there exists $m \not\equiv 0 \pmod N$ such that

$$|\widehat{A}(m)| > \delta(1 - 2c\delta)\,\frac{|A|}{6},$$

else we have a non-trivial solution to (3) by (4).

Now A is not uniformly distributed mod N. In particular, we have Error(A)$\gg \delta^2$ by Theorem 3.

In other words, there is some dilate of A and some long interval which does not contain the expected number of elements of the dilate of A. In fact it is out by a constant factor.

Therefore there exists $m \not\equiv 0 \pmod{N}$ such that

$$|\widehat{A}(m)| > \delta(1 - 2c\delta)\,\frac{|A|}{6},$$

else we have a non-trivial solution to (3) by (4).

Now A is not uniformly distributed mod N. In particular, we have Error(A)$\gg \delta^2$ by Theorem 3.

In other words, there is some dilate of A and some long interval which does not contain the expected number of elements of the dilate of A. In fact it is out by a constant factor.

Proof of Roth's Theorem

Select integer $l \gg \frac{1}{\delta}$, and define

$$A_j = \#\left\{a \in A: \ (ma)_N \in (\frac{jN}{l}, \frac{(j+1)N}{l}]\right\},$$

for $0 \le j \le l-1$.

If a is counted by A_j, then

$$e(\frac{ma}{N}) = e(\frac{j}{l}) + O(\frac{1}{l}).$$

Select integer $l \gg \frac{1}{\delta}$, and define

$$A_j = \#\left\{a \in A : \ (ma)_N \in (\frac{jN}{l}, \frac{(j+1)N}{l}]\right\},$$

for $0 \leq j \leq l-1$.

If a is counted by A_j, then

$$e(\frac{ma}{N}) = e(\frac{j}{l}) + O(\frac{1}{l}).$$

Proof of Roth's Theorem

Therefore by the similar method in the proof of Theorem 3, we have

$$\widehat{A}(m) = \sum_{j=0}^{l-1} A_j e(\frac{j}{l}) + O(\frac{|A|}{l})$$

$$= \sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l}) + O(\frac{|A|}{l}),$$

implying that

$$\sum_{j=0}^{l-1} |A_j - \frac{|A|}{l}| \geq \Big| \sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l}) \Big|$$

$$\geq |\widehat{A}(m)| - O(\frac{|A|}{l}) \gg \delta |A|.$$

Proof of Roth's Theorem

Therefore by the similar method in the proof of Theorem 3, we have

$$\begin{aligned}\widehat{A}(m) &= \sum_{j=0}^{l-1} A_j e(\frac{j}{l}) + O(\frac{|A|}{l}) \\ &= \sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l}) + O(\frac{|A|}{l}),\end{aligned}$$

implying that

$$\sum_{j=0}^{l-1} |A_j - \frac{|A|}{l}| \geq \Big|\sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l})\Big|$$

$$\geq |\widehat{A}(m)| - O(\frac{|A|}{l}) \gg \delta |A|.$$

Proof of Roth's Theorem

Therefore by the similar method in the proof of Theorem 3, we have

$$\begin{aligned}\widehat{A}(m) &= \sum_{j=0}^{l-1} A_j e(\frac{j}{l}) + O(\frac{|A|}{l}) \\ &= \sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l}) + O(\frac{|A|}{l}),\end{aligned}$$

implying that

$$\sum_{j=0}^{l-1} |A_j - \frac{|A|}{l}| \geq \Big| \sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l}) \Big|$$

$$\geq |\widehat{A}(m)| - O(\frac{|A|}{l}) \gg \delta|A|.$$

Proof of Roth's Theorem

Therefore by the similar method in the proof of Theorem 3, we have

$$\widehat{A}(m) = \sum_{j=0}^{l-1} A_j e(\frac{j}{l}) + O(\frac{|A|}{l})$$

$$= \sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l}) + O(\frac{|A|}{l}),$$

implying that

$$\sum_{j=0}^{l-1} \left|A_j - \frac{|A|}{l}\right| \geq \left|\sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l})\right|$$

$$\geq |\widehat{A}(m)| - O(\frac{|A|}{l}) \gg \delta|A|.$$

Proof of Roth's Theorem

Therefore by the similar method in the proof of Theorem 3, we have

$$\begin{aligned}\widehat{A}(m) &= \sum_{j=0}^{l-1} A_j e(\frac{j}{l}) + O(\frac{|A|}{l}) \\ &= \sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l}) + O(\frac{|A|}{l}),\end{aligned}$$

implying that

$$\begin{aligned}&\sum_{j=0}^{l-1} |A_j - \frac{|A|}{l}| \geq \Big| \sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) e(\frac{j}{l}) \Big| \\ &\geq |\widehat{A}(m)| - O(\frac{|A|}{l}) \gg \delta |A|.\end{aligned}$$

Adding this to

$$\sum_{j=0}^{l-1}(A_j - \frac{|A|}{l}) = 0,$$

we find that there exists j_0 for which

$$(A_{j_0} - \frac{|A|}{l}) \gg \delta \frac{|A|}{l}.$$

Proof of Roth's Theorem

Adding this to

$$\sum_{j=0}^{l-1} (A_j - \frac{|A|}{l}) = 0,$$

we find that there exists j_0 for which

$$(A_{j_0} - \frac{|A|}{l}) \gg \delta \frac{|A|}{l}.$$

We now define

$$A' = \left\{ i : \ [\frac{j_0 N}{l}] + i = (ma)_N \text{ for some } a \in A \text{ and } 1 \le i \le [\frac{N}{l}] \right\},$$

a subset of $\{1, 2, \ldots, N'\}$ where $N' = [\frac{N}{l}]$, with

$$|A'| \ge \delta(1 + c\delta)N'$$

and then assert that A' contains a non-trivial 3-AP.

Proof of Roth's Theorem

We now define

$$A' = \left\{ i : \ [\frac{j_0 N}{l}] + i = (ma)_N \text{ for some } a \in A \text{ and } 1 \leq i \leq [\frac{N}{l}] \right\},$$

a subset of $\{1, 2, \ldots, N'\}$ where $N' = [\frac{N}{l}]$, with

$$|A'| \geq \delta(1 + c\delta)N'$$

and then assert that A' contains a non-trivial 3-AP.

Proof of Roth's Theorem

We now define

$$A' = \left\{ i : \ [\frac{j_0 N}{l}] + i = (ma)_N \text{ for some } a \in A \text{ and } 1 \leq i \leq [\frac{N}{l}] \right\},$$

a subset of $\{1, 2, \ldots, N'\}$ where $N' = [\frac{N}{l}]$, with

$$|A'| \geq \delta(1 + c\delta)N'$$

and then assert that A' contains a non-trivial 3-AP.

Proof of Roth's Theorem

We proceed by noting that if u, v, $w \in A'$ for which $u + w = 2v$, then there exists a, b, $c \in A$ such that

$$ma \equiv [\frac{j_0 N}{l}] + u \pmod N,$$
$$mb \equiv [\frac{j_0 N}{l}] + w \pmod N,$$
$$mc \equiv [\frac{j_0 N}{l}] + v \pmod N.$$

Therefore

$$m(a + b - 2c) \equiv u + w - 2v \equiv 0 \pmod N,$$

and

$$a + b \equiv 2c \pmod N.$$

Proof of Roth's Theorem

We proceed by noting that if u, v, $w \in A'$ for which $u + w = 2v$, then there exists a, b, $c \in A$ such that

$$ma \equiv [\frac{j_0 N}{l}] + u \pmod{N},$$
$$mb \equiv [\frac{j_0 N}{l}] + w \pmod{N},$$
$$mc \equiv [\frac{j_0 N}{l}] + v \pmod{N}.$$

Therefore

$$m(a + b - 2c) \equiv u + w - 2v \equiv 0 \pmod{N},$$

and

$$a + b \equiv 2c \pmod{N}.$$

Proof of Roth's Theorem

We proceed by noting that if u, v, $w \in A'$ for which $u + w = 2v$, then there exists a, b, $c \in A$ such that

$$ma \equiv [\frac{j_0 N}{l}] + u \pmod{N},$$
$$mb \equiv [\frac{j_0 N}{l}] + w \pmod{N},$$
$$mc \equiv [\frac{j_0 N}{l}] + v \pmod{N}.$$

Therefore

$$m(a + b - 2c) \equiv u + w - 2v \equiv 0 \pmod{N},$$

and

$$a + b \equiv 2c \pmod{N}.$$

Proof of Roth's Theorem

However there is no guarantee that this implies $a + b = 2c$, as there may be "wraparound" which means $a + b$ might equal $2c \pm N$ or $2c \pm 2N$ or $\cdots$. Therefore we need to refine our construction to be able to deduce this final step.

The trick is to use the well-known result that if $RS = N$ with $R, S > 1$, then there exist $0 < r < R$, $0 < s < S$ such that $\pm m \equiv \frac{s}{r} \pmod{N}$.

This result comes from the fact that there are more than N integers of the form $j + im$, $0 \le i < R$, $0 \le j < S$ so that two of them must be congruent $\bmod N$, thus their difference $s \pm rm \equiv 0 \pmod{N}$.

Proof of Roth's Theorem

However there is no guarantee that this implies $a + b = 2c$, as there may be "wraparound" which means $a + b$ might equal $2c \pm N$ or $2c \pm 2N$ or $\cdots$. Therefore we need to refine our construction to be able to deduce this final step.

The trick is to use the well-known result that if $RS = N$ with $R, S > 1$, then there exist $0 < r < R$, $0 < s < S$ such that $\pm m \equiv \frac{s}{r} \pmod{N}$.

This result comes from the fact that there are more than N integers of the form $j + im$, $0 \le i < R$, $0 \le j < S$ so that two of them must be congruent $\bmod N$, thus their difference $s \pm rm \equiv 0 \pmod{N}$.

Proof of Roth's Theorem

However there is no guarantee that this implies $a + b = 2c$, as there may be "wraparound" which means $a + b$ might equal $2c \pm N$ or $2c \pm 2N$ or $\cdots$. Therefore we need to refine our construction to be able to deduce this final step.

The trick is to use the well-known result that if $RS = N$ with $R, S > 1$, then there exist $0 < r < R$, $0 < s < S$ such that $\pm m \equiv \frac{s}{r} \pmod N$.

This result comes from the fact that there are more than N integers of the form $j + im$, $0 \leq i < R$, $0 \leq j < S$ so that two of them must be congruent $\bmod N$, thus their difference $s \pm rm \equiv 0 \pmod N$.

Proof of Roth's Theorem

For convenience we will assume

$$m \equiv \frac{s}{r} \pmod N,$$

where

$$R = \sqrt{\frac{N}{\delta^3}}, \qquad S = \sqrt{N\delta^3},$$

with

$$x = [\frac{j_0 N}{l}], \qquad y = [\frac{N}{l}], \qquad l \asymp \frac{1}{\delta},$$

so that

$$\#\{a \in A : \ x < (ma)_N \le x + y\} \ge (1 + c\delta)\delta y.$$

Proof of Roth's Theorem

For convenience we will assume

$$m \equiv \frac{s}{r} \pmod N,$$

where

$$R = \sqrt{\frac{N}{\delta^3}}, \qquad S = \sqrt{N\delta^3},$$

with

$$x = [\frac{j_0 N}{l}], \qquad y = [\frac{N}{l}], \qquad l \asymp \frac{1}{\delta},$$

so that

$$\# \{a \in A : \ x < (ma)_N \leq x + y\} \geq (1 + c\delta)\delta y.$$

For convenience we will assume

$$m \equiv \frac{s}{r} \pmod N,$$

where

$$R = \sqrt{\frac{N}{\delta^3}}, \qquad S = \sqrt{N\delta^3},$$

with

$$x = [\frac{j_0 N}{l}], \qquad y = [\frac{N}{l}], \qquad l \asymp \frac{1}{\delta},$$

so that

$$\#\{a \in A : \ x < (ma)_N \le x + y\} \ge (1 + c\delta)\delta y.$$

Proof of Roth's Theorem

For convenience we will assume

$$m \equiv \frac{s}{r} \pmod N,$$

where

$$R = \sqrt{\frac{N}{\delta^3}}, \qquad S = \sqrt{N\delta^3},$$

with

$$x = [\frac{j_0 N}{l}], \qquad y = [\frac{N}{l}], \qquad l \asymp \frac{1}{\delta},$$

so that

$$\#\{a \in A: \; x < (ma)_N \le x + y\} \ge (1 + c\delta)\delta y.$$

We begin by partitioning this set depending only on the value of $(ma)_N \pmod{s}$. For $1 \le i \le s$, let $\alpha_i = (\frac{x+i}{m})_N$, and then define

$$A_i = \left\{ a \in A : \ a \equiv \alpha_i + jr \pmod{N} \ \text{and} \ 0 \le j \le [\frac{y-i}{s}] \right\}.$$

Note that $ma \equiv m(\alpha_i + jr) \equiv x + (i + js)$ so that $x < (ma)_N \le x + y$ for $a \in A_i$.

Hence there exists some value of i for which

$$\# A_i \ge (1 + c\delta)\delta \, \frac{y}{s}.$$

Proof of Roth's Theorem

We begin by partitioning this set depending only on the value of $(ma)_N \pmod s$. For $1 \leq i \leq s$, let $\alpha_i = (\frac{x+i}{m})_N$, and then define

$$A_i = \left\{ a \in A : \ a \equiv \alpha_i + jr \pmod N \ \text{ and } \ 0 \leq j \leq [\frac{y-i}{s}] \right\}.$$

Note that $ma \equiv m(\alpha_i + jr) \equiv x + (i + js)$ so that $x < (ma)_N \leq x + y$ for $a \in A_i$.

Hence there exists some value of i for which

$$\#A_i \geq (1 + c\delta)\delta \, \frac{y}{s}.$$

Proof of Roth's Theorem

We begin by partitioning this set depending only on the value of $(ma)_N \pmod{s}$. For $1 \leq i \leq s$, let $\alpha_i = (\frac{x+i}{m})_N$, and then define

$$A_i = \left\{ a \in A : \; a \equiv \alpha_i + jr \pmod{N} \; \text{and} \; 0 \leq j \leq [\frac{y-i}{s}] \right\}.$$

Note that $ma \equiv m(\alpha_i + jr) \equiv x + (i + js)$ so that $x < (ma)_N \leq x + y$ for $a \in A_i$.

Hence there exists some value of i for which

$$\#A_i \geq (1 + c\delta)\delta \, \frac{y}{s}.$$

Proof of Roth's Theorem

We begin by partitioning this set depending only on the value of $(ma)_N \pmod s$. For $1 \leq i \leq s$, let $\alpha_i = (\frac{x+i}{m})_N$, and then define

$$A_i = \left\{ a \in A : \ a \equiv \alpha_i + jr \pmod N \ \text{ and } \ 0 \leq j \leq [\frac{y-i}{s}] \right\}.$$

Note that $ma \equiv m(\alpha_i + jr) \equiv x + (i + js)$ so that $x < (ma)_N \leq x + y$ for $a \in A_i$.

Hence there exists some value of i for which

$$\# A_i \geq (1 + c\delta)\delta \, \frac{y}{s}.$$

Proof of Roth's Theorem

Even within A_i we still have the possibility of the "wraparound problem", so we deal with this by partitioning A_i.

Let

$$K = [\frac{\alpha_i + \frac{ry}{s}}{N}],$$

so that $\alpha_i \leq \alpha_i + jr \leq \alpha_i + \frac{ry}{s} < (K+1)N$.

For each $0 \leq k \leq K$, define

$$A_{i,k} = \{a \in A_i : \ kN < \alpha_i + jr \leq (k+1)N\}.$$

Proof of Roth's Theorem

Even within A_i we still have the possibility of the "wraparound problem", so we deal with this by partitioning A_i.

Let

$$K = [\frac{\alpha_i + \frac{ry}{s}}{N}],$$

so that $\alpha_i \leq \alpha_i + jr \leq \alpha_i + \frac{ry}{s} < (K+1)N$.

For each $0 \leq k \leq K$, define

$$A_{i,k} = \{a \in A_i : \ kN < \alpha_i + jr \leq (k+1)N\}.$$

Proof of Roth's Theorem

Even within A_i we still have the possibility of the "wraparound problem", so we deal with this by partitioning A_i.

Let

$$K = [\frac{\alpha_i + \frac{ry}{s}}{N}],$$

so that $\alpha_i \leq \alpha_i + jr \leq \alpha_i + \frac{ry}{s} < (K+1)N$.

For each $0 \leq k \leq K$, define

$$A_{i,k} = \{a \in A_i : \ kN < \alpha_i + jr \leq (k+1)N\}.$$

Proof of Roth's Theorem

Let $\alpha_{i,0} = \alpha_i - r$, and $\alpha_{i,k}$ be the largest integer $\leq kN$ which is $\equiv \alpha_i \pmod r$ for $1 \leq k \leq K$. Then

$$A_{i,k} = \{a \in A_i : \ a \equiv \alpha_{i,k} + jr \pmod N, 1 \leq j \leq J_k + O(1)\},$$

where $J_0 = \frac{N}{r} - \frac{\alpha_i}{r}$, $J_k = \frac{N}{r}$ for $1 \leq k \leq K-1$, and $J_K = \frac{y}{s} - \frac{KN}{r} + \frac{\alpha_i}{r}$.

We let T be the set of indices k, $1 \leq k \leq K-1$ together with $k = 0$ provided $J_0 > \frac{c\delta^2 y}{4s}$, and with $k = K$ provided $J_K > \frac{c\delta^2 y}{4s}$.

Proof of Roth's Theorem

Let $\alpha_{i,0} = \alpha_i - r$, and $\alpha_{i,k}$ be the largest integer $\leq kN$ which is $\equiv \alpha_i \pmod r$ for $1 \leq k \leq K$. Then

$$A_{i,k} = \{a \in A_i : \ a \equiv \alpha_{i,k} + jr \pmod N, \ 1 \leq j \leq J_k + O(1)\},$$

where $J_0 = \frac{N}{r} - \frac{\alpha_i}{r}$, $J_k = \frac{N}{r}$ for $1 \leq k \leq K-1$, and $J_K = \frac{y}{s} - \frac{KN}{r} + \frac{\alpha_i}{r}$.

We let T be the set of indices k, $1 \leq k \leq K-1$ together with $k = 0$ provided $J_0 > \frac{c\delta^2 y}{4s}$, and with $k = K$ provided $J_K > \frac{c\delta^2 y}{4s}$.

Let $\alpha_{i,\,0} = \alpha_i - r$, and $\alpha_{i,\,k}$ be the largest integer $\le kN$ which is $\equiv \alpha_i \pmod r$ for $1 \le k \le K$. Then

$$A_{i,\,k} = \{a \in A_i :\ a \equiv \alpha_{i,k} + jr \pmod N,\ 1 \le j \le J_k + O(1)\}\,,$$

where $J_0 = \frac{N}{r} - \frac{\alpha_i}{r}$, $J_k = \frac{N}{r}$ for $1 \le k \le K-1$, and $J_K = \frac{y}{s} - \frac{KN}{r} + \frac{\alpha_i}{r}$.

We let T be the set of indices k, $1 \le k \le K-1$ together with $k=0$ provided $J_0 > \frac{c\delta^2 y}{4s}$, and with $k = K$ provided $J_K > \frac{c\delta^2 y}{4s}$.

Note that

$$\sum_{k\in T}\#A_{i,\,k} \ge \#A_i - \frac{c\delta^2 y}{2s}$$
$$\ge (1+\frac{c\delta}{2})\delta\,\frac{y}{s} \ge (1+\frac{c\delta}{2})\delta\sum_{k\in T} J_k.$$

Thus there exists $k \in T$ such that

$$\#A_{i,\,k} \ge (1+\frac{c\delta}{2})\delta J_k.$$

Note that

$$\sum_{k\in T} \#A_{i,k} \geq \#A_i - \frac{c\delta^2 y}{2s}$$

$$\geq (1+\frac{c\delta}{2})\delta\,\frac{y}{s} \geq (1+\frac{c\delta}{2})\delta\sum_{k\in T} J_k.$$

Thus there exists $k \in T$ such that

$$\#A_{i,k} \geq (1+\frac{c\delta}{2})\delta J_k.$$

Proof of Roth's Theorem

Now define $N' = [J_k]$ and

$$A' = \left\{ j : \ 1 \le j \le N', \ \alpha_{i,\,k} + jr - kN \in A \right\},$$

a subset of $\{1, 2, \ldots, N'\}$, so that

$$\#A' = \#A_{i,\,k} \ge (1 + \frac{c\delta}{2})\delta N'.$$

Note that

$$N' \ge \min\left\{ \frac{N}{r}, J_0, J_K \right\} \gg \min\left\{ \frac{N}{r}, \frac{c\delta^2 y}{4s} \right\}$$
$$\gg \min\left\{ \frac{N}{R}, \frac{\delta^2 N}{lS} \right\} \gg \sqrt{\delta^3 N}.$$

Hence A' contains a non-trivial 3-AP.

Proof of Roth's Theorem

Now define $N' = [J_k]$ and

$$A' = \left\{ j : \ 1 \le j \le N', \ \alpha_{i,k} + jr - kN \in A \right\},$$

a subset of $\{1, 2, \ldots, N'\}$, so that

$$\#A' = \#A_{i,k} \ge (1 + \frac{c\delta}{2})\delta N'.$$

Note that

$$N' \ge \min\left\{ \frac{N}{r}, J_0, J_K \right\} \gg \min\left\{ \frac{N}{r}, \frac{c\delta^2 y}{4s} \right\}$$
$$\gg \min\left\{ \frac{N}{R}, \frac{\delta^2 N}{lS} \right\} \gg \sqrt{\delta^3 N}.$$

Hence A' contains a non-trivial 3-AP.

Proof of Roth's Theorem

Now define $N' = [J_k]$ and

$$A' = \left\{ j : \ 1 \le j \le N', \ \alpha_{i,k} + jr - kN \in A \right\},$$

a subset of $\{1, 2, \ldots, N'\}$, so that

$$\#A' = \#A_{i,k} \ge (1 + \frac{c\delta}{2})\delta N'.$$

Note that

$$N' \ge \min\left\{\frac{N}{r}, \ J_0, \ J_K\right\} \gg \min\left\{\frac{N}{r}, \ \frac{c\delta^2 y}{4s}\right\}$$

$$\gg \min\left\{\frac{N}{R}, \ \frac{\delta^2 N}{lS}\right\} \gg \sqrt{\delta^3 N}.$$

Hence A' contains a non-trivial 3-AP.

Proof of Roth's Theorem

Now define $N' = [J_k]$ and

$$A' = \left\{ j : \ 1 \le j \le N', \ \alpha_{i,k} + jr - kN \in A \right\},$$

a subset of $\{1, 2, \ldots, N'\}$, so that

$$\#A' = \#A_{i,k} \ge (1 + \frac{c\delta}{2})\delta N'.$$

Note that

$$N' \ge \min\left\{ \frac{N}{r}, \ J_0, \ J_K \right\} \gg \min\left\{ \frac{N}{r}, \ \frac{c\delta^2 y}{4s} \right\}$$
$$\gg \min\left\{ \frac{N}{R}, \ \frac{\delta^2 N}{lS} \right\} \gg \sqrt{\delta^3 N}.$$

Hence A' contains a non-trivial 3-AP.

Proof of Roth's Theorem

Now define $N' = [J_k]$ and

$$A' = \left\{ j : \ 1 \le j \le N', \ \alpha_{i,k} + jr - kN \in A \right\},$$

a subset of $\{1, 2, \ldots, N'\}$, so that

$$\#A' = \#A_{i,k} \ge (1 + \frac{c\delta}{2})\delta N'.$$

Note that

$$N' \ge \min\left\{ \frac{N}{r}, \ J_0, \ J_K \right\} \gg \min\left\{ \frac{N}{r}, \ \frac{c\delta^2 y}{4s} \right\}$$
$$\gg \min\left\{ \frac{N}{R}, \ \frac{\delta^2 N}{lS} \right\} \gg \sqrt{\delta^3 N}.$$

Hence A' contains a non-trivial 3-AP.

Proof of Roth's Theorem

If $u + v = 2w$ with u, v, $w \in A'$, then

$$a = \alpha_{i,k} + ur - kN,$$
$$b = \alpha_{i,k} + vr - kN,$$
$$c = \alpha_{i,k} + wr - kN.$$

So

$$a + b = 2c,$$

contradicting the supposition that A contains no non-trivial 3-AP.

Therefore the theorem is true for δ, if it is true for $\delta(1 + c\delta)$ with some $c > 0$.

Proof of Roth's Theorem

If $u + v = 2w$ with $u,\, v,\, w \in A'$, then

$$a = \alpha_{i,\,k} + ur - kN,$$
$$b = \alpha_{i,\,k} + vr - kN,$$
$$c = \alpha_{i,\,k} + wr - kN.$$

So

$$a + b = 2c,$$

contradicting the supposition that A contains no non-trivial 3-AP.

Therefore the theorem is true for δ, if it is true for $\delta(1 + c\delta)$ with some $c > 0$.

Proof of Roth's Theorem

If $u + v = 2w$ with $u,\ v,\ w \in A'$, then

$$a = \alpha_{i,\,k} + ur - kN,$$
$$b = \alpha_{i,\,k} + vr - kN,$$
$$c = \alpha_{i,\,k} + wr - kN.$$

So

$$a + b = 2c,$$

contradicting the supposition that A contains no non-trivial 3-AP.

Therefore the theorem is true for δ, if it is true for $\delta(1 + c\delta)$ with some $c > 0$.

Proof of Roth's Theorem

If $u + v = 2w$ with $u,\ v,\ w \in A'$, then

$$a = \alpha_{i,k} + ur - kN,$$
$$b = \alpha_{i,k} + vr - kN,$$
$$c = \alpha_{i,k} + wr - kN.$$

So

$$a + b = 2c,$$

contradicting the supposition that A contains no non-trivial 3-AP.

Therefore the theorem is true for δ, if it is true for $\delta(1 + c\delta)$ with some $c > 0$.

Proof of Roth's Theorem

If $u + v = 2w$ with $u,\, v,\, w \in A'$, then

$$a = \alpha_{i,\,k} + ur - kN,$$
$$b = \alpha_{i,\,k} + vr - kN,$$
$$c = \alpha_{i,\,k} + wr - kN.$$

So

$$a + b = 2c,$$

contradicting the supposition that A contains no non-trivial 3-AP.

Therefore the theorem is true for δ, if it is true for $\delta(1 + c\delta)$ with some $c > 0$.

Remark 2

In Roth's proof, one can take

$$\delta \approx \frac{1}{\log\log N}.$$

This was improved by Szemerédi to

$$\delta \approx \frac{1}{\exp(\sqrt{\log\log N})}.$$

Remark 2

In Roth's proof, one can take

$$\delta \approx \frac{1}{\log \log N}.$$

This was improved by Szemerédi to

$$\delta \approx \frac{1}{\exp(\sqrt{\log \log N})}.$$

Remark 2

In the last eighties, both Heath-Brown and Szemerédi showed that one can take

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

for some small $c > 0$.

The best result known, due to Bourgain, is that one can take

$$\delta \approx \sqrt{\frac{\log \log N}{\log N}}.$$

Remark 2

In the last eighties, both Heath-Brown and Szemerédi showed that one can take

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

for some small $c > 0$.

The best result known, due to Bourgain, is that one can take

$$\delta \approx \sqrt{\frac{\log \log N}{\log N}}.$$


CAFÉ
SAINT MALO

In the other direction, we have

Theorem 6 (Behrend)

For any sufficiently large integer N, there exists a subset $A \subseteq \{1, \ldots, N\}$ with

$$\#A \geq \frac{N}{\exp(c\sqrt{\log N})},$$

such that A has no non-trivial 3-AP.

Proof of Behrend's Theorem

Let

$$T = \{(x_0, \ldots, x_{n-1}) \in \mathbb{Z}^n : \ 0 \le x_i < d\}$$

and

$$T_k = \left\{\mathbf{x} \in T : \ |\mathbf{x}|^2 = k\right\}.$$

We have $|T| = d^n$, and $|\mathbf{x}|^2 < nd^2$ for every $\mathbf{x} \in T$, so there exists a positive integer k for which T_k has $\ge \frac{d^{n-2}}{n}$ elements. Let

$$A = \left\{x_0 + x_1(2d) + \cdots + x_{n-1}(2d)^{n-1} : \ \mathbf{x} \in T_k\right\}.$$

Proof of Behrend's Theorem

Let

$$T = \{(x_0, \dots, x_{n-1}) \in \mathbb{Z}^n : \ 0 \le x_i < d\}$$

and

$$T_k = \left\{ \mathbf{x} \in T : \ |\mathbf{x}|^2 = k \right\}.$$

We have $|T| = d^n$, and $|\mathbf{x}|^2 < nd^2$ for every $\mathbf{x} \in T$, so there exists a positive integer k for which T_k has $\ge \frac{d^{n-2}}{n}$ elements. Let

$$A = \left\{ x_0 + x_1(2d) + \cdots + x_{n-1}(2d)^{n-1} : \ \mathbf{x} \in T_k \right\}.$$

Proof of Behrend's Theorem

Let

$$T = \{(x_0, \ldots, x_{n-1}) \in \mathbb{Z}^n : \ 0 \le x_i < d\}$$

and

$$T_k = \left\{ \mathbf{x} \in T : \ |\mathbf{x}|^2 = k \right\}.$$

We have $|T| = d^n$, and $|\mathbf{x}|^2 < nd^2$ for every $\mathbf{x} \in T$, so there exists a positive integer k for which T_k has $\ge \frac{d^{n-2}}{n}$ elements. Let

$$A = \left\{ x_0 + x_1(2d) + \cdots + x_{n-1}(2d)^{n-1} : \ \mathbf{x} \in T_k \right\}.$$

Proof of Behrend's Theorem

Let

$$T = \{(x_0, \ldots, x_{n-1}) \in \mathbb{Z}^n : \ 0 \le x_i < d\}$$

and

$$T_k = \left\{\mathbf{x} \in T : \ |\mathbf{x}|^2 = k\right\}.$$

We have $|T| = d^n$, and $|\mathbf{x}|^2 < nd^2$ for every $\mathbf{x} \in T$, so there exists a positive integer k for which T_k has $\ge \frac{d^{n-2}}{n}$ elements. Let

$$A = \left\{x_0 + x_1(2d) + \cdots + x_{n-1}(2d)^{n-1} : \ \mathbf{x} \in T_k\right\}.$$

Proof of Behrend's Theorem

If $a + b = 2c$ with a, b, $c \in A$, then

$$a_0 + b_0 \equiv 2c_0 \pmod{2d}.$$

Since $-2d < a_0 + b_0 - 2c_0 < 2d$,

$$a_0 + b_0 = 2c_0.$$

Similarly one can prove that

$$a_1 + b_1 = 2c_1,$$

and indeed

$$a_i + b_i = 2c_i$$

for each $i \geq 0$.

Proof of Behrend's Theorem

If $a + b = 2c$ with a, b, $c \in A$, then

$$a_0 + b_0 \equiv 2c_0 \pmod{2d}.$$

Since $-2d < a_0 + b_0 - 2c_0 < 2d$,

$$a_0 + b_0 = 2c_0.$$

Similarly one can prove that

$$a_1 + b_1 = 2c_1,$$

and indeed

$$a_i + b_i = 2c_i$$

for each $i \geq 0$.

Proof of Behrend's Theorem

If $a + b = 2c$ with a, b, $c \in A$, then

$$a_0 + b_0 \equiv 2c_0 \pmod{2d}.$$

Since $-2d < a_0 + b_0 - 2c_0 < 2d$,

$$a_0 + b_0 = 2c_0.$$

Similarly one can prove that

$$a_1 + b_1 = 2c_1,$$

and indeed

$$a_i + b_i = 2c_i$$

for each $i \geq 0$.

Proof of Behrend's Theorem

If $a + b = 2c$ with a, b, $c \in A$, then

$$a_0 + b_0 \equiv 2c_0 \pmod{2d}.$$

Since $-2d < a_0 + b_0 - 2c_0 < 2d$,

$$a_0 + b_0 = 2c_0.$$

Similarly one can prove that

$$a_1 + b_1 = 2c_1,$$

and indeed

$$a_i + b_i = 2c_i$$

for each $i \geq 0$.

Then

$$\mathbf{a} + \mathbf{b} = 2\mathbf{c} \qquad \text{for} \;\; \mathbf{a}, \mathbf{b}, \mathbf{c} \in T_k.$$

So **c** is the central point in the line segment between points **a** and **b**, which is impossible as T_k is a sphere.

Therefore A contains no non-trivial 3-AP.

Then

$$\mathbf{a} + \mathbf{b} = 2\mathbf{c} \qquad \text{for} \ \ \mathbf{a}, \mathbf{b}, \mathbf{c} \in T_k.$$

So **c** is the central point in the line segment between points **a** and **b**, which is impossible as T_k is a sphere.

Therefore A contains no non-trivial 3-AP.

Then

$$\mathbf{a} + \mathbf{b} = 2\mathbf{c} \qquad \text{for} \;\; \mathbf{a}, \mathbf{b}, \mathbf{c} \in T_k.$$

So **c** is the central point in the line segment between points **a** and **b**, which is impossible as T_k is a sphere.

Therefore A contains no non-trivial 3-AP.

Proof of Behrend's Theorem

The elements of A are all

$$\leq (d-1)(1+2d+\cdots+(2d)^{n-1}) < (2d)^n.$$

For any sufficiently large integer N, we try to take n and d such that $(2d)^n \leq N$, $(2d)^n \sim N$ with $n2^n d^2$ as small as possible.

We take

$$n = [\sqrt{\log N}] \quad \text{and} \quad d = [\frac{N^{\frac{1}{n}}}{2}],$$

so that

$$\#A \geq \frac{(2d)^n}{n2^n d^2} \geq \frac{N}{\exp(c\sqrt{\log N})}.$$

Proof of Behrend's Theorem

The elements of A are all

$$\leq (d-1)(1+2d+\cdots+(2d)^{n-1}) < (2d)^n.$$

For any sufficiently large integer N, we try to take n and d such that $(2d)^n \leq N$, $(2d)^n \sim N$ with $n2^n d^2$ as small as possible.

We take

$$n = [\sqrt{\log N}] \quad \text{and} \quad d = [\frac{N^{\frac{1}{n}}}{2}],$$

so that

$$\#A \geq \frac{(2d)^n}{n2^n d^2} \geq \frac{N}{\exp(c\sqrt{\log N})}.$$

Proof of Behrend's Theorem

The elements of A are all

$$\leq (d-1)(1+2d+\cdots+(2d)^{n-1}) < (2d)^n.$$

For any sufficiently large integer N, we try to take n and d such that $(2d)^n \leq N$, $(2d)^n \sim N$ with $n2^n d^2$ as small as possible.

We take

$$n = [\sqrt{\log N}] \quad \text{and} \quad d = [\frac{N^{\frac{1}{n}}}{2}],$$

so that

$$\#A \geq \frac{(2d)^n}{n2^n d^2} \geq \frac{N}{\exp(c\sqrt{\log N})}.$$

Proof of Behrend's Theorem

The elements of A are all

$$\leq (d-1)(1+2d+\cdots+(2d)^{n-1}) < (2d)^n.$$

For any sufficiently large integer N, we try to take n and d such that $(2d)^n \leq N$, $(2d)^n \sim N$ with $n2^nd^2$ as small as possible.

We take

$$n = [\sqrt{\log N}] \quad \text{and} \quad d = [\frac{N^{\frac{1}{n}}}{2}],$$

so that

$$\#A \geq \frac{(2d)^n}{n2^nd^2} \geq \frac{N}{\exp(c\sqrt{\log N})}.$$

Remark 3

For any sufficiently large integer N, we shall take n and d such that $(2d)^n \leq N$, $(2d)^n \sim N$ with $n2^nd^2$ as small as possible.

Firstly we take

$$d = [\frac{N^{\frac{1}{n}}}{2}],$$

so that

$$\log d \sim \frac{\log N}{n}.$$

Since $n = o(2^n)$ is neglected, we make 2^nd^2 or

$$n \log 2 + 2 \log d \sim n \log 2 + \frac{2 \log N}{n}$$

as small as possible.

Remark 3

For any sufficiently large integer N, we shall take n and d such that $(2d)^n \leq N$, $(2d)^n \sim N$ with $n2^nd^2$ as small as possible.

Firstly we take

$$d = [\frac{N^{\frac{1}{n}}}{2}],$$

so that

$$\log d \sim \frac{\log N}{n}.$$

Since $n = o(2^n)$ is neglected, we make 2^nd^2 or

$$n \log 2 + 2 \log d \sim n \log 2 + \frac{2 \log N}{n}$$

as small as possible.

Remark 3

For any sufficiently large integer N, we shall take n and d such that $(2d)^n \leq N$, $(2d)^n \sim N$ with $n2^nd^2$ as small as possible.

Firstly we take

$$d = [\frac{N^{\frac{1}{n}}}{2}],$$

so that

$$\log d \sim \frac{\log N}{n}.$$

Since $n = o(2^n)$ is neglected, we make 2^nd^2 or

$$n \log 2 + 2 \log d \sim n \log 2 + \frac{2 \log N}{n}$$

as small as possible.

Remark 3

For any sufficiently large integer N, we shall take n and d such that $(2d)^n \leq N$, $(2d)^n \sim N$ with $n2^n d^2$ as small as possible.

Firstly we take

$$d = [\frac{N^{\frac{1}{n}}}{2}],$$

so that

$$\log d \sim \frac{\log N}{n}.$$

Since $n = o(2^n)$ is neglected, we make $2^n d^2$ or

$$n \log 2 + 2 \log d \sim n \log 2 + \frac{2 \log N}{n}$$

as small as possible.

Remark 3

Then we can see $n = [\sqrt{\log N}]$ is a suitable choice. In such choice of N,

$$d \sim \exp(\sqrt{\log N}).$$

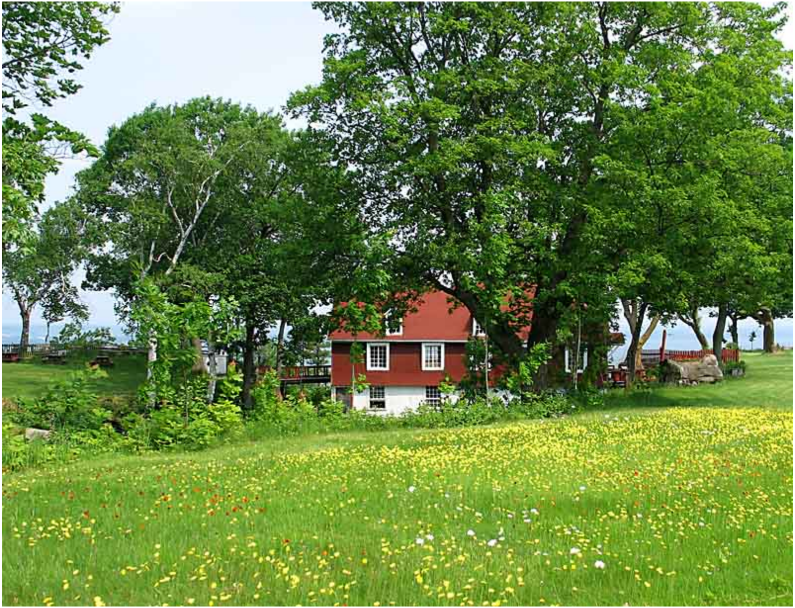
It is easy to check that $(2d)^n \leq N$, $(2d)^n \sim N$.

Remark 3

Then we can see $n = [\sqrt{\log N}]$ is a suitable choice. In such choice of N,

$$d \sim \exp(\sqrt{\log N}).$$

It is easy to check that $(2d)^n \leq N$, $(2d)^n \sim N$.



References

- Andrew Granville, *Uniform distribution, Roth's Theorem and beyond.*
- L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, New York: Wiley, 1974.
- Elias M. Stein and Rami Shakarchi, *Fourier Analysis: An Introduction*, Princeton University Press, 2005.