Arithmetic Combinatorics

Prof. W.T. Gowers

Michaelmas 2007

LaTeXed by Sebastian Pancratz

These notes are based on a course of lectures given by Prof. W.T. Gowers in Part III of the Mathematical Tripos at the University of Cambridge in the academic year 2007–2008.

These notes have not been checked by Prof. W.T. Gowers and should not be regarded as official notes for the course. In particular, the responsibility for any errors is mine — please email Sebastian Pancratz (`sfp25`) with any comments or corrections.

Contents

Chapter 1

Fourier Analysis on Finite Abelian Groups

The classification of finite Abelian groups tells us that they are all products of cyclic groups, i.e., they have the form

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k},$$

where we write $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$. Two important examples are $\mathbb{Z}_N$ and $\mathbb{Z}_p^n$, which we shall write as $\mathbb{F}_p^n$.

A *character* on a finite Abelian group G is a homomorphism $\psi\colon G \to \mathbb{C}^*$, the multiplicative group of $\mathbb{C}$. If $|G| = n$ then for every $x \in G$ we have $nx = 0$, so $(\psi(x))^n = 1$, i.e., $\psi(x)$ has to be an nth root of unity.

Example. (i) If $G = \mathbb{Z}_N$, let $\omega = e^{2\pi i/N}$. Then for every $r \in \mathbb{Z}_N$ the function $x \mapsto \omega^{rx}$ is a character. All characters have this form since $\psi(1)$ determines ψ, i.e., if $\psi(1) = \omega^r$ then $\psi(x) = \omega^{rx}$ for every $x \in G$.

(ii) If $G = \mathbb{F}_p^k$ let $\omega = e^{2\pi i/p}$ and for each $r = (r_1, \ldots, r_k) \in G$ and each $x = (x_1, \ldots, x_k) \in G$ write $r \cdot x = r_1x_1 + \cdots + r_kx_k$. Then the map $x \mapsto \omega^{r\cdot x}$ is a character. Again this gives all characters, since ψ is determined by its values on $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$,…,$(0, \ldots, 0, 1)$.

(iii) In general, if $G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, then setting $\omega_{m_j} = e^{2\pi i/m_j}$, the function $x \mapsto \omega_{m_1}^{r_1x_1} \cdots \omega_{m_k}^{r_kx_k}$ is a character for every $(r_1, \ldots, r_k) \in G$. We shall see that these are all the characters on G.

Lemma 1.1. If ψ and χ are distinct characters on finite Abelian group G, then

$$\mathbb{E}_{x\in G}\, \psi(x)\overline{\chi(x)} = 0.$$

Proof. Let us write $\phi = \psi\bar{\chi}$. It is easy to check that ϕ is a non-trivial character. Then See A.1.1.

$$\mathbb{E}_x\, \phi(x) = \mathbb{E}_x\, \phi(x + y)$$

for any $y \in G$, since adding y permutes the elements of G. But that is

$$\mathbb{E}_x\, \phi(x)\phi(y) = \phi(y)\, \mathbb{E}_x\, \phi(x).$$

Since ϕ is non-trivial, we can find y such that $\phi(y) \neq 1$, so $\mathbb{E}_x\, \phi(x) = 0$. □

We shall make frequent use of two normed spaces, $L_2(G)$ and $l_2(G)$. If $f\colon G \to \mathbb{C}$, then

$$\|f\|_{L_2(G)}^2 = \mathbb{E}_{x\in G}|f(x)|^2 = \frac{1}{|G|}\sum_{x\in G}|f(x)|^2,$$
$$\|f\|_{l_2(G)}^2 = \sum_{x\in G}|f(x)|^2.$$

Proposition 1.2. The characters form an orthonormal basis of $L_2(G)$.

Proof. We have just shown that distinct characters are orthogonal. Also, $\mathbb{E}_x|\psi(x)|^2 = 1$ since $\psi(x)$ is always a root of unity. Since we have constructed $|G|$ different characters, the proposition is proved. □

Let G be a finite Abelian group and let $f\colon G \to \mathbb{C}$. We define $\hat{G}$, the *dual group* of G, to be the group of all characters on G under pointwise multiplication.

The *Fourier transform* $\hat{f}$ of f is the function from $\hat{G}$ to $\mathbb{C}$, given by the formula

$$\hat{f}(\psi) = \mathbb{E}_{x\in G}\, f(x)\psi(x).$$

Example. If $G = \mathbb{Z}_N$, $\omega = e^{2\pi i/N}$, then let us identify r with the character $x \mapsto \omega^{rx}$. Then

$$\begin{aligned}\hat{f}(r) &= \mathbb{E}_x\, f(x)\omega^{rx}\\ &= \mathbb{E}_x\, f(x)e^{2\pi irx/N}\\ &= \frac{1}{N}\big(f(0) + f(1)e^{2\pi ir/N} + f(2)e^{4\pi ir/N} + \cdots\big).\end{aligned}$$

Compare this with the "usual formula"

$$\hat{f}(r) = \int_0^1 f(x)e^{2\pi irx}\,dx.$$

Proposition 1.3. Let G be a finite Abelian group. Then $\hat{\hat{G}} = G$.

See A.1.2 and A.1.3.

Proof. For $x \in G$ let $\delta_x\colon \hat{G} \to \mathbb{C}$ be the map $\psi \mapsto \psi(x)$. Then it is easy to check that the map $x \mapsto \delta_x$ is a homomorphism from G to $\hat{\hat{G}}$. If $x \neq y$, then we can find $\psi \in \hat{G}$ such that $\psi(x) \neq \psi(y)$ since there are $|G|$ linear independent characters. It follows that $\delta_x \neq \delta_y$, so the map $x \mapsto \delta_x$ is an injection. Therefore, $|G| \le |\hat{\hat{G}}| \le |\hat{G}| \le |G|$. □

Proposition 1.4. The Fourier transform has the following three properties.

(i) (Plancherel identity) $\langle \hat{f}, \hat{g}\rangle = \langle f, g\rangle$, i.e.,

$$\sum_{\psi\in\hat{G}} \hat{f}(\psi)\overline{\hat{g}(\psi)} = \mathbb{E}_{x\in G}\, f(x)\overline{g(x)}$$

In particular, $\|\hat{f}\|_{l_2(\hat{G})} = \|f\|_{L_2(G)}$.

(ii) (Inversion formula) $f(x) = \sum_{\psi\in\hat{G}} \hat{f}(\psi)\overline{\psi(x)}$.

(iii) (Convolution identity) Define $f * g$ and $\hat{f} * \hat{g}$ by

$$(f * g)(x) = \mathbb{E}_{y+z=x}\, f(y)g(z), \qquad (\hat{f} * \hat{g})(\psi) = \sum_{\phi\chi=\psi} \hat{f}(\phi)\hat{g}(\chi).$$

Then $\widehat{f * g} = \hat{f}\hat{g}$ and $\hat{f} * \hat{g} = \widehat{fg}$.

Proof. (i)

$$\begin{aligned}\langle \hat{f}, \hat{g} \rangle &= \sum_{\psi} \hat{f}(\psi)\overline{\hat{g}(\psi)} \\ &= \sum_{\psi} \mathbb{E}_x\, f(x)\psi(x)\, \mathbb{E}_y\, \overline{g(y)\psi(y)} \\ &= \mathbb{E}_{x,y}\, f(x)\overline{g(y)} \sum_{\psi} \psi(x-y)\end{aligned}$$

If $x \neq y$ then pick ϕ such that $\phi(x-y) \neq 1$. Then

$$\sum_{\psi} \psi(x-y) = \sum_{\psi} \phi\psi(x-y) = \phi(x-y) \sum_{\psi} \psi(x-y)$$

so $\sum_{\psi} \psi(x-y) = 0$. If $x = y$ then $\sum_{\psi} \psi(x-y) = |G|$. Hence we obtain

$$\mathbb{E}_{x,y}|G| f(x)\overline{g(y)}\delta_{xy} = \mathbb{E}_x|G|\, \mathbb{P}(y = x) f(x)\overline{g(y)} = \langle f, g \rangle.$$

(ii)

$$\begin{aligned}\sum_{\psi} \hat{f}(\psi)\overline{\psi(x)} &= \mathbb{E}_y\, f(y) \sum_{\psi} \psi(y)\overline{\psi(x)} \\ &= \mathbb{E}_y\, f(y)|G|\delta_{yx} \\ &= f(x)\end{aligned}$$

(iii) We first show that $\widehat{f * g}(\psi) = \hat{f}\hat{g}(\psi)$,

$$\begin{aligned}\widehat{f * g}(\psi) &= \mathbb{E}_x\, f * g(x)\psi(x) \\ &= \mathbb{E}_x\, \mathbb{E}_{y+z=x}\, f(y)g(z)\psi(x) \\ &= \mathbb{E}_x\, \mathbb{E}_{y+z=x}\, f(y)\psi(y)g(z)\psi(z) \\ &= \big(\mathbb{E}_y\, f(y)\psi(y)\big)\big(\mathbb{E}_z\, g(z)\psi(z)\big) \\ &= \hat{f}\hat{g}(\psi)\end{aligned}$$

We claim that $\hat{f} * \hat{g} = \widehat{fg}$. For $\psi \in \hat{G}$,

$$\begin{aligned}\widehat{fg}(\psi) &= \mathbb{E}_x\, f(x)g(x)\psi(x) \\ &= \mathbb{E}_x \sum_{\phi_1,\phi_2} \hat{f}(\phi_1)\overline{\phi_1(x)}\hat{g}(\phi_2)\overline{\phi_2(x)}\psi(x) \\ &= \sum_{\phi_1,\phi_2} \hat{f}(\phi_1)\hat{g}(\phi_2)\delta_{\phi_1\phi_2,\psi} \\ &= \sum_{\phi_1\phi_2=\psi} \hat{f}(\phi_1)\hat{g}(\phi_2) \\ &= \hat{f} * \hat{g}(\psi)\end{aligned}$$

as required. □

See A.1.4. If A is a subset of G, we will write $A(x)$ instead of $\chi_A(x)$ for the characteristic function. Notice that $\hat{A}(0) = \mathbb{E}_x\, A(x) \cdot 1 = |A|/|G|$, the density of A in G. Also,

$$\sum_\psi |\hat{A}(\psi)|^2 = \mathbb{E}_x |A(x)|^2 = \mathbb{E}_x\, A(x) = \frac{|A|}{|G|}.$$

Theorem 1.5 (Roth's Theorem in $\mathbb{F}_3^n$)**.** Let A be a subset of $\mathbb{F}_3^n$ of density at least $8/n$. Then A contains a subset of the form $\{x, x+d, x+2d\}$, $d \neq 0$, or equivalently, x, y, z not all equal such that $x + y + z = 0$.

See A.1.5 and A.1.6. *Proof.* A contains such a triple as long as

$$\mathbb{E}_{x+y+z=0}\, A(x)A(y)A(z) > 3^{-n}.$$

But

$$\begin{aligned}
\mathbb{E}_{x+y+z=0}\, A(x)A(y)A(z) &= A * A * A(0) \\
&= \sum_\psi \widehat{A * A * A}(\psi)\psi(0) \\
&= \sum_\psi \hat{A}(\psi)^3 \\
&= \hat{A}(0)^3 + \sum_{\psi\neq 0} \hat{A}(\psi)^3 \\
&\geq \hat{A}(0)^3 - \sum_{\psi\neq 0} |\hat{A}(\psi)|^3 \\
&\geq \hat{A}(0)^3 - \max_{\psi\neq 0} |\hat{A}(\psi)| \sum_{\psi\neq 0} |\hat{A}(\psi)|^2 \\
&\geq \hat{A}(0)^3 - \max_{\psi\neq 0} |\hat{A}(\psi)||A|.
\end{aligned}$$

Hence, if $|A| = \delta$ this is equal to $\delta^3 - \delta \max_{\psi\neq 0} |\hat{A}(\psi)|$. As a convention, if $A \subset G$ then $|A|$ means the density of A.

See A.1.7. In particular, if $|\hat{A}(\psi)| \leq \delta^2/2$ for every $\psi \neq 0$ then

$$\mathbb{E}_{x+y+z=0}\, A(x)A(y)A(z) \geq \frac{\delta^3}{2} \geq \frac{256}{n^3} > 3^{-n}$$

for all $n \in \mathbb{N}$, so we are done.

Otherwise, there exists $\psi \neq 0$ such that $|\hat{A}(\psi)| > \delta^2/2$. Suppose this corresponds in $r \in \mathbb{F}_3^n$, i.e.,

$$\psi(x) = \omega^{r\cdot x}$$

where $\omega = e^{2\pi i/3}$. So $\hat{A}(\psi) = \mathbb{E}_x\, A(x)\omega^{r\cdot x}$. Let $f(x) = A(x) - \delta$ and define $X_i = \{x : r \cdot x = i\}$ for $i = 0, 1, 2$. Then

$$\begin{aligned}
\hat{A}(\psi) &= \tfrac{1}{3}\big(\mathbb{E}_{x\in X_0}\, A(x) + \omega\, \mathbb{E}_{x\in X_1}\, A(x) + \omega^2\, \mathbb{E}_{x\in X_2}\, A(x)\big) \\
&= \tfrac{1}{3}\big(\mathbb{E}_{x\in X_0}\, f(x) + \omega\, \mathbb{E}_{x\in X_1}\, f(x) + \omega^2\, \mathbb{E}_{x\in X_2}\, f(x)\big).
\end{aligned}$$

Since $|\hat{A}(\psi)| \geq \delta^2/2$, there must exist i such that

$$|\mathbb{E}_{x \in X_i} f(x)| \geq \frac{\delta^2}{2}.$$

It follows that there exists j such that

$$\mathbb{E}_{x \in X_j} f(x) \geq \frac{\delta^2}{4}$$

for the following reason. $\mathbb{E}_x f(x) = 0$ so if

$$\mathbb{E}_{x \in X_i} f(x) \leq -\frac{\delta^2}{2}$$

then

$$\mathbb{E}_{x \in X_j} f(x) \geq \frac{\delta^2}{4}$$

for some $j \neq i$. It follows that

$$\mathbb{E}_{x \in X_j} A(x) \geq \delta + \frac{\delta^2}{4}$$

so the density of A in X_j is greater then δ by a factor of at least $1 + \delta/4$.

This allows us to iterate since $X_j \cong \mathbb{F}_3^{n-1}$. At each iteration, we lose a dimension, but the density η goes up by a factor of at least $1 + \eta/4$. In particular, after $4/\delta$ steps, the density reaches at least 2δ. Then after $4/2\delta$ steps it reaches 4δ, etc. Since the density can never exceed 1, the iteration stops before we reach

See A.1.8.

$$\frac{4}{\delta} + \frac{4}{2\delta} + \frac{4}{4\delta} + \cdots = \frac{8}{\delta}$$

steps. So long as $n \geq 8/\delta$, we obtain a triple of the desired kind.

We also need to check that at each stage "$\delta \geq 8/n$". But if $\delta \geq 8/n$ then

$$\delta\left(1 + \frac{\delta}{4}\right) \geq \frac{8}{n}\left(1 + \frac{2}{n}\right) \geq \frac{8}{n-1}.$$

□

Chapter 2

Roth's Theorem

The aim of this section is to prove the following result.

Theorem 2.1. There exists a constant $C > 0$ such that if $N \in \mathbb{N}$ and $A \subset [N]$ has cardinality at least $CN/\log\log N$ then A contains an arithmetic progression of length 3.

The proof will occupy the rest of the section. To begin with, let $A, B, C \subset \mathbb{Z}_N$ and suppose that N is odd. Then

$$\mathbb{E}_{x+z=2y} A(x)B(y)C(z) = \mathbb{E}_{x+z=y} A(x)B_2(y)C(z)$$

where $B_2(y) = B(y/2)$. Let α, β, γ be the densities of A, B, C and note that the density of B_2 is also β. Then the last expression is

$$\begin{aligned}\langle A * C, B_2\rangle &= \langle \hat{A}\hat{C}, \hat{B}_2\rangle \\ &= \sum_r \hat{A}(r)\hat{C}(r)\overline{\hat{B}_2(r)}\end{aligned}$$

where we identify r with the function $x \mapsto \omega^{rx}$, $\omega = e^{2\pi i/N}$,

$$\begin{aligned}&\geq \hat{A}(0)\hat{B}_2(0)\hat{C}(0) - \sum_{r\neq 0}|\hat{A}(r)||\hat{B}_2(r)||\hat{C}(r)| \\ &\geq \alpha\beta\gamma - \max_{r\neq 0}|\hat{A}(r)|\langle|\hat{B}_2|, |\hat{C}|\rangle \\ &\geq \alpha\beta\gamma - \max_{r\neq 0}|\hat{A}(r)|\|\hat{B}_2\|\|\hat{C}\| \\ &= \alpha\beta\gamma - (\beta\gamma)^{1/2}\max_{r\neq 0}|\hat{A}(r)|.\end{aligned}$$

Therefore, either the original expectation is at least $\alpha\beta\gamma/2$ or there exists $r \neq 0$ such that $|\hat{A}(r)| \geq \alpha(\beta\gamma)^{1/2}/2$.

Lemma 2.2. Let $N \in \mathbb{N}$ and $\varepsilon > 0$. Let $\psi\colon \mathbb{Z}_N \to \mathbb{C}$ be a character. Then it is possible to partition $\mathbb{Z}_N$ into arithmetic progressions P_i, when viewed as subsets of $\{0, 1, \ldots, N-1\}$, of length at least $c(\varepsilon)\sqrt{N}$ such that the diameter of $\psi(P_i)$ is at most ε for every i. The constant can be taken to be $c(\varepsilon) = \varepsilon/8\pi$.

Proof. Let $k = \lfloor\sqrt{N}\rfloor$. Since the unit circle has circumference 2π, there must be two of See A.2.1.

the values $\psi(0), \dots, \psi(k)$ that are within $2\pi/k$ of each other. Since ψ is a character, it follows easily that there exists $d \in \{1, \dots, k\}$ such that

$$|\psi(x+d) - \psi(x)| \leq \frac{2\pi}{k}$$

for every $x \in \mathbb{Z}_N$. Therefore, if P is an arithmetic progression of length at most r and common difference d, then $\operatorname{diam} \psi(P) \leq 2\pi r/k$ by the triangle inequality. Let $r = \varepsilon k/2\pi$.

See A.2.2. Now partition $\{0, 1, \dots, N-1\}$ into residue classes modulo d. Since $d \leq k$, each of these has size at least $N/2k$. It is easy to see that such a set can be partitioned into arithmetic progressions P_i of common difference d and lengths between $r/2$ and r.

We are therefore done since $r/2 \geq \varepsilon\sqrt{N}/8\pi$. □

Now we will prove Theorem 2.1.

Let $A \subset [N]$ have density δ. We set $B = C = A \cap [N/3, 2N/3]$ and consider two cases.

Case 1. If $|B| < \delta N/6$ then either

$$\left|A \cap \left[1, \frac{N}{3}\right]\right| \geq \frac{5N\delta}{12}$$

or

$$\left|A \cap \left[\frac{2N}{3}, N\right]\right| \geq \frac{5N\delta}{12}.$$

So there exists a subinterval of $[N]$ of length at least $N/6$ in which A has density at least $5\delta/4$.

Case 2. Now suppose $|B| = |C| \geq \delta N/6$. We first ensure that N is odd by passing to $N' = N - 1$ if necessary. Then the density of A in $[N']$ is $\delta' \geq \delta - 1/N$. Note that in particular, $\delta' \geq \delta/2$ provided $\delta N \geq 1$. The observation at the beginning of the section divides this case into two subcases.

Case 2A. If

$$\mathbb{E}_{x+y=2y}\, A(x)B(y)C(z) \geq \alpha\beta\gamma/2 \geq \frac{1}{2}\frac{\delta}{2}\frac{\delta}{6}\frac{\delta}{6} = \frac{\delta^3}{144}$$

then we have an arithmetic progression of length 3 modulo N in $A \times B \times C$ provided that $\delta^3/144 > 1/N$. This is a genuine arithmetic progression in $[N]$ as B and C lie in the middle third.

Case 2B. Otherwise, there exists an $r \neq 0$ such that

$$|\hat{A}(r)| \geq \frac{\alpha(\beta\gamma)^{1/2}}{2} \geq \frac{1}{2}\frac{\delta}{2}\frac{\delta}{6} = \frac{\delta^2}{24}.$$

Let $\psi\colon x \mapsto \omega^{rx}$. By Lemma 2.2, we can partition $\mathbb{Z}/N'\mathbb{Z}$ into arithmetic progressions $P_1, \dots, P_m$ all of cardinality at least $(\delta^2/48)\sqrt{N'}/8\pi \geq \delta^2\sqrt{N}/500\pi$ such that $\operatorname{diam} \psi(P_i) \leq \delta^2/48$ for every i.

Let $f(x) = A(x) - \delta'$ be the *balanced function* of A. Note that $\hat{f}(r) = \hat{A}(r)$ as $r \neq 0$ and so ψ is non-trivial. For each i, let x_i be some element of P_i. Then

$$\frac{\delta^2}{24} \leq |\hat{A}(r)| = |\hat{f}(r)| = |\mathbb{E}_x\, f(x)\omega^{rx}|$$

$$= \Big|\sum_i |P_i|\, \mathbb{E}_{x\in P_i} f(x)\psi(x)\Big|$$
$$\leq \sum_i |P_i| |\mathbb{E}_{x\in P_i} f(x)\psi(x)|.$$

But

$$|\mathbb{E}_{x\in P_i} f(x)\psi(x)| \leq |\mathbb{E}_{x\in P_i} f(x)\psi(x_i)| + |\mathbb{E}_{x\in P_i} f(x)(\psi(x_i)-\psi(x))|$$
$$= |\mathbb{E}_{x\in P_i} f(x)| + \frac{\delta^2}{48}.$$

Therefore,

$$\sum_i |P_i| |E_{x\in P_i} f(x)| \geq \frac{\delta^2}{48}.$$

But $\sum_i |P_i|\, \mathbb{E}_{x\in P_i} f(x) = 0$ so

$$\sum_i |P_i| \big(|\mathbb{E}_{x\in P_i} f(x)| + \mathbb{E}_{x\in P_i} f(x)\big) \geq \frac{\delta^2}{48}.$$

It follows that $\mathbb{E}_{x\in P_i} f(x) \geq \delta^2/96$ for some i. Therefore,

$$\frac{|A\cap P_i|}{|P_i|} \geq \delta' + \frac{\delta^2}{96} \geq \delta + \frac{\delta^2}{100}$$

provided $\delta^2 N \geq 2400$.

The proof is basically over. From now on, we argue slightly less formal. We have shown that if A does not contain an arithmetic progression of length 3 then there is a subprogression P of cardinality at least $\delta^2\sqrt{N}/5000$, inside which A has density at least $\delta+\delta^2/100$. As long as $\delta^8 N \geq (5000)^4$, this implies $|P| \geq N^{1/4}$. This leads to an iteration $A_0 \subset [N_0], A_1 \subset [N_1], \dots$ and our assumptions continue to be valid if $\delta^8 N_k \geq (5000)^4$.

Since $N_k \geq N^{(1/4)^k}$ and as we cannot have more than

$$\frac{100}{\delta} + \frac{100}{2\delta} + \frac{100}{4\delta} + \cdots = \frac{200}{\delta}$$

steps, the theorem is proved if

$$N^{(1/4)^{200/\delta}} \geq \frac{(5000)^4}{\delta^8}.$$

This is implied by

$$\Big(\frac{1}{4}\Big)^{\frac{200}{\delta}} \log N \geq 4\log 5000 - 8\log\delta$$
$$\iff \quad -\frac{200}{\delta}\log 4 + \log\log N \geq \log(4\log 5000 - 8\log\delta)$$
$$\iff \quad \log\log N \geq \frac{200}{\delta}\log 4 + \log(4\log 5000 - 8\log\delta)$$
$$\Longleftarrow \quad \log\log N \geq \frac{400}{\delta} + 36 + \frac{8}{\delta}.$$

It suffices to assume $\delta \log\log N \geq 500$, which is of the required form. □

Chapter 3

Quadratic Recurrence

Notation. $e(x)$ means $e^{2\pi ix}$, $\|x\|$ means the distance from x to the nearest integer, $\langle x\rangle$ means the residue class modulo 1 of x that lies in $(-\frac{1}{2},\frac{1}{2}]$. Hence $\|x\| = |\langle x\rangle|$.

In the previous section, we essentially proved the following result: if $\alpha \in \mathbb{R}$ and $k \in \mathbb{N}$ then there exists $d \in \{1, 2, \dots, k\}$ such that

$$|e(\alpha d) - 1| \leq \frac{2\pi}{k}$$

by the pigeonhole principle. Now we shall prove a much deeper result of a similar kind.

Theorem 3.1. For every $\varepsilon > 0$ there exists k such that for every $\alpha \in \mathbb{R}$ there exists $d \in \{1, \dots, k\}$ such that

$$|e(\alpha d^2) - 1| \leq \varepsilon.$$

Proof. By Roth's theorem, there exists k such that any subset $A \subset \{1, \dots, k\}$ of size at least $\varepsilon k/(8\pi)$ contains an arithmetic progression of length 3. See A.3.1.

Partition the unit circle into at most $8\pi/\varepsilon$ sets of diameter at most $\varepsilon/2$. Then there must be a set $A \subset \{1, \dots, k\}$ of density at least $\varepsilon/(8\pi)$ such that, for every $x \in A$, $e\big(\alpha x^2/2\big)$ lies in the same one of these sets. Inside A we can find $x-d, x, x+d$ with $d \neq 0$. Thus, rewriting $e(\alpha d^2)$ as See A.3.2 and A.3.3.

$$\begin{aligned} e(\alpha d^2) &= e\left(\frac{\alpha}{2}\left((x-d)^2 - 2x^2 + (x+d)^2\right)\right) \\ &= e\left(\frac{\alpha(x-d)^2}{2}\right)\overline{e\left(\frac{\alpha x^2}{2}\right)}e\left(\frac{\alpha(x+d)^2}{2}\right)\overline{e\left(\frac{\alpha x^2}{2}\right)}, \end{aligned}$$

we see that this is within $\varepsilon/2 + \varepsilon/2 = \varepsilon$ of 1. □

If one checks, one finds that k can be taken to be $e^{e^{c/\varepsilon}}$. We shall now obtain a much better bound. We shall investigate sums of the form

$$\sum_{x=0}^{k-1} e(\alpha x^2)$$

and derive Weyl's inequality. A useful trick is to look instead at

$$\left|\sum_{x=0}^{k-1} e(\alpha x^2)\right|^2 = \sum_{x=0}^{k-1}\sum_{y=0}^{k-1} e(\alpha(x^2 - y^2)) = \sum_{(u,v)\in W} e(\alpha uv)$$

where $u = x + y$, $v = x - y$. Here, u ranges from 0 to $2(k-1)$. If $u \le k-1$ then the possible pairs (x, y) with $x + y = u$ are $(0, u), (1, u-1), \ldots, (u, 0)$, so possible values of v are $-u, 2-u, 4-u, \ldots, u$, so the first part of the sum has modulus

$$\Big|\sum_{u=0}^{k-1}\sum_{w=0}^{u} e(\alpha u(2w-u))\Big| \le \sum_{u=0}^{k-1}\Big|\sum_{w=0}^{u} e(2\alpha uw)\Big|$$

since $|e(\alpha u^2)| = 1$. If $u \ge k$ then the possible pairs (x, y) are

$$(u-k+1, k-1), (u-k+2, k-2), \ldots, (k-1, u-k+1)$$

so the possible values of v are

$$u - 2(k-1), u - 2(k-2), \ldots, 2(k-1) - u.$$

Thus, the second part of the sum is

$$\sum_{u=k}^{2(k-1)}\sum_{w=0}^{2(k-1)-u} e(\alpha u(u - 2(k-1) + 2w))$$

and its modulus is at most

$$\sum_{u=k}^{2(k-1)}\Big|\sum_{w=0}^{2(k-1)-u} e(2\alpha uw)\Big|.$$

Lemma 3.2. Suppose $\|\alpha\| \ne 0$. Then

$$\Big|\sum_{w=0}^{t-1} e(\alpha w)\Big| \le \frac{1}{2\|\alpha\|}.$$

Proof. Summing a geometric series,

$$\Big|\sum_{w=0}^{t-1} e(\alpha w)\Big| = \Big|\frac{1-e(\alpha t)}{1-e(\alpha)}\Big|.$$

See A.3.4. But $|1 - e(\alpha t)| \le 2$ and $|1 - e(\alpha)| \ge 4\|\alpha\|$. □

Therefore,

$$\Big|\sum_{x=0}^{k-1} e(\alpha x^2)\Big|^2 \le \sum_{u=0}^{2(k-1)} \min\left\{k, \frac{1}{2\|2\alpha u\|}\right\}$$

since we also know that

$$\Big|\sum_{w=0}^{t-1} e(\alpha w)\Big| \le t.$$

Lemma 3.3. Let $\alpha \in \mathbb{R}$ and let p, q be integers with $(p, q) \le 2$ such that

$$\Big|\alpha - \frac{p}{q}\Big| \le \frac{2}{q^2}.$$

Suppose t is an integer with $1 \le t \le q/4$. Then

$$\|\alpha t\| \ge \frac{1}{2q}.$$

Proof. By the triangle inequality and as $tp/q \notin \mathbb{Z}$, See A.3.5.

$$\|\alpha t\| = \left\|\frac{p}{q}t + \left(\alpha - \frac{p}{q}\right)t\right\| \geq \left\|\frac{p}{q}t\right\| - \left\|\left(\alpha - \frac{p}{q}\right)t\right\| \geq \frac{1}{q} - \frac{2}{q^2}\frac{q}{4} = \frac{1}{2q}. \qquad \square$$

Assuming $\alpha \in \mathbb{R}$ and p, q are coprime integers such that $|\alpha - p/q| \leq 1/q^2$ then let us estimate the sum See A.3.6.

$$\sum_{u=v}^{v+\lfloor q/4 \rfloor} \min\left\{k, \frac{1}{2\|2\alpha u\|}\right\}.$$

Now $|2\alpha - 2p/q| \leq 2/q^2$ so 2α satisfies the hypothesis of Lemma 3.3. Therefore, the sum is bounded from above by

$$k + 2q + \frac{2q}{2} + \cdots + \frac{2q}{\lfloor q/4 \rfloor} \leq k + 4q \log q.$$

It follows that, provided $16k \geq q$,

$$\sum_{u=0}^{2(k-1)} \min\left\{k, \frac{1}{2\|2\alpha u\|}\right\} \leq \frac{16k}{q}(k + 4q \log q).$$

This gives us the next result.[1]

Theorem 3.4 (Weyl's Inequality)**.** Let $\alpha \in \mathbb{R}$, let $(p, q) = 1$ and suppose that $|\alpha - p/q| \leq 1/q^2$. Then

$$\left|\sum_{x=0}^{k-1} e(\alpha x^2)\right| \leq \frac{4k}{\sqrt{q}} + 8\sqrt{k \log q}.$$

Now let us tackle Theorem 3.1. So we let $\varepsilon > 0$, and consider $k \in \mathbb{N}$ and $\alpha = a/N$ for integers a, N. We first establish another lemma.

Lemma 3.5. Let $A \subset \mathbb{Z}_N$, $|A| = \alpha$ the density. Let $0 < \varepsilon \leq 1$ and suppose $A \cap [-\varepsilon N, \varepsilon N] = \emptyset$. Then there exists r such that $0 < |r| \leq 8/\varepsilon^2$ and $|\hat{A}(r)| \geq \varepsilon\alpha/16$.

Proof. Let $I = [-\varepsilon N/2, \varepsilon N/2]$. Then if $x, y \in I$ then $x - y \notin A$. It follows that $\langle A, I * -I\rangle = 0$, so $\langle \hat{A}, |\hat{I}|^2\rangle = 0$. Hence See A.3.7 and A.3.8.

$$\sum_{r \neq 0} |\hat{A}(r)||\hat{I}(r)|^2 \geq |\hat{A}(0)||\hat{I}(0)|^2 \geq \frac{\alpha\varepsilon^2}{2}.$$

But if $|\hat{A}(r)| < \varepsilon\alpha/16$ whenever $0 < |r| \leq 8/\varepsilon^2$ then the left-hand side is less than

$$\frac{\varepsilon\alpha}{16}\sum_r |\hat{I}(r)|^2 + \sum_{|r| > 8/\varepsilon^2} \alpha|\hat{I}(r)|^2.$$

But See A.3.9.

$$\sum_r |\hat{I}(r)|^2 = |I| \leq 2\varepsilon$$

so the first term is at most $\alpha\varepsilon^2/8$. Also, See A.3.10.

$$|\hat{I}(r)| \leq \frac{1}{2N\|\frac{r}{N}\|}$$

since $N\hat{I}(r)$ is a sum of a geometric progression with common ratio $e(r/N)$, which is
See A.3.11. equal to $1/2|r|$. Therefore,

$$\sum_{|r|>8/\varepsilon^2} \alpha|\hat{I}(r)|^2 \leq 2\sum_{r>8/\varepsilon^2} \frac{\alpha}{4r^2} \leq 2\Big(\frac{3\alpha\varepsilon^2}{16}\Big) = \frac{3\alpha\varepsilon^2}{8}.$$

But this is a contradiction. □

Now let $A = \{a, 4a, 9a, \ldots, k^2a\} \subset \mathbb{Z}_N$. We would like to prove that $A \cap [-\varepsilon N, \varepsilon N] \neq \emptyset$ unless ε is very small (as a function of k). So suppose $A \cap [-\varepsilon N, \varepsilon N] = \emptyset$. Then

$$\hat{A}(r) = \frac{1}{N}\sum_{x\in A} \omega^{rx} = \frac{1}{N}\sum_{y=1}^{k} \omega^{ary^2} = \frac{1}{N}\sum_{y=1}^{k} e(\alpha ry^2).$$

The previous lemma implies that there exists $r \leq 8/\varepsilon^2$ such that

$$\frac{1}{N}\Big|\sum_{y=1}^{k} e(\alpha ry^2)\Big| \geq \frac{|A|\varepsilon}{16} = \frac{k\varepsilon}{16N}$$

so

$$\Big|\sum_{y=1}^{k} e(\alpha ry^2)\Big| \geq \frac{\varepsilon k}{16}.$$

See A.3.12. Observe that, by the pigeonhole principle on the circle, there exist p and q with $1 \leq q < k$ and $(p, q) = 1$ such that

$$|\alpha r - \frac{p}{q}| \leq \frac{1}{kq}.$$

We now introduce a positive real parameter Q to be determined later, which we use to distinguish two cases. If $q \leq Q$ then

$$|\alpha r^2q^2 - rpq| \leq \frac{rq}{k} \leq \frac{8}{\varepsilon^2}\frac{Q}{k}.$$

If $ar^2q^2 \in A$, which is the case provided $1 \leq rq \leq k$, then from our assumption $A \cap [-\varepsilon N, \varepsilon N] = \emptyset$ we have that

$$\varepsilon \leq \frac{8Q}{\varepsilon^2 k}$$

so $\varepsilon^3 < 8Q/k$. Otherwise, if $rq > k$ then

$$\frac{8q}{\varepsilon^2} \geq rq > k$$

so $\varepsilon^2 < 8Q/k$. Provided $Q \leq k/8$, we conclude from these two bounds that $\varepsilon^3 \leq 8Q/k$.

Now assume $q > Q$. In this case, we shall use Fourier analysis. We would like to apply Weyl's inequality to obtain

$$\Big|\sum_{y=1}^{k} e(\alpha ry^2)\Big| \leq \frac{32k}{Q^{1/2}}.$$

[1] In our later application of Weyl's inequality we will even have $q \leq k$.

For this, it suffices to have

$$\frac{4k}{\sqrt{q}} + 8\sqrt{k \log q} \leq \frac{32k}{Q^{1/2}}$$

which is guaranteed if $Q \leq 12k/\log k$. This gives $\varepsilon/16 \leq 32/Q^{1/2}$, i.e., $\varepsilon \leq 512/Q^{1/2}$. See A.3.13.

Combining our requirements on the parameter Q from both cases

$$\frac{512}{Q^{1/2}} = \frac{2Q^{1/3}}{k^{1/3}}$$

gives $256k^{1/3} = Q^{5/6}$, i.e., $Q = 256^{6/5}k^{2/5}$. Note this also satisfies the requirements $Q \leq k/8$ and $Q \leq 12k/\log k$ for sufficiently large k. So this choice of Q shows that $\varepsilon \leq Ck^{-1/5}$ for some constant C. See A.3.14.

This shows that if $k > C^5\varepsilon^{-5}$ then the intersection $A \cap [-\varepsilon N, \varepsilon N]$ is non-empty. That is, there exists $d \in \{1, \ldots, k\}$ such that $ad^2 \in [-\varepsilon N, \varepsilon N]$ modulo N, so there exists an integer λ such that

$$|ad^2 - \lambda N| \leq \varepsilon N$$

so

$$\|\alpha d^2\| \leq |\alpha d^2 - \lambda| \leq \varepsilon.$$

This proves Theorem 3.1 □

Theorem 3.6. Let q be a function $x \mapsto \alpha x^2 + \beta x + \gamma$ and let $\psi(x) = e(q(x))$. Let P be an arithmetic progression of length m. Then, for all $\varepsilon > 0$, P can be partitioned into arithmetic progressions P_i of length at least $c(\varepsilon)m^{1/40}$, for each of which has $\operatorname{diam} \psi(P_i) \leq \varepsilon$.

Proof. By the previous result we can find $d \leq m^{1/2}$ such that $\|\alpha d^2\| \leq Cm^{-1/10}$.

Now $q(x + rd) - q(x) = \alpha(2rdx + r^2d^2) + \beta rd$ differs modulo 1 from $2\alpha rdx + \beta rd$ by at most $Cr^2m^{-1/10}$. As long as $r \leq c(\varepsilon)^{1/2}C^{-1/2}m^{1/20}$ this is at most $\varepsilon/8\pi$.

Therefore, we can approximate $e(\alpha(2rdx + r^2d^2) + \beta rd) = \psi(x + rd)\overline{\psi(x)}$ by $e(2\alpha rdx + \beta rd)$ with an error of at most $\varepsilon/4$. Partition P into progressions Q_i of common difference d and length at least $C'm^{1/20}$. On each one of these, $\psi(x+rd)\overline{\psi(x)}$ can be approximated to within $\varepsilon/4$ by a function of the form $e(\theta r + \theta')$ and therefore it be partitioned into subprogressions of length at least $C''m^{1/40}$, on which ψ is constant to within ε (see Section 2). □

Chapter 4

Quadratic Uniformity

Lemma 4.1. Let G be a finite Abelian group and let $f\colon G \to \mathbb{C}$. Then

(i) $\|\hat{f}\|_4^4 = \|f * f\|_2^2 = \mathbb{E}_{x,a,b}\, f(x)\overline{f(x+a)f(x+b)}f(x+a+b)$,

(ii) if $\|f\|_\infty \le 1$ then $\|\hat{f}\|_\infty^4 \le \|\hat{f}\|_4^4 \le \|\hat{f}\|_\infty^2$.

Proof. For the first part,

$$\begin{aligned}\|\hat{f}\|_4^4 &= \sum_\psi |\hat{f}(\psi)|^4 = \langle \hat{f}^2, \hat{f}^2\rangle = \langle f*f, f*f\rangle = \|f*f\|_2^2\\ &= \mathbb{E}_x |\mathbb{E}_{y+z=x}\, f(y)f(z)|^2\\ &= \mathbb{E}_{y+z=u+v}\, f(y)f(z)\overline{f(u)f(v)}\\ &= \mathbb{E}_{x,a,b}\, f(x)\overline{f(x+a)f(x+b)}f(x+a+b)\end{aligned}$$

where $y \to x$, $u \to x+a$, $v \to x+b$, $z \to x+a+b$.

For the second part, obviously $\|\hat{f}\|_\infty^4 \le \|\hat{f}\|_4^4$, and also

$$\begin{aligned}\|\hat{f}\|_4^4 &= \sum_\psi |\hat{f}(\psi)|^4 \le \max_\psi |\hat{f}(\psi)|^2 \sum_\psi |\hat{f}(\psi)|^2\\ &= \|\hat{f}\|_\infty^2 \|f\|_2^2 \le \|\hat{f}\|_\infty^2 \|f\|_\infty^2 \le \|\hat{f}\|_\infty^2.\end{aligned}$$

□

For practical purposes, $\|\hat{f}\|_\infty$ and $\|\hat{f}\|_4$ are equivalent.

Lemma 4.2. Let $f\colon G \to \mathbb{C}$, $f(x) = \delta + g(x)$ where δ is a constant and $\mathbb{E}_x\, g(x) = 0$, that is, $\delta = \mathbb{E}_x\, f(x)$. Then

(i)

$$\begin{aligned}&\mathbb{E}_{x,a,b}\, f(x)\overline{f(x+a)f(x+b)}f(x+a+b)\\ &\qquad = |\delta|^4 + \mathbb{E}_{x,a,b}\, g(x)\overline{g(x+a)g(x+b)}g(x+a+b),\end{aligned}$$

(ii)

$$\mathbb{E}_{x,d}\, f(x)f(x+d)f(x+2d) = \delta^3 + \mathbb{E}_{x,d}\, g(x)g(x+d)g(x+2d).$$

Proof. For the first part, the left-hand side is

$$\mathbb{E}_{x,a,b}(\delta + g(x))(\bar{\delta} + \overline{g(x+a)})(\bar{\delta} + \overline{g(x+b)})(\delta + g(x+a+b)),$$

which can be expanded into 16 terms. Two of these terms are $|\delta|^4$ and $\mathbb{E}_{x,a,b}\, g(x)\overline{g(x+a)g(x+b)}g(x+a+b)$ and all the others are zero. For example,

$$\mathbb{E}_{x,a,b}\, g(x)\bar{\delta}\overline{g(x+a)}g(x+a+b) = \mathbb{E}_{x,y,z}\, g(x)\bar{\delta}\overline{g(y)}g(z) = 0.$$

For the second part, the argument is similar. □

Proposition 4.3. Let G be a finite Abelian group of odd order, and let $A \subset G$, $|A| = \delta$. Suppose that

$$\mathbb{E}_{x,a,b}\, A(x)A(x+a)A(x+b)A(x+a+b) \leq \delta^4 + c.$$

Then

$$|\mathbb{E}_{x,d}\, A(x)A(x+d)A(x+2d) - \delta^3| \leq c^{1/2}.$$

Proof. Let $A(x) = \delta + g(x)$. Then the left-hand side of the first inequality equals $\delta^4 + \|g*g\|_2^2$ by the previous two lemmas. The left-hand side of the second inequality is

$$|\mathbb{E}_{x,d}\, g(x)g(x+d)g(x+2d)| = \langle g*g, g_2\rangle \leq \|g*g\|_2\|g_2\|_2 \leq \|g*g\|_2. \qquad \square$$

Definition. Let X, Y and Z be finite sets and let $f\colon X\times Y\times Z \to \mathbb{C}$. Then we define $\|f\|_{U_3}$ by

$$\|f\|_{U_3}^8 = \mathbb{E}_{x,x'}\, \mathbb{E}_{y,y'}\, \mathbb{E}_{z,z'}\, f(x,y,z)\overline{f(x,y,z')}\cdots\overline{f(x',y',z')}.$$

We also define

$$[f_0,f_1,\dots,f_7] = \mathbb{E}_{x,x',y,y',z,z'}\, f_0(x,y,z)\overline{f_1(x,y,z')}\cdots\overline{f_7(x',y',z')}.$$

Proposition 4.4. Let X, Y, Z be finite sets, and let $f_0,\dots,f_7$ be functions from $X\times Y\times Z$ to $\mathbb{C}$. Then

$$[f_0,\dots,f_7] \leq \|f_0\|_{U_3}\cdots\|f_7\|_{U_3}.$$

Proof. We use the Cauchy–Schwarz inequality to transform the left-hand side,

$$\begin{aligned}
&\mathbb{E}_{x,x'}\, \mathbb{E}_{y,y'}\, \mathbb{E}_{z,z'}\, f_0(x,y,z)\overline{f_1(x,y,z')f_2(x,y',z)}f_3(x,y',z')\\
&\qquad\qquad \overline{f_4(x',y,z)}f_5(x',y,z')f_6(x',y',z)\overline{f_7(x',y',z')}\\
&\leq \Big(\mathbb{E}_{y,y'}\, \mathbb{E}_{z,z'}|\mathbb{E}_x\, f_0(x,y,z)\overline{f_1(x,y,z')f_2(x,y',z)}f_3(x,y',z')|^2\Big)^{1/2}\\
&\quad\times\Big(\mathbb{E}_{y,y'}\, \mathbb{E}_{z,z'}|\mathbb{E}_{x'}\, f_4(x',y,z)\overline{f_5(x',y,z')f_6(x',y',z)}f_7(x',y',z')|^2\Big)^{1/2}\\
&= [f_0,f_1,f_2,f_3,f_0,f_1,f_2,f_3]^{1/2}[f_4,f_5,f_6,f_7,f_4,f_5,f_6,f_7]^{1/2}.
\end{aligned}$$

Applying the same argument to the y and z variables we end up with the result stated. □

Corollary 4.5. $\|\cdot\|_{U_3}$ is a norm on $\mathbb{C}^{X\times Y\times Z}$.

Proof. Let $f_0, f_1\colon X\times Y\times Z\to\mathbb{C}$. Then

$$\begin{aligned}
\|f_0+f_1\|_{U_3}^8 &= [f_0+f_1,\dots,f_0+f_1]\\
&= \sum_{\epsilon\in\{0,1\}^8}[f_{\epsilon_0},\dots,f_{\epsilon_7}]\\
&\leq \sum_{\epsilon\in\{0,1\}^8}\|f_{\epsilon_0}\|_{U_3}\cdots\|f_{\epsilon_7}\|_{U_3}\\
&= \left(\|f_0\|_{U_3}+\|f_1\|_{U_3}\right)^8.
\end{aligned}$$

□

Definition. Let G be a finite group and let $f\colon G \to \mathbb{C}$. Then

$$\|f\|_{U_3}^8 = \mathbb{E}_{x,a,b,c}\, f(x)\overline{f(x+a)f(x+b)}f(x+a+b) \\ \overline{f(x+c)}f(x+a+c)f(x+b+c)\overline{f(x+a+b+c)}.$$

Lemma 4.6. Let a, b, c be integers and let G be a group such that the order of every $g \in G$ is coprime to all of a, b, c. Let $f\colon G \to \mathbb{C}$ and define $F\colon G^3 \to \mathbb{C}$ by

$$F(x, y, z) = f(ax + by + cz).$$

Then $\|F\|_{U_3} = \|f\|_{U_3}$.

Proof.

$$\|F\|_{U_3}^8 = \mathbb{E}_{x,x',y,y',z,z'}\, f(ax+by+cz)\overline{f(ax+by+cz')f(ax+by'+cz)} \\ f(ax+by'+cz')\overline{f(ax'+by+cz)}f(ax'+by+cz') \\ f(ax'+by'+cz)\overline{f(ax'+by'+cz')}.$$

Now substitute $ax + by + cz \to X$, $a(x' - x) \to A$, $b(y' - y) \to B$, $c(z' - z) \to C$. Then this becomes

$$\mathbb{E}_{X,A,B,C}\, f(X)\overline{f(X+C)f(X+B)}f(X+B+C) \\ \overline{f(X+A)}f(X+A+C)f(X+A+B)\overline{f(X+A+B+C)}.$$

It is not hard to check that the map $(x, x', y, y', z, z') \mapsto (X, A, B, C)$ is $|G|^2$ to 1. □

Corollary 4.7. $\|\cdot\|_{U_3}$ is a norm on $\mathbb{C}^G$.

Proof. Let $f, g\colon G \to \mathbb{C}$. Let $F, G\colon G^3 \to \mathbb{C}$ be defined by $F(x, y, z) = f(x + y + z)$, $G(x, y, z) = g(x + y + z)$. Then $(F + G)(x, y, z) = (f + g)(x + y + z)$. So

$$\|f + g\|_{U_3} = \|F + G\|_{U_3} \leq \|F\|_{U_3} + \|G\|_{U_3} = \|f\|_{U_3} + \|g\|_{U_3}.$$ □

Lemma 4.8. Let X, Y, Z and W be finite sets, and let $f\colon X \times Y \times Z \to \mathbb{C}$, $g\colon X \times Y \times W \to \mathbb{C}$, $h\colon X \times Z \times W \to \mathbb{C}$ and $k\colon Y \times Z \times W \to \mathbb{C}$ be functions. Suppose that $\|f\|_\infty, \|g\|_\infty, \|h\|_\infty, \|k\|_\infty \leq 1$. Then

$$|\mathbb{E}_{x,y,z,w}\, f(x, y, z)g(x, y, w)h(x, z, w)k(y, z, w)| \\ \leq \min\{\|f\|_{U_3}, \|g\|_{U_3}, \|h\|_{U_3}, \|k\|_{U_3}\}.$$

Proof. We repeatedly apply the Cauchy–Schwarz inequality,

$$\begin{aligned} LHS^8 &= |\mathbb{E}_{y,z,w}\, k(y, z, w)\, \mathbb{E}_x\, f(x, y, z)g(x, y, w)h(x, z, w)|^8 \\ &\leq \left(\left(\mathbb{E}_{y,z,w}|k(y, z, w)|^2\right)\left(\mathbb{E}_{y,z,w}|\mathbb{E}_x\, f(x, y, z)g(x, y, w)h(x, z, w)|^2\right)\right)^4 \\ &\leq \left(\mathbb{E}_{x,x'}\, \mathbb{E}_{y,z,w}\, f_{x,x'}(y, z)g_{x,x'}(y, w)h_{x,x'}(z, w)\right)^4 \end{aligned}$$

where $f_{x,x'}(y, z)$ is shorthand for $f(x, y, z)\overline{f(x', y, z)}$ etc.

$$\leq \mathbb{E}_{x,x'}|\mathbb{E}_{y,z,w}\, f_{x,x'}(y, z)g_{x,x'}(y, w)h_{x,x'}(z, w)|^4$$

$$\leq \mathbb{E}_{x,x'} \left(\mathbb{E}_{z,w} |\mathbb{E}_y f_{x,x'}(y,z) g_{x,x'}(y,w)|^2\right)^2$$
$$= \mathbb{E}_{x,x'} \left(\mathbb{E}_{y,y'} \mathbb{E}_{z,w} f_{x,x',y,y'}(z) g_{x,x',y,y'}(w)\right)^2$$

where $f_{x,x',y,y'}(z) = f_{x,x'}(y,z)\overline{f_{x,x'}(y',z)}$,

$$\leq \mathbb{E}_{x,x',y,y'} |\mathbb{E}_{z,w} f_{x,x',y,y'}(z) g_{x,x',y,y'}(w)|^2$$
$$\leq \mathbb{E}_{x,x',y,y'} \mathbb{E}_w |\mathbb{E}_z f_{x,x',y,y'}(z)|^2$$
$$= \|f\|_{U_3}^8.$$

The same works for the other three functions, so the result is proved. □

Corollary 4.9. Let G be a group such that no element has order divisible by 2 or 3. Let $f, g, h, k \colon G \to \mathbb{C}$ with $\|f\|_\infty, \|g\|_\infty, \|h\|_\infty, \|k\|_\infty \leq 1$. Then

$$|\mathbb{E}_{x,d} f(x) g(x+d) h(x+2d) k(x+3d)| \leq \min\{\|f\|_{U_3}, \|g\|_{U_3}, \|h\|_{U_3}, \|k\|_{U_3}\}.$$

Proof. The left-hand side can be written as

$$|\mathbb{E}_{x,y,z,w} f(-y-2z-3w) g(x-z-2w) h(2x+y-w) k(3x+2y+z)|$$

By Lemma 4.8 and Lemma 4.6, this is at most

$$\min\{\|f\|_{U_3}, \|g\|_{U_3}, \|h\|_{U_3}, \|k\|_{U_3}\}$$

as claimed. □

Definition. Let G be a finite Abelian group and let $f \colon G \to \mathbb{C}$ be a function with $\|f\|_\infty \leq 1$. Then f is *c-quadratically uniform* if $\|f\|_{U_3}^8 \leq c$. Let $A \subset G$ be a subset of density δ. Then A is *c-quadratically uniform* if the function $f_A = A - \delta$ is c-quadratically uniform.

Corollary 4.10. Let $A, B, C, D \subset G$, where G is a group with no elements of order 2 or 3, be sets of density $\alpha, \beta, \gamma, \delta$, respectively. Suppose that A and B are c-quadratically uniform. Then

$$\mathbb{E}_{x,d} A(x) B(x+d) C(x+2d) D(x+3d) \geq \alpha\beta\gamma\delta - 5c^{1/8}.$$

Proof. The left-hand side can be written as

$$\mathbb{E}_{x,d} (\alpha + f_A(x))(\beta + f_B(x+d))(\gamma + f_C(x+2d))(\delta + f_D(x+3d)).$$

There are 16 terms. The main term is $\alpha\beta\gamma\delta$. Any other term is zero unless you choose f from at least 3 brackets. These terms involve either f_A or f_B, and therefore, by Corollary 4.9, each have magnitude at most $c^{1/8}$. There are 5 such terms. □

Chapter 5

Functions and Sets that are not Quadratically Uniform

Notation. Let $f\colon G \to \mathbb{C}$ and let $k \in G$. Then define

$$\Delta(f;k)\colon G \to \mathbb{C}, x \mapsto f(x)\overline{f(x-k)}.$$

Proposition 5.1. Let $f\colon G \to \mathbb{C}$ be a function such that $\|f\|_\infty \leq 1$. Then the following are equivalent.

(i) f is not c_1-quadratically uniform.
(ii) $\mathbb{E}_{k\in G}\sum_{\psi\in\hat{G}}\left|\Delta(f;k)\hat{}(\psi)\right|^4 > c_1$.
(iii) $\mathbb{E}_{k\in G}\max_{\psi\in\hat{G}}\left|\Delta(f;k)\hat{}(\psi)\right|^2 > c_2$.
(iv) There exist $B \subset G$ with $|B| > c_3$ and $\psi\colon B \to \hat{G}$ such that

$$\left|\Delta(f;k)\hat{}(\psi(k))\right|^2 > c_3$$

for every $k \in B$.

Proof. We have that

$$\begin{aligned}\|f\|_{U_3}^8 &= \mathbb{E}_{x,k,a,b} f(x)\overline{f(x+a)f(x+b)}f(x+a+b)\\ &\qquad \overline{f(x-k)}f(x-k+a)f(x-k+b)\overline{f(x-k+a+b)}\\ &= \mathbb{E}_{x,k,a,b}\Delta(f;k)(x)\overline{\Delta(f;k)(x+a)\Delta(f;k)(x+b)}\Delta(f;k)(x+a+b)\\ &= \mathbb{E}_k\|\Delta(f;k)\hat{}\|_4^4\\ &= \mathbb{E}_k\sum_\psi\left|\Delta(f;k)\hat{}(\psi)\right|^4\end{aligned}$$

using Lemma 4.1. Thus (i) $\iff$ (ii).

Also,

$$\begin{aligned}\mathbb{E}_k\sum_\psi\left|\Delta(f;k)\hat{}(\psi)\right|^4 &\leq \mathbb{E}_k\max_\psi\left|\Delta(f;k)\hat{}(\psi)\right|^2\sum_\psi\left|\Delta(f;k)\hat{}(\psi)\right|^2\\ &\leq \mathbb{E}_k\max_\psi\left|\Delta(f;k)\hat{}(\psi)\right|^2\end{aligned}$$

since $\|\Delta(f;k)\|_2^2 \leq 1$. Thus, (ii) implies (iii) with $c_2 = c_1$.

If (iii) holds then there must be a set B of density greater than $c_2/2$ such that $\max_\psi|\Delta(f;k)\hat{}(\psi)|^2 > c_2/2$ for every $k \in B$. For each $k \in B$, let $\psi(k)$ be a ψ where the maximum is attained.

If (iv) holds then

$$\mathbb{E}_{k\in G}\sum_{\psi\in\hat{G}}\big|\Delta(f;k)\hat{}(\psi)\big|^4 \geq \mathbb{E}_{k\in G}\,B(k)\big|\Delta(f;k)\hat{}(\psi(k))\big|^4 > c_3^3. \qquad \square$$

Lemma 5.2. Let $\lambda\colon G\times\hat{G}\to\mathbb{C}$ be a function. Let $f\colon G\to\mathbb{C}$ be a function such that $\|f\|_\infty\leq 1$. Then

$$\Big|\mathbb{E}_{k\in G}\sum_{\psi\in\hat{G}}\lambda(k,\psi)\big|\Delta(f;k)\hat{}(\psi)\big|^2\Big|^4 \leq \|\lambda\|_{U_2}^4$$

where $\|\lambda\|_{U_2}^4$ means

$$\mathbb{E}_{k_1+k_2=k_3+k_4}\sum_{\psi_1+\psi_2=\psi_3+\psi_4}\lambda(k_1,\psi_1)\lambda(k_2,\psi_2)\overline{\lambda(k_3,\psi_3)\lambda(k_4,\psi_4)}.$$

In particular, if $B\subset G$ and $\psi\colon B\to\hat{G}$ is such that

$$\mathbb{E}_k\,B(k)\big|\Delta(f;k)\hat{}(\psi(k))\big|^2\geq c$$

then there are at least $c^4|G|^3$ quadruples $k_1+k_2=k_3+k_4$ in B such that $\psi(k_1)+\psi(k_2)=\psi(k_3)+\psi(k_4)$. This follows from applying the lemma to

$$\lambda(k,\psi)=\begin{cases}1 & k\in B,\ \psi=\psi(k)\\ 0 & \text{otherwise}\end{cases}.$$

Proof. The left-hand side can be written as

$$\begin{aligned}
&\Big|\mathbb{E}_k\sum_\psi\lambda(k,\psi)|\mathbb{E}_{x,y}\,f(x)\overline{f(x-k)f(y)}f(y-k)\psi(x-y)|\Big|^4\\
&=\Big|\mathbb{E}_k\sum_\psi\lambda(k,\psi)\,\mathbb{E}_{x,u}\,f(x)\overline{f(x-k)f(x-u)}f(x-u-k)\psi(u)\Big|^4\\
&=\Big|\mathbb{E}_{u,x}\,f(x)\overline{f(x-u)}\,\mathbb{E}_k\,\overline{f(x-k)}f(x-u-k)\sum_\psi\lambda(k,\psi)\psi(u)\Big|^4\\
&\leq\left(\mathbb{E}_u\,\mathbb{E}_x\Big|\mathbb{E}_k\,\overline{f(x-k)}f(x-u-k)\sum_\psi\lambda(k,\psi)\psi(u)\Big|^2\right)^2
\end{aligned}$$

by Cauchy–Schwarz and $\|f\|_\infty\leq 1$. Let $f_u(s)=\overline{f(s)}f(s-u)$, $g_u(s)=\sum_\psi\lambda(s,\psi)\psi(u)$. Then this is

$$\begin{aligned}
&=\left(\mathbb{E}_u\,\mathbb{E}_x\Big|\mathbb{E}_k\,f_u(x-k)g_u(k)\Big|^2\right)^2\\
&=\big(\mathbb{E}_u\,\mathbb{E}_x|f_u*g_u(x)|^2\big)^2\\
&=\left(\mathbb{E}_u\sum_\phi|\hat{f}_u(\phi)|^2|\hat{g}_u(\phi)|^2\right)^2
\end{aligned}$$

by Parseval and the convolution identity

$$\leq \left(\mathbb{E}_u\Big(\sum_\phi |\hat{f}_u(\phi)|^4\Big)^{1/2}\Big(\sum_\phi |\hat{g}_u(\phi)|^4\Big)^{1/2}\right)^2$$

using Cauchy–Schwarz. But $\sum_\phi |\hat{f}_u(\phi)|^4 = \|f_u\|_{U_2}^4 \leq \|f\|_\infty^4 \leq 1$, so this is at most

$$\begin{aligned}
&\leq \left(\mathbb{E}_u\Big(\sum_\phi |\hat{g}_u(\phi)|^4\Big)^{1/2}\right)^2\\
&\leq \mathbb{E}_u \sum_\phi |\hat{g}_u(\phi)|^4\\
&= \mathbb{E}_u \|g_u\|_{U_2}^4\\
&= \mathbb{E}_u\, \mathbb{E}_{x_1+x_2=x_3+x_4} \sum_{\psi_1,\psi_2,\psi_3,\psi 4} \lambda(x_1,\psi_1)\lambda(x_2,\psi_2)\overline{\lambda(x_3,\psi_3)\lambda(x_4,\psi_4)}\\
&\qquad\qquad \times \psi_1(u)\psi_2(u)\overline{\psi_3(u)\psi_4(u)}\\
&= \mathbb{E}_{x_1+x_2=x_3+x_4} \sum_{\psi_1\psi_2=\psi_3\psi_4} \lambda(x_1,\psi_1)\lambda(x_2,\psi_2)\overline{\lambda(x_3,\psi_3)\lambda(x_4,\psi_4)}.
\end{aligned}$$

□

This makes us interested in the following question. Let G be a finite Abelian group, $B < G$, $|B| = \beta$, $\psi\colon B \to H$, where H is some other Abelian group, and suppose there are at least $c|G|^3$ quadruples $(x,y,z,w) \in B^4$ such that $x+y = z+w$ and $\psi(x)+\psi(y) = \psi(z)+\psi(w)$. What can we say about ψ? Our main case of interest will be $G = H = \mathbb{Z}_N$.

Lemma 5.3. Let G be a bipartite graph with finite vertex sets X, Y and density δ. Then X has a subset X' of density at least $\frac{1}{2}\delta^5$ such that at least $\frac{15}{16}|X'|^2$ pairs $(x,x') \in X'\times X'$ have neighbourhoods that intersect in a set of density at least $\frac{1}{2}\delta^2$.

Proof. Let us write $d(x)$ for the density of the neighbourhood $\Gamma(x)$ of x and $d(x,x')$ for the density of $\Gamma(x)\cap\Gamma(x')$. Let $y_1,\dots,y_5$ be chosen independently at random from Y and set

$$X' = \Gamma(y_1)\cap\cdots\cap\Gamma(y_5) = \{x : xy_i \text{ is an edge for } i = 1,\dots,5\}.$$

Note for all $x \in X$ we have $\mathbb{P}(x \in X') = d(x)^5$, and for each $(x,x') \in X\times X$ the probability that $(x,x') \in X'\times X'$ is $d(x,x')^5$. So the expected density of X' is $\mathbb{E}_x\, d(x)^5$ and so the expectation of the square of the density of X' is at least

$$\big(\mathbb{E}_x\, d(x)^5\big)^2 \geq (\mathbb{E}_x\, d(x))^{10} = \delta^{10}$$

by Hölder's inequality.

Call a pair $(x,x') \in X\times X$ *bad* if $d(x,x') < \frac{1}{2}\delta^2$. Let (x,x') be a bad pair. Then

$$\mathbb{P}[(x,x') \in X'\times X'] < \frac{1}{32}\delta^{10}.$$

So the expected density of bad pairs in $X'\times X'$, i.e., the number of bad pairs in $X'\times X'$ divided by $|X|^2$, is less than $\frac{1}{32}\delta^{10}$. Therefore,

$$\mathbb{E}\left[|X'|^2 - 16\times(\text{bad pair in } X'\times X' \text{ density})\right] \geq \delta^{10} - \frac{\delta^{10}}{2} = \frac{\delta^{10}}{2}.$$

In particular, there exist a choice of $y_1, \dots, y_5$ such that the proportion of bad pairs in $X' \times X'$ is at most $\frac{1}{16}$ and $|X'|^2 \geq \frac{1}{2}\delta^{10}$, hence $|X'| \geq \frac{1}{2}\delta^5$. □

Definition. Let G be a bipartite graph with finite vertex sets X and Y, let m be an even integer, and let $x, x' \in X$. Then the *path density* $d_m(x, x')$ is the number of paths in G of length m from x to x' divided by $|X|^{m/2-1}|Y|^{m/2}$.

Equivalently, it is the probability that $xy_1x_2y_2 \dots y_{m/2}x'$ is a path in G if $x_2, \dots, x_{m/2}$, $y_1, \dots, y_{m/2}$ are chosen randomly.

Corollary 5.4. Let G be a bipartite graph with finite vertex sets X and Y and density δ. Then X has a subset X'' of density at least $\frac{1}{4}\delta^5$ such that $d_4(x, x') \geq \frac{1}{16}\delta^9$ for every $x, x' \in X''$.

Proof. Let X' be given by Lemma 5.3. So $|X'| \geq \frac{1}{2}\delta^5$ and $d_2(x, x') \geq \frac{1}{2}\delta^2$ for at least $\frac{15}{16}|X'|^2$ pairs in $X' \times X'$.

Define a graph H with vertex set X' by joining x to x' if $d_2(x, x') \geq \frac{1}{2}\delta^2$. Then the average degree is at least $\frac{15}{16}|X'|$.

So at least half the vertices have degree at least $\frac{7}{8}|X'|$. Let X'' be the set of all such vertices. If $x, x' \in X''$ then there must be at least $\frac{3}{4}|X'|$ vertices z such that $d_2(x, z) \geq \frac{1}{2}\delta^2$ and $d_2(z, x') \geq \frac{1}{2}\delta^2$. This implies that $d_4(x, x') \geq \frac{3}{4}\frac{1}{2}\delta^5\frac{1}{2}\delta^2\frac{1}{2}\delta^2 \geq \frac{1}{16}\delta^9$. □

Theorem 5.5 (Balog–Szemerédi)**.** Let Γ be an Abelian group and let A be a finite subset of Γ. Let $|A| = n$, and suppose A^4 contains at least cn^3 quadruples (a, b, c, d) such that $a - b = c - d$. Then there is a subset $B \subset A$ of cardinality at least $c'n$ such that $|B - B| \leq Cn$. Here, c' and C depend only on c and $B - B = \{x - y : x, y \in B\}$.

Proof. For each $x \in \Gamma$ let $f(x)$ be the number of ways of writing x as $a - b$ with $a, b \in A$, i.e., $f(x)$ is proportional to $A * (-A)(x)$. Then $f(x) \geq \frac{1}{2}cn$ for at least $\frac{1}{2}cn$ values of x, since, by hypothesis,

$$\sum_x f(x)^2 \geq cn^3$$

and otherwise we would have

$$\sum_x f(x)^2 < \max_x f(x)^2 \cdot \frac{cn}{2} + \frac{cn}{2}\sum_x f(x) \leq \frac{cn^3}{2} + \frac{cn^3}{2} = cn^3.$$

Define a bipartite graph G with vertex sets A and A, by joining a to b if $f(b-a) \geq \frac{1}{2}cn$. We call this the *popular difference graph*. Then the number of edges in G is at least $\frac{1}{4}c^2n^2$, so G has density at least $\frac{1}{4}c^2$.

By Corollary 5.4 we can find $B \subset A$ such that $d_4(x, x') \geq \frac{1}{2^{22}}c^{18}$ for every $x, x' \in B$ and $|B| \geq \frac{c^{10}}{2^{12}}|A|$.

Let $x \in B - B$. Then we can write $x = b_1 - b_2$ with $b_1, b_2 \in B$. But $d_4(b_1, b_2) \geq \frac{1}{2^{22}}c^{18}$, so the number of triples u_1, u_2, u_3 such that

$$d_2(b_1, u_1), d_2(u_1, u_2), d_2(u_2, u_3), d_2(u_3, b_2) \geq \frac{c}{2}$$

is at least $\frac{1}{2^{22}}c^{18}n^3$. For each choice of u_1, u_2, u_3 there are at least $\left(\frac{1}{2}cn\right)^4$ ways of writing $b_1 - u_1 = a_1 - a_2$, $u_1 - u_2 = a_3 - a_4$, $u_2 - u_3 = a_5 - a_6$, $u_3 - b_2 = a_7 - a_8$

with $a_1, \dots, a_8 \in A$. This gives us $\frac{1}{2^{22}} c^{18} n^3 \left(\frac{1}{2} cn\right)^4 = \frac{1}{2^{26}} c^{22} n^7$ distinct ways of writing $x = a_1 - a_2 + a_3 - a_4 + a_5 - a_6 + a_7 - a_8$ with $a_1, \dots, a_8 \in A$.

Different $x \in B - B$ must produce different $(a_1, \dots, a_8)$ so

$$|B - B| \frac{1}{2^{26}} c^{22} n^7 \leq n^8$$

and hence

$$|B - B| \leq 2^{26} c^{-22} n.$$

Note we have found $|B| \geq \frac{1}{2^{12}} c^{10} n$. □

Lemma 5.6 (Ruzsa Triangle Inequality)**.** Let U, V, W be finite subsets of an Abelian group. Then

$$|U||V - W| \leq |U - V||U - W|.$$

Proof. Define functions $v \colon V - W \to V$ and $w \colon V - W \to W$ in such a way that $v(x) - w(x) = x$ for every $x \in V - W$. Then define a function $\phi \colon U \times (V - W) \to (U - V) \times (U - W)$ by $\phi \colon (u, x) \mapsto (u - v(x), u - w(x))$. This is an injection since

$$(u - w(x)) - (u - v(x)) = v(x) - w(x) = x$$

so we can recover x, and hence $v(x)$ and $w(x)$, and hence u, all from $(u - v(x), u - w(x)) = \phi(u, x)$. □

Lemma 5.7. Let Γ be an Abelian group and let A be a finite subset such that $|A - A| \leq C|A|$. Then $|2A - 2A| \leq 8C^6|A|$.

It is known that $|kA - lA| \leq C^{k+l}|A|$.

Proof. Let $f(x)$ be the number of ways of writing $x = a - b$ with $a, b \in A$, which is proportional to $A * -A(x)$. Then

$$f(x) \geq \frac{|A|}{2C}$$

for at least $|A|/2$ values of x, or else we would have

$$|A|^2 = \sum_{x \in \Gamma} f(x) < \frac{|A|}{2} \max_{x \in \Gamma} f(x) + |A - A| \frac{|A|}{2C} \leq \frac{|A|}{2} |A| + C|A| \frac{|A|}{2C} = |A|^2,$$

contradiction. Let

$$S = \left\{ x : f(x) \geq \frac{|A|}{2C} \right\}.$$

We claim that

$$|A - A + S| \leq 2C^3 |A|.$$

To show this, we shall define a (multi-valued) map from $A - A + S$ to $(A - A) \times (A - A)$ as follows. For each $x = a_1 - a_2 + s$, we can write s as $a_3 - a_4$ in at least $|A|/2C$ ways, and send it to $(a_1 - a_4, a_2 - a_3)$. Each of those images of x is distinct, and from it we can recover $x = (a_1 - a_4) - (a_2 - a_3)$. It follows that

$$\frac{|A|}{2C} |A - A + S| \leq |A - A|^2 \leq C^2 |A|^2$$

which proves the claim.

By the Ruzsa triangle inequality,

$$|S||2A - 2A| \le |A - A + S|^2$$

since this is

$$|S||(A - A) - (A - A)| \le |S - (A - A)||S - (A - A)|.$$

Thus

$$|2A - 2A| \le \frac{4C^6|A|^2}{|A|/2} = 8C^6|A|. \qquad \square$$

Definition. Let A be a subset of an Abelian group and let B be another one. A function $\phi\colon A \to B$ is a *(Freiman) homomorphism of order k* if

$$\begin{aligned} & x_1 + \cdots + x_k = y_1 + \cdots + y_k \\ \implies \quad & \phi(x_1) + \cdots + \phi(x_k) = \phi(y_1) + \cdots + \phi(y_k). \end{aligned}$$

It is an *isomorphism* if it is a bijective homomorphism and the above implication can be reversed.

Lemma 5.8. If ϕ is a Freiman homomorphism from a set A to a set B then ϕ induces a well-defined map $\psi\colon A - A \to B - B$ with formula $\psi(x - y) = \phi(x) - \phi(y)$. More generally, if ϕ is a homomorphism of order $2k$ then we can define $\psi\colon kA - kA \to kB - kB$ by

$$\psi(x_1 + \cdots + x_k - y_1 - \cdots - y_k) = \phi(x_1) + \cdots + \phi(x_k) - \phi(y_1) - \cdots - \phi(y_k).$$

Also, a homomorphism of order $2k$ on A induces a homomorphism of order k on $A - A$.

Proof. These statements are all easy exercises. We prove the third one. If $\phi\colon A \to B$ is a homomorphism of order $2k$ and we define $\psi\colon A - A \to B - B$ by $\psi(x - y) = \phi(x) - \phi(y)$ then

$$\begin{aligned} & x_1 - y_1 + \cdots + x_k - y_k = u_1 - v_1 + \cdots + u_k - v_k \\ \implies \quad & x_1 + \cdots + x_k + v_1 + \cdots + v_k = y_1 + \cdots + y_k + u_1 + \cdots + u_k \\ \implies \quad & \phi(x_1) + \cdots + \phi(x_k) + \phi(v_1) + \cdots + \phi(v_k) \\ & \qquad = \phi(y_1) + \cdots + \phi(y_k) + \phi(u_1) + \cdots + \phi(u_k) \\ \implies \quad & \psi(x_1 - y_1) + \cdots + \psi(x_k - y_k) = \psi(u_1 - v_1) + \cdots + \psi(u_k - v_k). \end{aligned} \qquad \square$$

Lemma 5.9. Let $A \subset G$, $|A - A| \le C|A|$. Then

$$|9A - 8A| \le 2^{24}C^{48}|A|.$$

Proof. By Ruzsa's triangle inequality,

$$\begin{aligned} |A||(2^k + 1)A - (2^k + 1)A| &= |A|\big|\big((2^{k-1} + 1)A - 2^{k-1}A\big) \\ &\qquad - \big((2^{k-1} + 1)A - 2^{k-1}A\big)\big| \\ &\le |(2^{k-1} + 1)A - (2^{k-1} + 1)A|^2 \end{aligned}$$

if $k \geq 1$. Therefore,

$$\frac{|9A - 9A|}{|A|} \leq \left(\frac{|2A - 2A|}{|A|}\right)^8 \leq (8C^6)^8$$

by Lemma 5.7. Therefore,

$$|9A - 8A| \leq (8C^6)^8 |A|,$$

as in general $|A + B| \geq |A|$. □

Lemma 5.10. Let B be a subset of $\mathbb{Z}_N$ and let $\phi\colon B \to \hat{\mathbb{Z}}_N$. Let Γ be the graph of ϕ. Suppose that $|9\Gamma - 8\Gamma| \leq K|\Gamma|$, viewing Γ as a group with $(x, \phi(x)) - (y, \phi(y)) = (x - y, \phi(x) - \phi(y))$. Then there is a subset $B' \subset B$ of cardinality at least $|B|/16K$ such that the restriction of ϕ to B' is a Freiman homomorphism of order 8.

Proof. Let $B' \subset B$. If the result is false for B', then we can find $x_1, \ldots, x_8$ and $y_1, \ldots, y_8$ in B' such that

$$x_1 + \cdots + x_8 = y_1 + \cdots + y_8$$

but

$$\phi(x_1) + \cdots + \phi(x_8) \neq \phi(y_1) + \cdots + \phi(y_8).$$

Let Y be the set of all $\phi(x_1) + \cdots + \phi(x_8) - \phi(y_1) - \cdots - \phi(y_8)$ such that $x_1, \ldots, x_8$ and $y_1, \ldots, y_8$ are in B and satisfy

$$x_1 + \cdots + x_8 = y_1 + \cdots + y_8.$$

Then $\{0\} \times Y \subset 8\Gamma - 8\Gamma$. Therefore,

$$\Gamma + (\{0\} \times Y) \subset 9\Gamma - 8\Gamma.$$

But

$$|\Gamma + (\{0\} \times Y)| = |\Gamma||Y|$$

and

$$|9\Gamma - 8\Gamma| \leq K|\Gamma|$$

so $|Y| \leq K$.

Let $P = \{1, \ldots, m\}$, and let $r \neq 0$ and s be random elements of $\mathbb{Z}_N$. Choose B' randomly to be

$$\{x \in B : \phi(x) \in r \cdot P + s\}$$

where

$$r \cdot P + s = \{r + s, 2r + s, \ldots, mr + s\}.$$

If $8(r \cdot P + s) - 8(r \cdot P + s) \cap Y = \{0\}$ then $\phi|_{B'}$ is a homomorphism of order 8. But

$$8(r \cdot P + s) - 8(r \cdot P + s) = 8r \cdot P - 8r \cdot P \subset Y \cap [-8(m-1), 8(m-1)]$$

so each non-zero element of Y has probability at most

$$\frac{16(m-1)}{N-1} \leq \frac{16m}{N}.$$

Therefore, as long as $16m(|Y|-1)/N < 1$ the intersection is $\{0\}$ with positive probability. So choose $m = \lceil N/16K \rceil$, and pick r such that the intersection is $\{0\}$. Now choose s such that

$$|B'| \geq |B| \cdot \frac{m}{N} \geq \frac{|B|}{16K}$$

which is possible by an easy averaging argument. □

Chapter 6

Bohr Neighbourhoods

Let G be a finite Abelian group. Let $\psi_1, \dots, \psi_k$ be characters, let $K = \{\psi_1, \dots, \psi_k\}$ and let $\delta > 0$. The *Bohr set* $B(K, \delta)$ is defined to be

$$\{x \in G : |\psi_i(x) - 1| \leq \delta \text{ for } i = 1, \dots, k\}.$$

We call k the *dimension* of the Bohr set and δ is the *radius*.

Lemma 6.1. The density of $B(K, \delta)$ is at least $(\delta/2\pi)^k$.

Proof. Let $\Pi = \{z \in \mathbb{C} : |z| = 1\}$. Pick $z = (e^{i\theta_1}, \dots, e^{i\theta_k})$ at random in Π^k and look at

$$U_z = \{x \in G : \theta_i \leq \arg \psi_i(x) < \theta_i + \delta \text{ for all } i\}.$$

Then the probability that $x \in U_z$ is $(\delta/2\pi)^k$ so we can find z such that U_z has density at least $(\delta/2\pi)^k$. But then if $x, y \in U_z$ then $\psi_i(x - y)$ has argument between $-\delta/2\pi$ and $\delta/2\pi$ so $|\psi_i(x - y) - 1| \leq \delta$. So $U_z - U_z \subset B(K, \delta)$, so $|B(K, \delta)| \geq (\delta/2\pi)^k$. □

Corollary 6.2. The Bohr set $B(K, \delta)$ in $\mathbb{Z}_N$ contains an arithmetic progression of length $c\delta N^{1/|K|}$.

Proof. By Lemma 6.1,

$$|B(K, \eta)| \geq \left(\frac{\eta}{2\pi}\right)^{|K|}.$$

So as long as that is greater than N^{-1}, $B(K, \eta)$ contains a non-zero element x. By the triangle inequality, $rx \in B(K, |r|\eta)$ as

$$|\psi_i(rx) - 1| \leq |\psi_i(rx) - \psi_i((r-1)x)| + \cdots + |\psi_i(x) - 1| \leq r|\psi_i(x) - 1|.$$

So if $0 < r \leq \delta/\eta$ then the progression $\{-rx, -(r-1)x, \dots, (r-1)x, rx\}$ is a subset of $B(K, \delta)$. But for $(\eta/2\pi)^{|K|} > N^{-1}$ we need $\eta > 2\pi N^{-1/|K|}$, so this gives a progression of length at least $\frac{1}{2\pi}\delta N^{1/|K|}$. □

Lemma 6.3 (Bogolyubov's Method)**.** Let G be a finite Abelian group and let $A \subset G$ be a set of density δ. Then $2A - 2A$ contains a Bohr set $B(K, \sqrt{2})$ with $|K| \leq \delta^{-2}$.

Proof. For each $x \in G$, let $f(x) = A * A * (-A) * (-A)(x)$, which is proportional to the number of ways of writing $x = a_1 + a_2 - a_3 - a_4$ with $a_i \in A$. Then $f(x) \neq 0$ if and only if $x \in 2A - 2A$.

Also, by the convolution and inversion formulae

$$f(x) = \sum_{\psi} |\hat{A}(\psi)|^4 \overline{\psi(x)}.$$

Let $K = \{\psi : |\hat{A}(\psi)| \geq \delta^{3/2}\}$. Then

$$\delta^3 |K| \leq \sum_{\psi} |\hat{A}(\psi)|^2 = \|A\|_2^2 = \delta$$

so $|K| \leq \delta^{-2}$. Now

$$f(x) = |\hat{A}(0)|^4 + \sum_{\psi \in K \setminus \{0\}} |\hat{A}(\psi)|^4 \overline{\psi(x)} + \sum_{\psi \notin K} |\hat{A}(\psi)|^4 \overline{\psi(x)}$$

and $|\hat{A}(0)|^4 = \delta^4$. If $x \in B(K, \sqrt{2})$ then $|\psi(x) - 1| \leq \sqrt{2}$ for each $\psi \in K$ so $\Re\psi(x) \geq 0$ as $|\psi(x)| = 1$. Therefore,

$$\Re\left(\sum_{\psi \in K \setminus \{0\}} |\hat{A}(\psi)|^4 \overline{\psi(x)} \right) \geq 0$$

for $x \in B(K, \sqrt{2})$.

$$\left| \sum_{\psi \notin K} |\hat{A}(\psi)|^4 \overline{\psi(x)} \right| \leq \max_{\psi \notin K} |\hat{A}(\psi)|^2 \sum_{\psi} |\hat{A}(\psi)|^2 < \delta^3 \cdot \delta = \delta^4.$$

Therefore, $\Re f(x) > 0$, which implies $f(x) \neq 0$ and hence $x \in 2A - 2A$. □

Chapter 7

Szemerédi's Theorem for Progressions of Length 4

Lemma 7.1. Let $f\colon \mathbb{Z}_N \to \mathbb{C}$ with $\|f\|_\infty \leq 1$ and let P be an arithmetic progression modulo N. Suppose that

$$\mathbb{E}_{k\in P}|\Delta(f;k)\hat{}(2\lambda k+\mu)|^2 \geq c.$$

Then for each $x \in \mathbb{Z}_N$ we can find a quadratic polynomial q_x in such a way that

$$\mathbb{E}_{x\in\mathbb{Z}_N}|\mathbb{E}_{s\in P+P} f(x-s)\omega^{q_x(s)}| > c'$$

where c' depends polynomially on c, and $\omega^{q_x(s)} = e(q_x(s)/N)$.

Proof. The left-hand side of the hypothesis equals

$$\mathbb{E}_{k\in P}\,\mathbb{E}_{x,y}\, f(x)\overline{f(x-k)f(y)}f(y-k)\omega^{(2\lambda k+\mu)(x-y)}$$
$$= \mathbb{E}_{x,u}\,\mathbb{E}_{k\in P}\, f(x)\overline{f(x-k)f(x-u)}f(x-u-k)\omega^{(2\lambda k+\mu)u}.$$

Now $2\lambda ku = \lambda(x^2-(x-k)^2-(x-u)^2+(x-k-u)^2)$ and $\mu u = \mu(x-(x-u))$. So this equals

$$\mathbb{E}_{x,u}\,\mathbb{E}_{k\in P}\, g_1(x)\overline{g_2(x-k)g_3(x-u)}g_4(x-k-u)$$

where $g_1(x) = g_3(x) = f(x)\omega^{\lambda x^2+\mu x}$ and $g_2(x) = g_4(x) = \omega^{\lambda x^2}f(x)$. On substituting $u = z+v$ with $z \in \mathbb{Z}_N$ and $v \in P$, this equals

$$\mathbb{E}_{x,z}\,\mathbb{E}_{k,v\in P}\, g_1(x)\overline{g_2(x-k)g_3(x-z-v)}g_4(x-z-v-k).$$

Therefore, there exists z such that

$$c \leq |\mathbb{E}_x\,\mathbb{E}_{k,v\in P}\, g_1(x)\overline{g_2(x-k)g_3(x-z-v)}g_4(x-z-v-k)|$$
$$\leq \mathbb{E}_x|\mathbb{E}_{k,v\in P}\,\overline{h_2(x-k)h_3(x-v)}h_4(x-v-k)|$$

where $h_2 = g_2$, $h_3(x) = g_3(x-z)$, and $h_4(x) = g_4(x-z)$. Thus there exists a z such that

$$c \leq \mathbb{E}_x|\mathbb{E}_{k,v\in P}\,\overline{h_2(x-k)h_3(x-v)}h_4(x-v-k)|$$
$$= \mathbb{E}_x\,\frac{N^2}{|P|^2}|\mathbb{E}_{k,v\in\mathbb{Z}_N}\,\overline{H_2^x(k)H_3^x(v)}H_4^x(k+v)|$$

where $H_2^x(k) = P(k)h_2(x-k)$, $H_3^x(v) = P(v)h_3(x-v)$, $H_4^x(s) = (P+P)(s)h_4(x-s)$. Hence

$$\begin{aligned}
&= \frac{N^2}{|P|^2}\,\mathbb{E}_x\langle H_4^x, H_2^x * H_3^x\rangle \\
&= \frac{N^2}{|P|^2}\,\mathbb{E}_x \sum_r \hat{H}_4^x(r)\overline{\hat{H}_2^x(r)\hat{H}_3^x(r)} \\
&\le \frac{N^2}{|P|^2}\,\mathbb{E}_x \max_r|\hat{H}_4^x(r)|\|\hat{H}_2^x\|_2\|\hat{H}_3^x\|_2 \\
&= \frac{N^2}{|P|^2}\,\mathbb{E}_x \max_r|\hat{H}_4^x(r)|\|H_2^x\|_2\|H_3^x\|_2 \\
&\le \frac{N}{|P|}\,\mathbb{E}_x \max_r|\hat{H}_4^x(r)|.
\end{aligned}$$

Therefore, for each x we can pick r_x so that

$$\begin{aligned}
& \frac{N}{|P|}\,\mathbb{E}_x|\mathbb{E}_s\, H_4^x(s)\omega^{r_x s}| \ge c \\
\Longrightarrow\quad & \frac{N}{|P|}\,\mathbb{E}_x\,\frac{|P+P|}{N}|\mathbb{E}_{s\in P+P}\, h_4(x-s)\omega^{r_x s}| \ge c \\
\Longrightarrow\quad & \mathbb{E}_x|\mathbb{E}_{s\in P+P}\, g_4(x-z-s)\omega^{r_x s}| \ge \frac{c}{2} \\
\Longrightarrow\quad & \mathbb{E}_x|\mathbb{E}_{s\in P+P}\, f(x-z-s)\omega^{\lambda(x-z-s)^2+r_x s}| \ge \frac{c}{2} \\
\Longrightarrow\quad & \mathbb{E}_x|\mathbb{E}_{s\in P+P}\, f(x-s)\omega^{\lambda(x-s)^2+r_{x+z} s}| \ge \frac{c}{2}.
\end{aligned}$$

Since $\lambda(x-s)^2 + r_{x+z}s$ is quadratic in s, we are done. □

Corollary 7.2. Under the assumptions of Lemma 7.1, we can find a collection of progressions P_i of size at least $a|P|^b$ with b and absolute constant and $a = a(c)$ such that $\mathbb{E}_{x\in P_i} f(x) \ge \frac{1}{8}c$.

Proof. Let $Q = P + P$. Then we have quadratics q_x such that

$$\mathbb{E}_x|\mathbb{E}_{s\in x-Q}\, f(s)\omega^{q_x(s)}| \ge \frac{c}{2}.$$

By an earlier lemma, we can partition each $x - Q$ into progressions $P_{i,x}$ of size at least $a(c)|Q|^b$ such that $\operatorname{diam}\omega^{q_x(P_{i,x})} \le \frac{1}{4}c$ for each $P_{i,x}$. So

$$\begin{aligned}
\frac{c}{2} &\le \mathbb{E}_x|\mathbb{E}_{s\in x-Q}\, f(x)\omega^{q_x(s)}| \\
&\le \mathbb{E}_x \sum_i \frac{|P_{i,x}|}{|x-Q|}\big|\mathbb{E}_{s\in P_{i,x}}\, f(s)\omega^{q_x(s)}\big| \\
&\le \mathbb{E}_x \sum_i \frac{|P_{i,x}|}{|Q|}\big|\mathbb{E}_{s\in P_{i,x}}\, f(s)\omega^{q_x(s_{i,x})}\big| \\
&\quad + \mathbb{E}_x \sum_i \frac{|P_{i,x}|}{|Q|}\Big|\mathbb{E}_{s\in P_{i,x}}\, f(s)\big(\omega^{q_x(s)} - \omega^{q_x(s_{i,x})}\big)\Big|
\end{aligned}$$

where $s_{i,x}$ is an arbitrary element of $P_{i,x}$, and hence

$$\leq \mathbb{E}_x \sum_i \frac{|P_{i,x}|}{|Q|} |\mathbb{E}_{s\in P_{i,x}} f(s)| + \frac{c}{4}.$$

Also,

$$\mathbb{E}_x \sum_i \frac{|P_{i,x}|}{|Q|} \mathbb{E}_{s\in P_{i,x}} f(s) = \mathbb{E}_x \mathbb{E}_{s\in x-Q} f(s) = \mathbb{E}_s f(s) = 0.$$

Therefore,

$$\mathbb{E}_x \sum_i \frac{|P_{i,x}|}{|Q|} \left(|\mathbb{E}_{s\in P_{i,x}} f(s)| + \mathbb{E}_{s\in P_{i,x}} f(s)\right) \geq \frac{c}{4}$$

so there exists x and i such that

$$|\mathbb{E}_{s\in P_{i,x}} f(s)| + \mathbb{E}_{s\in P_{i,x}} f(s) \geq \frac{c}{4}$$

because $\sum_i |P_{i,x}|/|Q| = 1$ for every x. Hence

$$\mathbb{E}_{s\in P_{i,x}} f(s) \geq \frac{c}{8}.$$ □

Convention. $c_1, c_2, \ldots$ is a sequence of constants, each with a power-type dependence on the previous one. Further, let $c_i^{-1} = C_i$.

Theorem 7.3 (Szemerédi's Theorem for Progressions of Length 4)**.** For every $\delta > 0$ there exists N such that every subset A of $\{1, \ldots, N\}$ of density at least δ contains an arithmetic progression of length 4.

Proof. (i) There exists c_1 depending with power-type on δ such that if A is c_1-quadratically uniform then A contains an arithmetic progression of length 4.

(ii) If A is non-c_1-quadratically uniform, let $f = A - \delta$. Then there exists $B \subset \mathbb{Z}_N$ of density at least c_2 and a function $\phi\colon B \to \hat{\mathbb{Z}}_N$ such that $|\Delta(f;k)\hat{}(\phi(k))| \geq c_2$ for every $k \in B$.

(iii) There are at least $c_3 N^3$ quadruples $x + y = z + w$ in B such that $\phi(x) + \phi(y) = \phi(z) + \phi(w)$.

(iv) Let Γ be the graph of ϕ. Then Γ has a subset Γ' of size at least $c_4 N$ such that $|\Gamma' - \Gamma'| \leq C_4|\Gamma|$.

(v) Therefore, $|9\Gamma' - 8\Gamma'| \leq C_5|\Gamma'|$.

(vi) Γ' has a subset Γ'', the graph of $\phi|_{B''}$, such that $\phi|_{B''}$ is a homomorphism of order 8 and B'' has density at least c_6.

(vii) There is a set K of size at most $C_7 = c_6^{-2}$ such that $2B'' - 2B''$ contains the Bohr neighbourhood $B(K, \sqrt{2})$.

(viii) $B(K, \sqrt{2})$ contains a progression P of length at least $\frac{1}{10}N^{c_7}$. Also, if ψ is the function induced by ϕ, that is,

$$\psi(a+b-c-d) = \phi(a) + \phi(b) - \phi(c) - \phi(d)$$

whenever $a, b, c, d \in B''$, then ψ is a homomorphism of order 2 on $2B'' - 2B''$, and therefore, we can find λ, μ such that $\psi(x) = 2\lambda x + \mu$ for every $x \in P$. Moreover, P is centred at 0, clearly $\psi(0) = 0$ so $\mu = 0$.

(ix) Writing $P = r[-m, m]$ for some r it follows that if $x, y \in B''$ with $|r^{-1}(x-y)| \leq m$ then

$$\phi(x) - \phi(y) = \phi(x) + \phi(x) - \phi(x) - \phi(y) = \psi(x-y) = 2\lambda(x-y)$$

since $x - y \in P$.

Letting $Q = r[0, m]$ then we can find some translate R of Q such that $|B'' \cap R| \geq c_6|R|$ since the right-hand side is the average over all translates.

This gives us a translate R and λ, μ such that $\phi(x)$ is defined and equals $2\lambda x + \mu$ for at least $c_6|R|$ values of $x \in R$. This is because if $x_0 \in B'' \cap R$ then for all $x \in B'' \cap R$,

$$\phi(x) - \phi(x_0) = 2\lambda(x - x_0)$$
$$\phi(x) = 2\lambda x + \phi(x_0) - 2\lambda x_0 = 2\lambda x + \mu.$$

(x) But Lemma 7.1 applied to $A - \delta$ then tells us that there exists some progression S of size at least N^{c_8} such that $|A \cap S| \geq (c_9 + \delta)|S|$. To see that the hypotheses hold, use the fact that $|\Delta(f; k)\hat{}(2\lambda k + \mu)| \geq c_2$ for at least $c_6|R|$ values of R.

(xi) Hence, by a Roth-style iteration, the theorem is proved.

The bound that results is that a density of $C_{11}(\log\log N)^{-c_{10}}$ is sufficient to guarantee a progression of length 4. □

Appendix A

Annotations

This chapter contains various annotations to the original lecture notes, which I found useful during revision in Lent term 2008. They range from stating and expanding the obvious to explanations of special cases omitted in lectures. Some of this work is due to Victor Falgas–Ravry and Paul Jefferys.

A.1 Annotations to Chapter 1

A.1.1 Lemma 1.1, Product of distinct characters

We claim that if ψ, χ are distinct characters on a finite Abelian group G then $\phi = \psi\bar{\chi}$ is a non-trivial character.

It is clear that ϕ is a character. Suppose ϕ is trivial. Then for all $g \in G$

$$\begin{aligned} & (\psi\bar{\chi})(g) = 1 \\ \implies \quad & \psi(g) = \bar{\chi}(g)^{-1} \\ \implies \quad & \psi(g) = (\chi(g)^{-1})^{-1} = \chi(g) \end{aligned}$$

as $\bar{z} = z^{-1}$ for all $z \in \mathbb{C}$ on the unit circle.

A.1.2 Proposition 1.3, Φ is a homomorphism

We claim that the map $\Phi\colon G \to \hat{\hat{G}}, x \mapsto \delta_x$ is a homomorphism.

Since ψ is a homomorphism we have

$$\begin{aligned} \Phi(x+y)(\psi) = \delta_{x+y}(\psi) = \psi(x+y) = \psi(x)\psi(y) = \delta_x(\psi)\delta_y(\psi) \\ = \Phi(x)(\psi)\Phi(y)(\psi). \end{aligned}$$

A.1.3 Proposition 1.3, $\hat{G}$ separates elements of G

We claim that if $x \neq y$ then there exists $\psi \in \hat{G}$ with $\psi(x) \neq \psi(y)$.

Suppose not. Let M be the $|\hat{G}| \times |G|$ matrix with rows indexed by $\hat{G}$ and columns indexed by G such that the entry at position (χ, z) is $\chi(z)$. By assumption, columns x and y are identical and hence $\operatorname{rank} M < |G|$, contradicting the linear independence of characters.

A.1.4 Note following Proposition 1.4, $\sum_\psi |\hat{A}(\psi)|^2 = \mathbb{E}_x |A(x)|^2$

We claim $\sum_\psi |\hat{A}(\psi)|^2 = \mathbb{E}_x |A(x)|^2$.

As a preliminary observation, recall that for $x \neq y$ in G there exists $\phi \in \hat{G}$ with $\phi(x-y) \neq 1$, so

$$\sum_\psi \psi(x-y) = \sum_\psi (\phi\psi)(x-y) = \phi(x-y) \sum_\psi \psi(x-y)$$

implying $\sum_\psi \psi(x-y) = 0$. Now

$$\begin{aligned}
\sum_\psi |\hat{A}(\psi)|^2 &= \sum_\psi \mathbb{E}_x\, A(x)\psi(x)\, \mathbb{E}_y\, \overline{A(y)\psi(y)} \\
&= \mathbb{E}_{x,y}\, A(x)\overline{A(y)} \sum_\psi \psi(x-y) \\
&= \mathbb{E}_x\, A(x) \frac{1}{|G|} \sum_y \overline{A(y)} \sum_\psi \psi(x-y) \\
&= \mathbb{E}_x\, A(x) \frac{1}{|G|} \overline{A(x)} |G| \\
&= \mathbb{E}_x |A(x)|^2
\end{aligned}$$

as desired.

A.1.5 Theorem 1.5, Reformulation of claim

Let $A \subset \mathbb{F}_3^n$. We claim there exists $\{x, x+d, x+2d\} \subset A$ for some $d \neq 0$ if and only if there exist x, y, z not all equal with $x+y+z = 0$.

Given $x, x+d, x+2d$ note these are distinct as $d \neq 0$ and $x + (x+d) + (x+2d) = 3x + 3d = 0$. Conversely, suppose $x+y+z = 0$. With $d = y - x$ we have $z = -x - y = 2x + 2y = 2x + 2x + 2d = x + 2d$, and $d \neq 0$ as $x \neq y$.

A.1.6 Theorem 1.5, Existence condition

We claim A contains such a triple as long as $\mathbb{E}_{x+y+z=0}\, A(x)A(y)A(z) > 3^{-n}$. To see this, note that

$$\frac{|\{(x,y,z) : x = y = z \text{ and } x+y+z = 0\}|}{|\{(x,y,z) : x+y+z = 0\}|} = \frac{3^n}{3^n \cdot 3^n} = \frac{1}{3^n}.$$

A.1.7 Theorem 1.5, $\delta^3/2 \geq 256/n^3 > 3^{-n}$

We check that $\delta^3/2 \geq 256/n^3 > 3^{-n}$ for all $n \in \mathbb{N}$, where $\delta \geq 8/n$.

Note $\delta^3/2 \geq 4 \cdot 64/n^3 = 256/n^3$. Further $3^n > n^3/256$ is true for all $n \in \mathbb{N}$ as it is true for $n = 1, 2, 3$ and from then on, the left-hand side is multiplied by 3 each step but the right-hand side is multipled by $(n+1)^3/n^3$ which for $n \geq 3$ is at most $64/27 < 3$.

A.1.8 Theorem 1.5, Iterations

We count the number of steps in the iteration. Let $\delta = \delta_0 \geq 8/n$ and note $(\delta_i)_{i\in\mathbb{N}}$ is strictly increasing. We have

$$\delta_i \geq \left(1 + \frac{\delta_{i-1}}{4}\right)\delta_{i-1} \geq \cdots \geq \left(1 + \frac{\delta_{i-1}}{4}\right)\cdots\left(1 + \frac{\delta_0}{4}\right)\delta_0 \geq \left(1 + \frac{\delta_0}{4}\right)^i \delta.$$

We claim that if $i \geq 4/\delta$ then $\delta_i \geq 2\delta$. It suffices to show

$$\begin{aligned} &\left(1 + \frac{\delta}{4}\right)^{4/\delta}\delta \geq 2\delta \\ \iff \quad &1 + \frac{\delta}{4} \geq 2^{\delta/4}. \end{aligned}$$

We show that for all $0 < y \leq 1$ we have $1 + y \geq 2^y$.

Define $g\colon \mathbb{R} \to \mathbb{R}, y \mapsto 1 + y - 2^y$. Note $g(0) = g(1) = 0$ and $g'(y) = 1 - (\log 2)2^y$. Now $g'(y) \geq 0$ if and only if $1 \geq (\log 2)2^y$ if and only if $y \leq -\log\log 2/\log 2$. With $y^* = -\log\log 2 \approx 0.53$, we see g is strictly increasing in $[0, y^*]$ and strictly decreasing in $[y^*, 1]$, giving the desired result.

Finally, we sum the geometric series

$$\frac{4}{\delta} + \frac{4}{2\delta} + \frac{4}{4\delta} + \cdots = \frac{4}{\delta}\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) = \frac{8}{\delta}.$$

A.2 Annotations to Chapter 2

A.2.1 Lemma 2.2, $|\psi(x+d) - \psi(x)| \leq 2\pi/k$

We claim there exists $d \in \{1, \ldots, k\}$ such that $|\psi(x+d) - \psi(x)| \leq 2\pi/k$ for all $x \in \mathbb{Z}_N$.

Suppose we have distinct $i, j \in \{0, \ldots, k\}$ such that $|\psi(i) - \psi(j)| \leq 2\pi/k$. Assume $i < j$ and set $x = i$, $d = j - i \in \{1, \ldots, k\}$. Then for all $y \in \mathbb{Z}_N$,

$$|\psi(y+d) - \psi(y)| = |\psi(y-x)||\psi(x+d) - \psi(x)| = |\psi(x+d) - \psi(x)| \leq \frac{2\pi}{k}.$$

A.2.2 Lemma 2.2, Partitioning into arithmetic progressions

The claim that we can partition a residue class modulo d into arithmetic progressions of lengths between $r/2$ and r holds provided $N/2k \geq r/2$. Since $r/2 = \varepsilon k/4\pi$ this is equivalent to $\varepsilon \leq 2\pi$.

Note this condition is essentially vacuous because in the case $\varepsilon \geq 2$ we note that $\operatorname{diam}\psi(A) \leq 2$ for any set $A \subset \mathbb{Z}_N$.

A.3 Annotations to Chapter 3

A.3.1 Theorem 3.1, Using Roth's theorem

By Roth's Theorem, there exists a constant C such that for $N \in \mathbb{N}$ and $A \subset [N]$ with $|A| \geq CN/\log\log N$ we know A contains a arithmetic progression of length 3.

Given $\varepsilon > 0$ choose $k \in \mathbb{N}$ such that

$$\frac{\varepsilon}{8\pi}k \geq \frac{Ck}{\log\log k}$$

that is, $k \geq e^{e^{8\pi C/\varepsilon}}$. Then any subset $A \subset [k]$ with density at least $\varepsilon/8\pi$ has size at least $Ck/\log\log k$ so contains an arithmetic progression of length 3 by Roth's Theorem.

A.3.2 Theorem 3.1, Pigeonhole principle on the circle

Suppose the unit circle is partitioned into at most $8\pi/\varepsilon$ sets each of diameter at most $\varepsilon/2$. Now consider the distribution of $e(\alpha x^2/2)$, $x = 1, \ldots, k$, among the partitioning sets. If each set contains fewer than $\varepsilon k/8\pi$ elements then the total number of elements, which is k, is strictly less than

$$\frac{8\pi}{\varepsilon}\frac{\varepsilon}{8\pi}k = k,$$

a contradiction. Thus one such set contains $e(\alpha x^2/2)$ for at least $\varepsilon k/8\pi$ values of x, and we denote the set of such x by A.

A.3.3 Theorem 3.1, Distance from 1

Observe

$$\begin{aligned}
\frac{\varepsilon}{2} &\geq \left|e\left(\frac{\alpha(x+d)^2}{2}\right) - e\left(\frac{\alpha x^2}{2}\right)\right| \\
&= \left|e\left(\frac{\alpha x^2}{2}\right)\right|\left|e\left(\frac{\alpha(x+d)^2}{2}\right)e\left(\frac{-\alpha x^2}{2}\right) - 1\right| \\
&= \left|e\left(\frac{\alpha(x+d)^2}{2}\right)\overline{e\left(\frac{-\alpha x^2}{2}\right)} - 1\right|
\end{aligned}$$

If we now consider two points $e^{i\theta_1}, e^{i\theta_2}$ on the unit circle within $\varepsilon/2$ of 1, we find

$$\begin{aligned}
|e^{i\theta_1}e^{i\theta_2} - 1| &= |e^{i\theta_2}||e^{i\theta_1} - e^{-i\theta_2}| = |e^{i\theta_1} - e^{-i\theta_2}| = |e^{i\theta_1} - 1 + 1 - e^{-i\theta_2}| \\
&\leq |e^{i\theta_1} - 1||1 - e{-i\theta_2}| \\
&\leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon
\end{aligned}$$

as required.

A.3.4 Lemma 3.2, $|1 - e(\alpha)| \geq 4\|\alpha\|$

We claim $|1 - e(\alpha)| \geq 4\|\alpha\|$ for all $\alpha \in \mathbb{R}$.

First note that both sides are only functions of the fractional part of α, so we may assume $\alpha \in (-1/2, 1/2]$. Further, both sides are invariant under changing α to $-\alpha$. Thus we may assume $\alpha \in [0, 1/2]$.

Let us write $\theta = 2\pi\alpha$, so $\theta \in [0, \pi]$. As $|1 - e(\alpha)|^2 = 2 - 2\Re e(\alpha) = 2(1 - \cos\theta)$ we have to show $1 - \cos\theta \geq 2\theta^2/\pi^2$. Using the series expansion of the cosine function, we find that

$$\begin{aligned} 1 - \cos\theta - 2\frac{\theta^2}{\pi^2} &= 1 - \sum_{n=0}^{\infty}(-1)^n \frac{\theta^{2n}}{(2n)!} - 2\frac{\theta^2}{\pi^2} \\ &= \theta^2 \frac{\pi^2 - 4}{2\pi^2} - \sum_{n=2}^{\infty}(-1)^n \frac{\theta^{2n}}{(2n)!} \\ &\geq \theta^2 \frac{\pi^2 - 4}{2\pi^2} - \sum_{n=2}^{\infty} \frac{\theta^{4n}}{(4n)!} \\ &\geq \theta^2 \frac{\pi^2 - 4}{2\pi^2} - \theta^2 \frac{1}{\pi^2} \sum_{n=2}^{\infty} \frac{\pi^{4n}}{(4n)!}. \end{aligned}$$

We can sum the geometric series,

$$\sum_{n=2}^{\infty} \frac{\pi^{4n}}{(4n)!} \leq \frac{\pi^8}{8!} + \frac{\pi^{12}}{12!} + \sum_{n=4}^{\infty}\left(\frac{\pi^4}{2000}\right)^n = \frac{\pi^8}{8!} + \frac{\pi^{12}}{12!} + \frac{\pi^{16}}{2000^3 \cdot (2000 - \pi^4)}.$$

It hence suffices to show

$$\frac{\pi^2 - 4}{2\pi^2} \geq \frac{\pi^8}{8!} + \frac{\pi^{12}}{12!} + \frac{\pi^{16}}{2000^3 \cdot (2000 - \pi^4)}.$$

Finally, the approximation $3 < \pi < 16/5$ gives the desired result.

A.3.5 Lemma 3.3, Properties of $\|\cdot\|$

We demonstrate some properties of the function $\|x\| = |\langle x \rangle|$.

We first claim that $\|x\| \leq |x|$. If $|x| \geq 1/2$ then $\|x\| = |\langle x \rangle| \leq 1/2 \leq |x|$. But if $|x| < 1/2$ then $\langle x \rangle = x$ and the result follows.

We also observe that $\|x\| = \|-x\|$.

Our second claim is the triangle inequality $\|x + y\| \leq \|x\| + \|y\|$.

Considering the range of $\|\cdot\|$, we are done if $\|x\|$ or $\|y\|$ is at least $1/2$. Thus assume $\|x\|, \|y\| < 1/2$. Similarly, we are done if both $\|x\|, \|y\| \geq 1/4$, so by symmetry we may assume that $\|x\| < 1/4$. Writing $x = [x] + \langle x \rangle$, $y = [y] + \langle y \rangle$,

$$\|x + y\| = \|[x] + \langle x \rangle + [y] + \langle y \rangle\| = \|\langle x \rangle + \langle y \rangle\|$$

and so we may assume $x, y \in (-1/2, 1/2]$. Summarising, we now assume $x \in (-1/4, 1/4), y \in (-1/2, 1/2)$ and aim to show $\|x + y\| \leq \|x\| + \|y\|$. Finally, note

that this inequality is invariant under the transformation $x \mapsto -x, y \mapsto -y$, so we may assume $y \in [0, 1/2)$, and our inequality becomes

$$\|x + y\| \leq |x| + y.$$

Note that our assumptions ensure $x + y \in (-1/4, 3/4)$. We consider two cases. If $x + y \leq 1/2$ then

$$\|x + y\| = |x + y| \leq |x| + |y| = |x| + y.$$

Otherwise, if $x + y > 1/2$ we know that $x > 0$ and so

$$\|x + y\| = |1 - (x + y)| < \frac{1}{2} < x + y = |x| + y.$$

A.3.6 Proof of Weyl's inequality

Lemma A.1. Let $k \in \mathbb{N}$ and $r \in \mathbb{R}$ with $r > 0$. For some $1 \leq l \leq k$ let $x_1, \ldots, x_l$ be real numbers with $\|x_i - x_j\| > 1/r$ for $i \neq j$. Suppose for all $i = 1, \ldots, l$ the fractional part $\langle x_i \rangle \in (-1/2, 1/2]$ has the same sign. Then

$$\sum_{i=1}^{l} \min\left\{ \frac{1}{\|x_i\|}, k \right\} \leq k + r + r \log(l - 1).$$

Proof. To prove this, we first observe that the statement is invariant under the transformation $(x_1, \ldots, x_l) \mapsto (-x_1, \ldots, -x_l)$ and we can further pass to fractional parts in $(-1/2, 1/2]$.

As all fractional parts have the same sign, we may assume that

$$0 \leq x_1 < \cdots < x_l \leq \frac{1}{2}$$

and our hypothesis becomes $x_j - x_i > 1/r$ for all $i < j$. Then

$$x_1 \geq 0, \qquad x_i \geq \frac{i - 1}{r}$$

for $i = 2, \ldots, l$. We now bound the sum under consideration

$$\begin{aligned}
\sum_{i=1}^{l} \min\left\{ \frac{1}{\|x_i\|}, k \right\} &\leq k + \sum_{i=2}^{l} \frac{1}{\|x_i\|} \\
&\leq k + r \sum_{i=2}^{l} \frac{1}{i - 1} = k + r \sum_{i=1}^{l-1} \frac{1}{i} = k + r + r \sum_{i=2}^{l-1} \frac{1}{i} \\
&\leq k + r + r \int_{1}^{l-1} \frac{1}{\tau} \, d\tau = k + r + r \log(l - 1),
\end{aligned}$$

completing the proof. □

Lemma A.2. Let $k \in \mathbb{N}$ and $r \in \mathbb{R}$ with $r > 0$. For some $2 \leq l \leq k$ let $x_1, \ldots, x_l$ be real numbers with $\|x_i - x_j\| > 1/r$ for $i \neq j$. Suppose not all fractional parts $\langle x_i \rangle \in (-1/2, 1/2]$ for $i = 1, \ldots, l$ have the same sign. Then

$$\sum_{i=1}^{l} \min\left\{ \frac{1}{\|x_i\|}, k \right\} \leq k + 4r + 2r \log \frac{l - 2}{2}.$$

Proof. Renaming the variables, we may assume

$$-\frac{1}{2} \le x_m < \cdots < x_1 < 0 \le y_1 < \cdots < y_n \le \frac{1}{2}$$

for some $1 \le m, n \le l-1$ with $m+n=l$, and where $x_j - x_i > 1/r$ and $y_j - y_i > 1/r$ for all $i<j$, $y_1 - x_1 > 1/r$ and $|x_1| \ge 1/(2r)$. Then as before

$$\begin{aligned} |x_1| &\ge 0, \qquad & y_1 &\ge \frac{1}{2r} \\ |x_i| &\ge \frac{i-1}{r}, \qquad & y_j &\ge \frac{j-1}{r} \end{aligned}$$

for $i = 2, \dots, m$ and $l = 2, \dots, n$, and so

$$\begin{aligned} &\sum_{i=1}^{m} \min\left\{ \frac{1}{\|x_i\|}, k \right\} + \sum_{j=1}^{n} \min\left\{ \frac{1}{\|y_i\|}, k \right\} \\ &\quad \le k + 2r + \sum_{i=2}^{m} \min\left\{ \frac{1}{\|x_i\|}, k \right\} + \sum_{j=2}^{n} \min\left\{ \frac{1}{\|y_i\|}, k \right\} \\ &\quad \le k + 4r + r\int_1^{m-1} \frac{1}{\tau}\, d\tau + r\int_1^{n-1} \frac{1}{\tau}\, d\tau \\ &\quad = k + 4r + r\log(m-1) + r\log(n-1) \\ &\quad \le k + 4r + 2r\log\frac{l-2}{2} \end{aligned}$$

as claimed. □

In our case, we have $r = 2q$ and $l = \lfloor q/4 \rfloor + 1$ and there is an additional factor of $1/2$ in all but the first summand. If all fractional parts have the same sign, we obtain

$$\begin{aligned} \sum_{u=v}^{v+\lfloor q/4 \rfloor} \min\left\{ k, \frac{1}{2\|2\alpha u\|} \right\} &\le k + \frac{r}{2} + \frac{r}{2}\log(l-1) \\ &\le k + q(1 + \log q - \log 4) \\ &\le k + q\log q. \end{aligned}$$

Otherwise,

$$\begin{aligned} \sum_{u=v}^{v+\lfloor q/4 \rfloor} \min\left\{ k, \frac{1}{2\|2\alpha u\|} \right\} &\le k + 2r + \frac{r}{2} + \frac{r}{2} + r\log\frac{l-2}{2} \\ &\le k + q\Big(6 + \log\frac{\lfloor q/4 \rfloor - 1}{2}\Big) \\ &\le k + q\Big(6 + \log\frac{q-4}{8}\Big) \\ &\le k + q\Big(8 + 4\log\frac{q-4}{8}\Big). \end{aligned}$$

We claim this is at most $k + 4q\log q$. Indeed,

$$k + q\Big(8 + 4\log\frac{q-4}{8}\Big) \le k + 4q\log q$$

$$\begin{aligned} &\iff \quad e^2\frac{q-4}{8} \le q \\ &\iff \quad \frac{-e^2}{2} \le \frac{8-e^2}{8}q \end{aligned}$$

which is true as $e^2 \le 8$.

Combining the bounds for the partial sums, we obtain

$$\begin{aligned} \sum_{u=0}^{2(k-1)} \min\left\{k, \frac{1}{2\|2\alpha u\|}\right\} &\le \left\lceil \frac{2(k-1)+1}{\lfloor q/4 \rfloor + 1} \right\rceil (k + 4q\log q) \\ &\le \left\lceil \frac{2k}{q/4} \right\rceil (k + 4q\log q) \\ &\le \frac{16k}{q}(k + 4q\log q) \end{aligned}$$

provided that $16k \ge q$. Under this assumption, we derive Weyl's inequality since

$$\begin{aligned} \left|\sum_{x=0}^{k-1} e(\alpha x^2)\right| &\le \sqrt{\frac{16k}{q}(k + 4q\log q)} \\ &\le \frac{4k}{\sqrt{q}} + 8\sqrt{k\log q}. \end{aligned}$$

A.3.7 Lemma 3.5, Density of I

We observe that the density of I is

$$\frac{|I|}{|\mathbb{Z}_N|} = \frac{2\left\lfloor \frac{\varepsilon N}{2} \right\rfloor + 1}{N}.$$

Note that

$$\begin{aligned} \langle A, I * (-I)\rangle &= \mathbb{E}_x\, A(x)\, \mathbb{E}_{y+z=x}\, I(y)(-I(z)) \\ &= \mathbb{E}_x\, A(x)\, \mathbb{E}_{y-z=x}\, I(y)I(z) \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} \langle A, I * (-I)\rangle &= \langle \hat{A}, \widehat{I * (-I)} \rangle \\ &= \langle \hat{A}, \hat{I}(\widehat{-I})\rangle. \end{aligned}$$

We claim this is $\langle \hat{A}, |\hat{I}|^2\rangle$. It suffices to show $\hat{I}(\widehat{-I}) = |\hat{I}|^2$. Indeed,

$$\begin{aligned} \hat{I}(\widehat{-I})(\psi) &= \Big(\sum_x I(x)\psi(x)\Big)\Big(\sum_y (-I(y))\psi(y)\Big) \\ &= \sum_{x,y} I(x)I(y)\psi(x)\psi(-y) \\ &= \sum_{x,y} I(x)\psi(x)\overline{I(y)\psi(y)} \end{aligned}$$

$$= \Big(\sum_x I(x)\psi(x)\Big)\Big(\overline{\sum_y I(y)\psi(y)}\Big)$$
$$= |\hat{I}|^2(\psi)$$

as required.

A.3.8 Lemma 3.5, $|I|^2 \geq \varepsilon^2/2$

To obtain the inequality $|\hat{A}(0)||\hat{I}(0)|^2 \geq \alpha\varepsilon^2/2$ we need to show $|\hat{I}(0)|^2 \geq \varepsilon^2/2$, that is, $|I|^2 \geq \varepsilon^2/2$. We will carry out equivalence transformations, writing $\beta = \varepsilon N/2 = s + t$ with $s \in \mathbb{Z}$ and $t \in [0, 1)$.

$$\begin{aligned} & |I|^2 \geq \frac{\varepsilon^2}{2} \\ \iff \quad & \frac{4\left\lfloor \frac{\varepsilon N}{2} \right\rfloor^2 + 4\left\lfloor \frac{\varepsilon N}{2} \right\rfloor + 1}{N^2} \geq \frac{\varepsilon^2}{2} \\ \iff \quad & 4\lfloor\beta\rfloor^2 + 4\lfloor\beta\rfloor + 1 \geq 2\beta^2 \\ \iff \quad & 2s^2 + 4s + 1 \geq 4st + 2t^2. \end{aligned}$$

We note that $4s \geq 4st$ and so if $s \geq 1$ we are done as $2s^2 + 1 > 2t^2$. But if $s = 0$ then the above is equivalent to $t \leq 1/\sqrt{2}$. That is, we are done unless

$$\sqrt{2} < \varepsilon N < 2.$$

In this case, we use an averaging argument to show the original claim of Lemma 3.5. The assumptions now are $\varepsilon \in (\sqrt{2}/N, 2/N)$ and $A \cap [-1, 1] = \emptyset$. Note that $4N < 8/\varepsilon$ and so it suffices to find $r \neq 0$ with $|\hat{A}(r)| \geq \alpha/8N \geq \varepsilon\alpha/16$. We know that

$$\begin{aligned} & \sum_r |\hat{A}(r)|^2 = |A| = \alpha \\ \iff \quad & \sum_{r\neq 0} |\hat{A}(r)|^2 + \alpha^2 = \alpha \end{aligned}$$

and hence by averaging we see that there exists an $r \neq 0$ such that

$$|\hat{A}(r)| \geq \sqrt{\frac{\alpha(1-\alpha)}{N-1}} > \sqrt{\frac{\alpha(1-\alpha)}{N}}.$$

We are done if

$$8\sqrt{\alpha(1-\alpha)N} \geq \alpha \quad \iff \quad \alpha \leq \frac{64N}{64N+1}$$

Finally, suppose this it not the case, i.e, $\alpha > 64N/(64N+1)$ and recall that $A \cap [-1, 1] = \emptyset$ and hence $\alpha \leq 1 - 3/N$. But now we observe that

$$1 - \frac{3}{N} \leq \frac{64N}{64N+1} \quad \iff \quad -191N - 3 \leq 0$$

which gives the desired contradiction.

A.3.9 Lemma 3.5, $|I| \leq 2\varepsilon$

Next we consider the inquality $|I| \leq 2\varepsilon$. Once again, this is not true in general, however, in the case when it this fails we can immediately prove the original Lemma 3.5.

$$\begin{aligned} & |I| = \frac{2\lfloor \frac{\varepsilon N}{2} \rfloor + 1}{N} \leq 2\varepsilon \\ \iff \quad & 2\left\lfloor \frac{\varepsilon N}{2} \right\rfloor + 1 \leq 2\varepsilon N \end{aligned}$$

Writing $\beta = \varepsilon N/2$ and further $\beta = s + t$ with $s \in \mathbb{Z}$ and $t \in [0, 1)$,

$$\begin{aligned} \iff \quad & 2\lfloor \beta \rfloor + 1 \leq 4\beta \\ \iff \quad & 1 \leq 2s + 4t. \end{aligned}$$

This is immediate if $s \geq 1$. But if $s = 0$ this is equivalent to $t \geq 1/4$. Thus, $|I| \leq 2\varepsilon$ unless

$$\frac{\varepsilon N}{2} \in \left(0, \frac{1}{4}\right)$$

so $\varepsilon \in (0, 1/2N)$, $A \cap [0] = \emptyset$ and $I = [0]$. As before, we will use an averaging argument to resolve this case. We aim to find an r with $0 < |r| \leq 8/\varepsilon^2$, but $16N < 8/\varepsilon^2$ so this condition reduces to $r \neq 0$. We further require $|\hat{A}(r)| \geq \varepsilon\alpha/16$ so it suffices to find $r \neq 0$ with $|\hat{A}(r)| \geq \alpha/32N$. Again,

$$\sum_{r \neq 0} |\hat{A}(r)|^2 = \alpha - \alpha^2$$

so, by averaging, there exists $r \neq 0$ such that

$$|\hat{A}(r)|^2 \geq \frac{\alpha(1-\alpha)}{N-1} \geq \frac{\alpha(1-\alpha)}{N}.$$

We are done if

$$\frac{\alpha(1-\alpha)}{N} \geq \frac{\alpha^2}{(32N)^2} \quad \iff \quad \alpha \leq \frac{1024N}{1024N+1}.$$

Finally, suppose this is not the case and recall that $A \cap [0] = \emptyset$ so $\alpha \leq 1 - 1/N$. But now we observe

$$1 - \frac{1}{N} \leq \frac{1024N}{1024N+1} \quad \iff \quad -1023N - 1 \leq 0,$$

giving the desired contradiction.

A.3.10 Lemma 3.5, $|\hat{I}(r)| \leq 1/(2N\|r/N\|)$

We now obtain the inequality

$$|\hat{I}(r)| \leq \frac{1}{2N\|\frac{r}{N}\|}.$$

Note that

$$N\hat{I}(r) = \sum_{k \in \mathbb{Z}_N} I(k) e^{2\pi i r k/N}$$

$$= \sum_{-\varepsilon N/2 \le k \le \varepsilon N/2} \left(e^{2\pi i r/N}\right)^k$$
$$= e(r/N)^{\lfloor \varepsilon N/2 \rfloor} \frac{1 - e(r/N)^{|I|}}{1 - e(r/N)}.$$

Thus

$$N|\hat{I}(r)| = \frac{|1 - e(r/N)^{|I|}|}{|1 - e(r/N)|} \le \frac{2}{4\|r/N\|}$$

so

$$|\hat{I}(r)| \le \frac{1}{2N\|r/N\|} = \frac{1}{2|r|}.$$

A.3.11 Lemma 3.5, Integral bound

To complete the proof, we obtain the inequality

$$\sum_{r > 8/\varepsilon^2} \frac{\alpha}{4r^2} \le \frac{3\alpha\varepsilon^2}{16},$$

that is

$$\sum_{r > 8/\varepsilon^2} \frac{1}{r^2} \le \frac{3\varepsilon^2}{4},$$

by integrating the function $1/r^2$ as follows.

$$\sum_{r > 8/\varepsilon^2} \frac{1}{r^2} \le \int_{8/\varepsilon^2 - 1}^{\infty} \frac{1}{r^2}\, dr = \left[-\frac{1}{r}\right]_{8/\varepsilon^2 - 1}^{\infty} = \frac{\varepsilon^2}{8 - \varepsilon^2}.$$

We are done provided

$$\frac{\varepsilon^2}{8 - \varepsilon^2} \le \frac{3\varepsilon^2}{4} \quad \iff \quad 3\varepsilon^2 + 4\varepsilon - 24 \le 0$$

which clearly holds for all $0 < \varepsilon \le 1$.

A.3.12 Second proof of Theorem 3.1, Pigeonhole principle on the circle

We claim that for $k \in \mathbb{N}$ there exists $1 \le q \le k$ and p coprime to q such that $|\alpha - p/q| < 1/kq$.

Partition the unit circle into intervals of width $2\pi/k$ and consider the distribution of $e(r\alpha)$ for $r = 0, \ldots, k$. By the pigeonhole principle, there exists $r < s$ such that $e(r\alpha)$ and $e(s\alpha)$ are in the same interval, i.e., there exists q with $1 \le q < k$ and $\|q\alpha\| \le 1/k$. Then there exists an integer p such that $|q\alpha - p| = \|q\alpha\| \le 1/k$ and so $|\alpha - p/q| \le 1/kq$. If we write $p/q = p'/q'$ in lowest terms so $(p', q') = 1$ so $1 \le q' \le q$ then $|\alpha - p'/q'| \le 1/kq \le 1/kq'$.

A.3.13 Second proof of Theorem 3.1, Case $q > Q$

We derive the sufficient condition $Q \leq 12k/\log k$ for the equation

$$\begin{aligned} & \frac{4k}{Q^{1/2}} + 8\sqrt{k \log q} \leq \frac{32k}{Q^{1/2}} \\ \iff \quad & 8\sqrt{k \log q} \leq \frac{28K}{Q^{1/2}} \\ \iff \quad & 4kQ \log q \leq 49k^2 \\ \impliedby \quad & Q \log q \leq 12k \\ \impliedby \quad & Q \leq 12k/\log k \end{aligned}$$

using that $q \leq k$.

A.3.14 Second proof of Theorem 3.1, Choice of Q

We show the choice $256k^{1/3} = Q^{5/6}$ satisfies the condition $Q \leq 12k/\log k$ for sufficiently large k.

$$256^6 k^2 \leq \frac{12^5 k^5}{(\log k)^5} \quad \iff \quad 256\Big(\frac{64}{3}\Big)^5 \leq \frac{k^3}{(\log k)^5}$$

We find the minimum of the right hand side by differentiating with respect to k,

$$\frac{d}{dk}\frac{k^3}{(\log k)^5} = \frac{3k^2}{(\log k)^5} - \frac{5k^2}{(\log k)^6} = 0 \quad \iff \quad \log k = \frac{5}{3}.$$

We deduce that for $k \geq e^{5/3}$ the right hand side is strictly increasing. We claim the inequality is satisfied for $k \geq 10^5$. As $64/3 \leq 25$, we have that

$$\begin{aligned} & 256\left(\frac{64}{3}\right)^5 \leq \frac{k^3}{(\log k)^5} \\ \impliedby \quad & 256 \cdot 25^5 \leq \frac{10^{15}}{(5 \log 10)^5} \\ \iff \quad & (\log 10)^5 \leq 2^7. \end{aligned}$$

Now $\log 10 < 5/2$, so we are done since $5^5 \leq 2^{12}$.