ADDITIVE COMBINATORICS EXAMPLES SHEET 2: SOLUTIONS

ALED WALKER

These are the ‘official’ solutions for the second example sheet. This is not to say that they cannot be improved, nor that there are no alternative approaches, nor that there won’t be the occasional small oversights or omissions! Nevertheless, this document should hopefully serve as a record of how to do all the questions, and be useful when it comes to your future revision and study.

If you have any questions about any of these solutions, please drop me an email at aw530@cam.ac.uk.

(1) Prove the Fourier inversion formula, that for any $f : G \to \mathbb{C}$,

$$f(x) = \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \widehat{f}(\gamma)\gamma(x),$$

both directly using orthogonality and also as a corollary of Parseval’s theorem.

Solution: Using the character property $\gamma(-g)\gamma(x) = \gamma(-g+x)$ and Fourier orthogonality in the form of

$$\mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \gamma(-g+x) = 1_{-g+x=0},$$

we derive

$$\begin{aligned}\mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \widehat{f}(\gamma)\gamma(x) &= \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \gamma(x)\sum_{g\in G} f(g)\gamma(-g)\\ &= \sum_{g\in G} f(g) \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \gamma(-g)\gamma(x)\\ &= \sum_{g\in G} f(g) \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \gamma(-g+x)\\ &= \sum_{g\in G} f(g)1_{-g+x=0}\\ &= f(x)\end{aligned}$$

as required.

Now, for each fixed $x \in G$, the function $\gamma \mapsto \overline{\gamma(x)}$ is the Fourier transform of the indicator function $1_{\{x\}} : G \mapsto \mathbb{C}$. So by Parseval’s identity we have

$$\mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \widehat{f}(\gamma)\gamma(x) = \langle \widehat{f}, \widehat{1_{\{x\}}}\rangle_{\widehat{G}} = \langle f, 1_{\{x\}}\rangle_G = f(x)$$

as required.

(2) (a) Show that $|\widehat{1_A}(\gamma)| \in \{0, |A|\}$ for all $\gamma \in \widehat{G}$ if and only if A is a coset of a subgroup.

(b) Use Fourier analysis to prove that $|A + A| = |A|$ if and only if A is a translate of a subgroup. *(We have already seen a simple elementary proof of this fact, but it is instructive to find a Fourier-analytic proof.)*

Solution: For part (a), assume first that $|\widehat{1_A}(\gamma)| \in \{0, |A|\}$ for all $\gamma \in \widehat{G}$. Let $\Gamma \subset \widehat{G}$ be the set of characters γ for which $|\widehat{1_A}(\gamma)| = |A|$. For all $\gamma \in \Gamma$, the triangle inequality gives

$$|\widehat{1_A}(\gamma)| = \Big| \sum_{a \in A} \gamma(-a) \Big| \leqslant \sum_{a \in A} |\gamma(-a)| = |A|$$

with equality if and only if all the terms $\gamma(-a)$ have the same argument. Therefore there is some constant c_γ such that $\gamma(a) = c_\gamma$ for all $a \in A$. Fixing some $a_0 \in A$, we get

$$A - a_0 \subset \bigcap_{\gamma \in \Gamma} \ker \gamma_0.$$

However, since $|\widehat{1_A}(\gamma)| = 0$ for $\gamma \notin \Gamma$, by Fourier inversion we see that $1_A(x) = 1_A(y)$ if $\gamma(x) = \gamma(y)$ for all $\gamma \in \Gamma$. Therefore A is the entirety of $a_0 + \cap_{\gamma \in \Gamma} \ker \gamma$, so A is a coset of a subgroup.

To prove the converse, suppose that $A = a_0 + H$ for some subgroup $H \leqslant G$. We have $G \cong H \times G/H$ and so $\widehat{G} \cong \widehat{H} \times \widehat{G/H}$. Picking $\gamma = (\gamma_1, \gamma_2) \in \widehat{H} \times \widehat{G/H}$, we observe that

$$|\widehat{1_A}(\gamma)| = \Big| \sum_{h \in H} \gamma(a_0 + h) \Big| = \Big| \sum_{h \in H} (\gamma_1, \gamma_2)(h, \widetilde{a_0}) \Big| = |\gamma_2(\widetilde{a_0})| \Big| \sum_{h \in H} \gamma_1(h) \Big| \in \{0, |H|\},$$

where $\widetilde{a_0}$ is the image of a_0 in the quotient group G/H. This is as required.

For part (b), the direction "A is a translate of a subgroup $\Rightarrow |A + A| = |A|$" is immediate from the underlying group theory (as $(a + H) + (a + H) = (a + a) + H$). We focus on the other direction. Since

$$|A|^2 = \sum_{g \in A+A} (1_A * 1_A)(g),$$

with the absolute value of each summand being at most $|A|$, since $|A + A| = |A|$ we conclude that $1_A * 1_A(g) = |A|$ for all $g \in A + A$. Then

$$\widehat{1_A}(\gamma)^2 = \widehat{1_A * 1_A}(\gamma) = |A|\widehat{1_{A+A}}(\gamma).$$

However, $A + A = A + a_0$ for some (in fact for all) $a_0 \in A$, and so

$$\widehat{1_{A+A}}(\gamma) = \widehat{1_A}(\gamma)\gamma(-a_0).$$

Hence

$$1_A(\gamma)^2 = \gamma(-a_0)|A|\widehat{1_A}(\gamma),$$

so $\widehat{1_A}(\gamma) \in \{0, |A|\}$. By part (a) then, we conclude that A must be a translate of a subgroup.

(3) (a) Prove that if $A \subset G$ with density $\alpha > 0$ and $|\widehat{1_A}(\gamma)| \leqslant \delta|A|$ for all $\gamma \neq \mathbf{1}$ then, for any $x \in G$ and $k \geqslant 2$, we have

$$\Big| 1_A * \cdots * 1_A(x) - \alpha|A|^{k-1} \Big| \leqslant \delta^{k-2}|A|^{k-1},$$

where the convolution is taken with k copies of A.

(b) Deduce that if $k \geqslant 3$ and $|\widehat{1_A}(\gamma)| < \alpha^{1/(k-2)}|A|$ for all $\gamma \neq \mathbf{1}$ then $kA = G$.

Solution: We will use $*_k$ to denote k-fold convolution. For part (a), we use Fourier inversion to conclude that

$$\begin{aligned}1_A *_k 1_A = \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \widehat{1_A *_k 1_A}(\gamma)\gamma(x) &= \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \widehat{1_A}(\gamma)^k\gamma(x)\\ &= \frac{|A|^k}{|G|} + \frac{1}{|G|}\sum_{\gamma\neq\mathbf{1}}\widehat{1_A}(\gamma)^k\gamma(x)\\ &= \alpha|A|^{k-1} + \frac{1}{|G|}\sum_{\gamma\neq\mathbf{1}}\widehat{1_A}(\gamma)^k\gamma(x).\end{aligned}$$

Now, from Parseval and the assumptions in the question,

$$\begin{aligned}\left|\frac{1}{|G|}\sum_{\gamma\neq\mathbf{1}}\widehat{1_A}(\gamma)^k\gamma(x)\right| &\leqslant \left|\frac{1}{|G|}\sum_{\gamma\neq\mathbf{1}}|\widehat{1_A}(\gamma)|^k\right|\\ &\leqslant \delta^{k-2}|A|^{k-2}\mathop{\mathbb{E}}_{\gamma\in\widehat{G}}|\widehat{1_A}(\gamma)|^2\\ &= \delta^{k-2}|A|^{k-2}\langle\widehat{1_A},\widehat{1_A}\rangle_{\widehat{G}}\\ &= \delta^{k-2}|A|^{k-2}\langle 1_A, 1_A\rangle_G\\ &= \delta^{k-2}|A|^{k-1},\end{aligned}$$

giving the required bound.

For part (b), let $\delta = \max_{\gamma\neq\mathbf{1}}|\widehat{1_A}(\gamma)|/|A|$ and note that $\delta < \alpha^{1/(k-2)}$. Then, by part (a), for all $x\in G$

$$\left|1_A *_k 1_A(x) - \alpha|A|^{k-1}\right| \leqslant \delta^{k-2}|A|^{k-1} < \alpha^{\frac{k-2}{k-2}}|A|^{k-1} = \alpha|A|^{k-1}.$$

So $1_A *_k 1_A(x) > 0$. Since x was arbitrary, we have $kA = G$.

(4) The higher additive energies are defined, for any $m \geqslant 1$ and finite set A, by

$$E_{2m}(A) = |\{(a_1,\dots,a_{2m}) : a_i\in A \text{ and } a_1+\dots+a_m = a_{m+1}+\dots+a_{2m}\}$$

(so that e.g. the usual additive energy $E(A)$ is $E_4(A)$).

(a) Show that
$$E_{2m}(A) = \mathop{\mathbb{E}}_{\gamma\in\widehat{G}}|\widehat{1_A}(\gamma)|^{2m}.$$

(b) Use Hölder's inequality to show that if $n\geqslant m\geqslant 1$ (and $n>1$) then
$$E_{2m}(A) \leqslant |A|^{\frac{n-m}{n-1}}E_{2n}(A)^{\frac{m-1}{n-1}}.$$

(c) Deduce that if $|A+A|\leqslant K|A|$ then for all $n\geqslant 2$ we have $E_{2n}(A)\geqslant K^{1-n}|A|^{2n-1}$. Compare this to what would follow by an application of Plünnecke's inequality.

(I've changed the index in part (c) from m to n to make the notation line up better with part (b).

Solution: For part (a), there is a slick solution, which is to note by Parseval that

$$E_{2m}(A) = \sum_{x\in G}1_A *_m 1_A(x)^2 = \langle 1_A *_m 1_A, 1_A *_m 1_A\rangle_G = \langle \widehat{1_A *_m 1_A}, \widehat{1_A *_m 1_A}\rangle_{\widehat{G}} = \mathop{\mathbb{E}}_{\gamma\in\widehat{G}}|\widehat{1_A}(\gamma)|^{2m}$$

as required.

However, I will go through a line by line derivation of a more laborious route (as for most students I would suspect that this is the first time they will have seen anything like this). Once you are more confident, you are allowed to skip some of these intermediate steps!

By definition we have

$$\begin{aligned}
\mathop{\mathbb{E}}_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)|^{2m} &= \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \Big|\sum_{a\in A}\gamma(-a)\Big|^{2m} \\
&= \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \Big(\sum_{a_1\in A}\gamma(-a_1)\cdot\overline{\sum_{a_{m+1}\in A}\gamma(-a_{m+1})}\Big)^m \\
&= \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \Big(\sum_{a_1\in A}\gamma(-a_1)\cdot\sum_{a_{m+1}\in A}\gamma(a_{m+1})\Big)^m \\
&= \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} \sum_{a_1,\dots,a_m\in A}\prod_{i=1}^{m}\gamma(-a_i)\sum_{a_{m+1},\dots,a_{2m}\in A}\prod_{j=m+1}^{2m}\gamma(a_j) \\
&= \sum_{\substack{a_1,\dots,a_m\in A\\ a_{m+1},\dots,a_{2m}\in A}} \mathop{\mathbb{E}}_{\gamma\in\widehat{G}}\prod_{i=1}^{m}\gamma(-a_i)\prod_{j=m+1}^{2m}\gamma(a_j) \\
&= \sum_{\substack{a_1,\dots,a_m\in A\\ a_{m+1},\dots,a_{2m}\in A}} \mathop{\mathbb{E}}_{\gamma\in\widehat{G}}\gamma(-a_1-\cdots-a_m+a_{m+1}+\cdots+a_{2m}) \\
&= \sum_{\substack{a_1,\dots,a_m\in A\\ a_{m+1},\dots,a_{2m}}} 1_{-a_1-\cdots-a_m+a_{m+1}+\cdots+a_{2m}=0} \\
&= E_{2m}(A)
\end{aligned}$$

as required. [For example, usually I would skip from line 1 until at least line 5 or 6.]

For part (b), we note that $E_2(A)=|A|$ for trivial reasons and thus the inequality is satisfied when $m=1$. The $n=m$ cases are also trivial. So w.l.o.g. $n>m>1$. We then apply Hölder's inequality with the exponents $p=\frac{n-1}{n-m}$ and $q=\frac{n-1}{m-1}$. Then $\frac{1}{p}+\frac{1}{q}$ and $1<p,q<\infty$, so these are valid exponents for Hölder, and we get

$$\begin{aligned}
E_{2m}(A) = \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)|^{2m} &= \mathop{\mathbb{E}}_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)|^{\frac{2(n-m)}{n-1}}\cdot|\widehat{1_A}(\gamma)|^{\frac{2n(m-1)}{n-1}} \\
&\leqslant \Big(\mathop{\mathbb{E}}_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)|^{\frac{2(n-m)p}{n-1}}\Big)^{\frac{1}{p}}\Big(\Big(\mathop{\mathbb{E}}_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)|^{\frac{2n(m-1)q}{n-1}}\Big)^{\frac{1}{q}} \\
&= \Big(\mathop{\mathbb{E}}_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)|^{2}\Big)^{\frac{n-m}{n-1}}\Big(\mathop{\mathbb{E}}_{\gamma\in\widehat{G}} |\widehat{1_A}(\gamma)|^{2n}\Big)^{\frac{m-1}{n-1}} \\
&= |A|^{\frac{n-m}{n-1}}E_{2n}(A)^{\frac{m-1}{n-1}}
\end{aligned}$$

as required.

For part (c) we may proceed by induction on n. The base case of $n=1$ is exactly the assumption $|A+A|\leqslant K|A|$, and then for the induction step we assume that

$n \geqslant 2$ and, assuming that the inequality holds for $n-1$, derive

$$\begin{aligned} E_{2n}(A) &\geqslant \Big(E_{2n-2}(A)|A|^{-\frac{1}{n-1}}\Big)^{\frac{n-1}{n-2}} \\ &\geqslant \Big(K^{1-(n-1)}|A|^{2(n-1)-1-\frac{1}{n-1}}\Big)^{\frac{n-1}{n-2}} \\ &= \Big(K^{2-n}|A|^{2n-3-\frac{1}{n-1}}\Big)^{\frac{n-1}{n-2}} \\ &= K^{2-n}|A|^{\frac{2n^2-5n+2}{n-2}} \\ &= K^{1-n}|A|^{2n-1} \end{aligned}$$

as required.

If we had applied Plünecke we would have deduced that $|nA| \leqslant K^n|A|$. Then by Cauchy-Schwarz we get

$$\begin{aligned} E_{2n}(A) &= \sum_{x\in nA} 1_A *_n 1_A(x)^2 \\ &\geqslant \Big(\sum_{x\in nA} 1\Big)^{-1}\Big(\sum_{x\in nA} 1_A *_n 1_A(x)\Big)^2 \\ &= |nA|^{-1}|A|^{2n} \\ &\geqslant K^{-n}|A|^{2n-1} \end{aligned}$$

So the Hölder argument gives a slightly stronger lower bound.

(5) (a) Using the density increment strategy and question 3, show that, for any $k \geqslant 3$, if $A \subset \mathbb{F}_p^n$ with density $\alpha = |A|/p^n$ then kA contains a coset of a subspace with codimension $O_k(\alpha^{-1/(k-2)})$.

(b) If $|\mathbf{x}|$ is the Hamming weight of $\mathbf{x} \in \mathbb{F}_2^n$, i.e. the numberof 1-s in $\mathbf{x}$, then let

$$A = \{\mathbf{x} \in \mathbb{F}_2^n : |\mathbf{x}| \geqslant n/2 + c\sqrt{n}\}$$

for an absolute constant $c > 0$. Show that (for large n) we have $|A| \gg_c 2^n$ and any coset of a subspace contained inside $A+A$ has codimension $\gg_c \sqrt{n}$. (In particular, in contrast to the situation for $k \geqslant 3$ in part (a), for $k=2$ it is not possible to guarantee a coset of a subspace with codimension $O_\alpha(1)$ in $A+A$.)

NB: Our statements of both part(a) and part (b) are slightly different to the example sheet, which had a typo in the numerics.

Solution: We know from Question 3 that if $|\widehat{1_A}(\gamma)| < \alpha^{\frac{1}{k-2}}|A|$ for all $\gamma \neq \mathbf{1}$ then $kA = G$, in which case we are done. Hence we may assume that there is some $\gamma \neq \mathbf{1}$ for which $|\widehat{1_A}(\gamma)| \geqslant \alpha^{\frac{1}{k-2}}|A|$.

Let $f_A := 1_A - \alpha$ be the balanced function of A. Then, since $\gamma \neq \mathbf{1}$, we have $\widehat{f_A}(\gamma) = \widehat{1_A}(\gamma)$. Define $c \in \mathbb{C}$ by $\overline{c}\widehat{f_A}(\gamma) = |\widehat{f_A}(\gamma)|$. Then

$$\langle f_A, c\gamma + 1\rangle_G = |\widehat{f_A}(\gamma)| + \sum_{x\in G} f_A(x) = |\widehat{f_A}(\gamma)|.$$

Let $V' = \ker\gamma$, which is a subspace of $\mathbb{F}_p^n$ of codimension 1, and let $V_0', \dots, V_{p-1}'$ denote the p cosets of V', where $V_i' := V' + x_i$ for some $x_i \in \mathbb{F}_p^n$. Then

$$|\widehat{f_A}(\gamma)| = \sum_{x\in G} f_A(x)(\overline{c\gamma(x)}+1) = \sum_{i=0}^{p-1}(|A\cap V_i'| - \alpha|V_i'|)(\overline{c\gamma(x_i)}+1) = \sum_{i=0}^{p-1}(|A\cap V_i'| - \alpha|V_i'|)c_i$$

for some $c_i \in \mathbb{C}$ with $\Re c_i \in [0,2]$. Taking real parts, we have

$$\alpha^{\frac{1}{k-2}}|A| \leqslant 2\sum_{i=0}^{p-1}(|A \cap V_i'| - \alpha|V_i'|).$$

So there must be some i for which

$$|A \cap V_i'| \geqslant \alpha|V_i'| + \frac{\alpha^{1/(k-2)}|A|}{2p} = \alpha|V_i'|(1 + \frac{\alpha^{\frac{1}{k-2}}}{2}).$$

The density increment thus constructed, we conclude as follows. Let (A_0, V_0), (A_1, V_1), ..., (A_l, V_l) be a maximal sequence of sets and subspaces, with $A_i \subset V_i + x_i$ for some translates x_i, for which

(a) $(A_0, V_0) := (A, \mathbb{F}_p^n)$;
(b) $V_i \cong \mathbb{F}_p^{n-i}$ for all i;
(c) $\alpha_i := |A_i|/|V_i|$ satisfies $\alpha_{i+1} \geqslant \alpha_i(1 + \frac{\alpha_i^{\frac{1}{k-2}}}{2})$;
(d) $kA_i \neq V_i$ for all $i \leqslant l-1$.

Then $\alpha_l < 1$. However, we observe from Bernoulli's inequality that

$$\alpha_{i+m} \geqslant \alpha_i(1 + \frac{m\alpha_i^{\frac{1}{k-2}}}{2}) \geqslant 2\alpha_i$$

if $m \geqslant 2\alpha_i^{-\frac{1}{k-2}}$. Since $2\alpha_i^{-\frac{1}{k-2}} \geqslant 1$ we certainly have

$$\alpha_{i+m} \geqslant 2\alpha_i \qquad \text{if} \qquad m = \lfloor 4\alpha_i^{-\frac{1}{k-2}} \rfloor.$$

Thus

$$l \leqslant \sum_{j=0}^{\log(1/\alpha)/\log 2} 4(2^j\alpha)^{-\frac{1}{k-2}} \ll_k \alpha^{-\frac{1}{k-2}}.$$

Since $kA_l = V_l$, we conclude that kA must contain a translate of a subspace of codimension $O_k(\alpha^{-\frac{1}{k-2}})$ as required.

For part (b), we can use the Central Limit Theorem to estimate $|A|$ (as applied to independent $\{0,1\}$ valued Bernoulli random variables X_1, ..., X_n). Thus

$$\mathbb{P}(\frac{\sum_{i=1}^n X_i - n/2}{\sqrt{n/4}} \geqslant 2c) \to \Phi(2c)$$

as $n \to \infty$, where

$$\Phi(2c) := \int_{-\infty}^{c} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt.$$

This certainly implies that $2^{-n}|A| \geqslant \Phi(2c)/2$ for large enough n, and thus $|A| \gg_c 2^n$ as desired.

In some case one may also use Stirling's approximation for the central binomial coefficient. Indeed,

$$|A| \geqslant 2^{n-1} - c\sqrt{n}\tbinom{n}{n/2}.$$

By Stirling,

$$\binom{n}{n/2} = (1+o(1))\frac{n^{n+1/2}e^{-n}\sqrt{2\pi}}{(n/2)^{n+1}e^{-n}2\pi} = (1+o(1))\frac{2^{n+1}}{\sqrt{2\pi n}}.$$

So $|A| \gg_c 2^n$ if c is small enough.

Observe that if $\mathbf{x} \in A + A$ then at least $2c\sqrt{n}$ of the coordinates of $\mathbf{x}$ are 0. Let V be an arbitrary subspace of $\mathbb{F}_2^n$ of codimension at most $2c\sqrt{n}$, and let $y \in \mathbb{F}_2^n$ also be arbitrary. We will find a vector $x \in (A+A) \setminus (y+V)$, thus proving that $A+A$ does not contain any coset of a subspace with codimension $\leqslant 2c\sqrt{n}$.

Indeed, letting $d = \dim V$, pick a basis $\mathbf{v_1}, \ldots, \mathbf{v_d}$ for V, and consider the d-by-n matrix over $\mathbb{F}_2$ whose rows are given by the vectors v_i. This matrix has row rank d by construction, so it also has column rank d, and in particular we may find a d-by-d submatrix of M that is invertible. Reordering the columns, we may assume without loss of generality that this submatrix consists of the first d columns, so $M = (D|E)$, where D is an invertible d-by-d matrix. Let $\mathbf{u} \in \mathbb{F}_2^d$ be such that $\mathbf{u}^T D = (1, \ldots, 1) - (\mathbf{y}|_D)^T$, where $(\mathbf{y}|_D)$ is the vector given by first d coordinates of $\mathbf{y}$. Such a $\mathbf{u}$ exists since D is invertible. Then $(\mathbf{u}^T M)^T + \mathbf{y}$ is a vector with d 1's in the first d coordinates, and since $d \geqslant 2c\sqrt{n}$ we have $(\mathbf{u}^T M)^T + \mathbf{y} \notin A+A$. But by construction $(\mathbf{u}^T M)^T + \mathbf{y} \in V + \mathbf{y}$, so we are done.

(6) Let $B = \mathrm{Bohr}(\Gamma; \rho)$ be a Bohr set of rank d and width $\rho \leqslant 1/2$ inside a finite abelian group G of order N.
(a) Show that if $\gamma \in \Gamma$ then $|\widehat{1_B}(\gamma)| \geqslant \frac{1}{2}|B|$.
(b) Deduce that $|B| \leqslant \frac{4}{d}N$.
(c) Show that, for arbitrarily large $d \geqslant 1$ and $N \geqslant 1$, there exists a Bohr set B of rank d and width $\rho \leqslant 1/2$ in $\mathbb{Z}/N\mathbb{Z}$ such that $|B| \gg \frac{1}{d}N$.

Solution: Part (a): By the triangle inequality we have

$$|\widehat{1_B}(\gamma)| = \Big|\sum_{b \in B} \gamma(-b)\Big| = \Big|\sum_{b \in B} \gamma(b)\Big| \geqslant \sum_{b \in B} 1 - \sum_{b \in B} |\gamma(b) - 1| \geqslant |B| - \frac{1}{2}|B| = \frac{1}{2}|B|$$

since $\rho \leqslant 1/2$.

Part (b): From Parseval, we have

$$|B| = \mathop{\mathbb{E}}_{\gamma \in \widehat{G}} |\widehat{1_A}(\gamma)|^2 \geqslant \frac{1}{N} \sum_{\gamma \in \Gamma} |\widehat{1_A}(\gamma)|^2 \geqslant \frac{d}{4N}|B|^2.$$

Then rearrange.

Part (c). Consider the Bohr set with $\rho = 1/2$ and

$$\Gamma = \{x \mapsto e(j/N) : j = 1, 2, \ldots, d\}.$$

Then $\mathrm{Bohr}(\Gamma, \rho) \supset \{0, 1, \ldots, k\}$ if $k \leqslant N/(100d)$, say. Indeed, for $1 \leqslant j \leqslant d$ and $0 \leqslant i \leqslant k$, we have

$$|e(ij/N) - 1| \leqslant \frac{\pi}{2}\|ij/N\| \leqslant \frac{\pi}{200} < 1/2.$$

(7) Show that for any Bohr set B of rank d and dilate $0 < \delta < 1/2$, the Bohr set B is $(1/\delta)^{O(d)}$-covered by its dilate B_δ.

Solution: Note that $B_{\delta/2} - B_{\delta/2} \subset B_\delta$, so it will be enough to show that B is $(1/\delta)^{O(d)}$ covered by $B_{\delta/2} - B_{\delta/2}$. By the Ruzsa covering lemma, it would be enough to show that

$$|B + B_{\delta/2}| \leqslant (1/\delta)^{O(d)}|B_{\delta/2}|.$$

Since $B + B_{\delta/2} \subset B_{1+\delta/2}$, it will be enough to show that

$$|B_{1+\delta/2}| \leqslant (1/\delta)^{O(d)}|B_{\delta/2}|.$$

But this follows from the result in lectures that $|B_\lambda| \geqslant (\lambda/2)^{3d}|B|$ for $\lambda \in (0,1)$. Indeed, applying this result with $\lambda = \delta/2(1+\delta/2)$ we get

$$|B_{\delta/2}| \geqslant \Big(\frac{\delta}{4(1+\delta/2)}\Big)^{3d}|B_{1+\delta/2}| \geqslant \delta^{O(d)}|B_{1+\delta}|$$

since $\delta < 1/2$. Rearranging gives the required inequality.

(8) Let B be a regular Bohr set of rank d and width $\rho \leqslant 1/2$.

(a) Show that for any $\eta, \delta > 0$ if $x \in B_\delta$ and $|\widehat{1_B}(\gamma)| \geqslant \eta|B|$ then

$$|1-\gamma(x)| \ll \frac{\delta}{\eta}d.$$

Hint: Consider the difference $\langle 1_B, \gamma\rangle - \langle 1_{B-x}, \gamma\rangle$.

(b) Deduce that if $\Delta = \{\gamma : |\widehat{1_B}(\gamma)| \geqslant \frac{1}{2}|B|\}$ then there is an absolute ocnstant $c > 0$ such that

$$B_{c\rho/d} \subset \mathrm{Bohr}(\Delta;\rho) \subset B.$$

Solution: For part (a), note that the statement is vacuous if $\eta > 1$, so we may assume that $\eta \leqslant 1$. Furthermore, by adjusting the implied constant in the conclusion, without loss of generality we may assume that $\delta < 1/200d$, since otherwise the claimed upper bound on $|1-\gamma(x)|$ is trivial.

Then on the one hand

$$|\langle 1_B, \gamma\rangle - \langle 1_{B-x}, \gamma\rangle| = |\widehat{1_B}(\gamma) - \gamma(x)\widehat{1_B}(\gamma)| = |1-\gamma(x)||\widehat{1_B}(\gamma)| \gg |1-\gamma(x)|\eta|B|.$$

On the other hand.

$$\begin{aligned}|\langle 1_B, \gamma\rangle - \langle 1_{B-x}, \gamma\rangle| &= \Big|\sum_{y\in G}(1_B - 1_{B-x})(y)\overline{\gamma}(y)\Big| \\ &\leqslant 2|B \triangle (B-x)| \\ &\ll |(B - B_\delta)\setminus B| + |(B+B_\delta)\setminus B| \\ &\ll |B_{1+\delta}| - |B| \\ &\ll \delta d|B|\end{aligned}$$

since B is regular. Putting these together we get

$$|1-\gamma(x)|\eta|B| \ll \delta d|B|,$$

which rearranges to the required inequality.

For part (b), we know by Question 6(a) that $\Delta \supset \Gamma$, which in turn implies that $\mathrm{Bohr}(\Delta;\rho) \subset B$. For the other inclusion, we note that if $x \in B_{c\rho/d}$ (for some small absolute c) and $\gamma \in \Delta$, then by applying part(a) with $\eta = 1/2$ we get $|1-\gamma(x)| \ll 2\Big(\frac{c\rho}{d}\Big)d \leqslant \rho$ if c is chosen small enough. Hence $B_{c\rho/d} \subset \mathrm{Bohr}(\Delta;\rho)$ as required.

(9) Suppose we new the following for some functions $D, \delta : [0,1] \longrightarrow \mathbb{R}$:

> If $A \subset \mathbb{F}_p^n$ is a subset of density α that contains no non-trivial three-term arithmetic progressions then either
> (a): $|A| \ll p^{n/2}$ or
> (b): there is a subspace $V \leqslant \mathbb{F}_p^n$ of codimension $\leqslant D(\alpha)$ and a translate x such that $|(A-x)\cap V|/|V| \geqslant (1+\delta(\alpha))\alpha$.

(So that e.g. Lemma 15 in lectures is this with $D(\alpha) = 1$ and $\delta(\alpha) = \alpha/4$.)

What upper bounds can you deduce for the maximal size of a subset of $\mathbb{F}_p^n$ which has no non-trivial three-term arithmetic progressions if...
(a) $D(\alpha) \ll \alpha^{-1/2}$ and $\delta(\alpha) \gg \alpha^{1/2}$,
(b) $D(\alpha) \ll \alpha^{-1}$ and $\delta(\alpha) \gg 1$, or
(c) $D(\alpha) \ll 1$ and $\delta(\alpha) \gg 1$.

Solution:

As in lectures, we let $k \geqslant 0$ be maximal such that the following holds. There is a sequence of sets $A_0, \dots, A_k$ and associated subspaces $V_0, \dots, V_k \leqslant \mathbb{F}_p^n$, with codimensions $d_0, \dots, d_k$, and translates $x_0, \dots, x_k \in \mathbb{F}_p^n$, for which

(i) $A_0 = A$ and $V_0 = \mathbb{F}_p^n$, with $d_0 = 0$ and $x_0 = \mathbf{0}$
(ii) $A_i \subset V_i + x_i$;
(iii) A_i has no non-trivial 3APs;
(iv) if $\alpha_i = |A_i|/|V_i|$ then

$$\alpha_{i+1} \geqslant (1 + \delta(\alpha_i))\alpha_i;$$

(v) $d_{i+1} \leqslant d_i + D(\alpha_i)$.

In all three cases below we will see that step (iv) guarantees that such a sequence of sets $A_0, A_1, \dots$ has finite length, and so it makes sense to talk of a maximal k.

We always have $\alpha_{i+m} \geqslant (1 + m\delta(\alpha_i))\alpha_i \geqslant 2\alpha_i$ if $m \geqslant \delta(\alpha_i)$, by Bernoulli's inequality. We also conclude by the maximality of k that $|A_k| \ll |V_k|^{1/2}$, and so $\alpha_k \ll |V_k|^{-1/2}$.

For part (a), we see that

$$d_k \leqslant \sum_{i=0}^{k-1} D(\alpha_i) \ll \sum_{i=0}^{k-1} \alpha_i^{-1/2} \ll k\alpha^{-1/2}.$$

But $k \ll \alpha^{-1/2}$. This is since $\alpha_{i+m} \geqslant 2\alpha_i$ if $m \geqslant \alpha_i^{-1/2}$, and thus $\alpha_l > 1$ if $l \geqslant \sum_{j=0}^{100\log(1/\alpha)/\log 2} (2^j\alpha)^{-1/2}$. This sum is $\ll \alpha^{-1/2}$ in size, and thus $k \ll \alpha^{-1/2}$ as claimed.

Therefore $d_k \ll \alpha^{-1}$. This the same situation as in lectures, where we concluded that

$$\alpha \leqslant \alpha_k \ll |V_k|^{-1/2} = (p^{n-d_k})^{-1/2} \ll p^{O(\alpha^{-1}) - \frac{n}{2}}.$$

Hence, rearranging and taking logs, we get

$$\alpha \ll_p n^{-1}$$

which was the same as in Meshulam's theorem.

For part (b), we get

$$d_k \leqslant \sum_{i=0}^{k-1} D(\alpha_i) \ll \sum_{i=0}^{k-1} ((1+c)^i\alpha)^{-1} \ll \alpha^{-1}$$

for some absolute constant c. So again

$$\alpha \leqslant \alpha_k \ll |V_k|^{-1/2} = (p^{n-d_k})^{-1/2} \ll p^{O(\alpha^{-1}) - \frac{n}{2}}.$$

Rearranging and taking logs as before, we get

$$\alpha \ll_p n^{-1},$$

i.e. the same bound.

For part (c), such a strong increment would imply that $k \ll \log(1/\alpha)$ and $d_k \ll \log(1/\alpha)$ (by similar calculations as above). So

$$\alpha \ll p^{O(\log(1/\alpha))-\frac{n}{2}}.$$

Taking logs and rearranging, we get

$$\alpha \leqslant e^{-c_p n}$$

for some absolute $c_p > 0$ (depending on the earlier $O(1)$ constants). This matches the shape of the bound that we now know to hold from the (non-Fourier analytic) work of Croot–Lev–Pach.

(10) Suppose we knew the following for some functions $D, \delta : [0,1] \longrightarrow \mathbb{R}$, for any finite abelian group G of odd order:

> Let B be a regular Bohr set of rank d and width ρ. If $A \subset B$ is a subset of density α that contains no non-trivial three-term arithmetic progressions then either (a): $|A| \ll (d/\alpha)^{O(d)}|B|^{1/2}$ or
> (b):there is a regular Bohr set $B' \subset B$ of rank $\leqslant d + D(\alpha)$ and width $\gg \rho(\alpha/d)^{O(1)}$ and a translate x such that $|(A-x) \cap B'|/|B'| \geqslant (1+\delta(\alpha))\alpha$.

(So that e.g. Lemma 20 in lectures is this with $D(\alpha) = 1$ and $\delta(\alpha) \gg \alpha$.)

What upper bounds can you deduce for the maximal size of a subset of $\{1, \ldots, N\}$ which has no non-trivial three-term arithmetic progressions if...
(a) $D(\alpha) \ll \alpha^{-1/2}$ and $\delta(\alpha) \gg \alpha^{1/2}$,
(b) $D(\alpha) \ll \alpha^{-1}$ and $\delta(\alpha) \gg 1$, or
(c) $D(\alpha) \ll 1$ and $\delta(\alpha) \gg 1$.

Solution:

The set-up is very similar to the previous question. If A contains no non-trivial 3APs, then – since we seek an upper-bound for α – by restricting to a subset of A we may assume that $\alpha < 1/2$. As in lectures, we let $k \geqslant 0$ be maximal such that the following holds. There is a sequence of sets $A_0, \ldots, A_k$ and associated Bohr sets $B_0, \ldots, B_k$ with rank $d_0, \ldots, d_k$ and width $\rho_0, \ldots, \rho_k$, and a series of translates $x_0, \ldots, x_k \in G$, for which

(i) $A_0 = A$ and $B_0 = G$ with $d_0 = 1$ and $\rho = 2$;
(ii) $A_i \subset B_i + x_i$ for all i;
(iii) A_i has no non-trivial 3APs;
(iv) if $\alpha_i = |A_i|/|B_i|$ then

$$\alpha_{i+1} \geqslant (1+\delta(\alpha_i))\alpha_i;$$

(v) $d_{i+1} \leqslant d_i + D(\alpha_i)$;
(vi) $\rho_{i+1} \gg \rho_i(\alpha_i/d_i)^{O(1)}$.

We always have $\alpha_{i+m} \geqslant (1+m\delta(\alpha_i))\alpha_i \geqslant 2\alpha_i$ if $m \geqslant \delta(\alpha_i)$. We also conclude by the maximality of k that $|A_k| \ll (d_k/\alpha_k)^{O(d_k)}|B_k|^{1/2}$, and so $\alpha_k \ll (d_k/\alpha_k)^{O(d_k)}|B_k|^{-1/2}$.

For part (a), by the same calculation as in Q9(a) we get $d_i \leqslant d_k \ll \alpha^{-1}$ and $k \ll \alpha^{-1/2}$. Therefore

$$\rho_k \gg \prod_{i=0}^{k-1}(\alpha_i/d_i)^{O(1)} \gg (c\alpha^2)^{O(\alpha^{-1/2})} = \alpha^{O(\alpha^{-1/2})}$$

since $\alpha < 1/2$. Therefore by the usual lower bounds on the size of Bohr sets,

$$|B_k| \gg \left(\frac{\rho_k}{8}\right)^{d_k} N \gg \alpha^{O(\alpha^{-3/2})}N.$$

Combining the inequalities we get

$$\alpha \leqslant \alpha_k \ll \Big(\frac{d_k}{\alpha_k}\Big)^{O(d_k)}|B_k|^{-1/2} \ll \Big(\frac{d_k}{\alpha}\Big)^{O(d_k)}|B_k|^{-1/2} \ll \Big(\frac{1}{\alpha}\Big)^{O(\alpha^{-1})} \cdot \Big(\frac{1}{\alpha}\Big)^{O(\alpha^{-3/2})}N^{-1/2}$$
$$\ll \Big(\frac{1}{\alpha}\Big)^{O(\alpha^{-3/2})}N^{-1/2}.$$

Taking logs and rearranging we get $\log N \ll \alpha^{-3/2}\log(1/\alpha)$, and hence

$$\alpha \ll \Big(\frac{\log\log N}{\log N}\Big)^{2/3}.$$

This is the same rough shape of bound (i.e. $(\log N)^{-2/3+o(1)}$) that was proved by Bourgain in 2008.

For part (b), again the calculations go through as in Q9 to yield $d_k \ll \alpha^{-1}$ and $k \ll \log(1/\alpha)$. Therefore

$$\rho_k \gg (\alpha/d_k)^{O(k)} \gg \alpha^{O(\log(1/\alpha))}.$$

The lower bound on $|B_k|$ yields

$$|B_k| \gg \alpha^{O(\alpha^{-1}\log(1/\alpha))}N.$$

Thus

$$\alpha \leqslant \alpha_k \ll \Big(\frac{d_k}{\alpha}\Big)^{O(d_k)}|B_k|^{-1/2} \ll \alpha^{O(\alpha^{-1})} \cdot \alpha^{O(\alpha^{-1}\log(1/\alpha))}N \ll \alpha^{O(\alpha^{-1}\log(1/\alpha))}N.$$

Taking logs and rearranging we get $\log N \ll \alpha^{-1}\log(1/\alpha)^2$, and hence

$$\alpha \ll \frac{(\log\log N)^2}{\log N}.$$

For part (c), the calculations go through as in Q9 to yield $d_k \ll \log(1/\alpha)$ and $k \ll \log(1/\alpha)$. The bound for ρ_k becomes

$$\rho_k \gg (\alpha\log(1/\alpha))^{O(\log(1/\alpha))}$$

and the lower bound for $|B_k|$ is

$$|B_k| \gg (\alpha\log(1/\alpha))^{O(\log(1/\alpha)^2)}N.$$

Putting everything together exacly as above, we get

$$\alpha \ll N^{-1/2}(\alpha\log(1/\alpha))^{O(\log(1/\alpha)^2)}.$$

Taking logs and rearranging, one ends up with the inequality

$$\alpha \ll e^{-c(\log N)^{1/3}}$$

for some absolute $c > 0$.

This is the dream density increment, but still doesn't match the best known lower construction. This is still due, essentially, to Behrend in the 40s, which shows that there is an example of a set $A \subset \mathbb{Z}/N\mathbb{Z}$ and $|A| \gg N\exp(-c(\log N)^{1/2})$ with no non-trivial 3APs.

(11) Let $m \geqslant 2$ and $p > m$ be prime.

(a) Sketch a proof that if $A \subset \mathbb{F}_p^n$ is a set of density α which has no solutions to $x_1 + \cdots + x_m = my$ with $x_1, \ldots, x_m, y \in A$ all distinct, then there is some constant $c_m > 0$ depending only on m such that either

- $|A| \gg (p^n)^{1-c_m}$, or
- there is a subspace $V \leqslant \mathbb{F}_p^n$ of codimension 1 and a translate x such that

$$|(A-x)\cap V|/|V| \geqslant (1 + c_m\alpha^{\frac{1}{m-1}})\alpha.$$

(b) Deduce that if $A \subset \mathbb{F}_p^n$ contains no solutions to $x_1 + \cdots + x_m = my_m$ with all variables distinct then
$$|A| \ll_{p,m} \frac{p^n}{n^{m-1}}.$$

Solution: For ease of notation we write $G = \mathbb{F}_p^n$. For part (a), the number of solutions to $x_1+\cdots+x_m = my$ with $x_1, \ldots, x_m, y \in A$ is equal to $\sum_{x_1,x_m,y\in G} \prod_{i=1}^m 1_A(x_i) \mathbb{E}_{\gamma\in\widehat{G}} \gamma(x_1+\cdots + x_m - my)$, in which in turn equals
$$\mathbb{E}_{\gamma\in\widehat{G}} \Big(\prod_{i=1}^m \sum_{x_i\in G} 1_A(x_i)\gamma(x_i)\Big)\Big(\sum_{y\in G} 1_A(y)\gamma(-my)\Big) = \mathbb{E}_{\gamma\in\widehat{G}} \Big(\prod_{i=1}^m \widehat{1_A}(\overline{\gamma})\Big)\widehat{1_A}(\gamma_m),$$
where $\gamma_m \in \widehat{G}$ is the character given by $x \mapsto \gamma(mx)$.

The term with γ being the trivial character gives a contribution of $|A|^{m+1}/|G|$, which is $\alpha^{m+1}p^{nm}$. Now, the number of trivial solutions to the equation (in which some of the variables are the same) is $O(m^2(p^n)^{m-1})$, as is seen by summing over all pairs of variables that could be equal and extending the range of the variables to the whole of G. Therefore, since A contains no non-trivial solutions to the equation, we conclude that
$$\frac{1}{p^n}\sum_{\gamma\neq\mathbf{1}} |\widehat{1_A}(\overline{\gamma})|^m|\widehat{1_A}(\gamma_m)| \geqslant \alpha^{m+1}p^{nm} - O(m^2p^{n(m-1)}).$$

There are now two cases. If we have $m^2p^{n(m-1)} \gg \alpha^{m+1}p^{nm}$ then $\alpha \ll m^{2/(m+1)}p^{-n/(m+1)}$, and thus $|A| \ll p^{n(1-c_m)}$ for some c_m (as in case 1 of the claim).

Otherwise we may assume that
$$\frac{1}{p^n}\sum_{\gamma\neq\mathbf{1}} |\widehat{1_A}(\overline{\gamma})|^m|\widehat{1_A}(\gamma_m)| \gg \alpha^{m+1}p^{nm}.$$
By taking out $m-1$ factors from the power, we get
$$\begin{aligned}\alpha^{m+1}p^{nm} &\ll (\max_{\gamma\neq\mathbf{1}} |\widehat{1_A}(\gamma)|)^{m-1} \mathbb{E}_{\gamma} |\widehat{1_A}(\gamma)||\widehat{1_A}(\gamma_m)| \\ &\ll (\max_{\gamma\neq\mathbf{1}} |\widehat{1_A}(\gamma)|)^{m-1}(\mathbb{E}_{\gamma} |\widehat{1_A}(\gamma)|^2)^{1/2}(\mathbb{E}_{\gamma} |\widehat{1_A}(\gamma_m)|^2)^{1/2} \\ &\ll |A|(\max_{\gamma\neq\mathbf{1}} |\widehat{1_A}(\gamma)|)^{m-1} \\ &\ll \alpha p^n(\max_{\gamma\neq\mathbf{1}} |\widehat{1_A}(\gamma)|)^{m-1}\end{aligned}$$
where the penultimate line follows by Parseval.

Therefore
$$(\max_{\gamma\neq\mathbf{1}} |\widehat{1_A}(\gamma)|) \gg \alpha p^n(\alpha^{1/(m-1)}).$$

By the usual argument from lectures, this means that there is a subspace V and a translate x with the desired property.

For part (b), as ever we let $k \geqslant 0$ be maximal such that the following holds. There is a sequence of sets $A_0, \ldots, A_k$ and associated subspaces $V_0, \ldots, V_k \leqslant \mathbb{F}_p^n$, with codimensions $d_0, \ldots, d_k$, and translates $x_0, \ldots, x_k \in \mathbb{F}_p^n$, for which

(i) $A_0 = A$ and $V_0 = \mathbb{F}_p^n$, with $d_0 = 0$ and $x_0 = \mathbf{0}$

(ii) $A_i \subset V_i + x_i$;

(iii) A_i had no non-trivial 3APs;

(iv) if $\alpha_i = |A_i|/|V_i|$ then
$$\alpha_{i+1} \geqslant (1 + c\alpha^{1/(m-1)})\alpha_i;$$

(v) $d_{i+1} \leqslant d_i + 1$.

We always have $\alpha_{i+m} \geqslant (1 + cm\alpha_i^{1/(m-1)})\alpha_i \geqslant 2\alpha_i$ if $m \geqslant c^{-1}\alpha_i^{-1/(m-1)}$. Therefore $d_k \leqslant \sum_{j=0}^{100\log(1/\alpha)/\log 2} c^{-1}(2^j\alpha)^{-1/(m-1)} \ll_m \alpha^{-1/(m-1)}$.

We also conclude by the maximality of k that $|A_k| \ll |V_k|^{1-c_m}$, and so $\alpha_k \ll |V_k|^{-c_m}$.

Therefore

$$\alpha \leqslant \alpha_k \ll p^{-c_m(n-d_k)} \ll p^{O_m(\alpha^{-1/(m-1)})-c_m n}.$$

Taking logs and rearranging we get $\alpha^{-1/(m-1)} \gg_{m,p} n$, which yields $\alpha \ll_{m,p} n^{-(m-1)}$ as claimed.

Of course much better bounds are now known in $\mathbb{F}_p^n$ by the polynomial method of Croot–Lev–Pach–Ellenberg–Gijswijt. However, even in $\mathbb{Z}/N\mathbb{Z}$, much stronger bounds are now available by analytic and combinatorial methods. Indeed, Schoen–Shkredov (*Roth's theorem in many variables*, Israel Journal of Mathematics, 199, 287-308) proved that if $A \subset \mathbb{Z}/N\mathbb{Z}$ lacks non-trivial solutions to $x_1+x_2+x_3+x_4+x_5 = 5y$, say, then $|A| \ll N \exp^{-(\log N)^{1/7}}$.

The idea behind this method is to use the fact that $2A - 2A$ contains a large Bohr set B (see material on Freiman's theorem), and so really the system looks more like $b + x_5 = 5y$. From this one can generate an extremely large density increment onto a translate of B.