ADDITIVE COMBINATORICS EXAMPLES SHEET 3: SOLUTIONS

ALED WALKER

These are the 'official' solutions for the third 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.

For Question 1 (c), I was not quite able to recover the bound that was stated in the question – I'm off by a factor of 2. I hope that one of you will tell me in the examples class where I was being stupid!

(1) This question indicates how (weaker) almost-periodicity results can be proved using only Fourier analysis. Let G be a finite abelian group of order N and $A \subset G$ with density $\alpha = |A|/N$.

(a) For any $0 \leqslant \eta \leqslant 1$ let

$$\Delta_\eta(A) = \{\gamma \in \widehat{G} : |\widehat{1_A}(\gamma)| \geqslant \eta |A|\}.$$

Use Parseval's identity to show that $|\Delta_\eta(A)| \leqslant \eta^{-2}\alpha^{-1}$.

(b) Show that the set of L^2-almost periods of $1_A * 1_A$ with error $\varepsilon|A|^{3/2}$ contains a Bohr set of rank $O(\varepsilon^{-2}\alpha^{-1})$ and width $\gg \varepsilon\alpha^{1/2}$. *[In fact, we will show that width $\gg \varepsilon$ is possible.]*

(c) Generalise your solution to part (b) to show that for any $m \geqslant 1$ the set of L^{2m}-almost periods of $1_A * 1_A$ with error $\varepsilon|A|^{1+1/2m}$ contains a Bohr set of rank $O(\varepsilon^{-2m}\alpha^{-1})$ and width $\gg \varepsilon\alpha^{1/2m}$. *[In fact, we will show that width $\gg \varepsilon$ is possible, but only for an error $3\varepsilon|A|^{1+1/2m}$.]*

(d) How does this compare to the Bohr set found by Theorem 10, the almost-periodicity result proved in lectures?

Solution: Part(a). Note that

$$\alpha N = |A| = \|1_A\|_2^2 = \|\widehat{1_A}\|_2^2 \geqslant \frac{1}{N}|\Delta_\eta(A)|(\eta|A|)^2 = \alpha^2\eta^2 N|\Delta_\eta(A)|.$$

Rearranging gives $|\Delta_\eta(A)| \leqslant \eta^{-2}\alpha^{-1}$ as desired.

For part (b), for an arbitrary $t \in G$ we have

$$\begin{aligned}\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_2^2 &= \langle \tau_t(1_A * 1_A) - 1_A * 1_A, \tau_t(1_A * 1_A) - 1_A * 1_A\rangle_G \\ &= \langle \tau_t(\widehat{1_A * 1_A}) - \widehat{1_A * 1_A}, \tau_t(\widehat{1_A * 1_A}) - \widehat{1_A * 1_A}\rangle_{\widehat{G}} \\ &= \langle (f_t - 1)(\widehat{1_A})^2, (f_t - 1)(\widehat{1_A})^2\rangle_{\widehat{G}} \\ &= \mathop{\mathbb{E}}_{\gamma} |\widehat{1_A}(\gamma)|^4 |\gamma(t) - 1|^2,\end{aligned}$$

where $f_t(\gamma) := \gamma(t)$. Now suppose that $t \in \mathrm{Bohr}(\Delta_{\varepsilon/10}(A), \varepsilon/2)$. Then

$$\begin{aligned}
\mathop{\mathbb{E}}_{\gamma} |\widehat{1_A}(\gamma)|^4 |\gamma(t) - 1|^2 &= \frac{1}{N} \sum_{\gamma \in \Delta_\varepsilon(A)} |\widehat{1_A}(\gamma)|^4 |\gamma(t) - 1|^2 + \frac{1}{N} \sum_{\gamma \notin \Delta_\varepsilon(A)} |\widehat{1_A}(\gamma)|^4 |\gamma(t) - 1|^2 \\
&\leqslant \frac{\varepsilon^2}{4N} \sum_{\gamma} |\widehat{1_A}(\gamma)|^4 + \frac{4}{N}\Big(\frac{\varepsilon |A|}{10}\Big)^2 \sum_{\gamma} |\widehat{1_A}(\gamma)|^2 \\
&\leqslant \frac{\varepsilon^2 |A|^3}{4} + \frac{\varepsilon^2 |A|^3}{25} \\
&\leqslant \varepsilon^2 |A|^3.
\end{aligned}$$

This is since

$$\mathop{\mathbb{E}}_{\gamma} |\widehat{1_A}(\gamma)|^4 = |\{a_1, a_2, a_3, a_4 \in A : a_1 + a_2 = a_3 + a_4\}| \leqslant |A|^3$$

and $\mathbb{E}_\gamma |\widehat{1_A}(\gamma)|^2 = \sum_x 1_A(x)^2 = |A|$. Therefore t is an L^2-almost period for $1_A * 1_A$ with error $\varepsilon |A|^{3/2}$. Since $|\Delta_{\varepsilon/10}(A)| \ll \varepsilon^{-2}\alpha^{-1}$ by part (a), $\mathrm{Bohr}(\Delta_{\varepsilon/10}(A), \varepsilon/2)$ has rank $O(\varepsilon^{-2}\alpha^{-1})$ and width $\gg \varepsilon$ as required.

For part (c), Fourier expanding we get that $\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_{2m}^{2m}$ is equal to

$$\begin{aligned}
&\sum_x \Big| \mathop{\mathbb{E}}_{\gamma} (\gamma(t) - 1)\gamma(x) \widehat{1_A}(\gamma)^2 \Big|^{2m} \\
&= \mathop{\mathbb{E}}_{\substack{\gamma_1, \dots, \gamma_m \\ \rho_1, \dots, \rho_m}} \prod_{i \leqslant m} (\gamma_i(t) - 1)\widehat{1_A}(\gamma_i)^2 \prod_{j \leqslant m} \overline{(\rho_j(t) - 1)\widehat{1_A}(\rho_j)^2} \sum_x \prod_{i \leqslant m} \gamma_i(x) \prod_{j \leqslant m} \overline{\rho_j(x)} \\
&\leqslant \frac{1}{N^{2m-1}} \sum_{\substack{\gamma_1, \dots, \gamma_m \\ \rho_1, \dots, \rho_m \\ \prod \gamma_i = \prod \rho_j}} \prod_{i \leqslant m} |\gamma_i(t) - 1| |\widehat{1_A}(\gamma_i)|^2 \prod_{j \leqslant m} |\rho_j(t) - 1| |\widehat{1_A}(\rho_j)|^2. \qquad (1)
\end{aligned}$$

Now suppose that $t \in \mathrm{Bohr}(\Delta_{\varepsilon^m/100}(A), \varepsilon)$. The contribution to the sum (1) when all $\gamma_1, \dots, \gamma_m, \rho_1, \dots, \rho_m \in \Delta_{\varepsilon^m/100}(A)$ is at most

$$\frac{1}{N^{2m-1}} \varepsilon^{2m} \sum_{\substack{\gamma_1, \dots, \gamma_m \\ \rho_1, \dots, \rho_m \\ \prod \gamma_i = \prod \rho_j}} \prod_{i \leqslant m} |\widehat{1_A}(\gamma_i)|^2 \prod_{j \leqslant m} |\widehat{1_A}(\rho_j)|^2.$$

Applying the L^∞ bound $|\widehat{1_A}(\rho_{2m})|^2 \leqslant |A|^2$, we get an upper bound of

$$\begin{aligned}
&\frac{1}{N^{2m-1}} \varepsilon^{2m} |A|^2 \sum_{\substack{\gamma_1, \dots, \gamma_m \\ \rho_1, \dots, \rho_{m-1}}} \prod_{i \leqslant m} |\widehat{1_A}(\gamma_i)|^2 \prod_{j \leqslant m-1} |\widehat{1_A}(\rho_j)|^2 \\
&\leqslant \varepsilon^{2m} |A|^{2+2m-1} = \varepsilon^{2m} |A|^{2m+1}
\end{aligned}$$

by Parseval.

Now consider the contribution to the sum (1) when at least one out of the characters $\gamma_1, \dots, \gamma_m, \rho_1, \dots, \rho_m$ is not in $\Delta_{\varepsilon^m/100}(A)$. Let σ be this character. Then, using the trivial bounds $|\gamma_i(t) - 1| \leqslant 2$, $|\rho_j(t) - 1| \leqslant 2$, and $|\widehat{1_A}(\sigma)|^2 \leqslant (\varepsilon^m |A|/100)^2$, and renaming indices, we may upper bound the contribution to (1) by

$$\begin{aligned}
&2m \cdot \frac{2^{2m}}{N^{2m-1}} \Big(\frac{\varepsilon^m |A|}{100}\Big)^2 \sum_{\substack{\gamma_1, \dots, \gamma_m \\ \rho_1, \dots, \rho_{m-1}}} \prod_{i \leqslant m} |\widehat{1_A}(\gamma_i)|^2 \prod_{j \leqslant m-1} |\widehat{1_A}(\rho_j)|^2 \\
&\leqslant \frac{2^{2m+1} m \varepsilon^{2m}}{100^2} |A|^{2+2m-1},
\end{aligned}$$

by Parseval, as above. So therefore we conclude that

$$\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_{2m}^{2m} \leqslant \varepsilon^{2m}|A|^{2m+1}\Big(1 + \frac{2^{2m+1}m}{100^2}\Big),$$

and hence

$$\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_{2m} \leqslant 3\varepsilon|A|^{1+1/2m}.$$

So τ is an L^{2m} -almost period of $1_A * 1_A$ with error $3\varepsilon|A|^{1+1/2m}$. And by part (a), the rank of the Bohr set $\mathrm{Bohr}(\Delta_{\varepsilon^m/100}(A), \varepsilon)$ is $O(\varepsilon^{-2m}\alpha^{-1})$.

For part (d), we look to applying Theorem 10 with $f = 1_A * 1_A$. In this case, $\|\widehat{f}\|_1 = |A| = \alpha N$. So, having an error $3\varepsilon|A|^{1+1/2m}$ is like having an error $3\varepsilon\alpha^{1/2m}\|\widehat{f}\|_1 N^{1/2m}$. Applying Theorem 10, this gives a Bohr set of L^{2m} almost periods with error $3\varepsilon|A|^{1+1/2m}$ with rank $O(m\varepsilon^{-2}\alpha^{-\frac{1}{m}})$ and width $\gg \varepsilon\alpha^{1/2m}$. We got a narrower width in our solution here, but with a massively larger rank $O(\varepsilon^{-2m}\alpha^{-1})$.

(2) Show that if A, B, C are sets with $|C| \geqslant |B|$ such that there is S with $|A+S| \leqslant K|A|$ then the set T of L^∞-almost periods for $1_A * 1_B * 1_C$ with error $\varepsilon|A||B|$ has size

$$|T| \gg \exp(-O(\varepsilon^{-2}(1 + \log(\frac{|C|}{|B|})) \log K))|S|.$$

Solution: Let m be a natural number with

$$\frac{1}{2}(1 + \log(|C|/|B|)) \leqslant m \leqslant 1 + \log(|C|/|B|).$$

Observe that

$$\begin{aligned}
&\max_x |\tau_t(1_A * 1_B * 1_C) - 1_A * 1_B * 1_C|\\
&= \max_x \Big|\sum_{y,z}(1_A(y)1_B(z)1_C(x+t-y-z) - 1_A(y)1_B(z)1_C(x+-y-z))\Big|\\
&= \max_x \Big|\sum_z 1_B(z)\sum_y(1_A(y)1_C(x+t-y-z) - 1_A(y)1_C(x-y-z))\Big|\\
&\leqslant \max_x \Big(\sum_z 1_B(z)^{\frac{2m}{2m-1}}\Big)^{\frac{2m-1}{2m}}\Big(\sum_z\Big(\sum_y(1_A(y)1_C(x+t-y-z) - 1_A(y)1_C(x-y-z))\Big)^{2m}\Big)^{\frac{1}{2m}}\\
&= |B|^{1-\frac{1}{2m}}\|\tau_t(1_A * 1_C) - 1_A * 1_C\|_{2m}.
\end{aligned}$$

Suppose that t is an L^{2m}-almost period of $1_A * 1_C$ with error $\frac{1}{100}\varepsilon|A||C|^{\frac{1}{2m}}$. Then

$$\begin{aligned}
\|\tau_t(1_A * 1_B * 1_C) - 1_A * 1_B * 1_C|\|_\infty &\leqslant \frac{1}{100}\varepsilon|A||B|^{1-\frac{1}{2m}}|C|^{\frac{1}{2m}}\\
&= \frac{1}{100}\varepsilon|A||B|\Big(\frac{|C|}{|B|}\Big)^{\frac{1}{2m}}\\
&< \varepsilon|A||B|.
\end{aligned}$$

So τ is an L^∞ almost period of $1_A * 1_B * 1_C$ with error $\varepsilon|A||B|$. Finally, by Theorem 12 from lectures, the number of such almost periods t is at least $\exp(-O(\varepsilon^{-2}m)\log K))|S|$, as required.

(3) Suppose that $|A|$ and x are such that $1_A * 1_A * 1_A(x) \geqslant \delta|A|^2$. Suppose further that there is some S such that $|A + S| \leqslant K|A|$. Show that, for any $k \geqslant 1$, there is a symmetric set X such that

$$x + kX \subset A + A + A$$

and
$$|X| > \exp(-O(k^2\delta^{-2}\log K))|S|.$$

Solution: This follows from the previous question. Indeed, let X be the set of L^∞ almost periods for $1_A * 1_A * 1_A$ with error $\frac{\delta}{2k}|A|^2$. From the previous question we have
$$|X| > \exp(-O(k^2\delta^{-2}\log K))|S|.$$
However, if $t \in kX$, write $t = t_1 + \cdots + t_k$ with $t_i \in X$ for all i. Let $t_0 := 0$. Then, by the triangle inequality,
$$\begin{aligned}|1_A * 1_A * 1_A(x+t) - 1_A * 1_A * 1_A(x)| &\leqslant \sum_{i \leqslant k} |1_A * 1_A * 1_A(x+t_i) - 1_A * 1_A * 1_A(x+t_{i-1})| \\ &\leqslant k \cdot \frac{\delta}{2k}|A|^2 \\ &= \frac{\delta}{2}|A|^2.\end{aligned}$$
Since $1_A * 1_A * 1_A(x) \geqslant \delta|A|^2$ we conclude that
$$1_A * 1_A * 1_A(x+t) > \frac{\delta}{2}|A|^2 > 0.$$
Hence $x + t \in A + A + A$, and so $x + kX \subset A + A + A$.

(4) Show that if $A, B \subset \mathbb{F}_p^n$ with densities α, β respectively then $A + B$ contains a coset of a subspace of dimension $\gg \alpha\beta n/\log p$.

Solution: Let $N = p^n$ be the size of the group, and let $f = 1_A * 1_B$. Then
$$\|\widehat{f}\|_1 = \mathop{\mathbb{E}}_\gamma |\widehat{1_A}(\gamma)||\widehat{1_B}(\gamma)| \leqslant (\mathop{\mathbb{E}}_\gamma |\widehat{1_A}(\gamma)|^2)^{\frac{1}{2}}(\mathop{\mathbb{E}}_\gamma |\widehat{1_B}(\gamma)|^2)^{\frac{1}{2}} = |A|^{\frac{1}{2}}|B|^{\frac{1}{2}} = \alpha^{\frac{1}{2}}\beta^{\frac{1}{2}}N.$$

Let T be the set of L^{2m}-almost periods of f with error $\frac{1}{4}\alpha^{\frac{1}{2}}\beta^{\frac{1}{2}}\|\widehat{f}\|_1 N^{\frac{1}{2m}}$. We know from Theorem 10 in lectures, applied to $\varepsilon = \frac{1}{4}\alpha^{\frac{1}{2}}\beta^{\frac{1}{2}}$, that T contains a Bohr set of rank $O(m\alpha^{-1}\beta^{-1})$ and width $\gg \alpha^{\frac{1}{2}}\beta^{\frac{1}{2}}$. So certainly T contains a subspace V of codimension $O(m\alpha^{-1}\beta^{-1})$.

Next, let $W \subset T$ be any subset. Then, for a natural number m to be chosen later,
$$\begin{aligned}\sum_x \sup_{t \in W} |1_A * 1_B(x+t) - 1_A * 1_B(x)| &\leqslant \sum_x \Big(\sum_{t \in W} |1_A * 1_B(x+t) - 1_A * 1_B(x)|^{2m}\Big)^{\frac{1}{2m}} \\ &\leqslant N^{1-\frac{1}{2m}}\Big(\sum_x \sum_{t \in W} |1_A * 1_B(x+t) - 1_A * 1_B(x)|^{2m}\Big)^{\frac{1}{2m}} \\ &\leqslant N^{1-\frac{1}{2m}}|W|^{\frac{1}{2m}} \max_{t \in W} \|\tau_t(1_A * 1_B) - 1_A * 1_B\|_{2m} \\ &\leqslant N^{1-\frac{1}{2m}}|W|^{\frac{1}{2m}} \cdot \frac{\alpha^{\frac{1}{2}}\beta^{\frac{1}{2}}}{4}\|\widehat{f}\|_1 N^{\frac{1}{2m}} \\ &\leqslant |W|^{\frac{1}{2m}}\frac{\alpha\beta N^2}{4} \\ &< \alpha\beta N^2\end{aligned}$$
provided $|W| < 4^{2m}$. Since
$$\sum_x 1_A * 1_B(x) = \alpha\beta N^2,$$

we conclude that there is some x for which

$$\sup_{t\in W} |1_A * 1_B(x+t) - 1_A * 1_B(x)| < 1_A * 1_B(x).$$

Hence $1_A * 1_B(x+t) > 0$ for all $t \in W$, and so $x + W \subset A + B$.

The rest of the proof is just sorting out the quantitative details. Let $10 < C_1 = O(1)$ be a fixed constant such that $\dim(V) \geqslant n - C_1 m\alpha^{-1}\beta^{-1}$. If $n\alpha\beta \leqslant 100C_1$ then the conclusion of the theorem is trivial, so without loss of generality $n\alpha\beta \geqslant 100C_1$.

Now let $c < 1/100$ be a small constant (to be chosen later, depending on C_1). Let C be a large parameter with the following properties: $C_1 \leqslant C < 2C_1$ and

$$\frac{n\alpha\beta}{C}\Big(1 - \frac{c\alpha\beta}{\log p}\Big) \in \mathbb{N}.$$

This is possible, since

$$\frac{n\alpha\beta}{C_1}\Big(1 - \frac{c\alpha\beta}{\log p}\Big) \geqslant 50.$$

Now let

$$m = \frac{n\alpha\beta}{C}\Big(1 - \frac{c\alpha\beta}{\log p}\Big).$$

In this case

$$\dim V \geqslant n - Cm\alpha^{-1}\beta^{-1} = c\frac{\alpha\beta n}{\log p}.$$

Let $W \leqslant V$ be a subspace with dimension

$$c\frac{\alpha\beta n}{\log p} - 1 \leqslant \dim W \leqslant c\frac{\alpha\beta n}{\log p}.$$

It is enough to show that

$$|W| < 4^{2m}$$

if c is small enough, since then $x + W \subset A + B$ by the above argument.

We can calculate

$$\begin{aligned}\log(4^{2m}/|W|) &\geqslant 2m\log 4 - (\dim W)\log p \\ &\geqslant \frac{2n\alpha\beta\log 4}{C}\Big(1 - c\frac{\alpha\beta}{\log p}\Big) - c\alpha\beta n \\ &\geqslant \alpha\beta n\Big(\frac{\log 4}{C_1}\Big(1 - c\frac{1}{\log p}\Big) - c\Big) \\ &> 0\end{aligned}$$

if c is small enough. So we are done.

(5) Let G be a finite abelian group and $A \subset G$ have density $\alpha = |A|/|G|$. Let $\varepsilon > 0$ and T be the set of L^2-almost periods of $1_A \times 1_A$ with error $\varepsilon|A|^{3/2}$.
   (a) Show that if $\varepsilon \geqslant 2$ then $T = G$.
   (b) Show that $|T| \gg \alpha^{O(\varepsilon^{-2})}N$.
   (c) Show that T contains a Bohr set of rank $O(\varepsilon^{-2}\alpha^{-1})$ and width $\gg \varepsilon\alpha^{1/2}$.
   (d) Show that if $\Delta_\eta(A)$ is defined as in Question 1 then, for any $\eta > 0$ the set of almost-periods T is contained inside the Bohr set with frequency set $\Delta_\eta(A)$ and width $\eta^{-2}\varepsilon\alpha^{-1/2}$.

Solution: For part (a), for an arbitrary $t \in G$ note that

$$\begin{aligned}\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_2 &\leqslant \|\tau_t(1_A * 1_A)\|_2 + \|1_A * 1_A\|_2 \\ &= 2\|1_A * 1_A\|_2 \\ &= 2\Big(\sum_{x \in G}\Big(\sum_{a_1+a_2=x} 1_A(a_1)1_A(a_2)\Big)^2\Big)^{1/2} \\ &= 2\Big(\sum_{a_1+a_2=a_3+a_4} 1_A(a_1)1_A(a_2)1_A(a_3)1_A(a_4)\Big)^{1/2} \\ &\leqslant 2|A|^{3/2}.\end{aligned}$$

So t is an L^2 almost period of $1_A * 1_A$ with error $2|A|^{3/2}$.

For part (b), this is just the result of Theorem 11 from lectures with $m = 1$. Part (c) was just part (a) of Question 1.

For part (d), suppose that $\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_2 \leqslant \varepsilon|A|^{3/2}$. Then

$$\begin{aligned}\varepsilon^2|A|^3 &\geqslant \langle \tau_t(1_A * 1_A) - 1_A * 1_A, \tau_t(1_A * 1_A) - 1_A * 1_A\rangle_G \\ &= \langle \widehat{\tau_t(1_A * 1_A)} - \widehat{1_A * 1_A}, \widehat{\tau_t(1_A * 1_A)} - \widehat{1_A * 1_A}\rangle_{\widehat{G}} \\ &= \langle (f_t - 1)(\widehat{1_A})^2, (f_t - 1)(\widehat{1_A})^2\rangle_{\widehat{G}} \\ &= \frac{1}{N}\sum_{\gamma} |\widehat{1_A}(\gamma)|^4|\gamma(t) - 1|^2,\end{aligned}$$

where $f_t(\gamma) = \gamma(t)$. If $\gamma \in \Delta_\eta(A)$ we conclude that

$$\varepsilon^2|A|^3 \geqslant \frac{1}{N}|\widehat{1_A}(\gamma)|^4|\gamma(t) - 1|^2 \geqslant \eta^4\alpha^4N^3|\gamma(t) - 1|^2.$$

Hence $|\gamma(t) - 1| \leqslant \varepsilon\alpha^{-1/2}\eta^{-2}$ as required.

(6) (a) Show that if $X \subset \mathbb{F}_3^n$ is a symmetric set (so $X = -X$) such that $0 \in X$ and which contains at least k elements which are linearly independent over $\mathbb{F}_3$ then kX contains a subspace of dimension k.
(b) Show that if $K \geqslant 4$ and $A \subset \mathbb{F}_3^n$ satisfies $|A + A| \leqslant K|A|$ then $A + A - A - A$ contains a subspace of dimension $\gg \sqrt{\log|A|}/\log K$.

Solution: For part (a), let $Y \subset X$ with $|Y| = k$ and Y being linearly independent over $\mathbb{F}_3$. Then $-Y \cup \{0\} \cup Y \subset X$, since X is symmetric and contains 0. Therefore, writing

$$V = \{\sum_{i \leqslant k} \varepsilon_i y_i : \varepsilon_i \in \{-1, 0, 1\}\},$$

we have $V \subset kX$. But $V = \mathrm{span}_{\mathbb{F}^3}(Y)$. Hence V has dimension k, as desired.

For part (b), let C and c be certain absolute constants, with C large enough and c small enough for what follows. Without loss of generality we may also assume that $\sqrt{\log|A|}/\log K$ is large enough in terms of c and C. Since $K \geqslant 4$, this contains the assumption that $|A|$ is large enough in terms of c and C.

Now, we know from Theorem 13 that $A + A - A - A$ contains a set kT with

$$|T| \geqslant \exp(-Ck^2(\log K)^2)|A|.$$

Choose an integer k in the range $\frac{c}{2}\frac{\sqrt{\log|A|}}{\log K} \leqslant k \leqslant c\frac{\sqrt{\log|A|}}{\log K}$. Such an integer exists since $\frac{\log|A|}{\log K}$ is large enough. Then we get

$$|T| \geqslant \exp(-Cc^2\log|A|) \geqslant |A|^{0.99}$$

if c is small enough. Hence T contains a linearly independent set of size at least $\log(|A|^{0.99})/\log(3)$, which is at least k (as $|A|$ is large). By part (a), kT contains a subspace of dimension k.

(7) Let $f : G \longrightarrow \mathbb{C}$. In Lemma 26 we found by random sampling a function g which was the linear combination of $O(m\varepsilon^{-2})$ characters such that $\|f-g\|_{2m} \leqslant \varepsilon\|\widehat{f}\|_1 N^{1/2m}$. In this exercise we provide an example that shows that the linear dependence on m is necessary.

Let $2m \leqslant n$ and choose some linearly independent $\gamma_1,\ldots\gamma_{2m} \in \mathbb{F}_2^n$. We write $N = 2^n$ for the size of the group as usual. Let $f(x) = \frac{1}{2m}(\gamma_1(x)+\cdots+\gamma_{2m}(x))$. Out of all those functions which are linear combinations of $\leqslant m$ characters, let g be such that $\|f-g\|_{2m}$ is minimal.

(a) Show that without loss of generality, the characters in g are from the subspace spanned by $\gamma_1,\ldots,\gamma_{2m}$.
(b) Show that $N^{1/2m}|1-g(0)| \leqslant 2\|f-g\|_{2m}$.
(c) Let $V \leqslant \mathbb{F}_2^n$ be the subspace orthogonal to those characters in the definition of g. Show that

$$\Big(\sum_{x\in V}|f(x)-g(x)|^{2m}\Big)^{1/2m} \geqslant \Big(\frac{1}{2}-|1-g(0)|\Big)|V|^{1/2m}.$$

(d) Deduce that

$$\|f-g\|_{2m} \geqslant \frac{1}{8}\|\widehat{f}\|_1 N^{1/2m}.$$

Solution: Part (a). Let $W \leqslant \mathbb{F}_2^n$ be the intersection of the kernels of $\gamma_1,\ldots,\gamma_{2m}$. Then $f * \frac{1}{|W|}1_W = f$. Furthermore, $g * \frac{1}{|W|}1_W$ is a linear combination of characters from the subspace spanned by $\gamma_1,\ldots,\gamma_{2m}$. This is since the Fourier transform of $g * \frac{1}{|W|}1_W$ is $\frac{1}{|W|}\widehat{g}\widehat{1_W}$ and

$$\widehat{1}_W(\gamma) = \sum_{x\in W}\overline{\gamma(x)} = \begin{cases} |W| & \text{if } \gamma|_W \text{ is the trivial character,} \\ 0 & \text{otherwise} \end{cases}$$

since W is a subspace. By dimension counting, $\gamma|_W$ is trivial if and only if γ is in $\mathrm{span}_{\mathbb{F}_2}(\gamma_1,\ldots,\gamma_{2m})$.

Write $g' := g * \frac{1}{|W|}1_W$. Then, by Young's inequality

$$\|f-g'\|_{2m} = \|\frac{1}{|W|}1_W * (f-g)\|_{2m} \leqslant \|\frac{1}{|W|}1_W\|_1\|f-g\|_{2m} = \|f-g\|_{2m}.$$

So, replacing g by g', we may assume that g is a linear combination of characters from the subspace spanned by $\gamma_1,\ldots,\gamma_{2m}$.

Part (b). Let W be as in part (a). Then

$$\|f-g\|_{2m}^{2m} \geqslant \sum_{x\in W}|f(x)-g(x)|^{2m} = \sum_{x\in W}|f(0)-g(0)|^{2m} = 2^{-2m}N|1-g(0)|^{2m}.$$

Taking $2m^{th}$-roots gives the claimed bound.

Part (c). With V as given, we have

$$\Big(\sum_{x\in V}|f(x)-g(x)|^{2m}\Big)^{1/2m} \geqslant \Big(\sum_{x\in V}|f(x)-1|^{2m}\Big)^{1/2m} - \Big(\sum_{x\in V}|g(x)-1|^{2m}\Big)^{1/2m}$$

by the triangle inequality. By definition of V we have

$$\Big(\sum_{x\in V}|g(x)-1|^{2m}\Big)^{1/2m} = |V|^{1/2m}|g(0)-1|.$$

By Jensen's inequality, we have

$$\begin{aligned}\Big(\sum_{x\in V}|f(x)-1|^{2m}\Big)^{1/2m} &= |V|^{1/2m}\Big(\frac{1}{|V|}\sum_{x\in V}|f(x)-1|^{2m}\Big)^{1/2m}\\ &\geqslant |V|^{1/2m}\Big(\frac{1}{|V|}\sum_{x\in V}|f(x)-1|\Big)\\ &= |V|^{1/2m}\Big(1-\frac{1}{|V|}\sum_{x\in V}f(x)\Big)\\ &= |V|^{1/2m}\Big(1-\frac{1}{2m}\sum_{i\leqslant 2m}\frac{1}{|V|}\sum_{x\in V}\gamma_i(x)\Big),\end{aligned}$$

since $f(x)\in[-1,1]$ for all x. Now, we have

$$\frac{1}{|V|}\sum_{x\in V}\gamma_i(x) = \begin{cases}1 & \text{if } \gamma_i|_V \text{ is the trivial character;}\\ 0 & \text{otherwise.}\end{cases}$$

Since V has codimension at most m, there are at most m values of i for which $\gamma_i|_V$ is the trivial character. So

$$\Big(\sum_{x\in V}|f(x)-1|^{2m}\Big)^{1/2m} \geqslant |V|^{1/2m}\Big(1-\frac{1}{2m}m\Big) \geqslant \frac{1}{2}|V|^{1/2m}.$$

Combining everything we have

$$\|f-g\|_{2m} \geqslant \Big(\frac{1}{2}-|g(0)-1|\Big)|V|^{1/2m}$$

as claimed.

Part (d). We have $\|\widehat{f}\|_1 = 1$. If $|1-g(0)|\geqslant 1/4$, from part (b) we have $\|f-g\|_{2m}\geqslant \frac{1}{8}N^{1/2m}$, as claimed. Otherwise, we have from part (c) that $\|f-g\|_{2m}\geqslant \frac{1}{4}|V|^{1/2m}\geqslant\frac{1}{4}(N2^{-m})^{1/2m}\geqslant\frac{1}{8}N^{1/2m}$ too.

(8) We say that a set $D\subset G$ is *dissociated* if all $3^{|D|}$ sums of the form $\sum_{x\in D}c_x x$ where $c_x\in\{-1,0,1\}$ are distinct. Fix some dissociated set D.

(a) Show that for any $\varepsilon\in\{-1,1\}^D$, if

$$P_\varepsilon(\gamma)=\prod_{x\in D}(1+\Re(\varepsilon_x\gamma(x)))$$

then $\mathbb{E}_\gamma\,|P_\varepsilon(\gamma)|=1$.

(b) Show that for any $f: D\longrightarrow\mathbb{C}$ and $\varepsilon\in\{-1,1\}^D$, if

$$F_\varepsilon(\gamma)=\sum_{x\in D}\varepsilon_x f(x)\overline{\gamma(x)},$$

then $\widehat{f}=2F_\varepsilon * P_\varepsilon$.

(c) Combining parts (a) and (b) with the ideas in the proof of the Marcinkiewicz–Zygmund inequality, prove Rudin's inequality: if D is dissociated then for any $f : D \longrightarrow \mathbb{C}$ and any $m \geqslant 1$,

$$\|\widehat{f}\|_{2m} \ll m^{1/2}\|f\|_2.$$

Solution: For part (a), let $\operatorname{span}(D) = \{\sum_{x\in D} c_x x : c_x \in \{-1,0,1\}\}$. By assumption $|\operatorname{span}(D)| = 3^{|D|}$. Note that $1 + \Re(\varepsilon_x\gamma(x)) \geqslant 0$ for all ε, γ, x, so

$$\mathop{\mathbb{E}}_{\gamma} |P_\varepsilon(\gamma)| = \mathop{\mathbb{E}}_{\gamma} P_\varepsilon(\gamma) = \mathop{\mathbb{E}}_{\gamma} \prod_{x\in D}(1 + \frac{1}{2}\varepsilon_x\gamma(x) + \frac{1}{2}\varepsilon_x\gamma(-x)).$$

Multiplying out the product, we get

$$\mathop{\mathbb{E}}_{\gamma} \sum_{y\in\operatorname{span}(D)} \gamma(y) \prod_{x\in S_y} \frac{\varepsilon_x}{2},$$

where, writing $y = \sum_{x\in D} c_x x$ with $c_x \in \{-1,0,1\}$ in the unique way, S_y is the set of $x \in D$ for which $c_x \in \{-1,1\}$. Swapping the sums, the only non-zero contribution comes from when $y = 0$, i.e.

$$\mathop{\mathbb{E}}_{\gamma} \sum_{y\in\operatorname{span}(D)} \gamma(y) \prod_{x\in S_y} \frac{\varepsilon_x}{2} = \sum_{y\in\operatorname{span}(D)} \prod_{x\in S_y} \frac{\varepsilon_x}{2} \mathop{\mathbb{E}}_{\gamma} \gamma(y) = \mathop{\mathbb{E}}_{\gamma} \gamma(0) = 1$$

as claimed.

For part (b), we abuse notation somewhat and let $\widehat{F_\varepsilon} : G \longrightarrow \mathbb{C}$ denote the inverse Fourier transform of F_ε (and similarly for other functions defined on $\widehat{G}$). Then

$$\begin{aligned}
\widehat{F_\varepsilon}(x) &= \mathop{\mathbb{E}}_{\gamma} F_\varepsilon(\gamma)\gamma(x) \\
&= \mathop{\mathbb{E}}_{\gamma} \Big(\sum_{y\in D} \varepsilon_y f(y)\overline{\gamma(y)}\Big)\gamma(x) \\
&= \sum_{y\in D} \varepsilon_y f(y) \mathop{\mathbb{E}}_{\gamma} \gamma(x-y) \\
&= \sum_{y\in D} \varepsilon_y f(y) 1_{y=x},
\end{aligned}$$

and so

$$\widehat{F_\varepsilon}(x) = \begin{cases} \varepsilon_x f(x) & \text{if } x \in D \\ 0 & \text{otherwise.} \end{cases}.$$

Also,

$$\begin{aligned}
\widehat{P_\varepsilon}(x) &= \mathop{\mathbb{E}}_{\gamma} \prod_{y} (1 + \frac{1}{2}\varepsilon_y\gamma(y) + \frac{1}{2}\varepsilon_y\gamma(-y))\gamma(x) \\
&= \sum_{z\in\operatorname{span}(D)} \prod_{y\in S_z} \frac{\varepsilon_y}{2} \mathop{\mathbb{E}}_{\gamma} \gamma(x-z) \\
&= \sum_{z\in\operatorname{span}(D)} \prod_{y\in S_z} \frac{\varepsilon_y}{2} 1_{x=z}.
\end{aligned}$$

For $x \in D$, this is just $\varepsilon_x/2$. Therefore, since f is supported on D,

$$f = 2\widehat{F_\varepsilon}\widehat{P_\varepsilon}.$$

Taking Fourier transforms, we get

$$\widehat{f} = 2F_\varepsilon * P_\varepsilon$$

as claimed.

For part (c), we note that by Young's convolution inequality

$$\|F_\varepsilon * P_\varepsilon\|_{2m} \ll \|F_\varepsilon\|_{2m}\|P_\varepsilon\|_1 \leqslant \|F_\varepsilon\|_{2m}.$$

Hence, by part (b), $\|\widehat{f}\|_{2m} \ll \|F_\varepsilon\|_{2m}$ for all $\varepsilon \in \{-1,1\}^D$. So

$$\|\widehat{f}\|_{2m}^{2m} \leqslant C^{2m} \mathop{\mathbb{E}}_{\varepsilon} \|F_\varepsilon\|_{2m}^{2m}$$

for some absolute constant C.

Now,

$$\begin{aligned}\mathop{\mathbb{E}}_{\varepsilon} \|F_\varepsilon\|_{2m}^{2m} &= \mathop{\mathbb{E}}_{\varepsilon}\mathop{\mathbb{E}}_{\gamma} \Big|\sum_{x\in D} \varepsilon_x f(x)\overline{\gamma(x)}\Big|^{2m} \\ &= \mathop{\mathbb{E}}_{\gamma} \sum_{\substack{x_1,\dots,x_m \in D\\ y_1,\dots,y_m\in D}} \prod_{i\leqslant m} f(x_i)\overline{\gamma(x_i)} \prod_{j\leqslant m} \overline{f(y_j)}\gamma(y_j) \mathop{\mathbb{E}}_{\varepsilon} \prod_{i\leqslant m}\varepsilon_{x_i}\prod_{j\leqslant m}\varepsilon_{y_j}\end{aligned}$$

The inner sum $\mathbb{E}_\varepsilon \prod_{i\leqslant m}\varepsilon_{x_i}\prod_{j\leqslant m}\varepsilon_{y_j}$ vanishes unless every element of D which is listed in $(x_1,\dots,x_m,y_1,\dots,y_m)$ appears to an even order, in which case the inner sum equals 1. So we may upper bound the expression above by

$$\sum_{l\leqslant m}\sum_{x_1,\dots,x_l\in D}\sum_{k_1+\dots+k_l=m}\binom{2m}{2k_1,\dots,2k_l}\prod_{i\leqslant l}|f(x_i)|^{2k_i}.$$

As in the proof of the Marcinkiewicz–Zygmund inequality in lectures, this is at most $m^m\Big(\sum_{x\in D}|f(x)|^2\Big)^m$, since by comparing binomial coefficients

$$\frac{(2m)!}{(2k_1)!\cdots(2k_l)!} \leqslant \frac{(2m)!}{2^m m!}\frac{m!}{k_1!\cdots k_l!} \leqslant m^m\frac{m!}{k_1!\cdots k_l!}.$$

Therefore

$$\|\widehat{f}\|_{2m} \leqslant C^{2m}m^m\|f\|_2^{2m},$$

and the result follows by taking $2m^{th}$-roots.

(9) Let the *dimension* of a set A, denoted by $\dim(A)$, be the size of the largest dissociated subset of A.
  (a) Show that if X is a dissociated set then for all $k\geqslant 1$ we have $|kX|\geqslant (Ck)^{-k}|X|^k$ for some absolute constant $C>0$.
  (b) Deduce that if $|A+A|\leqslant K|A|$ then $\dim(A)\ll K\log|A|$.
  (c) Use the above ideas combined with Theorem 13 from lectures to show that if $|A+A|\leqslant K|A|$ then there exists a set $X\subset A$ of size

$$|X|\geqslant \exp(-O((\log K)^4))|A|$$

such that $\dim(X)\ll \log|A|$.

Solution: Part (a). There are two approaches here. Either observe that $\|\widehat{1_X}\|_{2k}^{2k} = E_{2k}(X) = \#x_1+\dots+x_k = x_{k+1}+\dots+x_{2k}$. By Cauchy-Schwarz,

$$|X|^k = \sum_{g\in kX}|\{(x_1,\dots,x_k)\in X^k : x_1+\dots+x_k = g\}| \leqslant |kX|^{1/2}(E_{2k}(X))^{1/2}.$$

Finally, rearranging and using Rudin's inequality, there is some constant C for which

$$|kX| \geqslant \frac{|X|^{2k}}{E_{2k}(X)} \geqslant \frac{|X|^{2k}}{(Ck^{1/2})^{2k}\|1_X\|_2^{2k}} = (C^2k)^{-k}|X|^k$$

as required.

Alternatively, here is a more hands-on approach. Assume that $|X| \geqslant 100k$, else the conclusion is trivial. Let $k^\wedge X$ denote the restricted sum set, i.e $k^\wedge X = \{x_1 + \cdots + x_k : x_i \in X \text{ distinct.}\}$. We claim that $|k^\wedge X| \geqslant k^{-k}(|X| - k)^k$. Indeed, if $g = x_1 + \cdots + x_k = y_1 + \cdots + y_k$, with the $x_i \in X$ distinct and the $y_i \in X$ distinct, then $0 = x_1 + \cdots + x_k - y_1 - \cdots - y_k \in \operatorname{span}(X)$, contradicting the fact that X is dissociated unless $(y_1, \ldots, y_k)$ is a permutation of $(x_1, \ldots, x_k)$. Hence

$$\begin{aligned}|k^\wedge X| &\geqslant k^{-k}|\{(x_1, \ldots, x_k) \in X^k : \text{ all indices distinct}\}| \\ &\geqslant k^{-k}(|X| - k)^k \\ &\geqslant (Ck)^{-k}|X|^k\end{aligned}$$

as claimed.

For part (b), let X be the largest dissociated subset of A. Then by Plünnecke and part (a), for all $k \geqslant 1$ we have

$$(Ck)^{-k} \dim(A)^k \leqslant |kX| \leqslant |kA| \leqslant K^k|A|.$$

Hence $\dim(A) \leqslant CKk|A|^{1/k}$. Choosing $k \asymp \log |A|$ we derive $\dim(A) \ll K \log |A|$ as desired.

For part (c), let $k \asymp (\log K)$ and let T be the set of almost periods used in Theorem 13, for which $kT \subset A + A - A - A$ and $|T| \geqslant \exp(-O((\log K)^4))|A|$.

There is another fact about T which follows from the proof of Theorem 12 (which we used to construct the almost periods used in Theorem 13), namely that T may be taken to lie within a translate of A.

Then $klT \subset 2lA - 2lA$, so $|klT| \leqslant K^{4l}|A|$ for all $l \geqslant 1$, by Plünnecke. Now, let X be a translate of T with $X \subset A$. We have $|klX| \leqslant K^{4l}|A|$ and $|X| \geqslant \exp(-O((\log K)^4))|A|$ too.

Let $Y \subset X$ be a dissociated set of maximal size. Then

$$(Ckl)^{-kl} \dim(X)^{kl} = (Ckl)^{-kl}|Y|^{kl} \leqslant |klY| \leqslant |klX| \leqslant K^{4l}|A|.$$

So

$$\dim(X) \leqslant CklK^{\frac{4}{k}}|A|^{\frac{1}{kl}} \ll Ckl|A|^{\frac{1}{kl}}$$

since $k \asymp \log K$. Letting $l \asymp k^{-1} \log |A|$, we get

$$\dim(X) \ll \log |A|$$

as required.