LINEAR METHODS IN ADDITIVE COMBINATORICS - EXERCISES

THOMAS F. BLOOM

In all exercises G denotes an arbitrary finite abelian group.

1. Basics of Fourier Analysis

(1) (a) Give a simple explanation why $\widehat{G}$ is a finite abelian group.
(b) Use the orthogonality relationships and inverse formula to prove that $|G| = |\widehat{G}|$.

(2) Prove that $\widehat{f}(\gamma)$ is a non-negative real number for all $\gamma \in \widehat{G}$ if and only if $f = g \circ g$ for some $g : G \to \mathbb{C}$.

(3) Prove that for all $A \subseteq G$
$$|A|^{1/2} \geq \mathop{\mathbb{E}}_{\gamma} |\widehat{1_A}(\gamma)| \geq 1,$$
and give examples that show these bounds are best possible, up to constants.

(4) Prove that for any $A \subseteq G$ of density $\alpha = |A| / |G|$ and $\Delta \subseteq \widehat{G}$ and integer $m \geq 1$
$$\left(\sum_{\gamma \in \Delta} |\widehat{1_A}(\gamma)| \right)^{2m} \leq \alpha^{-1} |A|^{2m} \#\{\gamma_1, \ldots, \gamma_{2m} \in \Delta : \gamma_1 + \cdots + \gamma_m = \gamma_{m+1} + \cdots + \gamma_{2m}\}.$$
[*Hint: Find a way to change the order of summation on the left-hand side and apply Hölder's inequality.*]

2. Applications of Fourier Analysis

(1) (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 subgroup.
(b) Use Fourier analysis to prove that $|A + A| = |A|$ if and only if A is a translate of a subgroup. *(There are simple elementary proofs of this fact, but it is instructive to find a Fourier analytic proof.)*

(2) Let P be a property that is translation invariant (i.e. if A has property P then so does $A - x$ for all $x \in G$). Suppose we knew the following for some functions $D, \delta : [0, 1] \to \mathbb{R}$:

> If $A \subseteq \mathbb{F}_p^n$ is a subset of density α that satisfies property P then either
> (a) $|A| \ll p^{n/2}$ or
> (b) there is a subspace $V \leq \mathbb{F}_p^n$ of codimension $\leq D(\alpha)$ and a translate x such that $|(A - x) \cap V| / |V| \geq (1 + \delta(\alpha))\alpha$.

(So that e.g. in the first lecture we proved this is true when P is 'does not contain non-trivial three-term arithmetic progressions' with $D(\alpha) = 1$ and $\delta(\alpha) \gg \alpha$.)

What upper bounds can you deduce for the maximal size of a subset of $\mathbb{F}_p^n$ which satisfies property P if...
(a) $D(\alpha) \ll 1$ and $\delta(\alpha) \gg \alpha$,
(b) $D(\alpha) \ll \alpha^{-1}$ and $\delta(\alpha) \gg 1$, or
(c) $D(\alpha) \ll 1$ and $\delta(\alpha) \gg 1$.

What goes wrong if P is not translation invariant? Give an example of a non-translation invariant property P such that the boxed claim above holds with $D(\alpha) \ll 1$ and $\delta(\alpha) \gg \alpha$, and yet there is a set $A \subseteq \mathbb{F}_p^n$ of density $\gg 1$ satisfying property P.

(3) (a) Prove that if $A\subseteq G$ with density $\alpha>0$ and $\lvert\widehat{1_A}(\gamma)\rvert<\alpha^{1/2}\lvert A\rvert$ for all $\gamma\neq\mathbf{1}$ then $A+A-A-A=G$.
(b) Using the density increment strategy (e.g. as in Question 2) deduce that if $A\subseteq\mathbb{F}_p^n$ with density $\alpha=\lvert A\rvert/p^n$ then $A+A-A-A$ contains a coset of a subspace with codimension $O(\alpha^{-1/2})$.
(c) If $\lvert\mathbf{x}\rvert$ is the Hamming weight of $\mathbf{x}\in\mathbb{F}_2^n$, i.e. the number of 1s in $\mathbf{x}$, then let

$$A=\{\mathbf{x}\in\mathbb{F}_2^n:\lvert\mathbf{x}\rvert\geq n/2+\sqrt{n}\}.$$

Show that (for large n) we have $\lvert A\rvert\gg 2^n$ [*Hint: think probabilistically and use e.g. Hoeffding's inequality*] and any coset of a subspace contained inside $A+A$ has codimension $\gg\sqrt{n}$. (In particular, it is not possible to guarantee a coset of a subspace with codimension $O(1)$ in $A+A$ even when $\alpha\gg 1$.)

(4) (a) Using Fourier analysis and the density increment method prove that if $A\subseteq\mathbb{F}_p^n$ with density α is a 'Sidon set' (i.e. $a+b=c+d$ has only the trivial solutions $\{a,b\}=\{c,d\}$) then

$$\alpha\ll 1/n^2.$$

(b) Find a completely different and much simpler argument (not using Fourier analysis) that shows

$$\alpha\ll p^{-n/2}.$$

(5) (a) Let p be an odd prime and $A=\{x^2:x\in\mathbb{F}_p\}$. Prove that for any non-trivial character $\gamma\neq 1$

$$\lvert\widehat{1_A}(\gamma)\rvert\leq\frac{\sqrt{p}+1}{2}.$$

(b) Deduce that, for any $x\in\mathbb{F}_p$ and $k\geq 3$, the number of representations of x as the sum of k squares in $\mathbb{F}_p$ is

$$2^{-k}p^{k-1}+O(p^{k-2}).$$

3. Almost Periodicity

(1) Adapt the proof given in lectures to prove that if $A,B,S\subseteq G$ have $\lvert A+S\rvert\leq K\lvert A\rvert$ then there exists some set $T\subseteq S$ of size

$$\lvert T\rvert\geq\exp(-O(q\epsilon^{-2}\log K)\lvert S\rvert$$

such that, for all $t\in T-T$,

$$\lVert\tau_t(1_A*1_B)-1_A*1_B\rVert_q\leq\epsilon\lvert A\rvert\lvert B\rvert^{1/q}.$$

(2) Suppose that $\lvert A+A\rvert\leq K\lvert A\rvert$. Show that, for any $k\geq 1$, there is a set X such that

$$kX\subseteq A+A-A-A$$

and

$$\lvert X\rvert\geq\exp(-O(k^2(\log K)^2))\lvert A\rvert.$$

(3) Suppose that $\lvert A+A\rvert\leq K\lvert A\rvert$ and there are at least $\delta\lvert A\rvert^2$ solutions to $a+b+c=0$ with $a,b,c\in A$. Show that, for any $k\geq 1$ there is a set X such that

$$kX\subseteq A+A+A$$

and

$$\lvert X\rvert\geq\exp(-O(k^2\delta^{-2}(\log K)^2))\lvert A\rvert.$$

(4) (a) Show that if $X\subseteq\mathbb{F}_3^n$ 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 $K\geq 4$ and $A\subseteq\mathbb{F}_3^n$ satisfies $\lvert A+A\rvert\leq K\lvert A\rvert$ then $A+A-A-A$ contains a subspace of dimension $\gg\sqrt{\log\lvert A\rvert}/\log K$.

(5) (a) Let $q \geq 2$ and $\epsilon > 0$. Let $f : G \to \mathbb{C}$. Prove that there exist $k \ll q\epsilon^{-2}$ characters $\gamma_1, \ldots, \gamma_k \in \widehat{G}$ with associated $c_i \in \mathbb{C}$ with $|c_i| = 1$ such that

$$\|f - \tfrac{1}{k}\sum_i c_i\gamma_i\|_q \leq \epsilon \left(\mathop{\mathbb{E}}_{\gamma} |\widehat{f}(\gamma)|\right) |G|^{1/q}.$$

[*Hint: Choose* $\gamma_1, \ldots, \gamma_k \in \widehat{G}$ *randomly and independently with probability proportionate to* $|\widehat{f}(\gamma)|$, *and use the Marcinkiewicz-Zygmund inequality in a similar way as in lectures. Be careful of normalisations!*]

(b) Deduce that for any $f : G \to \mathbb{C}$ there exists a subspace V of codimension $O(q\epsilon^{-2})$ such that for all $t \in V$

$$\|\tau_t f - f\|_q \leq \epsilon \left(\mathop{\mathbb{E}}_{\gamma} |\widehat{f}(\gamma)|\right) |G|^{1/q}.$$

(c) Deduce that for any $A \subseteq G$ of density α there exists a subspace V of codimension $O(q\epsilon^{-2}\alpha^{-2/q})$ such that for all $t \in V$

$$\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_q \leq \epsilon |A|^{1+1/q}.$$

How does this compare to what the almost-periodicity result from lectures gives?

(6) Let q be some large integer and $\alpha > 0$ be some small constant.

(a) Prove that if $\alpha > 0$ and $A \subseteq \mathbb{F}_2^q$ is a random set where we include each element $x \in \mathbb{F}_2^q$ independently with probability α then $\mathbb{E}|A| = \alpha 2^q$ and for any $t \neq 0$

$$\mathbb{E}\, 1_A * 1_A(t) = \alpha^2 2^q.$$

(b) Using some kind of concentration inequality (e.g. Hoeffding) deduce that there exists some $A \subseteq \mathbb{F}_2^q$ such that

$$|A| \geq \tfrac{1}{2}\alpha 2^q$$

and for all $y \neq 0$

$$1_A * 1_A(y) \leq 2\alpha^2 2^q.$$

Deduce that for any $t \neq 0$

$$\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_q \gg |A|^{1+1/q}.$$

(c) Show that the linear dependence on q in almost-periodicity is best possible, in that for any large n there exists a set $A \subseteq \mathbb{F}_2^n$ of density $\gg 1$ such that, for some $\epsilon \gg 1$, if T is the set of t with

$$\|\tau_t(1_A * 1_A) - 1_A * 1_A\|_q \leq \epsilon |A|^{1+1/q}$$

then

$$|T| \leq 2^{n-cq}$$

for some constant $c > 0$.

(7) Let $A \subseteq \mathbb{F}_p^n$ with density α and $V \leq \mathbb{F}_p^n$ be a subspace. Prove that if there is $B \subseteq V$ with $|B| \gg |V|$ such that

$$\|\mu_B * 1_A \circ 1_A\|_\infty \geq (1 + c)\alpha |A|$$

then there is a subspace $W \leq V$ of codimension (relative to V) $\ll \mathcal{L}(\alpha)^{O(1)}$ such that

$$\|\mu_W * 1_A\|_\infty \geq (1 + c/32)\alpha.$$

[*This is a useful trick that allows one to upgrade 'density increment on 1% of a subspace' to increment on a genuine subspace.*]