Kelley and Meka's proof of Roth's theorem

by

Marcel K. Goh

5 August 2023

1. Introduction

Let A be a subset of $\mathbf{Z}$. We want to know how dense A can be before it must contain a subset $\{x, y, z\} \subseteq A$ with $x + z = 2y$, that is, an arithmetic progression of length 3.

Basic definitions and elementary lemmas. We will use G primarily to refer to a finite abelian group, on which we have the normalised counting measure. For functions $f, g : G \to \mathbf{C}$ we have the inner product

$$\langle f, g\rangle = \mathbf{E}_{x\in G}\, f(x)\overline{g(x)}$$

and the L_p norm

$$\|f\|_p = \Bigl(\mathbf{E}_{x\in G}\bigl|f(x)\bigr|^p\Bigr)^{1/p}.$$

In L_p spaces we have the useful Hölder inequality

$$\bigl|\langle f, g\rangle\bigr| \le \|f\|_p \cdot \|g\|_{1-p},$$

for $p, q \in [1, \infty]$ with $1/p + 1/q = 1$. Assuming now that f and g are $\mathbf{R}$-valued, we also have the convolution

$$(f * g)(x) = \mathbf{E}_{y\in G}\, f(y)g(x - y)$$

and the difference convolution

$$(f \circ g)(x) = \mathbf{E}_{y\in G}\, f(y)g(x + y)$$

that are related by the following adjoint property.

Lemma 1 (*Adjoint property*). *Let G be a finite abelian group and let $f, g, h : G \to \mathbf{R}$. Then*

$$\langle f, g * h\rangle = \langle h \circ f, g\rangle.$$

Proof. First expand

$$\begin{aligned}\langle f, g * h\rangle &= \mathbf{E}_{x\in G}\, f(x)(g * h)(x)\\ &= \mathbf{E}_{x\in G}\, f(x)\,\mathbf{E}_{y\in G}\, g(y)h(x - y)\\ &= \mathbf{E}_{y\in G}\, g(y)\,\mathbf{E}_{x\in G}\, f(x)h(x - y).\end{aligned}$$

Then substituting $z = x - y$ so that $x = z + y$ yields

$$\begin{aligned}\langle f, g * h\rangle &= \mathbf{E}_{y\in G}\, g(y)\, \mathbf{E}_{z\in G}\, f(z+y)h(z)\\ &= \mathbf{E}_{z\in G}(h \circ f)(z)g(z)\\ &= \langle h\circ f, g\rangle. \quad \blacksquare\end{aligned}$$

For a group G the dual group $\widehat{G}$ is the set of all homomorphisms from $G \to \mathbf{C}^\times$. The Fourier transform of $f : G \to \mathbf{R}$ is the function $\widehat{f} : \widehat{G} \to \mathbf{C}$ given by

$$\widehat{f}(\chi) = \mathbf{E}_{x\in G}\, f(x)\chi(-x).$$

The following lemma describes how the convolution and difference convolution behave under the Fourier transform.

Lemma 2 (*Convolution laws*). *Let G be a finite abelian group and let $f, g : G \to \mathbf{R}$. Then the following identities hold:*

i) $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$

ii) $\widehat{f \circ g} = \overline{\widehat{f}} \cdot \widehat{g}$

In particular, $\widehat{f \circ f} = |\widehat{f}|^2$.

Proof. Expand

$$\widehat{f * g}(\chi) = \mathbf{E}_{x\in G}(f * g)(\chi)\chi(-x)$$

and multiply the right-hand side by $1 = \chi(-y)\chi(y)$ to get

$$\widehat{f * g}(\chi) = \mathbf{E}_{x\in G}\, \mathbf{E}_{y\in G}\, f(y)g(x-y)\chi(-y)\chi(y-x).$$

Then we may interchange the order of summation and substitute $z = x - y$ to arrive at

$$\widehat{f * g}(\chi) = \mathbf{E}_{y\in G}\, \mathbf{E}_{z\in G}\, f(y)g(z)\chi(-y)\chi(-z) = \widehat{f}(\chi)\widehat{g}(\chi),$$

which proves (i). For part (ii), we expand and multiply by the same 1 to get

$$\widehat{f \circ g}(\chi) = \mathbf{E}_{x\in G}(f\circ g)(\chi)\chi(-x) = \mathbf{E}_{x\in G}\, \mathbf{E}_{y\in G}\, f(y)g(x+y)\chi(y)\chi(-x-y).$$

We again interchange the order of summation; this time substituting $z = x + y$ gives us

$$\begin{aligned}\widehat{f \circ g}(\chi) &= \mathbf{E}_{y\in G}\, \mathbf{E}_{z\in G}\, f(y)g(z)\chi(y)\chi(-z)\\ &= \overline{\mathbf{E}_{y\in G}\, f(y)\chi(-y)}\, \mathbf{E}_{z\in G}\, g(z)\chi(-z)\\ &= \overline{\widehat{f}(\chi)}\widehat{g}(\chi),\end{aligned}$$

which is what we wanted. $\blacksquare$

For sets A and X, let $\mu_X(A) = |A \cap X|/|X|$ denote the relative density of A in X, and if X is understood to be a subset of a larger set G, then we use μ_X also to denote the normalised indicator function given by

$$\mu_X(x) = \begin{cases} 1/\mu_G(X), & \text{if } x \in X; \\ 0, & \text{otherwise.} \end{cases}.$$

The scaling is done so that $\|\mu_X\|_1 = 1$ for any $X \subseteq G$, as can easily be checked.

2. Hölder lifting and unbalancing

Here we state and prove two lemmas that are general enough to apply in both the integer and finite-field settings.

Lemma 3 (*Hölder lifting*). *Let $\epsilon \ge 0$ and let A and C be subsets of a finite abelian group G, where C has relative density γ. Then at least one of the following two statements holds.*

i) $\big|\langle \mu_A * \mu_A, \mu_C \rangle\big| \le \epsilon$

ii) $\|\mu_A \circ \mu_A - 1\|_p \ge \epsilon/2$ *for some* $p = O\big(\log(1/\gamma)\big)$.

Proof. Bilinearity of the inner product gives

$$\langle \mu_A * \mu_A - 1, \mu_C \rangle = \langle \mu_A * \mu_A, \mu_C \rangle + \langle -1, \mu_C \rangle = \langle \mu_A * \mu_A, \mu_C \rangle - 1,$$

so if the first statement does not hold, then for $q = 1/(1 - 1/p)$, we have, by Hölder's inequality,

$$\begin{aligned} \epsilon < \big|\langle \mu_A * \mu_A, \mu_C \rangle\big| &\le \|\mu_A * \mu_A - 1\|_p \Big(\mathbf{E}_{x \in G} \big|\mu_C(x)\big|^q\Big)^{1/q} \\ &\le \|\mu_A * \mu_A - 1\|_p \gamma^{1/q-1} \le \|\mu_A * \mu_A - 1\|_p \gamma^{-1/p}. \end{aligned}$$

Letting p be an even integer greater than $\log_2(1/\gamma)$, we have $\log \gamma \ge p \log(1/2)$, whence $\gamma^{1/p} \ge 1/2$, which gives the inequality

$$\|\mu_A * \mu_A - 1\|_p \ge \frac{\epsilon}{2}.$$

Lastly, observe that since p is even,

3. The finite-field case

First, we give bounds for the size of a 3-AP-free subset of $\mathbf{F}_q^n$. As is common with problems of this sort, the finite-field case is a simpler prototype of the integer one.

References