An introduction to Fourier analysis and Roth's theorem

Martino Lupini

York University
Toronto, Canada

April 11th, 2013

Table of Contents

1. Fourier analysis
2. First application
3. Linear bias
4. Roth's theorem

Table of Contents

1 Fourier analysis

2 First application

3 Linear bias

4 Roth's theorem

Groups and duals

Suppose that Z is an additive abelian finite group.

Denote by $\widehat{Z}$ the dual of Z, i.e. the group of homomorphisms $\chi : Z \to \mathbb{T}$.

Any nondegenerate bilinear form

$$\begin{array}{ccc} Z \times Z & \to & \mathbb{T} \\ (x, y) & \mapsto & x \cdot y \end{array}$$

defines an isomorphism from Z to $\widehat{Z}$ by

$$y \mapsto \chi_y$$

where

$$\chi_y(x) = x \cdot y$$

Cyclic finite groups

Suppose that $Z = \mathbb{Z}/n\mathbb{Z}$ is cyclic of order n.

The map

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{R}/\mathbb{Z} \\ (a + n\mathbb{Z}, b + n\mathbb{Z}) &\mapsto ab + \mathbb{Z} \end{aligned}$$

is a nondegenerate bilinear form.

Thus any character of $\mathbb{Z}/n\mathbb{Z}$ is of the form

$$\chi_b(a + n\mathbb{Z}) = ab + \mathbb{Z}$$

for some $b \in \{0, 1, \ldots, n-1\}$.

Finite fields

Suppose that Z is the additive group of a finite field F.

Fix any nontrivial homomorphism $\phi : F \to \mathbb{T}$.

The map

$$\begin{array}{ccc} F \times F & \to & \mathbb{T} \\ (x, y) & \mapsto & \phi(xy) \end{array}$$

is a nondegenerate bilinear form.

Thus any character of F is of the form

$$\chi_y(x) = \phi(xy)$$

for some $x \in F$.

Mean value

Denote by $\mathbb{C}^Z$ the linear space of functions $f : Z \to \mathbb{C}$.

Define the mean value or expectation of $f \in \mathbb{C}^Z$

$$\mathbb{E}_Z(f) = \frac{1}{|Z|} \sum_{x \in Z} f(x)$$

If $f, g : Z \to \mathbb{C}$ define

$$\langle f, g \rangle = \mathbb{E}_Z(f\overline{g})$$

This makes $\mathbb{C}^Z$ a Hilbert space.

Fourier transform

If $\xi \in \widehat{Z}$ define $e_\xi \in \mathbb{C}^Z$ by

$$e_\xi(x) = \xi(x).$$

Note that $e_0 \equiv 1$.

The elements $(e_\xi)_{\xi \in \widehat{Z}}$ form an orthonormal basis of $\mathbb{C}^Z$.

If $f \in \mathbb{C}^Z$ define $\widehat{f} \in \mathbb{C}^{\widehat{Z}}$ by

$$\widehat{f}(\xi) = \langle f, e_\xi \rangle$$

Observe that $\widehat{f}(\xi)$ is just the coefficient of f corresponding to e_ξ.

In particular $\widehat{f}(0) = \mathbb{E}_Z(f)$.

Fourier inversion formula

Since the $(e_\xi)_{\xi \in \widehat{Z}}$ form an orthonormal basis we have

$$f = \sum_{x \in \widehat{Z}} \widehat{f}(\xi)\, e_\xi$$

and

$$\langle f, g \rangle = \sum_{\xi \in Z} \widehat{f}(\xi)\, \overline{\widehat{g}(\xi)}$$

In particular

$$\mathbb{E}_Z |f|^2 = \langle f, f \rangle = \sum_{\xi \in Z} \left| \widehat{f}(\xi) \right|^2$$

Probability

If $A \subset Z$ denote by 1_A the characteristic function of A.

The density or probability of A is

$$\mathbb{P}_Z(A) = \mathbb{E}_Z(1_A) = \frac{|A|}{|Z|}.$$

Define also the support of $f \in \mathbb{C}^Z$ by

$$supp(f) = \{x \in Z \,|\, f(x) \neq 0\}.$$

Convolution

If $f, g \in \mathbb{C}^Z$ define their convolution $f * g \in \mathbb{C}^Z$ by

$$\begin{aligned}(f * g)(x) &= \mathbb{E}_{y \in Z}\left(f(x-y)\, g(y)\right) \\ &= \mathbb{E}_{y \in Z}\left(f(y)\, g(x-y)\right)\end{aligned}$$

Analogously if $\psi, \varphi \in \mathbb{C}^{\widehat{Z}}$ define $\psi * \varphi \in \mathbb{C}^{\widehat{Z}}$ by

$$\begin{aligned}(\psi * \varphi)(\eta) &= \sum_{\xi \in \widehat{Z}} \psi(\xi)\, \varphi(\eta - \xi) \\ &= \sum_{\xi \in \widehat{Z}} \psi(\eta - \xi)\, \varphi(\xi)\end{aligned}$$

Convolution and sum sets

We have

$$\widehat{f * g} = \widehat{f}\,\widehat{g}$$

and

$$\widehat{fg} = \widehat{f} * \widehat{g}$$

In particular

$$\mathbb{E}(f * g) = \mathbb{E}(f)\,\mathbb{E}(g)$$

and

$$\mathbb{E}(fg) = \sum_{\xi \in \widehat{Z}} \widehat{f}(\xi)\,\widehat{g}(-\xi)$$

Moreover

$$(1_A * 1_B)(x) = \mathbb{P}_Z(A \cap (x - B))$$

and in particular

$$Supp(1_A * 1_B) = A + B$$

Table of Contents

1 Fourier analysis

2 First application

3 Linear bias

4 Roth's theorem

A first application

Theorem

If F is a finite field and $A \subset F$ is such that $\mathbb{P}_F(A) = \frac{|A|}{|F|} > |F|^{-\frac{1}{4}}$ then

$$AA + AA + AA = F$$

Identity $\widehat{F}$ with F via the bilinear form

$$(a, b) \mapsto \phi(ab)$$

where ϕ is any nondegenerate homomorphism from F to $\mathbb{T}$.

Define $f : F \to \mathbb{R}$ by

$$\begin{aligned} f &= \mathbb{E}_{a \in A} 1_{aA} \\ &= \frac{1}{|A|} \sum_{a \in A} 1_{aA} \end{aligned}$$

Observe that

$$(f * f * f)(z) = \mathbb{E}_{x \in F} \mathbb{E}_{y \in F} \mathbb{E}_{a \in A} \mathbb{E}_{b \in A} \mathbb{E}_{c \in A} 1_{aA}(x) 1_{bA}(y - x) 1_{cA}(z - y)$$

Thus

$$supp(f * f * f) = AA + AA + AA$$

We want to show that

$$supp(f * f * f) = F$$

By the Fourier inversion formula we have that

$$\begin{aligned} f*f*f &= \mathrm{Re}\left(f*f*f\right) \\ &= \mathrm{Re}\left(\sum_{\xi\in F}\widehat{\left(f*f*f\right)}\left(\xi\right)e_{\xi}\right) \\ &= \mathrm{Re}\left(\sum_{\xi\in F}\widehat{f}\left(\xi\right)^{3}e_{\xi}\right) \\ &\geq \widehat{f}\left(0\right)^{3}-\sum_{\xi\in F\setminus|0|}\left|\widehat{f}\left(\xi\right)\right|^{3} \end{aligned}$$

Observe now that

$$\begin{aligned}\widehat{f}(0) &= \mathbb{E}_{z\in F}(f(z)) \\ &= \mathbb{E}_{z\in F}(\mathbb{E}_{a\in A}1_{aA}(z)) \\ &= \mathbb{E}_{a\in A}(\mathbb{E}_{z\in F}1_{aA}(z)) \\ &= \mathbb{E}_{a\in A}\mathbb{P}_F(aA) \\ &= \mathbb{P}_F(A)\end{aligned}$$

If $\xi \in F$ is nonzero, the frequencies $\left(\frac{\xi}{a}\right)_{a\in A}$ are distinct

$$\begin{aligned}\widehat{f}(\xi) &= \langle \mathbb{E}_{a\in A}1_{aA}, e_\xi\rangle \\ &= \mathbb{E}_{a\in A}\langle 1_{aA}, e_\xi\rangle \\ &= \mathbb{E}_{a\in A}\left\langle 1_A, e_{\frac{\xi}{a}}\right\rangle \\ &= \mathbb{E}_{a\in A}\widehat{1}_A\left(\frac{\xi}{a}\right)\end{aligned}$$

By Cauchy-Schwartz

$$\begin{aligned}
\left|\widehat{f}(\xi)\right|^2 &= \frac{\left|\sum_{a\in A}\widehat{1}_A\left(\frac{\xi}{a}\right)\cdot 1\right|^2}{|A|^2} \\
&\leq \frac{\sum_{a\in A}\left|\widehat{1}_A\left(\frac{\xi}{a}\right)\right|^2\sum_{a\in A}1^2}{|A|^2} \\
&\leq \frac{1}{|A|}\left\|\widehat{1}_A\right\|^2_{\ell^2(F)} \\
&= \frac{1}{|A|}\left\|1_A\right\|^2_{L^2(F)} \\
&= \frac{1}{|F|}
\end{aligned}$$

Substituting and the hypothesis that

$$\mathbb{P}_F(A) > |F|^{-\frac{1}{4}}$$

we obtain

$$\begin{aligned}
f * f * f &\geq \widehat{f}(0)^3 - \sum_{\xi \in F \setminus \{0\}} \left|\widehat{f}(\xi)\right|^3 \\
&\geq \mathbb{P}_F(A)^3 - |F|^{-\frac{1}{2}} \sum_{\xi \in F} \left|\widehat{f}(\xi)\right|^2 \\
&= \mathbb{P}_F(A)^3 - |F|^{-\frac{1}{2}} \left\|\widehat{f}\right\|^2_{\ell^2(F)} \\
&= \mathbb{P}_F(A)^3 - |F|^{-\frac{1}{2}} \|f\|^2_{L^2(F)} \\
&> \mathbb{P}_F(A)^3 - \mathbb{P}_F(A)^2 \|f\|^2_{L^2(F)}
\end{aligned}$$

We just need to show that

$$\|f\|_{L^2(f)} \leq \mathbb{P}_F(A)$$

We have

$$\begin{aligned}
\|f\|^2_{L^2(F)} &= \mathbb{E}_{z\in F}\left(\mathbb{E}_{a\in A}1_{aA}(z)\right)^2 \\
&\leq \mathbb{E}_{z\in F}\mathbb{E}_{a\in A}1_{aA}(z) \\
&= \mathbb{E}_{a\in A}\mathbb{E}_{z\in F}1_{aA}(z) \\
&= \mathbb{E}_{a\in A}\mathbb{P}_F(aA) \\
&= \mathbb{E}_{a\in A}\mathbb{P}_F(A) \\
&= \mathbb{P}_F(A)
\end{aligned}$$

Table of Contents

1 Fourier analysis

2 First application

3 Linear bias

4 Roth's theorem

Fourier linear bias

In the proof of the previous theorem the estimate of

$$\widehat{f}(\xi)$$

for $\xi \neq 0$ nonzero plays a key role.

Definition

If Z is an additive abelian group and $A \subset Z$ the Fourier linear bias of A is

$$\|A\|_u = \sup_{\xi \in \widehat{Z} \setminus \{0\}} \left|\widehat{1}_A(\xi)\right|$$

Sets with small Fourier bias are pseudorandom.

Lemma (Pseudorandomness implies large sumsets)

If $A_1, A_2, A_3 \subset Z$ *and* $x \in Z$

$$\frac{1}{|Z|^2} \left|\{(a_1, a_2, a_3) \in A_1 \times A_2 \times A_3 \,|a_1 + a_2 + a_3 = x\}\right|$$

from

$$\mathbb{P}_Z(A_1)\,\mathbb{P}_Z(A_2)\,\mathbb{P}_Z(A_3)$$

is at most

$$\|A_1\|_u\,\mathbb{P}_Z(A_2)^{\frac{1}{2}}\,\mathbb{P}_Z(A_3)^{\frac{1}{2}}$$

In particular if

$$\|A_1\|_u < \mathbb{P}_Z(A_1)\,\mathbb{P}_Z(A_2)^{\frac{1}{2}}\,\mathbb{P}_Z(A_3)^{\frac{1}{2}}$$

then

$$A_1 + A_2 + A_3 = Z.$$

Here is a sketch of proof of the Lemma.

Consider the function

$$f = 1_{A_1} * 1_{A_2} * 1_{A_3}$$

Observe that

$$f(x) = \frac{1}{|Z|^2} |\{(a_1, a_2, a_3) | a_1 + a_2 + a_3 = x\}|$$

We want to estimate f from below and from above similarly as before

- the Fourier inversion formula;
- the Cauchy-Schwartz inequality;

We have

$$\begin{aligned}
f &\geq \operatorname{Re}(f) = \operatorname{Re}\left(\sum_{\xi\in\widehat{Z}} \widehat{f}(\xi)\, e_\xi\right) = \operatorname{Re}\left(\sum_{\xi\in\widehat{Z}} \widehat{1}_{A_1}(\xi)\,\widehat{1}_{A_2}(\xi)\,\widehat{1}_{A_3}(\xi)\, e_\xi\right) \\
&\geq \widehat{1}_{A_1}(0)\,\widehat{1}_{A_2}(0)\,\widehat{1}_{A_3}(0) - \sum_{\xi\in\widehat{Z}\setminus\{0\}} \left|\widehat{1}_{A_1}(\xi)\,\widehat{1}_{A_2}(\xi)\,\widehat{1}_{A_3}(\xi)\right| \\
&\geq \widehat{1}_{A_1}(0)\,\widehat{1}_{A_2}(0)\,\widehat{1}_{A_3}(0) - \|A_1\|_u \sum_{\xi\in\widehat{Z}\setminus\{0\}} \left|\widehat{1}_{A_2}(\xi)\,\widehat{1}_{A_3}(\xi)\right| \\
&\geq \widehat{1}_{A_1}(0)\,\widehat{1}_{A_2}(0)\,\widehat{1}_{A_3}(0) - \|A_1\|_u \left\|\widehat{1}_{A_2}\right\|_{\ell^2(\widehat{Z})} \left\|\widehat{1}_{A_3}\right\|_{\ell^2(\widehat{Z})} \\
&= \widehat{1}_{A_1}(0)\,\widehat{1}_{A_2}(0)\,\widehat{1}_{A_3}(0) - \|A_1\|_u \|1_{A_2}\|_{L^2(Z)} \|1_{A_3}\|_{L(Z)} \\
&= \widehat{1}_{A_1}(0)\,\widehat{1}_{A_2}(0)\,\widehat{1}_{A_3}(0) - \|A_1\|_u \mathbb{P}_Z(A_2)\,\mathbb{P}_Z(A_3)
\end{aligned}$$

Table of Contents

1 Fourier analysis

2 First application

3 Linear bias

4 Roth's theorem

Roth's theorem

Fourier analysis can be applied to prove **Roth's theorem**.

Theorem (Roth)

If $A \subset \mathbb{N}$ has positive asymptotic density, then it contains a 3-arithmetic progression.

One can make the statement more quantitative in terms of the **Erdös-Turán constants**.

Definition

Suppose that Z is an additive abelian group and $A \subset Z$.

Define $r_3(A)$ to be the largest cardinality of a subset of A without proper 3-arithmetic progressions.

Finitary Roth's theorem

Roth's theorem is equivalent to the statement

$$\lim_{n\to+\infty} \frac{r_3([0,n])}{n} = 0$$

where $[0,n] \subset \mathbb{Z}$.

Observe that if $n \in \mathbb{N}$ then

$$r_3\left(\left[0,\frac{n}{3}\right)\right) \leq r_3(\mathbb{Z}/n\mathbb{Z}) \leq r_3([0,n])$$

Thus Roth's theorem is also equivalent to the statement

$$\lim_{n\to+\infty} \frac{r_3(\mathbb{Z}/n\mathbb{Z})}{n} = 0$$

Roth's theorem generalization

This statement admits the following generalization, due to Meshulam:

Theorem

For any additive abelian group of odd order

$$r_3(Z) = o_{|Z|\to+\infty}(|Z|).$$

This means that for every $\varepsilon > 0$ there is $n \in \mathbb{N}$ such that if Z is an additive abelian group of odd order and

$$|Z| > n$$

then

$$r_3(Z) < \varepsilon |Z|.$$

Proof strategy

Strategy of the Fourier analytic proof of Roth's theorem:

1. **pseudorandomness** implies existence of 3-arithmetic progressions;
2. assume $A \subset Z$ has high density and no 3-arithmetic progressions;
3. A has large Fourier linear bias by point (1);
4. convert liner bias into **density increment** finding a structured subset Z' of Z where A has higher density;
5. repeating this argument leads to the contradictory conclusion

$$\mathbb{P}_Z(A) > 1$$

Proportion of 3-arithmetic progressions

If $A \subset Z$ define

$$\begin{aligned}\Lambda_A &= \mathbb{E}_{x,r\in Z} 1_A(x)\, 1_A(x+r)\, 1_A(x+2r) \\ &= \frac{1}{|Z|^2}\left|\{(x,r)\in Z\times Z \,|x, x+r, x+2r\in A\}\right| \\ &= \mathbb{P}_{x,r\in Z}(x, x+r, x+2r\in A)\end{aligned}$$

Observe that Λ_A measures

The heuristic of the pseudorandom case

If A is pseudorandom are approximately independent. Thus

$$\begin{aligned}\Lambda_A &= \mathbb{P}_{x,r\in Z}\left(x, x+r, x+2r \in A\right)\\ &\approx \mathbb{P}_{x,r\in Z}\left(x\in A\right)\mathbb{P}_{x,r\in Z}\left(x+r\in A\right)\mathbb{P}_{x,r\in Z}\left(x+2r\in A\right)\\ &= \mathbb{P}_{x\in Z}\left(x\in A\right)^3\end{aligned}$$

The trivial 3-arithmetic progressions (for $r=0$) are in a proportion of

$$\frac{1}{|Z|}\mathbb{P}_Z\left(A\right)$$

If $|Z|$ is large enough with respect to $\mathbb{P}_Z\left(A\right)$ then

$$\frac{1}{|Z|}\mathbb{P}_Z\left(A\right) < \mathbb{P}_Z\left(A\right)^3$$

Hence A contains proper arithmetic progressions.

Roth's theorem in the pseudorandom case

Proposition (Roth's theorem for pseudorandom sets)

If $A \subset Z$ and Z has odd order then

$$\left|\Lambda_A - \mathbb{P}_Z(A)^3\right| \leq \|A\|_u \mathbb{P}_Z(A)$$

In particular if A has no proper 3-arithmetic progression then

$$\|A\|_u \geq \mathbb{P}_Z(A)^2 - \frac{1}{|Z|}$$

The proof uses the previously proved estimate on sum sets in term of the Fourier linear biased.

The proof of Roth's theorem for pseudorandom sets

Observe that (x, y, z) is an arithmetic progression iff

$$z - 2y + z = 0$$

Thus

$$\Lambda_A = \frac{1}{|Z|^2} \{(a_1, a_2, a_3) \in A \times (-2A) \times A \,|\, a_1 + a_2 + a_3 = 0\}$$

It follows that

$$\begin{aligned} \left|\Lambda_A - \mathbb{P}(A)^3\right| &= |\Lambda_A - \mathbb{P}(A)\,\mathbb{P}(-2A)\,\mathbb{P}(A)| \\ &\leq \|A\|_u\, \mathbb{P}(-2A)^{\frac{1}{2}}\, \mathbb{P}(A)^{\frac{1}{2}} \\ &= \|A\|_u\, \mathbb{P}(A) \end{aligned}$$

The proof of Roth's theorem for pseudorandom sets

In particular if A has no proper 3-arithmetic progression then as before

$$\Lambda_A = \frac{1}{|Z|}\mathbb{P}_Z(A)$$

and hence

$$\mathbb{P}_Z(A)^2 - \frac{1}{|Z|} = \frac{1}{\mathbb{P}_Z(A)}\left|\Lambda_A - \mathbb{P}(A)^3\right| \leq \|A\|_u$$