

# Introduction to Additive Combinatorics

## Part III

Lectured by Julia Wolf

Artur Avameri

### Contents

<b>1</b>	<b>Fourier-analytic techniques</b>	<b>2</b>
<b>2</b>	<b>Combinatorial methods</b>	<b>11</b>
<b>3</b>	<b>Probabilistic tools</b>	<b>18</b>

# 1 Fourier-analytic techniques

19 Jan 2024,  
Lecture 1

Let  $G = \mathbb{F}_p^n$  for  $p$  a small fixed prime (usually  $p = 2, 3, 5$ ) and  $n$  is large (often we consider  $n \rightarrow \infty$ ).

**Notation.** Given a finite set  $B$  and any function  $f : B \rightarrow \mathbb{C}$ , we write  $\mathbb{E}_{x \in B} f(x)$  to mean  $\frac{1}{|B|} \sum_{x \in B} f(x)$ . Also write  $\omega = e^{2\pi i/p}$  for the  $p^{\text{th}}$  root of unity. Note that  $\sum_{a \in \mathbb{F}_p} \omega^a = 0$ .

**Definition 1.1.** Given  $f : \mathbb{F}_p^n \rightarrow \mathbb{C}$ , we define its **Fourier transform**  $\hat{f} : \mathbb{F}_p^n \rightarrow \mathbb{C}$  by

$$\hat{f}(t) = \mathbb{E}_{x \in \mathbb{F}_p^n} f(x) \omega^{x \cdot t} \quad \forall t \in \mathbb{F}_p^n$$

where  $x \cdot t$  is the standard scalar product.

It is easy to verify the **inversion formula**:

$$f(x) = \sum_{t \in \mathbb{F}_p^n} \hat{f}(t) \omega^{-x \cdot t} \quad \forall x \in \mathbb{F}_p^n.$$

Indeed,

$$\begin{aligned} \sum_{t \in \mathbb{F}_p^n} \hat{f}(t) \omega^{-x \cdot t} &= \sum_{t \in \mathbb{F}_p^n} (\mathbb{E}_y f(y) \omega^{y \cdot t}) \omega^{-x \cdot t} \\ &= \mathbb{E}_y f(y) \underbrace{\sum_{t \in \mathbb{F}_p^n} \omega^{(y-x) \cdot t}}_{p^n \mathbf{1}_{\{y=x\}}} = f(x). \end{aligned}$$

**Remark.** We could use an unnormalized sum in our definition and a normalized sum in the inversion formula, or a minus sign in our definition and a plus sign in the inversion formula – this doesn't matter as long as we're consistent.

Given a subset  $A$  of a finite group  $G$ , write:

- $1_A$  for the **characteristic function** of  $A$ , i.e.  $1_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$ .

This is also called the **indicator function**.

- $f_A$  for the **balanced function** of  $A$ , i.e.  $f_A(x) = 1_A(x) - \alpha$ , where  $\alpha = \frac{|A|}{|G|}$ .

- $\mu_A$  for the **characteristic measure** of  $A$ , i.e.  $\mu_A(x) = \alpha^{-1} 1_A(x)$ .

Note  $\mathbb{E}_{x \in G} f_A(x) = 0$  and  $\mathbb{E}_{x \in G} \mu_A(x) = 1$ . Given  $A \subset \mathbb{F}_p^n$ , we have

$$\hat{1}_A(t) = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) \omega^{x \cdot t}.$$

At  $t = 0$ , we get  $\hat{1}_A(0) = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) = \alpha$ .

Writing  $-A = \{-a \mid a \in A\}$ , we have

$$\begin{aligned} \hat{1}_{-A}(t) &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_{-A}(x) \omega^{x \cdot t} = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(-x) \omega^{x \cdot t} \\ &\stackrel{y=-x}{=} \mathbb{E}_{y \in \mathbb{F}_p^n} 1_A(y) \omega^{-y \cdot t} = \overline{\mathbb{E}_{y \in \mathbb{F}_p^n} 1_A(y) \omega^{y \cdot t}} = \overline{\hat{1}_A(t)}. \end{aligned}$$

**Example 1.2.** Let  $V \leq \mathbb{F}_p^n$ . Then

$$\hat{1}_V(t) = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_V(x) \omega^{x \cdot t} = \frac{|V|}{p^n} 1_{\{x \cdot t = 0 \ \forall x \in V\}} = \frac{|V|}{p^n} 1_{V^\perp}(t),$$

so  $\hat{\mu}_V(t) = 1_{V^\perp}(t)$ . (Here we use the fact that if  $t \notin \{x \cdot t = 0 \ \forall x \in V\}$ , then  $x \cdot t$  runs over the values uniformly and the sum is zero - details left as exercise).

**Example 1.3.** Let  $R \subset \mathbb{F}_p^n$  be such that each  $x \in \mathbb{F}_p^n$  lies in  $R$  independently with probability  $\frac{1}{2}$ . Then with high probability (i.e.  $\mathbb{P} \rightarrow 1$  as  $n \rightarrow \infty$ ),

$$\sup_{t \neq 0} |\hat{1}_R(t)| = O\left(\sqrt{\frac{\log(p^n)}{p^n}}\right).$$

Proving this is on Ex. Sheet 1. This is proved using a Chernoff-type bound: given complex-valued independent random variables  $X_1, \dots, X_n$  with mean 0,  $\forall \theta \geq 0$ ,

$$\mathbb{P}\left(\left|\sum_{i=1}^n X_i\right| \geq \theta \sqrt{\sum_{i=1}^n \|X_i\|_{L^\infty(\mathbb{P})}^2}\right) \leq 4 \exp(-\theta^2/4).$$

**Example 1.4.** Let  $Q = \{x \in \mathbb{F}_p^n \mid x \cdot x = 0\}$ . Then  $|Q| = \left(\frac{1}{p} + O(p^{-n})\right) p^n$  and  $\sup_{t \neq 0} |\hat{1}_Q(t)| = O(p^{-n/2})$ . This is again on Ex. Sheet 1.

**Notation.** Given  $f, g : \mathbb{F}_p^n \rightarrow \mathbb{C}$ , write

$$\langle f, g \rangle = \mathbb{E}_{x \in \mathbb{F}_p^n} f(x) \overline{g(x)}$$

and

$$\langle \hat{f}, \hat{g} \rangle = \sum_{t \in \mathbb{F}_p^n} \hat{f}(t) \overline{\hat{g}(t)}.$$

Consequently,  $\|f\|_2^2 = \mathbb{E}_x |f(x)|^2$  and  $\|\hat{f}\|_2^2 = \sum_t |\hat{f}(t)|^2$ .

**Lemma 1.5.** The following hold for all  $f, g : \mathbb{F}_p^n \rightarrow \mathbb{C}$ :

- (i)  $\langle f, g \rangle = \langle \hat{f}, \hat{g} \rangle$  (Plancherel's identity).
- (ii)  $\|f\|_2 = \|\hat{f}\|_2$  (Parseval's identity).

*Proof.* (ii) follows from (i). For (i), compute

$$\begin{aligned}\langle \hat{f}, \hat{g} \rangle &= \sum_{t \in \mathbb{F}_p^n} \hat{f}(t) \overline{\hat{g}(t)} = \sum_{t \in \mathbb{F}_p^n} \frac{1}{p^{2n}} \sum_{x \in \mathbb{F}_p^n} f(x) \omega^{x \cdot t} \sum_{y \in \mathbb{F}_p^n} \overline{g(y) \omega^{y \cdot t}} \\ &= \frac{1}{p^{2n}} \sum_{x, y \in \mathbb{F}_p^n} f(x) \overline{g(y)} \sum_{t \in \mathbb{F}_p^n} \omega^{(x-y)t} = \frac{1}{p^{2n}} \sum_{x \in \mathbb{F}_p^n} p^n f(x) \overline{g(x)} = \langle f, g \rangle.\end{aligned}$$

□

**Definition 1.6.** Let  $\rho > 0$  and  $f : \mathbb{F}_p^n \rightarrow \mathbb{C}$ . Define the  $\rho$ -large spectrum of  $f$  to be

$$\text{Spec}_\rho(f) = \{t \in \mathbb{F}_p^n \mid |\hat{f}(t)| \geq \rho \|f\|_1\}.$$

**Example 1.7.** By Example 1.2, if  $f = 1_V$  with  $V \leq \mathbb{F}_p^n$ , then  $\forall \rho > 0$ ,  $\text{Spec}_\rho(f) = V^\perp$ .<sup>1</sup>

**Lemma 1.8.** For all  $\rho > 0$ ,  $|\text{Spec}_\rho(f)| \leq \rho^{-2} \frac{\|f\|_2^2}{\|f\|_1^2}$ .

*Proof.* By Parseval,

$$\|f\|_2^2 = \|\hat{f}\|_2^2 \geq \sum_{t \in \text{Spec}_\rho(f)} |\hat{f}(t)|^2 \geq |\text{Spec}_\rho(f)| (\rho \|f\|_1)^2.$$

□

22 Jan 2024,  
Lecture 2

**Definition 1.9.** Given  $f, g : \mathbb{F}_p^n \rightarrow \mathbb{C}$ , define their **convolution**  $f * g : \mathbb{F}_p^n \rightarrow \mathbb{C}$  by

$$f * g(x) = \mathbb{E}_{y \in \mathbb{F}_p^n} f(y) g(x - y) \quad \forall x \in \mathbb{F}_p^n.$$

**Example 1.10.** Given  $A, B \subset \mathbb{F}_p^n$ ,

$$\begin{aligned}1_A * 1_B(x) &= \mathbb{E}_{y \in \mathbb{F}_p^n} 1_A(y) 1_B(x - y) = \frac{1}{p^n} |A \cap (x - B)| \\ &= \frac{1}{p^n} \# \text{ways } x \text{ can be written as } x = a + b \text{ with } a \in A, b \in B.\end{aligned}$$

In particular, the support of  $1_A * 1_B$  is the **sum set**

$$A + B = \{a + b \mid a \in A, b \in B\}$$

of  $A$  and  $B$ .

**Lemma 1.11.** Given  $f, g : \mathbb{F}_p^n \rightarrow \mathbb{C}$ ,

$$\widehat{f * g}(t) = \hat{f}(t) \hat{g}(t) \quad \forall t \in \mathbb{F}_p^n.$$

---

<sup>1</sup>Here we have  $0 < \rho \leq 1$ , since it is clear by triangle inequality that  $\|f\|_1 \geq |\hat{f}(t)|$ .

*Proof.* Set  $u = x - y$  to get

$$\begin{aligned}\widehat{f * g}(t) &= \mathbb{E}_{x \in \mathbb{F}_p^n} \left( \mathbb{E}_{y \in \mathbb{F}_p^n} f(y) g(x - y) \right) \omega^{x \cdot t} \\ &= \mathbb{E}_y f(y) \mathbb{E}_u g(u) \omega^{(u+y) \cdot t} \\ &= \hat{f}(t) \hat{g}(t).\end{aligned}$$

□

**Example 1.12.**  $\|\hat{f}\|_4^4 = \mathbb{E}_{x+y=z+w} f(x) f(y) \overline{f(z)} \overline{f(w)}$ . This is on Ex. Sheet 1.

**Lemma 1.13** (Bogolyubov's Lemma). Given  $A \subset \mathbb{F}_p^n$  of density  $\alpha > 0$ , there exists a subspace  $V \leq \mathbb{F}_p^n$  of codimension at most  $2\alpha^{-2}$  s.t.  $A + A - A - A \supset V$ .

*Proof.* Observe that

$$A + A - A - A = \text{supp}(\underbrace{1_A * 1_A * 1_{-A} * 1_{-A}}_{:=g}).$$

Hence we wish to find  $V \leq \mathbb{F}_p^n$  such that  $g(x) > 0 \forall x \in V$ . Let  $K = \text{Spec}_\rho(1_A)$  with  $\rho$  to be determined later and let  $V = \langle K \rangle^\perp$ . By Lemma 1.8<sup>2</sup>,  $|K| \leq \rho^{-2} \alpha^{-1}$  and hence  $\text{codim}(V) \leq |K| \leq \rho^{-2} \alpha^{-1}$ . By the inversion formula,

$$\begin{aligned}g(x) &= \sum_{t \in \mathbb{F}_p^n} (1_A * 1_A * \widehat{1_{-A}} * 1_{-A})(t) \omega^{-x \cdot t} \\ &= \sum_{t \in \mathbb{F}_p^n} |\hat{1}_A(t)|^4 \omega^{-x \cdot t} \\ &= \underbrace{\alpha^4 + \sum_{t \in K \setminus \{0\}} |\hat{1}_A(t)|^4 \omega^{-x \cdot t}}_{(1)} + \underbrace{\sum_{t \notin K} |\hat{1}_A(t)|^4 \omega^{-x \cdot t}}_{(2)}.\end{aligned}$$

For (1), we see it is  $\geq 0$  since  $x \cdot t = 0 \forall t \in K, x \in V$ . (Note we could give better lower bounds but we don't need them).

For (2), we have

$$\begin{aligned}|(2)| &\leq \sum_{t \notin K} |\hat{1}_A(t)|^4 \leq \sup_{t \notin K} |\hat{1}_A(t)|^2 \sum_{t \notin K} |\hat{1}_A(t)|^2 \leq \sup_{t \notin K} |\hat{1}_A(t)|^2 \sum_t |\hat{1}_A(t)|^2 \\ &\leq (\rho \alpha)^2 \|1_A\|_2^2 = \rho^2 \alpha^3.\end{aligned}$$

Now pick  $\rho$  such that  $\rho^2 \alpha^3 \leq \frac{\alpha^4}{2}$ , e.g.  $\rho = \sqrt{\frac{\alpha}{2}}$ , so  $g(x) \geq \frac{\alpha^4}{2} > 0 \forall x \in V$ . □

<sup>2</sup>Here  $f = 1_A$  and  $\alpha = \frac{\|f\|_1^2}{\|f\|_2^2} = \frac{\left(\frac{1}{p^n} \sum |f|\right)^2}{\left(\frac{1}{p^n} \sum |f|^2\right)} = \frac{|A|}{p^n} = \alpha$ .

**Example 1.14.** The set  $A = \{x \in \mathbb{F}_2^n \mid |x| \geq \frac{n}{2} + \frac{\sqrt{n}}{2}\}$  has density at least  $\frac{1}{4}$ , and there is no coset  $C$  of any subspace of codimension at most  $\sqrt{n}$  such that  $C \subset A + A$ . This is on Ex. Sheet 1.

**Lemma 1.15.** Let  $A \subset \mathbb{F}_p^n$  of density  $\alpha$  be such that  $\exists t \neq 0$  in  $\text{Spec}_\rho(1_A)$ . Then  $\exists V \leq \mathbb{F}_p^n$  of codimension 1 and  $\exists x \in \mathbb{F}_p^n$  such that

$$|A \cap (x + V)| \geq \alpha \left(1 + \frac{\rho}{2}\right) |V|.$$

*Proof.* Let  $t \neq 0$  be such that  $|\hat{1}_A(t)| \geq \rho\alpha$  and let  $V = \langle t \rangle^\perp$ . Write  $v_j + V$  for  $j \in [p] := \{1, 2, \dots, p\}$  for the cosets of  $V$  such that  $v_j + V = \{x \in \mathbb{F}_p^n \mid x \cdot t = j\}$ . Then

$$\begin{aligned} \rho\alpha &\leq \hat{1}_A(t) = \hat{f}_A(t) \\ &= \mathbb{E}_{x \in \mathbb{F}_p^n} (1_A(x) - \alpha) \omega^{x \cdot t} \\ &= \mathbb{E}_{j \in [p]} \underbrace{\mathbb{E}_{x \in v_j + V} (1_A(x) - \alpha) \omega^j}_{:= a_j = \frac{|A \cap (v_j + V)|}{|V|} - \alpha}. \end{aligned}$$

By the triangle inequality,  $\mathbb{E}_{j \in [p]} |a_j| \geq \rho\alpha$ . Since  $\mathbb{E}_{j \in [p]} a_j = \frac{|A|}{p^{n-1}} - p\alpha = 0$ ,  $\mathbb{E}_{j \in [p]} (a_j + |a_j|) \geq \rho\alpha$ , so  $\exists j \in [p]$  such that  $a_j + |a_j| \geq \rho\alpha \implies a_j \geq \frac{\rho\alpha}{2}$ .  $\square$

24 Jan 2024,  
Lecture 3

**Lemma 1.16.** Let  $p \geq 3$  and  $A \subset \mathbb{F}_p^n$  of density  $\alpha > 0$  be such that

$$\sup_{t \neq 0} |\hat{1}_A(t)| = o(1).$$

Then  $A$  contains  $(\alpha^3 + o(1))(p^n)^2$  3-term arithmetic progressions (3-APs).

In other words, a set with small Fourier coefficients has the same number of 3-APs as a truly random set of the same density.

**Notation.** Given  $f, g, h : \mathbb{F}_p^n \rightarrow \mathbb{C}$ ,  $T_3(f, g, h) = \mathbb{E}_{x,d} f(x)g(x+d)h(x+2d)$ .

Given  $A \subset \mathbb{F}_p^n$ , write  $2 \cdot A = \{2a \mid a \in A\}$ . This is different from  $2A = A + A = \{a + a' \mid a, a' \in A\}$ .

*Proof.* The number of 3-APs in  $A$  is  $(p^n)^2$  times  $T_3(1_A, 1_A, 1_A)$ , where

$$\begin{aligned} T_3(1_A, 1_A, 1_A) &= \mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) \\ &= \mathbb{E}_{x,y} 1_A(x) 1_A(y) 1_A(2y-x) && y = x + d \\ &= \mathbb{E}_y 1_A(y) (1_A * 1_A)(2y) \\ &= \langle 1_{2 \cdot A}, 1_A * 1_A \rangle && z = 2y \\ &= \langle \widehat{1_{2 \cdot A}}, \widehat{1_A * 1_A} \rangle. && \text{by Plancherel.} \end{aligned}$$

Continue the last manipulation to get

$$\begin{aligned}
 &= \langle \widehat{1_{2 \cdot A}}, \widehat{1_A}^2 \rangle \\
 &= \alpha^3 + \sum_{t \neq 0} \widehat{1_A}(t)^2 \overline{\widehat{1_{2 \cdot A}}(t)}.
 \end{aligned}$$

The last sum in absolute value is at most

$$\begin{aligned}
 &\leq \sup_{t \neq 0} |\widehat{1_A}(t)| \sum_{t \neq 0} |\widehat{1_A}(t) \overline{\widehat{1_{2 \cdot A}}(t)}| \\
 &\leq \sup_{t \neq 0} |\widehat{1_A}(t)| \left( \sum_t |\widehat{1_A}(t)|^2 \right)^{1/2} \left( \sum_t |\widehat{1_{2 \cdot A}}(t)|^2 \right)^{1/2} \\
 &\leq \sup_{t \neq 0} |\widehat{1_A}(t)| \cdot \alpha^{1/2} \cdot \alpha^{1/2} \\
 &\leq \sup_{t \neq 0} |\widehat{1_A}(t)|
 \end{aligned}$$

by C-S and Parseval.  $\square$

Using the above two results, we prove:

**Theorem 1.17** (Meshulam's Theorem). Let  $p \geq 3$  and let  $A \subset \mathbb{F}_p^n$  be a set containing no non-trivial 3-APs. Then  $|A| = O\left(\frac{p^n}{n \log p}\right)$ .

*Proof.* By assumption,  $T_3(1_A, 1_A, 1_A) = \frac{\alpha}{p^n}$ , but as in Lemma 1.16,

$$T_3(1_A, 1_A, 1_A) = \alpha^3 + \sum_{t \neq 0} \widehat{1_A}(t)^2 \overline{\widehat{1_{2 \cdot A}}(t)},$$

so  $\left| \frac{\alpha}{p^n} - \alpha^3 \right| \leq \sup_{t \neq 0} |\widehat{1_A}(t)| \cdot \alpha$ , which gives  $\sup_{t \neq 0} |\widehat{1_A}(t)| \geq \left| \frac{1}{p^n} - \alpha^2 \right| \geq \frac{\alpha^2}{2}$  provided  $p^n \geq 2\alpha^{-2}$ . By Lemma 1.15 with  $\rho = \frac{\alpha}{2}$ ,  $\exists V \leq \mathbb{F}_p^n$  of codimension 1 and  $x \in \mathbb{F}_p^n$  such that  $|A \cap (x + V)| \geq \left( \alpha + \frac{\alpha^2}{4} \right) |V|$ .

We iterate this observation. Let  $A_0 = A$ ,  $V_0 = \mathbb{F}_p^n$ ,  $\alpha_0 = \alpha = \frac{|A_0|}{|V_0|}$ . At step  $i$  of this iteration, we are given a set  $A_{i-1} \subset V_{i-1}$  of density  $\alpha_{i-1}$  with no nontrivial 3-APs. Provided that  $p^{\dim(V_{i-1})} \geq 2\alpha_{i-1}^{-2}$ ,  $\exists V_i \leq V_{i-1}$  of codimension 1 and  $x_i \in V_{i-1}$  such that  $|A_{i-1} \cap (x_i + V_i)| \geq \left( \alpha_{i-1} + \frac{\alpha_{i-1}^2}{4} \right) |V_i|$ . Set  $A_i = A_{i-1} - x_i$ . Note  $\alpha_i \geq \alpha_{i-1} + \frac{\alpha_{i-1}^2}{4}$  and  $A_i$  is free of nontrivial 3-APs. Through this iteration, the density of  $A$  increases from  $\alpha$  to  $2\alpha$  in at most  $\frac{\alpha}{\alpha^2/4} = 4\alpha^{-1}$  steps, from  $2\alpha$  to  $4\alpha$  in at most  $\frac{2\alpha}{(2\alpha)^2/4} = 2\alpha^{-1}$  steps, etc, which reaches 1 in at most

$$(4\alpha^{-1} + 2\alpha^{-1} + \alpha^{-1} + \dots) = 8\alpha^{-1}$$

steps. The argument must therefore end with  $\dim(V_i) \geq n - 8\alpha^{-1}$ , at which point we must have had  $p^{\dim(V_i)} \leq 2\alpha_i^{-2} \leq 2\alpha^{-2}$  (or else we could have continued). But we may assume that  $\alpha \geq \sqrt{2}p^{-n/4}$  (else we're done), whence  $p^{n-8\alpha^{-1}} \leq p^{n/2}$ , i.e.  $\frac{n}{2} \leq 8\alpha^{-1}$ , so  $\alpha \leq \frac{16}{n}$ , finishing the proof (in fact, we can now take  $C = 16 \log p$  as an explicit constant in the big O notation).  $\square$

26 Jan 2024,  
Lecture 4

So for  $A \subset \mathbb{F}_3^n$  containing no nontrivial 3-APs, we have  $|A| = O\left(\frac{3^n}{n}\right)$ . The largest known subset of  $\mathbb{F}_3^n$  containing no nontrivial 3-APs has size  $\geq (2.218)^n$ . (Proving  $2^n$  is trivial: take all combinations of zeroes and ones with no twos).

From now on, let  $G$  be a finite abelian group.  $G$  comes equipped with a set of **characters**, i.e. group homomorphisms  $\gamma : G \rightarrow \mathbb{C}^\times$ , which themselves form a group, denoted by  $\hat{G}$ , often referred to as the **dual** of  $G$ . It turns out that if  $G$  is finite and abelian, then  $\hat{\hat{G}} \cong G$ . For instance:

- If  $G = \mathbb{F}_p^n$ , then  $\hat{G} = \{\gamma_t : x \mapsto \omega^{x \cdot t} \mid t \in G\}$ .
- If  $G = \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ , then  $\hat{G} = \{\gamma_t : x \mapsto \omega^{xt} \mid t \in G\}$ .

**Definition 1.18.** Given  $f : G \rightarrow \mathbb{C}$ , define its **Fourier transform**  $\hat{f} : \hat{G} \rightarrow \mathbb{C}$  by

$$\hat{f}(\gamma) = \mathbb{E}_{x \in G} f(x) \gamma(x) \quad \forall \gamma \in \hat{G}.$$

It is easy to verify that we have an inversion formula, given by

$$f(x) = \sum_{\gamma \in \hat{G}} \hat{f}(\gamma) \overline{\gamma(x)}.$$

We can also check that Definition 1.6 and 1.9, Examples 1.3 and 1.10 and Lemmas 1.5, 1.8 and 1.11 go through in this general context.

**Example 1.19.** Let  $p$  be a prime, let  $L \leq p-1$  be even and consider  $J = [-\frac{L}{2}, \frac{L}{2}] \subset \mathbb{Z}_p$ . Then  $\forall t \neq 0$ ,

$$|\hat{1}_J(t)| \leq \min \left\{ \frac{L+1}{p}, \frac{1}{2|t|} \right\}.$$

This is on Ex. Sheet 1.

**Theorem 1.20** (Roth's Theorem). Let  $A \subset [N] := \{1, 2, \dots, N\}$  be a set containing no non-trivial 3-APs. Then  $|A| = O\left(\frac{N}{\log \log N}\right)$ .

**Lemma 1.21.** Let  $A \subset [N]$  be of density  $\alpha > 0$  satisfying  $N > 50\alpha^{-2}$  containing no nontrivial 3-APs. Let  $p$  be a prime in  $[\frac{N}{3}, \frac{2N}{3}]$  and write  $A' = A \cap [p] \subset \mathbb{Z}_p$ . Then either

- (i)  $\sup_{t \neq 0} |\hat{1}_{A'}(t)| \geq \frac{\alpha^2}{10}$  (where the Fourier coefficient is computed in  $\mathbb{Z}_p$ ); or



(ii)  $\exists$  interval  $J \subset [N]$  of length  $\geq \frac{N}{3}$  such that  $|A \cap J| \geq \alpha \left(1 + \frac{\alpha}{400}\right) |J|$ .

*Proof.* We may assume that  $|A'| = |A \cap [p]| \geq \alpha \left(1 - \frac{\alpha}{200}\right) p$ , since otherwise  $|A \cap [p+1, N]| \geq \alpha N - \alpha \left(1 - \frac{\alpha}{200}\right) p = \alpha(N-p) + \frac{\alpha^2 p}{200} \geq \alpha \left(1 + \frac{\alpha}{400}\right) (N-p)$ , so case (ii) holds with  $J = [p+1, N]$ .

Let  $A'' = A' \cap [\frac{p}{3}, \frac{2p}{3}]$ . Note that all 3-APs of the form  $(x, x+d, x+2d) \in A' \times A'' \times A''$  are in fact proper APs in  $[N]$  (and not only in  $\mathbb{Z}_p$ , since there's no "wrapping around", since  $x+d, x+2d \in [\frac{p}{3}, \frac{2p}{3}]$ ).

If  $|A' \cap [p/3]|$  or  $|A' \cap [2p/3, p]|$  are at least  $\frac{2|A'|}{5}$ , then we are again in case (ii) (details left as exercise). Hence we may assume that  $|A''| \geq \frac{|A'|}{5}$ . Now as in Lemma 1.16 and Theorem 1.17 with  $\alpha' = |A'|/p, \alpha'' = |A''|/p$ ,

$$\frac{\alpha''}{p} = \frac{|A''|}{p^2} = T_3(1_{A'}, 1_{A''}, 1_{A''}) = \alpha' \cdot \alpha''^2 + \sum_{t \neq 0} \hat{1}_{A'}(t) \hat{1}_{A''}(t) \overline{\hat{1}_{2 \cdot A''}(t)},$$

so as before,

$$\begin{aligned} \left| \frac{\alpha''}{p} - \alpha' \alpha''^2 \right| &\leq \frac{\alpha' \cdot \alpha''^2}{2} \leq \sup_{t \neq 0} |\hat{1}_{A'}(t)| \cdot \alpha'' \\ \implies \sup |\hat{1}_{A'}(t)| &\geq \frac{\alpha' \cdot \alpha''}{2} \geq \frac{(\alpha')^2}{10} \end{aligned}$$

provided that  $\frac{\alpha''}{p} \leq \frac{\alpha'(\alpha'')^2}{2}$  which holds since (using  $p \geq \frac{N}{3}$  and  $N > 50\alpha^{-2}$ )

$$\alpha' \alpha'' p \geq \alpha' \alpha'' \frac{N}{3} > \frac{\alpha'}{\alpha} \frac{\alpha''}{\alpha} \cdot 50 \geq \left(\frac{\alpha'}{\alpha}\right)^2 \cdot 10 = \left(1 - \frac{\alpha}{200}\right)^2 \cdot 10 \geq \frac{1}{2},$$

where the last step holds for  $\alpha = 1$  and hence for any  $\alpha \leq 1$ .  $\square$

We first now convert the large Fourier coefficient into a density increment.

**Lemma 1.22.** Let  $m \in \mathbb{N}$  and let  $\phi : [m] \rightarrow \mathbb{Z}_p$  by  $x \mapsto xt$  for some nonzero  $t$ . Given  $\epsilon > 0$ , there exists a partition of  $[m]$  into progressions  $P_i$  of length  $\in [\epsilon\sqrt{m}/2, \epsilon\sqrt{m}]$  such that  $\text{diam}(\phi(P_i)) = \max_{x,y \in P_i} |\phi(x) - \phi(y)| \leq \epsilon p \forall i$ .

*Proof.* Set  $u = \lfloor \sqrt{m} \rfloor$  and consider  $0, t, 2t, \dots, ut$ . By pigeonhole, we can find  $0 \leq v < w \leq u$  such that  $|wt - vt| \leq \frac{p}{u}$ . Divide  $[m]$  into residue classes mod  $s$ , where  $s = w - v$  (so  $|st| \leq \frac{p}{u}$ ). Each of these has size at least  $\frac{m}{s} \geq \frac{m}{u}$ . But each residue class can be divided into progressions of the form  $a, a+s, a+2s, a+ds$  with  $\frac{\epsilon u}{2} < d \leq \epsilon u$ . The diameter of the image of each progression under  $\phi$  is  $|dst| \leq \epsilon p$ .  $\square$

**Lemma 1.23.** Let  $A \subset [N]$  be of density  $\alpha > 0$ . Let  $p$  be a prime in  $[\frac{N}{3}, \frac{2N}{3}]$  and write  $A' = A \cap [p]$  as a subset of  $\mathbb{Z}_p$ . Suppose  $\exists t \neq 0$  such that  $\left| \widehat{1_{A'}}(t) \right| \geq \frac{\alpha^2}{10}$ .

Then there exists a progression  $P$  of length at least  $\frac{\alpha^2 \sqrt{N}}{500}$  such that  $|A \cap P| \geq \alpha \left(1 + \frac{\alpha}{80}\right) |P|$ .

*Proof.* Let  $\epsilon = \frac{\alpha^2}{40\pi}$  and use Lemma 1.22 to partition  $[p]$  into progressions  $P_i$  of length at least  $\frac{\epsilon \sqrt{p}}{2} \geq \frac{\alpha^2}{40\pi} \sqrt{\frac{N}{3}} \cdot \frac{1}{2} \geq \alpha^2 \sqrt{N} \cdot \frac{1}{500}$  and  $\text{diam}(\phi(P_i)) \leq \epsilon p$ . Fix one  $x_i$  from each  $P_i$ . Now work with the balanced function: since  $t \neq 0$ , the Fourier coefficient at  $t$  is the same for the indicator function and the balanced function.

$$\begin{aligned} \frac{\alpha^2}{10} &\leq \left| \widehat{f_{A'}}(t) \right| = \frac{1}{p} \left| \sum_{x \in \mathbb{Z}_p} f_{A'}(x) \omega^{xt} \right| = \frac{1}{p} \left| \sum_i \sum_{x \in P_i} f_{A'}(x) \omega^{xt} \right| \\ &= \frac{1}{p} \left| \sum_i \sum_{x \in P_i} f_{A'}(x) \omega^{x_i t} + \sum_i \sum_{x \in P_i} f_{A'}(x) (\omega^{xt} - \omega^{x_i t}) \right| \\ &\leq \frac{1}{p} \sum_i \left| \sum_{x \in P_i} f_{A'}(x) \right| + \frac{1}{p} \sum_i \sum_{x \in P_i} |f_{A'}(x)| 2\pi\epsilon \\ &\leq \frac{1}{p} \sum_i \left| \sum_{x \in P_i} f_{A'}(x) \right| + \frac{\alpha^2}{20} \end{aligned}$$

since  $|t(x_i - x)| \leq \epsilon p \ \forall x \in P_i$ . Hence

$$\frac{1}{p} \sum_i \left| \sum_{x \in P_i} f_{A'}(x) \right| \geq \frac{\alpha^2}{20}.$$

Since  $f_{A'}$  has mean zero,

$$\sum_i \left( \left| \sum_{x \in P_i} f_{A'}(x) \right| + \sum_{x \in P_i} f_{A'}(x) \right) \geq \frac{\alpha^2 p}{20},$$

so  $\exists i$  such that  $\left| \sum_{x \in P_i} f_{A'}(x) \right| + \sum_{x \in P_i} f_{A'}(x) \geq \frac{\alpha^2 |P_i|}{40}$  and so

$$\sum_{x \in P_i} f_{A'}(x) \geq \frac{\alpha^2 |P_i|}{80}.$$

□

This is about as technical as we get in this course.

*Proof of Roth's Theorem, theorem 1.20.* This is on Ex. Sheet 1. □

**Example 1.24** (Behrend's example). There exists a set  $A \subset [N]$  containing no nontrivial 3-APs of size  $|A| \geq C \exp(-c\sqrt{\log N}) N$ , where  $c$  and  $C$  are absolute constants. This is again on Ex. Sheet 1.

**Definition 1.25.** Let  $\Gamma \subset \widehat{G}$  and  $\rho > 0$ . By the **Bohr set**, written  $B(\Gamma, \rho)$ , we mean

$$B(\Gamma, \rho) = \{x \in G \mid |\gamma(x) - 1| \leq \rho \ \forall \gamma \in \Gamma\}.$$

We call  $|\Gamma|$  the **rank** and  $\rho$  the **radius** of the Bohr set.

**Example 1.26.** When  $G = \mathbb{F}_p^n$  and  $p = 3$ , we have  $B(\Gamma, \rho) = \langle \Gamma \rangle^\perp \ \forall \rho < 1$  (draw a picture!). For larger  $p$ , the same holds for smaller  $\rho$ .

**Lemma 1.27.** Let  $\Gamma \subset \widehat{G}$  be of size  $d$  and let  $\rho > 0$ . Then  $|B(\Gamma, \rho)| \geq \left(\frac{\rho}{2\pi}\right)^d |G|$ .

*Proof.* This is on Ex. Sheet 2. □

**Lemma 1.28** (Bogolyubov's lemma, again). Given  $A \subset \mathbb{Z}_p$  of density  $\alpha > 0$ ,  $\exists \Gamma \subset \widehat{\mathbb{Z}_p}$  of size at most  $2\alpha^{-2}$  such that  $B(\Gamma, \frac{1}{2}) \subset A + A - A - A$ .

31 Jan 2024,  
Lecture 6

*Proof.* Recall  $1_A * 1_A * 1_{-A} * 1_{-A}(x) = \sum_{t \in \widehat{\mathbb{Z}_p}} \left| \widehat{1_A}(t) \right|^4 \omega^{-xt}$ . Let  $\Gamma = \text{Spec}_{\sqrt{\frac{\alpha}{2}}}(1_A)$  and note that for all  $x \in B(\Gamma, \frac{1}{2})$  and  $t \in \Gamma$ ,  $\cos(2\pi xt/p) > 0$ . Hence

$$\begin{aligned} \text{Re} \left( \sum_{t \in \widehat{\mathbb{Z}_p}} \left| \widehat{1_A}(t) \right|^4 \omega^{-xt} \right) &= \underbrace{\sum_{t \in \Gamma} \left| \widehat{1_A}(t) \right|^4 \cos(2\pi xt/p)}_{\geq \alpha^4} + \\ &\quad \underbrace{\sum_{t \notin \Gamma} \left| \widehat{1_A}(t) \right|^4 \cos(2\pi xt/p)}_{\text{in absolute value } \leq \sup_{t \notin \Gamma} |\widehat{1_A}(t)|^2 \sum |\widehat{1_A}(t)|^2 \leq \left(\sqrt{\frac{\alpha}{2}} \cdot \alpha\right)^2 \cdot \alpha = \frac{\alpha^4}{2}}. \end{aligned}$$

□

## 2 Combinatorial methods

For now, let  $G$  be an abelian group. Given  $A, B \subset G$ . We defined  $A + B = \{a + b \mid a \in A, b \in B\}$  and can define  $A - B = \{a - b \mid a \in A, b \in B\}$ . If  $A$  and  $B$  are finite, then

$$\max(|A|, |B|) \leq |A \pm B| \leq |A| |B|$$

(and better bounds are available in certain settings).

**Example 2.1.** Let  $V \leq \mathbb{F}_p^n$  be a subspace. Then  $V + V = V$ , so  $|V + V| = |V|$ . In fact, if  $A \subset \mathbb{F}_p^n$  is such that  $|A + A| = |A|$ , then  $A$  must be a coset of a subspace.

**Example 2.2.** Let  $A \subset \mathbb{F}_p^n$  be such that  $|A + A| < \frac{3}{2} |A|$ . Then  $\exists V \leq \mathbb{F}_p^n$  such that  $A \subset V$  and  $|V| < \frac{3}{2} |A|$ . This is on Ex. Sheet 2.

**Example 2.3.** Let  $A \subset \mathbb{F}_p^n$  be a set of linearly independent vectors. Then  $A + A$  has size  $\binom{|A|}{2}$ . However,  $|A| \leq n$ , which is a small set.

Let  $A \subset \mathbb{F}_p^n$  be a set chosen randomly with probability  $p^{-\theta n}$  with  $\theta \in (\frac{1}{2}, 1]$ . Then with high probability,  $|A + A| = (1 - o(1)) \frac{|A|^2}{2}$ .

**Definition 2.4.** Given finite sets  $A, B \subset G$ , we define the **Rusza distance**  $d(A, B)$  between  $A$  and  $B$  by

$$d(A, B) = \log \frac{|A - B|}{\sqrt{|A||B|}}.$$

Observe that  $d(A, B)$  is nonnegative and symmetric.

**Lemma 2.5** (Rusza's triangle inequality). Given finite sets  $A, B, C$ , we have

$$d(A, C) \leq d(A, B) + d(B, C).$$

*Proof.* Observe that  $|B||A - C| \leq |A - B||B - C|$ . Indeed, writing each  $d \in A - C$  as  $d = a_d - c_d$  for some  $a_d \in A, c_d \in C$ , the map

$$\begin{aligned} \phi : B \times (A - C) &\rightarrow (A - B) \times (B - C) \\ (b, d) &\mapsto (a_d - b) \times (b - c_d) \end{aligned}$$

is injective (easy exercise). The triangle inequality now follows from the definition of the Rusza distance.  $\square$

**Definition 2.6.** Given a finite set  $A \subset G$ , we write  $\sigma(A) = \frac{|A+A|}{|A|}$  for the **doubling constant** and  $\delta(A) = \frac{|A-A|}{|A|}$  for the **difference constant**.

Then by Lemma 2.5,

$$\log \delta(A) = d(A, A) \leq d(A, -A) + d(A, -A) = 2 \log \sigma(A),$$

so  $\delta(A) \leq \sigma(A)^2$ , i.e.  $|A - A| \leq \frac{|A+A|^2}{|A|}$ .

**Notation.** Given  $A \subset G$  and  $l, m \in \mathbb{Z}_{\geq 0}$ , write  $lA - mA$  for the set

$$\underbrace{A + A + \dots + A}_{l \text{ times}} - \underbrace{A - A - \dots - A}_{m \text{ times}}.$$

**Theorem 2.7** (Plünnecke's inequality). Let  $A, B \subset G$  be finite sets such that  $|A + B| \leq K|A|$  for some  $K > 0$ . Then for any  $l, m \in \mathbb{Z}_{\geq 0}$ ,

$$|lB - mB| \leq K^{l+m} |A|.$$

02 Feb 2024,  
Lecture 7

*Proof.* WLOG assume that  $|A + B| = K |A|$ . Choose a nonempty subset  $A' \subset A$  such that the ratio  $\frac{|A' + B|}{|A'|}$  is minimized, and call this ratio  $K'$ . Then  $|A' + B| = K' |A'|$ ,  $K' \leq K$  and  $|A'' + B| \geq K' |A''| \ \forall A'' \subset A$ .

**Claim.** For any finite  $C \subset G$ ,  $|A' + B + C| \leq K' |A' + C|$ .

We first finish the proof assuming this claim, and then prove it. We first show that  $|A' + mB| \leq (K')^m |A| \ \forall m \in \mathbb{Z}_{\geq 0}$ . The cases  $m = 0$  and  $m = 1$  are clear. Now suppose that  $m > 1$  and the result holds for  $m - 1$ . By the claim with  $C = (m - 1)B$ ,

$$|A' + mB| = |A' + B + (m - 1)B| \leq K' |A' + (m - 1)B| \leq K' \cdot (K')^{m-1} |A'|.$$

But as in the proof of Rusza's triangle inequality,

$$\begin{aligned} |A'| |lB - mB| &\leq |A' + lB| |A' + mB| \leq (K')^l |A'| (K')^m |A'| \\ \implies |lB - mB| &\leq (K')^{l+m} |A'| \leq K^{l+m} |A|. \end{aligned}$$

Finally, we prove the claim by induction on  $|C|$ . For  $|C| = 1$ , we are just translating sets, so the claim holds. Now suppose the claim holds for some  $|C|$  and consider  $C' = C \cup \{x\}$  for some  $x \notin C$ . Observe

$$A' + B + C' = (A' + B + C) \cup (A' + B + x)$$

and in fact

$$A' + B + C' = (A' + B + C) \cup (A' + B + x) \setminus (D + B + x)$$

where  $D = \{a \in A' \mid A' + B + x \subset A' + B + C\}$ . By the definition of  $K$ ,  $|D + B| \geq K' |D|$ , so

$$\begin{aligned} |A' + B + C'| &\leq |A' + B + C| + |(A' + B + x) \setminus (D + B + x)| \\ &\leq |A' + B + C| + |A' + B| - |D + B| \\ &\leq K' |A' + C| + K' |A'| - K' |D| \\ &= K' (|A' + C| + |A'| - |D|). \end{aligned}$$

Now apply the same argument again for  $A' + C' = (A' + C) \sqcup ((A' + x) \setminus (E + x))$ , where  $E = \{a \in A' \mid a + x \in A' + C\} \subset D$ . Notice that the union is disjoint in this case. We conclude that

$$\begin{aligned} |A' + C'| &= |A' + C| + |A'| - |E| \geq |A' + C| + |A'| - |D| \\ \implies |A' + B + C'| &\leq K' (|A' + C| + |A'| - |D|) \leq K' |A' + C'|, \end{aligned}$$

proving the claim and hence the proof.  $\square$

We are now in a position to generalize Example 2.2.

**Theorem 2.8** (Freiman–Rusza theorem). Let  $A \subset \mathbb{F}_p^n$  be such that  $|A + A| \leq K|A|$  (i.e.  $\sigma(A) = K$ ) for some  $K > 0$ . Then  $A$  is contained in a coset of a subspace  $H \leq \mathbb{F}_p^n$  of size  $|H| \leq K^2 p^{K^4} |A|$ .

*Proof.* Choose maximal  $X \subset 2A - A$  such that the translates  $x + A$  for  $x \in X$  are disjoint.  $X$  cannot be too large:  $\forall x \in X, x + A \subset 3A - A$  and by Plünnecke,  $|3A - A| \leq K^4 |A|$ . But the translates  $x + A$  for  $x \in X$  are disjoint and each of size  $|A|$ , so

$$|X| |A| = \left| \bigcup_{x \in X} (x + A) \right| \leq |3A - A| \leq K^4 |A|,$$

hence  $|X| \leq K^4$ . We next show that  $2A - A \stackrel{(\star)}{\subset} X + A - A$ . Indeed, if  $y \in 2A - A$  and  $y \notin X$ , then  $y + A \cap (x + A) \neq \emptyset$  for some  $x \in X$  by maximality of  $X$ , so  $y \in X + A - A$ . If  $y \in X$ , then trivially  $y \in X + A - A$ . It follows by induction from  $(\star)$  that for all  $l \geq 2$ ,

$$lA - A \stackrel{(\star\star)}{\subset} (l-1)X + A - A,$$

since using the induction hypothesis,

$$\begin{aligned} lA - A &= A + (l-1)A - A \stackrel{\text{hyp}}{\subset} A + (l-2)X + A - A \\ &= (l-2)X + 2A - A \stackrel{(\star)}{\subset} (l-2)X + X + (A - A) = (l-1)X + A - A. \end{aligned}$$

Now let  $H$  be the subgroup of  $\mathbb{F}_p^n$  generated by  $A$ , which we can write in the form  $H = \cup_{l \geq 1} (lA - A) \stackrel{(\star\star)}{\subset} Y + A - A$ , where  $Y$  is the subgroup generated by  $X$ . Then  $|Y| \leq p^{|X|} \leq p^{K^4}$ , so

$$|H| \leq |Y + A - A| |Y| |A - A| \leq p^{K^4} K^2 |A|.$$

□

05 Feb 2024,  
Lecture 8

**Example 2.9.** This example shows that we need a constant that is exponential in  $K$  in the previous result. Let  $A = H \cup R \subset \mathbb{F}_p^n$  where  $H \leq \mathbb{F}_p^n$  is a subspace of dimension  $K \ll d \ll n - K$ , and  $R$  consists of  $K - 1$  linearly independent vectors in  $H^\perp$ . Then  $|A| = |H \cup R| \approx |H|$  and

$$|A + A| = |(H \cup R) + (H \cup R)| = |(H + H) \cup (H + R) \cup (R + R)| \approx K |H| \approx K |A|$$

since  $H + H = H$  and  $H + R$  gives us  $K - 1$  cosets of  $H$ , while  $R + R$  has tiny size.

However, a subspace  $V \leq \mathbb{F}_p^n$  containing  $A$  must have size  $\geq p^{d+(K-1)} = |H| \cdot p^{K-1} \approx |A| \cdot p^{K-1}$ , where the constant is exponential in  $K$ .

**Conjecture 2.10** (Polynomial Freiman–Rusza). Let  $A \subset \mathbb{F}_p^n$  be such that  $|A + A| \leq K |A|$ . Then there is a subspace  $H \leq \mathbb{F}_p^n$  of size at most  $C_1(K) |A|$  such that for some  $x \in \mathbb{F}_p^n$ ,

$$|A \cap (x + H)| \geq \frac{|A|}{C_2(K)}$$

where  $C_1(K)$  and  $C_2(K)$  are polynomials in  $K$ . For  $p = 2$ , this is now a theorem since November 2023 (by Gowers, Green, Manning, Tao).

**Definition 2.11.** Given an abelian group  $G$  and finite sets  $A, B \subset G$ , define the **additive energy** between  $A$  and  $B$  to be

$$E(A, B) = \frac{\#\{(a, a', b, b') \in A \times A \times B \times B \mid a + b = a' + b'\}}{|A|^{3/2} |B|^{3/2}}.$$

We refer to quadruples  $(a, a', b, b') \in A^2 \times B^2$  such that  $a + b = a' + b'$  as **additive quadruples**.

Observe that if  $G$  is finite and abelian, then

$$|A|^3 E(A, A) = |G|^3 \mathbb{E}_{x+y=z+w} 1_A(x) 1_A(y) 1_A(z) 1_A(w) \stackrel{(\star)}{=} |G|^3 \|\widehat{1_A}\|_4^4$$

where  $(\star)$  follows from Ex. Sheet 1, Q3.

**Example 2.12.** When  $H \leq \mathbb{F}_p^n$ , then  $E(V, V) = 1$ , i.e. the additive energy achieves its maximum. Exercise on Ex. Sheet 2: think of an example where the additive energy is small.

**Lemma 2.13.** Let  $G$  be abelian and let  $A, B \subset G$  be finite. Then

$$E(A, B) \geq \frac{\sqrt{|A| |B|}}{|A + B|}.$$

*Proof.* Note that for some  $x$  in  $G$ ,

$$|A|^{3/2} |B|^{3/2} E(A, B) = \#\{(a, a', b, b') \in A \times A \times B \times B \mid a + b = a' + b'\} = x = \sum_{x \in G} r_{A+B}(x)^2,$$

where  $r_{A+B}(x) = \#\text{ways of writing } x = a + b \text{ with } a \in A, b \in B$ . Observe that

$$\sum_{x \in G} r_{A+B}(x) = |A| |B|,$$

so

$$|A|^{3/2} |B|^{3/2} E(A, B) = \sum_{x \in G} r_{A+B}(x)^2 \geq \frac{(\sum_{x \in G} r_{A+B}(x))^2}{\sum_{x \in G} 1_{A+B}(x)^2} = \frac{(|A| |B|)^2}{|A+B|}$$

using Cauchy–Schwarz and the fact that we’re only summing over  $x \in G$  that are in  $A+B$ .  $\square$

In particular, if  $A \subset G$  such that  $|A+A| \leq K|A|$ , then  $E(A) \geq \frac{1}{K}$ . The converse is not true.

**Remark.** The same proof goes through for  $A-B$  instead of  $A+B$ .

**Example 2.14.** Let  $G$  be our favorite abelian group (really our favorite class of abelian groups, e.g.  $\mathbb{Z}_p$  for  $p$  running over primes). Then there exist constants  $\eta, \theta > 0$  such that for all sufficiently large  $n$ , there exists  $A \subset G$  with  $|A| = n$  satisfying  $E(A, A) \geq \eta$  and  $|A+A| \geq \theta |A|^2$ . This is on Ex. Sheet 2.

**Theorem 2.15** (Balog–Szemerédi–Gowers). Let  $G$  be an abelian group and let  $A \subset G$  be finite such that  $E(A, A) \geq \eta$  for some  $\eta > 0$ . Then  $\exists A' \subset A$  of size at least  $c(\eta)|A|$  such that

$$|A' + A'| \leq C(\eta) |A|.$$

Furthermore, here  $c(\eta)$  and  $C(\eta)$  are polynomials in  $\eta$ .<sup>3</sup>

We first prove a technical lemma using a method called ”dependent random choice”.

**Lemma 2.16.** Let  $A_1, A_2, \dots, A_m \subset [n]$  and suppose  $\sum_{i,j \in [m]} |A_i \cap A_j| \geq \delta^2 n m^2$ . Then there exists  $X \subset [m]$  of size at least  $\frac{\delta^5 m}{\sqrt{2}}$  such that  $|A_i \cap A_j| \geq \frac{\delta^2 n}{2}$  for at least 90% of the pairs  $(i, j) \in X^2$ .

*Proof.* First choose  $x_1, x_2, x_3, x_4, x_5$  at random from  $[n]$ , and then define the set  $X = \{i \in [m] \mid x_j \in A_i \ \forall j \in [5]\}$ . Observe that if  $|A_i \cap A_j| = \gamma n$ , then  $\mathbb{P}((i, j) \in X^2) = \gamma^5$ , and hence (by convexity or Hölder)

$$\mathbb{E} |X|^2 = \sum_{i,j} \mathbb{P}((i, j) \in X^2) \geq \delta^{10} m^2.$$

Call a pair  $(i, j)$  ”bad” if  $|A_i \cap A_j| < \frac{\delta^2 n}{2}$ . As before,

$$\mathbb{E}(\# \text{bad pairs in } X^2) \leq \frac{\delta^{10}}{2^5} m^2.$$

---

<sup>3</sup>TODO: see beginning of lec 9 - should it be  $C(\eta)|A'|$  in the above?



Hence  $\mathbb{E}(|X^2| - 16 \cdot \#\text{bad pairs in } X^2) = \frac{\delta^{10}}{2^5} m^2$ ,<sup>4</sup> so there must be a choice of  $x_1, x_2, \dots, x_5$  such that  $|X| \geq \frac{\delta^5 m}{\sqrt{2}}$  and the proportion of bad pairs in  $X$  is at most  $\frac{1}{16} < 10\%$ .  $\square$

*Proof of Theorem 2.15.* We call a difference  $d$  "popular" if  $d$  can be written as  $d = x - y$  with  $x, y \in A$  in at least  $\eta|A|/2$  ways, i.e.  $r_{A-A}(d) \geq \eta|A|/2$ . There must be at least  $\eta|A|/2$  popular differences, for if not, we get a contradiction through

$$\begin{aligned} \sum_d r_{A-A}(d)^2 &= \sum_{d \text{ popular}} r_{A-A}(d)^2 + \sum_{d \text{ not popular}} r_{A-A}(d)^2 \\ &< \eta \frac{|A|}{2} |A|^2 + \eta \frac{|A|}{2} \sum_d r_{A-A}(d) \\ &\leq \eta \frac{|A|}{2} |A|^2 + \eta \frac{|A|}{2} |A|^2. \end{aligned}$$

Define a graph with vertex set  $A$ , joining  $x$  and  $y$  by an edge if  $y - x$  is a popular difference. Then

$$\mathbb{E}_{x \in A} |N(x)| = \frac{1}{|A|} \sum_{x \in A} |N(x)| \geq \frac{\eta|A|}{2}.$$

We also have  $\mathbb{E}_{x, y \in A} |N(x) \cap N(y)| \geq \frac{\eta^2|A|}{4}$ . Indeed, by Cauchy-Schwarz,

$$\begin{aligned} \mathbb{E}_{x, y \in A} |N(x) \cap N(y)| &= \mathbb{E}_{x, y \in A} \sum_{z \in A} 1_{N(x)}(z) 1_{N(y)}(z) = \sum_{z \in A} (\mathbb{E}_{x \in A} 1_{N(x)}(z))^2 \\ &\geq \frac{1}{|A|} \left( \sum_{z \in A} \mathbb{E}_{x \in A} 1_{N(x)}(z) \right)^2 = \frac{1}{|A|} (\mathbb{E}_{x \in A} |N(x)|)^2 \geq \frac{1}{|A|} \left( \frac{\eta|A|}{2} \right)^2 = \frac{\eta^2|A|}{4}. \end{aligned}$$

We apply Lemma 2.16 with  $m = n = |A|$  and  $\delta^2 = \frac{\eta^2}{4}$  to find a subset  $A' \subset A$  of size  $\geq \eta^{10} \frac{|A|}{2^{11}}$  with the property that  $|N(x) \cap N(y)| \geq \frac{\eta^2|A|}{8}$  for at least 90% of  $(x, y) \in A'^2$ . But then for at least 10% of  $x \in A'$ ,  $|N(x) \cap N(y)| \geq \frac{\eta^2|A|}{8}$  for at least 80% of  $y \in A'$ . Hence  $\exists A'' \subset A'$  of size  $\geq \frac{\eta^{10}|A|}{2^{15}}$  such that  $\forall x \in A''$ , at least 80% of  $z \in A'$  satisfy  $|N(x) \cap N(z)| \geq \frac{\eta^2|A|}{8}$ . In particular, if  $x, y \in A''$ , then there are at least  $\frac{\eta^{10}|A|}{2^{12}}$  values of  $z \in A'$  such that  $|N(x) \cap N(z)| \geq \frac{\eta^2|A|}{8}$  and  $|N(y) \cap N(z)| \geq \frac{\eta^2|A|}{8}$ .

[We shall prove an upper bound of  $|A'' - A''|$  by showing that each element of  $A'' - A''$  can be written as a linear combination of distinct octuples from  $A$ .]

<sup>4</sup>TODO: This  $2^5$  should just be 2, right?

For each such  $z$ , there are thus  $\geq \left(\frac{\eta^2 |A|}{8}\right)^2$  pairs  $(u, v)$  such that  $u \in N(x) \cap N(y)$  and  $v \in N(y) \cap N(z)$ . For each such pair  $(u, v)$ , the elements  $u - x, z - u, v - z, y - v$  are all popular differences. Hence, for each pair  $(u, v)$ , there are at least  $\left(\frac{\eta |A|}{2}\right)^4$  octuples  $(a_1, a_2, \dots, a_8) \in A^8$  such that

$$u - x = a_2 - a_1, \quad z - u = a_4 - a_3, \quad v - z = a_6 - a_5, \quad y - v = a_8 - a_7.$$

In other words, there are at least

$$\underbrace{\left(\frac{\eta^{10} |A|}{2^{12}}\right)}_z \underbrace{\left(\frac{\eta^2 |A|}{8}\right)^2}_{u,v} \underbrace{\left(\frac{\eta |A|}{2}\right)^4}_{(a_1, \dots, a_8)} = \frac{\eta^{18}}{2^{22}} |A|^7$$

octuples  $(a_1, \dots, a_8) \in A^8$  such that

$$\begin{aligned} y - x &= (u - x) + (z - u) + (v - z) + (y - v) \\ &= a_2 - a_1 + a_4 - a_3 + a_6 - a_5 + a_8 - a_7. \end{aligned}$$

But distinct  $y - x$  give rise to distinct octuples, so

$$\begin{aligned} \frac{\eta^{18}}{2^{12}} |A|^7 \cdot |A'' - A''| &\leq |A|^8 \\ \implies |A'' - A''| &\leq 2^{12} \eta^{-18} |A| \leq 2^{27} \eta^{-28} |A''| \end{aligned}$$

(and  $|A'' + A''|$  follows from Plünnecke). □

### 3 Probabilistic tools

**Remark.** Assume in this chapter that all our probability spaces are finite, so we don't need to worry about convergence issues.

**Proposition 3.1** (Khintchine's inequality). Let  $X_1, X_2, \dots, X_n$  be independent random variables taking values  $\pm x_i$  with probability  $\frac{1}{2} \forall i = 1, \dots, n$ . Then  $\forall p \in [2, \infty)$ ,

$$\left\| \sum_{i=1}^n X_i \right\|_{L^p(\mathbb{P})} = O \left( p^{1/2} \left( \sum_{i=1}^n \|X_i\|_{L^2(\mathbb{P})}^2 \right)^{1/2} \right)$$

*Proof.* By nesting of norms, it suffices to prove the case  $p = 2k$  with  $k \in \mathbb{N}$ . For simplicity, write  $X = \sum_{i=1}^n X_i$  and WLOG assume that  $\sum_{i=1}^n \|X_i\|_{\infty}^2 =$

09 Feb 2024,  
Lecture 10

$\sum_{i=1}^n \|X_i\|_2^2 = 1$ . By Chernoff (Example 1.3), which states that  $\forall \theta > 0$ ,

$$\mathbb{P}(|X| \geq \theta) \leq 4 \exp(-\theta^2/4),$$

we have (using integration by parts, this is the alternative something formula, rewatch lecture to find out the name)

$$\|X\|_{2k}^{2k} = \int_0^\infty 2kt^{2k-1} \mathbb{P}(|X| \geq t) dt \leq 8k \underbrace{\int_0^\infty t^{2k-1} \exp(-t^2/4) dt}_{:=I(k)}.$$

We shall prove by induction that  $I(k) \leq C^{2k}(2k)^k/4k$  for some constant  $C > 0$ . For  $k = 1$ ,

$$\int_0^\infty t \exp(-t^2/4) dt = [-2 \exp(-t^2/4)]_0^\infty = 2 \leq C^2 \frac{2}{4}$$

for  $C \geq 2$ . For  $k > 1$ , we have

$$\begin{aligned} I(k) &= \int_0^\infty t^{2k-2} \cdot t \exp(-t^2/4) dt \\ &= [t^{2k-2}(-2) \exp(-t^2/4)]_0^\infty - \int_0^\infty (2k-2)t^{2k-3}(-2) \exp(-t^2/4) dt \\ &= 4(k-1) \int_0^\infty t^{2(k-1)-1} \exp(-t^2/4) dt \\ &= 4(k-1)I(k-1) \\ &\leq 4(k-1)C^{2(k-1)} \frac{(2(k-1))^{k-1}}{4(k-1)} \\ &\leq C^{2k} \frac{(2k)^k}{4k} \end{aligned}$$

for some  $C$ , where  $C \geq \sqrt{2}$  is claimed to work.  $\square$

**Corollary 3.2** (Rudin's inequality). Let  $\Lambda \subset \widehat{\mathbb{F}_2^n}$  be a linearly independent set and let  $p \in [2, \infty)$ . Then  $\forall \hat{f} \in \ell^2(\Lambda)$ , i.e.  $\hat{f} : \Lambda \rightarrow \mathbb{C}$ ,

$$\left\| \sum_{\gamma \in \Lambda} \hat{f}(\gamma) \gamma \right\|_{L^p(\mathbb{F}_2^n)} = O\left(\sqrt{p} \|\hat{f}\|_{\ell^2(\Lambda)}\right)$$

**Remark.** Note that here the LHS uses  $L^p$  for the normalized counting measure (i.e.  $\mathbb{E}$ ), while the RHS uses  $\ell^2$  for the counting measure (i.e.  $\sum$ ). In other words, these are the same, except one is normalized.

**Corollary 3.3** (Dual form of Rudin's inequality). Let  $\Lambda \subset \widehat{\mathbb{F}_2^n}$  be linearly

independent and let  $p \in (1, 2]$ . Then  $\forall f \in L^p(\mathbb{F}_2^n)$ ,

$$\|\widehat{f}\|_{\ell^2(\Lambda)} = O\left(\sqrt{\frac{p}{p-1}}\|f\|_{L^p(\mathbb{F}_2^n)}\right).$$

*Proof.* Let  $f \in L^p(\mathbb{F}_2^n)$  and write  $g = \sum_{\gamma \in \Lambda} \widehat{f}(\gamma)\gamma$ . Then, as  $g$  has the same Fourier coefficients as  $f$ ,

$$\|\widehat{f}\|_{\ell^2(\Lambda)}^2 = \sum_{\gamma \in \Lambda} \left|\widehat{f}(\gamma)\right|^2 = \sum_{\gamma \in \Lambda} \widehat{f}(\gamma)\overline{\widehat{f}(\gamma)} = \langle \widehat{f}, \widehat{g} \rangle_{\ell^2(\mathbb{F}_2^n)} = \langle f, g \rangle_{L^2(\mathbb{F}_2^n)},$$

but by Hölder,  $\langle f, g \rangle_{L^2(\mathbb{F}_2^n)} \leq \|f\|_{L^p(\mathbb{F}_2^n)}\|g\|_{L^{p'}(\mathbb{F}_2^n)}$ , where  $\frac{1}{p} + \frac{1}{p'} = 1$ . By Rudin's inequality for  $p' = \frac{p}{p-1}$ , we get

$$\|g\|_{L^{p'}(\mathbb{F}_2^n)} = O\left(\sqrt{p'}\|\widehat{g}\|_{\ell^2(\Lambda)}\right) = O\left(\sqrt{\frac{p}{p-1}}\|\widehat{f}\|_{\ell^2(\Lambda)}\right),$$

so

$$\begin{aligned} \|\widehat{f}\|_{\ell^2(\Lambda)}^2 &= \|f\|_{L^p(\mathbb{F}_2^n)} O\left(\sqrt{\frac{p}{p-1}}\|\widehat{f}\|_{\ell^2(\Lambda)}\right) \\ \implies \|\widehat{f}\|_{\ell^2(\Lambda)} &= O\left(\sqrt{\frac{p}{p-1}}\|f\|_{L^p(\mathbb{F}_2^n)}\right). \end{aligned} \quad \square$$

Recall that given  $A \subset \mathbb{F}_2^n$  of density  $\alpha > 0$ ,  $|\text{Spec}_\rho(1_A)| \leq \rho^{-2}\alpha^{-1}$ . This is the best possible, as the example of a subspace  $H \leq \mathbb{F}_2^n$  shows  $\text{Spec}_1(1_H) = H^\perp$ , so  $|\text{Spec}_1(1_H)| = |H^\perp| = \frac{|\mathbb{F}_2^n|}{|H|} = \left(\frac{|H|}{|\mathbb{F}_2^n|}\right)^{-1} = \alpha^{-1}$ .

**Theorem 3.4** (Special case of Chen's theorem). Let  $A \subset \mathbb{F}_2^n$  with density  $\alpha > 0$ . Then  $\forall \rho > 0$ , there exists a subspace  $H \leq \mathbb{F}_2^n$  of dimension at most  $O(\rho^{-2} \log \alpha^{-1})$  such that  $\text{Spec}_\rho(1_A) \subset H$ .

*Proof.* Let  $\Lambda \subset \text{Spec}_\rho(1_A)$  be a maximal linearly independent subset of  $\text{Spec}_\rho(1_A)$  and let  $H = \langle \text{Spec}_\rho(1_A) \rangle$ . Then  $\dim(H) = |\Lambda|$ . By dual Rudin (Corollary 3.3),  $\forall p \in (1, 2]$ ,

$$(\rho\alpha)^2 |\Lambda| \leq \sum_{\gamma \in \Lambda} \left|\widehat{1_A}(\gamma)\right|^2 = \|\widehat{1_A}\|_{\ell^2(\Lambda)}^2 = O\left(\frac{p}{p-1}\|1_A\|_{L^p(\mathbb{F}_2^n)}^2\right).$$

We can explicitly compute

$$\|1_A\|_{L^p(\mathbb{F}_2^n)}^2 = (\mathbb{E}_y |1_A(y)|^p)^{2/p} = \alpha^{2/p}.$$

Thus  $|\Lambda| \leq \rho^{-2}\alpha^{-2}O\left(\frac{p}{p-1}\alpha^{2/p}\right)$ . We want to choose  $p$  very close to 1, so choose

$p = 1 + (\log \alpha^{-1})^{-1}$  to conclude that

$$|\Lambda| \leq O(\rho^{-2} \log \alpha^{-1})$$

(calculation details omitted).  $\square$

12 Feb 2024,  
Lecture 11

**Theorem 3.5** (Chang's Theorem). Let  $G$  be a finite abelian group and let  $A \subset G$  have density  $\alpha > 0$ . If  $\Lambda \subset \text{Spec}_\rho(1_A)$  is dissociated, then  $|\Lambda| = O(\rho^{-2} \log \alpha^{-1})$ .

**Remark.** Last lecture, we wrote  $f \in L^p(G)$  to mean that  $f$  is a function on  $G$  with bounded  $L^p$ -norm and then said  $\|f\|_{L^p(G)} = (\mathbb{E}_{x \in G} f(x)^p)^{1/p}$ . Since we assumed that our groups are finite, the condition "with bounded  $L^p$ -norm" is unnecessary here, but we keep it as it is in line with the usual notation. We also said that  $\hat{f} \in \ell^2(\Lambda)$  if  $\hat{f}$  is a function supported on  $\Lambda \subset \hat{G}$  with bounded  $\ell^2$ -norm:  $\|\hat{f}\|_{\ell^2(\Lambda)} = \left( \sum_{\gamma \in \Lambda} |\hat{f}(\gamma)|^2 \right)^{1/2}$ . Finally,  $X \in L^p(\mathbb{P})$  means that the random variable  $X$  has bounded  $p^{\text{th}}$  moment, i.e.  $\mathbb{E}|X|^p < \infty$  (with expectation taken with respect to  $\mathbb{P}$ ).

**Remark.** The proofs of these probabilistic inequalities are nonexaminable. However, we are expected to be able to state them and apply them.

We may bootstrap Khintchine's inequality to obtain the following:

**Theorem 3.6** (Marcinkiewicz-Zygmund Inequality). Let  $p \in [2, \infty)$  and let  $X_1, X_2, \dots, X_n \in L^p(\mathbb{P})$  be independent random variables with  $\mathbb{E} \sum_{i=1}^n X_i = 0$ . Then

$$\left\| \sum_{i=1}^n X_i \right\|_{L^p(\mathbb{P})} = O \left( p^{1/2} \left\| \sum_{i=1}^n |X_i|^2 \right\|_{L^{p/2}(\mathbb{P})}^{1/2} \right).$$

*Proof.* For  $\mathbb{C}$ -valued random variables, the result follows from the real case by taking real and imaginary parts and applying the triangle inequality.

Next assume that the distribution of the  $X_i$ 's is symmetric, i.e.  $\mathbb{P}(X_i = a) = \mathbb{P}(X_i = -a) \forall a \in \mathbb{R}$ . Partition the probability space  $\Omega$  into sets  $\Omega_1, \Omega_2, \dots, \Omega_M$ , writing  $\mathbb{P}_j$  for the induced probability measure on  $\Omega_j$ , such that all  $X_i$ 's are symmetric and take at most two values on each  $\Omega_j$ . Applying Khintchine, for each  $j \in [M]$ ,

$$\begin{aligned} \left\| \sum_{i=1}^n X_i \right\|_{L^p(\mathbb{P}_j)}^p &= O(p^{p/2} \underbrace{\left( \sum_{i=1}^n \|X_i\|_{L^2(\mathbb{P}_j)}^2 \right)^{p/2}}_{= \left\| \sum_{i=1}^n |X_i|^2 \right\|_{L^{p/2}(\mathbb{P}_j)}^{p/2}}) \\ &= O(p^{p/2} \left\| \sum_{i=1}^n |X_i|^2 \right\|_{L^{p/2}(\mathbb{P}_j)}^{p/2}) \end{aligned}$$

so summing over all  $j \in [M]$  and taking the  $p^{\text{th}}$  roots gives the symmetric case.

Now suppose the  $X_i$ 's are arbitrary and let  $Y_1, \dots, Y_n$  be such that  $X_i \sim Y_i \forall i$  and  $X_1, \dots, X_n, Y_1, \dots, Y_n$  are independent. Applying the symmetric result to  $X_i - Y_i$ ,

$$\begin{aligned} \left\| \sum_{i=1}^n (X_i - Y_i) \right\|_{L^p(\mathbb{P} \times \mathbb{P})} &= O \left( p^{1/2} \left\| \sum_{i=1}^n |X_i - Y_i|^2 \right\|_{L^{p/2}(\mathbb{P} \times \mathbb{P})}^{1/2} \right) \\ &= O \left( p^{1/2} \left\| \sum_{i=1}^n |X_i|^2 \right\|_{L^{p/2}(\mathbb{P})}^{1/2} \right) \end{aligned}$$

by expanding  $|X_i - Y_i|^2$  and bounding above by  $4|X_i|^2$ . But also

$$\begin{aligned} \left\| \sum_{i=1}^n X_i \right\|_{L^p(\mathbb{P})} &= \left\| \sum_{i=1}^n X_i - \mathbb{E} \sum_{i=1}^n Y_i \right\|_{L^p(\mathbb{P})} \\ &\leq \left\| \sum_{i=1}^n (X_i - Y_i) \right\|_{L^p(\mathbb{P} \times \mathbb{P})} \end{aligned}$$

by convexity/Jensen.  $\square$

**Theorem 3.7** (Croo–Sisask Almost Periodicity). Let  $G$  be a finite abelian group, let  $\epsilon > 0$  and let  $p \in [2, \infty)$ . Let  $A, B \subset G$  be such that  $|A + B| \leq K|A|$  and let  $f : G \rightarrow \mathbb{C}$ . Then  $\exists b \in B$  and a set  $X \subset B - b$  such that

$$|X| \geq (2K)^{-O(\epsilon^{-2}p)} |B|$$

and

$$\|\tau_x(f * \mu_A) - f * \mu_A\|_{L^p(G)} \leq \epsilon \|f\|_{L^p(G)} \quad \forall x \in X,$$

where  $\tau_x g(y) = g(y + x)$  and  $\mu_A$  is the characteristic measure of  $A$ , defined by  $\mu_A(x) = \alpha^{-1} 1_A(x)$ .

**Remark.** We only need  $G$  to be discrete for the result to hold, but we consider the case "finite and abelian" as we don't want to introduce too much notation in the proof.

**Remark.** For intuition, work through the example  $f = 1_{A-A}$ .

*Proof.* The main idea is to approximate  $f * \mu_A(y) = \mathbb{E}_x \mu_A(x) f(y - x) = \mathbb{E}_{x \in A} f(y - x)$  by  $\frac{1}{k} \sum_{i=1}^k f(y - z_i)$  with  $z_i$  sampled independently at random from  $A$  for some suitable choice  $k$ .

For each  $y \in G$ , define  $Z_i(y) = \tau_{-z_i}(f)(y) - f * \mu_A(y)$  for  $i \in [k]$ . For fixed  $y \in G$ , these are independent and have mean 0, so by Marcinkiewicz–Zygmund,

for each  $y \in G$ ,

$$\begin{aligned} \left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mathbb{P})}^p &= O \left( p^{p/2} \left\| \sum_{i=1}^k |Z_i(y)|^2 \right\|_{L^{p/2}(\mathbb{P})}^{p/2} \right) \\ &= O \left( p^{p/2} \mathbb{E} \left( \sum_{i=1}^k |Z_i(y)|^2 \right)^{p/2} \right) \end{aligned}$$

Applying Hölder with  $\frac{2}{p} + \frac{1}{p'} = 1$  (so  $\frac{1}{p'} \cdot \frac{p}{2} = \frac{p}{2} - 1$ ) to the expression inside the expectation gives that it is

$$\begin{aligned} \left( \sum_{i=1}^k |Z_i(y)|^2 \right)^{p/2} &\leq \left( \sum_{i=1}^k 1^{p'} \right)^{\frac{1}{p'} \cdot \frac{p}{2}} \left( \sum_{i=1}^k |Z_i(y)|^{2 \cdot \frac{p}{2}} \right)^{\frac{2}{p} \cdot \frac{p}{2}} \\ &= k^{\frac{p}{2}-1} \sum_{i=1}^k |Z_i(y)|^p. \end{aligned}$$

So for each  $y \in G$ ,

$$\left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mathbb{P})}^p = O \left( p^{p/2} k^{\frac{p}{2}-1} \mathbb{E} \sum_{i=1}^k |Z_i(y)|^p \right).$$

Summing over  $y \in G$  gives

$$\mathbb{E}_{y \in G} \left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mathbb{P})}^p = O \left( p^{p/2} k^{\frac{p}{2}-1} \mathbb{E} \sum_{i=1}^k \mathbb{E}_{y \in G} |Z_i(y)|^p \right)$$

with

$$\left( \mathbb{E}_{y \in G} |Z_i(y)|^p \right)^{1/p} = \|Z_i\|_{L^p(G)} \leq \underbrace{\|\tau_{-z_i}(f)\|_{L^p(G)}}_{=\|f\|_{L^p(G)}} + \underbrace{\|f * \mu_A\|_{L^p(G)}}_{\leq \|f\|_{L^p(G)}} \leq 2\|f\|_{L^p(G)},$$

where the second underbrace estimate follows by Young's Convolution Inequality, which states that if  $1 + \frac{1}{r} = \frac{1}{p} + \frac{1}{q}$ , then  $\|f * g\|_r \leq \|f\|_p \|g\|_q$ . It follows that

$$\begin{aligned} \mathbb{E}_{(z_1, \dots, z_k) \in A^k} \mathbb{E}_{y \in G} \left\| \sum_{i=1}^k Z_i(y) \right\|^p &= O \left( p^{p/2} k^{p/2-1} \mathbb{E}_{(z_1, \dots, z_k) \in A^k} \sum_{i=1}^k 2 \cdot \|f\|_{L^p(G)}^p \right) \\ &= O \left( p^{p/2} k^{p/2} \|f\|_{L^p(G)}^p \right) \\ &= O \left( (pk \|f\|_{L^p(G)}^2)^{p/2} \right), \end{aligned}$$

which implies (after dividing through by  $k^p$ )

$$\mathbb{E}_{(z_1, \dots, z_k) \in A^k} \mathbb{E}_{y \in G} \underbrace{\left| \frac{1}{k} \sum_{i=1}^k \tau_{-z_i}(f)(y) - f * \mu_A(y) \right|^p}_{:= (\star)} = O\left((pk^{-1} \|f\|_{L^p(G)}^2)^{p/2}\right)$$

Choose  $k = O(\epsilon^{-2}p)$  such that RHS is at most  $(\frac{\epsilon}{4} \|f\|_{L^p(G)})^p$ . Write

$$L = \left\{ (z_1, \dots, z_k) \in A^k \mid (\star) \leq \left(\frac{\epsilon}{2} \|f\|_{L^p(G)}\right)^p \right\}.$$

By averaging/Markov, since  $\mathbb{E}(\star) \leq (\frac{\epsilon}{4} \|f\|_{L^p(G)})^p = 2^{-p} (\frac{\epsilon}{2} \|f\|_{L^p(G)})^p$ ,

$$\begin{aligned} \frac{|L^C|}{|A|^k} &= \mathbb{P}\left((\star) \geq \left(\frac{\epsilon}{2} \|f\|_{L^p(G)}\right)^p\right) \leq \mathbb{P}((\star) \geq 2^p \mathbb{E}(\star)) \leq 2^{-p} \\ \implies \frac{|L|}{|A|^k} &\geq 1 - 2^{-p}. \end{aligned}$$

So in particular,  $|L| \geq \frac{1}{2} |A|^k$ . Let

$$D = \left\{ \underbrace{(b, b, \dots, b)}_{k \text{ times}} \mid b \in B \right\},$$

so  $L + D \subset (A + B)^k$ , whence (as  $|L| \geq \frac{1}{2} |A|^k$ )

$$|L + D| \leq |(A + B)^k| \leq (K|A|)^k = K^k |A|^k \leq (2K)^k |L|$$

By Lemma 2.13,  $E(L + D, L + D) \geq \frac{|D|^2 |L|}{(2K)^k}$ , so there are at least  $\frac{|D|^2}{(2K)^k}$  pairs  $(b_1, b_2) \in D \times D$  such that  $r_{L-L}(b_1 - b_2) > 0$ . In particular, there exists  $b \in B$  and  $X \subset B - b$  of size  $|X| \geq \frac{|D|}{(2K)^k} = \frac{|B|}{(2K)^k}$  such that  $r_{L-L}(x) > 0 \forall x \in X$ . In other words,  $\forall x \in X, \exists l_1(x), l_2(x) \in L$  such that  $\forall i \in [k], l_1(x)_i = l_2(x)_i + x$ . By the triangle inequality, for each  $x \in X$ ,

$$\begin{aligned} & \|\tau_{-x}(f * \mu_A) - f * \mu_A\|_{L^p(G)} \\ & \leq \|t_{-x}(f * \mu_A) - \tau_{-x}\left(\frac{1}{k} \sum_{i=1}^k \tau_{-l_2(x)_i}(f)\right)\|_{L^p(G)} + \|\tau_{-x}\left(\frac{1}{k} \sum_{i=1}^k \tau_{-l_2(x)_i}(f)\right) - f * \mu_A\|_{L^p(G)} \\ & = \|f * \mu_A - \frac{1}{k} \sum_{i=1}^k \tau_{-l_2(x)_i}(f)\|_{L^p(G)} + \|\frac{1}{k} \sum_{i=1}^k \tau_{-x-l_2(x)_i}(f) - f * \mu_A\|_{L^p(G)} \\ & \leq 2 \cdot \frac{\epsilon}{4} \|f\|_{L^p(G)} \end{aligned}$$



by the definition of  $L$ . □

**Theorem 3.8** (Bogolyubov again, due to Sanders). Let  $A \subset \mathbb{F}_p^n$  be a set of density  $\alpha > 0$ . Then there exists a subspace  $V \leq \mathbb{F}_p^n$  of codimension  $O((\log(\alpha^{-1}))^4)$  such that  $V \subset A + A - A - A$ .

*Proof.* This is on Ex. Sheet 3. Use Croot–Sisask and Chang’s theorem. □

**Theorem 3.9** (due to Schoen and Shlvedov). Let  $p \neq 5$  and let  $A \subset \mathbb{F}_p^n$ . Suppose that  $A$  contains no nontrivial solutions to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 5y,$$

i.e. no solution  $(y, (x_i)_{i=1}^5) \in A^6$  such that  $y \neq x_i$  for some  $i \in [5]$ . Then  $|A| = \exp(-\Omega(n^{1/5})) |\mathbb{F}_p^n|^{.5}$

*Proof.* □

---

<sup>5</sup> $\Omega$  is the opposite to  $O$ , one lowerboudns while the other upperbounds.