ADDITIVE COMBINATORICS

— LECTURE NOTES —
FOURIER ANALYSIS AND MESHULAM'S THEOREM ON SUBSETS OF FINITE ABELIAN GROUPS WITHOUT 3AP

We recall the central theorem of this course.

Theorem 0.1 (Szemeredi's theorem)**.** *Let k be a positive integer and let $\alpha > 0$. Then there is a positive integer N_0 such that the following holds. If $n \geq N_0$ and $A \subseteq [n]$ has size $|A| \geq \alpha n$, then A contains a proper k-AP.*

In the next lecture we will prove the case $k = 3$ (Roth's theorem). In this lecture we will consider the technically simpler analogue of 3-APs in $\mathbb{F}_p^n$ and prove Meshulam's theorem (Theorem 2.1). We start by introducing Fourier analysis on finite abelian groups, which is used in the proof of Meshulam's theorem.

1. Fourier analysis on finite abelian groups

This section is a quick introduction to Fourier analysis on finite abelian groups. Throughout this section, let G be a finite abelian group written additively. We denote by $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ the multiplicative group of nonzero complex numbers. The complex conjugate of $z \in \mathbb{C}$ is denoted $\overline{z}$. For a set S and a function $f : S \to \mathbb{C}$, denote

$$\mathbb{E}_{s\in S}\, f(s) = \frac{1}{|S|} \sum_{s\in S} f(s).$$

If the set S is clear from the context then we may write $\mathbb{E}_s\, f(s)$ instead.

1.1. **Characters and the character group.** A *character* of G is a function $\chi : G \to \mathbb{C}^*$ that is a group homomorphism. That is, $\chi(a + b) = \chi(a)\chi(b)$ for all $a, b \in G$ (and hence the identity element of G is mapped to 1). Since G is finite, every element of G has finite order. If $a \in G$ is an element of order n then the order of $\chi(a)$ must be a divisor of n, so $\chi(a)$ is an n-th root of unity: $\chi(a) = e^{2\pi ik/n}$ for some integer k. In particular, we have $|\chi(a)| = 1$ and

$$\chi(-a) = \chi(a)^{-1} = \overline{\chi(a)}.$$

We denote the set of all characters of G by $\widehat{G}$, the *character group* of G. The set $\widehat{G}$ is indeed a group under the usual point-wise multiplication of functions with the identity element being the *trivial character* χ_0 given by $\chi_0(a) = 1$ for all $a \in G$. The inverse of a character χ is given by $\chi^{-1}(a) = \chi(a)^{-1} = \overline{\chi(a)}$.

Example 1.1. Let $G = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n and let $\omega = e^{2\pi i/n}$. For $c \in \mathbb{Z}/n\mathbb{Z}$ the map $\chi_c : G \to \mathbb{C}^*$ given by

$$\chi_c(a) := \omega^{ac}$$

is a character of G. The map χ_c is well-defined since for integers k, ℓ we have $\omega^k = \omega^\ell$ if $k \equiv \ell \pmod{n}$. Conversely, every character of G is of the form χ_c for some $c \in \mathbb{Z}/n\mathbb{Z}$. Indeed, χ is completely determined by $\chi(1)$ as $\chi(k) = \chi(1)^k$ for every k, and $\chi(1)$ must be an n-th root of

Date: February 23, 2021.

unity as $\chi(1)^n = \chi(n) = \chi(0) = 1$. It follows that the map $G \mapsto \widehat{G}$ given by $c \mapsto \chi_c$ is a group isomorphism.

Example 1.2. Let $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}$. Let $\omega_k = e^{2\pi i/n_k}$ for $k = 1, \ldots, d$. Then for every $c \in \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}$ there is a character $\chi_c : G \to \mathbb{C}^*$ given by

$$\chi_c(a) = \omega_1^{a_1 c_1} \omega_2^{a_2 c_2} \cdots \omega_d^{a_d c_d}.$$

These characters are pairwise different and every character of G is of this form, so $|\widehat{G}| = |G|$. Since $\chi_c \chi_{c'} = \chi_{c+c'}$ for all c and c', we see that in fact $G \cong \widehat{G}$.

We recall the fact that every abelian group is the product of cyclic groups.

Theorem 1.3 (Structure theorem for finite abelian groups). *Let G be a finite abelian group. Then*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}$$

for integers $n_1, \ldots, n_d$. The decomposition can be chosen such that n_i divides n_{i+1} for all $i = 1, \ldots, d-1$ (in which case $n_1, \ldots, n_d$ are uniquely determined by G).

Corollary 1.4. *Let G be a finite abelian group. Then there is an isomorphism $G \to \widehat{G}$. In particular, $|G| = |\widehat{G}|$.*

Proof: Since isomorphic groups have isomorphic character groups, this follows directly from Theorem 1.3 and Example 1.2. □

The following simple fact will turn out to be very useful.

Lemma 1.5. *Let χ be a character of G. Then*

$$\mathbb{E}_{a\in G}\, \chi(a) = \begin{cases} 1 & \text{if } \chi = \chi_0 \text{ (the trivial character)}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: We leave this as an exercise to the reader. □

1.2. **Fourier transform.** On the linear space $\mathbb{C}^G$ of functions $G \to \mathbb{C}$ we have the inner product

$$\langle f, g \rangle = \mathbb{E}_{a\in G}\, f(a)\overline{g(a)}.$$

Note that $\widehat{G} \subseteq \mathbb{C}^G$.

Proposition 1.6 (Orthogonality of characters). *Let $\chi, \chi' \in \widehat{G}$. Then*

$$\langle \chi, \chi' \rangle = \begin{cases} 1 & \text{if } \chi = \chi', \\ 0 & \text{otherwise.} \end{cases}$$

Proof: Let $\psi = \chi \cdot (\chi')^{-1}$. So $\psi(a) = \chi(a)\overline{\chi'(a)}$. We have

$$\langle \chi, \chi' \rangle = \mathbb{E}_{a\in G}\, \psi(a)$$

and the result follows from Lemma 1.5 applied to the character ψ. □

It now follows from Corollary 1.4 that the characters form an orthonormal basis of $\mathbb{C}^G$. The *Fourier transform* is the linear map $\mathbb{C}^G \to \mathbb{C}^{\widehat{G}}$ that maps $f : G \to \mathbb{C}$ to $\widehat{f} : \widehat{G} \to \mathbb{C}$ given by

$$\widehat{f}(\chi) = \langle f, \chi \rangle.$$

The function $\widehat{f}$ is called the *Fourier transform of* f and the numbers $\widehat{f}(\chi)$ are the *Fourier coefficients* of f. Note that $\widehat{f}(\chi_0) = \mathbb{E}_a\, f(a)$ is the average value of f.

Proposition 1.7 (Fourier inverse)**.** *Let* $f : G \to \mathbb{C}$*. Then*

$$f = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi.$$

In particular, we have $f(0) = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)$*.*

Proof: This follows directly from the fact that the characters of G form an orthonormal basis of $\mathbb{C}^G$. □

If we equip $\mathbb{C}^{\widehat{G}}$ with the standard inner product, then the Fourier transform is an isometry.

Proposition 1.8 (Parseval's theorem)**.** *Let* $f, g : G \to \mathbb{C}$*. Then*

$$\sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)} = \langle f, g \rangle.$$

Proof: Again, this follows directly from the fact that the characters form an orthonormal basis of $\mathbb{C}^G$:

$$\langle f, g \rangle = \langle \sum_{\chi} \widehat{f}(\chi)\chi, \sum_{\chi'} \widehat{g}(\chi')\chi' \rangle = \sum_{\chi,\chi'} \widehat{f}(\chi)\overline{\widehat{g}(\chi')} \cdot \langle \chi, \chi' \rangle = \sum_{\chi} \widehat{f}(\chi)\overline{\widehat{g}(\chi)}.$$

□

A special case of Parseval's theorem is 'Parseval's identity' which states:

$$\sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2 = \|f\|^2,$$

where $\|f\| = \langle f, f \rangle^{1/2}$ is the norm on $\mathbb{C}^G$ induced by the inner product.

1.3. **Convolution.** Let $f, g : G \to \mathbb{C}$. The *convolution* of f and g is the function $f * g : G \to \mathbb{C}$ defined by

$$f * g(a) = \mathbb{E}_{b \in G} f(b)g(a - b).$$

Proposition 1.9. *Let* $f, g : G \to \mathbb{C}$*. Then* $\widehat{f * g}(\chi) = \widehat{f}(\chi) \cdot \widehat{g}(\chi)$ *for all* $\chi \in \widehat{G}$*.*

Proof: We have

$$\begin{aligned}
\widehat{f * g}(\chi) &= \mathbb{E}_a (f * g)(a)\overline{\chi(a)} \\
&= \mathbb{E}_a \mathbb{E}_b f(b)g(a - b)\chi(-a) \\
&= \mathbb{E}_c \mathbb{E}_b f(b)g(c)\chi(-b - c) \\
&= \mathbb{E}_c \mathbb{E}_b f(b)g(c)\overline{\chi(b)\chi(c)} \\
&= \mathbb{E}_b f(b)\overline{\chi(b)} \cdot \mathbb{E}_c g(c)\overline{\chi(c)} \\
&= \widehat{f}(\chi)\widehat{g}(\chi).
\end{aligned}$$

□

Remark 1.10. If for $u, v \in \mathbb{C}^{\widehat{G}}$ we define $u * v(\chi) = \sum_{\psi} u(\psi)v(\chi\psi^{-1})$, then we get the analogous result $\widehat{f} * \widehat{g} = \widehat{fg}$ for $f, g \in \mathbb{C}^G$.

For a subset $A \subseteq G$ we denote by $\mathbf{1}_A \in \mathbb{C}^G$ the indicator function of A given by

$$\mathbf{1}_A(a) = \begin{cases} 1 & \text{if } a \in A, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 1.11. *Let $A_1, \dots, A_k \subseteq G$ and let $c \in G$. Then*

$$\mathbf{1}_{A_1} * \cdots * \mathbf{1}_{A_k}(c) = |G|^{1-k} \cdot |\{(a_1, \dots, a_k) \in A_1 \times \cdots \times A_k : a_1 + \cdots + a_k = c\}|.$$

Proof: We leave this as an exercise to the reader. □

2. Meshulam's theorem

Let p be an odd prime number. In this section we will consider subsets $A \subseteq (\mathbb{Z}/p\mathbb{Z})^n$ that do not contain a proper 3-term arithmetic progression. Recall that an arithmetic progression is called *proper* if it has nonzero common difference. It will be convenient to identify $(\mathbb{Z}/p\mathbb{Z})^n$ with $\mathbb{F}_p^n$, the n-dimensional vector space over the field of p elements. We are interested in the largest possible density of a subset of $\mathbb{F}_p^n$ that contains no proper 3-term arithmetic progression. We denote

$$\delta_n(p) = \max\left\{\frac{|A|}{p^n} : A \subseteq \mathbb{F}_p^n \text{ has no proper 3-AP}\right\}.$$

Note that $\delta_0(p) = 1$. For a fixed odd prime p, we are interested in the asymptotic behaviour of $\delta_n(p)$ as $n \to \infty$. The main theorem in this lecture implies that $\delta_n = O(n^{-1})$.

Theorem 2.1 (Meshulam)**.** *Let p be an odd prime number and let n be a positive integer. If $A \subseteq \mathbb{F}_p^n$ has no proper 3-term arithmetic progressions, then*

$$|A| \leq \frac{2p^n}{n}.$$

This theorem is in fact a special case of the theorem proved in [Mes95]. There, it is shown that if G is a finite abelian group of odd order with d constituents (the number of factors in the decomposition in Theorem 1.3), and $A \subseteq G$ has no proper 3-AP, then $|A| \leq \frac{2|G|}{d}$ holds. The proof relies on Fourier analysis on finite abelian groups and is based on earlier work, in particular on Roth's paper [Rot53].

For the rest of this section, we fix an odd prime number p and write δ_n for $\delta_n(p)$. For $a, b \in \mathbb{F}_p^n$ we write $a \cdot b$ for the sum $a_1 b_1 + \cdots + a_n b_n$. We will also put $\omega = e^{2\pi i/p}$. The characters $\mathbb{F}_p^n \to \mathbb{C}^*$ take the form

$$\chi_c(a) = \omega^{c_1 a_1 + \cdots + c_n a_n} = \omega^{c \cdot a}$$

for $c \in \mathbb{F}_p^n$. The trivial character is χ_0 (it is constant on the whole space).

For $c \neq 0$, the space $\mathbb{F}_p^n$ is partitioned into p parallel hyperplanes $W_\alpha = \{a \in \mathbb{F}_p^n : c \cdot a = \alpha\}$, where $\alpha \in \mathbb{F}_p$. Note that χ_c is constant on each of the hyperplanes. If $A \subseteq \mathbb{F}_p^n$ has no proper 3-AP, then the intersection $A \cap W_\alpha$ can be transformed into a subset $A' \subseteq \mathbb{F}_p^{n-1}$ without proper 3-AP of size $|A'| = |A \cap W_\alpha|$. It follows that $|A \cap W_\alpha| \leq \delta_{n-1} p^{n-1}$ and hence (summing over all $\alpha \in \mathbb{F}_p$) that $|A| \leq \delta_{n-1} p^n$.

Lemma 2.2. *Let $n \geq 1$ and let $A \subseteq \mathbb{F}_p^n$ contain no proper 3-AP. Let $u = \delta_{n-1}\mathbf{1} - \mathbf{1}_A$. Then for every $c \in \mathbb{F}_p^n$ we have*

$$|\widehat{u}(\chi_c)| \leq \delta_{n-1} - |A| \cdot p^{-n}.$$

Proof: For $c = 0$ we have $\widehat{u}(\chi_c) = \mathbb{E}_{a \in \mathbb{F}_p^n} u(a) = \delta_{n-1} - |A| \cdot p^{-n} \geq 0$.

Now let $c \neq 0$. Consider the partition of $\mathbb{F}_p^n$ into the p parallel hyperplanes

$$W_\alpha = \{x \in \mathbb{F}_p^n : c \cdot x = \alpha\}, \qquad (\alpha \in \mathbb{F}_p).$$

Denote $y_\alpha = \sum_{a\in W_\alpha} u(a)$. Since $|A\cap W_\alpha| \le \delta_{n-1}p^{n-1}$, we obtain

$$y_\alpha = \delta_{n-1}p^{n-1} - |A\cap W_\alpha| \ge 0.$$

It follows that

$$|\widehat{u}(\chi_c)| = p^{-n}\Big|\sum_{\alpha\in\mathbb{F}_p} y_\alpha \cdot \overline{\omega^\alpha}\Big| \le p^{-n}\sum_{\alpha\in\mathbb{F}_p}|y_\alpha| = p^{-n}\sum_{\alpha\in\mathbb{F}_p} y_\alpha = \delta_{n-1} - |A|p^{-n}.$$

□

Lemma 2.3. *Let $A\subseteq \mathbb{F}_p^n$ contain no proper 3-APs. Then*

$$|A| \le \frac{1+p^n\delta_{n-1}}{1+\delta_{n-1}}.$$

Proof: Let $B = -2A$. Observe that B also has no proper 3-AP and that $|B| = |A|$. Set $u = \delta_{n-1}\mathbf{1} - \mathbf{1}_B$. We will consider the function $f = \mathbf{1}_A * \mathbf{1}_A * u$.

By Lemma 1.11 we have

$$f(0) = \delta_{n-1}\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}(0) - \mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_B(0) = p^{-2n}(\delta_{n-1}|A|^2 - |A|) \tag{1}$$

since $a+b+c=0$ has $|A|^2$ solutions in $A\times A\times \mathbb{F}_p^n$, and has $|A|$ solutions in $A\times A\times B$ since A has no proper 3-AP.

Using that $f(0) = \sum_{c\in\mathbb{F}_p^n}\widehat{f}(\chi_c)$ and that $\widehat{f} = \widehat{\mathbf{1}_A}\cdot\widehat{\mathbf{1}_A}\cdot\widehat{u}$, we will estimate $f(0)$. For this, we use the following two ingredients:

$$|\widehat{u}(\chi_c)| \le \delta_{n-1} - |A|p^{-n} \quad \text{for every } c\in\mathbb{F}_p^n \tag{2}$$

$$\sum_{c\in\mathbb{F}_p^n}|\widehat{\mathbf{1}_A}(\chi_c)|^2 = \langle \mathbf{1}_A, \mathbf{1}_A\rangle = p^{-n}|A| \tag{3}$$

The first inequality follows from Lemma 2.2 since B has no proper 3-APs. The second inequality is Parseval's identity.

Here is our upper estimate of $f(0)$.

$$\begin{aligned}
f(0) &\le |f(0)| \\
&= \Big|\sum_{c\in\mathbb{F}_p^n}\widehat{f}(\chi_c)\Big| \\
&= \Big|\sum_{c\in\mathbb{F}_p^n}\widehat{\mathbf{1}_A}(\chi_c)^2\cdot\widehat{u}(\chi_c)\Big| \\
&\le \sum_{c\in\mathbb{F}_p^n}|\widehat{\mathbf{1}_A}(\chi_c)|^2\cdot|\widehat{u}(\chi_c)| \\
&\overset{(2)}{\le} \sum_{c\in\mathbb{F}_p^n}|\widehat{\mathbf{1}_A}(\chi_c)|^2\cdot(\delta_{n-1} - |A|p^{-n}) \\
&\overset{(3)}{=} p^{-n}|A|\cdot(\delta_{n-1} - |A|p^{-n}).
\end{aligned}$$

Combining this with (1) we get

$$p^{-2n}(\delta_{n-1}|A|^2 - |A|) \le p^{-n}|A|(\delta_{n-1} - |A|p^{-n})$$

and so

$$(\delta_{n-1}|A| - 1) \le (p^n\delta_{n-1} - |A|).$$

Rearranging terms concludes the proof. □

Proof of Theorem 2.1: The proof is by induction on n. The case $n = 1$ is clear.

It follows from Lemma 2.3 that
$$\frac{|A|}{p^n} \le \frac{\delta_{n-1} + p^{-n}}{1 + \delta_{n-1}} \le \frac{\delta_{n-1}}{1 + \delta_{n-1}} + p^{-n}.$$
By the induction hypothesis we have $\delta_{n-1} \le \frac{2}{n-1}$. Hence
$$\frac{\delta_{n-1}}{1 + \delta_{n-1}} \le \frac{2/(n-1)}{1 + 2/(n-1)} = \frac{2}{n+1}$$
Since $\frac{2}{n+1} + p^{-n} \le \frac{2}{n}$, the result follows. □

References

[Mes95] Roy Meshulam. On subsets of finite abelian groups with no 3-term arithmetic progressions. *Journal of Combinatorial Theory, Series A*, 71(1):168–172, 1995.

[Rot53] Klaus F Roth. On certain sets of integers. *Journal of the London Mathematical Society*, 1(1):104–109, 1953.