Discrete Fourier transform

If $f : \mathbb{F}_p^n \to \mathbb{C}$, then

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

where $\omega = e^{\frac{\tau i}{p}}$.

More generally, if $f : G \to \mathbb{C}$, then $\hat{f} : \hat{G} \to \mathbb{C}$ is defined by

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

Inversion formula for the discrete Fourier transform

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

Proof.

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

□

Ways to turn a set $A \subseteq \mathbb{F}_p^n$ into a function

- 1_A the *characteristic function* of A, ie
$$1_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$
Normalised in the ∞ norm.
- μ_A the *characteristic measure* of A, ie
$$\mu_A = \alpha^{-1} 1_A$$
where $\alpha = \frac{|A|}{|G|}$. Normalised in the L^1 norm.
- f_A the *balanced function* of A, ie
$$f_A(x) = 1_A(x) - \alpha$$
Normalised to have sum 0.

Fourier transform of $-A$

$$\widehat{1_{-A}} = \overline{1_A}$$

Proof.

$$\begin{aligned}
\widehat{1_{-A}}(t) &= \mathbb{E}_x 1_{-A}(x) \omega^{x \cdot t} \\
&= \mathbb{E}_x 1_A(-x) \omega^{x \cdot t} \\
&= \mathbb{E}_x 1_A(x) \omega^{-x \cdot t} \\
&= \overline{\widehat{1_A}(t)}
\end{aligned}$$

□

Fourier transform of a subspace

fourier-transform
fourier-analysis

dft-subspace

If $V \leq \mathbb{F}_p^n$, then

$$\widehat{\mu_V}(t) = 1_{V^\perp}(t)$$

Proof.

$$\widehat{1_V}(t) = \mathbb{E}_x 1_V(x)\omega^{x\cdot t} = \frac{|V|}{|G|} 1_{V^\perp}(t)$$

□

Fourier transform of a random set

fourier-transform
fourier-analysis

dft-random-set

Let $R \subseteq \mathbb{F}_p^n$ be such that each x is included with probability $\frac{1}{2}$ independently. Then with high probability

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

Proof. Chernoff □

Inner product, L^p norm

fourier-analysis

discrete-lp-norm-def

If $f, g : \mathbb{F}_p^n \to \mathbb{C}$, then

$$\langle f, g\rangle = \mathbb{E}_x f(x)\overline{g(x)}$$
$$\left\langle \hat{f}, \hat{g}\right\rangle = \sum_t \hat{f}(t)\overline{\hat{g}(t)}$$
$$\|f\|_p^p = \mathbb{E}_x |f(x)|^p$$
$$\left\|\hat{f}\right\|_p^p = \sum_t \left|\hat{f}(t)\right|^p$$

Plancherel and Parseval's identities

fourier-transform
fourier-analysis

discrete-plancherel-parseval

$$\langle f, g\rangle = \left\langle \hat{f}, \hat{g}\right\rangle \qquad \text{(Plancherel)}$$
$$\|f\|_2 = \left\|\hat{f}\right\|_2 \qquad \text{(Parseval)}$$

Proof.

$$\left\langle \hat{f}, \hat{g}\right\rangle = \sum_t \hat{f}(t)\overline{\hat{g}(t)} = \sum_{t,x,y} f(x)\overline{g(y)}\omega^{(x-y)\cdot t}$$
$$= \sum_{x,y} f(x)\overline{g(y)}1_{x=y} = \langle f, g\rangle$$

□

Large spectrum

large-spectrum
fourier-analysis

large-spectrum-def

The ρ-large spectrum of f is

$$\mathrm{Spec}_\rho(f) = \{t \mid |\hat{f}(t)| \geq \rho \|f\|_1\}$$

Large spectrum of a subspace

large-spectrum
fourier-analysis

large-spectrum-subspace

If $V \leq \mathbb{F}_p^n$ and $\rho > 0$, then

$$\mathrm{Spec}_\rho(1_V) = V^\perp$$

Upper bound on the size of the large spectrum

large-spectrum
fourier-analysis

card-large-spectrum-le

For all $\rho > 0$,

$$\left|\mathrm{Spec}_\rho(f)\right| \leq \rho^{-2} \frac{\|f\|_2^2}{\|f\|_1^2}$$

Proof.

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

□

Convolution of functions

convolution
fourier-analysis

convolution-def

Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$, their convolution $f * g : \mathbb{F}_p^n \to \mathbb{C}$ is given by

$$(f * g)(x) = \mathbb{E}_y f(y) g(x - y)$$

Meaning of $1_A * 1_B$

convolution
fourier-analysis

convolution-indicators

$$\begin{aligned}(1_A * 1_B)(x) &= \mathbb{E}_y 1_A(y) 1_B(x-y)\\ &= \frac{1}{p^n}\left|A \cap (x-B)\right|\\ &= \frac{\#\text{ ways to write } x = a+b, a \in A, b \in B}{p^n}\end{aligned}$$

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

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

Relationship between convolution and Fourier transform

convolution, fourier-transform
fourier-analysis

dft-convolution

Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$,

$$\widehat{f * g}(t) = \hat{f}(t)\hat{g}(t)$$

Proof.

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

□

Meaning of the L^4 norm of the Fourier transform

fourier-transform
fourier-analysis

l4-norm-fourier-transform

$$\left\|\hat{f}\right\|_4^4 = \mathbb{E}_{x+y=z+w} f(x) f(y) \overline{f(z) f(w)}$$

Proof.

$$\begin{aligned}\left\|\hat{f}\right\|_4^4 = \left\|\hat{f}^2\right\|_2^2 = \left\|\widehat{f * f}\right\|_2^2 &= \|f * f\|_2^2\\ &= \mathbb{E}_a (f * f)(a)\overline{(f * f)(a)}\\ &= \mathbb{E}_{a,x,y,z,w} f(x) f(y) 1_{x+y=a} \overline{f(z) f(w) 1_{z+w=a}}\\ &= \mathbb{E}_{x+y=z+w} f(x) f(y) \overline{f(z) f(w)}\end{aligned}$$

□

Bogolyubov's lemma

finite-field-model
fourier-analysis

bogolyubov

If $A \subseteq \mathbb{F}_p^n$ has density $\alpha > 0$, then there exists a subspace V of codimension at most $2\alpha^{-2}$ such that $V \subseteq (A + A) - (A + A)$.

Proof. Write $(A+A)-(A+A) = \operatorname{supp}(\underbrace{1_A * 1_A * 1_{-A} * 1_{-A}}_{g})$, set $K = \operatorname{Spec}_\rho(1_A)$ for $\rho = \sqrt{\frac{\alpha}{2}} > 0$ and define $V = \langle K \rangle^\perp$. We have $\operatorname{codim} V \leq |K| \leq \rho^{-2}\alpha^{-1} = 2\alpha^{-2}$ and

$$g(x) = \alpha^4 + \underbrace{\sum_{t \in K\setminus\{0\}} \left|\widehat{1_A}(t)\right|^4 \omega^{-x\cdot t}}_{(1)} + \underbrace{\sum_{t \notin K} \left|\widehat{1_A}(t)\right|^4 \omega^{-x\cdot t}}_{(2)}$$

Now prove $(1) \geq 0$ and $|(2)| \leq \rho^2\alpha^3 = \frac{\alpha^4}{2}$ so that $g(x) > 0$ whenever $x \in V$. □

Example of a set such that $A + A$ does not contain any subspace of bounded codimension

fourier-analysis

sumset-no-subspace, finite-field-model

The set $A = \{x \in \mathbb{F}_2^n \mid |x| \geq \frac{n}{2} + \frac{\sqrt{n}}{2}\}$ has density at least $\frac{1}{4}$ but there is no coset C of any subspace of codimension $\sqrt{n}$ such that $C \subseteq A + A$.

Density increment in $\mathbb{F}_p^n$

large-spectrum, finite-field-model
fourier-analysis

density-increment-ff

Let $A \subseteq \mathbb{F}_p^n$ of density α. If $t \neq 0$ is in $\mathrm{Spec}_\rho(1_A)$, then there exists x such that

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

where $V = \langle t \rangle^\perp$.

Proof. For $j = 1, \ldots, p$, write $v_j + V$ the cosets of V, $a_j = \frac{|A \cap (v_j + V)|}{|V|} - \alpha$ the density increment within each V_j. Calculate $\sum_j a_j = 0$ and $\widehat{1_A}(t) = \mathbb{E}_j a_j \omega^j$, so that

$$\rho\alpha \leq \left|\widehat{1_A}(t)\right| \leq \mathbb{E}_j |a_j| = \mathbb{E}_j(|a_j| + a_j)$$

and find j such that $|a_j| + a_j \geq \rho\alpha$. Take $x = v_j$. □

Definition of T_3

convolution
fourier-analysis

t3-def

If $f, g, h : \mathbb{F}_p^n \to \mathbb{C}$, then

$$T_3(f, g, h) = \mathbb{E}_x f(x) g(x + d) h(x + 2d) = \langle f * h, \overline{g} \rangle$$

Number of 3APs in a uniform set $A \subseteq \mathbb{F}_p^n$

3AP, finite-field-model
fourier-analysis

3AP-uniform

Let $\alpha > 0$ be the density of A and assume $\sup_{t \neq 0} \left|\widehat{1_A}(t)\right| = o(1)$. Then A contains $(\alpha^3 + o(1)) |G|^2$ 3APs.

Proof. The number of 3APs (including the trivial ones of the form a, a, a) in A is $|G|^2$ times

$$\begin{aligned} T_3(1_A, 1_A, 1_A) &= \langle 1_A * 1_A, 1_{2 \cdot A} \rangle = \left\langle \widehat{1_A}^2, \widehat{1_{2 \cdot A}} \right\rangle \\ &= \alpha^3 + \sum_{t \neq 0} \widehat{1_A}(t)^2 \overline{\widehat{1_{2 \cdot A}}(t)} \text{ by Plancherel} \end{aligned}$$

In absolute value, the error term is at most

$$\sup_{t \neq 0} \left|\widehat{1_{2 \cdot A}}(t)\right| \sum_t \left|\widehat{1_A}(t)\right|^2 = \alpha \sup_{t \neq 0} \left|\widehat{1_A}(t)\right|$$

□

Meshulam's theorem

3AP
fourier-analysis
meshulam, finite-field-model

IF $p \geq 3$ and $A \subseteq \mathbb{F}_p^n$ only contains trivial 3APs, then the density of A is $O(n^{-1})$.

Proof. By assumption, $T_3(1_A, 1_A, 1_A) = \frac{\alpha}{p^n}$. But

$$\left|T_3(1_A, 1_A, 1_A) - \alpha^3\right| \leq \alpha \sup_{t \neq 0} \left|\widehat{1_A}(t)\right|$$

Hence, provided that $2\alpha^{-2} \leq p^n$, we find a subspace $V \leq \mathbb{F}_p^n$ of codimension 1 and $x \in \mathbb{F}_p^n$ such that

$$|A \cap (x + V)| \geq \alpha \left(1 + \frac{\alpha^2}{4}\right) |V|$$

Iteratively increase α like this until $2\alpha^{-2} \leq p^n$. Since $\alpha \leq 1$, this takes at most $9\alpha^{-1}$ steps. So $p^{n-9\alpha^{-1}} \leq 2\alpha^{-2}$ which implies $\alpha \leq \frac{18}{n}$, as wanted. $\square$

Characters, dual group

character
fourier-analysis
character-def

Characters of the group G are group homomorphisms $\gamma : G \to \mathbb{C}^\times$. They form a group called the Pontryagin dual or dual group of G.

Duals of $\mathbb{F}_p^n, \mathbb{Z}/n\mathbb{Z}$

character
fourier-analysis
dual-ff

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

Fourier transform of an interval in $\mathbb{Z}/p\mathbb{Z}$

fourier-transform, integer-model
fourier-analysis
dft-interval

Let p be a prime, $L < p$ be even and $J = [-\frac{L}{2}, \frac{L}{2}] \subseteq \mathbb{Z}/p\mathbb{Z}$. Then for all $t \neq 0$ we have

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

Density increment for 3APs in an interval

3AP, integer-model
fourier-analysis

density-increment-int

Let $A \subseteq [N]$ be of density $\alpha > 0$ with $N > 50\alpha^{-2}$ and containing only trivial 3APs. Let p be a prime in $[\frac{N}{3}, \frac{2N}{3}]$ and write $A' = A \cap [p] \subseteq \mathbb{Z}/p\mathbb{Z}$. Then either

1. $\sup_{t \neq 0} \left| \widehat{1_A}(t) \right| \geq \frac{\alpha^2}{10}$
2. or there exists an interval J of length $\geq \frac{N}{3}$ such that

$$|A \cap J| \geq \alpha \left(1 + \frac{\alpha}{400}\right) |J|$$

Proof. There's no non-trivial 3AP with terms in A', A'', A'' where A'' is the middle third of A'. If A' and A'' are both dense enough, then we're in Case 1 by computing $T_3(1_{A'}, 1_{A''}, 1_{A''})$. Else we're in Case 2 by looking at the appropriate complement. □

Roth's theorem

3AP
fourier-analysis

roth

Let $A \subseteq [N]$ be a set containing only trivial 3APs. Then $|A| = O(\frac{N}{\log \log N})$.

Proof. Iterate the density increment. □