Discrete Fourier transform

fourier-transform
fourier-analysis

dft-def

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

fourier-transform
fourier-analysis

dft-inversion

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

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

fourier-analysis

indicator-mu-balance-def

- 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 $-A$

fourier-transform
fourier-analysis

dft-neg

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

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 $V \le \mathbb{F}_p^n$, 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

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

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 $\rho > 0$,

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

Proof.

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

□

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

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

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 in $\mathbb{F}_p^n$

finite-field-model
fourier-analysis

bogolyubov-ff

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 $\operatorname{codim} V \le |K| \le \rho^{-2}\alpha^{-1} = 2\alpha^{-2}$ 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 $(1) \ge 0$ and $|(2)| \le \rho^2 \alpha^3 = \frac{\alpha^4}{2}$ so that $g(x) > 0$ whenever $x \in V$. □

Example of a set $A \subseteq \mathbb{F}_2^n$ of fixed density 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 $j = 1, \dots, p$, 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

$$T_3(f,g,h) = \mathbb{E}_x f(x) g(x+d) h(x+2d) = \left\langle f * h, \overline{g}(2^{-1} \cdot) \right\rangle$$

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

3AP finite-field-model
fourier-analysis

3AP-uniform

If $\sup_{t\neq 0} \left|\widehat{1_A}(t)\right| = o(1)$, then A contains $(\alpha^3 + o(1))|G|^2$ 3APs.

Proof. The number of 3APs 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. □

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

Write $J = [-\frac{L}{2}, \frac{L}{2}] \subseteq \mathbb{Z}/p\mathbb{Z}$ with $L < p$ even. For all t,

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

Proof. If $t = 0$, then $\widehat{1_J}(t) = \frac{|J|}{p} = \frac{L+1}{p}$. If $t \neq 0$, then

$$\widehat{1_J}(t) = \mathbb{E}_x 1_J(x)\omega^{xt} = \mathbb{E}_{x=-\frac{L}{2}}^{\frac{L}{2}} \omega^{xt} = \frac{\omega^{(L+1)\frac{t}{2}} - \omega^{-(L+1)\frac{t}{2}}}{p(\omega^{\frac{t}{2}} - \omega^{-\frac{t}{2}})}$$

Noting that for all $x \in [-\pi, \pi]$ we have $\left|e^{ix} - 1\right| \geq \frac{2|x|}{\pi}$,

$$\left|\widehat{1_J}(t)\right| \leq \frac{2}{p}\left|\omega^t - 1\right|^{-1} \leq \frac{2}{p}\left(\frac{2}{\pi}\frac{2\pi t}{p}\right)^{-1} = \frac{1}{2|t|}$$

□

Density increment or large Fourier coefficient for 3APs in an interval

3AP integer-model
fourier-analysis
large-fourier-coeff-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. □

For $t \neq 0, \varepsilon > 0$ and $\phi : [m] \to \mathbb{Z}/p\mathbb{Z}$ multiplication by t, how to partition $[m]$ into progressions of length roughly $\varepsilon\sqrt{m}$ such that $\operatorname{diam}(t \cdot P_i) \leq \varepsilon p$?

integer-model
fourier-analysis
partition-progressions-small-diam

Let $u = \lfloor \sqrt{m} \rfloor$ and consider $0, t, \ldots, ut$. By pigeonhole, find $0 \leq v < w \leq u$ such that $|wt - vt| \leq \frac{p}{u}$. Set $s = w - v \leq u$ so that $|st| \leq \frac{p}{u}$. Divide $[m]$ into residue classes mod s. Each has size at least $\lfloor \frac{m}{s} \rfloor \geq \lfloor \frac{m}{u} \rfloor$ and can be divided into progressions of the form $a, a+s, \ldots, a+ds$ with $\frac{\varepsilon u}{2} < d \leq \varepsilon u$. The diameter of each progression under ϕ is $|dst| \leq \varepsilon p$.

Density increment from a large Fourier coefficient for 3APs in an interval

3AP integer-model
fourier-analysis
density-increment-int

Let $A \subseteq [N]$ be of density $\alpha > 0$. Let p be a prime in $[\frac{N}{3}, \frac{2N}{3}]$ and write $A' = A \cap [p]$. Suppose there 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 $\alpha^2 \frac{\sqrt{N}}{500}$ such that

$$|A \cap P| \geq \alpha \left(1 + \frac{\alpha}{50}\right) |P|$$

Proof. Let $\varepsilon = \frac{\alpha^2}{40\pi}$ and partition $[p]$ into progressions P_i of length at least $\frac{\varepsilon\sqrt{p}}{2} \geq \frac{\alpha^2\sqrt{N}}{500}$ and $\operatorname{diam} \phi(P_i) \leq \varepsilon p$. Fix one x_i inside each P_i. Write $\left|\widehat{f_{A'}}(t)\right| = \frac{1}{p} \left|\sum_i \sum_{x \in P_i} f_{A'}(x)\omega^{xt}\right|$ and use the fact that $\omega^{xt} \approx \omega^{x_i t}$ whenever $x \in P_i$ to find some i such that $\sum_{x \in P_i} f_{A'}(x) \geq \frac{\alpha^2|P_i|}{40}$. □

Roth's theorem

3AP integer-model
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. □

Behrend's construction

3AP integer-model
fourier-analysis

behrend

There exists a set $A \subseteq [N]$ containing non nontrivial 3APs of size at least $e^{-O(\sqrt{\log n})}$. See Example Sheet 1.

Bohr set

bohr-set
fourier-analysis

bohr-set-def

Let $\Gamma \subseteq \hat{G}$. The Bohr set of frequencies Γ and width ρ is

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

$|\Gamma|$ is the rank of the Bohr set.

Bohr set in $\mathbb{F}_p^n$

bohr-set finite-field-model
fourier-analysis

bohr-set-ff

When $G = \mathbb{F}_p^n$, $B(\Gamma, \rho) = \langle \Gamma \rangle^\perp$ for all small enough ρ (depending only on p, not n).

Lower bound on the size of a Bohr set

bohr-set
fourier-analysis

bohr-set-card-ge

If B is a Bohr set of rank d and width ρ, then $|B| \geq \left(\frac{\rho}{2\pi}\right)^d |G|$.

Bogolyubov's lemma in $\mathbb{Z}/p\mathbb{Z}$

bohr-set
fourier-analysis

bogolyubov-int

If $A \subseteq \mathbb{Z}/p\mathbb{Z}$ has density $\alpha > 0$, then there exists $\Gamma \subseteq \widehat{\mathbb{Z}/p\mathbb{Z}}$ of size at most $2\alpha^{-2}$ such that $B(\Gamma, \frac{1}{2}) \subseteq (A+A)-(A+A)$.

Proof. Pick $\Gamma = \operatorname{Spec}_{\sqrt{\frac{\alpha}{2}}}(1_A)$ and lower bound

$$\operatorname{Re}(1_A * 1_A * 1_{-A} * 1_{-A})(x) = \operatorname{Re} \sum_{t \in \widehat{\mathbb{F}_p}} \left|\widehat{1_A}(t)\right|^4 \omega^{-xt}$$

by splitting the sum over Γ and Γ^c. $\square$

Doubling constant, difference constant

doubling-constant
combinatorial-methods

doubling-constant-def

For a finite nonempty set $A \subseteq G$, its doubling and difference constants are

$$\sigma(A) = \frac{|A+A|}{|A|}, \delta(A) = \frac{|A-A|}{|A|}$$

When is the doubling constant 1?

doubling-constant
combinatorial-methods

doubling-constant-one

When the set is a subspace

If A has Small doubling constant then A lies in a small coset.

doubling-constant
combinatorial-methods

doubling-constant-lt-three-halves

If A is such that $|A+A| < \frac{3}{2}|A|$. Then there exists $V \leq \mathbb{F}_p^n$ such that A is contained in a coset of V and $|V| < \frac{3}{2}|A|$.

Example of a set with big doubling

doubling-constant
combinatorial-methods

big-doubling-random

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

Ruzsa distance

ruzsa-distance
combinatorial-methods

ruzsa-distance-def

Given finite sets $A, B \subseteq G$, we define the Ruzsa distance between A and B to be

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

Ruzsa's triangle inequality

ruzsa-distance
combinatorial-methods

ruzsa-triangle-inequality

For $A, B, C \subseteq G$ finite,

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

Proof. The inequality reduces to

$$|B|\,|A - C| \leq |A - B|\,|B - C|$$

This is true because

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

is injective, where for each $d \in A - C$ we have chosen $a_d \in A, c_d \in C$ such that $d = a - c$. $\square$

Plünnecke's inequality

doubling-constant
combinatorial-methods

pluennecke-inequality

Let $A, B \subseteq G$ be finite such that $|A + B| \leq K\,|A|$. Then for all ℓ, m,

$$|\ell B - mB| \leq K^{\ell+m}\,|B|$$

Proof. WLOG $|A + B| = K\,|A|$. Find $A' \subseteq A$ nonempty minimising $K' = \frac{|A'+B|}{|A'|}$.

Claim. For all finite $C \subseteq G$, $|A' + B + C| \leq K'\,|A' + C|$

From the claim, prove that $|A' + mB| \leq K'^m\,|A'|$ for all m by induction. Now, by the triangle inequality,

$$|A'|\,|\ell B - mB| \leq |A' + \ell B|\,|A' + mB| \leq K'^\ell\,|A'|\,K'^m\,|A'|$$

Namely, $|\ell B - mB| \leq K'^{\ell+m}\,|A'| \leq K^{\ell+m}\,|A|$. $\square$

Key claim within the proof of Plünnecke's inequality

combinatorial-methods

pluennecke-inequality-claim

WLOG $|A+B| = K|A|$. $A' \subseteq A$ is nonempty minimising $K' = \frac{|A'+B|}{|A'|}$.

Claim. For all finite $C \subseteq G$, $|A'+B+C| \leq K' |A'+C|$

Proof of claim. Induct on C. obvious if $C = \varnothing$. For $C' = C \cup \{x\}, x \notin C$, write

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

where $D = \{a \in A' \mid a + B + x \subseteq A' + B + C\}, E = \{a \in A' \mid a + x \in A' + C\} \subseteq D$. Note that the second union is disjoint. Use the induction hypothesis and the minimality assumption for K' to deduce the claim. □

Relationship between the doubling and difference constant

doubling-constant
combinatorial-methods

doubling-difference-constants-relation

If $|A-A| \leq K|A|$, then

$$|A||A+A| \leq |A-A||A-A| \leq K^2 |A|^2$$

by Ruzsa's triangle inequality. So $\sigma(A) \leq \delta(A)^2$.

If $|A+A| \leq K|A|$, then

$$|A-A| \leq K^{1+1}|A|$$

by Plünnecke's inequality. So $\delta(A) \leq \sigma(A)^2$.

The Freiman-Ruzsa theorem

combinatorial-methods

freiman-ruzsa

Let $A \subseteq \mathbb{F}_p^n$ be such that $|A+A| \leq K|A|$ for some $K > 0$. Then A is contained in a subspace $H \leq \mathbb{F}_p^n$ of size $|H| \leq K^2 p^{K^4} |A|$.

Proof. Write $S = A - A$ and choose $X \subseteq A + S$ maximal such that the translates $x + A$ for $x \in X$ are disjoint. Use that $X + A \subseteq 2A + S$ to prove $|X| \leq K^4$ by Plünnecke. Now $A + S \subseteq X + S$ because $y \in A + S$ is either in $X \subseteq X + S$ or $x + A$ and $y + A$ are not disjoint by maximality of X, namely $y \in x + A - A \subseteq X + S$. By induction, $\ell A + S \subseteq X + S$ for all ℓ. Hence, the subgroup generated by A is contained in $\langle X \rangle + S$ and size at most

$$|\langle X \rangle| |S| \leq p^{|X|} K^2 |A| \leq K^2 p^{K^4} |A|$$

□

Example of a set which generates a subgroup of size exponential in its doubling constant

doubling-constant
combinatorial-methods

subgroup-exponential-size-doubling-constant

Let $A = H \cup R \subseteq \mathbb{F}_p^n$ where H is a subspace of dimension $K \ll d \ll n - k$ and R consists of $K - 1$ linearly independent vectors in $H^\perp$. Then $|A| = |H \cup R| \sim |H|$ and $|A + A| = |H \cup H + R \cup R + R| \sim K|H| \sim K|A|$ but any subspace $V \leq \mathbb{F}_p^n$ containing A must have size $\geq p^{d+(K-1)} = p^{K-1}|H| \sim p^{K-1}|A|$ where the constant is exponential in K.

Polynomial Freiman-Ruzsa conjecture

combinatorial-methods polynomial-freiman-ruzsa

Let $A \subseteq \mathbb{F}_p^n$ be such that $|A+A| \leq K|A|$. Then there is a subspace $H \leq \mathbb{F}_p^n$ of size at most $C_1(K)|A|$ and $x \in \mathbb{F}_p^n$ such that $|A \cap (x+H)| \geq \frac{|A|}{C_2(K)}$ where $C_1(K)$ and $C_2(K)$ are polynomials.

Additive energy

additive-energy
combinatorial-methods additive-energy-def

Given an abelian group G and finite sets $A, B \subseteq G$, define additive quadruples to be the tuples $(a, a', b, b') \in A^2 \times B^2$ such that $a + b = a' + b'$ and the additive energy between A and B to be

$$E(A, B) = \frac{\#\{\text{additive quadruples}\}}{|A|^{\frac{3}{2}} |B|^{\frac{3}{2}}}$$

Relation between the additive energy and the Fourier transform

additive-energy fourier-transform
combinatorial-methods additive-energy-fourier-transform

If G is finite and $A \subseteq G$, then

$$\begin{aligned} |A|^3 E(A) &= |G|^3 \mathbb{E}_{x+y=z+w} 1_A(x) 1_A(y) 1_A(z) 1_A(w) \\ &= |G|^3 \left\| \widehat{1_A} \right\|_4^4 \end{aligned}$$

namely

$$\left\| \widehat{1_A} \right\|_4^4 = \alpha^3 E(A)$$

Additive energy of a subgroup

additive-energy
combinatorial-methods additive-energy-subgroup

When $H \leq G$, we have $E(H) = 1$.

Small doubling implies big energy

doubling-constant additive-energy
combinatorial-methods small-doubling-constant-implies-big-additive-energy

Let G be abelian and $A, B \subseteq G$ be finite. Then $E(A,B) \geq \frac{\sqrt{|A||B|}}{|A \pm B|}$. In particular, if $|A \pm A| \leq K|A|$ then $E(A) \geq \frac{1}{K}$.

Proof. Write $r(x) = \#\{(a,b) \in A \times B \mid a+b=x\}$ so that

$$|A|^{\frac{3}{2}} |B|^{\frac{3}{2}} E(A,B) = \#\{\text{additive quadruples}\} = \sum_x r(x)^2$$

Also note that $\sum_x r(x) = |A||B|$ so that

$$\begin{aligned} |A|^{\frac{3}{2}} |B|^{\frac{3}{2}} E(A,B) &= \sum_x r(x)^2 \\ &\geq \frac{\sum_x r(x) 1_{A+B}(x)}{\sum_x 1_{A+B}(x)^2} = \frac{(|A||B|)^2}{|A+B|} \end{aligned}$$

by Cauchy-Schwarz. Do similarly for $A - B$. □

Big energy does not imply small doubling

doubling-constant additive-energy
combinatorial-methods big-additive-energy-not-implies-small-doubling-constant

Let G be your favorite family of abelian groups. Then there are constants $\eta, \theta > 0$ such that for all sufficiently large n there exists $A \subseteq G$ with $|A| = n$ satisfying $E(A) \gg \eta$ and $|A+A| \geq \theta |A|^2$.

Balog-Szemerédi-Gowers

additive-energy
combinatorial-methods balog-szemeredi-gowers

Let G be an abelian group and let $A \subseteq G$ be finite such that $E(A) \geq \eta$ for some $\eta > 0$. Then there exists $A' \subseteq A$ of size at least $c(\eta)$ such that $|A' + A'| \leq C(\eta)|A|$ where $c(\eta)$ and $C(\eta)$ are polynomials in η.

Dependent random choice step within the proof of Balog-Szemerédi-Gowers

combinatorial-methods balog-szemeredi-gowers-dependent-random-choice

Let $A_1, \ldots, A_m \subseteq [n]$ and suppose that $\mathbb{E}_{i,j} |A_i \cap A_j| \geq \delta^2 n$. Then there exists $X \subseteq [m]$ 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. Let $x_1, \ldots, x_5$ be uniform random in $[n]$ and let $X = \{i \in [m] \mid \forall k, x_k \in A_i\}$. Call a pair **bad** if $|A_i \cap A_j| < \frac{\delta^2 n}{2}$. Prove that

$$\frac{\delta^{10} m^2}{2} + 16\mathbb{E}[\#\{\text{bad pairs in } X^2\}] \leq \mathbb{E}[|X|^2]$$

so that $\frac{\delta^{10} m^2}{2} + 16\#\{\text{bad pairs in } X^2\} \leq |X|^2$ for some $x_1, \ldots, x_5$. This gives $|X| \geq \frac{\delta^5 m}{\sqrt{2}}$ and $\#\{\text{bad pairs in } X^2\} \leq \frac{|X|^2}{16} \leq 10\% |X|^2$ □