Exponential sums, Sidon sets, and tannakian categories

Balufest, 16.3.2021
(70 years + 1 day)

Joint work in progress with A. Forey and J. Fresán

ICTP Trieste, 24.4.2007

Exponential sums

Sidon sets

Tannahian categories

} common link : equidistribution

Exponential sums : (families) exp. sums over finite fields

ex. $\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} e\left(\frac{ax+\bar{x}}{p}\right)$, $\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \chi(x^3+x+1)$

parameter $a \in \mathbb{F}_p$

$\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$

$$\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \chi(x)\, e\left(\frac{ax+\bar{x}}{p}\right)$$

two parameters

Replace par. by the corresponding ones over $\mathbb{F}_{p^n}$, let $n \to \infty$; Q. distribution?

[Variant: $p \to \infty$]

Sidon sets :

Def. (Sidon ; 1931)

A abelian group ; $S \subset A$ is called a Sidon set if with $x_i \in S$ implies $x_1 + x_2 = x_3 + x_4$ $x_1 \in \{x_3, x_4\}$.

Ex. (1) $2^{\mathbb{N}} \subset \mathbb{Z}$

(2) Ruzsa (Spence): K field

$$\Delta = \{ (x, x) \in K^* \times K \}$$

In $\mathbb{F}_p$, $p-1$ elements in $p(p-1)$ a group

(3) [Ellenberg - Venkatesh $\rightsquigarrow$ Green $\rightsquigarrow$ Eberhard - Manners]

$D < 0$ fund. disc.

$A = H(\mathbb{Q}(\sqrt{-D}))$ ideal class group

$|A| \simeq |D|^{1/2}$

$$S = \{ [\mathfrak{p}] \mid \mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-D})}, N\mathfrak{p} < |D|^{1/4} \}$$

is a Sidon set.

Tannakian categories: this is just a way to describe a groups G (by looking at "all linear actions of G on vector spaces over $\mathbb{C}$").

Useful "def" because sometimes we can construct groups this way.

Equidistribution of exp. sums

Deligne (~1980)

"Any family of exp. sums parameterized by $\mathbb{F}_{p^n}^d$ satisfies as $n \to \infty$ some equidistribution theorem"

More precisely: Deligne constructs two groups $G^{geo} \lhd G^{ari} \subset GL_r$ [sums $r \geq 0$]

and (if $G^{geo} = G^{ari}$) a compact group $K \subset G^{ari}$

s.t. the exp. sums, as $n \to \infty$, become distributed like $Tr(g)$, g random element in K.

Ex. (Katz; 1988)

$$\frac{1}{\sqrt{p^n}} \sum_{x \in \mathbb{F}_{p^n}} e\left(\frac{Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}\left(ax + \overline{x}\right)}{p} \right), \quad a \in \mathbb{F}_{p^n}^\times$$

($\overline{x}$: inverse in $\mathbb{F}_{p^n}$)

become equidistributed (like trace of g) in $K = SU_2(\mathbb{C})$

$\Rightarrow$ measure = Sato–Tate measure

$$\frac{1}{\pi}\sqrt{1 - \frac{x^2}{4}}\, dx \text{ on } [-2, 2]$$

Here the two groups are "not mysterious": they are defined as images of morphisms

some kind of Galois group $\pi_1 \longrightarrow GL_r$

Katz (2003 → 2011)

Families parameterized by $\chi : \mathbb{F}_{p^n}^\times \longrightarrow \mathbb{C}^\times$

These are <u>not</u> of the type treated by Deligne.

But numerical experiments indicate that there should be a similar equid. theorem!

Ex. (Evans) $\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \chi(x)\, e\left(\frac{x - \bar{x}}{p}\right)$

real number

These seem to be Sato – Tate – distributed (as $n \to \infty$).

Th. (Katz) [for families param. by $\chi : \mathbb{F}_{p^n}^\times \to \mathbb{C}^\times$]

Something like Deligne holds: there are two groups $G^{geo} \lhd G^{ari} \subset GL_r$ and if they are equal there is equid. like

L $\mathrm{Tr}(g)$, $g \in K \subset G^{ari}$ maximal compact.

Ex. (Evans) $G^{geo} = G^{ari} = SL_2 \subset GL_2$

$\longrightarrow$ measure is Sato–Tate

Now the groups are constructed using Tannakian categories (proof of equid. also relies on Deligne's Riemann Hypothesis).

(Why? Linear actions of $G \rightleftarrows$ traces as functions on $G \longrightarrow$ these can be multiplied; and this is crucial to reconstruct G

Katz observed:

$$\left(\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p^\times} \chi(x)\, t(x)\right) \times \left(\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p^\times} \chi(x)\, s(x)\right)$$

$$= \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p^\times} \chi(x)\, (t * s)(x)$$

convolution

$\longrightarrow$ reflects multiplication of traces of linear actions of G^{ari}.

Question: what about exp. sums parameterized by **characters** of

$\mathbb{F}_p^\times \times \mathbb{F}_p$? $\quad \frac{1}{\sqrt{p}} \sum_x \chi(x)\, e\left(\frac{ax+\bar{x}}{p}\right)$.

$\mathbb{F}_p^\times \times \dots \times \mathbb{F}_p^\times$? $\quad \left[\frac{1}{p^{d/2}} \sum \chi_1(x_1) \cdots \chi_d(x_d) \cdot e\left(\frac{f(x_1,\dots,x_d)}{p}\right) \right]$

abelian varieties / $\mathbb{F}_p$

Motivations: (1) natural question!

(2) $\mathbb{F}_p^\times \times \dots \times \mathbb{F}_p^\times$

has applications to e.g. variance of arithmetic functions in arith. progressions in $\mathbb{F}_p[t]$

[Hall - Keating - Roddity - Gershon]

Th. (Forey – Fresán - K., 2021)

For such situations there exist $r \geq 1$ and groups $G^{geo} \lhd G^{ari} \subset GL_r$ s.t. for $K \subset G^{ari}$ maximal compact, the sums: $S(M,\chi) = \sum_{x \in G(\mathbb{F}_{p^n})} \overline{\chi}(x)\, t_M(x)$

- $t_M(x)$ — trace function
- x — parameters, eg $(x_1,\dots,x_d)$
- $G(\mathbb{F}_{p^n})$ — group, eg $\mathbb{G}_m^d$

are equi. on average like $\mathrm{Tr}(g)$, g in K random:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} \frac{1}{|G(\mathbb{F}_{p^n})|} \sum_{\chi} f\big(S(M,\chi)\big) \to \int_K f(\mathrm{Tr}\, g)\, dg$$

for any continuous bounded $f: \mathbb{C} \to \mathbb{C}$.

Construction of G^{ari}: by Tannakian formalism using convolution.

Application:

$$\frac{1}{\sqrt{p}} \sum_{x\in\mathbb{F}_p} \chi(x)\, e\left(\frac{ax}{p}\right) \overline{f(x)}$$

$e\left(\frac{f(x)}{p}\right)$

parameters

We know there is equidistribution.

What is K?

One tool is:

Th. (Larsen)

If $K \subset U_n(\mathbb{C})$, $n \ge 2$, satisfies $\int_K |\mathrm{Tr}\, g|^4\, dg = 2$

Then either K is finite, or $K \supset SU_n(\mathbb{C})$.

We can use that because

$$\frac{1}{p(p-1)} \sum_a \sum_\chi |S|^4$$

$$= \frac{1}{p^2 p(p-1)} \sum_{x_1,x_2,x_3,x_4} \cdots \overline{\hat{f}(x_4)}$$

$$\sum_a \sum_\chi \chi\left(\frac{x_1 x_2}{x_3 x_4}\right) e\left(\frac{x_1+x_2-x_3-x_4}{p}\right)$$

$$= \frac{1}{p^2} \sum_{\substack{x_1 x_2 = x_3 x_4 \\ x_1 + x_2 = x_3 + x_4}} \hat{f}(x_1) \cdots \overline{\hat{f}(x_4)}$$

diagonal Sidon set!

$$\leq 2\left(\frac{1}{p}\sum_\chi |\hat{f}(\chi)|^2\right)^2$$

In many cases, this converges to 2!

So K is either finite or $\supset SU_1(\mathbb{C})$.