

Exponential sums in  
many variables  
over finite fields

1 - Context

We are interested in sums of the type

$$S(f) = \sum_{x \in \mathbb{F}_q^n} \psi(f(x))$$

$$\text{or } \sum_{x \in \mathbb{F}_q^n} \chi(g(x)) \psi(f(x)) = T(f, g, \chi, \psi)$$

$$\left[ \text{or } \sum_{x \in \mathbb{F}_q^n} t(x) \right]$$

where :

$\mathbb{F}_q$  is a finite field

$f \in \mathbb{F}_q[x_1, \dots, x_n]$

$g \in \mathbb{F}_q[x_1, \dots, x_n]$

$\psi$  is an additive character  $\neq 1$  of  $\mathbb{F}_q$

$\chi$  is a (mult.) character of  $\mathbb{F}_q^\times$

$t$  is a trace function of some sheaf / complex of wt  $\leq 0$

These appear in various contexts in number theory (and other fields ...):

- circle method
- automorphic forms
- mult. number theory (eg gaps between primes, ...)

In most cases, the main question concerns upper bounds: if (say)  $f$  is "not constant" in  $S(f)$ , we want to show that

where  $\delta > 0$ , "beating"  ~~$|k|^{n-1}$~~   $|k|^{n-\delta}$  substantially the trivial bound  $|k|^n$ .

In fact, on probabilistic grounds, one expects that in many cases we should have  $|S(f)| \leq C |k|^{n/2}$ : the sum is of size bounded by the square-root of the number of terms; and in many problems it is this which is required.

(E.g. note that

$$\frac{1}{p^{d+1}} \sum_{\deg f \leq d} |S(f)|^2 = p$$

Ex. (1)  $S = \sum_{x \text{ mod } p} e^{2i\pi x^2/p}$   $\rightarrow$  quadratic Gauss sum  $|S| = \sqrt{p}$

(2)  $S = \sum_{x \text{ mod } p} e^{2i\pi \frac{x^3+ax}{p}}$   $\rightarrow |S| \leq 2\sqrt{p}$  (Weil; Birch)

and  ~~$S$~~   $S$  is a real number in  $[-2, 2]$  which has a "regular" (non-uniform) distribution if we allow  $a$  to vary.

(general)

The "structural" properties of exponential sums is given by the fundamental results of Grothendieck and his school, and especially by Deligne's Riemann Hypothesis over finite fields: we can always write

$$S(f) = \sum_{j=0}^{2n} (-1)^j \sum_{1 \leq k \leq b_j} \alpha_{j,k}$$

(and similarly for other types of sums) where

$b_j \geq 0$  are integers ("Betti numbers") depending on the sum (i.e.  $f, g, X, \dots$ )

(Trace formula)

$\Rightarrow$

$\alpha_{j,k}$  is an algebraic number s.t.  $|\alpha_{j,k}| = |k|^{w_{j,k}/2}$

with  $w_{j,k} \leq j$ .

(Riemann Hypothesis)

It follows formally that

$$|S(f)| \leq C |k|^{r/2}$$

with

$$\begin{cases} C = \sum_{j=0}^{2n} b_j, \\ r = \max \{ j \mid b_j \neq 0 \} \end{cases}$$

so that good estimates depend on two problems:

(1) computing or estimating  $C$

(2) prove that  $b_j = 0$  for  $j$  "large"

starting from proving that  $b_{2n} = 0$ ; in this case, one already gets

$$|S(f)| \leq C |k|^{n-1/2}$$

In particular: if  $n=1$  (sum in one variable, going back to Weil) , the only requirement to get the "best possible" bound is that  $b_2 = 0$ .  
 in the case of  $S(f), T(f, g)$

There is a convenient criterion for that. For instance, if the char  $p$  is  $> \deg(f)$ , then it holds in all cases for  $S(f)$  or  $T(f, g)$ .

So the theory for  $n=1$  can go quicker towards the goal.

2. More than one variable

Of the two problems above, the question of bounding  $C$  is already very difficult sometimes. After work of Bombieri, Katz, which apply to "classical" sums, the general case has been essentially fully solved by Serre's recent Quantitative Sheaf Theory (put in form by Forey - Fresan - K.), which for all practical "standard" problems in analytic ab. theory gives a good upper bound for  $C$ .

The second problem, which is algebraically a question of vanishing of cohomology, is much more tricky, in particular because there are definitely cases where the only vanishing  $b_j$  is  $b_{2n}$ , which is not sufficient for certain applications.

However there have been many developments recently which provide many stronger and better results than previously known.

We discuss these in broad terms...

3 - Reducing to one variable

[More generally: using specific features of the specific sums...]

A sum  $S(f)$  in many variables may only be a mirage: for instance, in ~~Shang's~~ Zhang's paper on gaps between primes, a 3-variable sum appears, which was already at work earlier in ~~the~~ the study of  $d_3(n)$  in arithmetic progressions by Friedlander and Iwaniec:

$$S = \sum_{a,b,c} \sum_{u,v,w} \psi \left( \frac{bvw}{cw+a} + uw + \frac{1}{u} + \frac{1}{v} \right)$$

This looks complicated ~~but~~ but

$$S = \sum_{x \neq 0, -\frac{a}{c}} \text{Kl}_2(x; p) \text{Kl}_2 \left( \frac{bx}{cx+a} \right)$$

where  $\text{Kl}_2(a; p) = \sum \psi \left( ax + \frac{1}{x} \right)$  is a Kloosterman sum. This is now a 1-variable sum, with ~~the~~ "higher rank" trace functions as arguments.

One can deduce quite easily from Deligne's RH the expected square-root cancellation:

$$|S| \leq C |h|^{\frac{3}{2}}, \quad C \text{ independent of } p$$

[Similarly, one can e.g. write  $S(f) = \sum_{u \in h} \psi(u) \left( \sum_{x \in h^n} 1 \right)$  and try to understand the nb. of sol. of  $f(x) = u$  as  $u$  varies.]

### 4 - Stratification

Although "bad" sums exist, there are "few" of them  $\approx$ , in a sense, and the point is that many applications involve "families" of exponential sums where a few "bad" estimates are not too bad.

Here, families may mean  $\rightarrow$  "algebraic" families, e.g.

$$S(h) = \sum_{x \in h^n} \psi(f(x) + h \cdot x) \tag{1}$$

where  $h \in h^n$  (discrete Fourier transform of  $\psi(f(x))$ )  
 $= \sum h_i x_i$

$\rightarrow$  other discrete Fourier transforms  
for  $x: (h^x)^n \rightarrow \mathbb{C}^x$  (discrete "Mellin" transform)  
 $T_{\chi}(x) = \sum_{x \in (h^x)^n} \chi(x) \psi(f(x))$

In the algebraic case: another very general principle shows that for many sums (e.g.  $S(h)$  in (1)) there is a general "stratification" principle:

There are alg. varieties

$$A^n = Y_0 \supset Y_1 \supset \dots \supset Y_{n-1} \supset Y_n$$

with  $\dim Y_i \leq n - i$

so that  $h \in h^n - Y_i(k^n)$

$$|S(h)| \ll C |k|^{\frac{n+i-1}{2}} \rightarrow \text{independent of } h$$

⑦

In particular: for  $k$  in a dense open set  $(\mathbb{A}^n - Y_i)$  we get square-root cancellation.

However, again because of application we will often start with  $f \in \mathbb{Z}[x_1, \dots, x_n]$  and apply the above modulo  $p \rightarrow +\infty$ . Fouvry recognized the importance of a stronger stratification property, which is a uniformity property due to Katz - Laumon: the  $Y_i$  above, which a priori are defined over a finite field and depend on  $k$ , can be "defined over  $\mathbb{Z}$ ", i.e. by equations which are independent of  $p$  (maybe large enough).

In work in progress with Banerjee and Woo, we go even further from the point of view of uniformity: in some cases, one wants to apply the stratification ~~to~~ varying  $f_a$ , a in some further parameter space, and in particular B - Pierce - Woo need this for certain cases where it is essential ~~to~~ to have bounds for the coefficients and degrees of the varieties  $Y_i$  that appear for given  $a$ ...

In work with Forey and Frerón (relying heavily in many ways on Quant. Sheaf Theory), we perform the first "formal" stratification step for families parameterized by (e.g.) mult. characters of  $(\mathbb{h}^*)^n$ . A natural, non-obvious, question is to determine whether the "next" steps also apply here...