The large sieve and L-functions over finite fields

E. Kowalski

(Université Bordeaux I)

The large sieve

Trigonometric large-sieve inequality (Bombieri):

$$\sum_{q\leq Q}\ \sideset{}{^*}\sum_{a\,(\mathrm{mod}\,q)}\Bigl|\sum_{n\leq N}\alpha(n)e\Bigl(\frac{an}{q}\Bigr)\Bigr|^2 \leq (N-1+Q^2)\sum|\alpha(n)|^2$$

where $e(z)=\exp(2i\pi z)$ and $\alpha(n)\in\mathbf{C}$ are arbitrary.

Sieve application: $\Omega_p\subset\mathbf{Z}/p\mathbf{Z}$ for all p; then

$$|\{n\leq N\ \mid\ n\,(\mathrm{mod}\,p)\notin\Omega_p,\ \ p\leq Q\}|\leq(N-1+Q^2)H^{-1}$$

with

$$H=\sideset{}{^\flat}\sum_{q\leq Q}\prod_{p\mid q}\frac{|\Omega_p|}{p-|\Omega_p|}\geq\sum_{p\leq Q}|\Omega_p|p^{-1}.$$

An application

Theorem 1 (Gallagher)**.** For $d \geq 1$, $N \geq 1$, we have

$$|\{f = \sum_{i=0}^{d} a_i T^i \in \mathbf{Z}[T] \mid f \text{ monic, } \deg(f) = d, \\ |a_i| \leq N \text{ and } \mathrm{Gal}(K_f/\mathbf{Q}) \neq \mathfrak{S}_d\}| \ll N^{d-1/2}(\log N)$$

where K_f is the splitting field of f. In fact (K.), this is $\ll d^2 N^{d-1/2}(\log N)$ with an absolute implied constant.

Developments we will not go into...

Multiplicative form (Gallagher):

$$\sum_{q\le Q} \sum_{\chi \,(\mathrm{mod}\, q)}^{*} \Big|\sum_{n\le N} \alpha(n)\chi(n)\Big|^2 \le (N-1+Q^2)\sum |\alpha(n)|^2.$$

This is "as strong as GRH" on average: take $\alpha(n)=\mu(n)$; if $N \le Q^2$, get

$$\sum_{n\le N} \mu(n)\chi(n)$$

of order $\sqrt{N}$ on average over primitive q with modulus $\le Q$.

This is an ingredient in the Bombieri-Vinogradov theorem, and has been generalized to Fourier coefficients of modular forms (instead of $\chi(n)$) by Iwaniec, Deshouillers-Iwaniec, ...

Curves over finite fields

Let $C/\mathbf{F}_q$ be a smooth projective curve over $\mathbf{F}_q$ with $q = p^\nu$ elements,

$$Z(C) = \text{exp}\Big(\sum_{n\geq 1} \frac{|C(\mathbf{F}_{q^n})|}{n} T^n\Big)$$

the zeta function of C. It is known that

$$Z(C) = \frac{P_C(T)}{(1-T)(1-qT)},$$

where P_C is a polynomial with integer coefficients of degree $2g$, $g \geq 0$ being the *genus* of C.

The polynomial P_C satisfies a *functional equation*:

$$T^{2g} P_C(q/T) = P_C(T).$$

This reflects part of the *spectral interpretation*: there exists a $2g$-dimensional vector space V with a non-degenerate alternating form $\langle \cdot, \cdot \rangle$, and a linear operator F on V such that

$$P_C = \det(1 - TF \mid V)$$

and $\langle Fx, Fy \rangle = q\langle x, y \rangle$.

Moreover, the *Riemann Hypothesis* is true: if α is a root of P_C, then $|\alpha_i| = \sqrt{q}$ (so if q^{-s} is a root, then $\mathrm{Re}(s) = 1/2$).

Families of curves

Fix $f \in \mathbf{F}_q[T]$, monic, squarefree, of degree $2g$. Assume $p \neq 2$. Look at all the (smooth models of the) curves

$$C_t : y^2 = f(x)(x-t), \quad t \in \mathbf{F}_q \text{ not a zero of } f,$$

defined over $\mathbf{F}_q$. We obtain a “family” of about q curves of genus g; we can consider extensions $\mathbf{F}_{q^f}/\mathbf{F}_q$ and get about q^f curves (from the same polynomial f).

In particular we have about q^f polynomials P_{C_t} from the zeta functions of C_t. What are their properties? Are they “usually” irreducible?

Analogy

degree d	genus g
f of degree d or coefficients $(a_i) \in \mathbf{Z}^d$	P_C for C of genus g or Frobenius F_C for such C
Reduction $f \pmod{\ell}$	F_C acting on $V/\ell V$
Additive characters of $\mathbf{Z}/q\mathbf{Z}$	Irreducible representations of finite symplectic groups
All f with height $\max\|a_i\| \leq N$	Algebraic family C_t, $t \in \mathbf{F}_q$
The reductions are well-distributed	Chebotarev density theorem
Classical large sieve	New form of large sieve
Gallagher's theorem	...

More general families/framework

Katz and Sarnak have studied many types of “families of L-functions” over finite fields. For instance:

– Families of Kloosterman sums

$$K(a,1;q^f)=\sum_x \psi(\mathrm{Tr}(ax+1/x)), \qquad \text{with } a\in\mathbf{F}_{q^f},$$

– The family of reductions of elliptic curves/abelian varieties, e.g.

$$y^2=x(x-1)(x-t), \quad t\in\mathbf{F}_{q^f}-\{0,1\}, \qquad \text{defined over } \mathbf{F}_{q^f},$$

– Families of twists of elliptic curves over function fields (Katz), e.g.

$$f(x)y^2=x(x-1)(x-t), \quad f\in\mathbf{F}_{q^f}[X], \quad \deg(f)=d \text{ fixed}$$

(with extra conditions on f).

Common features

The families for which the theory is best understood are described as follows:

- There is a (very simple) “parameter” space $U/\mathbf{F}_q$, for instance all elements of $\bar{\mathbf{F}}_q$ except finitely many, and for each t, there is an L-function $L(\mathcal{F}_t, T)$ of interest.

- For each t, there is a matrix F_t of fixed size N with “essentially” integral coefficients, such that

$$\det(1 - TF_t) = L(\mathcal{F}_t, T).$$

The goal is to analyze the behavior of F_t on average over $t \in \mathbf{F}_q$ (or $\mathbf{F}_{q^f}$ with $f \to +\infty$).

For this, we hope some kind of equidistribution, similar to the fact that the reductions of integers (or primes...) modulo q are equidistributed in $\mathbf{Z}/q\mathbf{Z}$ (or $(\mathbf{Z}/q\mathbf{Z})^{\times}$).

For this algebraic setting, the situation is typically as follows: associated to the parameter variety $U/\mathbf{F}_q$, there is a (compact) group Π_1, a conjugacy class $\mathrm{Fr}_t \in \Pi_1$ for every t, and for every prime ℓ distinct from p, a map

$$\rho_\ell : \Pi_1 \rightarrow GL(N, \mathbf{Z}/\ell\mathbf{Z})$$

such that

$$L(\mathcal{F}_t, T) = \det(1 - TF_t) \equiv \det(1 - \rho_\ell(\mathrm{Fr}_t)T) \pmod{\ell}.$$

An analogue of the equidistribution of integers or primes modulo a fixed integer q would be that $\rho_\ell(\mathsf{Fr}_t)$ is equidistributed in the finite group $G_\ell = \mathrm{Im}(\rho_\ell) \subset GL(N, \mathbf{F}_\ell)$ for any fixed ℓ.

There is a small complication: there exists a normal subgroup Π_1^g of Π_1, with abelian quotient $\Gamma = \Pi_1/\Pi_1^g$, such that if we form the diagram

$$\begin{tikzcd}
1 \arrow[r] & \Pi_1^g \arrow[r] \arrow[d] & \Pi_1 \arrow[r, "d"] \arrow[d, "\rho_\ell"'] & \Gamma \arrow[r] \arrow[d, "\varphi"'] & 1 \\
1 \arrow[r] & G_\ell^g \arrow[r] & G_\ell \arrow[r, "d"] & \Gamma_\ell \arrow[r] & 1,
\end{tikzcd}$$

we have $d(\rho_\ell(\mathsf{Fr}_t)) = q^w$ for every $t \in U(\mathbf{F}_q)$ for some $w \in \mathbf{Z}$, equal to 1 in the case of families of curves.

The analogue of equidistribution is the *Chebotarev density theorem*: the $\rho_\ell(\mathsf{Fr}_t)$ become equidistributed in the (conjugacy classes in the) coset

$$|\{x \in G_\ell \mid d(x) = q^w\}|,$$

i.e.,

$$\max_{\substack{C \subset G_\ell \\ d(C)=q^{fw}}} \left| \frac{|\{t \in U(\mathbf{F}_{q^f}) \mid \rho_\ell(\mathsf{Fr}_t) \in C\}|}{|U(\mathbf{F}_{q^f})|} - \frac{|C|}{|G_\ell^g|} \right| \to 0$$

as $f \to +\infty$.

Large sieve inequality for families of L-functions

Theorem 2 (K.)**.** Let $\mathcal{F}_t$ be an algebraic family as above, $\mathcal{L}$ a finite set of primes $\leq L$, $\Omega_\ell \subset G_\ell$ a conjugacy invariant set with $d(\Omega_\ell) = q^w$ for $\ell \in \mathcal{L}$. Assume that for all $\ell_1 < \cdots < \ell_k$ in $\mathcal{L}$, the product map $\Pi_1^g \longrightarrow G_{\ell_1}^g \times \cdots \times G_{\ell_k}^g$ is *onto*. Then we have

$$|\{t \in U(\mathbf{F}_q) \mid \rho_\ell(\mathrm{Fr}_t) \notin \Omega_\ell \text{ for } \ell \in \mathcal{L}\}| \leq |U(\mathbf{F}_q)|\Bigl(1+Cq^{-1/2}L^A\Bigr)H^{-1}$$

where A, C are constants and

$$H = \sum_{\ell | m \Rightarrow \ell \in \mathcal{L}}^{\flat} \prod_{\ell | m} \frac{|\Omega_\ell|}{|G_\ell^g| - |\Omega_\ell|}.$$

Reference. `arXiv:math.NT/0503714`; to appear in *Crelle*.

First application

We come back to the families of curves above ($w = 1$):

$$C_t \,:\, y^2 = f(x)(x-t), \quad t \in \mathbf{F}_q \text{ not a zero of } f.$$

Let K_t be the splitting field over $\mathbf{Q}$ of the polynomial P_{C_t}, the numerator of the zeta function of C_t.

Theorem 3 (K.)**.** We have

$$|\{t \in \mathbf{F}_q \mid \mathsf{Gal}(K_t/\mathbf{Q}) \neq W_{2g}\}| \ll q^{1-c_g}(\log q)$$

where $c_g = (4g^2 + 2g + 4)^{-1}$, and the implied constant is *absolute*. Here W_{2g} is the group of permutations of g pairs $(2i-1, 2i)$ respecting the pairs.

N.B. The qualitative statement (i.e.,with $o(q)$ as $q \to +\infty$) was a conjecture of Katz proved by N. Chavdarov in 1995.

This is interesting in:

- “Vertical” direction: g fixed, characteristic $p \neq 2$ fixed, $q = p^k$, $k \to +\infty$.

- “Horizontal” direction: g fixed and $q = p \to +\infty$.

- “Random matrices” direction: $g \to +\infty$ (i.e., the size of matrices gets large), as long as $q \to +\infty$ somewhat faster than e^{g^2}.

Ingredients for the proof of Theorem 2

Using harmonic analysis on the finite groups G_ℓ to detect conditions such as $x \in \Omega_\ell$, and then using standard analytic number theory tricks, it suffices (essentially) to have *uniform* estimates for sums of the type

$$S(\ell,\pi,\ell',\pi') = \sum_{t\in U(\mathbf{F}_q)} \mathsf{Tr}\,\pi(\rho_\ell(\mathsf{Fr}_t))\overline{\mathsf{Tr}\,\pi'(\rho_{\ell'}(\mathsf{Fr}_t))}$$

where ℓ, $\ell' \in \mathcal{L}$, π, π' are irreducible (complex-valued) representations of G_ℓ and $G_{\ell'}$ respectively.

One expects orthogonality of characters and independence of the various ℓ to imply that $S(\ell,\pi,\ell',\pi')$ is small unless $(\ell,\pi) = (\ell',\pi')$.

Enter the Riemann Hypothesis

The Grothendieck-Lefschetz Trace Formula implies

$$S(\ell,\pi,\ell',\pi') = \sum_{i=0}^{2d} (-1)^d \operatorname{Tr}(F \mid H_c^i(\bar{U}, \Pi_{\pi,\pi'}))$$

for some étale sheaf $\Pi_{\pi,\pi'}$ depending on π, π', where F is the "global" Frobenius acting on $\bar{U}$.

Here d is the dimension of U; if U is geometrically irreducible, as in the applications considered, it is known that $|U(\mathbf{F}_q)| = q^d + O(q^{d-1/2})$.

Deligne's Riemann Hypothesis shows that

$$|\operatorname{Tr}(F \mid H_c^i(\Pi_{\pi,\pi'}))| \le q^{i/2} \dim H_c^i(\Pi_{\pi,\pi'}).$$

So only $i = 2d$ can contribute as much as q^d.

Standard facts show that $H_c^{2d} = 0$ *unless* $\ell = \ell'$ and $\pi \simeq \pi'$ when restricted to G_ℓ^g.

Taking representatives for this equivalence relation turns out to be sufficient for the sieve. So we have sums with

$$|S(\ell, \pi, \ell', \pi')| \leq q^d \delta(\ell, \pi; \ell', \pi') + q^{d-1/2} \sigma(\Pi_{\pi,\pi'})$$

where

$$\sigma(\Pi_{\pi,\pi'}) = \sum_{i=0}^{2d-1} \dim H_c^i(\Pi_{\pi,\pi'}).$$

The last step is to bound $\sigma(\Pi_{\pi,\pi'})$. This is almost done (but not quite) in works of Katz. Adapting some of his methods one gets:

Proposition 1 (K.). We have

$$\begin{aligned}\sigma(\Pi_{\pi,\pi'}) &\leq C|G_\ell|(\dim \pi) \text{ if } \ell = \ell',\\ &\leq C|G_\ell||G_{\ell'}|(\dim \pi)(\dim \pi') \text{ if } \ell \neq \ell'.\end{aligned}$$

For $d = 1$ and a family defined by a “compatible system”, one can remove $|G_\ell|$ in the estimate.

Ingredients for the proof of Theorem 3

– Before choosing Ω_ℓ, one must check the linear disjointness assumption. This follows by the Goursat-Ribet lemmas of group theory from:

Deep fact (J.K. Yu): for $\ell \geq 3$, G_ℓ^g is the whole group $Sp(2g, \mathbf{F}_\ell)$.

A simpler alternative proof of this, has been found recently by C. Hall, based on results of Katz and results in group theory by Zalesskiĭ and Serežkin.

Some group theory...

On the right-hand side of the large-sieve inequality, we have to deal with

$$\max_{\ell,\pi}\Bigl\{(\dim\pi)\sum_{\ell',\pi'}\dim\pi'\Bigr\}$$

where $\ell\in\mathcal{L}$, and π runs over representations of G_ℓ modulo the equivalence relation mentioned previously.

So we need to know as precisely as possible the maximal dimension and the sum of dimensions of irreducible representations of a subgroup of $CSp(2g,\mathbf{F}_\ell)$ containing $Sp(2g,\mathbf{F}_\ell)$.

Proposition 2 (J. Michel, K.)**.** We have

$$\dim \pi \leq (\ell + 1)^{g^2}, \quad \sum_{\pi'} \dim \pi' \leq (\ell + 1)^{(g^2+g)/2}.$$

For the first bound at least, one needs to go into Deligne-Lusztig generalized characters.

The second bound can be derived from an exact formula due to Vinroot.

N.B. The "trivial" bounds $\dim \pi \leq |G_\ell|^{1/2}$ and

$$\sum_{\pi'} \dim \pi' \leq (|G_\ell||G_\ell^\sharp|)^{1/2}$$

are sufficient for basic applications.

One wishes to take, e.g.,

$$\Omega_\ell = \{g \in CSp(2g, \mathbf{F}_\ell) \mid \langle gv, gw \rangle = q\langle v, w \rangle, \\ \text{and } \det(1 - Tg) \in \mathbf{F}_\ell[T] \text{ irreducible}\}.$$

One must compute Ω_ℓ quite precisely. Let ω_ℓ be the set of irreducible polynomials $f \in \mathbf{F}_\ell[T]$ such that

$$T^{2g} f(q/T) = f(T).$$

Proposition 3 (Chavdarov, Borel)**.** We have

$$\frac{|\Omega_\ell|}{|CSp(2g, \mathbf{F}_\ell)|} \geq \frac{|\omega_\ell|}{(\ell + 1)^g}.$$

Putting things together

When combining from primes to squarefree numbers the (optimal) bound for $\dim\pi$ becomes

$$\dim\pi \leq \psi(m)^{g^2} \text{ where } \psi(m) = \prod_{\ell|m}(\ell+1) \ll m\log\log m,$$

which may lead to the (dreadful) loss of a power of $\log\log q$. So we sum over squarefree integers m such that $\psi(m) \leq L$, with L small enough that $L^A \leq q^{1/2}$.

Fortunately bounds such as

$$\sum_{\psi(m)\leq L} \varphi(m)^k \gg L^{k+1}$$

are well-known in analytic number theory.

Other applications and perspective

– “Most” abelian varieties $A/\mathbf{F}_q$ over a finite field are determined up to isomorphism by the sequence of torsion fields $\mathbf{F}_q(A[n])$, $n \geq 1$ (K., J. London Math. Soc., to appear).

– Bounds for the number of quadratic twists of elliptic curves with “extra rank” (K. and work in progress by F. Jouve). Determining the image of ρ_ℓ, which typically lies in an orthogonal group is again very tricky (works of Katz, Larsen are used, the best results are due to C. Hall, in preparation).

– The large sieve setting can be vastly generalized to encompass the classical and Frobenius case in one framework, where the actual sieve bound is reduced to bounds for “exponential sums”. This may have many other applications (C. Zywina, K. in preparation, independently).

– For instance: take $G = SL(n, \mathbf{Z})$, S a finite set of generators, ℓ_S the word-length distance on G. Can one estimate

$$|\{g \in G, |\ \ell_S(g) \leq T \text{ and } \det(1 - Tg) \text{ irreducible}\}|?$$

(“small” sieves of this type are being developped by Bourgain, Gamburd and Sarnak; the main point is the property that the Cayley graphs $(SL(n, \mathbf{Z}/q\mathbf{Z}), S)$ are *expanders*.