Statistics of Kloosterman sums

OCT 2018

Yuk-Kam Lau
The University of Hong Kong

1. Classical Kloosterman sums

Let $c \geq 1, m, n \in \mathbb{Z}$. H. Kloosterman created

$$S(m,n,c) := \sum_{\substack{x \bmod c \\ (x,c)=1}} e\left(\frac{mx + n\bar{x}}{c}\right)$$

$e(u) = e^{2\pi i u}$

$x\bar{x} \equiv 1 \ (c)$

Kloosterman (1900-68)

In 1926, Kloosterman applied the Hardy-Littlewood (circle) method to study positive definite quadratic forms in four variables, for which $S(m,n,c)$ was introduced.

Remark.

1) $S(m,n,c)$ is a discrete analogue of Bessel functions.
2) $S(m,n,c)$ satisfies some multiplicative relation.

Specialize to: Let $a \in \mathbb{F}_p$. Define

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$$Kl(p,a) := \sum_{x \in \mathbb{F}_p^\times} e\left(\frac{1}{p}\left(x + \frac{a}{x}\right)\right)$$

$$= S(1,a,p)$$

Weil bound: $|\mathrm{Kl}(p,a)| \leq 2\sqrt{p}$

2. Katz's questions

1) Does there exist a GL(2) automorphic form ϕ so that its Hecke eigenvalue $\lambda_\phi(p) = \mathrm{Kl}(p,a)$ for all primes?

2) Is $\{\mathrm{K}\ell(p,a) : p \text{ primes}\}$ equidistributed?

Remark. (1) $\Longrightarrow$ (2) if Sato-Tato conjecture for ϕ holds.

(1) can hold for Maass forms only (i.e. not holomorphic modular forms).

Booker (2000) performed numerical experiments, demonstrating that the Laplacian eigenvalue and level of the Maass form, if exists, will be large.

Both (1) and (2) remains open today.

3. Statistical results for $\mathrm{Kl}(p,a)$

Katz's conjecture (1980):

$$\lim_{x\to\infty}\frac{\#\{p\le x:\ u<\frac{\mathrm{Kl}(p,a)}{2\sqrt{p}}\le v\}}{\#\{p\le x\}}=\frac{2}{\pi}\int_u^v\sqrt{1-x^2}\,dx$$

Katz's result (1988):

$$\lim_{p\to\infty}\frac{\#\{a\in\mathbb{F}_p^\times:\ u<\frac{\mathrm{Kl}(p,a)}{2\sqrt{p}}\le v\}}{p-1}=\frac{2}{\pi}\int_u^v\sqrt{1-x^2}\,dx$$

Model $\mathrm{Kl}(p,a)$ by a random variable Y_a distributed according to Sato-Tate measure μ_{ST}

Xi's Central Limit Theorem (2017):

$$\frac{\frac{1}{H}\sum_{a<b\leq a+H} h\left(\frac{\mathrm{Kl}(p,a)}{2\sqrt{p}}\right)-\mathrm{mean}}{(\mathrm{std\,dev})/\sqrt{H}} \xrightarrow[p\to\infty]{H=o(\log p)} N(0,1)$$

Perret-Gentil's Central Limit Theorem (2017):

$$\frac{1}{\sqrt{H}}\sum_{a<b\leq a+H} h\left(\frac{\mathrm{Kl}(p,a)}{2\sqrt{p}}\right) \xrightarrow[p\to\infty]{H=o(\log p)} N(0,1)$$

4. Moments for $\mathrm{Kl}(p,a)$

Moments: $s_h(p) := \sum_{a\in\mathbb{F}_p^\times} \mathrm{Kl}(p,a)^h.$

Probability moments: $\int_{-1}^{1} x^h \, d\mu_{\mathrm{ST}}$

Known (Salie): $s_2(p) = p^2 - p,\ s_3(p) = \left(\frac{p}{3}\right) p^2 + 2p$

$s_4(p) = 2p^3 - 3p^2 - 3p,$

Write $\mathrm{Kl}(p,a) = \alpha_a + \beta_a$. Set $\mathrm{Kl}_{\mathrm{sym}^d}(p,a) = \sum_{i=0}^{d} \alpha_a^{d-i}\beta_a^i$.

Define $m_d(p) := \sum_{a\in\mathbb{F}_p^\times} \mathrm{Kl}_{\mathrm{sym}^d}(p,a)$.

Evans' conjecture (2010):

$$(-m_5(p)-1)/p = a(p), \qquad (-m_6(p)-1) = b(p)$$

$$\left(\frac{p}{105}\right)(-m_7(p)-1)/p^2 = \varepsilon\lambda(p)^2 - p^2$$

$$-m_8(p) - 1 - p^4 = p^2\mu(p)$$

Yun’s result (2015):

- Let $d \geq 3$ be an odd integer. For any prime ℓ, there exists an orthogonal $\mathbb{Q}_\ell$-vector space M_ℓ of dimension $(d-1)/2$ and a continuous Galois representation ρ_ℓ:

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to O(M_\ell)$$

such that for all primes $d < p \neq \ell$ or $p = 2$ satisfying that ρ_ℓ is unramified at p,

$$-m_d(p) - 1 = p^{(d+1)/2}\mathrm{Tr}(\mathrm{Frob}_p, M_\ell).$$

The representation ρ_ℓ comes from geometry.

- Serre's modularity (conjecture) $\Longrightarrow$ Evans conjecture

5. Kloosterman sums over finite fields

Let $\mathbb{F}_q$ be a finite extension of $\mathbb{F}_p$ $(q = p^f)$. Define

$$\mathrm{Kl}(q,a) := \sum_{x \in \mathbb{F}_q^\times} e(\frac{1}{p}\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x + a/x))$$

where $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)$ denotes the trace function,

$$\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = x + x^p + \cdots + x^{p^{f-1}}$$

Remark. $\mathrm{Kl}(q,a)$ and $S(1,a,q)$ are different.

Weil bound: $\left|\mathrm{Kl}(q,a)\right| \leq 2\sqrt{q}$

Carlitz's result (1969):

$$\sum_{n\geq 1} \frac{\mathrm{Kl}(p^n,a)}{p^{n/2}} \frac{p^{-ns}}{n} = \log\left(1 + \frac{\mathrm{Kl}(p,a)}{\sqrt{p}} p^{-s} + p^{-2s}\right).$$

Consequences:

$$\begin{aligned} \mathrm{Kl}(p^n,a) &= (-2)^{1-n} \sum_{2r\leq n} \binom{n}{2r} \mathrm{Kl}(p,a)^{n-2r} \left(\mathrm{Kl}(p,a)^2 - 4q\right)^r \\ \mathrm{Kl}(p^n,a) &= -\sum_{2r\leq n} (-1)^{n-r} \frac{n}{n-r} \binom{n-r}{r} p^r \mathrm{Kl}(p,a)^{n-2r} \end{aligned}$$

Lachaud & Wolfmann's result (1987): $q = 2^f \ (f \geq 2)$

$$\sum_{a \in \mathbb{F}_q^\times} \mathrm{Kl}(q,a)^h = \sum_{\substack{|t|<2\sqrt{q} \\ t \equiv -1\,(4)}} H(t^2 - 4q)\, t^h$$

Katz & Livne's result (1989): $q = 3^f \ (f \geq 2)$

$$\sum_{a \in \mathbb{F}_q^\times} \mathrm{Kl}(q,a)^h = \sum_{\substack{|t|<2\sqrt{q} \\ t \equiv -1\,(3)}} H(t^2 - 4q)\, t^h$$

Question: Does it generalize to other prime powers q?

6. Ramanujan graphs and Quaternion group

Given a k-regular connected graph (i.e. vertices are connected by at most one line and have k neighbours). Its adjacency matrix A has the (trivial) eigenvalue k. The graph is a Ramanujan graph if all its non-trivial eigenvalues have absolute values $\leq 2\sqrt{k-1}$.

Question: How to construct Ramanujan graphs?

Let H be a definite quaternion algebra over $K = \mathbb{F}_q(t)$ with basis $1, i, j, ij$ where $i^2 = \delta, j^2 = t-1, ij = -ji$ and D denote the multiplicative group $H^\times$ mod its center.

Then H ramifies at 1 and ∞ only, and

$$X_{\mathcal{K}} = D(\mathcal{K}) \backslash D(\mathbb{A}_K) / D(K_\infty)\mathcal{K}$$

is the double coset space of the adelic points of D.

Here $\mathcal{K}$ is an open subgroup of $\prod_{v \neq \infty} D\mathcal{O}_v$ and $\mathcal{O}_v$ is ring of integers in the completion.

At the place 0 of K, we get

$$X_{\mathcal{K}} \approx \Gamma(\mathcal{K}) \backslash D(K_0) / D(\mathcal{O}_0) = \Gamma(\mathcal{K}) \backslash PGL_2(K_0) / PGL_2(\mathcal{O}_0)$$

where $\Gamma(\mathcal{K}) = D(K) \cap D(K_\infty)\mathcal{K}$.

The right coset space $PGL_2(K_0)/PGL_2(\mathcal{O}_0)$ has a natural structure as a ($q+1$)-regular infinite tree.

The quotient $X_{\mathcal{K}}$ is viewed as a finite (q+1)-regular graph.

In short $X_{\mathcal{K}}$ is now realized in two ways:

$$X_{\mathcal{K}} = D(\mathcal{K}) \setminus D(\mathbb{A}_K)/D(K_\infty)\mathcal{K} = \Gamma(\mathcal{K}) \setminus PGL_2(K_0)/PGL_2(\mathcal{O}_0)$$

a double coset space of $D(\mathbb{A}_K)$ and a graph.

Consequently the functions on the vertices of the graph $X_{\mathcal{K}}$ are interpreted as automorphic forms on the adelic quaternion group $D(\mathbb{A}_K)$; the adjacency matrix corresponds to the Hecke operator T_0 at the place 0.

What are the eigenvalues of T_0?

7. Kloosterman sums over function fields

Let $K=\mathbb{F}_p(t)$. Suppose $a\in K\setminus\{0\}$ and $f(x)=x+a/x$.

For any place of v, let $\mathbb{F}_v$ be the residue field of the completion of K at v. Define

$$\mathrm{Kl}(\mathbb{F}_v;a)=\sum_{x\in\mathbb{F}_v^{\times}} e(\frac{1}{p}\circ \mathrm{tr}_{\mathbb{F}_v/(\mathbb{Z}/p\mathbb{Z})}(x+a/x))$$

where a in the summation is the image of a in the residue Field $\mathbb{F}_v$.

If the place $v\in K$ is a monic irreducible polynomial of degree f, then $\mathbb{F}_v\cong\mathbb{F}_q$ $(q=p^f)$ under some isomorphism.

The eigenvalues of T_0: $-\mathrm{Kl}(\mathbb{F}_v,a)=\mathrm{Kl}(\mathbb{F}_q,a)$.

$X_{\mathcal{K}_0}$ is $(q+1)$-regular graph, so $X_{\mathcal{K}_0}$ is Ramanujan.

8. Katz's questions in function field cases

1) Does there exist a GL(2) automorphic form ϕ so that its Hecke eigenvalue $\lambda_\phi(p) = \mathrm{Kl}(\mathbb{F}_v, a)$ for all primes?

2) Is $\{\mathrm{Kl}(\mathbb{F}_v, a) : v \text{ monic irred poly}\}$ equidistributed?

Chai-Li (2003) solved (1) and hence (2).

Question: (2) says

$$\frac{\#\{v : N(v) \le x,\ \mathrm{Kl}(\mathbb{F}_v, a) \in I\}}{\#\{v : N(v) \le x\}} \longrightarrow \int_I d\mu_{ST} \text{ as } x \to \infty.$$

Is it possible to derive a short interval version?

Thank you

Set $\mathcal{K} = \mathcal{K}_0$ where $\mathcal{K}_0 = (1 + \mathcal{P}_1^2) \prod_{v \neq 1,\infty} D(\mathcal{O}_v)$ and

$\mathcal{P}_1$ = maximal ideal of $\mathcal{O}_1$ in quaternion algebra $H(K_1)$.

For any $a \in \mathbb{F}_q^\times$, $-\mathrm{Kl}(\mathbb{F}_v, a/(t-1))$ is eigenvalue of Hecke operator T_v, $v = 1, \infty$. In particular, let $v = 1, \infty$ be a place of degree one and $\pi_v = c(t-1)+1$ for some $c \in \mathbb{F}_q^\times$, the eigenvalue is given by

$$-\mathrm{Kl}(\mathbb{F}_v, a/(t-1)) = -\mathrm{Kl}(\mathbb{F}_q, -ac).$$

By Weil bound, RHS $\leq 2\sqrt{q}$, and $X_{\mathcal{K}_0}$ is $(q+1)$-regular graph.

i.e. $X_{\mathcal{K}_0}$ is Ramanujan.