



聊城大学

## On the generating fields of Kloosterman sums

---

Shenxing Zhang(HFUT)

*Liaocheng University*

[zhangshenxing@hfut.edu.cn](mailto:zhangshenxing@hfut.edu.cn)



Let  $f(x) \in \mathbb{F}_q[x]$  be a polynomial over a finite field with  $q = p^d$  elements, where  $p$  is a rational prime. Define the exponential sum

$$S_1(f) := \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(f(x))} \in \mathbb{Z}[\zeta_p].$$

A basic problem is

- (1) as a complex number,  $|S_1(f)| = ?$
- (2) as a  $p$ -adic number,  $|S_1(f)|_p = ?$
- (3) as an algebraic number,  $\deg S_1(f) = ?$

The first two questions have been studied extensively in the literature. Define

$$L(t, f) := \prod_{x \in \overline{\mathbb{F}}_p} \left(1 - \mathrm{Tr}_{\mathbb{F}_q(x)/\mathbb{F}_p}(f(x))t^{\deg x}\right)^{-1} = \exp\left(\sum_k S_k(f) \frac{t^k}{k}\right)$$

where  $S_k(f) := \sum_{x \in \mathbb{F}_{q^k}} \zeta_p^{\text{Tr}(f(x))} \in \mathbb{Z}[\zeta_p]$ .

## Theorem

**$L(t, f)$  is a rational function.**

Write

$$L(t, f) = \frac{\prod_j (1 - \beta_j t)}{\prod_i (1 - \alpha_i t)}.$$

Then

$$S_k(f) = \sum_i \alpha_i^k - \sum_j \beta_j^k.$$

How to estimate the characteristic roots  $\alpha_i$  and  $\beta_j$ ? We need  $\ell$ -adic method. To describe it, let's recall the definition of sheaves.

Given a topological space  $X$ , there is a site  $\text{Top}(X)$  with

- (1) objects: the open subsets of  $X$ ;
- (2) morphisms: the injection of open sets;
- (3) coverings: normal open coverings.

A sheaf  $\mathcal{F}$  on a topological space  $X$  over a field  $E$  is a contravariant functor  $\text{Top}(X)^{\text{op}} \rightarrow \text{Vect}/E$ , which can be uniquely glued locally. That's to say, for any open covering  $U = \cup_i U_i$ ,

$$\mathcal{F}(U) \rightarrow \prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_i \cap U_j)$$

is exact.

Let  $X$  be a scheme. Denote by  $X_{\text{ét}}$  the site with

- (1) objects: étale scheme  $X' \rightarrow X$ ;
- (2) morphisms: étale morphisms;
- (3) coverings:  $\varphi_i : X'_i \rightarrow X'$  with  $X' = \cup \varphi_i(X'_i)$ .

Fix a prime  $\ell \neq p$  and let  $E$  be a finite extension of  $\mathbb{Q}_\ell$ . An  $\ell$ -adic sheaf is a sheaf on  $X_{\text{ét}}$  over  $E$  (which is constructible at every finite level).

Let  $K$  be c.d.v.f, with higher ramification groups  $I^{(r)}, r \geq 0$ . For any  $E$ -representation  $M$  of  $P$ , we have a decomposition  $M = \oplus M(x)$ , such that

$$M(0) = M^P, \quad M(x)^{I(x)} = 0, \quad M(x)^{I(y)} = M(x), \quad y > x > 0.$$

We call  $x$  a break if  $M(x) \neq 0$ . Define

$$\mathrm{Sw}(M) = \sum x \dim M(x).$$

Let  $C$  be a proper smooth geometrically connected curve over a perfect field  $\mathbb{F}$ , with function field  $K = \mathbb{F}(C)$ . For any closed point  $x \in C(\mathbb{F})$ , we have the completion  $K_x$ .

For any non-empty open  $U \subset C$ , we have an equivalence of abelian categories

$$\begin{aligned} \text{isse } E\text{-sheaves on } U &\longrightarrow \text{Rep}_E^c \pi_1(U, \bar{\eta}) \\ \mathcal{F} &\longmapsto \mathcal{F}_{\bar{\eta}}. \end{aligned}$$

Since  $\pi_1(U, \bar{\eta})$  is a quotient of  $\text{Gal}(\bar{K}/K)$ , the decomposition group  $D_x \subset \text{Gal}(\bar{K}/K)$  acts on  $\mathcal{F}_{\bar{\eta}}$ . We can define Swan conductor of  $\mathcal{F}$  at  $x$ . If  $x \in U$ , the action of  $I_x$  is trivial.

We will take  $\mathbb{F} = \mathbb{F}_p, C = \mathbb{P}^1$  and  $U = \mathbb{G}_m$ .



Assume that  $\mu_p \subseteq E$ . Deligne constructed a certain locally free of rank one  $\ell$ -adic sheaf  $\mathcal{F}_\ell(f)$  over  $E$  on  $\mathbb{G}_{a, \overline{\mathbb{F}}_p} = \text{Spec } \overline{\mathbb{F}}_p[X]$ , such that

$$L(t, f) = \prod_i \det(1 - t\text{Frob}, H_c^i)^{(-1)^{i+1}}$$

and

$$S_k(f) = \sum_i (-1)^i \text{Tr}(\text{Frob}^k, H_c^i).$$

Here,  $\text{Frob}$  is the geometric Frobenius (inverse of  $\alpha \mapsto \alpha^p$ ),  $H_c^i = H_c^i(\mathbb{G}_{a, \overline{\mathbb{F}}_p}, \mathcal{F}_\ell(f))$  is the compact cohomology.

Denote by  $\omega_{ij}$  the eigenvalues of Frob on  $H_c^i$ , then

$$S_k(f) = \sum_{ij} (-1)^i \omega_{ij}^k.$$

Denote by  $B_i = \dim_E H_c^i$  the Betti number.

## Theorem

$\omega_{ij}$  is an algebraic integer and all its conjugates over  $\mathbb{Q}$  has same absolute value  $q^{r_{ij}/2}$ , where the weight  $0 \leq r_{ij} \leq i$  are integers.

Thus

$$|S_k| \leq \sum_i B_i q^{ki/2}.$$

## General case

In general,

- (1)  $V$  a closed variety over  $\mathbb{F}_q$  of  $\mathbb{A}^N$ ,
- (2)  $\psi$  a non-trivial additive character on  $\mathbb{F}_q$ ,  $\psi_k = \psi \circ \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ ,
- (3)  $f$  a regular function on  $V$  defined over  $\mathbb{F}_q$ ,
- (4)  $\chi$  a multiplicative character on  $\mathbb{F}_q^\times$ ,  $\chi_k = \chi \circ \mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ ,
- (5)  $g$  an invertible regular function on  $V$ .

## Define

$$S_k = \sum_{x \in V(\mathbb{F}_{q^k})} \psi_k(f(x)) \chi_k(g(x)).$$

Then Deligne's results still hold in this case. Moreover, Bombieri proved that the number of characteristic roots is at most

$$(4 \max \deg V + 1, \deg f + 5)^{2N+1}.$$

Now we will consider

$$V = V(X_1 \cdots X_n - a), \quad f = X_1 + \cdots + X_n.$$

Let  $\chi = \chi_1, \dots, \chi_n$  be an unordered  $n$ -tuple of multiplicative characters  $\chi_i : \mathbb{F}_q^\times \rightarrow \mu_{q-1}$ . Define the Kloosterman sum as

$$\mathrm{Kl}_n(\psi, \chi, q, a) = \sum_{\substack{x_1 \cdots x_n = a \\ x_i \in \mathbb{F}_q}} \chi_1(x_1) \cdots \chi_n(x_n) \psi(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_1 + \cdots + x_n)).$$

In this case, there are  $n$  characteristic roots with same weight  $n - 1$ . Hence  $|\text{Kl}_n| \leq nq^{(n-1)/2}$ .

Clearly,  $\text{Kl}_n \in \mathbb{Z}[\mu_{pc}]$ , where

$$c = \text{lcm}_i \text{ord}(\chi_i)$$

divides  $q - 1$ . Write

$$\text{Gal}(\mathbb{Q}(\mu_{pc})/\mathbb{Q}) = \sigma_t \tau_w \mid t \in (\mathbb{Z}/p\mathbb{Z})^\times, w \in (\mathbb{Z}/c\mathbb{Z})^\times,$$

where

$$\begin{aligned} \sigma_t(\zeta_p) &= \zeta_p^t, & \sigma_t(\zeta_c) &= \zeta_c, \\ \tau_w(\zeta_p) &= \zeta_p, & \tau_w(\zeta_c) &= \zeta_c^w. \end{aligned}$$

A basic observation tells

$$\sigma_t \tau_w \text{Kl}_n(\psi, \chi, q, a) = \prod \chi(t)^{-w} \text{Kl}_n(\psi, \chi^w, q, at^n).$$

To study the generating fields of  $\text{Kl}_n$ , we need to consider the distinctness of different Kloosterman sums.

When  $\chi = \mathbf{1} = 1, \dots, 1$  is trivial, it's easy to see that

$$a, b \text{ conjugate} \implies \text{Kl}_n(\psi, \mathbf{1}, q, a) = \text{Kl}_n(\psi, \mathbf{1}, q, b).$$

When  $p > (2n^{2d} + 1)^2$  (Fisher), or  $p \geq (d-1)n + 2$  and  $p$  does not divide a certain integer (Wan), this is necessary. In general, it's conjectured that it's true when  $p \geq nd$ . Thus

$$\deg \mathrm{Kl}_n(\psi, \mathbf{1}, q, a) = \frac{p-1}{(p-1, n)}$$

under these conditions.

sheaf. Deligne and Katz defined the Kloosterman

$$= \mathcal{K}l_{n,q}(\psi, \chi)$$

the following properties:

( $\psi$  finite level) of rank  $n$  and pure of weight  $n - 1$ .

$$(-1)^{n-1} \mathcal{K}l_n(\psi, \chi, q, a).$$

factor 1 at  $\infty$ . So all  $\infty$ -breaks are  $1/n$ .

sheaf. Deligne and Katz defined the Kloosterman

$$= \mathcal{K}l_{n,q}(\psi, \chi)$$

the following properties:

( $\psi$  finite level) of rank  $n$  and pure of weight  $n - 1$ .

$$(-1)^{n-1} \mathcal{K}l_n(\psi, \chi, q, a).$$

factor 1 at  $\infty$ . So all  $\infty$ -breaks are  $1/n$ .

sheaf. Deligne and Katz defined the Kloosterman

$$= \mathcal{K}l_{n,q}(\psi, \chi)$$

the following properties:

( $\psi$  finite level) of rank  $n$  and pure of weight  $n - 1$ .

$$(-1)^{n-1} \mathcal{K}l_n(\psi, \chi, q, a).$$

factor 1 at  $\infty$ . So all  $\infty$ -breaks are  $1/n$ .

- sheaf. Deligne and Katz defined the Kloosterman
- $$= \mathcal{K}l_{n,q}(\psi, \chi)$$
- the following properties:
- ( $\psi$  finite level) of rank  $n$  and pure of weight  $n - 1$ .
- $$(-1)^{n-1} \mathcal{K}l_n(\psi, \chi, q, a).$$
- factor 1 at  $\infty$ . So all  $\infty$ -breaks are  $1/n$ .

$$\mathcal{F}_a(\chi)|_{\mathbb{G}_m \otimes \mathbb{F}_q} = \bigotimes_{\sigma \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)} (t \mapsto \sigma(a)t^n)^* \mathcal{K}l_n(\psi \circ \sigma^{-1}, \chi \circ \sigma^{-1}).$$

- sheaves along an extension of finite fields. For  $(\chi)$  on  $\mathbb{G}_m \otimes \mathbb{F}_p$ , such that  $(t^n)^* \mathcal{K}l_n(\psi \circ \sigma^{-1}, \chi \circ \sigma^{-1})$  of weight  $d(n-1)$ .  $= (-1)^{(n-1)d} \mathcal{K}l_n(\psi, \chi, q, at^n)$ .  $\chi$  is at most 1.



**Let  $\mathcal{F}, \mathcal{F}'$  be lisse sheaves on  $\mathbb{G}_m \otimes \mathbb{F}_p$  of same rank  $r$  and pure of the same weight  $w$ . Assume that there is a root of unity  $\lambda$  such that for any  $t \in \mathbb{F}_p^\times$ , we have**

$$\mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}_t^-) = \lambda \mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}_t').$$

**Let  $\mathcal{G}$  be a geometrically irreducible sheaf of rank  $s$  on  $\mathbb{G}_m \otimes \mathbb{F}_p$ , pure of weight  $w$ , such that  $\mathcal{G} \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$  occurs exactly once in  $\mathcal{F} \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ . Then  $\mathcal{G} \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$  occurs at least once in  $\mathcal{F}' \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ , provided that  $p > [2rs(M_0 + M_\infty) + 1]^2$ , where  $M_\eta$  is the largest  $\eta$ -break of  $\mathcal{F} \oplus \mathcal{F}'$ .**

Assume not. Applying the Lefschetz Trace Formula to  $\mathcal{G}^\vee \otimes \mathcal{F}$  and  $\mathcal{G}^\vee \otimes \mathcal{F}'$ , we have

$$\sum_{i=0}^2 (-1)^i \text{Tr}(\text{Frob}, H_c^i(\mathcal{G}^\vee \otimes \mathcal{F})) = \lambda \sum_{i=0}^2 (-1)^i \text{Tr}(\text{Frob}, H_c^i(\mathcal{G}^\vee \otimes \mathcal{F}')).$$

Apply Euler-Poincaré formula

$$h_c^0(\mathcal{F}) - h_c^1(\mathcal{F}) + h_c^2(\mathcal{F}) \\ = \text{rank } \mathcal{F} \cdot \chi_c(\mathbb{G}_m \otimes \mathbb{F}_p) - \text{Sw}_0(\mathcal{F}) - \text{Sw}_\infty(\mathcal{F})$$

to estimate  $\mathrm{Tr}(\mathrm{Frob}, H_c^1)$  (weight  $\leq 1$  by Weil II).

uced if there exists a non-trivial character  $\Lambda$  such  
 lered  $n$ -tuples. In this case,  
 $= 1$ .

Kummer-induced. Then  $\mathcal{F}_a(\chi)$  has a highest  
 s a subsheaf  $\mathcal{G}_a(\chi)$  such that, as representations of  
 irreducible sub-representation with highest weight.  
 and occurs exactly once in  $\mathcal{F}_a(\chi)$  over  $\mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ .

uced if there exists a non-trivial character  $\Lambda$  such  
 lered  $n$ -tuples. In this case,  
 $= 1$ .

Kummer-induced. Then  $\mathcal{F}_a(\chi)$  has a highest  
 s a subsheaf  $\mathcal{G}_a(\chi)$  such that, as representations of  
 irreducible sub-representation with highest weight.  
 and occurs exactly once in  $\mathcal{F}_a(\chi)$  over  $\mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ .

## 18 / 26

[illegible]

19 / 26

Apply Lemma to  $r = s = n^d, M_0 = 0, M_\infty \leq 1$ .

Now

$$\mathcal{G}_a(\chi) \otimes \mathcal{L}_{\prod \bar{\chi}} \hookrightarrow \mathcal{F}_b(\rho) \otimes \mathcal{L}_{\prod \bar{\rho}}, \quad \mathcal{G}_b(\rho) \otimes \mathcal{L}_{\prod \bar{\rho}} \hookrightarrow \mathcal{F}_a(\chi) \otimes \mathcal{L}_{\prod \bar{\chi}}.$$

Thus the highest weight  $\lambda_a(\chi) = \lambda_b(\rho)$ . Derived from this, and combining Fisher's arguments, we have:

## Theorem

**Let  $a, b \in \mathbb{F}_q^\times$ . Assume that  $\chi, \rho$  are not Kummer-induced and neither of them is of type  $(\xi_1, \xi_1^{-1}, 1, \Lambda_2)\xi_2$ . If  $p > (2n^{2d} + 1)^2$  and**

$$\text{Kl}_n(\psi, \boldsymbol{\chi}, q, a) = \lambda \text{Kl}_n(\psi, \boldsymbol{\rho}, q, b)$$

**for some  $\lambda \in \mu_{q-1}$ , then there exists  $\sigma \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$  and a multiplicative character  $\eta$ , such that  $b = \sigma(a)$  and  $\rho = \eta \cdot (\chi \circ \sigma^{-1})$  as unordered tuples. Moreover, either both Kloosterman sums vanish or  $\eta(b) = \lambda^{-1}$ .**

The last step is to show the non-vanishingness.

## Theorem

**If  $p > (3n - 1)C_\chi - n$  and for any  $i, j$ ,  $\chi_i = \chi_j$  if  $\chi_i^n = \chi_j^n$ , then  $\text{Kl}_n(\psi, \chi, q, a)$  is nonzero. Here**

$$C_\chi = \max_{i,j} \text{lcm}(\text{ord}(\chi_i), \text{ord}(\chi_j)) \quad (1)$$

**is the supremum of least common multipliers of the orders of any two characters in  $\chi$ .**

We can express  $\text{Kl}_n$  as Gauss sums

$$(q-1)\text{Kl}_n(\psi, \chi, q, a) = \sum_{m=0}^{q-2} \omega^m(a) \prod_{i=1}^n g(m + s_i)$$

by Fourier transform on  $\mathbb{F}_q^\times$ , where  $\chi_i = \omega^{s_i}$  for a Teichmüller character. What we need to do is to prove there is a unique  $m$  such that the valuation of  $\prod_{i=1}^n g(m + s_i)$  is minimal.



## Theorem

**If  $p > \max(2n^{2d} + 1)^2, (3n - 1)C_\chi - n$  and for any  $i, j$ ,  $\chi_i = \chi_j$  if  $\chi_i^n = \chi_j^n$ , then  $\text{Kl}_n(\psi, \chi, q, a)$  generates  $\mathbb{Q}(\mu_{pc})^H$ , where  $H$  consists of those  $\sigma_t \tau_w$  such that there exists an integer  $\beta$  and a character  $\eta$  satisfying**

$$t = \lambda a_1^\beta, \lambda^{n_1} = 1, \chi^w = \eta \chi^{q_1^\beta}, \eta(a) = \prod \chi^w(t).$$

**Here**  $n_1 = (n, p - 1)$ ,  $q_1 = \#\mathbb{F}_p(a^{(p-1)/n_1})$  **and**  $a_1 \in \mathbb{F}_p^\times$  **such that**  $a_1^{n/n_1} = N_{\mathbb{F}_{q_1}/\mathbb{F}_p}(a^{(1-p)/n_1}) = a^{(1-q_1)/n_1}$ .

## An example: $n = 2$ case

Let  $\chi = 1, \chi$ , where  $\chi$  is a multiplicative character of order  $c \neq 2$ . If  $p > \max(2^{2d+1} + 1)^2, 5c - 2$ , then  $\text{Kl}(\psi, \chi, p^d, a)$  generates  $\mathbb{Q}(\mu_{pc})^H$ , where

$$H = \begin{cases} \langle \tau_{q_1} \sigma_{a_1}, \sigma_{-1}, \tau_{-1} \rangle, & \text{if } \chi(-1) = 1, \chi(a) = 1; \\ \langle \tau_{-q_1} \sigma_{a_1}, \sigma_{-1} \rangle, & \text{if } \chi(-1) = 1, \chi(a) = \chi(a_1) = -1; \\ \langle \tau_{q_1^\alpha} \sigma_{a_1^\alpha}, \sigma_{-1} \rangle, & \text{if } \chi(-1) = 1, \chi(a)^\alpha \neq 1; \\ \langle \tau_{q_1} \sigma_{-a_1}, \tau_{-1} \sigma_{-1} \rangle, & \text{if } \chi(-1) = -1, \chi(a) = \chi(a_1) = -1; \\ \langle \tau_{q_1} \sigma_{a_1}, \tau_{-1} \rangle, & \text{if } \chi(-1) = -1, \chi(a) = 1; \\ \langle \tau_{q_1} \sigma_{a_1}, \tau_{-1} \sigma_{-1} \rangle, & \text{if } \chi(-1) = -1, \chi(a) = -1, \chi(a_1) = 1; \\ \langle \tau_{q_1^{\alpha/2}} \sigma_{-a_1^{\alpha/2}} \rangle, & \text{if } \chi(-1) = -1, 2 \mid \alpha, \chi(a) \neq \pm 1; \\ \langle \tau_{q_1^\alpha} \sigma_{a_1^\alpha} \rangle, & \text{if } \chi(-1) = -1, 2 \nmid \alpha, \chi(a) \neq \pm 1. \end{cases}$$

$q_1 = \#\mathbb{F}_p(a^{(1-p)/2}), a_1 = a^{(1-q_1)/2}$  and  $\alpha$  is the order of  $\chi(a_1) \in \mu_{p-1}$ .

Consider the Kloosterman sums

$$S_k = \text{Kl}(\psi, \chi \circ N_{\mathbb{F}_{q^k}/\mathbb{F}_q}, q^k, a).$$

If  $p > \max(2n^{2dk} + 1)^2, (3n - 1)C_\chi - n$ , then  $\mathbb{Q}(S_k) = \mathbb{Q}(\mu_{pc})^H$ , where  $H$  consists of those  $\sigma_t \tau_w$  such that there exists an integer  $\beta$  and a character  $\eta$  on  $\mathbb{F}_q^\times$  satisfying

$$t = \lambda a_1^\beta, \lambda^{n_1} = 1, \quad \chi^w = \eta \chi^{q_1^\beta}, \quad \eta(a) = \gamma \cdot \prod \chi^w(t), \gamma^k = 1.$$

Thus  $\mathbb{Q}(S_k) = \mathbb{Q}(S_{k-c})$  since  $\gamma^c = 1$ .

The  $L$ -function

$$L(T) = \exp \left( \sum_{k=1}^{\infty} \frac{T^k}{k} S_k \right)$$

is a rational function. Thus the sequence  $S_k$  is linear recurrence sequence. The sequence  $\mathbb{Q}(S_k)_{k \geq N}$  is periodic of period  $r$  for some  $N$  (Wan, Yin). Thus if  $p > \max \left( 2n^{2d(N+r)} + 1 \right)^2, (3n-1)C_\chi - n$ , the generating field of  $S_k$  is determined by the previous equations for any  $k$ . For this purpose, we need to decrease the bound  $(2n^{2d} + 1)^2$  and estimate the period  $r$  and  $N$ . We conjecture that  $S_k$  has the predicted generating field if  $p > 3ndc$ .

*Thank you!*

