THE GENERATING FIELDS OF TWISTED KLOOSTERMAN SUMS

SHENXING ZHANG

Abstract. We use the Kloosterman sheaves constructed by Fisher to show when two twisted Kloosterman sums differ by a factor of a $(q-1)$-th root of unity, and use p-adic analysis to prove the non-vanishing of twisted Kloosterman sums. Then we determine generating fields of twisted Kloosterman sums by these results.

1. Introduction

1.1. **Background.** Let p be a prime number, $q = p^d$ a power of p, and $\mathbb{F}_q$ the field with q elements. Denote by $\mu_n \subseteq \overline{\mathbb{Q}}^\times$ the group of n-th roots of unity. Let $\psi : \mathbb{F}_p \to \mu_p$ be a fixed non-trivial additive character. For $\boldsymbol{\chi} = \{\chi_1, \dots, \chi_n\}$ an unordered n-tuple of multiplicative characters $\chi_i : \mathbb{F}_q^\times \to \mu_{q-1}$ and $a \in \mathbb{F}_q^\times$, define the *Kloosterman sum* as

$$\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a) = \sum_{\substack{x_1\cdots x_n = a \\ x_i \in \mathbb{F}_q^\times}} \chi_1(x_1)\cdots\chi_n(x_n)\psi\big(\mathrm{Tr}(x_1 + \cdots + x_n)\big),$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$. Clearly it lies in $\mathbb{Z}[\mu_{p(q-1)}]$.

When $\boldsymbol{\chi} = \mathbf{1} = \{1, \cdots, 1\}$ is trivial, the distinctness of Kloosterman sums is studied by many peoples. It's easy to see that

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

Fisher in [Fis92, Remark 4.28(2)] conjectured that the converse

$$\mathrm{Kl}_n(\psi, \mathbf{1}, q, a) = \mathrm{Kl}_n(\psi, \mathbf{1}, q, b) \implies a, b \text{ conjugate} \tag{1.1}$$

is also true if $p \geq nd$. It's known that (1.1) holds when $p > (2n^{2d}+1)^2$ in [Fis92], or $p \geq (d-1)n+2$ and p does not divide a certain integer in [Wan95, Theorem 1.3]. Once (1.1) holds, one can obtain that $\mathrm{Kl}_n(\psi, \mathbf{1}, q, a)$ generates $\mathbb{Q}(\mu_p)^H$, where

$$H = \Big\{ t \in \mathrm{Gal}\big(\mathbb{Q}(\mu_p)/\mathbb{Q}\big) \,\Big|\, \exists k \in \mathbb{Z} \text{ such that } t^n = a^{1-p^k} \Big\}.$$

1.2. **Notations and main results.** In this article, we will study the *generating fields* of twisted Kloosterman sums. We need the following notations:

- $c = c(\boldsymbol{\chi}) \mid (q-1)$ the minimal positive integer such that $\chi_i^c = 1, i = 1, \dots, n$, i.e., the least common multiplier of orders of χ_i.
- $\boldsymbol{\chi}^w := \{\chi_1^w, \cdots, \chi_n^w\}$, where $w \in \mathbb{Z}$ or $\mathbb{Z}/c\mathbb{Z}$.
- $\boldsymbol{\chi}\eta := \{\chi_1\eta, \cdots, \chi_n\eta\}$, where η is a multiplicative character.

Date: February 24, 2025.

2020 *Mathematics Subject Classification.* 11L05, 11L07, 11T23.

Key words and phrases. Kloosterman sums; Kloosterman sheaves; cyclotomic fields; algebraic numbers.

- $\boldsymbol{\chi} \circ \sigma := \{\chi_1 \circ \sigma, \cdots, \chi_n \circ \sigma\}$, where $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.
- $\prod \boldsymbol{\chi} := \chi_1 \cdots \chi_n$.

Clearly, the Galois group

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

where

$$\sigma_t(\zeta_p) = \zeta_p^t, \sigma_t(\zeta_c) = \zeta_c, \qquad \tau_w(\zeta_p) = \zeta_p, \tau_w(\zeta_c) = \zeta_c^w$$

for any $\zeta_p \in \mu_p, \zeta_c \in \mu_c$.

Theorem 1.1. *Assume that $p > \max\big\{(2n^{2d}+1)^2, (3n-1)c - n\big\}$ and for any i, j, $\chi_i = \chi_j$ if $\chi_i^n = \chi_j^n$. Then $\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a)$ generates $\mathbb{Q}(\mu_{pc})^H$, where H consists of those $\sigma_t\tau_w$ such that there exists an integer k and a character η satisfying*

$$t^n = a^{1-p^k}, \quad \boldsymbol{\chi}^w = \boldsymbol{\chi}^{p^k}\eta, \quad \eta(a) = \prod \boldsymbol{\chi}^w(t).$$

A basic observation tells that

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

To study the generating fields, we need to know when two twisted Kloosterman sums differ by a factor of some $\lambda \in \mu_{q-1}$. In § 2, we will recall the construction of Kloosterman sheaves by Fisher and show when two twisted Kloosterman sums differ by a factor of λ for sufficiently large p, see Theorem 2.7. We also need the non-vanishing of twisted Kloosterman sums, which will be proved by p-adic analysis in § 3. Then we will finish the proof in § 4 and end this paper with several examples in § 5.

2. Kloosterman sheaves and Fisher's descent

2.1. **Kloosterman sheaves.** Let $\ell \neq p$ be a prime and fix an embedding $\overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$. Then the additive and multiplicative characters ψ, χ_i can take value both in $\overline{\mathbb{Q}}_\ell$ or $\mathbb{C}$.

Deligne in [Del77, Theorem 7.8] and Katz in [Kat88, Theorem 4.11] defined the Kloosterman sheaf of $\overline{\mathbb{Q}}_\ell$-modules

$$\mathcal{K}\ell = \mathcal{K}\ell_{n,q}(\psi, \boldsymbol{\chi})$$

on $\mathbb{G}_{m/\mathbb{F}_q}$, with the following properties:

- $\mathcal{K}\ell$ is lisse of rank n and pure of weight $n-1$.
- For any $a \in \mathbb{F}_q^\times$, $\mathrm{Tr}(\mathrm{Frob}_a, \mathcal{K}\ell_{\overline{a}}) = (-1)^{n-1}\,\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a)$.
- $\mathcal{K}\ell$ is tame at 0.
- $\mathcal{K}\ell$ is totally wild with Swan conductor 1 at ∞. So all ∞-breaks are $1/n$.

Here Frob_a denotes the geometric Frobenius at a.

Definition 2.1. The n-tuple $\boldsymbol{\chi}$ is called *Kummer-induced* if there exists a non-trivial character Λ such that $\boldsymbol{\chi} = \boldsymbol{\chi}\Lambda$ as unordered n-tuples.

Remark 2.2. If $\boldsymbol{\chi}$ is Kummer-induced, then $\prod \boldsymbol{\chi} = \prod(\boldsymbol{\chi}\Lambda) = \Lambda^n \prod \boldsymbol{\chi}$, $\Lambda^n = 1$. Since

$$\mathrm{Kl}_n(\psi, \boldsymbol{\chi}\eta, q, a) = \eta(a)\,\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a),$$

we have $\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a) = 0$ if χ is Kummer-induced and $\Lambda(a) \neq 1$. See [Fis92, Remark 1.6].

Remark 2.3. When $\boldsymbol{\chi}$ is not Kummer-induced, $\mathcal{K}\ell$ is not *geometrically Kummer-induced*. That's to say, $\mathcal{K}\ell \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}$ is not of type $(t \mapsto t^N)_*\mathcal{F}$ for some integer $N > 1$ and some lisse sheaf $\mathcal{F}$ on $\mathbb{G}_{m/\overline{\mathbb{F}}_p}$. See [Fis92, Theorem 2.9].

2.2. **Fisher's descent.** In [Fis92, Theorem 3.12], Fisher gave a descent of Kloosterman sheaves along an extension of finite fields. For any $a \in \mathbb{F}_q^\times$, he defined a lisse sheaf $\mathcal{F}_a(\boldsymbol{\chi})$ on $\mathbb{G}_m = \mathbb{G}_{m/\mathbb{F}_p}$, such that

$$\mathcal{F}_a(\boldsymbol{\chi}) \mid \mathbb{G}_{m/\mathbb{F}_q} = \bigotimes_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \big(t \mapsto \sigma(a)t^n\big)^* \mathcal{K}\ell_{n,q}(\psi \circ \sigma^{-1}, \boldsymbol{\chi} \circ \sigma^{-1}).$$

Moreover,

- $\mathcal{F}_a(\boldsymbol{\chi})$ is lisse of rank n^d and pure of weight $d(n-1)$.
- For any $t \in \mathbb{F}_p^\times$, $\mathrm{Tr}\big(\mathrm{Frob}_t, \mathcal{F}_a(\boldsymbol{\chi})_{\bar{t}}\big) = (-1)^{(n-1)d}\,\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, at^n)$.
- $\mathcal{F}_a(\boldsymbol{\chi})$ is tame at 0 and its ∞-breaks are at most 1.

2.3. **Distinctness.** We will consider when

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

for some $\lambda \in \mu_{q-1}$. The argument almost follows [Fis92], while $\lambda = 1$ in his paper.

For a lisse sheaf $\mathcal{F}$ on $\mathbb{G}_m$, denote by $G_{\mathrm{geom}}(\mathcal{F})$ the geometric monodromy group of $\mathcal{F}$, i.e., the Zariski closure of $\pi_1(\mathbb{G}_{m/\overline{\mathbb{F}}_p})$ in $\mathrm{GL}(\mathcal{F})$. Let $G_{\mathrm{geom}}(\mathcal{F})^\circ$ be the connected component of $G_{\mathrm{geom}}(\mathcal{F})$ and $\mathfrak{g}(\mathcal{F})$ its Lie algebra.

Proposition 2.4 ([Fis92, Proposition 4.18])**.** *Assume that $p > 2n+1$ and $\boldsymbol{\chi}$ is not Kummer-induced.*

1. *As a representation of $\mathfrak{g}\big(\mathcal{F}_a(\boldsymbol{\chi})\big)$, $\mathcal{F}_a(\boldsymbol{\chi})$ has a highest weight $\lambda_a(\boldsymbol{\chi})$ with multiplicity one.*
2. *$\mathcal{F}_a(\boldsymbol{\chi})$ has a geometrically irreducible sub-sheaf $\mathcal{G}_a(\boldsymbol{\chi})$, such that as a representation of $\mathfrak{g}\big(\mathcal{F}_a(\boldsymbol{\chi})\big)$, $\mathcal{G}_a(\boldsymbol{\chi})$ is an irreducible sub-representation with unique highest weight $\lambda_a(\boldsymbol{\chi})$. Moreover, $\mathcal{G}_a(\boldsymbol{\chi}) \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}$ occurs exactly once in $\mathcal{F}_a(\boldsymbol{\chi}) \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}$.*

The multiplicative character χ can be viewed as a character on $\mathbb{F}_p$-points of $\mathbb{B}^\times = \mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_p}\mathbb{G}_m$. It gives a rank one lisse sheaf on $\mathbb{B}^\times$ constructed from the Lang torsor as in [Kat88, §4.3]. Denote by $\mathcal{L}_\psi$ its restriction on $\mathbb{G}_m$. Similarly, the additive character ψ gives a rank one lisse sheaf on $\mathbb{G}_{a/\mathbb{F}_p}$. Denote by $\mathcal{L}_\psi$ its restriction on $\mathbb{G}_m$. For any $t \in \mathbb{F}_p^\times$,

$$\mathrm{Tr}\big(\mathrm{Frob}_t, (\mathcal{L}_\chi)_{\bar{t}}\big) = \chi(t), \quad \mathrm{Tr}\big(\mathrm{Frob}_t, (\mathcal{L}_\psi)_{\bar{t}}\big) = \psi(t).$$

Lemma 2.5 ([Fis92, Lemma 4.9])**.** *Let $\mathcal{F}, \mathcal{F}'$ be lisse sheaves on $\mathbb{G}_m$ of same rank r and pure of the same weight w. Assume that for any $t \in \mathbb{F}_p^\times$,*

$$\mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}_{\bar{t}}) = \mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}'_{\bar{t}}).$$

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

Proposition 2.6 ([Fis92, Corollary 4.20])**.** *Let $a, b \in \mathbb{F}_q^\times$ and let $\boldsymbol{\chi}, \boldsymbol{\rho}$ be n-tuples of multiplicative characters $\chi_i, \rho_j : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}_\ell^\times$ respectively. Assume that $p > (2n^{2d}+1)^2$, $\boldsymbol{\chi}$ is not Kummer-induced and there is $\lambda \in \mu_{q-1}$ such that*

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

Then $\mathcal{G}_a(\boldsymbol{\chi}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\chi}}} \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}$ occurs at least once in $\mathcal{F}_b(\boldsymbol{\rho}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\rho}}} \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}$.

Proof. Denote by

$$\mathcal{F} = \mathcal{F}_a(\boldsymbol{\chi}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\chi}}}, \quad \mathcal{F}' = \mathcal{F}_b(\boldsymbol{\rho}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\rho}}}, \quad \mathcal{G} = \mathcal{G}_a(\boldsymbol{\chi}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\chi}}}.$$

For any $t \in \mathbb{F}_p^\times$, we have $\sigma_t \lambda = \lambda$. Since

$$\sigma_t\big(\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a)\big) = \prod \overline{\boldsymbol{\chi}}(t) \cdot \mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, at^n) = (-1)^{(n-1)d}\, \mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}_{\overline{t}}),$$
$$\sigma_t\big(\mathrm{Kl}_n(\psi, \boldsymbol{\rho}, q, b)\big) = \prod \overline{\boldsymbol{\rho}}(t) \cdot \mathrm{Kl}_n(\psi, \boldsymbol{\rho}, q, bt^n) = (-1)^{(n-1)d}\, \mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}'_{\overline{t}}),$$

we have $\mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}_{\overline{t}}) = \lambda\, \mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}'_{\overline{t}})$.

Let $V = \overline{\mathbb{Q}}_\ell \cdot e$ with $\mathrm{Frob}_p \cdot e = \lambda e$, where $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ denotes the geometric Frobenius. Denote by $\mathcal{L}_0$ the sheaf on $\mathrm{Spec}\,\mathbb{F}_p$ corresponding to this module and let $\mathcal{L}$ be its pulling-back along $\mathbb{G}_m \to \mathrm{Spec}\,\mathbb{F}_p$. Then for any $t \in \mathbb{F}_p^\times$,

$$\mathrm{Tr}(\mathrm{Frob}_t, \mathcal{L}_{\overline{t}}) = \mathrm{Tr}(\mathrm{Frob}_p, \mathcal{L}_0) = \lambda, \quad \mathrm{Tr}\big(\mathrm{Frob}_t, (\mathcal{F}' \otimes \mathcal{L})_{\overline{t}}\big) = \mathrm{Tr}(\mathrm{Frob}_t, \mathcal{F}_{\overline{t}}).$$

Since $\mathcal{L} \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}$ is trivial, the result then follows by applying Lemma 2.5 to sheaves $\mathcal{F}, \mathcal{F}' \otimes \mathcal{L}, \mathcal{G}$ with $r = s = n^d$, $M_0 = 0$ and $M_\infty \le 1$. ☐

Theorem 2.7. *Let $a, b \in \mathbb{F}_q^\times$ and let $\boldsymbol{\chi}, \boldsymbol{\rho}$ be n-tuples of multiplicative characters. Assume that $\boldsymbol{\chi}, \boldsymbol{\rho}$ 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*

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

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

Here, Λ_2 denotes the non-trivial quadratic character of $\mathbb{F}_q^\times$.

Proof. Denote by

$$\mathcal{H} = \mathcal{K}\ell_{n,q}(\psi, \boldsymbol{\chi}) \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p} \quad \text{and} \quad \mathcal{K} = \mathcal{K}\ell_{n,q}(\psi, \boldsymbol{\rho}) \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}.$$

By our assumptions, $\mathcal{H}$ and $\mathcal{K}$ are not Kummer-induced by [Fis92, Theorem 2.9].

By applying [Kat90, Theorems 8.8.1, 8.11.3] with $n = 4, m = 0$, we obtain that $G_{\mathrm{geom}}(\mathcal{H})^\circ = \mathrm{SO}(4)$ if and only if there is a multiplicative character η such that $\boldsymbol{\chi} = \overline{\boldsymbol{\chi}}\eta = \boldsymbol{\chi}^{-1}\eta$ as unordered 4-tuples and $\prod \boldsymbol{\chi} = \Lambda_2\eta^2$. In which case, there is a permutation $\varepsilon \in S_4$ such that $\chi_i\chi_{\varepsilon(i)} = \eta$.

- If $\varepsilon = 1$, then $\chi_i^2 = \eta$, $\chi_i = \chi_1$ or $\chi_1\Lambda_2$. Since $\prod \boldsymbol{\chi} = \Lambda_2\eta^2$, we have $\boldsymbol{\chi} = \{1, 1, 1, \Lambda_2\}\chi_1$ or $\{1, 1, 1, \Lambda_2\}\chi_1\Lambda_2$.
- If $\varepsilon = (1234)$ or $(12)(34)$, then $\chi_1\chi_2 = \chi_3\chi_4 = \eta$, which contradicts to $\prod \boldsymbol{\chi} = \Lambda_2\eta^2$.
- If $\varepsilon = (123)$, then $\chi_1\chi_2 = \chi_2\chi_3 = \chi_3\chi_1 = \eta$, $\chi_1 = \chi_2 = \chi_3$. Since $\prod \boldsymbol{\chi} = \Lambda_2\eta^2 = \Lambda_2\chi_1^4$, we have $\chi_4 = \chi_1\Lambda_2$ and $\boldsymbol{\chi} = \{1, 1, 1, \Lambda_2\}\chi_1$.

- If $\varepsilon = (12)$, then $\chi_1\chi_2 = \eta, \chi_3^2 = \chi_4^2 = \eta$. Since $\prod \boldsymbol{\chi} = \Lambda_2\eta^2, \chi_3\chi_4 = \Lambda_2\eta = \Lambda_2\chi_3^2$, we have $\chi_4 = \Lambda_2\chi_3$. Therefore,
$$\boldsymbol{\chi} = \{\chi_1, \chi_3^2\chi_1^{-1}, \chi_3, \chi_3\Lambda_2\} = \{\chi_1\chi_3^{-1}, \chi_1^{-1}\chi_3, 1, \Lambda_2\}\chi_3.$$
- The remaining cases can be discussed similarly.

Since the form of χ contradicts our assumptions, we have $G_{\mathrm{geom}}(\mathcal{H})^\circ \neq \mathrm{SO}(4)$. Similarly, $G_{\mathrm{geom}}(\mathcal{K})^\circ \neq \mathrm{SO}(4)$.

The following argument follows from [Fis92, Theorem 4.22]. For $a \in \overline{\mathbb{F}}_p^\times$, denote by $T_a : t \mapsto at$ a translation on $\mathbb{G}_{m/\overline{\mathbb{F}}_p}$ and
$$\mathcal{H}_\sigma := T^*_{\sigma(a)}(\mathcal{H} \circ \sigma^{-1}), \quad \mathcal{K}_\tau := T^*_{\tau(b)}(\mathcal{K} \circ \tau^{-1}).$$
Let G be the geometric monodromy group of
$$\bigoplus_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \mathcal{H}_\sigma \oplus \bigoplus_{\tau \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \mathcal{K}_\tau,$$
and $\mathfrak{g}$ the Lie algebra of G°. Since $G_{\mathrm{geom}}(\mathcal{H}) \neq \mathrm{SO}(4)$, we have $G_{\mathrm{geom}}(\mathcal{H}_\sigma) \neq \mathrm{SO}(4)$ for any σ. This implies that $\mathfrak{g}(\mathcal{H}_\sigma)$ is simple. Let λ_σ (resp. μ_τ) denote the highest weight of $\mathcal{H}_\sigma$ (resp. $\mathcal{K}_\tau$). Since
$$\mathcal{F}_a(\boldsymbol{\chi}) \mid \mathbb{G}_{m/\mathbb{F}_q} = \bigotimes_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \big(t \mapsto t^n\big)^* \mathcal{H}_\sigma,$$
we have $\lambda_a(\boldsymbol{\chi}) = \sum_\sigma \lambda_\sigma, \lambda_b(\boldsymbol{\rho}) = \sum_\tau \mu_\tau$. By Proposition 2.6, we have
$$\mathcal{G}_a(\boldsymbol{\chi}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\chi}}} \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p} \hookrightarrow \mathcal{F}_b(\boldsymbol{\rho}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\rho}}} \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p},$$
$$\mathcal{G}_b(\boldsymbol{\rho}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\rho}}} \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p} \hookrightarrow \mathcal{F}_a(\boldsymbol{\chi}) \otimes \mathcal{L}_{\prod \overline{\boldsymbol{\chi}}} \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}.$$
Since as representations of $\mathfrak{g}$, $\mathcal{G}_a(\boldsymbol{\chi}), \mathcal{F}_a(\boldsymbol{\chi})$ have the highest weight $\lambda_a(\boldsymbol{\chi})$, $\mathcal{G}_b(\boldsymbol{\rho}), \mathcal{F}_b(\boldsymbol{\rho})$ have the highest weight $\lambda_b(\boldsymbol{\rho})$, we have $\lambda_a(\boldsymbol{\chi}) = \lambda_b(\boldsymbol{\rho})$. Since λ_σ, μ_τ are fundamental weights, this implies that there is a σ such that $\lambda_\sigma = \mu_1$. Therefore, $\mathcal{H}_\sigma \cong \mathcal{K}_1$ as representations of $\mathfrak{g}$, and $\mathcal{H}_\sigma \otimes \mathcal{L} \cong \mathcal{K}_1$ as sheaves on $\mathbb{G}_{m/\overline{\mathbb{F}}_p}$ for some $\mathcal{L}$. By [Kat90, Lemma 8.11.7.1], $\mathcal{L} = \mathcal{L}_\eta$ for some tame character η. Hence
$$T_b^*\mathcal{K} \cong \mathcal{L}_\eta \otimes T^*_{\sigma(a)}(\mathcal{H} \circ \sigma^{-1}) = \mathcal{L}_\eta \otimes T^*_{\sigma(a)}\, \mathcal{K}\ell_{n,q}(\psi, \boldsymbol{\chi} \circ \sigma^{-1}) \mid \mathbb{G}_{m/\overline{\mathbb{F}}_p}.$$
By [Fis92, Lemma 4.11], we have $b = \sigma(a)$ and $\boldsymbol{\rho} = (\boldsymbol{\chi} \circ \sigma^{-1})\eta$ as unordered tuples. This implies that
$$\mathrm{Kl}_n(\psi, \boldsymbol{\rho}, q, b) = \eta(b)\, \mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a).$$
Hence both Kloosterman sums vanish or $\eta(b) = \lambda^{-1}$. □

Remark 2.8. In [Fis92, Corollary 4.27], Fisher showed that if $p > (2n^{4d}+1)^2$ and
$$|\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a)| = |\mathrm{Kl}_n(\psi, \boldsymbol{\rho}, q, b)|,$$
then $b = \sigma(a), \boldsymbol{\rho} = (\boldsymbol{\chi} \circ \sigma^{-1})\eta$, or $b = (-1)^n\sigma(a), \boldsymbol{\rho} = (\boldsymbol{\chi}^{-1} \circ \sigma^{-1})\eta$.

Corollary 2.9. *Keeping the hypotheses of Theorem 2.7. Assume that $\boldsymbol{\chi}$ is defined over $\mathbb{F}_p$, that's to say, $\boldsymbol{\chi} = \boldsymbol{\chi}_0 \circ \mathbf{N}_{\mathbb{F}_q/\mathbb{F}_p}$ for some n-tuple $\boldsymbol{\chi}_0$ of characters on $\mathbb{F}_p^\times$. If*
$$\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a) = \lambda\, \mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, b), \quad \lambda \in \mu_{q-1},$$
then $b = \sigma(a)$ for some $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, and $\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a) = \mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, b)$.

Proof. In this case, we have $\boldsymbol{\chi} = \boldsymbol{\chi}\eta$ and then $\eta = 1$. The result then follows easily. □

3. The non-vanishing of Kloosterman sums

The case $n=1$ is trivial. We will assume that $n\geq 2$ in this section.

Theorem 3.1. *Assume that $p>(3n-1)c-n$ and for any i,j, $\chi_i=\chi_j$ if $\chi_i^n=\chi_j^n$. Then $\mathrm{Kl}_n(\psi,\boldsymbol{\chi},q,a)$ is nonzero.*

Proof. Let $\mathfrak{p}$ be a prime above p in $\mathbb{Q}(\mu_{q-1})$ and $\mathfrak{P}$ the unique prime above $\mathfrak{p}$ in $\mathbb{Q}(\mu_{(q-1)p})$. Let v be the normalized $\mathfrak{P}$-adic valuation. Once we fix an isomorphism from $\mathbb{F}_q$ to the residue field of $\mathbb{Q}(\mu_{q-1})$ at $\mathfrak{p}$, the Teichmüller lifting of the residue map at $\mathfrak{p}$ gives a primitive character ω of $\mathbb{F}_q^\times$. Denote by

$$g(m):=\sum_{t\in\mathbb{F}_q^\times}\omega^{-m}(t)\psi\big(\mathrm{Tr}(t)\big)$$

the *Gauss sum*. Then the Stickelberger's congruence theorem tells that

$$v\big(g(m)\big)=\sum_{j=0}^{d-1}m_j, \tag{3.1}$$

where

$$0\leq m\leq q-2,\quad m=\sum_{j=0}^{d-1}m_jp^j,\ 0\leq m_j\leq p-1,$$

see [Sti90] or [Was97, Chapter 6].

For each $i\in\{1,2,\dots,n\}$, there is s_i such that $\chi_i=\omega^{-s_i}$. Take $x=x_1\cdots x_na^{-1}$ in the identity

$$\sum_{m=0}^{q-2}\omega^{-m}(x)=\begin{cases}q-1, & \text{if } x=1;\\ 0, & \text{if } x\neq 1,\end{cases}$$

we get

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

There is a unique m such that $v\big(\prod_{i=1}^n g(m+s_i)\big)$ is minimal by Proposition 3.2. This implies that $\mathrm{Kl}_n(\psi,\boldsymbol{\chi},q,a)$ is nonzero. □

We may assume that $1\leq s_i\leq q-1$ (notice the bound). Write

$$s_i=\sum_{j=0}^{d-1}s_{ij}p^j$$

with $0\leq s_{ij}\leq p-1$.

Proposition 3.2. *Assume that $p>(3n-1)c-n$ and for any i,j, $\chi_i=\chi_j$ if $\chi_i^n=\chi_j^n$. Then there is a unique $0\leq m\leq q-2$ such that $v\big(\prod_{i=1}^n g(m+s_i)\big)$ is minimal.*

Proof. Since $c(\boldsymbol{\chi}\chi_1^{-1})\leq c(\boldsymbol{\chi})$, we may assume that $\chi_1=1, s_1=q-1$ for simplicity.

Step 1: express the valuation in terms of m_{ij} and s_{ij}.

For each $i \in \{1, 2, \ldots, n\}$, let $\epsilon_{i,-1} \in \{0, 1\}$ be the integer part of $(m+s_i)/(q-1)$. Then we may write

$$m + s_i - (q-1)\epsilon_{i,-1} = \sum_{j=0}^{d-1} m_{ij} p^j, \quad 0 \le m_{ij} \le p-1.$$

By the Stickelberger's congruence theorem (3.1), we have

$$v\Big(\prod_{i=1}^{n} g(m+s_i)\Big) = \sum_{i=1}^{n} \sum_{j=0}^{d-1} m_{ij}. \tag{3.2}$$

Note that

$$m + s_i - (q-1)\epsilon_{i,-1} = \sum_{j=0}^{d-1} (m_j + s_{ij}) p^j - (q-1)\epsilon_{i,-1}.$$

For each $j \in \{0, 1, 2, \ldots, d-1\}$, denote by ϵ_{ij} the integer part of $(m_j + s_{ij} + \epsilon_{i,j-1})/p$ inductively. Then $\epsilon_{ij} \in \{0, 1\}$ and

$$\begin{aligned} &\sum_{j=0}^{d-1} (m_j + s_{ij} + \epsilon_{i,j-1} - p\epsilon_{ij}) p^j \\ =& m + s_i + \epsilon_{i,-1} - q\epsilon_{i,d-1} \\ =& \sum_{j=0}^{d-1} m_{ij} p^j + q(\epsilon_{i,-1} - \epsilon_{i,d-1}). \end{aligned}$$

Since both the left-hand side and $\sum_{j=0}^{d-1} m_{ij} p^j$ lie in the interval $[0, q-2]$, we have

$$m_{ij} = m_j + s_{ij} + \epsilon_{i,j-1} - p\epsilon_{ij}$$

and $\epsilon_{i,d-1} = \epsilon_{i,-1}$.

Step 2: express the valuation in terms of $s_{\sigma_j(u_j),j}$.

There exists a permutation $\sigma_j \in S_n$ such that

$$s_{\sigma_j(1),j} \ge s_{\sigma_j(2),j} \ge \cdots \ge s_{\sigma_j(n),j}. \tag{3.3}$$

If $s_{ij} = s_{i'j}$, then by Lemma 3.3, $\chi_i^n = \chi_{i'}^n$, $\chi_i = \chi_{i'}$ and $\epsilon_{ij} = \epsilon_{i'j}$. If $s_{ij} > s_{i'j}$, then

$$s_{ij} + \epsilon_{i,j-1} \ge s_{i'j} + \epsilon_{i',j-1} \quad \text{and} \quad \epsilon_{ij} \ge \epsilon_{i'j}.$$

In other words, $\{\epsilon_{ij}\}_i$ and $\{s_{ij} + \epsilon_{i,j-1}\}_i$ have the same orderings as (3.3). Therefore, there exists $0 \le u_j \le n$ such that

$$\epsilon_{\sigma_j(1),j} = \cdots = \epsilon_{\sigma_j(u_j),j} = 1, \quad \epsilon_{\sigma_j(u_j+1),j} = \cdots = \epsilon_{\sigma_j(n),j} = 0.$$

This implies that

$$m_{\sigma_j(1),j} \ge \cdots \ge m_{\sigma_j(u_j),j}, \quad m_{\sigma_j(u_j+1),j} \ge \cdots \ge m_{\sigma_j(n),j}.$$

Note that $s_1 = q-1, s_{1j} = p-1$ and $\epsilon_{1,-1} = 1$. One can show that $\epsilon_{1,j} = 1$ inductively, which means $u_j \ne 0$. If $u_j \ne n$ and $m_{\sigma_j(u_j),j} \ge m_{\sigma_j(n),j}$, then

$$0 \ge s_{\sigma_j(u_j),j} + \epsilon_{\sigma_j(u_j),j} - p \ge s_{\sigma_j(n),j} + \epsilon_{\sigma_j(n),j} \ge 0,$$

which forces that

$$s_{\sigma_j(u_j),j} = p-1, \epsilon_{\sigma_j(u_j),j} = 1, \quad s_{\sigma_j(n),j} = \epsilon_{\sigma_j(n),j} = 0.$$

By Lemma 3.3, this implies that $\chi^n_{\sigma_j(u_j)} = \chi^n_{\sigma_j(n)}$. Then $\chi_{\sigma_j(u_j)} = \chi_{\sigma_j(n)}$ and $\epsilon_{\sigma_j(u_j),j} = \epsilon_{\sigma_j(n),j}$, which is impossible. Hence

$$m'_j := m_{\sigma_j(u_j),j} = m_j + s_{\sigma_j(u_j),j} + \epsilon_{\sigma_j(u_j),j-1} - p$$

is the unique minimum among $\{m_{1j}, m_{2j}, \ldots, m_{nj}\}$. Therefore, the valuation (3.2) becomes

$$\begin{aligned}
\sum_{i,j} m_{ij} &= \sum_{i,j}\big(m_j + s_{ij} + \epsilon_{i,j-1} - p\epsilon_{ij}\big)\\
&= \sum_{i,j}\big(m'_j - s_{\sigma_j(u_j),j} - \epsilon_{\sigma_j(u_j),j-1} + p + s_{ij} + \epsilon_{i,j-1} - p\epsilon_{ij}\big)\\
&= ndp + \sum_j\Big(\sum_i s_{ij} + n\big(m'_j - s_{\sigma_j(u_j),j} - \epsilon_{\sigma_j(u_j),j-1}\big) + u_{j-1} - pu_j\Big)\\
&= ndp + \sum_{i,j} s_{ij} + n\sum_j\Big(m'_j - s_{\sigma_j(u_j),j} - \frac{p-1}{n}u_j - \epsilon_{\sigma_j(u_j),j-1}\Big). \qquad (3.4)
\end{aligned}$$

Here, $u_{-1} := \sum_{i=1}^d \epsilon_{i,-1} = u_{d-1}$.

Step 3: find the minimal valuation.

If

$$\Big|\big(s_{\sigma_j(i),j} + \frac{p-1}{n}i\big) - \big(s_{\sigma_j(i'),j} + \frac{p-1}{n}i'\big)\Big| \le 1,$$

then by Lemma 3.3, $\chi^n_{\sigma_j(i)} = \chi^n_{\sigma_j(i')}$, $\chi_{\sigma_j(i)} = \chi_{\sigma_j(i')}$, $s_{\sigma_j(i),j} = s_{\sigma_j(i'),j}$. This implies that $i = i'$ because $(p-1)/n > 1$. Therefore, there exists a unique U_j such that

$$s_{\sigma_j(U_j),j} + \frac{p-1}{n}U_j = \max_{1\le i\le n}\Big\{s_{\sigma_j(i),j} + \frac{p-1}{n}i\Big\}.$$

Moreover,

$$s_{\sigma_j(U_j),j} + \frac{p-1}{n}U_j > s_{\sigma_j(i),j} + \frac{p-1}{n}i + 1 \qquad (3.5)$$

for any $i \neq U_j$.

Write

$$E_{\sigma_j(1),j} = \cdots = E_{\sigma_j(U_j),j} = 1, \quad E_{\sigma_j(U_j+1),j} = \cdots = E_{\sigma_j(n),j} = 0.$$

If m is

$$M = \sum_{j=0}^{d-1} M_j p^j, \text{ where } M_j = p - s_{\sigma_j(U_j),j} - E_{\sigma_j(U_j),j-1},$$

then $m'_j = 0, \epsilon_{ij} = E_{ij}$ and $u_j = U_j$. Denote by V the corresponding valuation (3.2) for $m = M$.

If all $u_j = U_j$, then $\epsilon_{ij} = E_{ij}$ and

$$\sum_{i,j} m_{ij} = V + n\sum_j m'_j \ge V.$$

The equality holds if and only if all $m'_j = 0$, i.e., $m = M$. If there exists j such that $u_j \neq U_j$, then by (3.4) and (3.5), we have

$$\begin{aligned}
&\frac{1}{n}\Big(\sum_{i,j} m_{ij} - V\Big)\\
&=\sum_j\Big(m'_j - s_{\sigma_j(u_j),j} - \frac{p-1}{n}u_j - \epsilon_{\sigma_j(u_j),j-1}\Big)\\
&\qquad -\sum_j\Big(-s_{\sigma_j(U_j),j} - \frac{p-1}{n}U_j - E_{\sigma_j(U_j),j-1}\Big)\\
&\geq \sum_j\Big(s_{\sigma_j(U_j),j} + \frac{p-1}{n}U_j - s_{\sigma_j(u_j),j} - \frac{p-1}{n}u_j + E_{\sigma_j(U_j),j-1} - \epsilon_{\sigma_j(u_j),j-1}\Big)\\
&\geq \sum_{u_j\neq U_j}\Big(s_{\sigma_j(U_j),j} + \frac{p-1}{n}U_j - s_{\sigma_j(u_j),j} - \frac{p-1}{n}u_j - 1\Big) > 0.
\end{aligned}$$

Hence the valuation (3.2) is minimal if and only if $m = M$. □

Lemma 3.3. *Assume that $p > (3n-1)c - n$. If $\chi_i^n \neq \chi_{i'}^n$, then for each j, there is no integer $0 \leq \alpha \leq n$ such that $|s_{ij} - s_{i'j} - \frac{p-1}{n}\alpha| \leq 1$.*

Proof. There exist integers r, r' such that

$$s_i = \frac{(q-1)r}{c}, \quad s_{i'} = \frac{(q-1)r'}{c}.$$

Then

$$s_{ij} = \frac{a_{j+1}p - a_j}{c}, \quad s_{i'j} = \frac{a'_{j+1}p - a'_j}{c},$$

where $a_j \equiv rp^{-j}, a'_j \equiv r'p^{-j} \bmod c$ with $1 \leq a_j, a'_j \leq c$. Let $a''_j := a_j - a'_j$. Then $|a''_j| \leq c-1$.

If

$$\frac{p-1}{n}\alpha + t = s_{ij} - s_{i'j} = \frac{a''_{j+1}p - a''_j}{c}$$

for an integer $0 \leq \alpha \leq n$ and a real number t with $|t| \leq 1$, then

$$\big(na''_{j+1} - \alpha c\big)p = na''_j - \alpha c + nct.$$

There are three cases:

- If $na''_{j+1} - \alpha c \neq 0$ and $\alpha = n$, then $a''_{j+1} \neq c$,

  $$p \leq |(a''_{j+1} - c)p| = |a''_j - c + ct| \leq 3c - 1 \leq (3n-1)c - n$$

  since $n \geq 2$.
- If $na''_{j+1} - \alpha c \neq 0$ and $\alpha < n$, then

  $$p \leq \big|na''_j - \alpha c + nct\big| \leq n(c-1) + c(n-1) + nc \leq (3n-1)c - n.$$

- If $na''_{j+1} - \alpha c = 0$, then $n(r-r') \equiv n(a_{j+1} - a'_{j+1})p^{j+1} = \alpha c p^{j+1} \equiv 0 \bmod c$. That is to say, $\chi_i^n = \chi_{i'}^n$.

These finish the proof. □

Remark 3.4. When $n = 2$, $p > 3c - 2$ is enough by a careful estimation. See [Zha21, Lemma 3.4, Proposition 3.6].

4. Proof of the main theorem

Theorem 4.1. *Assume that* $p > \max\{(2n^{2d}+1)^2, (3n-1)c-n\}$ *and for any* i, j, $\chi_i = \chi_j$ *if* $\chi_i^n = \chi_j^n$*. Then* $\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a)$ *generates* $\mathbb{Q}(\mu_{pc})^H$*, where* H *consists of those* $\sigma_t\tau_w$ *such that there exists an integer* k *and a character* η *satisfying*

$$t^n = a^{1-p^k}, \quad \boldsymbol{\chi}^w = \boldsymbol{\chi}^{p^k}\eta, \quad \eta(a) = \prod \boldsymbol{\chi}^w(t).$$

Proof. Note that if $\boldsymbol{\chi}$ is Kummer-induced, then there is a non-trivial character Λ such that $\boldsymbol{\chi} = \boldsymbol{\chi}\Lambda$ and $\Lambda^n = 1$. Thus there exists $i \neq j$ such that $\chi_i = \chi_j\Lambda$ and $\chi_i^n = \chi_j^n$, which contradicts to our assumptions. Certainly, $\boldsymbol{\chi} = (\xi_1, \xi_1^{-1}, 1, \Lambda_2)\xi_2$ is also impossible.

By Theorems 2.7, 3.1 and the fact that

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

we have that $\sigma_t\tau_w$ fixes $\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a)$ if and only if

$$at^n = \sigma(a), \quad \boldsymbol{\chi}^w = (\boldsymbol{\chi}\circ\sigma^{-1})\eta, \quad \eta\big(\sigma(a)\big) = \prod \boldsymbol{\chi}^w(t)$$

for some $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and character η. Write $\sigma(x) = x^{p^{-k}}$. Since $t^p = t$, we have

$$t^n = t^{np^k} = \big(\sigma(a)/a\big)^{p^k} = a^{1-p^k},$$

$$\eta(a) = \eta\big(\sigma(a)\big)^{p^k} = \prod \boldsymbol{\chi}^w(t^{p^k}) = \prod \boldsymbol{\chi}^w(t)$$

and $\boldsymbol{\chi}^w = \boldsymbol{\chi}^{p^k}\eta$. □

Remark 4.2. Denote by $\alpha = \gcd(k, d)$ and $\lambda := a^{p^\alpha - 1}$. Since the order of a divides

$$\gcd\big((p^k-1)(p-1), p^d-1\big) = (p^\alpha - 1)\gcd\big(p-1, \frac{p^d-1}{p^\alpha-1}\big) = (p^\alpha-1)\gcd\big(p-1, \frac{d}{\alpha}\big),$$

we have $\lambda^{d/\alpha} = 1$. If $\lambda \neq 1$, then

$$\mathrm{Tr}(a) = \big(1 + \lambda + \cdots + \lambda^{\frac{d}{\alpha}-1}\big)\cdot\big(a + a^p + \cdots + a^{p^{\alpha-1}}\big) = 0.$$

Hence, $\mathrm{Tr}(a) \neq 0$ implies that $\lambda = 1, t^n = a^{1-p^k} = 1$. If moreover $\boldsymbol{\chi} = \mathbf{1}$, then

$$H = \big\{t \in \mathrm{Gal}\big(\mathbb{Q}(\mu_p)/\mathbb{Q}\big) \,\big|\, t^n = 1\big\}.$$

In fact, this holds for any p, see [Wan95]. See also [KRV11] for an attempt on a weaker condition.

Remark 4.3. Consider the Kloosterman sums

$$S_m = \mathrm{Kl}(\psi, \boldsymbol{\chi}\circ\mathbf{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}, q^m, a).$$

The L-function

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

is a rational function over $\mathbb{Q}(\mu_{p(q-1)})$ by the Dwork-Bombieri-Grothendick rationality theorem. Thus the sequence $\{S_m\}_m$ is a linear recurrence sequence. As shown in [WY20, Theorem 3], the sequence $\{\mathbb{Q}(S_m)\}_{m\geq N}$ is periodic of period r for some r, N.

Assume that for any i, j, $\chi_i = \chi_j$ if $\chi_i^n = \chi_j^n$. By Theorem 1.1, if $p > \max\{(2n^{2dm}+1)^2, (3n-1)c-n\}$, then $\mathbb{Q}(S_m) = \mathbb{Q}(\mu_{pc})^H$, where H consists of those $\sigma_t\tau_w$ such that there exists an integer k and a character η on $\mathbb{F}_q^\times$ satisfying

$$t^n = a^{1-p^k}, \quad \boldsymbol{\chi}^w = \boldsymbol{\chi}^{p^k}\eta, \quad \eta(a) = \gamma \cdot \prod \boldsymbol{\chi}^w(t) \text{ with } \gamma^m = 1. \tag{4.1}$$

Hence $\mathbb{Q}(S_m) = \mathbb{Q}(S_{m-c})$ since $\gamma^c = 1$.

If $p > \max\left\{\left(2n^{2d(N+r)}+1\right)^2, (3n-1)c-n\right\}$, then the generating field of S_m is determined by (4.1) for any m. But unfortunately, we do not have a bound on N. We roughly guess that S_m has the predicted generating field if $p > 3ndc$.

5. Examples

Denote by $n_0 := (n, p-1), d_0$ the degree of $a^{(1-p)/n_0}$ and

$$a_0 := \mathbf{N}_{\mathbb{F}_{p^{d_0}}/\mathbb{F}_p}\left(a^{(1-p)/n_0}\right) = a^{(1-p^{d_0})/n_0}.$$

Since

$$\left(a^{(1-p)/n_0}\right)^{p^k-1} = t^{(p-1)n/n_0} = 1,$$

we have $k = d_0\beta$ for some integer β. Moreover,

$$t^n = a^{1-p^k} = a_0^{n_0(1-p^k)/(1-p^{d_0})} = a_0^{n_0\beta}.$$

5.1. The case $n = 2$.

Proposition 5.1. *Let $\boldsymbol{\chi} = \{1, \chi\}$, where χ is a multiplicative character of order $c \neq 2$. If $p > \max\{(2^{2d+1}+1)^2, 5c-2\}$, then $\mathrm{Kl}(\psi, \boldsymbol{\chi}, p^d, a)$ generates $\mathbb{Q}(\mu_{pc})^H$, where*

$$H = \begin{cases} \langle \tau_{q_0}\sigma_{a_0}, \sigma_{-1}, \tau_{-1}\rangle, & \text{if } \chi(-1) = 1, \chi(a) = 1; \\ \langle \tau_{-q_0}\sigma_{a_0}, \sigma_{-1}\rangle, & \text{if } \chi(-1) = 1, \chi(a) = \chi(a_0) = -1; \\ \langle \tau_{q_0^\alpha}\sigma_{a_0^\alpha}, \sigma_{-1}\rangle, & \text{if } \chi(-1) = 1, \chi(a)^\alpha \neq 1; \\ \langle \tau_{q_0}\sigma_{-a_0}, \tau_{-1}\sigma_{-1}\rangle, & \text{if } \chi(-1) = -1, \chi(a) = \chi(a_0) = -1; \\ \langle \tau_{q_0}\sigma_{a_0}, \tau_{-1}\rangle, & \text{if } \chi(-1) = -1, \chi(a) = 1; \\ \langle \tau_{q_0}\sigma_{a_0}, \tau_{-1}\sigma_{-1}\rangle, & \text{if } \chi(-1) = -1, \chi(a) = -1, \chi(a_0) = 1; \\ \langle \tau_{q_0^{\alpha/2}}\sigma_{-a_0^{\alpha/2}}\rangle, & \text{if } \chi(-1) = -1, 2 \mid \alpha, \chi(a) \neq \pm 1; \\ \langle \tau_{q_0^\alpha}\sigma_{a_0^\alpha}\rangle, & \text{if } \chi(-1) = -1, 2 \nmid \alpha, \chi(a) \neq \pm 1. \end{cases}$$

is a subgroup of $\mathrm{Gal}\big(\mathbb{Q}(\mu_{pc})/\mathbb{Q}\big)$, *$q_0 = \#\mathbb{F}_p(a^{(1-p)/2}), a_0 = a^{(1-q_0)/2} \in \mathbb{F}_p^\times$ and α is the order of $\chi(a_0) \in \mu_{p-1}$.*

Proof. As remarked above, $k = d_0\beta$ and $t^2 = a_0^{2\beta}$ for some integer β, where $q_0 = p^{d_0}$. Hence $t = \pm a_0^\beta$ and

$$\boldsymbol{\chi}^w = \{1, \chi^w\} = \boldsymbol{\chi}^{q_0^\beta}\eta = \left\{\eta, \eta\chi^{q_0^\beta}\right\}, \quad \eta(a) = \chi^w(t).$$

There are two cases:

(i) If $\eta = 1, \chi^w = \chi^{q_0^\beta}$, then $w \equiv q_0^\beta \bmod c$ and

$$1 = \eta(a) = \chi^w(t) = \chi(t) = \chi(\pm a_0^\beta).$$

(ii) If $\eta = \chi^w, \eta\chi^{q_0^\beta} = 1$, then $w \equiv -q_0^\beta \bmod c$. Since $\chi^w(a) = \eta(a) = \chi^w(t)$, we have $\chi(a) = \chi(t) = \chi(\pm a_0^\beta)$. Since $a_0 = a^{(1-q_0)/2} \in \mathbb{F}_p^\times$, we have

$$\chi(a_0)^2 = \chi(a)^{1-q_0} = \chi(a_0)^{(1-q_0)\beta} = 1.$$

Thus $\chi(a_0) = \pm 1$ and $\alpha = 1$ or 2.

The case $\chi(-1) = 1$.

(i) $\beta = \alpha m$ for some m and $w \equiv q_0^{\alpha m}, t = \pm a_0^{\alpha m}$.

(ii) If $\alpha = 1$, $\chi(a_0) = \chi(a) = 1$, then $w \equiv -q_0^m, t = \pm a_0^m$; if $\alpha = 2$, $\chi(a_0) = \chi(a) = -1$, then $w \equiv -q_0^{1+2m}, t = \pm a_0^{1+2m}$.

The case $\chi(-1) = -1$ and $2 \mid \alpha$.

(i) $w \equiv q_0^{\alpha m}, t = a_0^{\alpha m}$ or $w \equiv q_0^{\alpha(m+1/2)}, t = -a_0^{\alpha(m+1/2)}$.

(ii) $\alpha = 2$, $\chi(a) = \chi(a_0) = -1$. Then $w \equiv -q_0^{1+2m}, t = a_0^{1+2m}$ or $w \equiv -q_0^{2m}, t = -a_0^{2m}$.

The case $\chi(-1) = -1$ and $2 \nmid \alpha$.

(i) $w \equiv q_0^{\alpha m}, t = a_0^{\alpha m}$.

(ii) $\alpha = 1$ and $\chi(a_0) = 1$. If $\chi(a) = 1$, then $w \equiv -q_0^m, t = a_0^m$; if $\chi(a) = -1$, then $w \equiv -q_0^m, t = -a_0^m$. □

Example 5.2. If $a \in \mathbb{F}_p^\times$, then $q_0 = p, \alpha = 1$ or 2. One can easily obtain that

$$H = \begin{cases} \langle \tau_p, \tau_{-1}, \sigma_{-1} \rangle, & \text{if } \chi(-1) = 1 \text{ and } \chi(a) = 1; \\ \langle \tau_p, \sigma_{-1} \rangle, & \text{if } \chi(-1) = 1 \text{ and } \chi(a) = -1; \\ \langle \tau_p, \tau_{-1} \rangle, & \text{if } \chi(-1) = -1 \text{ and } \chi(a) = 1; \\ \langle \tau_p, \tau_{-1}\sigma_{-1} \rangle, & \text{if } \chi(-1) = -1 \text{ and } \chi(a) = -1; \\ \langle \tau_p \rangle, & \text{if } \chi(-1) = -1 \text{ and } \chi(a) \neq \pm 1. \end{cases}$$

This drops the combinatorial condition on (p, d) and the non-vanishing condition on $\mathrm{Tr}(a)$ in [Zha21, Theorems 1.1, 1.3], while we require that p is large with respect to d.

Remark 5.3. Assume that $\chi = \Lambda_2$. If $\Lambda_2(a) \neq 1$, then the Kloosterman sum vanishes. If $\Lambda_2(a) = 1$ and $\mathrm{Tr}(\sqrt{a}) \neq 0$, then the Kloosterman sum generates $\mathbb{Q}(\mu_p)^+$ if $\chi(-1) = 1$; $\mathbb{Q}(\mu_p)$ if $\chi(-1) = -1$. See [Zha21, Theorem 1.1(1)].

5.2. **The upper bound of the generating field.** If $\eta = 1$, then $\chi_i^w = \chi_i^{q_0^\beta}$. Thus $w \equiv q_0^\beta \bmod c$. Denote by

$$\alpha := \min \left\{ \alpha \in \mathbb{Z}_{>0} \,\middle|\, \exists t_0 \in \mathbb{F}_p^\times \text{ such that } t_0^n = a_0^{n_0 \alpha}, \prod \boldsymbol{\chi}(t_0) = 1 \right\}.$$

Write $\beta = \alpha s + r, 0 \leq r < \alpha$. Then

$$(t t_0^{-s})^n = a_0^{n_0\beta - n_0\alpha s} = a_0^{n_0 r}, \quad \prod \boldsymbol{\chi}(t t_0^{-s}) = 1.$$

This forces $r = 0$ and $t = \lambda t_0^s$ with $\lambda^n = 1, \prod \boldsymbol{\chi}(\lambda) = 1$. Hence

$$H \supseteq H_0 := \left\langle \tau_{q_0^\alpha} \sigma_{t_0}, \sigma_\lambda \mid \lambda^n = 1, \prod \boldsymbol{\chi}(\lambda) = 1 \right\rangle$$

and $\mathrm{Kl}(\psi, \boldsymbol{\chi}, q, a) \in \mathbb{Q}(\mu_{pc})^{H_0}$. This gives an upper bound of the degree of $\mathrm{Kl}(\psi, \boldsymbol{\chi}, q, a)$.

Example 5.4. Denote by $m(\xi)$ the multiplicity of ξ in the n-tuple $\boldsymbol{\chi}$. Assume that there exists a character ξ such that $m(\xi) \neq m(\xi')$ for any $\xi' \neq \xi$. Then one can easily show that $\eta = 1$ and $H = H_0$.

Acknowledgments. The author would like to thank Yang Cao and the anonymous reviewers for their helpful discussions and comments. This work is partially supported by the NSFC (Grant No. 12001510), the Fundamental Research Funds for the Central Universities (No. JZ2023HGTB0217) and the Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200).

References

[Del77] Pierre Deligne. *Cohomologie étale*, volume 569 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1977. Séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$.

[Del80] Pierre Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, 52:137–252, 1980.

[Fis92] Benji Fisher. Distinctness of Kloosterman sums. In *p-adic methods in number theory and algebraic geometry*, volume 133 of *Contemp. Math.*, pages 81–102. Amer. Math. Soc., Providence, RI, 1992.

[Kat88] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[Kat90] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1990.

[KRV11] Keijo Kononen, Marko Rintaaho, and Keijo Väänänen. On the degree of a kloosterman sum as an algebraic integer. *arXiv: Number Theory*, page 6, 2011.

[Sti90] Ludwig Stickelberger. Ueber eine Verallgemeinerung der Kreistheilung. *Math. Ann.*, 37(3):321–367, 1890.

[Wan95] Da Qing Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields Appl.*, 1(2):189–203, 1995. Special issue dedicated to Leonard Carlitz.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[WY20] Daqing Wan and Hang Yin. Algebraic degree periodicity in recurrence sequences. *arXiv: Number Theory*, page 7, 2020.

[Zha21] Shenxing Zhang. The generating fields of two kloosterman sums. *J. Univ. Sci. Technol. China*, 51(12):879–888, 2021.

School of Mathematics, Hefei University of Technology, Hefei, Anhui 230009, China
Email address: zhangshenxing@hfut.edu.cn