THE GENERATING FIELDS OF TWO TWISTED KLOOSTERMAN SUMS

SHENXING ZHANG

ABSTRACT. In this paper, we study the generating fields of the twisted Kloosterman sums $\mathrm{Kl}(q,a,\chi)$ and the partial Gauss sums $g(q,a,\chi)$. We require that the characteristic p is large with respect to the order d of the character χ and the trace of the coefficient a is nonzero. When $p \equiv \pm 1 \bmod d$, we can characterize the generating fields of these character sums. For general p, when a lies in the prime field, we propose a combinatorial condition on (p,d) to ensure one can determine the generating fields.

1. INTRODUCTION

1.1. **Background.** Let p be a prime, $q=p^k$ a power of p. Let $f\in\mathbb{F}_q[x_1^{\pm 1},\dots,x_n^{\pm 1}]$ be a Laurent polynomial. Let $\chi_1,\dots,\chi_n:\mathbb{F}_q^\times\to\mu_{q-1}$ be multiplicative characters. The *twisted exponential sum* of f with respect to $\chi_1,\dots,\chi_n$ is defined as

$$S_q^*(f,\chi_1,\dots,\chi_n):=\sum_{x_i\in\mathbb{F}_q^\times}\chi_1(x_1)\dots\chi_n(x_n)\zeta^{\mathrm{Tr}(f(x_1,\dots,x_n)}\in\mathbb{Z}[\mu_{dp}],$$

where d is the least common multiplier of orders of $\chi_1,\dots,\chi_n$, ζ is a fixed primitive p-th root of unity and $\mathrm{Tr}=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$. If all χ_i are trivial and f is a polynomial, we denote by

$$S_q(f):=\sum_{x_i\in\mathbb{F}_q}\zeta^{\mathrm{Tr}(f(x_1,\dots,x_n)}\in\mathbb{Z}[\mu_p]$$

the *exponential sum* of f. If ζ is replaced by another primitive p-th root of unity, the twisted exponential sum is replaced by a Galois conjugate and its degree does not change. There are various results about estimation on the exponential sums, their absolute values and p-adic valuations we will not list here. What we will discuss is their generating fields for some special f,χ_i.

The generating fields of exponential sums are relate to the distinctness of exponential sums and the generators of cyclotomic fields. When all χ_i are trivial, to give the generating field of $S_q(f)$ or $S_q^*(f)$ is equivalent to give its degree as an algebraic number. We list some known results here.

(1) $\deg f=1$: $S_q(f)=0$.

Date: June 12, 2021.

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

Key words and phrases. cyclotomic fields, Kloosterman sums.

This work is partially supported by NSFC (Grant No. 12001510), the Fundamental Research Funds for the Central Universities (No. WK0010000061) and Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200). The author would like to thank Daqin Wan, Yi Ouyang and Yue Xu for many helpful suggestions and discussions.

(2) $\deg f = 2, p \geq 3$: $S_p(x^2) = \sqrt{(-1)^{(p-1)/2}p}$ is the Gauss sum of the non-trivial quadratic character modulo p. Hasse-Davenport proved that $S_q(x^2) = (-1)^{k-1}S_p(x^2)^k$. Hence $S_q(x^2+a) = (-1)^{k+1}S_p(x^2)^k\zeta^{\mathrm{Tr}(a)}$ and

$$\deg S_q(x^2+a) = \begin{cases} p-1, & \text{if } \mathrm{Tr}(a) \neq 0; \\ 2, & \text{if } \mathrm{Tr}(a) = 0 \text{ and } 2 \nmid k; \\ 1, & \text{if } \mathrm{Tr}(a) = 0 \text{ and } 2 \mid k. \end{cases}$$

(3) $f = ax^d, p \geq 3$: We may assume that $d \mid (q-1)$. Then $\deg S_q(f)$ divides $(p-1)/(p-1, \frac{q-1}{d})$. If $d \mid (p-1)$ or $d \mid (q-1)/(p-1)$, then $\deg S_q(f) = (p-1)/(p-1, \frac{q-1}{d})$. See [Wan19, Example 3.10].

(4) $f = ax^{dd_2} + x^{dd_1}$ with coprime d_1, d_2: If $p \equiv 1 \bmod d$, p is large with respect to $\deg f$ and $\mathrm{Tr}(a^{-d_1}) \neq 0$, then $\deg S_q(f) = \frac{p-1}{(d_2-d_1, p-1)}$. See [Zha20, Theorem 1.1].

(5) For $f \in \mathbb{F}_q[x]$, $(p-1)/\deg S_p(f)$ is a factor of

$$(\#\left\{(x,y) \in \mathbb{F}_q^2 \mid y^p - y = f(x)\right\} - 1, p-1).$$

See [Wan19, Theorem 3.16].

(6) The sequence $\left\{S_{q^k}(f)\right\}_k$ is periodic for $k \geq N$ for some constant N, see [WaY20, Theorem 1]. The author gave a bound on the period in [Zha20, Corollary 2.4]. Combining this result and the bound on the degree of the L-function of f in [Bom78, Theorem 1], the author showed that: under certain coprime condition, the degree of $S_{p^k}(ax^{d+1}+x) = (p-1)/d$ for sufficiently large k if $p \equiv 1 \bmod d$ and p is large with respect to d. See [Zha20, Corollary 1.2(2)].

The exponential sum of

$$f = ax_1 \cdots x_n + x_1^{-1} + \cdots + x_n^{-1}, \quad a \in \mathbb{F}_q^\times$$

is called the *Kloosterman sum* $\mathrm{Kl}_n(q,a)$. When $\mathrm{Tr}(a) \neq 0$, the degree of $\mathrm{Kl}(q,a)$ is $(p-1)/(n+1,p-1)$, see [Wan95, Theorem 1.1]. When $\mathrm{Tr}(a) = 0$, the degree of f can be obtained by the work in [Fis92, Corollary 4.24] and [Wan95, Theorem 5.1] if p is large or p does not divide a certain integer, with respect to n and k. But no simple formula is known in general, see also [KRV11, Theorem 2].

1.2. Main results.

We see that all of these results are about untwisted exponential sums. In this article, we will consider the generating field of the *general Kloosterman sum*

$$\mathrm{Kl}_n(\chi_1,\dots,\chi_n;d_1,\dots,d_n)(q,a) = \sum_{\substack{x_1^{d_1}\cdots x_n^{d_n}=a \\ x_1,\dots,x_n \in \mathbb{F}_q^\times}} \zeta^{\mathrm{Tr}(\sum_i x_i)} \prod_{i=1}^n \chi_i(x_i) \in \mathbb{Q}(\mu_{dp})$$

in two cases, where $\chi_1,\dots,\chi_n$ are multiplicative characters on $\mathbb{F}_q^\times$ and $a \in \mathbb{F}_q^\times$. See [Kat88, page 48].

When $\mathrm{Tr}(a) \neq 0$, we study the generating field of the *twisted Kloosterman sum*

$$\mathrm{Kl}(q,a,\chi) := \mathrm{Kl}_2(\chi,\mathbf{1};1,1)(q,a) = \sum_{x \in \mathbb{F}_q^\times} \chi(x)\zeta^{\mathrm{Tr}(x+a/x)},$$

and the generating field of the *partial Gauss sum*

$$g(q,a,\chi) := \mathrm{Kl}_1(\chi; q+1)(q^2,a) = \sum_{x^{q+1}=a} \chi(x)\zeta^{\mathrm{Tr}(x+a/x)}.$$

These character sums are motivated from the exponential sums of cubic polynomials. When χ is cubic, the exponential sum

$$S_q(x^3-3ax) := \sum_{x\in\mathbb{F}_q} \zeta^{\mathrm{Tr}(x^3-3ax)} = \begin{cases} \mathrm{Kl}(q,a^3,\chi), & \text{if } q\equiv 1 \bmod 3;\\ g(q,a^3,\chi), & \text{if } q\equiv -1 \bmod 3. \end{cases}$$

See Proposition 2.2.

Fix isomorphisms

$$\sigma_- : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$$

where $\sigma_t(\zeta_p) = \zeta_p^t$ for any $\zeta_p \in \mu_p$,

$$\tau_- : (\mathbb{Z}/d\mathbb{Z})^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$$

where $\tau_w(\zeta_d) = \zeta_d^w$ for any $\zeta_d \in \mu_d$. Both σ_t and τ_w can be viewed as elements in $\mathrm{Gal}(\mathbb{Q}(\mu_{dp})/\mathbb{Q})$ since $p \nmid d$.

Theorem 1.1. *Let d be the order of χ.*

(1) When $d = 2$,

- $\mathrm{Kl}(q,a,\chi) = 0$ *if* $\chi(a) = -1$*;*
- $\mathrm{Kl}(q,a,\chi)$ *generates* $\mathbb{Q}(\mu_p)^+$ *if* $\chi(a) = 1$*,* $\chi(-1) = 1$ *and* $\mathrm{Tr}(\sqrt{a}) \neq 0$*;*
- $\mathrm{Kl}(q,a,\chi)$ *generates* $\mathbb{Q}(\mu_p)$ *if* $\chi(a) = 1$*,* $\chi(-1) = -1$ *and* $\mathrm{Tr}(\sqrt{a}) \neq 0$*;*

(2) When $d \geq 3$ and $p > 5d-2$, $\mathrm{Kl}(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where

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

if $p \equiv \pm 1 \bmod d$ and $\mathrm{Tr}(a) \neq 0$.

See Propositions 3.3 and 3.10.

Theorem 1.2. *Let d be the order of χ. Assume that $\mathrm{Tr}(a) \neq 0$.*

(1) If $d \mid (q-1)$ and $p > 2$, then $g(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where

$$H = \{\tau_w\sigma_{\pm 1} \mid w \equiv 1 \bmod d_1\}$$

and $d_1 \mid d$ is the order of $a^{(q-1)/d}$.

(2) If $d \mid (p+1)$ and $p > 7d-2$, then $g(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where

$$H = \begin{cases} \langle \tau_{-1}, \sigma_{-1}\rangle, & \text{if } a \notin \mathbb{F}_q^{\times 2} \text{ or } 4 \nmid d;\\ \langle \tau_{d/2+1}, \tau_{-1}, \sigma_{-1}\rangle, & \text{if } a \in \mathbb{F}_q^{\times 2} \text{ and } 4 \mid d. \end{cases}$$

See Propositions 4.3 and 4.8.

For general d, if (p,d) satisfies a combinatorial condition, we characterize the generating fields of these character sums when $a \in \mathbb{F}_p$. Let n be the order of

$p \bmod d$. For any $r \in \mathbb{Z}$ or $\mathbb{Z}/d\mathbb{Z}$, write $a_j \equiv rp^{-j} \bmod d$ with $0 \leq a_j \leq d-1$. Define

$$V_r := \frac{1}{n}\sum_{j=0}^{n-1} \min\left\{\delta_j + \frac{a_{j+1}p - a_j}{d}, p - \delta_j - \frac{a_{j+1}p - a_j}{d}\right\}$$

where

$$\delta_j = \begin{cases} 0, & \text{if } a_j \leq d/2; \\ 1, & \text{if } a_j > d/2. \end{cases}$$

Denote by

$$T_{p,d} = \left\{r \in (\mathbb{Z}/d\mathbb{Z})^\times \mid V_{rs} = V_s, \forall s \in (\mathbb{Z}/d\mathbb{Z})^\times\right\}.$$

This is a subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ containing $-1, p$.

Theorem 1.3. *Let d be the order of χ. Assume that $a \in \mathbb{F}_p^\times$ and $p \nmid k$.*

(1) If $d \geq 3$, $p > 5d - 2$ and $T_{p,d} = \langle -1, p\rangle$, then $\mathrm{Kl}(q, a, \chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where

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

In particular, this holds for $d \leq 31$ with $p \not\equiv \pm(d/2+1) \bmod d$ if $4 \mid d$.

(2) If $d \mid (q+1)$, $p > 7d - 2$ and $T_{p,d/(2,d)} = \langle p\rangle$, then $g(q, a, \chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where

$$H = \begin{cases} \langle \tau_p, \sigma_{-1}\rangle, & \text{if } a \notin \mathbb{F}_p^{\times 2} \text{ or } 4 \nmid d; \\ \langle \tau_{d/2+1}, \tau_p, \sigma_{-1}\rangle, & \text{if } a \in \mathbb{F}_p^{\times 2} \text{ and } 4 \mid d. \end{cases}$$

In particular, this holds if $d/(2,d) \leq 31$.

See Theorems 3.11 and 4.9.

It's an interesting phenomenon that these two different Kloosterman sums depend on similar conbinatorial conditions. It seems that there should be a direct relation between these two Kloosterman sums.

We will express the Kloosterman sums as a Fourier expansion and use Stickelberger's congruence theorem to determine the first several terms of the $\mathfrak{P}$-adic expansions for a fixed prime $\mathfrak{P}$ in $\mathbb{Q}(\mu_{(q-1)p})$. The main estimation is in Lemma 3.4. Then the generating fields are obtained by these results.

2. Preliminaries

2.1. **The Stickelberger's congruence theorem.** We will use this theorem to estimate the valuations of Gauss sums. The prime p splits into $f = \varphi(q-1)/k$ primes as

$$p\mathbb{Z}[\mu_{q-1}] = \mathfrak{p}_1 \cdots \mathfrak{p}_f$$

in $\mathbb{Q}(\mu_{q-1})$ and $\mathfrak{p}_i$'s are totally ramified as

$$\mathfrak{p}_i\mathbb{Z}[\mu_{(q-1)p}] = \mathfrak{P}_i^{p-1}$$

in $\mathbb{Q}(\mu_{(q-1)p})$. Let $\mathfrak{p}$ be a fixed 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. Then $v(p) = p-1$ and $v(\pi) = 1$ where $\pi = \zeta - 1$.

$$\begin{tikzcd}
& \mathbb{Q}(\mu_{(q-1)p}) \supset \mathfrak{P}_1, \dots, \mathfrak{P}_f \arrow[dl, dash] \arrow[dd, dash] \\
\mathfrak{p}_1, \dots, \mathfrak{p}_f \subset \mathbb{Q}(\mu_{q-1}) \arrow[dd, dash] & \\
& \mathbb{Q}(\mu_p) \supset (\pi) = (\zeta - 1) \arrow[dl, dash] \\
p\mathbb{Z} \subset \mathbb{Q} &
\end{tikzcd}$$

Let κ be the residue field of $\mathfrak{p}$ and ω the Teichmüller lifting of the quotient map $\mathbb{Z}[\mu_{q-1}]^\times \twoheadrightarrow \kappa^\times$ associated to $\mathfrak{p}$. We can view ω as a character on $\mathbb{F}_q^\times$ if we fix an isomorphism $\mathbb{F}_q \cong \kappa$. Different choice of the isomorphism may cause a composite by a power of the Frobenius map. Take $\omega(0) = 0$ for convention. Then ω is multiplicative and

$$\omega(a) + \omega(b) - \omega(a+b) \in \mathfrak{p}.$$

In particular, its $\mathfrak{P}$-adic valuation is at least $p-1$. Denote by

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

the *Gauss sum* of ω^{-m}. Clearly, $g(0) = -1$ and $g(pm) = g(m)$. Recall the Stickelberger's congruence theorem, see [Sti90], [Was82, Chap. 6].

Theorem 2.1. *For $0 \le m < q-1$,*

$$g(m) \equiv -\frac{\pi^{m_0 + \cdots + m_{k-1}}}{m_0! \cdots m_{k-1}!} \bmod \mathfrak{P}^{m_0 + \cdots + m_{k-1} + 1},$$

where

$$m = m_0 + m_1 p + \cdots + m_{k-1} p^{k-1}, \quad 0 \le m_i \le p-1.$$

In particular, $v(g(m)) \equiv m \bmod (p-1)$ has same parity with m.

2.2. **Relation to the exponential sums of cubic polynomials.** In this subsection, we will show the relations between the cubic exponential sums and the twisted Kloosterman sums or the partial Gauss sums. This fact is well known to experts. Let's show it briefly.

Proposition 2.2. *Assume that $p > 3$ and $a \in \mathbb{F}_q^\times$.*

(1) If $q \equiv 1 \bmod 3$, then $S_q(x^3 - 3ax) = \mathrm{Kl}(q, a^3, \chi)$ where χ is any non-trivial 3-th character of $\mathbb{F}_q^\times$.

(2) If $q \equiv -1 \bmod 3$, then $S_q(x^3 - 3ax) = g_\chi(q, a^3)$ where χ is any non-trivial 3-th character of $\mathbb{F}_{q^2}^\times$.

From this, $S_q(x^3 - 3ax)$ generates $\mathbb{Q}(\mu_p)^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ if $\mathrm{Tr}(a^3) \neq 0$ and $p > 19$.

Proof. Denote by N_c the number of the equation

$$f(x) = x^3 - 3ax = c \in \mathbb{F}_q$$

with multiplicities. The discriminant of $f - c$ is

$$\Delta = -27\varsigma^2 = -27(c^2 - 4a^3) \in \mathbb{F}_q.$$

Then $N_c = 1$ if and only if $\sqrt{\Delta} \notin \mathbb{F}_q$. Indeed, there are three cases:

- $N_c = 1$, $f - c$ decomposes into a linear factor and a degree 2 irreducible polynomial. Thus the splitting field of $f - c$ is $\mathbb{F}_{q^2}$ and $\sqrt{\Delta} \notin \mathbb{F}_q$.
- $N_c = 3$, clearly $\sqrt{\Delta} \in \mathbb{F}_q$.
- $N_c = 0$, $f - c$ is irreducible and $\sqrt{\Delta} \in \mathbb{F}_{q^3} \cap \mathbb{F}_{q^2} = \mathbb{F}_q$.

Fix a nontrivial 3-th root of unity $\lambda \in \mathbb{F}_{q^2}$. Then $\sqrt{\Delta} = \pm 3(2\lambda + 1)\varsigma$.

(1) In this case, $\lambda \in \mathbb{F}_q$. Assume that $\varsigma = \sqrt{c^2 - 4a^3} \in \mathbb{F}_q$. That's equivalently to say, $N_c = 0$ or 3. By Cardano's formula, the solutions of $f(x) = c$ in $\overline{\mathbb{F}}_q$ are

$$u + au^{-1},\ \lambda u + \lambda^2 au^{-1},\ \lambda^2 u + \lambda au^{-1},$$

where $u^3 = (c+\varsigma)/2$. If $N_c = 3$, then $u + au^{-1} \in \mathbb{F}_q$, u lies in $\mathbb{F}_{q^2} \cap \mathbb{F}_{q^3} = \mathbb{F}_q$ and vice versa. Hence $N_c = 3$ if and only if $v := (c + \varsigma)/2 \in \mathbb{F}_q^{\times 3}$. We have $a^3/v = (c - \varsigma)/2$ and $c = v + a^3/v$.

If $N_c = 3$ and $c = \pm 2a^{3/2}$, we have $\varsigma = 0$ and there is a root with multiplicity 2. Denote by

$$B_i = \sum_{N_c = i, c \neq \pm 2a^{3/2}} \zeta^{\mathrm{Tr}(c)}.$$

Then

$$B_3 = \frac{1}{2} \sum_{v \in \mathbb{F}_q^{\times 3}, v \neq \pm a^{3/2}} \zeta^{\mathrm{Tr}(v + a^3/v)}, \quad B_0 = \frac{1}{2} \sum_{v \notin \mathbb{F}_q^{\times 3}} \zeta^{\mathrm{Tr}(v + a^3/v)}.$$

and

$$B_0 + B_1 + B_3 + \zeta^{\mathrm{Tr}(2a^{3/2})} + \zeta^{\mathrm{Tr}(-2a^{3/2})} = \sum_{c \in \mathbb{F}_q} \zeta^{\mathrm{Tr}(c)} = 0.$$

If $a \notin \mathbb{F}_q^{\times 2}$, the terms $\zeta^{\mathrm{Tr}(\pm 2a^{3/2})}$ disappear. Now

$$\begin{aligned}
S_q(f) &= B_1 + 3B_3 + 2\zeta^{\mathrm{Tr}(2a^{3/2})} + 2\zeta^{\mathrm{Tr}(-2a^{3/2})} \\
&= 2B_3 - B_0 + \zeta^{\mathrm{Tr}(2a^{3/2})} + \zeta^{\mathrm{Tr}(-2a^{3/2})} \\
&= \sum_{v \in \mathbb{F}_q^{\times 3}, v \neq \pm a^{3/2}} \zeta^{\mathrm{Tr}(v + a^3/v)} - \frac{1}{2} \sum_{v \notin \mathbb{F}_q^{\times 3}} \zeta^{\mathrm{Tr}(v + a^3/v)} + \zeta^{\mathrm{Tr}(2a^{3/2})} + \zeta^{\mathrm{Tr}(-2a^{3/2})} \\
&= \sum_{v \in \mathbb{F}_q^{\times}} \frac{\chi(v) + \overline{\chi}(v)}{2} \cdot \zeta^{\mathrm{Tr}(v + a^3/v)} \\
&= \frac{\mathrm{Kl}(q, a^3, \chi) + \mathrm{Kl}(q, a^3, \overline{\chi})}{2} = \mathrm{Kl}(q, a^3, \chi)
\end{aligned}$$

by Lemma 3.1(1).

(2) In this case, $p \equiv -1 \bmod 3$, $k = 2\ell + 1$ is odd and $\lambda \in \mathbb{F}_{q^2} - \mathbb{F}_q$. Thus -27 is not a square in $\mathbb{F}_q$. Assume that $(2\lambda + 1)\varsigma \in \mathbb{F}_q$. That's equivalently to say, $N_c = 0$ or 3. Let $\delta : x \mapsto x^q$ be the nontrivial element in $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. The solutions of $f(x) = c$ in $\overline{\mathbb{F}}_q$ are

$$u + u^\delta, \lambda u + \lambda^2 u^\delta, \lambda^2 u + \lambda u^\delta,$$

where $u^3 = (c + \varsigma)/2$. If $u \in \mathbb{F}_{q^2}^{\times}$, then $N_c = 3$ and vice versa. Hence $N_c = 3$ if and only if $v := (c + \varsigma)/2 \in \mathbb{F}_{q^2}^{\times 3}$. We have $v^\delta = (c - \varsigma)/2 = a^3/v$ and $c = v + v^\delta$.

Similar to (1), we have

$$S_q(f) = \sum_{vv^\delta = a^3} \frac{\chi(v) + \overline{\chi}(v)}{2} \cdot \zeta^{\mathrm{Tr}(v+v^\delta)} = \frac{g_\chi(q, a^3) + g_{\overline{\chi}}(q, a^3)}{2} = g_\chi(q, a^3)$$

by Lemma 4.1(1).

Finally, the claim on the generating field of $S_q(x^3 - 3ax)$ follows from Propositions 3.10 and 4.8. □

Remark 2.3. The condition on p can be weaken to $p > 11$, see [Zha20, Corollary 1.2].

3. The twisted Kloosterman sums

In this section, we will study the generating field of the twisted Kloosterman sum

$$\mathrm{Kl}(q, a, \chi) := \sum_{x \in \mathbb{F}_q^\times} \chi(x) \zeta^{\mathrm{Tr}(x + a/x)} \in \mathbb{Q}(\mu_{dp}), \quad a \in \mathbb{F}_q^\times,$$

where $d \mid (q-1)$ is the order of χ.

Lemma 3.1. *We have*
(1) $\mathrm{Kl}(q, a, \chi) = \chi(a)\mathrm{Kl}(q, a, \overline{\chi})$*;*
(2) $\mathrm{Kl}(q, a, \chi^p) = \mathrm{Kl}(q, a^p, \chi)$*.*

Proof. We substitute x by a/x or x^p respectively, then the result follows. □

There is an integer w prime to d such that $\chi = \omega^{-(q-1)w/d}$. Then

$$\mathrm{Kl}(q, a, \chi) = \tau_w \mathrm{Kl}(q, a, \omega^{-(q-1)/d}).$$

Since we are interested in the generating field of $\mathrm{Kl}(q, a, \chi)$, we may assume that $\chi = \omega^{-(q-1)/d}$ from now on.

Lemma 3.2. *We have a Fourier expansion*

$$(q-1)\mathrm{Kl}(q, a, \chi^r) = \sum_{m=0}^{q-2} \omega^m(a) g(m) g\left(m + \tfrac{q-1}{d} r\right).$$

Proof. We have

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

Thus

$$\begin{aligned}(q-1)\mathrm{Kl}(q, a, \chi^r) &= (q-1) \sum_{xy=a} \chi^r(x) \zeta^{\mathrm{Tr}(x+y)} \\ &= \sum_{x,y \in \mathbb{F}_q^\times} \omega^{-(q-1)r/d}(x) \sum_{m=0}^{q-2} \omega^{-m}(a^{-1}xy) \zeta^{\mathrm{Tr}(x+y)} \\ &= \sum_{m=0}^{q-2} \omega^m(a) g(m) g\left(m + \tfrac{q-1}{d} r\right).\end{aligned}$$

□

3.1. The quadratic twist.

Proposition 3.3. *Assume that $d=2$.*

(1) $\mathrm{Kl}(q,a,\chi)=0$ *if* $\chi(a)=-1$.

(2) If $\chi(a)=1$ *and* $\mathrm{Tr}(\sqrt{a})\neq 0$, *then* $\mathrm{Kl}(q,a,\chi)$ *generates* $\mathbb{Q}(\mu_p)^+$ *if* $\chi(-1)=1$*; generates* $\mathbb{Q}(\mu_p)$ *if* $\chi(-1)=-1$.

Proof. (1) Note that $\chi(a)=-1$ and $\overline{\chi}=\chi$, the result follows from Lemma 3.1(1).

(2) Write $a=b^2$. By Lemma 3.2, we have

$$(q-1)\mathrm{Kl}(q,a,\chi)=2\sum_{m=0}^{(q-3)/2}\omega^m(a)g(m)g\left(m+\tfrac{q-1}{2}\right).$$

Write

$$m=\sum_{j=0}^{k-1}m_jp^j,\quad m+\frac{q-1}{2}=\sum_{j=0}^{k-1}n_jp^j$$

with $0\leq m_j,n_j\leq p-1$. Then

$$n_j=m_j+\frac{p-1}{2}+\epsilon_{j-1}-p\epsilon_j,$$

where $\epsilon_j\in\{0,1\}$ and $\epsilon_{-1}=\epsilon_{k-1}=0$. Denote by $m_j'=\min\{m_j,n_j\}$ and $\epsilon_j'=|\epsilon_j-\epsilon_{j+1}|$. Then

$$m_j+n_j=\frac{p-1}{2}+2m_j'+\epsilon_{j-1}'$$

and

$$v\Big(g(m)g\left(m+\tfrac{q-1}{2}\right)\Big)=\sum_{j=0}^{k-1}(m_j+n_j)$$
$$=\frac{(p-1)k}{2}+\sum_{j=0}^{k-1}\big(2m_j'+\epsilon_{j-1}'\big)\geq V:=\frac{(p-1)k}{2}.$$

The equality holds if and only all $m_j'=\epsilon_j'=0$, that's to say, $m=0$.

There are two cases such that the valuation is secondly minimal.

i) All $m_j'=\epsilon_j'=0$ except $m_i'=1$ for a unique i with $0\leq i\leq k-1$. That's to say, $m=p^i$, $m+(q-1)/2\equiv p^i(q+1)/2 \bmod (q-1)$. The summation of Fourier terms over these m is

$$2\sum_{i=0}^{k-1}\omega^{p^i}(a)g(p^i)g\left(p^i+\tfrac{q-1}{2}\right)=2\omega(\mathrm{Tr}(a))g(1)g\left(\tfrac{q+1}{2}\right)$$
$$\equiv\frac{2\omega(\mathrm{Tr}(a))\pi^{V+2}}{\left(\frac{p-1}{2}\right)!^{k-1}\left(\frac{p+1}{2}\right)!}\equiv C\omega(\mathrm{Tr}(a))\pi^{V+2} \bmod \mathfrak{P}^{V+3},$$

where $C=4\left(\frac{p-1}{2}\right)!^{-k}$.

ii) All $m_j'=\epsilon_j'=0$ except $\epsilon_i'=\epsilon_{i'}'=1$ for a unique pair i,i' with $0\leq i<i'\leq k-1$. That's to say, $\epsilon_{i+1}=\cdots=\epsilon_{i'}=1$ and zero otherwise, $m=(p^i+p^{i'})/2, m+(q-1)/2\equiv(p^{i'}+p^{i+k})/2 \bmod (q-1)$. The summation

of Fourier terms over these m is

$$2\sum_{0\le i<i'\le k-1}\omega^{(p^i+p^{i'})/2}(a)g\left(\frac{p^i+p^{i'}}{2}\right)g\left(\frac{p^i+p^{i'}}{2}+\frac{q-1}{2}\right)$$

$$\equiv\sum_{0\le i<i'\le k-1}\frac{2\omega^{p^i+p^{i'}}(b)\pi^{V+2}}{\left(\frac{p-1}{2}\right)!^{k-2}\left(\frac{p+1}{2}\right)!^2}\equiv C\omega\big(\mathrm{Tr}(b)^2-\mathrm{Tr}(b^2)\big)\pi^{V+2}\bmod\mathfrak{P}^{V+3}.$$

Now we have

$$(q-1)\mathrm{Kl}(q,a,\chi)\equiv-2g(\tfrac{q-1}{2})+C\omega(\mathrm{Tr}(b))^2\pi^{V+2}\bmod\mathfrak{P}^{V+3}.\tag{3.1}$$

If σ_t fixes $\mathrm{Kl}(q,a,\chi)$, we have $\sigma_t\mathrm{Kl}(q,a,\chi)=\chi(t)^{-1}\mathrm{Kl}(q,at^2,\chi)=\mathrm{Kl}(q,a,\chi)$ and then $\chi(t)=1$,

$$\omega(\mathrm{Tr}(bt))^2\equiv\omega(\mathrm{Tr}(b))^2\bmod\mathfrak{P}.$$

Note that $\mathrm{Tr}(b)\neq0$. If $\chi(-1)=-1$, we have $t=\pm1$ and $\mathrm{Kl}(q,a,\chi)$ generates $\mathbb{Q}(\mu_p)^+$. If $\chi(-1)=1$, we have $t=1$ and $\mathrm{Kl}(q,a,\chi)$ generates $\mathbb{Q}(\mu_p)$. □

3.2. **The d-th twist with $d\geq3$.** We need the following lemma to obtain the $\mathfrak{P}$-adic expansion of $\mathrm{Kl}(q,a,\chi)$.

Lemma 3.4. *Let*

$$s=\sum_{j=0}^{k-1}s_jp^j,\quad 0\le s_j\le p-1,$$

be an integer less than $q-1$, satisfying $s_j\neq(p-1)/2$ for all j. Denote by

$$M:=\sum_{\delta_j=1}(p-\delta_{j-1}-s_j)p^j,\quad M+s\equiv\sum_{\delta_j=0}(\delta_{j-1}+s_j)p^j\bmod(q-1)$$

and

$$V:=v\big(g(M)g(M+s)\big)=\sum_{j=0}^{k-1}\min\left\{\delta_{j-1}+s_j,p-\delta_{j-1}-s_j\right\},$$

where

$$\delta_j=\begin{cases}0, & \text{if } s_j<p/2;\\ 1, & \text{if } s_j>p/2.\end{cases}$$

Consider $v\big(g(m)g(m+s)\big)$ for $0\le m<q-1$.

(1) If $|(p-1)/2-s_j|>1$ for all j, then the valuation is minimal: $m=M$, $v=V$.

(2) If $|(p-1)/2-s_j|>2$ for all j, then the valuation is secondly minimal: $m\equiv M+p^i\bmod(q-1)$ for some i, $v=V+2$.

(3) If $|(p-1)/2-s_j|>3$ for all j, then the valuation is thirdly minimal: $m\equiv M+p^i+p^{i'}\bmod(q-1)$ for some i,i', $v=V+4$.

Proof. Denote by $s'_j=\min\{s_j,p-1-s_j\}$. Write

$$m+s-(q-1)\epsilon_{k-1}=\sum_{j=0}^{k-1}n_jp^j<q-1,\quad 0\le n_j\le p-1,$$

where $\epsilon_{k-1}\in\{0,1\}$. Then

$$n_j=m_j+s_j+\epsilon_{j-1}-p\epsilon_j,$$

where $\epsilon_j \in \{0,1\}$ and $\epsilon_{-1} = \epsilon_{k-1}$. Denote by $m'_j = \min\{m_j, n_j\}$ and $\epsilon'_j = |\epsilon_j - \epsilon_{j+1}|$. Then

$$m_j + n_j = \begin{cases} 2m'_j + s'_j + \epsilon'_{j-1}, & \text{if } \delta'_j = 0; \\ 2m'_j + (p-1-s'_j) + \epsilon'_{j-1}, & \text{if } \delta'_j = \pm 1, \end{cases}$$

where $\delta'_j = \delta_j - \epsilon_j$. Assume that $|(p-1)/2 - s_j| > \lambda$ for all j.

(1) Place $\delta'_0, \dots, \delta'_{k-1}$ in a circle. If all $\delta'_j = 0$,

$$v\big(g(m)g(m+s)\big) = \sum_{j=0}^{k-1}(2m'_j + s'_j + \epsilon'_{j-1}) \geq \sum_{j=0}^{k-1}(s'_j + \epsilon'_{j-1}) = V.$$

Otherwise there are α strings of ±1's, with total length z. If $\delta'_j = \delta'_{j+1} = 0$, then $\epsilon'_j = |\delta_j - \delta_{j+1}|$. Thus

$$\begin{aligned} v\big(g(m)g(m+s)\big) &= \sum_{j=0}^{k-1}(m_j + n_j) \\ &\geq V + \sum_{\delta'_j \neq 0}(p-1-2s'_j) + \sum_{j=0}^{k-1}(\epsilon'_{j-1} - |\delta_{j-1} - \delta_j|) \\ &\geq V + \sum_{\delta'_j \neq 0}|p-1-2s_j| - (z+\alpha) \\ &> V + 2\lambda z - 2z = V + 2(\lambda - 1). \end{aligned}$$

Therefore, $v\big(g(m)g(m+s)\big) \geq V$ with equality holds if and only if $m = M$.

(2) Note that the valuation has same parity with s. When $z \geq 1$, we have that $v\big(g(m)g(m+s)\big) > V + 2$. Thus the valuation is secondly minimal if and only if all $\delta'_j = 0$ and only one $m'_i = 1$. The result then follows.

(3) When $z \geq 1$, we have that $v\big(g(m)g(m+s)\big) > V + 4$. Thus the valuation is thirdly minimal if and only if all $\delta'_j = 0$, $m'_i = 2$ for some i or $m'_i = m'_{i'} = 1$ for some $i \neq i'$, and other entries are zero. The result then follows. □

Definition 3.5. Let p be a prime prime to d. Let n be a positive integer such that $p^n \equiv 1 \bmod d$. For any $r \in \mathbb{Z}$ or $\mathbb{Z}/d\mathbb{Z}$, write $a_j \equiv rp^{-j} \bmod d$ with $0 \leq a_j \leq d-1$. Define

$$V_r := \frac{1}{n}\sum_{j=0}^{n-1} \min\left\{\delta_j + \frac{a_{j+1}p - a_j}{d}, p - \delta_j - \frac{a_{j+1}p - a_j}{d}\right\} \tag{3.2}$$

where

$$\delta_j = \begin{cases} 0, & \text{if } a_j \leq d/2; \\ 1, & \text{if } a_j > d/2. \end{cases}$$

This definition does not depend on the choice of n.

Proposition 3.6. *If $p > 3d - 2$, then the valuation of $\mathrm{Kl}(q, a, \chi^r)$ is kV_r.*

Proof. If $r \equiv d/2 \bmod d$, $V_r = (p-1)/2$ and the valuation of

$$\mathrm{Kl}(q, a, \chi^r) = \mathrm{Kl}(q, a, \omega^{(q-1)/2}) = \sum_{m=0}^{q-2} \omega^m(a) g(m) g\left(m + \tfrac{q-1}{2}\right)$$

is $(p-1)k/2$ by (3.1).

If $r \not\equiv d/2 \bmod d$, then $a_j \neq d/2$ and

$$\left|\frac{p-1}{2} - \frac{a_{j+1}p - a_j}{d}\right| = \frac{|(2a_{j+1}-d)p + (d-2a_j)|}{2d} \geq \frac{p-(d-2)}{2d} > 1.$$

Thus

$$\frac{(q-1)r}{d} = \sum_{j=0}^{k-1} \frac{a_{j+1}p - a_j}{d} p^j$$

satisfies the condition in Lemma 3.4(1) and then the valuation of $\mathrm{Kl}(q, a, \chi^r)$ is kV_r by Lemma 3.2. □

Definition 3.7. For any $s \in \mathbb{Z}$ or $\mathbb{Z}/d\mathbb{Z}$, define

$$T^s_{p,d} := \{r \bmod d \mid (r,d) = 1, V_{rs} = V_s\} \subseteq (\mathbb{Z}/d\mathbb{Z})^\times. \tag{3.3}$$

Define

$$T_{p,d} := \bigcap_{(s,d)=1} T^s_{p,d}.$$

Proposition 3.8. *Assume that $p > 3d - 2$.*

(1) $T_{p,d}$ is a group containing $\left\{\pm p^\lambda \bmod d \mid \lambda \in \mathbb{Z}\right\}$.

(2) If $p \equiv \pm 1 \bmod d$, then $T_{p,d} = \{\pm 1\}$.

(3) If $4 \mid d \geq 16$ and $p \equiv d/2 \pm 1 \bmod d$, then $T_{p,d} = (\mathbb{Z}/d\mathbb{Z})^\times$.

(4) If $3 \leq d \leq 31$ and (p, d) does not satisfies (3), then $T_{p,d} = \left\{\pm p^\lambda \bmod d \mid \lambda \in \mathbb{Z}\right\}$.

Proof. (1) If $r_1, r_2 \in T_{p,d}$, then $V_{r_1 r_2^{-1} s} = V_{r_2^{-1} s} = V_s$. Thus $r_1 r_2^{-1} \in T_{p,d}$ and $T_{p,d}$ is a group. Since $V_{\pm pr} = V_r$ by the definition, the group $T_{p,d}$ contains $-1, p$.

(2) That's because if $p \equiv \pm 1 \bmod d$, we have

$$V_r = \frac{p \mp 1}{d} \cdot \min\{r, d-r\}. \tag{3.4}$$

(3) If $p \equiv d/2 \pm 1 \bmod d$, then

$$a_{2i} = r, \quad a_{2i+1} = \begin{cases} d/2 \pm r, & \text{if } r < d/2; \\ d/2 \mp (d-r), & \text{if } r > d/2. \end{cases}$$

Thus $V_r = (p \pm 1)k/4$ and $T_{p,d} = (\mathbb{Z}/d\mathbb{Z})^\times$. When $4 \mid d \geq 16$, $\varphi(d) > 4$. Hence $T_{p,d}$ does not equal $\langle -1, p\rangle$.

(4) We have already know the case $p \equiv \pm 1 \bmod d$ in (2). Clearly the assertion holds if p and -1 generate $(\mathbb{Z}/d\mathbb{Z})^\times$. The rest cases are listed in Table 1. □

Remark 3.9. (1) One may expect that $T^s_{p,d}$ is also a group. Unfortunately it's not true. For instance, take $d = 33$, $p \equiv \pm 10 \bmod 33$, then $T^1_{p,d} = \{\pm 1, \pm 4, \pm 7, \pm 10\}$.

(2) One can find more pairs (p, d) such that $T_{p,d} \neq \langle -1, p\rangle$ like (3), where d is divisible by a high power of 2. It's conjectured that $T_{p,d} = \langle -1, p\rangle$ when $4 \nmid d$ and $p > 3d - 2$.

(3) It seems that $T_{p,d} = T_{p',d}$ if $p' \equiv p \bmod d$ and both $p, p' > 3d - 2$. But I don't have a proof or a counterexample.

Table 1. V_r for $d \leq 32$, $(r,d)=1$.

d	$\pm\overline{p}$	$rH/\{\pm 1\}$	V_r
13	3	$\{1,3,4\}$	$(8p\pm 2)/39$
		$\{2,5,6\}$	$(p\mp 1)/3$
	4	$\{1,3,4\}$	$(8p\mp 6)/39$
		$\{2,5,6\}$	$(p\pm 1)/3$
	5	$\{1,5\}$	$(3p\mp 2)/13$
		$\{2,3\}$	$(5p\pm 1)/26$
		$\{4,6\}$	$(5p\pm 1)/13$
15	4	$\{1,4\}$	$(p\mp 1)/6$
		$\{2,7\}$	$(3p\pm 3)/10$
16	7	$\{1,7\}$	$\boldsymbol{(p\mp 1)/4}$
		$\{3,5\}$	
17	2	$\{1,2,4,8\}$	$(15p\mp 13)/68$
		$\{3,5,6,7\}$	$(21p\pm 9)/68$
	4	$\{1,4\}$	$(5p\mp 3)/34$
		$\{2,8\}$	$(5p\mp 3)/17$
		$\{3,5\}$	$(4p\pm 1)17$
		$\{6,7\}$	$(13p\mp 1)/34$
19	7	$\{1,7,8\}$	$(16p\pm 2)/57$
		$\{2,3,5\}$	$(10p\pm 6)/57$
		$\{4,6,9\}$	$(p\mp 1)/3$
	8	$\{1,7,8\}$	$(16p\mp 14)/57$
		$\{2,3,5\}$	$(10p\mp 4)/57$
		$\{4,6,9\}$	$(p\pm 1)/3$
20	9	$\{1,9\}$	$\boldsymbol{(p\mp 1)/4}$
		$\{3,7\}$	
21	4	$\{1,4,5\}$	$(10p\pm 2)/63$
		$\{2,8,10\}$	$(20p\pm 4)/63$
	5	$\{1,4,5\}$	$(10p\mp 8)/63$
		$\{2,8,10\}$	$(20p\mp 16)/63$
	8	$\{1,8\}$	$(3p\mp 3)/14$
		$\{2,5\}$	$(p\pm 1)/6$
		$\{4,10\}$	$(p\pm 1)/3$
24	5	$\{1,5\}$	$(p\mp 1)/8$
		$\{7,11\}$	$(3p\mp 3)/8$
	7	$\{1,7\}$	$(p\mp 1)/6$
		$\{5,11\}$	$(p\mp 1)/3$
	11	$\{1,11\}$	$\boldsymbol{(p\mp 1)/4}$
		$\{5,7\}$	
25	4	$\{1,4,6,9,11\}$	$(31p\pm 1)/125$
		$\{2,3,7,8,12\}$	$(32p\mp 28)/125$
	6	$\{1,4,6,9,11\}$	$(31p\mp 11)/125$
		$\{2,3,7,8,12\}$	$(32p\pm 8)/125$
	7	$\{1,7\}$	$(4p\mp 3)/25$
		$\{2,11\}$	$(13p\pm 9)/50$
		$\{3,4\}$	$(7p\pm 1)/50$
		$\{6,8\}$	$(7p\pm 1)/25$
		$\{9,12\}$	$(21p\pm 3)/50$
	9	$\{1,4,6,9,11\}$	$(31p\mp 29)/125$
		$\{2,3,7,8,12\}$	$(32p\pm 12)/125$
	11	$\{1,4,6,9,11\}$	$(31p\pm 9)/125$
		$\{2,3,7,8,12\}$	$(32p\mp 2)/125$
26	3	$\{1,3,9\}$	$(p\mp 1)/6$
		$\{5,7,11\}$	$(23p\pm 9)/78$
	5	$\{1,5\}$	$(3p\mp 2)/26$
		$\{3,11\}$	$(7p\pm 4)/26$
		$\{7,9\}$	$(8p\mp 1)/26$
	9	$\{1,3,9\}$	$(p\mp 1)/6$
		$\{5,7,11\}$	$(23p\pm 1)/78$

d	$\pm\overline{p}$	$rH/\{\pm 1\}$	V_r/k
27	8	$\{1,8,10\}$	$(19p\mp 17)/81$
		$\{2,7,11\}$	$(20p\pm 2)/81$
		$\{4,5,13\}$	$(22p\mp 14)/81$
	10	$\{1,8,10\}$	$(19p\mp 1)/81$
		$\{2,7,11\}$	$(20p\pm 16)/81$
		$\{4,5,13\}$	$(22p\mp 4)/81$
28	3	$\{1,3,9\}$	$(13p\mp 11)/84$
		$\{5,11,13\}$	$(29p\mp 3)/84$
	9	$\{1,3,9\}$	$(13p\mp 5)/84$
		$\{5,11,13\}$	$(29p\pm 19)/84$
	13	$\{1,13\}$	$\boldsymbol{(p\mp 1)/4}$
		$\{3,11\}$	
		$\{5,9\}$	
29	4	$\{1,4,5,6,7,9,13\}$	$(45p\pm 23)/203$
		$\{2,3,8,10,11,12,14\}$	$(60p\mp 8)/203$
	5	$\{1,4,5,6,7,9,13\}$	$(45p\pm 7)/203$
		$\{2,3,8,10,11,12,14\}$	$(60p\mp 10)/203$
	6	$\{1,4,5,6,7,9,13\}$	$(45p\mp 9)/203$
		$\{2,3,8,10,11,12,14\}$	$(60p\mp 12)/203$
	7	$\{1,4,5,6,7,9,13\}$	$(45p\mp 25)/203$
		$\{2,3,8,10,11,12,14\}$	$(60p\mp 14)/203$
	9	$\{1,4,5,6,7,9,13\}$	$(45p\pm 1)/203$
		$\{2,3,8,10,11,12,14\}$	$(60p\mp 18)/203$
	12	$\{1,12\}$	$(13p\mp 11)/58$
		$\{2,5\}$	$(7p\pm 3)/58$
		$\{3,7\}$	$(5p\mp 2)/29$
		$\{4,10\}$	$(7p\pm 3)/29$
		$\{6,14\}$	$(10p\mp 4)/29$
		$\{8,9\}$	$(17p\mp 1)/58$
		$\{11,13\}$	$(12p\pm 1)/29$
	13	$\{1,4,5,6,7,9,13\}$	$(45p\mp 5)/203$
		$\{2,3,8,10,11,12,14\}$	$(60p\mp 26)/203$
30	11	$\{1,11\}$	$(p\mp 1)/5$
		$\{7,13\}$	$(p\pm 1)/3$
31	2	$\{1,2,4,8,15\}$	$(30p\pm 2)/155$
		$\{3,6,12,7,14\}$	$(42p\mp 22)/155$
		$\{5,10,9,11,13\}$	$(48p\pm 28)/155$
	4	$\{1,4,2,8,15\}$	$(30p\pm 4)/155$
		$\{3,12,6,14,7\}$	$(42p\pm 18)/155$
		$\{5,10,9,11,13\}$	$(48p\mp 6)/155$
	5	$\{1,5,6\}$	$(12p\pm 2)/93$
		$\{2,10,12\}$	$(24p\pm 4)/93$
		$\{3,15,13\}$	$(p\mp 1)/3$
		$\{4,7,11\}$	$(22p\pm 14)/93$
		$\{8,9,14\}$	$(p\mp 1)/3$
	6	$\{1,6,5\}$	$(12p\mp 10)/93$
		$\{2,12,10\}$	$(24p\mp 20)/93$
		$\{3,15,13\}$	$(p\pm 1)/3$
		$\{4,7,11\}$	$(22p\mp 8)/93$
		$\{8,9,14\}$	$(p\pm 1)/3$
	8	$\{1,8,2,4,15\}$	$(30p\pm 8)/155$
		$\{3,6,12,7,14\}$	$(42p\pm 36)/155$
		$\{5,9,10,13,11\}$	$(48p\mp 12)/155$
32	7	every coset	$\boldsymbol{p/4}$
	9	every coset	
	15	every coset	$\boldsymbol{(p\mp 1)/4}$

Proposition 3.10. *Assume that $d \geq 3$ and $p > 5d-2$. If $p \equiv \pm 1 \bmod d$ and $\mathrm{Tr}(a) \neq 0$, then $\mathrm{Kl}(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where*

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

Proof. We may assume that $\chi = \omega^{-(q-1)/d}$. Denote by M_r the M in Lemma 3.4 for $s = (q-1)r/d$. By Lemma 3.4 and Proposition 3.6, we have

$$\begin{aligned} &(q-1)\mathrm{Kl}(q,a,\chi^r) \\ \equiv&\omega^{M_r}(a)g(M_r)g\left(M_r + \tfrac{q-1}{d}\right) + \sum_{i=0}^{k-1} \omega^{M_r+p^i}(a)g(M_r+p^i)g\left(M_r + \tfrac{q-1}{d} + p^i\right) \\ \equiv&\omega^{M_r}(a)g(M_r)g\left(M_r + \tfrac{q-1}{d}\right) + C\pi^{kV_r+2}\omega^{M_r}(a)\omega(\mathrm{Tr}(a)) \bmod \mathfrak{P}^{kV_r+3}, \end{aligned} \tag{3.5}$$

where C is a constant prime to p.

By Lemma 3.1(1), we have

$$\tau_w\sigma_t\mathrm{Kl}(q,a,\chi) = \chi(t)^{-w}\mathrm{Kl}(q,t^2a,\chi^w) = \chi(ta)^w\mathrm{Kl}(q,t^2a,\chi^{-w}). \tag{3.6}$$

If $\tau_w\sigma_t$ fixes $\mathrm{Kl}(q,a,\chi)$, then $V_w = V_1$. Thus $w = \pm 1$ by Proposition 3.8(2). If $w = 1$, $\chi(t)^{-1}\mathrm{Kl}(q,t^2a,\chi) = \mathrm{Kl}(q,a,\chi)$ and we have

$$\chi(t)^{-1}\omega^{M_1}(t^2a) \equiv \omega^{M_1}(a) \bmod \mathfrak{P}.$$

This forces $\chi(t)^{-1}\omega^{M_1}(t^2) = 1$ and then

$$\chi(t)^{-1}\omega^{M_1}(t^2a)\omega(\mathrm{Tr}(t^2a)) \equiv \omega^{M_1}(a)\omega(\mathrm{Tr}(a)) \bmod \mathfrak{P}.$$

Since $\omega(\mathrm{Tr}(a)) \neq 0$, we have $\omega(t^2) = 1$, $t = \pm 1$ and $\chi(t) = 1$.

If $w = -1$, $\chi(ta)^{-1}\mathrm{Kl}(q,t^2a,\chi) = \mathrm{Kl}(q,a,\chi)$ and we have

$$\chi(ta)^{-1}\omega^{M_1}(t^2a) \equiv \omega^{M_1}(a) \bmod \mathfrak{P}.$$

This forces $\chi(ta)^{-1}\omega^{M_1}(t^2) = 1$ and then

$$\chi(ta)^{-1}\omega^{M_1}(t^2a)\omega(\mathrm{Tr}(t^2a)) \equiv \omega^{M_1}(a)\omega(\mathrm{Tr}(a)) \bmod \mathfrak{P}.$$

Since $\omega(\mathrm{Tr}(a)) \neq 0$, we have $\omega(t^2) = 1$, $t = \pm 1$ and $\chi(ta) = 1$. The result then follows. □

When $T_{p,d}$ equals $\langle -1, p \rangle$, we can determine the generating field of $\mathrm{Kl}(q,a,\chi)$, where $a \in \mathbb{F}_p^\times$ and $p \nmid k$.

Theorem 3.11. *Assume that $3 \leq d \mid (q-1)$, $p > 5d-2$, $a \in \mathbb{F}_p^\times$ and $p \nmid k$. If $T_{p,d} = \langle -1, p \rangle$, then $\mathrm{Kl}(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where*

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

In particular, this holds for $d \leq 31$ with $p \not\equiv \pm(d/2-1) \bmod d$ if $4 \mid d$.

Proof. If $\tau_w\sigma_t$ fixes $\mathrm{Kl}(q,a,\chi)$, it also fixes $\tau_r\mathrm{Kl}(q,a,\chi)=\mathrm{Kl}(q,a,\chi^r)$. Thus $V_{wr}=V_r$ by (3.5), (3.6) and Proposition 3.6. Then $w\in T_{p,d}$ and $w\equiv\pm p^\lambda \bmod d$ for some λ. For $w\equiv p^\lambda$, by Lemma 3.1(2), we have

$$\mathrm{Kl}(q,a,\chi^w)=\mathrm{Kl}(q,a,\chi^{p^\lambda})=\mathrm{Kl}(q,a^{p^\lambda},\chi)=\mathrm{Kl}(q,a,\chi).$$

Similar to the proof of Proposition 3.10, if $\mathrm{Tr}(a)\neq 0$, we have $\omega(t^2)\equiv 1$ and then $t=\pm1$, $\chi(t)=1$.

For $w\equiv -p^\lambda$, by Lemma 3.1(2), we have $\mathrm{Kl}(q,a,\chi^{-w})=\mathrm{Kl}(q,a,\chi)$. Similarly, if $\mathrm{Tr}(a)\neq 0$, we have $t=\pm1$ and $\chi(ta)=1$.

The last claim follows from Proposition 3.8(4). □

4. The partial Gauss sums

In this section, we will study the partial Gauss sum

$$g(q,a,\chi):=\sum_{xx^\delta=a}\chi(x)\zeta^{\mathrm{Tr}'(x)}\in\mathbb{Q}(\mu_{dp}),\quad a\in\mathbb{F}_q^\times,$$

where $\delta: x\mapsto x^q$ is the non-trivial element in $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$, $\mathrm{Tr}'(x)=\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x)=\mathrm{Tr}(x+x^\delta)$ and $d\mid(q^2-1)$ is the order of χ. The notations ω, v, g are defined as in Subsection 2.1, but q is replaced by q^2.

Lemma 4.1. *We have*

(1) $g(q,a,\chi)=\chi(a)g(q,a,\overline{\chi})$;

(2) $g(q,a,\chi^p)=g(q,a^p,\chi)$.

(3) When d is even, we have $g(q,a,\chi^{d/2+1})=\chi_2(a)g(q,a,\chi)$, where χ_2 is the quadratic character on $\mathbb{F}_q^\times$.

Proof. We substitute x by $x^\delta=a/x$ or x^p respectively, then (1)(2) follows. If $xx^\delta=a$, then $\chi^{d/2}(x)=\omega^{(q-1)/2}(a)=\chi_2(a)$ and (3) follows. □

Similar to Section 3, we may assume that $\chi=\omega^{-(q^2-1)/d}$ since we are interested in the generating field of $g(q,a,\chi)$.

Lemma 4.2. *We have a Fourier expansion*

$$(q-1)g(q,a,\chi^r)=\sum_{m=0}^{q-2}\omega^m(a)g\big((q+1)m+\tfrac{q^2-1}{d}r\big).$$

Proof. Write $a=\alpha^{q+1}=\alpha\alpha^\delta$ for some $\alpha\in\mathbb{F}_{q^2}^\times$, then we have

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

Thus

$$\begin{aligned}(q-1)g(q,a,\chi^r)=&(q-1)\sum_{xx^\delta=a}\chi^r(x)\zeta^{\mathrm{Tr}'(x)}\\ =&\sum_{m=0}^{q-2}\sum_{x\in\mathbb{F}_{q^2}^\times}\chi^r(x)\omega^{(q+1)m}(\alpha^{-1}x)\zeta^{\mathrm{Tr}'(x)}\\ =&\sum_{m=0}^{q-2}\omega^m(a)g\big((q+1)m+\tfrac{q^2-1}{d}r\big).\end{aligned}$$

□

We will consider the cases $d \mid (q \pm 1)$ respectively.

4.1. The case $d \mid (q-1)$.

Proposition 4.3. *Assume that $d \mid (q-1)$ and $p > 2$. If $\mathrm{Tr}(a) \neq 0$, then $g(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where*
$$H = \{\tau_w \sigma_{\pm 1} \mid w \equiv 1 \bmod d_1\}$$
and $d_1 \mid d$ is the order of $a^{(q-1)/d}$.

Proof. We have
$$g(q,a,\chi^r) = \omega^{-(q-1)r/d}(a) g(q,a,\mathbf{1}) \tag{4.1}$$
and
$$(q-1)g(q,a,\mathbf{1}) \equiv 1 + \omega(\mathrm{Tr}(a)) g(q+1) \bmod \mathfrak{P}^3 \tag{4.2}$$
by Lemma 4.2. Since
$$\tau_w \sigma_t g(q,a,\chi) = \sum_{x x^\delta = a t^2} \chi^w(x t^{-1}) \zeta^{\mathrm{Tr}'(x)} = \chi^{-w}(t) g(q, a t^2, \chi^w), \tag{4.3}$$
if $\tau_w \sigma_t$ fixes $g(q,a,\chi)$, we have $\chi^{-w}(t)\omega^{-(q-1)(w-1)/d}(a) = 1$. Thus we have
$$\omega(\mathrm{Tr}(t^2 a)) \equiv \omega(\mathrm{Tr}(a)) \bmod \mathfrak{P}.$$
If $\mathrm{Tr}(a) \neq 0$, then $t = \pm 1$ and $\chi(t) = \omega^{-(q-1)/d}(t^{q+1}) = 1$. Then $w \equiv 1 \bmod d_1$ and $g(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^H$. □

4.2. The case $d \mid (q+1)$.

We need the following lemma to obtain the $\mathfrak{P}$-adic expansion of $g(q,a,\chi)$.

Lemma 4.4. *Let s be a positive integer less than $(q-1)/2$. Let s_j, δ_j, M, V be the notations as in Lemma 3.4. Assume that $|(p-1)/2 - s_j| > 3$ for all j; $s_0 \geq 2$ and not all δ_j are same.*

(1) The valuation $v\big(g((q+1)m+s)\big)$ is
- *minimal: $m = M$, $v = V$;*
- *secondly minimal: $m = M + p^j$, $v = V + 2$.*

(2) The valuation $v\big(g((q+1)m-s)\big)$ is
- *minimal: $m = M + s$, $v = V$;*
- *secondly minimal: $m = M + s + p^j$, $v = V + 2$.*

Proof. By the assumptions, $p \geq 11$ and $s_{k-1} \leq (p-9)/2$. Then $s < (p-7)p^{k-1}/2$ and
$$M = \sum_{\delta_j = 1} (p - \delta_{j-1} - s_j) p^j \leq \sum_{j=0}^{k-2} p^{1+j} < \frac{11}{10} p^{k-1}.$$
Thus
$$M + 2\delta_0 - 1 + p^i + p^{i'} + s < \left(\frac{11}{10} + 2 + \frac{p-7}{2} \right) p^{k-1} + 2 < q, \tag{4.4}$$
Denote by g_q the Gauss sum with respect to $\mathbb{F}_q$.

(1) If $m + s \geq q$, then
$$v\big(g((q+1)m+s)\big) = v\big(g_q(m+s-q) g_q(m+1)\big) = v\big(g_q(m+s-1) g_q(m+1)\big).$$
Since $s-2$ has same δ_i sequence as s, by Lemma 3.4, the valuation is
- minimal: $m = M + 2\delta_0 - 1$, $v = V + 4\delta_0 - 2$;
- secondly minimal: $m = M + 2\delta_0 - 1 + p^i$, $v = V + 4\delta_0$;

- thirdly minimal: $m = M + 2\delta_0 - 1 + p^i + p^{i'}$, $v = V + 4\delta_0 + 2$.

But by (4.4), these three cases do not happen and the valuation is at least $V + 4$.

If $m + s < q$, then $v\big(g((q+1)m + s)\big) = v\big(g_q(m)g_q(m+s)\big)$. By Lemma 3.4, the valuation is

- minimal: $m = M$, $v = V$;
- secondly minimal: $m = M + p^i$, $v = V + 2$.

The result then follows.

(2) If $m < s$, then

$$v\big(g((q+1)m - s)\big) = v\big(g_q(m-1)g_q(m+q-s)\big) = v\big(g_q(m')g_q(m'+s-2)\big),$$

where $m' = m + q - s$. Since $s - 2$ has same δ_i sequence as s, by Lemma 3.4, the valuation is

- minimal: $m = M + 2\delta_0 - 1 + s$, $v = V + 4\delta_0 - 2$;
- secondly minimal: $m = M + 2\delta_0 - 1 + s + p^i$, $v = V + 4\delta_0$;
- thirdly minimal: $m = M + 2\delta_0 - 1 + s + p^i + p^{i'}$, $v = V + 4\delta_0 + 2$

by (4.4). But $m < s$, these three cases do not happen and then the valuation is at least $V + 4$.

If $m \geq s$, then $v\big(g((q+1)m - s)\big) = v\big(g_q(m-s)g_q(m)\big)$. By Lemma 3.4, the valuation is

- minimal: $m = M + s$, $v = V$;
- secondly minimal: $m = M + s + p^i$, $v = V + 2$.

The result then follows. □

Proposition 4.5. *If $p > 7d - 2$, then the valuation of $g(q, a, \chi^r)$ is kV_{2r}.*

Proof. If $r \equiv 0, d/2 \bmod d$, then $V_{2r} = 0$ and the order of χ^r is at most 2, which divides $q - 1$. Thus the valuation of $g(q, a, \chi^r)$ is zero by (4.1) and (4.2).

If $r \not\equiv 0, d/2 \bmod d$, by Lemma 4.1(1) and the fact that $V_{2r} = V_{-2r}$, we may assume that $1 \leq r < d/2$. Write

$$\frac{q^2-1}{d}r = s_L + qs_M, \quad s_L = \frac{(d-r)q - r}{d}, \quad s_M = \frac{rq - (d-r)}{d}.$$

Then

$$s = s_L - s_M = (d - 2r)\frac{q+1}{d} = \sum_{j=0}^{k-1} \frac{b_{j+1}p - b_j}{d} p^j,$$

where $b_j p^j \equiv 2r \bmod d$ with $0 \leq b_j \leq d - 1$. By Lemmas 4.2, 4.4 and

$$g\big((q+1)m + \tfrac{q^2-1}{d}r\big) = \begin{cases} g\left((q+1)(m + s_M + 1) - 2r\frac{q+1}{d}\right), & \text{if } 1 \leq r < \frac{d}{4}; \\ g\left((q+1)(m + s_M) + (d - 2r)\frac{q+1}{d}\right), & \text{if } \frac{d}{4} \leq r < \frac{d}{2}, \end{cases}$$

the valuation of $g(q, a, \chi^r)$ is $kV_{2r} = kV_{d-2r}$. □

Definition 4.6. Let $p > 7d - 2$ be a prime prime to d. Define

$$T'_{p,d} := \bigcap_{(s,d)=1} T^{2s}_{p,d} = \{r \bmod d \mid (r,d) = 1, V_{2rs} = V_{2s}, \forall (s,d) = 1\} \subset (\mathbb{Z}/d\mathbb{Z})^{\times},$$

where $T^s_{p,d}$ is defined as (3.3).

Proposition 4.7. *Assume that* $p > 7d - 2$.

(1) If d *is odd, then* $T'_{p,d} = T_{p,d}$. *If* d *is even, then* $T'_{p,d} = \{r | r \bmod d/2 \in T_{p,d/2}\}$. *Thus* $T'_{p,d}$ *is a group containing* $\langle d/2+1, -1, p\rangle$.

(2) If $p \equiv \pm 1 \bmod d$, *then* $T'_{p,d} = \{\pm 1, \pm(d/2+1)\}$.

(3) $T'_{p,d} = \langle d/2+1, -1, p\rangle$ *if and only if* $T_{p,d/(2,d)} = \langle -1, p\rangle$.

(4) If -1 *is a power of* $p \bmod d$, *then* $T'_{p,d} = \langle d/2+1, p\rangle$ *if* $d/(2,d) \leq 31$.

Here, $d/2+1$ *appears only if* $4 \mid d$.

Proof. Note that $(d/2-1, d) = (d/2-1, 2) = 1$ holds only if $4 \mid d$.

(1) follows from the definition directly. (2) follows from (1) and Proposition 3.8(2). (3) follows from (1). For (4), $p \not\equiv \pm(d/4+1) \bmod d/2$ if $4 \mid d/2 \geq 16$. Then the result follows from (1) and Proposition 3.8(4). □

Proposition 4.8. *Assume that* $p > 7d - 2$. *If* $p \equiv -1 \bmod d$ *and* $\mathrm{Tr}(a) \neq 0$, *then* $g(q, a, \chi)$ *generates* $\mathbb{Q}(\mu_{dp})^H$, *where*

$$H = \begin{cases} \langle \tau_{-1}, \sigma_{-1}\rangle, & \text{if } a \notin \mathbb{F}_q^{\times 2} \text{ or } 4 \nmid d; \\ \langle \tau_{d/2-1}, \tau_{-1}, \sigma_{-1}\rangle, & \text{if } a \in \mathbb{F}_q^{\times 2} \text{ and } 4 \mid d. \end{cases}$$

Proof. We may assume that $\chi = \omega^{-(q^2-1)/d}$. The cases $d = 1, 2$ is shown in Proposition 4.3 and we may assume that $d \geq 3$.

Denote by $N_r = \frac{q^2-1}{d} r + (q+1)M_r$ such that $v(N_r) = kV_{2r}$ is minimal. Then by Lemma 4.4, the valuation is secondly minimal if and only if $m = M_r + p^i$ for some i, in which case, the valuation is $kV_{2r} + 2$. By Lemma 4.2, we have

$$\begin{aligned} &(q-1)g(q, a, \chi^r) \\ \equiv&\omega^{M_r}(a)g(N_r) + \sum_{i=0}^{k-1} \omega^{M_r+p^i}(a)g\big(N_r + (q+1)p^i\big) \\ =&\omega^{M_r}(a)g(N_r) + \sum_{i=0}^{k-1} \omega^{M_r+p^i}(a)g\big(N_r + (q+1)p^i\big) \\ =&\omega^{M_r}(a)g(N_r) + C\pi^{kV_{2r}+2}\omega^{M_r}(a)\omega(\mathrm{Tr}(a)) \bmod \mathfrak{P}^{kV_{2r}+3}. \end{aligned} \tag{4.5}$$

Note that $\chi(x) = 1$ for any $x \in \mathbb{F}_q^\times$ since $d \mid (q+1)$. By Lemma 4.1, we have

$$g(q, a, \chi^{-r}) = g(q, a, \chi^r), \quad g(q, a, \chi^{d/2 \pm r}) = \chi_2(a)g(q, a, \chi^r).$$

If $\tau_w\sigma_t$ fixes $g(q, a, \chi)$, then by (4.3), $V_{2w} = V_2$. Thus $w \equiv \pm 1, \pm(d/2+1) \bmod d$ by (3.4). If $\tau_{\pm 1}\sigma_t$ fixes $g(q, a, \chi)$, we have

$$\omega^{M_1}(t^2 a) \equiv \omega^{M_1}(a) \bmod \mathfrak{P}.$$

This forces $\omega^{M_1}(t^2) = 1$ and then

$$\omega^{M_1}(t^2 a)\omega(\mathrm{Tr}(t^2 a)) \equiv \omega^{M_1}(a)\omega(\mathrm{Tr}(a)) \bmod \mathfrak{P}.$$

Since $\mathrm{Tr}(a) \neq 0$, we have $\omega(t^2) = 1$ and $t = \pm 1$.

If $4 \mid d$ and $w = d/2 \pm 1$, we have $\chi_2(a) = 1$ and σ_t fixes $g(q, a, \chi)$. Since $\mathrm{Tr}(a) \neq 0$, we have $t = \pm 1$. The result then follows. □

Theorem 4.9. *Assume that $d \mid (q+1)$, $p > 7d-2$, $a \in \mathbb{F}_p^\times$ and $p \nmid k$. If $T_{p,d/(2,d)}$ is generated by p, then $g(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where*

$$H = \begin{cases} \langle \tau_p, \sigma_{-1} \rangle, & \text{if } a \notin \mathbb{F}_p^{\times 2} \text{ or } 4 \nmid d; \\ \langle \tau_{d/2+1}, \tau_p, \sigma_{-1} \rangle, & \text{if } a \in \mathbb{F}_p^{\times 2} \text{ and } 4 \mid d. \end{cases}$$

In particular, this holds if $d/(2,d) \leq 31$.

Proof. If $\tau_w \sigma_t$ fixes $g(q,a,\chi)$, it also fixes $\tau_r g(q,a,\chi) = g(q,a,\chi^r)$. Thus $V_{2wr} = V_{2r}$ by (4.5), (4.3) and Proposition 4.5. Note that -1 is a power of p modulo d. Then $w \in T'_{p,d}$ and $w \equiv p^\lambda$ or $(d/2+1)p^\lambda \bmod d$ for some λ. For $w \equiv p^\lambda$, by Lemma 4.1(2), we have

$$g(q,a,\chi^w) = g(q, a^{p^\lambda}, \chi) = g(q,a,\chi).$$

Similar to the proof of Proposition 4.8, if $\mathrm{Tr}(a) \neq 0$, we have $\omega(t^2) = 1$ and then $t = \pm 1$.

For $4 \mid d$ and $w \equiv (d/2+1)p^\lambda \bmod d$, by Lemma 4.1(2)(3), we have

$$g(q,a,\chi^w) = \chi_2(a) g(q,a,\chi).$$

Thus $\chi_2(a) = 1$ by (4.5). Similarly, if $\mathrm{Tr}(a) \neq 0$, we have $t = \pm 1$. □

References

[Bom78] E. Bombieri. On exponential sums in finite fields. II. *Invent. Math.* 47 (1978), 29–39.

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

[Kat88] N. M. Katz. Gauss sums, Kloosterman sums, and monodromy groups. Annals of Mathematics Studies, 116. *Princeton University Press, Princeton, NJ*, 1988. x+246 pp.

[KRV11] K. Kononen, M. Rinta-aho and K. Väänänen. On the degree of a Kloosterman sum as an algebraic integer. *ArXiv:*1107.0188, 2011.

[Sti90] L. Stickelberger. Ueber eine Verallgemeinerung der Kreistheilung. *Math. Ann.* 37 (1890), no. 3, 321–367.

[Wan95] D. Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields Appl.* 2 (1995), no. 1, 189–203.

[Wan19] D. Wan. Algebraic theory of exponential sums over finite fields. Lecture Notes at 2019 HIT Undergraduate Number Theory Summer School. Available at `https://www.math.uci.edu/~dwan/Wan_HIT_2019.pdf`.

[Was82] L. C. Washington. Introduction to cyclotomic fields. Graduate Texts in Mathematics, 83. *Springer-Verlag, New York*, 1982. xi+389 pp.

[WaY20] D. Wan, H. Yin. Algebraic degree periodicity in recurrence sequences. *ArXiv:*2009.14382, 2020.

[Zha20] S. Zhang. The degrees of exponential sums of binomials. *ArXiv:*2010.08342, 2020.

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, PR China

Email address: `zsxqq@mail.ustc.edu.cn`