第51卷第12期 中国科学技术大学学报 Vol. 51, No. 12
2021年12月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Dec. 2021
Received: 2021-03-17; Revised: 2021-05-18 doi:10.52396/JUST-2021-0077

The generating fields of two twisted Kloosterman sums

ZHANG Shenxing *
CAS Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China
* Corresponding author. E-mail: zsxqq@mail.ustc.edu.cn

Abstract: The generating fields of the twisted Kloosterman sums $\mathrm{Kl}(q, a, \chi)$ and the partial Gauss sums $g(q, a, \chi)$ are studied. 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.

Keywords: Kloosterman sum; exponential sum; cyclotomic field; algebraic number
CLC number: O156.2 **Document code**: A
2020 Mathematics Subject Classification: 11L05; 11L07; 11T23

1 Introduction

1.1 Background

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

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

where d is the least common multiplier of orders of $\chi_1, \cdots, \chi_n$, 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

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

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

② $\deg f=2, p\geqslant 3$: $S_p(x^2)=\sqrt{(-1)^{(p-1)/2}p}$ is the Gauss sum of the non-trivial quadratic character modulo p. Hasse and Davenport[1] 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

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

③ $f=ax^d$, $p\geqslant 3$: 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 Ref. [2, 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 Ref. [3, Theorem 1.1].

⑤ For $f\in\mathbb{F}_q[x]$, $(p-1)/\deg S_p(f)$ is a factor of $(\#\{(x, y)\in\mathbb{F}_q^2 \mid y^p-y=f(x)\}-1, p-1)$. See Ref. [2, Theorem 3.16].

⑥ The sequence $\{S_{q^k}(f)\}_k$ is periodic for $k\geqslant N$ for some constant N, see Ref. [4, Theorem 1]. Zhang gave a bound on the period in Ref. [3, Corollary 2.4]. Combining this result and the bound on the degree of the L-function of f in Ref. [5, Theorem 1], Zhang 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 Ref. [3, Corollary 1.2(2)].

The exponential sum of

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

is called the Kloosterman sum $\mathrm{Kl}_n(q, a)$. When $\mathrm{Tr}(a)$

Citation: Zhang Shenxing. The generating fields of two twisted Kloosterman sums. J. Univ. Sci. Tech. China, 2021, 51(12): 879-888.

$\neq 0$, the degree of $\mathrm{Kl}_n(q, a)$ is $(p-1)/(n+1, p-1)$, see Ref. [6, Theorem 1.1]. When $\mathrm{Tr}(a)=0$, the degree of f can be obtained by the work in Ref. [7, Corollary 4.24] and [6, 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 Ref. [8, 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

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

in two cases, where $\chi_1, \cdots, \chi_n$ are multiplicative characters on $\mathbb{F}_q^\times$ and $a \in \mathbb{F}_q^\times$. See Ref. [9, 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 2.1.

Fix isomorphisms

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

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

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

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 $d \geqslant 3$ 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 3.1 and 3.4.

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 4.1 and 4.4.

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

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

Denote by

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

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 $d \geqslant 3$, $p > 5d-2$ 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 $d \leqslant 31$ 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 $d/(2, d) \leqslant 31$.

See Theorems 3.1 and 4.1.

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 3.3. Then the generating fields are obtained by these results.

2 Preliminaries

2.1 The Stickelberger's congruence theorem

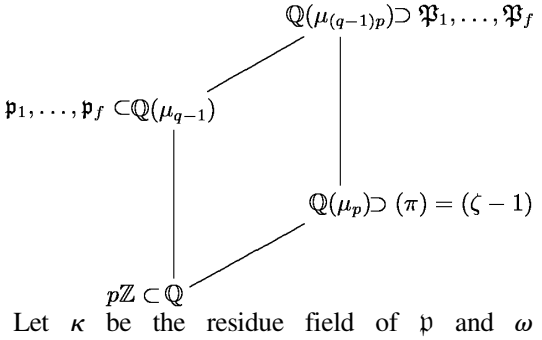
We will use this theorem to estimate the valuations of Gauss sums. The prime p splits into $f = \varphi(q-1)/k$ primes as

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

in $\mathbb{Q}(\mu_{q-1})$ and each $\mathfrak{p}_i$ is 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 $\pi=\zeta-1$.



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 Ref. [10;11, Chap. 6].

Theorem 2.1 For $0\leqslant m<q-1$,

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

where

$$m=m_0+m_1p+\cdots+m_{k-1}p^{k-1},\ 0\leqslant m_i\leqslant p-1.$$

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

① If $q\equiv1 \bmod 3$, then

$$S_q(x^3-3ax)=\mathrm{Kl}(q,a^3,\chi)$$

where χ is any non-trivial cubic 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 cubic 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 $\mathrm{Tr}(a^3)\neq0$ 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 cube root of unity $\lambda\in\mathbb{F}_{q^2}$. Then $\sqrt{\Delta}=\pm3(2\lambda+1)\varsigma$.

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

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

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 $v:=(c+\varsigma)/2\in\mathbb{F}_q^{\times3}$. We have $a^3/v=(c-\varsigma)/2$ and $c=v+a^3/v$.

If $N_c=3$ and $c=\pm2a^{3/2}$, we have $\varsigma=0$ and there is a root with multiplicity 2. Denote by

$$B_i=\sum_{N_c=i,\,c\neq\pm2a^{3/2}}\zeta^{\mathrm{Tr}(c)}.$$

Then

$$B_3=\frac{1}{2}\sum_{v\in\mathbb{F}_q^{\times3},\,v\neq\pm a^{3/2}}\zeta^{\mathrm{Tr}(v+a^3/v)},$$

$$B_0=\frac{1}{2}\sum_{v\notin\mathbb{F}_q^{\times3}}\zeta^{\mathrm{Tr}(v+a^3/v)}.$$

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 $a\notin\mathbb{F}_q^{\times2}$, the terms $\zeta^{\mathrm{Tr}(\pm2a^{3/2})}$ disappear. Now

$$S_q(f)=B_1+3B_3+2\zeta^{\mathrm{Tr}(2a^{3/2})}+2\zeta^{\mathrm{Tr}(-2a^{3/2})}=$$
$$2B_3-B_0+\zeta^{\mathrm{Tr}(2a^{3/2})}+\zeta^{\mathrm{Tr}(-2a^{3/2})}=$$
$$\sum_{v\in\mathbb{F}_q^{\times3},\,v\neq\pm a^{3/2}}\zeta^{\mathrm{Tr}(v+a^3/v)}-\frac{1}{2}\sum_{v\notin\mathbb{F}_q^{\times3}}\zeta^{\mathrm{Tr}(v+a^3/v)}+$$
$$\zeta^{\mathrm{Tr}(2a^{3/2})}+\zeta^{\mathrm{Tr}(-2a^{3/2})}=$$
$$\sum_{v\in\mathbb{F}_q^\times}\frac{\chi(v)+\bar{\chi}(v)}{2}\cdot\zeta^{\mathrm{Tr}(v+a^3/v)}=$$
$$\frac{\mathrm{Kl}(q,a^3,\chi)+\mathrm{Kl}(q,a^3,\bar{\chi})}{2}=\mathrm{Kl}(q,a^3,\chi)$$

by Lemma 3.1①.

② In this case, $p\equiv-1 \bmod 3$, $k=2l+1$ 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

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

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 $v:=(c+\varsigma)/2\in\mathbb{F}_{q^2}^{\times3}$. We have $v^\delta=(c-\varsigma)/2=a^3/v$ and $c=v+v^\delta$. Similar to ①, we have

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

by Lemma 4.1①.

Finally, the claim on the generating field of $S_q(x^3-3ax)$ follows from Propositions 3.4 and 4.4.

Remark 2.1 The condition on p can be weaken to $p>11$, see Ref. [3, Corollary 1.2].

3 The twisted Kloosterman sums

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

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

where $d|(q-1)$ is the order of χ.

Lemma 3.1 We have

① $\mathrm{Kl}(q,a,\chi)=\chi(a)\ \mathrm{Kl}(q,a,\bar{\chi})$;

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

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

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

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

3.1 The quadratic twist

Proposition 3.1 Assume that $d=2$.

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

② If $\chi(a)=1$ and $\mathrm{Tr}(\sqrt{a})\neq0$, 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 $\bar{\chi}=\chi$, the result follows from Lemma 3.1①.

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

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

Write

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

with $0\leqslant m_j,\ n_j\leqslant p-1$. 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

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

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 $0\leqslant i\leqslant k-1$. 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

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

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

(ii) All $m_j'=\epsilon_j'=0$ except $\epsilon_i'=\epsilon_{i'}'=1$ for a unique pair i,i' with $0\leqslant i<i'\leqslant k-1$. 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

$$2\sum_{0\leqslant i<i'\leqslant k-1}\omega^{(p^i+p^{i'})/2}(a)g(\frac{p^i+p^{i'}}{2})g(\frac{p^i+p^{i'}}{2}+\frac{q-1}{2})\equiv\sum_{0\leqslant i<i'\leqslant k-1}\frac{2\omega^{p^i+p^{i'}}(b)\pi^{V+2}}{(\frac{p-1}{2})!^{k-2}(\frac{p+1}{2})!^2}\equiv C\omega(\mathrm{Tr}(b)^2-\mathrm{Tr}(b^2))\pi^{V+2}\bmod\mathfrak{P}^{V+3}.$$

Now we have

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

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 $d\geqslant3$

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

Lemma 3.3 Let

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

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

all j. Denote by

$$M:=\sum_{\delta_j=1}(p-\delta_{j-1}-s_j)p^j,$$

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

and

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

where

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

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

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

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

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

$$m_j+n_j=\begin{cases}2m_j'+s_j'+\epsilon_{j-1}',\text{if } \delta_j'=0;\\ 2m_j'+(p-1-s_j')+\epsilon_{j-1}',\text{if } \delta_j'=\pm1,\end{cases}$$

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

① Place $\delta_0',\ \cdots,\ \delta_{k-1}'$ in a circle. If all $\delta_j'=0$,

$$v(g(m)g(m+s))=\sum_{j=0}^{k-1}(2m_j'+s_j'+\epsilon_{j-1}')\geqslant\sum_{j=0}^{k-1}(s_j'+\epsilon_{j-1}')=V.$$

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

$$v(g(m)g(m+s))=\sum_{j=0}^{k-1}(m_j+n_j)\geqslant$$

$$V+\sum_{\delta_j'\neq0}(p-1-2s_j')+\sum_{j=0}^{k-1}(\epsilon_{j-1}'-|\delta_{j-1}-\delta_j|)\geqslant$$

$$V+\sum_{\delta_j'\neq0}|p-1-2s_j|-(z+\alpha)>$$

$$V+2\lambda z-2z=V+2(\lambda-1).$$

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

② Note that the valuation has same parity with s. When $z\geqslant1$, we have that $v(g(m)g(m+s))>V+2$. 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 $z\geqslant1$, we have that $v(g(m)g(m+s))>V+4$. 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 3.1 Let p be a prime prime to d. Let n be a positive integer such that $p^n\equiv1 \bmod d$. For any $r\in\mathbb{Z}$ or $\mathbb{Z}/d\mathbb{Z}$, write $a_j\equiv rp^{-j} \bmod d$ with $0\leqslant a_j\leqslant d-1$. Define

$$V_r:=\frac{1}{n}\sum_{j=0}^{n-1}\min\{\delta_j+\frac{a_{j+1}p-a_j}{d},\ p-\delta_j-\frac{a_{j+1}p-a_j}{d}\}\tag{2}$$

where

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

This definition does not depend on the choice of n.

Proposition 3.2 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

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

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

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

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

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 3.3① and then the valuation of $\mathrm{Kl}(q,\ a,\ \chi^r)$ is kV_r by Lemma 3.2.

Definition 3.2 For any $s\in\mathbb{Z}$ or $\mathbb{Z}/d\mathbb{Z}$, define

$$T^s_{p,\ d}:=\{r \bmod d\mid (r,\ d)=1,\ V_{rs}=V_s\}\subseteq(\mathbb{Z}/d\mathbb{Z})^\times\tag{3}$$

Define

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

Proposition 3.3 Assume that $p>3d-2$.

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

② If $p\equiv\pm1 \bmod d$, then $T_{p,\ d}=\{\pm1\}$.

③ If $4\mid d\geqslant16$ and $p\equiv d/2\pm1 \bmod d$, then $T_{p,\ d}=(\mathbb{Z}/d\mathbb{Z})^\times$.

④ If $3\leqslant d\leqslant31$ and $(p,\ d)$ does not satisfies ③, then $T_{p,\ d}=\{\pm p^\lambda \bmod d\mid\lambda\in\mathbb{Z}\}$.

Proof ① If $r_1,\ r_2\in T_{p,\ d}$, then $V_{r_1r_2^{-1}s}=V_{r_2^{-1}s}=V_s$. Thus $r_1r_2^{-1}\in T_{p,\ d}$ 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 $p\equiv\pm1 \bmod d$, we have

$$V_r=\frac{p\mp1}{d}\cdot\min\{r,\ d-r\}\tag{4}$$

③ If $p\equiv d/2\pm1 \bmod d$, then

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

Thus $V_r=(p\pm1)k/4$ and $T_{p,\ d}=(\mathbb{Z}/d\mathbb{Z})^\times$. When $4\mid d\geqslant16$, $\varphi(d)>4$. Hence $T_{p,\ d}$ does not equal $\langle-1,\ p\rangle$.

④ We have already know the case $p\equiv\pm1 \bmod d$ 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.

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

d	$\pm\bar{p}$	$rH/\{\pm 1\}$	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	$\{1, 7\}$	$(p\mp 1)/4$
		$\{3, 5\}$	
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	$\{1, 9\}$	$(p\mp 1)/4$
		$\{3, 7\}$	
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	$\{1, 11\}$	$(p\mp 1)/4$
		$\{5, 7\}$	
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	$\{1, 3, 9\}$	$(p\mp 1)/6$
		$\{5, 7, 11\}$	$(23p\pm 1)/78$
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	$\{1, 13\}$ $\{3, 11\}$ $\{5, 9\}$	$(p\mp 1)/4$
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	$p/4$
	9	every coset	
	15	every coset	$(p\mp 1)/4$

Remark 3.1 ① One may expect that $T^s_{p,d}$ is also a group. Unfortunately it's not true. For instance, take $d=33, p\equiv\pm10 \bmod 33$, then $T^1_{p,d}=\{\pm1, \pm4, \pm7, \pm10\}$.

② One can find more pairs (p, d) such that $T_{p,d}\neq\langle-1, p\rangle$ like Proposition 3.3③, 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 do not have a proof or a counterexample.

Proposition 3.4 Assume that $d\geqslant3$ and $p>5d-2$. If $p\equiv\pm1 \bmod d$ and $\mathrm{Tr}(a)\neq0$, then $\mathrm{Kl}(q, a, \chi)$ generates $\mathbb{Q}(\mu_{dp})^H$, where

$$H=\begin{cases}\langle\tau_{-1}, \sigma_{-1}\rangle, \text{if } \chi(-1)=1 \text{ and } \chi(a)=1;\\ \langle\sigma_{-1}\rangle, \text{if } \chi(-1)=1 \text{ and } \chi(a)=-1;\\ \langle\tau_{-1}\rangle, \text{if } \chi(-1)=-1 \text{ and } \chi(a)=1;\\ \langle\tau_{-1}\sigma_{-1}\rangle, \text{if } \chi(-1)=-1 \text{ and } \chi(a)=-1;\\ \{1\}, \text{if } \chi(-1)=-1 \text{ and } \chi(a)\neq\pm1.\end{cases}$$

Proof We may assume that $\chi=\omega^{-(q-1)/d}$. Denote by M_r the M in Lemma 3.3 for $s=(q-1)r/d$. By Lemma 3.3 and Proposition 3.2, we have

$$\begin{aligned}&(q-1)\mathrm{Kl}(q, a, \chi^r)\equiv\\ &\omega^{M_r}(a)g(M_r)g\Big(M_r+\frac{q-1}{d}\Big)+\\ &\sum_{i=0}^{k-1}\omega^{M_r+p^i}(a)g(M_r+p^i)g\Big(M_r+\frac{q-1}{d}+p^i\Big)\equiv\\ &\omega^{M_r}(a)g(M_r)g\Big(M_r+\frac{q-1}{d}\Big)+\\ &C\pi^{kV_r+2}\omega^{M_r}(a)\omega(\mathrm{Tr}(a)) \bmod \mathfrak{P}^{kV_r+3}\end{aligned}\tag{5}$$

where C is a constant prime to p.

By Lemma 3.1①, we have

$$\begin{aligned}\tau_w\sigma_t\,\mathrm{Kl}(q, a, \chi)&=\chi(t)^{-w}\,\mathrm{Kl}(q, t^2a, \chi^w)=\\ &\chi(ta)^w\,\mathrm{Kl}(q, t^2a, \chi^{-w})\end{aligned}\tag{6}$$

If $\tau_w\sigma_t$ fixes $\mathrm{Kl}(q, a, \chi)$, then $V_w=V_1$. Thus $w=\pm1$ by Proposition 3.3②. 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

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

Since $\omega(\mathrm{Tr}(a))\neq0$, we have $\omega(t^2)=1, t=\pm1$ 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

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

Since $\omega(\mathrm{Tr}(a))\neq0$, we have $\omega(t^2)=1, t=\pm1$ 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 3.1 Assume that $3\leqslant d\mid(q-1), p>5d-2, a\in\mathbb{F}_p^\times$ 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

$$H=\begin{cases}\langle\tau_p, \tau_{-1}, \sigma_{-1}\rangle, \text{if } \chi(-1)=1 \text{ and } \chi(a)=1;\\ \langle\tau_p, \sigma_{-1}\rangle, \text{if } \chi(-1)=1 \text{ and } \chi(a)=-1;\\ \langle\tau_p, \tau_{-1}\rangle, \text{if } \chi(-1)=-1 \text{ and } \chi(a)=1;\\ \langle\tau_p, \tau_{-1}\sigma_{-1}\rangle, \text{if } \chi(-1)=-1 \text{ and } \chi(a)=-1;\\ \langle\tau_p\rangle, \text{if } \chi(-1)=-1 \text{ and } \chi(a)\neq\pm1.\end{cases}$$

In particular, this holds for $d\leqslant31$ 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 Equations (5), (6) and Proposition 3.2. Then $w\in T_{p,d}$ and $w\equiv\pm p^\lambda \bmod d$ for some λ. For $w\equiv p^\lambda$, by Lemma3.1②, we have

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

Similar to the proof of Proposition 3.4, if $\mathrm{Tr}(a)\neq0$, we have $\omega(t^2)\equiv1$ and then $t=\pm1, \chi(t)=1$.

For $w\equiv-p^\lambda$, by Lemma 3.1②, we have

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

Similarly, if $\mathrm{Tr}(a)\neq0$, we have $t=\pm1$ and $\chi(ta)=1$.

The last claim follows from Proposition 3.3④.

4 The partial Gauss sums

In this section, we will study the partial Gauss sum

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

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 $g(q, a, \chi)=\chi(a)g(q, a, \bar{\chi})$.

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 and 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

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

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

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

We will consider the cases $d\mid(q\pm1)$ respectively.

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

Proposition 4.1 Assume that $d\mid(q-1)$ and $p>2$. If $\mathrm{Tr}(a)\neq0$, then $g(q,a,\chi)$ generates $\mathbb{Q}(\mu_{dp})^{H}$, where

$$H=\{\tau_w\sigma_{\pm1}\mid w\equiv1 \bmod d_1\}$$

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

Proof We have

$$g(q,a,\chi^{r})=\omega^{-(q-1)r/d}(a)g(q,a,\mathbf{1}) \tag{7}$$

and

$$(q-1)g(q,a,\mathbf{1})\equiv 1+\omega(\mathrm{Tr}(a))g(q+1) \bmod \mathfrak{P}^3 \tag{8}$$

by Lemma 4.2. Since

$$\tau_w\sigma_t g(q,a,\chi)=\sum_{xx^{\delta}=at^2}\chi^{w}(xt^{-1})\zeta^{\mathrm{Tr}'(x)}=\chi^{-w}(t)g(q,at^2,\chi^{w}) \tag{9}$$

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

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

If $\mathrm{Tr}(a)\neq0$, then $t=\pm1$ and $\chi(t)=\omega^{-(q-1)/d}(t^{q+1})=1$. Then $w\equiv1 \bmod d_1$ 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 4.3 Let s be a positive integer less than $(q-1)/2$. Let s_j, δ_j, M, V be the notations as in Lemma 3.3. Assume that $|(p-1)/2-s_j|>3$ for all j; $s_0\geqslant2$ and not all δ_j are same.

① The valuation $v(g((q+1)m+s))$ is

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

② The valuation $v(g((q+1)m-s))$ is

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

Proof By the assumptions, $p\geqslant11$ and $s_{k-1}\leqslant(p-9)/2$. Then $s<(p-7)p^{k-1}/2$ and

$$M=\sum_{\delta_j=1}(p-\delta_{j-1}-s_j)p^{j}\leqslant\sum_{j=0}^{k-2}p^{1+j}<\frac{11}{10}p^{k-1}.$$

Thus

$$M+2\delta_0-1+p^{i}+p^{i'}+s<(\frac{11}{10}+2+\frac{p-7}{2})p^{k-1}+2<q \tag{10}$$

Denote by g_q the Gauss sum with respect to $\mathbb{F}_q$.

① If $m+s\geqslant q$, then

$$v(g((q+1)m+s))=v(g_q(m+s-q)g_q(m+1))=v(g_q(m+s-1)g_q(m+1)).$$

Since $s-2$ has same δ_i sequence as s, by Lemma 3.3, 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 (10), these three cases do not happen and the valuation is at least $V+4$.

If $m+s<q$, then

$$v(g((q+1)m+s))=v(g_q(m)g_q(m+s)).$$

By Lemma 3.3, 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

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

where $m'=m+q-s$. Since $s-2$ has same δ_i sequence as s, by Lemma 3.3, 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 (10). But $m<s$, these three cases do not happen and then the valuation is at least $V+4$.

If $m\geqslant s$, then

$$v(g((q+1)m-s))=v(g_q(m-s)g_q(m)).$$

By Lemma 3.3, the valuation is

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

The result then follows.

Proposition 4.2 If $p>7d-2$, then the valuation of $g(q,a,\chi^{r})$ is kV_{2r}.

Proof If $r\equiv0, d/2 \bmod d$, 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 (7) and (8).

If $r\not\equiv0, d/2 \bmod d$, by Lemma 4.1① and the fact that $V_{2r}=V_{-2r}$, we may assume that $1\leqslant r<d/2$. Write

$$\frac{q^2-1}{d}r=s_L+qs_M,$$

$$s_L=\frac{(d-r)q-r}{d},$$

$$s_M=\frac{rq-(d-r)}{d}.$$

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 $0 \leqslant b_j \leqslant d-1$. By Lemmas 4.2, 4.3 and

$$g((q+1)m + \frac{q^2-1}{d}r) =$$

$$\begin{cases} g((q+1)(m+s_M+1) - 2r\frac{q+1}{d}), \text{if } 1 \leqslant r < \frac{d}{4}; \\ g((q+1)(m+s_M) + (d-2r)\frac{q+1}{d}), \text{if } \frac{d}{4} \leqslant r < \frac{d}{2}, \end{cases}$$

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

Definition 4.1 Let $p > 7d-2$ be a prime prime to d.

$$T'_{p,d} := \bigcap_{(s,d)=1} T_{p,d}^{2s} = \{r \bmod d \mid (r,d) = 1,$$

$$V_{2rs} = V_{2s}, \forall (s,d) = 1\} \subset (\mathbb{Z}/d\mathbb{Z})^\times,$$

where $T_{p,d}^s$ is defined as Equation(3).

Proposition 4.3 Assume that $p > 7d-2$.

① If d is odd, then $T'_{p,d} = T_{p,d}$. If d is even, then $T'_{p,d} = \{r \mid r \bmod d/2 \in T_{p,d/2}\}$. 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 mod d, then $T'_{p,d} = \langle d/2+1, p\rangle$ if $d/(2,d) \leqslant 31$.

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 3.3②. ③ follows from ①. For ④, $p \not\equiv \pm(d/4+1) \bmod d/2$ if $4 \mid d/2 \geqslant 16$. Then the result follows from ① and Proposition 3.3④.

Proposition 4.4 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 4.1 and we may assume that $d \geqslant 3$.

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 4.3, 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

$$(q-1)g(q, a, \chi^r) \equiv$$

$$\omega^{M_r}(a)g(N_r) + \sum_{i=0}^{k-1}\omega^{M_r+p^i}(a)g(N_r + (q+1)p^i) =$$

$$\omega^{M_r}(a)g(N_r) + \sum_{i=0}^{k-1}\omega^{M_r+p^i}(a)g(N_r + (q+1)p^i) =$$

$$\omega^{M_r}(a)g(N_r) + C\pi^{kV_{2r}+2}\omega^{M_r}(a)\omega(\mathrm{Tr}(a)) \bmod \mathfrak{P}^{kV_{2r}+3} \quad (11)$$

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

$$g(q, a, \chi^{-r}) = g(q, a, \chi^r),$$

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

If $\tau_w\sigma_t$ fixes $g(q, a, \chi)$, then by (9), $V_{2w} = V_2$. Thus $w \equiv \pm 1, \pm(d/2+1) \bmod d$ by (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 4.1 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 $d/(2,d) \leqslant 31$.

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 (9), (11) and Proposition 4.2. 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 4.1②, we have

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

Similar to the proof of Proposition 4.4, 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 ②③, we have

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

Thus $\chi_2(a) = 1$ by (11). Similarly, if $\mathrm{Tr}(a) \neq 0$, we have $t = \pm 1$.

Acknowledgments

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

Conflict of interest

The author declares no conflict of interest.

Author information

ZHANG Shenxing is a post-doctoral fellow at the University of

Science and Technology of China. He received his PhD from the University of Science and Technology of China, under the supervision of Professor OUYANG Yi. His research interests focus on elliptic curves, class groups and character sums.

References

[1] Davenport H, Hasse H. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. J. Reine Angew. Math., 1935, 172: 151-182.
[2] Wan D. Algebraic theory of exponential sums over finite fields. https://www.math.uci.edu/~dwan/Wan_HIT_2019.pdf.
[3] Zhang S. The degrees of exponential sums of binomials. https://arxiv.org/abs/2010.08342.
[4] Wan D, Yin H. Algebraic degree periodicity in recurrence sequences. https://arxiv.org/abs/2009.14382.
[5] Bombieri E. On exponential sums in finite fields. II. Invent. Math., 1978, 47: 29-39.
[6] Wan D. Minimal polynomials and distinctness of Kloosterman sums. Finite Fields and Their Applications, 1995, 1: 189-203.
[7] Fisher B. Distinctness of Kloosterman sums. In: *p*-Adic Methods in Number Theory and Algebraic Geometry. Providence, RI: Amer. Math. Soc., 1992.
[8] Kononen K, Rinta-aho M, Väänänen K. On the degree of a Kloosterman sum as an algebraic integer. https://arxiv.org/abs/1107.0188.
[9] Katz N M. Gauss Sums, Kloosterman Sums, and Monodromy Groups. Princeton, NJ: Princeton University Press, 1988.
[10] Stickelberger L. Ueber eine Verallgemeinerung der Kreistheilung. Math. Ann., 1890, 37(3): 321-367.
[11] Washington L C. Introduction to Cyclotomic Fields. New York: Springer-Verlag, 1982.

两类扭 Kloosterman 和的生成域

张神星*

中国科学技术大学数学科学学院中科院吴文俊数学重点实验室,安徽合肥 230026

* 通讯作者. E-mail:zsxqq@mail.ustc.edu.cn

摘要: 研究了扭 Kloosterman 和 $\mathrm{Kl}(q, a, \chi)$ 和部分高斯和 $g(q, a, \chi)$ 的生成域. 我们要求特征 p 相对于 χ 的阶 d 充分大,且系数 a 的迹非零. 当 $p \equiv \pm 1 \bmod d$ 时,可以确定这些特征和的生成域. 对于一般的 p,当 a 落在底域中时,提出了一个关于 (p, d) 的组合条件以得到生成域.

关键词: Kloosterman 和;指数和;分圆域;代数数