

MIXED EXPONENTIAL SUMS OVER FINITE FIELDS

FRANCIS N. CASTRO AND CARLOS J. MORENO

(Communicated by David E. Rohrlich)

ABSTRACT. In this paper we calculate the conductor of a character that consists of the product of an additive and a multiplicative character. This computation improves the bound for exponential sums given by G. I. Perel'muter. This calculation gives an easy method to compute the conductor associated to a character of the Galois group of the composite of an Artin-Schreier extension and a Kummer extension.

1. INTRODUCTION

Exponential sums over the projective line were studied by A. Weil as applications of his proof of the Riemann Hypothesis for function fields (see [9]). In [1], Bombieri showed how to extend the results of Weil to more general exponential sums (in several variables) over arbitrary algebraic curves. Mixed exponential sums are built with multiplicative and additive characters and they have appeared in the work of Perel'muter ([6, Theorem 1]). In this paper we strengthen the estimates of Perel'muter concerning such mixed exponential sums.

Let ψ be an additive character of the finite field \mathbf{F}_q and χ a multiplicative character of \mathbf{F}_q^\times of order n . Let X be a non-singular projective algebraic curve of genus g_X and consider two rational functions $f, g \in \mathbf{F}_q(X)$ which satisfy $f \neq h^p - h$ (resp. $g \neq h^n$) for $h \in \overline{\mathbf{F}}_q(X)$. These two functions define maps to the affine line $f, g : X \rightarrow \mathbf{A}$ and we can construct the exponential sum

$$S_m(f, g, X) = \sum'_{x \in X_m} \chi(N(g(x)))\psi(\text{Tr}(f(x))),$$

where the sum runs over the points on X which are rational over \mathbf{F}_{q^m} and N, Tr denote the usual norm and trace from \mathbf{F}_{q^m} to \mathbf{F}_q and the prime in the summation denotes that the poles of f, g are to be excluded. Then, the principal result of Perel'muter ([6, Theorem 1]) is the estimate

$$|S_m(f, g, X)| \leq (2g_X - 2 + s + l + \deg((f)_\infty))q^{m/2},$$

where l is the number of poles of f , s is the number of points in the support of the divisor (g) of g and $\deg((f)_\infty)$ is the degree of the polar part of the divisor of f . As an application of our results we prove the following theorem.

Theorem. *With notation and assumptions as above we have*

$$|S_m(f, g, X)| \leq (2g_X - 2 + s + l + \deg((f)_\infty) - r)q^{m/2},$$

Received by the editors October 7, 1998.

1991 *Mathematics Subject Classification.* Primary 11L40; Secondary 11S15.

where r is the number of closed points common to the support of $(f)_\infty$ and the divisor (g) .

The proof of this result is given in section 4. The principal tool here is the calculation of the conductor given in section 3 for the composite field of an Artin-Schreier extension associated to f and a Kummer extension associated to g . In section 5 we give some examples. Section 2 is a summary of some results from ramification theory which are used throughout the paper.

2. SUMMARY OF RESULTS FOR RAMIFICATION GROUPS

In this section we review all the facts that we need in the rest of the paper. We follow the notation of Serre and the proof of all the theorems that we quote in this section can be found in [7, Chapters 5,6].

Let \mathbf{k} be a complete field under the discrete valuation $ord_{\mathbf{k}}$. Let $A_{\mathbf{k}}$ be the valuation ring of the field \mathbf{k} , and $M_{\mathbf{k}}$ be its maximal ideal. Let $\overline{\mathbf{k}} = A_{\mathbf{k}}/M_{\mathbf{k}}$. Let \mathbf{K} be a finite Galois extension of \mathbf{k} and let $A_{\mathbf{K}}$ be the integral closure of $A_{\mathbf{k}}$ in \mathbf{K} . $A_{\mathbf{K}}$ is a complete discrete valuation ring. Let $ord_{\mathbf{K}}$ be the discrete valuation of \mathbf{K} and $M_{\mathbf{K}}$ be the maximal ideal of $A_{\mathbf{K}}$. Let $A_{\mathbf{K}}/M_{\mathbf{K}} = \overline{\mathbf{K}}$. We assume that $\overline{\mathbf{K}}/\overline{\mathbf{k}}$ is a separable extension. Let G be the Galois group of the extension \mathbf{K}/\mathbf{k} .

Definition 1. For an integer $i \geq -1$, the i -th ramification group G_i of G is defined to be

$$G_i = \{ \sigma \in G \mid ord_{\mathbf{K}}(\sigma(t) - t) \geq i + 1 \text{ for all } t \in A_{\mathbf{K}} \}.$$

It is clear that the G_i form a decreasing sequence of normal subgroups of G and there is an i_0 such that $G_{i_0} = 1$.

Theorem 2. *If the characteristic of $\overline{\mathbf{K}}$ is $p > 0$, then the quotients G_i/G_{i+1} , $i \geq 1$, are abelian groups, and are direct products of cyclic groups of order p . The group G_1 is a p -group.*

The proof of Theorem 2 as well as that of the following can be found in [7, Chapter 4.1].

Theorem 3. *The integers $i \geq 1$ such that $G_i \neq G_{i+1}$ are all congruent to one another mod p .*

The two most fundamental results from ramification theory that we use in section 3 are those of Herbrand and Hasse-Arf. We now recall their statement. We define first the function φ . Let $u \in [-1, \infty)$; then G_u denotes the ramification group G_i , where i is the smallest integer $\geq u$.

Definition 4. For a real number $u \geq -1$ we put

$$\varphi_{\mathbf{K}/\mathbf{k}}(u) = \int_0^u \frac{dt}{[G_0 : G_t]}.$$

It is clear that if $u \in [m, m + 1]$, where m is a positive integer, then

$$\varphi_{\mathbf{K}/\mathbf{k}}(u) = \frac{1}{g_0}(g_1 + \dots + g_m + (u - m)g_{m+1}), \text{ where } g_i = |G_i|.$$

Let H be a subgroup of G and \mathbf{K}' be its corresponding field. We can now state Herbrand's theorem.

Theorem 5 (Herbrand). *If $v = \varphi_{\mathbf{K}/\mathbf{K}'}(u)$, then*

$$G_u H/H = (G/H)_v.$$

The proof can be found in [7, Chapter 4.1]. Now we state Hasse-Arf's theorem.

Theorem 6 (Hasse-Arf). *If G is an abelian group, and if v is a jump in the filtration G^v , then v is an integer; equivalently, if $G_i \neq G_{i+1}$, then $\varphi_{\mathbf{K}/\mathbf{k}}(i)$ is an integer.*

The proof of Theorem 6 can be found in [7, Chapter 5.7].

The following is the definition of the Artin conductor of a character of G .

Definition 7. Let \mathbf{L}/\mathbf{K} be a finite Galois extension with Galois group G and let \mathbf{K} be a local field. Let λ be a character of G of dimension $\lambda(1)$. The conductor of λ is defined by:

$$\mathcal{F}(\lambda) = \sum_{i \geq 0} \frac{g_i}{g_0} (\lambda(1) - \lambda(G_i)),$$

where g_i is the order of the i -th ramification group G_i of G and

$$\chi(G_i) = \frac{1}{g_i} \sum_{\sigma \in G_i} \lambda(\sigma).$$

We now prove another equivalent definition of the conductor of λ when λ is a character of degree 1.

Theorem 8. *Let λ be a character of degree 1 on G . Let c_λ be the largest integer for which the restriction of λ to the ramification group G_{c_λ} is not the trivial character (if $\lambda = 1$, take $c_\lambda = -1$). Then*

$$\mathcal{F}(\lambda) = \varphi_{\mathbf{K}/\mathbf{k}}(c_\lambda) + 1.$$

Proof. As for the proof we note that if $c_\lambda \geq i$, then $\chi(G_i) = 0$ and if $c_\lambda < i$, then $\chi(G_i) = 1$. The substitution of these values in the definition of conductor and using the definition of $\varphi_{\mathbf{K}/\mathbf{k}}$ gives

$$\begin{aligned} \mathcal{F}(\lambda) &= \sum_{i \geq 0} \frac{g_i}{g_0} (\lambda(1) - \lambda(G_i)) \\ &= \sum_{i=0}^{c_\lambda} \frac{g_i}{g_0} \\ &= \varphi_{\mathbf{K}/\mathbf{k}}(c_\lambda) + 1. \end{aligned}$$

□

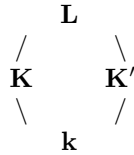
This result will be used in the next section to study the jumps in the ramification filtration for the Galois groups of composite extensions.

3. RAMIFICATION GROUPS OF THE COMPOSITE FIELD OF AN ARTIN-SCHREIER AND A KUMMER EXTENSION

In this section, we compute the filtration of the ramification groups of the composite field of an Artin-Schreier and a Kummer extension.

Let \mathbf{k} be a local field of characteristic p . Let \mathbf{K} be an Artin-Schreier extension of \mathbf{k} , i.e., \mathbf{K}/\mathbf{k} is a separable field of degree p . We assume that \mathbf{K}/\mathbf{k} is a totally ramified Artin-Schreier extension. Recall that the Galois group $G(\mathbf{K}/\mathbf{k})$ of the

extension \mathbf{K}/\mathbf{k} is isomorphic to \mathbf{Z}/p . We identify $G(\mathbf{K}/\mathbf{k})$ with \mathbf{Z}/p . Let \mathbf{K}' be a Kummer extension of \mathbf{k} of degree n , i.e., \mathbf{K}'/\mathbf{k} is a cyclic extension of degree n where n is relatively prime to p . Note that \mathbf{k} has to contain a primitive n -th root of unity. Recall that the Galois group $G(\mathbf{K}'/\mathbf{k})$ is isomorphic to \mathbf{Z}/n . We use this identification throughout this section. The fields \mathbf{K} and \mathbf{K}' are linearly disjoint. We assume that the extensions \mathbf{K}/\mathbf{k} and \mathbf{K}'/\mathbf{k} ramify at the same prime. Let $\mathbf{L} = \mathbf{K}\mathbf{K}'$ be the composite field of \mathbf{K} and \mathbf{K}' and let G be the Galois group of the field extension \mathbf{L}/\mathbf{k} . We can identify $G \simeq G(\mathbf{K}/\mathbf{k}) \times G(\mathbf{K}'/\mathbf{k})$ with $\mathbf{Z}/p \times \mathbf{Z}/n$.



We can identify the Galois group of the field extension \mathbf{L}/\mathbf{K} with $0 \times \mathbf{Z}/n$ and the Galois group of the field extension \mathbf{L}/\mathbf{K}' with $\mathbf{Z}/p \times 0$. We can assume that \mathbf{K}'/\mathbf{k} is totally ramified. Therefore, \mathbf{L}/\mathbf{k} is a totally ramified extension of degree np .

Let $G(\mathbf{K}/\mathbf{k})_0 = \dots = G(\mathbf{K}/\mathbf{k})_j \supset 0$ be the filtration groups of $G(\mathbf{K}/\mathbf{k})$ and let $G(\mathbf{K}'/\mathbf{k})_0 \supset 0$ be the filtration of the ramification groups of $G(\mathbf{K}'/\mathbf{k})$. We suppose that $G_0 \supset \dots \supset G_i \supset 0$ is the filtration of the ramification groups of G .

Theorem 9. *The filtration of the ramification groups of G is equal to*

$$G_0 \supset G_1 = \dots = G_{nj} \supset 0,$$

where $G_0 = \mathbf{Z}/p \times \mathbf{Z}/n$ and $G_1 = \mathbf{Z}/p \times 0$.

Proof. We have that $G_0 = G(\mathbf{K}/\mathbf{k}) \times G(\mathbf{K}'/\mathbf{k})$ and G_1 is a p -group, therefore $G_1 = G(\mathbf{K}/\mathbf{k}) = \mathbf{Z}/p \times 0$. We assume that $G_l = \mathbf{Z}/p \times 0$ and $G_{l+1} = (0, 0)$ for $l > 1$. Then $G(\mathbf{L}/\mathbf{K})_l = (0, 0)$. Therefore

$$\varphi_{\mathbf{L}/\mathbf{K}}(l) = \frac{1}{n} \overbrace{(1 + \dots + 1)}^l$$

and

$$\varphi_{\mathbf{L}/\mathbf{K}}(l + 1) = \frac{1}{n} \overbrace{(1 + \dots + 1 + 1)}^{l+1}.$$

Now, we use Herbrand's theorem to obtain

$$\begin{aligned}
 G_l G(\mathbf{L}/\mathbf{K}) / G(\mathbf{L}/\mathbf{K}) &\simeq (\mathbf{Z}/p \times 0)(0 \times \mathbf{Z}/n) / (0 \times \mathbf{Z}/n) \\
 &\simeq \mathbf{Z}/p \\
 &\simeq \left(G / G(\mathbf{L}/\mathbf{K}) \right)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} \\
 &= \left(G / G(\mathbf{L}/\mathbf{K}) \right)_{\frac{l}{n}}.
 \end{aligned}$$

We thus get $\frac{l}{n} \leq j$, and

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &\simeq 0 \\ &\simeq \left(G/G(\mathbf{L}/\mathbf{K}) \right)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} \\ &= \left(G/G(\mathbf{L}/\mathbf{K}) \right)_{\frac{l}{n} + \frac{1}{n}}. \end{aligned}$$

This implies that $\frac{l}{n} + \frac{1}{n} > j$. The above two inequalities yield

$$(1) \quad \frac{l}{n} \leq j < \frac{l}{n} + \frac{1}{n}.$$

By the Hasse-Arf theorem

$$\varphi_{\mathbf{L}/\mathbf{k}}(l) = \frac{1}{pn}(g_1 + \dots + g_l) = \frac{l}{n}$$

is an integer. Therefore n divide l . Hence, the first inequality of (1) becomes an equality, i.e., $j = \frac{l}{n}$. If we solve for l , we get $l = nj$. This proves the theorem. \square

Remark. If $\lambda \neq 1$ is a character of G , then

$$\mathcal{F}(\lambda) = \begin{cases} 1 & \text{if } \lambda(G(\mathbf{K}/\mathbf{k})) = 1, \\ j + 1 & \text{otherwise.} \end{cases}$$

The above remark is going to be used in the proof of Lemma 11.

4. APPLICATIONS TO EXPONENTIAL SUMS

In this section we use Theorem 9 to estimate the degree of the L -function associated to a character of the composite field of an Artin-Schreier extension and a Kummer extension. The result obtained is applied to mixed exponential sums in one variable.

Let X be a complete non-singular curve of genus g_X , defined over \mathbf{F}_q ($q = p^k$). Let \mathbf{k} be its function field, and let $\mathbf{k}\overline{\mathbf{F}}_q(X)$ be the function field of X considered as a curve over the algebraic closure $\overline{\mathbf{F}}_q$ of \mathbf{F}_q . Let $f, g \in \mathbf{k}$ be rational functions on X , satisfying the condition

$$(2) \quad f \neq h^p - h \text{ for } h \in \mathbf{k}\overline{\mathbf{F}}_q(X),$$

$$(3) \quad g \neq h^n \text{ for } h \in \mathbf{k}\overline{\mathbf{F}}_q(X).$$

Let \mathbf{K}/\mathbf{k} be the function field of the curve defined by the equation $y^p - y = f$ and \mathbf{K}'/\mathbf{k} be the function field of the curve defined by the equation $z^n = g$. We assume that $(n, p) = 1$ and \mathbf{F}_q contains a n -th root of unity. Let \mathbf{L} be the composite field of \mathbf{K} and \mathbf{K}' and G be its Galois group. Let Y be a smooth model for the function field \mathbf{L} and $\pi : Y \rightarrow X$ be its corresponding covering. Let λ be a character of G . Now we define the L -function associated to the character λ of G .

Definition 10. With the above assumptions and notation, the L -function associated to λ, X is defined by

$$L(t, Y, X, \lambda) = \prod_{P \in X} (1 - \lambda(F_P)t^{\deg(P)})^{-1},$$

where the product is over all unramified closed points of X and F_P is the Frobenius automorphism.

It is well known that $L(t, Y, X, \lambda)$ is a polynomial in t of degree $2g_X - 2 + D$, where D is the conductor of λ . By the Riemann hypothesis, the roots of $L(t, Y, X, \lambda)$ have absolute value equal to $q^{1/2}$.

Let $(f)_\infty$ be the divisor of the poles of f on X , and write

$$(f)_\infty = \sum_{i=1}^l a_i P_i,$$

where a_i is the order of the pole of f at P_i . Let (g) be the divisor corresponding to g , and write

$$(g) = \sum_{i=1}^s b_i Q_i,$$

where b_i is the order of g at Q_i .

Remarks. 1. The covering $\pi : Y \rightarrow X$ can ramify at the poles P_i of f and if $(p, a_i) = 1$, then ramification does occur.

or

2. The covering $\pi : Y \rightarrow X$ can ramify at the zeros or poles Q_i of g and if n does not divide b_i , then ramification does occur.

Let r be the number of closed points of X that $(f)_\infty$ and (g) have in common.

Lemma 11. *With the above notation and assumptions, we have*

$$(4) \quad \deg(L(t, Y, X, \lambda)) \leq 2g_X - 2 + s + l + \deg((f)_\infty) - r.$$

Moreover, we have equality in (4) if $(a_i, p) = 1$ for all $i = 1, \dots, l$ and n does not divide b_i for all $i = 1, \dots, s$.

Proof. We need to compute the conductor of λ . We are going to prove that $D \leq s + l + \deg((f)_\infty) - r$. Without loss of generality, we only need to consider in the calculation of the conductor of λ the closed points of X that appear in $(g) \cup (f)_\infty$. The question here is local, therefore we work in the completion of \mathbf{k} . Let P be a closed point in the support of $(g) \cup (f)_\infty$ ($P = P_i$ or Q_j for some i and j). If P does not divide g , then $P = P_i$ for some i and the local conductor is less than or equal to $a_i + 1$ (recall that P_i is a pole of f and a_i is the order of the pole P_i of f on X). The local conductor is equal to $a_i + 1$ if $(a_i, p) = 1$. If P does not divide $(f)_\infty$, then $P = Q_i$ for some i and the local conductor less than or equal to 1. The local conductor is equal to 1 if n does not divide b_i . If P is a closed point of X that divides $(f)_\infty$ and (g) , then $P = P_i = Q_j$ for some i and j . By Theorem 8 and Theorem 9 the local conductor is less than or equal to $a_i + 1$, where a_i is the order of the pole of f at P_i (see Remark of the previous section). The local conductor is equal to $a_i + 1$ if $(a_i, p) = 1$. Note that if $(a_i, p) = 1$, the local conductor is not affected by either n divides b_j or n does not divide b_i . If we put together all the contributions from the closed points appearing in $(f)_\infty$ and (g) , we get what we want. If $(a_i, p) = 1$ for all $i = 1, \dots, l$ and n does not divide b_i for all $i = 1, \dots, s$, then $D = l + s - r + \deg((f)_\infty)$. This proves the lemma. \square

The exponential sum associated to X, λ is defined as the coefficient of t in

$$t \frac{d \log(L(t, Y, X, \lambda))}{dt}.$$

Definition 12. With assumptions and notation as above, the exponential sum $S_m(X, \lambda)$ associated to X, λ is defined by

$$S_m(X, \lambda) = \sum_{\substack{P \in X \\ \deg(P)=m}} ' \lambda(F_p),$$

where the sum runs over the closed points of degree m in X and the prime in the summation means that the ramified points of X are excluded.

If we replace \mathbf{F}_q by \mathbf{F}_{q^m} in Lemma 11, the degree of $L(Y, X, \lambda)$ does not change and the roots of $L(Y, X, \lambda)$ have absolute value $q^{m/2}$.

As preparation for the statement and proof of the main result, we note the following corollary.

Corollary 11.1. *With assumptions and notation as above, we have*

$$S_m(X, \lambda) = - \sum_{i=1}^d \theta_i,$$

where

$$|\theta_i| = q^{m/2}$$

and

$$(5) \quad d \leq 2g_X - 2 + s + l + \deg((f)_\infty) - r.$$

Moreover, we have equality in (5) if $(a_i, p) = 1$ for all $i = 1, \dots, l$ and n does not divide b_i for all $i = 1, \dots, s$.

Proof. By Lemma 11, $L(t, Y, X, t)$ is a polynomial in t of degree $\leq 2g_X - 2 + s + l + \deg((f)_\infty) - r$, with equality if $(a_i, p) = 1$ for all $i = 1, \dots, l$ and n does not divide b_i for all $i = 1, \dots, s$. By the Riemann Hypothesis for $L(t, Y, X, \lambda)$, we have $|\theta_i| = q^{m/2}$ for $i = 1, \dots, d$. This proves the corollary. \square

We can assume that $\lambda = \chi\psi$, where ψ is an additive character of \mathbf{F}_q and χ is a multiplicative character of \mathbf{F}_q^\times . Let X_m be the set of points of X defined over F_{q^m} . The exponential sum associated to f, g and X is defined by

$$S_m(f, g, X) = \sum_{x \in X_m} ' \chi(N(g(x)))\psi(Tr(f(x))),$$

where the summation is over the points of X_m except the poles of f, g and Tr is the trace map from \mathbf{F}_{q^m} to \mathbf{F}_q and N is the norm map from $\mathbf{F}_{q^m}^\times$ to \mathbf{F}_q . If $\pi : Y \rightarrow X$ is ramified at all points of $(g) \cup (f)_\infty$, then

$$S(X, \lambda) = S(f, g, X).$$

Note that if $(a_i, p) = 1$ for all $i = 1, \dots, l$ and n does not divide b_i for all $i = 1, \dots, s$, then the covering π is ramified at all points of $(g) \cup (f)_\infty$.

We can now state the main theorem of this section.

Theorem 13. *Let X be a complete non-singular curve over \mathbf{F}_q of genus g_X and let f and g be two rational functions on X satisfying condition (2) and (3). Then*

$$|S_m(f, g, X)| \leq (2g_X - 2 + l + s - r + \deg((f)_\infty))q^{m/2}.$$

Proof. If A is a set, then $|A|$ denotes the cardinality of A . Let

$$\begin{aligned} A &= \{ P \in X \mid P \text{ is a point of } (g) \cup (f)_\infty \text{ and } P \text{ is unramified} \}, \\ l_0 &= |\{ P_i \in A \mid (a_i, p) > 1 \}|, \\ s_0 &= |\{ Q_i \in A \mid n \text{ divides } b_i \}|, \\ r_0 &= |\{ P_i \in A \mid (a_i, p) > 1 \} \cap \{ Q_i \in A \mid n \text{ divides } b_i \}|. \end{aligned}$$

Note that $|A| = l_0 + s_0 - r_0$. We have

$$\sum_{\substack{P \in X \\ \deg(P)=m}} \lambda(F_P) = \sum_{x \in X_m} \chi(N(g(x)))\psi(\text{Tr}(f(x))) + \sum_{P \in A} \lambda(F_P).$$

Using Corollary 11.1, we have

$$\left| \sum_{x \in X_m} \chi(N(g(x)))\psi(\text{Tr}(f(x))) \right| \leq (2g_X - 2 + D)q^{m/2} + |A|,$$

where D is the conductor of λ . In this case $D = l - l_0 + s - s_0 - (r - r_0) + \deg((f)_\infty)$. Therefore

$$\begin{aligned} |S(f, g, X)| &\leq (2g_X - 2 + l - l_0 + s - s_0 - (r - r_0))q^{m/2} + l_0 + s_0 - r_0 \\ &\leq (2g_X - 2 + l - l_0 + s - s_0 - (r - r_0) + l_0 + s_0 - r_0)q^{m/2} \\ &= (2g_X - 2 + l + s - r)q^{m/2}. \end{aligned}$$

The second inequality is strict if $l_0 \neq 0$ and $s_0 \neq 0$. This proves the theorem. \square

5. EXAMPLES

Now we discuss some examples.

Example 1. Let $\psi(x) = (-1)^{\text{Tr}(x)}$ be an additive character of \mathbf{F}_4 and $\chi(\alpha^j) = e^{2\pi i j/3}$ be a multiplicative character of \mathbf{F}_4^\times , where α is a primitive element of \mathbf{F}_4 . We consider the exponential sum $S_m(f, g) = \sum_{x \in \mathbf{F}_{2^m}} \psi(f(x))\chi(g(x))$.

a. If $f(x) = x^3 + 1$ and $g(x) = x^3 + 1$, then by Theorem 13 we have

$$\deg(L(\mathbf{P}^1, f, g, \psi, \chi)) \leq 5.$$

We need to compute $S_m(\mathbf{P}^1, f, g)$ for $m = 1, \dots, 5$.

| $\mathbf{F}_{2^{2m}}$ | $S_m(x^3 + 1, x^3 + 1)$ |
|-----------------------|-------------------------|
| 1 | 1 |
| 2 | 7 |
| 3 | 13 |
| 4 | -17 |
| 5 | 61 |

Using the above table, we have

$$\begin{aligned} L(\mathbf{P}^1, x^3 + 1, x^3 + 1) &= 1 + t + 4t^2 + 8t^3 + 8t^4 + 32t^5 \\ &= (2t + 1)(4t^2 - 2t + 1)(4t^2 + t + 1). \end{aligned}$$

b. If $f(x) = \frac{1}{x+1}$ and $g(x) = x^2 + x$, then by Theorem 13 we have

$$\deg(L(\mathbf{P}^1, f, g, \psi, \chi)) \leq 2.$$

We need to compute $S_m(\mathbf{P}^1, f, g)$ for $m = 1, 2$.

| | |
|-----------------------|-------------------------------|
| $\mathbf{F}_{2^{2m}}$ | $S_m(x^2 + x, \frac{1}{x+1})$ |
| 1 | -2 |
| 2 | 4 |

Using the above table, we have $L(\mathbf{P}^1, x^2 + x, \frac{1}{x+1}) = 1 + 2t + 4t^2$. Note that Theorem 13 is tight in this case, i.e.,

$$S_m(x^2 + x, \frac{1}{x+1}) = 2^{m+1} = 2 \times q^{m/2}.$$

ACKNOWLEDGMENT

We would like to thank the referee for his valuable suggestions and for pointing out some mistakes. The referee's suggestions have made the paper clearer. We are also grateful to the editor.

REFERENCES

- [1] Bombieri, E., On exponential sums in finite fields *Am. J. Math.*, **88**(1966), 71-105. MR **34**:166
- [2] Deligne, P., Applications de la formule des traces aux sommes trigonometriques, SGA 4.5, *Lectures Notes In Math.*, **569**,(1977), 168-232.
- [3] Deligne, P., La conjecture de Weil II, *Publ. Math. I.H.E.S.* **52**(1981), 313-428.
- [4] Moreno, C. J., *Algebraic Curves over Finite Fields*, Cambridge Tracts in Mathematics, **97**, Cambridge Univ, Press, Cambridge, 1991. MR **92d**:11066
- [5] Katz, N., Gauss sums, and Monodromy groups, *Ann. of Math. Stud.*, Princeton, **116**, 988.N., Exponential sums and differential equations, *Ann. of Math. Studies*, Princeton, **124**, 1990.
- [6] Perel'muter, G. I., Estimation of a sum along an algebraic curve, *Mat. Zametki*, **5**(1969), 373-380. MR **39**:2764
- [7] Serre, J. P., *Local Fields*, Herman, Paris, 1968.
- [8] Stichtenoth, H., *Algebraic Fields and Codes*, Universitext Springer-Verlag, New York, 1991. MR **94k**:14016
- [9] Weil, A., On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.*, **34**(1948), 204-207. MR **10**:234e

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PUERTO RICO, RIO PIEDRAS, COLLEGE PARK
274 SALERNO, SAN JUAN, PUERTO RICO 00931

E-mail address: fcastro@goliath.cnet.clu.edu

DEPARTMENT OF MATHEMATICS, BARUCH COLLEGE, CUNY, P.O. BOX 545, N. SALEM, NEW
YORK 10560

E-mail address: carlos@kepler.baruch.cuny.edu