FINITE FIELDS AND THEIR APPLICATIONS 1, 395–398 (1995)

NOTE

A Note on Exponential Sums

NICHOLAS M. KATZ

Department of Mathematics, Princeton University, Princeton, New Jersey 08544
E-mail: nmk@princeton.edu

Communicated by Neal Koblitz

Received September 9, 1994

INTRODUCTION AND STATEMENT OF RESULTS

In this note, we will be concerned with estimating two sorts of exponential sums, especially in characteristic two. The interest of these estimates in characteristic two is that, when combined with some recent work of Evans [4], they prove that Terras's "upper half plane over a finite field" [9] is a "Ramanujan graph" in characteristic two (a result already known in odd characteristic). I thank Ron Evans for telling me about this problem.

In what follows, k is a finite field of characteristic p and cardinality q, $\psi\colon \mathbb{F}_p \to \mathbb{C}$ is a nontrivial additive character of the prime field $\mathbb{F}_p$, and $\psi_k\colon k \to \mathbb{C}$ denotes the nontrivial additive character of k given by

$$\psi_k(x) := \psi(\mathrm{Trace}_{k/\mathbb{F}_p}(x)).$$

THEOREM 1. *Let $\chi\colon k^\times \to \mathbb{C}$ be any nontrivial multiplicative character of k. For any b in k with $b \neq 0$, $b \neq 1$,*

$$\begin{aligned} \left|\textstyle\sum_{x \text{ in } k^\times, x^2+1\neq 0} \chi(x)\psi_k(bx/(x^2+1))\right| &\leq 4\ \mathrm{Sqrt}(q) \qquad \textit{if } p \textit{ odd} \\ &\leq 2\ \mathrm{Sqrt}(q) \qquad \textit{if } p = 2. \end{aligned}$$

1071-5797/95 $12.00

To state the second result, denote by K/k the quadratic extension of k, and by

$$N_{K/k}\colon K \to k, \qquad \mathrm{Tr}_{K/k}\colon K \to k,$$

the norm and trace maps. Denote by $U \subset K^\times$ the subgroup consisting of those elements x in $K^\times$ with $N_{K/k}(x) = 1$.

THEOREM 2. *Let $\chi\colon U \to \mathbb{C}$ be any nontrivial character of U. For any bink with $b \neq 0$, $b \neq 1$,*

$$\begin{aligned} |\textstyle\sum_{x \text{ in } U,\, \mathrm{Tr}_{K/k}(x)\neq 0} \chi(x)\psi_k(b/(\mathrm{Tr}_{K/k}(x)))| &\leq 4\ \mathrm{Sqrt}(q) \qquad \textit{if } p \textit{ odd} \\ &\leq 2\ \mathrm{Sqrt}(q) \qquad \textit{if } p = 2. \end{aligned}$$

Remark. In Theorem 2 above, note that for x in K of norm 1 to k, its trace to k is $x + 1/x = (x^2 + 1)/x$. Thus Theorem 2 bears a formal resemblance to Theorem 1. We will see that in fact Theorem 2 results from (the proof of) Theorem 1.

Proof of Theorem 1. Fix a prime number $l \neq p$, an isomorphism of $\overline{\mathbb{Q}}_l$ with $\mathbb{C}$, and consider the lisse $\overline{\mathbb{Q}}_l$-sheaf

$$\mathcal{F} := \mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi(bx/x^2+1)}$$

on the open set $\mathbb{A}^1_k[1/x(x^2 + 1)]$ of $\mathbb{A}^1_k$, where $x(x^2 + 1)$ is invertible. The sheaf $\mathcal{F}$ is lisse of rank one and pure of weight zero (being of finite order). By the Lefschetz trace formula [5],

$$\begin{aligned} &\textstyle\sum_{x \text{ in } k^\times, x^2+1\neq 0} \chi(x)\psi_k(bx/(x^2 + 1)) \\ &\qquad = \textstyle\sum_i (-1)^i \mathrm{Trace}(F_k \mid H^i_c(\mathbb{A}^1_k[1/x(x^2 + 1)] \otimes_k \bar{k}, \mathcal{F})). \end{aligned}$$

Since we are on a curve, the only possibly nonzero H^i_c have $0 \leq i \leq 2$. Because $\mathcal{F}$ is lisse and the curve is open, $H^0_c = 0$. What about H^2_c? The sheaf $\mathcal{F}$ is ramified at $x = 0$; indeed $\mathcal{L}_{\chi(x)}$ is ramified at $x = 0$ because χ is nontrivial, while $\mathcal{L}_{\psi(bn/x^2+1)}$ is lisse at $x = 0$. Therefore $\mathcal{F}$ is not geometrically constant and, hence, being of rank one, has $H^2_c = 0$. Thus our exponential sum is equal to

$$-\mathrm{Trace}(F_k \mid H^1_c(\mathbb{A}^1_k[1/x(x^2 + 1)] \otimes_k \bar{k}, \mathcal{F})),$$

and

$$\dim H^1_c(\mathbb{A}^1_k[1/x(x^2 + 1)] \otimes_k \bar{k}, \mathcal{F}) = -\chi_c(\mathbb{A}^1_k[1/x(x^2 + 1)] \otimes_k \bar{k}, \mathcal{F}).$$

By Weil [10], cf. also [3], we know that this H_c^1 is mixed of weight ≤ 1, so it suffices to show that

$$\chi_c(\mathbb{A}_k^1[1/x(x^2+1)] \otimes_k \bar{k}, \mathcal{F}) = -4, \qquad \text{if } p \text{ is odd,}$$
$$= -2, \qquad \text{if } p = 2.$$

For p odd, the sheaf $\mathcal{F}$ is tame at $x = 0$, while at $\pm i$ it has Swan conductor 1 [write $bx/(x^2+1) = ((b/2)(1/(x+i) + 1/(x-i))$], so the formula $\chi_c = -4$ is immediate from the Euler–Poincare formula [7].

For $p = 2$, it will be more convenient to write b as β^2 with β in k not 0 or 1. Then

$$\begin{aligned} bx/(x^2+1) &= \beta^2 x/(x+1)^2 = \beta^2(x+1)/(x+1)^2 - \beta^2/(x+1)^2 \\ &= \beta^2/(x+1) - \beta^2/(x+1)^2 \\ &= (\beta^2 - \beta)/(x+1) + [(\beta/(x+1)) - \beta/(x+1))^2]. \end{aligned}$$

The expression in square brackets above is of the form $w - w^p$, with $p = 2$, so by Artin–Schreier theory,

$$\mathcal{L}_{\psi(bx/x^2+1)} \approx \mathcal{L}_{\psi((\beta^2-\beta)/(x+1))},$$
$$\mathcal{F} \approx \mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi((\beta^2-\beta)/(x+1))}.$$

Thus in characteristic 2, we see that $\mathcal{F}$ is tame at $x = 0$, and has Swan conductor 1 at $x = 1$. Again, the formula $\chi_c = -2$ is immediate from the Euler–Poincare formula [7]. Q.E.D.

Proof of Theorem 2. Fix a prime number $l \neq p$, and an isomorphism of $\overline{\mathbb{Q}}_l$ with $\mathbb{C}$. Exactly as explained in [6] we consider the set of points x in U where $\mathrm{Tr}_{K/k}(x) \neq 0$ as the k-points of an open smooth curve $U[1/\mathrm{Tr}]$ over k, and our exponential sum as the alternating sum of traces of Frobenius on the groups

$$H_c^i(U[1/\mathrm{Tr}] \otimes_k \bar{k}, \mathcal{F}), \qquad \mathcal{F} := \mathcal{L}_\chi \otimes \mathcal{L}_{\psi(b/\mathrm{Tr})}.$$

Just as above, the only possibly nonzero groups are the H_c^i with $0 < i \leq 2$. The sheaf $\mathcal{F}$ is again lisse of rank one, and pure of weight zero. As above, $H_c^0 = 0$ ($\mathcal{F}$ is lisse and $U[1/\mathrm{Tr}]$ is open). By [10], H_c^1 is mixed of weight ≤ 1, so it suffices to show that $H_c^2 = 0$ and that $\chi_c = -4$ if p is odd, while $\chi_c = -2$ if p is 2.

These are both geometric statements. But already over K, the group-scheme U splits: $U \otimes_k K \pm \mathbb{G}_{m,K}$, and Tr becomes the function $x \mapsto x + 1/x$ on $\mathbb{G}_{m,K}$. The sheaf $\mathcal{L}_\chi$ on U pulls back to become the sheaf $\mathcal{L}_\rho$ on

$\mathbb{G}_{m,K}$, where ρ is the (necessarily nontrivial) character of $\mathbb{G}_{m,K}(K) := K^\times$ which is $z \mapsto \chi(z^{1-q})$; indeed, the intrinsic norm from $U(K) = K^\times$ to $U(k) = \{\text{elements } x \text{ in } K^\times \text{ with } x^{1+q} = 1\}$ is the surjective homomorphism $z \mapsto z^{1-q}$. The sheaf $\mathcal{L}_{\psi(b/\mathrm{Tr})}$ on $U[1/\mathrm{Tr}]$ pulls back to become the sheaf $\mathcal{L}_{\psi(b/(x+1/x))} = \mathcal{L}_{\psi(bx/(x^2+1))}$ on $U[1/\mathrm{Tr}] \otimes_k K = \mathbb{A}^1_K[1/x(x^2+1)]$. Thus both the vanishing of H^2_c and the calculation of χ_c have already been proven above: just repeat the proof of Theorem 1, but over the field K. Q.E.D.

Remark. In both Theorems 1 and 2, the H^1_c is in fact pure of weight one, because (cf. [3, 3.2.3]) the lisse rank one sheaf $\mathcal{F}$ is nontrivially ramified at each of the missing points, including ∞.

QUESTION. One gets a natural generalization of the sum considered in Theorem 2 by allowing K/k to have arbitrary degree $n \geq 2$. The "split" version of this sum is the "inverted n-variable Kloosterman sum"

$$\sum_{\prod_i x_i = 1, \sum_i x_i \neq 0} \chi_1(x_1)\chi_2(x_2) \cdots \chi_n(x_n)\psi(b/(x_1 + x_2 + \cdots + x_n)).$$

What can be said about such sums, and what are they good for?

REFERENCES

1. P. Deligne, Application de la formule des traces aux sommes trigonométriques, *in* "Cohomolgie Etale (SGA 4 1/2)," Springer Lecture Notes in Math., Vol. 569, (1977), 168–232.
2. P. Deligne, Rapport sur la formule des traces, *in* "Cohomologie Etale (SGA 4 1/2)," Springer Lecture Notes in Mathematics 569, (1977), 76–109.
3. P. Deligne, La conjecture de Weil II, *Pub. Math. I.H.E.S.* **52** (1981), 313–428.
4. R. Evans, Spherical functions for finite upper half planes with characteristic 2, to appear.
5. A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L, Séminaire Bourbaki 1964–65, Exposé 279, reprinted in Dix Exposés sur la cohomologie des schémas, North-Holland, Amsterdam, 1968.
6. N. M. Katz, Estimates for Soto-Andrade Sums, *J. Reine Angew. Math.* **438** (1993), 143–161.
7. M. Raynaud, Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes, "Séminaire Bourbaki 1964/65, Exposé 286," W. A. Benjamin, New York, 1966.
8. A. Grothendieck *et al.*, Séminaire de Géométrie Algébrique du Bois-Marie, SGA 1, SGA 4 Parts I, II, and III, SGA 4 1/2, SGA 5, SGA 7 Parts I and II, Springer Lecture Notes in Math. 224, 269–305, 569, 589, 288–340, 1971–1977.
9. A. Terras, Fourier Analysis on Finite Groups and Applications, Chapter 2, The finite affine and Heisenberg groups and other non-abelian finite groups, preprint dated 4/6/92.
10. A. Weil, On the Riemann Hypothesis in function-fields, *Proc. Nat. Acad. Sci. U.S.A.* **27** (1941), 345–347.