ON A QUESTION OF BOMBIERI AND BOURGAIN

NICHOLAS M. KATZ

1. Introduction and statement of the main results

Let k be a finite field, p its characteristic, and

$$\psi : (k, +) \to \mathbb{Z}[\zeta_p]^\times \subset \mathbb{C}^\times$$

a nontrivial additive character of k. We are given an integer $n \geq 1$. We wish to consider certain character sums over $k \times k^n = k^{n+1}$, with coordinates $(y, x) = (y, (x_1, ..., x_n))$. We are given the following initial data:

(1) an $n+1$-tuple $(\rho, \chi_1, ..., \chi_n)$ of nontrivial $\mathbb{C}^\times$-valued multiplicative characters of $k^\times$, each extended to k by the requirement that it vanish at $0 \in k$.

(2) an $n+1$-tuple $(g, f_1, ..., f_n)$ of nonzero one-variable k-polynomials, which are adapted to the character list above in the following sense. Whenever $\alpha \in \overline{k}$ is a zero of g (respectively of some f_i), then $\rho^{ord_\alpha(g)}$ (respectively $\chi_i^{ord_\alpha(f_i)}$) is nontrivial. We define

$$m_i := \text{number of distinct zeroes of } f_i \text{ in } \overline{k},$$

$$m_0 := \text{number of distinct zeroes of } g \text{ in } \overline{k},$$

(3) an $n+1$-tuple $(G, F_1, ..., F_n)$ of one-variable k-polynomials (some possibly 0), each of which is either 0 or of degree > 1 and prime to p. We assume these polynomials are adapted to the data above in the following sense. If g (respectively some f_i) is a nonzero constant, i.e., if m_0 (resp. some m_i) $= 0$, then G (respectively F_i) has degree > 1. We define

$$d_i := Max(1, deg(F_i)),$$

$$d_0 := Max(1, deg(G)).$$

We then form the sum

$$\sum_{(y,x)\in k^{n+1}} \rho(g(y))\psi(G(y)) \prod_i (\chi_i(f_i(x_i))\psi(F_i(x_i))\psi(yx_i)).$$

And for each $n+1$-tuple $(b,a) \in k^{n+1}$, we form the sum

$$\sum_{(y,x)\in k^{n+1}} \rho(g(y))\psi(G(y)+by)\prod_i(\chi_i(f_i(x_i))\psi(F_i(x_i)+a_ix_i)\psi(yx_i)).$$

In recent work [B-B] of Bombieri and Bourgain on derandomization, the question arose of specifying conditions on the above initial data under which *all* of these sums have uniform square root cancellation.

For $i = 1, ..., n$, we define

$$r_i := m_i + d_i - 1.$$

Notice that under our assumptions on the initial data, each $r_i \geq 1$. We define the constant

$$C = C(n,m,d) := (m_0 - 1 + \sum_{i=1}^{n} 1/r_i + Max(d_0, 2))\prod_i r_i.$$

Theorem 1.1. *Suppose that any of the following three conditions holds.*

1. *We have $d_0 \geq 3$.*
2. *We have $m_0 \geq n+1$.*
3. *We have $m_0 \geq 1$, and for each $i = 1, ..., n$, either $d_i > 1$ or $\chi_i^{deg(f_i)}$ is trivial.*

Then for each $n+1$-tuple $(b,a) \in k^{n+1}$, the sum

$$S(a,b) := \sum_{(y,x)\in k^{n+1}} \rho(g(y))\psi(G(y)+by)\prod_i(\chi_i(f_i(x_i))\psi(F_i(x_i)+a_ix_i)\psi(yx_i))$$

satisfies the bound

$$|S(a,b)| \leq C(\#k)^{(n+1)/2}.$$

This result is not quite optimal in the sense that sometimes the constant C can be slightly improved.

Theorem 1.2. *Under the hypotheses of Theorem 1.1, suppose in addition that $d_i = 1$ for $i = 1, .., n$. Define the constant*

$$C_1 = C_1(n,m,d) := (m_0 - 1 + \sum_{i=1}^{n} 1/m_i + d_0)\prod_{i=1}^{n} m_i.$$

Then for each $n+1$-tuple $(b,a) \in k^{n+1}$, the sum

$$S(a,b) := \sum_{(y,x)\in k^{n+1}} \rho(g(y))\psi(G(y)+by)\prod_i(\chi_i(f_i(x_i))\psi(F_i(x_i)+a_ix_i)\psi(yx_i))$$

satisfies the bound

$$|S(a,b)| \leq C_1(\#k)^{(n+1)/2}.$$

Here is a specific instance of Theorem 1.2, where each $\chi_i^{deg(f_i)}$ is trivial, and where $d_0 = d_1 = ... = d_n = 1$.

Corollary 1.3. *Consider the case when $m_0 \geq 1$, $p \neq 2$, $G = 0$, all $F_i = 0$, and ρ and all the χ_i are the quadratic character χ_{quad}. Suppose that $deg(f_i)$ is even for each $i = 1, ..., n$. Define the constant*

$$C_2 = C_2(n, m, d) := (m_0 + \sum_{i=1}^{n} 1/m_i) \prod_{i=1}^{n} m_i.$$

Then for each $n+1$-tuple $(b, a) \in k^{n+1}$, the sum

$$S(a, b) := \sum_{(y,x) \in k^{n+1}} \chi_{quad}(g(y))\psi(by) \prod_i (\chi_{quad}(f_i(x_i))\psi(a_i x_i)\psi(y x_i))$$

satisfies the bound

$$|S(a, b)| \leq C_2 (\#k)^{(n+1)/2}.$$

2. Proof of the theorems

As customary in such questions, we choose a prime number $\ell \neq p$ and choose an embedding of $\mathbb{Q}(\zeta_p, \zeta_{\#k-1})$ into $\overline{\mathbb{Q}}_\ell$, so that we can view all our characters, both additive and multiplicative, as having values in $\overline{\mathbb{Q}}_\ell^\times$, and so that we can apply ℓ-adic cohomology.

In the general sum we are to treat,

$$\sum_{(y,x) \in k^{n+1}} \rho(g(y))\psi(G(y) + by) \prod_i (\chi_i(f_i(x_i))\psi(F_i(x_i) + a_i x_i)\psi(y x_i)),$$

we first sum over $(x_1, ..., x_n)$. Then our sum becomes

$$\sum_{y \in k} \rho(g(y))\psi(G(y) + by) \prod_i \mathbb{H}_i(y + a_i)$$

where the factors $\mathbb{H}_i$ are the functions on k

$$\mathbb{H}_i(y) = \sum_{x \in k} \psi(y x_i)\chi_i(f_i(x_i))\psi(F_i(x_i)).$$

To translate this into sheaf-theoretic language, we invoke the sheaves

$$\mathcal{G}_b := \mathcal{L}_{\psi(G(y)+by)} \otimes \mathcal{L}_{\rho(g(y))}$$

and

$$\mathcal{F}_i := \mathcal{L}_{\psi(F_i(x))} \otimes \mathcal{L}_{\chi_i(f_i(x))},$$

whose traces of Frobenius at k-points of $\mathbb{A}^1_k$ are given by the expected formulas

$$\mathcal{G}_b(y, k) := Trace(Frob_{y,k}|\mathcal{G}) = \psi(G(y) + by)\rho(g(y)),$$

$$\mathcal{F}_i(x,k) := Trace(Frob_{x,k}|\mathcal{F}_i) = \psi(F_i(x))\chi_i(f_i(x)),$$

cf. [De-ST].

Our hypotheses on initial data insure that $\mathcal{G}_b$ and all the $\mathcal{F}_i$'s are geometrically irreducible middle extension sheaves, none of which is geometrically isomorphic to a sheaf of the form $\mathcal{L}_\psi(ax)$ for any $a \in k$.

In general, given a geometrically irreducible middle extension sheaf $\mathcal{F}$ on $\mathbb{A}^1_k$ which is not geometrically isomorphic to a sheaf of the form $\mathcal{L}_\psi(ax)$ for any $a \in k$, its naive Fourier Transform [Ka-GKM, 8.2] $NFT_\psi(\mathcal{F})$ is a geometrically irreducible middle extension sheaf $\mathcal{F}$ on $\mathbb{A}^1_k$ whose trace function at k-points is related to that of the input sheaf $\mathcal{F}$ by (minus) the usual Fourier Transform formula:

$$Trace(Frob_{y,k}|NFT_\psi(\mathcal{F})) = -\sum_{x \in k} \psi(yx) Trace(Frob_{x,k}|\mathcal{F}).$$

One knows that if such an $\mathcal{F}$ is pure of weight 0 (in the sense that its restriction to any dense open set where it is lisse is pure of weight zero) then $NFT_\psi(\mathcal{F})$ is is pure of weight 1. By Laumon [Lau-TFCEF, 2.3] one also knows the local monodromies of $NFT_\psi(\mathcal{F})$ in terms of the local monodromies of $\mathcal{F}$; this will be important in a moment.

For $i = 1, ..., n$ we define

$$\mathcal{H}_i := NFT_\psi(\mathcal{F}_i).$$

Then our sum is

$$(-1)^n \sum_{y \in k} \mathcal{G}_b(y,k) \prod_i \mathcal{H}_i(y + a_i, k)$$

$$= (-1)^n \sum_{y \in k} \mathcal{G}_b(y,k) \prod_i (T^\star_{a_i}\mathcal{H}_i)(y,k),$$

where we denote by T_a the additive translation $x \mapsto x + a$. The local monodromies of the middle extension sheaves $\mathcal{H}_i$ and their additive translates $T^\star_{a_i}\mathcal{H}_i$ are as follows, cf. [Ka-ESDE, 7.4.5,7.4.6,7.5].

(1) If $d_i > 1$, then $\mathcal{H}_i$ [and hence also $T^\star_{a_i}\mathcal{H}_i$] is lisse on $\mathbb{A}^1$ of rank $r_i := m_i + d_i - 1$, with all $I(\infty)$-breaks $\le d_i/(d_i - 1) \le 2$.

(2) If $d_i = 1$, then $F_i(x) = \alpha_i x + \beta_i$, and $\mathcal{H}_i$ [respectively $T^\star_{a_i}\mathcal{H}_i$] is lisse on $\mathbb{A}^1 - \{-\alpha_i\}$ [respectively on $\mathbb{A}^1 - \{-\alpha_i - a_i\}$] of rank $r_i := m_i + d_i - 1$. Local monodromy at $-\alpha_i$ [respectively at $-\alpha_i - a_i$] is a tame pseudoreflection of determinant $\chi_i^{-deg(f_i)}$, and all $I(\infty)$-breaks are ≤ 1.

We form the tensor product sheaf on $\mathbb{A}^1_k$

$$\mathcal{K} = \mathcal{K}^{(b,a)} := \mathcal{G}_b \otimes (\otimes_i (T^\star_{a_i}\mathcal{H}_i)).$$

This sheaf, which is mixed of weight $\leq n$, need not be a middle extension, but, because it is a tensor product of middle extensions, it has no nonzero punctual sections, and hence

$$H^0_c(\mathbb{A}^1_k \otimes_k \overline{k}, \mathcal{K}) = 0.$$

By the Lefshcetz Trace formula [Gr-Rat], our sum is thus ($(-1)^n$ times)

$$\sum_{y \in k} \mathcal{K}(y,k) = Trace(Frob_k | H^2_c(\mathbb{A}^1_k \otimes_k \overline{k}, \mathcal{K})) - Trace(Frob_k | H^1_c(\mathbb{A}^1_k \otimes_k \overline{k}, \mathcal{K})).$$

By Deligne [De-Weil II, 3.3.1], the H^1_c is mixed of weight $\leq n+1$, and the H^2_c is mixed of weight $\leq n+2$. So to prove the theorems, we must show that the H^2_c vanishes, and bound from above $dim H^1_c$. To show that H^2_c vanishes, it suffices to show that for some point $x \in \mathbb{P}^1(\overline{k})$, the inertia group $I(x)$ acting on $\mathcal{K}_{\overline{\eta}}$ has no nonzero invariants.

We now show that H^2_c vanishes in each of the three situations of Theorem 1.1. Suppose first that $d_0 \geq 3$. Then the $I(\infty)$-slope of $\mathcal{G}_b$ is d_0. As the other tensor factors $T^\star_{a_i}\mathcal{H}_i)$ have all their $I(\infty)$-slopes ≤ 2, it follows that all the $I(\infty)$-slopes of $\mathcal{K}$ are d_0. In particular, $\mathcal{K}$ is totally wild at ∞, so there are no nonzero $I(\infty)$-invariants.

Suppose next that $m_0 \geq n+1$. The individual tensor factors $T^\star_{a_i}\mathcal{H}_i)$ are each lisse outside of at most one point of $\mathbb{A}^1(\overline{k})$. So their tensor product is lisse outside at most n points of $\mathbb{A}^1(\overline{k})$. But $\mathcal{G}_b$ has at least $n+1$ finite singularities, and at each the local monodromy is by a nontrivial scalar. So there exists a point $\gamma \in \mathbb{A}^1(\overline{k})$ at which $\otimes_i(T^\star_{a_i}\mathcal{H}_i)$ is lisse, but at which $\mathcal{G}_b$ has local monodromy a nontrivial scalar. At any such point, $I(\gamma)$ acting on $\mathcal{K}$ has no nonzero invariants.

Suppose finally that $m_0 \geq 1$, and that for each $i = 1, ..., n$, either $d_i > 1$ or $\chi_i^{deg(f_i)}$ is trivial. Then the individual tensor factors are either lisse on $\mathbb{A}^1$, or at their unique singularity in $\mathbb{A}^1(\overline{k})$, the local monodromy is unipotent. So at each of the points, if any, of $\mathbb{A}^1(\overline{k})$ at which $\otimes_i(T^\star_{a_i}\mathcal{H}_i)$ fails to be lisse, its local monodromy is unipotent. On the other hand, at any of the m_0 finite singularities δ_j of $\mathcal{G}_b$, its local monodromy is by a nontrivial scalar; hence at any such point, $I(\delta_j)$ acting on $\mathcal{K}$ has no nonzero invariants.

We now turn to the problem of bounding $dim H^1_c$. For this, we will make use of a "sheaves of perverse origin" argument. We fix the $n+1$ middle extension sheaves $\mathcal{G}_0, \mathcal{F}_1, ..., \mathcal{F}_n$ on $\mathbb{A}^1$. On $\mathbb{A}^{n+1} \times \mathbb{A}^{n+1}$, with coordinates $(y, x_1, ..., x_n; b, a_1, ..., a_n)$, we define the sheaf

$$\mathcal{M} := \mathcal{L}_{\psi(by + \sum_i (y+a_i)x_i)} \otimes \mathcal{G}_0(y) \otimes \mathcal{F}_1(x_1) ... \otimes \mathcal{F}_n(x_n).$$

Then $\mathcal{M}[2n+2]$ is a perverse sheaf on $\mathbb{A}^{n+1} \times \mathbb{A}^{n+1}$. The (sheaf theoretic incarnation of the) arguments above show that for the projection pr_2

onto the second $\mathbb{A}^{n+1}$ factor, we have

$$R^i pr_{2,!}\mathcal{M} = 0 \ if \ i \neq n+1.$$

Moreover, the stalk of

$$\mathcal{N} := R^{n+1}pr_{2,!}\mathcal{M}$$

at a point $(b, a_1, ..., a_n) \in \mathbb{A}^{n+1}(\overline{k})$ is the cohomology group of interest:

$$\mathcal{N}_{(a,b)} = H^1_c(\mathbb{A}^1_{\overline{k}}, \mathcal{K}^{(b,a)}) := H^1_c(\mathbb{A}^1_{\overline{k}}, \mathcal{G}_b \otimes (\otimes_i (T^\star_{a_i}\mathcal{H}_i))).$$

By [Ka-SCMD, Introduction and Cor. 5], $\mathcal{N}$ is a sheaf of perverse origin on $\mathbb{A}^{n+1}_k$. For a sheaf of perverse origin, one knows [Ka-SCMD, Prop.'s 11, 12] that the stalk at any point has rank at most the generic rank, and that the open set U where the sheaf is lisse consists precisely of the points where the stalk has this maximum rank.

We partition the indices $i = 1, ..., n$ into two subsets L and NL by decreeing that $i \in L$ if $d_i > 1$, otherwise $i \in NL$. Thus $i \in L$ if and only if $\mathcal{G}_i$ is lisse on $\mathbb{A}^1$. For $i \in L$, all $I(\infty)$-slopes of $\mathcal{G}_i$ are $\leq d_i/(d_i - 1)$. For $i \in NL$, $\mathcal{G}_i$ has a unique finite singularity $-\alpha_i$, and has all $I(\infty)$-slopes ≤ 1. For $i \in NL$, the isomorphism class of the $I(\infty)$-representation of $T^\star_{a_i}\mathcal{G}_i$ is independent of the choice of additive translate a_i.

We next describe a dense open set U_1 of $\mathbb{A}^{n+1}_k$ as follows. We first define a dense open set U_0 of $\mathbb{A}^n_k$ as follows. We require that for the indices $i \in NL$, the unique finite singularities $-\alpha_i - a_i$ of $T^\star_{a_i}\mathcal{G}_i$ be pairwise distinct, and that none of them be a finite singularity of $\mathcal{G}_0$. We then define U_1 to be the dense open set of $\mathbb{A}^1_k \times U_0$ on which the Swan conductor at ∞ of $\mathcal{K}^{(b,a)}$ is maximal. [By Deligne's semicontinuity theorem [Lau-SCCS, Thm. 2.1.1], this maximality occurs on a dense open set.]

To compute the generic rank of $\mathcal{N}$, we may work at a point $(b, a) \in U \cap U_1$. Then $\mathcal{K}^{(b,a)}$ is a middle extesion, and has precisely $\#NL + m_0$ finite singularities, namely $-\alpha_i - a_i$ for each $i \in NL$, and the finite singularities if any, of $\mathcal{G}_0$, say $\lambda_1, ..., \lambda_{m_0}$. All these singularities are tame. At $-\alpha_i - a_i$, the stalk has dimension

$$(r_i - 1)\prod_{j \neq i} r_j = (1 - 1/r_i)\prod_j r_j.$$

At the λ's, if any, the stalk vanishes. What about $Swan_\infty(\mathcal{K}^{(b,a)})$? If L is empty, and all F_i have degree ≤ 1,then each $T^\star_{a_i}\mathcal{G}_i$ has all $I(\infty)$-breaks ≤ 1, so (as b is general) all $I(\infty)$-breaks of $\mathcal{K}^{(b,a)}$ are equal to $d_0 := Max(deg(G), 1)$. If $d_0 \geq 3$, then also all $I(\infty)$-breaks of $\mathcal{K}^{(b,a)}$ are equal to d_0. In the general case, we can only assert that all $I(\infty)$-breaks of $\mathcal{K}^{(b,a)}$ are at most $Max(d_0, 2)$.

The Euler-Poincaré formula [Ray] now gives

$$-dimH^1_c(\mathbb{A}^1_k \otimes_k \overline{k}, \mathcal{K}^{(b,a)})$$

$$= (1 - \#NL - m_0)\prod_i r_i + \sum_{j \in NL}(1 - 1/r_j)\prod_i r_i - Swan_\infty(\mathcal{K}^{(b,a)}).$$

Thus we have the inequality

$$dimH^1_c(\mathbb{A}^1_k \otimes_k \overline{k}, \mathcal{K}^{(b,a)})$$

$$\leq (m_0 + \#NL - 1 - \sum_{j \in NL}(1 - 1/r_j))\prod_i r_i + Swan_\infty(\mathcal{K}^{(b,a)})$$

$$= (m_0 - 1 + \sum_{j \in NL} 1/r_j)\prod_i r_i + Swan_\infty(\mathcal{K}^{(b,a)}).$$

Combining this with the general inequality

$$Swan_\infty(\mathcal{K}^{(b,a)}) \leq Max(d_0, 2)\prod_i r_i,$$

we get the inequality

$$dimH^1_c(\mathbb{A}^1_k \otimes_k \overline{k}, \mathcal{K}^{(b,a)})$$

$$\leq (m_0 - 1 + \sum_{j \in NL} 1/r_j + Max(d_0, 2))\prod_i r_i.$$

This proves Theorem 1.1, or more precisely the tiny improvement thereof in which the term $\sum_{j \in NL} 1/r_j$ replaces the term $\sum_{j=1}^n 1/r_j$.

In the case when $d_i = 1$ for $i = 1, ..., n$, then we have the improved inequality

$$Swan_\infty(\mathcal{K}^{(b,a)}) \leq d_0\prod_i r_i,$$

and we have $r_i = m_i$ for $i = 1, ..., n$. So we get

$$dimH^1_c(\mathbb{A}^1_k \otimes_k \overline{k}, \mathcal{K}^{(b,a)})$$

$$\leq (m_0 - 1 + \sum_{j \in NL} 1/m_j + d_0)\prod_{i=1}^n m_i.$$

which gives Theorem 1.2.

References

[B-B] Bombieri, E., and Bourgain, J., manuscript in preparation.

[De-ST] Deligne, P., Applications de la formule des traces aux sommes trigonométriques, pp. 168-232 in SGA 4 1/2, cited below.

[De-Weil II] Deligne, P., La conjecture de Weil II. Publ. Math. IHES 52 (1981), 313-428.

[Gr-Rat] Grothendieck, A., Formule de Lefschetz et rationalité des fonctions L. Séminaire Bourbaki, Vol. 9, Exp. No. 279, 41-55, Soc. Math. France, 1995.

[Ka-ESDE] Katz, N., Exponential sums and differential equations, Annals of Math. Study 124, Princeton Univ. Press, 1990.

[Ka-GKM] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups, Annals of Math. Study 116, Princeton Univ. Press, 1988.

[Ka-SCMD] Katz, N., A semicontinuity result for monodromy under degeneration. Forum Math. 15 (2003), no. 2, 191-200.

[Lau-SCCS] Laumon, G. Semi-continuité du conducteur de Swan (d'après P. Deligne). Caractéristique d'Euler-Poincaré, pp. 173-219, Astérisque, 82-83, Soc. Math. France, Paris, 1981.

[Lau-TFCEF] Laumon, G., Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil. Inst. Hautes tudes Sci. Publ. Math. No. 65 (1987), 131-210.

[Ray] Raynaud, M., Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes. Séminaire Bourbaki, Vol. 9, Exp. No. 286, 129-147, Soc. Math. France, Paris, 1995.

[SGA 4 1/2] Cohomologie Etale. Séminaire de Géométrie Algébrique du Bois Marie SGA 4 1/2. par P. Deligne, avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie, et J. L. Verdier. Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, 1977.

[SGA 1] Revêtements étales et groupe fondamental. Séminaire de Géométrie Algébrique du Bois Marie 1960-1961 (SGA 1). Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud. Lecture Notes in Mathematics, Vol. 224, Springer-Verlag, 1971.

[SGA 4 Tome 3] Théorie des Topos et Cohomologie Etale des Schémas, Tome 3. Séminaire de Géométrie Algébrique du Bois Marie 1963-1964 (SGA 4). Dirigé par M. Artin, A. Grothendieck, J. L. Verdier. Lecture Notes in Mathematics, Vol.305, Springer-Verlag, 1973.

[SGA 7 II] Groupes de monodromie en géométrie algébrique. II. Séminaire de Géométrie Algébrique du Bois-Marie 1967-1969 (SGA 7 II). Dirigé par P. Deligne et N. Katz. Lecture Notes in Mathematics, Vol. 340. Springer-Verlag, 1973.

Princeton University, Mathematics, Fine Hall, NJ 08544-1000, USA
E-mail address: nmk@math.princeton.edu