AN ESTIMATE FOR CHARACTER SUMS

NICHOLAS M. KATZ

In this note, we give estimates for a class of character sums that occur as eigenvalues of adjacency matrices of certain graphs constructed by F. R. K. Chung. Her situation is as follows. We are given a finite field $F$, an integer $n \geq 1$, an extension field $E$ of $F$ of degree $n$, and an element $x$ in $E$ that generates $E$ over $F$, i.e., an element $x$ such that $E$ is $F(x)$.

Theorem 1. Let $\chi$ be any nontrivial complex-valued multiplicative character of $E^\times$ (extended by zero to all of $E$), and $x$ in $E$ any element that generates $E$ over $F$. Then

$$\left| \sum_{t \in F} \chi(t - x) \right| \leq (n - 1)\sqrt{\#(F)}.$$

It turns out to be easier to consider the following more general situation. $F$ is a finite field, $n \geq 1$ is an integer, and $B$ is a finite etale $F$-algebra of dimension $n$ over $F$ (i.e., over a finite extension $K$ of $F$, there exists an isomorphism of $K$-algebras $B \otimes_F K \simeq K \times K \times \cdots \times K$). We assume given an element $x$ in $B$ that is regular in the sense that its characteristic polynomial $\det_T(T - x|B)$ in the regular representation of $B$ on itself has $n$ distinct eigenvalues. (In terms of the above isomorphism $B \otimes_F K \simeq K \times K \times \cdots \times K$, $x$ is regular if and only if $x \otimes 1 \simeq (x_1, \ldots, x_n)$ with all distinct components $x_i$. Or equivalently, $x$ is regular if and only if $B$ is equal to the $F$-subalgebra $F[x]$ generated by $x$. In the special case when $B$ is a field $F$, the element $x$ is regular if and only if $F(x) = E$.)

Theorem 2. Let $\chi$ be any nontrivial complex-valued multiplicative character of $B^\times$ (extended by zero to all of $B$), and $x$ in $B$ any regular element. Then

$$\left| \sum_{t \in F} \chi(t - x) \right| \leq (n - 1)\sqrt{\#(F)}.$$

Proof. The basic idea is that the theorem is an immediate consequence of Weil's estimates for one-variable character sums in the case when the $F$-algebra $B$ is completely split, and that one can reduce to this case by thinking geometrically about suitable Lang torsors.

Received by the editors February 10, 1988.
We begin by explaining how to view the problem geometrically. Given any finite-dimensional commutative $F$-algebra $A$, we denote by $A$ the smooth affine scheme over $F$ given by "$A$ as algebraic group over $F"$; concretely, for any $F$-algebra $R$, the group $A(R)$ of $R$-valued points of $A$ is $A \otimes_F R$. We denote by $A^\times$ the open subscheme of $A$ given by "$A^\times$ as algebraic group over $F"$; concretely, for any $F$-algebra $R$, the group $A^\times(R)$ of $R$-valued points of $A$ is $(A \otimes_F R)^\times$. These concepts will be applied to the cases $A = B$ and $A = F$. It will be important in what follows to think of $A^\times$ as a smooth commutative group scheme over $F$, but to think of $A$ only as an ambient scheme (not as a group scheme) containing $A^\times$ as an open subscheme.

Because $B^\times$ is a smooth, geometrically connected commutative group scheme over the finite field $F$, the Lang isogeny $1 - \text{Frob}_F: B^\times \to B^\times$ makes $B^\times$ into a $B^\times$-torsor over itself, the "Lang torsor" $L$. Let us now fix a prime number $l \neq \text{char}(F)$, an algebraic closure $\overline{Q}_l$ of $Q_l$, and an isomorphism of fields $C \cong \overline{Q}_l$. This isomorphism allows us to view $\chi$ as a $\overline{Q}_l$-valued character of $B^\times$, by which it makes sense to push out the Lang torsor $L$ to obtain a lisse rank one $\overline{Q}_l$-sheaf $L_\chi$ on $B^\times$ which is pure of weight zero. If we denote by $j: B^\times \to B$ the inclusion, we may form the extension by zero $j_*L_\chi$ on $B$. Now consider the morphism of $F$-schemes of $f: F \to B$ defined by $f(t) := t - x$, and the pullback sheaf $\mathcal{F} := f^*(j_*L_\chi)$ on $F$. The sheaf $\mathcal{F}$ is lisse of rank one and pure of weight zero on the open set $f^{-1}(B^\times)$, and zero outside. The sheaf $\mathcal{F}$ is everywhere tamely ramified, simply because on $f^{-1}(B^\times)$ it is lisse of order dividing that of $\chi$, hence of order prime to the characteristic of $F$.

In terms of this data, the character sum in question is given by

$$\sum_{t \in F} \chi(t - x) = \sum_{t \in f^{-1}(B^\times)(F)} \text{Trace}(\text{Frob}_t, F | \mathcal{F}),$$

and by the Lefschetz Trace Formula this last sum is equal to

$$\sum_i (-1)^i \text{Trace}(\text{Frob}_F | H^i_{\text{comp}}(f^{-1}(B^\times) \otimes_F \overline{F}, \mathcal{F})).$$

By Weil (but expressed in the language of Deligne's paper [De]) we know that the above cohomology groups $H^i_{\text{comp}}$ are mixed of weight $\leq i$. For dimension reasons, $H^i_{\text{comp}}$ vanishes for $i > 2$, and $H^0_{\text{comp}}$ vanishes because $\mathcal{F}$ is lisse on the incomplete curve $f^{-1}(B^\times) \otimes_F \overline{F}$. It thus remains only to establish the following two facts:

(a) $H^2_{\text{comp}}(f^{-1}(B^\times) \otimes_F \overline{F}, \mathcal{F}) = 0$,

(b) $\dim H^1_{\text{comp}}(f^{-1}(B^\times) \otimes_F \overline{F}, \mathcal{F}) = n - 1$.

Both of these facts are geometric, i.e., they concern the situation over the algebraic closure of $F$, and hence it suffices to verify them universally in the case when the $F$-algebra $B$ is completely split. (The key point here is that our hypothesis that $\chi$ is nontrivial is stable under finite extension of scalars.)
Indeed, after extension of scalars from $F$ to any finite extension field $K$, the pullback to $(B^\times) \otimes_F K$ of $L_{\bar{\chi}}$ is $L_{\bar{\chi}^i}$, where $\bar{\chi}$ is the character of $(B \otimes_F K)^\times$ obtained from $\chi$ by composition with the norm homomorphism $\text{Norm}_{K/F}$ from $(B \otimes_F K)^\times$ to $B^\times$. Because this norm map is surjective, the character $\bar{\chi}$ is nontrivial provided that $\chi$ is nontrivial.

Suppose now that $B$ is simply the $n$-fold self product of $F$ with itself. Then a nontrivial character $\chi$ of $B^\times$ is simply an $n$-tuple $(\chi_1, \ldots, \chi_n)$ of characters of $F^\times$, not all of which are trivial, the regular element $x$ is just an $n$-tuple $(x_1, \ldots, x_n)$ with all distinct components $x_i$, the open set $f^{-1}(B^\times)$ is just the complement $F - \{x_1, \ldots, x_n\}$ of the $n$ distinct points $x_i$ in $F$, the sheaf $\mathcal{F}$ is just the tensor product of the sheaves $[t \mapsto t - x_i]^\ast L_{\bar{\chi}_i} | F - \{x_1, \ldots, x_n\}$, and the sum in question is

$$\sum_{t \in F - \{x_1, \ldots, x_n\}} \chi_1(t - x_1)x_2(t - x_2) \cdots x_n(t - x_n).$$

By assumption, at least one of the $\chi_i$ is nontrivial. For such an index $i$, the sheaf $[t \mapsto t - x_i]^\ast L_{\bar{\chi}_i}$ is tamely but nontrivially ramified at $x_i$, while all the other factors $[t \mapsto t - x_j]^\ast L_{\bar{\chi}_j}$ with $j \neq i$ are lisse at $x_i$ (by the hypothesis that all the $x_j$ are distinct). Therefore, the sheaf $\mathcal{F}$ is nontrivially ramified at the point $x_i$. Because $\mathcal{F}$ is lisse of rank one on $F - \{x_1, \ldots, x_n\}$, its coinvariants under the inertia group $I_{x_i}$ must vanish, and a fortiori its covariants under the entire $\pi_1^{\text{geom}}$ of $F - \{x_1, \ldots, x_n\}$ must also vanish, i.e., its $H^2_{\text{comp}}$ vanishes. Once we have the vanishing of all the $H^1_{\text{comp}}$ save for $i = 1$, the asserted dimension formula $\dim H^1_{\text{comp}} = n - 1$ is then equivalent to the Euler characteristic formula

$$\sum_i (-1)^i \dim (\mathcal{F}^\ast) = 1 - n,$$

which holds because $\mathcal{F}$ is lisse of rank one and everywhere tame on the open curve $(F - \{x_1, \ldots, x_n\}) \otimes_F \overline{F}$, whose Euler characteristic is $1 - n$. Q.E.D.

Remarks and Questions. (1) If we drop the hypothesis that the element $x$ be regular, then Theorem 2 remains valid for characters $\chi$ of $B^\times$ whose restriction to $F^\times$ is nontrivial. The proof proceeds along the same lines as above, reducing to the completely split case in which $\chi$ is simply an $n$-tuple $(\chi_1, \ldots, \chi_n)$ of characters of $F^\times$, with the property that their product $\prod_{i} \chi_i$ is nontrivial on $F^\times$. Now one gets the vanishing of $H^2_{\text{comp}}$ by observing that the sheaf $\mathcal{F}$ is nontrivially ramified at $\infty$ (as an $I_{\infty}$-representation, $\mathcal{F}$ is isomorphic to $L_{\prod_{i} \chi_i}$), and the constant "$n - 1$" actually improves to "(the number of distinct $\chi_i$) - 1." Indeed, in the case of the choice $x := 0$, the character sum in question is exactly $\sum_{t \in F^\times} \chi(t)$. (Alternately, one could apply Theorem 2 directly to the (automatically finite etale) subalgebra $B_0 := F[x]$ of $B$ generated by $x$ over $F$, to the regular element $x$ of $B_0$, and to the nontrivial (because nontrivial on $F^\times$) character $\chi | (B_0)^\times$.)
(2) What happens if we also drop the hypothesis that $B$ be etale? Suppose that we are given an arbitrary $n$-dimensional commutative $F$-algebra $A$, a multiplicative character $\chi$ of $A^\times$ (extended by zero to all of $A$) whose restriction to $F^\times$ is nontrivial, and an element $x$ in $A$. It seems plausible that the estimate

$$\left| \sum_{t \in F} \chi(t - x) \right| \leq (n - 1) \sqrt{\#(F)}$$

should still hold. For example, in the case when $A$ is the algebra of dual numbers $F[x]/(x^2)$, the character sums in question are none other than the usual Gauss sums attached to the field $F$.

REFERENCES


DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08544