ON A QUESTION OF RUDNICK: DO WE HAVE SQUARE ROOT CANCELLATION FOR ERROR TERMS IN MOMENT CALCULATIONS?

NICHOLAS M. KATZ

1. Background: Lang-Weil

Start with a finite field k and X/k separated of finite type, which is smooth and geometrically connected, of dimension $n \geq 1$. The Lang-Weil estimate [La-We] is the assertion that for variable finite extensions K of k, we have the estimate

$$\#X(K) = (\#K)^n + O((\#K)^{n-1/2}).$$

Lang and Weil proved this by using its truth for curves, established by Weil, together with a fibration argument. From a modern point of view, Lang-Weil is best seen as resulting from Grothendieck's Lefschetz trace formula [Gro-FL], combined with Deligne's estimates [De-Weil II, 3.3.4]. For any prime ℓ not the characteristic p of k, we have

$$\#X(K) = \sum_{i=0}^{2n} (-1)^i \mathrm{Trace}(Frob_K | H^i_c(X_{\overline{k}}, \mathbb{Q}_\ell)).$$

One knows that $H^{2n}_c(X_{\overline{k}}, \mathbb{Q}_\ell)$ is one-dimension, with $Frob_K$ acting as $(\#K)^n$, and, thanks to Deligne, that each $H^i_c(X_{\overline{k}}, \mathbb{Q}_\ell))$ is mixed of weight $\leq i$ (for any chosen embedding of $\mathbb{Q}_\ell$ into $\mathbb{C}$).

So the formula becomes

$$\#X(K) = (\#K)^n + \sum_{i=0}^{2n-1} (-1)^i \mathrm{Trace}(Frob_K | H^i_c(X_{\overline{k}}, \mathbb{Q}_\ell)),$$

with

$$\sum_{i=0}^{2n-1} (-1)^i \mathrm{Trace}(Frob_K | H^i_c(X_{\overline{k}}, \mathbb{Q}_\ell)) = O((\#K)^{n-1/2}).$$

2. Background: Deligne's equidistribution theorem

How does Deligne's equidistribution theorem relate to this? The situation is that we have a lisse $\overline{\mathbb{Q}_\ell}$-sheaf, $\ell \neq p$, $\mathcal{F}$ on X which is pure of weight zero, of rank $r \geq 1$. Attached to it are its geometric

and arithmetic monodromy groups $G_{geom} \trianglelefteq G_{arith} \subset GL(r)$. These are algebraic groups over $\overline{\mathbb{Q}_\ell}$. One knows, again by Deligne, that (the identity component of) G_{geom} is semisimple, cf. [De-Weil II, 1.3.9 **and** its proof, and 3.4.1 (iii)].

Suppose that our $\mathcal{F}$ has $G_{geom} = G_{arith}$. Embed $\overline{\mathbb{Q}_\ell}$ into $\mathbb{C}$, view G_{arith} as a group over $\mathbb{C}$, and choose a maximal compact subgroup $\mathbb{K}$ of the complex Lie group $G_{arith}(\mathbb{C})$. Then for each finite extension K/k, and each $x \in X(K)$, (the semi simplification, in the sense of Jordan normal form, of) the Frobenius conjugacy class $Frob_{x,K}$ meets $\mathbb{K}$ in a unique $\mathbb{K}$-conjugacy class $\theta_{x,K}$.

Deligne's equdistribution theorem asserts that as $\#K \to \infty$, the classes $\{\theta_{x,K}\}_{x\in X(K)}$ become equidistributed in $\mathbb{K}^\#$, the space of conjugacy classes in $\mathbb{K}$, for (the direct image from $\mathbb{K}$ of) Haar measure of total mass one, cf. [De-Weil II, 3.5.3], [Ka-GKM, 3.6], and [Ka-Sar, 9.2.6].

The proof goes along the now usual lines, of estimating the appropriate Weyl sums. More precisely, for each irreducible nontrivial representation ρ of G_{arith}, we form the corresponding "pushout" sheaf $\rho(\mathcal{F})$ on X. By Peter-Weyl, what must be shown is that the large $\#K$ limit of

$$(1/\#X(K)) \sum_{x\in X(K)} \mathrm{Trace}(Frob_{x,K}|\rho(\mathcal{F}))$$

vanishes.

This sum is

$$(1/\#X(K)) \sum_{i=0}^{2n} (-1)^i \mathrm{Trace}(Frob_K | H^i_c(X_{\overline{k}}, \rho(\mathcal{F}))),$$

in which H^i_c is mixed of weight $\leq i$, and in which the highest term $H^{2n}_c(X_{\overline{k}}, \rho(\mathcal{F})))$ is (the Tate twist by $-n$ of) the space of coinvariants of G_{geom} in the representation ρ. So the leading term vanishes:

$$H^{2n}_c(X_{\overline{k}}, \rho(\mathcal{F}))(n) = 0,$$

and we get the estimate

$$\sum_{x\in X(K)} \mathrm{Trace}(Frob_{x,K}|\rho(\mathcal{F})) = O((\#K)^{n-1/2}).$$

In view of Lang-Weil, we get

$$(1/\#X(K)) \sum_{x\in X(K)} \mathrm{Trace}(Frob_{x,K}|\rho(\mathcal{F})) = O(\frac{1}{\sqrt{\#K}}).$$

An equivalent formulation is this. Take **any** representation σ of G_{arith}, and denote by $N(\sigma)$ the multiplicity of the trivial representation

in σ. Thus $N(\sigma)$ is the dimension of $H_c^{2n}(X_{\overline{k}}, \rho(\mathcal{F}))$, upon which $Frob_K$ operates as the scalar $(\#K)^n$. Write σ as the direct sum of $N(\sigma)$ copies of the trivial representation with a finite sum of irreducible nontrivial representation ρ of G_{arith}, say $\sigma = N(\sigma)\mathbb{1} \oplus \tau$, with $N(\tau) = 0$. For $N(\sigma)\mathbb{1}$, i.e. for the constant sheaf $\overline{\mathbb{Q}_\ell}^{N(\sigma)}$, we have the tautological equality

$$(1/\#X(K)) \sum_{x \in X(K)} \text{Trace}(Frob_{x,K} | \overline{\mathbb{Q}_\ell}^{N(\sigma)}) = N(\sigma).$$

For the sheaf $\tau(\mathcal{F})$, whose H_c^{2n} vanishes, the Lefschetz trace formula gives

$$(1/\#X(K)) \sum_{x \in X(K)} \text{Trace}(Frob_{x,K} | \tau(\mathcal{F})) =$$

$$= (1/\#X(K)) \sum_{i \leq 2n-1} (-1)^i \text{Trace}(Frob_K | H_c^i(X_{\overline{k}}, \tau(\mathcal{F}))).$$

By Deligne (and Lang-Weil), this last sum is $O(\frac{1}{\sqrt{\#K}})$, so we get

$$(1/\#X(K)) \sum_{x \in X(K)} \text{Trace}(Frob_{x,K} | \sigma(\mathcal{F})) = N(\sigma) + O(\frac{1}{\sqrt{\#K}}).$$

To the extent that the sum $\sum_{i \leq 2n-1} (-1)^i \text{Trace}(Frob_K | H_c^i(X_{\overline{k}}, \tau(\mathcal{F})))$ has a better estimate, e.g. because some of its H_c^i vanish for large i, or have lower weight than allowed by Deligne's generaal theorem that H_c^i has weight $\leq i$, we get a better estimate of the error term.

3. Rudnick's question

Zeev Rudnick raised what is, in hindsight, the obvious question:

If $n := \dim(X) \geq 2$, when can we do better? When will we get "square root cancellation", i.e. an estimate, for every irreducible nontrivial representation ρ of G_{arith},

$$(1/\#X(K)) \sum_{x \in X(K)} \text{Trace}(Frob_{x,K} | \rho(\mathcal{F})) = O(\frac{1}{\sqrt{\#K}^n}).$$

Equivalently, when will we get an estimate, for every representation σ of G_{arith},

$$(1/\#X(K)) \sum_{x \in X(K)} \text{Trace}(Frob_{x,K} | \sigma(\mathcal{F})) = N(\sigma) + O(\frac{1}{\sqrt{\#K}^n}).$$

4. Examples showing a largely negative response

In the following sections, we will give examples in which some σ's have square root cancellation, and in which many others do not.

Fix integers $N \geq n \geq 2$, a prime $p > 2N+1$, and a nontrivial additive character ψ of $\mathbb{F}_p$. For $K/\mathbb{F}_p$ a finite extension, $\psi_K := \psi \circ \mathrm{Trace}_{K/\mathbb{F}_p}$ is a nontrivial additive character of K. Consider the n parameter family of sums, for each K, given by

$$S(t_1, t_2, ...t_n, K) := (-1/\sqrt{\#K}) \sum_{x \in K} \psi_K(x^{N+1} + \sum_{i=1}^{n} t_i x^i).$$

There is a lisse sheaf $\mathcal{F}$ on the $\mathbb{A}^n$ of $(a_1, a_2, ...a_n)$ whose trace function is given by these sums:

$$\mathrm{Trace}(Frob_{(t_1,t_2,...t_n),K}|\mathcal{F}) = S(t_1, t_2, ...t_n, K).$$

This sheaf $\mathcal{F}$ is lisse of rank N and pure of weight zero. One knows [Ka-MG, Thm. 19] that for this sheaf $\mathcal{F}$ we have

$$SL(n) \subset G_{geom} \subset G_{arith} \subset GL(N).$$

Lemma 4.1. *After passing to a finite extension $\mathbb{F}_q/\mathbb{F}_p$, the sheaf $\mathcal{F}$ on $\mathbb{A}^n/\mathbb{F}_q$ has*

$$SL(n) \subset G_{geom} = G_{arith} \subset GL(N).$$

Proof. First extend scalars to $\mathbb{F}_{p^2}$. For any finite extension $K/\mathbb{F}_{p^2}$, each $Frob_{x,K}$ has its characteristic polynomial with coefficients in $\mathbb{Q}(\zeta_p)$, so in particular has its determinant in $\mathbb{Q}(\zeta_p)$. The key point is that this field has a unique place $\mathcal{P}$ lying over p. So $\det(Frob_{x,K})$ has absolute value 1 at each archimedean place (purity), and is a unit at all finite places of residue characteristic $\ell \neq p$ (existence of ℓ-adic cohomology). By the product formula, the determinant must be a unit at $\mathcal{P}$ as well, so is a root of unity of order dividing $2p$. If we take an extension $K/\mathbb{F}_p$ of odd degree, then the square of each $Frob_{x,K}$ has such a determinant. Thus we have inclusions

$$SL(n) \subset G_{geom} \subset G_{arith} \subset \{A \in GL(N) | \det(A)^{4p} = 1\}.$$

From these inclusions we certainly have

$$G_{arith} \subset \mathbb{G}_m G_{geom} \quad (= GL(N)),$$

so there exist an ℓ-adic unit α such that after the constant field twist α^{deg} of $\mathcal{F}$, we have $G_{geom} = G_{arith}$, cf. [Ka-ST, Lemma 3.1]. It remains only to show that any such α is a root of unity. [For if $\alpha^N = 1$, then after extension of scalars from $\mathbb{F}_p$ to to $\mathbb{F}_{p^N}$, we will have $G_{geom} = G_{arith}$ for $\mathcal{F}$.] To see that any such α is a root of unity, choose any point

$x \in \mathbb{A}^n(\mathbb{F}_p)$. Then both $Frob_{x,F_p}|\mathcal{F}$ and $\alpha Frob_{x,F_p}|\mathcal{F}$ lie in G_{arith}, indeed the latter lies in G_{geom}. Comparing determinants, both of which are roots of unity of order dividing $4p$, we see that α^N is a root of unity of order dividing $4p$. □

For the remainder of this section, and in the two sections to follow, we work with the sheaf $\mathcal{F}$ on $\mathbb{A}^n/\mathbb{F}_q$, with $\mathbb{F}_q$ large enough that

$$SL(N) \subset G_{geom} = G_{arith} \subset GL(N).$$

We denote by std the given ("standard") n-dimensional representation of G_{arith}, and by $std^\vee$ the dual representation. We will be concerned with the representations

$$std^{\otimes A} \otimes (std^\vee)^{\otimes B}$$

of G_{arith}, for each pair of integers (A, B) with $0 \leq A, B \leq n$ (excluding the case $a = b = 0$, the trivial representation). We denote

$$M_{A,B} := \dim(std^{\otimes A} \otimes (std^\vee)^{\otimes B})^{G_{arith}},$$

the dimension of the space of invariants in $std^{\otimes A} \otimes (std^\vee)^{\otimes B}$, and by

$$M_{A,B}(\mathbb{F}_q)$$

the "empirical moment"

$$M_{A,B}(\mathbb{F}_q) := (1/q^n) \sum_{(t_1,...,t_n)\in\mathbb{A}^n(\mathbb{F}_q)} S(t_1, t_2, ...t_n, \mathbb{F}_q)^A \overline{S(t_1, t_2, ...t_n, \mathbb{F}_q)}^B.$$

We know that $M_{A,B}$ is the large q limit of $M_{A,B}(\mathbb{F}_q)$. Our concern is with estimating the difference

$$M_{A,B} - M_{A,B}(\mathbb{F}_q).$$

5. Explicit calculation of $M_{A,B}(\mathbb{F}_q)$

For any (A, B), the empirical moments $M_{A,B}(\mathbb{F}_q)$ and $M_{B,A}(\mathbb{F}_q)$ are complex conjugates of each other (after any embedding of $\overline{\mathbb{Q}_\ell}$ into $\mathbb{C}$). So we will assume from now on that

$$A \geq B.$$

In the affine space $\mathbb{A}^A \times \mathbb{A}^B$, with coordinates $(x_1, ..., x_A, y_1, ..., y_b)$, denote by $V(A, B, n) \subset \mathbb{A}^A \times \mathbb{A}^B$ the closed subscheme defined by the n equations

$$\sum_{a\leq A} x_a^d = \sum_{b\leq B} y_b^d, \quad 1 \leq d \leq n.$$

[In the case $B = 0$, $V(A, 0, n) \subset \mathbb{A}^A$ is the closed subschema defined by the n equations

$$\sum_{a \leq A} x_a^d = 0, \quad 1 \leq d \leq n.]$$

Lemma 5.1. *For $\mathbb{F}_q$ a finite field of characteristic $p > n$, the points of $V(A, B, n)(\mathbb{F}_q)$ have the following explicit description.*

(1) *If $n \geq A = B > 0$, then a point $(x_1, ..., x_A, y_1, ..., y_A) \in \mathbb{A}^{A+A}(\mathbb{F}_q)$ lies in $V(A, A, n)(\mathbb{F}_q)$ if and only if the two lists $(x_1, ..., x_A)$ and $(y_1, ..., y_A)$ are rearrangements of each other, i.e. if and only the first A elementary symmetric functions agree on them.*

(2) *If $n \geq A > B \geq 0$, then a point $(x_1, ..., x_A, y_1, ..., y_B) \in \mathbb{A}^{A+B}(\mathbb{F}_q)$ lies in $V(A, B, n)(\mathbb{F}_q)$ if and only if the two lists of length A, $(x_1, ..., x_A)$ and $(y_1, ..., y_B, 0, 0.., 0)$ (the second list obtained by padding out the list of y_i's by appending $A - B$ zeros) are rearrangements of each other.*

(3) *(a special case of (2) above) If $n \geq A$ and $B = 0$, the only point of $V(A, 0, n)(\mathbb{F}_q)$ is $(0, ..., 0)$.*

Proof. Because the characteristic $p > n$, for $A \leq n$ the equality of the first A Newton symmetric functions is equivalent to the equality of the first A elementary symmetric functions. □

Lemma 5.2. *For $n \geq A \geq B \geq 0$, but $(A, B) \neq (0, 0)$, and $\mathbb{F}_q$ a finite field of characteristic $p > n$, we have*

$$M_{A,B}(\mathbb{F}_q) = (-1/\sqrt{q})^{A+B} \# V(A, B, n)(\mathbb{F}_q).$$

Proof. Expand each term $S(t_1, t_2, ...t_n, \mathbb{F}_q)^A \overline{S(t_1, t_2, ...t_n, \mathbb{F}_q)}^B$ of the sum defining $M_{A,B}(\mathbb{F}_q)$. By definition, we have

$$S(t_1, t_2, ...t_n, \mathbb{F}_q) := (-1/\sqrt{q}) \sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(x^{N+1} + \sum_{i=1}^{n} t_i x^i).$$

Its $A'th$ power is then

$$S(t_1, t_2, ...t_n, \mathbb{F}_q)^A = (-1/\sqrt{q})^A \sum_{x_1, ..., x_A \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(\sum_{a \leq A}(x_a^{N+1} + \sum_{i=1}^{n} t_i x_a^i)).$$

The B'th power of its complex conjugate is 1 if $B = 0$, and for $B > 0$ it is

$$\overline{S(t_1, t_2, ...t_n, \mathbb{F}_q)}^B = (-1/\sqrt{q})^B \sum_{y_1, ..., y_B \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(-\sum_{b \leq B}(y_b^{N+1} + \sum_{i=1}^{n} t_i y_b^i)),$$

So $M_{A,B}(\mathbb{F}_q)$ is $(-1/\sqrt{q})^{A+B}(-1/q)^n$ times

$$\sum_{t_1,...,t_n\in\mathbb{F}_q}\ \sum_{x_1,...,x_A,y_1,...,y_B} \psi_{\mathbb{F}_q}(\sum_{a\le A} x_a^{N+1} - \sum_{b\le B} y_b^{N+1} + \sum_{i=1}^{n} t_i(\sum_{a\le A} x_a^i - \sum_{b\le B} y_b^i)).$$

Reversing the order of summation, and using orthogonality of characters, we see that $M_{A,B}(\mathbb{F}_q)$ is $(-1/\sqrt{q})^{A+B}$ times

$$\sum_{(x_1,...,x_A,y_1,...,y_B)\in V(A,B,n)(\mathbb{F}_q)} \psi_{\mathbb{F}_q}(\sum_{a\le A} x_a^{N+1} - \sum_{b\le B} y_b^{N+1}).$$

From the previous lemma, we know that for a point i$(x_1, ..., x_A, y_1, ..., y_B)$ in $V(A, B, n)(\mathbb{F}_q)$, the lists $(x_1, ..., x_A)$ and $(y_1, ..., y_B, 0, 0.., 0)$ are rearrangements of each other. The function $\sum_{a\le A} x_a^{N+1} - \sum_{b\le B} y_b^{N+1}$ vanishes at such a point, and hence this last sum is just $\#V(A, B, n)(\mathbb{F}_q)$. □

Proposition 5.3. *For $n \ge A > 0$, $M_{A,0}(\mathbb{F}_q) = M_{0,A}(\mathbb{F}_q) = (-1/\sqrt{q})^A$, and $M_{A,0} = M_{0,A} = 0$.*

Proof. The first assertion is immediate from the previous two lemmas, and the second follows because $M_{A,0}$ (resp. $M_{0,A}$) is the large q limit of $M_{A,0}(\mathbb{F}_q)$ (resp. of $M_{0,A}(\mathbb{F}_q)$). □

Corollary 5.4. *If $N = n$, the group G_{geom} for our sheaf $\mathcal{F}$ is $\{A \in GL(n) | \det(A)^p = 1\}$.*

Proof. In the previous section, we have seen that over $\mathbb{F}_{p^2}$ we have inclusions (remember $N = n$ here)

$$SL(n) \subset G_{geom} \subset G_{arith} \subset \{A \in GL(n) | \det(A)^{2p} = 1\}.$$

Hence $\det(\mathcal{F})^{\otimes p}$ is a lisse rank one sheaf on $\mathbb{A}^n_{\overline{\mathbb{F}_p}}$ which is of order dividing 2. But the group $H^1(\mathbb{A}^n_{\overline{\mathbb{F}_p}}, \mu_2)$ vanishes, because p is odd. So we have inclusions

$$SL(n) \subset G_{geom} \subset \{A \in GL(n) | \det(A)^p = 1\}.$$

We must rule out the possibility that G_{geom} is $SL(n)$. But if it were, then $\det(\mathcal{F})$, would be a geometrically trivial summand of $\mathcal{F}^{\otimes n}$, and $M_{n,0}$ would be nonzero. □

Proposition 5.5. *Suppose $n \ge A > B > 0$. For $C := A - B$, we have $M_{A,B} = 0$,*

$$M_{A,B}(\mathbb{F}_q) = O((1/\sqrt{q})^C),$$

and $(\sqrt{q})^C M_{A,B}(\mathbb{F}_q)$ has a nonzero large q limit.

Proof. In this case, $0 < A - B < n \leq N$, so already the scalars in $SL(N)$, namely μ_N, act by a nontrivial character, namely the $A-B$'th power of the "identical" character $\zeta \mapsto \zeta$, in the representation

$$std^{\otimes A} \otimes (std^\vee)^{\otimes B}.$$

A point in $V(A,B,n)(\mathbb{F}_q)$ is of the form $(x_1, ..., x_A, y_1, ..., y_B)$ such that at least $C := A - B$ of the x_i vanish, and such that the list of (at most B) nonvanishing x_a's is a rearrangement of the list of nonvanishing y_b's. Now break up $V(A,B,n)(\mathbb{F}_q)$ by the number d of distinct nonzero x_a in a point. There is exactly one point whose d is zero. For given d with $B \geq d \geq 1$, the number of points with d distinct nonzero x_a is the product of $\prod_{i=1}^{d}(q-i)$ with a strictly positive combinatorially defined integer, call it $D(A,B,n,d)$. Thus we have

$$\#V(A,B,n)(\mathbb{F}_q) = D(A,B,n,B)q^B + O(q^{B-1}).$$

Dividing by $\sqrt{q}^{A+B}$, we see that

$$M_{A,B}(\mathbb{F}_q) = (-1/\sqrt{q}^{A+B})\#V(A,B,n)(\mathbb{F}_q)$$

is

$$= (-1)^{A+B}D(A,B,n,B)/\sqrt{q}^C + O(1/\sqrt{q}^{C+2}).$$

□

Proposition 5.6. *For $n \geq A \geq 1$, we have the following results.*

(1) *For $A = 1$, $M_{1,1}(\mathbb{F}_q)$=1, and $M_{1,1} = 1$.*
(2) *For $A = 2$, we have*

$$M_{2,2}(\mathbb{F}_q) = 2 - 1/q.$$

(3) *For $n \geq A \geq 3$, we have*

$$M_{A,A}(\mathbb{F}_q) = A! - A(A-1)A!/4q + O(1/q^2).$$

Proof. Assertion (1) is immediate from the fact that $\#V(1,1,n)(\mathbb{F}_q) = q$. Assertion (2) is immediate from the fact that $\#V(2,2,n)(\mathbb{F}_q) = 2q(q-1) + q = 2q^2 - q$.

For $n \geq A \geq 3$, we break up $V(A,A,n)(\mathbb{F}_q)$ by the number d of distinct coordinates x_a in a point. The number of points with precisely d distinct x_a's is the product of $\prod_{i=0}^{d-1}(q-i)$ with a strictly positive combinatorially defined integer, call it $D(A,A,n,d)$.

We have $D(A,A,n,A) = A!$, and $D(A,A,n,A-1) = \binom{A}{2}^2 \times (A-2)!$. [The term $\binom{A}{2}^2$ is to specify on each side the placement of the double root, and the term $(A-2)!$ is to specify the reordering of the $A-2$ simple roots.

So looking at the two highest order terms, we have

$$\#V(A,A,n)(\mathbb{F}_q) =$$
$$A!\prod_{i=0}^{A-1}(q-i) + \binom{A}{2}^2 (A-2)!\prod_{i=0}^{A-2}(q-i) + O(q^{A-2}).$$

Expanding out $\prod_{i=0}^{A-1}(q-i)$, we get

$$\prod_{i=0}^{A-1}(q-i) = q^A - (A(A-1)/2)q^{A-1} + \text{lower terms}.$$

Thus $\#V(A,A,n)(\mathbb{F}_q)$ is

$$A!q^A - (A(A-1)/2)q^{A-1} + \binom{A}{2}^2 (A-2)!q^{A-1} + O(q^{A-2}) =$$
$$= A!q^A - (A(A-1)A!/4)q^{A-1} + O(q^{A-2}).$$

Dividing through by q^A gives the assertion. □

6. Cohomological consequences

We have seen in Lemma 5.2 that, up to a factor $(-1/\sqrt{q})^{A+B}$, $M_{A,B}$ is a polynomial in q, in principle quite explicit. A natural question is the extent to which we can infer from such information the vanishing, or nonvanishing, of various cohomology groups. Here are some results along this line.

Let us begin with the fact that $M_{1,1}(\mathbb{F}_q) = 1$. By the Lefschetz Trace Formula, this is equivalent to

$$\sum_{i=0}^{2n}(-1)^i \text{Trace}(Frob_{\mathbb{F}_q}|H_c^i(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, \mathcal{F}\otimes\mathcal{F}^\vee)) = q^n.$$

Already the trace on the H_c^{2n} is q^n. This suggests that $H_c^i(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, \mathcal{F}\otimes\mathcal{F}^\vee)$ vanishes for $i \neq 2n$. We will now show that this is in fact the case. Here is an equivalent formulation.

The sheaf $\mathcal{F}\otimes\mathcal{F}^\vee = End(\mathcal{F})$ has a direct sum decomposition

$$End(\mathcal{F}) = \overline{\mathbb{Q}_\ell} \oplus End^0(\mathcal{F}),$$

in which $End^0(\mathcal{F})$ is the subsheaf of endomorphisms of trace zero. The fact that $M_{1,1}(\mathbb{F}_q) = 1$ is thus equivalent to

$$\sum_{i=0}^{2n}(-1)^i \text{Trace}(Frob_{\mathbb{F}_q}|H_c^i(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, End^0(\mathcal{F}))) = 0.$$

Lemma 6.1. *The cohomology groups $H_c^i(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, End^0(\mathcal{F}))$ all vanish.*

Proof. Compute the cohomology via the Leray spectral sequence for the projection

$$pr : \mathbb{A}^n \to \mathbb{A}^{n-1}, \quad (a_1, ..., a_n) \mapsto (a_2, ..., a_n).$$

It suffices to show that all the $R^i pr_! End^0(\mathcal{F})$ vanish. By proper base change, it suffices to do this fibre by fibre. On the fibre over the point $\overline{a} := (a_2, ..., a_n)$, say with values in some finite extension $k/\mathbb{F}_q$, we have the polynomial

$$f_{\overline{a}}(x) := x^{N+1} + \sum_{i=2}^{n} a_i x^i \in k[x],$$

and our sheaf $\mathcal{F}$ on this fibre is the (naive) Fourier Transform of $\mathcal{L}_{\psi(f_{\overline{a}})}$. So the restriction of $\mathcal{F}$ to this fibre is geometrically irreducible, and **its** $M_{1,1}(k)$ is 1, by the same calculation as above. Therefore the restriction to this fibre of $End^0(\mathcal{F})$ has no H_c^2 (because $\mathcal{F}$ on this fibre is geometrically irreducible), and the alternating sum of traces of $Frob_k$ on its H_c^i is zero. On the other hand, its H_c^0 vanishes (because $End^0(\mathcal{F})$ is lisse on an open curve), and hence its H_c^1 must vanish, as all powers of $Frob_k$ have trace zero on this H_c^1. □

At the opposite extreme, we have the following result.

Lemma 6.2. *For $n \geq A \geq 1$, the cohomology group*

$$H_c^{2n-1}(\mathbb{A}^n_{\overline{\mathbb{F}_p}}, \mathcal{F}^{\otimes A} \otimes (\mathcal{F}^\vee)^{\otimes A-1})$$

is nonzero, and its subspace of highest weight $2n-1$ is nonzero.

Proof. This is immediate from Proposition 5.5. First it gives the vanishing of the H_c^{2n}. Then it tells us that

$$\sum_{i=0}^{2n-1} (-1)^i \text{Trace}(Frob_{\mathbb{F}_q} | H_c^i(\mathbb{A}^n_{\overline{\mathbb{F}_q}}, \mathcal{F}^{\otimes A} \otimes (\mathcal{F}^\vee)^{\otimes A-1})$$

is $O(\sqrt{q}^{2n-1})$, and that after division by $\sqrt{q}^{2n-1}$, its large q limit is nonzero. By Deligne, the H_c^i for $i < 2n-1$ have lower weight, so we get the asserted nonvanishing of the weight $2n-1$ part of the H_c^{2n-1}. □

Lemma 6.3. *For $n \geq A \geq 2$, the weight $2n-2$ part of*

$$H_c^{2n-1}(\mathbb{A}^n_{\overline{\mathbb{F}_p}}, \mathcal{F}^{\otimes A} \otimes (\mathcal{F}^\vee)^{\otimes A})$$

is nonzero, and has dimension at least $A(A-1)A!/4$, but its weight $2n-1$ part vanishes.

Proof. By Proposition 5.6, we have

$$\sum_{i=0}^{2n-1}(-1)^i\mathrm{Trace}(Frob_{\mathbb{F}_q}|H^i_c(\mathbb{A}^n_{\overline{\mathbb{F}_q}},\mathcal{F}^{\otimes A}\otimes(\mathcal{F}^\vee)^{\otimes A}))=$$

$$=-(A(A-1)A!/4)q^{n-1}+\text{ a polynomial in } q \text{ of lower degree.}$$

This already shows that the weight $2n-1$ part of H^{2n-1}_c vanishes. If we look at the parts of weight $2n-2$, only $(H^{2n-1}_c)^{wt.=2n-2}$ and $(H^{2n-2}_c)^{wt.=2n-2}$ are possibly nonzero, and we get

$$-\mathrm{Trace}(Frob_q|(H^{2n-1}_c)^{wt.=2n-2})+\mathrm{Trace}(Frob_q|(H^{2n-2}_c)^{wt.=2n-2})=$$

$$=-(A(A-1)A!/4)q^{n-1}.$$

We rewrite this as

$$\mathrm{Trace}(Frob_q|(H^{2n-1}_c)^{wt.=2n-2})=$$

$$=(A(A-1)A!/4)q^{n-1}+\mathrm{Trace}(Frob_q|(H^{2n-2}_c)^{wt.=2n-2}),$$

which gives the asserted result. □

7. Another example

We fix an **odd** integer $n\geq 3$, and a prime p not dividing $n(n-1)$. We consider, in characteristic p, the two parameter family of hyperelliptic curves

$$y^2=x^n+ax+b$$

over the open set of $\mathbb{A}^2$, parameters (a,b), where the discriminant of x^n+ax+b, namely

$$\Delta=\Delta(a,b):=(n-1)^{n-1}a^n+n^nb^{n-1},$$

is invertible. For this family of curves, its H^1 along the fibres, Tate twisted by $1/2$, is a lisse sheaf $\mathcal{F}$ on $\mathbb{A}^2[1/\Delta]$ of rank $2g=n-1$ which is pure of weight zero. Its trace function at a point (a,b) with values in a finite extension $\mathbb{F}_q$ is given by

$$\mathrm{Trace}(Frob_{(a,b),\mathbb{F}_q}|\mathcal{F})=(-1/\sqrt{q})\sum_{x\in\mathbb{F}_q}\chi_{2,\mathbb{F}_q}(x^n+ax+b).$$

Here $\chi_{2,\mathbb{F}_q}$ denotes the quadratic character of $\mathbb{F}_q^\times$, extended by zero to all of $\mathbb{F}_q$. To define $\sqrt{q}$, we fix a choice of $\sqrt{p}$ in $\overline{\mathbb{Q}_\ell}$ and then define $\sqrt{q}$ to be the appropriate power of $\sqrt{p}$.

One knows that for this $\mathcal{F}$, we have $G_{geom}=G_{arith}=Sp(n-1)$, cf. [Ka-ACT, Thm. 5.4 (1)]. In particular, the standard representation is irreducible, and hence $M_{1,0}=0$, i.e., $H^4_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}[1/\Delta],\mathcal{F})$ vanishes. Moreover, we have

Lemma 7.1. *For any finite extension $\mathbb{F}_q/\mathbb{F}_p$, $M_{1,0}(\mathbb{F}_q) = 0$.*

Proof. By definition, $M_{1,0}(\mathbb{F}_q)$ is $(1/\#\mathbb{A}^2[1/\Delta](\mathbb{F}_q))(-1/\sqrt{q})$ times the sum

$$\sum_{(a,b)\in\mathbb{A}^2[1/\Delta](\mathbb{F}_q),x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b).$$

If this sum extended over **all** $(a, b) \in \mathbb{A}^2[(\mathbb{F}_q)$, it would vanish; simply reverse the order of summation, i.e., write it as

$$\sum_{(a,x)\in\mathbb{A}^2(\mathbb{F}_q)} \sum_{b\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b),$$

and notice that the innermost sum $\sum_{b\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b)$ vanishes.

So it remains to show that

$$\sum_{(a,b)\in\mathbb{A}^2(\mathbb{F}_q)|\Delta(a,b)=0,x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b) = 0.$$

The condition $\Delta(a, b) = 0$ is the condition

$$(n-1)^{n-1}a^n + n^n b^{n-1} = 0,$$

which we rewrite as

$$(-a/n)^n = (b/(n-1))^{n-1}.$$

This means precisely that $(-a/n, b/(n-1))$ is of the form (t^{n-1}, t^n) for a unique $t \in \mathbb{F}_q$. So our sum is

$$\sum_{t\in\mathbb{F}_q,x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n - nt^{n-1}x + (n-1)t^n).$$

For $t = 0$, the inner sum becomes $\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n)$, which vanishes because n is odd. For $t \neq 0$, we use the fact that $x^n - nt^{n-1}x + (n-1)t^n$ is homogeneous in x, t of degree n, so we write it as $t^n(X^n - nX + n - 1)$ with $X := x/t$. The sum over $t \neq 0$ becomes

$$\sum_{t\in\mathbb{F}_q^\times,X\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(t^n(X^n - nX + n - 1)),$$

which is the product

$$(\sum_{t\in\mathbb{F}_q^\times} \chi_{2,\mathbb{F}_q}(t^n))(\sum_{X\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(X^n - nX + n - 1)),$$

in which the first factor vanishes (again because n is odd). □

In fact, we have the following explanation of this vanishing.

Lemma 7.2. *The cohomology groups $H^i_c(\mathbb{A}^2_{\mathbb{F}_p}[1/\Delta], \mathcal{F})$ all vanish.*

Proof. The idea is simply to imitate, cohomologically, the argument given above.

We first define a sheaf $\mathcal{F}$ on all of $\mathbb{A}^2$ which agrees with our previously defined $\mathcal{F}$ on $\mathbb{A}^2[1/\Delta]$ and whose trace function at any point $(a,b) \in \mathbb{A}^2(\mathbb{F}_q)$ is

$$(-1/\sqrt{q}) \sum_{x \in \mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b).$$

For this, we consider the sheaf $\mathcal{L}_{\chi_2(x^n+ax+b)}$ on the $\mathbb{A}^3$ of (x,a,b), with the understanding that this sheaf has been extended by zero across the points where $x^n + ax + b = 0$. For the projection of $\mathbb{A}^3$ onto $\mathbb{A}^2$ given by $pr(x,a,b) := (a,b)$, $R^i pr_!(\mathcal{L}_{\chi_2(x^n+ax+b)})$ vanishes for $i \neq 1$ (check fibre by fibre). The Tate-twisted sheaf $R^1 pr_!(\mathcal{L}_{\chi_2(x^n+ax+b)})(1/2)$ is the desired $\mathcal{F}$.

We wish to show that all the groups $H^i_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}[1/\Delta], \mathcal{F})$ vanish. Using the excision long exact sequence

$$\to H^i_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}[1/\Delta], \mathcal{F}) \to H^i_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}, \mathcal{F}) \to H^i_c((\Delta = 0)_{\overline{\mathbb{F}_p}}, \mathcal{F}) \to ...$$

we are reduced to showing the vanishing of all the groups $H^i_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}, \mathcal{F})$ and of all the groups $H^i_c((\Delta = 0)_{\overline{\mathbb{F}_p}}, \mathcal{F})$.

To show the vanishing of the groups $H^i_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}, \mathcal{F})$, we notice first that, from the construction of $\mathcal{F}$ as (a Tate twist of) the only nonvanishing $R^j pr_!(\mathcal{L}_{\chi_2(x^n+ax+b)})$, namely the R^1, we have

$$H^i_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}, \mathcal{F}) = H^{i+1}_c(\mathbb{A}^3_{\overline{\mathbb{F}_p}}, \mathcal{L}_{\chi_2(x^n+ax+b)})(1/2).$$

To show that these groups vanish, we use the projection $pr_{1,2}$ of $\mathbb{A}^3$ onto $\mathbb{A}^2$ given by $(x,a,b) \mapsto (x,a)$.

For this projection, all the $R^j(pr_{1,2})_!(\mathcal{L}_{\chi_2(x^n+ax+b)})$ vanish, as one sees looking fibre by fibre (the cohomological version of summing over b).

To show that the groups $H^i_c((\Delta = 0)_{\overline{\mathbb{F}_p}}, \mathcal{F})$ all vanish, we use the construction of $\mathcal{F}$ once again, this time to write

$$H^i_c((\Delta = 0)_{\overline{\mathbb{F}_p}}, \mathcal{F}) = H^{i+1}_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}, \mathcal{L}_{\chi_2(x^n - nt^{n-1}x + (n-1)t^n)}),$$

where the $\mathbb{A}^2$ in question is that of (x,t). By excision on this $\mathbb{A}^2$, it suffices to treat separately the open set $\mathbb{A}^1 \times \mathbb{G}_m$, coordinates x,t, and the line $t = 0$. On this line, with coordinate x, we are looking at the groups

$$H^{i+1}_c(\mathbb{A}^1_{\overline{\mathbb{F}_p}}, \mathcal{L}_{\chi_2(x^n)}),$$

which all vanish. On the product $\mathbb{A}^1 \times \mathbb{G}_m$, we make the $(t, x/t)$ substitution to write our sheaf as the external tensor product of $\mathcal{L}_{\chi_2(X^n - nX + n - 1)}$ on the first $\mathbb{A}^1$ factor with $\mathcal{L}_{\chi_2(t^n)}$ on the $\mathbb{G}_m$ factor. The vanishing

then results from Kunneth, because on the second factor all the groups $H^j_c((\mathbb{G}_m)_{\overline{\mathbb{F}_p}}, \mathcal{L}_{\chi_2(t^n)})$ vanish (again because n is odd). □

Thanks to a marvelous formula of Davenport-Lewis, we do have square root cancellation for $M_{1,1}(\mathbb{F}_q)$.

Lemma 7.3. *We have* $M_{1,1}(\mathbb{F}_q) = 1 + O(1/q)$.

Proof. Davenport and Lewis prove (cf. [Dav-Lew, (19) on page 55] or [Ka-MF, Lemma 8]) that for **any** $n \geq 0$, we have

$$\sum_{(a,b)\in\mathbb{A}^2(\mathbb{F}_q)} (\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b))^2 = q^2(q-1).$$

The sum over $(a,b) \in \mathbb{A}^2(\mathbb{F}_q)$ with $\Delta = 0$ is, as we have seen above, the sum

$$\sum_{t\in\mathbb{F}_q^\times} (\chi_{2,\mathbb{F}_q}(t^n) \sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n - nx + n - 1))^2 =$$

$$= (q-1)(\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n - nx + n - 1))^2 = O(q^2).$$

Thus the sum over $(a,b) \in \mathbb{A}^2[1/\Delta](\mathbb{F}_q)$ is $q^2(q-1) + O(q^2)$. Dividing by $\#\ A^2[1/\Delta](\mathbb{F}_q) = q^2(q-1)$, we find the asserted result. □

8. A third example

We fix an **even** integer $n \geq 4$, and a prime p not dividing $n(n-1)$. We consider, in characteristic p, the two parameter family of hyperelliptic curves

$$y^2 = x^n + ax + b$$

over the open set of $\mathbb{A}^2$, parameters (a,b), where the discriminant of $x^n + ax + b$, namely

$$\Delta = \Delta(a,b) := (n-1)^{n-1}a^n + n^n b^{n-1},$$

is invertible. For this family of curves, its H^1 along the fibres, Tate twisted by $1/2$, is a lisse sheaf $\mathcal{F}$ on $\mathbb{A}^2[1/\Delta]$ of rank $2g = n-2$ which is pure of weight zero. Its trace function at a point (a,b) with values in a finite extension $\mathbb{F}_q$ is given by

$$\mathrm{Trace}(Frob_{(a,b),\mathbb{F}_q}|\mathcal{F}) = (-1/\sqrt{q})(1 + \sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b)).$$

One knows [Ka-ACT, Thm. 5.17 (1)] that for this $\mathcal{F}$, we have $G_{geom} = G_{arith} = Sp(n-2)$. In particular, the standard representation is irreducible, and hence $M_{1,0} = 0$, i.e., $H^4_c(\mathbb{A}^2_{\overline{\mathbb{F}_p}}[1/\Delta], \mathcal{F})$ vanishes. However, in contradistinction to the case when n is odd, we have the following lemma.

Lemma 8.1. *We have*

$$M_{1,0}(\mathbb{F}_q) = -1/\sqrt{q} + O(1/q).$$

Proof. Here the discriminant $\Delta(a,b)$ vanishes precisely when

$$(n-1)^{n-1}a^n = n^n b^{n-1},$$

in other words when (a,b) is of the form $(a,b) = (nt^{n-1}, (n-1)t^n)$ for a unique $t \in \mathbb{F}_q$. Thus there are q points in $\mathbb{A}^2(\mathbb{F}_q)$ at which Δ vanishes. By definition, $M_{1,0}(\mathbb{F}_q)$ is $(-1/\sqrt{q})(1/(q(q-1))$ times the sum

$$\sum_{(a,b)\in\mathbb{A}^2[1/\Delta](\mathbb{F}_q)} (1 + \sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b)).$$

If this sum extended over all points (a,b) in $\mathbb{A}^2(\mathbb{F}_q)$, it would be q^2 (from summing the term 1); the sum over all (a,b,x) of $\chi_{2,\mathbb{F}_q}(x^n + ax + b)$ vanishes (for each (a,x), sum over b).

The sum over the $\mathbb{F}_q$ points where Δ vanishes is the sum

$$\sum_{(t,x)\in\mathbb{A}^2(\mathbb{F}_q)} (1 + \chi_{2,\mathbb{F}_q}(x^n + nt^{n-1}x + (n-1)t^n)) =$$

$$= q + \sum_{(t,x)\in\mathbb{A}^2(\mathbb{F}_q)} \chi_{2,\mathbb{F}_q}(x^n + nt^{n-1}x + (n-1)t^n).$$

In this second sum, the sum over the points $(0,x)$ is $q-1$ (because n is even). For each $t \neq 0$, we write

$$x^n + nt^{n-1}x + (n-1)t^n = t^n(X^n + nX + n - 1),$$

with $X := x/t$. Because n is even, for each $t \neq 0$ the sum over x of $\chi_{2,\mathbb{F}_q}(x^n + nt^{n-1}x + (n-1)t^n)$ is independent of t, equal to the quantity

$$\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + nx + n - 1).$$

So all in all, the sum over the $\mathbb{F}_q$ points where Δ vanishes is

$$2q - 1 + (q-1)\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + nx + n - 1).$$

So $M_{1,0}(\mathbb{F}_q)$ is $(-1/\sqrt{q})(1/(q(q-1))$ times the quantity

$$q^2 - 2q + 1 - (q-1)\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + nx + n - 1).$$

One checks easily that the polynomial $x^n + nx + n - 1$ has no triple roots, and that its unique double root is $x = -1$. We readily compute that

$$x^n + nx + n - 1 = (x+1)^2 P_{n-2}(x), \;\; P_{n-2}(x) = x^{n-2} - 2x^{n-3} + 3x^{n-4} + ... + (n-1).$$

Thus $P_{n-2}(x)$ is square free. As $x^n + nx + n - 1$ vanishes at $x = -1$, we have

$$\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + nx + n - 1) = \sum_{x\in\mathbb{F}_q, x\neq -1} \chi_{2,\mathbb{F}_q}(P_{n-2}(x)).$$

The value of $P_{n-2}(x)$ at $x = -1$ is $n(n-1)/2)$ (L'Hôpital's rule), so we get

$$\sum_{x\in\mathbb{F}_q, x\neq -1} \chi_{2,\mathbb{F}_q}(P_{n-2}(x)) = -1 - \chi_{2,\mathbb{F}_q}(n(n-1)/2) - S_{n-2}(\mathbb{F}_q).$$

with

$$S_{n-2}(\mathbb{F}_q) = -(1 + \sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(P_{n-2}(x))).$$

Here $S_{n-2}(\mathbb{F}_q)$ is the trace of $Frob_{\mathbb{F}_q}$ on H^1 of the complete nonsingular model of the hyperelliptic curve $y^2 = P_{n-2}(x))$ of genus $(n-4)/2$. In particular, $S_{n-2}(\mathbb{F}_q) = O(\sqrt{q})$.

Thus $M_{1,0}(\mathbb{F}_q)$ is $(-1/\sqrt{q})(1/(q(q-1))$ times the quantity

$$(q-1)^2 - (q-1)(-1 - \chi_{2,\mathbb{F}_q}(n(n-1)/2) - S_{n-2}(\mathbb{F}_q)) =$$

$$= q(q-1) + O(q^{3/2}).$$

Thus

$$M_{1,0}(\mathbb{F}_q) = -1/\sqrt{q} + O(1/q).$$

□

Lemma 8.2. *The cohomology group $H^4_c(\mathbb{A}^2_{\overline{\mathbb{F}}_p}[1/\Delta], \mathcal{F})$ vanishes, but the weight 3 part of $H^3_c(\mathbb{A}^2_{\overline{\mathbb{F}}_p}[1/\Delta], \mathcal{F})$ is one-dimensional, and $Frob_{\mathbb{F}_q}$ acts on it as $q^{3/2}$.*

Proof. The vanishing of the H^4_c is the fact that $M_{1,0} = 0$. By the Lefschetz trace formula, $M_{1,0}(\mathbb{F}_q)$ is $(1/(q(q-1))$ times the two term sum

$$-\mathrm{Trace}(Frob_{\mathbb{F}_q} | H^3_c(\mathbb{A}^2_{\overline{\mathbb{F}}_p}[1/\Delta], \mathcal{F}) + \mathrm{Trace}(Frob_{\mathbb{F}_q} | H^2_c(\mathbb{A}^2_{\overline{\mathbb{F}}_p}[1/\Delta], \mathcal{F}).$$

From our estimate that $M_{1,0}(\mathbb{F}_q) = -1/\sqrt{q} + O(1/q)$, we see that this sum is $-q^{3/2} + O(q)$. As H^i_c is mixed of weight $\leq i$, we get the asserted result. □

Remark 8.3. The reader may be concerned by the apparent sign ambiguity in the statement above, that the eigenvalue of $Frob_{\mathbb{F}_q}$ on the weight three part of $H^3_c(\mathbb{A}^2_{\overline{\mathbb{F}}_p}[1/\Delta], \mathcal{F})$ is $q^{3/2}$. Here is a more intrinsic way to say this. Instead of $\mathcal{F}$, consider the sheaf $\mathcal{H}$ which is the H^1 along the fibres of our family of curves $y^2 = x^n + ax + b$. In terms of

$\mathcal{H}$, we defined $\mathcal{F}$ to be the one-half Tate twist $\mathcal{H}(1/2)$, which involved a choice of $\sqrt{p}$ and a consequent determination of $\sqrt{q}$. The sheaf $\mathcal{H}$ is pure of weight one, the cohomology group $H^3_c(\mathbb{A}^2_{\overline{\mathbb{F}}_p}[1/\Delta], \mathcal{H})$ is mixed of weight ≤ 4, and what is being asserted is that its weight four part is one-dimensional, with $Frob_{\mathbb{F}_q}$ acting as q^2.

Exactly as in Lemma 7.3, the Davenport-Lewis formula gives square root cancellation for $M_{1,1}(\mathbb{F}_q)$.

Lemma 8.4. *We have $M_{1,1}(\mathbb{F}_q) = 1 + O(1/q)$.*

Proof. By definition, $M_{1,1}(\mathbb{F}_q)$ is $(1/q)(1/(q(q-1))$ times the sum

$$\sum_{(a,b)\in\mathbb{A}^2[1/\Delta](\mathbb{F}_q)} (1 + \sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b))^2.$$

Expanding the square, this is

$$q(q-1) + 2 \sum_{(a,b)\in\mathbb{A}^2[1/\Delta](\mathbb{F}_q)} \sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b) +$$

$$\sum_{(a,b)\in\mathbb{A}^2[1/\Delta](\mathbb{F}_q)} (\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b))^2.$$

If these last two summations extended over all $(a,b) \in \mathbb{A}^2(\mathbb{F}_q)$, the first would vanish, and the second would be $q^2(q-1)$ by the Davenport-Lewis formula. So our sum is

$$q(q-1) - 2 \sum_{(a,b)\in\mathbb{A}^2(\mathbb{F}_q), \Delta(a,b)=0} \sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b)$$

$$+q^2(q-1) - \sum_{(a,b)\in\mathbb{A}^2(\mathbb{F}_q), \Delta(a,b)=0} (\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b))^2.$$

The summands for $(a,b) = (0,0)$ are respectively $q-1$ and $(q-1)^2$, so both are $O(q^2)$. For each of the $q-1$ summands with $(a,b) \neq (0,0)$ but $\Delta(a,b) = 0$, the polynomial $x^n + ax + b$ has precisely $n-1$ roots, of which $n-2 > 0$ are simple roots. In particular, this polynomial is not geometrically a square, so the Weil bound gives

$$|\sum_{x\in\mathbb{F}_q} \chi_{2,\mathbb{F}_q}(x^n + ax + b)| \leq (n-1)\sqrt{q}.$$

So all in all, the total contribution of the $\Delta = 0$ terms is $O(q^2)$, and our sum over $\mathbb{A}^2[1/\Delta](\mathbb{F}_q)$ is $q^2(q-1) + O(q^2)$. Dividing through by $q^2(q-1)$ gives the asserted result. □

References

[Dav-Lew] Davenport, H.; Lewis, D. J. Notes on congruences. I. Quart. J. Math. Oxford Ser. (2) 14 1963 51-60.

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

[Gro-FL] Grothendieck, Alexander. Formule de Lefschetz et rationalité des fonctions L. (French) [Lefschetz formula and rationality of L-functions] Séminaire Bourbaki, Vol. 9, Exp. No. 279, 41-55, Soc. Math. France, Paris, 1995.

[Ka-ACT] Katz, Nicholas M. Affine cohomological transforms, perversity, and monodromy. J. Amer. Math. Soc. 6 (1993), no. 1, 149-222.

[Ka-GKM] Katz, Nicholas M. Gauss sums, Kloosterman sums, and monodromy groups. Annals of Mathematics Studies, 116. Princeton University Press, Princeton, NJ, 1988. x+246 pp.

[Ka-MF] Katz, Nicholas M. Monodromy of families of curves: applications of some results of Davenport-Lewis. Seminar on Number Theory, Paris 1979-80, pp. 171-195, Progr. Math., 12, Birkhäuser, Boston, Mass., 1981

[Ka-MG] Katz, Nicholas M. On the monodromy groups attached to certain families of exponential sums. Duke Math. J. 54 (1987), no. 1, 41-56.

[Ka-ST] Katz, Nicholas M. Sato-Tate in the higher dimensional case: elaboration of 9.5.4 in Serre's NX(p) book. Enseign. Math. 59 (2013), no. 3-4, 359-377.

[Ka-TLFM] Katz, Nicholas M. Twisted L-functions and monodromy. Annals of Mathematics Studies, 150. Princeton University Press, Princeton, NJ, 2002. viii+249 pp.

[Ka-Sar] Katz, Nicholas M.; Sarnak, Peter. Random matrices, Frobenius eigenvalues, and monodromy. American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, RI, 1999. xii+419 pp.

[La-We] Lang, S.; Weil, A. Number of points of varieties in finite fields. Amer. J. Math. 76, (1954). 819-827.

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