On a question of Rudnick: do we have square root cancellation for error terms in moment calculations?

Nicholas M. Katz

Department of Mathematics, Princeton University, Fine Hall, NJ 08544-1000, USA

We answer a question of Rudnick, largely in the negative, as to whether we have square root cancellation for error terms in moment calculations.

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 \([1]\) 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 \([2]\), combined with Deligne’s estimates \([3, \text{Corollary 3.3.4}]\). For any prime \( \ell \) not the characteristic \( p \) of \( k \), we have

\[
\#X(K) = \sum_{i=0}^{2n-1} (-1)^i \text{Trace} (\text{Frob}_K|H^i_c(X_{\bar{k}}, \mathbb{Q}_\ell)).
\]

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

So the formula becomes

\[
\#X(K) = (\#K)^n + \sum_{i=0}^{2n-1} (-1)^i \text{Trace} (\text{Frob}_K|H^i_c(X_{\bar{k}}, \mathbb{Q}_\ell)),
\]

with

\[
\sum_{i=0}^{2n-1} (-1)^i \text{Trace} (\text{Frob}_K|H^i_c(X_{\bar{k}}, \mathbb{Q}_\ell)) = O((\#K)^{n-1/2}).
\]
2. Background: Deligne's equidistribution theorem

How does Deligne’s equidistribution theorem relate to this? The situation is that we have a lisse $\tilde{\mathcal{Q}}_{\ell}$-sheaf, $\ell \neq p$, $\mathcal{F}$ on $X$ which is pure of weight zero, of rank $r \geq 1$. Attached to it is its geometric and arithmetic monodromy groups $G_{\text{geom}} \subseteq G_{\text{arith}} \subseteq GL(r)$. These are algebraic groups over $\tilde{Q}_{\ell}$. One knows, again by Deligne, that (the identity component of) $G_{\text{geom}}$ is semi-simple, cf. [3, Corollary 1.3.9 and its proof, and Theorem 3.4.1 (iii)].

Suppose that our $\mathcal{F}$ has $G_{\text{geom}} = G_{\text{arith}}$. Embed $\tilde{\mathcal{Q}}_{\ell}$ into $\mathbb{C}$, view $G_{\text{arith}}$ as a group over $\mathbb{C}$, and choose a maximal compact subgroup $K$. Say $\sigma$ is equidistributed in $K$. One knows, again by Deligne, that (the identity component of) $G_{\text{geom}}$ is semi-simple, cf. [3, Corollary 1.3.9 and its proof, and Theorem 3.4.1 (iii)].

Deligne’s equidistribution 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 $K$, for (the direct image from $\mathbb{K}$ of) Haar measure of total mass one, cf. [3, Theorem 3.5.3], [4, Theorem 3.6] and [5, Theorem 9.2.6].

The proof goes along the now usual lines, of estimating the appropriate Weyl sums. More precisely, for each irreducible non-trivial representation $\rho$ of $G_{\text{arith}}$, 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

$$\left(\frac{1}{#X(K)}\right) \sum_{x \in X(K)} \text{Trace}(\text{Frob}_{x,K} | \rho(\mathcal{F}))$$

vanishes.

This sum is

$$\left(\frac{1}{#X(K)}\right) \sum_{i=0}^{2n} (-1)^i \text{Trace}(\text{Frob}_{K} | H^i_{\mathcal{F}}(X_{\bar{K}}, \rho(\mathcal{F}))),$$

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

$$H^{2n}_{\mathcal{F}}(X_{\bar{K}}, \rho(\mathcal{F}))(n) = 0,$$

and we get the estimate

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

In view of Lang–Weil, we get

$$\left(\frac{1}{#X(K)}\right) \sum_{x \in X(K)} \text{Trace}(\text{Frob}_{x,K} | \rho(\mathcal{F})) = O\left(\frac{1}{\sqrt{# K}}\right).$$

An equivalent formulation is this. Take any representation $\sigma$ of $G_{\text{arith}}$, and denote by $N(\sigma)$ the multiplicity of the trivial representation in $\sigma$. Thus, $N(\sigma)$ is the dimension of $H^{2n}_{\mathcal{F}}(X_{\bar{K}}, \rho(\mathcal{F}))$, upon which Frob$_K$ operates as the scalar $(# K)^n$. Write $\sigma$ as the direct sum of $N(\sigma)$ copies of the trivial representation with a finite sum of irreducible non-trivial representation $\rho$ of $G_{\text{arith}}$, say $\sigma = N(\sigma) \mathbf{1} \oplus \tau$, with $N(\tau) = 0$. For $N(\sigma) \mathbf{1}$, i.e. for the constant sheaf $\tilde{\mathcal{Q}}^N_{\ell}(\sigma)$, we have the tautological equality

$$\left(\frac{1}{#X(K)}\right) \sum_{x \in X(K)} \text{Trace}(\text{Frob}_{x,K} | \tilde{\mathcal{Q}}^N_{\ell}(\sigma)) = N(\sigma).$$

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

$$\left(\frac{1}{#X(K)}\right) \sum_{x \in X(K)} \text{Trace}(\text{Frob}_{x,K} | \tau(\mathcal{F})) = \left(\frac{1}{#X(K)}\right) \sum_{i \leq 2n-1} (-1)^i \text{Trace}(\text{Frob}_{K} | H^i_{\mathcal{F}}(X_{\bar{K}}, \tau(\mathcal{F}))).$$
By Deligne (and Lang–Weil), this last sum is $O(1/\sqrt{#K})$, so we get

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

To the extent that the sum $\sum_{i \leq 2n-1} (-1)^i \text{Trace}({\text{Frob}}_K|H^i_c(X_{\mathbb{A}_K}, \tau(\mathcal{F})))$ has a better estimate, e.g. because some of its $H^i_c$ vanish for large $i$, or have lower weight than allowed by Deligne’s general theorem that $H^i_c$ 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 non-trivial representation $\rho$ of $G_{\text{arith}}$,

$$\left(\frac{1}{#X(K)}\right) \sum_{x \in X(K)} \text{Trace}({\text{Frob}}_{x,K}|\rho(\mathcal{F})) = O\left(\frac{1}{\sqrt{#K}}\right).$$

Equivalently, when will we get an estimate, for every representation $\sigma$ of $G_{\text{arith}}$,

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

4. Examples showing a largely negative response

In the following sections, we will give examples in which some $\sigma$’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 non-trivial additive character $\psi$ of $\mathbb{F}_p$. For $K/\mathbb{F}_p$, a finite extension, $\psi_K := \psi \circ \text{Trace}_{K/\mathbb{F}_p}$ is a non-trivial additive character of $K$. Consider the $n$ parameter family of sums, for each $K$, given by

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

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

$$\text{Trace}({\text{Frob}}_{t_1, t_2, \ldots, t_n, K}|\mathcal{F}) = S(t_1, t_2, \ldots, t_n, K).$$

This sheaf $\mathcal{F}$ is lisse of rank $N$ and pure of weight zero. One knows [6, Theorem 19] that for this sheaf $\mathcal{F}$ we have

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

**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

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

**Proof.** First extend scalars to $\mathbb{F}_{p^2}$. For any finite extension $K/\mathbb{F}_{p^2}$, each $\text{Frob}_{x,K}$ 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 $\det(\text{Frob}_{x,K})$ 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 $\ell$-adic cohomology). By the product formula, the determinant must be a unit also at
\( \mathcal{P} \), so is a root of unity of order dividing \( 2p \). If we take an extension \( K/F_p \) of odd degree, then the square of each \( \text{Frob}_{x,K} \) has such a determinant. Thus, we have inclusions

\[
SL(n) \subset G_{\text{geom}} \subset G_{\text{arith}} \subset \{ A \in GL(N) \mid \det(A)^{2p} = 1 \}.
\]

From these inclusions, we certainly have

\[
G_{\text{arith}} \subset G_mG_{\text{geom}} \quad (=GL(N),
\]

so there exist an \( \ell \)-adic unit \( \alpha \) such that after the constant field twist \( \alpha^{\text{deg}} \) of \( \mathcal{F} \), we have \( G_{\text{geom}} = G_{\text{arith}} \), cf. [7, Lemma 3.1]. It remains only to show that any such \( \alpha \) is a root of unity. [If for \( \alpha = 1 \), then after extension of scalars from \( F_p \) to \( F_{pN} \), we will have \( G_{\text{geom}} = G_{\text{arith}} \) for \( \mathcal{F} \).] To see that any such \( \alpha \) is a root of unity, choose any point \( x \in \mathbb{A}^n(F_p) \). Then both \( \text{Frob}_{x,F_p}|\mathcal{F} \) and \( \alpha \text{Frob}_{x,F_p}|\mathcal{F} \) lie in \( G_{\text{arith}} \), indeed the latter lies in \( G_{\text{geom}} \). Comparing determinants, both of which are roots of unity of order dividing \( 4p \), we see that \( \alpha \) 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 \( \mathbb{A}^n/F_q \), with \( F_q \) large enough that

\[
SL(n) \subset G_{\text{geom}} = G_{\text{arith}} \subset GL(N).
\]

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

\[
\text{std} \otimes^A \otimes (\text{std}^\vee)^\otimes B
\]

of \( G_{\text{arith}} \), 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

\[
M_{A,B} := \dim(\text{std} \otimes^A \otimes (\text{std}^\vee)^\otimes B)_{G_{\text{arith}}},
\]

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

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

the ‘empirical moment’

\[
M_{A,B}(\mathbb{F}_q) := (\frac{1}{q^n}) \sum_{(t_1, \ldots, t_n) \in \mathbb{A}^n(\mathbb{F}_q)} S(t_1, t_2, \ldots, t_n, \mathbb{F}_q)^A S(t_1, t_2, \ldots, t_n, \mathbb{F}_q)^B.
\]

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 \( \hat{\mathbb{Q}}_\ell \) 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 \( (t_1, \ldots, t_A, y_1, \ldots, y_B) \), 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 \((x_1, \ldots, x_A, y_1, \ldots, y_A) \in \mathbb{A}^{A+A}(\mathbb{F}_q)\) lies in \( V(A, A, n)(\mathbb{F}_q) \) if and only if the two lists \((x_1, \ldots, x_A)\) and \((y_1, \ldots, y_A)\) are rearrangements of each other, i.e. if and only if the first \( A \) elementary symmetric functions agree on them.
2. If \( n \geq A > B \geq 0 \), then a point \((x_1, \ldots, x_A, y_1, \ldots, y_B) \in \mathbb{A}^{A+B}(\mathbb{F}_q)\) lies in \( V(A, B, n)(\mathbb{F}_q) \) if and only if the two lists of length \( A \), \((x_1, \ldots, x_A)\) and \((y_1, \ldots, y_B, 0, 0, \ldots, 0)\) (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 \((0, \ldots, 0)\).

**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. \( \blacksquare \)

**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

\[
M_{A,B}(\mathbb{F}_q) = \left( -\frac{1}{\sqrt{q}} \right)^{A+B} \# V(A, B, n)(\mathbb{F}_q).
\]

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

\[
S(t_1, t_2, \ldots, t_n, \mathbb{F}_q) := \left( -\frac{1}{\sqrt{q}} \right)^{n} \sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q} \left( x^{N+1} + \sum_{i=1}^{n} t_i x^i \right).
\]

Its \( A \)’th power is then

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

The \( B \)th power of its complex conjugate is 1 if \( B = 0 \), and for \( B > 0 \) it is

\[
\bar{S}(t_1, t_2, \ldots, t_n, \mathbb{F}_q)^B = \left( -\frac{1}{\sqrt{q}} \right)^{B} \sum_{y_1, \ldots, y_B \in \mathbb{F}_q} \psi_{\mathbb{F}_q} \left( -\sum_{b \leq B} y_b^{N+1} + \sum_{i=1}^{n} t_i y_b^i \right),
\]

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

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

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

\[
\sum_{(x_1, \ldots, x_A, y_1, \ldots, y_B) \in V(A, B, n)(\mathbb{F}_q)} \psi_{\mathbb{F}_q} \left( \sum_{a \leq A} x_a^{N+1} - \sum_{b \leq B} y_b^{N+1} \right).
\]

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

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

**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 \( M_{0,A}(\mathbb{F}_q) \)). \( \blacksquare \)

**Corollary 5.4.** If \( N = n \), the group \( G_{\text{geom}} \) for our sheaf \( \mathcal{F} \) is \( \{ A \in GL(n) \mid \text{det}(A)^q = 1 \} \).
Proof. In the previous section, we have seen that over $\mathbb{F}_p^2$ we have inclusions (remember $N = n$ here)

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

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

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

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

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

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

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

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

$$\text{std}^{o_A} \otimes (\text{std}^y)^{o_B}.$$ 

A point in $V(A,B,n)(\mathbb{F}_q)$ is of the form $(x_1, \ldots, x_A, y_1, \ldots, y_B)$ such that at least $C := A - B$ of the $x_i$ vanish, and such that the list of (at most $B$) non-vanishing $x_i$s is a rearrangement of the list of non-vanishing $y_i$s. Now break up $V(A,B,n)(\mathbb{F}_q)$ by the number $d$ of distinct non-zero $x_a$ 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 non-zero $x_a$ 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

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

is

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

□

**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

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

3. For $n \geq A \geq 3$, we have

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

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 $\prod_{i=1}^{d-1} (q - i)$ with a strictly positive combinatorially defined integer, call it $D(A,A,n,d)$. 
We have $D(A, A, n, A) = A!$ and $D(A, A, n, A - 1) = (A - 2)^2 \times (A - 2)!$ [The term $(A - 2)^2$ 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

$$\# V(A, A, n)(\mathbb{F}_q) = A! + \frac{(A - 2)!}{2^2}$$

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

$$A!q^A - \frac{(A - 1)A!}{2}q^{A-1} + \frac{A!}{2}q^{A-2} + O(q^{A-2}).$$

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 non-vanishing, 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

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

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

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

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

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

$$\sum_{i=0}^{2n} (-1)^i \text{Trace}(\text{Frob}_{\mathbb{F}_q}|H^i_c(\mathbb{A}^n_{\mathbb{F}_q}, \text{End}^0(\mathcal{F}))) = 0.$$

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

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

$$pr : \mathbb{A}^n \to \mathbb{A}^{n-1}, \quad (a_1, \ldots, a_n) \mapsto (a_2, \ldots, a_n).$$
It suffices to show that all the $R^i \text{pr}_1 \text{End}^0(\mathcal{F})$ vanish. By proper base change, it suffices to do this fibre by fibre. On the fibre over the point $\tilde{a} := (a_2, \ldots, a_n)$, say with values in some finite extension $k/\mathbb{F}_q$, we have the polynomial

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

and our sheaf $\mathcal{F}$ on this fibre is the (naive) Fourier Transform of $L_{\psi(f)}$. 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 $\text{End}^0(\mathcal{F})$ has no $H^i_c$ (because $\mathcal{F}$ on this fibre is geometrically irreducible), and the alternating sum of traces of $\text{Frob}_k$ on its $H^i_c$ is zero. On the other hand, its $H^0_c$ vanishes (because $\text{End}^0(\mathcal{F})$ is lisse on an open curve), and hence its $H^1_c$ must vanish, as all powers of $\text{Frob}_k$ have trace zero on this $H^1_c$.

At the opposite extreme, we have the following result.

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

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

is non-zero and its subspace of highest weight $2n - 1$ is non-zero.

**Proof.** This is immediate from proposition 5.5. First it gives the vanishing of the $H^{2n}_c$. Then it tells us that

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

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

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

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

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

**Proof.** By proposition 5.6, we have

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

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

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 $(H^{2n-1}_c)^{\text{wt.}=2n-2}$ and $(H^{2n-2}_c)^{\text{wt.}=2n-2}$ are possibly non-zero, and we get

$$-\text{Trace}(\text{Frob}_{\mathbb{F}_q}(H^{2n-1}_c)^{\text{wt.}=2n-2}) + \text{Trace}(\text{Frob}_{\mathbb{F}_q}(H^{2n-2}_c)^{\text{wt.}=2n-2}) = -\left(\frac{A(A - 1)!}{4}\right) q^{n-1}.$$ 

We rewrite this as

$$\text{Trace}(\text{Frob}_{\mathbb{F}_q}(H^{2n-1}_c)^{\text{wt.}=2n-2}) = \left(\frac{A(A - 1)!}{4}\right) q^{n-1} + \text{Trace}(\text{Frob}_{\mathbb{F}_q}(H^{2n-2}_c)^{\text{wt.}=2n-2}),$$

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

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

is invertible. For this family of curves, its \( H^1 \) along the fibres, Tate twisted by \( \frac{1}{2} \), is a lisse sheaf \( \mathcal{F} \)
on \( \mathbb{A}^2[1/\Delta] \) of rank \( 2q = n - 1 \) 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

\[ \text{Trace} (\text{Frob}_{(a,b), \mathbb{F}_q} | \mathcal{F}) = \left( -\frac{1}{\sqrt{q}} \right) \sum_{x \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q} (x^n + ax + b). \]

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 \( \bar{\mathbb{Q}}_l \) and then define \( \sqrt{q} \) to be the appropriate power of \( \sqrt{p} \).

One knows that for this \( \mathcal{F} \), we have \( G_{\text{geom}} = G_{\text{arith}} = Sp(n-1) \), cf. \([8, \text{Theorem 5.4 (1)}]\). In particular, the standard representation is irreducible, and hence \( M_{1,0} = 0 \), i.e. \( H^1_{\text{cris}}(\mathbb{A}^2_{\mathbb{F}_p} [1/\Delta], \mathcal{F}) \) 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 note 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

\[ (n-1)^{n-1}a^n + n^b b^{n-1} = 0, \]

which we rewrite as

\[ \left( -\frac{a}{n} \right)^n = \left( \frac{b}{(n-1)} \right)^{n-1}. \]

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
It is known that \( t^n (X^n - nX + n - 1) \) with \( X := x/t \). The sum over \( t \neq 0 \) becomes

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

which is the product

\[
\left( \sum_{t \in \mathbb{F}_q^*} \chi_{2, \mathbb{F}_q}(t^n) \right) \left( \sum_{X \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q}(X^n - nX + n - 1) \right),
\]

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 \( H^i_c(\mathbb{A}_2^2 [1/\Delta], \mathcal{F}) \) all vanish.

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

We first define a sheaf \( \mathcal{F} \) on all of \( \mathbb{A}_2^2 \) which agrees with our previously defined \( \mathcal{F} \) on \( \mathbb{A}_2^2[1/\Delta] \) and whose trace function at any point \( (a, b) \in \mathbb{A}_2^2(\mathbb{F}_p) \) is

\[
\left( -\frac{1}{\sqrt{q}} \right) \sum_{x \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q}(x^n + ax + b).
\]

For this, we consider the sheaf \( \mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n + ax + b)} \) on the \( \mathbb{A}_2^3 \) 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 \( \mathbb{A}_2^3 \) onto \( \mathbb{A}_2^2 \) given by \( pr(x, a, b) := (a, b) \), \( R^1 pr_*(\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n + ax + b)}) \) vanishes for \( i \neq 1 \) (check fibre by fibre).

The Tate-twisted sheaf \( R^1 pr_*(\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n + ax + b)})(1/2) \) is the desired \( \mathcal{F} \).

We wish to show that all the groups \( H^i_c(\mathbb{A}_2^2 [1/\Delta], \mathcal{F}) \) vanish. Using the excision long exact sequence

\[
\to H^i_c(\mathbb{A}_2^2 [1/\Delta], \mathcal{F}) \to H^i_c(\mathbb{A}_2^2, \mathcal{F}) \to H^i_c((\Delta = 0)_{\mathbb{F}_p}, \mathcal{F}) \to \ldots
\]

we are reduced to showing the vanishing of all the groups \( H^i_c(\mathbb{A}_2^2, \mathcal{F}) \) and of all the groups \( H^i_c((\Delta = 0)_{\mathbb{F}_p}, \mathcal{F}) \).

To show the vanishing of the groups \( H^i_c(\mathbb{A}_2^2, \mathcal{F}) \), we note first that, from the construction of \( \mathcal{F} \) as (a Tate twist of) the only non-vanishing \( R^1 pr_*(\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n + ax + b)}) \), namely the \( R^1 \), we have

\[
H^i_c(\mathbb{A}_2^2, \mathcal{F}) = H^{i+1}_c(\mathbb{A}_2^3, \mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n + ax + b)})(1/2).
\]

To show that these groups vanish, we use the projection \( pr_{1,2} \) of \( \mathbb{A}_2^3 \) onto \( \mathbb{A}_2^2 \) given by \( (x, a, b) \mapsto (x, a) \).

For this projection, all the \( R^1(pr_{1,2})*(\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n + ax + b)}) \) vanish, as one sees looking fibre by fibre (the cohomological version of summing over \( b \)).

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

\[
H^i_c((\Delta = 0)_{\mathbb{F}_p}, \mathcal{F}) = H^{i+1}_c(\mathbb{A}_2^2, \mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)})
\]

where the \( \mathbb{A}_2^2 \) in question is that of \( (x, t) \). By excision on this \( \mathbb{A}_2^2 \), it suffices to treat separately the open set \( \mathbb{A}_1^1 \times \mathbb{G}_m \), coordinates \( x, t \) and the line \( t = 0 \). On this line, with coordinate \( x \), we are looking at the groups

\[
H^{i+1}_c(\mathbb{A}_1^1, \mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n)}),
\]

which all vanish. On the product \( \mathbb{A}_1^1 \times \mathbb{G}_m \), we make the \( (t, x/t) \) substitution to write our sheaf

\[
\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)}
\]

which is the product

\[
\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n)} \times \mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)}
\]

where all vanish. On the product \( \mathbb{A}_1^1 \times \mathbb{G}_m \), we make the \( (t, x/t) \) substitution to write our sheaf

\[
\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)}
\]

which is the product

\[
\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n)} \times \mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)}
\]

where all vanish. On the product \( \mathbb{A}_1^1 \times \mathbb{G}_m \), we make the \( (t, x/t) \) substitution to write our sheaf

\[
\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)}
\]

which is the product

\[
\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n)} \times \mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)}
\]

where all vanish. On the product \( \mathbb{A}_1^1 \times \mathbb{G}_m \), we make the \( (t, x/t) \) substitution to write our sheaf

\[
\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)}
\]

which is the product

\[
\mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n)} \times \mathcal{L}_{\mathbb{X}_2(\mathbb{A}^n - nX + n - 1)}
\]
Thanks to a marvelous formula of Davenport–Lewis, we do have square root cancellation for $M_{1,1}(F_q)$.

**Lemma 7.3.** We have $M_{1,1}(F_q) = 1 + O(1/q)$.

**Proof.** Davenport and Lewis prove (cf. [9, eqn (19), p. 55] or [10, Lemma 8]) that for any $n \geq 0$, we have

$$\sum_{(a,b) \in A^2(F_q)} \left( \sum_{x \in F_q} \chi_2(F_q)(x^n + ax + b) \right)^2 = q^2(q-1).$$

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

$$\sum_{t \in F_q^*} \left( \sum_{x \in F_q} \chi_2(F_q)(t^n - nx + n - 1) \right)^2 = (q-1) \left( \sum_{x \in F_q} \chi_2(F_q)(x^n - nx + n - 1) \right)^2 = O(q^2).$$

Thus, the sum over $(a,b) \in A^2(1/\Delta)(F_q)$ is $q^2(q-1) + O(q^2)$. Dividing by $\# A^2(1/\Delta)(F_q) = q^2(q-1)$, 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 $A^2$, parameters $(a,b)$, where the discriminant of $x^n + ax + b$, namely

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

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 $A^2(1/\Delta)$ 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 $F_q$ is given by

$$\text{Trace}(\text{Frob}_{(a,b),F_q}, \mathcal{F}) = \left( \frac{1}{\sqrt{q}} \right) \left( 1 + \sum_{x \in F_q} \chi_2(F_q)(x^n + ax + b) \right).$$

One knows [8, Theorem 5.17 (1)] that for this $\mathcal{F}$, we have $G_{\text{geom}} = G_{\text{arith}} = \text{Sp}(n-2)$. In particular, the standard representation is irreducible, and hence $M_{1,0} = 0$, i.e., $H^1_c(A^2(F_q), \mathcal{F})$ vanishes. However, in contradistinction to the case when $n$ is odd, we have the following lemma.

**Lemma 8.1.** We have

$$M_{1,0}(F_q) = -\frac{1}{\sqrt{q}} + O\left( \frac{1}{q} \right).$$

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

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

\[\text{on June 28, 2017 http://rsta.royalsocietypublishing.org/ Downloaded from } \text{http://rsta.royalsocietypublishing.org/}\]
in other words when \((a, b)\) is of the form \((a, b) = (nt^m - 1, (n - 1)t^m)\) for a unique \(t \in \mathbb{F}_q\). Thus, there are \(q\) points in \(\mathbb{A}^2(\mathbb{F}_q)\) at which \(\Delta\) vanishes. By definition, \(M_{1,0}(\mathbb{F}_q)\) is \((-1/\sqrt{q})(1/(q(q - 1)))\) times the sum
\[
\sum_{(a, b) \in \mathbb{A}^2(\mathbb{F}_q)} \left( 1 + \sum_{x \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q}(x^m + ax + b) \right).
\]
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 \(\chi_{2, \mathbb{F}_q}(x^m + ax + b)\) vanishes (for each \((a, x)\), sum over \(b\)).

The sum over the \(\mathbb{F}_q\) points where \(\Delta\) vanishes is the sum
\[
\sum_{(t, x) \in \mathbb{A}^2(\mathbb{F}_q)} (1 + \chi_{2, \mathbb{F}_q}(x^m + nt^{m-1}x + (n - 1)t^m))
= q + \sum_{(t, x) \in \mathbb{A}^2(\mathbb{F}_q)} \chi_{2, \mathbb{F}_q}(x^m + nt^{m-1}x + (n - 1)t^m).
\]
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
\[
x^m + nt^{m-1}x + (n - 1)t^m = t^m(X^m + nX + n - 1),
\]
with \(X := x/t\). Because \(n\) is even, for each \(t \neq 0\) the sum over \(x\) of \(\chi_{2, \mathbb{F}_q}(x^m + nt^{m-1}x + (n - 1)t^m)\) is independent of \(t\), equal to the quantity
\[
\sum_{x \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q}(x^m + nx + n - 1).
\]
So all in all, the sum over the \(\mathbb{F}_q\) points where \(\Delta\) vanishes is
\[
2q - 1 + (q - 1) \sum_{x \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q}(x^m + nx + n - 1).
\]
So \(M_{1,0}(\mathbb{F}_q)\) is \((-1/\sqrt{q})(1/(q(q - 1)))\) times the quantity
\[
q^2 - 2q + 1 - (q - 1) \sum_{x \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q}(x^m + nx + n - 1).
\]
One checks easily that the polynomial \(x^m + nx + n - 1\) has no triple roots, and that its unique double root is \(x = -1\). We readily compute that
\[
x^m + nx + n - 1 = (x + 1)^2P_{n-2}(x), \quad P_{n-2}(x) := x^{m-2} - 2x^{m-3} + 3x^{m-4} + \cdots + (n - 1).
\]
Thus \(P_{n-2}(x)\) is square free. As \(x^m + nx + n - 1\) vanishes at \(x = -1\), we have
\[
\sum_{x \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q}(x^m + nx + n - 1) = \sum_{x \in \mathbb{F}_q, x \neq -1} \chi_{2, \mathbb{F}_q}(P_{n-2}(x)).
\]
The value of \(P_{n-2}(x)\) at \(x = -1\) is \(n(n - 1)/2\) (L’Hôpital’s rule), so we get
\[
\sum_{x \in \mathbb{F}_q, x \neq -1} \chi_{2, \mathbb{F}_q}(P_{n-2}(x)) = -1 - \chi_{2, \mathbb{F}_q} \left( \frac{n(n - 1)}{2} \right) - S_{n-2}(\mathbb{F}_q)
\]
with
\[
S_{n-2}(\mathbb{F}_q) = - \left(1 + \sum_{x \in \mathbb{F}_q} \chi_{2, \mathbb{F}_q}(P_{n-2}(x))\right).
\]
Here \(S_{n-2}(\mathbb{F}_q)\) is the trace of \(\text{Frob}_{\mathbb{F}_q}\) on \(H^1\) of the complete non-singular 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,

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

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

**Proof.** The vanishing of the $H^4$ 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

$$-\text{Trace}(\text{Frob}_{\mathbb{F}_q} | H^2_c(\mathbb{A}^2_{\mathbb{F}_q}/[1/\Delta], \mathcal{F})) + \text{Trace}(\text{Frob}_{\mathbb{F}_q} | H^2_c(\mathbb{A}^2_{\mathbb{F}_q}/[1/\Delta], \mathcal{F})).$$

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 $H^3$ 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 Frobenius on the weight three part of $H^3_c(\mathbb{A}^2_{\mathbb{F}_q}/[1/\Delta], \mathcal{F})$ 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 $\sqrt{q}$ and a consequent determination of $\sqrt{q}$. The sheaf $\mathcal{H}$ is pure of weight one, the cohomology group $H^3_c(\mathbb{A}^2_{\mathbb{F}_q}/[1/\Delta], \mathcal{H})$ is mixed of weight less than or equal to 4, and what is being asserted is that its weight 4 part is one-dimensional, with Frobenius 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

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

Expanding the square, this is

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

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 $q(q-1)$ by the Davenport–Lewis formula. So our sum is

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

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

The summands for $(a,b) = (0,0)$ are $q - 1$ and $(q-1)^2$, respectively, 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
of which $n - 2 > 0$ are simple roots. In particular, this polynomial is not geometrically a square, so the Weil bound gives

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

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

References