RIGID LOCAL SYSTEMS AND A QUESTION OF WOOTTERS

NICHOLAS M. KATZ

How it started

Recently we learned from Ron Evans of some fascinating questions raised by Wootters [A-S-S-W]. These questions, which concern exponential sums, arose from his investigations of a particular quantum state with special properties, where the underlying vector space is the space of functions on the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, p a prime which is 3 mod 4. Due to our ignorance of the underlying physics, we concentrate on the exponential sums themselves. In our approach, it costs us nothing to work over an arbitrary finite field $\mathbb{F}_q$ of odd characteristic. [Thus $\mathbb{F}_q$ is "the" finite field of q elements, q a power of some odd prime p.] We also introduce a parameter $a \in \mathbb{F}_q^\times$. In the Wootters setup, where $q = p$ is 3 mod 4, the parameter a is simply $a = -1$. Ultimately we end up proving identities among exponential sums, but not at all in a straightforward way; we need to invoke the theory of Kloosterman sheaves and their rigidity properties, as well as the fundamental results of [De-Weil II] and [BBD]. It would be interesting to find direct proofs of these identities.

1. Statement of the problem

In what follows, we fix a finite field $\mathbb{F}_q$ of odd characteristic p, a nonzero element $a \in \mathbb{F}_q^\times$, and a nontrivial additive character ψ of $\mathbb{F}_q$:

$$\psi : (\mathbb{F}_q, +) \to \mu_p(\mathbb{C}) \subset \mathbb{C}^\times.$$

For example, when q is a power of p, we might begin with the additive character $\psi_{\mathbb{F}_p}$, $x \mapsto \exp(2\pi i x/p)$, of the prime field $\mathbb{F}_p$, and then take $\psi(y) := \psi_{\mathbb{F}_p}(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_p}(y))$. Once we have one choice of nontrivial ψ, any other is of the form

$$\psi_b(x) := \psi(bx)$$

for some unique $b \in \mathbb{F}_q^\times$. We denote by $\chi_2 : \mathbb{F}_q^\times \to \pm 1$ the quadratic character, which we extend to a function on all of F_q by decreeing that

$\chi_2(0) = 0$. We denote by $g(\psi, \chi_2)$ the Gauss sum

$$g(\psi, \chi_2) := \sum_{x \in \mathbb{F}_q} \psi(x)\chi_2(x).$$

One knows that $g(\psi, \chi_2)^2 = \chi_2(-1)q$. [Recall that $\chi_2(-1)$ is 1 if $q \equiv 1 \bmod 4$, and $\chi_2(-1)$ is -1 if $q \equiv 3 \bmod 4$. One knows that when $q = p$ and ψ is the $\psi_{\mathbb{F}_p}$ above, then $g(\psi_{\mathbb{F}_p}, \chi_2) = \sqrt{p}$ if $p \equiv 1 \bmod 4$, and $g(\psi_{\mathbb{F}_p}, \chi_2) = i\sqrt{p}$ if $p \equiv 3 \bmod 4$.]

The basic sums which underlie the Wootters story are the following. For $j, k \in \mathbb{F}_q$, we define

$$S(j,k) := \frac{-\sum_{x \in \mathbb{F}_q^\times} \chi_2(ax - x^3)\psi((j+k)^2 x + (j-k)^2(a/x))}{-g(\psi, \chi_2)}$$

$$= \frac{-\sum_{x \in \mathbb{F}_q^\times} \chi_2(a/x - x)\psi((j+k)^2 x + (j-k)^2(a/x))}{-g(\psi, \chi_2)}$$

$$= \frac{-\sum_{uv=a; u,v \in \mathbb{F}_q^\times} \chi_2(u - v)\psi((j+k)^2 v + (j-k)^2 u)}{-g(\psi, \chi_2)}.$$

The third expression makes most visible various symmetries. We have the identities

$$S(j,k) = S(k,j), \quad S(j,-k) = \chi_2(-1)S(j,k).$$

Because the complex conjugate of $g(\psi, \chi_2)$ is $\chi_2(-1)g(\psi, \chi_2)$, the sums $S(j,k)$ are all real. For $j, k \in \mathbb{F}_q$, we then define

$$P(j,k) := \delta_{j,k} + \chi_2(-1)\delta_{j,-k} + S(j,k).$$

Thus

$$P(j,k) := S(j,k), \text{ if } j^2 \neq k^2,$$
$$P(0,0) = 1 + \chi_2(-1) + S(0,0),$$

and for $j \neq 0$ we have

$$P(j,j) := 1 + S(j,j),$$

and

$$P(j,-j) := \chi_2(-1) + S(j,-j).$$

Thus the $P(j,k)$ are real, and satisfy

$$P(j,k) = P(k,j), \quad P(j,-k) = \chi_2(-1)P(j,k).$$

[When $q = p$, $p \equiv 3 \bmod 4$, $a = -1$ and we take $\psi(x) := \psi_{\mathbb{F}_p}(x/4)$, these $P(j,k)$ are equal to $p+1$ times the $P_{j,k}$ of Wootters.]

The key fact, that we learned from Wootters [A-S-S-W], and for which Ron Evans supplied a direct, "exponential sum" proof that we reproduce later on for the reader's convenience, is that if we view the $P(j,k)$ as forming a $q \times q$ matrix P, then

$$\mathrm{Trace}(P) = q - \chi_2(a),$$

and $(1/(q - \chi_2(a)))P$ is idempotent, i.e.

$$P^2 = (q - \chi_2(a))P,$$

i.e.,

$$(q - \chi_2(a))P(j,k) = \sum_{i \in \mathbb{F}_q} P(j,i)P(i,k).$$

Thus $(1/(q - \chi_2(a)))P$ is a real symmetric idempotent matrix of trace 1, so it is the orthogonal projection (for the usual inner product $\sum_i x_i y_i$ on $\mathbb{R}^q$) onto some one-dimensional subspace of $\mathbb{R}^q$. Let us choose a unit vector

$$v := (v_j)_{j \in \mathbb{F}_q} \in \mathbb{R}^q$$

in the one-dimensional subspace $Image(P)$. The vector v is unique up to sign. In terms of this vector v, the orthogonal projection onto its span is given by the matrix $v_j v_k$. So we have the identity

$$(1/(q - \chi_2(a)))P(j,k) = v_j v_k.$$

Equivalently, if we introduce the q rescaled numbers

$$V_j := (q - \chi_2(a))^{1/2} v_j, \ j \in \mathbb{F}_q,$$

we have the identities

$$P(j,k) = V_j V_k,$$

and these identities characterize [1] the vector

$$V := (V_j)_{j \in \mathbb{F}_q} \in \mathbb{R}^q$$

up to sign as the unique, up to sign, vector in $Image(P)$ of square norm $q - \chi_2(a)$.

Wootters found experimentally in the situation he was considering, namely $q = p$ and $a = -1$, that the V_j all lie in the closed interval $[-2, 2]$, and are approximately equidistributed, (i.e., as p grows) for the semicircle measure $(1/2\pi)\sqrt{4 - x^2}dx$ on this interval $[-2, 2]$. Equivalently, if we write $V_j = 2\cos\theta_j$, with $\theta_j \in [0, \pi]$, Wootters found experimentally that the p angles $\{\theta_j\}_{j \in \mathbb{F}_p}$ are approximately equidistributed for the Sato-Tate measure $(2/\pi)\sin^2\theta d\theta$ on $[0, \pi]$.

The problem posed by Wootters [A-S-S-W] was to prove this approximate equidistribution. We will show that so long as the characteristic

[1] I am told by Wootters that this vector V is a "minimum-uncertainty state" in the sense of [S-W], and that, at least when q is 3 mod 4, it may be the unique eigenvector of the antiunitary operator of section 9 of [Ap].

p satisfies $p \geq 5$, then whatever the finite extension $\mathbb{F}_q$ of $\mathbb{F}_p$, and whatever the value of $a \in \mathbb{F}_q^\times$, the V_j all lie in the closed interval $[-2, 2]$, and are approximately equidistributed, (i.e., as q grows) for the semicircle measure $(1/2\pi)\sqrt{4 - x^2}dx$ on this interval $[-2, 2]$. [The equidistribution statement is false in characteristic 3.]

2. Statement of the results: first formulation

We will define sums $V(j)$, for $j \in \mathbb{F}_q$. These $V(j)$ will also have the property that

$$V(-j) = \chi_2(-1)V(j).$$

We will first show that

$$V(j)^2 = P(j, j).$$

We will then show that

$$V(j)V(k) = P(j, k)$$

for all $j, k \in \mathbb{F}_q$.

The sums $V(j)$ will be real, and lie in the closed interval $[-2, 2]$. It will be a (known) theorem that the q sums $\{V(j)\}_{j \in \mathbb{F}_q}$, are approximately equidistributed, (i.e., as q grows) for the semicircle measure $(1/2\pi)\sqrt{4 - x^2}dx$ on this interval $[-2, 2]$. Equivalently, if we write $V(j) = 2\cos\theta_j$, with $\theta_j \in [0, \pi]$, then the q angles $\{\theta_j\}_{j \in \mathbb{F}_q}$ are approximately equidistributed for the Sato-Tate measure $(2/\pi)\sin^2\theta d\theta$ on $[0, \pi]$. This known theorem then solves the problem posed by Wootters.

3. Definition of the sums $V(j)$, when $q \equiv 1 \bmod 4$

Recall that we have fixed both an element $a \in \mathbb{F}_q^\times$ and a nontrivial additive character of $\mathbb{F}_q$. We now make two further auxiliary choices.

We choose a character χ_4 of $\mathbb{F}_q^\times$. Concretely, since $q \equiv 1 \bmod 4$ and $\mathbb{F}_q^\times$ is cyclic, the set $\mu_4(\mathbb{F}_q)$ of solutions in $\mathbb{F}_q^\times$ of the equation $X^4 = 1$ is a cyclic group of order 4, and the map $x \mapsto x^{(q-1)/4}$ is a surjective homomorphism of $\mathbb{F}_q^\times$ onto $\mu_4(\mathbb{F}_q)$. If we then pick one of the two possible group isomorphisms between $\mu_4(\mathbb{F}_q)$ and $\mu_4(\mathbb{C})$, call it ω, then we may take $\chi_4(x) := \omega(x^{(q-1)/4})$. We next choose a square root ϵ of $\chi_4(-a)$. These are our two auxiliary choices. We define

$$A := \epsilon\sqrt{q}.$$

We next define, for $j \in \mathbb{F}_q$, sums $W(j)$ by

$$W(j) := \frac{-\sum_{x \in \mathbb{F}_q^\times} \chi_4(x)\psi(x + aj^4/x)}{A}.$$

We then define

$$V(j) := W(j) \text{ for } j \neq 0.$$

For $j = 0$, $W(0)$ is a rescaled quartic Gauss sum, so has absolute value 1, and we define

$$V(0) := 2Re(W(0)) = W(0) + \overline{W(0)} = W(0) + 1/W(0).$$

Lemma 3.1. *When $q \equiv 1 \bmod 4$, the sums $V(j)$ are real, and satisfy*

$$V(-j) = \chi_2(-1)V(j)(= V(j)).$$

Proof. The second assertion is obvious from the definition.For $j = 0$, the reality is obvious from the definition. For $j \neq 0$, the complex conjugate of of $V(j)$ is

$$\frac{-\sum_{x\in\mathbb{F}_q^\times} \chi_4(1/x)\psi(-x - aj^4/x)}{\overline{A}}.$$

Under the involution $x \mapsto at^4/x$, this sum becomes

$$\frac{-\sum_{x\in\mathbb{F}_q^\times} \chi_4(x/aj^4)\psi(-x - aj^4/x)}{\overline{A}},$$

and writing $-x$ for x it becomes

$$\frac{-\sum_{x\in\mathbb{F}_q^\times} \chi_4(x/(-aj^4))\psi(x + aj^4/x)}{\overline{A}},$$

which is just

$$\overline{\chi_4}(-aj^4)(A/\overline{A})V(j) = \overline{\chi_4}(-a)(A/\overline{A})V(j) = \overline{\chi_4}(-a)\epsilon^2 V(j) = V(j)$$

the last equality by the definition of ϵ as a square root of $\chi_4(-a)$. □

4. Definition of the sums $V(j)$, when $q \equiv 3 \bmod 4$

In this case, the definition of our sums involves the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$, and the Trace and Norm maps from $\mathbb{F}_{q^2}$ down to $\mathbb{F}_q$,

$$\text{Trace} := \text{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q} \text{ and Norm} := \text{Norm}_{\mathbb{F}_{\mathrm{q}^2}/\mathbb{F}_{\mathrm{q}}}.$$

Again we make two auxiliary choices. Since $q^2 \equiv 1 \bmod 8$, we may choose a character χ_8 of order 8 of $\mathbb{F}_{q^2}^\times$.

In what follows, we will have to consider the quantity $\chi_8(-a)$, where we now view a as lying in the larger field $\mathbb{F}_{q^2}$. But this is simple to evaluate. For if $x \in \mathbb{F}_q^\times$ and $q \equiv 3 \bmod 4$, then we can write

$$x^{(q^2-1)/8} = (x^{(q-1)/2})^{(q+1)/4}.$$

So for $\chi_{2,\mathbb{F}_q}$ the quadratic character of $\mathbb{F}_q^\times$, we have

$$\chi_8(x) = \chi_{2,\mathbb{F}_q}(x)^{(q+1)/4}.$$

Thus $\chi_8(x) = 1$ for all $x \in \mathbb{F}_q^\times$ if $q \equiv 7 \bmod 8$, and $\chi_8(x) = \chi_{2,\mathbb{F}_q}(x)$ for $x \in \mathbb{F}_q^\times$ if $q \equiv 3 \bmod 8$. Our second choice is of a square root δ of $\chi_8(-a)$. We then define

$$A := \delta\sqrt{q}.$$

With these choices, we define $V(j)$ by

$$V(j) := \frac{-\chi_{2,\mathbb{F}_q}(j)\sum_{z\in\mathbb{F}_{q^2},\mathrm{Norm}(z)=aj^4}\chi_8(z)\psi(\mathrm{Trace}(z))}{A}.$$

Notice that in this $q \equiv 3 \bmod 4$ case, we have

$$V(0) = 0.$$

Lemma 4.1. *When $q \equiv 3 \bmod 4$, the sums $V(j)$ are real, and satisfy*

$$V(-j) = \chi_2(-1)V(j)(= -V(j)).$$

Proof. For $j = 0$ there is nothing to prove. For $j \neq 0$, the complex conjugate of $V(j)$ is

$$\frac{-\chi_{2,\mathbb{F}_q}(j)\sum_{z\in\mathbb{F}_{q^2},\mathrm{Norm}(z)=aj^4}\chi_8(1/z)\psi(\mathrm{Trace}(-z))}{\overline{A}}.$$

Denote by σ the nontrivial automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$. Then $\mathrm{Norm}(z) = z\sigma(z) = aj^4$, so $1/z = \sigma(z)/aj^4$ in this sum, which is thus

$$\frac{-\chi_{2,\mathbb{F}_q}(j)\sum_{z\in\mathbb{F}_{q^2},\mathrm{Norm}(z)=aj^4}\chi_8(\sigma(z)/aj^4)\psi(\mathrm{Trace}(-z))}{\overline{A}}.$$

Writing $-z$ for z, which doesn't change the norm of z, this sum is

$$\frac{-\chi_{2,\mathbb{F}_q}(j)\sum_{z\in\mathbb{F}_{q^2},\mathrm{Norm}(z)=aj^4}\chi_8(\sigma(z)/(-aj^4))\psi(\mathrm{Trace}(z))}{\overline{A}}.$$

Now replacing z by $\sigma(z)$, and remembering that z and $\sigma(z)$ have the same Trace, this sum is

$$\frac{-\chi_{2,\mathbb{F}_q}(j)\sum_{z\in\mathbb{F}_{q^2},\mathrm{Norm}(z)=aj^4}\chi_8(z/(-aj^4))\psi(\mathrm{Trace}(z))}{\overline{A}} =$$

$$= \overline{\chi_8}(-aj^4)(A/\overline{A})V(j).$$

As already noted, $\chi_8(j) = \pm 1$ (because $j \in \mathbb{F}_q$), and so the factor $\overline{\chi_8}(-aj^4)(A/\overline{A})$ is just $\overline{\chi_8}(-a)\delta^2 = 1$, this last equality by the definition of δ as a square root of $\chi_8(-a)$. □

5. Definition of the sums $S(j,k), P(j,k), V(j)$ over finite extensions of $\mathbb{F}_q$

Given a finite extension field $E/\mathbb{F}_q$, we may view the element $a \in \mathbb{F}_q$ as lying in E. We take for ψ_E the additive character of E given by $x \mapsto \psi(\mathrm{Trace}_{E/\mathbb{F}_q}(x))$, and for $\chi_{2,E}$ the quadratic character of $E^\times$; thus $\chi_{2,E} = \chi \circ \mathrm{Norm}_{E/\mathbb{F}_q}$. We may then define, for $j, k \in E$, the sums $S(j,k)$ and $P(j,k)$ over E, denoting them $S(j,k,E)$ and $P(j,k,E)$ to show that we are now working over E.

In order to define the sums $V(j)$ over E, which we will denote $V(j,E)$, we now specify how, given the choices we made in defining them over $\mathbb{F}_q$, we are to make the "correct" choices over E.

In the case when $q \equiv 1 \bmod 4$, then $\#E \equiv 1 \bmod 4$. We take for $\chi_{4,E}$ the quartic character of $E^\times$ given by $x \mapsto \chi_4(\mathrm{Norm}_{E/\mathbb{F}_q}(x))$, and for ϵ_E the square root of $\chi_{4,E}(-a)$ given by $\epsilon^{deg(E/\mathbb{F}_q)}$. With these choices, for an element $j \in E$ we apply the $\#E \equiv 1 \bmod 4$ recipe, now over the ground field E, to define the sum $V(j,E)$.

In the case when $q \equiv 3 \bmod 4$, the situation is a bit more complicated. If $E/\mathbb{F}_q$ has odd degree d, then $\#E \equiv 3 \bmod 4$. The quadratic extension E_2/E of E is a degree d extension of $\mathbb{F}_{q^2}$. We take for χ_{8,E_2} the octic character of E_2 given by $x \mapsto \chi_8(\mathrm{Norm}_{E_2/\mathbb{F}_{q^2}}(x))$, and we take for δ_E the square root of $\chi_{8,E_2}(-a)$ given by δ^d. With these choices, for an element $j \in E$ we apply the $\#E \equiv 3 \bmod 4$ recipe, now over the ground field E, to define the sum $V(j,E)$.

If, on the other hand, $q \equiv 3 \bmod 4$ and $E/\mathbb{F}_q$ has even degree d, then $\#E \equiv 1 \bmod 4$. We take for $\chi_{4,E}$ either quartic character. [To fix one system of choices, view E as an extension of $\mathbb{F}_{q^2}$, take $\chi_{4,\mathbb{F}_{q^2}} := \chi_8^2$, and then take $\chi_{4,E}$ to be the composition of $\chi_{4,\mathbb{F}_{q^2}}$ with the Norm from E down to $\mathbb{F}_{q^2}$.] Because $-a \in \mathbb{F}_q$, we have $\chi_{4,E}(-a) = 1$; we take as its square root $\delta_E := (-1)^{(\#E-1)/8} = \chi_{8,E}(-1)$ (this last equality valid for any octic character $\chi_{8,E}$ of $E^\times$) and thus our new A over E is

$$A := \chi_{8,E}(-1)q^{deg(E/\mathbb{F}_{q^2})}.$$

With these choices, for an element $j \in E$ we apply the $\#E \equiv 1 \bmod 4$ recipe, now over the ground field E, to define the sum $V(j,E)$. [The fact that this sum does not depend on which choice of $\chi_{4,E}$ we take results from the fact, already noted, that as $a \in \mathbb{F}_q$, we have $\chi_8(a) = \pm 1$, and hence $\chi_4(a) = 1$ for either choice of χ_4. Hence also $\chi_{4,E}(at^4) = 1$ for every $t \in E^\times$. The involution $x \mapsto at^4/x$ then turns the $\chi_{4,E}$ sum for $V(j, E)$, namely

$$-\sum_{x\in E^\times} \chi_{4,E}(x)\psi_E(x + at^4/x)/A,$$

into the $\overline{\chi_{4,E}}$ sum.]

6. Sheaf-theoretic reformulation of the $V(j)$, via Kloosterman sheaves

We choose a prime number $\ell \neq p$ (e.g., $\ell = 2$ is always an allowed choice, as p is odd), and an embedding of the cyclotomic field $\mathbb{Q}(\zeta_p, \zeta_8)$ into $\overline{\mathbb{Q}_\ell}$. This allows us to view all of our sums as lying in $\overline{\mathbb{Q}_\ell}$. In what follows, we will make free use of the theory of Kloosterman sheaves, cf. [Ka-ClausCar, Section 2] for a quick review, or [Ka-GKM, 4.1.1, with all b_i's taken to be 1, and 4.1.2 (2)] for the relevant existence and uniquenness theorems. We will also make free use of Kummer sheaves $\mathcal{L}_\chi$, cf. [Ka-GKM, 4.3] for their definition and basic properties.

When $q \equiv 1 \bmod 4$, we have the Kloosterman sheaf $Kl(\psi; \chi_4, \mathbb{1})$ on $\mathbb{G}_m/\mathbb{F}_q$ and its constant field twist $Kl(\psi; \chi_4, \mathbb{1}) \otimes A^{-deg}$. This is a lisse sheaf of rank two on $\mathbb{G}_m/\mathbb{F}_q$, which is pure of weight zero. We define the lisse sheaf $\mathcal{V}_0$ on $\mathbb{G}_m/\mathbb{F}_q$ as its pullback by $t \mapsto at^4$:

$$\mathcal{V}_0 := [t \mapsto at^4]^\star Kl(\psi; \chi_4, \mathbb{1}) \otimes A^{-deg}.$$

When $q \equiv 3 \bmod 4$, we have the additive character

$$\psi_{\mathbb{F}_{q^2}} := \psi \circ \mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$$

of the quadratic extension $\mathbb{F}_{q^2}$, and the Kloosterman sheaf on $\mathbb{G}_m/\mathbb{F}_{q^2}$ given by $Kl(\psi_{\mathbb{F}_{q^2}}; \chi_8, \chi_8^q)$. As explained in [Ka-GKM, 8.8, esp. 8.8.7], this sheaf has a canonical descent to a lisse sheaf denoted $Kl(\mathbb{F}_{q^2}, \psi_{\mathbb{F}_{q^2}}, \chi_8)$ on $\mathbb{G}_m/\mathbb{F}_q$. We first form its constant field twist $Kl(\mathbb{F}_{q^2}, \psi_{\mathbb{F}_{q^2}}, \chi_8) \otimes A^{-deg}$. This is a lisse sheaf of rank two on $\mathbb{G}_m/\mathbb{F}_q$, which is pure of weight zero. We then form its pullback by $t \mapsto at^4$, and tensor this pullback with the Kummer sheaf $\mathcal{L}_{\chi_2(t)}$ for the quadratic character χ_2. The resulting sheaf we define to be $\mathcal{V}_0$.

$$\mathcal{V}_0 := \mathcal{L}_{\chi_2(t)} \otimes [t \mapsto at^4]^\star Kl(\mathbb{F}_{q^2}, \psi_{\mathbb{F}_{q^2}}, \chi_8) \otimes A^{-deg}.$$

[We remark in passing that with these definitions, the pullback of this $\mathcal{V}_0$ to $\mathbb{G}_m/\mathbb{F}_{q^2}$ is

$$\mathcal{L}_{\chi_{2,\mathbb{F}_{q^2}}(t)} \otimes [t \mapsto at^4]^\star Kl(\psi_{\mathbb{F}_{q^2}}; \chi_8, \chi_8^q) \otimes (A^2)^{-deg},$$

which is isomorphic to $[t \mapsto at^4]^\star Kl(\psi_{\mathbb{F}_{q^2}}; \chi_4, \mathbb{1}) \otimes (\chi_8(-1)q)^{-deg}$. This last isomorphism, on the level of character sums, is the identity that for $t \in \mathbb{F}_{q^2}^\times$, we have

$$-\chi_{2,\mathbb{F}_{q^2}}(t) \sum_{x \in \mathbb{F}_{q^2}^\times} \chi_8(x)\chi_8^q(at^4/x)\psi_{\mathbb{F}_{q^2}}(x + at^4/x)/(\chi_8(-a)q) =$$

$$-\sum_{x \in \mathbb{F}_{q^2}^\times} \chi_4(x)\psi_{\mathbb{F}_{q^2}}(x + at^4/x)/(\chi_8(-1)q)$$

(and the analogous identity over all finite extensions $E/\mathbb{F}_{q^2}$).To see this, write

$$\chi_{2,\mathbb{F}_{q^2}}(t)/\chi_8(-a) = \chi_{2,\mathbb{F}_{q^2}}(1/t)/\chi_8(-a) = \chi_8^q(1/at^4),$$

which then gives the first sum as being

$$-\sum_{x \in \mathbb{F}_{q^2}^\times} \chi_8(x)\chi_8^q(1/x)\psi_{\mathbb{F}_{q^2}}(x + at^4/x)/(\chi_8(-1)q),$$

which, with the choice of $\chi_4 := \chi_8^{1-q}$, is precisely the second sum.]

Given the definition of Kloosterman sheaves and their canonical descents, the following theorem is a tautology.

Theorem 6.1. *The trace function of the lisse sheaf $\mathcal{V}_0$ on $\mathbb{G}_m/\mathbb{F}_q$ is given as follows. For $E/\mathbb{F}_q$ a finite extension, and $t \in \mathbb{G}_m(E) = E^\times$,*

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{V}_0) = V(t, E).$$

From the known [Ka-GKM, 7.4.1] local monodromy at 0 of Kloosterman sheaves, we see that

Lemma 6.2. *For $j : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion, the sheaf*

$$\mathcal{V} := j_\star \mathcal{V}_0$$

is lisse on $\mathbb{A}^1$. It is the unique lisse sheaf on $\mathbb{A}^1$ whose restriction to $\mathbb{G}_m$ is $\mathcal{V}_0$.

Proof. That $j_\star \mathcal{V}_0$ is lisse at 0 is a geometric statement. Geometrically, i.e. over $\overline{\mathbb{F}_q}$, $\mathcal{V}_0$ is $[t \mapsto at^4]^\star Kl(\psi; \chi_4, \mathbb{1})$. Geometrically, the local monodromy of $Kl(\psi; \chi_4, \mathbb{1})$ at 0 is the direct sum $\chi_4 \oplus \mathbb{1}$, whose pullback by $t \mapsto at^4$ is geometrically $\mathbb{1} \oplus \mathbb{1}$. If we interpret lisse sheaves as representations of the fundamental group π_1, uniqueness is simply the statement that $\pi_1(\mathbb{G}_m)$ maps **onto** $\pi_1(\mathbb{A}^1)$. □

We have the following fundamental result on the geometric and arithmetic monodromy groups of $\mathcal{V}$.

Theorem 6.3. *The sheaf $\mathcal{V}$ on $\mathbb{A}^1$ is lisse of rank two and pure of weight zero. If $p \geq 5$, its geometric and arithmetic monodromy groups on $\mathbb{A}^1$ are given by $G_{geom} = G_{arith} = SL(2)$.*

Proof. We have proven that $\mathcal{V}$ is lisse of rank two on $\mathbb{A}^1$. Its restriction to $\mathbb{G}_m$ is pure of weight zero. Then $\mathcal{V}[1]$ on $\mathbb{A}^1$ is a lisse perverse sheaf which is the middle extension of its restriction $\mathcal{V}_0[1]$ to $\mathbb{G}_m$. As a perverse sheaf on $\mathbb{G}_m$, $\mathcal{V}_0[1]$ is pure of weight one. One knows that middle extension preserves purity [BBD, 5.3.2] of a given weight, hence $\mathcal{V}[1]$ as perverse sheaf is pure of weight one, which in turn means precisely that $\mathcal{V}$ is pure of weight zero.

We now turn to showing that $G_{geom} = G_{arith} = SL(2)$ when $p \geq 5$. We will first show that the identity component G^0_{geom} is $SL(2)$. By a general result of Deligne [De-Weil II, 3.4.1 (iii), 1.3.9 and the second sentence of its proof], G^0_{geom} is a connected semisimple subgroup of $GL(2)$, so it must be either $SL(2)$ or the trivial group. Of the two choices, it is $SL(2)$ precisely when G^0_{geom} acts irreducibly in the given two-dimensional representation, i.e., precisely when $\mathcal{V}$ is geometrically Lie-irreducible. Now $\mathcal{V}$ and $\mathcal{V}_0$ have the same G_{geom} (again because $\pi_1^{geom}(\mathbb{G}_m)$ maps onto $\pi_1^{geom}(\mathbb{A}^1)$, and G_{geom} is the Zariski closure of the image of the corresponding π_1^{geom}). So it is equivalent to show that $\mathcal{V}_0$ is geometrically Lie-irreducible. Geometrically, $\mathcal{V}_0$ is the pullback by a finite morphism (here $t \mapsto at^4$) of the Kloosterman sheaf $Kl(\psi; \chi_4, \mathbb{1})$, and under finite pullback the group G^0_{geom} does not change. So it is equivalent to show that $Kl(\psi; \chi_4, \mathbb{1})$ is geometrically Lie-irreducible.This sheaf is geometrically irreducible, because its $I(\infty)$-representation, having both slopes $1/2$, is irreducible. Whatever the odd characteristic p, $Kl(\psi; \chi_4, \mathbb{1})$ is not Kummer induced. When $p > 5$, it then results from [Ka-ESDE, 7.2.6 (4)] that $Kl(\psi; \chi_4, \mathbb{1})$ is Lie-irreducible.

We now treat the case $p = 5$ by a separate argument. The group G_{geom} does not change if we make a multiplicative translation of our sheaf, and in particular is independent of the particular choice of ψ, which we may therefore take to be a character of the prime field F_5. The arithmetic determinant formula [Ka-ESDE, 7.4.1.3]

$$\det(Frob_{t,E}|Kl(\psi; \chi_4, \mathbb{1})) = q\chi_{4,E}(-t)$$

shows that $Kl(\psi; \chi_4, \mathbb{1}) \otimes (\sqrt{p})^{-deg}$, which is pure of weight zero, has determinant which is arithmetically of finite order (four). To show that G^0_{geom} is $SL(2)$ (and not the trivial group), it is equivalent to show that G_{geom} is not a finite group. By [Ka-ESDE, 8.14.4], G_{geom} is finite for this sheaf $Kl(\psi; \chi_4, \mathbb{1}) \otimes (\sqrt{p})^{-deg}$ if and only if all its traces are algebraic integers. This is not the case for $p = 5$, already for $Frob_{1,\mathbb{F}_5}$. We see this by computing in the field $\mathbb{Q}_5(\zeta_5)$. If we take 2 as a multiplicative generator of $\mathbb{F}_5^\times$, and denote by $i \in \mathbb{Q}_5$ the fourth root of unity which is its Teichmuller representative, then there is a unique

χ_4 with $\chi_4(2) = i$. [The other choice of χ_4 comes from using 3 as a generator of $\mathbb{F}_5^\times$.] We readily compute

$$Trace(Frob_{1,\mathbb{F}_5}|Kl(\psi;\chi_4,\mathbb{1})) = -\sum_{x\in\mathbb{F}_5^\times}\chi_4(x)\psi(x+1/x) =$$

$$-(1\psi(2)+i\psi(0)+(-i)\psi(0)+(-1)\psi(3)) = -(\zeta_5^2-\zeta_5^3) = -\zeta_5(1-\zeta_5).$$

The quantity $(1-\zeta_5)$ has $ord_5(1-\zeta_5) = 1/4$, so the quantity

$$\mathrm{Trace}(Frob_{1,\mathbb{F}_5}|Kl(\psi;\chi_4,\mathbb{1})\otimes(\sqrt{5})^{-deg}) = -\zeta_5(1-\zeta_5)/\sqrt{5}$$

has $ord_5 = -1/4$, so is not an algebraic integer. This single calculation then shows that in characteristic 5 as well, $Kl(\psi;\chi_4,\mathbb{1})$ has $G^0_{geom} = SL(2)$.

We next show that $G_{geom} = SL(2)$ for $\mathcal{V}$, or equivalently for $\mathcal{V}_0$. The question is geometric, so we may extend scalars to reduce to the case when $q \equiv 1 \bmod 4$. Then the arithmetic determinant formula [Ka-ESDE, 7.4.1.3]

$$\det(Frob_{at^4,E}|Kl(\psi;\chi_4,\mathbb{1})) = q\chi_{4,E}(-at^4) = q\chi_{4,E}(-a)$$

shows that $\mathcal{V}_0 := Kl(\psi;\chi_4,\mathbb{1})\otimes A^{-deg}$ has arithmetically trivial determinant. So **after** such an extension of scalars, we have $G_{arith}\subset SL(2)$. Since in any case we have inclusions

$$SL(2) = G^0_{geom}\subset G_{geom}\subset G_{arith}\subset SL(2),$$

it follows that $G_{geom} = SL(2)$.

It remains to show that $G_{arith} = SL(2)$. If we are over an $\mathbb{F}_q$ with $q \equiv 1 \bmod 4$, the previous paragraph proves this. In the general case, we argue as follows. Because $\mathcal{V}_0$ has real traces and is pure of weight zero, it is (isomorphic to) its own dual. Because it is arithmetically irreducible (because already geometrically irreducible), its autoduality is unique up to a nonzero scalar factor, and is either of sign -1 (:= symplectic) or of sign $+1$ (:= orthogonal). This autoduality gives by restriction a geometric autoduality, again unique up to a nonzero scalar factor, of the **same** sign. But $G_{geom} = SL(2) = Sp(2)$, so the geometric autoduality has sign -1. Therefore the arithmetic autoduality is of sign -1, i.e. symplectic, which is to say that $G_{arith}\subset SL(2)$. So from the inclusions of the previous paragraph, we get $G_{geom} = G_{arith} = SL(2)$. □

In view of Theorem 6.1 and Lemma 6.2, it is natural to ask whether we have the identity $\mathrm{Trace}(Frob_{0,\mathbb{F}_q}|\mathcal{V}) = V(0)$.This is indeed the case, as we show in the next two lemmas.

Lemma 6.4. *If* $q \equiv 1 \bmod 4$, *then* $\mathrm{Trace}(Frob_{0,\mathbb{F}_q}|\mathcal{V}) = V(0)$.

Proof. Suppose that $q \equiv 1 \bmod 4$. Then

$$\mathcal{V}_0 := [t \mapsto at^4]^\star Kl(\psi; \chi_4, \mathbb{1}) \otimes A^{-deg}.$$

One knows [Ka-ClausCar, 2.6.1] that for the sheaf $Kl(\psi; \chi_4, \mathbb{1}) \otimes A^{-deg}$, its space of $I(0)$-invariants is one dimensional, with $Frob_{0,\mathbb{F}_q}$ acting as the scalar $-g(\psi, \chi_4)/A$, the quantity called $W(0)$ in section 3. After we pull back by $t \mapsto at^4$, the space of inertial invariants can only grow. Since we know that this pullback has trivial action of $I(0)$, it follows that of the two eigenvalues of $Frob_{0,\mathbb{F}_q}|\mathcal{V}$, one is $W(0)$. But as $G_{arith} = SL(2)$, we have $\det(Frob_{0,\mathbb{F}_q}|\mathcal{V}) = 1$. Hence the other eigenvalue is $1/W(0)$, so $\mathrm{Trace}(Frob_{0,\mathbb{F}_q}|\mathcal{V}) = W(0) + 1/W(0) := V(0)$. □

When $q \equiv 3 \bmod 4$, we have, by definition, $V(0) = 0$.

Lemma 6.5. *If* $q \equiv 3 \bmod 4$*, then* $\mathrm{Trace}(Frob_{0,\mathbb{F}_q}|\mathcal{V}) = V(0) = 0$.

Proof. Suppose that $q \equiv 3 \bmod 4$. Let the two eigenvalues of $Frob_{0,\mathbb{F}_q}|\mathcal{V}$ be denoted ω and $1/\omega$. [The eigenvalues have this form because $\mathcal{V}$ has $G_{arith} \subset SL(2)$.] We will show that $V(0)^2 = 0$. Now

$$V(0)^2 = 2 + \omega^2 + 1/\omega^2,$$

so we must show that $\omega^2 = -1$. For this, we argue as follows. The quantities ω^2 and $1/\omega^2$ are the eigenvalues of $Frob_{0,\mathbb{F}_{q^2}}|\mathcal{V}$, so they are the quantities

$$W(0) := -\sum_{x \in \mathbb{F}_{q^2}} \chi_4(x)\psi_{\mathbb{F}_q^2}(x)/\chi_8(-1)q$$

and $1/W(0)$. Thus we must show that $W(0) = -1$, i.e., we must show that when $q \equiv 3 \bmod 4$, then for any nontrivial additive character ψ of $\mathbb{F}_q$, and for any quartic character of $\mathbb{F}_{q^2}^\times$, the quartic gauss sum is given by the formula

$$-\sum_{x \in \mathbb{F}_{q^2}} \chi_4(x)\psi_{\mathbb{F}_q^2}(x) = -\chi_8(-1)q.$$

As already noted, for any $a \in \mathbb{F}_q^\times$, we have $\chi_4(a) = 1$. Therefore this sum is independent of the particular choice of nontrivial additive character ψ of $\mathbb{F}_q$. Because of this independence, we write simply

$$-g(\mathbb{F}_{q^2}; \chi_4) := -\sum_{x \in \mathbb{F}_{q^2}} \chi_4(x)\psi_{\mathbb{F}_q^2}(x)$$

for this quartic Gauss sum. It will be convenient to pick some nontrivial additive character $\psi_{\mathbb{F}_p}$ of the prime field, and then take the particular choice

$$\psi := \psi_{\mathbb{F}_p} \circ \mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_p}.$$

There are unique quartic and octic characters $\chi_{4,\mathbb{F}_{p^2}}$ and $\chi_{8,\mathbb{F}_{p^2}}$ of $\mathbb{F}_{p^2}^\times$ whose compositions with the Norm $\mathrm{Norm}_{\mathbb{F}_{q^2}/\mathbb{F}_{p^2}}$ are our characters χ_4 and χ_8 of $\mathbb{F}_{q^2}^\times$.

Because $q \equiv 3 \bmod 4$, $\mathbb{F}_q$ is an odd degree, say degree d, extension of $\mathbb{F}_p$, and $p \equiv 3 \bmod 4$. By Hasse-Davenport, we have the relation

$$-g(\mathbb{F}_{q^2};\chi_4) = (-g(\mathbb{F}_{p^2};\chi_{4,\mathbb{F}_{p^2}}))^d.$$

Because d is odd and $-1 \in \mathbb{F}_p$, $\mathrm{Norm}_{\mathbb{F}_{q^2}/\mathbb{F}_{p^2}}(-1) = (-1)^d = -1$, so we have

$$\chi_8(-1) := \chi_{8,\mathbb{F}_{p^2}}((-1)^d) = (\chi_{8,\mathbb{F}_{p^2}}(-1))^d.$$

So it suffices to prove that

$$-g(\mathbb{F}_{p^2};\chi_{4,\mathbb{F}_{p^2}}) = -\chi_{8,\mathbb{F}_{p^2}}(-1)p,$$

i.e., to prove that (when $p \equiv 3 \bmod 4$) we have

$$g(\mathbb{F}_{p^2};\chi_{4,\mathbb{F}_{p^2}}) = p \text{ if } p \equiv 7 \bmod 8,$$

$$g(\mathbb{F}_{p^2};\chi_{4,\mathbb{F}_{p^2}}) = -p \text{ if } p \equiv 3 \bmod 8.$$

This was proven by Stickelberger in 1890, see [Be-Ev, (10.3)], [Be-Ev-Wi, Thm. 11.6.1] and [Stick, 3.6 and 3.10]. □

We now elaborate and then exploit the $I(\infty)$-structure of $\mathcal{V}$. The question is geometric, so we may assume that $q \equiv 1 \bmod 8$ and that the parameter $a \in \mathbb{F}_q^\times$ is a square, $a = \alpha^2$, for some $\alpha \in \mathbb{F}_q^\times$.

Lemma 6.6. *The $I(\infty)$-representation attached to $[t \mapsto t^2]^\star Kl(\psi_\alpha;\chi_4,\mathbb{1})$ is (the restriction to $I(\infty)$ of the sheaf on the x-line)*

$$\mathcal{L}_{\chi_4(x)} \otimes \mathcal{L}_{\psi(2\alpha x)} \bigoplus \mathcal{L}_{\chi_4(x)} \otimes \mathcal{L}_{\psi(-2\alpha x)}.$$

The $I(\infty)$-representation attached to $\mathcal{V}$ is (the restriction to $I(\infty)$ of the sheaf on the x-line)

$$\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(2\alpha x^2)} \bigoplus \mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(-2\alpha x^2)}.$$

Proof. In terms of the additive character $\psi_\alpha(x) := \psi(\alpha x)$, we have $[t \mapsto at]^\star Kl(\psi;\chi_4,\mathbb{1}) = Kl(\psi_\alpha;\chi_4,\mathbb{1})$. Hence we have a geometric isomorphism

$$\mathcal{V}_0 = [t \mapsto t^4]^\star Kl(\psi_\alpha;\chi_4,\mathbb{1}).$$

If we pick an octic character χ_8 such that $\chi_8^2 = \chi_4$, then we have

$$Kl(\psi_\alpha;\chi_4,\mathbb{1}) \cong \mathcal{L}_{\chi_8(x)} \otimes Kl(\psi_\alpha;\overline{\chi_8},\chi_8).$$

Pulling back by $t \mapsto t^2$, we get

$$[t \mapsto t^2]^\star Kl(\psi_\alpha;\chi_4,\mathbb{1}) \cong \mathcal{L}_{\chi_4(x)} \otimes [t \mapsto t^2]^\star Kl(\psi_\alpha;\overline{\chi_8},\chi_8).$$

One knows [Ka-ClausCar, 2.5, the d=2 case] that the $I(\infty)$-representation of $[t \mapsto t^2]^\star Kl(\psi_\alpha; \overline{\chi_8}, \chi_8)$ is given by

$$\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(2\alpha x)} \bigoplus \mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(-2\alpha x)}.$$

Tensoring with $\mathcal{L}_{\chi_4(x)}$ gives the first assertion.

Geometrically, $\mathcal{V}_0$ is $[t \mapsto t^4]^\star Kl(\psi_\alpha; \chi_4, \mathbb{1})$, so we get the second assertion as the $t \mapsto t^2$ pullback of the first. □

Corollary 6.7. *Let $\mathcal{F}$ be a lisse sheaf of rank two on $\mathbb{A}^1/\overline{\mathbb{F}_q}$ whose $I(\infty)$-representation is isomorphic to (the restriction to $I(\infty)$ of the sheaf on the x-line)*

$$\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(2\alpha x^2)} \bigoplus \mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(-2\alpha x^2)}.$$

Then $\mathcal{F}$ is geometrically irreducible.

Proof. If $\mathcal{F}$ were geometrically reducible, its geometric semisimplication would contain as direct summand a sheaf $\mathcal{N}$ which is lisse of rank one on $\mathbb{A}^1/\overline{\mathbb{F}_q}$ and whose $I(\infty)$-representation is $\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(2\alpha x^2)}$. But no such $\mathcal{N}$ can exist, for by tensoring it with $\mathcal{L}_{\psi(-2\alpha x^2)}$ we would obtain a lisse rank one sheaf on $\mathbb{A}^1/\overline{\mathbb{F}_q}$ whose local monodromy at ∞ is tame but nontrivial (namely $\mathcal{L}_{\chi_2(x)}$). □

Theorem 6.8. *We have the following rigidity results concerning the geometrically irreducible lisse sheaf $\mathcal{V}$ on $\mathbb{A}^1/\mathbb{F}_q$.*

1. *The sheaf $\mathcal{V}$ is cohomologically rigid, i.e. for $j : \mathbb{A}^1 \subset \mathbb{P}^1$ the inclusion,*
$$\chi(\mathbb{P}^1 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, j_\star End(\mathcal{V})) = 2.$$
2. *If $\mathcal{F}$ is a lisse sheaf on $\mathbb{A}^1/\overline{\mathbb{F}_q}$ whose $I(\infty)$-representation is isomorphic to that of $\mathcal{V}$, then $\mathcal{F}$ is geometrically isomorphic to $\mathcal{V}$.*
3. *If $\mathcal{F}$ is a lisse sheaf on $\mathbb{A}^1/\mathbb{F}_q$ with $G_{arith} \subset SL(2)$, whose $I(\infty)$-representation is isomorphic to that of $\mathcal{V}$, then $\mathcal{F}$ is arithmetically isomorphic to either $\mathcal{V}$ or to its constant field twist $\mathcal{V} \otimes (-1)^{deg}$.*

Proof. To prove (1), we use the fact that $\mathcal{V}$ is geometrically self dual to write $End(\mathcal{V}) \cong \mathcal{V} \otimes \mathcal{V}$. Thus $End(\mathcal{V})$ is lisse of rank 4 on $\mathbb{A}^1$, and its $I(\infty)$-representation is given by

$$(\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(2\alpha x^2)} \bigoplus \mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(-2\alpha x^2)})^{\otimes 2} =$$

$$\overline{\mathbb{Q}_\ell} \oplus \overline{\mathbb{Q}_\ell} \oplus \mathcal{L}_{\psi(4\alpha x^2)} \oplus \mathcal{L}_{\psi(-4\alpha x^2)}.$$

Thus $j_\star End(\mathcal{V})$ has a two-dimensional stalk at ∞, and $Swan_\infty(End(\mathcal{V})) = 4$. The Euler-Poincaré formula then gives

$$\chi(\mathbb{P}^1 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, j_\star End(\mathcal{V})) = 2 + \chi(\mathbb{A}^1 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, End(\mathcal{V})) =$$
$$2 + 4 - Swan_\infty(End(\mathcal{V})) = 2.$$

That (1) implies (2) is standard, cf. [Ka-RLS, 5.0.2]. To prove (3), we argue as follows. By (2), $\mathcal{F}$ is geometrically isomorphic to $\mathcal{V}$. As both are geometrically irreducible, $\mathrm{Hom}_{geom}(\mathcal{V}, \mathcal{F})$ is a one-dimensional $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-representation, i.e. it is B^{deg} for some $B \in \overline{\mathbb{Q}_\ell}$, so

$$\mathcal{F} \cong \mathcal{V} \otimes \mathrm{Hom}_{geom}(\mathcal{V}, \mathcal{F}) \cong \mathcal{V} \otimes B^{deg}.$$

Both $\mathcal{F}$ and $\mathcal{V}$ are lisse of rank two with arithmetically trivial determinants, hence $B = \pm 1$.

□

What can we say about the situation in characteristic $p = 3$? It follows from a result of Kubert [Ka-G2Hyper, 13.2 and 13.3 (2)] that in characteristic 3, the sheaf $Kl(\psi; \chi_4, \mathbb{1})$ has finite G_{geom}. [The Kubert result we are using is that if q is a power of a prime p, and if we take all but two of the characters of order dividing $q+1$, then the Kloosterman sheaf of rank $q-1$ formed with those characters has finite G_{geom}. We are applying it with $q = 3$.]

Theorem 6.9. *In characteristic* 3, *the sheaf* $\mathcal{V}$ *is geometrically irreducible, we have*

$$G_{geom} \subset G_{arith} \subset SL(2),$$

and both G_{geom} *and* G_{arith} *are finite primitive irreducible subgroups of* $SL(2)$.

Proof. The geometric irreducibility results from Lemma 6.6 and Corollary 6.7. We know from Kubert that $\mathcal{V}$ has finite G_{geom} (as geometrically it is a pullback of $Kl(\psi; \chi_4, \mathbb{1})$). The arithmetic determinant formula argument in the proof of Theorem 6.3 shows that $G_{geom} \subset SL(2)$. Thus G_{geom} is an irreducible subgroup of $SL(2)$, and hence the larger group G_{arith} is also irreducible. The fact that $\mathcal{V}$ has real traces and is pure of weight zero shows that $\mathcal{V}$ is arithmetically self dual. the irreducibility of G_{arith} shows that this autoduality has a well defined sign. The irreducibility of G_{geom} shows that this sign is the same as that of the induced geometric autoduality of $\mathcal{V}$. This last autoduality must have sign -1. If the sign were $+1$, we would have $G_{geom} \subset O(2)$. But $G_{geom} \subset SL(2)$, so we would get $G_{geom} \subset SO(2)$. But $SO(2)$ is abelian, so G_{geom} would be abelian, which it is not, since it is an irreducible subgroup of $SL(2)$. So $\mathcal{V}$ is symplectically self dual, and hence $G_{arith} \subset SL(2)$. That G_{arith} is finite results from the fact that it lies in $SL(2)$ and normalizes a finite irreducible subgroup (namely G_{geom}) of $SL(2)$. Indeed, for N the order of the automorphism group $Aut(G_{geom})$, every element $\gamma \in G_{arith}$ has γ^N acting trivially on G_{geom} by conjugation, i.e., commuting with the irreducible group G_{geom}, so scalar, so ± 1. Thus G_{arith}, and hence $Lie(G_{arith})$, is killed by $2N$, so $Lie(G_{arith}) = 0$, i.e., G_{arith} is finite.

It remains to explain why both G_{geom} and G_{arith}, finite irreducible subgroups of $SL(2)$, are primitive. It suffices to show that G_{geom} is primitive, for then G_{arith} is "even more" primitive. The group $G_{geom,Kl}$ for $Kl(\psi; \chi_4, \mathbb{1})$ is primitive, because $Kl(\psi; \chi_4, \mathbb{1})$ is geometrically irreducible and not induced (because not Kummer induced, cf. Pink's lemma [Ka-MGF, Lemma 11]). Since geometrically $\mathcal{V}_0$ is the pullback of $Kl(\psi; \chi_4, \mathbb{1})$ by a finite etale galois cover (namely $[t \mapsto t^4]$), it follows that G_{geom} is an irreducible normal subgroup of the primitive irreducible group $G_{geom,Kl}$. But if G_{geom} were imprimitive, there would be a unique pair of lines, say L_1 and L_2, in the two-dimensional representation space, which are either stabilized or interchanged by each element of G_{geom}. By normality, for each $g \in G_{geom,Kl}$, the two lines gL_1 and gL_2 would also be either stabilized or interchanged by each element of G_{geom}. By the unicity of such a pair of lines, we find that $G_{geom,Kl}$ itself is imprimitive. □

To end this section, let us make explicit how Deligne's general equidistribution theorem applies to the sheaf $\mathcal{V}$. Recall that for the group $SU(2)$, the trace map

$$\text{Trace} : SU(2) \to [-2, 2]$$

is an isomorphism of the space $SU(2)^\#$ of conjugacy classes in $SU(2)$ with $[-2, 2]$, an element $x \in [-2, 2]$ representing the conjugacy class of elements $A \in SU(2)$ whose characteristic polynomial is $\det(T - A)$ is $T^2 - xT + 1$. In this picture, the Sato-Tate measure, i.e., the direct image of (total mass one) Haar measure on $SU(2)$ is the measure $(1/2\pi)\sqrt{4 - x^2}dx$ on $[-2, 2]$. If we use the bijection

$$2\cos : [0, \pi] \cong [-2, 2], \quad \theta \in [0, \pi] \mapsto 2\cos(\theta) \in [-2, 2],$$

then we get $[0, \pi]$ as the space of conjugacy classes, with an angle $\theta \in [0, \pi]$ representing the conjugacy class whose eigenvalues are $e^{i\theta}, e^{-i\theta}$. In this picture, the Sato-Tate measure is the measure $(2/\pi)\sin^2\theta d\theta$ on $[0, \pi]$.

Now let us turn to the lisse sheaf $\mathcal{V}$ on $\mathbb{A}^1/\mathbb{F}_q$. Recall that its definition depends on the choice of an element $a \in \mathbb{F}_q^\times$. Given a finite extension $E/\mathbb{F}_q$, and a point $t \in \mathbb{A}^1(E) = E$, we denote by

$$\theta_{a,t,E} \in [0, \pi]$$

the unique angle for which $\mathrm{Trace}(Frob_{t,E}|\mathcal{V}) = 2\cos(\theta_{a,t,E})$.

For each integer $n \geq 1$, $SU(2)$ has exactly one irreducible representation of dimension n, namely $Sym^{n-1}(std_2)$, whose character is the function

$$s_n(\theta) := \sin(n\theta)/\sin(\theta).$$

Here s_1 is the constant function 1. By Peter-Weyl (or by trigonometry), the functions $s_n, n \geq 1$ form an orthonormal basis of the space $L^2([0, \pi], (2/\pi)\sin^2\theta d\theta)$.

Theorem 6.10. *For $\mathbb{F}_q$ of characteristic $p \geq 5$, and $E/\mathbb{F}_q$ a finite extension, with $\#E$ "large", the angles $\{\theta_{a,t,E}\}_{t \in E}$ are approximately equidistributed in $[0, \pi]$ for the Sato-Tate measure $(2/\pi)\sin^2\theta d\theta$ on $[0, \pi]$ in the following sense. For each $n \geq 2$, and each finite extension $E/\mathbb{F}_q$, we have the estimate*

$$|(1/\#E)\sum_{t \in E} s_n(\theta_{a,t,E})| \leq 2n/(\#E)^{1/2}.$$

Proof. For each $n \geq 2$, we form the lisse sheaf $Sym^{n-1}(\mathcal{V})$, which is geometrically irreducible nontrivial, lisse on $\mathbb{A}^1$ of rank n, and pure of weight zero on $\mathbb{A}^1/\mathbb{F}_q$. So the compact cohomology groups

$$H^i_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, Sym^{n-1}(\mathcal{V}))$$

vanish for $i \neq 1$, the H^1_c is mixed of weight ≤ 1, and of dimension $Swan_\infty(, Sym^{n-1}(\mathcal{V}))$. Because $\mathcal{V}$ has both its ∞-slopes 2, $Sym^{n-1}(\mathcal{V})$ has each of its n ∞-slopes ≤ 2, so we have

$$\dim H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, Sym^{n-1}(\mathcal{V})) = Swan_\infty(Sym^{n-1}(\mathcal{V})) \leq 2n.$$

By the Lefschetz trace formula, the sum we are estimating is given by

$$\sum_{t \in E} s_n(\theta_{a,t,E}) = -\mathrm{Trace}(Frob_E|H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, Sym^{n-1}(\mathcal{V}))).$$

The H^1_c here is mixed of weight ≤ 1, and of dimension $\leq 2n$, so the right hand side is bounded in absolute value by $2n(\#E)^{1/2}$. □

Corollary 6.11. *In any sequence of pairs (k_i, a_i) with k_i a finite field of (possibly varying) characteristic ≥ 5 , $a_i \in k_i^\times$ such that the sequence $\#k_i$ tends archimedeanly to ∞, the measures*

$$\mu_i := (1/\#k_i)\sum_{t \in k_i} \delta_{\theta_{a_i,t,k_i}}$$

on $[0,\pi]$ tend weak $\star$ to the Sato-Tate measure: For any continuous function f on $[0,\pi]$,

$$(2/\pi)\int_0^\pi f(\theta)\sin(\theta)^2 d\theta = \lim_{i\to\infty}(1/\#k_i)\sum_{t\in k_i} f(\theta_{a_i,t,k_i}).$$

We have the more precise estimate that for each $n \geq 2$, we have

$$|(1/\#k_i)\sum_{t\in k_i} s_n(\theta_{a_i,t,k_i})| \leq 2n/(\#k_i)^{1/2}.$$

7. Sheaf-theoretic reformulation of the $S(j,j)$

On the open set U of $\mathbb{A}^1$ where $ax - x^3$ is invertible, we have the lisse rank one sheaf $\mathcal{L}_{\chi_2(ax-x^3)}$, which we prefer to write as $\mathcal{L}_{\chi_2(a/x-x)}$. For $j : U \subset \mathbb{A}^1$ the inclusion, we form the sheaf $j_\star\mathcal{L}_{\chi_2(a/x-x)}$. This sheaf has vanishing stalk at 0 and at the two square roots $\pm\alpha$ of a. Its shift $j_\star\mathcal{L}_{\chi_2(a/x-x)}[1]$ is a perverse sheaf on $\mathbb{A}^1$ which is geometrically irreducible. Denoting by ψ_4 the additive character $x \mapsto \psi(4x)$, we form the Fourier Transform

$$\mathcal{T}_0 := FT_{\psi_4}(j_\star\mathcal{L}_{\chi_2(a/x-x)} \otimes (-g(\psi,\chi_2))^{-deg}).$$

This is a single sheaf, indeed $\mathcal{T}_0[1]$ is a perverse sheaf on $\mathbb{A}^1$ which is geometrically irreducible (being the Fourier Transform of such an input). The trace function of $\mathcal{T}_0$ is given as follows: for $E/\mathbb{F}_q$ a finite extension, and $t \in E$,

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{T}_0) = \frac{-\sum_{x\in E^\times}\chi_{2,E}(a/x-x)\psi_E(4tx)}{-g(\psi_E,\chi_{2,E})}.$$

We then define

$$\mathcal{S}_0 := [t \mapsto t^2]^\star\mathcal{T}_0.$$

The following lemma is then a tautology.

Lemma 7.1. *For $E/\mathbb{F}_q$ a finite extension, and $t \in E$,*

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{S}_0) = S(t,t,E).$$

The geometric structure of $\mathcal{T}_0$ is given as follows.

Theorem 7.2. *We have the following results on the sheaf $\mathcal{T}_0$ on $\mathbb{A}^1$.*

(1) *The $I(\infty)$-representation of $\mathcal{T}_0$ is*

$$\mathcal{L}_{\chi_2(t)}\bigoplus\mathcal{L}_{\chi_2(t)}\otimes\mathcal{L}_{\psi(4\alpha t)}\bigoplus\mathcal{L}_{\chi_2(t)}\otimes\mathcal{L}_{\psi}(-4\alpha t).$$

(2) *The sheaf $\mathcal{T}_0$ is lisse of rank three, pure of weight zero, and geometrically irreducible on $\mathbb{G}_m$.*

(3) *The $I(0)$-representation of $\mathcal{T}_0|\mathbb{G}_m$ is*

$$\overline{\mathbb{Q}_\ell} \oplus \overline{\mathbb{Q}_\ell} \oplus \mathcal{L}_{\chi_2(t)}.$$

(4) *For $j_0 : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion, we have an isomorphism $\mathcal{T}_0 \cong j_{0\star}(\mathcal{T}_0|\mathbb{G}_m)$.*

(5) *The sheaf $\mathcal{T}_0|\mathbb{G}_m$ is cohomologically rigid, i.e., for $j : \mathbb{G}_m \subset \mathbb{P}^1$ the inclusion,*

$$\chi(\mathbb{P}^1 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, j_\star End(\mathcal{T}_0)) = 2.$$

(6) *Any lisse rank 3 sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_q}$ whose $I(0)$ and $I(\infty)$-representations are isomorphic to those of $\mathcal{T}_0$ is geometrically isomorphic to $\mathcal{T}_0|\mathbb{G}_m$.*

Proof. Assertion (1) is an instance of Laumon's stationary phase theorem [Ka-ESDE, 7.4.2 and 7.4.4 (2)], in which the input sheaf $j_\star\mathcal{L}_{\chi_2(a/x-x)}$ is tame at ∞ and has three finite singularities $0, \alpha, -\alpha$. At these three points, the stalk vanishes. The local monodromies are $\mathcal{L}\chi_2(x)$, $\mathcal{L}\chi_2(x-\alpha)$, and $\mathcal{L}\chi_2(x+\alpha)$ respectively.

That $\mathcal{T}_0$ has generic rank three is visible from (1). That $\mathcal{T}_0$ is lisse on $\mathbb{G}_m$ holds because the input sheaf $j_\star\mathcal{L}_{\chi_2(a/x-x)}$ is tame at ∞, so in particular has all ∞-slopes < 1, cf. [Ka-ESDE, 7.4.5 (1)]. The purity is equivalent to the statement that as perverse sheaf, $\mathcal{T}_0[1]$ is pure of weight one. This follows from the fact that that the input $j_\star\mathcal{L}_{\chi_2(a/x-x)} \otimes (-g(\psi,\chi_2))^{-deg}[1]$ as perverse sheaf is pure of weight zero, and the fact that Fourier Transform preserves purity, but increases the weight by one.

Assertion (3) results from the fact that the $I(\infty)$-representation of the input sheaf $(j_\star\mathcal{L}_{\chi_2(a/x-x)}$ is $\mathcal{L}_{\chi_2(x)}$, Laumon's results [Ka-ESDE, 7.4.4 (2) and 7.4.3 (1)], and the fact that $\mathcal{T}_0|\mathbb{G}_m$ has rank three. That $\mathcal{T}_0|\mathbb{G}_m$ is geometrically irreducible results from the geometric irreducibility of the (nonpunctual) perverse sheaf $\mathcal{T}_0[1]$ on $\mathbb{A}^1$

Assertion (4) is simply the fact that the input sheaf, shifted by [1], is geometrically perverse irreducible, so it Fourier Transform shifted by [1], namely $\mathcal{T}_0[1]$, is geometrically perverse irreducible; this implies in particular that $\mathcal{T}_0$ is the extension by direct image from any open set on which is it lisse.

The cohomological rigidity of $\mathcal{T}_0|\mathbb{G}_m$ results from $\mathcal{T}_0$'s being, geometrically, the Fourier Transform of a middle extension sheaf of generic rank one (namely $(j_\star\mathcal{L}_{\chi_2(a/x-x)}))$. Such an input is cohomologically rigid (indeed, its $j_\star End$ sheaf is just the constant sheaf $\overline{\mathbb{Q}_\ell}$ on $\mathbb{P}^1 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$), and one knows [Ka-RLS, 3.0.2] that Fourier Transform preserves cohomological rigidity. That (5) implies (6) is again [Ka-RLS, 5.0.2]. □

Theorem 7.3. *We have geometric isomorphisms on $\mathbb{G}_m$*

$$Sym^2([t \mapsto t^2]^\star Kl(\psi_\alpha; \chi_4, \mathbb{1}) \cong \mathcal{T}_0|\mathbb{G}_m$$

and

$$Sym^2(\mathcal{V}_0) \cong \mathcal{S}_0|\mathbb{G}_m.$$

Proof. The $I(0)$-representation of $[t \mapsto t^2]^\star Kl(\psi_\alpha; \chi_4, \mathbb{1})$ is visibly

$$\overline{\mathbb{Q}_\ell} \oplus \mathcal{L}_{\chi_2(x)},$$

and its $I(\infty)$-representation is, by Lemma 6.6,

$$\mathcal{L}_{\chi_4(x)} \otimes \mathcal{L}_{\psi(2\alpha x)} \bigoplus \mathcal{L}_{\chi_4(x)} \otimes \mathcal{L}_{\psi(-2\alpha x)}.$$

The $I(0)$ and $I(\infty)$-representations of $Sym^2([t \mapsto t^2]^\star Kl(\psi_\alpha; \chi_4, \mathbb{1})$ are thus isomorphic to those of $\mathcal{T}_0|\mathbb{G}_m$, thanks to Theorem 7.2, parts (1) and (3). The first result now follows from part (6) of Theorem 7.2. The second result is the $t \mapsto t^2$ pullback of the first. □

We now define a sheaf $\mathcal{S}$ on $\mathbb{A}^1$ which agrees with $\mathcal{S}_0$ on $\mathbb{G}_m$, but which has the "correct" stalk at 0. For $j : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion, we define

$$\mathcal{S} := j_\star j^\star \mathcal{S}_0 = j_\star(\mathcal{S}_0|\mathbb{G}_m).$$

Lemma 7.4. *The sheaf $\mathcal{S}$ on $\mathbb{A}^1$ is lisse of rank 3, pure of weight zero and we have a geometric isomorphism*

$$Sym^2(\mathcal{V}) \cong \mathcal{S}.$$

The sheaf $\mathcal{S}$ on $\mathbb{A}^1$ is geometrically irreducible. If the characteristic $p \geq 5$, its G_{geom} is $SO(3)$. [In characteristic $p = 3$, its G_{geom} is one of the groups A_4, S_4, A_5.]

Proof. By Theorem 7.2, part (3), the $I(0)$-representation of $\mathcal{T}_0|\mathbb{G}_m$ is

$$\overline{\mathbb{Q}_\ell} \oplus \overline{\mathbb{Q}_\ell} \oplus \mathcal{L}_{\chi_2(t)},$$

which becomes trivial after pullback by $t \mapsto t^2$. Hence $\mathcal{S}$ is lisse of rank 3 on $\mathbb{A}^1$. It is pure of weight zero because it is lisse on $\mathbb{A}^1$ and is the middle extension of its (pure of weight zero) restriction to the dense open set $\mathbb{G}_m$. On the dense open set $\mathbb{G}_m$ we have an isomorphism of lisse sheaves

$$Sym^2(\mathcal{V})|\mathbb{G}_m \cong \mathcal{S}|\mathbb{G}_m,$$

by Theorem 7.3. Applying $j_\star$ to this isomorphism gives the asserted isomorphism.

To see the geometric irreducibility, we argue as follows. In characteristic $p \geq 5$, $\mathcal{V}$ has $G_{geom} = SL(2)$, so its $Sym^2(\mathcal{V})$ has $G_{geom} = SO(3)$. In characteristic 3, G_{geom} for $\mathcal{V}$ is, by Theorem 6.9 a primitive irreducible subgroup of $SL(2)$, so by classification its image under Sym^2

is one of the three subgroups A_4, S_4, A_5 of $SO(3)$, each of which is irreducible. □

Theorem 7.5. *In characteristic $p \geq 5$, $\mathcal{S}$ has $G_{geom} = G_{arith} = SO(3)$. In characteristic 3, we have $G_{geom} \subset G_{arith} \subset SO(3)$, with G_{geom} and G_{arith} finite irreducible subgroups of $SO(3)$.*

Proof. The lisse sheaf $\mathcal{S}$ on $\mathbb{A}^1$ and its restriction to $\mathbb{G}_m$ have the same G_{arith} as each other. The sheaf $\mathcal{S}|\mathbb{G}_m$, is lisse of rank 3, pure of weight zero, and has real traces, so is arithmetically isomorphic to its dual. As it is also geometrically irreducible, its autoduality has a sign, which must be $+1$ because we are in odd dimension 3 (we can only have sign -1 in even dimension). Therefore we have an a priori inclusion

$$G_{arith} \subset O(3).$$

So in any characteristic we have inclusions

$$G_{geom} \subset G_{arith} \subset O(3),$$

with G_{geom} a normal subgroup of G_{arith}.

It suffices to prove that $G_{arith} \subset SO(3)$. Indeed, once we have this inclusion, then in characteristic $p \geq 5$, we use the resulting inclusions

$$SO(3) = G_{geom} \subset G_{arith} \subset SO(3).$$

In characteristic 3, we use the fact that G_{arith} normalizes G_{geom}, and the fact that the normalizers of the groups A_4, S_4, A_5 in $SO(3)$ are respectively S_4, S_4, A_5.

We know that $G_{geom} \subset SO(3)$. Therefore $\det(\mathcal{S})$ is a ± 1-valued character which is geometrically constant. In other words, either $\det(\mathcal{S})$ is arithmetically trivial, or it is $(-1)^{deg}$. So to prove that $\det(\mathcal{S})$ is arithmetically trivial, it suffices to exhibit a single $\mathbb{F}_q$-rational point $t \in \mathbb{A}^1(\mathbb{F}_q)$ with

$$\det(Frob_{t,\mathbb{F}_q}|\mathcal{S}) = 1.$$

We will show that this holds at the point $t = 0$. Denote by $j : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion. Denote

$$[2_{\mathbb{G}_m}] := [t \mapsto t^2 \text{ on } \mathbb{G}_m]$$

as endomorphism of $\mathbb{G}_m$, and denote

$$[2_{\mathbb{A}^1}] := [t \mapsto t^2 \text{ on } \mathbb{A}^1]$$

as endomorphism of $\mathbb{A}^1$. We must compute the action of $Frob_{0,\mathbb{F}_q}$ on the stalk at 0 of

$$\mathcal{F} := j_\star j^\star \mathcal{S}_0 = j_\star [2_{\mathbb{G}_m}]^\star j^\star \mathcal{T}_0.$$

Because $[2_{\mathbb{A}^1}]$ is totally ramified over 0, this stalk is the same as the stalk at 0 of

$$[2_{\mathbb{A}^1}]_\star \mathcal{F}.$$

From the commutative diagram

$$\begin{tikzcd}
\mathbb{G}_m \arrow[r, "j"] \arrow[d, "{[2_{\mathbb{G}_m}]}"] & \mathbb{A}^1 \arrow[d, "{[2_{\mathbb{A}^1}]}"] \\
\mathbb{G}_m \arrow[r, "j"] & \mathbb{A}^1
\end{tikzcd}$$

we see that

$$[2_{\mathbb{A}^1}]_\star \mathcal{F} := [2_{\mathbb{A}^1}]_\star j_\star [2_{\mathbb{G}_m}]^\star j^\star \mathcal{T}_0 = j_\star [2_{\mathbb{G}_m}]_\star [2_{\mathbb{G}_m}]^\star j^\star \mathcal{T}_0.$$

By the projection formula,

$$[2_{\mathbb{G}_m}]_\star [2_{\mathbb{G}_m}]^\star j^\star \mathcal{T}_0 = j^\star \mathcal{T}_0 \otimes [2_{\mathbb{G}_m}]_\star \overline{\mathbb{Q}_\ell}.$$

But

$$[2_{\mathbb{G}_m}]_\star \overline{\mathbb{Q}_\ell} = \overline{\mathbb{Q}_\ell} \oplus \mathcal{L}_{\chi_2(x)},$$

so

$$[2_{\mathbb{A}^1}]_\star \mathcal{F} = j_\star(j^\star \mathcal{T}_0 \oplus j^\star(\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)})) = j_\star j^\star \mathcal{T}_0 \oplus j_\star j^\star(\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)}).$$

We have already noted, in Theorem 7.2, (4), that $j_\star j^\star \mathcal{T}_0 = \mathcal{T}_0$. To compute $j_\star j^\star(\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)})$, we argue as follows. From the known $I(0)$-representation of $\mathcal{T}_0$, we see that $\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)}$ has a one-dimensional space of $I(0)$-invariants at 0, i.e., $j_\star j^\star(\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)})$ has a one-dimensional stalk at 0. So any sheaf $\mathcal{G}$ on $\mathbb{A}^1$ which agrees with $\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)}$ on $\mathbb{G}_m$, geometrically has no nonzero punctual sections, and has a nonzero stalk at 0 must be $j_\star j^\star(\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)})$.

Let us first explain the character sum calculation which motivates the construction of such a sheaf $\mathcal{G}$. For $t \neq 0$ in $\mathbb{F}_q$, we have

$$\mathrm{Trace}(Frob_{t,\mathbb{F}_q} | \mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)}) = \frac{-\chi_2(t) \sum_{x \in \mathbb{F}_q^\times} \chi_2(a/x - x)\psi(4tx)}{-g(\psi, \chi_2)}.$$

We rewrite this sum as

$$\frac{-\sum_{x \in \mathbb{F}_q^\times} \chi_2(at/x - tx)\psi(4tx)}{-g(\psi, \chi_2)},$$

then sum over x/t to get

$$\frac{-\sum_{x \in \mathbb{F}_q^\times} \chi_2(at^2/x - x)\psi(4x)}{-g(\psi, \chi_2)},$$

To obtain these sums geometrically, we consider the second projection $pr_2 : \mathbb{G}_m \times \mathbb{A}^1 \to \mathbb{A}^1$, and endow the source, with coordinates (x, t), with the sheaf

$$\mathcal{H} := \mathcal{L}_{\chi_2(at^2/x-x)} \otimes \mathcal{L}_{\psi(4x)} \otimes (-g(\psi, \chi_2))^{-deg}.$$

Then $\mathcal{H}[2]$ on the source is perverse, and hence

$$\mathcal{G} := R^1 pr_{2!}\mathcal{H}$$

is a "sheaf of perverse origin" on $\mathbb{A}^1$, and hence has no nonzero punctual sections, cf. [Ka-SC, Cor. 5]. The $R^i pr_{2!}\mathcal{H}$ vanish for $i \neq 1$, so the trace function of $\mathcal{G}$ on $\mathbb{G}_m$ is exactly that of $\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)}$, and at $t = 0$ is given by the formula

$$\mathrm{Trace}(Frob_{0,\mathbb{F}_q}|\mathcal{G}) = \frac{-\sum_{x\in\mathbb{F}_q^\times} \chi_2(-x)\psi(4x)}{-g(\psi, \chi_2)} = \chi_2(-1).$$

This shows that on the one-dimensional stalk at 0 of $j_\star j^\star(\mathcal{T}_0 \otimes \mathcal{L}_{\chi_2(x)})$,$Frob_{0,\mathbb{F}_q}$ acts as multiplication by $\chi_2(-1)$.

Now let us consider in greater detail the action of $Frob_{0,\mathbb{F}_q}$ on the two-dimensional stalk at 0 of $\mathcal{T}_0$. Here we have, for any finite extension $E/\mathbb{F}_q$,

$$\mathrm{Trace}(Frob_{0,E}|\mathcal{T}_0) = \frac{-\sum_{x\in E^\times} \chi_{2,E}(a/x - x)}{-g(\psi_E, \chi_{2,E})}.$$

The numerator is the trace of $Frob_E$ on the H^1 of the elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$ of equation

$$y^2 = ax - x^3.$$

In other words, the two-dimensional stalk of $\mathcal{T}_0$ at 0, as $Frob_{0,\mathbb{F}_q}$-module, is

$$H^1(\mathcal{E} \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{\mathbb{Q}_\ell}) \otimes (-g(\psi, \chi_2))^{-deg}$$

as $Frob_{\mathbb{F}_q}$-module.

Thus the stalk at 0 of $\mathcal{S}$ is the direct sum

$$(\chi_2(-1))^{deg} \oplus H^1(\mathcal{E} \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \overline{\mathbb{Q}_\ell}) \otimes (-g(\psi, \chi_2))^{-deg}.$$

So the determinant of $Frob_{0,\mathbb{F}_q}$ on this stalk is the product its determinants on each of the two summands. On the first summand, the determinant is $\chi_2(-1)$. On the second summand, the determinant is $q/(-g(\psi, \chi_2))^2 = q/(\chi_2(-1)q) = \chi_2(-1)$. Thus we find $\det(Frob_{0,\mathbb{F}_q}, \mathcal{S}) = 1$. □

Making use of the above calculation of the stalk at 0 of $\mathcal{S}$, we get the following variant of Lemma 7.1.

Lemma 7.6. *For $E/\mathbb{F}_q$ a finite extension, and $t \in E^\times$,*

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{S}) = S(t,t,E).$$

For $t = 0$, we have

$$\mathrm{Trace}(Frob_{0,E}|\mathcal{S}) = \chi_{2,E}(-1) + S(0,0,E).$$

Theorem 7.7. *We have an arithmetic isomorphism of lisse sheaves on $\mathbb{A}^1$*

$$Sym^2\mathcal{V} \cong \mathcal{S}.$$

Proof. We have already proven in Lemma 7.4 that $Sym^2\mathcal{V}$ and $\mathcal{S}$ are geometrically isomorphic and that $\mathcal{S}$, and hence $Sym^2\mathcal{V}$ as well, are geometrically irreducible. Therefore arithmetically one is a constant field twist of the other, so we have an arithmetic isomorphism $Sym^2\mathcal{V} \cong \mathcal{S} \otimes \beta^{deg}$ for some $\beta \in \overline{\mathbb{Q}_\ell}^\times$. We have shown in Theorem 7.5 that $\mathcal{S}$ has its $G_{arith,\mathcal{S}} \subset SO(3)$. By Theorems 6.3 and 6.9, we know that $\mathcal{V}$ has its $G_{arith,\mathcal{V}} \subset SL(2)$, and hence $Sym^2\mathcal{V}$ has its $G_{arith,Sym^2\mathcal{V}} \subset SO(3)$. Thus both $Sym^2\mathcal{V}$ and $\mathcal{S}$ have their groups $G_{arith} \subset SO(3)$. Therefore the scalar β lies in $SO(3)$. But the only scalar in $SO(3)$ is 1, hence $\beta = 1$. □

We can now relate $\mathcal{V}$ to the sums $P(t,t,E)$.

Corollary 7.8. *For $E/\mathbb{F}_q$ a finite extension, and $t \in E$, we have the identities*

$$(\mathrm{Trace}(Frob_{t,E}|\mathcal{V}))^2 = 1 + \mathrm{Trace}(Frob_{t,E}|\mathcal{S}) = P(t,t,E).$$

Proof. We have the tautological identity

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{V}^{\otimes 2}) = (\mathrm{Trace}(Frob_{t,E}|\mathcal{V}))^2.$$

Because $\mathcal{V}$ has its $G_{arith,\mathcal{V}} \subset SL(2)$, we have the decomposition

$$\mathcal{V}^{\otimes 2} = Sym^2\mathcal{V} \oplus \Lambda^2\mathcal{V} \cong Sym^2\mathcal{V} \oplus \overline{\mathbb{Q}_\ell}.$$

This proves the first identity. The second results from Lemma 7.6 and the definition of the sums $P(t,t,E)$. □

For the sums $V(t,E)$, we have the following result.

Corollary 7.9. *For $E/\mathbb{F}_q$ a finite extension, and $t \in E$, we have the identity*

$$V(t,E)^2 = P(t,t,E).$$

Proof. Immediate from the previous result, Theorem 6.1 and Lemmas 6.4 and 6.5. □

Here is a slight variant.

Corollary 7.10. *For $E/\mathbb{F}_q$ a finite extension, and $t \in E$, we have the identity*

$$V(t, E)V(-t, E) = P(t, -t, E).$$

Proof. Immediate from the previous result, the fact that $V(-t, E) = \chi_{2,E}(-1)V(-t, E)$ (Lemmas 3.1 and 4.1), and the fact that $P(t, -t, E) = \chi_{2,E}(-1)P(t, t, E)$. □

8. The projection property of the $P(j, k)$, following Evans

In this section, we give a proof, due to Evans, of a result we learned from Wootters [A-S-S-W].

Theorem 8.1. *The $q \times q$ matrix $P := P(j, k)_{j,k\in\mathbb{F}_q}$ satisfies the identities*

$$\mathrm{Trace}(P) = q - \chi_2(a),$$
$$P^2 = (q - \chi_2(a))P.$$

Proof. We first prove the trace identity. By definition,

$$\mathrm{Trace}(P) = P(0, 0)+\sum_{t\in\mathbb{F}_q^\times}(1+S(t, t)) = 1+\chi_2(-1)+\sum_{t\in\mathbb{F}_q} S(t, t)+q-1 =$$

$$q + \chi_2(-1) + (1/g(\psi, \chi_2)) \sum_{uv=a} \chi_2(u - v) \sum_{t\in\mathbb{F}_q} \psi(4t^2v).$$

In the innermost sum, v is nonzero (since $uv = a$), so this innermost sum is

$$\sum_{t\in\mathbb{F}_q} \psi(4t^2v) = \chi_2(v)g(\psi, \chi_2),$$

hence

$$\mathrm{Trace}(P) = q+\chi_2(-1)+\sum_{uv=a} \chi_2(u-v)\chi_2(v) = q+\chi_2(-1)+\sum_{v\in\mathbb{F}_q^\times} \chi_2(a-v^2).$$

But we have the identity

$$\chi_2(a) + \chi_2(-1) + \sum_{v\in\mathbb{F}_q^\times} \chi_2(a - v^2) = 0,$$

because this expression is minus the trace of $Frob_{\mathbb{F}_q}$ on H^1 of the complete nonsingular model of the curve $y^2 = a - v^2$, and this H^1 vanishes.This last identity gives the asserted value for Trace(P).

We now turn to the second identity. We must show that for every $j, k \in \mathbb{F}_q$, we have

$$\sum_{t\in\mathbb{F}_q} P(j, t)P(t, k) = (q - \chi_2(a))P(j, k).$$

For brevity, we will now write $\sum_t$ for $\sum_{t\in\mathbb{F}_q}$, and we will abbreviate

$$g := g(\psi, \chi_2).$$

Writing each

$$P(j,k) := \delta_{j,k} + \chi_2(-1)\delta_{j,-k} + S(j,k)$$

and expanding, we get

$$\sum_t P(j,t)P(t,k) = sum_1 + sum_2 + sum_3 + sum_4,$$

with

$$sum_1 = \sum_t (\delta_{j,t} + \chi_2(-1)\delta_{j,-t})(\delta_{t,k} + \chi_2(-1)\delta_{t,-k}),$$

$$sum_2 = \sum_t (\delta_{j,t} + \chi_2(-1)\delta_{j,-t})S(t,k),$$

$$sum_3 = \sum_t (\delta_{t,k} + \chi_2(-1)\delta_{t,-k})S(j,t),$$

$$sum_4 = \sum_t S(j,t)S(t,k).$$

We have

$$sum_1 = \begin{cases} 0 & \text{if } j^2 \neq k^2, \\ (1+\chi_2(-1))^2 & \text{if } j = k = 0, \\ 2 & \text{if } j = k \neq 0, \\ 2\chi_2(-1) & \text{if } j = -k \neq 0. \end{cases}$$

We have

$$sum_2 + sum_3 =$$

$$S(j,k) + \chi_2(-1)S(-j,k) + S(j,k) + \chi_2(-1)S(j,-k) = 4S(j,k).$$

So the real work comes in evaluating $sum_4 := \sum_t S(j,t)S(t,k)$. We write

$$sum_4 = (1/g^2) \sum_{uv=a,xy=a} \chi_2((u-v)(x-y))\times$$

$$\sum_t \psi((j+t)^2 v + (j-t)^2 u + (k+t)^2 y + (k-t)^2 x) =$$

$$(1/g^2) \sum_{uv=a,xy=a} \chi_2((u-v)(x-y)\psi(j^2(v+u) + k^2(y+x))\times$$

$$\sum_t \psi(t^2(u+v+x+y) + 2t(j(v-u) + k(y-x))).$$

If $u + v + x + y = 0$, the innermost sum is $q\delta_{0,j(v-u)+k(y-x)}$. If $u+v+x+y \neq 0$, the innnermost sum is (complete the square)

$$\chi_2(u+v+x+y)g\psi(\frac{-(j(v-u)+k(y-x))^2}{u+v+x+y}).$$

Following closely Evans, we denote by $\mathbb{A}$ the sum of those terms in the entire sum with $u+v+x+y=0$, and by $\mathbb{B}$ the sum of those terms in the entire sum with $u+v+x+y \neq 0$.

To analyze $\mathbb{A}$, we argue as follows. Since $uv = xy = (-x)(-y)$ (all are a), and $u+v = (-x)+(-y)$, we conclude (symmetric functions) that the unordered sets $\{u,v\}$ and $\{-x,-y\}$ coincide. If in addition $u = v$, the factor $u-v$ inside the χ_2 kills this term. For each pair u,v with $uv = a, u \neq v$, there are two pairs, $(x,y) = (-u,-v)$ and $(x,y) = (-v,-u)$, with $u+v+x+y = 0$.

Still with the $\mathbb{A}$ sum, suppose first $j = k = 0$. Then every innermost sum is q, and for each pair u,v with $uv = a, u \neq v$, the outer sum has a term which $\chi_2((u-v)^2)$ (from taking $(x,y) = (-v,-u)$) and a term $\chi_2(-(u-v)^2)$ (from taking $(x,y) = (-u,-v)$). The number of pairs $uv = a, u \neq v$ is the number of $u \in \mathbb{F}_q^\times$ with $u^2 \neq a$, so there are $q-1-(1+\chi_2(a)) = q-2-\chi_2(a)$ terms. So we have

$$\mathbb{A} = (1/g^2)q(q-2-\chi_2(a))(1+\chi_2(-1)) = \chi_2(-1)(q-2-\chi_2(a))(1+\chi_2(-1)) =$$
$$(q-2-\chi_2(a))(1+\chi_2(-1)) \text{ if } j=k=0.$$

We now analyze the $\mathbb{A}$ term when $j^2 \neq k^2$ (and hence at least one of j,k is nonzero). In these cases, the innermost sum, $q\delta_{0,j(v-u)+k(y-x)}$, vanishes (because $y-x = \pm(v-u)$ in each $\mathbb{A}$ summand, and again only terms with $u \neq v$ contribute). Thus

$$\mathbb{A} = 0 \text{ if } j^2 \neq k^2.$$

We now analyze the $\mathbb{A}$ term when $j = k \neq 0$. Here for each pair u,v with $uv = a, u \neq v$, there is just one pair, $(x,y) = (-u,-v)$ for which the innermost sum, $q\delta_{0,j(v-u)+k(y-x)}$, is nonzero. But for these terms, $\chi_2((u-v)(y-x)) = \chi_2(-(u-v)^2) = \chi_2(-1)$, so we get

$$\mathbb{A} = q-2-\chi_2(a) \text{ if } j = k \neq 0.$$

In a similar fashion, we find

$$\mathbb{A} = \chi_2(-1)(q-2-\chi_2(a)) \text{ if } j = -k \neq 0.$$

We now turn to the analysis of the $\mathbb{B}$ sum. We will prove below that

$$\mathbb{B} = (q-4-\chi_2(a))S(j,k).$$

If we admit this, then we get the required assertion. In all cases,

$$sum_2 + sum_3 + \mathbb{B} = (q-\chi_2(a))S(j,k).$$

Suppose first $j^2 \neq k^2$. Then $sum_1 = 0$, $\mathbb{A} = 0$, and $P(j,k) := S(j,k)$, so we are done.

If $j = k = 0$, then $sum_1 = (1+\chi_2(-1))^2 = 2((1+\chi_2(-1))$, and $\mathbb{A} = (q-2-\chi_2(a))(1+\chi_2(-1))$. In this case $P(0,0) := 1|\chi_2(-1)+S(0,0)$, so again we are done.

If $j = k \neq 0$, then $sum_1 = 2$ and $\mathbb{A} = q-2-\chi_2(a)$. In this case $P(j,j) := 1+S(j,j)$, so we are done.

If $j = -k \neq 0$, then $sum_1 = 2\chi_2(-1)$ and $\mathbb{A} = \chi_2(-1)(q-2-\chi_2(a))$. In this case $P(j,j) := \chi_2(-1)+S(j,j)$, so we are done. □

To finish the proof of Theorem 8.1, it remains to prove the following.

Lemma 8.2. *We have*

$$\mathbb{B} = (q-4-\chi_2(a))S(j,k).$$

Proof. Recall that $\mathbb{B}$ is given by

$$(1/g^2) \sum_{uv=a,xy=a,u\neq v,x\neq y,u+v+x+y\neq 0} \chi_2((u-v)(x-y)\psi(j^2(v+u)+k^2(y+x))\times$$

$$\chi_2(u+v+x+y)g\psi(\frac{-(j(v-u)+k(y-x))^2}{u+v+x+y})$$

$$= (1/g) \sum_{uv=a,xy=a,u\neq v,x\neq y,u+v+x+y\neq 0} \chi_2((u-v)(x-y)(u+v+x+y))\times$$

$$\psi(j^2(v+u)+k^2(y+x)-\frac{(j(v-u)+k(y-x))^2}{u+v+x+y}).$$

To see some structure in the argument of χ_2, we need two identities. The first is

$$vy(u+v+x+y) = ay+v^2y+av+y^2v = a(y+v)+vy(y+v) = (a+vy)(y+v).$$

The second, using the first, is

$$(yv)^2(u-v)(x-y)(u+v+x+y) = (a-v^2)(a-y^2)(a+vy)(y+v) =$$

$$(a^2-av^2-ay^2+y^2v^2)(a+vy)(y+v) =$$

$$((a+vy)^2-a(y+v)^2)(a+vy)(y+v).$$

In the χ_2 argument, we may multiply by the invertible square $(vy)^2$ and divide by the invertible square $(a+vy)^2(y+v)^2$, so $\mathbb{B}$ is

$$(1/g) \sum_{uv=a,xy=a,u\neq v,x\neq y,u+v+x+y\neq 0} \chi_2(\frac{a+vy}{v+y} - \frac{a(y+v)}{a+vy})\times$$

$$\psi(j^2(v+u)+k^2(y+x)-\frac{(j(v-u)+k(y-x))^2}{u+v+x+y}).$$

The argument of ψ is of the form

$$j^2C + k^2D - 2jkE,$$

with

$$C = \frac{(v+u)(u+v+x+y) - (u-v)^2}{u+v+x+y},$$
$$D = \frac{(y+x)(u+v+x+y) - (y-x)^2}{u+v+x+y},$$
$$E = \frac{(v-u)(y-x)}{u+v+x+y}.$$

We first observe that

$$C = D.$$

Indeed, the numerator of C is

$$(v+u)(u+v+x+y) - (u-v)^2 = (u+v)^2 - (u-v)^2 + (u+v)(x+y) = 4a + (u+v)(x+y),$$

which is also the numerator of D. Thus the argument of ψ is

$$j^2C + k^2C - 2jkE = (j+k)^2((C-E)/2) + (j-k)^2((C+E)/2).$$

We have

$$(C-E)/2 = \frac{4a + (u+v)(x+y) - (v-u)(y-x)}{2(u+v+x+y)} =$$
$$= \frac{(yv)(4a + (u+v)(x+y) - (v-u)(y-x))}{2(a+vy)(y+v)} =$$
$$= \frac{4ayv + (a+v^2)(a+y^2) - (v^2-a)(y^2-a)}{2(a+vy)(y+v)} =$$
$$= \frac{4ayv + 2ay^2 + 2av^2}{2(a+vy)(y+v)} = \frac{a(v+y)^2}{(a+vy)(y+v)} = \frac{a(v+y)}{a+vy}.$$

In a completely similar fashion, we get

$$(C+E)/2 = \frac{a+vy}{v+y}.$$

Putting this all together, we find

$$\mathbb{B} = (1/g) \sum_{uv=a, xy=a, u\neq v, x\neq y, u+v+x+y\neq 0} \chi_2((\frac{a+vy}{v+y}) - (\frac{a(y+v)}{a+vy}))\times$$
$$\psi((j+k)^2(\frac{a(v+y)}{a+vy}) + (j-k)^2(\frac{a+vy}{v+y})).$$

So if we put

$$X := \frac{a(v+y)}{a+vy},$$

then we have

$$\mathbb{B} = (1/g) \sum_{X \in \mathbb{F}_q^\times, X \neq a/X} \chi_2(a/X - X)\psi((j+k)^2X + (j-k)^2(a/X))Mult(X),$$

where $Mult(X)$ is the number of inputs $uv = a, xy = a, u \neq v, x \neq y, u + v + x + y \neq 0$ for which

$$X = \frac{a(v+y)}{a+vy}.$$

So our remaining task is to show that for any $X \in \mathbb{F}_q^\times$ with $X \neq a/X$, we have

$$Mult(X) = q - 4 - \chi_2(a).$$

In view of the identity

$$vy(u + v + x + y) = (a + vy)(y + v),$$

$Mult(X)$ is the number of pairs (v, y) in ${\mathbb{F}_q}^2$ with $vy(v+y)(a+vy)(a-v^2)(a-y^2)$ invertible and

$$X = \frac{a(v+y)}{a+vy}.$$

If we fix a choice of y with $a - y^2$ invertible, then

$$v \mapsto \frac{a(v+y)}{a+vy}$$

is a fractional linear transformation, say L_y, given by the 2 by 2 matrix $((a, ay), (y, a))$. This matrix is invertible, because $a - y^2$ is invertible. Then there is a unique $v \in \mathbb{P}^1(\mathbb{F}_q)$ with $L_y(v) = X$, given by

$$v = \frac{a(X-y)}{a-Xy}.$$

Thus v lies in $\mathbb{F}_q^\times$ provided that $y \neq X$ and $y \neq a/X$. So for each y with $y(a-y^2)(y-X)(y-a/X)$ invertible, $v = \frac{a(X-y)}{a-Xy}$ is invertible and $X = \frac{a(v+y)}{a+vy}$. We claim that this v is such that $vy(v+y)(a+vy)(a-v^2)(a-y^2)$ is invertible. Indeed, we have

$$v + y = \frac{a(X-y)}{a-Xy} + y = \frac{a(X-y) + y(a-Xy)}{a-Xy} = \frac{X(a-y^2)}{a-Xy},$$

so $v+y$ is invertible. Once $v+y$ is invertible, the fact that $X = \frac{a(v+y)}{a+vy}$ is invertible shows that $a + vy$ is invertible. That $v^2 \neq a$, or equivalently that $v \neq a/v$, or equivalently that

$$\frac{a(X-y)}{a-Xy} \neq \frac{a-Xy}{X-y},$$

amounts to

$$a(X-y)^2 \neq (a-Xy)^2,$$

i.e.

$$(a-y^2)(X^2-a) \neq 0,$$

which is indeed the case.

On the other hand, if $y^2 = a$, then

$$X = \frac{a(v+y)}{a+vy} = \frac{y^2(v+y)}{y^2+vy} = y.$$

But $X^2 \neq a$, so no such y contributes to $Mult(X)$.

So for each invertible X with $X \neq a/X$, we may take $y \in \mathbb{F}_q$ other than $0, X, a/X$ or any root of $y^2 = a$. If there are roots of $y^2 = a$ in $\mathbb{F}_q$, none of them is X or a/X, exactly because $X^2 \neq a$. So the number of y which contribute to $Mult(X)$, each exactly once, is

$$q-3-(1+\chi(2)(a)) = q-4-\chi_2(a),$$

as required. □

As explained in the first section, Theorem 8.1, together with the fact that the matrix P is real and symmetric, shows that there is a (unique up to a ±1 factor) vector

$$V := (V_j)_{j\in\mathbb{F}_q} \in \mathbb{R}^q$$

such that we have the identities

$$P(j,k) = V_j V_k.$$

In particular, we have the identities

$$P(j,k)^2 = P(j,j)P(k,k).$$

In view of Corollary 7.9, it follows that

$$P(j,k)^2 = V(j)^2 V(k)^2,$$

and hence we have

$$P(j,k) = \pm V(j)V(k).$$

Repeating these considerations over a finite extension $E/\mathbb{F}_q$, we find

Corollary 8.3. *For $E/\mathbb{F}_q$ a finite extension, and $s,t \in E$, we have*

$$P(s,t,E) = \pm V(s,E)V(t,E).$$

9. Interlude:The ± Trace problem

In this section, we work over $\mathbb{C}$. We are given a group Γ, a finite dimensional $\mathbb{C}$-vector space V with $dim(V) \geq 2$, and two irreducible $\mathbb{C}$-representations of Γ,

$$\rho_1,\ \rho_2 : \Gamma \to GL(V).$$

We are told that for every $\gamma \in \Gamma$, we have

$$\mathrm{Trace}(\rho_1(\gamma))^2 = \mathrm{Trace}(\rho_2(\gamma))^2.$$

When is it then true that there exists a character $\chi \in \mathrm{Hom}(\Gamma, \pm 1)$ such that $\rho_2 = \chi \otimes \rho_1$?

Let us consider the following slightly more general problem. Suppose we are given a nonzero polynomial $F(X, Y) \in \mathbb{C}[X, Y]$ and we are told that for every $\gamma \in \Gamma$,

$$F(\mathrm{Trace}(\rho_1(\gamma)), \mathrm{Trace}(\rho_2(\gamma))) = 0.$$

How can this happen, and will it have a representation-theoretic explanation? Here is an answer, in a special case.

Theorem 9.1. *In the above situation, define, for $i = 1, 2$,*

$$G_i := \text{the Zariski closure of } \rho_i(\Gamma) \text{ in } GL(V).$$

Suppose that G_1 and G_2 are conjugate in $GL(V)$, i.e., for some $A \in GL(V)$ we have $G_2 = AG_1A^{-1}$. Suppose further G_1 is a connected semisimple group, and that

$$Lie(\rho_1) : Lie(G_1) \to End(V)$$

is the unique irreducible representation of $Lie(G_1)$ of dimension $dim(V)$. Then there is a divisor $d \geq 1$ of the order f of the center $Z(G_1)$ such that

1. *There is a unique character $\chi \in \mathrm{Hom}(\Gamma, \mu_d)$ such that $\rho_2 = \chi \otimes \rho_1$.*
2. *The polynomial $F(X, Y)$ is divisible by the polynomial $X^d - Y^d$.*

Proof. View each ρ_i as a homomorphism from Γ to G_i, and define

$$H := \text{the Zariski closure of } (\rho_1 \times \rho_2)(\Gamma) \text{ in } G_1 \times G_2.$$

Then H is a closed subgroup of $G_1 \times G_2$ which projects onto both factors (by the Zariski density of Γ in all three of H, G_1, G_2). By (the algebraic group version of) Goursat's lemma, there exist closed normal subgroups $N_1 \subset G_1$ and $N_2 \subset G_2$ and an isomorphism

$$\phi : G_1/N_1 \cong G_2/N_2$$

such that

$$H = \{(g_1, g_2) \in G_1 \times G_2 \mid \phi(g_1 \bmod N_1) = g_2 \bmod N_2\}.$$

By the Zariski density of Γ in H, we have

$$F(\mathrm{Trace}(g_1|V), \mathrm{Trace}(g_2|V)) = 0, \text{ for all } (g_1, g_2) \in H.$$

The key observation at this point is that we have an inclusion

$$N_1 \times N_2 \subset H.$$

Using this, we first show that N_1 and N_2 are both finite. Indeed, the existence of the isomorphism $\phi : G_1/N_1 \cong G_2/N_2$, together with the fact that G_1 and G_2 are themselves isomorphic, shows that N_1 and N_2 have the same dimension as each other. Each G_i is reductive (because it has a faithful completely reducible representation), hence its normal subgroup N_i is also reductive. So if the N_i have strictly positive dimension, each of them contains a one-dimensional torus, say $T_i \subset N_i$. Then we have

$$T_1 \times T_2 \subset H.$$

Now V is a faithful representation of both the T_i, so if we view each T_i as $\mathbb{G}_m$, say $T_1 = Spec(\mathbb{C}[X, 1/X])$, $T_2 = Spec(\mathbb{C}[Y, 1/Y])$, then $\mathrm{Trace}(t_1(X)|V)$ is a nonconstant Laurent polynomial $f(X) \in \mathbb{C}[X, 1/X])$, and $\mathrm{Trace}(t_1(Y)|V)$ is a nonconstant Laurent polynomial $g(Y) \in \mathbb{C}[Y, 1/Y])$. But $T_1 \times T_2 \subset H$, so we find that $F(f(X), g(Y)) = 0$. As $f(X), g(Y)$ are nonconstant polynomials in X and Y respectively, they are algebraically independent over $\mathbb{C}$, hence F is the zero polynomial, contradiction.

So now we know that N_1 and N_2 are finite normal subgroups of G_1 and G_2 respectively. But the only finite normal subgroups of a connnected semisimple group are the subgroups of its center. Moreover, since each G_i is an irreducible subgroup of $GL(V)$, its center is a (finite, because G_i is semisimple) group of scalars, so the group μ_{f_i} of f_i'th roots of unity for some $f_i \geq 1$. But G_1 and G_2 are isomorphic, so $f_1 = f_2$, let us call it f. So $N_1 = \mu_{d_1}$ for some divisor d_1 of f, and $N_2 = \mu_{d_2}$ for some divisor d_2 of f. We next claim that $d_1 = d_2$. One way to see this is to pass from the isomorphism

$$\phi : G_1/N_1 \cong G_2/N_2$$

to the induced isomorphism of the universal covering groups

$$\tilde{\phi} : \tilde{G}_1 \cong \tilde{G}_2.$$

Now we make use of our assumption that

$$Lie(\rho_1) : Lie(G_1) \to End(V)$$

is the unique irreducible representation of $Lie(G_1)$ of dimension $dim(V)$, in the equivalent form that the composite homomorphism $\tilde{G_1} \to G_1 \subset GL(V)$ is the unique irreducible representation of $\tilde{G_1}$ of dimension $dim(V)$. In particular, this representation is equivalent to the composition

$$\tilde{G_1} \overset{\tilde{\phi}}{\to} \tilde{G_2} \to G_2 \subset GL(V).$$

Then $\tilde{\phi}$ must map the kernel of this representation to itself, i.e., it must map the fundamental group of G_1 to the fundamental group of G_2. Thus $\tilde{\phi}$ induces an isomorphism ϕ_G of G_1 to G_2, which maps N_1 isomorphically to N_2. Now we use the uniqueness to say that our isomorphism of G_1 to G_2 must be conjugation by some element B of the ambient $GL(V)$. Thus

$$H = \{(g_1, g_2) \in G_1 \times G_2 \mid \exists \zeta \in \mu_d \text{ with } g_2 = Bg_1B^{-1}\zeta\}.$$

As $\mathrm{Trace}(Bg_1B^{-1}\zeta|V) = \zeta\mathrm{Trace}(g_1|V)$, we find that

$$F(\mathrm{Trace}(g_1|V), \zeta\mathrm{Trace}(g_1|V)) = 0 \ \ \forall g_1 \subset G_1, \forall \zeta \in \mu_d.$$

Restricting to g_1 running over some one-dimensional torus T_1 of G_1, with character $f(X)$ a nonconstant Laurent polynomial, we get the polynomial relation

$$F(f(X), \zeta f(X)) = 0 \ \forall \zeta \in \mu_d,$$

hence the polynomial relation $F(X, \zeta X) = 0 \ \forall \zeta \in \mu_d$. So $F(X, \zeta Y)$ vanishes on the diagonal, so is divisible by $X - Y$. Hence $F(X, Y)$ is divisible by $X - \zeta^{-1}Y$. As the various factors $X - \zeta^{-1}Y$ for the various $\zeta \in \mu_d$ are relatively prime, $F(X, Y)$ is divisible by their product $X^d - Y^d$.

Returning to H, we observe that the assignment which attaches to $(g_1, g_2) \in H$ the unique element $\zeta \in \mu_d$ for which $g_2 = Bg_1B^{-1}\zeta$ is indeed a character $\chi : H \to \mu_d$. Restricting this χ to Γ, we have

$$\mathrm{Trace}(\rho_2(\gamma)) = \chi(\gamma)\mathrm{Trace}(\rho_1(\gamma)),$$

hence we have an equality $\rho_2 = \chi \otimes \rho_1$ of (irreducible) representations of Γ.

To show the uniqueness of χ, we argue as follows.The ratio of two such is a character Λ for which we have an isomorphism of nonzero (in fact irreducible) representations

$$\rho_1 \cong \Lambda \otimes \rho_1.$$

Because the Zariski closure of $\rho_1(\Gamma)$ is connected (being G_1), the last line of the proof of [Ka-RLS, 2.18.2bis] shows that any such Λ is trivial. □

Corollary 9.2. *Let $X/\mathbb{F}_q$ be smooth and geometrically irreducible, $\ell \neq p := char(\mathbb{F}_q)$, $\mathcal{F}$ and $\mathcal{G}$ lisse $\overline{\mathbb{Q}_\ell}$-sheaves on X, both of the same rank $n \geq 2$. Suppose that for all finite extensions $E/\mathbb{F}_q$, and all points $x \in X(E)$, we have*

$$\mathrm{Trace}(Frob_{x,E}|\mathcal{F})^2 = \mathrm{Trace}(Frob_{x,E}|\mathcal{G})^2.$$

Suppose further that one of the following three hypotheses holds.

(1) *The common rank n is even, $\mathcal{F}$ and $\mathcal{G}$ are symplectically self dual, and $G_{geom,\mathcal{F}} = G_{arith,\mathcal{G}} = Sp(n)$.*
(2) *The common rank n is even, $n \geq 4$, $\mathcal{F}$ and $\mathcal{G}$ are orthogonally self dual, and $G_{geom,\mathcal{F}} = G_{arith,\mathcal{G}} = SO(n)$.*
(3) *The common rank n is odd, $n \geq 3$, $\mathcal{F}$ and $\mathcal{G}$ are orthogonally self dual, and $G_{geom,\mathcal{F}} = G_{arith,\mathcal{G}} = SO(n)$.*

Then there exists a lisse rank one $\overline{\mathbb{Q}_\ell}$ sheaf $\mathcal{L}$ on X with $\mathcal{L}^{\otimes 2}$ arithmetically trivial, and an arithmetic isomorphism $\mathcal{G} \cong \mathcal{L} \otimes \mathcal{F}$. In case (3), $\mathcal{L}$ is trivial, and $\mathcal{G} \cong \mathcal{F}$. The sheaf $\mathcal{L}$ is unique.

Proof. We pick (!) an isomorphism of fields $\overline{\mathbb{Q}_\ell} \cong \mathbb{C}$, and apply Theorem 9.1, with Γ taken to be $\pi_1^{arith}(X)$ and with ρ_1 and ρ_2 the representations corresponding to $\mathcal{F}$ and $\mathcal{G}$ respectively. [The theorem applies because the groups in question, $Sp(n)$ for n even, $n \geq 2$ and $SO(n)$, $n \geq 3$ are connected semisimple groups with a unique representation of dimension n. By Chebotarev, for every $\gamma \in \Gamma = \pi_1^{arith}(X)$, we have

$$\mathrm{Trace}(\gamma|\mathcal{F})^2 = \mathrm{Trace}(\gamma|\mathcal{G})^2.]$$

The map from $\pi_1^{arith}(X)$ to $H(\overline{\mathbb{Q}_\ell})$ is continuous, so the character χ produced in the Theorem gives by composition a continuous character of $\pi_1^{arith}(X)$, which is our $\mathcal{L}$. In cases (1) and (2), the center has order $f = 2$. In case (3), the center is trivial, $f = 1$, so $\mathcal{L}$ is trivial. □

Corollary 9.3. *In the situation of Corollary 9.2, suppose in addition that $X/\mathbb{F}_q$ is $\mathbb{A}^1/\mathbb{F}_q$ and that p is odd. Then in cases (1) and (2), either $\mathcal{G} \cong \mathcal{F}$ or $\mathcal{G} \cong (-1)^{deg} \otimes \mathcal{F}$.*

Proof. Because p is odd, $\pi_1^{geom}(\mathbb{A}^1)$ has no nontrivial homomorphism to any finite group of order prime to p. So $\mathcal{L}$ is geometrically constant, of order dividing two, so is either trivial or is $(-1)^{deg}$. □

10. The identity $P(j,k) = V(j)V(k)$; preparations

We restate Corollary 8.3 here, as the following (key) lemma.

Lemma 10.1. *For $E/\mathbb{F}_q$ a finite extension, and $s, t \in E$, we have*

$$P(s,t,E) = \pm V(s,E)V(t,E).$$

We now turn to proving the following theorem.

Theorem 10.2. *Suppose $p \geq 5$. For any $s, t \in \mathbb{F}_q$, we have*

$$P(s,t) = V(s)V(t).$$

Corollary 10.3. *Suppose $p \geq 5$. For any finite extension $E/\mathbb{F}_q$, and any $s, t \in E$, we have*

$$P(s,t,E) = V(s,E)V(t,E).$$

Proof. This is just Theorem 10.2, applied after extension of scalars. □

We will prove Theorem 10.2 by focusing on the difference $s - t$. Thanks to Corollary 7.9, Theorem 10.2 is equivalent to the following Theorem.

Theorem 10.4. *Suppose $p \geq 5$. Fix $\lambda \in \mathbb{F}_q^\times$. For each $t \in \mathbb{F}_q$, we have*

$$P(t+\lambda, t-\lambda) = V(t+\lambda)V(t-\lambda).$$

We now fix $\lambda \in \mathbb{F}_q^\times$. Our first task will be to exhibit sheaf-theoretic incarnations of the products $V(t+\lambda)V(t-\lambda)$ and the sums $P(t+\lambda, t-\lambda)$.

To incarnate the products $V(t+\lambda)V(t-\lambda)$, we define two lisse sheaves on $\mathbb{A}^1$, both additive translates of $\mathcal{V}$, namely

$$\mathcal{V}_+^\lambda := [t \mapsto t+\lambda]^\star \mathcal{V}, \quad , \mathcal{V}_-^\lambda := [t \mapsto t-\lambda]^\star \mathcal{V}.$$

We then form their tensor product on $\mathbb{A}^1$

$$\mathcal{A}^\lambda := \mathcal{V}_+^\lambda \otimes \mathcal{V}_-^\lambda.$$

The sheaf $\mathcal{A}^\lambda$ is lisse of rank four and pure of weight zero. In view of Theorem 6.1 and Lemmas 6.4 and 6.5, we have

Lemma 10.5. *The trace function of the lisse sheaf $\mathcal{A}^\lambda$ on $\mathbb{A}^1$ is given as follows. For $E/\mathbb{F}_q$ a finite extension, and $t \in E$,*

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{A}^\lambda) = V(t+\lambda, E)V(t-\lambda, E).$$

Theorem 10.6. *If the characteristic $p \geq 5$, the sheaf $\mathcal{A}^\lambda$ has $G_{geom} = G_{arith} = SO(4)$.*

Proof. Because $p \geq 5$, $\mathcal{V}$ has $G_{geom} = G_{arith} = SL(2)$, cf. Theorem 6.3. One knows that the image of $SL(2) \times SL(2)$ in the tensor product $std_2 \otimes std_2$ of their standard representations is $SO(4)$. So we have a priori inclusions

$$G_{geom,\mathcal{A}^\lambda} \subset G_{arith,\mathcal{A}^\lambda} \subset SO(4).$$

So it suffices to show that $G_{geom,\mathcal{A}^\lambda} = SO(4)$. For this, we argue as follows. By the Goursat-Kolchin-Ribet criterion [Ka-ESDE, 1.8.2], it suffices to show that the two lisse sheaves $\mathcal{V}_+^\lambda$ and $\mathcal{V}_-^\lambda$ on $\mathbb{A}^1$ are not geometrically isomorphic, or equivalently that $\mathcal{V}$ is not geometrically isomorphic to $[t \mapsto t+2\lambda]^\star\mathcal{V}$. [In the $SL(2)$ case, we also have to show that neither is obtained from the other by tensoring with a character of $\pi_1^{geom}(\mathbb{A}^1)$ with values in ± 1, but as we are in odd characteristic, there are no such nontrivial characters.] This nonisomorphy is obvious already from looking at the $I(\infty)$-representations. By Lemma 6.6, the $I(\infty)$-representation of $\mathcal{V}$ is

$$\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(2\alpha x^2)} \bigoplus \mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(-2\alpha x^2)},$$

which, as we are in odd characteristic, is visibly nonisomorphic to any nontrivial additive translate of itself. □

To incarnate the sums $P(t+\lambda, t-\lambda)$, we must proceed in two steps. For $t \neq 0$, we have $(t+\lambda)^2 \neq (t-\lambda)^2$, hence

$$P(t+\lambda, t-\lambda) := \frac{-\sum_{uv=a} \chi_2(u-v)\psi(4t^2v + 4\lambda^2 u)}{-g} =$$

$$\frac{-\sum_{x \in \mathbb{F}_q^\times} \chi_2(a/x - x)\psi(4t^2x + 4\lambda^2 a/x)}{-g},$$

where we have written

$$g := g(\psi, \chi_2).$$

We now imitate the constuction of the sheaf $\mathcal{T}_0$ in Section 7. On the open set U of $\mathbb{A}^1$ where $ax - x^3$ is invertible, we have the lisse rank one sheaf $\mathcal{L}_{\chi_2(a/x-x)} \otimes \mathcal{L}_{\psi(4\lambda^2 a/x)}$. For $j : U \subset \mathbb{A}^1$ the inclusion, we form the sheaf $j_\star(\mathcal{L}_{\chi_2(a/x-x)} \otimes \mathcal{L}_{\psi(4\lambda^2 a/x)})$. This sheaf has vanishing stalk at 0 and the two square roots $\pm\alpha$ of a. Its shift $j_\star\mathcal{L}_{\chi_2(a/x-x)}[1]$ is a perverse sheaf on $\mathbb{A}^1$ which is geometrically irreducible. Denoting by ψ_4 the additive character $x \mapsto \psi(4x)$, we form the Fourier Transform

$$\mathcal{R}_0^\lambda := FT_{\psi_4}(j_\star(\mathcal{L}_{\chi_2(a/x-x)} \otimes \mathcal{L}_{\psi(4\lambda^2 a/x)}) \otimes (-g)^{-deg}).$$

This is a single sheaf, indeed $\mathcal{R}_0^\lambda[1]$ is a perverse sheaf on $\mathbb{A}^1$ which is geometrically irreducible (being the Fourier Transform of such an input). The trace function of $\mathcal{R}_0^\lambda$ is given as follows: for $E/\mathbb{F}_q$ a finite extension, and $t \in E$,

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{R}_0^\lambda) = \frac{-\sum_{x \in E^\times} \chi_{2,E}(a/x - x)\psi_E(4tx + 4\lambda^2 a/x)}{-g(\psi_E, \chi_{2,E})}.$$

We then define

$$\mathcal{P}_0^\lambda := [t \mapsto t^2]^\star\mathcal{R}_0.$$

The following lemma is a tautology.

Lemma 10.7. *For $E/\mathbb{F}_q$ a finite extension, and $t \in E$,*

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{P}_0^\lambda) = S(t+\lambda, t-\lambda, E).$$

For $t \neq 0$, we have

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{P}_0^\lambda) = P(t+\lambda, t-\lambda, E).$$

We thus have the following relation between $\mathcal{P}_0^\lambda$ and $\mathcal{A}^\lambda$.

Lemma 10.8. *For $E/\mathbb{F}_q$ a finite extension, and $t \in E^\times$,*

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{P}_0^\lambda) = \pm\mathrm{Trace}(Frob_{t,E}|\mathcal{A}^\lambda).$$

Proof. Simply combine Lemmas 10.7 and 10.5 with the fact that

$$P(j,k,E) = \pm V(j,E)V(k,E).$$

□

The geometric structure of $\mathcal{R}_0^\lambda$ is given as follows.

Theorem 10.9. *We have the following results on the sheaf $\mathcal{R}_0^\lambda$ on $\mathbb{A}^1$.*

(1) *The $I(\infty)$-representation of $\mathcal{R}_0^\lambda$ is*

$$Wild_2 \bigoplus \mathcal{L}_{\chi_2(t)} \otimes \mathcal{L}_{\psi(4\alpha t)} \bigoplus \mathcal{L}_{\chi_2(t)} \otimes \mathcal{L}_\psi(-4\alpha t),$$

with $Wild_2$ a two dimensional representation of $I(\infty)$ with both slopes $1/2$.

(2) *The sheaf $\mathcal{R}_0^\lambda$ is lisse of rank four, pure of weight zero, and geometrically irreducible on $\mathbb{G}_m$.*

(3) *The $I(0)$-representation of $\mathcal{R}_0^\lambda|\mathbb{G}_m$ is*

$$\overline{\mathbb{Q}_\ell} \oplus \overline{\mathbb{Q}_\ell} \oplus \overline{\mathbb{Q}_\ell} \oplus \mathcal{L}_{\chi_2(t)}.$$

(4) *For $j_0 : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion, we have an isomorphism $\mathcal{R}_0^\lambda \cong j_{0\star}(\mathcal{R}_0^\lambda|\mathbb{G}_m)$.*

(5) *The sheaf $\mathcal{R}_0^\lambda|\mathbb{G}_m$ is cohomologically rigid, i.e., for $j : \mathbb{G}_m \subset \mathbb{P}^1$ the inclusion,*

$$\chi(\mathbb{P}^1 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, j_\star End(\mathcal{R}_0^\lambda)) = 2.$$

(6) *Any lisse rank 4 sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_q}$ whose $I(0)$ and $I(\infty)$-representations are isomorphic to those of $\mathcal{R}_0^\lambda$ is geometrically isomorphic to $\mathcal{R}_0^\lambda|\mathbb{G}_m$.*

Proof. Assertion (1) results from Laumon's stationary phase. Here the input is tame at ∞, tame at the finite singularities at the two square roots of a, but at 0 has an $I(\infty)$-representation of dimension one and Swan conductor one (which contributes the $Wild_2$ piece). The proofs of assertions (2) through (5) are entirely analogous to the proofs of their analogues for $\mathcal{T}_0$ given in Theorem 7.2. □

Theorem 10.10. *The sheaf $\mathcal{R}_0^\lambda|\mathbb{G}_m$ has $G_{geom} \subset G_{arith} \subset O(4)$. If the characteristic $p \geq 5$, then $G_{geom} = G_{arith} = O(4)$.*

Proof. The sheaf $\mathcal{R}_0^\lambda$ has real traces. Hence $\mathcal{R}_0^\lambda|\mathbb{G}_m$, being lisse and pure of weight zero, is isomorphic to its dual. As $\mathcal{R}_0^\lambda|\mathbb{G}_m$ is geometrically irreducible, its autoduality has a sign. But its local monodromy at 0 is a reflection, which does not lie in $Sp(4)$ (because it has determinant -1). So the autoduality is orthogonal, i.e., we have inclusions $G_{geom} \subset G_{arith} \subset O(4)$.

Suppose now that $p \geq 5$. In view of the a priori inclusions, it suffices to prove that $G_{geom} = O(4)$. For this, it suffices to show that $\mathcal{R}_0^\lambda|\mathbb{G}_m$ is Lie-irreducible. For if we know this, then the fact that $Lie(G_{geom})$ is normalized by a reflection allows us to apply [Ka-ESDE, 1.5] to conclude that $Lie(G_{geom}) = Lie(SO(4))$. Hence G_{geom} contains $SO(4)$, and as it contains a reflection, it must be the entire group $O(4)$.

To show that $\mathcal{R}_0|\mathbb{G}_m$ is Lie-irreducible, we apply the trichotomy of [Ka-MGF, Prop. 1], according to which either $\mathcal{R}_0^\lambda|\mathbb{G}_m$ is Lie-irreducible, or it is induced from a finite etale covering of $\mathbb{G}_m/\overline{\mathbb{F}_q}$ of degree 2 or 4, or it is the tensor product of something Lie-irreducible of rank $d = 1$ or $d = 2$ with something or rank $4/d$ having finite G_{geom}. Because $p \geq 5$, the only finite etale coverings we need to consider are the Kummer coverings of degrees 2 and 4, and it is obvious from the $I(0)$ representation that $\mathcal{R}_0^\lambda|\mathbb{G}_m$ is not Kummer-induced. The fact that the $I(0)$-representation is through a reflection shows that already this $I(0)$-representation is not the tensor product of two $I(0)$-representations each of rank 2 (a reflection is never a tensor product in a nontrivial way).

It remains to show that G_{geom} is not a finite primitive subgroup of $O(4)$. If it were, then G_{arith} would be finite (lying inside the normalizer in $O(4)$ of a finite irreducible subgroup). Then the G_{arith} for the pullback $\mathcal{P}_0|\mathbb{G}_m = [2]^\star\mathcal{R}_0|\mathbb{G}_m$ would be (even more) finite. In that case, the traces

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{P}_0^\lambda),$$

as $E/\mathbb{F}_q$ runs over all finite extensions, and t runs over $E^\times$, would all lie in a **finite set**. By Lemma 10.9, this would imply that the traces

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{A}^\lambda),$$

as $E/\mathbb{F}_q$ runs over all finite extensions, and t runs over $E^\times$, would all lie in a finite set. This is nonsense, because $\mathcal{A}^\lambda|\mathbb{G}_m$ is lisse, pure of weight zero, and has $G_{geom} = G_{arith} = SO(4)$, so by Deligne's equidistribution theorem [Ka-GKM, 3.6] the traces

$$\{\mathrm{Trace}(Frob_{t,E}|\mathcal{A}^\lambda)\}_{t \in E^\times}$$

becomes equidistributed (as $\#E$ grows) in $[-4,4]$ for the direct image by the trace map

$$\text{Trace} : SO(4,\mathbb{R}) \to [-4,4]$$

of (total mass one) Haar measure on $SO(4,\mathbb{R})$. This measure (concretely, the additive convolution of semicircle measure $(1/(2\pi))\sqrt{4-x^2}dx$ on $[-2,2]$ with itself) is absolutely continuous with respect to Lebesgue measure on $[-4,4]$ and gives every nonvoid open set in $[-4,4]$ strictly positive measure, and in particular it is not a finite sum of point masses. □

We now define a sheaf $\mathcal{P}^\lambda$ on $\mathbb{A}^1$ which agrees with $\mathcal{P}_0$ on $\mathbb{G}_m$, but which has the "correct" stalk at 0. For $j : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion, we define

$$\mathcal{P}^\lambda := j_\star j^\star \mathcal{P}_0^\lambda = j_\star(\mathcal{P}_0^\lambda|\mathbb{G}_m).$$

Lemma 10.11. *The sheaf $\mathcal{P}^\lambda$ on $\mathbb{A}^1$ is lisse of rank four and pure of weight zero, with $G_{geom} \subset SO(4)$. In characteristic $p \geq 5$, $G_{geom} = SO(4)$.*

Proof. Local monodromy at 0 for $\mathcal{R}_0^\lambda|\mathbb{G}_m$ is a reflection, so the local monodromy at 0 of $\mathcal{P}^\lambda|\mathbb{G}_m$ is trivial, hence $\mathcal{P}$ is lisse at 0. That it has rank four and is pure of weight zero results from its being both lisse and the direct image from $\mathbb{G}_m$ of a lisse sheaf with these properties. The group G_{geom} for $\mathcal{P}^\lambda$ on $\mathbb{A}^1$ is the same as for $\mathcal{P}^\lambda|\mathbb{G}_m = [2]^\star\mathcal{R}_0^\lambda|\mathbb{G}_m$. So we again have an inclusion $G_{geom,\mathcal{P}^\lambda} \subset O(4)$. But $\det(\mathcal{P}^\lambda)$ is geometrically trivial, since it is a character of $\pi_1^{geom}(\mathbb{A}^1)$, and there are no such nontrivial characters. Thus we have $G_{geom} \subset SO(4)$.

Suppose now $p \geq 5$. In general, the identity component of G_{geom} does not change under finite pullback, so by Theorem 10.10 we have inclusions

$$SO(4) = G^0_{geom,\mathcal{P}^\lambda} \subset G_{geom,\mathcal{P}^\lambda} \subset SO(4).$$

□

Theorem 10.12. *In characteristic $p \geq 5$, $\mathcal{P}^\lambda$ has $G_{geom} = G_{arith} = SO(4)$.*

Proof. Given the inclusions

$$SO(4) = G_{geom} \subset G_{arith} \subset O(4),$$

the only other possibility is that $G_{geom} = SO(4)$ and $G_{arith} = O(4)$. In that case, $\det(\mathcal{P}^\lambda)$ is geometrically trivial but not arithmetically trivial, so we would have $\det(\mathcal{P}^\lambda) = (-1)^{deg}$. In view of Deligne's equidistribution theorem when G_{geom} is of finite index in G_{arith}, cf.

[Ka-Sar, 9.7.10], as $E/\mathbb{F}_q$ grows over larger and larger extensions of **odd** degree, the traces

$$\{\mathrm{Trace}(Frob_{t,E}|\mathcal{P}^\lambda)\}_{t\in E^\times}$$

would become equidistributed for the direct image by the trace map

$$\mathrm{Trace} : O_-(4,\mathbb{R}) \to [-4,4]$$

of the restriction of (total mass 2) Haar measure to the coset $O_-(4,\mathbb{R}) \subset O(4)$ of elements with determinant -1. On this coset, all traces lie in the interval $[-2,2]$. [Indeed every element in this coset has eigenvalues of the form $e^{i\theta}, e^{-i\theta}, 1, -1$.]

We arrive at a contradiction as follows. By Lemma 10.9, the traces of $\mathcal{P}^\lambda$ at points of $\mathbb{G}_m$ are, up to sign, those of $\mathcal{A}^\lambda$. By Theorem 10.6 $\mathcal{A}^\lambda$ has $G_{geom} = G_{arith} = SO(4)$. By equidistribution the traces of $\mathcal{A}^\lambda$, over larger and larger extensions, in particular over larger and larger extensions of **odd** degree, become equidistributed in $[-4,4]$ for a measure which gives every open set of $[-4,4]$ strictly positive measure. So over a large extension of odd degree, a positive proportion of the traces of $\mathcal{A}^\lambda$ have absolute value > 2. But $\mathcal{A}^\lambda$ and $\mathcal{P}^\lambda$ have the same $|\mathrm{Trace}|$ at all points of $\mathbb{G}_m$. □

We must now compute the action of $Frob_{0,E}$ on the stalk at 0 of $\mathcal{P}^\lambda$.

Theorem 10.13. *For $E/\mathbb{F}_q$ a finite extension, we have the identity*

$$\mathrm{Trace}(Frob_{0,E}|\mathcal{P}^\lambda) = P(\lambda,-\lambda,E),$$

and hence (by Lemma 10.7) for any $t \in E$, we have

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{P}^\lambda) = P(t+\lambda,t-\lambda,E),$$

Proof. The calculation is very similar to that for $\mathcal{S}$ occurring in the proof of Theorem 7.5. Lemma 10.7 gives, at $t=0$ the identity

$$\mathrm{Trace}(Frob_{0,E}|\mathcal{P}_0^\lambda) = S(\lambda,-\lambda,E).$$

By definition, we have

$$P(\lambda,-\lambda,E) = \chi_{2,E}(-1) + S(\lambda,-\lambda,E).$$

What must be shown is that the "new" eigenvalue of $Frob_{0,E}$ is $\chi_{2,E}(-1)$. Just as in the proof of Theorem 7.5, this eigenvalue is the action of of $Frob_{0,E}$ on the one-dimensional stalk at 0 of $j_\star j^\star(\mathcal{R}_0^\lambda \otimes \mathcal{L}_{\chi_2(x)})$. Any sheaf $\mathcal{G}$ on $\mathbb{A}^1$ which agrees with $\mathcal{R}_0^\lambda \otimes \mathcal{L}_{\chi_2(x)}$ on $\mathbb{G}_m$, geometrically has no nonzero punctual sections, and has a nonzero stalk at 0 must be $j_\star j^\star(\mathcal{R}_0^\lambda \otimes \mathcal{L}_{\chi_2(x)})$. Exactly as there, we show that the eigenvalue is

$\chi_{2,E}(-1)$ by giving the analogous "sheaf of perverse origin" construction of the needed $\mathcal{G}$, whose sole purpose is to provide a geometric justification of the following character sum calculation (and its E-version). For $t \neq 0$ in $\mathbb{F}_q$, we have

$$\mathrm{Trace}(Frob_{t,\mathbb{F}_q}|\mathcal{R}_0^\lambda \otimes \mathcal{L}_{\chi_2(x)}) = \frac{-\chi_2(t)\sum_{x\in\mathbb{F}_q^\times}\chi_2(a/x - x)\psi(4tx + 4\lambda^2 a/x)}{-g(\psi,\chi_2)}.$$

We rewrite this sum as

$$\frac{-\sum_{x\in\mathbb{F}_q^\times}\chi_2(at/x - tx)\psi(4tx + 4\lambda^2 a/x)}{-g(\psi,\chi_2)},$$

then sum over x/t to get

$$\frac{-\sum_{x\in\mathbb{F}_q^\times}\chi_2(at^2/x - x)\psi(4x + 4\lambda^2 at/x)}{-g(\psi,\chi_2)}.$$

Its value at $t = 0$ is indeed

$$\frac{-\sum_{x\in\mathbb{F}_q^\times}\chi_2(-x)\psi(4x)}{-g(\psi,\chi_2)} = \chi_2(-1).$$

□

Corollary 10.14. *For $E/\mathbb{F}_q$ a finite extension, and any $t \in E$, we have*

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{P}^\lambda) = \pm\mathrm{Trace}(Frob_{t,E}|\mathcal{A}^\lambda).$$

Proof. By Lemmas 10.1 and 10.5, and the above theorem, both sides are $\pm P(t+\lambda, t-\lambda, E)$. □

Theorem 10.15. *Suppose $p \geq 5$. If $P(\lambda, -\lambda) \neq 0$, then we have an arithmetic isomorphism $\mathcal{P}^\lambda \cong \mathcal{A}^\lambda$. For $E/\mathbb{F}_q$ a finite extension, and any $t \in E$, we have*

$$P(t+\lambda, t-\lambda, E) = V(t+\lambda, E)V(t-\lambda, E).$$

Proof. By Corollary 9.3, either $\mathcal{P}^\lambda \cong \mathcal{A}^\lambda$ or $\mathcal{P}^\lambda \cong (-1)^{deg} \otimes \mathcal{A}^\lambda$. By Corollary 7.10, Lemma 10.5 and Theorem 10.13, we have

$$P(\lambda,-\lambda) = \mathrm{Trace}(Frob_{0,\mathbb{F}_q}|\mathcal{P}^\lambda) = \mathrm{Trace}(Frob_{0,\mathbb{F}_q}|\mathcal{A}^\lambda) = V(\lambda)V(-\lambda).$$

If $P(\lambda, -\lambda) \neq 0$, this rules out the $(-1)^{deg}$ possibility. So we have an arithmetic isomorphism $\mathcal{P}^\lambda \cong \mathcal{A}^\lambda$. Equating their traces gives the second assertion. □

11. The end of the proof when $p \equiv 1 \bmod 4$

Lemma 11.1. *If* $p \equiv 1 \bmod 4$*, then for every* $\lambda \in \mathbb{F}_q^\times$*, we have* $P(\lambda, -\lambda) \neq 0$.

Proof. Because $P(\lambda, -\lambda) = \chi_2(-1)P(\lambda, \lambda)$, it is equivalent to prove that $P(\lambda, \lambda) \neq 0$. The quantity $P(\lambda, \lambda)$ lies in $\mathbb{Q}(\zeta_p)$, which has one place, π_p, lying over p. For this place, $1-\zeta_p$ is a uniformizing parameter. We denote by ord_q this valuation, normalized so that $ord_q(q) = 1$. We will show that, if $p \equiv 1 \bmod 4$, we have $ord_q(P(\lambda, \lambda)) = -1/2$, which forces $P(\lambda, \lambda) \neq 0$. By definition,

$$P(\lambda, \lambda) = 1 + S(\lambda, \lambda) = 1 + \frac{-\sum_{x \in \mathbb{F}_q^\times} \chi_2(ax - x^3)\psi(4\lambda^2 x)}{-g(\psi, \chi_2)}.$$

So it is equivalent to show that $ord_q(S(\lambda, \lambda)) = -1/2$. The denominator $-g(\psi, \chi_2)$ has $ord_q = 1/2$, so it suffices to show that the numerator,

$$-\sum_{x \in \mathbb{F}_q^\times} \chi_2(ax - x^3)\psi(4\lambda^2 x),$$

which lies in $\mathbb{Z}[\zeta_p]$, is a p-adic unit. For this, it suffices to show that it is congruent modulo the uniformizing parameter $1 - \zeta_p$ to a p-adic unit in $\mathbb{Z}$. Modulo the uniformizing parameter $1 - \zeta_p$, the numerator is the integer

$$-\sum_{x \in \mathbb{F}_q^\times} \chi_2(ax - x^3),$$

which is the trace of $Frob_{\mathbb{F}_q}$ on H^1 of the elliptic curve $y^2 = ax - x^3$, which has complex multiplication by $\mathbb{Z}[i]$. Because $p \equiv 1 \bmod 4$, this curve is ordinary at p, so this trace is a p-adic unit. □

Combining Lemma 11.1 with Theorem 10.15 (and Corollary 7.9), we get

Theorem 11.2. *If* $p \equiv 1 \bmod 4$*, Theorem 10.2 holds.*

12. The end of the proof in the general case

When $p \equiv 3 \bmod 4$, we do not know whether every $\lambda \in \mathbb{F}_q^\times$ has $P(\lambda, -\lambda) \neq 0$. However, we do have the following

Lemma 12.1. *Suppose* $p \geq 5$*. There exists* $\lambda \in \mathbb{F}_q^\times$ *with* $P(\lambda, -\lambda) \neq 0$.

Proof. As $P(\lambda, -\lambda) = \chi_2(-1)P(\lambda, \lambda)$, it is equivalent to show that there exists $\lambda \in \mathbb{F}_q^\times$ with $P(\lambda, \lambda) \neq 0$.

The case $p = 5$ is covered by Lemma 11.1. For $p \geq 7$, we have $q \geq 7$. By Theorem 8.1, we have

$$\sum_{t \in \mathbb{F}_q} P(t,t) = q - \chi_2(a).$$

We have the bound

$$|P(0,0)| \leq 4,$$

because $|S(0,0)| \leq 2$ (the Riemann Hypothesis for the elliptic curve $y^2 = ax - x^3$ over $\mathbb{F}_q$). So some other term in the sum $\sum_{t \in \mathbb{F}_q} P(t,t)$ must be nonzero. □

For the rest of this section, we fix a choice of $\lambda \in \mathbb{F}_q^\times$ with $P(\lambda, -\lambda) \neq 0$. By Theorem 10.15, we have an arithmetic isomorphism of lisse sheaves on $\mathbb{A}^1/\mathbb{F}_q$,

$$\mathcal{P}^\lambda \cong \mathcal{A}^\lambda.$$

We will make use of the restriction of this isomorphism to $\mathbb{G}_m$,

$$\mathcal{P}^\lambda | \mathbb{G}_m \cong \mathcal{A}^\lambda | \mathbb{G}_m.$$

We first explain the strategy. We begin with $\mathbb{A}^2/\mathbb{F}_q$, coordinates (s,t). We work on the open set

$$U := \mathbb{A}^2[1/(s^2 - t^2)]$$

of $\mathbb{A}^2/\mathbb{F}_q$ where $s^2 - t^2$ is invertible. We will construct a lisse, rank four sheaf $\mathcal{P}^{total}$ on U whose trace function is given by

$$\mathrm{Trace}(Frob_{(s,t),E} | \mathcal{P}^{total}) = P(s,t,E),$$

for any finite extension $E/\mathbb{F}_q$ and any point $(s,t) \in U(E)$. On this same open set U, we have the restriction to U of the lisse, rank four sheaf $\mathcal{V} \boxtimes \mathcal{V}$ on $\mathbb{A}^2/\mathbb{F}_q$, the external tensor product of $\mathcal{V}$ with itself. Let us call this restriction $\mathcal{A}^{total}$:

$$\mathcal{A}^{total} := \mathcal{V} \boxtimes \mathcal{V} | U.$$

Its trace function is given by

$$\mathrm{Trace}(Frob_{(s,t),E} | \mathcal{A}^{total}) = V(s,E), V(t,E).$$

We will prove that we have an arithmetic isomorphism of lisse sheaves on U,

$$\mathcal{P}^{total} \cong \mathcal{A}^{total}.$$

Once we have this isomorphism, then comparing their trace functions gives the truth of Theorem 10.2 at points where $s \neq \pm t$; the cases $s = \pm t$ are handled by Corollaries 7.9 and 7.10.

The sheaf $\mathcal{V}$ on $\mathbb{A}^1$ has $G_{geom} = G_{arith} = SL(2)$, so its external external tensor product with itself, $\mathcal{V} \boxtimes \mathcal{V}$, has $G_{geom} = G_{arith} = SO(4)$.

Both G_{geom}, G_{arith} are birational invariants, so the lisse sheaf $\mathcal{A}^{total}$ on U also has $G_{geom} = G_{arith} = SO(4)$.

We now explain the construction of the sheaf $\mathcal{P}^{total}$. We begin by defining a lisse sheaf $\mathcal{H}$ on $\mathbb{G}_m \times \mathbb{G}_m$, with coordinates (A, B), as follows. We begin with the curve $uv = a$, and pass to the open set W where $v^2 - a$ is invertible. On this open set W, we have the lisse sheaf $\mathcal{L}_{\chi_2(u-v)} \otimes (-g(\psi, \chi_2))^{-deg}$. On the product $W \times \mathbb{G}_m \times \mathbb{G}_m$, we have the lisse sheaf

$$\mathcal{F} := \mathcal{L}_{\chi_2(u-v)} \otimes \mathcal{L}_{\psi(Av+Bu)} \otimes (-g(\psi, \chi_2))^{-deg}.$$

We consider the projection $pr : W \times \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m \times \mathbb{G}_m$, and form

$$\mathcal{H} := R^1 pr_!(\mathcal{F}).$$

Each fibre is a $\mathbb{P}^1$, coordinate v, with the four points $0, \infty, \pm\sqrt{a}$ removed. Our sheaf is tame along the two missing points $\pm\sqrt{a}$, and has Swan conductor 1 at both $0, \infty$ (because A, B are both invertible). By Deligne's semicontinuity theorem [Lau-SCCS, 2.1.2], $\mathcal{H}$ is lisse. Looking fibre by fibre, we see that $R^i pr_!(\mathcal{F})$ vanishes for $i \neq 1$, and that $\mathcal{H}$ is punctually pure of weight zero. The Euler-Poincaré formula shows that $\mathcal{H}$ has rank four. The trace function of $\mathcal{H}$ is real, given by

$$\mathrm{Trace}(Frob_{(A,B),E}|\mathcal{H}) = \frac{-\sum_{uv=a\in E^\times} \chi_{2,E}(u-v)\psi_E(Av+Bu)}{-g(\psi_E, \chi_{2,E})}.$$

We now define the sheaf $\mathcal{P}^{total}$. We have a morphism

$$f : U \to \mathbb{G}_m \times \mathbb{G}_m, \quad (s,t) \mapsto ((s+t)^2, (s-t)^2).$$

We define

$$\mathcal{P}^{total} := f^\star \mathcal{H}.$$

Thus $\mathcal{P}^{total}$ is lisse of rank four, pure of weight zero, with a real trace function given by

$$\mathrm{Trace}(Frob_{(s,t),E}|\mathcal{P}^{total}) = P(s,t,E),$$

for any finite extension $E/\mathbb{F}_q$ and any point $(s,t) \in U(E)$.

Although we fixed a choice of $\lambda \in \mathbb{F}_q^\times$ with $P(\lambda, -\lambda) \neq 0$, we are not quite ready to use it. For **any** $\mu \in F_q^\times$, we have in U an embedded $\mathbb{G}_m$ with coordinate t, given by

$$i_\mu : \mathbb{G}_m \subset U, \quad t \in \mathbb{G}_m \mapsto (t+\mu, t-\mu) \in U.$$

Lemma 12.2. *We have arithmetic isomorphisms of lisse sheaves on* $\mathbb{G}_m/\mathbb{F}_q$

$$\mathcal{P}^\mu \cong i_\mu^\star \mathcal{P}^{total}, \quad \mathcal{A}^\mu \cong i_\mu^\star \mathcal{A}^{total}.$$

Proof. The trace function of $i_\mu^\star \mathcal{P}^{total}$ (resp. of $i_\mu^\star \mathcal{A}^{total}$) is equal to that of $\mathcal{P}^\mu$ (resp. of $\mathcal{A}^\mu$). So by Chebotarev their arithmetic semisimplifications are isomorphic. But both $\mathcal{P}^\mu$ and $\mathcal{A}^\mu$ are arithmetically irreducible, so the two pullbacks are arithmetically irreducible as well. □

Lemma 12.3. *The sheaf $\mathcal{P}^{total}$ on U has $G_{geom} = G_{arith} = SO(4)$.*

Proof. We know this sheaf is lisse of rank four, pure of weight zero, and has a real trace, so it is arithmetically isomorphic to its dual. By the previous lemma, it has a geometrically irreducible pullback, for example any $\mathcal{P}^\mu$, so it is geometrically (and arithmetically) irreducible. Thus its autoduality has a well defined sign. But we can read this sign from its pullback, and conclude that the autoduality is orthogonal. So we have a priori inclusions

$$G_{geom,\mathcal{P}^{total}} \subset G_{arith,\mathcal{P}^{total}} \subset O(4).$$

We also know that each $\mathcal{P}^\mu$ has $G_{geom,\mathcal{P}^\mu} = G_{arith,\mathcal{P}^\mu} = SO(4)$. Since G_{geom} can only decrease under a pullback, we have inclusions

$$SO(4) = G_{geom,\mathcal{P}^\mu} \subset G_{geom,\mathcal{P}^{total}} \subset G_{arith,\mathcal{P}^{total}} \subset O(4).$$

It remains only to show that $G_{arith,\mathcal{P}^{total}} \subset SO(4)$, i.e. to show that $\det(\mathcal{P}^{total})$ is arithmetically trivial. But every point of $U(\mathbb{F}_q)$ lies in one of the embedded $\mathbb{G}_m$'s (i.e. the point (s,t) lies in $i_\mu(\mathbb{G}_m)$ for $\mu = (s-t)/2$). But each $\mathcal{P}^\mu$ has $G_{arith} = SO(4)$. So for every rational point $(s,t) \in U(\mathbb{F}_q)$, we have $\det((Frob_{(s,t),\mathbb{F}_q}|\mathcal{P}^{total}) = 1$. Repeating this argument over finite extensions $E/\mathbb{F}_q$, we get that $\det(\mathcal{P}^{total})$ is arithmetically trivial. □

We complete the proof of Theorem 10.2 with the following theorem.

Theorem 12.4. *In any characteristic $p \geq 5$, we have an arithmetic isomorphism*

$$\mathcal{P}^{total} \cong \mathcal{A}^{total}$$

of lisse sheaves on $\mathbb{A}^2[1/(s^2-t^2)]$.

Proof. The trace functions of the lisse sheave $\mathcal{P}^{total}$ and $\mathcal{A}^{total}$ have the same square, and each has $G_{geom} = G_{arith} = SO(4)$. By Corollary 9.3, there is a lisse, rank one sheaf $\mathcal{L}$ on U with $\mathcal{L}^{\otimes 2}$ arithmetically trivial, for which we have an arithmetic isomorphism

$$\mathcal{P}^{total} \cong \mathcal{L} \otimes \mathcal{A}^{total}$$

of lisse sheaves on $\mathbb{A}^2[1/(s^2-t^2)]$.

We will first show that this $\mathcal{L}$ is geometrically trivial.

To analyze the possible geometric $\mathcal{L}$, we use the Kummer sequence

$$0 \to \mu_2 \to \mathbb{G}_m \overset{x \mapsto x^2}{\to} \mathbb{G}_m \to 0$$

on $U_{\overline{\mathbb{F}_q}} = \mathbb{A}^2[1/(s^2-t^2)]_{\overline{\mathbb{F}_q}} = Spec(R), R = \overline{\mathbb{F}_q}[s,t][1/(s^2-t^2)]$. Since R is a UFD, it has trivial Picard group: $H^1(U_{\overline{\mathbb{F}_q}}, \mathbb{G}_m) = 0$. So the long exact étale cohomology sequence gives a coboundary isomorphism

$$R^\times/(R^\times)^2 \cong H^1(U_{\overline{\mathbb{F}_q}}, \mu^2) := Hom(\pi_1^{geom}(U), \mu_2).$$

In this isomorphism, an element of $R^\times/(R^\times)^2$ represented by a function $g \in R^\times$ corresponds to $\mathcal{L}_{\chi_2(g)}$. For this R, the cokernel $R^\times/(R^\times)^2$ is the two-dimensional $\mathbb{F}_2$-vector space with basis $s-t, s+t$. So $\mathcal{P}^{total}$ is geometrically isomorphic to exactly one of following four sheaves:

$$\mathcal{A}^{total}, \ \ \mathcal{L}_{\chi_2(s-t)} \otimes \mathcal{A}^{total}, \ \ \mathcal{L}_{\chi_2(s+t)} \otimes \mathcal{A}^{total}, \ \ \mathcal{L}_{\chi_2(s^2-t^2)} \otimes \mathcal{A}^{total}.$$

Under the involution $(s,t) \mapsto (s,-t)$, the trace functions of both $\mathcal{P}^{total}$ and $\mathcal{A}^{total}$ on E-valued points multiply by the same constant field twist factor, $\chi_{2,E}(-1)$. So our $\mathcal{L}$ must, by uniqueness, be isomorphic to its pullback by this involution. So our $\mathcal{L}$ cannot be either $\mathcal{L}_{\chi_2(s-t)}$ or $\mathcal{L}_{\chi_2(s+t)}$. We next rule out the $\mathcal{L}_{\chi_2(s^2-t^2)}$ possibility. If we had a geometric isomorphism

$$\mathcal{P}^{total} \cong \mathcal{L}_{\chi_2(s^2-t^2)} \otimes \mathcal{A}^{total},$$

then after pullback by i_λ, we would get a geometric isomorphism

$$\mathcal{P}^\lambda \cong \mathcal{L}_{\chi_2(4\lambda t)} \otimes \mathcal{A}^\lambda.$$

This contradicts (the restriction to $\mathbb{G}_m$ of) Theorem 10.15.

So we have a geometric isomorphism

$$\mathcal{P}^{total} \cong \mathcal{A}^{total}.$$

So the $\mathcal{L}$ is a geometrically constant character of order dividing two, so it is either arithmetically trivial or it is $(-1)^{deg}$. So either we have an arithmetic isomorphism $\mathcal{P}^{total} \cong \mathcal{A}^{total}$, in which case we are done, or we have an arithmetic isomorphism

$$\mathcal{P}^{total} \cong (-1)^{deg} \otimes \mathcal{A}^{total}.$$

This cannot happen, because its pullback by i_λ would give an arithmetic isomorphism

$$\mathcal{P}^\lambda \cong (-1)^{deg} \otimes \mathcal{A}^\lambda$$

on $\mathbb{G}_m$, and then on $\mathbb{A}^1$ as well (simply becaus $\pi_1^{arith}(\mathbb{G}_m)$ maps onto $\pi_1^{arith}(\mathbb{A}^1)$). This contradicts Theorem 10.15. □

References

[A-S-S-W] Amburg, R., Sharma, R., Sussman, D.M., and Wootters, W., in preparation.

[Ap] Appleby, D.M., Properties of the extended Clifford group with applications to SIC-POVMs and MUBs, arXiv:0909.5233v1 (2009) on arXiv.org.

[BBD] Beilinson, A., Bernstein, J., and Deligne, P., Faisceaux pervers. (entire contents of) Analyse et topologie sur les éspaces singuliers, I (Conférence de Luminy, 1981), 5-171, Astérisque, 100, Soc. Math. France, Paris, 1982.

[Be-Ev] Berndt, B.C. and Evans, R.J., The determination of Gauss sums. Bull. Amer. Math. Soc. (N.S.) 5 (1981), 107-129.

[Be-Ev-Wi] Berndt, B.C., Evans, R.J., and Williams,K.S., Gauss and Jacobi Sums. Can. Math. Soc. Series of Monographs and Advanced Texts. Wiley, New York, 1998. xii+583 pp.

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

[Ka-ClausCar] Katz, N., From Clausen to Carlitz: Low-dimensional spin groups and identities among character sums. Moscow Math. J. 9 (2009), no. 1, 57-89.

[Ka-ESDE] Katz, N., Exponential sums and differential equations. Annals of Mathematics Studies, 124. Princeton Univ. Press, Princeton, NJ, 1990. xii+430 pp.

[Ka-G2Hyper] Katz, N., G_2 and hypergeometric sheaves. Finite Fields Appl. 13 (2007), no. 2, pp. 175-223.

[Ka-GKM] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups. Annals of Math. Studies, 116. Princeton Univ. Press, Princeton, NJ,1988. x+246 pp.

[Ka-MGF] Katz, N., On the monodromy groups attached to certain families of exponential sums, Duke Math. J. 54 (1987), no. 1, 5765.

[Ka-RLS] Katz, N., Rigid local systems. Annals of Mathematics Studies, 139. Princeton University Press, Princeton, NJ, 1996. viii+223 pp.

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

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

[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.

[Stick] Stickelberger, L., Ueber eine Verallgemeinerung der Kreistheilung, Math. Ann. 37 (1890), 321-367.

[S-W] Sussman, D.M., and Wootters, W., Discrete Phase Space and Minimum-Uncertainty States, in Proceedings of the Eighth International Conference on Quantum Communication, Measurement and Computing, edited by O. Hirota, J. H. Shapiro and M. Sasaki (NICT Press, 2007). Also available on arXiv.org as arXiv:0704.1277v1.

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