WITT VECTORS AND A QUESTION OF KEATING AND RUDNICK

NICHOLAS M. KATZ

1. Introduction

We work over a finite field $k = \mathbb{F}_q$ inside a fixed algebraic closure $\overline{k}$, and fix an integer $n \geq 2$. We form the k-algebra

$$B := k[X]/(X^{n+1}).$$

Following Keating and Rudnick, we say that a character

$$\Lambda : B^\times \to \mathbb{C}^\times$$

is "even" if it is trivial on the subgroup $k^\times$.

The quotient group $B^\times/k^\times$ is the group of "big" Witt vectors mod X^{n+1} with values in k. Recall that for any ring A, the group $BigWitt(A)$ is simply the abelian group $1 + XA[[X]]$ of formal series with constant term 1, under multiplication of formal series. In this group, the elements $1 + X^{n+1}A[[X]]$ form a subgroup; the quotient by this subgroup is $BigWitt_n(A)$:

$$BigWitt_n(A) := (1 + XA[[X]])/(1 + X^{n+1}A[[X]]).$$

We will restrict this functor $A \mapsto BigWitt_n(A)$ to variable k-algebras A. In this way, $BigWitt_n$ becomes a commutative unipotent group-scheme over k.

The Lang torsor construction

$$1 - Frob_k : BigWitt_n \to BigWitt_n$$

defines a finite étale cover of $BigWitt_n$ by itself, with structural group $BigWitt(k)$. Given a character Λ of $BigWitt_n(k)$, the pushout of this torsor by Λ gives the lisse, rank one Artin-Schrier-Wtt sheaf $\mathcal{L}_\Lambda$ on $BigWitt$.

We have a morphism of k-schemes

$$\mathbb{A}^1 \to BigWitt_n,\ t \mapsto 1 - tX \bmod X^{n+1}.$$

The pullback of $\mathcal{L}_\Lambda$ by this morphism is, by definition, the lisse, rank one sheaf $\mathcal{L}_{\Lambda(1-tX)}$ on the affine t-line.

A character Λ of $BigWitt_n(k)$ is called primitive, or maximally ramified, if it is nontrivial on the subgroup $1 + kX^n$. The Swan conductor

$Swan(\Lambda)$ of Λ is the largest integer $d \le n$ such that Λ is nontrivial on the subgroup $1 + kX^d$. [Thus only the trivial character has conductor 0, and the primitive characters are precisely those of Swan conductor n.] Let us admit for the moment the following compatibility between the Swan conductor of Λ and the Swan conductor at ∞ of the lisse, rank one sheaf $\mathcal{L}_{\Lambda(1-tX)}$ on the affine t-line.

Lemma 1.1. *We have the equality* $Swan(\Lambda) = Swan_\infty(\mathcal{L}_{\Lambda(1-tX)})$.

Given an even character Λ of $B^\times$, i.e., a character Λ of $BigWitt_n(k)$, we can form an L-function on $\mathbb{G}_m/k$ as follows. Gvien an irreducible monic polynomial $P(t) \in k[t]$ with $P(0) \neq 0$, the irreducible polynomial $P(t)/P(0)$ has constant term 1, so $P(X)/P(0) \bmod X^{n+1}$ lies in $BigWitt_n(k)$, and we define

$$\Lambda(P) := \Lambda(P(X)/P(0) \bmod X^{n+1}).$$

We then define

$$L(\mathbb{G}_m/k, \Lambda)(T) := \prod_{irred.\ monic\ P,\ P(0)\neq 0} (1 - \Lambda(P)T^{deg(P)})^{-1}.$$

It is routine that this L-function has a cohomological interpretation:

$$L(\mathbb{G}_m/k, \Lambda)(T) = L(\mathbb{G}_m/k, \mathcal{L}_{\Lambda(1-tX)})(T).$$

This second expression, with coefficient sheaf which is lisse at 0, leads us to consider the "completed" L-function

$$L(\mathbb{A}^1/k, \mathcal{L}_{\Lambda(1-tX)})(T) = L(\mathbb{G}_m/k, \mathcal{L}_{\Lambda(1-tX)})(T)/(1-T) =$$

$$= L(\mathbb{G}_m/k, \Lambda)(T)/(1-T).$$

One knows that so long as Λ is nontrivial, this completed L-function is a polynomial in T of degree $Swan(\Lambda) - 1$, which is "pure of weight one". In other words, it is of the form $\prod_{i=1}^{Swan(\Lambda)-1}(1 - \beta_i T)$ with each β_i an algebraic integer all of whose complex absolute values are $\sqrt{q}$.

For Λ primitive, we define a conjugacy class $\theta_{k,\Lambda}$ in the unitary group $U(n-1)$ in terms of its reversed characteristic polynomial by the formula

$$\det(1 - T\theta_{k,\Lambda}) = L(\mathbb{A}^1/k, \mathcal{L}_{\Lambda(1-tX)})(T/\sqrt{q}).$$

Our goal is to prove the following equidistribution theorem. Denote by $PU(n-1)$ the projective unitary group, i.e. the quotient of $U(n-1)$ by the group S^1 of unitary scalars. Endow this group with its total mass one Haar measure, and then endow its space of conjugacy classes with the direct image of this measure.

Theorem 1.2. *Fix an integer $n \geq 4$. In any sequence of finite fields k_i (of possibly varying characteristics) whose cardinalities q_i are archimedeanly increasing to ∞, the collections of conjugacy classes*

$$\{\theta_{k_i,\Lambda}\}_{\Lambda \text{ primitive even}}$$

become equidistributed in $PU(n-1)^{\#}$. We have the same result for $n = 3$ if we require that no k_i have characteristic 2 or 5.

Remark 1.3. The conjugacy classes $\{\theta_{k_i,\Lambda}\}$ begin life in the unitary group $U(n-1)$, but it is only their projections to the projective unitary group $PU(n-1)$ which are equidistributed. As we will see in sections 4 and 5, in each characteristic p, these conjugacy classes arise as the Frobenius conjugacy classes of a lisse sheaf of rank $n-1$, pure of weight zero, on a smooth, geometrically connected $\mathbb{F}_p$-scheme (the sheaf $L_{univ}(1/2)$ on the space $Prim_n/\mathbb{F}_p$). Intrinsically, the classes $\{\theta_{k_i,\Lambda}\}$ will live in a compact form of the algebraic group G_{arith} attached to this situation. We have a priori inclusions

$$G_{geom} \subset G_{arith} \subset GL(n-1)$$

and we will prove (Theorem 5.1) that G_{geom} contains $SL(n-1)$. So we have inclusions

$$SL(n-1) \subset G_{geom} \subset G_{arith} \subset GL(n-1).$$

However, in Remark 8.3 we will explain that we have an a priori inclusion

$$G_{arith} \subset \{A \in GL(n-1) | \ \det(A)^{4p^{r+1}} = 1\}$$

for p^r the largest power of p with $p^r \leq n$. In particular, the classes $\{\theta_{k_i,\Lambda}\}$ are **not** equidistributed as classes in $U(n-1)$, already their determinants fail to be equidistributed in the unit circle.

2. Review of the relation of *BigWitt* to p-Witt vectors

In this section, we fix a prime number p, and work over the ring $\mathbb{Z}_{(p)} = \mathbb{Z}[1/\ell, \text{all primes } \ell \neq p]$. [So $\mathbb{Z}_{(p)}$ is the local ring of $\mathbb{Z}$ at its prime idea $p\mathbb{Z}$; its completion is the ring $\mathbb{Z}_p$ of p-adic integers.] Concretely, a $\mathbb{Z}_{(p)}$-algebra A is simply a ring in which all primes other than p are invertible. The Artin-Hasse exponential[1] is the formal series, a priori in $1 + X\mathbb{Q}[[X]]$, defined by

$$AH(X) := \exp(-\sum_{n \geq 0} X^{p^n}/p^n) = 1 - X + ...$$

[1] Some authors call $\exp(\sum_{n\geq 0} X^{p^n}/p^n)$ the Artin-Hasse exponential

The "miracle" is that in fact $AH(X)$ has p-integral coefficients, i.e., it lies in $1 + X\mathbb{Z}_{(p)}[[X]]$.

Over any ring R, any element of $BigWitt(R) = 1 + XR[[X]]$ has a unique expression as an infinite product $\prod_{n\geq 1}(1 - r_n X^n)$ with elements $r_n \in R$. Over a $\mathbb{Z}_{(p)}$-algebra A, any element of $BigWitt(A)$ has a unique expression as an infinite product

$$\prod_{n\geq 1} AH(a_n X^n)$$

with elements $a_n \in A$. We now rewrite this expression. Factor each integer $n \geq 1$ as

$$n = mp^a$$

with m prime to p, and $a \geq 0$. Because raising to the m'th power is bijective on $BigWitt(A)$, we may write any element of $BigWitt(A)$ uniquely as an infinite product

$$\prod_{m\geq 1 \text{ prime to } p,\ a\geq 0} AH(a_{mp^a} X^{mp^a})^{1/m}.$$

On the other hand, having fixed the prime p, we have, for each $\mathbb{Z}_{(p)}$-algebra A, the abelian group $W(A)$, of all sequences $(a_0, a_1, ...)$ of elements of A indexed by nonnegative integers, with addition defined by the Witt polynomials. The key point for us is that the map

$$W(A) \to BigWitt(A),\ (a_0, a_1, ...) \mapsto \prod_{i\geq 0} AH(a_i X^{p^i})$$

is a group homomorphism. In view of the above factorization of elements of $BigWitt(A)$, we find a (huge) isomorphism

$$BigWitt(A) \cong \prod_{m\geq 1 \text{ prime to } p} W(A)$$

given by attaching to an element

$$\prod_{m\geq 1 \text{ prime to } p,\ a\geq 0} AH(a_{mp^a} X^{mp^a})^{1/m} \in BigWitt(A)$$

the tuple of elements of $W(A)$ whose m'th component is the Witt vector $(a_m, a_{mp}, a_{mp^2}, ...) \in W(A)$.

Lemma 2.1. *For any $\mathbb{Z}_{(p)}$-algebra A, and any element $a \in A$, under the above isomorphism*

$$BigWitt(A) \cong \prod_{m\geq 1 \text{ prime to } p} W(A),$$

the element $1-aX \in BigWitt(A)$ *maps to the element in* $\prod_{m\geq 1 \text{ prime to } p} W(A)$ *whose m'th component is the Witt vector* $(a^m, 0, 0, 0, ...)$. *Equivalently, we have the identity*

$$1 - aX = \prod_{m\geq 1 \text{ prime to } p} AH(a^m X^m)^{1/m}.$$

Proof. It suffices to treat the universal case, where a is the element T in the polynomial ring $\mathbb{Z}_{(p)}[T]$. Extending scalars to $\mathbb{Q}[T]$, we may check by taking the log's of both sides. So what we must show is the identity

$$\log(1 - TX) = -\sum_{m\geq 1 \text{ prime to } p} \sum_{a\geq 0} (T^m)^{p^a} X^{mp^a}/(mp^a).$$

This is just the usual series expansion of $\log(1-TX) = -\sum_{n\geq 1}(TX)^n/n$, with n factored as mp^a. □

Recall that for each integer $n \geq 1$ we have the truncated Witt vectors $W_n(A)$, whose elements are n-tuples $(a_0, ..., a_{n-1})$ of elements of A, with addition given by the Witt polynomials. Alternatively, the elements of $W(A)$ whose first n components vanish form a subgroup[2], and the quotient of $W(A)$ by this subgroup is $W_n(A)$. Truncating the isomorphism

$$BigWitt(A) \cong \prod_{m\geq 1 \text{ prime to } p} W(A)$$

mod T^{n+1}, we get an isomorphism

$$BigWitt_n(A) \cong \prod_{m\geq 1 \text{ prime to } p,\ m\leq n} W_{\ell(m,n)}(A),$$

with $\ell(m, n)$ the integer defined by

$$\ell(m, n) = 1 + \text{the largest integer } k \text{ such that } mp^k \leq n.$$

The "reduction mod X^{n+1}" of the previous lemma gives

Lemma 2.2. *For any* $\mathbb{Z}_{(p)}$*-algebra* A*, and any element* $a \in A$*, under the above isomorphism*

$$BigWitt_n(A) \cong \prod_{m\geq 1 \text{ prime to } p,\ m\leq n} W_{\ell(m,n)}(A),$$

[2] Indeed, this is the subgroup consisting of those elements which, under the homomorphism to $BigWitt(A)$ given by $(a_0, a_1, ..) \mapsto \prod_{i\geq o} AH(a_i X^{p^i})$, land in the subgroup $1 + Z^{p^n} A[[X]]$

the element $1 - aX \in BigWitt_n(A)$ maps to the element in

$$\prod_{m\geq 1 \text{ prime to } p,\ m\leq n} W_{\ell(m,n)}(A)$$

whose m'th component is the Witt vector $(a^m, 0'\mathrm{s}) \in \mathrm{W}_{\ell(\mathrm{m,n})}(\mathrm{A})$.

Before proceeding, we need to recall that $W_r(A)$ carries a ring structure. The main things we will need to know are that for this ring structure, we have the multiplication formulas

$$(a_0, 0, 0, ..., 0) \times (b_0, b_1, ...b_{r-1}) = (a_0 b_0, a_0^p b_1, ..., a_0^{p^{r-1}} b_{r-1})$$

and

$$(a_0, ..., a_{r-1})(0'\mathrm{s}, \mathrm{b_{r-1}}) = (0'\mathrm{s}, \mathrm{a_0^{p^{r-1}} b_{r-1}}).$$

We also recall that in Witt vector addition, “disjoint” Witt vectors add naively, i.e.,

$$(a_0, a_1, ..., a_{r-1}) = (a_0, 0'\mathrm{s}) + (0, \mathrm{a_1}, 0'\mathrm{s}) + ... + (0'\mathrm{s}, \mathrm{a_{r-1}}).$$

When A is the prime field $\mathbb{F}_p$, we have a ring isomorphism $W_r(\mathbb{F}_p) \cong \mathbb{Z}/p^r\mathbb{Z}$,

$$(a_0, a_1, ..., a_{r-1}) \mapsto \sum_{i=0}^{r-1} Teich(a_i)p^i \bmod p^r.$$

Here $Teich(a_i) \in \mu_{p-1}(\mathbb{Z}_p) \cup \{0\}$ is the Teichmuller representative of a_i in $\mathbb{Z}_p$.

3. Calculation of conductors

We now recall a result of Brylinski [Bry, Cor. of Thm.1]. We view W_r as a connected unipotent groupscheme over our finite field k. One knows that the trace pairing

$$W_r(k) \times W_r(k) \to W_r(\mathbb{F}_p) = \mathbb{Z}/p^r\mathbb{Z},\ (a, b) \to \mathrm{Trace}_{W_r(k)/W_r(\mathbb{F}_p}(ab)$$

is makes $W_r(k)$ its own $\mathbb{Z}/p^r\mathbb{Z}$-dual. If we fix a faithful character

$$\psi_r : \mathbb{Z}/p^r\mathbb{Z} \cong \mu_{p^r}(\mathbb{C}),$$

then every character of $W_r(k)$ is of the form

$$w \mapsto \psi(\mathrm{Trace}_{W_r(k)/W_r(\mathbb{F}_p}(aw))$$

for a unique element $a \in W_r(k)$. Let us denote this character $\psi_{r,a}$:

$$\psi_{r,a}(w) := \psi(\mathrm{Trace}_{W_r(k)/W_r(\mathbb{F}_p}(aw)).$$

Attached to the character $\psi_{r,a}$ of $W_r(k)$ we have the Artin-Schreier-Witt sheaf $\mathcal{L}_{\psi_{r,a}} = \mathcal{L}_{\psi_r(aw)}$ on W_r. Given an integer $m \geq 1$ prime to p, we have the morphism of k-schemes $\mathbb{A}^1 \to W_r$ given by $t \mapsto (t^m, 0'\mathrm{s})$. The pullback of $\mathcal{L}_{\psi_{r,a}}$ by this morphism is denoted $\mathcal{L}_{\psi_{r,a}(t^m,0'\mathrm{s})} = \mathcal{L}_{\psi_r(a(t^m,0'\mathrm{s}))}$. It is a lisse rank one sheaf on $\mathbb{A}^1$.

Lemma 3.1. *If $a = (a_0, ..., a_{r-1})$ in $W_r(k)$ is nonzero, then $\psi_{r,a}$ has order p^{r-d} for d the largest integer such that $a_i = 0$ for all $i \leq d-1$, and for such an a, the Swan conductor of $\mathcal{L}_{\psi_r(a(t^m,0'\mathrm{s}))}$ is given by*

$$Swan_\infty(\mathcal{L}_{\psi_r(a(t^m,0'\mathrm{s}))}) = mp^{r-1-d}.$$

Proof. The sheaf $\mathcal{L}_{\psi_r(a(t^m,0'\mathrm{s}))}$ is the pullback by the m'th power mapping of $\mathbb{A}^1$ to itself, so by the known behavior of Swan conductors under tame pullback (remember m is prime to p), it suffices to treat the case $m = 1$.

We have the multiplication formula

$$(t, 0'\mathrm{s})(\mathrm{a}_0, ..., \mathrm{a}_{r-1}) = (\mathrm{a}_0\mathrm{t}, \mathrm{a}_1\mathrm{t}^{\mathrm{p}}, ..., \mathrm{a}_{r-1}\mathrm{t}^{\mathrm{p}^{r-1}}) =$$

$$= (a_0t, 0'\mathrm{s}) + (0, \mathrm{a}_1\mathrm{t}^{\mathrm{p}}, 0'\mathrm{s}) + ...(0'\mathrm{s}, \mathrm{a}_{r-1}\mathrm{t}^{\mathrm{p}^{r-1}}).$$

Using Artin-Schreier equivalence, we have

$$(0, a_1t^p, 0'\mathrm{s}) \cong (0, \mathrm{a}_1^{1/\mathrm{p}}\mathrm{t}, 0'\mathrm{s}), ..., (0'\mathrm{s}, \mathrm{a}_{r-1}\mathrm{t}^{\mathrm{p}^{r-1}}) \cong, (0'\mathrm{s}, \mathrm{a}_{r-1}^{1/\mathrm{p}^{r-1}}\mathrm{t}).$$

Thus for $a = (a_0, a_1, ..., a_{r-1})$, $a(t, 0'\mathrm{s})$ is Artin-Schreier equivalent to the Witt vector

$$(b_0t, b_1t, ..., b_{r-1}t)$$

with components $b_i = a_i^{1/p^i}$.

If $b_0 \in k^\times$, the fact that the Swan conductor is p^{r-1} is given by [Bry, Cor. of Thm. 1]. If $b_i = 0$ for all $i \leq d-1$ but $b_d \in k^\times$, then we are reduced to the same statement, but now for W_{r-d} instead of for W_r. □

Thus a character Λ of $BigWitt_n(k)$, under the isomorphism

$$BigWitt_n(k) \cong \prod_{m \geq 1 \text{ prime to } p,\ m \leq n} W_{\ell(m,n)}(k),$$

becomes a character of $\prod_{m\geq 1 \text{ prime to } p,\ m\leq n} W_{\ell(m,n)}(k)$, where it is of the form

$$(w(m))_m \mapsto \prod_m \psi_{\ell(m,n),a(m)}(w(m))$$

for uniquely defined elements $a(m) \in W_{\ell(m,n)}(k)$.

The lisse sheaf $\mathcal{L}_{\Lambda(1-tu)}$ on $\mathbb{A}^1/k$ thus becomes the tensor product

$$\mathcal{L}_{\Lambda(1-tu)} \cong \otimes_m \mathcal{L}_{\psi_{\ell(m,n)}(a(m)(t^m,0'\mathrm{s}))}.$$

Lemma 3.2. *Write $n = n_0p^{r-1}$ with n_0 prime to p and $r \geq 1$. Then we have the following results.*

(1) *We have* $Swan_\infty(\otimes_m \mathcal{L}_{\psi_{\ell(m,n)}(a(m)(t^m,0's))}) = n$ *if and only if the Witt vector* $a(n_0) \in W_{\ell(n_0,n)}(k) = W_r(k)$ *has its initial component* $a(n_0)_0 \in k^\times$.

(2) *We have* $Swan_\infty(\mathcal{L}_{\Lambda(1-tu)}) = n$ *if and only if* Λ *is a primitive character of* $BigWitt_n(k)$.

Proof. To prove the first assertion, we argue as follows. For each $m \le n$, write $m = m_0 p^{k_m - 1}$ with m_0 prime to p and $k_m \ge 1$. By the previous lemma, the tensor factor $\mathcal{L}_{\psi_{\ell(m_0,n)}(a(m_o)(t^{m_0},0's))})$ has $Swan_\infty \le m$.

So our sheaf $\otimes_m \mathcal{L}_{\psi_{\ell(m,n)}(a(m)(t^m,0's))})$ is of the form

$$\mathcal{L}_{\psi_{\ell(m_0,n)}(a(m_o)(t^{m_0},0's))} \otimes (\text{lisse, rank one }, Swan_\infty < n).$$

Such a tensor product has $Swan_\infty = n$ if and only if the first factor $\mathcal{L}_{\psi_{\ell(m_0,n)}(a(m_o)(t^{m_0},0's))}$ has $Swan_\infty = n$, and by the previous lemma, this happens if and only if $a(n_0)_0 \in k^\times$.

To prove the second assertion, observe that in the isomorphism

$$BigWitt_n(k) \cong \prod_{m \ge 1 \text{ prime to } p,\ m \le n} W_{\ell(m,n)}(k),$$

the subgroup $1 + kX^n$ of $BigWitt_n(k)$ maps to the subgroup $(0'\mathrm{s}, \mathrm{k})$ of the factor $W_{\ell(n_0,n)}(k)$. The character Λ is primitive, i.e., nontrivial on the subgroup $1+kX^n$, if and only if the character $\psi_{r,a(m_0)}$ of $W_{\ell(n_0,n)}(k)$ is nontrivial on the subgroup $(0'\mathrm{s}, \mathrm{k})$ of the factor $W_{\ell(n_0,n)}(k)$. By the multiplication formula for Witt vectors, we have

$$(a_0, ..., a_{r-1})(0'\mathrm{s}, \mathrm{t}) = (0'\mathrm{s}, \mathrm{a}_0^{\mathrm{p}^{r-1}}\mathrm{t}).$$

So the character $\psi_{r,a(m_0)}$ is nontrivial on this subgroup if and only if the Witt vector $a(n_0) \in W_{\ell(n_0,n)}(k) = W_r(k)$ has its initial component $a(n_0)_0 \in k^\times$, i.e., if and only if (by part (1)), $Swan_\infty(\mathcal{L}_{\Lambda(1-tu)}) = n$. □

4. The universal family

We continue with $n \ge 2$ written as $n = n_0 p^{r-1}$ with n_0 prime to p and $r \ge 1$. As explained in the last section, the sheaves $\mathcal{L}_{\Lambda(1-tu)}$ with Λ primitive are exactly the sheaves

$$\otimes_m \mathcal{L}_{\psi_{\ell(m,n)}(a(m)(t^m,0's))}$$

for which the Witt vector $a(n_0) \in W_{\ell(n_0,n)}(k) = W_r(k)$ has its initial component $a(n_0)_0 \in k^\times$. Let us denote by

$$W_r^\times \subset W_r$$

the open subscheme of W_r defined by the condition that the initial component a_0 be invertible.

Inside the product space $\prod_{m\geq 1 \text{ prime to } p,\ m\leq n} W_{\ell(m,n)}$, let us denote by

$$Prim_n \subset \prod_{m\geq 1 \text{ prime to } p,\ m\leq n} W_{\ell(m,n)}$$

the open set defined by the condition that the n_0 component lie in $W_r^\times$. Then on the space $\mathbb{A}^1 \times_k Prim_n$, with coordinates $(t, (a(m)_m)$, we have the lisse rank one sheaf

$$\mathcal{L}_{univ} := \otimes_m \mathcal{L}_{\psi_{\ell(m,n)}(a(m)(t^m, 0's))}.$$

We now apply cohomological techniques. Pick a prime number $\ell \neq p$ and an embedding of $\mathbb{Q}(\mu_{p^\infty})$ into $\overline{\mathbb{Q}_\ell}$. Extending scalars from $\mathbb{Q}(\mu_{p^\infty})$ to $\overline{\mathbb{Q}_\ell}$, our sheaf $\mathcal{L}_{univ}$ on $\mathbb{A}^1 \times_k Prim_n$ becomes a lisse $\overline{\mathbb{Q}_\ell}$-sheaf on that space. Denoting by

$$pr_2 : \mathbb{A}^1 \times_k Prim_n \to Prim_n,$$

the projection onto the second factor, we form the sheaf

$$L_{univ} := R^1(pr_2)_!(\mathcal{L}_{univ})$$

on $Prim_n$.

Lemma 4.1. *The sheaf L_{univ} on $Prim_n$ is lisse of rank $n-1$ and pure of weight one. For $i \neq 1$, the sheaf $R^i(pr_2)_!(\mathcal{L}_{univ})$ vanishes. For E/k a finite extension, and $((a(m))_m \in Prim_n(E)$, with $\Lambda_{((a(m))_m}$ the corresponding character of $BigWitt_n(E)$, we have*

$$\det(1 - TFrob_{E,((a(m))_m)}|L_{univ}) =$$

$$\det(1 - TFrob_E, H^1_c(\mathbb{A}^1 \otimes_k \overline{k}, \mathcal{L}_{\Lambda_{((a(m))_m}(1-tu)})) =$$

$$= L(\mathbb{A}^1/E, \Lambda_{((a(m))_m})(T).$$

Proof. On each geometric fibre of $\mathbb{A}^1 \times_k Prim_n$ over $Prim_n$, $\mathcal{L}_{univ}$ is lisse of rank one, pure of weight zero, and has $Swan_\infty = n$. So fibre by fibre, the only possibly nonvanishing H^i_c is H^1_c, and that has constant rank $n-1$. By Deligne's semicontinuity theorem [Lau-SCCS, 2.1.2], the sheaf L_{univ} is lisse. By proper base change, the $R^i(pr_2)_!(\mathcal{L}_{univ})$ vanish for $i \neq 1$, and the stalks of L_{univ} are as asserted. That the lisse sheaf L_{univ} is pure of weight one is checked fibre by fibre, where it goes back to Weil, cf. [Weil, page 82]. □

5. The monodromy of the universal family: the target theorem

We will show that, with two exceptions (namely $p = 2, 5$ and $n = 3$), the geometric monodromy group G_{geom} of the lisse sheaf L_{univ} on $Prim_n$ contains $SL(n-1)$. The case $n = 2$ has no content, any subgroup of $GL(1)$ contains $SL(1)$.

Theorem 5.1. *Let p be a prime, and $n \geq 3$. Then G_{geom} contains $SL(n-1)$ except in the cases $(p = 5, n = 3)$ and $(p = 2, n = 3)$. In the case $(p = 5, n = 3)$, G_{geom} is finite*[3].

6. Preliminaries for the proof of the target theorem

Recall that a polynomial $f(T) = \sum_i a_i T^i \in k[T]$ is said to be Artin-Schreier reduced if $a_i = 0$ for each index i such that $p|i$.

Lemma 6.1. *Given $n \geq 2$, a nontrivial additive character ψ of k, and an Artin-Schreier reduced polynomial $f(T) = \sum_m a_m T^m \in k[T]$ with $deg(f) \leq n$, there exists a character Λ_f of $BigWitt(k)$ of order p such that the lisse sheaf $\mathcal{L}_{\Lambda(1-tu)}$ on $\mathbb{A}^1/k$ is isomorphic to the Artin-Schreier sheaf $\mathcal{L}_{\psi(f(t))}$.*

Proof. For each $m \leq n$ which is prime to p, $BigWitt_n$ has a factor $W_{\ell(m,n)}$ in which $1 - tX$ projects to $(t^m, 0'\mathrm{s})$, and this in turn projects onto a factor W_1 in which $1 - tX$ projects onto t^m. Thus $BigWitt_n$ has a quotient $\prod_{m \leq n \text{ prime to } p} W_1$, and the image of $1 - tX$ in this quotient is the tuple $(x^m)_m$. The character of $\prod_{m \leq n \text{ prime to } p} W_1(k)$ given by

$$(c_m)_m \mapsto \psi(\sum a_m c_m)$$

is the desired Λ_f. □

Corollary 6.2. *For any polynomial $f(t) = \sum_i a_i T^i \in k[T]$ with $deg(f) \leq n$ and $f(0) \neq 0$, there exists a character Λ_f of $BigWitt(k)$ of order p such that the lisse sheaf $\mathcal{L}_{\Lambda(1-tu)}$ on $\mathbb{A}^1/k$ is isomorphic to the Artin-Schreier sheaf $\mathcal{L}_{\psi(f(t))}$.*

Proof. Replace f by the Artin-Schreier reduced polynomial f^{red} to which it is Artin-Schreier equivalent. Then the sheaves $\mathcal{L}_{\psi(f(t))}$ and $\mathcal{L}_{\psi(f^{red}(t))}$ on $\mathbb{A}^1/k$ are isomorphic, and we apply the previous lemma. Concretely, we take Λ_f to be the $\Lambda_{f^{red}}$ of the previous lemma. □

[3] We suspect that it is also finite in the $(p = 2, n = 3)$ case, but have not proved this.

Remark 6.3. If $p > n$, then $BigWitt_n$ is just the n-fold self product of W_1's, and so the sheaves $\mathcal{L}_{\Lambda(1-tu)}$ on A^1/k are exactly the Artin-Schreier sheaves $\mathcal{L}_{\psi(f(t))}$ for variable polynomials $f(T) = \sum_i a_i T^i \in k[T]$ with $deg(f) \leq n$ and $f(0) \neq 0$. The Swan conductor here is just $deg(f)$. [Of course one does not need the general decomposition of $BigWitt_n$ as a product of W_r's to see this. One can simply use the truncated logarithm $\log_n(1-Z) := -\sum_{j=1}^{n} Z^n/n \bmod T^{n+1}$ to provide a group isomorphism from $BigWitt_n$ to the additive group of polynomials in one variable X of degree at most n with vanishing constant term. Using this isomorphism, $1-tX$ maps to the polynomial whose coefficients are $(-t, t^2/2, ..., -t^n/n)$.]

We next recall the simplest case of the calculation of moments, cf. [Ka-LFM, Interlude: The Idea Behind the Calculation, page 115]. Recall that for V a finite dimensional $\overline{\mathbb{Q}_\ell}$-vector space of dimension $dim(V) \geq 1$, $G \subset GL(V)$ a Zariski closed reductive subgroup, and $2d \geq 2$ an even integer, we define the $2d$'th moment $M_{2d}(G,V)$ to be the dimension of the space of G-invariants (or of G-coinvariants, given that G is reductive) in $V^{\otimes d} \otimes (V^{dual})^{\otimes d}$.

When we are given a lisse sheaf $\mathcal{F}$ which is pure of some weight on a smooth, geometrically connected scheme X/k , then by Deligne [De-Weil II, 3.4.1(iii) and 1.3.9], $\mathcal{F}$ as a representation of $\pi_1^{geom}(X, \overline{\eta})$ is completely reducible, and $G_{geom} :=$ the Zariski closure of $\pi_1^{geom}(X, \overline{\eta})$ in $GL(\mathcal{F}_{\overline{\eta}})$ is semisimple (i.e., G^0_{geom} is a connected semisimple algebraic group over $\overline{\mathbb{Q}_\ell}$). So we may speak of the moments $M_{2d}(G_{geom}, \mathcal{F}_{\overline{\eta}})$, which we will denote simply

$$M_{2d}(\mathcal{F}) := M_{2d}(G_{geom}, \mathcal{F}_{\overline{\eta}}).$$

Lemma 6.4. *Let $\mathcal{L}$ be a lisse, rank one $\overline{\mathbb{Q}_\ell}$-sheaf on $\mathbb{A}^1/k$ which is pure of weight zero, with $Swan_\infty(\mathcal{L}) = n \geq 2$. Given an integer d with $1 \leq d < n$, form its "naive degree d Fourier transform" $NFT_d(\mathcal{L})$, i.e., the lisse sheaf $NFT_d(\mathcal{L})$ on $\mathbb{A}^d/k$ with coordinates $(a_1, ..., a_d)$ defined as follows. On $\mathbb{A}^1 \times_k \mathbb{A}^d$, with coordinates $(t, a_1, ..., a_d)$ we have the lisse rank one sheaf $\mathcal{L} \otimes \mathcal{L}_{\psi(\sum_i a_i t^i)}$. We define*

$$NFT_d(\mathcal{L}) := R^1(pr_2)_!(\mathcal{L} \otimes \mathcal{L}_{\psi(\sum_i a_i t^i)}).$$

Then we have the following results.

1. *The sheaf $NFT_d(\mathcal{L})$ is lisse of rank $n-1$ and pure of weight one on $\mathbb{A}^d/k$, and the $R^1(pr_2)_!(\mathcal{L} \otimes \mathcal{L}_{\psi(\sum_i a_i t^i)})$ vanish for $i \neq 1$.*
2. *If $d < p$, then $M_{2d}(NFT_d(\mathcal{L})) = d!$.*

Proof. Because $d < n$, on each geometric fibre the sheaf $\mathcal{L} \otimes \mathcal{L}_{\psi(\sum_i a_i t^i)})$ has constant $Swan_\infty = n > 0$, so an H^1_c of dimension $n-1$, and all other H^i_c vanishing. Each H^1_c is pure of weight one, by Weil (using the fact that, up to a constant field twist, a lisse rank one $\mathcal{L}$ is of finite order).So assertion (1) results from Deligne's semicontinuity theorem [Lau-SCCS, 2.1.2] and proper base change. For the second assertion, we argue as follows. For

$$\mathcal{G} := NFT_d(\mathcal{L}),$$

its M_{2d} is the dimension of $H^{2d}_c(\mathbb{A}^d \otimes_k \overline{k}, \mathcal{G}^{\otimes d} \otimes \overline{\mathcal{G}}^{\otimes d})$, where we have written $\overline{\mathcal{G}}$ for the complex conjugate $\mathcal{G}^{dual}(-1)$ of $\mathcal{G}$. The sheaf $\mathcal{G}$ is pure of weight one, so $\mathcal{G}^{\otimes d} \otimes \overline{\mathcal{G}}^{\otimes d}$ is pure of weight $2d$, and so the group H^{2d}_c is pure of weight $4d$. The groups H^i_c with $i < 2d$ are of lower weight, so we recover

$$M_{2d}(\mathcal{G}) = \dim(H^{2d}_c(\mathbb{A}^d \otimes_k \overline{k}, \mathcal{G}^{\otimes d} \otimes \overline{\mathcal{G}}^{\otimes d})) =$$

$$= \limsup_{E/k \text{ finiteextn}} (1/\#E)^{2d} |\mathrm{Trace}(Frob_E|H^{2d}_c)| =$$

$$= \limsup_{E/k \text{ finiteextn}} (1/\#E)^{2d} |\sum_i (-1)^i \mathrm{Trace}(Frob_E|H^i_c)| =$$

$$= \limsup_{E/k \text{ finiteextn}} (1/\#E)^{2d} |\sum_{f \in \mathbb{A}^d(E)} \mathrm{Trace}(Frob_{E,f}|(\mathcal{G}^{\otimes d} \otimes \overline{\mathcal{G}}^{\otimes d}))|,$$

the last equality by the Lefschetz trace formula.

The sum $\sum_{f \in \mathbb{A}^d(E)} \mathrm{Trace}(Frob_{E,f}|(\mathcal{G}^{\otimes d} \otimes \overline{\mathcal{G}}^{\otimes d}))$ is explicitly

$$\sum_{(a_1,\ldots,a_d) \in \mathbb{A}^d(E)} |\mathrm{Trace}(Frob_{E,f}|\mathcal{G})|^{2d}.$$

Each inner summand $|\mathrm{Trace}(Frob_{E,f}|\mathcal{G})|^{2d}$ is

$$(\sum_{t \in E}(Frob_{E,t}|\mathcal{L})\psi_E(\sum_i a_i t^i))^d (\sum_{t \in E}(\overline{Frob_{E,t}|\mathcal{L}})\psi_E(-\sum_i a_i t^i))^d.$$

If we write

$$\mathcal{L}(E,t) := Frob_{E,t}|\mathcal{L}, \quad f(t) := \sum_{i=1}^d a_i t^i,$$

then expanding the d'th powers by writing each factor d times, this inner summand is

$$\sum_{(t_1,\ldots,t_d,s_1,\ldots,s_d) \in \mathbb{A}^{2d}(E)} (\prod_{i=1}^d \mathcal{L}(E,t_i))(\prod_{j=1}^d \overline{\mathcal{L}(E,s_j)})\psi_E(\sum_{i=1}^d f(t_i) - \sum_{j=1}^d f(s_j)).$$

If we now sum over all $f(t) := \sum_{i=1}^{d} a_i t^i$ and interchange the order of summation, the innermost sum becomes

$$\sum_{(a_1,...,a_d)\in A^d(E)} \psi(a_1(\sum_{i=1}^{d} t_i - \sum_{j=1}^{d} s_j) + ... + a_d(\sum_{i=1}^{d} t_i^d - \sum_{j=1}^{d} s_j^d)).$$

This sum vanishes unless $(t_1, ..., t_d)$ and $(s_1, .., s_d) \in \mathbb{A}^d(E)$ have the same first d Newton symmetric functions as each other, in which case the sum is $\mathbb{E}^d$. Because we assumed $d < p$, having the same first d Newton symmetric functions is equivalent to having the same first d elementary symmetric functions. So the sum vanishes unlesss the two d-tuples $(t_1, ..., t_d)$ and $(s_1, .., s_d) \in \mathbb{A}^d(E)$ are permutations of each other. For such a pair of d-tuples, the expression $(\prod_{i=1}^{d} \mathcal{L}(E, t_i))(\prod_{j=1}^{d} \overline{\mathcal{L}(E, s_j)})$ is identically 1.

So the sum $\sum_{f\in\mathbb{A}^d(E)} \mathrm{Trace}(Frob_{E,f}|(\mathcal{G}^{\otimes d} \otimes \overline{\mathcal{G}}^{\otimes d}))$ is equal to

$$(\#E^d) \sum_{(t_1,...,t_d),(s_1,..,s_d)\in\mathbb{A}^d(E) \text{ permutations of each other}} 1.$$

For each of the $(\#E)(\#E - 1)..(\#E - (d - 1)) = \#E^d + O(\#E^{d-1})$ d-tuples with all distinct components, there are exactly $d!$ partner $(s_1, ..., s_d)$ tuples which are permuations. So this entire sum is equal to

$$d!\#E^{2d} + O(\#E^{2d-1}).$$

Dividing this sum by $\#E^{2d}$, the lim sup formula gives the asserted value $d!$ for the $2d$'th moment. □

We now combine this moment calculation with Larsen's Alternative and the truth, due to Guralnick and Tiep, of Larsen's Eighth Moment Conjecture. Let us recall the relevant parts of those results, cf. [Ka-LFM, page 113] and [G-T, Thm. 1.4]

Theorem 6.5. *Let V be a finite dimensional $\overline{\mathbb{Q}_\ell}$-vector space of dimension $dim(V) \geq 1$, $G \subset GL(V)$ a Zariski closed reductive subgroup. Then we have the following results.*

(1) *(***Larsen's Alternative, for** *SL) If $M_4(G, V) = 2$, then either G is finite or $SL(V) \subset G$.*
(2) *(***Larsen's Eighth Moment Conjecture, for** *SL) If $M_8(G, V) = 4!$, and $\dim(V) \geq 5$ then $SL(V) \subset G$.*

Using the truth of Larsen's Eighth Moment Conjecture, we get the following lemma.

Corollary 6.6. *Let $\mathcal{L}$ be a lisse, rank one $\overline{\mathbb{Q}_\ell}$-sheaf on $\mathbb{A}^1/k$ which is pure of weight zero, with $Swan_\infty(\mathcal{L}) = n \geq 2$. If $p \geq 5$ and $n \geq 6$, then G_{geom} for $NFT_4(\mathcal{L})$ contains $SL(n-1)$.*

Using Larsen's Alternative, we get the following lemma.

Corollary 6.7. *Let $\mathcal{L}$ be a lisse, rank one $\overline{\mathbb{Q}_\ell}$-sheaf on $\mathbb{A}^1/k$ which is pure of weight zero, with $Swan_\infty(\mathcal{L}) = n \geq 3$. If $p \geq 3$ and $n \geq 3$, then G_{geom} for $NFT_2(\mathcal{L})$ is either finite or contains $SL(n-1)$.*

What about the case $p = 2$? Here we must use NFT_3 to get information about the fourth moment.

Lemma 6.8. *Let k be a finite field of characteristic $p = 2$, and $\mathcal{L}$ a lisse, rank one $\overline{\mathbb{Q}_\ell}$-sheaf on $\mathbb{A}^1/k$ which is pure of weight zero, with $Swan_\infty(\mathcal{L}) = n \geq 4$. Suppose that the function on $\mathbb{A}^1(k)$ given by $t \mapsto (\mathrm{Trace} Frob_{k,t}|\mathcal{L})^2 = \mathrm{Trace} Frob_{k,t}|\mathcal{L}^{\otimes 2}$ is not constant. Then $NFT_3(\mathcal{L})$ has fourth moment $M_4 = 2$, and consequently G_{geom} for $NFT_2(\mathcal{L})$ is either finite or contains $SL(n-1)$.*

Proof. As explained in [Ka-LFM, pp. 118-119], we will get $M_4 = 2$ provided that the input $\mathcal{L}$ is not geometrically self dual. If $\mathcal{L}$ were geometrically self dual, its autoduality would be orthogonal, since $\mathcal{L}$ is geometrically irreducible of odd rank (namely 1). But the orthogonal group $O(1)$ is ± 1, so $\mathcal{L}^{\otimes 2}$ would be geometrically constant, i.e., of the form α^{deg} for some $\alpha \in \overline{\mathbb{Q}_\ell}^\times$. In particular, its trace function would be constant on $\mathbb{A}^1(k)$. □

7. Proof of the target theorem

Let us recall its statement.

Theorem 7.1. *(***restatement of Thm. 5.1***) Let p be a prime, and $n \geq 3$. Then G_{geom} contains $SL(n-1)$ except in the cases $(p = 5, n = 3)$ and $(p = 2, n = 3)$. In the case $(p = 5, n = 3)$, G_{geom} is finite.*

Proof. Suppose first that $p \geq 5$, and $n \geq 6$. Choose a primitive character Λ of $BigWitt(\mathbb{F}_p)$. Then $\mathcal{L} := \mathcal{L}_{\Lambda((1-tu)}$ has $Swan_\infty = n$. Because $n > 4$ and $p > 4$, we can form $NFT_4(\mathcal{L})$, which has $M_8 = 4!$. From Theorem 6.5, part (1), we get that its G_{geom} contains $SL(n-1)$. But this $NFT_4(\mathcal{L})$ on its $\mathbb{A}^4$ is a pullback of L_{univ} to on $Prim_n$. [The point is that for $f(t) \in k[t]$ a polynomial of degree at most 4, and Λ a primitive character, the sheaf $\mathcal{L}_{\psi(f(t))}$ itself of the form $\mathcal{L}_{\Lambda_f(1-tu)}$ for a characterΛ_f of $BigWitt_n(k)$ of conductor $deg(f) \leq 4$. So the tensor product sheaf $\mathcal{L}_{\Lambda((1-tu)} \otimes \mathcal{L}_{\psi(f(t))}$ is of the form $\mathcal{L}_{\Lambda_1(1-tu)}$ for the primitive character $\Lambda_1 := \Lambda\Lambda_f$ of $BigWitt_n(k)$. This construction $f \mapsto \Lambda\Lambda_f$

gives an embedding of $\mathbb{A}^4$ into $Prim_n$ such that the pullback of L_{univ} is $NFT_4(\mathcal{L})$.] Since G_{geom} can only decrease under pullback, we conclude that G_{geom} for L_{univ} must contain $SL(n-1)$.

If $p \geq 7$, we treat the cases $3 \leq n \leq 6$ as follows. In these $n < p$ cases, the primitive Λ's give rise exactly to the sheaves $\mathcal{L}_{\psi(f(t))}$ with $f(t)$ a varying polynomial, with zero constant term, of the imposed degree n. In this case, we are dealing with the one-variable case of the universal family of "Deligne polynomials", albeit with vanishing constant term, and the result here is [Ka-MMP, 3.8.2, 3(a)]. [In the reference cited, the Deligne polynomials are allowed constant terms a_0, but the effect of this on the output sheaf on the space of coefficients is to tensor with the rank one sheaf $\mathcal{L}_{\psi(a_0)}$, an operation which does not change the question of whether or not G_{geom} contains $SL(n-1)$.]

For $p = 5$, we deal with the case $n = 4$ the same way, now appealing to [Ka-MMP, 3.8.2, 3(c)]. Still with $p = 5$, we attack the case $n = 3$ the same way, but now the fact that all curves $y^5 - y = f_3(x)$ with f_3 a cubic are supersingular in characteristic 5 shows that we have a finite G_{geom} in this $(p = 5, n = 3)$ case.

We still need to treat the case $p = n = 5$, and we need to treat all cases $n \geq 3$ with $p = 3$. We also need to treat the case $p = 2$, all $n \geq 4$.

For $p \geq 3$ and $n \geq 3$, we can perform a similar pullback argument with NFT_2, whose M_4 will be 2. But here the conclusion will only be that whenever we pull back L_{univ} to certain $\mathbb{A}^2$'s, the pullback has a G_{geom} which is either finite or contains $SL(n-1)$. To get around this difficulty, we will show that, both for $p = 5$ and $n = 5$, and for $p = 3$ and any $n \geq 3$, we can choose a particular primitive character Λ of $BigWitt(\mathbb{F}_p)$ whose associated $\mathcal{L} := \mathcal{L}_{\Lambda((1-tu)}$ has an $NFT_2(\mathcal{L})$ which is **not** finite (and hence must contain $SL(n-1)$, by Larsen's Alternative).

We will do this by making use of the diophantine criterion [Ka-ESDE, 8.14.3] for the finiteness of G_{geom}, applied to an $NFT_2(\mathcal{L})$ sheaf on $\mathbb{A}^2$ with coordinates (a_1, a_2). This sheaf is geometrically irreducible, because its restriction to the line $a_2 = 0$ it is geometrically irreducible, being the $NFT_1(\mathcal{L})$, the usual Fourier transform of the geometrically irreducible input $\mathcal{L}$. Its determinant $\det(NFT_2(\mathcal{L}))$ is lisse of rank one and pure of weight $n-1$ (simply because $NFT_2(\mathcal{L})$ is pure of weight one and lisse of rank $n-1$). According to [Ka-ESDE, 8.14.3], if G_{geom} for $NFT_2(\mathcal{L})$ is finite, then for any finite extension $E/\mathbb{F}_p$ and for any point $f \in \mathbb{A}^2(E)$, some power of $Frob_{E,f}|NFT_2(\mathcal{L})$ is a scalar. In particular, taking $E = \mathbb{F}_p$ and f the origin, some power of $Frob_{\mathbb{F}_p}$ on $H^1_c(\mathbb{A}^1 \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}, \mathcal{L})$ is a scalar. That scalar must then be of the form (a root of unity) × (an $n-1$'th root of $\det(Frob_{\mathbb{F}_p}|H^1_c(\mathbb{A}^1 \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}, \mathcal{L})))$.

Choose a nontrivial additive character ψ of $\mathbb{F}_p$, and denote by $g(\psi, \chi_2)$ the quadratic gauss sum. We claim that

$$\det(Frob_{\mathbb{F}_p}|H^1_c(\mathbb{A}^1 \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}, \mathcal{L})) = (\text{a root of unity})g(\psi, \chi_2)^{n-1}.$$

To see this, notice that the L-function of $\mathcal{L}$ as a polynomial has coefficients in the cyclotomic integer ring $\mathbb{Z}[\zeta_{p^t}]$, for p^t the order of Λ. So the determinant, being ± the leading coefficient of the L-function, lies in this ring. By Weil, all of its complex absolute values are $p^{(n-1)/2}$. But in the cyclotomic field $\mathbb{Q}[\zeta_{p^t}]$, there is only one place over the prime p. So for any integer $d \geq 0$, the only elements $\alpha \in \mathbb{Z}[\zeta_{p^t}]$ all of whose complex absolute values are $p^{d/2}$ are of the form (a root of unity in $\mathbb{Z}[\zeta_{p^t}]) \times g(\psi, \chi_2)^d$. [For such an α, $\alpha\overline{\alpha}$ must be p^d. Hence α is a unit at all finite places not over p. The ratio $\alpha/g(\psi, \chi_2)^d$ lies in $\mathbb{Q}[\zeta_{p^t}]$, is integral outside of (the unique place lying over) p, and has absolute value 1 at all places. By the product formula, this ratio is a unit at p as well, so is a root of unity.]

So what we find is that if G_{geom} for $NFT_2(\mathcal{L})$ is finite, then every eigenvalue of $Frob_{\mathbb{F}_p}$ on $H^1_c(\mathbb{A}^1 \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}, \mathcal{L})$ is of the form (a root of unity)$g(\psi, \chi_2)$. In particular, (minus) the sum of these eigenvalues, namely

$$\text{Trace}(Frob_{\mathbb{F}_p}|H^1_c(\mathbb{A}^1 \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}, \mathcal{L}) = -\sum_{t \in \mathbb{F}_p} \Lambda(1 - tX),$$

is an algebraic integer (in fact an element of $\mathbb{Z}[\zeta_{p^t}]$) divisible (as an algebraic integer, or equivalently as an element of $\mathbb{Z}[\zeta_{p^t}]$) by $g(\psi, \chi_2)$.

Let us denote by ord_p the p-adic valuation of $\mathbb{Q}\zeta_{p^t}]$ normalized by $ord_p(p) = 1$. Then $ord_p(g(\psi, \chi_2)) = 1/2$ (since $g(\psi, \chi_2)^2 = \pm p$). So the upshot is that if we produce a primitive character Λ of $BigWitt(\mathbb{F}_p)$ for which the sum $\sum_{t \in \mathbb{F}_p} \Lambda(1 - tX)$ has $ord_p < 1/2$, then $NFT_2(\mathcal{L})$ does not have finite G_{geom}.

We first treat the cases $p = 3$ for all $n \geq 3$, and the case $p = 5 = n$. These are both covered by the following lemma.

Lemma 7.2. *Suppose $n \geq p$. Then there exist primitive characters Λ of $BigWitt_n(\mathbb{F}_p)$ for which the sum $\sum_{t \in \mathbb{F}_p} \Lambda(1 - tX)$ has $ord_p \leq 1/p$.*

Proof. We first treat the case when n is divisible by p, say $n = mp^r$ with $m \geq 1$ prime to p and $r \geq 1$. Then $W_{r+1}(\mathbb{F}_p) \cong \mathbb{Z}/p^{r+1}$ is a quotient of $BigWitt_n(\mathbb{F}_p)$ The image of $1 - tX$ in this quotient is the Witt vector $(t^m, 0, ..., 0)$, which is the reduction mod p^{r+1} of the Teichmuller representative $Teich(t^m) \in \mathbb{Z}_p$ of $t^m \in \mathbb{F}_p$. Pick a primitive p^{r+1}'st root of unity ζ_{r+1}. Then $x \mapsto \zeta_{r+1}^x$ is a faithful character of $\mathbb{Z}/p^{r+1}$. Via the isomorphism $W_{r+1}(\mathbb{F}_p) \cong \mathbb{Z}/p^{r+1}$, it becomes a faithful character Λ of $W_{r+1}(\mathbb{F}_p)$. Composing with the projection of $BigWitt_n(\mathbb{F}_p)$ onto $W_{r+1}(\mathbb{F}_p)$, it becomes a primitive character Λ of $BigWitt_n(\mathbb{F}_p)$, for which we have the formula

$$\Lambda(1 - tX) = \zeta_{p^{r+1}}^{Teich(t^m)} \text{ for } t \in \mathbb{F}_p.$$

Now define

$$\pi_{p^{r+1}} := \zeta_{p^{r+1}} - 1.$$

One knows that $\pi_{p^{r+1}}$ has $ord_p(\pi_{p^{r+1}}) = \frac{1}{p^r(p-1)}$. So the sum in question may be written

$$\sum_{t \in \mathbb{F}_p} \Lambda(1 - tX) = \sum_{t \in \mathbb{F}_p} (1 + \pi_{p^{r+1}})^{Teich(t^m)}.$$

We now expand each summand by the binomial theorem. Our sum becomes

$$p + \sum_{i \geq 1} (\pi_{p^{r+1}})^i \sum_{t \in \mathbb{F}_p} Binom(Teich(t^m), i).$$

Work now in the ring $\mathbb{Z}[\zeta_{p^t}]/(\pi_{p^{r+1}}^p)$. In this quotient, our sum becomes

$$\sum_{i=1}^{p-1} (\pi_{p^{r+1}})^i \sum_{t \in \mathbb{F}_p} Binom(Teich(t^m), i).$$

The coefficients $Binom(Teich(t^m), i)$ only matter mod p, and as $i < p$ their value mod p depends only on t^m mod p. So in this quotient ring our sum is

$$\sum_{i=1}^{p-1} (\pi_{p^{r+1}})^i \sum_{t \in \mathbb{F}_p} Binom(t^m, i).$$

Let d be the least integer $d \geq 1$ such that $md \equiv 0 \bmod p-1$. [Notice that in any case we have $d \leq p - 1$.] We claim that

$$\sum_{t \in \mathbb{F}_p} Binom(t^m, i) = 0 \in \mathbb{F}_p \text{ for } 1 \leq i < d,$$

but

$$\sum_{t \in \mathbb{F}_p} Binom(t^m, d) \neq 0 \in \mathbb{F}_p.$$

Because $m \geq 1$ and $i \geq 1$, these sums vanish for $t = 0$. Expand the binomial coefficient $Binom(t^m, i)$ as a polynomial in t^m,

$$Binom(t^m, i) = t^{mi}/i! + \text{lower terms in } t^m, \text{ vanishing constant term.}$$

For an integer $j \geq 1$, we have $\sum_{t \in \mathbb{F}_p^\times} t^k = 0 \in \mathbb{F}_p$ unless $k \equiv 0 \mod p-1$, in which case $\sum_{t \in \mathbb{F}_p^\times} t^k = -1 \in \mathbb{F}_p$. Therefore for $1 \leq i < d$, we have

$$\sum_{t \in \mathbb{F}_p} Binom(t^m, i) = 0 \in \mathbb{F}_p,$$

while for $i = d$ we have

$$\sum_{t \in \mathbb{F}_p} Binom(t^m, d) = -1/d! \neq 0 \in \mathbb{F}_p.$$

The conclusion is that our character sum

$$\sum_{t \in \mathbb{F}_p} \Lambda(1 - tX) = \sum_{t \in \mathbb{F}_p} (1 + \pi_{p^{r+1}})^{Teich(t^m)}$$

has $ord_p = d/(p^r(p-1)) \leq 1/p^r \leq 1/p$, as required. This concludes the proof in the case when n is divisible by p.

We now treat the case when $n \geq p \geq 3$ but n is prime to p. Because $n \geq p$, the highest power of p which is $\leq n$ is pr for some $r \geq 1$. In this case, $BigWitt_n(\mathbb{F}_p)$ has both $W_1(\mathbb{F}_p)$ as a quotient, where $1 - tX$ maps to $t^n \in \mathbb{F}_p = W_1(\mathbb{F}_p)$, and a quotient $W_{r+1}(\mathbb{F}_p)$, where $1 - tX$ maps to $(t, 0, ..., 0)$. Take both a nontrivial additive character ψ of $\mathbb{F}_p$, and a faithful character of $\mathbb{Z}/p^{r+1}$. The first gives a primitive character whose value on $1 - tX, t \in \mathbb{F}_p$, is $\psi(t)$, and the second gives a nonprimitive character whose value on $1 - tX, t \in \mathbb{F}_p$ is $\zeta_{p^{r+1}}^{Teich(t^m)}$. The product of these two characters is a primitive character, whose value on $1 - tX, t \in \mathbb{F}_p$ is $\psi(t^m)\zeta_{p^{r+1}}^{Teich(t^m)}$. Because $r \geq 1$,while ψ has values in $1 + (\pi_p)$, the values of ψ are 1 in the quotient ring $\mathbb{Z}[\zeta_{p^t}]/(\pi_{p^{r+1}}^p)$. So in that quotient ring, we are dealing with the sum we treated in the case $n = p^r$, and hence our sum has $ord_p = 1/p^r$. □

Here is the variant we need for the case $p = 2$ (taking $r = 2$ then).

Lemma 7.3. *Suppose $r \geq 1$ and $n \geq p^r$. Then there exist primitive characters Λ of $BigWitt_n(\mathbb{F}_p)$ for which the sum $\sum_{t \in \mathbb{F}_p} \Lambda(1 - tX)$ has $ord_p \leq 1/p^r$.*

Proof. If $p^r | n$, proceed as in the $p|n$ case of the previous lemma. If not, proceed as in the second case. □

Corollary 7.4. *Suppose $p = 2$, $r = 2$, and $n \geq 4$. For any primitive character Λ of $BigWitt_n(\mathbb{F}_2)$ for which the sum $\sum_{t \in \mathbb{F}_p} \Lambda(1 - tX)$ has $ord_p \leq 1/p^r = 1/4$, the associated lisse rank one sheaf $\mathcal{L} := \mathcal{L}_{\Lambda(1-tX)}$ is not geometrically self dual, and its $NFT_3(\mathcal{L})$ has G_{geom} containing $SL(n-1)$.*

Proof. At $t = 0$, we have $\Lambda(1 - tX) = \Lambda(1) = 1$. If $\Lambda(1 - X)$ were ± 1, the sum $\sum_{t \in \mathbb{F}_p} \Lambda(1 - tX)$ would be either 2 or 0, neither of which has $ord_2 \leq 1/4$. Lemma 6.8 then tells us that its $NFT_3(\mathcal{L})$ has $M_4 = 2$, and the diophantine criterion □

Putting together these ingredients, we have produced, for any $n \geq 3$ and any p, with the exception of the two cases $n = 3$ and $p = 2, 5$, an $\mathcal{L}$ whose $NFT_2(\mathcal{L})$ (for odd p), respectively whose $NFT_3(\mathcal{L})$ (for $p = 2$) has a G_{geom} containing $SL(n-1)$. So in all the asserted cases, the G_{geom} for L_{univ} on $Prim_n$ has a G_{geom} containing $SL(n-1)$. □

8. Applying the target theorem to prove Theorem 1.2

Fix a prime p, and an $n \geq 3$. If p is 2 or 5, take $n \geq 4$. Then we know that L_{univ} on $Prim_n/\mathbb{F}_p$ has its G_{geom} containing $SL(n-1)$. If we take the Tate-twisted unitarized sheaf $L_{univ}(1/2)$, whose Frobenii give the conjugacy classes $\theta_{k,\Lambda}$ which are the subject of Theorem 1.2, it has the same G_{geom}, and for it we have a priori inclusions

$$SL(n-1) \subset G_{geom} \subset G_{arith} \subset GL(n-1).$$

Consequently, G_{geom} and G_{arith} have the **same** image in $PGL(n-1)$. So by Deligne's general equidistribution theorem, cf. [De-Weil II, 3.5.3], [Ka-Sar, 9.2.6], we get the following equicharacteristic version of Theorem 1.2.

Theorem 8.1. *Fix a prime p, and an $n \geq 3$. If p is 2 or 5, take $n \geq 4$. In any sequence of finite extension fields k_i of $\mathbb{F}_p$ whose cardinalities q_i are archimedeanly increasing to ∞, the collections of conjugacy classes*

$$\{\theta_{k_i,\Lambda}\}_{\Lambda \text{ primitive even}}$$

become equidistributed in $PU(n-1)^{\#}$.

Let us briefly recall how the proof goes. For a fixed irreducible nontrivial representation Ξ of $PU(n-1)$, one shows that the divided Weyl sums

$$(1/\#Prim_n(k_i)) \sum_{\Lambda \in Prim_n(k_i)} \mathrm{Trace}(\Xi(\theta_{k_i,\Lambda}))$$

tend to 0 as $\#k_i$ grows, by showing that this sum is bounded in absolute value by

$$C(p, n, \Xi)/\sqrt{\#k_i}, \quad \text{for } C(p, n, \Xi) := \sum_i h_c^i(Prim_n \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}, \Xi(L_{univ}))$$

for $\Xi(L_{univ})$ the lisse sheaf on $Prim_n/\mathbb{F}_p$ formed by "pushing out" L_{univ} along the the representation Ξ, now viewed as a representation of $PGL(n-1)$.

At present, we do not know uniform bounds for these sums of Betti numbers $C(p,n,\Xi)$ as p varies (n and Ξ fixed). But we can bypass this problem, if we can, by other means, show that for fixed n and $p > 2n-1$, we have a bound of the form $D(n,\Xi)/\sqrt{\#k_i}$ with a constant $D(n,\Xi)$ which is independent of p. Then we use this constant for $p > 2n-1$, and we use the constant $C(p,n,\Xi)$ for the finitely many primes $p \le 2n-1$. We will show that in fact we can take $D(n,\Xi) := 3\dim(\Xi)/(n-1)$. This will then prove Theorem 1.2.

Theorem 8.2. *Suppose $n \ge 3$ and $p > 2n-1$. Then for any irreducible nontrivial representation Ξ of $PU(n-1)$, and any finite field k of characteristic p, we have the estimate*

$$|\sum_{\Lambda \in Prim_n(k)} \mathrm{Trace}(\Xi(\theta_{k,\Lambda}))| \le \frac{3\dim(\Xi)\#Prim_n(k)}{(n-1)\sqrt{\#k}}.$$

Proof. There are three key points here. The first is that, because $p > n$, the sheaves $\mathcal{L}_{\Lambda(1-tu)}$ attached to primitive characters Λ of $BigWitt_n(k)$ are just the Artin-Shreier sheaves $\mathcal{L}_{\psi(f(t))}$ for $f(t) \in k[t]$ a variable polynomial of degree n with vanishing constant term, cf. Remark 6.3. The second is that $NFT_1(\mathcal{L}_{\psi(f(t))})$ is lisse of rank $n-1$ and all its ∞-slopes are $n/(n-1)$. The third concerns the group G_{geom} for $NFT_1(\mathcal{L}_{\psi(f(t))})$. If either $n = 3$, or if n is even, then G_{geom} contains $SL(n-1)$. For $n \ge 5$ and odd, the situation is a bit more complicated. Unless there is some constant $c \in k$ such that $f(t+c) - f(c)$ is an odd funtion of t, G_{geom} contains $SL(n-1)$, cf. [Ka-MG, Thm. 17]. [In the theorem cited, the condition "$p > 2n+1$" there should read $pfrm{-}e(n-1)+1$, as it is $n-1$ which is the rank of the sheaf in question, and one is applying [Ka-MG, Thm. 9].]

Suppose first that $n = 3$ or n is even. Then for any irreducible nontrivial representation Ξ of $PU(n-1)$, and any polynomial $f(t) \in k[t]$ of degree n with vanishing constant term, with $\Lambda_{f(t)}$ the corresponding primitive character, $NFT_1(\mathcal{L}_{\psi(f(t))})$ has G_{geom} containing $SL(n-1)$, hence we have the estimate

$$|\sum_{a_1 \in \mathbb{A}^1(k)} \mathrm{Trace}(\Xi(\Lambda_{f(t)+a_1 t})| \le h^1_c(\mathbb{A}^1 \otimes_k \overline{k}, \Xi(NFT_1(\mathcal{L}_{\psi(f(t))})))\sqrt{\#k}.$$

The other h^i_c vanish, so the h^1_c is the absolute value of the Euler characteristic of $\mathbb{A}^1 \otimes_k \overline{k}$ with coefficients in $\Xi(NFT_1(\mathcal{L}_{\psi(f(t))})$. But (minus) this Euler characteristic is

$$-\chi = Swan_\infty(\Xi(NFT_1(\mathcal{L}_{\psi(f(t))})) - \mathrm{rank}(\Xi(NFT_1(\mathcal{L}_{\psi(f(t))})).$$

The largest ∞-slope of $\Xi(NFT_1(\mathcal{L}_{\psi(f(t))})$ is at most the largest ∞-slope of $\mathcal{L}_{\psi(f(t))}$, which is $n/(n-1)$. So we get the estimate

$$h^1_c = -\chi \le \dim(\Xi)(n/(n-1)) - \dim(\Xi) = \dim(\Xi)/(n-1).$$

So we have

$$|\sum_{a_1 \in \mathbb{A}^1(k)} \mathrm{Trace}(\Xi(\Lambda_{f(t)+a_1 t})| \le \#\mathbb{A}^1(k)(\dim(\Xi)/(n-1))/\sqrt{\#k}.$$

Breaking the $f(t)$'s into equivalence classes "agreeing except for the linear term" and summing this estimate for the $NFT_1(\mathcal{L}_{\psi(f(t))})$ of a representative of each equivalence class, we get the asserted estimate (without needing the factor 3 in this case).

Suppose now that n is odd and $n \ge 5$. In this case, over $k = \mathbb{F}_q$ we can repeat the above argument for all the$f(t)$ of degree n, of which there are $q^{n-1}(q-1)$, **except** for those of the form $f_{odd}(t+c) - f_{odd}(c)$ for some odd polynomial $f_{odd}(t)$ of degree n, the "bad" f's. There are $(q-1)q^{(n-1)/2}$ possible f_{odd}, so at most $(q-1)q^{(n+1)/2}$ bad f's. The set of bad f's (and hence also the set of good ones) are stable by $f(t) \mapsto f(t) + at$. So we repeat the argument for the good f's to get

$$|\sum_{\Lambda_f \in Prim_n(k), f \text{ good}} \mathrm{Trace}(\Xi(\theta_{k,\Lambda_f}))| \le \frac{\dim(\Xi)\#Prim_{n,\mathrm{good}}(k)}{(n-1)\sqrt{\#k}}.$$

For each bad f, we use the trivial bound

$$|\mathrm{Trace}(\Xi(\theta_{k,\Lambda_f}))| \le \dim(\Xi).$$

So we get

$$|\sum_{\Lambda_f \in Prim_n(k), f \text{ bad}} \mathrm{Trace}(\Xi(\theta_{k,\Lambda_f}))| \le \dim(\Xi)\#Prim_{n,\mathrm{bad}}(k).$$

But we have the elementary estimate (remember $p \ge 2n+1$ and $n \ge 5$),

$$\#Prim_{n,\mathrm{bad}}(k) \le \frac{2\#Prim_{n,\mathrm{good}}(k)}{(n-1)\sqrt{\#k}}.$$

□

Remark 8.3. The determinant discussion which occurs in the proof of Theorem 7.1 shows that the group G_{arith} attached to the sheaf $L_{univ}(1/2)$ on $Prim_n/\mathbb{F}_p$ is constrained by an inclusion

$$G_{arith} \subset \{A \in GL(n-1) |\ \det(A)^{4p^{r+1}} = 1\}$$

for p^r the largest power of p with $p^r \leq n$. So we have a chain of inclusions

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

If it were the case that $G_{geom} = G_{arith}$, Deligne's equidistribution theorem would give us an equidistribution result for the conjugacy classes

$$\{\theta_{k_i,\Lambda}\}_{\Lambda \text{ primitive even}}$$

now seen as conjugacy classes in a compact form of this group $G_{geom} = G_{arith}$. It is because we do not know whether or not the equality $G_{geom} = G_{arith}$[4] holds that we project onto $PGL(n-1)$, where the equality does hold, and whose compact form is $PU(n-1)$.

References

[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.

[Bry] Brylinski, J.-L., Théorie du corps de classes de Kato et revêtements abéliens de surfaces. Annales de l'institut Fourier 33 (1983), n^o 3 , 23-38.

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

[G-T] Guralnick,R., and Tiep, P., Decompositions of small tensor powers and Larsen's conjecture. Represent. Theory 9 (2005), 138208 (electronic).

[Ka-CE] Katz, N., Convolution and Equidistribution: Sato-Tate Theorems for Finite-Field Mellin Transforms. Annals of Mathematics Studies, 180. Princeton Univ. Press, Princeton, NJ, 2012.

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

[Ka-LFM] Katz, N., L-functions and monodromy: four lectures on Weil II. Adv. Math. 160 (2001), no. 1, 81132.

[Ka-MG] Katz, N., On the monodromy groups attached to certain families of exponential sums. Duke Math. J. 54 (1987), no. 1, 4156.

[Ka-MMP] Katz, N., Moments, monodromy, and perversity: a Diophantine perspective. Annals of Mathematics Studies, 159. Princeton University Press, Princeton, NJ, 2005. viii+475 pp.

[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.

[Ka-TLFM] Katz, N., Twisted L-functions and monodromy. Annals of Math. Studies, 150. Princeton Univ. Press, Princeton, NJ,2002. viii+249 pp.

[4] Nor do we know the exact value of either of these groups!

[La] Lang, S., Algebraic Groups over Finite Fields, Am. J. Math. Vol. 78, No. 3 (Jul., 1956), pp. 555-563.

[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.

[Weil] Weil, Andé, Variétés abéliennes et courbes algébriques. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948. 165 pp.

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