# Larsen's Alternative, Moments, and the Monodromy of Lefschetz Pencils

Nicholas M. Katz

to Joe Shalika on his 60'th birthday

## Introduction

We work over an algebraically closed field "$\mathbb{C}$" of characteristic zero. Let V be a $\mathbb{C}$-vector space of dimension $N \geq 2$. We fix a (not necessarily connected) Zariski closed subgroup $G \subset GL(V)$ which is reductive (i.e., every finite-dimensional representation of G is completely reducible). We are interested in criteria which guarantee that G is one of the standard classical groups, i.e. that either G is caught between SL(V) and GL(V), or that G is one of SO(V) or O(V) or (if dim(V) is even) Sp(V).

Larsen's Alternative (cf. [Lar-Char] and [Lar-Normal]) is a marvelous criterion, in terms of having a sufficiently small "fourth moment", which guarantees that G is either a standard classical group **or** is a finite group. We have already made use of this criterion in [Ka-LFM, page 113]. In that application, we were content with either alternative.

However, in many applications, especially to the determination of (Zariski closures of) geometric monodromy groups in explicitly given families, we want to be able to rule out the possibility that G be finite. Failing this, we would at least like to have a better understanding of the cases in which G can in fact be finite.

Part I of this paper represents very modest progress toward these two goals. Toward the first goal, we give criteria for ruling out the possibility that G be finite. These criteria rely on the observation that if G is finite and has a sufficiently small fourth moment, it must be primitive. This observation in turn allows us to bring to bear classical results of Blichfeld and of Mitchell, and more recent results of Wales and Zalesskii. Toward the second goal, we give examples of finite G with a very low fourth moment.

In Part II, we apply the results proven in Part I to the monodromy of Lefschetz pencils. Start with a projective smooth variety X of dimension $n+1 \geq 1$, and take the universal family of (or a sufficiently general Lefschetz pencil of) smooth hypersurface sections of degree d. By its monodromy group $G_d$, we mean the

Zariski closure of the monodromy of the local system $\mathcal{F}_d$ on the space of all smooth, degree d, hypersurface sections, given by

$$H \mapsto H^n(X\cap H)/H^n(X).$$

Let us denote by $N_d$ the rank of this local system.

For n odd, the monodromy group $G_d$ is the full symplectic group $Sp(N_d)$, cf [De-Weil II, 4.4.1 and 4.4.2$^a$].

For n = 0, X is a curve, $X\cap H$ is finite, $N_d + 1 = \mathrm{Card}((X\cap H)(\overline{k}))$ $= d\times\deg(X)$, and the monodromy group $G_d$ is well known to be the full symmetric group $S_{N_d+1} := \mathrm{Aut}((X\cap H)(\overline{k}))$, cf. 2.4.4.

For $n \geq 2$ and even, the situation is more involved. Deligne proved [De-Weil II, 4.4.1, 4.4.2$^s$, and 4.4.9] that the monodromy group $G_d$ is either the full orthogonal group $O(N_d)$, or it is a finite reflection group, and that the only finite reflection groups that arise are the Weyl groups of root systems of type A, D, or E in their standard representations. Deligne needed this more precise information for his pgcd theorem [De-Weil II, 4.5.1], where the $O(N_d)$ case was easy, but the finite case required case by case argument. Using the criteria developed in Part I, we show that the monodromy group $G_d$ is in fact the full orthogonal group $O(N_d)$ for all sufficiently large d (more precisely, for all d with $d \geq 3$ and $N_d > 8$, and also for all d with $d \geq 7$ and $N_d > 2$, cf. 2.2.4, 2.2.15, and 2.3.6).

I would like to thank CheeWhye Chin for his assistance in using the computer program GAP [GAP] to compute moments of exceptional Weyl groups. I would also like to thank the referee, for suggesting Theorem 2.3.6.

# Part I: Group Theory

## 1.1 Review of Larsen's Alternative

(1.1.1) Recall that $\mathbb{C}$ is an algebraically closed field of characteristic zero, V is a $\mathbb{C}$-vector space of dimension $N \geq 2$, and G is a Zariski closed, reductive subgroup of GL(V).

(1.1.2) For each pair (a, b) of non-negative integers, we denote by $M_{a,b}(G, V)$ the dimension of the space of G-invariant vectors in $V^{\otimes a}\otimes(V^\vee)^{\otimes b}$:

(1.1.2.1) $$M_{a,b}(G, V) := \dim_{\mathbb{C}} (V^{\otimes a} \otimes (V^{\vee})^{\otimes b})^G.$$

We call $M_{a,b}(G, V)$ the (a, b)'th moment of (G, V). For each even integer $2n \geq 2$, we denote by $M_{2n}(G, V)$ the 2n'th absolute moment, defined by

(1.1.2.2) $$M_{2n}(G, V) := M_{n,n}(G, V).$$

If H is any subgroup of G, we have the a priori inequalities

(1.1.2.3) $$M_{a,b}(G, V) \leq M_{a,b}(H, V)$$

for every (a, b).

(1.1.3) The reason for the terminology "moments" is this. If $\mathbb{C}$ is the field of complex numbers, and if $K \subset G(\mathbb{C})$ is a maximal compact subgroup of $G(\mathbb{C})^{an}$, then K is Zariski dense in G (Weyl's unitarian trick). If we denote by dk the Haar measure on K of total mass one, and by

$$\chi : G(\mathbb{C}) \to \mathbb{C}$$
$$\chi(g) := \mathrm{Trace}(g|V),$$

the character of V as G-module, then we have the formulas

(1.1.3.1) $$M_{a,b}(G, V) = \int_K \chi(k)^a \bar{\chi}(k)^b dk,$$

(1.1.3.2) $$M_{2n}(G, V) = \int_K |\chi(k)|^{2n} dk.$$

Thus the terminology "moments" and "absolute moments".

(1.1.4) The most computationally straightforward interpretation of the 2n'th absolute moment $M_{2n}(G, V)$ is this. Decompose the G-module $V^{\otimes n}$ as a sum of irreducibles with multiplicities:

(1.1.4.1) $$V^{\otimes n} \cong \oplus_i m_i W_i.$$

Then by Schur's Lemma we have

(1.1.4.2) $$M_{2n}(G, V) = \Sigma_i (m_i)^2.$$

More precisely, given any decomposition of $V^{\otimes n}$ as a sum of (not necessarily irreducible) G-modules $V_i$ with (strictly positive integer) multiplicities $m_i$,

(1.1.4.3) $$V^{\otimes n} \cong \oplus_i m_i V_i,$$

we have the inequality

(1.1.4.4) $$M_{2n}(G, V) \geq \Sigma_i (m_i)^2,$$

with equality if and only if the $V_i$ are distinct irreducibles.

(1.1.5) If n is itself even, say n = 2m, there is another interpretation of $M_{4m}(G, V)$. Decompose the G-module $V^{\otimes m}\otimes(V^{\vee})^{\otimes m} = \mathrm{End}(V^{\otimes m})$ as a sum of irreducibles with multiplicities:

(1.1.5.1) $$\mathrm{End}(V^{\otimes m}) \cong \oplus_i n_iW_i.$$

Then we have, again by Schur's Lemma,

(1.1.5.2) $$M_{4m}(G, V) = \Sigma_i (n_i)^2.$$

More precisely, given any decomposition of $\mathrm{End}(V^{\otimes m})$ as a sum of (not necessarily irreducible) G-modules $V_i$ with (strictly positive integer) multiplicities $n_i$,

(1.1.5.3) $$\mathrm{End}(V^{\otimes m}) \cong \oplus_i n_iV_i,$$

we have the inequality

(1.1.5.4) $$M_{2n}(G, V) \geq \Sigma_i (n_i)^2,$$

with equality if and only if the $V_i$ are distinct irreducibles.

**Theorem 1.1.6 (Larsen's Alternative**, cf [Lar-Char], [Lar-Normal], [Ka-LFM, page 113]**)** Let $V$ be a $\mathbb{C}$-vector space of dimension $N \geq 2$, $G \subset GL(V)$ a (not necessarily connected) Zariski closed reductive subgroup of $GL(V)$.

0) If $M_4(G, V) \leq 5$, then $V$ is G-irreducible.

1) If $M_4(G, V) = 2$, then either $G \supset SL(V)$, or $G/(G\cap\text{scalars})$ is finite. If in addition $G\cap$scalars is finite (e.g., if $G$ is semisimple), then either $G^0 = SL(V)$, or $G$ is finite.

2) Suppose $\langle,\rangle$ is a nondegenerate symmetric bilinear form on $V$, and suppose $G$ lies in the orthogonal group $O(V) := \mathrm{Aut}(V, \langle,\rangle)$. If $M_4(G, V) = 3$, then either $G = O(V)$, or $G = SO(V)$, or $G$ is finite. If $\dim(V)$ is 2 or 4, then $G$ is not contained in $SO(V)$.

3) Suppose $\langle,\rangle$ is a nondegenerate alternating bilinear form on $V$ (such a form exists only if $\dim(V)$ is even), suppose $G$ lies in the symplectic group $Sp(V) := \mathrm{Aut}(V, \langle,\rangle)$, and suppose $\dim(V) > 2$. If $M_4(G, V) = 3$, then either $G = Sp(V)$, or $G$ is finite.

**proof** To prove 0), suppose that $V = V_1\oplus V_2$ is the direct sum of two non-zero G-modules. Then we have a G-isomorphism

$$V^{\otimes 2} \cong (V_1)^{\otimes 2} \oplus (V_2)^{\otimes 2} \oplus 2(V_1\otimes V_2),$$

and this in turn forces $M_4(G, V) \geq 1 + 1 + 2^2 = 6$.

To prove 1), we use the second interpretation (1.1.5) of $M_4(G, V)$. If $M_4(G, V) = 2$, then End(V) is the sum of two distinct irreducible representations of G. But under the bigger group GL(V), End(V) is the sum of two representations of GL(V), namely

$$\mathrm{End}(V) = \mathrm{End}^0(V) \oplus \mathbb{1} = \mathrm{Lie}(SL(V)) \oplus \mathbb{1}.$$

[The two summands are inequivalent irreducible representations of GL(V), but we will not use this fact.] Because $M_4(G, V) = 2$, this must be the decomposition of End(V) as the sum of two distinct irreducible representations of G. In particular, Lie(SL(V)) is G-irreducible.

The derived group $G^{der}$ lies in SL(V), so $\mathrm{Lie}(G^{der})$ lies in Lie(SL(V)). As $G^{der}$ is a normal subgroup of G, $\mathrm{Lie}(G^{der})$ is a G-stable submodule of Lie(SL(V)). So by the G-irreduciblity of Lie(SL(V)), either $\mathrm{Lie}(G^{der}) = \mathrm{Lie}(SL(V))$, or $\mathrm{Lie}(G^{der}) = 0$. In the first case, $(G^{der})^0 = SL(V)$, and so $G \supset SL(V)$. Thus if in addition $G \cap$scalars is finite, $G^0$ is SL(V).

In the second case, $G^{der}$ is finite. For any fixed element $\gamma$ in $G(\mathbb{C})$, the morphism from $G^0$ to $G^{der}$ defined by $g \mapsto g\gamma g^{-1}\gamma^{-1}$ is therefore the constant map $g \mapsto e$. Therefore $G^0$ lies in Z(G). As G acts irreducibly on V, its center Z(G) lies in the $\mathbb{G}_m$ of scalars. But $G^0 \subset Z(G)$, so $G^0$ lies in the $\mathbb{G}_m$ of scalars. Therefore $G^0 \subset G\cap$scalars, whence $G/(G\cap$scalars$)$ is finite. So if in addition $G\cap$scalars is finite, then G is finite.

To prove 2), use the first interpretation (1.1.4) of $M_4(G, V)$. If $M_4(G, V) = 3$, then $V^{\otimes 2}$ is the sum of three distinct irreducible representations of G. Under GL(V), we first decompose

$$V^{\otimes 2} = \mathrm{Sym}^2(V) \oplus \Lambda^2(V).$$

As O(V)-modules, we have an isomorphism

$$\Lambda^2(V) \cong \mathrm{Lie}(SO(V))$$

and the further decompostion

$$\mathrm{Sym}^2(V) = \mathrm{SphHarm}^2(V) \oplus \mathbb{1}.$$

Thus as O(V)-module, we have the three term decomposition

$$V^{\otimes 2} = \mathrm{SphHarm}^2(V) \oplus \mathbb{1} \oplus \mathrm{Lie}(SO(V)).$$

[For $\dim(V) \geq 2$, the three summands are distinct irreducible representations of O(V). If dim(V) is neither 2 nor 4, they are distinct irreducible representations of SO(V). For $n = 2$ (resp. $n = 4$), $\mathrm{SphHarm}^2(V)$ (resp. Lie(SO(V))) is a reducible representation of SO(V). We will not use these facts.]

If $M_4(G, V) = 3$, then

$$V^{\otimes 2} = \mathrm{SphHarm}^2(V) \oplus \mathbb{1} \oplus \mathrm{Lie}(SO(V))$$

must be the decomposition of of $V^{\otimes 2}$ as the sum of three distinct irreducible representations of G.

We now exploit the fact that Lie(SO(V)) is G-irreducible. Since $G \subset O(V)$, $G^0 \subset SO(V)$, so $\mathrm{Lie}(G^0)$ is a G-stable submodule of Lie(SO(V)). By G-irreducibility, $\mathrm{Lie}(G^0)$ is either Lie(SO(V)) or is zero. If $\mathrm{Lie}(G^0) = \mathrm{Lie}(SO(V))$, then $G^0$ is SO(V) and G, being caught between SO(V) and O(V), is either SO(V) or O(V). If $\mathrm{Lie}(G^0)$ is zero, then G is finite.

If dim(V) is 2 or 4, we claim G cannot lie in SO(V). Indeed, for $\dim(V) = 2$, SO(V) is $\mathbb{G}_m$, Lie(SO(V)) is $\mathbb{1}$ as SO(V)-module, and $\mathrm{SphHarm}^2(V)$ is SO(V)-reducible, so if $G \subset SO(V)$ then $M_4(G, V) \geq 6$. If $\dim(V) = 4$, then SO(4) is $(SL(2)\times SL(2))/\pm(1,1)$, hence Lie(SO(4)) is SO(4)-reducible: so if $G \subset SO(V)$ then $M_4(G, V) \geq 4$.

To prove 3), we begin with the GL(V)-decomposition

$$V^{\otimes 2} = \mathrm{Sym}^2(V) \oplus \Lambda^2(V).$$

As Sp(V)-modules, we have an isomorphism

$$\mathrm{Lie}(Sp(V)) \cong \mathrm{Sym}^2(V),$$

and the further (because $\dim(V) > 2$) decomposition

$$\Lambda^2(V) = (\Lambda^2(V)/\mathbb{1}) \oplus \mathbb{1}.$$

Thus as Sp(V)-module we have a three term deomposition

$$V^{\otimes 2} = \mathrm{Lie}(Sp(V)) \oplus (\Lambda^2(V)/\mathbb{1}) \oplus \mathbb{1}.$$

[The three summands are distinct irreducible representations of Sp(V), but we will not use this fact.] Exactly as in the SO case above, we infer that Lie(Sp(V)) is G-irreducible. But $G \subset Sp(V)$, so $\mathrm{Lie}(G^0)$ is a G-stable submodule of Lie(Sp(V)), and so either $\mathrm{Lie}(G^0) = \mathrm{Lie}(Sp(V))$, or $\mathrm{Lie}(G^0)$ is zero. In the first case, G is Sp(V), and in the second case G is finite. QED

## 1.2 Remarks

(1.2.1) We should call attention to a striking result of Beukers, Brownawell and Heckmann, [BBH, Theorems A5 and A7 together], which is similar in spirit to 1.1, though more difficult: if G is a Zariski closed subgroup of GL(V) which acts irreducibly on $\mathrm{Sym}^2(V)$, then either G/(G∩scalars) is finite, or G contains SL(V), or dim(V) is even and Sp(V) ⊂ G ⊂ GSp(V).

(1.2.2) There are connected semisimple subgroups G ⊂ GL(V) with $M_4(G, V) = 3$ other than SO(V) (for dim(V) ≥ 3, but ≠ 4) and Sp(V) (for dim(V) ≥ 4). The simplest examples are these. Take a $\mathbb{C}$-vector space W of dimension $\ell+1$. Then for V either $\mathrm{Sym}^2(W)$, if $\ell \geq 2$, or $\Lambda^2(W)$, if $\ell \geq 4$, the image G of SL(W) in GL(V) has $M_4(G, V) = 3$, but V is not self-dual as a representation of G (not self dual because we excluded the case $\ell=3$, $V = \Lambda^2(W)$). Here is a bad proof. In the Bourbaki notation [Bour-L8, page 188], $\mathrm{Sym}^2(W)$ is the highest weight module $E(2\omega_1)$, and $\Lambda^2(W)$ is the highest weight module $E(\omega_2)$. We use the first interpretation (1.1.4) of the fourth absolute moment. We have

(1.2.2.1) $\mathrm{End}(E(2\omega_1)) = E(2\omega_1)\otimes E(2\omega_1)^{\vee} = E(2\omega_1)\otimes E(2\omega_\ell)$

and

(1.2.2.2) $\mathrm{End}(E(\omega_2)) = E(\omega_2)\otimes(\omega_2)^{\vee} = E(\omega_2)\otimes E(\omega_{\ell-1})$.

Now End(any nonntrivial rep'n of SL(W)) contain both the trivial representation $\mathbb{1}$ of SL(W) and its adjoint representation $E(\omega_1 + \omega_\ell)$. From looking at highest weights, we see that $\mathrm{End}(E(2\omega_1))$ contains $E(2\omega_1 + 2\omega_\ell)$, and we see that $\mathrm{End}(E(\omega_2))$ contains $E(\omega_2 + \omega_{\ell-1})$. Thus we have a priori decompositions

(1.2.2.3) $\mathrm{End}(E(2\omega_1)) = \mathbb{1} \oplus E(\omega_1 + \omega_\ell) \oplus E(2\omega_1 + 2\omega_\ell) \oplus (?)$,

(1.2.2.4) $\mathrm{End}(E(\omega_2)) = \mathbb{1} \oplus E(\omega_1 + \omega_\ell) \oplus E(\omega_2 + \omega_{\ell-1}) \oplus (?)$.

To see that in both cases there is no (?) term, it suffices to check that the dimensions add up, an exercise in the Weyl dimension formula we leave to the reader.

(1.2.3) Other examples are (the image of) $E_6$ in either of its 27-dimensional irreducible representations, or Spin(10) in either of its 16-dimensional spin represenstions: according to simpLie [MPR], these all have fourth absolute moment 3.

## 1.3 The case of G finite: the primitivity theorem

(1.3.1) What about finite groups $G \subset GL(V)$ with $M_4(G, V) = 2$, or finite groups G in O(V) or Sp(V) with $M_4(G, V) = 3$?

**Primitivity Theorem 1.3.2** Let V be a $\mathbb{C}$-vector space of dimension $N \geq 2$, $G \subset GL(V)$ a finite subgroup of GL(V). With the notations of the previous theorem, suppose that one of the following conditions 1), 2) or 3) holds.

1) $M_4(G, V) = 2$

2) G lies in O(V), $\dim(V) \geq 3$, and $M_4(G, V) = 3$.

3) G lies in Sp(V), $\dim(V) \geq 4$, and $M_4(G, V) = 3$.

Then G is an (irreducible) primitive subgroup of GL(V), i.e., there exists no proper subgroup H of G such that V is induced from a representation of H.

(1.3.3) Before giving the proof, we recall the following well-known lemma.

**Lemma 1.3.4** Let G be a group, H a subgroup of G of finite index, and A and B two finite-dimensional $\mathbb{C}$-representations of H.

1) Denoting by $^\vee$ the dual (contragredient) representation, we have a canonical G-isomorphism

$$(\mathrm{Ind}_H{}^G(A))^\vee \cong \mathrm{Ind}_H{}^G(A^\vee).$$

2) There is a canonical surjective G-morphism ("cup product")

$$(\mathrm{Ind}_H{}^G(A))\otimes_{\mathbb{C}}(\mathrm{Ind}_H{}^G(B)) \twoheadrightarrow \mathrm{Ind}_H{}^G(A\otimes_{\mathbb{C}}B).$$

**proof of Lemma 1.3.4** Assertion 1) is proven in [Ka-TLFM, 3.1.3]. For assertion 2), we view induction as Mackey induction, cf. [Ka-TLFM, 3.0.1.2]. Thus $\mathrm{Ind}_H{}^G(A)$ is $\mathrm{Hom}_{\text{left H-sets}}(G, A)$, with left G-action defined by $(L_g\varphi)(x) := \varphi(xg)$. We define a $\mathbb{C}$-bilinear map

$$(\mathrm{Ind}_H{}^G(A))\otimes_{\mathbb{C}}(\mathrm{Ind}_H{}^G(B)) \to \mathrm{Ind}_H{}^G(A\otimes_{\mathbb{C}}B)$$

as follows. Given maps $\varphi : G \to A$ and $\psi: G \to B$ of left H-sets, we define their cup product $\varphi\otimes\psi : G \to A\otimes_{\mathbb{C}}B$ by

$$(\varphi\otimes\psi)(x) := \varphi(x)\otimes\psi(x).$$

It is immediate that $\varphi\otimes\psi$ is a map of left H-sets, and so the cup product construction $(\varphi, \psi) \mapsto \varphi\otimes\psi$ is a $\mathbb{C}$-linear map

$$(\mathrm{Ind}_H{}^G(A))\otimes_{\mathbb{C}}(\mathrm{Ind}_H{}^G(B)) \to \mathrm{Ind}_H{}^G(A\otimes_{\mathbb{C}}B).$$

This map is easily checked to be G-equivariant and surjective. **QED**

**proof of Theorem 1.3.2** Let H be a subgroup of a finite group G, of finite index $d \geq 2$, and A a finite-dimensional $\mathbb{C}$-representation of H, of dimension $a \geq 1$. We wish to compute a lower bound for $M_4(G, \mathrm{Ind}_H{}^G(A))$. To do this we attempt to decompose $\mathrm{Ind}_H{}^G(A) \otimes (\mathrm{Ind}_H{}^G(A))^\vee$ as a sum of G-modules. By the previous lemma, we have a g-isomorphism

$$(\mathrm{Ind}_H{}^G(A))^\vee \cong \mathrm{Ind}_H{}^G(A^\vee),$$

and a surjective G-map

$$\mathrm{Ind}_H{}^G(A) \otimes \mathrm{Ind}_H{}^G(A^\vee) \to \mathrm{Ind}_H{}^G(A \otimes A^\vee).$$

Its source has dimension $d^2a^2$, while its target has lower dimension $da^2$, so this map has a nonzero kernel "Ker", which is a G-module of dimension $(d^2 - d)a^2$. So we have a G-isomorphism

$$\mathrm{Ind}_H{}^G(A) \otimes (\mathrm{Ind}_H{}^G(A))^\vee \cong \mathrm{Ker} \oplus \mathrm{Ind}_H{}^G(A \otimes A^\vee).$$

Now the H-module $A \otimes A^\vee = \mathrm{End}(A)$ itself has an H-decomposition

$$\mathrm{End}(A) \cong \mathrm{End}^0(A) \oplus \mathbb{1}_H,$$

as the sum of the endomorphisms of trace zero with the scalars. [Of course, if A is one-dimensional, then $\mathrm{End}^0(A)$ vanishes.] Thus we have a G-decomposition

$$\mathrm{Ind}_H{}^G(A \otimes A^\vee) \cong \mathrm{Ind}_H{}^G(\mathrm{End}^0(A)) \oplus \mathrm{Ind}_H{}^G(\mathbb{1}_H),$$

Now the trivial representation $\mathbb{1}_G$ occurs once in $\mathrm{Ind}_H{}^G(\mathbb{1}_H)$, so we have a further decomposition

$$\mathrm{Ind}_H{}^G(\mathbb{1}_H) \cong \mathrm{Ind}_H{}^G(\mathbb{1}_H)/\mathbb{1}_G \oplus \mathbb{1}_G.$$

So all in all we have a four term G-decomposition

$$\mathrm{Ind}_H{}^G(A) \otimes (\mathrm{Ind}_H{}^G(A))^\vee \cong$$
$$\mathrm{Ker} \oplus \mathrm{Ind}_H{}^G(\mathrm{End}^0(A)) \oplus \mathrm{Ind}_H{}^G(\mathbb{1}_H)/\mathbb{1}_G \oplus \mathbb{1}_G,$$

in which the dimensions of the terms are respectively $(d^2 - d)a^2$, $d(a^2 - 1)$, $d - 1$, and 1. So we obtain the a priori estimate

$$M_4(G, \mathrm{Ind}_H{}^G(A)) \geq 4 \text{ if } \dim(A) \geq 2,$$

$$M_4(G, \mathrm{Ind}_H{}^G(A)) \geq 3 \text{ if } \dim(A) = 1.$$

Thus if $M_4(G, V) = 2$, then G is a primitive subgroup of $GL(V)$.

Suppose now that $M_4(G, V) = 3$, and that V is induced from a subgroup H of G of finite index $d \geq 2$, from an H-module A. Then $\dim(A) = 1$, and $\dim(V) = d$. Moreover, $\mathrm{Ind}_H{}^G(A)\otimes(\mathrm{Ind}_H{}^G(A))^\vee$ is the sum of three distinct irreducibles, of dimensions $d^2 - d$, $d - 1$, and 1.

If we further suppose that G lies in either O(V) or Sp(V), then $V \cong \mathrm{Ind}_H{}^G(A)$ is self-dual, so we have a G-isomorphism

$$\mathrm{Ind}_H{}^G(A)\otimes(\mathrm{Ind}_H{}^G(A))^\vee \cong \mathrm{Ind}_H{}^G(A)\otimes\mathrm{Ind}_H{}^G(A). \cong V\otimes V.$$

If G lies in O(V), and $\dim(V) \geq 3$, then we have the G-decomposition

$$V\otimes V \cong \mathrm{SphHarm}^2(V) \oplus \Lambda^2(V) \oplus \mathbb{1}_G.$$

In this decomposition, the dimensions of of the terms are respectively $d(d+1)/2 - 1$, $d(d-1)/2$, and 1. Since $M_4(G, V) = 3$, these three terms must be distinct irreducibles. Thus $V\otimes V \cong V\otimes V^\vee$ is simultaneously presented as the sum of three distinct irreducibles of dimensions $d^2 - d$, $d - 1$, and 1, and the sum of three distinct irreducibles of dimensions $d(d+1)/2 - 1$, $d(d-1)/2$, and 1. As $d \geq 2$, we have $d(d+1)/2 - 1 \geq d(d-1)/2$. Comparing the dimensions of the largest irreducible constituent in the two presentations, we find

$$d^2 - d = d(d+1)/2 -1,$$

which forces $d = 1$ or 2, contradiction.

If G lies in Sp(V), and $\dim(V) \geq 4$, the argument is similar. We have the G-decomposition

$$V\otimes V \cong \mathrm{Sym}^2(V) \oplus \Lambda^2(V)/\mathbb{1}_G \oplus \mathbb{1}_G.$$

into what must be three distinct irreducibles, of dimensions $d(d+1)/2$, $d(d-1)/2 - 1$, and 1. Exactly as above, we compare dimensions of the largest irreducible constituent in the two presentations. We find

$$d^2 - d = d(d+1)/2,$$

which forces $d= 3$, contradiction. QED

**Remark 1.3.5** In the primitivity theorem, when V is either symplectic or orthogonal, we required $\dim(V) > 2$. This restriction is necessary, because there exist imprimitive finite groups G in both O(2) and in Sp(2) = SL(2) whose fourth moment is 3 in their given representations. Indeed, fix an integer $n \geq 1$ which is not a divisor of 4, and denote by $\zeta$ a primitive n'th root of unity. The dihedral group

$D_{2n} \subset O(2)$ of order 2n (denoted $D_n$ in [C-R-MRT, page 22]), the group generated by $\mathrm{Diag}(\zeta, \zeta^{-1})$ and Antidiag(1, 1), is easily checked to have fourth moment 3 in its given representation. If we further require n to be even, the generalized quaternion group $Q_{2n} \subset SL(2)$ of order 2n (denoted $Q_{n/2}$ in [C-R-MRT, page 23]), the group generated by $\mathrm{Diag}(\zeta, \zeta^{-1})$ and Antidiag(1, -1), is easily checked to have fourth moment 3 in its given representation.

**Tensor Indecomposability Lemma 1.3.6** Let V be a $\mathbb{C}$-vector space of dimension $N \geq 2$, $G \subset GL(V)$ a finite subgroup of GL(V). Suppose that $M_4(G, V) \leq 3$. Then V is tensor-indecomposable in the following (strong) sense. There exists no expression of the $\mathbb{C}$-vector space V as a tensor product

$$V = V_1 \otimes V_2$$

of $\mathbb{C}$-vector spaces $V_1$ and Y in such a way that all three of the following conditions are satisfied:

$\dim(V_1) \geq 2$,

$\dim(V_2) \geq 2$,

every element g in G, viewed as lying in $GL(V) = GL(V_1 \otimes V_2)$, can be written in the form $A \otimes B$ with A in $GL(V_1)$ and with B in $GL(V_2)$.

**proof** If not, G lies in the image "$GL(V_1)\otimes GL(V_2)$" of the product group $GL(V_1)\times GL(V_2)$ in $GL(V_1 \otimes V_2)$. So we have the trivial inequality

$$M_4(G, V) = M_4(G, V_1 \otimes V_2) \geq M_4(GL(V_1)\otimes GL(V_2), V_1 \otimes V_2).$$

But by definition

$$\begin{aligned}
&M_4(GL(V_1)\otimes GL(V_2), V_1\otimes V_2)\\
&= \dim(((V_1\otimes V_2)^{\otimes 2}\otimes((V_1\otimes V_2)^{\vee})^{\otimes 2})^{GL(V_1)\times GL(V_2)})\\
&= \dim(((V_1^{\otimes 2}\otimes(V_1^{\vee})^{\otimes 2})\otimes(V_2^{\otimes 2}\otimes(V_2^{\vee})^{\otimes 2}))^{GL(V_1)\times GL(V_2)})\\
&\geq \dim(((V_1^{\otimes 2}\otimes(V_1^{\vee})^{\otimes 2})^{GL(V_1)})\otimes((V_2^{\otimes 2}\otimes(V_2^{\vee})^{\otimes 2})^{GL(V_2)}))\\
&\quad = M_4(GL(V_1), V_1)\times M_4(GL(V_2), V_2)\\
&\quad = 2\times 2 = 4.
\end{aligned}$$

QED

**Normal Subgroup Corollary 1.3.7 [Larsen-Char, 1.6]** Let V be a $\mathbb{C}$-vector space of dimension $N \geq 2$, $G \subset GL(V)$ a finite subgroup of GL(V). Let H be a proper normal subgroup of G. Suppose that one of the following conditions 1), 2) or 3) holds.

1) $M_4(G, V) = 2$

2) G lies in O(V), $\dim(V) \geq 3$, and $M_4(G, V) = 3$.

3) G lies in Sp(V), $\dim(V) \geq 4$, and $M_4(G, V) = 3$.

Then either H acts on V as scalars and lies in the center Z(G), or V is H-irreducible.

**proof** By the Primitivity Theorem 1.3.2, G is primitive. So the restriction of V to H must be H-isotypical, as otherwise V is induced. Say $V|H \cong nV_1$, for some irreducible representation $V_1$ of H. If $\dim(V_1) = 1$, then H acts on V as scalars. But $H \subset G \subset GL(V)$, so H certainly lies in Z(G). If $n = 1$, then $V = V_1$ is H-irreducible. It remains to show that the case where $\dim(V_1) \geq 2$ and $n \geq 2$ cannot arise. To see this, write the vector space V as $X \otimes Y$ with $X := V_1$ and $Y := \mathrm{Hom}_H(V_1, V)$. Then dim(X) and dim(Y) are both at least 2, and, by [C-R-MRT, 51.7], every element of g is of the form $A \otimes B$ with A in GL(X) and B in GL(Y). But this contradicts the Tensor Indecomposability Lemma 1.3.5. QED

**1.4 Criteria for G to be big**

(1.4.1) We next combine these results with some classical results of Blichfeld and of Mitchell, and with recent results of Wales and Zalesskii, to give criteria which force G to be big. Recall that an element A in GL(V) is called a pseudoreflection if $\mathrm{Ker}(A - 1)$ has codimension 1 in V. A pseudoreflection of order 2 is called a reflection. Given an integer r with $1 \leq r < \dim(V)$, an element A of GL(V) is called quadratic of drop r if its minimal polynomial is $(T-1)(T-\lambda)$ for some nonzero $\lambda$, if $V/\mathrm{Ker}(A - 1)$ has dimension r, and if A acts on this space as the scalar $\lambda$. Thus a quadratic element of drop 1 is precisely a pseudoreflection.

**Theorem 1.4.2** Let V be a $\mathbb{C}$-vector space of dimension $N \geq 2$, G in GL(V) a (not necessarily connected) Zariski closed reductive subgroup of GL(V) with $M_4(G, V) = 2$. Fix an integer r with $1 \leq r < \dim(V)$. If any of the following conditions is satisfied, then $G \supset SL(V)$.

0) G contains a unipotent element $A \neq 1$.

1) $G$ contains a quadratic element $A$ of drop $r$ which has finite order $n \geq 6$.
2) $G$ contains a quadratic element $A$ of drop $r$ which has finite order 4 or 5, and $\dim(V) > 2r$.
3) $G$ contains a quadratic element $A$ of drop $r$ which has finite order 3, and $\dim(V) > 4r$.
4) $G$ contains a reflection $A$, and $\dim(V) > 8$.

**proof** Suppose we have already proven the theorem in the case when $G \cap$scalars is finite. To treat the remaining case, when $G$ contains the scalars, we make use of the following elementary lemma.

**Lemma 1.4.3** Let $V$ be a $\mathbb{C}$-vector space of dimension $N \geq 2$, $G \subset GL(V)$ a (not necessarily connected) Zariski closed reductive subgroup of $GL(V)$ which contains the scalars $\mathbb{C}^\times$. For each integer $d \geq 1$, denote by $G_d \subset G$ the closed subgroup

$$G_d := \{g \text{ in } G \mid \det(g)^d = 1\}.$$

Then $G_d$ is reductive, and for every integer $n \geq 1$, we have

$$M_{2n}(G_d, V) = M_{2n}(G, V).$$

**proof of Lemma 1.4.3** Since $G$ contains the scalars, every element of $G$ can be written as $\lambda g_1$ with $\lambda$ any chosen $N$'th root of $\det(g)$, and $g_1 := \lambda^{-1}g$ an element of $G_1$. So we have $G = \mathbb{G}_m G_d$ for every $d \geq 1$. So for every $n \geq 1$, $G$ and $G_d$ acting on $V^{\otimes n}(V^\vee)^{\otimes n}$ have the same image in $GL(V^{\otimes n}(V^\vee)^{\otimes n})$ (simply because the scalars in $GL(V)$ act trivially on $V^{\otimes n}(V^\vee)^{\otimes n}$). Therefore we have the asserted equality of moments. Moreover, $G$ being reductive, each $V^{\otimes n}(V^\vee)^{\otimes n}$ is a completely reducible representation of $G_d$. Each has a finite kernel (because its kernel in $GL(V)$ is the scalars), so $G_d$ is reductive. QED

**proof of Theorem 1.4.2, suite** Thus if $G$ contains the scalars, each $G_d$ is reductive, $G_d \cap$scalars is finite, and $G_d$ has fourth moment 2. So we already know the theorem for $G_d$. In all of the cases 0) through 4), the given element $A$ in $G$ lies in some $G_d$. So $G_d \supset SL(V)$, and we are done.

It remains to treat the case in which $G\cap$scalars is finite. By Larsen's theorem together with the primitivity theorem, either $G^0 = SL(V)$, or G is a finite irreducible primitive subgroup of GL(V). Suppose that G is a finite irreducible primitive subgroup of GL(V). We will show that each of the conditions 0) through 4) leads to a contradiction

For assertion 0), the contradiction is obvious: a nontrivial unipotent element is of infinite order.

Assertion 1) contradicts Blichfeld's "$60^{\circ}$ theorem" [Blich-FCG, paragraph 70, Theorem 8, page 96], applied to that power of A whose only eigenvalues are 1 and $\exp(2\pi i/n)$: in a finite irreducible primitive subgroup G of $GL(N, \mathbb{C})$, if an element g in G has an eigenvalue $\alpha$ such that every other eigenvalue of g is within $60^{\circ}$ of $\alpha$ (on either side, including the endpoints), then g is a scalar.

Assertion 2) in the case $n = 5$ (resp. $n = 4$) contradicts a result of Zalesskii [Zal, 11.2] (resp. Wales [Wales, Thm. 1]), applied to A: if a finite irreducible primitive subgroup G of $GL(N, \mathbb{C})$ contains a quadratic element of drop r and order 5 (resp. order 4), then $\dim(V) = 2r$.

Assertion 3) contradicts a result of Wales [Wales, section 5], applied to A: if a finite irreducible primitive subgroup G of $GL(N, \mathbb{C})$ contains a quadratic element of drop r and order 3, then $\dim(V) \leq 4r$.

Assertion 4) contradicts the following theorem, the first (and essential) part of which was proved by Mitchell nearly a century ago.

**Theorem 1.4.4 (Mitchell)** Let V be a $\mathbb{C}$-vector space of dimension $N > 8$, $G \subset GL(V)$ a finite irreducible primitive subgroup of $GL(V) \cong GL(N, \mathbb{C})$ which contains a reflection A. Let $\Gamma \subset G$ denote the normal subgroup of G generated by all the reflections in G. Then we have:
1) $\Gamma$ is (conjugate in GL(V) to) the group $S_{N+1}$, viewed as a subgroup of $GL(N, \mathbb{C})$ by its "permutation of coordinates" action on the hyperplane $Aug_N$ in $\mathbb{C}^{N+1}$ consisting of those vectors whose coordinates sum to zero.
2) G is the product of $\Gamma$ with the group $G\cap$(scalars).

3) $M_4(G, V) > 3$.

**proof** By a theorem of Mitchell [Mi], if $N > 8$, and if G is a finite irreducible primitive subgroup of $GL(V) \cong GL(Aug_N)$ which contains a reflection, then the image of G in the projective group $PGL(Aug_N) = GL(Aug_N)/\mathbb{C}^\times$ is the image in that group of the symmetric group $S_{N+1}$.

We first exhibit an $S_{N+1}$ inside G. For this, we argue as follows. We have our reflection A in G. Its image in $S_{N+1}$, and indeed the image in $S_{N+1}$ of any reflection in G, is a transposition. Renumbering, we may suppose $A \mapsto (1,2)$. As all transpositions in $S_{N+1}$ are $S_{N+1}$-conjugate, for each i with $1 \le i \le N$, there is a G-conjugate $A_i$ of A which maps to the transposition $\sigma_i := (i, i+1)$. Now $A_i$ is itself a reflection, being a conjugate of the reflection A. We claim it is the unique reflection in G which maps to $\sigma_i$. Indeed, any element in G which maps to $\sigma_i$ is of the form $\lambda A_i$ for some invertible scalar $\lambda$; but $\lambda A_i$ has $\lambda$ as eigenvalue with multiplicity $N - 1 > 1$, so $\lambda A_i$ can be a reflection only if $\lambda = 1$. We next claim that the subgroup H of G generated by the $A_i$ maps isomorphically to $S_{N+1}$. We know H maps onto $S_{N+1}$ (because $S_{N+1}$ is generated by the $\sigma_i$), so it suffices to show that the order of H divides $(N+1)!$. For this, it suffices to show that H is a quotient of $S_{N+1}$. We know [Bour-L4, pages 12 and 27] that $S_{N+1}$ is generated by elements $s_i$, $1 \le i \le N$, subject to the Coxeter relations

$$(s_i s_j)^{m(i,j)} = 1,$$

where

$$m(i,i) = 1,$$
$$m(i,j) = 2 \text{ if } |i - j| \ge 2,$$
$$m(i,j) = 3 \text{ if } |i - j| = 1.$$

[If we map $s_i$ to $\sigma_i$, we get the required isomorphism with $S_{N+1}$.] So it suffices to show that the $A_i$ satisfy these relations. Each $A_i$ is a reflection, so of order 2. For any i and j, the subspace

$$\mathrm{Ker}(A_i - 1) \cap \mathrm{Ker}(A_j - 1)$$

of $V$ has codimension at most 2, and the product $A_iA_j$ fixes each element of this subspace. Therefore its power $(A_iA_j)^{m(i,j)}$ also fixes each element of this subspace. But $(A_iA_j)^{m(i,j)}$ maps to $(\sigma_i\sigma_j)^{m(i,j)} = 1$ in $S_{N+1}$, and hence $(A_iA_j)^{m(i,j)}$ is a scalar $\lambda$. As this scalar $\lambda$ fixes every vector in a subspace of codimension at most 2, we must have $\lambda = 1$.

We next observe that $H = \Gamma$, i.e., that $H$ contains every reflection $A$ in $G$. For the image of $A$ in the projective group is a transposition, so $A = \lambda h$ for some scalar $\lambda$ and some transposition $h$ in $H$. But such an $h$ is a reflection in $GL(\mathrm{Aug}_N)$. Thus both $h$ and $\lambda h$ are reflections, which forces $\lambda = 1$. This proves 1).

Since $H = \Gamma$ maps isomorphically to the image $S_{N+1} \cong G/G\cap(\text{scalars})$ of $G$ in $PGL(\mathrm{Aug}_N)$, $G$ is generated by $\Gamma$ and by the central subgroup $G\cap(\text{scalars})$, and $\Gamma\cap(\text{scalars}) = \{1\}$. This proves 2).

To prove 3), notice that the scalars in $GL(V)$ act trivially on the tensor spaces $V^{\otimes n}\otimes(V^\vee)^{\otimes n}$ for every $n$, in particular for $n = 2$. So the action of $G = \Gamma \times G\cap(\text{scalars})$ on $V^n\otimes(V^\vee)^{\otimes n}$ factors through the action of $\Gamma$. Thus we have

$$M_{2n}(G, V) = M_{2n}(\Gamma, V) = M_{2n}(S_{N+1}, \mathrm{Aug}_N).$$

So it remains only to prove the following lemma.

**Lemma 1.4.5** For any $N \geq 4$, we have $M_4(S_{N+1}, \mathrm{Aug}_N) > 3$ .

**Remark 1.4.5.1** We will see later (2.4.3) that, in fact, we have $M_4(S_{N+1}, \mathrm{Aug}_N) = 4$ for $N \geq 3$, but we do not need this finer result here.

**Proof of Lemma 1.4.5** $\mathrm{Aug} := \mathrm{Aug}_N$ is an orthogonal representation of $S_{N+1}$, so we have an $S_{N+1}$-decomposition

$$(\mathrm{Aug})^{\otimes 2} \cong \mathbb{1} \oplus \Lambda^2(\mathrm{Aug}) \oplus \mathrm{SphHarm}^2(\mathrm{Aug}),$$

and thus an a priori inequality $M_4(S_{N+1}, \mathrm{Aug}_N) \geq 3$, with equality if and only if the following condition (1.4.5.2) holds:

(1.4.5.2) $\mathbb{1}$, $\Lambda^2(\mathrm{Aug})$, and $\mathrm{SphHarm}^2(\mathrm{Aug})$ are three inequivalent irreducible representations of $S_{N+1}$.

The dimensions of these three representations are 1, $N(N-1)/2$, and $N(N+1)/2 - 1$ respectively. Because $N \geq 4$, none of these dimensions is N. So if (1.4.5.2) holds, then the irreducible representation Aug does not occur in $(\mathrm{Aug})^{\otimes 2}$, or equivalently (Aug being self-dual), $\mathbb{1}$ does not occur in $(\mathrm{Aug})^{\otimes 3}$, or equivalently

$$\int_{S_{N+1}} \mathrm{Trace}(g \mid \mathrm{Aug})^3 = 0.$$

But in fact we have

$$\int_{S_{N+1}} \mathrm{Trace}(g \mid \mathrm{Aug})^3 > 0,$$

as the following argument shows. The representation Aug being irreducible and nontrivial, we have

$$\int_{S_{N+1}} \mathrm{Trace}(g \mid \mathrm{Aug}) = 0.$$

For g in $S_{N+1}$, let us denote by Fix(g) the number of fixed points of g, viewed as a perrmutation of $\{1, ..., N+1\}$. Then

$$\mathrm{Trace}(g \mid \mathrm{Aug}) = \mathrm{Fix}(g) - 1.$$

So we get

$$\int_{S_{N+1}} (\mathrm{Fix}(g) - 1) = 0.$$

Now break up $S_{N+1}$ as the disjoint union $\mathrm{Fix}_{\geq 2} \amalg \mathrm{Fix}_{=1} \amalg \mathrm{Fix}_{=0}$, according to the number of fixed points. Then we may rewrite the above vanishing as

$$\int_{\mathrm{Fix}_{\geq 2}} (\mathrm{Fix}(g) - 1) - \int_{\mathrm{Fix}_{=0}} (1) = 0.$$

At the same time, we have

$$\int_{S_{N+1}} \mathrm{Trace}(g \mid \mathrm{Aug})^3 = \int_{\mathrm{Fix}_{\geq 2}} (\mathrm{Fix}(g) - 1)^3 - \int_{\mathrm{Fix}_{=0}} (1).$$

At every point of $\mathrm{Fix}_{\geq 2}$, we have

$$(\mathrm{Fix}(g) - 1)^3 \geq \mathrm{Fix}(g) - 1,$$

with strict inequality on the nonempty set $\mathrm{Fix}_{\geq 3}$. Thus we have

$$\int_{S_{N+1}} \mathrm{Trace}(g \mid \mathrm{Aug})^3 > \int_{S_{N+1}} \mathrm{Trace}(g \mid \mathrm{Aug}) = 0.$$

Therefore (1.4.5.2) does not hold, i.e., we have $M_4(S_{N+1}, \mathrm{Aug}_N) > 3$. QED for both Lemma 1.4.5 and Theorem 1.4.4

Using Theorem 1.4.4, we also get a result in the orthogonal case.

**Theorem 1.4.6** Let V be a $\mathbb{C}$-vector space of dimension $N > 8$ equipped with a nondegenerate quadratic form. Let $G \subset O(V)$ be a (not necessarily connected) Zariski closed reductive subgroup of $O(V)$ with $M_4(G, V) = 3$. If $G$ contains a reflection, then $G = O(V)$.

**proof** Theorem 1.4.4 rules out the possibility that $G$ is a finite irreducible primitive subgroup of $GL(V)$. So $G$ is either $SO(V)$ or $O(V)$. But $SO(V)$ does not contain a reflection. QED

For the sake of completeness, let us also record the immediate consequence of Larsen's theorem (1.1.6) in the symplectic case.

**Theorem 1.4.7** Let $V$ be a $\mathbb{C}$-vector space of dimension $N \geq 2$ equipped with a nondegenerate alternating form. Suppose that $G \subset Sp(V)$ is a (not necessarily connected) Zariski closed reductive subgroup of $Sp(V)$ with $M_4(G, V) = 3$. If $G$ contains a unipotent element $A \neq 1$, then $G = Sp(V)$.

**proof** By Theorem 1.1.6, $G$ is either $Sp(V)$ or it is finite. Since $A$ has infinite order, $G$ is not finite. QED

## 1.5 Examples of finite G: the Weil-Shale case

(1.5.1) We begin with some examples of finite groups $G \subset GL(V)$ with $M_4(G, V) = 2$, pointed out to me by Deligne. Let $q$ be a power of an odd prime $p$, i.e., $q$ is the cardinality of a finite field $\mathbb{F}_q$ of odd characteristic $p$. Fix an integer $n \geq 1$, and a $2n$-dimensional $\mathbb{F}_q$-vector space $F$, endowed with a nondegenerate symplectic form $\langle,\rangle$. The Heisenberg group $Heis_{2n}(\mathbb{F}_q)$ is the central extension of $F$ by $\mathbb{F}_q$ defined as the set of pairs ($\lambda$ in $\mathbb{F}_q$, $f$ in $F$), with group operation

$$(\lambda, f)(\mu, g) := (\lambda + \mu + \langle f, g\rangle, f+g).$$

The symplectic group $Sp(F)$ acts on $Heis_{2n}(\mathbb{F}_q)$, $\gamma$ in $Sp(F)$ acting by

$$\gamma(\lambda, f) := (\lambda, \gamma(f)).$$

The irreducible $\mathbb{C}$-representations of the group $Heis_{2n}(\mathbb{F}_q)$ are well-known. There are $q^{2n}$ one-dimensional representations, those trivial on the center. For each of the $q-1$ nontrivial $\mathbb{C}^\times$-valued characters $\psi$ of the center, there is precisely one irreducible representation with central character $\psi$, say $V_\psi$, which has dimension $q^n$. Because the action of $Sp(F)$ on $Heis_{2n}(\mathbb{F}_q)$ is trivial on the center, the action of $Heis_{2n}(\mathbb{F}_q)$ on $V_\psi$ extends to a projective representation of the semidirect product group $Heis_{2n}(\mathbb{F}_q)\ltimes Sp(F)$ on $V_\psi$. Because we are over a finite field, this projective representation in turn extends to a linear representation of $\mathrm{Heis}_{2n}(\mathbb{F}_q)\ltimes\mathrm{Sp}(F)$ on $V_\psi$, the Weil-Shale representation.

(1.5.2) We claim that for any nontrivial character $\psi$ of the center, we have

(1.5.2.1) $$M_4(\mathrm{Heis}_{2n}(\mathbb{F}_q)\ltimes\mathrm{Sp}(F), V_\psi) = 2.$$

To see this, it suffices to work over the complex numbers. We fix a choice of the nontrivial character $\psi$, and denote by

$$\chi : \mathrm{Heis}_{2n}(\mathbb{F}_q)\ltimes\mathrm{Sp}(F) \to \mathbb{C}$$

the character of $V_\psi$:

$$\chi((\lambda,f,\gamma)) := \mathrm{Trace}((\lambda,f,\gamma)|V_\psi).$$

According to Howe [Howe, Prop. 2, (i), page 290], $\chi$ is supported on those conjugacy classes which meet (the center Z of $\mathrm{Heis}_{2n}(\mathbb{F}_q))\ltimes\mathrm{Sp}(F)$, where it is given by

(1.5.2.2) $$|\chi((\lambda,0,\gamma))|^2 = q^{\dim(\mathrm{Ker}(\gamma-1)\text{ in }F)}.$$

Moreover, an element $(\lambda, f, \gamma)$ in $\mathrm{Heis}_{2n}(\mathbb{F}_q)\ltimes\mathrm{Sp}(F)$ is conjugate to an element of $Z\ltimes\mathrm{Sp}(F)$ if and only if it is conjugate to $(\lambda, 0, \gamma)$, and this happens if and only if f lies in $\mathrm{Image}(\gamma-1)$, cf. [Howe, page 294, first paragraph]. Thus we have

(1.5.2.3) $$|\chi((\lambda, f, \gamma))|^2 = q^{\dim(\mathrm{Ker}(\gamma-1))}, \text{ if } f \in \mathrm{Image}(\gamma-1),$$
$$|\chi((\lambda, f, \gamma))|^2 = 0, \text{ if not.}$$

(1.5.3) Using this explicit formula, we find a striking relation between the absolute moments of $\mathrm{Heis}_{2n}(\mathbb{F}_q)\ltimes\mathrm{Sp}(F)$ on $V_\psi$ and the absolute moments of its subgroup $\mathrm{Sp}(F)$ on $V_\psi$. For any integer $k \geq 1$, we have

(1.5.3.1) $$M_{2k+2}(\mathrm{Heis}_{2n}(\mathbb{F}_q)\ltimes\mathrm{Sp}(F), V_\psi).= M_{2k}(\mathrm{Sp}(F), V_\psi).$$

To see this, we use the fact that $\dim(\mathrm{Ker}(\gamma-1)) + \dim(\mathrm{Im}(\gamma-1)) = \dim(F)$, and simply compute:

$$\#(\mathrm{Heis}_{2n}(\mathbb{F}_q)\ltimes\mathrm{Sp}(F))\times M_{2k+2}(\mathrm{Heis}_{2n}(\mathbb{F}_q)\ltimes\mathrm{Sp}(F), V_\psi)$$
$$:= \Sigma_{(\lambda,\ f,\ \gamma)}\ |\chi((\lambda, f, \gamma))|^{2k+2}$$
$$= \Sigma_{(\lambda,\ 0,\ \gamma)}\ \Sigma_{f\text{ in }\mathrm{Im}(\gamma-1)}\ |\chi((\lambda, f, \gamma))|^{2k+2}$$
$$= \Sigma_{(\lambda,\ 0,\ \gamma)}\ q^{\dim(\mathrm{Im}(\gamma-1))}\times|q^{\dim(\mathrm{Ker}(\gamma-1))}|^{k+1}$$
$$= \Sigma_{\gamma\text{ in }\mathrm{Sp}(F)}\ q^{1+\dim(F)}\times|q^{\dim(\mathrm{Ker}(\gamma-1)}|^{k}$$

$= \Sigma_{\gamma \text{ in } Sp(F)} q^{1+\dim(F)} \times |\chi((0, 0, \gamma))|^{2k}$

$= q^{1+\dim(F)} \times \#(Sp(F)) \times M_{2k}(Sp(F), V_\psi)$

$= \#(Heis_{2n}(\mathbb{F}_q) \ltimes Sp(F)) \times M_{2k}(Sp(F), V_\psi)$.

So in particular we have

(1.5.3.2) $M_4(Heis_{2n}(\mathbb{F}_q) \ltimes Sp(F), V_\psi) .= M_2(Sp(F), V_\psi)$.

(1.54.) The formula (1.5.2.2)

$|\chi((0, 0, \gamma))|^2 = q^{\dim(Ker(\gamma-1))} = \#(\text{fixed points of } \gamma \text{ on } F)$

means precisely that $End(V_\psi)$ as $Sp(F)$-module is isomorphic to the natural permutation representation of $Sp(F)$ on the space of $\mathbb{C}$-valued functions on F. So

(1.54.1) $M_2(Sp(F), V_\psi) = M_{1,0}(Sp(F), Fct(F, \mathbb{C}))$

is the dimension of the space of $Sp(F)$-invariant functions on F, which is in turn equal to the number of $Sp(F)$-orbits in F, cf. [Ger, proof of Cor. 4.4, first paragraph, page 85]. But $Sp(F)$ acts transitively on $F - \{0\}$, so there are just two orbits. Thus

(1.54.2) $M_4(Heis_{2n}(\mathbb{F}_q) \ltimes Sp(F), V_\psi) = M_2(Sp(F), V_\psi) =$

$= M_{1,0}(Sp(F), Fct(F, \mathbb{C})) = 2$,

as asserted.

## 1.6 Examples of finite G from the Atlas

(1.6.1) A perusal of the Atlas [CCNPW-Atlas] gives some finite simple groups G with a low dimensional irreducible representation V for which we have $M_4(G, V) = 2$. Here are some of them. In the table below, we give (in Atlas notation) the simple group G, the character $\chi$ of the lowest dimensional such V, the dimension of V, and the expression of $|\chi|^2$ as the sum of two distinct irreducible characters.

| G | character $\chi$ of V | dim(V) | $\lvert\chi\rvert^2$ |
|---|---|---|---|
| $L_3(2) = L_2(7)$ | $\chi_2$, $\chi_3$ | 3 | $\mathbb{1} + \chi_6$ |
| $U_4(2) = S_4(3)$ | $\chi_2$, $\chi_3$ | 5 | $\mathbb{1} + \chi_{10}$ |
| $U_5(2)$ | $\chi_3$, $\chi_4$ | 11 | $\mathbb{1} + \chi_{16}$ |
| ${}^2F_4(2)'$ | $\chi_2$, $\chi_3$ | 26 | $\mathbb{1} + \chi_{15}$ |
| $M_{23}$ | $\chi_3$, $\chi_4$ | 45 | $\mathbb{1} + \chi_{17}$ |
| $M_{24}$ | $\chi_3$, $\chi_4$ | 45 | $\mathbb{1} + \chi_{19}$ |
| $J_4$ | $\chi_2$, $\chi_3$ | 1333 | $\mathbb{1} + \chi_{11}$ |

(1.6.2) What about finite subgroups of O(V) with $M_4(G, V) = 3$? Again the Atlas gives some examples of finite simple groups G with a low dimensional irreducible orthogonal representation V for which we have $M_4(G, V) = 3$. Here are some of them.

| G | character $\chi$ of V | dim(V) | $\chi^2$ |
|---|---|---|---|
| $U_4(2)$ | $\chi_4$ | 6 | $\mathbb{1} + \chi_7 + \chi_9$ |
| $S_6(2)$ | $\chi_2$ | 7 | $\mathbb{1} + \chi_4 + \chi_6$ |
| $S_4(5)$ | $\chi_2$ | 13 | $\mathbb{1} + \chi_7 + \chi_9$ |
| | $\chi_3$ | 13 | $\mathbb{1} + \chi_8 + \chi_9$ |
| $G_2(3)$ | $\chi_2$ | 14 | $\mathbb{1} + \chi_6 + \chi_7$ |
| McL | $\chi_2$ | 22 | $\mathbb{1} + \chi_3 + \chi_4$ |
| $U_6(2)$ | $\chi_2$ | 22 | $\mathbb{1} + \chi_3 + \chi_4$ |
| $CO_2$ | $\chi_2$ | 23 | $\mathbb{1} + \chi_3 + \chi_4$ |
| $Fi_{22}$ | $\chi_2$ | 78 | $\mathbb{1} + \chi_6 + \chi_7$ |
| HN = $F_{5+}$ | $\chi_2$ | 133 | $\mathbb{1} + \chi_6 + \chi_8$ |
| | $\chi_3$ | 133 | $\mathbb{1} + \chi_7 + \chi_8$ |
| Th | $\chi_2$ | 248 | $\mathbb{1} + \chi_6 + \chi_7$ |

(1.6.3) What about finite subgroups of Sp(V) with $M_4(G, V) = 3$? The Atlas gives a few cases of finite simple groups G with a low dimensional irreducible symplectic representation V for which we have $M_4(G, V) = 3$. [As Deligne and Ramakrishnan explained to me, "most" simple groups have no symplectic representations, cf. the article [Pra] of Prasad.] Here are two lonely examples.

| G | character of V | dim(V) | $\chi^2$ |
|---|---|---|---|
| $U_3(2)$ | $\chi_2$ | 6 | $\mathbb{1} + \chi_6 + \chi_7$ |
| $U_5(2)$ | $\chi_2$ | 10 | $\mathbb{1} + \chi_5 + \chi_6$ |

## 1.7 Questions

(1.7.1) Given a connected algebraic group G over $\mathbb{C}$ with Lie(G) simple, what if any are the finite subgroups of G which act irreducibly on Lie(G)?

(1.7.2) Given a finite set of irreducible representations $\{V_i\}_i$ of such a G, what if any are the finite subgroups $\Gamma$ of G which act irreducibly on every $V_i$? From the data (G, $\{V_i\}_i$), how can one tell if any such $\Gamma$ will exist? For example, if G is simple and simply connected, can we find such a $\Gamma$ if we take for $\{V_i\}_i$ all the fundamental representations of G. [For SL(N), pick any even $m \geq 4$: then the subgroup $\Gamma_m \subset SL(N)$ consisting of all permutation-shaped matrices of determinant one with entries in $\mu_m$ is such a subgroup.] If we take for $\{V_i\}_i$ all the irreducible representations whose highest weight is the sum of at most two fundamental weights? [[For SL(N), the groups $\Gamma_m$ above fail here, already for $\mathrm{Sym}^2(\mathrm{std}_N) = E(2\omega_1)$. Indeed, the $\mathbb{C}$-span of the squares $(e_1)^2$ of the standard basis e]ements $e_i$ of $\mathbb{C}^N$ is a $\Gamma_m$-stable subspace of $\mathrm{Sym}^2(\mathrm{std}_N)$.]

(1.7.3) Given a reductive, Zariski closed subgroup G of GL(V), can one classify the finite subgroups $\Gamma \subset G$ for which $M_4(\Gamma, V) = M_4(G, V)$?

(1.7.4) Given G as in 3) above, and an integer $k \geq 1$, let us say that a finite subgroup $\Gamma \subset G$ "spoofs" G to order k if we have

(1.7.4.1) $$M_{2\ell}(\Gamma, V) = M_{2\ell}(G, V) \text{ for all } 1 \leq \ell \leq k?$$

For a given G, what can we say about the set Spoof(G) of integers $k \geq 1$ for which there exists a finite subgroup $\Gamma \subset G$ which spoofs G to order k? This set may consist of all $k \geq 1$. Take for G the diagonal subgroup of GL(N), and, for each integer $m \geq 2$, take $\Gamma_m$ the finite subgroup of G consisting of diagonal matrices with entries in $\mu_m$. Then $\Gamma_m$ spoofs G to order m-1 . Or take G itself to be finite, then $\Gamma$ = G spoofs G to any order. Is it true that if $G^0$ is semisimple and nontrivial, then the set Spoof(G) is finite.?

## Part II: Applications to the Monodromy of Lefschetz Pencils

### 2.1 Diophantine preliminaries

(2.1.1) Let k be a finite field of cardinality q and characteristic p, $\ell$ a prime number other than p, w a real number, $\iota$ an embedding of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$, S/k a smooth, geometrically connected k-scheme of dimension $D \geq 1$, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}}_\ell$-sheaf on S of rank $r \geq 1$ which is $\iota$-pure of integer weight w. Pick a geometric point s in S, and define $V := \mathcal{F}_s$. Denote by

(2.1.1.1) $\qquad \rho_{\mathcal{F}} : \pi_1(S, s) \to GL(V) = GL(\mathcal{F}_s) \cong GL(r, \overline{\mathbb{Q}}_\ell)$

the $\ell$-adic representation that $\mathcal{F}$ "is". Denote by $G \subset GL(V)$ the Zariski closure of the image of $\pi_1{}^{geom}(S, s) := \pi_1(S\otimes_k \overline{k}, s)$ under $\rho_{\mathcal{F}}$. Because $\mathcal{F}$ is $\iota$-pure of some weight, we know [De-Weil II, 1.3.8 and 3.4.3 (iii)] that G is a (not necessarily connected) semisimple subgroup of GL(V).

(2.1.2) Denote by $\mathcal{F}^\vee$ the linear dual (contragredient representation) of $\mathcal{F}$, and by $\overline{\mathcal{F}} := \mathcal{F}^\vee(-w)$ the "complex conjugate" of $\mathcal{F}$; the sheaves $\mathcal{F}$ and $\overline{\mathcal{F}}$ have, via $\iota$, complex conjugate local trace functions.

(2.1.3) Our first task is to give a diophantine calculation of the absolute moments $M_{2n}(G, V)$, $n \geq 1$, in terms of moments $S_{2n}$ of the local trace function of $\mathcal{F}$. For each finite extension field E/k, define the real number $S_{2n}(E, \mathcal{F})$ by

(2.1.3.1) $\quad S_{2n}(E, \mathcal{F}) :=$

$$(\#E)^{-\dim(S)-nw} \sum_{x \text{ in } S(E)} |\iota(\mathrm{Trace}(\mathrm{Frob}_{E,x} \mid \mathcal{F}))|^{2n}.$$

**Lemma 2.1.4** Hypotheses and notations as in 2.1.1-3 above, for each $n \geq 1$ we have the limit formula

$$M_{2n}(G, V) = \limsup_{E/k \text{ finite}} S_{2n}(E, \mathcal{F}).$$

**proof** The moment $M_{2n}(G, V)$ is the dimension of the space of G-invariants, or equivalently of $\pi_1{}^{geom}(S, s)$-invariants, in $(V\otimes V^\vee)^{\otimes n}$, i.e., it is the dimension of $H^0(S\otimes_k \overline{k}, (\mathcal{F}\otimes\overline{\mathcal{F}})^{\otimes n})$. So, by Poincare duality, we have

$$M_{2n}(G, V) = \dim H_c{}^{2\dim(S)}(S\otimes_k \overline{k}, (\mathcal{F}\otimes\overline{\mathcal{F}})^{\otimes n}).$$

Because $\mathcal{F}$ is pure or weight w, $(\mathcal{F}\otimes\overline{\mathcal{F}})^{\otimes n}$ is $\iota$-pure of weight 2nw, so this last cohomology group is $\iota$-pure of weight $2nw + 2\dim(S)$. So the endomorphism $A := \mathrm{Frob}_k/q^{wn+\dim(S)}$ acting on it has, via $\iota$, all its eigenvalues on the unit circle. By a standard compactness argument (cf. [Ka-SE, 2.2.2.1]), we recover the dimension of the cohomology group by the limsup formula

$\dim H_c^{2\dim(S)}(S\otimes_k\bar{k}, (\mathcal{F}\otimes\bar{\mathcal{F}})^{\otimes n})$

$= \limsup_m |\iota(\mathrm{Trace}(A^m \mid H_c^{2\dim(S)}(S\otimes_k\bar{k}, (\mathcal{F}\otimes\bar{\mathcal{F}})^{\otimes n})))|$

$= \limsup_{E/k \text{ finite}}$

$(\#E)^{-\dim(S)-nw} |\iota(\mathrm{Trace}(\mathrm{Frob}_E \mid H_c^{2\dim(S)}(S\otimes_k\bar{k}, (\mathcal{F}\otimes\bar{\mathcal{F}})^{\otimes n})))|$.

By [De-Weil II, 3.3.4], the lower cohomology groups $H_c^j$, $j < 2\dim(S)$, are $\iota$-mixed of strictly lower weight, so we get $M_{2n}(G, V)$ as the limsup, over E/k finite, of the quantities

$(\#E)^{-\dim(S)-nw} \Sigma_j |\iota( \Sigma_j (-1)^j\mathrm{Trace}(\mathrm{Frob}_E \mid H_c^j(S\otimes_k\bar{k}, (\mathcal{F}\otimes\bar{\mathcal{F}})^{\otimes n})))|$.

By the Lefschetz Trace Formula, this last quantity is precisely $S_{2n}(E, \mathcal{F})$. QED

**First Variant Lemma 2.1.5** Hypotheses and notations as in Lemma 2.1.4, suppose we are given in addition a $\bar{\mathbb{Q}}_\ell$-valued function $\varphi(E, x)$ on the set of pairs

(a finite extension field E/k, a point x in S(E))

such that there exists a positive real constant C for which we have the estimate

$|\iota(\varphi(E, x))| \le C(\#E)^{w - 1/2}$.

For each finite extension E/k, define the approximate moment $\tilde{S}_{2n}(E, \mathcal{F})$ by

$\tilde{S}_{2n}(E, \mathcal{F}) :=$

$(\#E)^{-\dim(S)-nw} \Sigma_{x \text{ in } S(E)} |\iota(\mathrm{Trace}(\mathrm{Frob}_{E,x} \mid \mathcal{F}) + \varphi(E, x))|^{2n}$.

Then we have the limit formula

$M_{2n}(G, V) = \limsup_{E/k \text{ finite}} \tilde{S}_{2n}(E, \mathcal{F})$.

**proof** One checks easily that $\tilde{S}_{2n}(E, \mathcal{F}) - S_{2n}(E, \mathcal{F}) \to 0$ as $\#E$ grows. QED

**Second Variant Lemma 2.1.6** Hypotheses and notations as in Lemma 2.1.5, suppose that S is an open subscheme of a smooth, geometrically connected k-scheme T/k (necessarily of the same dimension D). Suppose that we are given a $\bar{\mathbb{Q}}_\ell$-valued function

$\tau(E, x)$ on the set of pairs

(a finite extension field $E/k$, a point $x$ in $T(E)$),

such that whenever $x$ lies in $S(E)$, we have

$$\tau(E, x) = \mathrm{Trace}(\mathrm{Frob}_{E,x} \mid \mathcal{F}) + \varphi(E, x).$$

For each finite extension $E/k$, define the mock moment $T_{2n}(E, \mathcal{F})$ by

$$T_{2n}(E, \mathcal{F}) := (\#E)^{-\dim(S)-nw} \Sigma_{x \text{ in } T(E)} |\iota(\tau(E, x))|^{2n}.$$

Then we have the inequality

$$M_{2n}(G, V) \le \mathrm{limsup}_{E/k \text{ finite}} T_{2n}(E, \mathcal{F}).$$

**proof** Obvious from the previous result and the observation that for each $E/k$ we have

$$\tilde{S}_{2n}(E, \mathcal{F}) \le T_{2n}(E, \mathcal{F})$$

simply because we obtain $T_{2n}(E, \mathcal{F})$ by adding postive quantities to $\tilde{S}_{2n}(E, \mathcal{F})$. QED

## 2.2 Universal families of hypersurface sections

(2.2.1) Recall that $k$ is a finite field, and $X/k$ is a projective, smooth, geometrically variety of dimension $n + 1 \ge 1$, given with a projective embedding $X \subset \mathbb{P}$. We denote by $\mathrm{PHyp}_d/k$ the projective space of degree $d$ hypersurfaces in $\mathbb{P}$, and by

(2.2.1.1) $$\mathrm{Good}_X\mathrm{PHyp}_d \subset \mathrm{PHyp}_d$$

the dense open set consisting of those degree $d$ hypersurfaces $H$ which are transverse to $X$, i.e., such that the scheme-theoretic intersection $X \cap H$ is smooth and of codimension one in $X$. Over $\mathrm{Good}_X\mathrm{PHyp}_d$ we have the universal family of all smooth, degree $d$ hypersurface sections of $X$, say

(2.2.1.2) $$\pi : \mathrm{Univ}_d \to \mathrm{Good}_X\mathrm{PHyp}_d,$$

whose fibre over a degree $d$ hypersurface $H$ in $\mathbb{P}$ is $X \cap H$.

(2.2.2) For any finite extension $E/k$, and any point $H$ in $\mathrm{Good}_X\mathrm{PHyp}_d(E)$, the weak Lefschetz theorem tells us that the restriction map

$$H^i(X \otimes_k \bar{k}, \bar{\mathbb{Q}}_\ell) \to H^i((X \otimes_k \bar{k}) \cap H, \bar{\mathbb{Q}}_\ell)$$

is an isomorphism for $i < n$, and injective for $i = n$. By Poincare duality, the Gysin map

$$H^i((X \otimes_k \bar{k}) \cap H, \bar{\mathbb{Q}}_\ell) \to H^{i+2}(X \otimes_k \bar{k}, \bar{\mathbb{Q}}_\ell)(1)$$

is an isomorphism for $i > n$, and surjective for $i = n$. Thanks to the hard Lefschetz theorem, we know that, for $i = n$, the kernel of the

Gysin map is a subspace

$$\mathrm{Ev}^n((X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell) \subset H^n((X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell)$$

on which the cup-product remains non-degenerate, and which maps isomorphically to the quotient $H^n((X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell)/H^n(X\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell)$.

(2.2.3) Over the space $\mathrm{Good}_X\mathrm{PHyp}_d$, there is a lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}_d$, such that for any finite extension $E/k$, and any $E$-valued point $H$ of $\mathrm{Good}_X\mathrm{PHyp}_d$, the stalk of $\mathcal{F}_d$ at $H$ is $\mathrm{Ev}^n((X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell)$. The sheaf $\mathcal{F}_d$ is pure of weight $n$, and carries a cup-product autoduality toward $\bar{\mathbb{Q}}_\ell(-n)$. The autoduality is symplectic if $n$ is odd, and orthogonal if $n$ is even. For fixed $X$ but variable $d$, the rank $N_d$ of $\mathcal{F}_d$ is a polynomial in $d$ of degree $n+1$, of the form $\deg(X)d^{n+1}$ + lower terms.

**Theorem 2.2.4** Suppose that $n \geq 2$ is even, that $d \geq 3$, and that $N_d > 8$. Then the geometric monodromy group $G_d$ of the lisse sheaf $\mathcal{F}_d$ is the full orthogonal group $O(N_d)$.

**proof** The group $G_d$ is a priori a Zariski closed subgroup of $O(N_d)$. We first recall that $G_d$, indeed its subgroup $\rho_{\mathcal{F}_d}(\pi_1{}^{\mathrm{geom}}(\mathrm{Good}_X\mathrm{PHyp}_d))$, contains a reflection.

Take a sufficiently general line $L$ in $\mathrm{PHyp}_d$. Over its intersection $L - \Delta$ with $\mathrm{Good}_X\mathrm{PHyp}_d$, we get a Lefschetz pencil of smooth hypersurface sections of degree $d$ of $X$. Denote by

$$i : L - \Delta \to \mathrm{Good}_X\mathrm{PHyp}_d$$

the inclusion. We have the inequality

$$\#\Delta(\bar{k}) \geq 1 \text{ if } N_d \neq 0,$$

because $\mathrm{Ev}^n((X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell)$ is spanned by the images, using all possible "chemins", of the vanishing cycles, one at each point of $\Delta(\bar{k})$, cf. [De-Weil II, 4.2.4 and 4.3.9]. [So long as char(k) is not 2, we can choose a single chemin for each vanishing cycle, and we have the inequality $\#\Delta(\bar{k}) \geq N_d$, cf. [SGA 7, Expose XVIII, 6.6 and 6.6.1]]

By the Picard-Lefschetz formula [SGA 7, Exposé XV, 3.4], each of the $\#\Delta(\bar{k})$ local monodromies in a Lefschetz pencil is a reflection.

Thus $\pi_1^{\mathrm{geom}}(L - \Delta)$ contains elements which act on $i^*\mathcal{F}_d$ as reflections, and their images in $\pi_1^{\mathrm{geom}}(\mathrm{Good}_X\mathrm{PHyp}_d)$ act as reflections on $\mathcal{F}_d$.

In view of Theorem 1.4.6, it suffices to show that, denoting by $V_d$ the representation of $G_d$ given by $\mathcal{F}_d$, we have $M_4(G_d, V_d) = 3$. Since $G_d$ lies in $O(N_d)$ and $N_d > 1$, we have the a priori inequality

$$M_4(G_d, V_d) \geq M_4(O(N_d), \mathrm{std}) = 3.$$

So the desired conclusion results from the following theorem.

**Theorem 2.2.5** Suppose that $n \geq 1$ and $d \geq 3$. Then $M_4(G_d, V_d) \leq 3$. If $n = 0$ and $d \geq 3$, we have $M_4(G_d, V_d) \leq 4$.

**proof** Denote by $\mathrm{Hyp}_d/k$ the affine space over $k$ which is the affine cone of the projective space $\mathrm{PHyp}_d/k$. For any $k$-algebra $A$, the $A$-valued points of $\mathrm{Hyp}_d$ are the elements of $H^0(\mathbb{P}, \mathcal{O}(d))\otimes_k A$. The natural projection map

$$\overline{\pi} : \mathrm{Hyp}_d - \{0\} \to \mathrm{PHyp}_d$$

is a (Zariski locally trivial) $\mathbb{G}_m$-bundle. We denote by

$$\mathrm{Good}_X\mathrm{Hyp}_d \subset \mathrm{Hyp}_d - \{0\}$$

the dense open set which is the inverse image of $\mathrm{Good}_X\mathrm{PHyp}_d$, and by

$$\pi : \mathrm{Good}_X\mathrm{Hyp}_d \to \mathrm{Good}_X\mathrm{PHyp}_d$$

its projection. Thus we have a cartesian diagram

$$\begin{array}{ccc} \mathrm{Good}_X\mathrm{Hyp}_d & \subset & \mathrm{Hyp}_d - \{0\} \\ \overline{\pi}\downarrow & & \pi\downarrow \\ \mathrm{Good}_X\mathrm{PHyp}_d & \subset & \mathrm{PHyp}_d \end{array}$$

We form the lisse sheaf $\pi^*\mathcal{F}_d$ on $\mathrm{Good}_X\mathrm{Hyp}_d$. By [Ka-La-FGCFT, Lemma 2, part (2)], for any geometric point $\xi$ of $\mathrm{Good}_X\mathrm{Hyp}_d$, the map

$$\pi_* : \pi_1^{\mathrm{geom}}(\mathrm{Good}_X\mathrm{Hyp}_d, \xi) \to \pi_1^{\mathrm{geom}}(\mathrm{Good}_X\mathrm{PHyp}_d, \pi(\xi))$$

is surjective. So we recover $G_d$ as the Zariski closure of the image of $\pi_1^{\mathrm{geom}}(\mathrm{Good}_X\mathrm{Hyp}_d)$ acting on $\pi^*\mathcal{F}_d$.

The advantage is that the base space is now a dense open set of an affine space, namely $\mathrm{Hyp}_d$. We will now apply the diophantine method explained above, to the sheaf $\pi^*\mathcal{F}_d$ on the dense open set $\mathrm{Good}_X\mathrm{Hyp}_d$ of $\mathrm{Hyp}_d$.

Let $E/k$ be a finite extension field, and $H$ an $E$-valued point of $\mathrm{Good}_X\mathrm{Hyp}_d$. Then the stalk of $\pi^*\mathcal{F}_d$ at $H$ is $\mathrm{Ev}^n((X\otimes_k\bar{k})\cap(H = 0), \bar{\mathbb{Q}}_\ell)$.

**Key Lemma 2.2.6** Given $X/k$ as above, denote by $\Sigma(X\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell)$ the sum of the $\bar{\mathbb{Q}}_\ell$-Betti numbers. Then for any finite extension field $E/k$, and for any $E$-valued point $H$ of $\mathrm{Good}_X\mathrm{Hyp}_d$, putting $Y := X\cap(H = 0)$, we have the estimate

$$|\mathrm{Trace}(\mathrm{Frob}_{E,H} \mid \pi^*\mathcal{F}_d) - (-1)^n(\#Y(E) - \#X(E)/\#E)|$$
$$\leq\Sigma(X\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell)(\#E)^{(n-1)/2}.$$

**proof** Use the Lefschetz Trace Formula on $Y$ to write $\#Y(E)$ as a sum of three terms:

$$\#Y(E) = \Sigma_{i \leq n-1} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H^i(Y\otimes_E\bar{k}, \bar{\mathbb{Q}}_\ell))$$
$$+ (-1)^n\mathrm{Trace}(\mathrm{Frob}_E \mid H^n(Y\otimes_E\bar{k}, \bar{\mathbb{Q}}_\ell))$$
$$+ \Sigma_{i \geq n+1} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H^i(Y\otimes_E\bar{k}, \bar{\mathbb{Q}}_\ell)).$$

Use the same formula to write $\#X(E)/\#E$ as the sum of three terms:

$$\#X(E)/\#E = \Sigma_{i \leq n+1} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H^i(X\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell)(1))$$
$$+ (-1)^{n+2}\mathrm{Trace}(\mathrm{Frob}_E \mid H^{n+2}(X\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell)(1))$$
$$+ + \Sigma_{i \geq n+3} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H^i(X\otimes_k k, \bar{\mathbb{Q}}_\ell)(1)).$$

By the Poincare dual of the weak Lefschetz theorem, the third terms in the two expressions are equal. The difference of the second terms is precisely $(-1)^n\mathrm{Trace}(\mathrm{Frob}_E \mid \mathrm{Ev}^n((X\otimes_k\bar{k})\cap(H = 0), \bar{\mathbb{Q}}_\ell))$, i.e., it is $(-1)^n\mathrm{Trace}(\mathrm{Frob}_{E,H} \mid \pi^*\mathcal{F}_d)$. The difference of the first terms is

$$\Sigma_{i \leq n-1} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H^i(Y\otimes_E\bar{k}, \bar{\mathbb{Q}}_\ell))$$
$$- \Sigma_{i \leq n+1} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H^i(X\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell)(1)).$$

By Deligne's Weil I, each cohomology group occurring here is pure of some weight $\leq n - 1$, so we get the asserted estimate with the constant

$$\Sigma_{i \leq n-1} h^i(Y\otimes_E\bar{k}, \bar{\mathbb{Q}}_\ell) + \Sigma_{i \leq n+1}h^i(X\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell).$$

Using weak Lefschetz, this is equal to

$$= \Sigma_{i \le n-1} h^i(X\otimes_k\overline{k}, \overline{\mathbb{Q}}_\ell) + \Sigma_{i \le n+1} h^i(X\otimes_k\overline{k}, \overline{\mathbb{Q}}_\ell).$$

Using Poincare duality on X, this in turn is equal to

$$= \Sigma_{i \ge n+3} h^i(X\otimes_k\overline{k}, \overline{\mathbb{Q}}_\ell) + \Sigma_{i \le n+1} h^i(X\otimes_k\overline{k}, \overline{\mathbb{Q}}_\ell)$$

$$\le \Sigma_i h^i(X\otimes_k\overline{k}, \overline{\mathbb{Q}}_\ell) := \Sigma(X\otimes_k\overline{k}, \overline{\mathbb{Q}}_\ell).$$ QED

For any finite extension field E/k, and for any E-valued point H of $Hyp_d$, we define

$$\tau(E, H) := (-1)^n((-1)^n(\#(X\cap(H=0))(E) - \#X(E)/\#E).$$

Notice that $\tau$ takes values in $\mathbb{Q}$.

We then define the mock moment $T_4(E, \pi^*\mathcal{F}_d)$ by

$$T_4(E, \pi^*\mathcal{F}_d) := (\#E)^{-\dim(Hyp_d)-2n} \Sigma_{H \text{ in } Hyp_d(E)} |\tau(E, H)|^4$$

$$= (\#E)^{-\dim(Hyp_d)-2n} \Sigma_{H \text{ in } Hyp_d(E)} (\#(X\cap(H=0))(E) - \#X(E)/\#E)^4.$$

[Because $\tau$ takes values in $\mathbb{Q}$, there is no need for the $\iota$ which figured in the general definition, where $\tau$ was allowed to be $\overline{\mathbb{Q}}_\ell$-valued.]

In view of the Second Variant Lemma 2.1.6, Theorem 2.2.5 now results from the following theorem.

**Theorem 2.2.7** Let X/k be as above, of dimension $n + 1 \ge 1$. If $n \ge 1$, then for any $d \ge 3$, we have the estimate

$$|T_4(E, \pi^*\mathcal{F}_d) - 3| = O((\#E)^{-1/2}).$$

If $n = 0$, then for any $d \ge 3$, we have the estimate

$$|T_4(E, \pi^*\mathcal{F}_d) - 4| = O((\#E)^{-1/2}).$$

**proof** Fix a finite field extension E/k with $\#E \ge 6$. We will use an exponential sum method to calculate $T_4(E, \pi^*\mathcal{F}_d)$ in closed form. Fix a nontrivial $\mathbb{C}^\times$-valued additive character $\psi$ of E. View the ambient $\mathbb{P} = \mathbb{P}^m$ as the space of lines in $\mathbb{A}^{m+1}$. For each point x in $\mathbb{P}^m(E)$, choose a point $\tilde{x}$ in $\mathbb{A}^{m+1}(E) - \{0\}$ which lifts it. For any fixed H in $Hyp_d(E)$, the value $H(\tilde{x})$ depends upon the choice of $\tilde{x}$ lifting x, but only up to an $E^\times$-multiple. So the sum

$$\Sigma_{\lambda \text{ in } E^\times} \psi(\lambda H(\tilde{x}))$$

depends only on the original point x in $\mathbb{P}(E)$. By the orthogonality relations for characters, we have

$$\Sigma_{\lambda \text{ in } E^\times} \psi(\lambda H(\tilde{x})) = -1 + \Sigma_{\lambda \text{ in } E} \psi(\lambda H(\tilde{x}))$$
$$= \#E - 1, \text{ if } H(x) = 0,$$
$$= -1, \text{ if not.}$$

So we get the identity

$$\Sigma_{x \text{ in } X(E)} \Sigma_{\lambda \text{ in } E^\times} \psi(\lambda H(\tilde{x})) = (\#E)(\#(X \cap (H=0))(E)) - \#X(E)$$
$$= (-1)^n (\#E)\tau(E, H).$$

This in turn gives the identity

$$(\#E)^{\dim(\mathrm{Hyp}_d)+2n+4}\, T_4(E, \pi^*\mathcal{F}_d)$$
$$= \Sigma_{H \text{ in } \mathrm{Hyp}_d(E)} (\Sigma_{x \text{ in } X(E)} \Sigma_{\lambda \text{ in } E^\times} \psi(\lambda H(\tilde{x})))^4.$$

We next open the inner sum and interchange orders of summation, to get

$$= \Sigma_{(x_i) \text{ in } X(E)^4} \Sigma_{(\lambda_i) \text{ in } (E^\times)^4} \Sigma_{H \text{ in } \mathrm{Hyp}_d(E)} \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i H(\tilde{x}_i)).$$

The key observation is given by the following lemma.

**Singleton Lemma 2.2.8** Suppose $\#E \geq 4$. Given four (not necessarily distinct) points $x_1$, $x_2$, $x_3$, $x_4$ in $\mathbb{P}(E)$, suppose among them there is a singleton, i.e., a point which is not equal to any of the others. Then for any $(\lambda_i)$ in $(E^\times)^4$, we have the vanishing

$$\Sigma_{H \text{ in } \mathrm{Hyp}_d(E)} \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i H(\tilde{x}_i)) = 0.$$

Before proving this lemma, it will be convenient to give two other lemmas.

**Lemma 2.2.9** If $\#E \geq 4$, then given four (not necessarily distinct) points $x_1$, $x_2$, $x_3$, $x_4$ in $\mathbb{P}(E)$, there exists an E-rational hyperplane L in $\mathbb{P}$, i.e., a point L in $\mathrm{PHyp}_1(E)$, such that all four points $x_i$ lie in the affine open set $\mathbb{P}^m[1/L]$.

**proof** Say $\mathbb{P}$ is $\mathbb{P}^m$. In the dual projective space, the set of hyperplanes through a given point $x_i$ in $\mathbb{P}^m(E)$ form a $\mathbb{P}^{m-1}$, so there are precisely

$$((\#E)^m - 1)/(\#E - 1)$$

E-rational hyperplanes through $x_i$. So there are at least

$$((\#E)^{m+1} - 1)/(\#E - 1) - 4((\#E)^m - 1)/(\#E - 1)$$

E-rational hyperplanes which pass through none of the $x_i$. As $\#E$ is at least 4, this difference is strictly positive. QED

**Evaluation Lemma 2.2.10** Let E be a field, $m \geq 1$ and $d \geq 1$ integers. Denote by $\mathrm{Poly}_{\leq d}(E)$ the E-vector space of E-rational polynomial functions on $\mathbb{A}^m$. For any integer $r \leq d + 1$, and for any r distinct points $x_i$, i = 1 to r, in $\mathbb{A}^m(E)$, the E-linear multi-evaluation map

$$\mathrm{Poly}_{\leq d}(E) \to E^r$$
$$f \mapsto (f(x_1), \ldots, f(x_r))$$

is surjective.

**proof** The map being E-linear, its surjectivity map be checked over any extension field. Passing to a large enough such extension, we may add additional distinct points, so that our $x_i$ are the first r of d+1 distinct points. It suffices to prove the lemma in the hardest case r = d+1 (then project onto the first r coordinates in the target). To do this hardest case, we first treat the case m=1. In this case, source and target have the same dimension, d+1, so it suffices that the map be injective. But its kernel consists of those polynomials in one variable of degree at most d, which have d+1 distinct zeroes. To do the general case, it suffices to find a linear form T from $\mathbb{A}^m$ to $\mathbb{A}^1$ under which the d+1 points $x_i$ have d+1 distinct images. For then already polynomials of degree at most d in T will be a subspace of the source $\mathrm{Poly}_{\leq d}(E)$ which will map onto $E^r$. We can do this as soon as $\#E \geq \mathrm{Binom}(d+1, 2)$. Indeed, we are looking for a linear form T with the property that for each of the Binom(d+1, 2) pairs $(x_i, x_j)$ with $i < j$, we have $T(x_i) - T(x_j) \neq 0$. For each such pair, the set of T for which $T(x_i) - T(x_j) = 0$ is a hyperplane in the dual space. So we need T to not lie in the union of Binom(d+1, 2) linear subspaces of codimension one. Since they all intersect in zero, their union has cardinality strictly less that $\mathrm{Binom}(d+1, 2)(\#E)^{m-1}$. So as soon as $\#E \geq \mathrm{Binom}(d+1, 2)$, the desired T exists. QED

With these preliminaries out of the way, we can prove the Singleton Lemma 2.2.8. Because $\#E \geq 4$, we can find a non-zero linear form L in $\mathrm{Hyp}_1(E)$ such that our four points $x_i$ all lie in $\mathbb{P}]1/L] \cong \mathbb{A}^m$. By means of the map $H \mapsto H/L^d$, we get an E-linear isomorphism

$$\mathrm{Hyp}_d(E) \cong \mathrm{Poly}_{\leq d}(E)$$

of $\mathrm{Hyp}_d(E)$ with the E-rational polynomial functions on $\mathbb{P}]1/L] \cong \mathbb{A}^m$ of degree at most d.

Moreover, for any x in $\mathbb{P}[1/L](E)$, and any lifting $\tilde{x}$ in $\mathbb{A}^{m+1}(E)$, the two E-linear forms on $\mathrm{Hyp}_d(E)$,

$$H \mapsto H(\tilde{x})$$

and

$$H \to (H/L^d)(x),$$

are proportional. So whatever the four points $(x_i)$ in $\mathbb{P}[1/L](E) \cong \mathbb{A}^m(E)$, we can rewite the sum

$$\Sigma_{H \text{ in } \mathrm{Hyp}_d(E)} \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i H(\tilde{x}_i))$$
$$= \Sigma_{h \text{ in } \mathrm{Poly}_{\leq d}(E)} \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i h(x_i)).$$

Renumbering, we may suppose that $x_1$ is a singleton. We consider separately various cases (which, up to renumbering, cover all the cases when $x_1$ is a singleton).

If the four points are all distinct, then as h runs over $\mathrm{Poly}_{\leq d}(E)$, the vector $(h(x_i))$ runs over $E^4$, and our sum becomes #(Ker of eval at $(x_i)$) times

$$\Sigma_{(t_i) \text{ in } E^4} \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i t_i).$$

Since the vector $(\lambda_i)$ is nonzero, $(t_i) \mapsto \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i t_i)$ is a nontrivial additive character of $E^4$, so the inner sum vanishes.

If the three remaining points are all equal, then as h runs over $\mathrm{Poly}_{\leq d}(E)$, the vector $(h(x_1), h(x_2))$ runs over $E^2$, and our sum becomes #(Ker of eval at $(x_1, x_2)$) times

$$\Sigma_{(t_1, t_2) \text{ in } E^2} \psi(\lambda_1 t_1 + (\lambda_2 + \lambda_3 + \lambda_4)t_2).$$

Since the vector $(\lambda_1, \lambda_2 + \lambda_3 + \lambda_4)$ is nonzero, the sum again vanishes.

If the first three points are distinct, but $x_4 = x_3$, then our sum becomes #(Ker of eval at $(x_1, x_2, x_3)$) times

$$\Sigma_{(t_1, t_2, t_3) \text{ in } E^3} \psi(\lambda_1 t_1 + \lambda_2 t_2 + (\lambda_3 + \lambda_4)t_3).$$

Since the vector $(\lambda_1, \lambda_2, \lambda_3 + \lambda_4)$ is nonzero, the sum again vanishes. QED

In exactly the same way, we prove the following two elementary lemmas.

**Twinning Lemma 2.2.11** Suppose $\#E \geq 2$. Given two distinct points $x_1$, $x_2$ in $\mathbb{P}(E)$, put $x_3 = x_1$, and put $x_4 = x_2$. Then for $(\lambda_i)$ in $(E^\times)^4$, we have

$$\Sigma_{H \text{ in } Hyp_d(E)} \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i H(\tilde{x}_i))$$
$$= \#Hyp_d(E), \text{ if } \lambda_1 + \lambda_2 = \lambda_3 + \lambda_4 = 0,$$
$$= 0, \text{ otherwise.}$$

**Quadruples Lemma 2.2.12** Given a point $x$ in $\mathbb{P}(E)$, put $x_i = x$ for $i = 1$ to 4. Then for $(\lambda_i)$ in $(E^\times)^4$, we have

$$\Sigma_{H \text{ in } Hyp_d(E)} \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i H(\tilde{x}_i))$$
$$= \#Hyp_d(E), \text{ if } \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0,$$
$$= 0, \text{ otherwise.}$$

**proof of Theorem 2.2.7 suite** Recall that we have the identity

$$(\#E)^{\dim(Hyp_d)+2n+4} T_4(E, \pi^*\mathcal{F}_d)$$
$$= \Sigma_{(x_i) \text{ in } X(E)^4} \Sigma_{(\lambda_i) \text{ in } (E^\times)^4} \Sigma_{H \text{ in } Hyp_d(E)} \psi(\Sigma_{i=1 \text{ to } 4} \lambda_i H(\tilde{x}_i)).$$

We now break up this sum by the coincidence pattern of the four-tuple $(x_1, x_2, x_3, x_4)$.

If there is any singleton, the entire inner sum vanishes.

If all the $x_i$ coincide, the inner sum is

$$\#Hyp_d(E) \times \#\{(\lambda_i) \text{ in } (E^\times)^4 \text{ with } \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0\}.$$

This case occurs $\#X(E)$ times, one for each of the possible common values of the $x_i$.

If there are no singletons and exactly two among the $x_i$ are distinct, put $x := x_1$, and take for $y$ the other. Then the pattern is either $(x, x, y, y)$ or $(x, y, x, y)$ or $(x, y, y, x)$. In each case, the inner sum is

$$\#\mathrm{Hyp}_d(E)\times\#\{(\lambda_i) \text{ in } (E^\times)^4 \text{ with } \lambda_1 + \lambda_2 = \lambda_3 + \lambda_4 = 0\}$$
$$= \#\mathrm{Hyp}_d(E)\times(\#E - 1)^2.$$

This case occurs $3(\#X(E))(\#X(E) - 1)$ times, 3 for the possible repeat pattern, $\#X(E)$ for the choice of $x_1$, $\#X(E) - 1$ for the choice of $y \neq x_1$.

So all in all, we get a closed formula

$$(\#E)^{\dim(\mathrm{Hyp}_d)+2n+4}\ T_4(E, \pi^*\mathcal{F}_d)$$
$$= 3(\#X(E))(\#X(E) - 1)(\#\mathrm{Hyp}_d(E))(\#E - 1)^2$$
$$+(\#X(E))(\#\mathrm{Hyp}_d(E))(\#\{(\lambda_i) \text{ in } (E^\times)^4 \text{ with } \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0\}).$$

Dividing through by $\#\mathrm{Hyp}_d(E) = (\#E)^{\dim(\mathrm{Hyp}_d)}$, we get

$$(\#E)^{2n+4}\ T_4(E, \pi^*\mathcal{F}_d)$$
$$= 3(\#X(E))(\#X(E) - 1)(\#E - 1)^2$$
$$+(\#X(E))(\#\{(\lambda_i) \text{ in } (E^\times)^4 \text{ with } \lambda_1 + \lambda_2 = \lambda_3 + \lambda_4 = 0\}).$$

**Lemma 2.2.13** We have the identity

$$\#\{(\lambda_i) \text{ in } (E^\times)^4 \text{ with } \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0\}$$
$$= (\#E - 1)^3 - ((\#E - 1)^2 - (\#E - 1)).$$

**proof of Lemma 2.2.13** View the set in question as the subset of $(E^\times)^3$ where $\lambda_1 + \lambda_2 + \lambda_3 \neq 0$ (solve for $\lambda_4$). Its complement in $(E^\times)^3$ is the subset of $(E^\times)^2$ where $\lambda_1 + \lambda_2 \neq 0$ (solve for $\lambda_3$). The complement in $(E^\times)^2$ of this last set is the set of pairs $(\lambda, -\lambda)$. QED

So now we have the identity

$$(\#E)^{2n+4}\ T_4(E, \pi^*\mathcal{F}_d)$$
$$= 3(\#X(E))(\#X(E) - 1)(\#E - 1)^2$$
$$+(\#X(E))((\#E - 1)^3 - ((\#E - 1)^2 - (\#E - 1))).$$

Dividing through, we get

$$T_4(E, \pi^*\mathcal{F}_d)$$
$$= 3(\#X(E)/(\#E)^{n+1})(\#X(E)/(\#E)^{n+1} - 1/(\#E)^{n+1})(1 - 1/\#E)^2$$
$$+(\#X(E)/(\#E)^{n+1})((\#E - 1)^3 - ((\#E - 1)^2 - (\#E - 1)))//(\#E)^{n+3}.$$

By Lang-Weil, we have

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

So the first term is $3 + O((\#E)^{-1/2})$. If $n = 0$, the second term is $1 + O((\#E)^{-1/2})$, while if $n \geq 1$ the second term is $O((\#E)^{-1})$. This concludes the proof of Theorem 2.2.7, and, with it, the proofs of Theorems 2.2.5 and 2.2.4. QED

(2.2.14) We now give a supplement to Theorem 2.2.4, by combining our results with those of Deligne [De-Weil II, 4.4.1, $4.4.2^s$, and 4.4.9]. This supplement will itself be supplemented in 2.3.6.

**Theorem 2.2.15 (supplement to Theorem 2.2.4)** Suppose that $n \geq 2$ is even, and that $d \geq 3$.
1) If $N_d$ is 1, 3, 4, or 5, or if $N_d \geq 9$, then the geometric monodromy group $G_d$ of the lisse sheaf $\mathcal{F}_d$ is the full orthogonal group $O(N_d)$.
2) If $N_d$ is 6, 7, or 8, then $G_d$ is either the full orthogonal group $O(N_d)$, or $G_d$ is the Weyl group of the root system $E_\alpha$, $\alpha := N_d$, in its standard $N_d$-dimensional representation as a Weyl group.
3) If $N_d = 2$, then $G_d$ is the symmetric group $S_3$ in the representation $Aug_2$.

**proof** According to [De-Weil II, 4.4.1, $4.4.2^s$, and 4.4.9], if $N_d \geq 1$, $G_d$ is either the full orthogonal group $O(N_d)$, or it is a finite reflection group. Moreover, the only finite reflection groups that arise are the Weyl groups of root systems of type $A_\alpha$ for $\alpha \geq 1$, $D_\alpha$ for $\alpha \geq 4$, or $E_\alpha$ for $\alpha = 6, 7$, or 8, in their standard $\alpha$-dimensional representations.

We have shown (Theorem 2.2.5) that for any $d \geq 3$, we have $M_4(G_d, V_d) \leq 3$. Suppose first that $G_d$ is finite, and that $N_d \geq 3$.

We cannot have the Weyl group of $A_\alpha$ for any $\alpha \geq 3$, in its standard representation, i.e., we cannnot have he group $S_{\alpha+1}$ in the representation $Aug_\alpha$, because $M_4(S_{\alpha+1}, Aug_\alpha) > 3$ for $\alpha \geq 3$. Indeed, for $\alpha \geq 4$ this is proven in Lemma 1.4.5, and for $\alpha = 3$ it is an elementary calculation we leave to the reader (or the reader can observe that $A_3 = D_3$, and see the discussion of $D_\alpha$ just below).

We can rule out having the Weyl group of $D_\alpha$ for any $\alpha \geq 3$, in its standard representation, as follows. By Theorem 1.3.2, $G_d$ is primitive. But the standard representation of the Weyl group of $D_\alpha$ is induced (in the Bourbaki notations [Bour-L6, Planche IV, page 257], the lines spanned by the $\varepsilon_i$ are permuted among themselves).

So the only surviving finite group cases with $N_d \geq 3$ are the Weyl groups of $E_6$, $E_7$, and $E_8$ in their standard representations.

If $N_d = 2$, then $G_d$ must be finite, because it is a semisimple subgroup of $O(2)$. The only possibility is the Weyl group of $A_2$, i.e., $S_3$ in the representation $Aug_2$.

If $N_d = 1$, then $O(1) = \{\pm 1\} = S_2$ in $Aug_1$, so there is only one possibility. QED

**Remark 2.2.16** The Weyl groups of type E in their standard Weyl group representations all have fourth moment 3. The Weyl group of $E_6$ occurs as the monodromy group attached to the universal family of smooth cubic surfaces in $\mathbb{P}^3$. [Since a smooth cubic surface has middle Betti number 7, and all its cohomology is algebraic, we have a case with $d = 3$, $N_d = 6$, and $G_d$ finite, so necessarily the Weyl group of $E_6$, cf. also [Beau].] We do not know if the Weyl groups of $E_7$ or of $E_8$ can occur as the monodromy group of the universal family of smooth hypersurface sections of degree $d \geq 3$ of some projective smooth X. [These groups certainly occur as the monodromy of suitable families of del Pezzo surfaces, but those families are not of the required form.]

**Remark 2.2.17** In Theorems 2.2.4 and 2.2.15, the hypothesis that d be at least 3 is absolutely essential. Indeed, fix an even integer $n \geq 0$, take for X a smooth quadric hypersurface in $\mathbb{P}^{n+2}$, and consider the universal family of smooth, degree $d=2$ hypersurface sections of X. Each member of this family is a smooth complete intersection of multi-degree (2, 2) in $\mathbb{P}^{n+2}$, so has middle betti number $n+4$, and all cohomology algebraic. This family has $N_d = n+3$, and its finite $G_d$ is the Weyl group of $D_{n+3}$. [Indeed, if $n = 0$ the two possibilities coincide. If $n \geq 2$, the only other possibility is $S_{n+4}$ in $Aug_{n+3}$, or, if n

= 4, the Weyl group of $E_7$ in its standard Weyl group representation, both of which are primitive. But by [Reid], cf. [Beau, page 16], the monodromy for the universal family of smooth complete intersections of multi-degree (2, 2) in $\mathbb{P}^{n+2}$ is the Weyl group of $D_{n+3}$. So our $G_d$ is a subgroup of the Weyl group of $D_{n+3}$. In particular, our $G_d$ is imprimitive.]

## 2.3 Higher Moments

(2.3.1) The same ideas used in proving Theorem 2.2.5 allow one to prove the following estimate for higher moments.

**Theorem 2.3.2** Suppose that $n \geq 1$ and $d \geq 3$. For any integer $b \geq 1$ with $2b \leq d + 1$, we have the estimate

$$M_{2b}(G_d, V_d) \leq (2b)!! := \prod_{j = 1 \text{ to } b}(2j - 1).$$

**proof** We proceed as in the proof of Theorem 2.2.7. We define the mock moment $T_{2b}(E, \pi^*\mathcal{F}_d)$ by

$$T_{2b}(E, \pi^*\mathcal{F}_d) := (\#E)^{-\dim(\mathrm{Hyp}_d)-bn} \Sigma_{H \text{ in } \mathrm{Hyp}_d(E)} |\tau(E, H)|^{2b}$$

$$= (\#E)^{-\dim(\mathrm{Hyp}_d)-bn} \Sigma_{H \text{ in } \mathrm{Hyp}_d(E)} (\#(X\cap(H=0))(E) - \#X(E)/\#E)^{2b}.$$

It suffices to show that

$$|T_{2b}(E, \pi^*\mathcal{F}_d) - (2b)!!| = O((\#E)^{-1/2}).$$

Exactly as in the discussion of $T_4$, we find for $T_{2b}$ the identity

$$(\#E)^{\dim(\mathrm{Hyp}_d)+bn+2b} T_{2b}(E, \pi^*\mathcal{F}_d)$$

$$= \Sigma_{H \text{ in } \mathrm{Hyp}_d(E)} (\Sigma_{x \text{ in } X(E)} \Sigma_{\lambda \text{ in } E^\times} \psi(\lambda H(\tilde{x})))^{2b}.$$

We next open the inner sum and interchange orders of summation, to get

$$= \Sigma_{(x_i) \text{ in } X(E)^{2b}} \Sigma_{(\lambda_i) \text{ in } (E^\times)^{2b}} \Sigma_{H \text{ in } \mathrm{Hyp}_d(E)} \psi(\Sigma_{i=1 \text{ to } 2b} \lambda_i H(\tilde{x}_i)).$$

We next break up this sum according to the coincidence pattern of the 2b not necessarily distinct points $x_1, ..., x_{2b}$ in $X(E)$.

The coincidence pattern among the $x_i$ gives a partition $\mathcal{P}$ of the set $\{1, 2, ..., 2b\}$ into $\#\mathcal{P}$ disjoint nonempty subsets $S_\alpha$: $x_i = x_j$ if and only if i and j lie in the same $S_\alpha$.

Fix a point $(x_i)$ in $X(E)^{2b}$ with partition $\mathcal{P}$. Exaactly as in the proof of Theorem 2.2.7, the innermost sum vanishes unless, for each

$S_\alpha$ in $\mathcal{P}$, we have $\Sigma_{i \text{ in } S_\alpha}\lambda_i = 0$, in which case the innermost sum is equal to $(\#E)^{\dim(\mathrm{Hyp}_d)}$. So the inner double sum is equal to $(\#E)^{\dim(\mathrm{Hyp}_d)}\Pi_{\alpha \text{ in } \mathcal{P}}\ \#\{(\lambda_i)_{i \text{ in } S_\alpha}$ with $\lambda_i$ in $E^\times$ and $\Sigma_{i \text{ in } S_\alpha}\lambda_i = 0\}$. This visibly vanishes if some $S_\alpha$ is a singleton. More generally,consider the sequence of integer polynomials $P_r(X)$, $r \geq 1$, defined inductively by

$$P_1(X) = 0,$$

$$P_r(X) = X^{r-1} - P_{r-1}(X),$$

i.e.,

$$P_r(X) = X^{r-1} - X^{r-2} + X^{r-3} \ldots + (-1)^{r-2}X.$$

We have the elementary identity

$$\#\{(\lambda_i)_{i \text{ in } S_\alpha} \text{ with } \lambda_i \text{ in } E^\times \text{ and } \Sigma_{i \text{ in } S_\alpha}\lambda_i = 0\} = P_{\#S_\alpha}(\#E).$$

So the innermost double sum is

$$(\#E)^{\dim(\mathrm{Hyp}_d)}\Pi_{\alpha \text{ in } \mathcal{P}}\ P_{\#S_\alpha}(\#E).$$

This vanishes if any $S_\alpha$ is a singleton, otherwise it is given by a polynomial in $\#E$ of the form

$$(\#E)^{\dim(\mathrm{Hyp}_d)}\Pi_{\alpha \text{ in } \mathcal{P}}\ (\#E)^{\#S_\alpha - 1} + \text{lower terms}$$
$$= (\#E)^{\dim(\mathrm{Hyp}_d) + 2b - \#\mathcal{P}} + \text{lower terms}.$$

The number of points $(x_i)$ in $X(E)^{2b}$ with given partition $\mathcal{P}$ is

$$\Pi_{j = 0 \text{ to } \#\mathcal{P} - 1}\ (\#X(E) - j) = \#X(E)^{\#\mathcal{P}} + \text{lower terms}$$
$$= (\#E)^{(n+1)\#\mathcal{P}} + O((\#E)^{(n+1)\#\mathcal{P} - 1/2}).$$

As we have seen above, partitions with a singleton do not contribute.

For each partition $\mathcal{P}$ without singletons, the total contribution of all points with that coincidence pattern is thus the product

$$((\#E)^{\dim(\mathrm{Hyp}_d) + 2b - \#\mathcal{P}} + \text{lower terms})$$
$$\times((\#E)^{(n+1)\#\mathcal{P}} + O((\#E)^{(n+1)\#\mathcal{P} - 1/2}))$$
$$= (\#E)^{\dim(\mathrm{Hyp}_d) + 2b + n\#\mathcal{P}}(1 + \ + O(\#E)^{-1/2}).$$

So the terms of biggest size $(\#E)^{\dim(\mathrm{Hyp}_d) + 2b + nb}$ come from those $\mathcal{P}$ without singletons having exact b members, and there are exactly $(2b)!!$ such partitions. QED

(2.3.3) The relevance of Theorem 2.3.2 is this. Recall (cf. [Weyl, Theorem (2.9.A), page 53 and Theorem (6.1.A), page 167], [ABP, Appendix I, pages 322-326]) that for O(V) or Sp(V), the invariants in the dual of any even tensor power $V^{\otimes 2b}$, $b \geq 1$, are the $\mathbb{C}$-span of the "complete contractions", i.e., the linear forms on $V^{\otimes 2b}$ obtained by choosing a partition $\mathcal{P}$ of the index set $\{1, 2, ..., 2b\}$ into b disjoint sets $S_\alpha$ of pairs, say $S_\alpha = \{i_\alpha, j_\alpha\}$ with $i_\alpha < j_\alpha$, and mapping

$$v_1 \otimes v_2 \otimes ... \otimes v_{2b} \mapsto \prod_{\alpha \text{ in } \mathcal{P}} \langle v_{i_\alpha}, v_{j_\alpha} \rangle$$

There are (2b)!! such complete contractions. If $\dim(V) \geq 2b$, they are linearly independent (cf. [Weyl, section 5 of Chapter V, pages 147-149]). So for any $N \geq 2b$, we have

$$M_{2b}(O(N), \text{std}) = (2b)!!,$$

and for any even $N \geq 2b$, we have

$$M_{2b}(Sp(N), \text{std}) = (2b)!!,$$

(cf. [Larsen-Normal], [Dia-Sha]).

**Corollary 2.3.4** Suppose $n \geq 1$, and $d \geq 3$. For each $b \geq 1$ with

$$2b \leq \text{Max}(N_d, d+1),$$

we have the equality

$$M_{2b}(G_d, V_d) = (2b)!!.$$

**proof** Suppose n is odd. Since $G_d$ is a subgroup of $Sp(N_d) = Sp(V_d)$, we have the a priori inequality

$$M_{2b}(G_d, V_d) \geq M_{2b}(Sp(N_d), \text{std}).$$

If $2b \leq N_d$, we have

$$M_{2b}(Sp(N), \text{std}) = (2b)!!,$$

as explained in (2.3.3) above. So we find

$$M_{2b}(G_d, V_d) \geq (2b)!!.$$

If in addition $d \geq 3$ and $d + 1 \geq 2b$, we have the reverse inequality from Theorem 2.3.2. For the proof in the case of even n, simply replace $Sp(N_d)$ by$O(N_d)$ in the above argument. QED

(2.3.5) We now use these estimates for higher moments to eliminate more possibilities of finite monodromy in our universal families.

**Theorem 2.3.6 (supplement to Theorem 2.2.15)**
Suppose that $n \geq 2$ is even, that $d \geq 5$, and that $N_d \geq 3$. If $N_d \neq 8$, or

if $d \geq 7$, then the geometric monodromy group $G_d$ of the lisse sheaf $\mathcal{F}_d$ is the full orthogonal group $O(N_d)$.

**proof** Unless $N_d$ is 6, 7, or 8, the desired conclusion is given by 2.2.15.

If $N_d$ is 6, then $G_d$ is either $O(6)$ or it is $W(E_6)$, the Weyl group of $E_6$, in its standard reflection representation $std_6$. According to the the computer program GAP [GAP], the sixth moment of $W(E_6)$ in $std_6$ is given by

$$M_6(W(E_6), std_6) = 16.$$

But if $d \geq 5$, then by 2.3.2, we have $M_6(G_d, V_d) \leq 6!! = 15$. So we cannot have $W(E_6)$ if $d \geq 5$.

If $N_d$ is 7, then $G_d$ is either $O(7)$ or it is $W(E_7)$, the Weyl group of $E_7$, in its standard reflection representation $std_7$. According to GAP [GAP], the sixth moment of $W(E_7)$ in $std_7$ is given by

$$M_6(W(E_7), std_7) = 16.$$

But if $d \geq 5$, then by 2.3.2, we have $M_6(G_d, V_d) \leq 6!! = 15$. So we cannot have $W(E_7)$ if $d \geq 5$.

If $N_d = 8$, then $G_d$ is either $O(8)$ or it is $W(E_8)$, the Weyl group of $E_8$, in its standard reflection representation $std_8$. According to GAP [GAP], the eighth moment of $W(E_8)$ in $std_8$ is given by

$$M_8(W(E_8), std_8) = 106.$$

But if $d \geq 7$, then by 2.3.2 we have $M_8(G_d, V_d) \leq 8\,!! = 105$. So we cannot have $W(E_8)$ if $d \geq 7$. QED

## 2.4 Remarks on Theorem 2.2.4

(2.4.1) We have stated Theorem 2.2.4 in terms of the universal family of smooth hypersurface sections of degree d. It results from Bertini's theorem [Ka-ACT, 3.11.1] that we also get the same $G_d$ for any sufficiently general Lefschetz pencil of hypersurface sections of degree d.

(2.4.2) We have given a diophantine proof of Theorem 2.2.4, based on having a finite ground field. It follows, by standard spreading out techniques, that the same theorem is valid, for either the universal family of smooth hypersurface sections of degree d, or for a sufficiently general Lefschetz pencil thereof, over any field k in which $\ell$ is invertible. When k is $\mathbb{C}$, we have integral cohomology theory

$$X \mapsto H^*(X(\mathbb{C})^{an}, \mathbb{Z}),$$

so $\mathcal{F}_d$ has a natural $\mathbb{Z}$-form, and we can speak of the integral monodromy group. In some cases, this finer invariant is known, cf. [Beau].

(2.4.3) In the case n = 0, if we take X to be $\mathbb{P}^1$, then $G_d$ is a subgroup of the symmetric group $S_d$, and $V_d$ is just the representation $\mathrm{Aug}_{d-1}$. [Of course, $G_d$ is equal to $S_d$, thanks to Abel, but we will not use this fact here, cf. 2.4.4 just below.] Since we have proven that

$$M_4(G_d, V_d = \mathrm{Aug}_{d-1}) \le 4,$$

it follows that for the larger group $S_d$ we have

$$M_4(S_d, \mathrm{Aug}_{d-1}) \le 4.$$

On the other hand, we have already proven (1.4.5) that

$$M_4(S_d, \mathrm{Aug}_{d-1}) > 3 \text{ for } d \ge 5.$$

Since in any case the moments are integers, we have

$$M_4(S_d, \mathrm{Aug}_{d-1}) = 4 \text{ for } d \ge 5.$$

[One can check by hand that
$M_4(S_4, \mathrm{Aug}_3) = 4$, but that $M_4(S_3, \mathrm{Aug}_2) = 3$.]

(2.4.4) In the case n = 0, $X \subset \mathbb{P}$ any smooth, geometrically connected, projective curve, we can see that $G_d$, the geometric monodromy group of $\mathcal{F}_d$, is the full symmetric group $S_{N_d+1}$ as follows. Since $G_d$ is a priori a subgroup of $S_{N_d+1}$, it suffices to exhibit a pullback of $\mathcal{F}_d$ whose geometric monodromy group is $S_{N_d+1}$. Any Lefschetz pencil of degree d hypersurface sections on X will do this. Indeed, such a pencil gives a finite flat map f: $X \to \mathbb{P}^1$ which is finite etale of degree

$$\deg(f) = \deg(\mathcal{O}_X(d)) = d\times\deg(X) = 1 + N_d$$

over a dense open set $\mathbb{P}^1 - S$, inclusion denoted

$$j : \mathbb{P}^1 - S \to \mathbb{P}^1,$$

such that for each geometric point s in S, the geometric fibre $f^{-1}(s)$

consists of deg(f) - 1 distinct points. The pullback to $\mathbb{P}^1 - S$ of the sheaf $\mathcal{F}_d$ is $j^*(f_*\overline{\mathbb{Q}}_\ell/\overline{\mathbb{Q}}_\ell)$. We must show that $j^*(f_*\overline{\mathbb{Q}}_\ell)$ has geometric monodromy group $S_{\deg(f)}$. From the commutative diagram

$$\begin{array}{ccc} X - f^{-1}(S) & \overset{k}{\subset} & X \\ \tilde{f} \downarrow & & \downarrow f \\ \mathbb{P}^1 - S & \underset{j}{\subset} & \mathbb{P}^1 \end{array}$$

we see that $f_*\overline{\mathbb{Q}}_\ell = f_*k_*\overline{\mathbb{Q}}_\ell = j_*\tilde{f}_*\overline{\mathbb{Q}}_\ell = j_*j^*f_*\overline{\mathbb{Q}}_\ell$. From the equality $f_*\overline{\mathbb{Q}}_\ell = j_*j^*f_*\overline{\mathbb{Q}}_\ell$, we see that the local monodromy of $j^*(f_*\overline{\mathbb{Q}}_\ell)$ at each point of S has a fixed space of codimension one, so is a reflection. The monodromy group of $j^*(f_*\overline{\mathbb{Q}}_\ell)$ is a subgroup of $S_{\deg(f)}$ which is transitive (the total space $X - f^{-1}(S)$ is geometrically connected) and generated by reflections (all the conjugates of the local monodromies at all the points of S), hence is the whole group $S_{\deg(f)}$.

## 2.5 A p-adic approach to ruling out finite monodromy for universal families of hypersurface sections

(2.5.1) In the case of odd fibre dimension n, we know [De-Weil II, 4.4.1] that any Lefschetz pencil has monodromy group which is Zariski dense in the full symplectic group. The moment technique gives a variant proof, valid for the universal family (and then by Bertini for any sufficiently general Lefschtz pencil) of hypersurface sections of degree $d \geq 3$ such that $N_d \geq 4$. Indeed, the fourth moment is 3, so $G_d$ is either $Sp(N_d)$ or it is finite. But $G_d$ cannot be finite, because in odd fibre dimension the local monodromies in a Lefschetz pencil are unipotent pseudoreflections (and so of infinite order).

(2.5.2) In our discussion so far, we have made essential use of the Picard-Lefschetz formula [SGA 7, Exposé XV, 3.4], to know that $G_d$ contains a reflection in the case of even fibre dimension n, and, a unipotent pseudoreflection in the case of odd fibre dimension.

(2.5.3) Suppose we did not know the Picard-Lefschetz formula, but did know all the results of [De-Weil II], an admittedly unlikely but nonetheless logically possible situation. In that case, a result of Koblitz [Kob, Lemma 4, page 132, and Theorem 1, page 139] leads to a p-adic proof that, given X/k as above of dimension $n + 1 \geq 2$, then for all d sufficiently large, the group $G_d$ is not finite. Once $G_d$ is not finite for a given $d \geq 3$ with $N_d \geq 3$, we know from Larsen's Alternative that $G_d$ is $Sp(N_d)$ if n is odd, and that $G_d$ is either $SO(N_d)$ or $O(N_d)$ if n is even. We do not know how to prove, in the case of even fibre dimension, that the SO case cannot occur, without appealing to the Picard-Lefschetz formula!

(2.5.4) We now explain the p-adic proof that if X/k as above has dimension $n + 1 \geq 2$, then for d sufficiently large, the group $G_d$ is not finite.

(2.5.4.1) We know that $G_d$ is an irreducible subgroup of $GL(V_d)$. If $G_d$ is finite, then any element A of the ambient $GL(V_d)$ which normalizes $G_d$ has some power a scalar. For the group $Aut(G_d)$ is itself finite, so a power of A, acting by conjugation on $G_d$, will act trivially, i.e., a power of A will commute with $G_d$, which, $G_d$ being irreducible, makes that power a scalar. This applies to the image in $GL(V_d)$ of any Frobenius element in $\pi_1(\mathrm{Good}_X\mathrm{PHyp}_d)$. So if $G_d$ is finite, then for any finite extension field E/k, and any H in $\mathrm{Good}_X\mathrm{PHyp}_d(E)$, we find that a power of $\mathrm{Frob}_E$ acting on $\mathrm{Ev}^n((X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell)$ is a scalar. Moreover, we know that $\mathrm{Frob}_E/(\#E)^{n/2}$ lies in either Sp or O, so has determinant $\pm 1$. Since $\mathrm{Frob}_E/(\#E)^{n/2}$ has a power which is a scalar, that scalar must be a root of unity. Thus every eigenvalue of $\mathrm{Frob}_E$ acting on $\mathrm{Ev}^n((X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell)$ is of the form (a root of unity)$\times(\#E)^{n/2}$, so in particular of the form p×(an algebraic integer).

(2.5.4.2) On the other hand, we know that the characteristic polynomial of $\mathrm{Frob}_E$ on $H^i((X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell)$ or on $H^i(X\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell)$ has $\mathbb{Z}$-coefficients. By the hard Lefschetz theorem on X, for $i > n$, all eigenvalues of $\mathrm{Frob}_E$ on $H^i(X\otimes_k\bar{k})\cap H, \bar{\mathbb{Q}}_\ell)$ are also of the form p×(an algebraic integer). So we get a congruence mod p for the zeta function of $X\cap H/E$, viewed as an element of $1 + T\mathbb{Z}[[T]]$:

$$\mathrm{Zeta}(X\cap H/E, T)$$
$$\equiv \prod_{i=0 \text{ to } n}\det(1 - T\mathrm{Frob}_E \mid H^i((X\otimes_k \bar{k})\cap H, \bar{\mathbb{Q}}_\ell)^{(-1)^{i+1}}.$$

Using the weak Lefschetz theorem, this last product is equal to the product

$$(\prod_{i=0 \text{ to } n}\det(1 - T\mathrm{Frob}_E \mid H^i(X\otimes_k \bar{k}, \bar{\mathbb{Q}}_\ell)^{(-1)^{i+1}})$$
$$\times\det(1 - T\mathrm{Frob}_E \mid \mathrm{Ev}^n((X\otimes_k \bar{k})\cap H, \bar{\mathbb{Q}}_\ell)^{(-1)^{n+1}}.$$

If $G_d$ is finite, then the second term is 1 mod p. So we get a congruence formula for Zeta($X\cap H/E$, T) which shows that its reduction mod p is a rational function whose degree as a rational function depends only on X. Indeed, if we denote by $\sigma_i$ the degree of the reduction mod p of the integer polynomial

$$\det(1 - T\mathrm{Frob}_k \mid H^i(X\otimes_k \bar{k}, \bar{\mathbb{Q}}_\ell),$$

then Zeta($X\cap H/E$, T) mod p has degree $\sigma(X) := \Sigma_{i=0 \text{ to } n}(-1)^{i+1}\sigma_i$, for every finite extension E/k, and every point H in $\mathrm{Good}_X\mathrm{PHyp}_d(E)$.

(2.5.4.3) We now explains how this last conclusion leads to a contradiction for large d. By the congruence formula [SGA 7, Part II, Exposé XXII, 3.1] for the zeta function, we have the mod p congruence

$$\mathrm{Zeta}(X\cap H/E, T)$$
$$\equiv \prod_{i=0 \text{ to } n}\det(1 - T\mathrm{Frob}_E \mid H^i(X\cap H,\mathcal{O}_{X\cap H}))^{(-1)^{i+1}}.$$

For d sufficiently large, the restriction map

$$H^i((X,\mathcal{O}_X) \to H^i(X\cap H,\mathcal{O}_{X\cap H})$$

is an isomorphism for i < n, and is injective for i = n (i.e., for large d we have vanishing of $H^i(X, \mathcal{O}_X(-d))$ for $i \le n$). So we can factor this mod p product as

$$(\prod_{i=0 \text{ to } n}\det(1 - T\mathrm{Frob}_E \mid H^i(X,\mathcal{O}_X))^{(-1)^{i+1}})$$
$$\times\det(1 - T\mathrm{Frob}_E \mid H^n(X\cap H,\mathcal{O}_{X\cap H})/H^n(X,\mathcal{O}_X))^{(-1)^{n+1}}.$$

The degree of the first factor depends only on X. Indeed, if we denote by $\tau_i$ the degree of the mod p polynomial

$$\det(1 - T\mathrm{Frob}_k \mid H^i(X,\mathcal{O}_X)),$$

this degree is $\tau(X) := \Sigma_{i=0 \text{ to } n}(-1)^{i+1}\tau_i$. So if $G_d$ is finite, then we conclude that the mod p polynomial

$$\det(1 - T\mathrm{Frob}_E \mid H^n(X\cap H, \mathcal{O}_{X\cap H})/H^n(X, \mathcal{O}_X))$$

has degree $(-1)^n(\sigma(X) - \tau(X))$, for every finite extension E/k, and every point H in $\mathrm{Good}_X\mathrm{PHyp}_d(E)$.

(2.5.4.4) Thanks to Koblitz [Kob, Lemma 4, page 132, and Theorem 1, page 139], for d sufficiently large, there is a dense open set of $\mathrm{Good}_X\mathrm{PHyp}_d$ on which the degree of the mod p polynomial

$$\det(1 - T\mathrm{Frob}_E \mid H^n(X\cap H, \mathcal{O}_{X\cap H})/H^n((X, \mathcal{O}_X))$$

is constant, say F(d), and F(d) goes to infinity with d. More precisely, Koblitz shows that there is a $\mathbb{Q}$-polynomial $P_X(T)$ of degree n+1, of the form $\deg(X)T^{n+1}/(n+1)!$ + lower terms, such that $F(d) \geq P_X(d)$. So for d large enough that the following three conditions hold:

$d \geq 3$,

$H^i(X, \mathcal{O}_X(-d)) = 0$ for $i \leq n$,

$F(d) > (-1)^n(\sigma(X) - \tau(X))$,

$G_d$ is not finite.

## References

[ABP] Atiyah, M.; Bott, R.; Patodi, V. K. On the heat equation and the index theorem. Invent. Math. 19 (1973), 279-330.

[Beau] Beauville, A., Le groupe de monodromie des familles universelles d'hypersurfaces et d'intersections complètes, pages 8-18 in *Complex analysis and algebraic geometry (Göttingen, 1985)*, Springer Lecture Notes in Math. 1194, 1986.

[BBH] Beukers, F., Brownawell, D., and Heckman, G., Siegel Normality, Ann. Math. 127 (1988), 279-308.

[Blich-FCG] Blichfeldt, H.F., *Finite Collineation Groups*, U. Chicago Press, 1917.

[Bour-L4] Bourbaki, N., *Groupes et Algebres de Lie*, Chapitres 4, 5, et 6, Masson, Paris, 1981.

[Bour-L8] Bourbaki, N., *Groupes et Algebres de Lie*, Chapitres 7 et 8, Diffusion CCLS, Paris, 1975.

[CCNPW-Atlas] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., Wilson, R. A., *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray*, Oxford University Press, Oxford, 1985.

[C-R-MRT] Curtis, C.W., and Reiner, I., *Methods of Representation Theory with applications to finite groups and orders, Vol. I*, John Wiley and Sons, New York, 1981.

[De-Weil II] Deligne, P., La conjecture de Weil II, Pub. Math. I.H.E.S. 52 (1981), 313-428.

[Dia-Sha] Diaconis, Persi; Shahshahani, Mehrdad On the eigenvalues of random matrices. Studies in applied probability. J. Appl. Probab. 31A (1994), 49-62.

[GAP] Lehrstuhl D für Mathematik, RWTH Aachen, GAP, computer program, available from http://www-gap.dcs.st-and.ac.uk/~gap

[Ger] Gerardin P., Weil representations associated to finite fields, J. Alg. 46 (1977), 54-101.

[Howe] Howe, R., On the character of Weil's representation, Trans. A. M. S. 177 (1973), 287-298.

[Ka-ACT] Katz, N., Affine cohomological transforms, perversity and monodromy, JAMS, Vol. 6, No. 1, January, 1993, 149-222.

[Ka-LFM] Katz, N., L-functions and monodromy: four lectures on Weil II, Adv. Math. 160, 81-132 (2001).

[Ka-SE] Katz, N., *Sommes Exponentielles*, rédigé par G. Laumon, Asterisque 79, 1980.

[Ka-TLFM] Katz, N., *Twisted L-Functions and Monodromy*, Annals of Math. Study 150, Princeton University Press, 2001.

[Ka-La-FGCFT], Katz, N., and Lang, S., Finiteness theorems in geometric classfield theory. With an appendix by Kenneth A. Ribet. Enseign. Math. (2) 27 (1981), no. 3-4, 285-319.

[Kob] Koblitz, Neal, p-adic variation of the zeta-function over families of varieties defined over finite fields. Compositio Math. 31 (1975), no. 2, 119-218.

[Lar-Char] Larsen, Michael, A characterization of classical groupss by invariant theory, preprint, middle 1990's.

[Lar-Normal], Larsen, Michael, The normal distribution as a limit of generalized Sato-Tate measures, preprint, early 1990's.

[Mi] Mitchell, H. H., Determination of all primitive collineation groups in more than four variables which contain homologies, Amer. J. Math. 36 (1914), 1-12.

[MPR] Moody, R. V., Patera, J., and Rand, D. W., simpLie,Version 2.1, Macintosh Software for Representations of Simple Lie Algebras, December, 2000, available from http://www.crm.umontreal.ca/~rand/simpLie.html

[Pra] Prasad, Dipendra On the self-dual representations of finite groups of Lie type, J. Alg. 210 (1998), 298-310.

[Reid] Reid, Miles, The intersection of two or more quadrics, Ph.D. thesis, Cambridge University, 1972, unpublished.

[SGA] A. Grothendieck et al - *Séminaire de Géométrie Algébrique du Bois-Marie*, SGA 1, SGA 4 Parts I, II, and III, SGA 4½, SGA 5, SGA 7 Parts I and II, Springer Lecture Notes in Math. 224, 269-270-305, 569, 589, 288-340, 1971 to 1977.

[Wales] Wales, D., Quasiprimitive linear groups with quadratic elements, J. Alg. 245 (2001), 584-606.

[Weyl] Weyl, Hermann *The Classical Groups. Their Invariants and Representations*. Princeton University Press, Princeton, N.J., 1939. xii+302 pp.

[Zal] Zalesskii , A. E., Linear groups, Russian Math Surveys 36:5 (1981), 63-128.