Frobenius–Schur indicator and the ubiquity of Brock–Granville Quadratic Excess

Nicholas M. Katz

Introduction In a recent paper, Brock and Granville consider the following question. Fix a genus g ≥ 1. For a finite field $\mathbb{F}_q$ of odd characteristic, denote by $S_{2g+1}(\mathbb{F}_q)$ the set of those monic polynomials f(x) in $\mathbb{F}_q[x]$ of the form

$$x^{2g+1} + (\text{a polynomial of degree} \leq 2g-1),$$

which in addition have 2g+1 distinct roots in $\overline{\mathbb{F}}_q$. For each point f in $S_{2g+1}(\mathbb{F}_q)$, consider the projective smooth hyperelliptic curve $\mathcal{C}_f/\mathbb{F}_q$ of genus g, whose affine equation is

$$y^2 = f(x),$$

and which has a single point at infinity. For each f in $S_{2g+1}(\mathbb{F}_q)$, and for integer r ≥ 1, consider the number $\#\mathcal{C}_f(\mathbb{F}_q r)$ of $\mathbb{F}_q r$–valued points of $\mathcal{C}_f$. For given r, Brock and Granville ask what can be said about the average value of $\#\mathcal{C}_f(\mathbb{F}_q r)$, as f varies over $S_{2g+1}(\mathbb{F}_q)$.

For r=1, this average value is q+1. Indeed, any single hyperelliptic curve and its quadratic twist have between them a total of 2q+2 points over $\mathbb{F}_q$. This same trick of considering quadratic twists shows that for any odd r, the average value is $q^r + 1$.

For r=2, they show that the situation is quite different. The average value of $\#\mathcal{C}_f(\mathbb{F}_q 2)$, as f varies over $S_{2g+1}(\mathbb{F}_q)$ is **not** $q^2 + 1$, but rather it is $q^2 + q + O(q^{1/2})$. This phenomenon, of "extra" points in quadratic extensions, is the quadratic excess of the title.

In this note, we will show that Brock–Granville quadratic excess is ubiquitous, and occurs in families of varietes of all sorts. Roughly speaking, it occurs in any family whose monodromy is irreducible, nontrivial, and self–dual. Quadratic excess is just the diophantine expression of the (cohomological incarnation of the) Frobenius–Schur indicator. We will also explore the question of excess in extensions of higher degree.

The Frobenius–Schur indicator (cf. [F–S], [Cur, pp. 150–154])

When a compact group G operates irreducibly on a finite–dimensional $\mathbb{C}$–vector space V, we have the following trichotomy: either the representation V of G is not self–dual, or it is orthogonally self–dual, or it symplectically self–dual. As Frobenius and Schur discovered in 1906, the integral (for the total mass one Haar measure dg on G)

$$\int_G \mathrm{Trace}(g^2 \mid V)dg,$$

now called the Frobenius–Schur indicator, distinguishes among these cases:

$$\begin{aligned}\int_G \mathrm{Trace}(g^2 \mid V)dg \quad &= 0, \text{ if V is not self–dual,}\\ &= 1, \text{ if V is orthogonally self–dual,}\\ &= -1, \text{ if V is symplectically self–dual.}\end{aligned}$$

To see this, recall the universal linear algebra identities

$$\mathrm{Trace}(g \mid V\otimes V) = \mathrm{Trace}(g \mid \mathrm{Sym}^2(V)) + \mathrm{Trace}(g \mid \Lambda^2(V)),$$
$$\mathrm{Trace}(g^2 \mid V) = \mathrm{Trace}(g \mid \mathrm{Sym}^2(V)) - \mathrm{Trace}(g \mid \Lambda^2(V)),$$

and the representation theory identity

$$\int_G \mathrm{Trace}(g \mid \text{any rep'n. } W \text{ of } G)dg = \dim(W^G).$$

The last identity gives

$$\int_G \mathrm{Trace}(g|V\otimes V)dg = \dim((V\otimes V)^G) = \dim(\mathrm{Hom}_G(V^\vee, V)),$$

which is equal to 1 if V is self−dual and 0 if not. The linear algebra identities give

$$\int_G \mathrm{Trace}(g \mid V\otimes V)dg = \dim(\mathrm{Sym}^2(V))^G + \dim(\Lambda^2(V))^G,$$
$$\int_G \mathrm{Trace}(g^2 \mid V)dg = \dim(\mathrm{Sym}^2(V))^G - \dim(\Lambda^2(V))^G,$$

so we find the asserted value for $\int_G \mathrm{Trace}(g^2 \mid V)dg$.

On the other hand, so long as the irreducible action of G on V is nontrivial, we have

$$\int_G \mathrm{Trace}(g|V)dg = \dim(V^G) = 0.$$

A notational convention

We will frequently be averaging a $\mathbb{C}$−valued function f over some finite set S. In what follows, we will write

$$\int_S f(s)ds := (1/\#S)\Sigma_{s \text{ in } S}\, f(s).$$

Application to families of curves

Fix a genus g ≥ 1. Let k be a finite field, S/k a smooth, geometrically connected k−scheme of dimension d ≥ 1, and

$$\pi : \mathcal{C} \to S$$

a proper smooth family of geometrically connected curves of genus g. Fix a prime number ℓ invertible in k. We have the lisse sheaf

$$\mathcal{F} := R^1\pi_*\overline{\mathbb{Q}}_\ell$$

of rank 2g on S, which is pure of weight one, and carries a symplectic autoduality (cup−product) toward $\overline{\mathbb{Q}}_\ell(-1)$. For each finite extension E/k, and each point s in S(E), the genus g curve $\mathcal{C}_s$/E has

$$\#\mathcal{C}_s(E) = \#E + 1 - \mathrm{Trace}(\mathrm{Frob}_{E,s} \mid R^1\pi_*\overline{\mathbb{Q}}_\ell).$$

It is known that $\mathcal{F}$ is completely reducible as a representation of $\pi_1{}^{\mathrm{geom}}(S) := \pi_1(S\otimes_k\bar{k})$. We say that the family has irreducible monodromy if $\mathcal{F}$ is irreducible as a representation of $\pi_1{}^{\mathrm{geom}}(S)$, or equivalently (using the complete reducibility) if $\mathrm{End}(\mathcal{F})$ as a representation of $\pi_1{}^{\mathrm{geom}}(S)$ has a one−dimensional space of invariants (or equivalently, of coinvariants). Using the autoduality of $\mathcal{F}$ toward $\overline{\mathbb{Q}}_\ell(-1)$, we see that the monodromy is irreducible if and only if the cup−product pairing

$$\mathcal{F}\otimes\mathcal{F} \to \overline{\mathbb{Q}}_\ell(-1)$$

induces an isomorphism

$$H_c{}^{2d}(S\otimes_k\bar{k}, \mathcal{F}\otimes\mathcal{F}) \cong H_c{}^{2d}(S\otimes_k\bar{k}, \overline{\mathbb{Q}}_\ell(-1)) = \overline{\mathbb{Q}}_\ell(-1-d).$$

There is a simple diophantine criterion for this irreducibility, as follows. The family has irreducible monodromy if and only if

$$\lim_{\#E \to \infty} (1/\#(E))\int_{S(E)} (\#E + 1 - \#\mathcal{C}_s(E))^2 = 1,$$

cf. [Ka–MFC].

We refer to [Ka–Sar, RMFEM, 10.1.16, 10.1.18.3–5, 10.2.2, 10.3.1–4 (which covers the hyperelliptic family considered in the introduction), 10.6.11] for examples of families of curves with irreducible monodromy. In all these examples, the geometric monodromy group is not only irreducible, it is the full symplectic group. But there are also families of curves with quite small, but still irreducible, monodromy. For example, there are iso–trivial families whose monodromy is a finite irreducible group (e.g., the two–parameter family of supersingular elliptic curves

$$y^2 - y = x^3 + Ax + B$$

in characteristic two).

Suppose now that the monodromy is irreducible. Since $\mathcal{F}$ has rank $2g > 1$, the irreducible monodromy is necessarily nontrivial, so we have

$$H_c^{2d}(S\otimes_k\bar{k}, \mathcal{F}) = 0.$$

Now consider the direct sum decomposition

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

Since the cup–product pairing is alternating, it induces a surjection

$$\Lambda^2(\mathcal{F}) \to \bar{\mathbb{Q}}_\ell(-1),$$

so in turn a surjection

$$H_c^{2d}(S\otimes_k\bar{k}, \Lambda^2(\mathcal{F})) \to H_c^{2d}(S\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell(-1)) = \bar{\mathbb{Q}}_\ell(-1-d).$$

From the decomposition

$$H_c^{2d}(S\otimes_k\bar{k}, \mathcal{F}\otimes\mathcal{F}) = H_c^{2d}(S\otimes_k\bar{k}, \mathrm{Sym}^2(\mathcal{F})) \oplus H_c^{2d}(S\otimes_k\bar{k}, \Lambda^2(\mathcal{F}))$$

of the one–dimensional space $H_c^{2d}(S\otimes_k\bar{k}, \mathcal{F}\otimes\mathcal{F}) \cong = \bar{\mathbb{Q}}_\ell(-1-d)$, we infer that

$$H_c^{2d}(S\otimes_k\bar{k}, \Lambda^2(\mathcal{F})) \cong \bar{\mathbb{Q}}_\ell(-1-d),$$
$$H_c^{2d}(S\otimes_k\bar{k}, \mathrm{Sym}^2(\mathcal{F})) = 0.$$

This is the cohomological incarnation of the fact that the Frobenius–Schur indicator is -1 for an irreducible symplectic representation.

Quadratic Excess Theorem Suppose our family $\mathcal{C}/S$ of curves of genus $g \geq 1$ has irreducible monodromy. Define constants A, C_1, and C_2 as follows:

$$A := \Sigma_i\, h_c^i(S\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell),$$
$$C_1 := \Sigma_i\, h_c^i(S\otimes_k\bar{k}, \mathcal{F}),$$
$$C_2 := \Sigma_i\, h_c^i(S\otimes_k\bar{k}, \mathcal{F}\otimes\mathcal{F}).$$

For any finite extension E/k with $\#E > 4A^2$, S(E) is nonempty, and denoting by E_2/E the quadratic extension of E, we have the inequalities

$$|\int_{S(E)} (\#E + 1 - \#\mathcal{C}_s(E))ds| \le (3/2)C_1,$$

and

$$|\#E + \int_{S(E)} (\#E_2 + 1 - \#\mathcal{C}_s(E_2))ds| \le 2C_2(\#E)^{1/2}.$$

Quadratic Excess Corollary Hypotheses as above, for any finite extension E/k we have

$$\int_{S(E)} \#\mathcal{C}_s(E)ds = \#E + O(1),$$

and

$$\int_{S(E)} \#\mathcal{C}_s(E_2)ds = \#E_2 + \#E + O((\#E)^{1/2}).$$

proof The corollary is a trivial rewriting of the theorem. For A the sum of the $h_c{}^i(S\otimes_k\bar{k}, \bar{\mathbb{Q}}_\ell)$, we have the Lang–Weil estimate

$$|\#S(E) - (\#E)^d| \le A(\#E)^{d-1/2}.$$

So to prove the theorem it suffices to show that

$$|\Sigma_{s \text{ in } S(E)} (\#E + 1 - \#\mathcal{C}_s(E))| \le C_1(\#E)^d,$$

and

$$|(\#E)^{d+1} + \Sigma_{s \text{ in } S(E)} (\#E_2 + 1 - \#\mathcal{C}_s(E_2))| \le C_2(\#E)^{d + 1/2}.$$

The first sum is (by the Lefschetz trace formula)

$$\Sigma_{s \text{ in } S(E)} (\#E + 1 - \#\mathcal{C}_s(E)) = \Sigma_{s \text{ in } S(E)} \mathrm{Trace}(\mathrm{Frob}_{E,s} \mid \mathcal{F})$$
$$=\Sigma_{i=0 \text{ to } 2d} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H_c{}^i(S\otimes_k\bar{k}, \mathcal{F})).$$

In this sum, the i'th term is mixed of weight ≤ i+1 by Weil II, and the 2d'th term vanishes. So we get the desired estimate.

In the second sum, we have

$$\Sigma_{s \text{ in } S(E)} (\#E_2 + 1 - \#\mathcal{C}_s(E_2))$$
$$= \Sigma_{s \text{ in } S(E)} \mathrm{Trace}((\mathrm{Frob}_{E,s})^2 \mid \mathcal{F})$$
$$= \Sigma_{s \text{ in } S(E)} \mathrm{Trace}((\mathrm{Frob}_{E,s})\mid \mathrm{Sym}^2(\mathcal{F}))$$
$$- \Sigma_{s \text{ in } S(E)} \mathrm{Trace}((\mathrm{Frob}_{E,s})\mid \Lambda^2(\mathcal{F}))$$
$$= \Sigma_{i=0 \text{ to } 2d} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H_c{}^i(S\otimes_k\bar{k}, \mathrm{Sym}^2(\mathcal{F})))$$
$$- \Sigma_{i=0 \text{ to } 2d} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H_c{}^i(S\otimes_k\bar{k}, \Lambda^2(\mathcal{F})))$$
$$= \Sigma_{i=0 \text{ to } 2d-1} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H_c{}^i(S\otimes_k\bar{k}, \mathrm{Sym}^2(\mathcal{F})))$$
$$- \Sigma_{i=0 \text{ to } 2d-1} (-1)^i\mathrm{Trace}(\mathrm{Frob}_E \mid H_c{}^i(S\otimes_k\bar{k}, \Lambda^2(\mathcal{F})))$$
$$-(\#E)^{d+1},$$

the last equality because, as already noted above,

$$H_c{}^{2d}(S\otimes_k\bar{k}, \Lambda^2(\mathcal{F})) \cong \bar{\mathbb{Q}}_\ell(-1-d),$$

$$H_c{}^{2d}(S\otimes_k\bar{k}, \mathrm{Sym}^2(\mathcal{F})) = 0.$$

In this final expression, both $\mathrm{Sym}^2(\mathcal{F})$ and $\Lambda^2(\mathcal{F})$ are pure of weight two, so for $i \le 2d-1$ both $H_c{}^i(S\otimes_k\bar{k}, \mathrm{Sym}^2(\mathcal{F}))$ and $H_c{}^i(S\otimes_k\bar{k}, \Lambda^2(\mathcal{F}))$ are mixed of weight $\le 2d + 1$. So we get the desired estimate for the second sum. QED

Uniform Quadratic Excess Theorem Take as ground ring a normal integral domain A which is finitely generated over $\mathbb{Z}$. Let S/A be a smooth A–scheme with all fibres geometrically connected of some common dimension $d \ge 1$. Let $\pi : \mathcal{C} \to S$ be a proper smooth family of geometrically connected curves of genus g. Suppose that for any finite field k, and for any ring homomorphism $\alpha : A \to k$, the resulting family on $S_\alpha/k := S\otimes_A k/k$ has irreducible monodromy. There exist constants A, C_1, and C_2 with the following properties. For any finite field E with $\#E \ge 4A^2$, any ring homomorphism $\alpha : A \to E$, denoting by E_2/E the quadratic extension of E, we have the estimates

$$|\textstyle\int_{S_\alpha(E)} (\#E + 1 - \#\mathcal{C}_{\alpha,s}(E))ds| \le (3/2)C_1,$$

and

$$|\#E + \textstyle\int_{S_\alpha(E)} (\#E_2 + 1 - \#\mathcal{C}_s(E_2))ds| \le 2C_2(\#E)^{1/2}.$$

proof The constants A, C_1, C_2 in the previous theorem applied to $\mathcal{C}_\alpha/S_\alpha$ stay bounded as α varies over all finite–field–valued points of Spec(A), cf. [Ka–Sar, RMFEM, 9.3.3–4]. QED

Quadratic Excess in other self–dual contexts

Fix an integer $n \ge 0$, and a degree $d \ge 3$. Denote by

$$\pi: X \to \mathcal{H}_{n,d}$$

the universal family over $\mathbb{Z}$ of smoth, degree d hypersurfaces in $\mathbb{P}^{n+1}$. Given a finite field k and a point h in $\mathcal{H}_{n,d}(k)$, corresponding to a projective smooth degree d hypersurface X_h/k in $\mathbb{P}^{n+1}$, the zeta function of $X_h/\mathbb{F}_q$ has the form

$$P(X_h/k, T)^{(-1)^{n+1}}/(\textstyle\prod_{i=0 \text{ to } n}(1 - (\#k)^i T))$$

with P(T) a $\mathbb{Z}$–polynomial with constant term one, of degree

$$\mathrm{prim}(n,d) := (d-1)((d-1)^{n+1} - (-1)^{n+1})/d.$$

Fix a prime number ℓ. On the space $\mathcal{H}_{n,d}[1/\ell]$, we have a lisse sheaf $\mathcal{F}$ (the sheaf $\mathrm{Prim}^n{}_\ell$ of [Ka–Sar, RMFEM, 11.4.8]) of rank prim(n, d), which is pure of weight n, and which is equipped with an autoduality toward $\bar{\mathbb{Q}}_\ell(-n)$ which is alternating for n odd, and orthogonal for n even. For odd n, $\mathcal{F}$ is just $R^n\pi_*\bar{\mathbb{Q}}_\ell$, while for even n it is the codimension one orthogonal in $R^n\pi_*\bar{\mathbb{Q}}_\ell$ of the image of H^n of the ambient projective space. For a finite field k and a point h in $\mathcal{H}_{n,d}(k)$, we have

$$\#X_h(k) = \#\mathbb{P}^n(k) + (-1)^n \mathrm{Trace}(\mathrm{Frob}_{k,h} \mid \mathcal{F}), \text{ i.e.,}$$
$$P(X_h/k, T) = \det(1 - T\mathrm{Frob}_{k,h} \mid \mathcal{F}).$$

It is known that for every finite field k, the universal family over $\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}k$ has irreducible monodromy: for every ℓ invertible in k, the lisse sheaf $\mathcal{F}$ on $\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}k$ is geometrically irreducible (and nontrivial, because its rank, prim(n,d), is ≥ 2). For n ≥ 1, cf. [Ka–Sar, RMFEM, 11.4.9 and its proof]. For n = 0, we are looking at the universal family of binary forms of degree d, so the assertion amounts to Abel's theorem, that the generic polynomial of degree d in one variable has galois group the full symmetric group S_d, together with the fact that $\mathcal{F}$ in this case is the d–1 dimensional augmentation representation of S_d, a representation which is well known to be irreducible, and orthogonally self–dual.

Let us denote by

$$D := \mathrm{Binomial}(n+1+d, d) - 1$$

the dimension of $\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}k$. From the nontriviality of the geometrically irreducible $\mathcal{F}$, we get

$$H_c^{2D}(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \mathcal{F}) = 0.$$

If n is odd, the autoduality is alternating, the Frobenius–Schur indicator is –1, and we get

$$H_c^{2D}(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \Lambda^2(\mathcal{F})) \cong \bar{\mathbb{Q}}_\ell(-n - D),$$
$$H_c^{2D}(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \mathrm{Sym}^2(\mathcal{F})) = 0.$$

If n is even, the autoduality is orthogonal, the Frobenius–Schur indicator is +1, and we get

$$H_c^{2D}(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \Lambda^2(\mathcal{F})) = 0,$$
$$H_c^{2D}(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \mathrm{Sym}^2(\mathcal{F})) \cong \bar{\mathbb{Q}}_\ell(-n - D).$$

We can now derive the diophantine consequences of these cohomological incarnations of the value ±1 of Frobenius–Schur indicator, exactly as we did at some length in the case of irreducible families of curves, where n was odd and the indicator was –1. If n is even, the Frobenius–Schur indicator, always $(-1)^n$, changes sign, as does the sign with which $\mathrm{Trace}(\mathrm{Frob}_{k,h} \mid \mathcal{F})$ occurs in the expression

$$\#X_h(k) = \#\mathbb{P}^n(k) + (-1)^n \mathrm{Trace}(\mathrm{Frob}_{k,h} \mid \mathcal{F}).$$

These two sign changes **cancel**: whatever the parity of n, we end up with quadratic excess (rather than quadratic defect). Here is the precise statement.

Quadratic Excess Theorem Fix integers n ≥ 0 and d ≥ 3. There exist constants A, C_1, and C_2 with the following properties. For any finite field E with $\#E \geq 4A^2$, denoting by E_2/E the quadratic extension of E, we have the estimates

$$\left|\int_{\mathcal{H}_{n,d}(E)} (\#\mathbb{P}^n(E) - \#X_h(E))dh\right| \leq (3/2)C_1(\#E)^{(n-1)/2},$$

and

$$\left|(\#E)^n + \int_{\mathcal{H}_{n,d}(E)} (\#\mathbb{P}^n(E_2) - \#X_h(E_2))dh\right| \leq 2C_2(\#E)^{(2n-1)/2}.$$

Quadratic Excess Corollary Hypotheses as above, for any finite field E we have

$$\int_{\mathcal{H}_{n,d}(E)} \#X_h(E)dh = \#\mathbb{P}^n(E) + O((\#E)^{(n-1)/2}),$$

and

$$\int_{\mathcal{H}_{n,d}(E)} \#X_h(E_2)dh = \#\mathbb{P}^n(E_2) + (\#E)^n + O((\#E)^{(2n-1)/2}).$$

Remarks 1) Instead of taking the universal family of smooth hypersurfaces of given degree $d \geq 3$ and dimension $n \geq 1$, we could have taken any family with irreducible monodromy, for example a Lefschetz pencil.

2) For even $n \geq 2$, the geometric monodromy group for the universal family is the full orthogonal group, except in the case n=2, d = 3. In the case n=2, d=3, of cubic surfaces in $\mathbb{P}^3$, the group is a finite irreducible reflection group.

3) If n is even, we can also take d=2. In this case $\mathcal{F}$ has rank one, and is nontrivial: its geometric monodromy group is the full orthogonal group $O(1) = \{\pm 1\}$. So also in the universal family of even dimensional quadrics, we get quadratic excess. Limiting case: take d=2, n=0.

4) In the case n=0, we are saying that, on average, degree d square–free polynomials over $\mathbb{F}_q$ have one root in $\mathbb{F}_q$ and two roots in $\mathbb{F}_{q^2}$. This incarnation of quadratic excess has an elementary number field analogue. Here is the simplest case. Take a degree d polynomial f over $\mathbb{Z}$ whose galois group is the full symmetric group S_d. By the classical Chebotarev density theorem, we have

$$\lim_{X \to \infty} (1/\pi(X))\Sigma_{p \leq X} \#\{\text{roots of f in } \mathbb{F}_p\} = 1,$$

while

$$\lim_{X \to \infty} (1/\pi(X))\Sigma_{p \leq X} \#\{\text{roots of f in } \mathbb{F}_{p^2}\} = 2.$$

Excess in extensions of arbitrary degree r ≥ 1

To fix ideas, take the universal family

$$\pi : X \to \mathcal{H}_{n,d}$$

of the last section, with $n \geq 1$, $d \geq 3$, but exclude the case (n=2, d=3). In order to analyze the question of excess in extensions of arbitrary degree $r \geq 1$, it no longer suffices to have irreducible monodromy, we must know what the geometric monodromy group is. We will succeed for these universal families because, for each finite field k, the family over $\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}k$ has biggest possible geometric monodromy group

$$G_{geom} = Sp(prim(n,d)), \text{ if n is odd,}$$
$$= O(prim(n,d)), \text{ if n is even.}$$

In both cases, there is no excess in extensions of odd degree, and in both cases there is excess in extensions of low even degree. In the symplectic case, the excess disappears in extensions of high even degree, while in the orthogonal case the even degree excess never disappears. Here is the precise statement.

Symplectic Higher Degree Excess Theorem Fix integers $n \geq 1$, $d \geq 3$. Suppose n is odd. Fix an integer $r \geq 1$. There exist constants A, and C_r with the following property. For any finite field E with $\#E \geq 4A^2$, denoting by E_r/E the extension of degree r, we have the following estimates.

1) if r is odd, or if r > prim(n,d), we have

$$|\int_{\mathcal{H}_{n,d}(E)} (\#\mathbb{P}^n(E_r) - \#X_h(E_r))dh| \le 2C_r(\#E)^{(rn-1)/2}.$$

2) If r is even, and $2 \le r \le \mathrm{prim}(n,d)$, we have

$$|(\#E)^{rn/2} + \int_{\mathcal{H}_{n,d}(E)} (\#\mathbb{P}^n(E_r) - \#X_h(E_r))dh| \le 2C_r(\#E)^{(rn-1)/2}.$$

Orthogonal Higher Degree Excess Theorem Fix integers $n \ge 2$, $d \ge 3$. Suppose n is even, and exclude the case n=2, d=3. Fix an integer $r \ge 1$. There exist constants A and C_r with the following property. For any finite field E with $\#E \ge 4A^2$, denoting by E_r/E the extension of degree r, we have the following estimates.

1) if r is odd, we have

$$|\int_{\mathcal{H}_{n,d}(E)} (\#\mathbb{P}^n(E_r) - \#X_h(E_r))dh| \le 2C_r(\#E)^{(rn-1)/2}.$$

2) If r is even, we have

$$|(\#E)^{rn/2} + \int_{\mathcal{H}_{n,d}(E)} (\#\mathbb{P}^n(E_r) - \#X_h(E_r))dh| \le 2C_r(\#E)^{(rn-1)/2}.$$

Proof of the higher degree excess theorems

Fix a finite field, and a prime number ℓ invertible in k. Over $\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}k$ we have the lisse $\overline{\mathbb{Q}}_\ell$–sheaf $\mathcal{F}$. Pick an embedding ι of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$, and denote by $(\#k)^{1/2}$ in $\overline{\mathbb{Q}}_\ell$ the choice of square root which maps under ι to the positive one in $\mathbb{C}$. The choice of $(\#k)^{1/2}$ allows us to define the fractional Tate–twist $\mathcal{F}(n/2)$ of $\mathcal{F}$. The sheaf $\mathcal{F}(n/2)$ on $\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}k$ is pure of weight zero and lisse of rank prim(n,d). If n is even (respectively odd), $\mathcal{F}(n/2)$ is orthogonally (respectively symplectically) self–dual, and its geometric monodromy group G_{geom} is O(prim(n,d)) (respectively Sp(prim(n,d)). Because $\mathcal{F}(n/2)$ is self dual, all the Frobenii $\mathrm{Frob}_{E,h}$ respect the autoduality, and hence all Frobenii land in G_{geom}.

With k and ℓ fixed, we define constants A and C_r by

$$A := \Sigma_i\, h_c{}^i(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \overline{\mathbb{Q}}_\ell),$$

$$C_r = \Sigma_{a\ge1,b\ge0,\ a+b=r}\Sigma_{i=0 \text{ to } 2D}\ a\times\dim H_c{}^i(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \Lambda^a(\mathcal{F})\otimes\mathrm{Sym}^b(\mathcal{F})).$$

It suffices to prove that as E varies only over finite extensions of k, the theorems hold with these constants. Indeed, for fixed ℓ, these constants remain bounded as k varies over all finite fields of characteristic not ℓ, cf. [Ka–Sar, RMFEM, 9.3.3–4]. Let $A(\ell)$ and $C_r(\ell)$ be upper bounds. Then the theorems hold with the constants $A(\ell)$ and $C_r(\ell)$ if we restrict to finite fields E in which ℓ is invertible. So if we pick any two distinct primes ℓ_1 and ℓ_2, the theorems hold universally with the constants $A := \mathrm{Sup}(A(\ell_1), A(\ell_2))$, $C_r = \mathrm{Sup}(C_r(\ell_1), C_r(\ell_2))$.

We now turn to proving the theorem over $\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}k$. For E/k a finite extension, and h in $\mathcal{H}_{n,d}(E)$, we have

$$\#X_h(E_r) = \#\mathbb{P}^n(E_r) + (-1)^n\mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}).$$

So we have

$$\int_{\mathcal{H}_{n,d}(E)} (\#\mathbb{P}^n(E_r) - \#X_h(E_r))dh$$
$$= (-1)^{n+1}\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F})dh$$
$$= (-1)^{n+1}(\#E)^{rn/2}\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh.$$

So we must show the following three statements:

1) If r is odd, or if n is odd and r > prim(n,d) = rank($\mathcal{F}$), we have

$$\left|\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh\right| \le 2C_r/(\#E)^{1/2}.$$

2) If n is odd and r is even with 2 ≤ r ≤ prim(n,d), we have

$$\left|\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh - (-1)^n\right| \le 2C_r/(\#E)^{1/2},$$

3) If n is even and if r ≥ 2 is even, we have

$$\left|\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh - (-1)^n\right| \le 2C_r/(\#E)^{1/2}.$$

These will follow from Deligne's equidistribution theorem [De−Weil II, 3.5.3], cf also [Katz−Sarnak, RMFEM, 9.2.6], which tells us that the large E limit of

$$\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh$$

may be computed as follows. Using ι, view the semisimple $\overline{\mathbb{Q}}_\ell$−algebraic group G_{geom} as a complex semisimple group, and pick a maximal compact subgroup K in $G_{geom}(\mathbb{C})$. In our case, G_{geom} is either the full orthogonal group or the symplectic group, of size prim(n,d), so K is either the compact orthogonal group O(prim(n,d), $\mathbb{R}$), or the compact symplectic group USp(prim(n,d)). In either case, the compact group K is given inside GL(prim(n,d), $\mathbb{C}$), and it is in that sense that we will speak of the traces of elements of K. We endow K with its total mass one Haar measure dk. Then we have

$$\lim_{\#E \to \infty}\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh$$
$$= \int_K \mathrm{Trace}(k^r)dk.$$

Moreover, because the function Trace(k^r) on K is the trace of a virtual representation (as we will see below), we also get an effective estimate for the absolute value of the difference: whenever E/k is a finite extension with #k ≥ $4A^2$, we have

$$\left|\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh - \int_K \mathrm{Trace}(k^r)dk\right|$$
$$\le 2C_r/(\#E)^{1/2}.$$

Let us explain briefly how this comes about. A key ingredient is the following classical linear algebra indentity.

Lemma Let R be a ring, N ≥ 1 a positive integer, V a free R−module of rank N, and A an element of GL(V). For any integer r ≥ 1, we have the identity in R

Trace(A^r|V)

$$= \Sigma_{a\geq 1,\ b\geq 0,\ a+b=r}\ a(-1)^{a-1}\mathrm{Trace}(A \mid \Lambda^a(V)\otimes \mathrm{Sym}^b(V)).$$

proof By first reducing to the universal case (when R is the coordinate ring of $GL(N)/\mathbb{Z}$, and A has independent indeterminates as entries) and then embedding R into $R\otimes_{\mathbb{Z}}\mathbb{Q}$, we reduce to the case when R is a $\mathbb{Q}$−algebra. Then we have the following three standard identities:

$$\det(1 - TA) = \exp(-\Sigma_{n\geq 1}\ \mathrm{Trace}(A^n)T^n/n),$$
$$\det(1 - TA) = \Sigma_{n\geq 0}\ (-1)^n\mathrm{Trace}(\Lambda^n(A))T^n,$$
$$1/\det(1 - TA) = \Sigma_{n\geq 0}\ \mathrm{Trace}(\mathrm{Sym}^n(A))T^n.$$

Apply $(Td/dT)\circ\log$ to the first, to get

$$(Td/dT(\det(1 - TA)))/\det(1 - TA) = -\Sigma_{n\geq 1}\ \mathrm{Trace}(A^n)T^n.$$

Now use the second and third to rewrite the numerator and denominator respectively. We get

$$(\Sigma_{n\geq 0}\ n(-1)^n\mathrm{Trace}(\Lambda^n(A))T^n)\times(\Sigma_{n\geq 0}\ \mathrm{Trace}(\mathrm{Sym}^n(A))T^n)$$
$$= -\Sigma_{n\geq 1}\ \mathrm{Trace}(A^n)T^n.$$

Equating coefficients of like powers of T gives the assertion. QED

Apply this to $\mathrm{Frob}_{E,h}$ acting on $\mathcal{F}(n/2)$. We get

$$\mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))$$
$$= \Sigma_{a\geq 1,\ b\geq 0,\ a+b=r}\ a(-1)^{a-1}\mathrm{Trace}(\mathrm{Frob}_{E,h} \mid \Lambda^a(\mathcal{F})\otimes \mathrm{Sym}^b(\mathcal{F})(rn/2)).$$

Summing over h in $\mathcal{H}_{n,d}(E)$, and using the Lefschetz trace formula, we get

$$(\#\mathcal{H}_{n,d}(E))\textstyle\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh$$
$$= \Sigma_{a\geq 1,\ b\geq 0,\ a+b=r}\ a(-1)^{a-1} \times$$
$$\times\Sigma_{i\ =\ 0\ \mathrm{to}\ 2D}\ \mathrm{Trace}(\mathrm{Frob}_E, H_c{}^i(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \Lambda^a(\mathcal{F})\otimes \mathrm{Sym}^b(\mathcal{F})(rn/2)).$$

The coefficient sheaves $\Lambda^a(\mathcal{F})\otimes \mathrm{Sym}^b(\mathcal{F})(rn/2)$ are all pure of weight zero, so by Weil II the sum of all the terms with $i < 2D$ is bounded by $C_r(\#E)^{D - 1/2}$. What about the terms with $i = 2D$? Here we find the Tate−twisted coinvariants under $G = G_{geom}$:

$$H_c{}^{2D}(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \Lambda^a(\mathcal{F})\otimes \mathrm{Sym}^b(\mathcal{F})(rn/2))$$
$$\cong (\Lambda^a(\mathcal{F})\otimes \mathrm{Sym}^b(\mathcal{F})(rn/2))^G(-D).$$

Because all the $\mathrm{Frob}_{E,h}$ lie in G_{geom}, Frob_E acts on these twisted G_{geom}−coinvariants as the scalar $(\#E)^D$. Of course we do not yet know the dimension of this cohomology group. Let us name it:

$$\mathrm{Invar}(a,b) := \dim H_c^{2D}(\mathcal{H}_{n,d}\otimes_{\mathbb{Z}}\bar{k}, \Lambda^a(\mathcal{F})\otimes\mathrm{Sym}^b(\mathcal{F})(rn/2)).$$

And let us define

$$\mathrm{Inv} := \Sigma_{a\geq1,\ b\geq0,\ a+b=r}\ a(-1)^{a-1}\ \mathrm{Invar}(a,b).$$

Then the above discussion gives the estimate

$$|(\#\mathcal{H}_{n,d}(E))\textstyle\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh - \mathrm{Inv}\times(\#E)^D|$$
$$\leq C_r(\#E)^{D\ -\ 1/2}.$$

Dividing through by $\#\mathcal{H}_{n,d}(E)$, we get

$$|\textstyle\int_{\mathcal{H}_{n,d}(E)} \mathrm{Trace}((\mathrm{Frob}_{E,h})^r \mid \mathcal{F}(n/2))dh - \mathrm{Inv}| \leq 2C_r/(\#E)^{1/2}.$$

So now we are reduced to computing the integer Inv, which is the dimension of the space of invariants of G_{geom} in the virtual representation

$$= \Sigma_{a\geq1,\ b\geq0,\ a+b=r}\ a(-1)^{a-1}\Lambda^a(\mathcal{F}(n/2))\otimes\mathrm{Sym}^b(\mathcal{F}(n/2)).$$

Here G_{geom} is either Sp(N) or O(N), for N := rank($\mathcal{F}$) = prim(n,d), and $\mathcal{F}(n/2)$ is its standard representation, which we will call std_N. So Inv is the dimension of the space of invariants of either Sp(N) or O(N) in the virtual representation

$$\Sigma_{a\geq1,\ b\geq0,\ a+b=r}\ a(-1)^{a-1}\Lambda^a(\mathrm{std}_N)\otimes\mathrm{Sym}^b(\mathrm{std}_N).$$

By the unitarian trick, i.e., the fact that K is Zariski dense in G_{geom}, this is also the dimension of the space of invariants of K (= USp(N) or O(N, $\mathbb{R}$)) in this virtual representation. So by the linear algebra identity above, now applied to K (= USp(N) or O(N, $\mathbb{R}$)) in its standard representation, we find

$$\mathrm{Inv} = \textstyle\int_K \mathrm{Trace}(k^r)dk.$$

So the theorems on higher degree excess now result from the following two lemma, which are surely well−known to the experts, e.g., cf. [Di−Sha], but for which I do not know a reference.

Symplectic Higher Indicator Lemma Suppose g ≥ 1. For r ≥ 1, we have the formulas

$$\textstyle\int_{USp(2g)}\mathrm{Trace}(A^r)dA = -1, \text{ if r is even and } r \leq 2g,$$
$$\textstyle\int_{USp(2g)}\mathrm{Trace}(A^r)dA = 0, \text{ if r is odd, or if } r > 2g.$$

Orthogonal Higher Indicator Lemma Suppose N ≥ 1. For r ≥ 1, we have the formulas

$$\textstyle\int_{O(N,\ \mathbb{R})}\mathrm{Trace}(A^r)dA \quad = 1, \text{ if r is even,}$$
$$= 0, \text{ if r is odd.}$$

Proof of the higher indicator lemmas

For G either USp(2g) or O(N, $\mathbb{R}$), we have seen that

$$\textstyle\int_G \mathrm{Trace}(A^r)dA$$
$$= \Sigma_{a\geq1,\ b\geq0,\ a+b=r}\ a(-1)^{a-1}\dim((\Lambda^a(\mathrm{std})\otimes\mathrm{Sym}^b(\mathrm{std}))^G).$$

For either G, all the representations Λ^a(std) and Sym^b(std) are self−dual, so we can rewrite this formula as

$\int_G \mathrm{Trace}(A^r)dA$

$$= \sum_{a\geq 1,\ b\geq 0,\ a+b=r} a(-1)^{a-1}\dim\mathrm{Hom}_G(\mathrm{Sym}^b(\mathrm{std}), \Lambda^a(\mathrm{std})).$$

Lemma On USp(2g), we have the following results. If $b = 0$ and if a is both even and $\leq 2g$, then

$$\dim\mathrm{Hom}_G(\mathrm{Sym}^b(\mathrm{std}), \Lambda^a(\mathrm{std})) = 1.$$

If $b = 1$ and if a is both odd and $< 2g$, then

$$\dim\mathrm{Hom}_G(\mathrm{Sym}^b(\mathrm{std}), \Lambda^a(\mathrm{std})) = 1.$$

In all other cases,

$$\dim\mathrm{Hom}_G(\mathrm{Sym}^b(\mathrm{std}), \Lambda^a(\mathrm{std})) = 0.$$

proof For each dominant weight ω of Sp(2g), we denote by $V(\omega)$ the irreducible representation with highest weight ω. In terms of the fundamental weights $\omega_1,..., \omega_g$ of Sp(2g), the representations we are looking at are as follows. For every $b \geq 0$, we have

$$\mathrm{Sym}^b(\mathrm{std}) = V(b\omega_1).$$

For $a > 2g$, we have

$$\Lambda^a(\mathrm{std}) = 0.$$

For $g < a \leq 2g$, we have (by autoduality)

$$\Lambda^a(\mathrm{std}) = \Lambda^{2g-a}(\mathrm{std}).$$

For $a \leq g$ odd, we have

$$\Lambda^a(\mathrm{std}) = \oplus_{0 \leq j \leq [a/2]} V(\omega_{a-2j}).$$

For $a \leq g$ even, we have

$$\Lambda^a(\mathrm{std}) = \mathbb{1} \oplus (\oplus_{1 \leq j \leq [a/2]} V(\omega_{2j})).$$

So for $b \geq 2$, $\mathrm{Sym}^b(\mathrm{std})$, whose highest weight is $b\omega_1$, does not occur in any $\Lambda^a(\mathrm{std})$. For $b = 1$, $\mathrm{Sym}^1(\mathrm{std}) = V(\omega_1)$ occurs precisely in those $\Lambda^a(\mathrm{std})$ with a odd and $a < 2g$, and it occurs once in each. For $b = 0$, $\mathrm{Sym}^0(\mathrm{std}) = \mathbb{1}$ occurs precisely in those $\Lambda^a(\mathrm{std})$ with a even and $a \leq 2g$, and it occurs once in each. QED

Using this lemma and the above formula

$\int_{USp(2g)} \mathrm{Trace}(A^r)dA$

$$= \sum_{a\geq 1,\ b\geq 0,\ a+b=r} a(-1)^{a-1}\dim\mathrm{Hom}_G(\mathrm{Sym}^b(\mathrm{std}), \Lambda^a(\mathrm{std})),$$

we easily prove the symplectic indicator lemma. If r is odd, all the pairs (a, b) which sum to r have have opposite parity, so give zero contribution. If r is even, then there are precisely two terms which could possibly contribute, namely the ($a=r-1$, $b=1$) term and the ($a=r$, $b=0$) term. If $r > 2g$, then $r \geq 2g+2$, and both terms vanish. If $r \leq 2g$, the first contributes $(r-1)(-1)^{r-2} = r-1$, the second contributes $r(-1)^{r-1} = -r$. QED

We now turn to the proof of the orthogonal indicator lemma.

The group $O(N, \mathbb{R})$ contains the scalar -1, so we trivially have

$$\int_{O(N, \mathbb{R})}\mathrm{Trace}(A^r)dA = 0, \text{ if r is odd.}$$

Suppose now r is even, $r = 2k$, $k \geq 1$. We first explain how the question reduces to one on $SO(N, \mathbb{R})$.

Consider the case when N is odd, $N = 2n+1$. Then

$$O(2n+1, \mathbb{R}) = (\pm 1)\times SO(2n+1, \mathbb{R}),$$

and the integrand is invariant under the subgroup ± 1. Hence we have

$$\int_{O(2n+1, \mathbb{R})}\mathrm{Trace}(A^{2k})dA = \int_{SO(2n+1, \mathbb{R})}\mathrm{Trace}(A^{2k})dA.$$

So for $N = 2n+1$ odd, we must show that

$$\int_{SO(2n+1, \mathbb{R})}\mathrm{Trace}(A^{2k})dA = 1, \text{ for all } k \geq 1.$$

It suffices to treat the case $n \geq 1$, the case $n = 0$ being trivially correct.

If $N = 2n$ is even, then we have

$$\int_{O(2n, \mathbb{R})}\mathrm{Trace}(A^{2k})dA$$
$$= (1/2)\int_{SO(2n, \mathbb{R})}\mathrm{Trace}(A^{2k})dA + (1/2)\int_{O\_(2n, \mathbb{R})}\mathrm{Trace}(A^{2k})dA.$$

Let us first treat the case $N = 2$. Every element in $O\_(2, \mathbb{R})$ has eigenvalues $\{1, -1\}$, so the function $\mathrm{Trace}(A^{2k})$ on $O\_(2, \mathbb{R})$ is the constant function 2. Therefore we find

$$\int_{O(2, \mathbb{R})}\mathrm{Trace}(A^{2k})dA = (1/2)\int_{SO(2, \mathbb{R})}\mathrm{Trace}(A^{2k})dA + 1.$$

If we view $SO(2, \mathbb{R})$ as the unit circle $S^1 = \mathbb{R}/2\pi\mathbb{Z}$ with parameter θ in $[0, 2\pi)$, then Haar measure is $d\theta/2\pi$, and the function $\mathrm{Trace}(A^{2k})$ is $2\cos(2k\theta)$. Since $k \geq 1$, we see that

$$\int_{SO(2, \mathbb{R})}\mathrm{Trace}(A^{2k})dA = (1/2\pi)\int_{[0,2\pi)} 2\cos(2k\theta)d\theta = 0.$$

Thus for N=2, the Proposition is proved.

Now suppose $N = 2n$ is even, $n \geq 2$. Every element in $O\_(2n, \mathbb{R})$ has both 1 and -1 as eigenvalues, and the remaining $2n-2$ eigenvalues fall into $n-1$ pairs of inverses $\{e^{i\theta(j)}, e^{-i\theta(j)}\}$. If we interpret these $n-1$ pairs of inverses as arising from a conjugacy class in $USp(2n-2)$, we get a bijection of spaces of conjugacy classes

$$O\_(2n, \mathbb{R})^\# \cong USp(2n-2)^\#.$$

It is a marvelous fact that under this bijection, the total mass one Haar measures coincide, cf. [Ka−Sar, RMFEM, 5.0.4 and 5.0.7] And under this bijection, the function $\mathrm{Trace}(A^{2k})$ on $O\_(2n, \mathbb{R})^\#$ becomes the function $2 + \mathrm{Trace}(A^{2k})$ on $USp(2n-2)^\#$. Thus we find

$$\int_{O(2n, \mathbb{R})}\mathrm{Trace}(A^{2k})dA$$
$$= (1/2)\int_{SO(2n, \mathbb{R})}\mathrm{Trace}(A^{2k})dA + (1/2)\int_{USp(2n-2)}(2 + \mathrm{Trace}(A^{2k}))dA$$
$$= 1 + (1/2)\int_{SO(2n, \mathbb{R})}\mathrm{Trace}(A^{2k})dA + (1/2)\int_{USp(2n-2)}\mathrm{Trace}(A^{2k})dA.$$

We have already evaluated the final term:

$$\int_{USp(2n-2)}\mathrm{Trace}(A^{2k})dA \quad = -1 \text{ for } 1 \le k \le n-1,$$
$$= 0 \text{ for } k \ge n.$$

So for N = 2n even with n ≥ 2, we must show

$$\int_{SO(2n, \mathbb{R})}\mathrm{Trace}(A^{2k})dA \quad = 1, \text{ if } 1 \le k \le n-1,$$
$$= 0, \text{ if } k \ge n.$$

So the orthogonal higher indicator lemma above is equivalent to the following one.

Special Orthogonal Indicator Lemma

1) For $N \ge 3$ odd, and for any $k \ge 1$, we have

$$\int_{SO(N, \mathbb{R})}\mathrm{Trace}(A^{2k})dA = 1.$$

2) For $N \ge 4$ even, and $k \ge 1$, we have

$$\int_{SO(N, \mathbb{R})}\mathrm{Trace}(A^{2k})dA = 1, \text{ if } 2 \le 2k < N,$$
$$= 0, \text{ if } 2k \ge N.$$

proof We first treat separately the case N = 4. The group SO(4, $\mathbb{R}$) in its standard representation std_4 is the quotient of USp(2)×USp(2) in $\mathrm{std}_2 \otimes \mathrm{std}_2$. by the subgroup of order two generated by (−1, −1). Thus we have

$$\int_{SO(4, \mathbb{R})}\mathrm{Trace}(A^{2k})dA = \int_{USp(2)\times USp(2)}\mathrm{Trace}((A\otimes B)^{2k})dAdB$$
$$= \int_{USp(2)\times USp(2)}\mathrm{Trace}(A^{2k})\mathrm{Trace}(B^{2k})dAdB$$
$$= (\int_{USp(2)}\mathrm{Trace}(A^{2k})dA)^2.$$

We have already seen that for $k \ge 1$, we have

$$\int_{USp(2)}\mathrm{Trace}(A^{2k})dA =-1, \text{ if } k = 1,$$
$$= 0, \text{ if } k \ge 2,$$

so the proposition is correct for N = 4.

We next treat separately the case N = 3. For SO(3, $\mathbb{R}$), every conjugacy class meets the maximal torus $\mathrm{Diag}(e^{i\theta}, 1, e^{-i\theta})$. We have $SO(3, \mathbb{R})^\# = [0, \pi]$, and the direct image of Haar measure is $(2/\pi)\sin(\theta/2)^2 d\theta$. The function $\mathrm{Trace}(A^{2k})$ on $SO(3, \mathbb{R})^\#$ is the function $1 + 2\cos(2k\theta)$ on $[0, \pi]$. The proposition amounts to the vanishing of $\int_{[0,\pi]} \cos(2k\theta)\sin(\theta/2)^2 d\theta$ for $k \ge 1$.

We now treat the remaining cases N ≥ 5. Denote by std the standard representation of G =SO(N, $\mathbb{R}$). We will use the identity

$$\int_{SO(N, \mathbb{R})}\mathrm{Trace}(A^r)dA$$
$$= \sum_{a\ge 1,\ b\ge 0,\ a+b=r} a(-1)^{a-1}\mathrm{dimHom}_G(\Lambda^a(\mathrm{std}), \mathrm{Sym}^b(\mathrm{std})).$$

Let us temporarily admit the truth of the following lemma.

Lemma Let N ≥ 5. On G = SO(N, $\mathbb{R}$), we have the following results.

If a = 0 and if b is even, then

$$\mathrm{dimHom}_G(\Lambda^a(\mathrm{std}), \mathrm{Sym}^b(\mathrm{std})) = 1.$$

If a = 1 and if b is odd, then

$$\mathrm{dimHom}_G(\Lambda^a(\mathrm{std}), \mathrm{Sym}^b(\mathrm{std}))) = 1.$$

If a = N−1 and if b is odd, then

$$\mathrm{dimHom}_G(\Lambda^a(\mathrm{std}), \mathrm{Sym}^b(\mathrm{std}))) = 1.$$

If a = N and if b is even, then

$$\mathrm{dimHom}_G(\Lambda^a(\mathrm{std}), \mathrm{Sym}^b(\mathrm{std}))) = 1.$$

In all other cases,

$$\mathrm{dimHom}_G(\Lambda^a(\mathrm{std}), \mathrm{Sym}^b(\mathrm{std})) = 0.$$

We first explain why this lemma implies the special orthogonal indicator lemma. Indeed, if N is odd, then the only term (a, b) which can contribute to

$$\Sigma_{a\geq 1,\ b\geq 0,\ a+b=2k}\ a(-1)^{a-1}\mathrm{dimHom}_G(\Lambda^a(\mathrm{std}), \mathrm{Sym}^b(\mathrm{std})).$$

is the single term (1, 2k−1), which contributes 1.This proves part 1) . If N is even, there at most three terms (a, b) which can contribute to this sum:

(1, 2k−1), which contributes 1,

and, if 2k ≥ N−1, the two terms

(N−1, 2k+1−N), which contributes N−1,

(N, 2k − N), which contributes −N.

This proves part 2).

It remains to prove the lemma. Suppose first N = 2n +1 is odd, n ≥ 2. In terms of the fundamental weights $\omega_1, ..., \omega_n$, we have

$$\mathrm{std} = V(\omega_1),$$

$$\Lambda^0(\mathrm{std}) = \mathbb{1} = V(0\omega_1),$$

$$\Lambda^a(\mathrm{std}) = V(\omega_a), \text{ for } 1 \leq a \leq n-1,$$

$$\Lambda^n(\mathrm{std}) = V(2\omega_n),$$

$$\Lambda^{N-a}(\mathrm{std}) \cong \Lambda^a(\mathrm{std}) \text{ for } 1 \leq a \leq N,$$

$$\mathrm{Sym}^b(\mathrm{std}) = \oplus_{0 \leq j \leq [b/2]} V((b-2j)\omega_1)), \text{ for } b \geq 0,$$

So the lemma is clear in this case: the highest weights of the irreducible constituents of any $\mathrm{Sym}^b(\mathrm{std})$ are integer multiples of ω_1, and the only $\Lambda^a(\mathrm{std})$ of this type have a either 0 or 1 or N or N−1.

Suppose now N = 2n is even, n ≥ 3. In terms of the fundamental weights $\omega_1, ..., \omega_n$, we have

$$\mathrm{std} = V(\omega_1),$$

$$\Lambda^0(\mathrm{std}) = \mathbb{1}= V(0\omega_1),$$

$$\Lambda^a(\mathrm{std}) = V(\omega_a), \text{ for } 1 \leq a \leq n-2,$$

$\Lambda^{n-1}(\mathrm{std}) = V(\omega_{n-1} + \omega_n)$

$\Lambda^{n}(\mathrm{std}) = V(2\omega_{n-1}) \oplus V(2\omega_n)$,

$\Lambda^{N-a}(\mathrm{std}) \cong \Lambda^{a}(\mathrm{std})$ for $1 \le a \le N$,

$\mathrm{Sym}^{b}(\mathrm{std}) = \oplus_{0 \le j \le [b/2]} V((b-2j)\omega_1))$, for $b \ge 0$,

The highest weights of the irreducible constituents of any $\mathrm{Sym}^{b}(\mathrm{std})$ are integer multiples of ω_1, As $n \ge 3$, the only $\Lambda^{a}(\mathrm{std})$ of this type have a either 0 or 1 or N or N−1. So the lemma is clear in this case as well. QED

Remark We formulated the quadratic excess theorems for certain universal families of smooth projective hypersurfaces, whose geometric monodromy groups we knew to be the full orthogonal or symplectic groups. But any family X/S of smooth projective hypersurfaces whose geometric monodromy group is the full orthogonal or symplectic group would work as well. As would any family of curves *C*/S of genus g ≥ 1 whose geometric monodromy group is the full symplectic group.

References

[Br−Gr] Brock, B., and Granville, A., More points on curves over finite field extensions than expected, to appear

[Cur] Curtis, C. W., *Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Brauer*, History of Mathematics 15, A.M.S. and L.M.S., 1999.

[Di−Sha] Diaconis, P., and Shahshahani, M., On the eigenvalues of random matrices, in *Studies in applied probability*, J. Appl. Prob. 31A (1994), 49−−62

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

[F−S] Frobenius, F.G., and Schur, I., Uber die reelen Darstellungen der endlichen Gruppen, S'ber. Akad. Wis. Berlin (1906), 186−208.

[Ka−MFC] Katz, N., Monodromy of families of curves; applications of some results of Davenport−Lewis, Seminaire D.P.P. 1979/80, Progress in Mathematics 12, Birkhauser, 1983, 171−195.

[Ka−Sar, RMFEM] Katz, N., and Sarnak, P., *Random Matrices, Frobenius Eigenvalues, and Monodromy*, A.M.S. Colloquium Publications 45, 1999.