TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 364, Number 5, May 2012, Pages 2539–2566
S 0002-9947(2012)05406-7
Article electronically published on January 6, 2012

CYCLE INDICES FOR FINITE ORTHOGONAL GROUPS OF EVEN CHARACTERISTIC

JASON FULMAN, JAN SAXL, AND PHAM HUU TIEP

Dedicated to Peter M. Neumann on the occasion of his seventieth birthday

ABSTRACT. We develop cycle index generating functions for orthogonal groups in even characteristic and give some enumerative applications. A key step is the determination of the values of the complex linear-Weil characters of the finite symplectic group, and their induction to the general linear group, at unipotent elements. We also define and study several natural probability measures on integer partitions.

1. INTRODUCTION

Pólya [34], in a landmark paper on combinatorics (see [35] for an English translation), introduced the cycle index of the symmetric groups. This can be written as follows. Let $a_i(\pi)$ be the number of i-cycles of π. The Taylor expansion of e^z and the fact that there are $n!/\prod_i (a_i! i^{a_i})$ elements of S_n with a_i i-cycles yield the following theorem.

Theorem 1.1 (Pólya [34])**.**

$$1 + \sum_{n=1}^{\infty} \frac{u^n}{n!} \sum_{\pi \in S_n} \prod_i x_i^{a_i(\pi)} = \prod_{m=1}^{\infty} e^{\frac{x_m u^m}{m}}.$$

The Pólya cycle index has been a key tool in understanding what a typical permutation $\pi \in S_n$ "looks like". It is useful for studying properties of a permutation which depend only on its cycle structure. Here are a few examples of theorems which can be proved using the cycle index. Shepp and Lloyd [40] showed that for any $i < \infty$, the joint distribution of $(a_1(\pi), \ldots, a_i(\pi))$ for π chosen uniformly in S_n converges to independent (Poisson(1), ..., Poisson($\frac{1}{i}$)) random variables as $n \to \infty$. Goncharov [19] proved that the number of cycles in a random permutation is asymptotically normal with mean and variance $\log(n)$. Goh and Schmutz [18] proved that if μ_n is the average order of an element of S_n, then

$$\log(\mu_n) = C\sqrt{\frac{n}{\log(n)}}(1 + o(1)),$$

where $C = 2.99047....$

Received by the editors April 15, 2010 and, in revised form, June 21, 2010.
2010 *Mathematics Subject Classification.* Primary 20G40; Secondary 20C33, 05E15.
Key words and phrases. Random matrix, cycle index, Weil representation, random partition.
The first author was partially supported by NSF grant DMS-0802082 and NSA grant H98230-08-1-0133.
The third author was partially supported by NSF grant DMS-0901241.
The authors are grateful to Martin Liebeck for kindly sending them the preprint [26] which plays an important role in the current paper.

Given the above facts, it is very natural to seek cycle indices for finite classical groups. Kung [23] and Stong [42] developed cycle indices for the tower of groups $GL_n(q)$; applications, and extensions to $GU_n(q)$ and odd characteristic symplectic and orthogonal groups appear in [9]. The paper [45] independently uses generating function methods to study various proportions in $GL_n(q)$, and the memoir [16] extends results in [9] and [45] to other finite classical groups. Britnell [3], [4], [5], [6] extends cycle index techniques to $SL_n(q)$, $SU_n(q)$, and odd characteristic groups related to the finite symplectic and orthogonal groups. The case of even characteristic symplectic groups was treated in [12], using representation theory.

These cycle indices for finite classical groups are quite useful; they have applications in computational group theory [32], and were fundamental to the proof of the Boston-Shalev conjecture that the proportion of derangements in a primitive action of a simple group on a set X with $|X| > 1$ is uniformly bounded away from 0 (see [13] and the references therein). Even quite complicated statistics such as the order of a random matrix can be studied using cycle index techniques [38]; Schmutz's results along these lines were crucially applied by Shalev in [39].

The purpose of this paper is to obtain results for one important remaining case: even characteristic orthogonal groups. Throughout this paper $O^{\pm}(n,q)$ denotes the full orthogonal group (not the conformal group), though some authors use the notation $GO^{\pm}(n,q)$. Since odd dimensional orthogonal groups are isomorphic to symplectic groups and one can easily move between the corresponding rational canonical forms in $GL_{2n}(q)$ and $GL_{2n+1}(q)$ (see Lemma 3.1), we assume that the dimension is even. In principle the cycle indices could be obtained by adding conjugacy class sizes of $O^{\pm}_{2n}(q)$ with a given GL rational canonical form, and using formulas of Wall [44]. However this seems quite a daunting task, and Wall's treatment of conjugacy classes in even characteristic finite orthogonal groups is so complicated that experts (Liebeck and Seitz) have initiated a program of revisiting Wall's work (see for instance [26]), and Lusztig ([28], [29], [30]) has three recent papers on the topic. As another example of the complexity of the characteristic two case, see Andrews' proof [2] of the Lusztig-Macdonald-Wall conjectures on enumerating conjugacy classes in $O^{\pm}(2n,q)$. Our strategy for studying characteristic two cycle indices employs representation theory, and a crucial step is the derivation of a formula for the complex linear-Weil characters of $Sp_{2n}(q)$ on unipotent elements.

This paper is organized as follows. Section 2 performs the needed character theory calculations. This includes several intermediate results such as a branching formula and parameterizations of unipotent classes which may be of independent interest. Section 3 briefly treats odd dimensional orthogonal groups, and Section 4 develops the cycle indices for $O^{\pm}(2n,q)$ and $\Omega^{\pm}(2n,q)$. Some enumerative applications are given in Section 5. Section 6 defines and studies several probability measures on integer partitions, which we speculate may arise as an orthogonal analog of the Cohen-Lenstra number field/function field heuristics.

2. Character theory calculations

2.1. **Some permutation characters.** To begin we review some representation theory. Let $S := Sp_{2n}(q)$ be the finite symplectic group stabilizing a nondegenerate symplectic form $(\cdot,\cdot)$ on $V = \mathbb{F}_q^{2n}$, with q a power of 2. Then S acts as a permutation group on the set of quadratic forms polarized to $(\cdot,\cdot)$. There are two

orbits, depending on the Witt index (or the type) of the forms. The two permutation characters, π^+ and π^-, are both multiplicity-free. This is well known; a proof appears in [22], and we sketch it below. We use the methods of [22] to obtain a decomposition of these characters into irreducible characters. We first show that $\pi = \pi^+ + \pi^-$ is equal to the permutation character $\boldsymbol{\tau}_n$ of S acting on the set of vectors of V. We then show that

$$\pi^+ = 1_S + \boldsymbol{\rho}_n^2 + \sum_{i=1}^{(q-2)/2} \boldsymbol{\tau}_n^i,\ \pi^- = 1_S + \boldsymbol{\rho}_n^1 + \sum_{i=1}^{(q-2)/2} \boldsymbol{\tau}_n^i, \tag{1}$$

where $1_S + \boldsymbol{\rho}_n^1 + \boldsymbol{\rho}_n^2$ is the permutation character of the well-known rank 3 permutation action of S on the set of 1-subspaces of V, and each of the $\boldsymbol{\tau}_n^i$ is an irreducible character of degree $(q^{2n}-1)/(q-1)$. These characters $\boldsymbol{\tau}_n^i$ are restrictions of irreducible characters of the corresponding general linear group $G = GL_{2n}(q)$ and are the complex linear-Weil characters, investigated by Guralnick and Tiep [20]. We will only use the fact that for g unipotent,

$$\boldsymbol{\tau}_n^i(g) = \frac{q^{d(g)}-1}{q-1}, \tag{2}$$

for all i, where $d(g)$ is the dimension of the kernel of $g-1$.

Let $g \in S$. Then $\pi(g) > 0$; the proof of this, due to Inglis, appears in [37, Lemma 4.1]. Let Q be a quadratic form supported by $(\cdot,\cdot)$, and fixed by g. If R is a quadratic form supported by $(\cdot,\cdot)$, then $Q+R$ is a quadratic form on V which is totally defective (that is, $Q+R$ is a quadratic form supported by the zero symplectic form). Any such quadratic form is the square of a unique linear functional $f_{Q,R}$ on V, and R is fixed by g if and only if $f_{Q,R}$ is fixed by g. It follows that π equals the permutation character $\boldsymbol{\tau}_n$ of S on the set of vectors of V.

Inglis takes this further: for bilinear forms Q and R supported by $(\cdot,\cdot)$, let $y_{Q,R}$ be the unique vector such that $(Q+R)(x) = (x, y_{Q,R})^2$ for all $x \in V$, and then define $a(Q,R) = Q(y_{Q,R}) = R(y_{Q,R})$. The pairs (Q,R) and (Q_1,R_1) lie in the same orbit of S on ordered pairs of forms if and only if $a(Q,R) = a(Q_1,R_1)$. From this it follows that the permutation rank of the action of S on the quadratic forms of a given type $+$ or $-$ is $(q+2)/2$. Since $a(Q,R) = a(R,Q)$, it follows that each orbital in these actions of S is self-paired, whence the permutation characters π^+ and π^- are both multiplicity free. This last claim can also be seen directly: in dimension two it is a very easy computation, and for $Sp_{2n}(q)$ it is seen by restriction to $Sp_2(q^n)$ (note that $Sp_2(q^n)$ is transitive in our actions of $Sp_{2n}(q)$).

It is shown in [20, §3] that

$$\boldsymbol{\tau}_n = 2 \cdot 1_S + \boldsymbol{\rho}_n^1 + \boldsymbol{\rho}_n^2 + 2 \sum_{i=1}^{(q-2)/2} \boldsymbol{\tau}_n^i.$$

Now the claimed decomposition (1) for π^+ and π^- easily follows since the characters π^+, π^- are multiplicity free, each with $(q+2)/2$ constituents.

2.2. **Branching rules for linear-Weil characters.** We recall the construction [43] of the dual pair $Sp_{2n}(q) \times O_2^+(q)$ in characteristic 2. Let $U = \mathbb{F}_q^{2n}$ be endowed with the standard symplectic form $(\cdot,\cdot)$. We will also consider the $\mathbb{F}_2$-symplectic form $\langle u, v\rangle = \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_2}((u,v))$ on U, and let

$$E = \mathbb{C}^{q^{2n}} = \langle e_u \mid u \in U\rangle_{\mathbb{C}}.$$

Clearly, $S := Sp_{2n}(q)$ acts on E via $g \ : \ e_u \mapsto e_{g(u)}$. Fix $\delta \in \mathbb{F}_q^\times$ of order $q-1$ and consider the following endomorphisms of E:

$$\boldsymbol{\delta} \ : \ e_u \mapsto e_{\delta u}$$

(for any $u \in U$), and

$$j \ : \ e_0 \mapsto e_0, \ e_v \mapsto \frac{1}{q^n+1} \sum_{0 \neq w \in U, \ \langle v,w \rangle = 0} e_w - \frac{q^n+2}{q^n(q^n+1)} \sum_{w \in U, \ \langle w,v \rangle \neq 0} e_w$$

(for any $0 \neq v \in U$). One can check that $D := < \boldsymbol{\delta}, j > \simeq O_2^+(q)$ (a dihedral group of order $2(q-1)$), and that D centralizes S. The subgroup $S \times D$ of $GL(E)$ is the desired dual pair $Sp_{2n}(q) \times O_2^+(q)$. Let $\boldsymbol{\omega}_n$ denote the character of $S \times D$ acting on E. It is shown in [43] that $\boldsymbol{\omega}_n|_S = \boldsymbol{\tau}_n$, the permutation character of S on the point set of its natural module $V = \mathbb{F}_q^{2n}$. Moreover one can label the irreducible characters of D as $\boldsymbol{\nu}_2 = 1_D$, $\boldsymbol{\nu}_1$ of degree 1, and $\boldsymbol{\mu}_i$, $1 \leq i \leq (q-2)/2$, of degree 2 such that

$$\boldsymbol{\omega}_n|_{S \times D} = (\boldsymbol{\rho}_n^1 + 1_S) \otimes \boldsymbol{\nu}_1 + (\boldsymbol{\rho}_n^2 + 1_S) \otimes \boldsymbol{\nu}_2 + \sum_{i=1}^{(q-2)/2} \boldsymbol{\tau}_n^i \otimes \boldsymbol{\mu}_i. \tag{3}$$

We can repeat the above construction but with $n = k + l$ replaced throughout by $k > 0$, resp. by $l > 0$, and subscript 1, resp. 2, attached to all letters U, E, S, D, $\boldsymbol{\delta}$, and j. Thus we get the dual pair $S_1 \times D_1 \simeq Sp_{2k}(q) \times O_2^+(q)$ inside $GL(E_1)$ with character $\boldsymbol{\omega}_k$, and the dual pair $S_2 \times D_2 \simeq Sp_{2l}(q) \times O_2^+(q)$ inside $GL(E_2)$ with character $\boldsymbol{\omega}_l$. Now we can identify U with $U_1 \oplus U_2$. This in turn identifies E with $E_1 \otimes E_2$ and $\boldsymbol{\delta}$ with $\boldsymbol{\delta}_1 \otimes \boldsymbol{\delta}_2$. This identification also embeds $S_1 \otimes S_2$ in S. In what follows, we denote $x_1 := \boldsymbol{\delta}_1^a j_1^b$ and $x_2 := \boldsymbol{\delta}_2^a j_2^b$ for $x = \boldsymbol{\delta}^a j^b$.

Lemma 2.1. *Let $Sp_{2k}(q) \times Sp_{2l}(q)$ be a standard subgroup of $Sp_{2n}(q)$. Then $\boldsymbol{\omega}_n(gx) = \boldsymbol{\omega}_k(g_1x_1) \cdot \boldsymbol{\omega}_l(g_2x_2)$ for any $x \in O_2^+(q)$ and any $g = g_1 \otimes g_2 \in Sp_{2k}(q) \times Sp_{2l}(q)$.*

Proof. First suppose that $x = \boldsymbol{\delta}^a$. Then

$$gx = (g_1 \otimes g_2)(\boldsymbol{\delta}_1 \otimes \boldsymbol{\delta}_2)^a = (g_1 \otimes g_2)(\boldsymbol{\delta}_1^a \otimes \boldsymbol{\delta}_2^a) = g_1\boldsymbol{\delta}_1^a \otimes g_2\boldsymbol{\delta}_2^a = g_1x_1 \otimes g_2x_2,$$

whence the statement follows by taking the trace.

It remains to consider the case $x = \boldsymbol{\delta}^a j$. Since all the elements $\boldsymbol{\delta}^a j$ for $0 \leq a < q-1$ are conjugate in D, we may assume that $a = 0$. Let

$$N := |\{w \in U \mid \langle w, g(w) \rangle = 0\}|, \ N_i := |\{w \in U_i \mid \langle w, g_i(w) \rangle = 0\}|$$

for $i = 1, 2$. One can check that

$$\boldsymbol{\omega}_n(gx) = 2q^{-n}N - q^n, \ \boldsymbol{\omega}_k(g_1x_1) = 2q^{-k}N_1 - q^k, \ \boldsymbol{\omega}_l(g_2x_2) = 2q^{-l}N_2 - q^l.$$

To relate N to N_1 and N_2, write $w = u_1 + u_2$ for $w \in W$ and $u_i \in U_i$. Then $g_i(u_i) \in U_i$ and so

$$\langle w, g(w) \rangle = \langle u_1 + u_2, g_1(u_1) + g_2(u_2) \rangle = \langle u_1, g_1(u_1) \rangle + \langle u_2, g_2(u_2) \rangle.$$

It follows that $\langle w, g(w) \rangle = 0$ if and only if

$$\langle u_1, g_1(u_1) \rangle = \langle u_2, g_2(u_2) \rangle = 0 \text{ or } \langle u_1, g_1(u_1) \rangle = \langle u_2, g_2(u_2) \rangle = 1.$$

Hence $N = N_1N_2 + (q^{2k} - N_1)(q^{2l} - N_2)$, and so

$$\begin{aligned}\boldsymbol{\omega}_n(gx) &= 2q^{-n}(N_1N_2 + (q^{2k} - N_1)(q^{2l} - N_2)) - q^n \\ &= (2q^{-k}N_1 - q^k)(2q^{-l}N_2 - q^l),\end{aligned}$$

as stated. □

A well-known consequence of orthogonality relations (see e.g. Lemma 5.5 of [25]) implies that, for any $g \in S$ and $x \in D$,

$$\boldsymbol{\omega}_n(gx) = \sum_{\alpha \in \ \mathrm{Irr}(D)} \alpha(x) \cdot D_\alpha(g), \tag{4}$$

where

$$D_\alpha(g) = \frac{1}{|D|} \sum_{x \in D} \overline{\alpha(x)} \boldsymbol{\omega}_n(gx).$$

We will use the decomposition (4) and Lemma 2.1 to prove the following branching rule for the virtual character $\boldsymbol{\lambda}_n := \pi^+ - \pi^- = \boldsymbol{\rho}_n^2 - \boldsymbol{\rho}_n^1$; see (1).

Lemma 2.2. *Let $Sp_{2k}(q) \times Sp_{2l}(q)$ be a standard subgroup of $Sp_{2n}(q)$. Then $\boldsymbol{\lambda}_n(g) = \boldsymbol{\lambda}_k(g_1) \cdot \boldsymbol{\lambda}_l(g_2)$ for any $g = g_1 \otimes g_2 \in Sp_{2k}(q) \times Sp_{2l}(q)$.*

Proof. We will use the notation introduced before Lemma 2.1. Applying (4) to the dual pairs $S_1 \times D$ and $S_2 \times D$, we can also write

$$\boldsymbol{\omega}_k(g_1x_1) = \sum_{\alpha \in \ \mathrm{Irr}(D)} \alpha(x_1) \cdot E_\alpha(g_1), \ \boldsymbol{\omega}_l(g_2x_2) = \sum_{\alpha \in \ \mathrm{Irr}(D)} \alpha(x_2) \cdot F_\alpha(g_2),$$

where E_α, resp. F_α, plays the role of D_α for S_1, resp. for S_2, and $g = g_1 \otimes g_2$. By Lemma 2.1, we now have

$$\boldsymbol{\omega}_n(gx) = \boldsymbol{\omega}_k(g_1x_1) \cdot \boldsymbol{\omega}_l(g_2x_2) = \sum_{\beta,\gamma \in \ \mathrm{Irr}(D)} \beta(x_1)\gamma(x_2) \cdot E_\beta(g_1)F_\gamma(g_2).$$

It follows that

$$D_\alpha(g) = \frac{1}{|D|} \sum_{x \in D, \ \beta,\gamma \in \mathrm{Irr}(D)} \overline{\alpha(x)}\beta(x_1)\gamma(x_2)E_\beta(g_1)F_\gamma(g_2)$$

$$= \sum_{\beta,\gamma} \left(\frac{1}{|D|} \sum_{x \in D} \overline{\alpha(x)}\beta(x)\gamma(x) \right) E_\beta(g_1)F_\gamma(g_2) = \sum_{\beta,\gamma} [\beta\gamma, \alpha] E_\beta(g_1)F_\gamma(g_2),$$

where $[\cdot, \cdot]$ is the usual scalar product on the space of class functions on D. We will apply this identity to the cases where $\alpha \in \{\boldsymbol{\nu}_1, \boldsymbol{\nu}_2\}$. In these cases, α is linear; furthermore, any $\beta \in \mathrm{Irr}(D)$ is real. Hence $[\beta\gamma, \alpha] \neq 0$ if and only if $\beta = \alpha\gamma$, which means that $\beta = \gamma$ if $\alpha = \boldsymbol{\nu}_2 = 1_D$. If $\alpha = \boldsymbol{\nu}_1$, the unique nonprincipal linear irreducible character of D, then $\alpha\gamma$ equals γ, resp. $\boldsymbol{\nu}_2$, or $\boldsymbol{\nu}_1$, if $\gamma = \boldsymbol{\mu}_i$, resp. $\gamma = \boldsymbol{\nu}_1$, or $\gamma = \boldsymbol{\nu}_2$. We have therefore shown that

$$(D_{\boldsymbol{\nu}_1})|_{S_1 \times S_2} = E_{\boldsymbol{\nu}_1} \otimes F_{\boldsymbol{\nu}_2} + E_{\boldsymbol{\nu}_2} \otimes F_{\boldsymbol{\nu}_1} + \sum_{i=1}^{(q-2)/2} E_{\boldsymbol{\mu}_i} \otimes F_{\boldsymbol{\mu}_i},$$

$$(D_{\boldsymbol{\nu}_2})|_{S_1 \times S_2} = E_{\boldsymbol{\nu}_1} \otimes F_{\boldsymbol{\nu}_1} + E_{\boldsymbol{\nu}_2} \otimes F_{\boldsymbol{\nu}_2} + \sum_{i=1}^{(q-2)/2} E_{\boldsymbol{\mu}_i} \otimes F_{\boldsymbol{\mu}_i}.$$

On the other hand, by (3) we have $D_{\boldsymbol{\nu}_1} = \boldsymbol{\rho}_n^1 + 1_S$ and $D_{\boldsymbol{\nu}_2} = \boldsymbol{\rho}_n^2 + 1_S$; in particular, $\boldsymbol{\lambda}_n = D_{\boldsymbol{\nu}_2} - D_{\boldsymbol{\nu}_1}$, and similarly $\boldsymbol{\lambda}_k = E_{\boldsymbol{\nu}_2} - E_{\boldsymbol{\nu}_1}$ and $\boldsymbol{\lambda}_l = F_{\boldsymbol{\nu}_2} - F_{\boldsymbol{\nu}_1}$. Hence the statement follows. □

2.3. **Homogeneous unipotent elements.** In this subsection we consider unipotent elements of $S = Sp_{2n}(q)$ which are *homogeneous*; i.e., its Jordan canonical form on $V = \mathbb{F}_q^{2n}$ contains only Jordan blocks of the same size. Recall that we fix an S-invariant nondegenerate symplectic form $(\cdot,\cdot)$ on V. Let J_a denote the $a \times a$ Jordan block with eigenvalue 1. We say that $g \in S$ is *decomposable* if V can be written as an orthogonal sum of nonzero g-invariant subspaces, and *indecomposable* otherwise.

Lemma 2.3. *Assume that the Jordan canonical form of $g \in Sp_{2n}(q)$ on $V = \mathbb{F}_q^{2n}$ is $kJ_a = J_a \oplus \ldots \oplus J_a$ with $2n = ka$ and $a \geq 2$. If $a = 2$, assume in addition that g is indecomposable. Then one of the following holds.*

(i) *$n \geq 2$, all the g-invariant quadratic forms on V which are polarized to $(\cdot,\cdot)$ have the same type $\epsilon = \pm$, and $\boldsymbol{\lambda}_n(g) = \epsilon q^k$. Moreover, if $a = 2$, then $k = 2$, and $\epsilon = +$.*

(ii) *$n = k = 1$, $a = 2$, $\boldsymbol{\lambda}_n(g) = 0$.*

Proof. 1) Consider a basis $(e_1, \ldots, e_a, f_1, \ldots, f_a, \ldots, h_1, \ldots, h_a)$, in which g is represented by the matrix kJ_a. Let $\mathcal{Q}$ be the set of all g-invariant quadratic forms on V which are polarized to $(\cdot,\cdot)$. Then $\mathcal{Q} \neq \emptyset$ and in fact $|\mathcal{Q}| = \boldsymbol{\tau}_n(g) = q^k$ as mentioned above. By [41, Lemma 6.10], if $Q \in \mathcal{Q}$, then

$$Q(e_i) = (e_i, e_{i+1}),\ Q(f_i) = (f_i, f_{i+1}), \ldots, Q(h_i) = (h_i, h_{i+1})$$

for $1 \leq i \leq a-1$. Thus Q is completely determined by the k-tuple $(Q(e_a), \ldots, Q(h_a)) \in \mathbb{F}_q^k$.

2) Suppose that $a \geq 3$ and some $Q \in \mathcal{Q}$ has type $+$. Then we can find a symplectic basis $(u_1, \ldots, u_n, v_1, \ldots, v_n)$ of V such that $Q(u_i) = Q(v_i) = 0$. Since $a \geq 3$, by [41, Lemma 6.10] the subspace $W := \langle e_1, f_1, \ldots, h_1 \rangle_{\mathbb{F}_q}$ is totally singular with respect to any $Q' \in \mathcal{Q}$, in particular with respect to Q; moreover,

$$W^\perp = \langle e_1, \ldots, e_{a-1}, f_1, \ldots, f_{a-1}, \ldots, h_1, \ldots, h_{a-1} \rangle_{\mathbb{F}_q}.$$

Notice that $U := \langle u_1, u_2, \ldots, u_a \rangle_{\mathbb{F}_q}$ is totally Q-singular of the same dimension a as of W. Hence by Witt's Theorem, $W = \varphi(U)$ and $W^\perp = \varphi(U^\perp)$ for some $\varphi \in S$ which preserves Q. But $U^\perp$ contains the n-dimensional totally Q-singular subspace $M := \langle u_1, u_2, \ldots, u_n \rangle_{\mathbb{F}_q}$. It follows that $W^\perp$ contains the n-dimensional totally Q-singular subspace $\varphi(M)$. Now consider any $Q' \in \mathcal{Q}$. As mentioned in 1), Q' and Q coincide on $W^\perp$. Hence $\varphi(M)$ is also totally singular with respect to Q' and so Q' is of type $+$.

We have shown that all $Q \in \mathcal{Q}$ have the same type $\epsilon = \pm$. Recall that $\boldsymbol{\lambda}_n(g)$ is the difference between the number of $Q \in \mathcal{Q}$ of type $+$ and the number of $Q \in \mathcal{Q}$ of type $-$. It follows that $\boldsymbol{\lambda}_n(g) = \epsilon q^k$.

3) Next we consider the case $a = 2$ and $k \geq 2$. If $(e_1, e_2) \neq 0$, then $E := \langle e_1, e_2 \rangle_{\mathbb{F}_q}$ is g-invariant and nondegenerate and so $V = E \oplus E^\perp$, contradicting the assumption that g is indecomposable. Thus $(e_1, e_2) = (f_1, f_2) = \ldots = (h_1, h_2) = 0$. As mentioned in 2), e_1 is orthogonal to all the vectors $e_1, \ldots, h_1$. Since $(\cdot,\cdot)$ is nondegenerate, we may assume that $(e_1, f_2) = b \neq 0$. Then again by [41, Lemma 6.10], $(e_2, f_1) = b$. One can now check that $F := \langle e_1, e_2, f_1, f_2 \rangle_{\mathbb{F}_q}$ is g-invariant and

nondegenerate. By the assumption that g is indecomposable, we must have $k = 2$. Furthermore, E is totally singular with respect to any $Q \in \mathcal{Q}$. Now we can finish the argument as in 2).

Finally, assume $a = 2$ and $k = 1$. Then $\boldsymbol{\rho}_n^1 = 0$ and $\boldsymbol{\rho}_n^2$ is just the Steinberg character (of degree q) of $S \simeq SL_2(q)$, whence $\boldsymbol{\lambda}_n(g) = 0$. □

Of course if $a = 1$ in Lemma 2.3, then $\boldsymbol{\lambda}_n(g) = q^{k/2}$. For a general unipotent element $u \in S$, it is well known (see e.g. [41, Cor. 6.12]) that V can be written as an orthogonal sum of (possibly zero) u-invariant subspaces $V = \bigoplus_{i=1}^{\infty} V_i$ such that all Jordan blocks of $u|_{V_i}$ are of size i. Hence, combining Lemmas 2.2 and 2.3 we can compute $\boldsymbol{\lambda}_n(u)$ for any unipotent element $u \in S$. To evaluate $\boldsymbol{\Lambda}_n = \mathrm{Ind}_{Sp_{2n}(q)}^{GL_{2n}(q)}(\boldsymbol{\lambda}_n)$ at u we however need more information about unipotent classes in S with a given Jordan canonical form. This will be done in the next subsection, which also is of independent interest.

2.4. **A parametrization of unipotent classes in finite symplectic and orthogonal groups in characteristic 2.** The conjugacy classes of finite classical groups are described in [44]. A new, better, treatment of this topic, particularly in bad characteristics, has recently been given in [26]. We will use the latter results to give a parametrization of unipotent classes in finite symplectic and orthogonal groups in characteristic 2 which works well for our purposes and which also has independent interest.

Let $2|q$ as above and let $g \in S = Sp_{2n}(q)$ be any unipotent element. It is shown in [26] that the natural S-module $V = \mathbb{F}_q^{2n}$ can be written as an orthogonal sum

$$V|_{\langle g \rangle} = \sum_i W(m_i)^{a_i} \oplus \sum_{j=1}^{r} V(2k_j)^{b_j} \tag{5}$$

of g-invariant nondegenerate subspaces of two types: $V(m)$ with even m, on which g has the Jordan form J_m, and $W(m)$, on which g is indecomposable and has the Jordan form $2J_m$; moreover,

$$m_1 < m_2 < m_3 < \ldots,\ k_1 < k_2 < k_3 < \ldots,\ a_i > 0,\ 2 \geq b_j \geq 1. \tag{6}$$

Given such a decomposition (5) subject to (6) (called a *canonical decomposition* in [26]), let I be the set of indices i such that m_i is odd and larger than 1 and there does **not** exist j such that $2k_j = m_i \pm 1$, and let $s := |I|$. Next, let t be the number of indices j such that $k_{j+1} - k_j \geq 2$. We also fix $\delta \in \{0, 1\}$ with $\delta = 1$ precisely when $r > 0$ and $k_1 > 1$. We can view S as the fixed point subgroup $\mathcal{G}^F$ for a Frobenius endomorphism F on $\mathcal{G} = Sp_{2n}(\overline{\mathbb{F}}_q)$.

According to [26, Theorem 5.1], $g^{\mathcal{G}} \cap S$ splits into $2^{s+t+\delta}$ S-classes. Furthermore, $C_S(g)$ is a (not necessarily split) extension of a 2-group D by R, where $|D| = q^{\dim R_u(C_{\mathcal{G}}(g))}$, with $R_u(\cdot)$ denoting the unipotent radical, and

$$R = \left(\prod_{i\,:\,m_i \text{ even}} Sp_{2a_i}(q) \right) \times \left(\prod_{i\,:\,m_i \text{ odd}} I_{2a_i}(q) \right) \times C_2^{t+\delta}. \tag{7}$$

Here, C_2 denotes a cyclic group of order 2, $I_{2a_i}(q) = Sp_{2a_i}(q)$ if either $m_i = 1$ or there exists j such that $2k_j = m_i \pm 1$, and $I_{2a_i}(q) = O_{2a_i}^{\epsilon_i}(q)$ for some $\epsilon_i = \pm$ otherwise; in particular, s is the number of O-factors in the above factorization. We will see that these ϵ_i are related to the type of g-invariant quadratic forms discussed in Lemma 2.3(i).

If $r > 0$, partition $K := \{k_1, k_2, \dots, k_r\}$ into a disjoint union $K_\delta \sqcup K_{\delta+1} \sqcup \dots \sqcup K_{t+\delta}$ of $t+1$ "intervals" of consecutive integers, such that

$$\max\{k \mid k \in K_i\} \le \min\{l \mid l \in K_{i+1}\} - 2;$$

this is possible by the definition of the parameter t. Now, if $m_i > 1$ is odd and $m_i = 2k_j \pm 1 = 2k_{j'} \pm 1$ for distinct j and j', then $|k_j - k_{j'}| = 1$ and so k_j and $k_{j'}$ must belong to the same interval K_u. In this situation, we will say that m_i is *linked* to K_u. Next, for $\delta \le u \le t+\delta$, let

$$V_u = \left(\sum_{k_j \in K_u} V(2k_j)^{b_j} \right) \oplus \left(\sum_{m_i > 1,\ \text{odd, linked to } K_u} W(m_i)^{a_i} \right).$$

Also, if $I = \{i_1, \dots, i_s\}$, then set $W_v := W(m_{i_v})^{a_{i_v}}$ for $1 \le v \le s$. Finally, let

$$W_0 = \sum_{m_i = 1 \text{ or } m_i \text{ even}} W(m_i)^{a_i}.$$

Thus we obtain the decomposition

$$V|_{\langle g \rangle} = W_0 \oplus W_1 \oplus \dots \oplus W_s \oplus V_\delta \oplus V_{1+\delta} \oplus \dots \oplus V_{t+\delta}. \tag{8}$$

Theorem 2.4. *Consider the decomposition* (8) *for any unipotent element $g \in S = Sp_{2n}(q)$. Let $\mathcal{G} = Sp_{2n}(\overline{\mathbb{F}}_q)$. Then $g^{\mathcal{G}} \cap S$ splits into $2^{s+t+\delta}$ S-classes. Each such class is uniquely determined by the sequence $\boldsymbol{\varepsilon} = (\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_{t+\delta})$, where $\alpha_i, \beta_j = \pm$, and every g-invariant quadratic form polarized to $(\cdot,\cdot)$ on W_i with $i \ge 1$, respectively on V_j with $j \ge 1$, is of type α_i, respectively β_j. Furthermore, if the S-class of g is determined by $\boldsymbol{\varepsilon}$, then in the factorization* (7) *for R the factor $I_{2a_i}(q)$ equals $O^{\alpha_v}_{2a_i}(q)$ for $i = i_v \in I$, and $Sp_{2a_i}(q)$ otherwise.*

Proof. 1) First we observe that the invariant $\boldsymbol{\varepsilon}$ is well defined for g. Indeed, by Lemma 2.3, if U is a g-invariant nondegenerate subspace of V of type $W(m)^a$ or $V(m)^b$ with $m \ge 3$, then all g-invariant quadratic forms polarized to $(\cdot,\cdot)$ on U have the same type. This applies in particular to any W_i with $i \ge 1$ and any V_j with $j \ge 1$, whence the observation follows. It is also clear that $\boldsymbol{\varepsilon}$ is the same for all $x \in g^S$.

2) Next we aim to show that if two elements $g, h \in g^{\mathcal{G}} \cap S$ have the same invariant $\boldsymbol{\varepsilon}$, then they are conjugate in S. Applying [26, Lemma 4.2] and conjugating h by an element in S, we may assume that g and h have the same canonical decomposition (5) and the subsequent decomposition (8).

First we look at the case where the decomposition (8) reduces to $V = W_0$ or $V = V_0 \oplus V_0$; in particular, $s = t = \delta = 0$. In this case, $g^{\mathcal{G}} \cap S$ constitutes a single S-class by [26, Theorem 5.1 (ii)], whence g and h are S-conjugate.

Next we look at the case where the decomposition (8) reduces to $V = V_u$. In this case, $\delta = 1$, $s = t = 0$, and $g^{\mathcal{G}} \cap S \ne \emptyset$ by [26, Theorem 5.1 (i)]; furthermore, $g^{\mathcal{G}} \cap S$ splits into two S-classes by [26, Theorem 5.1 (ii)]. By [26, Theorem 5.1 (i)], for each $\epsilon = \pm$ we can pick $u_\epsilon \in g^{\mathcal{G}} \cap S$ such that some, hence all by Lemma 2.3, u_ϵ-invariant quadratic forms polarized to $(\cdot,\cdot)$ on V are of type ϵ. Also by Lemma 2.3 we have $\mathbf{\Lambda}_n(u_\epsilon) = \epsilon q^k$ for some integer k which depends only on $g^{\mathcal{G}}$. It follows that u_+ and u_- are not S-conjugate, whence $g^{\mathcal{G}} \cap S = (u_+)^S \sqcup (u_-)^S$. Now, denoting $\beta_1 = \beta$, we see by Lemma 2.3 that $\mathbf{\Lambda}_n(g) = \mathbf{\Lambda}_n(h) = \beta q^k$ and so g and h cannot be S-conjugate to $u_{-\beta}$. Thus both g and h are S-conjugate to u_β.

The same argument also applies to the case where the decomposition (5) reduces to $V = W_v$.

We have therefore shown that all the pairs of elements $(g|_U, h|_U)$ are conjugate in $Sp(U)$, where $U = W_0$ (or $W_0 \oplus V_0$ if $\delta = 0$), W_i with $i > 0$, or V_j with $j > 0$. Since V is the orthogonal sum of those subspaces U, we conclude that g and h are conjugate in $Sp(V) = S$.

3) Consequently, each g^S is uniquely determined by the sequence $\boldsymbol{\varepsilon}$. It remains to determine the factors $I_{2a_i}(q)$ of type $O^{\pm}_{2a_i}(q)$ in the factorization (7) for R. As noted in the proof of [26, Theorem 5.1], each of the summands in the canonical decomposition (5) can be written over $\mathbb{F}_2$, and so the Frobenius endomorphism F stabilizes each of the factors $Sp_{2a_i}(q)$, $I_{2a_i}(q)$, and C_2 which appear in $C_{\mathcal{G}}(g)/R_u(C_{\mathcal{G}}(u))$ and in R. So without loss of generality we may assume that the decomposition (8) reduces to $V = W_v$; in particular, $\boldsymbol{\varepsilon} = (\alpha_v)$ and $\dim V = 2a_{i_v}$. We fix a g-invariant quadratic form polarized to $(\cdot,\cdot)$ on V of type α_v. Direct computation using relations (3.7.3) – (3.7.5) of [44] shows that the $2'$-parts of $|C_{Sp(V)}(g)|$ and $|C_{O(V)}(g)|$ are both equal to $|O^{\alpha_v}_{2a_{i_v}}(q)|_{2'}$. On the other hand, we know that $I_{2a_{i_v}}(q) = O^{\epsilon_v}_{2a_{i_v}}(q)$ and so the $2'$-part of $|C_{Sp(V)}(g)|$ is $|O^{\epsilon_v}_{2a_{i_v}}(q)|_{2'}$. It follows that $\epsilon_v = \alpha_v$ and $I_{2a_{i_v}}(q) = O^{\alpha_v}_{2a_{i_v}}(q)$, as stated. □

Define $\mathcal{H} = O(V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q)$ (notice that $\mathcal{H}$ is disconnected) and a Frobenius endomorphism F on $\mathcal{H}$ such that $\mathcal{H}^F = H := O^{\epsilon}_{2n}(q)$ for $\epsilon = \pm$. For any unipotent element $g \in \mathcal{H}$ we again consider the canonical decomposition (5). Let I be the set of indices i such that m_i is odd and there does **not** exist j such that $2k_j = m_i \pm 1$, and let $s := |I|$. Next, let t be the number of indices j such that $k_{j+1} - k_j \geq 2$. We also fix $\delta \in \{0,1\}$ with $\delta = 1$ precisely when $r > 0$. If $r > 0$, partition $K := \{k_1, k_2, \ldots, k_r\}$ into a disjoint union $K_1 \sqcup K_2 \sqcup \ldots \sqcup K_{t+\delta}$ of $t + \delta$ intervals of consecutive integers, such that

$$\max\{k \mid k \in K_i\} \leq \min\{l \mid l \in K_{i+1}\} - 2.$$

As in the symplectic case, if m_i is odd and $m_i = 2k_j \pm 1 = 2k_{j'} \pm 1$ for distinct j and j', then $|k_j - k_{j'}| = 1$ and so k_j and $k_{j'}$ must belong to the same interval K_u. In this situation, we will again say that m_i is *linked* to K_u. Let $W_0 = \sum_{2|m_i} W(m_i)^{a_i}$ and $I = \{i_1, \ldots, i_s\}$. Next, we define

$$V_u = \left(\sum_{k_j \in K_u} V(2k_j)^{b_j} \right) \oplus \left(\sum_{m_i \text{ odd, linked to } K_u} W(m_i)^{a_i} \right)$$

if $r > 0$ and $1 \leq u \leq t + \delta$, and $W_v := W(m_{i_v})^{a_{i_v}}$ for $1 \leq v \leq s$. Thus we obtain the decomposition

$$V|_{\langle g \rangle} = W_0 \oplus W_1 \oplus \ldots \oplus W_s \oplus V_1 \oplus V_2 \oplus \ldots \oplus V_{t+\delta}. \tag{9}$$

We say that g is *exceptional* if $V|_{\langle g \rangle} = \sum_i W(m_i)^{a_i}$ with all m_i even. Now we exhibit the following analogue of Theorem 2.4 for orthogonal groups.

Theorem 2.5. *Consider the decomposition* (8) *for any unipotent element* $g \in \mathcal{H} = O_{2n}(\overline{\mathbb{F}}_q)$. *Let* $H := O^{\epsilon}_{2n}(q)$ *and* $K := \Omega^{\epsilon}_{2n}(q)$ *for some* $\epsilon = \pm$.

(i) *Then* $g^{\mathcal{H}} \cap H \neq \emptyset$ *unless* $H = O^{-}_{2n}(q)$ *and* g *is exceptional, in which case* $g^{\mathcal{H}} \cap H = \emptyset$.

(ii) *Assume* $g^{\mathcal{H}} \cap H \neq \emptyset$. *Then* $g^{\mathcal{H}} \cap H$ *splits into* $2^{s+t+\delta-1}$ H*-classes, if* g *is not exceptional, and constitutes a single* H*-class, if* g *is exceptional.*

(a) *Each such H-class constitutes a single K-class, except when g is exceptional, in which case it splits into two K-classes.*

(b) *Each such H-class is uniquely determined by the sequence $\boldsymbol{\varepsilon} = (\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_{t+\delta})$, where $\alpha_i, \beta_j = \pm$, and every g-invariant quadratic form polarized to $(\cdot,\cdot)$ on W_i with $i \geq 1$, respectively on V_j with $j \geq 1$, is of type α_i, respectively β_j, and*

$$\prod_{i=1}^{s} \alpha_i \cdot \prod_{j=1}^{t+\delta} \beta_j = \epsilon. \tag{10}$$

(c) *If the H-class of $g \in H$ is determined by $\boldsymbol{\varepsilon}$, then $C_H(g)$ is an extension of a 2-group of order $q^{\dim R_u(C_{\mathcal{H}}(g))}$ by R and the factorization (7) holds for R. The factor $I_{2a_i}(q)$ equals $O^{\alpha_v}_{2a_i}(q)$ for $i = i_v \in I$ and equals $Sp_{2a_i}(q)$ otherwise.*

Proof. (i) Notice that if $g \in H$ is exceptional, then $g \in K$ as the quasi-determinant $(-1)^{\dim \mathrm{Ker}(g-1)}$ is 1. Hence the statement follows from [26, Theorem 5.1 (i)].

(ii) First we consider the case that g is exceptional; in particular, $s = t = \delta = 0$. Then $C_{\mathcal{H}}(g)$ is connected by [26, Theorem 4.20]; hence $g^{\mathcal{H}} \cap H$ constitutes a single H-class. The connectedness of $C_{\mathcal{H}}(g)$ also implies that $C_H(g) \leq H \cap \mathcal{H}^\circ = K$ (the latter equality can be seen by using the quasi-determinant), whence g^H splits into two K-classes. The structure of $C_H(g)$ is described in [26, Theorem 5.1 (iii)].

From now on we may assume that g is not exceptional. In particular, $C_H(g) \not\leq K$ (see e.g. the proof of [26, Prop. 4.21]); hence g^H constitutes a single K-class. By the same reason, $g^{\mathcal{H}} = g^{\mathcal{H}^\circ}$.

Next, by [26, Theorem 5.1 (i)], every g-invariant quadratic form polarized to $(\cdot,\cdot)$ on W_0 is of type $+$. Also, according to Lemma 2.3, all such forms on W_v, respectively on V_u, have the same type α_v, respectively β_u, as long as $m_{i_v} > 1$, respectively $\min\{k \mid k \in K_u\} > 1$. Let α_1, respectively β_1, denote the type of such a form on W_1 with $m_{i_1} = 1$, respectively on W_1 with $k_1 = 1$. We claim that in this situation, α_1, respectively β_1, is also uniquely determined by g^H, and moreover in all cases (10) holds. Indeed, the latter equality follows from the decomposition (9) and the fact that the type of W_0 is $+$. Assume $k_1 = 1$. Notice that in this case $m_{i_1} > 1$ (as otherwise it is linked to $K_1 \ni k_1 = 1$). Thus all α_i with $i \geq 1$ and all β_j with $j \geq 2$ are uniquely determined by g^H, and so is β_1 by virtue of (10). The same argument applies to the case $k_1 > 1$ and $m_{i_1} = 1$.

Thus we have shown that the invariant $\boldsymbol{\varepsilon}$ is well defined for g^H. Furthermore, Theorem 2.4 implies that, given any $\beta_u = \pm$, there is a g-invariant quadratic form polarized to $(\cdot,\cdot)$ on V_u of type β_u. (Indeed, the claim is clear if V_u does not involve any summand $W(m_i)$ with $m_i = 1$. The statement also holds in the case that V_u involves the summand $W(1)^{2a}$: just write $V_u = Y \oplus W(1)^{2a}$, fix a g-invariant quadratic form polarized to $(\cdot,\cdot)$ on Y, say of type γ, and then choose any quadratic form of type $\gamma\beta_u$ on $W(1)^{2a}$ on which g acts trivially.) Similarly, given any $\alpha_v = \pm$, there is a g-invariant quadratic form polarized to $(\cdot,\cdot)$ on W_v of type α_v. Thus there are exactly $2^{s+t+\delta-1}$ possible values for the sequence $\boldsymbol{\varepsilon}$ subject to the condition (10), whence the conclusion (b) follows.

Finally, the arguments given in part 3 of the proof of Theorem 2.4 also show that $I_{2a_v}(q) = O^{\alpha_v}_{2a_{i_v}}(q)$. □

2.5. **The induced virtual character $\boldsymbol{\Lambda}_n = \mathrm{Ind}_{Sp_{2n}(q)}^{GL_{2n}(q)}(\boldsymbol{\lambda}_n)$.** Denote $G = GL_{2n}(q)$, $S = Sp_{2n}(q)$, and $\mathcal{G} = Sp_{2n}(\overline{\mathbb{F}}_q)$ as usual. For any unipotent element $g \in G$, if

$g^G \cap S = \bigsqcup_{i=1}^N (g_i)^S$ splits into N S-classes, then the definition of induced characters yields

$$\mathbf{\Lambda}_n(g) = |C_G(g)| \cdot \sum_{i=1}^{N} \frac{\boldsymbol{\lambda}_n(g_i)}{|C_S(g_i)|}. \tag{11}$$

Clearly, $g^G \cap S$ is just the set of all unipotent elements $x \in S$ with the same Jordan canonical form as of g. It follows that $g^G \cap S$ is the union of $g^{\mathcal{G}} \cap S$ for all $\mathcal{G}$-classes $g^{\mathcal{G}}$ with the same Jordan canonical form.

Consider the canonical decomposition (5) for $g^{\mathcal{G}} \cap S$. By Lemmas 2.2 and 2.3, $\boldsymbol{\lambda}_n(g) = 0$ if $k_1 = 1$. Assume that $r > 0$ and $k_1 > 1$; in particular, $\delta = 1$. By Theorem 2.4, $g^{\mathcal{G}} \cap S$ splits into 2^{s+t+1} S-classes which are uniquely determined by the sequence $\boldsymbol{\varepsilon}$. Now we use the decomposition (8) and Lemma 2.2 to compute $\boldsymbol{\lambda}_n(g)$:

$$\boldsymbol{\lambda}_n(g) = \prod_{i=0}^{s} \boldsymbol{\lambda}_{(\dim W_i)/2}(g|_{W_i}) \cdot \prod_{j=1}^{t+1} \boldsymbol{\lambda}_{(\dim V_j)/2}(g|_{V_j}).$$

First we look at $g|_{W_0}$. Allowing a_1 to be zero if necessary, we may assume that $m_1 = 1$. As mentioned in the proof of Theorem 2.5, all g-invariant quadratic forms polarized to $(\cdot,\cdot)$ on W_0 are of type $+$. Applying Lemma 2.3, we see that

$$\boldsymbol{\lambda}_{(\dim W_0)/2}(g|_{W_0}) = q^{a_1 + 2\sum_{2|m_i} a_i}.$$

On the other hand, by Lemmas 2.2 and 2.3 we have

$$\boldsymbol{\lambda}_{(\dim W_v)/2}(g|_{W_v}) = \alpha_v q^{2a_{i_v}}$$

for $1 \le v \le s$, and

$$\boldsymbol{\lambda}_{(\dim V_u)/2}(g|_{V_u}) = \beta_u q^{\sum_{k_j \in K_u} b_j + \sum_{m_i > 1,\ \text{odd, linked to } K_u} 2a_i}$$

for $1 \le u \le t+1$. Thus, there is an explicit constant C depending only on $g^{\mathcal{G}} \cap S$ such that $\boldsymbol{\lambda}_n(g) = [\boldsymbol{\varepsilon}] \cdot q^C$ if the conjugacy class g^S is determined by $\boldsymbol{\varepsilon}$ and $[\boldsymbol{\varepsilon}] := \prod_{v=1}^{s} \alpha_v \cdot \prod_{u=1}^{t+1} \beta_u$. Recall we are assuming that $r > 0$ and $k_1 > 1$. Then we can pair up the 2^{s+t+1} S-classes in $g^{\mathcal{G}} \cap S$ into 2^{s+t} pairs, each consisting of $(h_+)^S$ and $(h_-)^S$, determined by $\boldsymbol{\varepsilon}_+$ and $\boldsymbol{\varepsilon}_-$, which differ only at $\beta_1 = \pm$ and have the same α_i with $i > 0$ and the same β_j with $j > 1$. The above computation shows that $\boldsymbol{\lambda}_n(h_-) = -\boldsymbol{\lambda}_n(h_+)$. On the other hand, $|C_S(h_+)| = |C_S(h_-)|$ by Theorem 2.4. Hence the contributions of the pair $(h_+)^S$ and $(h_-)^S$ to $\mathbf{\Lambda}_n(g)$ in (11) cancel out each other, and so the total contribution of $g^{\mathcal{G}} \cap S$ in (11) is 0.

We have shown that the only nonzero contributions in (11) can only come from the classes in $g^{\mathcal{G}} \cap S$ with $r = t = \delta = 0$. In particular, $\mathbf{\Lambda}_n(g) = 0$ if the multiplicity c_i of some Jordan block J_i in the Jordan canonical form $\sum_{i=1}^{\infty} c_i J_i$ of g is odd. Thus we may now assume that c_i is even for all i, and the decompositions (5) and (8) of g reduce to

$$V = \sum_i W(m_i)^{a_i} = W_0 \oplus W_1 \oplus \ldots \oplus W_s$$

(so $a_i = c_{m_i}$). We will assume that the S-class of $g_{\boldsymbol{\varepsilon}} \in S$ is determined by $\boldsymbol{\varepsilon} = (\alpha_1, \ldots, \alpha_s)$. The above computation then shows that

$$\boldsymbol{\lambda}_n(g_{\boldsymbol{\varepsilon}}) = [\boldsymbol{\varepsilon}] \cdot q^{c_1/2 + \sum_{i>1} c_i}$$

with $[\boldsymbol{\varepsilon}] = \prod_{j=1}^{s} \alpha_j$, and, according to Theorem 2.4,

$$|C_S(g_{\boldsymbol{\varepsilon}})| = q^D \cdot \prod_{m_i=1 \text{ or } 2|m_i} |Sp_{2a_i}(q)| \cdot \prod_{v=1}^{s} |O^{\alpha_v}_{2a_{i_v}}(q)|,$$

where $I = \{i_1, \dots, i_s\}$ is the set of indices i such that $m_i > 1$ is odd, as before.

Observe that

$$\sum_{\alpha=\pm} \frac{\alpha 1}{|O^{\alpha}_{2a}(q)|} = \frac{q^a}{|Sp_{2a}(q)|}.$$

Hence, the 2^s contributions of all $g_{\boldsymbol{\varepsilon}}$ in (11) sum up to

$$\begin{aligned} \mathbf{\Lambda}_n(g) &= \frac{|C_G(g)| \cdot q^{-D+c_1/2+\sum_{i>1} c_i}}{\prod_{m_i=1 \text{ or } 2|m_i} |Sp_{2a_i}(q)|} \cdot \prod_{v=1}^{s} \frac{q^{a_{i_v}}}{|Sp_{2a_{i_v}}(q)|} \\ &= \frac{|C_G(g)| \cdot q^{-D+\sum_{i>1} c_i+\sum_{i \text{ odd}} c_i/2}}{\prod_i |Sp_{c_i}(q)|}, \end{aligned}$$

where we use the convention that $|Sp_0(q)| = 1$. By [44],

$$D = \dim R_u(C_{\mathcal{G}}(g)) = \sum_{i<j} ic_ic_j + \sum_i (i-1)c_i^2/2 + \sum_{2|i} c_i/2 + \sum_{i>1 \text{ odd}} c_i.$$

Putting everything together, we obtain

Theorem 2.6. *Let $g \in Sp_{2n}(q)$ be a unipotent element with Jordan canonical form $\sum_{i=1}^{\infty} c_i J_i$. Then*

$$\mathbf{\Lambda}_n(g) = q^{\frac{1}{2}\sum_i c_i - \sum_{i<j} ic_ic_j - \frac{1}{2}\sum_i (i-1)c_i^2} \cdot \frac{|C_{GL_{2n}(q)}(g)|}{\prod_i |Sp_{c_i}(q)|}$$

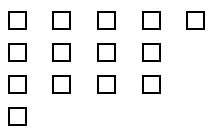
if all c_i are even, and $\mathbf{\Lambda}_n(g) = 0$ otherwise. □

Noting from Theorem 2.6 that $\mathbf{\Lambda}_n(g) \geq 0$, the following corollary is immediate.

Corollary 2.7. *A random unipotent element of $Sp_{2n}(q)$ with given Jordan canonical form fixes a positive type quadratic form with probability at least as large as that of fixing a negative type quadratic form.*

2.6. **Main result.** To state the main result of this section requires notation about partitions, much of it standard [31]. Let λ be a partition of some nonnegative integer $|\lambda|$ into parts $\lambda_1 \geq \lambda_2 \geq \cdots$. The symbol $m_i(\lambda)$ will denote the number of parts of λ of size i, and λ' is the partition dual to λ in the sense that $\lambda'_i = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$. Let $n(\lambda) = \sum_i \binom{\lambda'_i}{2}$. Let $l(\lambda)$ denote the number of parts of λ and $o(\lambda)$ the number of odd parts of λ.

It is often helpful to view partitions diagrammatically. The diagram associated to λ is the set of ordered pairs (i, j) of integers such that $1 \leq j \leq \lambda_i$. We use the convention that the row index i increases as one goes downward and the column index j increases as one goes from left to right. So the diagram of the partition $(5, 4, 4, 1)$ is



and one has that $n(\lambda) = 15, l(\lambda) = 4$, and $o(\lambda) = 2$.

Theorem 2.8. *Let $p^{\pm}(\lambda)$ denote the proportion of elements of $O^{\pm}_{2n}(q)$ which are unipotent and have the $GL_{2n}(q)$ rational canonical form of type λ.*

(1) *$p^+(\lambda)+p^-(\lambda)$ is equal to 0 unless $|\lambda| = 2n$ and all odd parts of λ have even multiplicity. If $|\lambda| = 2n$ and all odd parts of λ have even multiplicity, then*

$$\begin{aligned} & p^+(\lambda) + p^-(\lambda) \\ = \ & \frac{q^{l(\lambda)}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}} \prod_i (1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2\lfloor m_i(\lambda)/2 \rfloor})}. \end{aligned}$$

(2) *$p^+(\lambda) - p^-(\lambda)$ is equal to 0 unless $|\lambda| = 2n$ and all parts of λ have even multiplicity. If $|\lambda| = 2n$ and all parts of λ have even multiplicity, then*

$$p^+(\lambda) - p^-(\lambda) = \frac{1}{q^{\sum (\lambda_i')^2/2} \prod_{i\geq 1}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{m_i(\lambda)})}.$$

Proof. Let g be a unipotent element of $GL_{2n}(q)$ of type λ, and let $d(g)$ be the dimension of the kernel of $g-1$. From the above discussion and denoting the principal character by [1], it follows that

$$\begin{aligned} & \mathrm{Ind}_{O^+_{2n}(q)}^{Sp_{2n}(q)}[1](g) + \mathrm{Ind}_{O^-_{2n}(q)}^{Sp_{2n}(q)}[1](g) \\ = \ & 1 + \boldsymbol{\rho}_n^1(g) + \boldsymbol{\rho}_n^2(g) + 1 + 2\left[\sum_{i=1}^{(q-2)/2} \boldsymbol{\tau}_n^i\right](g) \\ = \ & \frac{q^{d(g)}-1}{q-1} + 1 + 2\left[\sum_{i=1}^{(q-2)/2} \boldsymbol{\tau}_n^i\right](g) \\ = \ & \frac{q^{d(g)}-1}{q-1} + 1 + (q-2)\frac{q^{d(g)}-1}{q-1} \\ = \ & q^{d(g)}. \end{aligned}$$

The first equality used formula (1) in Subsection 2.1, the second equality used the fact that $[1] + \boldsymbol{\rho}_n^1 + \boldsymbol{\rho}_n^2$ is the permutation character of $Sp_{2n}(q)$ on lines, and the third equality used formula (2) in Subsection 2.1.

Let C denote the $GL_{2n}(q)$ class of g. Using the fact that $q^{d(\cdot)}$ is constant on conjugacy classes of $GL_{2n}(q)$, it follows by the general formula for induced characters (page 34 of [17]) that

$$\mathrm{Ind}_{Sp_{2n}(q)}^{GL_{2n}(q)}[q^{d(\cdot)}](g) = q^{d(g)} |C_{GL_{2n}(q)}(g)| \frac{|C \cap Sp_{2n}(q)|}{|Sp_{2n}(q)|},$$

where $C_{GL_{2n}(q)}(g)$ denotes the centralizer of g in $GL_{2n}(q)$. A formula for $\frac{|C\cap Sp_{2n}(q)|}{|Sp_{2n}(q)|}$ in even characteristic appears in Theorem 5.2 of [12]; using this and transitivity of

induction, one concludes that

$$\begin{aligned}
&\mathrm{Ind}_{O_{2n}^+(q)}^{GL_{2n}(q)}[1](g) + \mathrm{Ind}_{O_{2n}^-(q)}^{GL_{2n}(q)}[1](g)\\
=\ &\mathrm{Ind}_{Sp_{2n}(q)}^{GL_{2n}(q)}[q^{d(\cdot)}](g)\\
=\ &q^{d(g)}|C_{GL_{2n}(q)}(g)|\frac{|C\cap Sp_{2n}(q)|}{|Sp_{2n}(q)|}\\
=\ &\frac{|C_{GL_{2n}(q)}(g)|\cdot q^{l(\lambda)}}{q^{n(\lambda)+n+o(\lambda)/2}\prod_i(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2\lfloor m_i(\lambda)/2\rfloor})}.
\end{aligned}$$

Again using the general formula for induced characters, one has that

$$p^+(\lambda)+p^-(\lambda)=\frac{1}{|C_{GL_{2n}(q)}(g)|}\left[\mathrm{Ind}_{O_{2n}^+(q)}^{GL_{2n}(q)}[1](g)+\mathrm{Ind}_{O_{2n}^-(q)}^{GL_{2n}(q)}[1](g)\right],$$

and part (1) follows.

By the general formula for induced characters and Theorem 2.6, one concludes that

$$\begin{aligned}
&p^+(\lambda)-p^-(\lambda)\\
=\ &\frac{1}{|C_{GL_{2n}(q)}(g)|}\left[\mathrm{Ind}_{O_{2n}^+(q)}^{GL_{2n}(q)}[1](g)-\mathrm{Ind}_{O_{2n}^-(q)}^{GL_{2n}(q)}[1](g)\right]\\
=\ &\frac{\mathbf{\Lambda}_n(g)}{|C_{GL_{2n}(q)}(g)|}\\
=\ &\frac{q^{\frac{1}{2}\sum_{i\geq 1}m_i(\lambda)-\sum_{i<j}im_i(\lambda)m_j(\lambda)-\frac{1}{2}\sum_i(i-1)m_i(\lambda)^2}}{\prod_i|Sp_{m_i(\lambda)}(q)|}\\
=\ &\frac{1}{q^{\frac{1}{2}\sum_i im_i(\lambda)^2+\sum_{i<j}im_i(\lambda)m_j(\lambda)}\prod_{i\geq 1}(1-1/q^2)\cdots(1-1/q^{m_i(\lambda)})}.
\end{aligned}$$

Since $\lambda_j'=m_j(\lambda)+m_{j+1}(\lambda)+\cdots$, one checks that

$$\sum_j(\lambda_j')^2=\sum_j[jm_j(\lambda)+2\sum_{i<j}im_i(\lambda)]m_j(\lambda),$$

which completes the proof. □

Remark. Comparing the expression in part (2) with the formula for centralizer sizes in $GL_n(q^2)$ (page 181 of [31]), one concludes that when all $m_i(\lambda)$ are even, $p^+(\lambda)-p^-(\lambda)$ is equal to the proportion of elements in $GL_n(q^2)$ which are unipotent and have part i occurring with multiplicity $m_i(\lambda)/2$.

3. Orthogonal groups in odd dimensions

Let q be a power of 2 as above. It is well known that $O_{2n+1}(q)\simeq Sp_{2n}(q)$, and this isomorphism can be realized as follows. Let $U=\mathbb{F}_q^{2n+1}$ be endowed with a nondegenerate quadratic form Q. Since $\dim U$ is odd, the associated symplectic form $(\cdot,\cdot)$ has a 1-dimensional radical $J=\langle v\rangle_{\mathbb{F}_q}$, with $Q(v)\neq 0$ and $g(v)=v$ for all $g\in O(Q)$. Then $O(Q)$ preserves the nondegenerate symplectic form on $W:=U/J=\mathbb{F}_q^{2n}$ induced by $(\cdot,\cdot)$, and this action induces the isomorphism $O_{2n+1}(q)=O(Q)\simeq Sp(W)=Sp_{2n}(q)$. Even though the $O(Q)$-module U is indecomposable, we will show that it is easy to relate the Jordan canonical form of any element

$g \in O(Q)$ in $GL(U)$ and $GL(W)$. Let $J_k(\alpha)$ denote the $k \times k$ Jordan block with eigenvalue $\alpha \in \overline{\mathbb{F}}_q$.

Lemma 3.1. *Keep the above notation and let $g \in O(Q)$. Then the Jordan canonical form for g in $GL(U \otimes \overline{\mathbb{F}}_q)$ is just the direct sum of the Jordan canonical form for g in $GL(W \otimes \overline{\mathbb{F}}_q)$ and the Jordan block $J_1(1)$.*

Proof. To simplify the notation, we will extend the scalars to $\overline{\mathbb{F}}_q$ and denote the corresponding spaces also by U, J, and W. Let $\sum_{i,\alpha} a_i(\alpha)J_i(\alpha)$, respectively $\sum_{i,\alpha} b_i(\alpha)J_i(\alpha)$, be the Jordan canonical form for g in $GL(U)$, respectively in $GL(W)$. We need to show that $a_i(\alpha) - b_i(\alpha)$ equals 1 if $(i, \alpha) = (1, 1)$ and 0 otherwise. For any $j \geq 0$ and $\alpha \in \overline{\mathbb{F}}_q$, let

$$U_j(\alpha) = \{x \in U \mid (g - \alpha \cdot 1_U)^j(x) = 0\}$$

and similarly for $W_j(\alpha)$; also set $U_0(\alpha) = 0$ and $W_0(\alpha) = 0$. Then it is easy to check for $j \geq 1$ that $\dim U_j(\alpha) = \sum_i \min\{i, j\} \cdot a_i(\alpha)$. It follows that $\dim U_{j+1}(\alpha)/U_j(\alpha) = \sum_{i \geq j+1} a_i(\alpha)$, and so

$$a_j(\alpha) = -(\dim U_{j+1}(\alpha)) + 2(\dim U_j(\alpha)) - (\dim U_{j-1}(\alpha)),$$

and similarly

$$b_j(\alpha) = -(\dim W_{j+1}(\alpha)) + 2(\dim W_j(\alpha)) - (\dim W_{j-1}(\alpha)).$$

Since g acts trivially on J, it is straightforward to check that $\dim U_j(\alpha) = \dim W_j(\alpha)$ for $\alpha \neq 1$, whence $a_j(\alpha) = b_j(\alpha)$ for any such α. Let $j \geq 1$ and $u + J \in W_j(1)$. Denoting $w := (g-1)^{j-1}(u)$, we have $w + J \in W_1(1)$, i.e. $g(w) = w + av$ for some $a \in \overline{\mathbb{F}}_q$. But then $Q(w) = Q(w + av) = Q(w) + a^2Q(v)$ (since $(v, U) = 0$), and so $a = 0$ as $Q(v) \neq 0$. Thus $(g-1)^j(u) = (g-1)w = 0$, i.e. $u \in U_j(1)$. We conclude that $W_j(1) = U_j(1)/J$, and so $\dim U_j(1) = 1 + \dim W_j(1)$ for $j \geq 1$. Recall that $U_0(1) = W_0(1) = 0$. Hence $a_i(1) - b_i(1)$ equals 1 if $i = 1$ and 0 otherwise. □

Cycle indices for even characteristic symplectic groups were derived in [12], and Lemma 3.1 reduces the cycle index of $O^{\pm}(2n+1, q)$ to that of $Sp(2n, q)$. Thus we can focus attention on $O^{\pm}(2n, q)$, which we do in the next section.

4. Cycle index

Recall that we are interested in the $GL_{2n}(q)$ rational canonical form of random elements of $O^{\pm}_{2n}(q)$. The rational canonical forms of $GL_{2n}(q)$ are parameterized by associating a partition λ_ϕ to each monic, nonconstant irreducible polynomial ϕ over the finite field $\mathbb{F}_q$, such that

(1) $|\lambda_z| = 0$,
(2) $\sum_\phi |\lambda_\phi| \cdot \deg(\phi) = 2n$.

Here $\deg(\phi)$ denotes the degree of ϕ, and $|\lambda_\phi|$ is the size of λ_ϕ. For elements in $O^{\pm}_{2n}(q)$, it follows from Wall [44] that there are additional restrictions:

(1) $\lambda_\phi = \lambda_{\phi^*}$, where $\phi^*(z) = \phi(0)^{-1} z^n \phi(z^{-1})$.
(2) The odd parts of λ_{z-1} occur with even multiplicity.

For the remainder of this section, we use the notation:

$$A(\phi, \lambda_\phi, i) = \begin{cases} |U_{m_i(\lambda_\phi)}(q^{\deg(\phi)/2})| & \text{if } \phi = \phi^*, \\ |GL_{m_i(\lambda_\phi)}(q^{\deg(\phi)})|^{1/2} & \text{if } \phi \neq \phi^*. \end{cases}$$

We remind the reader that $|GL_n(q)| = q^{n^2}(1-1/q)\cdots(1-1/q^n)$ and that the size of $U_n(q)$ is $(-1)^n|GL_n(-q)|$. For $\phi \neq z-1$, we define $B(\phi,\lambda_\phi)$ as

$$q^{\deg(\phi)[\sum_{h<i} hm_h(\lambda_\phi)m_i(\lambda_\phi)+\frac{1}{2}\sum_i (i-1)m_i(\lambda_\phi)^2]}\prod_i A(\phi,\lambda_\phi,i).$$

Next we give an explicit formula for the cycle index of the orthogonal groups in even characteristic. We let $x_{\phi,\lambda}$ be variables, and $\lfloor y \rfloor$ denote the largest integer not exceeding y.

Theorem 4.1. *The following statements hold.*

(1)

$$\begin{aligned}
&1+\sum_{n\geq 1}\frac{u^{2n}}{|O^+_{2n}(q)|}\sum_{g\in O^+_{2n}(q)}\prod_\phi x_{\phi,\lambda_\phi(g)}+\sum_{n\geq 1}\frac{u^{2n}}{|O^-_{2n}(q)|}\sum_{g\in O^-_{2n}(q)}\prod_\phi x_{\phi,\lambda_\phi(g)}\\
=&\left(\sum_{\substack{|\lambda| \text{ even}\\ i \text{ odd}\Rightarrow m_i \text{ even}}}\frac{x_{z-1,\lambda}u^{|\lambda|}q^{l(\lambda)}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}}\prod_i(1-1/q^2)\cdots(1-1/q^{2\lfloor\frac{m_i(\lambda)}{2}\rfloor})}\right)\\
&\cdot\prod_{\substack{\phi=\phi^*\\ \phi\neq z-1}}\left(\sum_\lambda\frac{x_{\phi,\lambda}u^{|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)}\right)\prod_{\substack{\{\phi,\phi^*\}\\ \phi\neq\phi^*}}\left(\sum_\lambda\frac{x_{\phi,\lambda}x_{\phi^*,\lambda}u^{2|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)B(\phi^*,\lambda)}\right)
\end{aligned}$$

(2)

$$\begin{aligned}
&1+\sum_{n\geq 1}\frac{u^{2n}}{|O^+_{2n}(q)|}\sum_{g\in O^+_{2n}(q)}\prod_\phi x_{\phi,\lambda_\phi(g)}-\sum_{n\geq 1}\frac{u^{2n}}{|O^-_{2n}(q)|}\sum_{g\in O^-_{2n}(q)}\prod_\phi x_{\phi,\lambda_\phi(g)}\\
=&\left(\sum_{\substack{\lambda\\ \text{all } m_i(\lambda) \text{ even}}}\frac{x_{z-1,\lambda}u^{|\lambda|}}{q^{\sum(\lambda_i')^2/2}\prod_{i\geq 1}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{m_i(\lambda)})}\right)\\
&\cdot\prod_{\substack{\phi=\phi^*\\ \phi\neq z-1}}\left(\sum_\lambda\frac{x_{\phi,\lambda}(-1)^{|\lambda|}u^{|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)}\right)\prod_{\substack{\{\phi,\phi^*\}\\ \phi\neq\phi^*}}\left(\sum_\lambda\frac{x_{\phi,\lambda}x_{\phi^*,\lambda}u^{2|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)B(\phi^*,\lambda)}\right)
\end{aligned}$$

Proof. Consider the first part. The coefficient of $u^{2n}\prod_\phi x_{\phi,\lambda_\phi}$ on the left-hand side is the sum of the proportions of elements in $O^\pm_{2n}(q)$ with rational canonical form data $\{\lambda_\phi\}$ in $GL_{2n}(q)$. By Theorem 3.7.4 of [44] and part (1) of Theorem 2.8, this is equal to the coefficient of $u^{2n}\prod_\phi x_{\phi,\lambda_\phi}$ on the right-hand side, yielding the first assertion. The second assertion is proved similarly, using part (2) of Theorem 2.8. □

Remark. $\Omega^\pm_{2n}(q)$ is defined as the index 2 subgroup of $O^\pm_{2n}(q)$ with the property that $l(\lambda_{z-1}(g))$ is even. Thus our techniques can be easily modified to study these groups as well. Namely in the left-hand side of Theorem 4.1, one replaces the sum over $g\in O^\pm_{2n}(g)$ by the sum over $g\in\Omega^\pm_{2n}(q)$ (but leaving the $|O^\pm_{2n}(q)|$ unchanged), and in the right-hand terms adds the additional restriction that the number of parts of λ_{z-1} is even.

5. Enumerative applications

In this section we present a small sample of enumerative applications of the cycle indices from Section 4. We first collect four known lemmas which will be used in the proofs; this might assist the reader in future applications of the cycle index.

Lemma 5.1 goes back to Euler; a proof can be found on page 19 of [1].

Lemma 5.1. *For $|u|<1, |q|>1$,*

$$1+\sum_{n\geq 1}\frac{u^n}{q^{\binom{n}{2}}(1-1/q)(1-1/q^2)\cdots(1-1/q^n)}=\prod_{i\geq 0}(1+u/q^i).$$

Lemma 5.2 is a useful expansion, proved as Theorem 349 of the text [21].

Lemma 5.2. *For $|u|, |x|<1$,*

$$\frac{1}{(1-ux)(1-ux^2)\cdots(1-ux^j)}=1+ux\frac{1-x^j}{1-x}+u^2x^2\frac{(1-x^j)(1-x^{j+1})}{(1-x)(1-x^2)}+\cdots.$$

Lemma 5.3 is proved as Lemma 1.3.17 (parts a and d) of [16].

Lemma 5.3. *Let $N^*(q;d)$ denote the number of monic irreducible self-conjugate polynomials ϕ of degree d over $\mathbb{F}_q$ and let $M^*(q;d)$ denote the number of (unordered) monic irreducible conjugate pairs $\{\phi,\phi^*\}$ of non-self-conjugate polynomials of degree d over $\mathbb{F}_q$. Then in even characteristic, and for $|u|<q^{-1}$,*

(1)
$$\prod_{d\geq 1}(1-u^d)^{-N^*(q;2d)}\prod_{d\geq 1}(1-u^d)^{-M^*(q;d)}=\frac{1-u}{1-qu};$$

(2)
$$\prod_{d\geq 1}(1+u^d)^{-N^*(q;2d)}\prod_{d\geq 1}(1-u^d)^{-M^*(q;d)}=1-u.$$

Lemma 5.4 has several proofs; the most group-theoretic proof is due to Stong [42] and uses Steinberg's result that $GL(n,q)$ has $q^{n(n-1)}$ unipotent elements.

Lemma 5.4. (1) *If $\phi=\phi^*$ and $\phi\neq z-1$, then*

$$\sum_{\lambda}\frac{u^{|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)}=\prod_{i\geq 1}\left(1+(-1)^i(u^2/q^i)^{\deg(\phi)/2}\right)^{-1}.$$

(2) *If $\phi\neq\phi^*$, then*

$$\sum_{\lambda}\frac{u^{2|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)B(\phi^*,\lambda)}=\prod_{i\geq 1}\left(1-(u^2/q^i)^{\deg(\phi)}\right)^{-1}.$$

Next we proceed to the applications.

5.1. Example 1: Enumeration of elements by dimension of fixed space.

Let $p^{\pm}_{2n}(k)$ denote the probability that an element of $O^{\pm}_{2n}(q)$ has a fixed space of dimension k. These probabilities were computed in a long paper of Rudvalis and Shinoda [36] using Möbius inversion. Theorem 5.5 shows how to compute these probabilities using cycle indices.

Theorem 5.5 ([36]). *The following statements hold.*

(1)

$$\begin{aligned} p_{2n}^{\pm}(2k) &= \frac{q^k}{2|GL_k(q^2)|}\sum_{j=0}^{n-k}\frac{(-1)^j}{q^{(2k-1)j}(q^{2j}-1)\cdots(q^4-1)(q^2-1)} \\ &\quad \pm \frac{1}{2}\frac{(-1)^{n-k}}{q^{2k(n-k)}|GL_k(q^2)|(q^{2(n-k)}-1)\cdots(q^4-1)(q^2-1)}. \end{aligned}$$

(2) $p_{2n}^{\pm}(2k+1) = \frac{1}{2q^k|GL_k(q^2)|}\sum_{j=0}^{n-k-1}\frac{(-1)^j}{q^{j^2+2(k+1)j}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2j})}$.

Proof. By part (1) of Theorem 4.1, $p_{2n}^{+}(2k)+p_{2n}^{-}(2k)$ is the coefficient of u^{2n} in

$$\begin{aligned} &\sum_{\substack{l(\lambda)=2k \\ i \text{ odd}\Rightarrow m_i \text{ even}}} \frac{u^{|\lambda|}q^{2k}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}}\prod_i(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2\lfloor\frac{m_i(\lambda)}{2}\rfloor})} \\ &\cdot \prod_{\substack{\phi=\phi^* \\ \phi\neq z-1}}\left(\sum_\lambda \frac{u^{|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)}\right)\prod_{\substack{\{\phi,\phi^*\} \\ \phi\neq\phi^*}}\left(\sum_\lambda \frac{u^{2|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)B(\phi^*,\lambda)}\right) \\ = \;& \frac{u^{2k}q^k}{q^{2k^2}(1-u^2/q)(1-1/q^2)\cdots(1-u^2/q^{2k-1})(1-1/q^{2k})} \\ &\cdot \prod_{\substack{\phi=\phi^* \\ \phi\neq z-1}}\left(\sum_\lambda \frac{u^{|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)}\right)\prod_{\substack{\{\phi,\phi^*\} \\ \phi\neq\phi^*}}\left(\sum_\lambda \frac{u^{2|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)B(\phi^*,\lambda)}\right) \\ = \;& \frac{u^{2k}q^k}{q^{2k^2}(1-u^2/q)(1-1/q^2)\cdots(1-u^2/q^{2k-1})(1-1/q^{2k})} \\ &\cdot \prod_{\substack{\phi=\phi^* \\ \phi\neq z-1}}\prod_{i\geq 1}\left(1+(-1)^i(u^2/q^i)^{\deg(\phi)/2}\right)^{-1}\prod_{\substack{\{\phi,\phi^*\} \\ \phi\neq\phi^*}}\prod_{i\geq 1}\left(1-(u^2/q^i)^{\deg(\phi)}\right)^{-1}. \end{aligned}$$

The first equality used Theorem 3 of [11], together with the fact from [12] that the λ_{z-1} part of an element of $Sp_{2n}(q)$ has the same behavior in odd and even characteristic. The second equality used Lemma 5.4. Using both parts of Lemma 5.3, this becomes

$$\begin{aligned} &\frac{u^{2k}q^k}{q^{2k^2}(1-u^2/q)(1-1/q^2)\cdots(1-u^2/q^{2k-1})(1-1/q^{2k})} \\ &\cdot\left[\frac{\prod_{i\geq 1}(1-u^2/q^{2i-1})}{1-u^2}\right] \\ = \;& \frac{u^{2k}q^k\prod_{i\geq k+1}(1-u^2/q^{2i-1})}{(1-u^2)|GL_k(q^2)|}. \end{aligned}$$

It now follows from Lemma 5.1 that

$$p_{2n}^{+}(2k)+p_{2n}^{-}(2k) = \frac{q^k}{|GL_k(q^2)|}\sum_{j=0}^{n-k}\frac{(-1)^j}{q^{(2k-1)j}(q^{2j}-1)\cdots(q^2-1)}. \tag{12}$$

Part (2) of Theorem 4.1 gives that $p^+_{2n}(2k) - p^-_{2n}(2k)$ is the coefficient of u^{2n} in

$$\prod_{i\geq 1}(1-u^2/q^{2i}) \cdot \sum_{\substack{l(\lambda)=2k \\ \text{all } m_i(\lambda) \text{ even}}} \frac{u^{|\lambda|}}{q^{\sum(\lambda_i')^2/2}\prod_{i\geq 1}(1-1/q^2)\cdots(1-1/q^{m_i(\mu)})}.$$

Here the term $\prod_{i\geq 1}(1-u^2/q^{2i})$ comes from the polynomials other than $z-1$ by an argument similar to that in the previous paragraph. By the remark after Theorem 2.8 and Theorem 5 of [10], this is the coefficient of u^n in

$$\frac{u^k}{|GL_k(q^2)|}\frac{\prod_{i\geq 1}(1-u/q^{2i})}{\prod_{i=1}^k(1-u/q^{2i})} = \frac{u^k}{|GL_k(q^2)|}\prod_{i\geq k+1}(1-u/q^{2i}).$$

It now follows from Lemma 5.1 that

$$p^+_{2n}(2k) - p^-_{2n}(2k) = \frac{(-1)^{n-k}}{q^{2k(n-k)}|GL_k(q^2)|(q^{2(n-k)}-1)\cdots(q^4-1)(q^2-1)}. \tag{13}$$

Combining equations (12) and (13) proves part (1) of the theorem.

For part (2) of the theorem, arguing as in part (1) of the theorem gives that $p^+_{2n}(2k+1) + p^-_{2n}(2k+1)$ is the coefficient of u^{2n} in

$$\begin{aligned} &\frac{u^{2k+2}}{q^{2k^2+k}(1-u^2/q)(1-1/q^2)\cdots(1-1/q^{2k})(1-u^2/q^{2k+1})} \\ &\cdot\frac{\prod_{i\geq 1}(1-u^2/q^{2i-1})}{1-u^2} \\ = \quad &\frac{u^{2k+2}}{q^{2k^2+k}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2k})}\frac{\prod_{i\geq k+1}(1-u^2/q^{2i+1})}{1-u^2}. \end{aligned}$$

Again using Lemma 5.1, this is equal to

$$\frac{1}{q^k|GL_k(q^2)|}\sum_{j=0}^{n-k-1}\frac{(-1)^j}{q^{j^2+2(k+1)j}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2j})}.$$

Part (2) of Theorem 4.1 implies that $p^+_{2n}(2k+1) - p^-_{2n}(2k+1) = 0$ (if all parts of λ_{z-1} occur with even multiplicity, the total number of parts can't be odd), and the result follows. □

Since $\Omega^\pm(2n,q)$ is the index 2 subgroup of $O^\pm(2n,q)$ consisting of elements with an even dimensional fixed space, the following corollary of Theorem 5.5 is immediate.

Corollary 5.6. *Let $q^\pm_{2n}(k)$ be the probability that an element of $\Omega^\pm(2n,q)$ has a k-dimensional fixed space. Then $q^\pm_{2n}(2k+1) = 0$ and*

$$\begin{aligned} q^\pm_{2n}(2k) \quad = \quad &\frac{q^k}{|GL_k(q^2)|}\sum_{j=0}^{n-k}\frac{(-1)^j}{q^{(2k-1)j}(q^{2j}-1)\cdots(q^4-1)(q^2-1)} \\ &\pm \frac{(-1)^{n-k}}{q^{2k(n-k)}|GL_k(q^2)|(q^{2(n-k)}-1)\cdots(q^4-1)(q^2-1)}. \end{aligned}$$

5.2. **Example 2: Enumeration of unipotent elements by dimension of fixed space.** The paper [14] used generating functions to enumerate unipotent elements in orthogonal groups of even characteristic, showing that the number of unipotent elements of $O^{\pm}_{2n}(q)$ is $q^{2n^2-2n+1}\left(1+\frac{1}{q}\mp\frac{1}{q^n}\right)$. In this example, we give a more refined count. Similar results for the finite general linear and unitary groups appear in [27], [10].

Theorem 5.7. (1) *The proportion of elements of $O^{\pm}_{2n}(q)$ which are unipotent and have a fixed space of dimension $2k$ is*

$$\frac{(1-1/q^{2k})(1-1/q^{2(k+1)})\cdots(1-1/q^{2(n-1)})}{q^{n-2k}|GL_k(q^2)|(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2(n-k)})}\left[\frac{1}{2}\pm\frac{1}{2q^n}\right].$$

(2) *The proportion of elements of $O^{\pm}_{2n}(q)$ which are unipotent and have a fixed space of dimension $2k+1$ is*

$$\frac{1}{2\cdot q^{n-1}|GL_k(q^2)|}\frac{(1-1/q^{2(k+1)})(1-1/q^{2(k+2)})\cdots(1-1/q^{2(n-1)})}{(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2(n-k-1)})}.$$

Proof. Let $u^{\pm}_{2n}(2k,q)$ denote the proportion of elements of $O^{\pm}_{2n}(q)$ which are unipotent and have a fixed space of dimension $2k$. For part (1) of the theorem, arguing as in the proof of Theorem 5.5 (and noting that all partitions coming from polynomials other than $z-1$ are empty) gives that $u^{+}_{2n}(2k)+u^{-}_{2n}(2k)$ is the coefficient of u^{2n} in

$$\frac{u^{2k}q^k}{q^{2k^2}(1-u^2/q)(1-1/q^2)\cdots(1-u^2/q^{2k-1})(1-1/q^{2k})}.$$

This is equal to $\frac{q^n}{|GL_k(q^2)|}$ multiplied by the coefficient of u^{n-k} in

$$\frac{1}{(1-u/q^2)(1-u/q^4)\cdots(1-u/q^{2k})}.$$

Applying Lemma 5.2, one concludes that

$$\begin{aligned} & u^{+}_{2n}(2k)+u^{-}_{2n}(2k) \\ = \ & \frac{1}{q^{n-2k}|GL_k(q^2)|}\frac{(1-1/q^{2k})(1-1/q^{2(k+1)})\cdots(1-1/q^{2(n-1)})}{(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2(n-k)})}. \end{aligned}$$

By part (2) of Theorem 2.8 and the remark following it, $u^{+}_{2n}(2k)-u^{-}_{2n}(2k)$ is the proportion of elements of $GL_n(q^2)$ which are unipotent and have a fixed space of dimension k. This is known ([27], [10]) to be

$$\frac{1}{q^{2(n-k)}|GL_k(q^2)|}\frac{(1-1/q^{2k})(1-1/q^{2(k+1)})\cdots(1-1/q^{2(n-1)})}{(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2(n-k)})},$$

and part (1) of the theorem follows.

For part (2) of the theorem, arguing as in the proof of part (2) of Theorem 5.5 (again noting that all partitions coming from polynomials other than $z-1$ are empty), one obtains that $u^{+}_{2n}(2k+1)+u^{-}_{2n}(2k+1)$ is the coefficient of u^{2n} in

$$\frac{u^{2k+2}}{q^{2k^2+k}(1-u^2/q)(1-1/q^2)\cdots(1-1/q^{2k})(1-u^2/q^{2k+1})}.$$

This is equal to $\frac{1}{q^k|GL_k(q^2)|}$ multiplied by the coefficient of u^{n-k-1} in

$$\frac{1}{(1-u/q)(1-u/q^3)\cdots(1-u/q^{2k+1})}.$$

Applying Lemma 5.2, one concludes that

$$\begin{aligned} & u^+_{2n}(2k+1)+u^-_{2n}(2k+1) \\ = \ & \frac{1}{q^{n-1}|GL_k(q^2)|}\frac{(1-1/q^{2(k+1)})(1-1/q^{2(k+2)})\cdots(1-1/q^{2(n-1)})}{(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2(n-k-1)})}. \end{aligned}$$

By part (2) of Theorem 2.8, $u^+_{2n}(2k+1)=u^-_{2n}(2k+1)$, and the result follows. □

5.3. **Example 3: Cyclic matrices.** A matrix over $\mathbb{F}_q$ is called cyclic if its characteristic polynomial is equal to its minimal polynomial. Motivated by applications to computational group theory [32], the proportion of cyclic matrices in $O^\pm_{2n}(q)$ (even characteristic included) has been studied in [33] via geometric techniques and in [16] via generating functions. Let us illustrate how Theorem 4.1 reproduces the generating functions of [16].

Let $c^\pm_O(2n,q)$ denote the proportion of cyclic matrices in the even characteristic orthogonal groups $O^\pm_{2n}(q)$. Define generating functions

$$C_{O^+}(u)=1+\sum_{n\geq 1}c_{O^+}(2n,q)u^n; \quad C_{O^-}(u)=\sum_{n\geq 1}c_{O^-}(2n,q)u^n.$$

An element of $O^\pm_{2n}(q)$ is cyclic if and only if all the λ_ϕ appearing in its rational canonical form have at most one part. Thus part (1) of Theorem 4.1 implies that

$$\begin{aligned} & C_{O^+}(u)+C_{O^-}(u) \\ = \ & \left(1+\frac{u}{1-u/q}\right)\prod_{d\geq 1}\left(1+\frac{u^d}{(q^d+1)(1-u^d/q^d)}\right)^{N^*(q;2d)} \\ & \cdot\prod_{d\geq 1}\left(1+\frac{u^d}{(q^d-1)(1-u^d/q^d)}\right)^{M^*(q;d)}. \end{aligned}$$

Here, as in the statement of Lemma 5.3, $N^*(q;d)$ denotes the number of monic irreducible self-conjugate polynomials ϕ of degree d over $\mathbb{F}_q$ and $M^*(q;d)$ denotes the number of (unordered) monic irreducible conjugate pairs $\{\phi,\phi^*\}$ of non-self-conjugate polynomials of degree d over $\mathbb{F}_q$. Part (2) of Theorem 4.1 implies that

$$\begin{aligned} C_{O^+}(u)-C_{O^-}(u) \ = \ & \prod_{d\geq 1}\left(1-\frac{u^d}{(q^d+1)(1+u^d/q^d)}\right)^{N^*(q;2d)} \\ & \cdot\prod_{d\geq 1}\left(1+\frac{u^d}{(q^d-1)(1-u^d/q^d)}\right)^{M^*(q;d)}. \end{aligned}$$

Similarly, Theorem 4.1 reproduces the generating functions of [16] for the proportions of separable (square-free characteristic polynomial) and semisimple (square-free minimal polynomial) matrices in $O^\pm_{2n}(q)$. The proportions of regular semisimple

elements in $O^{\pm}_{2n}(q)$ and $\Omega^{\pm}_{2n}(q)$ were studied by generating functions in [15], and Theorem 4.1 captures those results too.

6. Random partitions

In this section we use our results about the even characteristic orthogonal groups to define and study a probability measure $R_{(u,q)}$ on the set of all partitions λ of all natural numbers such that all odd parts of λ occur with even multiplicity. We also study related measures $R^e_{(u,q)}$, $R^o_{(u,q)}$ arising from the index-two simple subgroup $\Omega^{\pm}(2n,q)$ of $O^{\pm}(2n,q)$ and its nontrivial coset respectively.

These random partitions are very natural objects (analogous to those defined in [10], [11] for the other classical groups). One reason to be interested in these measures is that they can be used to give probabilistic proofs of Theorems 5.5 and 5.7 (arguing along the lines of [11]). We also mention that the corresponding measures for the general linear groups arise in the Cohen-Lenstra [7] heuristics for number fields (the thesis [24] discusses this), and we have high hopes that the measures $R_{(u,q)}$ will arise in a number-theoretic context too.

Definition 6.1. Fix $0 < u < q^{1/2}$ and q a prime power. The measure $R_{(u,q)}$ is defined on the set of all partitions λ (the size can vary) such that all odd parts occur with even multiplicity, by the formula:

$$R_{(u,q)}(\lambda) = \frac{\prod_{i\geq 1}(1-u^2/q^{2i-1})}{1+u^2} \cdot \frac{q^{l(\lambda)}u^{|\lambda|}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}}\prod_i(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2\lfloor m_i(\lambda)/2\rfloor})}.$$

Theorem 6.2 relates the measure $R_{(u,q)}$ to the asymptotics of finite orthogonal groups. The use of auxiliary randomization (i.e. randomizing the variable n) is a mainstay of statistical mechanics known as the grand canonical ensemble. We say that an infinite collection of random variables is independent if any finite subcollection is.

Theorem 6.2. (1) *Fix u with $0 < u < 1$. Then choose a random even natural number N such that the probability that $N = 0$ is $\frac{1-u^2}{1+u^2}$ and the probability that $N = 2n \geq 2$ is equal to $2u^{2n}\frac{1-u^2}{1+u^2}$. Choose one of $O^{\pm}(N,q)$ at random (each with probability $1/2$), and let g be a random element of the chosen group. Let $\Lambda_\phi(g)$ be the partition corresponding to the polynomial ϕ in the rational canonical form of g. Then as ϕ varies, aside from the fact that $\Lambda_\phi = \Lambda_{\phi^*}$, these random variables are independent with probability laws the same as for the symplectic groups in Theorem 1 of* [11]*, except for the polynomial $z-1$, which has the distribution $R_{(u,q)}$.*

(2) *Choose one of $O^{\pm}_{2n}(q)$ at random (each with probability $1/2$), and let g be a random element of the chosen group. Let $\Lambda_\phi(g)$ be the partition corresponding to the polynomial ϕ in the rational canonical form of g. Let q be fixed and $n \to \infty$. Then as ϕ varies, aside from the fact that $\Lambda_\phi = \Lambda_{\phi^*}$, these random variables are independent with probability laws the same as for the symplectic groups in Theorem 1 of* [11]*, except for the polynomial $z-1$, which has the distribution $R_{(1,q)}$.*

Proof. The method of proof is analogous to that used for the other classical groups (see the survey [8]), so we demonstrate the claim for Λ_{z-1}, as that is the interesting new feature. In part (1) of Theorem 4.1, set $x_{\phi,\lambda} = 1$ for $\phi \neq z-1$ and $x_{z-1,\lambda} = x_{z-1,\lambda} \cdot u^{|\lambda|}$. One obtains the equation

$$\begin{aligned}
& 1 + \sum_{n\geq 1} \frac{u^{2n}}{|O^+_{2n}(q)|} \sum_{g\in O^+_{2n}(q)} x_{z-1,\lambda_{z-1}(g)} u^{|\lambda_{z-1}(g)|} \\
& + \sum_{n\geq 1} \frac{u^{2n}}{|O^-_{2n}(q)|} \sum_{g\in O^-_{2n}(q)} x_{z-1,\lambda_{z-1}(g)} u^{|\lambda_{z-1}(g)|} \\
= & \left(\sum_{\substack{|\lambda| \text{ even} \\ i \text{ odd} \Rightarrow m_i \text{ even}}} \frac{x_{z-1,\lambda} u^{|\lambda|} q^{l(\lambda)}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}} \prod_i (1-1/q^2)\cdots(1-1/q^{2\lfloor \frac{m_i(\lambda)}{2} \rfloor})} \right) \\
& \cdot \prod_{\substack{\phi=\phi^* \\ \phi\neq z-1}} \left(\sum_\lambda \frac{u^{|\lambda|\cdot \deg(\phi)}}{B(\phi,\lambda)} \right) \prod_{\substack{\{\phi,\phi^*\} \\ \phi\neq\phi^*}} \left(\sum_\lambda \frac{u^{2|\lambda|\cdot\deg(\phi)}}{B(\phi,\lambda)B(\phi^*,\lambda)} \right) \\
= & \left[\frac{\prod_{i\geq 1}(1-u^2/q^{2i-1})}{1-u^2} \right] \\
& \cdot \left(\sum_{\substack{|\lambda| \text{ even} \\ i \text{ odd} \Rightarrow m_i \text{ even}}} \frac{x_{z-1,\lambda} u^{|\lambda|} q^{l(\lambda)}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}} \prod_i (1-1/q^2)\cdots(1-1/q^{2\lfloor \frac{m_i(\lambda)}{2} \rfloor})} \right).
\end{aligned}$$

The final equality follows as in the proof of part (1) of Theorem 5.5. Multiplying both sides by $(1-u^2)/(1+u^2)$ implies that

$$\begin{aligned}
& \frac{1-u^2}{1+u^2} + \sum_{n\geq 1} \frac{2(1-u^2)u^{2n}}{1+u^2} \left[\frac{\sum_{g\in O^+_{2n}(q)} x_{z-1,\lambda_{z-1}(g)} u^{|\lambda_{z-1}(g)|}}{2|O^+_{2n}(q)|} \right] \\
& + \sum_{n\geq 1} \frac{2(1-u^2)u^{2n}}{1+u^2} \left[\frac{\sum_{g\in O^-_{2n}(q)} x_{z-1,\lambda_{z-1}(g)} u^{|\lambda_{z-1}(g)|}}{2|O^-_{2n}(q)|} \right] \\
= & \frac{\prod_{i\geq 1}(1-u^2/q^{2i-1})}{1+u^2} \\
& \cdot \sum_{\substack{|\lambda| \text{ even} \\ i \text{ odd} \Rightarrow m_i \text{ even}}} \frac{q^{l(\lambda)} u^{|\lambda|} x_{z-1,\lambda}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}} \prod_i (1-1/q^2)\cdots(1-1/q^{2\lfloor m_i(\lambda)/2 \rfloor})} \\
= & \sum_\lambda R_{(u,q)}(\lambda) x_{z-1,\lambda},
\end{aligned}$$

which proves part (1).

To prove the second assertion, one uses the fact that if a Taylor series of a function $f(u^2)$ around 0 converges at $u = 1$, then the $n \to \infty$ limit of the coefficient of u^{2n} in $\frac{f(u^2)(1+u^2)}{2(1-u^2)}$ is equal to $f(1)$. □

Next, we give a Markov chain method for sampling from the distribution $R_{(u,q)}$. Define two Markov chains K_1, K_2 on the natural numbers with transition probabilities

$$K_1(a,b) = \begin{cases} \dfrac{u^a P'_{O,u}(b)}{P'_{Sp,u}(a) q^{\frac{a^2-b^2+2(a+1)b}{4}} (q^{a-b}-1)\cdots(q^4-1)(q^2-1)} & \text{if } a-b \text{ even, } b \le a \\ 0 & \text{else,} \end{cases}$$

$$K_2(a,b) = \begin{cases} \dfrac{u^a P'_{Sp,u}(b) q^{(a-b)^2/4}}{P'_{O,u}(a) q^{\frac{a^2+b}{2}-a} (q^{a-b}-1)\cdots(q^4-1)(q^2-1)} & \text{if } a-b \text{ even, } b \le a \\ \dfrac{u^a P'_{Sp,u}(b) q^{((a-b)^2-1)/4}}{P'_{O,u}(a) q^{\frac{a^2-a}{2}} (q^{a-b-1}-1)\cdots(q^4-1)(q^2-1)} & \text{if } a-b \text{ odd, } b \le a \\ 0 & \text{else,} \end{cases}$$

where $P'_{Sp,u}, P'_{O,u}$ are defined as follows:

$$\begin{aligned} P'_{Sp,u}(2k) &= \frac{u^{2k}}{q^{2k^2+k}(1-u^2/q)(1-1/q^2)\cdots(1-u^2/q^{2k-1})(1-1/q^{2k})}, \\ P'_{Sp,u}(2k+1) &= \frac{u^{2k+2}}{q^{2k^2+3k+1}(1-u^2/q)(1-1/q^2)\cdots(1-1/q^{2k})(1-u^2/q^{2k+1})}, \\ P'_{O,u}(2k) &= \frac{u^{2k}}{q^{2k^2-k}(1-u^2/q)(1-1/q^2)\cdots(1-u^2/q^{2k-1})(1-1/q^{2k})}, \\ P'_{O,u}(2k+1) &= \frac{u^{2k+1}}{q^{2k^2+k}(1-u^2/q)(1-1/q^2)\cdots(1-1/q^{2k})(1-u^2/q^{2k+1})}. \end{aligned}$$

Theorem 6.3. *Let λ'_1 be a random natural number which is equal to $2k$ with probability*

$$\frac{\prod_{i=1}^{\infty}(1-u^2/q^{2i-1})}{1+u^2} \frac{u^{2k}}{q^{2k^2-k}(1-u^2/q)(1-1/q^2)\cdots(1-u^2/q^{2k-1})(1-1/q^{2k})}$$

and equal to $2k+1$ with probability

$$\frac{\prod_{i=1}^{\infty}(1-u^2/q^{2i-1})}{1+u^2} \frac{u^{2k+2}}{q^{2k^2+k}(1-u^2/q)(1-1/q^2)\cdots(1-1/q^{2k})(1-u^2/q^{2k+1})}.$$

Define $\lambda'_2, \lambda'_3, \ldots$ according to the rules that if $\lambda'_i = a$, then $\lambda'_{i+1} = b$ with probability $K_1(a,b)$ if i is odd and with probability $K_2(a,b)$ if i is even. Then the resulting partition is distributed according to $R_{(u,q)}$.

Proof. The crucial observation is that $R_{(u,q)}$ can be related to a measure $P_{Sp,u}$ studied in [11]. Indeed, comparing formulas one sees that

$$R_{(u,q)}(\lambda) = \frac{q^{l(\lambda)}}{(1+u^2)} \cdot P_{Sp,u}(\lambda)$$

for all λ. Hence the theorem follows from Theorems 3 and 4 of [11]. □

Next, we define and study the measures $R^e_{(u,q)}$ and $R^o_{(u,q)}$.

Definition 6.4. Fix $0 < u < q^{1/2}$ and q a prime power. The measure $R^e_{(u,q)}$ is defined on the set of all partitions λ (the size can vary) with an even number of

parts and such that all odd parts occur with even multiplicity, by the formula:

$$R^e_{(u,q)}(\lambda) = \prod_{i\geq 1}(1-u^2/q^{2i-1}) \cdot \frac{q^{l(\lambda)}u^{|\lambda|}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}}\prod_i(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2\lfloor m_i(\lambda)/2\rfloor})}.$$

We also define a measure $R^o_{(u,q)}$ on the set of all partitions λ (the size can vary) with an odd number of parts and such that all odd parts occur with even multiplicity, by the formula:

$$R^o_{(u,q)}(\lambda) = \frac{1}{u^2}\prod_{i\geq 1}(1-u^2/q^{2i-1}) \cdot \frac{q^{l(\lambda)}u^{|\lambda|}}{q^{n(\lambda)+\frac{|\lambda|}{2}+\frac{o(\lambda)}{2}}\prod_i(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2\lfloor m_i(\lambda)/2\rfloor})}.$$

These measures arise from $\Omega^{\pm}$ and its nontrivial coset in the following way. We omit the proof, which is almost identical to that of Theorem 6.2.

Theorem 6.5. (1) *Fix u with $0<u<1$. Then choose a random even natural number N such that the probability that $N=2n$ is equal to $(1-u^2)u^{2n}$. Choose one of $\Omega^{\pm}_N(q)$ at random (each with probability $1/2$), and let g be a random element of the chosen group. Let $\Lambda_\phi(g)$ be the partition corresponding to the polynomial ϕ in the rational canonical form of g. Then as ϕ varies, aside from the fact that $\Lambda_\phi=\Lambda_{\phi^*}$, these random variables are independent with probability laws the same as for the symplectic groups in Theorem 1 of* [11], *except for the polynomial $z-1$ which has the distribution $R^e_{(u,q)}$.*

(2) *Choose one of $\Omega^{\pm}_{2n}(q)$ at random (each with probability $1/2$), and let g be a random element of the chosen group. Let $\Lambda_\phi(g)$ be the partition corresponding to the polynomial ϕ in the rational canonical form of g. Let q be fixed and $n\to\infty$. Then as ϕ varies, aside from the fact that $\Lambda_\phi=\Lambda_{\phi^*}$, these random variables are independent with probability laws the same as for the symplectic groups in Theorem 1 of* [11], *except for the polynomial $z-1$, which has the distribution $R^e_{(1,q)}$.*

(3) *Fix u with $0<u<1$. Then choose a random even natural number N such that the probability that $N=2n\geq 2$ is equal to $(1-u^2)u^{2(n-1)}$. Choose one of the nontrivial cosets of $\Omega^{\pm}_N(q)$ at random (each with probability $1/2$), and let g be a random element of the chosen coset. Let $\Lambda_\phi(g)$ be the partition corresponding to the polynomial ϕ in the rational canonical form of g. Then as ϕ varies, aside from the fact that $\Lambda_\phi=\Lambda_{\phi^*}$, these random variables are independent with probability laws the same as for the symplectic groups in Theorem 1 of* [11], *except for the polynomial $z-1$, which has the distribution $R^o_{(u,q)}$.*

(4) *Choose one of the nontrivial cosets of $\Omega^{\pm}_{2n}(q)$ at random (each with probability $1/2$), and let g be a random element of the chosen coset. Let $\Lambda_\phi(g)$ be the partition corresponding to the polynomial ϕ in the rational canonical form of g. Let q be fixed and $n\to\infty$. Then as ϕ varies, aside from the fact that $\Lambda_\phi=\Lambda_{\phi^*}$, these random variables are independent with probability*

laws the same as for the symplectic groups in Theorem 1 of [11]*, except for the polynomial* $z-1$*, which has the distribution* $R^o_{(1,q)}$.

Finally, we describe an algorithm for sampling from $R^e_{(u,q)}$ and $R^o_{(u,q)}$, which is proved along the same lines as Theorem 6.3.

Theorem 6.6. (1) *Let* λ'_1 *be a random even natural number which is equal to* $2k$ *with probability*

$$\prod_{i=1}^{\infty}(1-u^2/q^{2i-1})\frac{u^{2k}}{q^{2k^2-k}(1-u^2/q)(1-1/q^2)\cdots(1-u^2/q^{2k-1})(1-1/q^{2k})}.$$

Define $\lambda'_2, \lambda'_3, \ldots$ *according to the rules that if* $\lambda'_i = a$*, then* $\lambda'_{i+1} = b$ *with probability* $K_1(a,b)$ *if* i *is odd and probability* $K_2(a,b)$ *if* i *is even. Then the resulting partition is distributed according to* $R^e_{(u,q)}$.

(2) *Let* λ'_1 *be a random odd natural number which is equal to* $2k+1$ *with probability*

$$\prod_{i=1}^{\infty}(1-u^2/q^{2i-1})\frac{u^{2k}}{q^{2k^2+k}(1-u^2/q)(1-1/q^2)\cdots(1-1/q^{2k})(1-u^2/q^{2k+1})}.$$

Define $\lambda'_2, \lambda'_3, \ldots$ *according to the rules that if* $\lambda'_i = a$*, then* $\lambda'_{i+1} = b$ *with probability* $K_1(a,b)$ *if* i *is odd and probability* $K_2(a,b)$ *if* i *is even. Then the resulting partition is distributed according to* $R^o_{(u,q)}$.

References

[1] Andrews, G. E., The theory of partitions. Reprint of the 1976 original. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1998. xvi+255 pp. MR1634067 (99c:11126)

[2] Andrews, G. E., Partitions, q-series and the Lusztig-Macdonald-Wall conjectures, *Invent. Math.* **41** (1977), 91-102. MR0446991 (56:5307)

[3] Britnell, J. R., Cyclic, separable and semisimple matrices in the special linear groups over a finite field, *J. London Math. Soc.* **66** (2002), 605-622. MR1934295 (2003k:11039)

[4] Britnell, J. R., Cyclic, separable and semisimple transformations in the special unitary groups over a finite field, *J. Group Theory* **9** (2006), 547-569. MR2243246 (2007e:20101)

[5] Britnell, J. R., Cyclic, separable and semisimple transformations in the finite conformal groups, *J. Group Theory* **9** (2006), 571-601. MR2253954 (2007h:20047)

[6] Britnell, J. R., Cycle index methods for finite groups of orthogonal type in odd characteristic, *J. Group Theory* **9** (2006), 753-773. MR2272715 (2007i:20075)

[7] Cohen, H. and Lenstra, H.W., Jr., Heuristics on class groups, in: *Number theory (New York, 1982)*, 26-36, Lecture Notes in Math., 1052, Springer, Berlin, 1984. MR750661

[8] Fulman, J., Random matrix theory over finite fields, *Bull. Amer. Math. Soc.* **39** (2002), 51-85. MR1864086 (2002i:60012)

[9] Fulman, J., Cycle indices for the finite classical groups, *J. Group Theory* **2** (1999), 251-289. MR1696313 (2001d:20045)

[10] Fulman, J., A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups, *J. Algebra* **212** (1999), 557-590. MR1676854 (2000c:20072)

[11] Fulman, J., A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups, *J. Algebra* **234** (2000), 207-224. MR1799484 (2002j:20094)

[12] Fulman, J. and Guralnick, R., Conjugacy class properties of the extension of $\mathrm{GL}(n,q)$ generated by the inverse transpose involution, *J. Algebra* **275** (2004), 356-396. MR2047453 (2005f:20085)

[13] Fulman, J. and Guralnick, R., Derangements in simple and primitive groups, in: *Groups, combinatorics, and geometry (Durham, 2001)*, 99-121, World Sci. Publ., River Edge, NJ, 2003. MR1994962 (2004e:20003)

[14] Fulman, J. and Guralnick, R., Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, arXiv:0902.2238 (2009).
[15] Fulman, J. and Guralnick, R., Derangements in subspace actions of finite classical groups, preprint.
[16] Fulman, J., Neumann, P. M., and Praeger, C. E., A generating function approach to the enumeration of matrices in classical groups over finite fields. Mem. Amer. Math. Soc. **176** (2005), no. 830, vi+90 pp. MR2145026 (2006b:05125)
[17] Fulton, W. and Harris, J., Representation theory. A first course. Graduate Texts in Mathematics, 129. Readings in Mathematics. Springer-Verlag, New York, 1991. xvi+551 pp. MR1153249 (93a:20069)
[18] Goh, W. and Schmutz, E., The expected order of a random permutation, *Bull. London Math. Soc.* **23** (1991), 34-42. MR1111532 (93a:11080)
[19] Goncharov, V., Du domaine d'analyse combinatoire, *Bull. Acad. Sci. URSS Ser. Math* **8** (1944), 3-48. MR0010922 (6:88b)
[20] Guralnick, R. M. and Tiep, P. H., Cross characteristic representations of even characteristic symplectic groups, *Trans. Amer. Math. Soc.* **356** (2004), 4969-5023. MR2084408 (2005j:20012)
[21] Hardy, G. H. and Wright, E. M., An introduction to the theory of numbers, Fifth edition, Oxford University Press, 1979. MR568909 (81i:10002)
[22] Inglis, N. F. J., The embedding of $O(2m, 2^k) \leq Sp(2m, 2^k)$, *Arch. Math.* **54** (1990), 327-330. MR1042124 (91c:11021)
[23] Kung, J. P. S., The cycle structure of a linear transformation over a finite field, *Linear Algebra Appl.* **36** (1981), 141-155. MR604337 (82d:15012)
[24] Lengler, J., The Cohen-Lenstra heuristic for finite abelian groups, Dissertation zur Erlangung des Grades des Doktors der Naturwissenschaften (2009), available at http://www.math.uni-sb.de/ag/gekeler/PERSONEN/Lengler/Dissertation_Lengler.pdf
[25] Liebeck, M. W., O'Brien, E., Shalev, A., and Tiep, P. H., The Ore conjecture, *J. Europ. Math. Soc.* **12** (2010), 939–1008. MR2654085 (2011e:20016)
[26] Liebeck, M. W. and Seitz, G. M., Nilpotent and unipotent classes in classical groups in bad characteristic, preprint.
[27] Lusztig, G., A note on counting nilpotent matrices of a fixed rank, *Bull. London Math. Soc.* **8** (1976), 77-80. MR0407050 (53:10833)
[28] Lusztig, G., Unipotent elements in small characteristic, *Transform. Groups* **10** (2005), 449-487. MR2183120 (2006m:20074)
[29] Lusztig, G., Unipotent elements in small characteristic. II. *Transform. Groups* **13** (2008), 773-797. MR2452615 (2009j:20066)
[30] Lusztig, G., Unipotent elements in small characteristic. III. *J. Algebra* **329** (2011), 163-189. MR2769321
[31] Macdonald, I. G., Symmetric functions and Hall polynomials, Second edition, Clarendon Press, Oxford, 1995. MR1354144 (96h:05207)
[32] Neumann, P. M. and Praeger, C. E., Cyclic matrices and the MEATAXE, in: *Groups and computation, III (Columbus, OH, 1999)*, 291-300, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001. MR1829488 (2002d:20018)
[33] Neumann, P. and Praeger, C., Cyclic matrices in classical groups over finite fields. Special issue in honor of Helmut Wielandt, *J. Algebra* **234** (2000), 367-418. MR1800732 (2002c:20079)
[34] Pólya, G., Kombinatorische anzahlbestimmungen fuer gruppen, graphen und chemische verbindungen, *Acta Math.* **68** (1937), 145-254.
[35] Pólya, G. and Read, R. C., Combinatorial enumeration of groups, graphs, and chemical compounds. Springer-Verlag, New York, 1987. MR884155 (89f:05013)
[36] Rudvalis, A. and Shinoda, K., An enumeration in finite classical groups, U-Mass Amherst Technical Report, 1988.
[37] Saxl, J. and Seitz, G. M., Subgroups of algebraic groups containing regular elements, *J. London Math. Soc.* **55** (1997), 370-386. MR1438641 (98m:20057)
[38] Schmutz, E., The order of a typical matrix with entries in a finite field, *Israel J. Math.* **91** (1995), 349-371. MR1348322 (97e:15011)
[39] Shalev, A., A theorem on random matrices and some applications, *J. Algebra* **199** (1998), 124-141. MR1489358 (99a:20048)

[40] Shepp, L. A. and Lloyd, S. P., Ordered cycle lengths in a random permutation, *Trans. Amer. Math. Soc.* **121** (1966), 340-357. MR0195117 (33:3320)
[41] Spaltenstein, N., *Classes unipotentes et sous-groupes de Borel*, Lecture Notes in Math. **946**, Springer, 1982. MR672610 (84a:14024)
[42] Stong, R., Some asymptotic results on finite vector spaces, *Adv. Appl. Math.* **9** (1988), 167-199. MR937520 (89c:05007)
[43] Tiep, P. H., Dual pairs of finite classical groups in cross characteristics in Character theory of finite groups, 161-179, Contemp. Math. 524, Amer. Math. Soc., Providence, RI, 2010. MR2731928 (2012a:20025)
[44] Wall, G. E., On the conjugacy classes in the unitary, symplectic, and orthogonal groups, *J. Aust. Math. Soc.* **3** (1963), 1-63. MR0150210 (27:212)
[45] Wall, G. E., Counting cyclic and separable matrices over a finite field, *Bull. Austral. Math. Soc.* **60** (1999), 253-284. MR1711918 (2000k:11137)

Department of Mathematics, University of Southern California, Los Angeles, California 90089
E-mail address: fulman@usc.edu

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge CB3 0WB, United Kingdom
E-mail address: J.Saxl@dpmms.cam.ac.uk

Department of Mathematics, University of Arizona, Tucson, Arizona 85721-0089
E-mail address: tiep@math.arizona.edu