On involutions and indicators of finite orthogonal groups

Gregory K. Taylor and C. Ryan Vinroot

Abstract

We study the numbers of involutions and their relation to Frobenius-Schur indicators in the groups $\mathrm{SO}^{\pm}(n, q)$ and $\Omega^{\pm}(n, q)$. Our point of view for this study comes from two motivations. The first is the conjecture that a finite simple group G is strongly real (all elements are conjugate to their inverses by an involution) if and only if it is totally orthogonal (all Frobenius-Schur indicators are 1), and we observe this holds for all finite simple groups G other than the groups $\Omega^{\pm}(4m, q)$ with q even. We prove computationally that for small m this statement indeed holds for these groups by equating their character degree sums with the number of involutions. We also prove a result on a certain twisted indicator for the groups $\mathrm{SO}^{\pm}(4m + 2, q)$ with q odd. Our second motivation is to continue the work of Fulman, Guralnick, and Stanton on generating functions and asymptotics for involutions in classical groups. We extend their work by finding generating functions for the numbers of involutions in $\mathrm{SO}^{\pm}(n, q)$ and $\Omega^{\pm}(n, q)$ for all q, and we use these to compute the asymptotic behavior for the number of involutions in these groups when q is fixed and n grows.

2010 *AMS Subject Classification*: 20G40, 20C33, 05A15, 05A16

Key words and phrases: Orthogonal groups over finite fields, Frobenius-Schur indicators, involutions, generating functions, asymptotic enumeration

1   Introduction

An element g in a group G is *real* in G if g is conjugate to its inverse in G. In this case, all elements in the G-conjugacy class of g are also real, and the class is called a *real class*. If g is G-conjugate to its inverse by an element $h \in G$ which satisfies $h^2 = 1$, then we say that the element g is *strongly real* in G, and the conjugacy class of g in G is called a *strongly real class*. If all classes of G are real (or strongly real), then G is said to be a *real group* (or a *strongly real group*). If G is a finite group, then the number of real classes of G is equal to the number of complex irreducible characters of G which are real-valued. If χ is a real-valued irreducible character of G, then the complex irreducible representation (π, V) which affords χ may or may not be realizable as a representation over the real numbers. The *Frobenius-Schur indicator* of χ, denoted $\varepsilon(\chi)$, is defined to be $\varepsilon(\chi) = 1$ if (π, V) is realizable as a real representation, $\varepsilon(\chi) = -1$ if (π, V) is not realizable as a real representation but χ is real-valued, and $\varepsilon(\chi) = 0$ if χ is not real-valued. The group G is said to be *totally orthogonal* if $\varepsilon(\chi) = 1$ for all complex irreducible characters χ of G.

Brauer [4, Problem 14] asked for a group-theoretical interpretation for the number of complex irreducible χ of G which satisfy $\varepsilon(\chi) = 1$. Because of many important classes of examples, it is suspected that an answer to Brauer's question should involve the strongly real classes of G. In particular, it has been stated as a conjecture in [21] (attributed to P. H. Tiep) that if G is a finite simple group, then G is strongly real if and only if G is totally orthogonal. It is known that this does not hold for finite groups in general; indeed, Kaur and Kulshretha [21] have exhibited

families of 2-groups groups that are strongly real but not totally orthogonal, and families which are totally orthogonal but not strongly real.

After establishing some preliminary notation and results in Section 2, we consider in Section 3 the conjecture that a finite simple group is strongly real if and only if it is totally orthogonal. Except for the case that G is of the form $\Omega^{\pm}(4m, q)$ with q even, we observe that this conjecture holds for all other finite simple groups G by applying the classification of strongly real simple groups and known results on Frobenius-Schur indicators, in Theorem 3.2. In Section 4, we enumerate various sets of involutions in the finite orthogonal groups and certain subgroups, which is directly related to the above conjecture since a finite group G is totally orthogonal if and only if its character degree sum is equal to the number of involutions in G (see Lemma 2.2). We immediately apply these counts in Section 5, where we use data obtained by Lübeck [26] to show computationally that the groups $\Omega^{\pm}(4m, q)$ with q even are indeed totally orthogonal for small rank, and that certain twisted indicators of $\Omega^{\pm}(4m + 2, q)$ are all 1 for small rank, in Theorem 5.2. We show the analogous twisted indicators are always 1 for $\mathrm{SO}^{\pm}(4m + 2, q)$ when q is odd in Theorem 5.1.

In Sections 6 and 7 we extend results of Fulman, Guralnick, and Stanton [11] on the asymptotics for the numbers of involutions in finite classical groups. Specifically, in Section 6 we find generating functions for the numbers of involutions in $\mathrm{SO}^{\pm}(n, q)$ and $\Omega^{\pm}(n, q)$ (for q odd and even), and in Section 7 we compute asymptotics for the number of involutions in these groups (as n grows and q is fixed), as is suggested could be done in the introduction of [11]. Several interesting results emerge, for example in Corollary 7.3 we see that as n grows $\Omega^{\pm}(n, q)$ asymptotically has half the number of involutions as $\mathrm{SO}^{\pm}(n, q)$, when q is odd and fixed.

The generating functions in Section 6 are also significant in the problem of computing Frobenius-Schur indicators for the groups of interest. By using the generating function for the number of involutions in $\mathrm{Sp}(2n, q)$ found in [11], and applying Deligne-Lusztig theory and extending the techniques from [12], the second-named author showed that when q is even the group $\mathrm{Sp}(2n, q)$ is totally orthogonal [37]. The hope is that a similar method, using the relevant generating functions from Section 6 in this paper, will yield the analogous result for $\Omega^{\pm}(4m, q)$ with q even and thus complete the last case in Theorem 3.2.

2 Preliminaries

2.1 The finite orthogonal groups

We primarily study various types of orthogonal groups defined over finite fields, which we now discuss. Considerations of other groups are isolated to Section 3.

Let $\mathbb{F}_q$ denote a finite field with q elements, and let V be a vector space over $\mathbb{F}_q$ of dimension N where $N \in \{2n, 2n + 1\}$. We first consider the case that q is odd. Let Q be a non-degenerate quadratic form defined on V (that is, the symmetric form on V defined by Q is non-degenerate). In this case, Q must be equivalent to one of four possible forms. We label these as follows, where the form is given by the image of a vector in V with some coordinates $(x_1, \ldots, x_N)$:

$$
\begin{array}{cl}
(\mathbf{0}) & x_1 x_2 + x_3 x_4 + \cdots + x_{2n-1} x_{2n} \\
(\mathbf{w}) & x_1 x_2 + x_3 x_4 + \cdots + x_{2n-3} x_{2n-2} + x_{2n-1}^2 - \delta x_{2n}^2 \\
(\mathbf{1}) & x_1 x_2 + x_3 x_4 + \cdots + x_{2n-1} x_{2n} + x_{2n+1}^2 \\
(\mathbf{d}) & x_1 x_2 + x_3 x_4 + \cdots + x_{2n-1} x_{2n} + \delta x_{2n+1}^2,
\end{array}
$$

2

where δ is some fixed element in $\mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$. We define $\boldsymbol{W} = \{\boldsymbol{0}, \boldsymbol{w}, \boldsymbol{1}, \boldsymbol{d}\}$, and the *Witt type* of Q is defined to be the symbol in $\boldsymbol{W}$ corresponding to the quadratic form in the list above to which Q is equivalent. We may define the orthogonal group on V corresponding to Q, denoted by $\mathrm{O}_Q(V)$, and since the isomorphism type depends only on the Witt type, we may also write this as $\mathrm{O}_Q(V) = \mathrm{O}^{(\boldsymbol{s})}(N, q)$, where $\boldsymbol{s} \in \boldsymbol{W}$ is the Witt type of Q. When $N = 2n$ is even, we will denote $\mathrm{O}^{(\boldsymbol{0})}(N, q) = \mathrm{O}^+(2n, q)$ and $\mathrm{O}^{(\boldsymbol{w})}(N, q) = \mathrm{O}^-(2n, q)$. When $N = 2n + 1$ is odd, denote $\mathrm{O}^{(\boldsymbol{1})}(N, q) = \mathrm{O}^+(2n + 1, q)$ and $\mathrm{O}^{(\boldsymbol{d})}(N, q) = \mathrm{O}^-(2n + 1, q)$, and in fact we further have

$$\mathrm{O}^+(2n + 1, q) \cong \mathrm{O}^-(2n + 1, q),$$

which we commonly denote by $\mathrm{O}(2n + 1, q)$. We will write $\mathrm{O}^\pm(N, q)$ for a general orthogonal group of one of the types just described. We let $\mathrm{SO}^\pm(N, q)$ denote the special orthogonal group, or the index 2 subgroup consisting of determinant 1 elements of the corresponding orthogonal group $\mathrm{O}^\pm(N, q)$. Note that we have

$$\mathrm{O}(2n + 1, q) \cong \mathrm{SO}(2n + 1, q) \times \{\pm 1\},$$

where $Z = \{\pm 1\}$ is the center of $\mathrm{O}^\pm(N, q)$. We let $\Omega^\pm(N, q)$ denote the derived subgroup of $\mathrm{SO}^\pm(N, q)$, which has index 2 in $\mathrm{SO}^\pm(N, q)$. Then $\Omega^\pm(N, q)$ has center $Z = \Omega^\pm(N, q) \cap \{1, -1\}$, and the projective group $\mathrm{P}\Omega^\pm(N, q) = \Omega^\pm(N, q)/Z$ is known to be simple in all but finitely many cases (see [18, Theorem 6.31], for example).

We now consider the case that q is even, and the orthogonal group $\mathrm{O}_Q(V)$ corresponding to some *non-defective* quadratic form Q defined on V. The classification of equivalence classes of such quadratic forms when q is even is only somewhat different from the situation when q is odd given above, although we do not need the full description here, and we refer to [18, Chapter 12] for details. In particular, when $\dim(V) = 2n + 1$ is odd, there is again only one isomorphism class of orthogonal groups, which we denote by $\mathrm{O}(2n + 1, q)$. In this case, we have

$$\mathrm{O}(2n + 1, q) \cong \mathrm{Sp}(2n, q),$$

where $\mathrm{Sp}(2n, q)$ is the symplectic group corresponding to the unique class of non-degenerate alternating forms that one can define on an $\mathbb{F}_q$-vector space of dimension $2n$, for example see [18, Theorem 14.2]. When q is even, we have that $\mathrm{Sp}(2n, q) = \mathrm{PSp}(2n, q)$ is a simple group for all but finitely many cases. When $N = 2n$ is even, there are two equivalence classes of non-defective quadratic forms on V, see [18, Theorem 12.9(2)]. We write $\mathrm{O}^+(2n, q)$ for the group corresponding to the form which may be defined as $Q(x_1, \ldots, x_{2n}) = x_1 x_{1+n} + x_2 x_{2+n} + \cdots + x_n x_{2n}$, and we write $\mathrm{O}^-(2n, q)$ for the group corresponding to the other possible class of quadratic form. In the case that q is even, we let $\Omega^\pm(2n, q)$ denote the derived group of $\mathrm{O}^\pm(2n, q)$, which has index 2 in $\mathrm{O}^\pm(2n, q)$, and is a simple group for all but finitely many cases. There is also the following useful criterion for determining when an element of $\mathrm{O}^\pm(2n, q)$ is in its derived subgroup $\Omega^\pm(2n, q)$ (see [30, Proposition 3.2]).

Lemma 2.1. *If q is even and $g \in \mathrm{O}^\pm(2n, q)$, then $g \in \Omega^\pm(2n, q)$ if and only if $\mathrm{rank}(1 + g)$ is even.*

We will need to use the orders of the groups described above numerous times throughout this paper, and so we list them here for reference. The first formula holds whether q is even or odd:

$$|\mathrm{O}^\pm(2n, q)| = 2q^{n(n-1)}(q^n \mp 1) \prod_{i=1}^{n-1}(q^{2i} - 1). \tag{2.1}$$

3

When q is odd,

$$|\mathrm{O}(2n+1, q)| = 2q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1). \tag{2.2}$$

When q is even,

$$|\mathrm{O}(2n+1, q)| = |\mathrm{Sp}(2n, q)| = q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1). \tag{2.3}$$

We also have

$$|\mathrm{SO}^{\pm}(N, q)| = \frac{1}{2}|\mathrm{O}^{\pm}(N, q)| \quad \text{and} \quad |\Omega^{\pm}(N, q)| = \frac{1}{2}|\mathrm{SO}^{\pm}(N, q)| \quad \text{when } q \text{ is odd,} \tag{2.4}$$

and

$$|\Omega^{\pm}(2n, q)| = \frac{1}{2}|\mathrm{O}^{\pm}(2n, q)| \quad \text{when } q \text{ is even.} \tag{2.5}$$

Note that when q is odd we have $|\mathrm{O}(1, q)| = 2$, while when q is even we have $|\mathrm{O}(1, q)| = |\mathrm{Sp}(0, q)| = 1$. For q even or odd, we define $|\mathrm{O}^{+}(0, q)| = 1$, but we do not define $|\mathrm{O}^{-}(0, q)|$.

2.2 Characters and Frobenius-Schur indicators

Let G be a finite group, and we let $\mathrm{Irr}(G)$ denote the collection of irreducible complex characters of G, and we let $\langle \cdot, \cdot \rangle$ denote the standard inner product on class functions of G. If $\chi \in \mathrm{Irr}(G)$ and (π, V) is the representation of G affording χ, let $[\pi]_{\mathcal{B}}$ denote the matrix representation corresponding to a choice of basis $\mathcal{B}$ for V. We say that (π, V) is *defined over* $\mathbb{R}$ if there is a basis $\mathcal{B}$ for V such that $[\pi(g)]_{\mathcal{B}}$ has all entries in $\mathbb{R}$ for all $g \in G$. Recall that the *Frobenius-Schur indicator* of $\chi \in \mathrm{Irr}(G)$, denoted $\varepsilon(\chi)$, is defined to be $\varepsilon(\chi) = 0$ if χ is not real-valued, $\varepsilon(\chi) = 1$ if (π, V) is defined over $\mathbb{R}$, and $\varepsilon(\chi) = -1$ if χ is real-valued but (π, V) is not defined over $\mathbb{R}$. Then we have $\varepsilon(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$, and $\sum_{\chi \in \mathrm{Irr}(G)} \varepsilon(\chi)\chi(1) = \#\{g \in G \mid g^2 = 1\}$ (see [19, Chapter 4], for example).

We now discuss a useful generalization of the Frobenius-Schur indicator. Let ι be an automorphism of G such that $\iota^2 = 1$, and we denote the action of ι on $g \in G$ by ${}^{\iota}g$. We also let ${}^{\iota}\chi$ and ${}^{\iota}\pi$ be defined by ${}^{\iota}\chi(g) = \chi({}^{\iota}g)$ and ${}^{\iota}\pi(g) = \pi({}^{\iota}g)$, respectively. Given $\chi \in \mathrm{Irr}(G)$, the representation (π, V) which affords χ, and the automorphism ι of G, define the *twisted Frobenius-Schur indicator* of χ, denoted $\varepsilon_{\iota}(\chi)$, by

$$\varepsilon_{\iota}(\chi) = \begin{cases} 1 & \text{if there is some } \mathcal{B} \text{ such that } [{}^{\iota}\pi(g)]_{\mathcal{B}} = \overline{[\pi(g)]_{\mathcal{B}}} \text{ for all } g \in G, \\ -1 & \text{if } {}^{\iota}\chi = \bar{\chi} \text{ but there is no } \mathcal{B} \text{ such that } [{}^{\iota}\pi(g)]_{\mathcal{B}} = \overline{[\pi(g)]_{\mathcal{B}}} \text{ for all } g \in G, \\ 0 & \text{if } {}^{\iota}\chi \neq \bar{\chi}. \end{cases}$$

Note that $\varepsilon_{\iota}(\chi) = \pm 1$ for all $\chi \in \mathrm{Irr}(G)$ if and only if ${}^{\iota}g$ is conjugate to g^{-1} for every $g \in G$. It was proved by Kawanaka and Matsuyama [22] that a formula for $\varepsilon_{\iota}(\chi)$ is given by

$$\varepsilon_{\iota}(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g \, {}^{\iota}g).$$

Further, by applying orthogonality relations, the following formula is obtained by Bump and Ginzburg [5, Proposition 1]:

$$\sum_{\chi \in \mathrm{Irr}(G)} \varepsilon_{\iota}(\chi)\chi(1) = \#\left\{g \in G \mid {}^{\iota}g = g^{-1}\right\}.$$

An immediate consequence of this formula that we will need is as follows.

4

Lemma 2.2. *If G is a finite group with automorphism ι such that $\iota^2 = 1$, then $\varepsilon_\iota(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$ if and only if*

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1) = \# \left\{ g \in G \mid {}^\iota g = g^{-1} \right\}.$$

When $\iota = 1$, we recover the classical Frobenius-Schur indicator, $\varepsilon_\iota(\chi) = \varepsilon(\chi)$, in which case $\varepsilon(\chi) = \pm 1$ if and only if χ is real-valued, and $\varepsilon(\chi) = \pm 1$ for all $\chi \in \mathrm{Irr}(G)$ if and only if G is a real group, so g is conjugate to g^{-1} for all $g \in G$. Further, Lemma 2.2 says that $\varepsilon(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$, that is G is *totally orthogonal*, exactly when the sum of the degrees of the irreducible characters of χ is the number of involutions in G, where we define an involution of G to be any element $g \in G$ such that $g^2 = 1$. When ι is defined by an inner automorphism, say ${}^\iota g = hgh^{-1}$ with $h \in G$, such that $h^2 = z \in Z(G)$ where $Z(G)$ is the center of G, we have an explicit relationship between $\varepsilon_\iota(\chi)$ and $\varepsilon(\chi)$. In particular, if we let ω_χ denote the central character of the representation of G which affords π, we have [35, Lemma 2.1]

$$\varepsilon_\iota(\chi) = \omega_\chi(z)\varepsilon(\chi). \tag{2.6}$$

Now suppose $H \leq G$ is an index 2 subgroup of G, such that for some $s \in G \setminus H$ with $s^2 = 1$ we have $G = H\langle s \rangle = H \cup sH$. We have the following relationship between indicators and twisted indicators of G and H in this case.

Lemma 2.3. *Suppose G is a finite group, $H \leq G$, $[G : H] = 2$, $G = H\langle s \rangle$ with $s^2 = 1$, and define ι on H by ${}^\iota h = shs^{-1}$. Then the following hold.*

(i) *If $\varepsilon(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$, and H is a real group, then for all $\psi \in \mathrm{Irr}(H)$, we have $\varepsilon(\psi) = 1$ and $\varepsilon_\iota(\psi) \geq 0$.*

(ii) *If $\varepsilon(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$, and ${}^\iota h$ is H-conjugate to h^{-1} for all $h \in H$, then for all $\psi \in \mathrm{Irr}(H)$, we have $\varepsilon_\iota(\psi) = 1$ and $\varepsilon(\psi) \geq 0$.*

(iii) *If G is a real group, and if $\varepsilon(\psi) = 1$ for all $\psi \in \mathrm{Irr}(H)$, then for all $\chi \in \mathrm{Irr}(G)$ we have $\varepsilon(\chi) = 1$, and for all $\psi \in \mathrm{Irr}(H)$ we have $\varepsilon_\iota(\psi) \geq 0$*

(iv) *If G is a real group, and if $\varepsilon_\iota(\psi) = 1$ for all $\psi \in \mathrm{Irr}(H)$, then for all $\chi \in \mathrm{Irr}(G)$ we have $\varepsilon(\chi) = 1$, and for all $\psi \in \mathrm{Irr}(H)$ we have $\varepsilon(\psi) \geq 0$.*

Proof. All of the statements essentially follow from [36, Proposition 2.1], which may be applied as follows. Given any $\psi \in \mathrm{Irr}(H)$, the induced character $\psi^G = \chi$ is either irreducible or else $\psi^G = \chi_1 + \chi_2$ where $\chi_1, \chi_2 \in \mathrm{Irr}(G)$. Then [36, Proposition 2.1] says that in these two cases, we have

$$\varepsilon(\chi) = \varepsilon(\psi) + \varepsilon_\iota(\psi), \quad \text{or} \quad \varepsilon(\chi_1) + \varepsilon(\chi_2) = \varepsilon(\psi) + \varepsilon_\iota(\psi) \text{ with } \varepsilon(\chi_1) = \varepsilon(\chi_2), \tag{2.7}$$

respectively.

In cases (i) and (ii), we have $\varepsilon(\chi) = \varepsilon(\chi_1) = \varepsilon(\chi_2) = 1$. If H is a real group, then $\varepsilon(\psi) = \pm 1$ for all $\psi \in \mathrm{Irr}(G)$, and the only possibility for (2.7) to hold is that $\varepsilon(\psi) = 1$ and $\varepsilon_\iota(\psi) \geq 0$ for all $\psi \in \mathrm{Irr}(G)$, and (i) follows. Likewise for (ii), if ${}^\iota h$ is conjugate to h^{-1} in H for all $h \in H$, then $\varepsilon_\iota(\psi) = \pm 1$ for all $\psi \in \mathrm{Irr}(G)$, and it follows from (2.7) we must have $\varepsilon_\iota(\psi) = 1$ and $\varepsilon(\psi) \geq 0$ for all $\psi \in \mathrm{Irr}(H)$.

In cases (iii) and (iv), we have $\varepsilon(\chi) = \pm 1$ and $\varepsilon(\chi_1) = \varepsilon(\chi_2) = \pm 1$. In (iii), since $\varepsilon(\psi) = 1$ for all $\psi \in \mathrm{Irr}(H)$, we have (2.7) holds only if $\varepsilon(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$ and $\varepsilon_\iota(\psi) \geq 0$ for

all $\psi \in \mathrm{Irr}(H)$. Similarly in (iv), since $\varepsilon_\iota(\psi) = 1$ for all $\psi \in \mathrm{Irr}(H)$, the only way (2.7) can be satisfied is if $\varepsilon(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$ (so G is totally orthogonal) and $\varepsilon(\psi) \geq 0$ for all $\psi \in \mathrm{Irr}(H)$. $\qquad\square$

We will also need the following relationship between indicators of G and $G/Z(G)$ when considering projective classical groups.

Lemma 2.4. *Let G be a finite group with automorphism ι such that $\iota^2 = 1$, and let $Z = Z(G)$ be the center of G. Let ι also denote the automorphism of G/Z defined by $\iota(gZ) = \iota(g)Z$. If $\varepsilon_\iota(\chi) = 1$ for every $\chi \in \mathrm{Irr}(G)$, then $\varepsilon_\iota(\psi) = 1$ for every $\psi \in \mathrm{Irr}(G/Z)$.*

Proof. Note that ι is well-defined on G/Z by $\iota(gZ) = \iota(g)Z$. Let $\psi \in \mathrm{Irr}(G/Z)$ and define the class function χ on G by $\chi(g) = \psi(gZ)$. It follows that $\chi \in \mathrm{Irr}(G)$, since

$$\langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 = \frac{1}{|G|} \sum_{g \in G} |\psi(gZ)|^2 = \frac{|Z|}{|G|} \sum_{gZ \in G/Z} |\psi(gZ)|^2 = \langle \psi, \psi \rangle = 1.$$

By assumption we have $\varepsilon_\iota(\chi) = 1$, and we can compute $\varepsilon_\iota(\psi)$ as follows:

$$\varepsilon_\iota(\psi) = \frac{|Z|}{|G|} \sum_{gZ \in G/Z} \psi(g^\iota g Z) = \frac{|Z|}{|G|} \sum_{gZ \in G/Z} \chi(g^\iota g) = \frac{1}{|G|} \sum_{g \in G} \chi(g^\iota g) = \varepsilon_\iota(\chi) = 1,$$

as claimed. $\qquad\square$

3 Real Simple Groups

Tiep and Zalesski classified all finite quasi-simple groups (and so all finite simple groups) which are real [32]. The following theorem, stated in [34, Theorems 2 and 3], solves the problem of classifying all finite simple groups which are strongly real, and it turns out that a finite simple group is real if and only if it is strongly real. This theorem follows from the work of many authors [2, 8, 10, 13, 16, 24, 25, 30, 32, 34, 39].

Theorem 3.1. *Let G be a finite simple group. Then G is real if and only if G is strongly real, and this occurs if and only if G is isomorphic to one of the following groups:*
    (1) One of the Janko sporadic groups J_1 or J_2;
    (2) One of the alternating groups A_{10} or A_{14};
    (3) The Steinberg triality group ${}^3D_4(q)$;
    (4) $\Omega(2n+1, q)$ for $q \equiv 1 (mod\ 4)$ and $n \geq 3$;
    (5) $\Omega(9, q)$ for $q \equiv 3 (mod\ 4)$;
    (6) $\mathrm{P}\Omega^-(4m, q)$ for $m \geq 2$;
    (7) $\mathrm{P}\Omega^+(4m, q)$ for $q \not\equiv 3 (mod\ 4)$ and $m \geq 3$;
    (8) $\mathrm{P}\Omega^+(8, q)$;
    (9) $\mathrm{PSp}(2n, q)$ for $q \not\equiv 3 (mod\ 4)$ and $n \geq 1$.

As mentioned in the introduction, it has been conjectured that a finite simple group is strongly real if and only if it is totally orthogonal. We now prove this statement for all but one family of groups, namely $\mathrm{P}\Omega^\pm(4m, q) = \Omega^\pm(4m, q)$ for q even.

Theorem 3.2. *Let G be a finite simple group other than one of the form $\Omega^\pm(4m, q)$ with q even. Then G is strongly real if and only if G is totally orthogonal.*

Proof. First, if G is totally orthogonal, then in particular G is real, and from Theorem 3.1 we know G is strongly real.

Conversely, suppose that G is strongly real, so listed in Theorem 3.1, but is not $\Omega^\pm(4m, q)$ with q even. We go through each type of group in the classification, and give references or show that it is totally orthogonal.

If G is one of the Janko groups J_1 or J_2, then the fact that G is totally orthogonal follows from the Atlas of finite groups [7, pgs. 36, 42-43].

If G is A_{10} or A_{14}, then G is an index 2 subgroup of S_{10} or S_{14}. For all n, S_n is totally orthogonal (all representations of S_n are defined over $\mathbb{Q}$ by [20, Theorem 2.1.12]). Since G is real, it follows from Lemma 2.3(i) that G is totally orthogonal.

If $G = {}^3D_4(q)$, then for q odd, G is totally orthogonal by Barry [3]. If q is even, then G is totally orthogonal by Ohmori [29].

Consider the cases when either $G = \Omega(2n + 1, q)$ with $n \geq 3, q \equiv 1 \pmod 4$ or $G = \Omega(9, q)$ with $q \equiv 3 \pmod 4$. It is a result of Gow [17, Theorem 2] that $\mathrm{SO}(2n+1, q)$ is totally orthogonal when q is odd. Since G is both a real group and an index 2 subgroup in some $\mathrm{SO}(2n + 1, q)$, it follows from Lemma 2.3(i) that G is totally orthogonal.

Now consider the case when either $G = \mathrm{P}\Omega^+(8, q)$ with q odd, $G = \mathrm{P}\Omega^-(4m, q)$ with q odd and $m \geq 2$, or $G = \mathrm{P}\Omega^+(4m, q)$ with $q \equiv 1 \pmod 4$ and $m \geq 3$. Gow [17, Theorem 2] proved that for q odd and $m \geq 1$ the groups $\mathrm{SO}^\pm(4m, q)$ are all totally orthogonal, and so by Lemma 2.4 the groups $\mathrm{PSO}^\pm(4m, q)$ are totally orthogonal. Since in each case G is an index 2 subgroup of some $\mathrm{PSO}^\pm(4m, q)$, and G is a real group, then it follows from Lemma 2.3(i) that G is totally orthogonal.

The case when $G = \mathrm{PSp}(2n, q) = \mathrm{Sp}(2n, q)$ with q even is proved in [37, Theorem 4.2].

Finally, we consider the case when $G = \mathrm{PSp}(2n, q)$ with $q \equiv 1 \pmod 4$ and $n \geq 1$. Gow proved [17, Theorem 1] that if χ is an irreducible character of $\mathrm{Sp}(2n, q)$ with $q \equiv 1 \pmod 4$, then $\varepsilon(\chi) = \omega_\chi(-I)$, where ω_χ is the central character of the representation with character χ. Let $\alpha \in \mathbb{F}_q$ such that $\alpha^2 = -1$. If we define $\mathrm{Sp}(2n, q)$ via the alternating form corresponding to $\begin{bmatrix} 0 & -I_n \\ I_n & 0 \end{bmatrix}$ (which may always be done), then $h = \begin{bmatrix} \alpha I_n & 0 \\ 0 & -\alpha I_n \end{bmatrix} \in \mathrm{Sp}(2n, q)$. Then define ι to be the order 2 inner automorphism of $\mathrm{Sp}(2n, q)$ defined by conjugation by h. Since $h^2 = -I$, then by (2.6) we have $\varepsilon_\iota(\chi) = \omega_\chi(-I)\varepsilon(\chi)$ for any irreducible character χ of $\mathrm{Sp}(2n, q)$. From the result of Gow, for $q \equiv 1 \pmod 4$ it follows that $\varepsilon_\iota(\chi) = 1$ for every irreducible character χ of $\mathrm{Sp}(2n, q)$. By Lemma 2.4, we have that $\varepsilon_\iota(\psi) = 1$ for any irreducible character ψ of G, where ι is the induced inner automorphism defined by hZ in G. In this case, $(hZ)^2 = -IZ = Z$ in G, and so again by (2.6) we have $1 = \varepsilon_\iota(\psi) = \omega_\psi(Z)\varepsilon(\psi) = \varepsilon(\psi)$ for any irreducible character ψ of G. Thus G is totally orthogonal. $\qquad\square$

4   Numbers of Involutions

In this section we count the number of involutions in various subgroups and cosets in the finite orthogonal groups. In general, if G is a group (or some subset of a group), then we will write $i(G)$ for the number of involutions in G.

4.1   Groups over fields of odd characteristic

We first consider the case that q is odd. Below we recall the number of involutions in the full orthogonal group $\mathrm{O}^\pm(n, q)$, which is given in [11, Lemma 6.1].

Proposition 4.1. *Let q be odd.*

(1) *The number of involutions in $\mathrm{O}^+(2n, q)$ is equal to*

$$i(\mathrm{O}^+(2n, q)) = \sum_{k=0}^{2n} \frac{|\mathrm{O}^+(2n, q)|}{|\mathrm{O}^+(k, q)||\mathrm{O}^+(2n-k, q)|} + \sum_{k=1}^{2n-1} \frac{|\mathrm{O}^+(2n, q)|}{|\mathrm{O}^-(k, q)||\mathrm{O}^-(2n-k, q)|}.$$

(2) *The number of involutions in $\mathrm{O}^-(2n, q)$ is equal to*

$$i(\mathrm{O}^-(2n, q)) = \sum_{k=0}^{2n-1} \frac{|\mathrm{O}^-(2n, q)|}{|\mathrm{O}^+(k, q)||\mathrm{O}^-(2n-k, q)|} + \sum_{k=1}^{2n} \frac{|\mathrm{O}^-(2n, q)|}{|\mathrm{O}^-(k, q)||\mathrm{O}^+(2n-k, q)|}.$$

(3) *The number of involutions in $\mathrm{O}(2n+1, q)$ is equal to*

$$i(\mathrm{O}(2n+1, q)) = \sum_{k=0}^{2n+1} \frac{|\mathrm{O}(2n+1, q)|}{|\mathrm{O}^+(k, q)||\mathrm{O}^+(2n+1-k, q)|} + \sum_{k=1}^{2n} \frac{|\mathrm{O}(2n+1, q)|}{|\mathrm{O}^-(k, q)||\mathrm{O}^-(2n+1-k, q)|}.$$

The quantities in Proposition 4.1 are obtained by noting that an involution in $\mathrm{O}^\pm(N, q)$ has only $+1$ or -1 as eigenvalues. If we fix the -1-eigenspace to have dimension k and so the $+1$-eigenspace has dimension $N - k$, there are two conjugacy classes of involutions with this property, and their centralizers are products of smaller orthogonal groups whose orders are given in the denominators of the above expressions. The type of orthogonal groups making up the direct product of their centralizer depends on the Witt type obtained when restricting the quadratic form to the eigenspaces. Only slight modifications to this reasoning are needed to obtain expressions for other required involution counts.

Proposition 4.2. *Let q be odd.*

(1) *The number of involutions in $\mathrm{SO}^+(2n, q)$ is equal to*

$$i(\mathrm{SO}^+(2n, q)) = \sum_{R=0}^{n} \frac{|\mathrm{O}^+(2n, q)|}{|\mathrm{O}^+(2R, q)||\mathrm{O}^+(2n-2R, q)|} + \sum_{R=1}^{n-1} \frac{|\mathrm{O}^+(2n, q)|}{|\mathrm{O}^-(2R, q)||\mathrm{O}^-(2n-2R, q)|}.$$

(2) *The number of involutions in $\mathrm{SO}^-(2n, q)$ is equal to*

$$i(\mathrm{SO}^-(2n, q)) = \sum_{R=0}^{n-1} \frac{|\mathrm{O}^-(2n, q)|}{|\mathrm{O}^+(2R, q)||\mathrm{O}^-(2n-2R, q)|} + \sum_{R=1}^{n} \frac{|\mathrm{O}^-(2n, q)|}{|\mathrm{O}^-(2R, q)||\mathrm{O}^+(2n-2R, q)|}$$

$$= 2 \sum_{R=0}^{n-1} \frac{|\mathrm{O}^-(2n, q)|}{|\mathrm{O}^+(2R, q)||\mathrm{O}^-(2n-2R, q)|}.$$

(3) *The number of involutions in $\mathrm{SO}(2n+1, q)$ is equal to*

$$i(\mathrm{SO}(2n+1, q)) = \sum_{R=0}^{n} \frac{|\mathrm{O}(2n+1, q)|}{|\mathrm{O}^+(2R, q)||\mathrm{O}(2n+1-2R, q)|} + \sum_{R=1}^{n} \frac{|\mathrm{O}(2n+1, q)|}{|\mathrm{O}^-(2R, q)||\mathrm{O}(2n+1-2R, q)|}$$

$$= \frac{1}{2} i(\mathrm{O}(2n+1, q)).$$

8

Proof. In the expressions given in Proposition 4.1, the index k corresponds to the dimension of the -1-eigenspace of the involution. The involution is in $\mathrm{SO}^{\pm}(N, q)$ if and only if k is even, and so we let $k = 2R$ and take only these relevant terms from the sums in Proposition 4.1. In case (2), the two sums are the same after re-indexing. In (3), the fact that $\mathrm{O}(2n + 1, q) \cong \mathrm{SO}(2n + 1, q) \times \{\pm 1\}$ implies $i(\mathrm{SO}(2n + 1, q)) = (1/2)i(\mathrm{O}(2n + 1, q))$. $\qquad\square$

We also consider the number of involutions with determinant -1 in the orthogonal group of even dimension.

Proposition 4.3. *Let q be odd. The number of involutions in $\mathrm{O}^{\pm}(2n, q) \setminus \mathrm{SO}^{\pm}(2n, q)$ is equal to*

$$i(\mathrm{O}^{\pm}(2n, q) \setminus \mathrm{SO}^{\pm}(2n, q)) = 2 \sum_{R=0}^{n-1} \frac{|\mathrm{O}^{\pm}(2n, q)|}{|\mathrm{O}(2R + 1, q)||\mathrm{O}(2n - 2R - 1, q)|}.$$

Proof. This expression is obtained by considering when $k = 2R + 1$ is odd in the sums in Proposition 4.1. Since $\mathrm{O}^{+}(N, q) \cong \mathrm{O}^{-}(N, q)$ when N is odd, then the orders in the denominators of the two sums obtained are the same, and so the terms in each resulting sum are the same. $\quad\square$

The following is needed to count involutions in the groups $\Omega^{\pm}(n, q)$ when q is odd, and is a special case of [6, Proposition 16.30] (noting involutions are semisimple elements when q is odd).

Lemma 4.1. *Let q be odd, and let C be a class of involutions in $\mathrm{SO}^{\pm}(N, q)$. Let d be the dimension of the -1-eigenspace of C (where d must be even). If Q is the quadratic form corresponding to $\mathrm{SO}^{\pm}(N, q)$, then let $\mathbf{s}_{-1}$ be the Witt type of the form Q restricted to the -1-eigenspace of an involution in C. Define*

$$v_{-} = \begin{cases} \frac{d(q-1)}{4} & \text{if } \mathbf{s}_{-1} = \mathbf{0} \\ 1 + \frac{d(q-1)}{4} & \text{if } \mathbf{s}_{-1} = \mathbf{w}. \end{cases}$$

Then C lies in $\Omega^{\pm}(N, q)$ if and only if v_{-} is an even integer, and C defines a unique class of involutions in $\Omega^{\pm}(N, q)$ in this case.

We now have the following.

Proposition 4.4. *Let $q \equiv 1 \pmod 4$.*

(1) *The number of involutions in $\Omega^{+}(2n, q)$ is equal to*

$$i(\Omega^{+}(2n, q)) = \sum_{R=0}^{n} \frac{|\mathrm{O}^{+}(2n, q)|}{|\mathrm{O}^{+}(2R, q)||\mathrm{O}^{+}(2n - 2R, q)|}.$$

(2) *The number of involutions in $\Omega^{-}(2n, q)$ is equal to*

$$i(\Omega^{-}(2n, q)) = \sum_{R=0}^{n-1} \frac{|\mathrm{O}^{-}(2n, q)|}{|\mathrm{O}^{+}(2R, q)||\mathrm{O}^{-}(2n - 2R, q)|}.$$

(3) *The number of involutions in $\Omega(2n + 1, q)$ is equal to*

$$i(\Omega(2n + 1, q)) = \sum_{R=0}^{n} \frac{|\mathrm{O}(2n + 1, q)|}{|\mathrm{O}^{+}(2R, q)||\mathrm{O}(2n + 1 - 2R, q)|}.$$

9

Proof. Applying Lemma 4.1, let V_{-1} be the -1-eigenspace of some involution, where $\dim(V_{-1}) = d = 2R$. Since $q \equiv 1(\bmod\ 4)$ and d is even, then v_- is always even if $\mathbf{s}_{-1} = \mathbf{0}$ and v_- is always odd if $\mathbf{s}_{-1} = \mathbf{w}$. Hence an involution lies in $\Omega^{\pm}(n, q)$ if and only if the quadratic form restricted to V_{-1} has Witt type $\mathbf{0}$, corresponding to the orthogonal group $\mathrm{O}^+(2R, q)$. Taking the corresponding terms in the summations of Proposition 4.1, we obtain the expressions as claimed. $\qquad\square$

Proposition 4.5. *Let $q \equiv 3(\bmod\ 4)$.*

(1) *The number of involutions in $\Omega^+(2n, q)$ is equal to*

$$i(\Omega^+(2n, q)) = \sum_{\substack{R=0 \\ R\ even}}^{n} \frac{|\mathrm{O}^+(2n, q)|}{|\mathrm{O}^+(2R, q)||\mathrm{O}^+(2n - 2R, q)|} + \sum_{\substack{R=1 \\ R\ odd}}^{n-1} \frac{|\mathrm{O}^+(2n, q)|}{|\mathrm{O}^-(2R, q)||\mathrm{O}^-(2n - 2R, q)|}.$$

(2) *The number of involutions in $\Omega^-(2n, q)$ is equal to*

$$i(\Omega^-(2n, q)) = \sum_{\substack{R=0 \\ R\ even}}^{n-1} \frac{|\mathrm{O}^-(2n, q)|}{|\mathrm{O}^+(2R, q)||\mathrm{O}^-(2n - 2R, q)|} + \sum_{\substack{R=1 \\ R\ odd}}^{n} \frac{|\mathrm{O}^-(2n, q)|}{|\mathrm{O}^-(2R, q)||\mathrm{O}^+(2n - 2R, q)|}.$$

(3) *The number of involutions in $\Omega(2n + 1, q)$ is equal to*

$$i(\Omega(2n+1, q)) = \sum_{\substack{R=0 \\ R\ even}}^{n} \frac{|\mathrm{O}(2n + 1, q)|}{|\mathrm{O}^+(2R, q)||\mathrm{O}(2n + 1 - 2R, q)|} + \sum_{\substack{R=1 \\ R\ odd}}^{n} \frac{|\mathrm{O}(2n + 1, q)|}{|\mathrm{O}^-(2R, q)||\mathrm{O}(2n + 1 - 2R, q)|}.$$

Proof. We use the same notation and idea as in the proof of Proposition 4.4, and apply Lemma 4.1. Since $q \equiv 3(\bmod\ 4)$ and $d = 2R$, then v_- is even either when R is even and $\mathbf{s}_{-1} = \mathbf{0}$, or when R is odd and $\mathbf{s}_{-1} = \mathbf{w}$. These situations apply to the terms from Proposition 4.1 when either R is even and the first factor in the denominator is $|\mathrm{O}^+(2R, q)|$ (corresponding to $\mathbf{s}_{-1} = \mathbf{0}$), or when R is odd and the first factor in the denominator is $|\mathrm{O}^-(2R, q)|$ (when $\mathbf{s}_{-1} = \mathbf{w}$), respectively. The result follows. $\qquad\square$

4.2 Groups over fields of characteristic two

We now deal with sets of involutions when q is even. The next result is [11, Theorems 5.6].

Proposition 4.6. *Let q be even, and let*

$$A_k^{\pm} = q^{k(k-1)/2 + k(2n-2k)}|\mathrm{Sp}(k, q)|\,|\mathrm{O}^{\pm}(2n - 2k, q)|,$$
$$B_k = 2q^{k(k+1)/2 + (k-1)(2n-2k)-1}q^{k-1}|\mathrm{Sp}(k - 2, q)|\,|\mathrm{Sp}(2n - 2k, q)|,$$
$$C_k = 2q^{k(k-1)/2 + (k-1)(2n-2k)}|\mathrm{Sp}(k - 1, q)|\,|\mathrm{Sp}(2n - 2k, q)|.$$

(1) *The number of involutions in $\mathrm{O}^+(2n, q)$ is equal to*

$$i(\mathrm{O}^+(2n, q)) = \sum_{\substack{k=0 \\ k\ even}}^{n} \frac{|\mathrm{O}^+(2n, q)|}{A_k^+} + \sum_{\substack{k=2 \\ k\ even}}^{n} \frac{|\mathrm{O}^+(2n, q)|}{B_k} + \sum_{\substack{k=1 \\ k\ odd}}^{n} \frac{|\mathrm{O}^+(2n, q)|}{C_k}.$$

(2) The number of involutions in $\mathrm{O}^-(2n, q)$ *is equal to*

$$i(\mathrm{O}^-(2n, q)) = \sum_{\substack{k=0 \\ k \ even}}^{n-1} \frac{|\mathrm{O}^-(2n, q)|}{A_k^-} + \sum_{\substack{k=2 \\ k \ even}}^{n} \frac{|\mathrm{O}^-(2n, q)|}{B_k} + \sum_{\substack{k=1 \\ k \ odd}}^{n} \frac{|\mathrm{O}^-(2n, q)|}{C_k},$$

Note that in the A_k *sum in part (2),* k *only ranges from* 0 *to* $n - 1$, *and that the values of* B_k *and* C_k *are the same in parts (1) and (2).*

For the next result, we use Lemma 2.1 and the ideas used to prove Proposition 4.6. We note that these results can also be concluded from [9, Section 8].

Proposition 4.7. *Let* q *be even, and let* $A_k^\pm$, B_k, *and* C_k *be as in Proposition 4.6.*

(1) The number of involutions in $\Omega^+(2n, q)$ *is equal to*

$$i(\Omega^+(2n, q)) = \sum_{\substack{k=0 \\ k \ even}}^{n} \frac{|\mathrm{O}^+(2n, q)|}{A_k^+} + \sum_{\substack{k=2 \\ k \ even}}^{n} \frac{|\mathrm{O}^+(2n, q)|}{B_k}.$$

(2) The number of involutions in $\Omega^-(2n, q)$ *is equal to*

$$i(\Omega^-(2n, q)) = \sum_{\substack{k=0 \\ k \ even}}^{n-1} \frac{|\mathrm{O}^-(2n, q)|}{A_k^-} + \sum_{\substack{k=2 \\ k \ even}}^{n} \frac{|\mathrm{O}^-(2n, q)|}{B_k}.$$

(3) The number of involutions in $\mathrm{O}^\pm(2n, q) \setminus \Omega^\pm(2n, q)$ *is*

$$i(\mathrm{O}^\pm(2n, q) \setminus \Omega^\pm(2n, q)) = \sum_{\substack{k=1 \\ k \ odd}}^{n} \frac{|\mathrm{O}^\pm(2n, q)|}{C_k}.$$

Proof. In the proof of Proposition 4.6 given in [11, Theorem 5.6], the authors prove that any involution in $\mathrm{O}^\pm(2n, q)$ with q even is conjugate to an element g, given in block form as

$$g = \begin{bmatrix} I & 0 & h \\ 0 & I & 0 \\ 0 & 0 & I \end{bmatrix}.$$

If we define $k = \mathrm{rank}(h)$, then the expressions in Proposition 4.6 count the involutions by considering the possible values for k. By Lemma 2.1, the involution g is in $\Omega^\pm(2n, q)$ if and only if $\mathrm{rank}(1 + g) = \mathrm{rank}(h)$ is even. So, to count the involutions in $\Omega^\pm(2n, q)$, we only include the sums with k even from Proposition 4.6, which gives (1) and (2). The expression in (3) is the remaining sum. $\qquad\square$

5 Results on Indicators

5.1 $\mathrm{SO}^\pm(2n, q)$ with q odd

It is a result of Gow [17] that for any $n \geq 1$ and q odd, the group $\mathrm{O}^\pm(n, q)$ is totally orthogonal, as is the group $\mathrm{SO}^\pm(4m, q)$ for q odd and $m \geq 1$. We expand these results to certain twisted

11

indicators for the groups $\mathrm{SO}^{\pm}(4m+2, q)$ with q odd. We first need the following result, which essentially follows from the results of Wonenburger [39] along with the description of conjugacy classes in finite orthogonal groups due to Wall [38]. A slightly stronger version of the following result is proved in [31, Lemma 4.7], and statement (i) is proved by Gal't [13, Theorem 1], but the statements in the proposition below are also implied by the more general results of Knüppel and Thomssen [24].

Proposition 5.1. *Let q be odd, $n \geq 1$, $G = \mathrm{O}^{\pm}(2n, q)$, and $H = \mathrm{SO}^{\pm}(2n, q)$.*

  (i) Let $n = 2m$, $m \geq 1$, so $H = \mathrm{SO}^{\pm}(4m, q)$. Then H is a strongly real group.

  (ii) Let $n = 2m+1$, $m \geq 0$, so $G = \mathrm{O}^{\pm}(4m+2, q)$ and $H = \mathrm{SO}^{\pm}(4m+2, q)$. For any $h \in H$, there exists an element $t \in G \setminus H$ such that $tht^{-1} = h^{-1}$ and $t^2 = 1$.

We apply Proposition 5.1 to prove the following. The result that $\mathrm{SO}^{\pm}(4m, q)$ is totally orthogonal, already proved by Gow, is included to show how it fits into the general framework.

Theorem 5.1. *Let q be odd, $n \geq 1$, $G = \mathrm{O}^{\pm}(2n, q)$, and $H = \mathrm{SO}^{\pm}(2n, q)$. Fix an involution $s \in G \setminus H$, and define ι on H by ${}^{\iota}h = shs^{-1}$.*

  (i) Let $n = 2m$ so $H = \mathrm{SO}^{\pm}(4m, q)$. Then $\varepsilon(\psi) = 1$ and $\varepsilon_{\iota}(\psi) \geq 0$ for all $\psi \in \mathrm{Irr}(H)$.

  (ii) Let $n = 2m+1$ so $H = \mathrm{SO}^{\pm}(4m+2, q)$. Then $\varepsilon_{\iota}(\psi) = 1$ and $\varepsilon(\psi) \geq 0$ for all $\psi \in \mathrm{Irr}(H)$. In particular, the character degree sum $\sum_{\psi \in \mathrm{Irr}(H)} \psi(1)$ is given by the expression in Proposition 4.3.

Proof. As already mentioned, if q is odd, $n \geq 1$, and $G = \mathrm{O}^{\pm}(2n, q)$, it is a result of Gow [17, Theorem 1] that $\varepsilon(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$. In case (i), since H is a real group (in fact, strongly real) by Proposition 5.1(i), and $G = H\langle s \rangle$, then Lemma 2.3(i) implies statement (i).

To prove statement (ii), it suffices to prove that for all $h \in H$, ${}^{\iota}h$ is H-conjugate to h^{-1}, by Lemma 2.3(ii). Given $h \in H$, we apply Proposition 5.1 to ${}^{\iota}h \in H$, so there is some $t \in G \setminus H$ such that $t^2 = 1$ and $t({}^{\iota}h)t = {}^{\iota}h^{-1} = sh^{-1}s$. Conjugating by s on both sides yields $(st){}^{\iota}h(st)^{-1} = h^{-1}$, and since $s, t \in G \setminus H$, we have $st \in H$ and ${}^{\iota}h$ is H-conjugate to h^{-1}. By Lemma 2.2, we have

$$\sum_{\psi \in \mathrm{Irr}(H)} \psi(1) = \#\{h \in H \mid shs^{-1} = h^{-1}\}.$$

Note that since $s \in G \setminus H$, we have $sh \in G \setminus H$, and $shs^{-1} = h^{-1}$ if and only if $(sh)^2 = 1$. That is, the character degree sum is equal to the number of involutions in $G \setminus H$, which is given by Proposition 4.3. $\qquad\square$

5.2 $\mathrm{O}^{\pm}(2n, q)$ and $\Omega^{\pm}(2n, q)$ with q even

We now consider the groups $\Omega^{\pm}(4m, q)$ with q even, which we suspect to be totally orthogonal. It is further suspected that the groups $\mathrm{O}^{\pm}(2n, q)$ with q even are totally orthogonal, since they are known to be strongly real groups [10, 16], and when q is odd all of the groups $\mathrm{O}^{\pm}(N, q)$ are known to be totally orthogonal [17]. Next we relate the total orthogonality of the groups $\mathrm{O}^{\pm}(2n, q)$ with q even to indicators of the groups $\Omega^{\pm}(2n, q)$. Note the resemblance to the case when q is odd given in Theorem 5.1.

Lemma 5.1. *Let q be even, $n \geq 1$, $G = \mathrm{O}^{\pm}(2n, q)$, and $H = \Omega^{\pm}(2n, q)$. Fix an involution $s \in G \setminus H$, and define ι on H by ${}^{\iota}h = shs^{-1}$.*

(i) *Let* $n = 2m$ *so* $G = \mathrm{O}^{\pm}(4m, q)$ *and* $H = \Omega^{\pm}(4m, q)$. *If* $\varepsilon(\psi) = 1$ *for all* $\psi \in \mathrm{Irr}(H)$, *then* $\varepsilon(\chi) = 1$ *for all* $\chi \in \mathrm{Irr}(G)$ *and* $\varepsilon_\iota(\psi) \geq 0$ *for all* $\psi \in \mathrm{Irr}(H)$.

(ii) *Let* $n = 2m + 1$ *so* $G = \mathrm{O}^{\pm}(4m + 2, q)$ *and* $H = \Omega^{\pm}(4m + 2, q)$. *If* $\varepsilon_\iota(\psi) = 1$ *for all* $\psi \in \mathrm{Irr}(H)$, *then* $\varepsilon(\chi) = 1$ *for all* $\chi \in \mathrm{Irr}(G)$ *and* $\varepsilon(\psi) \geq 0$ *for all* $\psi \in \mathrm{Irr}(H)$.

Proof. Since $[G : H] = 2$ and $G = H\langle s \rangle$, we may apply Lemma 2.3. It is proved by Gow [16] and by Ellers and Nolte [10] that $G = \mathrm{O}^{\pm}(2n, q)$ is a strongly real group when q is even, and in particular G is a real group. In the case that $n = 2m$, statement (i) follows from Lemma 2.3(iii), and in the case that $n = 2m + 1$, statement (ii) follows from Lemma 2.3(iv). □

Using direct computation, we get the following results for $\Omega^{\pm}(2n, q)$ and $\mathrm{O}^{\pm}(2n, q)$ with n small.

Theorem 5.2. *Let* q *be even. Fix an involution* $s \in \mathrm{O}^{\pm}(2n, q) \setminus \Omega^{\pm}(2n, q)$, *and define* ι *on* $\Omega^{\pm}(2n, q)$ *by* ${}^{\iota}h = shs^{-1}$.

(i) *If* $n = 2m$, *and* $H = \Omega^{\pm}(4m, q)$ *with* $m \leq 3$, *or* $H = \Omega^{+}(16, q)$, *then* $\varepsilon(\psi) = 1$ *(and* $\varepsilon_\iota(\psi) \geq 0$*) for all* $\psi \in \mathrm{Irr}(H)$, *so* H *is totally orthogonal and Theorem 3.2 holds for these groups when they are simple.*

(ii) *If* $n = 2m + 1$, *and* $H = \Omega^{\pm}(4m + 2, q)$ *with* $m \leq 3$, *then* $\varepsilon_\iota(\psi) = 1$ *(and* $\varepsilon(\psi) \geq 0$*) for all* $\psi \in \mathrm{Irr}(H)$.

(iii) *If* $G = \mathrm{O}^{\pm}(2n, q)$ *with* $n \leq 7$, *or* $G = \mathrm{O}^{+}(16, q)$, *then* $\varepsilon(\chi) = 1$ *for all* $\chi \in \mathrm{Irr}(G)$, *so* G *is totally orthogonal.*

Proof. In (i), by Lemma 2.2 we have $\varepsilon(\psi) = 1$ for all $\psi \in \mathrm{Irr}(H)$ if and only if the sum of the character degrees of H is the number of involutions of $H = \Omega^{\pm}(4m, q)$, an expression for which is given in Proposition 4.7(1) and (2). In (ii), also by Lemma 2.2, we have $\varepsilon_\iota(\psi) = 1$ for all $\psi \in \mathrm{Irr}(H)$ if and only if the character degree sum of H is the number of $h \in H$ such that $h^{\iota}h = 1$. From the definition of ι, we have $h^{\iota}h = (hs)^2$, where $hs \in \mathrm{O}^{\pm}(4m+2, q)\setminus\Omega^{\pm}(4m+2, q)$. Thus the number of $h \in H$ such that $h^{\iota}h = 1$ is the number of involutions in $\mathrm{O}^{\pm}(4m+2, q)\setminus\Omega^{\pm}(4m+2, q)$, an expression for which is given in Proposition 4.7(3).

We again apply the data of Lübeck [26], who has computed all of the character degrees of $\Omega^{\pm}(2n, q)$ when q is even and $4 \leq n \leq 7$, and for $\Omega^{+}(16, q)$ when q is even, which are the groups $D_n(q)_{\mathrm{SO}}$ (for $\Omega^{+}(2n, q)$), and ${}^2D_n(q)_{\mathrm{SO}}$ (for $\Omega^{-}(2n, q)$) for $q \equiv 0 \mod 2$ in Lübeck's data. When $1 \leq n \leq 3$, we apply small rank group isomorphisms and known results.

When $n = 1$, we have by [23, Proposition 2.9.1(iii)] that $\mathrm{O}^{\pm}(2, q)$ is isomorphic to the dihedral group of order $2(q \mp 1)$, and $\Omega^{\pm}(2, q)$ is isomorphic to the cyclic subgroup of rotations of order $q \mp 1$. The number of involutions in $\mathrm{O}^{\pm}(2, q) \setminus \Omega^{\pm}(2, q)$ is thus $q \mp 1$, corresponding to the reflections of the dihedral group, which is also the sum of the degrees of the cyclic group of order $q \mp 1$. When $n = 2$, we have by [23, Proposition 2.9.1(iv) and (v)] that $\Omega^{+}(4, q) \cong \mathrm{SL}(2, q) \times \mathrm{SL}(2, q)$ (noting that q is even) and $\Omega^{-}(4, q) \cong \mathrm{SL}(2, q^2)$. It is known that $\mathrm{SL}(2, q)$ is totally orthogonal when q is even, for example by [16, Lemma 7] and [33, Lemma 6.4], and so the statement follows for $\Omega^{-}(4, q)$. The property of being totally orthogonal is preserved under taking direct products (see [27, Lemma 2.2], for example), and it follows that $\Omega^{+}(4, q)$ is also totally orthogonal. When $n = 3$, we have $\Omega^{+}(6, q) \cong \mathrm{SL}_4(q)$ and $\Omega^{-}(6, q) \cong \mathrm{SU}_4(q)$, from [23, Proposition 2.9(vii)], noting that $Z(\mathrm{SL}_4(q)) = Z(\mathrm{SU}_4(q)) = 1$ when q is even. In this case, we may compute the number of involutions in $\mathrm{O}^{\pm}(6, q) \setminus \Omega^{\pm}(6, q)$ given by Proposition 4.7(3)

and match this to the character degree sums of $\mathrm{SL}_4(q)$ and $\mathrm{SU}_4(q)$, respectively, where these character degrees are given by Lübeck's data for the groups $A_3(q)_{\mathrm{sc}}$ and $^2A_3(q)_{\mathrm{sc}}$ for q even.

For $4 \leq n \leq 8$, we compute the relevant number of involutions given in Proposition 4.7, and match this with the character degree sums obtained from Lübeck's data. The polynomial in q we obtain in each case for $2 \leq n \leq 8$ is given in the second table of the Appendix. In particular we get the statements in (i) and (ii) that $\varepsilon(\psi) = 1$ or $\varepsilon_\iota(\psi) = 1$ for all $\psi \in \mathrm{Irr}(H)$. The second claims in (i) and (ii) that $\varepsilon_\iota(\psi) \geq 0$ or $\varepsilon(\psi) \geq 0$ for all $\psi \in \mathrm{Irr}(H)$, and the statement in (iii) that the groups $\mathrm{O}^\pm(2n, q)$ are totally orthogonal, both follow from Lemma 5.1. $\qquad\square$

6 Generating Functions

In this section we give generating functions for the numbers of involutions found in Section 4. We use the following standard notation:

$$(x; y)_n = \prod_{i=1}^{n}(1 - xy^{i-1}), \quad (x; y)_\infty = \prod_{i \geq 1}(1 - xy^{i-1}) \quad \text{if} \quad |y| < 1.$$

Then we can write

$$|\mathrm{O}(2n+1, q)| = 2q^{2n^2+n}(1/q^2; 1/q^2)_n \text{ for } q \text{ odd}, \ |\mathrm{Sp}(2n, q)| = q^{2n^2+n}(1/q^2; 1/q^2)_n \text{ for } q \text{ even},$$

$$\text{and } |\mathrm{O}^\pm(2n, q)| = \frac{2q^{2n^2}}{q^n \pm 1}(1/q^2; 1/q^2)_n \text{ for any } q.$$

From the above expression for $|\mathrm{O}^-(2n, q)|$, and for the purposes of convenience in power series coefficients, we will adopt the convention that $1/|\mathrm{O}^-(0, q)| = 0$.

6.1 Groups over fields of odd characteristic

We begin with finding generating functions for the number of involutions in the groups $\mathrm{SO}^\pm(2n, q)$ for q odd. These essentially follow from computations made in [11]. We note that in this section and in Section 6.2, all radii of convergence are obtained by applying the quoted computations from [11], with the exception of Theorem 6.4.

Theorem 6.1. *For q odd and $|u| < 1/q$, we have the generating functions*

$$(1) \qquad \sum_{n \geq 0} \frac{i(\mathrm{SO}^\pm(2n, q))}{|\mathrm{O}^\pm(2n, q)|} q^{n^2} u^n = \frac{1}{2} \left[\frac{\prod_{i \geq 1}(1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-2)})} \pm \frac{\prod_{i \geq 1}(1 + u/q^{2i-1})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} \right],$$

$$(2) \qquad \sum_{n \geq 0} \frac{i(\mathrm{SO}(2n+1, q))}{|\mathrm{O}(2n+1, q)|} q^{n^2} u^n = \frac{1}{2} \frac{1}{1 - u} \frac{\prod_{i \geq 1}(1 + u/q^{2i})^2}{\prod_{i \geq 1}(1 - u^2/q^{2i})}.$$

Proof. In [11, CASE 1, Proof of Theorem 2.15], it is proved that

$$S_1^+ := \sum_{n \geq 0} u^n q^{n^2} \sum_{R=0}^{n} \frac{1}{|\mathrm{O}^+(2R, q)||\mathrm{O}^+(2n - 2R, q)|}$$

$$= \frac{1}{4} \left[\frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} + 2\frac{(-u/q; 1/q^2)_\infty(-u; 1/q^2)_\infty}{(qu^2; 1/q^2)_\infty} + \frac{(-u; 1/q^2)_\infty^2}{(q^2u^2; 1/q^2)_\infty} \right],$$

14

and in [11, CASE 3, Proof of Theorem 2.15] it is proved that

$$S_3^+ := \sum_{n \geq 0} u^n q^{n^2} \sum_{R=1}^{n-1} \frac{1}{|O^-(2R,q)||O^-(2n-2R,q)|}$$

$$= \frac{1}{4} \left[\frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} - 2 \frac{(-u/q; 1/q^2)_\infty(-u; 1/q^2)_\infty}{(qu^2; 1/q^2)_\infty} + \frac{(-u; 1/q^2)_\infty^2}{(q^2 u^2; 1/q^2)_\infty} \right].$$

By Proposition 4.2(1) and the above, we have

$$\sum_{n \geq 0} \frac{i(SO^+(2n,q))}{|O^+(2n,q)|} q^{n^2} u^n = S_1^+ + S_3^+ = \frac{1}{2} \left[\frac{(-u; 1/q^2)_\infty^2}{(q^2 u^2; 1/q^2)_\infty} + \frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} \right]$$

$$= \frac{1}{2} \left[\frac{\prod_{i \geq 1}(1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-2)})} + \frac{\prod_{i \geq 1}(1 + u/q^{2i-1})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} \right].$$

In [11, CASE 1, Proof of Theorem 2.16], it is proved that

$$S_1^- := \sum_{n \geq 0} u^n q^{n^2} \sum_{R=0}^{n-1} \frac{1}{|O^+(2R,q)||O^-(2n-2R,q)|} = \frac{1}{4} \left[\frac{(-u; 1/q^2)_\infty^2}{(q^2 u^2; 1/q^2)_\infty} - \frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} \right].$$

From this and Proposition 4.2(2), we have

$$\sum_{n \geq 0} \frac{i(SO^-(2n,q))}{|O^-(2n,q)|} q^{n^2} u^n = 2S_1^- = \frac{1}{2} \left[\frac{(-u; 1/q^2)_\infty^2}{(q^2 u^2; 1/q^2)_\infty} - \frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} \right]$$

$$= \frac{1}{2} \left[\frac{\prod_{i \geq 1}(1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-2)})} - \frac{\prod_{i \geq 1}(1 + u/q^{2i-1})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} \right],$$

which gives the result in (1).

For (2), it follows from [11, Theorem 2.17] and Proposition 4.1(3) that

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

Since $i(SO(2n+1,q)) = (1/2)i(O(2n+1,q))$ from Proposition 4.2(3), the generating function in (2) follows. $\qquad \square$

From the result of Gow stated in Theorem 5.1(1) that $SO^\pm(4m,q)$ is totally orthogonal when q is odd, the character degree sum of $SO^\pm(4m,q)$ is $|O^\pm(4m,q)|/q^{4m^2}$ times the coefficient of u^{2m} of the generating function in Theorem 6.1(1). By Theorem 5.1(2), the character degree sum of $SO^\pm(4m+2,q)$ is $|O^\pm(4m+2,q)|/q^{(2m+1)^2}$ times the coefficient of u^{2m+1} in the following generating function.

Theorem 6.2. *For q odd and $|u| < 1/q$, we have the generating function*

$$\sum_{n \geq 0} \frac{i(O^\pm(2n,q) \setminus SO^\pm(2n,q))}{|O^\pm(2n,q)|} q^{n^2} = \frac{uq}{2} \frac{\prod_{i \geq 1}(1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-2)})}.$$

15

Proof. From [11, Theorems 2.15 and 2.16], we have for q odd and $|u| < 1/q$,

$$\sum_{n \geq 0} \frac{i(\mathrm{O}^{\pm}(2n, q))}{|\mathrm{O}^{\pm}(2n, q)|} q^{n^2} u^n = \frac{1}{2(1 - uq)} \frac{\prod_{i \geq 1}(1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} \pm \frac{1}{2} \frac{\prod_{i \geq 1}(1 + u/q^{2i-1})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})}.$$

The result is obtained by taking the difference of this and the generating function in Theorem 6.1(1). □

Generating functions for the number of involutions in $\Omega^{\pm}(n, q)$ with $q \equiv 1 \pmod 4$ also follow quickly from calculations in [11], because of the convenient formula for the number of involutions in this case, given in Proposition 4.4.

Theorem 6.3. *For $q \equiv 1 \pmod 4$ and $|u| < 1/q$, we have the generating functions*

(1)
$$\sum_{n \geq 0} \frac{i(\Omega^+(2n, q))}{|\mathrm{O}^+(2n, q)|} q^{n^2} u^n$$

$$= \frac{1}{4} \left[\frac{\prod_{i \geq 1}(1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-2)})} + \frac{2 \prod_{i \geq 1}(1 + u/q^{i-1})}{\prod_{i \geq 1}(1 - u^2/q^{2i-3})} + \frac{\prod_{i \geq 1}(1 + u/q^{2i-1})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} \right],$$

(2)
$$\sum_{n \geq 0} \frac{i(\Omega^-(2n, q))}{|\mathrm{O}^-(2n, q)|} q^{n^2} u^n = \frac{1}{4} \left[\frac{\prod_{i \geq 1}(1 + u/q^{2(i-1)})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-2)})} - \frac{\prod_{i \geq 1}(1 + u/q^{2i-1})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} \right],$$

(3)
$$\sum_{n \geq 0} \frac{i(\Omega(2n + 1, q))}{|\mathrm{O}(2n + 1, q)|} q^{n^2} u^n = \frac{1}{4} \left[\frac{(1 + u) \prod_{i \geq 1}(1 + u/q^{2i})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} + \frac{\prod_{i \geq 1}(1 + u/q^i)}{\prod_{i \geq 1}(1 - u^2/q^{2i-1})} \right].$$

Proof. For (1), as in the proof of Theorem 6.1, it was proved in [11] that

$$\sum_{n \geq 0} u^n q^{n^2} \sum_{R=0}^{n} \frac{1}{|\mathrm{O}^+(2R, q)||\mathrm{O}^+(2n - 2R, q)|}$$

$$= \frac{1}{4} \left[\frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} + 2 \frac{(-u/q; 1/q^2)_\infty(-u; 1/q^2)_\infty}{(qu^2; 1/q^2)_\infty} + \frac{(-u; 1/q^2)_\infty^2}{(q^2 u^2; 1/q^2)_\infty} \right].$$

The result follows by simplifying this expression, noting that

$$(-u/q; 1/q^2)_\infty(-u; 1/q^2)_\infty = \prod_{i \geq 1}(1 + u/q^{2i-1}) \prod_{i \geq 1}(1 + u/q^{2i-2}) = \prod_{i \geq 1}(1 + u/q^{i-1}),$$

together with Proposition 4.4(1).

The generating function in (2) follows directly from Proposition 4.4(2) and Theorem 6.1(1), since $i(\Omega^-(2n, q)) = (1/2)i(\mathrm{SO}^-(2n, q))$ when $q \equiv 1 \pmod 4$.

For (3), we use the identity proved in [11, CASE 1, Proof of Theorem 2.17] that

$$\sum_{n \geq 0} u^n q^{n^2} \left[\sum_{R=0}^{n} \frac{1}{|\mathrm{O}^+(2R, q)||\mathrm{O}(2n + 1 - 2R, q)|} \right]$$

$$= \frac{1}{4} \left[\frac{(-u/q^2; 1/q^2)_\infty(-u; 1/q^2)_\infty}{(u^2; 1/q^2)_\infty} + \frac{(-u/q^2; 1/q^2)_\infty(-u/q; 1/q^2)_\infty}{(u^2/q; 1/q^2)_\infty} \right]$$

16

$$= \frac{1}{4}\left[\frac{\prod_{i\geq 1}(1+u/q^{2i})\prod_{i\geq 1}(1+u/q^{2(i-1)})}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})} + \frac{\prod_{i\geq 1}(1+u/q^{2i})\prod_{i\geq 1}(1+u/q^{2i-1})}{\prod_{i\geq 1}(1-u^2/q^{2i-1})}\right]$$

$$= \frac{1}{4}\left[\frac{(1+u)\prod_{i\geq 1}(1+u/q^{2i})^2}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})} + \frac{\prod_{i\geq 1}(1+u/q^i)}{\prod_{i\geq 1}(1-u^2/q^{2i-1})}\right].$$

The result follows by Proposition 4.4(3). $\qquad\square$

The last case that we deal with in this section, which is for $\Omega^\pm(n,q)$ with $q \equiv 3 (\mathrm{mod}\ 4)$, does not immediately follow from calculations made in [11]. We apply the q-binomial theorem and a slight variant, in the following form. A proof of the first statement is in [1, pg. 17], and the second statement is [11, Corollary 2.3].

Lemma 6.1. *If $|y| < 1$, then*

(1) $\displaystyle\sum_{n\geq 0} \frac{(A;y)_n}{(y;y)_n}x^n = \frac{(Ax;y)_\infty}{(x;y)_\infty}$, *if $|x| < 1$, and*

(2) $\displaystyle\sum_{n\geq 0} \frac{y^{\binom{n}{2}}}{(y;y)_n}x^n = \frac{1}{(-x;y)_\infty}$.

We may now prove the following.

Theorem 6.4. *Let $q \equiv 3 (\mathrm{mod}\ 4)$.*

(1) For $|u| < 1/q$, we have the generating function

$$\sum_{n\geq 0} \frac{i(\Omega^\pm(2n,q))}{|O^\pm(2n,q)|}q^{n^2}u^n = \frac{1}{4}\left[\frac{\prod_{i\geq 1}(1+u/q^{2(i-1)})^2}{\prod_{i\geq 1}(1-u^2/q^{2(i-2)})} + \frac{\prod_{i\geq 1}(1+(-1)^{i-1}u/q^{i-1})}{\prod_{i\geq 1}(1+u^2/q^{2i-3})}\right.$$
$$\left.\pm\frac{\prod_{i\geq 1}(1-(-1)^{i-1}u/q^{i-1})}{\prod_{i\geq 1}(1+u^2/q^{2i-3})} \pm \frac{\prod_{i\geq 1}(1+u/q^{2i-1})^2}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})}\right].$$

(2) For $|u| < 1$, we have the generating function

$$\sum_{n\geq 0} \frac{i(\Omega(2n+1,q))}{|O(2n+1,q)|}q^{n^2}u^n = \frac{1}{4}\left[\frac{(1+u)\prod_{i\geq 1}(1+u/q^{2i})^2}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})} + \frac{\prod_{i\geq 1}(1+(-1)^iu/q^i)}{\prod_{i\geq 1}(1+u^2/q^{2i-1})}\right].$$

Proof. For (1), by Proposition 4.5(1) and (2), we must find generating functions for

$$\sum_{n\geq 0} u^n q^{n^2}\left[\sum_{\substack{R=0\\R\ \mathrm{even}}}^{n} \frac{1}{|O^+(2R,q)||O^+(2n-2R,q)|} + \sum_{\substack{R=1\\R\ \mathrm{odd}}}^{n-1} \frac{1}{|O^-(2R,q)||O^-(2n-2R,q)|}\right]$$

and

$$\sum_{n\geq 0} u^n q^{n^2}\left[\sum_{\substack{R=0\\R\ \mathrm{even}}}^{n-1} \frac{1}{|O^+(2R,q)||O^-(2n-2R,q)|} + \sum_{\substack{R=1\\R\ \mathrm{odd}}}^{n} \frac{1}{|O^-(2R,q)||O^+(2n-2R,q)|}\right].$$

17

Consider first the sum

$$S_1 := \sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{R=0 \\ R \text{ even}}}^{n} \frac{1}{|O^+(2R,q)||O^+(2n-2R,q)|} = \sum_{n \geq 0} u^n q^{n^2} \sum_{R=0}^{\lfloor n/2 \rfloor} \frac{1}{|O^+(4R,q)||O^+(2n-4R,q)|}$$

$$= \sum_{n \geq 0} u^n q^{n^2} \sum_{R=0}^{\lfloor n/2 \rfloor} \frac{(q^{2R}+1)(q^{n-2R}+1)}{4q^{8R^2}(1/q^2;1/q^2)_{2R} \, q^{2(n-2R)^2}(1/q^2;1/q^2)_{n-2R}}$$

$$= \sum_{R \geq 0} \sum_{n \geq 0} u^n q^{n^2} \frac{(q^{2R}+1)(q^{n-2R}+1)}{4q^{8R^2}(1/q^2;1/q^2)_{2R} \, q^{2(n-2R)^2}(1/q^2;1/q^2)_{n-2R}}.$$

Now replace n by $n + 2R$ to obtain

$$S_1 = \sum_{R \geq 0} \sum_{n \geq 0} u^{n+2R} q^{(n+2R)^2} \frac{(q^{2R}+1)(q^n+1)}{4q^{8R^2}(1/q^2;1/q^2)_{2R} \, q^{2n^2}(1/q^2;1/q^2)_n}$$

$$= \sum_{R \geq 0} \sum_{n \geq 0} u^{n+2R} \frac{q^{4nR}(q^{n+2R}+q^n+q^{2R}+1)}{4q^{4R^2}(1/q^2;1/q^2)_{2R} \, q^{n^2}(1/q^2;1/q^2)_n}$$

$$= \sum_{R \geq 0} \frac{u^{2R}}{4q^{4R^2}(1/q^2;1/q^2)_{2R}} \sum_{n \geq 0} \frac{q^{2R}(uq^{4R})^n + (uq^{4R})^n + q^{2R}(uq^{4R-1})^n + (uq^{4R-1})^n}{q^{2\binom{n}{2}}(1/q^2;1/q^2)_n}.$$

Now apply Lemma 6.1(2) with $y = 1/q^2$ to each of the terms in the summation over n. This gives

$$S_1 = \sum_{R \geq 0} u^{2R} \frac{(-uq^{4R};1/q^2)_\infty (q^{2R}+1) + (-uq^{4R-1};1/q^2)_\infty (q^{2R}+1)}{4q^{4R^2}(1/q^2;1/q^2)_{2R}}.$$

We apply the facts that

$$(-uq^{4R};1/q^2)_\infty = u^{2R} q^{4R^2+2R}(-1/uq^2;1/q^2)_{2R}(-u;1/q^2)_\infty, \quad \text{and}$$

$$(-uq^{4R-1};1/q^2)_\infty = u^{2R} q^{4R^2}(-1/uq;1/q^2)_{2R}(-u/q;1/q^2)_\infty,$$

to rewrite S_1 as

$$S_1 = \frac{(-u;1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(u^2 q^2)^{2R}(-1/uq^2;1/q^2)_{2R} + (u^2 q)^{2R}(-1/uq^2;1/q^2)_{2R}}{(1/q^2;1/q^2)_{2R}}$$

$$+ \frac{(-u/q;1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(u^2 q)^{2R}(-1/uq;1/q^2)_{2R} + (u^2)^{2R}(-1/uq;1/q^2)_{2R}}{(1/q^2;1/q^2)_{2R}}. \qquad (6.1)$$

Now we consider the sum

$$T_1 := \sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{R=1 \\ R \text{ odd}}}^{n-1} \frac{1}{|O^-(2R,q)||O^-(2n-2R,q)|}$$

$$= \sum_{n \geq 1} u^n q^{n^2} \sum_{R=0}^{\lfloor (n-1)/2 \rfloor} \frac{1}{|O^-(4R+2,q)||O^-(2n-4R-2,q)|}$$

$$= \sum_{R \geq 0} \sum_{n \geq 1} u^n q^{n^2} \frac{(q^{2R+1}-1)(q^{n-2R-1}-1)}{4q^{2(2R+1)^2}(1/q^2;1/q^2)_{n-2R-1} \, q^{2(n-2R-1)^2}(1/q^2;1/q^2)_{n-2R-1}}.$$

18

Replace n with $n + 2R + 1$ to rewrite T_1 as

$$T_1 = \sum_{R \geq 0} \sum_{n \geq 0} u^{n+2R+1} q^{(n+2R+1)^2} \frac{(q^{2R+1} - 1)(q^n - 1)}{4q^{2(2R+1)^2}(1/q^2; 1/q^2)_{2R+1} q^{2n^2}(1/q^2; 1/q^2)_n}$$

$$= \sum_{R \geq 0} \frac{u^{2R+1}}{4q^{(2R+1)^2}(1/q^2; 1/q^2)_{2R+1}} \sum_{n \geq 0} \frac{q^{2R+1}(uq^{4R+2})^n - (uq^{4R+2})^n - q^{2R+1}(uq^{4R+1})^n + (uq^{4R+1})^n}{q^{2\binom{n}{2}}(1/q^2; 1/q^2)_n}.$$

As we did with S_1, we apply Lemma 6.1(2) with $y = 1/q^2$ to each term in the summation over n, and we obtain

$$T_1 = \sum_{R \geq 0} u^{2R+1} \frac{(-uq^{4R+2}; 1/q^2)_\infty (q^{2R+1} - 1) - (-uq^{4R+1}; 1/q^2)_\infty (q^{2R+1} - 1)}{4q^{(2R+1)^2}(1/q^2; 1/q^2)_{2R+1}}.$$

Now apply the identities

$$(-uq^{4R+2}; 1/q^2)_\infty = u^{2R+1} q^{(2R+1)(2R+2)}(-1/uq^2; 1/q^2)_{2R+1}(-u; 1/q^2)_\infty, \quad \text{and}$$

$$(-uq^{4R+1}; 1/q^2)_\infty = u^{2R+1} q^{(2R+1)^2}(-1/uq; 1/q^2)_{2R+1}(-u/q; 1/q^2)_\infty$$

to rewrite T_1 as

$$T_1 = \frac{(-u; 1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(u^2 q^2)^{2R+1}(-1/uq^2; 1/q^2)_{2R+1} + (-u^2 q)^{2R+1}(-1/uq^2; 1/q^2)_{2R+1}}{(1/q^2; 1/q^2)_{2R+1}}$$

$$+ \frac{(-u/q; 1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(-u^2 q)^{2R+1}(-1/uq; 1/q^2)_{2R+1} + (u^2)^{2R+1}(-1/uq; 1/q^2)_{2R+1}}{(1/q^2; 1/q^2)_{2R+1}}. \quad (6.2)$$

By combining (6.1) and (6.2) as even and odd terms, we have

$$S_1 + T_1 = \frac{(-u; 1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(-1/uq^2; 1/q^2)_R}{(1/q^2; 1/q^2)_R} \left[(u^2 q^2)^R + (-u^2 q)^R \right]$$

$$+ \frac{(-u/q; 1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(-1/uq; 1/q^2)_R}{(1/q^2; 1/q^2)_R} \left[(-u^2 q)^R + (u^2)^R \right].$$

Now apply Lemma 6.1(1) to each term in the summations over R, with $y = 1/q^2$, $A = -1/uq^2, -1/uq$, and $x = u^2 q^2, -u^2 q, -u^2$, to obtain

$$S_1 + T_1 = \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (6.3)$$

$$= \frac{1}{4} \left[\frac{(-u; 1/q^2)_\infty^2}{(u^2 q^2; 1/q^2)_\infty} + \frac{(-u; 1/q^2)_\infty (u/q; 1/q^2)_\infty + (u; 1/q^2)_\infty (-u/q; 1/q^2)_\infty}{(-u^2 q; 1/q^2)_\infty} + \frac{(-u/q; 1/q^2)_\infty^2}{(u^2; 1/q^2)_\infty} \right],$$

where $|u| < 1/q$ is the smallest radius of convergence coming from Lemma 6.1(1).

Next consider

$$S_2 := \sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{R=0 \\ R \text{ even}}}^{n-1} \frac{1}{|O^+(2R, q)||O^-(2n - 2R, q)|} = \sum_{n \geq 0} \sum_{R=0}^{\lfloor (n-1)/2 \rfloor} \frac{u^n q^{n^2}}{|O^+(4R, q)||O^-(2n - 4R, q)|}$$

$$= \sum_{R \geq 0} \sum_{n \geq 0} u^n q^{n^2} \frac{(q^{2R} + 1)(q^{n-2R} - 1)}{4q^{8R^2}(1/q^2; 1/q^2)_{2R} q^{2(n-2R)^2}(1/q^2; 1/q^2)_{n-2R}}.$$

19

We note this is the same expression we obtained for S_1, except for the $(q^{n-2R}-1)$ factor instead of $(q^{n-2R}+1)$ in the numerator. Repeating the same calculations made for S_1, while keeping track of the sign change, gives

$$S_2 = \frac{(-u;1/q^2)_\infty}{4} \sum_{R\geq 0} \frac{(u^2 q^2)^{2R}(-1/uq^2;1/q^2)_{2R} + (u^2 q)^{2R}(-1/uq^2;1/q^2)_{2R}}{(1/q^2;1/q^2)_{2R}}$$
$$- \frac{(-u/q;1/q^2)_\infty}{4} \sum_{R\geq 0} \frac{(u^2 q)^{2R}(-1/uq;1/q^2)_{2R} + (u^2)^{2R}(-1/uq;1/q^2)_{2R}}{(1/q^2;1/q^2)_{2R}}. \qquad (6.4)$$

Similarly, we consider

$$T_2 := \sum_{n\geq 0} u^n q^{n^2} \sum_{\substack{R=1 \\ R \text{ odd}}}^{n} \frac{1}{|O^-(2R,q)||O^+(2n-2R,q)|} = \sum_{n\geq 1}\sum_{R\geq 0} \frac{u^n q^{n^2}}{|O^-(4R+2,q)||O^+(2n-4R-2,q)|}$$

$$= \sum_{R\geq 0}\sum_{n\geq 1} u^n q^{n^2} \frac{(q^{2R+1}-1)(q^{n-2R-1}+1)}{4q^{2(2R+1)^2}(1/q^2;1/q^2)_{n-2R-1} \, q^{2(n-2R-1)^2}(1/q^2;1/q^2)_{n-2R-1}}.$$

We again have an expression that is almost exactly the same as T_1, except for the $(q^{n-2R-1}+1)$ factor in the numerator instead of $(q^{n-2R-1}-1)$. Following the calculation for T_1 and making the appropriate sign changes yields

$$T_2 = \frac{(-u;1/q^2)_\infty}{4} \sum_{R\geq 0} \frac{(u^2 q^2)^{2R+1}(-1/uq^2;1/q^2)_{2R+1} + (-u^2 q)^{2R+1}(-1/uq^2;1/q^2)_{2R+1}}{(1/q^2;1/q^2)_{2R+1}}$$
$$- \frac{(-u/q;1/q^2)_\infty}{4} \sum_{R\geq 0} \frac{(-u^2 q)^{2R+1}(-1/uq;1/q^2)_{2R+1} + (u^2)^{2R+1}(-1/uq;1/q^2)_{2R+1}}{(1/q^2;1/q^2)_{2R+1}}. \qquad (6.5)$$

From (6.4) and (6.5) we have

$$S_2 + T_2 = \frac{(-u;1/q^2)_\infty}{4} \sum_{R\geq 0} \frac{(-1/uq^2;1/q^2)_R}{(1/q^2;1/q^2)_R} \left[(u^2 q^2)^R + (-u^2 q)^R \right]$$
$$- \frac{(-u/q;1/q^2)_\infty}{4} \sum_{R\geq 0} \frac{(-1/uq;1/q^2)_R}{(1/q^2;1/q^2)_R} \left[(-u^2 q)^R + (u^2)^R \right].$$

Apply Lemma 6.1(1) for each term, and we have

$$S_2 + T_2 = \qquad (6.6)$$
$$= \frac{1}{4}\left[\frac{(-u;1/q^2)^2_\infty}{(u^2 q^2;1/q^2)_\infty} + \frac{(-u;1/q^2)_\infty(u/q;1/q^2)_\infty - (u;1/q^2)_\infty(-u/q;1/q^2)_\infty}{(-u^2 q;1/q^2)_\infty} - \frac{(-u/q;1/q^2)^2_\infty}{(u^2;1/q^2)_\infty} \right],$$

when $|u| < 1/q$.

Finally, the expressions (6.3) and (6.6) simplify to the generating function claimed in (1), after noticing that

$$(\mp u;1/q^2)_\infty (\pm u/q;1/q^2)_\infty = \prod_{i\geq 1}(1 \pm u/q^{2(i-1)})(1 \mp u/q^{2i-1}) = \prod_{i\geq 1}(1 \pm (-1)^{i-1}u/q^{i-1}).$$

For (2), by Proposition 4.5(3) we need the generating function for

$$\sum_{n\geq 0} u^n q^{n^2} \left[\sum_{\substack{R=0 \\ R \text{ even}}}^{n} \frac{1}{|O^+(2R,q)||O(2n+1-2R,q)|} + \sum_{\substack{R=1 \\ R \text{ odd}}}^{n} \frac{1}{|O^-(2R,q)||O(2n+1-2R,q)|} \right].$$

20

We proceed as we did in (1), and we first consider

$$S_3 := \sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{R=0 \\ R \text{ even}}}^{n} \frac{1}{|O^+(2R, q)||O(2n+1-2R, q)|} = \sum_{n \geq 0} \sum_{R=0}^{\lfloor n/2 \rfloor} \frac{u^n q^{n^2}}{|O^+(4R, q)||O(2n+1-4R, q)|}$$

$$= \sum_{R \geq 0} \sum_{n \geq 0} \frac{u^n q^{n^2}(q^{2R}+1)}{4q^{8R^2}(1/q^2; 1/q^2)_{2R} \, q^{2(n-2R)^2+(n-2R)}(1/q^2; 1/q^2)_{n-2R}}.$$

We replace n with $n + 2R$ and simplify to obtain

$$S_3 = \sum_{R \geq 0} \sum_{n \geq 0} \frac{u^{n+2R} q^{(n+2R)^2}(q^{2R}+1)}{4q^{8R^2}(1/q^2; 1/q^2)_{2R} q^{2n^2+n}(1/q^2; 1/q^2)_n}$$

$$= \sum_{R \geq 0} \frac{u^{2R}}{4q^{4R^2}(1/q^2; 1/q^2)_{2R}} \sum_{n \geq 0} \frac{q^{2R}(uq^{4R-2})^n + (uq^{4R-2})^n}{q^{2\binom{n}{2}}(1/q^2; 1/q^2)_n}.$$

By applying Lemma 6.1(2) to each term in the summation over n, we have

$$S_3 = \sum_{R \geq 0} \frac{u^{2R}(q^{2R}+1)(-uq^{4R-2}; 1/q^2)_\infty}{4q^{4R^2}(1/q^2; 1/q^2)_{2R}},$$

and from the identity

$$(-uq^{4R-2}; 1/q^2)_\infty = u^{2R} q^{2R(2R-1)}(-1/u; 1/q^2)_{2R}(-u/q^2; 1/q^2)_\infty,$$

we have

$$S_3 = \frac{(-u/q^2; 1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(u^2)^{2R}(-1/u; 1/q^2)_{2R} + (u^2/q)^{2R}(-1/u; 1/q^2)_{2R}}{(1/q^2; 1/q^2)_{2R}}. \qquad (6.7)$$

Next we consider

$$T_3 := \sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{R=1 \\ R \text{ odd}}}^{n} \frac{1}{|O^-(2R, q)||O(2n+1-2R, q)|}$$

$$= \sum_{n \geq 1} \sum_{R=0}^{\lfloor (n-1)/2 \rfloor} \frac{u^n q^{n^2}}{|O^-(4R+2, q)||O(2n-1-4R, q)|}$$

$$= \sum_{R \geq 0} \sum_{n \geq 1} \frac{u^n q^{n^2}(q^{2R+1}-1)}{4q^{8R^2}(1/q^2; 1/q^2)_{2R} \, q^{2(n-2R)^2+(n-2R)}(1/q^2; 1/q^2)_{n-2R}}.$$

We replace n with $n + 2R + 1$, and rewrite the expression to obtain

$$T_3 = \sum_{R \geq 0} \frac{u^{2R+1}}{4q^{(2R+1)^2}(1/q^2; 1/q^2)_{2R+1}} \sum_{n \geq 0} \frac{q^{2R+1}(uq^{4R})^n - (uq^{4R})^n}{q^{2\binom{n}{2}}(1/q^2; 1/q^2)_n}.$$

Apply Lemma 6.1(2) again for each term in the summation over n to get

$$T_3 = \sum_{R \geq 0} \frac{u^{2R+1}(q^{2R+1}-1)(-uq^{4R}; 1/q^2)_\infty}{4q^{(2R+1)^2}(1/q^2; 1/q^2)_{2R+1}}.$$

21

Now use the identity

$$(-uq^{4R}, 1/q^2)_\infty = u^{2R+1} q^{2R(2R+1)} (-1/u; 1/q^2)_{2R+1} (-u/q^2; 1/q^2)_\infty$$

to rewrite T_3 as

$$T_3 = \frac{(-u/q^2; 1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(u^2)^{2R+1}(-1/u; 1/q^2)_{2R+1} + (-u^2/q)^{2R+1}(-1/u; 1/q^2)_{2R+1}}{(1/q^2; 1/q^2)_{2R+1}}. \quad (6.8)$$

From (6.7) and (6.8), we have

$$S_3 + T_3 = \frac{(-u/q^2; 1/q^2)_\infty}{4} \sum_{R \geq 0} \frac{(u^2)^R(-1/u; 1/q^2)_R + (-u^2/q)^R(-1/u; 1/q^2)_R}{(1/q^2; 1/q^2)_R}.$$

Apply Lemma 6.1(1) $y = 1/q^2$, $A = -1/u$, and $x = -u^2, -u^2/q$ to the terms in the sum above to obtain

$$S_3 + T_3 = \frac{1}{4} \left[\frac{(-u/q^2; 1/q^2)_\infty (u; 1/q^2)_\infty}{(-u^2; 1/q^2)_\infty} + \frac{(-u/q^2; 1/q^2)_\infty (u/q; 1/q^2)_\infty}{(-u^2/q; 1/q^2)_\infty} \right],$$

for $|u| < 1$, which simplifies to the desired generating function. $\qquad \square$

6.2 Groups over fields of characteristic two

Theorem 6.5. *For q even and $|u| < 1/q$, we have the generating function*

$$\sum_{n \geq 0} \frac{i(\Omega^\pm(2n, q))}{|\mathrm{O}^\pm(2n, q)|} q^{n^2} u^n = \frac{1}{2} \left[\frac{\prod_{i \geq 1}(1 + u/q^{2(i-1)})}{\prod_{i \geq 1}(1 - u^2/q^{2(i-2)})} \pm \frac{\prod_{i \geq 1}(1 + u/q^{2i-1})}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} \right].$$

Proof. Let $A_k^\pm$ and B_k be as in Proposition 4.6. We use the computations made in [11, Proof of Theorem 2.18]. We have

$$\sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{k=2 \\ k \text{ even}}}^n \frac{1}{B_k} = \sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{k=0 \\ k \text{ even}}}^n \frac{1}{2 q^{k(k+1)/2 + (k-1)(2n-2k) - 1} |\mathrm{Sp}(k-2, q)| |\mathrm{Sp}(2n-2k, q)|}.$$

By substituting $2R + 2$ for k and using $|\mathrm{Sp}(2n, q)| = q^{2n^2 + n}(1/q^2; 1/q^2)_n$, an application of [11, Lemma 2.5] yields

$$\sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{k=2 \\ k \text{ even}}}^n \frac{1}{B_k}$$

$$= \frac{q^4}{2} \sum_{n \geq 0} u^n q^{n^2} \sum_{R=0}^{\lfloor (n-2)/2 \rfloor} \frac{q^{8R-2n}}{q^{4nR - 6R^2} q^{2R^2}(1/q^2; 1/q^2)_R \, q^{2(n-2R-2)^2}(1/q^2; 1/q^2)_{n-2R-2}}$$

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

Next, we have

$$\sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{k=0 \\ k \text{ even}}}^n \frac{1}{A_k^+} = \sum_{n \geq 0} u^n q^{n^2} \sum_{\substack{k=0 \\ k \text{ even}}}^n \frac{1}{q^{k(k-1)/2 + k(2n-2k)} |\mathrm{Sp}(k, q)| |\mathrm{O}^+(2n-2k, q)|}.$$

22

Again, following [11, Proof of Theorem 2.18], we use that $|O^+(2n, q)| = \frac{2q^{2n^2}}{q^n+1}(1/q^2; 1/q^2)_n$, substitute $2R$ for k to obtain

$$\sum_{n\geq 0} u^n q^{n^2} \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \frac{1}{A_k^+} = \frac{1}{2}\sum_{n\geq 0} u^n q^{n^2-n} \sum_{R=0}^{\lfloor n/2 \rfloor} \frac{q^{2n-2R} + q^n}{q^{4nR-6R^2}q^{2R^2}(1/q^2;1/q^2)_R\, q^{2(n-2R)^2}(1/q^2;1/q^2)_{n-2R}}.$$

Applying [11, Lemma 2.5] twice, once for each term in the numerator, gives us

$$\sum_{n\geq 0} u^n q^{n^2} \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \frac{1}{A_k^+} = \frac{1}{2}\frac{(-u;1/q^2)_\infty}{(u^2;1/q^2)_\infty} + \frac{1}{2}\frac{(-u/q;1/q^2)_\infty}{(u^2;1/q^2)_\infty}$$

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

For the case of A_k^- terms, we use the convention that $1/|O^-(0,q)| = 0$ so that we can apply the same computations as above, which gives

$$\sum_{n\geq 0} u^n q^{n^2} \sum_{\substack{k=0 \\ k \text{ even}}}^{n-1} \frac{1}{A_k^-} = \sum_{n\geq 0} u^n q^{n^2} \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \frac{1}{A_k^-}$$

$$= \frac{1}{2}\sum_{n\geq 0} u^n q^{n^2-n} \sum_{R=0}^{\lfloor n/2 \rfloor} \frac{q^{2n-2R} - q^n}{q^{4nR-6R^2}q^{2R^2}(1/q^2;1/q^2)_R\, q^{2(n-2R)^2}(1/q^2;1/q^2)_{n-2R}}$$

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

From all of the above, Proposition 4.7(1) and (2), and the fact that

$$\frac{u^2q^2}{2}\frac{\prod_{i\geq 1}(1+u/q^{2(i-1)})}{\prod_{i\geq 1}(1-u^2/q^{2(i-2)})} + \frac{1}{2}\frac{\prod_{i\geq 1}(1+u/q^{2(i-1)})}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})}$$

$$= \frac{u^2q^2}{2}\frac{\prod_{i\geq 1}(1+u/q^{2(i-1)})}{\prod_{i\geq 1}(1-u^2/q^{2(i-2)})} + \frac{1-u^2q^2}{2}\frac{\prod_{i\geq 1}(1+u/q^{2(i-1)})}{\prod_{i\geq 1}(1-u^2/q^{2(i-2)})} = \frac{1}{2}\frac{\prod_{i\geq 1}(1+u/q^{2(i-1)})}{\prod_{i\geq 1}(1-u^2/q^{2(i-2)})},$$

the claimed generating function follows. $\qquad\square$

We note the results in Theorem 5.2 hold for all n if and only if the character degree sum of $\Omega^\pm(4m, q)$ is $|O^\pm(4m,q)|/q^{4m^2}$ times the coefficient of u^{2m} of the generating function in Theorem 6.5, and the character degree sum of $\Omega^\pm(4m+2, q)$ is $|O^\pm(4m+2,q)|/q^{(2m+1)^2}$ times the coefficient of u^{2m+1} in the following generating function.

Theorem 6.6. *For q even and $|u| < 1/q$, we have the generating function*

$$\sum_{n\geq 0}\frac{i(O^\pm(2n,q)\setminus\Omega^\pm(2n,q))}{|O^\pm(2n,q)|}q^{n^2}u^n = \frac{uq}{2}\frac{\prod_{i\geq 1}(1+u/q^{2i-1})}{\prod_{i\geq 1}(1-u^2/q^{2(i-2)})}.$$

Proof. From [11, Theorems 2.18 and 2.19] and Proposition 4.6, we have for q even and $|u| < 1/q$,

$$\sum_{n\geq 0}\frac{i(O^\pm(2n,q))}{|O^\pm(2n,q)|}q^{n^2}u^n = \frac{1}{2(1-uq)}\frac{\prod_{i\geq 1}(1+u/q^{2(i-1)})}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})} \pm \frac{1}{2}\frac{\prod_{i\geq 1}(1+u/q^{2i-1})}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})}.$$

The result is obtained by taking the difference of this and the generating function in Theorem 6.5. $\qquad\square$

23

7 Asymptotics on Involutions

In this section, we compute the asymptotic behavior of the number of involutions in the groups $\mathrm{SO}^\pm(n,q)$ and $\Omega^\pm(n,q)$ when q is fixed and n grows. The main tool we use is the following result of Darboux, which is the same method used in [11], and which may be found in [28]. The idea is to treat the generating functions in the previous section as analytic functions, and then equate coefficients of power series. If $f(u)$ is a power series in u, then we denote by $[u^n]f(u)$ the coefficient of u^n in this power series.

Lemma 7.1. *Suppose for some $r > 0$ that $f(u)$ is analytic on $|u| < r$ and has a finite number of simple poles on $|u| = r$, denoted by w_j. Suppose we may write $f(u) = \sum_j \frac{g_j(u)}{1-u/w_j}$ with $g_j(u)$ analytic in a neighborhood of w_j. Then we have*

$$[u^n]f(u) = \sum_j \frac{g_j(w_j)}{w_j^n} + o(1/r^n).$$

The following result is implicit in [11], and follows directly from Lemma 7.1. We state it here for convenience, as it is used repeatedly.

Corollary 7.1. *If f satisfies the assumptions of Lemma 7.1 with $r > 1$, then*

$$\lim_{n\to\infty} [u^n]f(u) = 0.$$

Since the proofs of the results in this section are very similar to each other, we give all details in the first proof, and give fewer details for the proofs that follow.

7.1 Groups over fields of odd characteristic

Theorem 7.1. *If q is odd and fixed, then*

$$\lim_{m\to\infty} \frac{i(\mathrm{SO}^\pm(4m,q))}{q^{(2m)^2}} = \frac{1}{2}\left(\prod_{i\geq 1}(1+1/q^{2i-1})^2 + \prod_{i\geq 1}(1-1/q^{2i-1})^2\right),$$

and

$$\lim_{m\to\infty} \frac{i(\mathrm{SO}^\pm(4m+2,q))}{q^{(2m+1)^2}} = \frac{1}{2}\left(\prod_{i\geq 1}(1+1/q^{2i-1})^2 - \prod_{i\geq 1}(1-1/q^{2i-1})^2\right).$$

Proof. First replace u by u/q in the generating function in Theorem 6.1 to obtain

$$\sum_{n\geq 0} \frac{i(\mathrm{SO}^\pm(2n,q))}{|\mathrm{O}^\pm(2n,q)|} q^{n^2-n}u^n = \sum_{n\geq 0} u^n \frac{i(\mathrm{SO}^\pm(2n,q))}{2q^{n^2}(1\mp 1/q^n)(1-1/q^2)\cdots(1-1/q^{2(n-1)})} \tag{7.1}$$

$$= \frac{1}{2}\left[\frac{\prod_{i\geq 1}(1+u/q^{2i-1})^2}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})} \pm \frac{\prod_{i\geq 1}(1+u/q^{2i})^2}{\prod_{i\geq 1}(1-u^2/q^{2i})}\right] \tag{7.2}$$

We now consider the limit as $n \to \infty$ of the coefficient of u^n in both (7.1) and (7.2). In (7.2), first note that the second quotient of products is analytic for $|u| < q$, where $q > 1$. It follows from Corollary 7.1 that the limit as $n \to \infty$ of the coefficient of u^n in this expression is 0. The first quotient of products in (7.2) is analytic in the unit disk, and has simple poles at $u = 1$ and

24

$u = -1$ (which we take as w_1 and w_2 in applying Lemma 7.1 here). By factoring out $1/(1-u^2)$, we may rewrite this quotient of products as

$$\frac{1}{4} \frac{\prod_{i\geq 1}(1 + u/q^{2i-1})^2}{\prod_{i\geq 1}(1 - u^2/q^{2i})} \left[\frac{1}{1+u} + \frac{1}{1-u} \right],$$

where the quotient of products outside of the brackets is analytic in neighborhoods of 1 and -1 (and this expression is $g_1(u)$ and $g_2(u)$ in Lemma 7.1). By Lemma 7.1, the coefficient of u^n is

$$\frac{1}{4} \left(\frac{\prod_{i\geq 1}(1 + 1/q^{2i-1})^2 + (-1)^n \prod_{i\geq 1}(1 - 1/q^{2i-1})^2}{\prod_{i\geq 1}(1 - 1/q^{2i})} \right) + o(1).$$

If we take either $n = 2m$ or $n = 2m + 1$, this gives the limit as $m \to \infty$ of the coefficient of u^n in (7.2) to be

$$\frac{1}{4} \left(\frac{\prod_{i\geq 1}(1 + 1/q^{2i-1})^2 \pm \prod_{i\geq 1}(1 - 1/q^{2i-1})^2}{\prod_{i\geq 1}(1 - 1/q^{2i})} \right), \tag{7.3}$$

where we take $+$ if $n = 2m$ and $-$ if $n = 2m + 1$.

If we take either $n = 2m$ or $n = 2m + 1$, we compute the limit of the coefficient of u^n in (7.1) to be

$$\lim_{m\to\infty} \frac{i(\mathrm{SO}^\pm(2n,q))}{2q^{n^2}(1 \mp 1/q^n)(1 - 1/q^2)\cdots(1 - 1/q^{2(n-1)})} = \frac{1}{2\prod_{i\geq 1}(1 - 1/q^{2i})} \lim_{m\to\infty} \frac{i(\mathrm{SO}^\pm(2n,q))}{q^{n^2}(1 \mp 1/q^n)}$$

$$= \frac{1}{2\prod_{i\geq 1}(1 - 1/q^{2i})} \lim_{m\to\infty} \frac{i(\mathrm{SO}^\pm(2n,q))}{q^{n^2}} \tag{7.4}$$

Equating the expressions in (7.3) and (7.4) gives the result. $\qquad\square$

From Theorem 7.1 and the asymptotics for the number of involutions in $\mathrm{Sp}(2n,q)$ computed in [11, Theorem 5.2], we have the following interesting result that the number of involutions in $\mathrm{SO}^\pm(2n,q)$ and $\mathrm{Sp}(2n,q)$ are asymptotically equal for q odd, although the numbers of involutions in these groups are not equal in general. We note that in the case that n is odd, this result follows by dividing both sides of [11, Theorem 5.2(2)] by q.

Corollary 7.2. *Let q be odd and fixed. Then*

$$\lim_{n\to\infty} \frac{i(\mathrm{SO}^\pm(2n,q))}{i(\mathrm{Sp}(2n,q))} = 1.$$

The following is a quick result, and we include it for the sake of completeness.

Theorem 7.2. *If q is odd and fixed, then*

$$\lim_{n\to\infty} \frac{i(\mathrm{SO}(2n+1,q))}{q^{n^2+n}} = \prod_{i\geq 1}(1 + 1/q^{2i})^2.$$

Proof. We have $i(\mathrm{SO}(2n+1,q)) = (1/2)i(\mathrm{O}(2n+1,q))$ from Proposition 4.1(3). We also have from [11, Theorem 6.3] that

$$\lim_{n\to\infty} \frac{i(\mathrm{O}(2n+1,q))}{q^{n^2+n}} = 2\prod_{i\geq 1}(1 + 1/q^{2i})^2,$$

and the result follows. $\qquad\square$

We note the sign switch in the following result, in comparison with Theorem 7.1, and its relation to indicators of these groups in Theorem 5.1.

Theorem 7.3. *If q is odd and fixed, then*

$$\lim_{m\to\infty} \frac{i(\mathrm{O}^\pm(4m,q)\setminus \mathrm{SO}^\pm(4m,q))}{q^{(2m)^2}} = \frac{1}{2}\left(\prod_{i\geq 1}(1+1/q^{2i-1})^2 - \prod_{i\geq 1}(1-1/q^{2i-1})^2\right),$$

and

$$\lim_{m\to\infty} \frac{i(\mathrm{O}^\pm(4m+2,q)\setminus \mathrm{SO}^\pm(4m+2,q))}{q^{(2m+1)^2}} = \frac{1}{2}\left(\prod_{i\geq 1}(1+1/q^{2i-1})^2 + \prod_{i\geq 1}(1-1/q^{2i-1})^2\right).$$

Proof. This follows from Theorem 7.1 and the result [11, Theorem 6.2] that when q is odd and fixed,

$$\lim_{n\to\infty} \frac{i(\mathrm{O}^\pm(2n,q))}{q^{n^2}} = \prod_{i\geq 1}(1+1/q^{2i-1})^2,$$

by taking the difference. $\qquad\square$

In the next two results, we note that the asymptotics we obtain are independent of q mod 4 and the type of defining quadratic form, even though the generating functions for these cases are quite different.

Theorem 7.4. *If q is odd and fixed, then*

$$\lim_{m\to\infty} \frac{i(\Omega^\pm(4m,q))}{q^{(2m)^2}} = \frac{1}{4}\left(\prod_{i\geq 1}(1+1/q^{2i-1})^2 + \prod_{i\geq 1}(1-1/q^{2i-1})^2\right),$$

and

$$\lim_{m\to\infty} \frac{i(\Omega^\pm(4m+2,q))}{q^{(2m+1)^2}} = \frac{1}{4}\left(\prod_{i\geq 1}(1+1/q^{2i-1})^2 - \prod_{i\geq 1}(1-1/q^{2i-1})^2\right).$$

Proof. We first replace u by u/q in each of the generating functions in Theorems 6.3(1), 6.3(2), and 6.4(1). After this substitution, all products of quotients have poles with magnitude greater than 1 (with the largest in magnitude of the others being $\pm q$, $\pm\sqrt{q}$, and $\pm\sqrt{-q}$), except for the term

$$\frac{1}{4}\frac{\prod_{i\geq}(1+u/q^{2i-1})^2}{\prod_{i\geq 1}(1-u^2/q^{2(i-1)})} = \frac{1}{8}\frac{\prod_{i\geq 1}(1+u/q^{2i-1})^2}{\prod_{i\geq 1}(1-u^2/q^{2i})}\left[\frac{1}{1+u} + \frac{1}{1-u}\right],$$

which is analytic on $|u| < 1$. If $f(u)$ is any of the generating functions of interest, then we obtain from Lemma 7.1 and Corollary 7.1 that if $n = 2m$ or $n = 2m+1$, then

$$\lim_{m\to\infty}[u^n]f(u) = \frac{1}{8}\left(\frac{\prod_{i\geq 1}(1+1/q^{2i-1})^2 \pm \prod_{i\geq 1}(1-1/q^{2i-1})^2}{\prod_{i\geq 1}(1-1/q^{2i})}\right), \tag{7.5}$$

where we take $+$ if $n = 2m$ and $-$ if $n = 2m+1$.

This expression is equal to the coefficient of u^n as $n \to \infty$ of

$$\sum_{n\geq 0}\frac{i(\Omega^\pm(2n,q))}{|\mathrm{O}^\pm(2n,q)|}q^{n^2-n}u^n = \sum_{n\geq 0}u^n\frac{i(\Omega^\pm(2n,q))}{2q^{n^2}(1\mp 1/q^n)(1-1/q^2)\cdots(1-1/q^{2(n-1)})}. \tag{7.6}$$

26

Taking $n = 2m$ or $n = 2m + 1$, the limit of the coefficient of u^n as $m \to \infty$ of this is

$$\frac{1}{2 \prod_{i \geq 1}(1 - 1/q^{2i})} \lim_{m \to \infty} \frac{i(\mathrm{SO}^\pm(2n, q))}{q^{n^2}}. \tag{7.7}$$

Equating (7.5) and (7.7) gives the result. $\qquad \square$

Theorem 7.5. *If q is odd and fixed, then*

$$\lim_{n \to \infty} \frac{i(\Omega(2n + 1, q))}{q^{n^2+n}} = \frac{1}{2} \prod_{i \geq 1}(1 + 1/q^{2i})^2.$$

Proof. We consider the power series

$$\sum_{n \geq 0} \frac{i(\Omega(2n + 1, q))}{|\mathrm{O}(2n + 1, q)|} q^{n^2} u^n = \sum_{n \geq 0} u^n \frac{i(\Omega(2n + 1, q))}{2q^{n^2+n}(1 - 1/q^2) \cdots (1 - 1/q^{2n})}, \tag{7.8}$$

which is also given by the generating functions in Theorems 6.3(3) and 6.4(2). In both of those generating functions, the first product of quotients term, given by

$$\frac{1}{4} \frac{(1 + u) \prod_{i \geq 1}(1 + u/q^{2i})^2}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} = \frac{1}{4} \frac{1}{1 - u} \frac{\prod_{i \geq 1}(1 + u/q^{2i})^2}{\prod_{i \geq 1}(1 - u^2/q^{2i})},$$

has a simple pole at $u = 1$ and is analytic in $|u| < 1$. The second product of quotients in each of those generating functions has pole of smallest magnitude given by $\pm\sqrt{q}$ and $\pm\sqrt{-q}$, respectively. It follows from Lemma 7.1 and Corollary 7.1 that the limit as $n \to \infty$ of the coefficient of u^n in each of these generating functions is given by

$$\frac{1}{4} \frac{\prod_{i \geq 1}(1 + 1/q^{2i})^2}{\prod_{i \geq 1}(1 - 1/q^{2i})}. \tag{7.9}$$

Meanwhile, the limit as $n \to \infty$ of the coefficient of u^n in (7.8) is

$$\frac{1}{2 \prod_{i \geq 1}(1 - q^{2i})} \lim_{n \to \infty} \frac{i(\Omega(2n + 1, q))}{q^{n^2+n}}. \tag{7.10}$$

Equating (7.9) and (7.10) gives the result. $\qquad \square$

While we do have $i(\Omega^-(2n, q)) = (1/2)i(\mathrm{SO}^-(2n, q))$ when $q \equiv 1(\mathrm{mod}\ 4)$, in general $\Omega^\pm(n, q)$ does not have half of the number of involutions of $\mathrm{SO}^\pm(n, q)$. However, we do have this asymptotically in the following, which follows from Theorems 7.1, 7.2, 7.4, and 7.5.

Corollary 7.3. *For any fixed odd q, we have*

$$\lim_{n \to \infty} \frac{i(\Omega^\pm(n, q))}{i(\mathrm{SO}^\pm(n, q))} = \frac{1}{2}.$$

One might expect for a similar result to hold for $i(\mathrm{SO}^\pm(n, q))/i(\mathrm{O}^\pm(n, q))$. However, it follows from Theorem 7.1 and [11, Theorem 6.2] that when n is even, the limit of this expression is dependent on q.

7.2 Groups over fields of characteristic two

In our last two asymptotic results, we note the similarity to the results in Theorems 7.1 and 7.3.

Theorem 7.6. *If q is even and fixed, then*

$$\lim_{m \to \infty} \frac{i(\Omega^{\pm}(4m, q))}{q^{(2m)^2}} = \frac{1}{2} \left(\prod_{i \geq 1}(1 + 1/q^{2i-1}) + \prod_{i \geq 1}(1 - 1/q^{2i-1}) \right),$$

and

$$\lim_{m \to \infty} \frac{i(\Omega^{\pm}(4m + 2, q))}{q^{(2m+1)^2}} = \frac{1}{2} \left(\prod_{i \geq 1}(1 + 1/q^{2i-1}) - \prod_{i \geq 1}(1 - 1/q^{2i-1}) \right).$$

Proof. We replace u by u/q in Theorem 6.5 to obtain

$$\sum_{n \geq 0} \frac{i(\Omega^{\pm}(2n, q))}{|O^{\pm}(2n, q)|} q^{n^2-n} u^n = \sum_{n \geq 0} u^n \frac{i(\Omega^{\pm}(2n, q))}{2q^{n^2}(1 \mp 1/q^n)(1 - 1/q^2) \cdots (1 - 1/q^{2(n-1)})} \tag{7.11}$$

$$= \frac{1}{2} \left[\frac{\prod_{i \geq 1}(1 + u/q^{2i-1})}{\prod_{i \geq 1}(1 - u^2/q^{2(i-1)})} \pm \frac{\prod_{i \geq 1}(1 + u/q^{2i})}{\prod_{i \geq 1}(1 - u^2/q^{2i})} \right] \tag{7.12}$$

The second quotient of products in (7.12) is analytic when $|u| < q$, where $q > 1$, and so by Corollary 7.1 the limit of the coefficient of u^n in this expression as $n \to \infty$ is 0. The first quotient of products is analytic in the unit disk with simple poles at $u = 1$ and $u = -1$. We rewrite this quotient of products as

$$\frac{1}{4} \frac{\prod_{i \geq 1}(1 + u/q^{2i-1})}{\prod_{i \geq 1}(1 - u^2/q^{2i})} \left[\frac{1}{1 + u} + \frac{1}{1 - u} \right],$$

where the quotient of products outside of the brackets is analytic in neighborhoods of 1 and -1. If we take either $n = 2m$ or $n = 2m + 1$, then by Lemma 7.1, the limit as $m \to \infty$ of the coefficient of u^n in (7.12) to be

$$\frac{1}{4} \left(\frac{\prod_{i \geq 1}(1 + 1/q^{2i-1}) \pm \prod_{i \geq 1}(1 - 1/q^{2i-1})}{\prod_{i \geq 1}(1 - 1/q^{2i})} \right), \tag{7.13}$$

where we take $+$ if $n = 2m$ and $-$ if $n = 2m + 1$.

If we take either $n = 2m$ or $n = 2m + 1$, we compute the limit of the coefficient of u^n in (7.11) to be

$$\frac{1}{2 \prod_{i \geq 1}(1 - 1/q^{2i})} \lim_{m \to \infty} \frac{i(\Omega^{\pm}(2n, q))}{q^{n^2}}. \tag{7.14}$$

Equating the expressions in (7.13) and (7.14) gives the result. $\square$

Theorem 7.7. *If q is even and fixed, then*

$$\lim_{m \to \infty} \frac{i(O^{\pm}(4m, q) \setminus \Omega^{\pm}(4m, q))}{q^{(2m)^2}} = \frac{1}{2} \left(\prod_{i \geq 1}(1 + 1/q^{2i-1}) - \prod_{i \geq 1}(1 - 1/q^{2i-1}) \right),$$

and

$$\lim_{m \to \infty} \frac{i(O^{\pm}(4m + 2, q) \setminus \Omega^{\pm}(4m + 2, q))}{q^{(2m+1)^2}} = \frac{1}{2} \left(\prod_{i \geq 1}(1 + 1/q^{2i-1}) + \prod_{i \geq 1}(1 - 1/q^{2i-1}) \right).$$

28

Proof. This follows directly from Theorem 7.6, and the result [11, Theorem 6.7] that for q even and fixed,

$$\lim_{n\to\infty} \frac{i(\mathrm{O}^\pm(2n,q))}{q^{n^2}} = \prod_{i\geq 1}(1 + 1/q^{2i-1}),$$

by taking the difference. □

Appendix

The following table gives the number of involutions in either $\Omega^\pm(2n,q)$ or $\mathrm{O}^\pm(2n,q) \setminus \Omega^\pm(2n,q)$ (using Proposition 4.7), and the character degree sum (using [26]) of $\Omega^\pm(2n,q)$, for q even and the values of n needed for the proof of Theorem 5.2.

Character degree sum of	Number of involutions in	Expression
$\Omega^\pm(4,q)$	$\Omega^\pm(4,q)$	q^4
$\Omega^\pm(6,q)$	$\mathrm{O}^\pm(6,q) \setminus \Omega^\pm(6,q)$	$q^9 \mp q^6$
$\Omega^\pm(8,q)$	$\Omega^\pm(8,q)$	$q^{16} + q^{12} - q^4$
$\Omega^\pm(10,q)$	$\mathrm{O}^\pm(10,q) \setminus \Omega^\pm(10,q)$	$q^{25} + q^{21} \mp q^{20} \mp q^{16} - q^{13} \pm q^8$
$\Omega^\pm(12,q)$	$\Omega^\pm(12,q)$	$q^{36} + q^{32} + q^{30} + q^{28} - q^{22} - q^{20} - q^{18} - q^{16} + q^{10}$
$\Omega^\pm(14,q)$	$\mathrm{O}^\pm(14,q) \setminus \Omega^\pm(14,q)$	$q^{49} + q^{45} + q^{43} \mp q^{42} + q^{41} \mp q^{38} \mp q^{36} - q^{35} \mp q^{34} - q^{33} - q^{31} - q^{29} \pm q^{28} \pm q^{26} \pm q^{24} + q^{23} \pm q^{22} \mp q^{16}$
$\Omega^+(16,q)$	$\Omega^+(16,q)$	$q^{64} + q^{60} + q^{58} + 2q^{56} + q^{54} + q^{52} - q^{46} - 2q^{44} - 2q^{42} - 2q^{40} - q^{38} - q^{36} + q^{30} + q^{28} + q^{26}$

References

[1] G. Andrews, The theory of partitions, Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading, Mass.-London-Amsterdam, 1976.

[2] C. Bagiński, On sets of elements of the same order in the alternating group A_n, *Publ. Math. Debrecen* **34** (1987), no. 3-4, 313–315.

[3] M. J. J. Barry, Schur indices and ${}^3D_4(q^3)$, q odd, *J. Algebra* **117** (1988), no. 2, 522–524.

[4] R. Brauer, Representations of finite groups, In: *Lectures on Modern Mathematics, Vol. I*, pp. 133–175, Wiley, New York, 1963.

[5] D. Bump and D. Ginzburg, Generalized Frobenius-Schur numbers, *J. Algebra* **278** (2004), no. 1, 294–313.

[6] M. Cabanes and M. Enguehard, Representation theory of finite reductive groups, New Mathematical Monographs, 1, Cambridge University Press, Cambridge, 2004.

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

[8] D. Ž. Djoković, Product of two involutions, *Arch. Math. (Basel)* **18** (1967), 582–584.

[9] R. H. Dye, On the conjugacy classes of involutions of the simple orthogonal groups over perfect fields of characteristic two, *J. Algebra* **18** (1971), 414–425.

[10] E. W. Ellers and W. Nolte, Bireflectionality of orthogonal and symplectic groups, *Arch. Math. (Basel)* **39** (1982), no. 2, 113–118.

[11] J. Fulman, R. Guralnick, and D. Stanton, Asymptotics of the number of involutions in finite classical groups, *J. Group Theory* **20** (2017), no. 5, 871–902.

[12] J. Fulman and C. R. Vinroot, Generating functions for real character degree sums of finite general linear and unitary groups, *J. Algebraic Combin.* **40** (2014), no. 2, 387–416.

[13] A. A. Gal't, Strongly real elements in finite simple orthogonal groups, *Sib. Math. J.* **51** (2010), no. 2, 193–198.

[14] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.7; 2017, (http://www.gap-system.org).

[15] R. Gow, Schur indices of some groups of Lie type, *J. Algebra*, **42** (1976), no. 1, 102–120.

[16] R. Gow, Products of two involutions in classical groups of characteristic 2, *J. Algebra* **71** (1981), no. 2, 583–591.

[17] R. Gow, Real representations of the finite orthogonal and symplectic groups of odd characteristic, *J. Algebra* **96** (1985), no. 1, 249–274.

[18] L. C. Grove, Classical groups and geometric algebra, Graduate Studies in Mathematics, Vol. 39, American Mathematical Society, Providence, RI, 2002.

[19] I. M. Isaacs, Character theory of finite groups, Pure and Applied Mathematics, No. 69, Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976.

[20] G. James and A. Kerber, The representation theory of the symmetric group, Encyclopedia of Mathematics and its Applications, vol. 16, Addison-Wesley Publishing Co., Reading, Mass., 1981.

[21] D. Kaur and A. Kulshretha, Strongly real special 2-groups, *Comm. Algebra* **43** (2015), no. 3, 1176–1193.

[22] N. Kawanaka and H. Matsuyama, A twisted version of the Frobenius-Schur indicator and multiplicity-free representations, *Hokkaido Math. J.* **19** (1990), no. 3, 495–508.

[23] P. Kleidman and M. Liebeck, The subgroup structure of the finite classical groups, London Mathematical Society Lecture Note Series, 129, Cambridge University Press, Cambdridge, 1990.

[24] F. Knüppel and G. Thomsen, Involutions and commutators in orthogonal groups, *J. Austral. Math. Soc.* **65** (1998), no. 1, 1–36.

[25] S. G. Kolesnikov and Ya. N. Nuzhin, On strong reality of finite simple groups, *Acta Appl. Math.* **85** (2005), no. 1-3, 195–203.

[26] F. Lübeck, Character degrees and their multiplicities for some groups of Lie type of rank < 9, http://www.math.rwth-aachen.du/~Frank.Luebeck/chev/DegMult/index.html

[27] K. Lux, A. Schaeffer Fry, and C. R. Vinroot, Strong reality properties of normalizers of parabolic subgroups in finite Coxeter groups, *Comm. Algebra* **40** (2012), no. 8, 3056–3070.

[28] A. Odlyzko, Asymptotic enumeration methods, Chapter 22 in Handbook of Combinatorics, Volume 2, MIT Press and Elsevier, 1995.

[29] J. Ohmori, On the Schur indices of characters of finite reductive groups in bad characteristic cases, *Osaka J. Math* **40** (2003), no. 4, 1011–1019.

[30] J. Rämö, Strongly real elements of orthogonal groups in even characteristic, *J. Group Theory* **14** (2011), no. 1, 9–30.

[31] A. A. Schaeffer Fry and C. R. Vinroot, Real classes of finite special unitary groups, *J. Group Theory* **19** (2016), no. 5, 735–762.

[32] P. H. Tiep and A. E. Zalesski, Real conjugacy classes in algebraic groups and finite groups of Lie type, *J. Group Theory* **8** (2005), no. 3, 291–315.

[33] A. Turull, The Schur indices of the irreducible characters of the special linear groups, *J. Algebra* **235** (2001), no. 1, 275–314.

[34] E. P. Vdovin and A. A. Gal't, Strong reality of finite simple groups, *Sib. Math. J.* **51** (2010), no. 4, 610–615.

[35] C. R. Vinroot, Twisted Frobenius-Schur indicators of finite symplectic groups, *J. Algebra* **293** (2005), no. 1, 279–311.

[36] C. R. Vinroot, Character degree sums and real representations of finite classical groups of odd characteristic, *J. Algebra Appl.* **9** (2010), no. 4, 633–658.

[37] C. R. Vinroot, Real representations of finite symplectic groups over fields of characteristic two, Preprint, 2017, `arXiv:1708.07176`.

[38] G. E. Wall, On the conjugacy classes in the unitary, orthogonal and symplectic groups, *J. Austral. Math. Soc.* **3** (1962), 1–62.

[39] M. Wonenburger, Transformations which are products of two involutions, *J. Math. Mech.* **16** (1966), 327–338.

DEPARTMENT OF MATHEMATICS, STATISTICS, AND COMPUTER SCIENCE (MC249)
UNIVERSITY OF ILLINOIS AT CHICAGO
851 SOUTH MORGAN STREET
CHICAGO, IL 60680-7045
USA
e-mail: `gtaylo9@uic.edu`

DEPARTMENT OF MATHEMATICS
COLLEGE OF WILLIAM AND MARY
P. O. BOX 8795
WILLIAMSBURG, VA 23187-8795
USA
e-mail: `vinroot@math.wm.edu`