Finite Fields and Their Applications 17 (2011) 532–551

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A semi-recursion for the number of involutions in special orthogonal groups over finite fields

Feiqi Jiang [a], C. Ryan Vinroot [b,*]

[a] Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, MI 48109, United States
[b] Department of Mathematics, College of William and Mary, P.O. Box 8795, Williamsburg, VA 23187, United States

ARTICLE INFO

Article history:
Received 27 August 2010
Revised 21 January 2011
Accepted 27 March 2011
Available online 21 April 2011
Communicated by Zhe-Xian Wan

MSC:
05A19
05A30
20G40

Keywords:
Involutions
Special orthogonal groups over finite fields
q-binomial coefficients
Vector spaces over finite fields
Recursions
Character degree sums

ABSTRACT

Let $I(n)$ be the number of involutions in a special orthogonal group $\mathrm{SO}(n, \mathbb{F}_q)$ defined over a finite field with q elements, where q is the power of an odd prime. Then the numbers $I(n)$ form a semi-recursion, in that for $m > 1$ we have

$$I(2m+3) = \left(q^{2m+2}+1\right)I(2m+1) + q^{2m}\left(q^{2m}-1\right)I(2m-2).$$

We give a purely combinatorial proof of this result, and we apply it to give a universal bound for the character degree sum for finite classical groups defined over $\mathbb{F}_q$.

1. Introduction

An *involution* in a group G is an element $g \in G$ such that $g^2 = 1$. Involutions play an important role in finite group theory, for example, because the centralizers of involutions must be studied in the classification of finite simple groups [3]. The enumeration of specific types of involutions in finite classical groups is a well-studied problem in computational group theory [10,12]. Also, the enumeration of involutions in finite groups is related to the real representations of the group, and is equivalent to computing character degree sums of real characters in certain finite classical groups [16]. As we

* Corresponding author.
E-mail addresses: feiqij@umich.edu (F. Jiang), vinroot@math.wm.edu (C.R. Vinroot).

1071-5797/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2011.03.002

will see, counting the involutions in finite classical groups is equivalent to counting non-degenerate subspaces of the underlying finite vector spaces, the enumeration of which is a well-studied problem, see [17] for instance. The enumeration of flags of such subspaces is used in [6] to construct number-theoretic functions which are related to certain p-adic integrals.

In this paper, we study the enumeration of involutions in special orthogonal groups defined over a finite field of odd characteristic. Let $\mathbb{F}_q$ denote a finite field with q elements, where q is the power of an odd prime, and let $\mathrm{SO}(n, \mathbb{F}_q)$ denote a special orthogonal group defined over the field $\mathbb{F}_q$. There are different types of symmetric forms which can give distinct isomorphism classes of special orthogonal groups, but as we explain in Sections 2 and 3 below, the number of involutions in the group is independent of the symmetric form. The main topic we concentrate on is the following result, which relates the number of involutions in special orthogonal groups of different sizes.

Theorem 1.1. *Let q be the power of an odd prime, and let $I(n)$ denote the number of involutions in the special orthogonal group $\mathrm{SO}(n, \mathbb{F}_q)$ (of any type). Then for any $m > 1$, we have*

$$I(2m+3) = \left(q^{2m+2}+1\right)I(2m+1) + q^{2m}\left(q^{2m}-1\right)I(2m-2).$$

Theorem 1.1 was first proved by Kutler and the second-named author [9], although the original proof is by algebraic manipulation of the formulas for $I(n)$, which are given in Corollary 2.1 below. In this paper, we give a purely combinatorial proof of Theorem 1.1, which gives much more insight as to why the result “should” be true, based on the combinatorics of the involutions in special orthogonal groups over finite fields. We refer to the relationship amongst the involutions in finite special orthogonal groups given in Theorem 1.1 as a *semi-recursion*, since the odd-indexed term $I(2m+3)$ depends on the previous odd-indexed term $I(2m+1)$, but also on an even-indexed term.

There are several ways to relate Theorem 1.1 to other results. The original motivation for looking for such a result in [9] is that the number of involutions in the symmetric group forms a recursion, a result which has an elementary combinatorial proof and numerous applications [1]. Also, the number of involutions in a finite special orthogonal group is equal to the number of even-dimensional non-degenerate subspaces of the underlying vector space with a symmetric form, and so Theorem 1.1 is also a semi-recursion for the number of even-dimensional non-degenerate subspaces. The total number of subspaces of a linear vector space over a finite field is also recursive, which is a result studied by Goldman and Rota [2]. The combinatorial proof of this recursion, due to Nijenhuis, Solow and Wilf [13], gives motivation for our finding a combinatorial proof of Theorem 1.1.

This paper is organized as follows. In Section 2, we give the bijection between involutions in special orthogonal groups and even-dimensional non-degenerate subspaces, and we find formulas for the number of involutions in the finite special orthogonal groups. In the process, we notice that several expressions are equal. In particular, we note that the number of even-dimensional non-degenerate subspaces in an even-dimensional vector space over $\mathbb{F}_q$ with a symmetric form is the same as the number of ways to partition a vector space over $\mathbb{F}_{q^2}$ of half the dimension into a subspace and a complement. This fact is the key to our proof of Theorem 1.1, and so we give a combinatorial proof of it in Section 3. Also in Section 3, we give an argument which explains why the number of involutions in the finite special orthogonal groups is independent of the chosen symmetric form. In Section 4, we apply these results to give a combinatorial proof of Theorem 1.1. Finally, in Section 5, we bound the expressions for $I(n)$ by polynomials in q, and in the process apply the semi-recursion in Theorem 1.1. The main application for the obtained bounds is given in Theorem 5.1, which is a universal bound for the sum of the degrees of the irreducible characters of finite classical groups defined over a finite field with odd characteristic.

2. Involutions in finite special orthogonal groups

For any $q \neq 1$, and integers $n \geqslant k \geqslant 0$, define the *q-binomial coefficient*, denoted $\binom{n}{k}_q$, as

$$\binom{n}{k}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q-1)}{(q^k-1)\cdots(q-1)(q^{n-k}-1)\cdots(q-1)},$$

and define $\binom{n}{0}_q = 1$. The q-binomial coefficient has properties which parallel those of the classical binomial coefficient, such as the symmetric property $\binom{n}{k}_q = \binom{n}{n-k}_q$, and the q-Pascal identity $\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q$ for $k \geqslant 1$. The q-Pascal identity and induction imply that $\binom{n}{k}_q$ is a polynomial in q. We also have $\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}$. The combinatorial interpretation of the q-binomial coefficient which will be most important for us is in terms of finite vector spaces. In particular, if q is the power of a prime, and $\mathbb{F}_q$ is a finite field with q elements, then $\binom{n}{k}_q$ is exactly the number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$. For a more detailed discussion of the properties of q-binomial coefficients, see one of [2,7,15].

Unless otherwise stated, we now assume that q is the power of an odd prime. We are interested in enumerating the number of involutions in special orthogonal groups over the finite field $\mathbb{F}_q$. Beginning with the general linear group $\mathrm{GL}(n, \mathbb{F}_q)$, if g is an involution, we notice that g is diagonalizable and only has eigenvalues 1 and -1, and g is completely determined by the eigenspace E_+ for 1, and the eigenspace E_- for -1. Furthermore, if $V \cong \mathbb{F}_q^n$ is the underlying vector space, then E_+ and E_- form a direct sum decomposition of $V = E_+ \oplus E_-$. In particular, we have that the involutions in $\mathrm{GL}(n, \mathbb{F}_q)$ are in one-to-one correspondence with direct sum decompositions of $\mathbb{F}_q^n$ into two subspaces. To count such decompositions, we note that E_+ can have dimension 0 through n, and once E_+ is chosen, E_- must be a complement. If E_+ has dimension k, then there are exactly $\binom{n}{k}_q$ ways to choose it. The number of ways to choose E_- as a complement is exactly $q^{k(n-k)}$ by [14, Lemma 3]. We use this result several times throughout, the proof of which is a direct counting argument, and so we state it formally here.

Lemma 2.1. *If V is an n-dimensional vector space over $\mathbb{F}_q$, and W is a k-dimensional subspace of V, then the number of subspaces U of V such that $U \oplus W = V$ is $q^{k(n-k)}$.*

Thus, the total number of involutions in $\mathrm{GL}(n, \mathbb{F}_q)$, which we denote by $\tilde{I}(n,q)$, is exactly (see also [11, Section 1.11])

$$\tilde{I}(n,q) = \sum_{k=0}^{n} q^{k(n-k)}\binom{n}{k}_q. \tag{2.1}$$

We now consider vector spaces equipped with a non-degenerate bilinear form. In general, if V is a finite dimensional vector space over a field F of characteristic not equal to 2, and $B : V \times V \to F$ is a non-degenerate bilinear form on V which is either symmetric or skew-symmetric, we denote

$$G_B(V) = \{g \in \mathrm{GL}(V) \mid B(gv, gw) = B(v, w) \text{ for all } v, w \in V\}.$$

Recall that the bilinear form B being non-degenerate means that for all $v \in V$, $B(v, w) = 0$ for all $w \in V$ implies $v = 0$. A subspace W of V is non-degenerate if the form B when restricted to $W \times W$ is also non-degenerate. Although we are specifically interested in the case that $F = \mathbb{F}_q$ and B is symmetric, we have the following more general result.

Lemma 2.2. *Let V be a finite dimensional vector space over a field of characteristic not 2, and let B be a non-degenerate bilinear form on V which is either symmetric or skew-symmetric. Define T to be the set of involutions in $G_B(V)$, and S the set of non-degenerate subspaces of V. For an element $g \in T$, if $E_-(g)$ is the -1-eigenspace of g, then the map $g \mapsto E_-(g)$ is a bijection from T to S.*

Proof. Let $g \in T$. Let $E_+(g)$ and $E_-(g)$ denote the $+1$- and -1-eigenspaces of g, respectively. If $v \in E_+(g)$ and $w \in E_-(g)$, then

$$B(v, w) = B(gv, gw) = B(v, -w) = -B(v, w),$$

and thus $B(v, w) = 0$. This implies we have $E_+(g) \subseteq E_-(g)^\perp$. Also, since $V = E_+(g) \oplus E_-(g)$, we in fact have $E_+(g) = E_-(g)^\perp$. Now note that since we now have $E_-(g) \cap E_-(g)^\perp = \{0\}$, then $E_-(g)$ is a non-degenerate subspace of V.

Suppose that there is an element $g' \in T$ such that $E_-(g) = E_-(g')$. But then $E_+(g) = E_-(g)^\perp = E_-(g')^\perp = E_+(g')$, which implies $g = g'$. Finally, given any non-degenerate subspace $W \in S$, we have $V = W \oplus W^\perp$, and we may define a unique linear map g_W defined by $g_W w = w$ for all $w \in W$ and $g_W w' = -w'$ for all $w' \in W^\perp$. It follows that $g_W \in G_B(V)$ and $g_W^2 = I$. We now have that the map $g \mapsto E_-(g)$ is a bijection from T to S. □

Now consider the case that V is an n-dimensional vector space over $\mathbb{F}_q$, q odd, with a non-degenerate symmetric bilinear form B. Then $G_B(V) = \mathrm{O}_B(n, \mathbb{F}_q)$ is an orthogonal group over the finite field $\mathbb{F}_q$, and the special orthogonal group is $\mathrm{SO}_B(n, \mathbb{F}_q) = \{g \in \mathrm{O}_B(n, \mathbb{F}_q) \mid \det(g) = 1\}$. Recall [5, Chapter 9] that under the relation of similarity, there are exactly two equivalence classes of non-degenerate symmetric forms on V. In the case that n is odd, the two classes of forms are represented by the symmetric matrices $\mathrm{diag}(1, -1, 1, \dots, 1, -1, -1)$ and $\mathrm{diag}(1, -1, 1, \dots, -1, -d)$, where d is a non-square in $\mathbb{F}_q$, and when n is even, the two classes are represented by $\mathrm{diag}(1, -1, \dots, 1, -1)$, and $\mathrm{diag}(1, -1, \dots, 1, -d)$, where d is a non-square in $\mathbb{F}_q$. We will call these two types of forms $+$-type and $-$-type (also called *split* and *non-split*), and the corresponding orthogonal groups will be denoted as $\mathrm{O}^+(n, \mathbb{F}_q)$ and $\mathrm{O}^-(n, \mathbb{F}_q)$, respectively, and the special orthogonal groups as $\mathrm{SO}^+(n, \mathbb{F}_q)$ and $\mathrm{SO}^-(n, \mathbb{F}_q)$. When $n = 2m + 1$ is odd, then we in fact have $\mathrm{O}^+(n, \mathbb{F}_q) \cong \mathrm{O}^-(n, \mathbb{F}_q)$ and $\mathrm{SO}^+(n, \mathbb{F}_q) \cong \mathrm{SO}^-(n, \mathbb{F}_q)$, and we will often denote the common groups as $\mathrm{O}(2m+1, \mathbb{F}_q)$ and $\mathrm{SO}(2m+1, \mathbb{F}_q)$.

We now give an expression for the number of non-degenerate subspaces in an $\mathbb{F}_q$-vector space with a non-degenerate symmetric form. Since the following is also stated in [6, Section 4], and the enumeration of various types of subspaces is thoroughly studied in [17], we omit the proof.

Proposition 2.1. *Let V be an n-dimensional vector space over $\mathbb{F}_q$, with a non-degenerate symmetric form B, and let j be an integer,* $0 \leqslant j \leqslant n$.

(i) *If B is a $+$-type symmetric form, then the number of non-degenerate subspaces of V of dimension j is*

$$\frac{|\mathrm{O}^+(n, \mathbb{F}_q)|}{|\mathrm{O}^+(j, \mathbb{F}_q)| \cdot |\mathrm{O}^+(n-j, \mathbb{F}_q)|} + \frac{|\mathrm{O}^+(n, \mathbb{F}_q)|}{|\mathrm{O}^-(j, \mathbb{F}_q)| \cdot |\mathrm{O}^-(n-j, \mathbb{F}_q)|}.$$

(ii) *If B is a $-$-type symmetric form, then the number of non-degenerate subspaces of V of dimension j is*

$$\frac{|\mathrm{O}^-(n, \mathbb{F}_q)|}{|\mathrm{O}^+(j, \mathbb{F}_q)| \cdot |\mathrm{O}^-(n-j, \mathbb{F}_q)|} + \frac{|\mathrm{O}^-(n, \mathbb{F}_q)|}{|\mathrm{O}^-(j, \mathbb{F}_q)| \cdot |\mathrm{O}^+(n-j, \mathbb{F}_q)|}.$$

Now let $A(m, k)$ denote the number of $2k$-dimensional non-degenerate subspaces of a $(2m+1)$-dimensional $\mathbb{F}_q$-vector space V with a non-degenerate symmetric form, and let $B^\pm(m, k)$ denote the number of $2k$-dimensional non-degenerate subspaces of a $2m$-dimensional $\mathbb{F}_q$-vector space V with a non-degenerate symmetric form of $\pm$-type, respectively. Despite the similarity in notation for the quantity $B^\pm(m, k)$ and the bilinear form B, we trust that context will keep these from being confused. Using the results above, we may now count the number of involutions in the finite special orthogonal groups. Although the following is also computed in a slightly different way in [16], we give one computation below to highlight the origin of the q^2-binomial coefficient which appears.

Corollary 2.1. *Let $I(2m+1)$ denote the number of involutions in the special orthogonal group $\mathrm{SO}(2m+1, \mathbb{F}_q)$, $I^+(2m)$ the number of involutions in the group $\mathrm{SO}^+(2m, \mathbb{F}_q)$, and $I^-(2m)$ the number of involutions in the group $\mathrm{SO}^-(2m, \mathbb{F}_q)$. Then:*

(i) *$I(2m+1) = \sum_{k=0}^{m} A(m,k)$, where $A(m,k) = q^{2k(m+1-k)}\binom{m}{k}_{q^2}$.*

(ii) *$I^+(2m) = \sum_{k=0}^{m} B^+(m,k)$ and $I^-(2m) = \sum_{k=0}^{m} B^-(m,k)$, where $B^+(m,k) = B^-(m,k) = q^{2k(m-k)}\binom{m}{k}_{q^2}$. In particular, $I^+(2m) = I^-(2m)$.*

Proof. By Lemma 2.2, the number of involutions in a finite orthogonal group is equal to the number of non-degenerate subspaces of the underlying space. For an involution to be in the special orthogonal group, the element must have determinant 1, and so the -1-eigenspace must have even dimension. To compute the number of even-dimensional non-degenerate subspaces, we apply Proposition 2.1, and use the values for the orders of the finite orthogonal groups [5, Theorem 9.11]. We give one such computation, and the rest are very similar.

To compute $B^+(m,k)$, for example, we use $|\mathrm{O}^{\pm}(2k,\mathbb{F}_q)| = 2q^{k(k-1)}(q^k \mp 1)\prod_{i=1}^{k-1}(q^{2i}-1)$. From Proposition 2.1, we have

$$\begin{aligned}
B^+(m,k) &= \frac{|\mathrm{O}^+(2m,\mathbb{F}_q)|}{|\mathrm{O}^+(2k,\mathbb{F}_q)|\cdot|\mathrm{O}^+(2(m-k),\mathbb{F}_q)|} + \frac{|\mathrm{O}^+(2m,\mathbb{F}_q)|}{|\mathrm{O}^-(2k,\mathbb{F}_q)|\cdot|\mathrm{O}^-(2(m-k),\mathbb{F}_q)|} \\
&= \frac{2q^{m(m-1)}(q^m-1)\prod_{i=1}^{m-1}(q^{2i}-1)}{(2q^{k(k-1)}(q^k-1)\prod_{i=1}^{k-1}(q^{2i}-1))(2q^{(m-k)(m-k-1)}(q^{m-k}-1)\prod_{i=1}^{m-k-1}(q^{2i}-1))} \\
&\quad + \frac{2q^{m(m-1)}(q^m-1)\prod_{i=1}^{m-1}(q^{2i}-1)}{(2q^{k(k-1)}(q^k+1)\prod_{i=1}^{k-1}(q^{2i}-1))(2q^{(m-k)(m-k-1)}(q^{m-k}+1)\prod_{i=1}^{m-k-1}(q^{2i}-1))} \\
&= \frac{q^{2k(m-k)}(q^m-1)\prod_{i=1}^{m-1}(q^{2i}-1)}{2\prod_{i=1}^{k-1}(q^{2i}-1)\prod_{i=1}^{m-k-1}(q^{2i}-1)}\left(\frac{2(q^m+1)}{(q^{2k}-1)(q^{2(m-k)}-1)}\right) \\
&= q^{2k(m-k)}\frac{\prod_{i=1}^{m}(q^{2i}-1)}{\prod_{i=1}^{k}(q^{2i}-1)\prod_{i=1}^{m-k}(q^{2i}-1)} = q^{2k(m-k)}\binom{m}{k}_{q^2},
\end{aligned}$$

from the formula for the q^2-binomial coefficient. □

We note that it seems to be a coincidence that $I^+(2m) = I^-(2m)$ (the common quantity will be denoted $I(2m)$), and that $B^+(m,k) = B^-(m,k)$, which comes from the calculations in Corollary 2.1. In particular, we have that the number of $2k$-dimensional non-degenerate subspaces of a $2m$-dimensional vector space over $\mathbb{F}_q$ with a symmetric form B is the same whether B is $+$- or $-$-type.

A seeming coincidence which is more striking is that the number of involutions $\tilde{I}(m,q^2)$ in the finite general linear group $\mathrm{GL}(m,\mathbb{F}_{q^2})$, given in (2.1), is equal to the number of involutions $I(2m)$ in the groups $\mathrm{SO}^{\pm}(2m,\mathbb{F}_q)$, which comes from the q^2-binomial coefficient popping up at the end of the calculation in Corollary 2.1. In particular, the number of ways to choose a k-dimensional subspace of an m-dimensional vector space over $\mathbb{F}_{q^2}$, together with an $(m-k)$-dimensional complementary subspace, is equal to the number of ways to choose a $2k$-dimensional non-degenerate subspace of a $2m$-dimensional vector space over $\mathbb{F}_q$ with a non-degenerate symmetric form, the common quantity being $q^{2k(m-k)}\binom{m}{k}_{q^2}$. In the next section, we give explanations as to why these equalities are not merely coincidental.

Just as the quantities $B^{\pm}(m,k)$ have an interpretation in terms of $\mathbb{F}_{q^2}$-linear spaces, so does the quantity $A(m,k)$. If U is an $(m+1)$-dimensional vector space over $\mathbb{F}_{q^2}$ with U' a fixed m-dimensional subspace, the number of k-dimensional subspaces of U' is $\binom{m}{k}_{q^2}$, and the number of $(m+1-k)$-dimensional complements of this subspace in U is $q^{2k(m+1-k)}$ by Lemma 2.1. That is, the number of ways to choose a k-dimensional subspace of U', together with a complementary subspace in U, is exactly $A(m,k)$. We will prove this correspondence in a different way when we use it in our combinatorial proof of Theorem 1.1.

3. Correspondences between sets of involutions

As in the previous section, we let $B^+(m,k)$ and $B^-(m,k)$ denote the number of $2k$-dimensional non-degenerate subspaces of a $2n$-dimensional vector space over $\mathbb{F}_q$ with a non-degenerate symmetric form which is of $+$-type and $-$-type, respectively. These are also the number of involutions in $\mathrm{SO}^+(2m,\mathbb{F}_q)$ and $\mathrm{SO}^-(2m,\mathbb{F}_q)$, respectively, with a $2k$-dimensional -1-eigenspace. We let $\tilde{B}(m,k)$ denote the number of k-dimensional subspaces, together with an $(m-k)$-dimensional complementary subspace, of an m-dimensional vector space over $\mathbb{F}_{q^2}$. This is the number of involutions in $\mathrm{GL}(m,\mathbb{F}_{q^2})$ with a k-dimensional -1-eigenspace. As discussed in Corollary 2.1 and the paragraphs which followed, we have $B^+(m,k)=B^-(m,k)=\tilde{B}(m,k)$, which came from directly computing each quantity. The goal in this section is to prove these equalities in another way, without directly counting them, so as to explain them from a more bijective point of view. So, in this section, we ignore the fact that we have formulas for each of these quantities, and give combinatorial proofs of our results. Although our proofs that $B^+(m,k)=B^-(m,k)=\tilde{B}(m,k)$ in Theorems 3.1 and 3.2 are not completely bijective, they do give a more combinatorially satisfying explanation of these equalities than the incidental observation that their formulas are the same.

3.1. $B^+(m,k)=B^-(m,k)$

First, we deal with the equality $B^+(m,k)=B^-(m,k)$. We begin with a technical lemma. For any $\mathbb{F}_q$-vector space V with a symmetric form B, and any $a\in\mathbb{F}_q$, define $\mathcal{S}_a(V)=\{v\in V \mid B(v,v)=a\}$.

Lemma 3.1. *Let V be a $2m$-dimensional $\mathbb{F}_q$-vector space with symmetric form B. For any $a\in\mathbb{F}_q$ and any non-square $d\in\mathbb{F}_q$, there exists a linear automorphism of V which restricts to a bijection from $\mathcal{S}_b(V)$ to $\mathcal{S}_{db}(V)$.*

Proof. Let $v_1,v_2,\ldots,v_{2m}$ be a basis of V such that the representation of B relative to this basis is $\mathrm{diag}(a_1,a_2,\ldots,a_{2m})$ (see [5, Theorem 4.2]). Define B' to be another symmetric form on V such that the representation of B' relative to $v_1,v_2,\ldots,v_{2m}$ is $\mathrm{diag}(da_1,da_2,\ldots,da_{2m})$, where d is a fixed non-square in $\mathbb{F}_q$. Note that B and B' are equivalent forms on V since

$$\frac{\det(\mathrm{diag}(da_1,da_2,\ldots,da_{2m}))}{\det(\mathrm{diag}(a_1,a_2,\ldots,a_{2m}))}=d^{2m},$$

which is a perfect square (see [5, Corollary 4.10]). It follows that there exists a linear isomorphism $\delta: V\to V$ with $B'(v,w)=B(\delta(v),\delta(w))$ (so δ is an isometry with respect to B' and B). If $v\in\mathcal{S}_b(V)$, so $B(v,v)=b$, then $B'(v,v)=db$. It follows that $B(\delta(v),\delta(v))=B'(v,v)=db$, so $\delta(v)\in\mathcal{S}_{db}(V)$. Hence the image of δ restricted to $\mathcal{S}_b(V)$ is contained in $\mathcal{S}_{db}(V)$. Similarly, the image of δ^{-1} restricted to $\mathcal{S}_{db}(V)$ is contained in $\mathcal{S}_b(V)$, since $B(v,v)=B'(\delta^{-1}(v),\delta^{-1}(v))=db$, or $B(\delta^{-1}(v),\delta^{-1}(v))=b$. Both δ and δ^{-1} are injective maps, and so δ restricted to $\mathcal{S}_b(V)$ gives the desired bijection. □

Our proof that $B^+(m,k)=B^-(m,k)$, in the end, will be an induction argument, and the main work occurs with $k=1$ below.

Lemma 3.2. *For any $m\geqslant 1$, $B^+(m,1)=B^-(m,1)$, given by a bijection constructed below.*

Proof. Let V and W be $2m$-dimensional $\mathbb{F}_q$-vector spaces, with non-degenerate symmetric forms B and B', respectively. Let $v_1,v_2,\ldots,v_{2m}$ and $w_1,w_2,\ldots,w_{2m}$ be bases of V and W respectively, so that the representation of B with respect to $v_1,v_2,\ldots,v_{2m}$ is $\mathrm{diag}(1,-1,1,-1,\ldots,1,-d)$ and the representation of B' with respect to $w_1,w_2,\ldots,w_{2m}$ is $\mathrm{diag}(1,-1,\ldots,1,-1)$, where d is non-square in $\mathbb{F}_q$. Then B and B' are $-$-type and $+$-type symmetric forms, respectively. We wish to construct a bijection from the set of all 2-dimensional non-degenerate subspaces of V to the set of all 2-dimensional non-degenerate subspaces of W.

Let $V' = \operatorname{span}(v_1, v_2, \dots, v_{2m-1})$ and $W' = \operatorname{span}(w_1, w_2, \dots, w_{2m-1})$. The map $\varphi : V' \to W'$ defined by $\varphi(v_i) = w_i$ is an isometry with respect to B and B' restricted to V' and W', respectively. We may expand φ to a linear isomorphism $\overline{\varphi} : V \to W$ by defining $\overline{\varphi}(v_{2m}) = w_{2m}$. We define ψ piecewise in three cases. If X is a 2-dimensional non-degenerate subspace of V', we define $\psi(X)$ to be the subspace $\varphi(X)$ of W', which must also be non-degenerate since φ is an isometry. Now assume that X is a 2-dimensional non-degenerate subspace of V which is not contained in V'. It follows that $\dim(X \cap V') = 1$, and let $X \cap V' = \operatorname{span}(x_1)$. There are now two cases to consider: either $B(x_1, x_1) \neq 0$ or $B(x_1, x_1) = 0$.

If $B(x_1, x_1) = 0$, then we define $\psi(X) := \overline{\varphi}(X)$. Since X is non-degenerate, there exists an $x' \in X$ such that $B(x_1, x') \neq 0$. We know then that x' and x_1 are linearly independent, and we may assume $x' = x'' + v_{2m}$ for some $x'' \in V'$, by replacing x' by a scalar multiple. This implies that $B(x_1, x'') = B(x_1, x') \neq 0$. Now, $\overline{\varphi}(x') = \varphi(x'') + w_{2m}$, and $B'(\varphi(x_1), \varphi(x'') + w_{2m}) = B'(\varphi(x_1), \varphi(x'')) = B(x_1, x'') \neq 0$. The restriction of B' to $\overline{\varphi}(X)$ can be represented by the matrix

$$\begin{pmatrix} 0 & B(x_1, x'') \\ B(x_1, x'') & B(x'', x'') \end{pmatrix}$$

relative to the basis $\overline{\varphi}(x_1), \overline{\varphi}(x')$. Since this matrix has nonzero determinant, $\psi(X) = \overline{\varphi}(X)$ is non-degenerate. Note that thus far, ψ is injective since $\overline{\varphi}$ is.

If $B(x_1, x_1) \neq 0$, then consider $\operatorname{span}(x_1)^{\perp} \cap X$, which is a 1-dimensional non-degenerate subspace of X, so let x be a nonzero element in $\operatorname{span}(x_1)^{\perp} \cap X$. By replacing x by a scalar multiple, we may assume $x = x_2 + v_{2m}$ for some $x_2 \in V'$, and x_2 is uniquely determined in this way. Then $X = \operatorname{span}(x_1, x_2 + v_{2m})$ and $B(x_1, x_2 + v_{2m}) = 0$, which implies $B(x_1, x_2) = 0$, or $x_2 \in \operatorname{span}(x_1)^{\perp} \cap V'$. Note also that $B(x_2, x_2) \neq d$ since $B(v_{2m}, v_{2m}) = -d$ and $B(x_2 + v_{2m}, x_2 + v_{2m}) \neq 0$. Since $\operatorname{span}(\varphi(x_1))^{\perp} \cap W'$ is $(2m-2)$-dimensional and $d \in \mathbb{F}_q$ is a non-square, by Lemma 3.1 there exists a linear automorphism δ_{x_1} of $\operatorname{span}(\varphi(x_1))^{\perp} \cap W'$ which restricts to a bijection from $\mathcal{S}_1(\operatorname{span}(\varphi(x_1))^{\perp} \cap W')$ to $\mathcal{S}_d(\operatorname{span}(\varphi(x_1))^{\perp} \cap W')$. We now define $\psi(X)$ as follows:

$$\psi(X) := \begin{cases} \operatorname{span}(\varphi(x_1), \varphi(x_2) + w_{2m}) & \text{if } B(x_2, x_2) \neq 1, \\ \operatorname{span}(\varphi(x_1), \delta_{x_1}(\varphi(x_2)) + w_{2m}) & \text{if } B(x_2, x_2) = 1. \end{cases}$$

In the first case, $B'(\varphi(x_2) + w_{2m}, \varphi(x_2) + w_{2m}) \neq 0$, since $B'(\varphi(x_2), w_2) = 0$, $B'(w_{2m}, w_{2m}) = -1$, and $B'(\varphi(x_2), \varphi(x_2)) = B(x_2, x_2) \neq 1$. Since $B'(\varphi(x_1), \varphi(x_2) + w_{2m}) = 0$, we have $\psi(X)$ is non-degenerate. In the second case, $B'(\delta_{x_1}(\varphi(x_2)) + w_{2m}, \delta_{x_1}(\varphi(x_2)) + w_{2m}) = d - 1 \neq 0$ since d is a non-square, and so we have $\psi(X)$ is always non-degenerate. The injectivity of ψ for this case follows from the linearity of φ and δ_{x_1}, and the fact that $B(x_2, x_2) \neq d$. Note that in the case $B(x_2, x_2) \neq 1$ above, we have defined $\psi(X) = \overline{\varphi}(X)$.

We have seen ψ is an injective map from 2-dimensional non-degenerate subspaces of V to 2-dimensional non-degenerate subspaces of W. To see that ψ is surjective, we notice that any 2-dimensional non-degenerate subspace Y of W is either contained in W', or $Y \cap W' = \operatorname{span}(y_1)$ for some y_1. Any $Y \subset W'$ is in the image of ψ since φ is an isometry, and if $B'(y_1, y_1) = 0$, then $\overline{\varphi}^{-1}(Y)$ is a non-degenerate subspace of V follows from a similar argument that $\overline{\varphi}(X)$ is non-degenerate above. Finally, if $B'(y_1, y_1) \neq 0$, then $Y = \operatorname{span}(y_1, y_2 + w_{2m})$ for a uniquely determined $y_2 \in W'$ such that $B'(y_2, y_2) \neq 1$. Then $y_2 = \varphi(x_2)$ or $y_2 = \delta_{\varphi^{-1}(y_1)}(\varphi(x_2))$, for some $x_2 \in V$ as above, and ψ is surjective, and thus a bijection as required. □

We are now able to prove the equality of interest.

Theorem 3.1. *For any $m \geqslant k \geqslant 0$, $B^{+}(m, k) = B^{-}(m, k)$.*

Proof. When $k = 0$, the only non-degenerate subspace is the trivial subspace, and so $B^{+}(m, 0) = B^{-}(m, 0)$ for all $m \geqslant 0$. In Lemma 3.2, we proved the statement for all $m \geqslant 1$ when $k = 1$, and so we will use $B(m, 1)$ to denote either $B^{+}(m, 1)$ or $B^{-}(m, 1)$. Now fix any $k > 1$, and we will prove by induction on m that $B^+(m,k) = B^-(m,k)$ for any $m \geqslant k$. For the base case of $m = k$, the only non-degenerate subspace of dimension $2m$ is the space itself, and so $B^+(k,k) = B^-(k,k)$. Now we assume that $B^+(m,k) = B^-(m,k)$ for some $m \geqslant k$, and we will use $B(m,k)$ for either quantity when we do not have to distinguish between the two types.

Let V be a $(2m+2)$-dimensional $\mathbb{F}_q$-vector space with a non-degenerate symmetric form of $+$-type. Now, choosing a $2m$-dimensional non-degenerate subspace of V is equivalent to choosing its 2-dimensional non-degenerate orthogonal complement, and thus $B^+(m+1,m) = B^+(m+1,1) = B(m+1,1)$, and so there are $B(m+1,1)$ non-degenerate subspaces of V of dimension $2m$. For each $2m$-dimensional subspace V' of V, there are $B(m,k)$ non-degenerate subspaces of V' of dimension $2k$, since by the inductive hypothesis, the number of these subspaces does not depend on the type of non-degenerate subspace V'. Now we will show that each $2k$-dimensional non-degenerate subspace of V is contained in exactly $B(m-k+1,1)$ non-degenerate subspaces of dimension $2m$. Given a $2k$-dimensional non-degenerate subspace $W \subset V$, $W^\perp$ is $2(m-k+1)$-dimensional, so there are $B(m-k+1,1)$ non-degenerate subspaces of $W^\perp$ of dimension $2(m-k)$. For each such non-degenerate subspace U of $W^\perp$, $W \oplus U$ is a non-degenerate subspace of dimension $2m$ which contains W, and any such subspace containing W must be of this form. Therefore, $B^+(m+1,k) = B(m+1,1)B(m,k)/B(m-k+1,1)$. By a completely parallel argument we also obtain $B^-(m+1,k) = B(m+1,1)B(m,k)/B(m-k+1,1)$. Thus $B^+(m+1,k) = B^-(m+1,k)$, which completes the induction. □

From now on, we will let $B(m,k)$ denote both $B^+(m,k)$ and $B^-(m,k)$, and we let $I(m) = \sum_{k=0}^{m} B(m,k)$ denote the total number of involutions in either of the groups $\mathrm{SO}^\pm(2m, \mathbb{F}_q)$.

3.2. $B(m,k) = \tilde{B}(m,k)$

We now turn to our combinatorial proof of the equality $B(m,k) = \tilde{B}(m,k)$, where $\tilde{B}(m,k)$ is the number of pairs (U_1,U_2) of subspaces of an m-dimensional $\mathbb{F}_{q^2}$-vector space W, such that $\dim(U_1) = k$ and $U_1 \oplus U_2 = W$, so $\dim(U_2) = m-k$, and U_2 is a complementary subspace to U_1. Our argument has similar structure to the one in Section 3.1, in that the proof that $B(m,k) = \tilde{B}(m,k)$ in the end will be by induction, and the main work is in proving that $B(m,1) = \tilde{B}(m,1)$.

Before a technical lemma, we establish some notation. In the vector space $\mathbb{F}_q^{2m+1}$, let $\mathcal{X}_m$ denote the subspace of all vectors with first coordinate 0, and let $\mathcal{X}_m^* = \mathbb{F}_q^{2m+1} \setminus \mathcal{X}_m$ denote the set of all vectors with nonzero first coordinate. If V is any $\mathbb{F}_q$-vector space with non-degenerate symmetric form B, then let $\mathcal{S}_0(V) = \{v \in V \mid B(v,v) = 0\}$ as in Lemma 3.1, and let $\mathcal{S}_0(V)^* = V \setminus \mathcal{S}_0(V)$.

Lemma 3.3. *Let V be a $(2m+1)$-dimensional $\mathbb{F}_q$-vector space with non-degenerate symmetric form B. Then there exists a bijection $\phi : V \to \mathbb{F}_q^{2m+1}$, constructed below, such that $\phi(\mathcal{S}_0(V)) = \mathcal{X}_m$ and $\phi(\mathcal{S}_0(V)^*) = \mathcal{X}_m^*$.*

Proof. Let $x_1, x_2, \ldots, x_{2m+1}$ be a basis of V such that the symmetric form B may be represented by the matrix $\mathrm{diag}(c_1, c_2, \ldots, c_{2m+1})$. For any $v \in V$, if $v = \sum_{i=1}^{2m+1} a_i x_i$, then define a linear map $\gamma : V \to \mathbb{F}_q^{2m}$ by $\gamma(v) = (a_1, a_2, \ldots, a_{2m})$.

Now consider another symmetric form on V which can be represented with respect to the basis $x_1, x_2, \ldots, x_{2m+1}$ by $\mathrm{diag}(dc_1, dc_2, \ldots, dc_{2m+1})$, for some fixed non-square $d \in \mathbb{F}_q$. Note that $B'(v,w) = dB(v,w)$ for any $v, w \in V$. If we restrict B and B' to $V' = \mathrm{span}(x_1, \ldots, x_{2m})$, then as in Lemma 3.1, $B|_{V'}$ and $B'|_{V'}$ are equivalent forms. Thus, there exists a linear automorphism L of V' such that $B'(v,w) = B(L(v), L(w))$ for all $v, w \in V'$.

Fix a set $J \subset \mathbb{F}_q^\times$ such that $a \in J$ if and only if $-a \notin J$. We define the desired $\phi : V \to \mathbb{F}_q^{2m+1}$ as follows. If $v \in V$ with $v = \sum_{i=1}^{2m+1} a_i x_i$, then define

$$\phi(v) := \begin{cases} (B(v,v), a_1, a_2, \ldots, a_{2m}) & \text{if } a_{2m+1} \in J \cup \{0\}, \\ (dB(v,v), \gamma \circ L(v - a_{2m+1}x_{2m+1})) & \text{if } a_{2m+1} \notin J \cup \{0\}. \end{cases}$$

It follows immediately that $\phi(\mathcal{S}_0(V)) \subseteq \mathcal{X}_m$ and $\phi(\mathcal{S}_0(V)^*) \subseteq \mathcal{X}_m^*$. Since $|V| = |\mathbb{F}_q^{2m+1}|$, to check that ϕ is a bijection, it is enough to check that it is injective.

Suppose that $v, w \in V$ and $\phi(v) = \phi(w)$, and let $v = \sum_{i=1}^{2m+1} a_i x_i$ and $w = \sum_{i=1}^{2m+1} b_i x_i$. If either $a_{2m+1}, b_{2m+1} \in J \cup \{0\}$ or $a_{2m+1}, b_{2m+1} \notin J \cup \{0\}$, then by considering the last $2m$ coordinates of $\phi(v) = \phi(w)$, we obtain $a_i = b_i$ for $i < 2m+1$. By equating the first coordinate of $\phi(v) = \phi(w)$, we find $a_{2m+1}^2 = b_{2m+1}^2$, and it follows that $a_{2m+1} = b_{2m+1}$ by the definition of the set J. Thus $v = w$. We now prove by contradiction that we cannot have $a_{2m+1} \in J \cup \{0\}$ while $b_{2m+1} \notin J \cup \{0\}$, so assume otherwise, still under the assumption that $\phi(v) = \phi(w)$. If $L(\sum_{i=1}^{2m} b_i x_i) = \sum_{i=1}^{2m} \beta_i x_i$, then by the definition of ϕ we obtain $a_i = \beta_i$ for $i < 2m+1$, and so $L(w') = v'$, where $w' = w - b_{2m+1}x_{2m+1}$ and $v' = v - a_{2m+1}x_{2m+1}$. Now we have

$$B\big(v', v'\big) = B\big(L\big(w'\big), L\big(w'\big)\big) = B'\big(w', w'\big), \quad \text{which implies} \quad \sum_{i=1}^{2m} a_i^2 c_i = \sum_{i=1}^{2m} d b_i^2 c_i. \tag{3.1}$$

Considering the first coordinate of $\phi(v) = \phi(w)$, we obtain $\sum_{i=1}^{2m+1} a_i^2 c_i = d \sum_{i=1}^{2m+1} b_i^2 c_i$, which combined with (3.1), gives $a_{2m+1}^2 = d b_{2m+1}^2$. This is a contradiction, as $b_{2m+1} \neq 0$ since $b_{2m+1} \notin J \cup \{0\}$, and the left side of this equation is a square, while the right side is a non-square. We now have ϕ is injective, and thus ϕ is bijective.

Finally, since ϕ is bijective, and $\phi(\mathcal{S}_0(V)) \subseteq \mathcal{X}_m$ and $\phi(\mathcal{S}_0(V)^*) \subseteq \mathcal{X}_m^*$, it follows that $\phi(\mathcal{S}_0(V)) = \mathcal{X}_m$ and $\phi(\mathcal{S}_0(V)^*) = \mathcal{X}_m^*$. □

We now fix V to be a $2m$-dimensional $\mathbb{F}_q$-vector space with non-degenerate symmetric form B, and fix W to be an m-dimensional $\mathbb{F}_{q^2}$-vector space. The following is the main tool which is used to show $B(m,1) = \tilde{B}(m,1)$.

Lemma 3.4. *Let $\alpha \in \mathbb{F}_{q^2}$ such that $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$. Define $\mathcal{I}$ and $\mathcal{J}$ to be the following sets:*

$$\mathcal{I} := \big\{(x,y) \,\big|\, x, y \in V,\ \operatorname{span}(x,y) \textit{ is non-degenerate and 2-dimensional}\big\},$$
$$\mathcal{J} := \big\{\big(w, (a+b\alpha)w, U\big) \,\big|\, w \in W,\ w \neq 0,\ a, b \in \mathbb{F}_q,\ b \neq 0,\ U \leqslant W,\ U \oplus \operatorname{span}(w) = W\big\},$$

where $U \leqslant W$ means that U is a subspace of W. Then there exists a bijection $\theta : \mathcal{I} \to \mathcal{J}$, constructed below.

Proof. Before defining θ, we fix the following. Since W is an $\mathbb{F}_{q^2}$-vector space of dimension m, then viewed as an $\mathbb{F}_q$-vector space it has dimension $2m$, and is thus isomorphic to V as an $\mathbb{F}_q$-vector space. Fix an $\mathbb{F}_q$-linear isomorphism $f : V \to W$. Next, for any $x \in V$, we have $\operatorname{span}(x)^\perp$ is $(2m-1)$-dimensional. If $B(x,x) \neq 0$, then $\operatorname{span}(x)^\perp$ is non-degenerate. In this case, by Lemma 3.3, using the notation there, there is a bijection, which we fix, $\phi_x : \operatorname{span}(x)^\perp \to \mathbb{F}_q^{2m-1}$ satisfying $\phi_x(\mathcal{S}_0(\operatorname{span}(x)^\perp)^*) = \mathcal{X}_{m-1}^*$. For each $x \in V$ with $B(x,x) = 0$, fix a basis $\mu(x)_0, \mu(x)_1, \ldots, \mu(x)_{2m-1}$ of V such that $\operatorname{span}(x)^\perp = \operatorname{span}(\mu(x)_1, \ldots, \mu(x)_{2m-1})$. Finally, for each $w \in W$, $w \neq 0$, fix a basis $w, \nu(w)_1, \nu(w)_2, \ldots, \nu(w)_{m-1}$ of W.

Given $(x,y) \in \mathcal{I}$, we now define $\theta((x,y))$ as follows, depending on whether $B(x,x) = 0$ or $B(x,x) \neq 0$.

If $B(x,x) = 0$, then since $\operatorname{span}(x,y)$ is non-degenerate, we have $B(x,y) \neq 0$, that is, $y \notin \operatorname{span}(x)^\perp$. Now write $y = \sum_{i=0}^{2m-1} y_i \mu(x)_i$, for $y_i \in \mathbb{F}_q$. Then $y_0 \neq 0$ since $y \notin \operatorname{span}(x)^\perp$. Now define $\theta((x,y)) = (f(x), (y_1 + y_0\alpha)f(x), U)$, where

$$U = \bigoplus_{i=1}^{m-1} \operatorname{span}\big(\nu\big(f(x)\big)_i + (y_{2i} + y_{2i+1}\alpha) f(x)\big).$$

Note that U is indeed an $(m-1)$-dimensional $\mathbb{F}_{q^2}$-subspace of W, and $f(x) \notin U$, due to the linear independence of $f(x), \nu(f(x))_1, \dots, \nu(f(x))_{m-1}$, and so $(f(x), (y_1 + y_0\alpha)f(x), U) \in \mathcal{J}$.

If $B(x,x) \neq 0$, then $V = \operatorname{span}(x) \oplus \operatorname{span}(x)^{\perp}$, and so we may write y uniquely as $y = ax + z$ for $a \in \mathbb{F}_q$ and $z \in \operatorname{span}(x)^{\perp}$, so $B(x,z) = 0$. Then since $\operatorname{span}(x,y) = \operatorname{span}(x,z)$ is non-degenerate, we must have $B(z,z) \neq 0$, and so $z \in \operatorname{span}(x)^{\perp}$, and in particular, $z \in \mathcal{S}_0(\operatorname{span}(x)^{\perp})^*$. Let $\phi_x(z) = (z_1, \dots, z_{2m-1}) \in \mathcal{X}^*_{m-1} \subset \mathbb{F}_q^{2m-1}$, where $z_1 \neq 0$ by definition of $\mathcal{X}^*_{m-1}$. Now define $\theta((x,y)) = (f(x), (a + z_1\alpha)f(x), U)$, where

$$U = \bigoplus_{i=1}^{m-1} \operatorname{span}\bigl(\nu\bigl(f(x)\bigr)_i + (z_{2i} + z_{2i+1}\alpha)f(x)\bigr).$$

Then $(f(x), (a + z_1\alpha)f(x), U) \in \mathcal{J}$ for the same reason as in the previous case.

We now establish θ is a bijection by giving its inverse. Let $(w, (a + b\alpha)w, U) \in \mathcal{J}$. Since $W = \operatorname{span}(w) \oplus U$, then for each $i = 1, \dots, m-1$, there are unique $a_i, b_i \in \mathbb{F}_q$ such that $\nu(w)_i + (a_i + b_i\alpha)w \in U$. Since the $\nu(w)_i$ are linearly independent, it follows that

$$U = \bigoplus_{i=1}^{m-1} \operatorname{span}\bigl(\nu(w)_i + (a_i + b_i\alpha)w\bigr).$$

If $B(f^{-1}(w), f^{-1}(w)) = 0$, then define $y_w = b\mu(f^{-1}(w))_0 + a\mu(f^{-1}(w))_1 + \sum_{i=1}^{m-1} a_i\mu(f^{-1}(w))_{2i} + b_i\mu(f^{-1}(w))_{2i+1}$. If $B(f^{-1}(w), f^{-1}(w)) \neq 0$, then let

$$z_w = \phi^{-1}_{f^{-1}(w)}\bigl((b, a_1, b_1, a_2, b_2, \dots, a_{m-1}, b_{m-1})\bigr),$$

and define $y_w = af^{-1}(w) + z_w$. In either case, letting $x_w = f^{-1}(w)$, we may check that $\operatorname{span}(x_w, y_w)$ is non-degenerate by considering the determinant of the matrix

$$\begin{pmatrix} B(x_w, x_w) & B(x_w, y_w) \\ B(x_w, y_w) & B(y_w, y_w) \end{pmatrix}.$$

In the first case, $B(x_w, x_w) = 0$, we have $y_w \notin \operatorname{span}(x)^{\perp}$, since $b \neq 0$, and the span of the vectors $\mu(x_w)_1, \dots, \mu(x_w)_{2m-1}$ is $\operatorname{span}(x)^{\perp}$. Thus $B(x_w, y_w) \neq 0$, and the determinant of the above matrix is not zero. In the case that $B(x_w, x_w) \neq 0$, we compute that the determinant of the above matrix is $B(x_w, x_w)B(z_w, z_w) - B(x_w, z_w)^2$. Also, $B(z_w, z_w) \neq 0$ and $B(x_w, z_w) = 0$ since z_w is in the image of $\phi^{-1}_{x_w}$. Thus, the determinant is nonzero in both cases, and $\operatorname{span}(x_w, y_w)$ is non-degenerate. Finally, it follows that $\theta^{-1}((w, (a + b\alpha)w, U)) = (x_w, y_w)$, and thus θ is a bijection. □

Lemma 3.5. *For any $m \geqslant 1$, $B(m,1) = \tilde{B}(m,1)$.*

Proof. Let $\mathcal{I}$ and $\mathcal{J}$ be the sets defined in Lemma 3.4. We define equivalence relations on $\mathcal{I}$ and $\mathcal{J}$ as follows. Define (x,y) and (x', y') in $\mathcal{I}$ to be equivalent when $\operatorname{span}(x,y) = \operatorname{span}(x', y')$, and define $(w, (a + b\alpha)w, U)$ and $(w', (a' + b'\alpha)w', U')$ in $\mathcal{J}$ to be equivalent when $\operatorname{span}(w) = \operatorname{span}(w')$ and $U = U'$. Then, each equivalence class in $\mathcal{I}$ corresponds to a 2-dimensional non-degenerate subspace of V, while each equivalence class in $\mathcal{J}$ corresponds to a pair (U, U_1) such that U is an $(m-1)$-dimensional subspace of W, U_1 is a 1-dimensional subspace of W, and $U \oplus U_1 = W$. In particular, the number of equivalence classes in $\mathcal{I}$ is $B(m,1)$, and the number of equivalence classes in $\mathcal{J}$ is $\tilde{B}(m,1)$. The number of elements in each equivalence class in $\mathcal{I}$ is the number of bases of a 2-dimensional vector space over $\mathbb{F}_q$. Similarly, the number of elements in an equivalence class in $\mathcal{J}$ is the number of ways to pick a nonzero $\mathbb{F}_{q^2}$-multiple of a fixed w, which is equivalent to choosing a nonzero vector in a 2-dimensional $\mathbb{F}_q$-vector space, along with a pair $a, b \in \mathbb{F}_q$, with $b \neq 0$, which is the same in number as choosing a second vector in a 2-dimensional $\mathbb{F}_q$-vector space which is not a scalar multiple of the first. That is, an equivalence class in $\mathcal{J}$ has the same size as an equivalence class in $\mathcal{I}$. Since also $|\mathcal{I}| = |\mathcal{J}|$ from Lemma 3.4, then the number of equivalence classes in each set is the same, and thus $B(m,1) = \tilde{B}(m,1)$. $\square$

Finally, we have the following result.

Theorem 3.2. *For any $m \geqslant k \geqslant 0$, $B(m,k) = \tilde{B}(m,k)$.*

Proof. For $k = 0$, then only non-degenerate subspace of an $\mathbb{F}_q$-vector space with a symmetric form is the trivial subspace, and the only way to choose a 0-dimensional subspace of an $\mathbb{F}_{q^2}$-vector space with a complement is the trivial subspace and the subspace itself. Thus $B(m,0) = \tilde{B}(m,0)$. Lemma 3.5 gives the statement for $k = 1$. We now fix $k > 1$, and we show by induction on m that $B(m,k) = \tilde{B}(m,k)$. For the base case, $m = k$, we have $B(k,k) = \tilde{B}(k,k)$ by essentially the same argument that $B(m,0) = \tilde{B}(m,0)$. Now assume $B(m,k) = \tilde{B}(m,k)$ for some $m \geqslant k$.

Let W be an $(m+1)$-dimensional vector space over $\mathbb{F}_{q^2}$. For any vector space $\mathcal{V}$ over $\mathbb{F}_{q^2}$, and any $j \leqslant n$, let $\mathcal{C}_j(\mathcal{V})$ denote the set of pairs $(\mathcal{Y}, \mathcal{Y}')$ such that $\mathcal{Y}$ is a j-dimensional subspace of $\mathcal{V}$, and $\mathcal{Y}'$ is a subspace of $\mathcal{V}$ which is a complement to $\mathcal{Y}$, so that $\mathcal{Y} \oplus \mathcal{Y}' = \mathcal{V}$. The number of ways to choose a 1-dimensional subspace X of W, with an m-dimensional complement $X' \subset W$, is $\tilde{B}(m+1,1) = |\mathcal{C}_1(W)|$. Given such a pair $(X, X') \in \mathcal{C}_1(W)$, we say a pair of subspaces $(Z, Z') \in \mathcal{C}_k(W)$ is *generated* by (X, X') if $(Z, Z') = (Y, Y' \oplus X)$ for some $(Y, Y') \in \mathcal{C}_k(X')$. Then, each element $(Y, Y') \in \mathcal{C}_k(X')$ determines a unique element in $\mathcal{C}_k(W)$ which is generated by (X, X'). It follows that each $(X, X') \in \mathcal{C}_1(W)$ generates exactly $|\mathcal{C}_k(X')| = \tilde{B}(m,k)$ elements in $\mathcal{C}_k(W)$.

Now, given some element $(Z, Z') \in \mathcal{C}_k(W)$, (Z, Z') is generated by some fixed $(X, X') \in \mathcal{C}_1(W)$ if and only if there exists a subspace U such that $Z' = X \oplus U$ and $Z \oplus U = X'$. Thus, for a fixed (Z, Z'), any $(X, U) \in \mathcal{C}_1(Z')$ determines a unique $(X, X') \in \mathcal{C}_1(W)$ which generates (Z, Z'), and each (X, X') is determined by at least one such (X, U). It follows that each (Z, Z') is generated by exactly $|\mathcal{C}_1(Z')| = \tilde{B}(m-k+1,1)$ elements in $\mathcal{C}_1(W)$. Therefore, we have that

$$\tilde{B}(m+1,k) = \tilde{B}(m+1,1)\tilde{B}(m,k)/\tilde{B}(m-k+1,1). \tag{3.2}$$

Finally, we have from the proof of Theorem 3.1 that $B(m+1,k) = B(m+1,1)B(m,k)/B(m-k+1,1)$, and since $\tilde{B}(m+1,1) = B(m+1,1)$ and $\tilde{B}(m-k+1,1) = B(m-k+1,1)$ from Lemma 3.5, and $\tilde{B}(m,k) = B(m,k)$ from the induction hypothesis, it follows from (3.2) that $\tilde{B}(m+1,k) = B(m+1,k)$, as desired. $\square$

4. Proof of the semi-recursion

In this section, we give a combinatorial proof of Theorem 1.1. As in the previous sections, we let $A(m,k)$ and $B(m,k)$ denote the number of $2k$-dimensional non-degenerate subspaces of a $(2m+1)$-dimensional and $2m$-dimensional, respectively, $\mathbb{F}_q$-vector space with a non-degenerate symmetric form. We continue to prove all statements combinatorially and without using the formulas for these quantities, and we begin by giving a relationship between $A(m,k)$ and $B(m,k)$.

Lemma 4.1. *For any $m \geqslant k \geqslant 0$, we have $A(m,k) = q^{2k}B(m,k)$. In particular, we have $A(m,m) = q^{2m}B(m,m) = q^{2m}$.*

Proof. For the case $k = m$, we have $A(m,m)$ is the number of ways to choose a $2m$-dimensional non-degenerate subspace, which is equivalent to choosing its 1-dimensional orthogonal complement. Now, the number of generating vectors of all 1-dimensional non-degenerate subspaces is equal to the number of vectors x such that $B(x,x) \neq 0$, where $B(\cdot,\cdot)$ is our non-degenerate symmetric form. By Lemma 3.3, this is equal to the number of elements in $\mathbb{F}_q^{2m+1}$ with nonzero first coordinate, of which there are $q^{2m+1} - q^{2m} = q^{2m}(q-1)$. Since each 1-dimensional $\mathbb{F}_q$-vector space has exactly $q-1$ generating vectors, we have $A(m,m) = q^{2m}$.

Now consider the general case, with $k \geqslant 1$. If V is a $(2m+1)$-dimensional $\mathbb{F}_q$-vector space with a non-degenerate symmetric form, then as we just obtained, there are $A(m,m) = q^{2m}$ non-degenerate subspaces of V with dimension $2m$. For each $2m$-dimensional non-degenerate subspace V', there are $B(m,k)$ non-degenerate subspaces of V' with dimension $2k$. Now, given any $2k$-dimensional non-degenerate subspace W of V, we have $W^{\perp}$ is a non-degenerate $(2(m-k)+1)$-dimensional subspace of V. There are exactly $A(m-k, m-k) = q^{2(m-k)}$ non-degenerate subspaces of $W^{\perp}$ which are $2(m-k)$-dimensional. Given any such subspace U, $W \oplus U$ is a $2m$-dimensional non-degenerate subspace of V which contains W. Also, any $2m$-dimensional non-degenerate subspace Y of V which contains W may be written as $Y = W \oplus (W^{\perp} \cap Y)$. So, the total number of $2k$-dimensional non-degenerate subspaces of V is exactly $q^{2m}B(m,k)/q^{2(m-k)} = q^{2k}B(m,k)$. □

We now reduce the proof of the identity in Theorem 1.1 to another identity.

Lemma 4.2. *Theorem* 1.1 *follows from the identity that for any $m > 1$, $m \geqslant k \geqslant 1$,*

$$A(m+1,k) = A(m,k) + q^{2m}\big(q^{2m}-1\big)B(m-1,k-1) + q^{2m+2}A(m,m-k+1).$$

Proof. Suppose that the identity is true. From Corollary 2.1, we have $I(2m+1) = \sum_{k=0}^{m} A(m,k)$ and $I(2m) = \sum_{k=0}^{m} B(m,k)$. Now, for any $m > 1$,

$$\begin{aligned} I(2m+3) = \sum_{k=0}^{m+1} A(m+1,k) &= A(m+1,0) + A(m+1,m+1) \\ &\quad + \sum_{k=1}^{m}\big(A(m,k) + q^{2m}\big(q^{2m}-1\big)B(m-1,k-1) + q^{2m+2}A(m,m-k+1)\big). \end{aligned}$$

Since $A(m+1,0) = 1 = A(m,0)$, and by Lemma 4.1 $A(m+1,m+1) = q^{2m+2}B(m+1,m+1) = q^{2m+2} = q^{2m+2}A(m+1,0)$, we have

$$\begin{aligned} I(2m+3) &= \sum_{k=0}^{m} A(m,k) + q^{2m}\big(q^{2m}-1\big)\sum_{k=0}^{m-1} B(m-1,k) + q^{2m+2}\sum_{k=1}^{m+1} A(m,m-k+1) \\ &= \big(q^{2m+2}+1\big)\sum_{k=0}^{m} A(m,k) + q^{2m}\big(q^{2m}-1\big)\sum_{k=0}^{m-1} B(m-1,k) \\ &= \big(q^{2m+2}+1\big)I(2m+1) + q^{2m}\big(q^{2m}-1\big)I(2m-2), \end{aligned}$$

which is exactly the identity in Theorem 1.1. □

The key to our proof of Theorem 1.1 is to interpret the quantities $A(m,k)$ and $B(m,k)$ in terms of linear subspaces of $\mathbb{F}_{q^2}$-vector spaces. We have done this for $B(m,k)$ in Theorem 3.2, in which we showed $B(m,k)$ is also the number of ordered pairs (W, W') of subspaces of an m-dimensional $\mathbb{F}_{q^2}$-vector space V, where $\dim W = k$ and $W \oplus W' = V$. We mentioned a similar interpretation of $A(m,k)$ at the end of Section 2, for which we now give a proof from our current point of view.

Lemma 4.3. *Let V be an $(m+1)$-dimensional $\mathbb{F}_{q^2}$-vector space, and let V' be a fixed m-dimensional subspace of V. The number of ordered pairs (U, U') of subspaces of V such that U is a k-dimensional subspace of V' and $U \oplus U' = V$ is $A(m,k)$.*

Proof. By Lemma 4.1, it is enough to show that the number of such ordered pairs is $q^{2k}B(m,k)$, and by Theorem 3.2, we know that $B(m,k)$ is the number of ordered pairs (W, W') of subspaces of V' such that $\dim W = k$ and $W \oplus W' = V'$. Fix an element $v \in V \setminus V'$. If $v' \in V'$, then (U, U'), where $U = W$ and $U' = W' \oplus \operatorname{span}(v + v')$, is a pair of subspaces of V such that $\dim U = k$ and $U \oplus U' = V$. Note that for $v', v'' \in V'$, we have $W' \oplus \operatorname{span}(v + v') = W' \oplus \operatorname{span}(v + v'')$ if and only if $v' - v'' \in W'$. This implies that the number of choices for $W' \oplus \operatorname{span}(v + v')$ is exactly $|V'|/|W'| = q^{2m}/q^{2m-2k} = q^{2k}$. Thus, there are a total of $q^{2k}B(m,k) = A(m,k)$ pairs (U, U') of subspaces of V such that $\dim U = k$, $U \oplus U' = V$, and $U \subset V'$. □

We now concentrate on the identity in Lemma 4.2 which implies Theorem 1.1. The main work in proving the identity is in the next two lemmas.

Lemma 4.4. *Let X be an $(m+2)$-dimensional $\mathbb{F}_{q^2}$-vector space, V a fixed $(m+1)$-dimensional subspace of X, and V' a fixed m-dimensional subspace of V. The number of ordered pairs (U, U') of subspaces of X such that $U \subset V$, $\dim U = k$, $U \oplus U' = X$, and $U \not\subset V'$, is*

$$q^{2m+2}A(m, m-k+1).$$

Proof. Consider the set of ordered pairs (W, W') of subspaces of V, such that $\dim W = k$, $W \oplus W' = V$, and $W \not\subset V'$. Given such a pair, as in the proof of Lemma 4.3, there are exactly q^{2k} pairs (U, U'), where $U = W$ and $W' \subset U'$, of subspaces of X such that $\dim U = k$, $U \oplus U' = X$, and $U \not\subset V'$. Thus, it is enough to show that the number of such pairs (W, W') of subspaces of V is $q^{2(m-k+1)}A(m, m-k+1)$.

Suppose that (Y, Y') is a pair of subspaces of V such that $Y \subset V'$, $\dim Y = k-1$, and $Y \oplus Y' = V$. We call a pair (W, W') of subspaces of V such that $\dim W = k$, $W \oplus W' = V$, and $W \not\subset V'$, a *semi-extension* of (Y, Y') if $W \cap V' = Y$, $W' \subset Y'$, and $\dim(W \cap Y') = 1$. We now count the number of semi-extensions of a fixed pair of such subspaces (Y, Y') of V.

If (W, W') is a semi-extension of (Y, Y'), then $\dim(W \cap Y') = 1$, and $W \cap V' = Y$, which implies $W = (W \cap Y') \oplus Y$. Also, $Y' = W' \oplus (W \cap Y')$, where $\dim W' = m-k+1$. Now, each semi-extension (W, W') uniquely describes the pair $(W', W \cap Y')$. Conversely, each ordered pair (J, K) of subspaces of Y' such that $\dim J = m-k+1$, $\dim K = 1$, $K \not\subset V'$, and $J \oplus K = Y'$, determines a unique semi-extension $(Y \oplus K, J)$ of (Y, Y'). Thus, to count the number of semi-extensions of (Y, Y'), we need to count the number of such pairs (J, K). We have $\dim Y' = (m+1) - (k-1) = m-k+2$, and so $\dim(Y' \cap V') = m-k+1$, while we must choose $K \not\subset V'$. So, the number of choices of K is the number of 1-dimensional complements to $Y' \cap V'$ in Y', of which there are $q^{2(m-k+1)}$ by Lemma 2.1. Once K is chosen, J is a complementary subspace to K in Y', the number of which is also $q^{2(m-k+1)}$, again by Lemma 2.1. This gives a total of $q^{4(m-k+1)}$ semi-extensions of (Y, Y').

Now, given a pair (W, W') of subspaces of V such that $\dim W = k$, $W \oplus W' = V$, and $W \not\subset V'$, then to determine a pair (Y, Y') for which (W, W') is a semi-extension, we note $Y = W \cap V'$ is uniquely determined. Since we must have $Y' = W' \oplus (W \cap Y')$ where $\dim(W \cap Y') = 1$, then Y' is uniquely determined by the choice of a 1-dimensional subspace of W, which is a complement to Y, since $W = (W \cap Y') \oplus Y$. There are $q^{2(k-1)}$ such 1-dimensional subspaces, and so (W, W') is a semi-extension of exactly $q^{2(k-1)}$ pairs (Y, Y').

Finally, the number of pairs of subspaces (Y, Y') of V such that $Y \subset V'$, $\dim Y = k-1$, and $Y \oplus Y' = V$ is $A(m, k-1)$ by Lemma 4.3, and there are $q^{4(m-k+1)}$ semi-extensions (W, W') of (Y, Y'), and a pair (W, W') is a semi-extension of $q^{2(k-1)}$ pairs (Y, Y'). It follows that the number of pairs of subspaces (W, W') of V such that $\dim W = k$, $W \oplus W' = V$, and $W \not\subset V'$ is

$$\begin{aligned} A(m, k-1)q^{4(m-k+1)}/q^{2(k-1)} &= q^{2(k-1)}B(m, k-1)q^{4(m-k+1)}/q^{2(k-1)} \\ &= B(m, m-k+1)q^{4(m-k+1)} \\ &= q^{2(m-k+1)}A(m, m-k+1), \end{aligned}$$

as desired, where we have applied Lemma 4.1 twice, and the fact that $B(m,k-1)=B(m,m-k+1)$. □

Lemma 4.5. *Let X be an $(m+2)$-dimensional $\mathbb{F}_{q^2}$-vector space, V a fixed $(m+1)$-dimensional subspace of X, and V' a fixed m-dimensional subspace of V. The number of ordered pairs (U,U') of subspaces of X such that $U \subset V$, $\dim U = k$, $U \oplus U' = X$, and $U \subset V'$, is*

$$A(m,k)+q^{2m}\bigl(q^{2m}-1\bigr)B(m-1,k-1).$$

Proof. As in the proof of Theorem 3.2, we let $\mathcal{C}_k(X)$ denote the set of ordered pairs of subspaces (Z,Z') of X such that $\dim Z = k$ and $Z \oplus Z' = X$, and similarly for $\mathcal{C}_k(V)$.

Fix a vector $x \in X \setminus V$. For pairs $(U,U') \in \mathcal{C}_k(X)$ such that $U \subset V'$, we consider the cases that either $x \in U'$ or $x \notin U'$. In the case $x \in U'$, for any pair $(W,W') \in \mathcal{C}_k(V)$ with $W \subset V'$, there is a unique pair $(U,U') \in \mathcal{C}_k(X)$ satisfying $U = W \subset V'$ and $W' \subset U'$, namely $U' = W' \oplus \operatorname{span}(x)$. Since $\mathcal{C}_k(V)$ has exactly $A(m,k)$ elements, then the number of pairs $(U,U') \in \mathcal{C}_k(X)$ such that $U \subset V'$ and $x \in U'$ is exactly $A(m,k)$.

We now count pairs $(U,U') \in \mathcal{C}_k(X)$ such that $U \subset V'$ and $x \notin U'$. Fix a vector $y \in V \setminus V'$. Consider a nonzero vector $v' \in V'$, and a subspace Z of V' such that $(\operatorname{span}(v'),Z) \in \mathcal{C}_1(V')$, so $\operatorname{span}(v') \oplus Z = V'$ and $\dim Z = m-1$, and let $(Y,Y') \in \mathcal{C}_{k-1}(Z)$. Now, for any $w \in V'$, take the pair of subspaces

$$\bigl(U,U'\bigr)=\bigl(Y \oplus \operatorname{span}\bigl(v'\bigr), Y' \oplus \operatorname{span}(y+w) \oplus \operatorname{span}\bigl(x+v'\bigr)\bigr).$$

Then we have $\dim U = k$, $U \subset V'$, $U \oplus U' = X$, and $x \notin U'$, since $x+v' \in U'$ and $v' \notin U'$. Furthermore, all pairs (U,U') with these properties are of this form. In constructing this pair (U,U'), there are $q^{2m}-1$ choices for v', $q^{2(m-1)}$ choices for Z by Lemma 2.1, $B(m-1,k-1)$ ways to choose (Y,Y'), and q^{2m} choices for $w \in V'$. We now count how many of these choices produce the same pair (U,U').

Fix (U,U') constructed as above. Given $\operatorname{span}(v')$, there are $q^{2(k-1)}$ choices for Y which are complements to $\operatorname{span}(v')$ in U, again by Lemma 2.1. Now, given choices for Y' and v', we may replace $w \in V'$ by any element in $w+Y'$ to obtain the same U', for which there are $|Y'| = q^{2(m-k)}$ choices. We now show that if we fix a choice of Y, then v', Y', $w+Y'$, and Z are uniquely determined by (U,U'). This is enough, since this will give that the total number of pairs $(U,U') \in \mathcal{C}_k(X)$ such that $U \subset V'$ and $x \notin U'$ is

$$\bigl(q^{2m}-1\bigr)q^{2(m-1)}q^{2m}B(m-1,k-1)/\bigl(q^{2(k-1)}q^{2(m-k)}\bigr)=q^{2m}\bigl(q^{2m}-1\bigr)B(m-1,k-1).$$

We have $U \oplus U' = X$, so given any $v \in X$, define $\operatorname{pr}_U(v)$ and $\operatorname{pr}_{U'}(v)$ to be the unique vectors in U and U', respectively, so that $\operatorname{pr}_U(v)+\operatorname{pr}_{U'}(v)=v$. Now, considering the vector $x \in X \setminus V$, we have $x+v' \in U'$ and $v' \in U$, and so $\operatorname{pr}_U(x) = -v'$ and $\operatorname{pr}_{U'}(x) = x+v'$. Since x is fixed, we have $v' = -\operatorname{pr}_U(x)$ is uniquely determined by (U,U'). Next, since $Y' = U' \cap V'$, then Y' is uniquely determined by (U,U') as well, and since we have fixed our choice of Y, $Y \oplus Y' = Z$ is uniquely determined. Finally, we have $V' = U \oplus Y'$, and so to show that $w+Y'$ is uniquely determined, we may assume $w \in U$ and prove w is then uniquely determined by (U,U'). We have $U' \cap V = Y' \oplus \operatorname{span}(y+w)$, and $V = U \oplus (U' \cap V)$. Since $y = -w+(y+w)$ where $-w \in U$ and $y+w \in U' \cap V$, we have $-w = \operatorname{pr}_U(y)$ and $y+w = \operatorname{pr}_{U' \cap V}(y)$. This implies $w = -\operatorname{pr}_U(y)$ is uniquely determined by (U,U'), as claimed. □

Finally, we have the following, which completes the proof of Theorem 1.1 by Lemma 4.2.

Lemma 4.6. *For any $m > 1$, $m \geqslant k \geqslant 1$,*

$$A(m+1,k)=A(m,k)+q^{2m}\bigl(q^{2m}-1\bigr)B(m-1,k-1)+q^{2m+2}A(m,m-k+1).$$

Proof. Let X be an $(m+2)$-dimensional $\mathbb{F}_{q^2}$-vector space, V a fixed $(m+1)$-dimensional subspace of X, and V' a fixed m-dimensional subspace of V. By Lemma 4.3, $A(m+1,k)$ is the number of pairs of subspaces (U,U') of X such that $U \subset V$, $\dim U = k$, and $U \oplus U' = X$. Given any such pair, we either have $U \subset V'$ or $U \not\subset V'$. By Lemma 4.5, the number of pairs (U,U') such that $U \subset V'$ is $A(m,k) + q^{2m}(q^{2m}-1)B(m-1,k-1)$, and by Lemma 4.4, the number of pairs such that $U \not\subset V'$ is $q^{2m+2}A(m,m-k+1)$, the sum of which gives the result. □

5. An application to bounding character degree sums

In sieving applications, Kowalski [8] needed to bound the sums of the degrees of the complex irreducible characters of certain finite groups, and he obtained an explicit bound for the character degree sum of a large class of finite reductive groups. More specifically, if **G** is a connected reductive group with connected center which is defined over a finite field $\mathbb{F}_q$ by a split Frobenius map, Kowalski gave a bound for the character degree sum for the finite group $\mathbf{G}(\mathbb{F}_q)$ in terms of the rank, dimension, and the order of the Weyl group of **G**, and in terms of q [8, Proposition 5.5]. He noted that the one factor in the bound which contained the order of the Weyl group could be dropped in several cases, and the second-named author proved [16, Theorem 6.1] that this is true whenever **G** is classical and q is odd, and without any assumption on the Frobenius map. Furthermore, it was conjectured by the second-named author [16, Conjecture 7.1] that an even tighter bound should be true for any connected reductive group with connected center. The purpose of this section is to prove Theorem 5.1, which confirms this conjecture when **G** is classical and q is odd. The main connection with the previous sections of this paper is that the character degree sums for various finite orthogonal groups may be bounded by using the number of involutions, and in particular, we use Theorem 1.1 to obtain one such bound.

We begin with a bound on the q-binomial coefficient by a polynomial in q. Note that although we are concerned with q being a power of an odd prime in our applications, the following result, and the next lemma, are true for any real number $q \geqslant 2$.

Lemma 5.1. *For any $q \geqslant 2$ and any integers $m \geqslant k \geqslant 0$, we have*

$$\binom{m}{k}_q \leqslant q^{k(m-k-2)}(q+1)^{2k}.$$

Proof. For $k=0$, the statement reduces to $1 \leqslant 1$. For $k=1$, we have $\binom{m}{k}_q = 1+q+\cdots+q^{m-1}$. Then, for $m=1$, $\binom{1}{1}_q = 1 \leqslant (1+1/q)^2 = q^{-2}(q+1)^2$; for $m=2$, $\binom{2}{1}_q = 1+q \leqslant (1+1/q)(q+1) = q^{-1}(q+1)^2$; and for $m=3$, $\binom{3}{1}_q = 1+q+q^2 \leqslant (q+1)^2$. Now suppose $k=1$ and $m \geqslant 4$. Since $q \geqslant 2$, we have

$$1+q+\cdots+q^{m-4} = \frac{q^{m-3}-1}{q-1} \leqslant q^{m-3}-1 < q^{m-2}.$$

Thus, we have

$$\begin{aligned}\binom{m}{1}_q &= 1+q+\cdots+q^{m-1} < q^{m-2}+q^{m-3}+q^{m-2}+q^{m-1}\\ &= q^{m-3}(q+1)^2.\end{aligned}$$

We may now assume $k \geqslant 2$, and our induction hypothesis is that the inequality holds for $\binom{m-1}{k}_q$ for any $k \leqslant m-1$. We apply the q-Pascal identity $\binom{m}{k}_q = \binom{m-1}{k}_q + q^{m-k}\binom{m-1}{k-1}_q$, $k \geqslant 1$. We have

$$\binom{m}{k}_q = \binom{m-1}{k}_q + q^{m-k}\binom{m-1}{k-1}_q \leqslant q^{k(m-k-3)}(q+1)^{2k} + q^{m-k}q^{(k-1)(m-k-2)}(q+1)^{2k-2}$$
$$= q^{k(m-k-3)}(q+1)^{2k} + q^{k(m-k-2)}q^2(q+1)^{2k-2} = q^{k(m-k-2)}(q+1)^{2k}\left(\frac{1}{q^k} + \frac{q^2}{(q+1)^2}\right).$$

Since $k \geqslant 2$ and $q \geqslant 2$, we have $\frac{1}{q^k} \leqslant \frac{1}{q^2} \leqslant \frac{1}{q+1}$, and $\frac{q^2}{(q+1)^2} \leqslant \frac{q^2}{q^2+q} = \frac{q}{q+1}$. Thus,

$$\frac{1}{q^k} + \frac{q^2}{(q+1)^2} \leqslant \frac{1}{q+1} + \frac{q}{q+1} = 1.$$

This gives $\binom{m}{k}_q \leqslant q^{k(m-k-2)}(q+1)^{2k}$, as desired. □

By applying Lemma 5.1, we are now able to bound $I(2m)$, the number of involutions in the special orthogonal groups $\mathrm{SO}^{\pm}(2m, \mathbb{F}_q)$.

Lemma 5.2. *For any $q \geqslant 2$ and any $m \geqslant 1$, we have*

$$\sum_{k=0}^{m} q^{2k(m-k)}\binom{m}{k}_{q^2} \leqslant \begin{cases} q^{m^2-2m}(q^2+1)^m & \text{if } m \text{ is even}, \\ 2q^{m^2-2m-1}(q^2+1)^m & \text{if } m \text{ is odd}. \end{cases}$$

Proof. From the symmetry in k and $m-k$ in the sum, we have

$$\sum_{k=0}^{m} q^{2k(m-k)}\binom{m}{k}_{q^2} = \begin{cases} q^{m^2/2}\binom{m}{m/2}_{q^2} + 2\sum_{k=0}^{(m/2)-1} q^{2k(m-k)}\binom{m}{k}_{q^2} & \text{if } m \text{ is even}, \\ 2\sum_{k=0}^{(m-1)/2} q^{2k(m-k)}\binom{m}{k}_{q^2} & \text{if } m \text{ is odd}. \end{cases} \tag{5.1}$$

First consider the case that m is even. By [16, Lemma 5.1], for any $q > 1$ and any integers $m \geqslant k \geqslant 1$, we have $\binom{m}{k}_q \leqslant q^{k(m-k)-m+1}(q+1)^{m-1}$. Thus, for $k = m/2$, we have

$$q^{m^2/2}\binom{m}{m/2}_{q^2} \leqslant q^{m^2-2m+2}\left(q^2+1\right)^{m-1}. \tag{5.2}$$

For any $k < m/2$, we apply Lemma 5.1 to obtain

$$q^{2k(m-k)}\binom{m}{k}_{q^2} \leqslant q^{2k(m-k)}q^{2k(m-k-2)}\left(q^2+1\right)^{2k} = q^{4k(m-k-1)}\left(q^2+1\right)^{2k}. \tag{5.3}$$

As a function of x, $4x(m-x-1)$ is strictly increasing on the interval $[0, (m-1)/2]$, and thus for each $k \leqslant m/2-1$ we have

$$q^{4k(m-k-1)} \leqslant q^{4(m/2-1)(m-(m/2-1)-1)} = q^{m^2-2m}. \tag{5.4}$$

Applying inequalities (5.3) and (5.4), we have

$$2\sum_{k=0}^{m/2-1} q^{2k(m-k)}\binom{m}{k}_{q^2} \leqslant 2\sum_{k=0}^{m/2-1} q^{m^2-2m}\left(q^2+1\right)^{2k} = 2q^{m^2-2m}\frac{(q^2+1)^m - 1}{(q^2+1)^2 - 1}.$$

Now, $\frac{(q^2+1)^m-1}{(q^2+1)^2-1} < \frac{(q^2+1)^m}{q^2(q^2+1)} = \frac{(q^2+1)^{m-1}}{q^2}$. Using this, and the fact that $q \geqslant 2$, we obtain

$$2\sum_{k=0}^{m/2-1} q^{2k(m-k)}\binom{m}{k}_{q^2} \leqslant 2q^{m^2-2m}\frac{(q^2+1)^{m-1}}{q^2} \leqslant q^{m^2-2m}\left(q^2+1\right)^{m-1}. \tag{5.5}$$

Finally, by combining (5.1), (5.2), and (5.5), we have

$$\begin{aligned}\sum_{k=0}^{m} q^{2k(m-k)}\binom{m}{k}_{q^2} &= q^{m^2/2}\binom{m}{m/2}_{q^2} + 2\sum_{k=0}^{(m/2)-1} q^{2k(m-k)}\binom{m}{k}_{q^2} \\ &\leqslant q^{m^2-2m+2}\left(q^2+1\right)^{m-1} + q^{m^2-2m}\left(q^2+1\right)^{m-1} = q^{m^2-2m}\left(q^2+1\right)^{m},\end{aligned}$$

when m is even, as desired.

Now assume that m is odd. Similar to (5.3), we have for any $k \leqslant (m-1)/2$,

$$q^{4k(m-k-1)} \leqslant q^{4(\frac{m-1}{2})(m-\frac{m-1}{2}-1)} = q^{m^2-2m+1}.$$

Combining this with Lemma 5.1, we have

$$q^{2k(m-k)}\binom{m}{k}_{q^2} \leqslant q^{4k(m-k-1)}\left(q^2+1\right)^{2k} \leqslant q^{m^2-2m+1}\left(q^2+1\right)^{2k}, \tag{5.6}$$

for any $k \leqslant (n-1)/2$. Now, by (5.1) and (5.6), we have for m odd,

$$\sum_{k=0}^{m} q^{2k(m-k)}\binom{m}{k}_{q^2} \leqslant 2q^{m^2-2m+1}\sum_{k=0}^{(m-1)/2}\left(q^2+1\right)^{2k} = 2q^{m^2-2m+1}\frac{(q^2+1)^{m+1}-1}{(q^2+1)^2-1}.$$

We have $\frac{(q^2+1)^{m+1}-1}{(q^2+1)^2-1} < \frac{(q^2+1)^{m+1}}{q^2(q^2+1)} = \frac{(q^2+1)^m}{q^2}$. So, finally, when m is odd,

$$\sum_{k=0}^{m} q^{2k(m-k)}\binom{m}{k}_{q^2} \leqslant 2q^{m^2-2m+1}\frac{(q^2+1)^m}{q^2} = 2q^{m^2-2m-1}\left(q^2+1\right)^{m},$$

as claimed. □

Now that we have obtained a bound for $I(2m)$, we may bound $I(2m+1)$ by using the semi-recursion in Theorem 1.1. When considering that each $I(n)$ is a polynomial in q, and that we proved Theorem 1.1 when q is the power of an odd prime, then by continuity the semi-recursion for these polynomials in q is true for real numbers q. So, the inequality given below in fact holds for all real $q \geqslant 2$.

Proposition 5.1. *For any $q \geqslant 2$ and any integer $m \geqslant 0$,*

$$\sum_{k=0}^{m} q^{2k(m-k+1)}\binom{m}{k}_{q^2} \leqslant q^{m^2}(q+1)^m.$$

Proof. We will prove by induction on m that

$$\sum_{k=0}^{m} q^{2k(m-k+1)} \binom{m}{k}_{q^2} \leqslant q^{m^2-m}\bigl(q^2+1\bigr)^m,$$

which is enough, since $(q^2+1) \leqslant q(q+1)$, and so $q^{m^2-m}(q^2+1)^m \leqslant q^{m^2}(q+1)^m$. The inequality reduces to $1 \leqslant 1$ when $m=0$, and to $q^2+1 \leqslant q^2+1$ when $m=1$. When $m=2$, the expression on the left is equal to $1+q^4(q^2+1)+q^4$, which is indeed less than or equal to $q^2(q^2+1)^2$. Now, we assume that the inequality holds for some $m \geqslant 2$. Since the expression we are bounding is $I(2m+1)$, and the expression bounded in Lemma 5.2 is $I(2m)$, we may apply Theorem 1.1. We have, when $m \geqslant 2$,

$$I(2m+3) = \bigl(q^{2m+2}+1\bigr)I(2m+1) + q^{2m}\bigl(q^{2m}-1\bigr)I(2m-2).$$

By Lemma 5.2, since $q \geqslant 2$, we have for both m even and odd,

$$I(2m-2) \leqslant q^{(m-1)^2-2(m-1)}\bigl(q^2+1\bigr)^{m-1} = q^{m^2-4m+3}\bigl(q^2+1\bigr)^{m-1}.$$

Applying this and the semi-recursion, we obtain

$$I(2m+3) \leqslant \bigl(q^{2m+2}+1\bigr)q^{m^2-m}\bigl(q^2+1\bigr)^m + \bigl(q^{2m}-1\bigr)q^{m^2-2m+3}\bigl(q^2+1\bigr)^{m-1}. \tag{5.7}$$

Since $m \geqslant 2$, we have $q^{-m+3} < q^2+1$, which gives $q^{m^2-2m+3} < q^{m^2-m}(q^2+1)$. Combining this with (5.7) gives

$$\begin{aligned} I(2m+3) &\leqslant \bigl(q^{2m+2}+1\bigr)q^{m^2-m}\bigl(q^2+1\bigr)^m + \bigl(q^{2m}-1\bigr)q^{m^2-m}\bigl(q^2+1\bigr)^m \\ &= q^{m^2-m}\bigl(q^2+1\bigr)^m\bigl(q^{2m+2}+q^{2m}\bigr) = q^{m^2+m}\bigl(q^2+1\bigr)^{m+1}, \end{aligned}$$

which completes the induction. □

Finally, we come to the main result of this section. Recall that for an algebraic group **G** over the algebraically closed field $\bar{\mathbb{F}}_q$, the *dimension* of **G** is its dimension as an algebraic variety over $\bar{\mathbb{F}}_q$, and its *rank* is the dimension of a maximal torus in **G**. For a more thorough discussion of the relevant material on algebraic and classical groups over $\mathbb{F}_q$, and character theory of finite groups, see [16] and its references.

Theorem 5.1. *Let q be the power of an odd prime, and let* **G** *be a connected classical group with connected center defined over $\mathbb{F}_q$, where the rank of* **G** *is r, and the dimension of* **G** *is d. Then the sum of the degrees of the irreducible characters of the finite group $\mathbf{G}(\mathbb{F}_q)$ may be bounded as follows*:

$$\sum_{\chi \in \mathrm{Irr}(\mathbf{G}(\mathbb{F}_q))} \chi(1) \leqslant q^{(d-r)/2}(q+1)^r,$$

where $\mathrm{Irr}(\mathbf{G}(\mathbb{F}_q))$ is the collection of irreducible complex characters of $\mathbf{G}(\mathbb{F}_q)$, and $\chi(1)$ is the degree of χ.

Proof. The groups $\mathbf{G}(\mathbb{F}_q)$ which are relevant are the finite general linear group $\mathrm{GL}(n,\mathbb{F}_q)$, the finite unitary group $\mathrm{U}(n,\mathbb{F}_{q^2})$, the finite group of symplectic similitudes $\mathrm{GSp}(2n,\mathbb{F}_q)$, the finite special orthogonal group $\mathrm{SO}(2n+1,\mathbb{F}_q)$, and the connected component of the split or non-split finite group of orthogonal similitudes $\mathrm{GO}^{\pm,\circ}(2n,\mathbb{F}_q)$. For the groups $\mathrm{GL}(n,\mathbb{F}_q)$, $\mathrm{U}(n,\mathbb{F}_{q^2})$, and $\mathrm{GSp}(2n,\mathbb{F}_q)$, this bound on the sum of the character degrees is proved in [16, Section 7]. So, we must prove the statement for the groups $\mathrm{SO}(2n+1,\mathbb{F}_q)$ and $\mathrm{GO}^{\pm,\circ}(2n,\mathbb{F}_q)$.

If $\mathbf{G}(\mathbb{F}_q)=\mathrm{SO}(2n+1,\mathbb{F}_q)$, then $d=2n^2+n$ and $r=n$, and the sum of the degrees of the irreducible characters of $\mathrm{SO}(2n+1,\mathbb{F}_q)$ is exactly equal to $I(2n+1)$. This follows from a result of Gow [4, Theorem 2] which states that every irreducible character of $\mathrm{SO}(2n+1,\mathbb{F}_q)$ is the character of a representation which may be realized over the real numbers. The bound for the sum of the degrees of the characters, then, follows exactly from Proposition 5.1, since we have

$$\sum_{\chi\in\mathrm{Irr}(\mathbf{G}(\mathbb{F}_q))}\chi(1)=I(2n+1)\leqslant q^{n^2}(q+1)^n=q^{(d-r)/2}(q+1)^r.$$

If $\mathbf{G}(\mathbb{F}_q)=\mathrm{GO}^{\pm,\circ}(2n,\mathbb{F}_q)$, then for either of these groups we have $d=2n^2-n+1$ and $r=n+1$. It is shown in [16, Proof of Theorem 6.1] that for either of these groups, we have the bound

$$\sum_{\chi\in\mathrm{Irr}(\mathbf{G}(\mathbb{F}_q))}\chi(1)\leqslant(q-1)\bigl(I(2n)+q^{n-1}\bigl(q^n+1\bigr)I(2n-2)\bigr).$$

If n is even, then by Lemma 5.2 we have

$$\begin{aligned}\sum_{\chi\in\mathrm{Irr}(\mathbf{G}(\mathbb{F}_q))}\chi(1)&\leqslant(q-1)\bigl(q^{n^2-2n}\bigl(q^2+1\bigr)^n+q^{n-1}\bigl(q^n+1\bigr)2q^{(n-1)^2-2(n-1)-1}\bigl(q^2+1\bigr)^{n-1}\bigr)\\&\leqslant(q-1)\bigl(q^{n^2-n}(q+1)^n+2q^{n^2-n-1}(q+1)^n\bigr),\end{aligned}$$

where we have used that $q^2+1\leqslant q(q+1)$ and $q^n+1\leqslant q^{n-1}(q+1)$. Now we have

$$\begin{aligned}\sum_{\chi\in\mathrm{Irr}(\mathbf{G}(\mathbb{F}_q))}\chi(1)&\leqslant q^{n^2-n-1}(q+1)^n(q-1)(q+2)=q^{n^2-n-1}(q+1)^n\bigl(q^2+q-2\bigr)\\&\leqslant q^{n^2-n}(q+1)^{n+1}=q^{(d-r)/2}(q+1)^r,\end{aligned}$$

as desired. Similarly, when n is odd, we have by Lemma 5.2,

$$\begin{aligned}\sum_{\chi\in\mathrm{Irr}(\mathbf{G}(\mathbb{F}_q))}\chi(1)&\leqslant(q-1)\bigl(2q^{n^2-2n-1}\bigl(q^2+1\bigr)^n+q^{n-1}\bigl(q^n+1\bigr)q^{(n-1)^2-2(n-1)}\bigl(q^2+1\bigr)^{n-1}\bigr)\\&\leqslant(q-1)\bigl(2q^{n^2-n-1}(q+1)^n+q^{n^2-n}(q+1)^n\bigr)\\&=q^{n^2-n-1}(q+1)^n(q-1)(q+2)\leqslant q^{n^2-n}(q+1)^{n+1}=q^{(d-r)/2}(q+1)^r,\end{aligned}$$

which concludes the last case. □

Acknowledgments

The authors thank the referees for helpful comments, and for pointing out the reference [17]. Both authors were supported by NSF grant DMS-0854849.

References

[1] S. Chowla, I.N. Herstein, W.K. Moore, On recursions connected with symmetric groups. I, Canad. J. Math. 3 (1951) 328–334.

[2] J. Goldman, G.-C. Rota, The number of subspaces of a vector space, in: Recent Progress in Combinatorics, Proc. Third Waterloo Conf. on Combinatorics, 1968, Academic Press, New York, 1969, pp. 75–83.

[3] D. Gorenstein, Centralizers of involutions in finite simple groups, in: Finite Simple Groups, Proc. Instructional Conf., Oxford, 1969, Academic Press, London, 1971, pp. 65–133.

[4] R. Gow, Real representations of the finite orthogonal and symplectic groups of odd characteristic, J. Algebra 96 (1) (1985) 249–274.

[5] L.C. Grove, Classical Groups and Geometric Algebra, Grad. Stud. Math., vol. 39, American Mathematical Society, Providence, RI, 2002.

[6] B. Klopsch, C. Voll, Igusa-type functions associated to finite formed spaces and their functional equations, Trans. Amer. Math. Soc. 361 (8) (2009) 4405–4436.

[7] V. Kac, P. Cheung, Quantum Calculus, Universitext, Springer-Verlag, New York, 2002.

[8] E. Kowalski, The Large Sieve and Its Applications. Arithmetic Geometry, Random Walks, and Discrete Groups, Cambridge Tracts in Math., vol. 175, Cambridge University Press, Cambridge, 2008.

[9] M.B. Kutler, C.R. Vinroot, On q-analogs of recursions for the number of involutions and prime order elements in symmetric groups, J. Integer Seq. 13 (3) (2010), Article 10.3.6, 12 pp.

[10] F. Lübeck, A.C. Niemeyer, C.E. Praeger, Finding involutions in finite Lie type groups of odd characteristic, J. Algebra 321 (11) (2009) 3397–3417.

[11] K. Morrison, Integer sequences and matrices over finite fields, J. Integer Seq. 9 (2) (2006), Article 06.2.1, 28 pp.

[12] A.C. Niemeyer, T. Popiel, C.E. Praeger, On proportions of pre-involutions in finite classical groups, J. Algebra 324 (5) (2010) 1016–1043.

[13] A. Nijenhuis, A.E. Solow, H.S. Wilf, Bijective methods in the theory of finite vector spaces, J. Combin. Theory Ser. A 37 (1) (1984) 80–84.

[14] M.K. Srinivasan, The Eulerian generating function of q-derangements, Discrete Math. 306 (17) (2006) 2134–2140.

[15] R.P. Stanley, Enumerative Combinatorics, vol. 1, Cambridge Stud. Adv. Math., vol. 49, Cambridge University Press, Cambridge, 1997.

[16] C.R. Vinroot, Character degree sums and real representations of finite classical groups of odd characteristic, J. Algebra Appl. 9 (4) (2010) 633–658.

[17] Z.X. Wan, Geometry of Classical Groups over Finite Fields, Studentlitteratur/Chartwell-Bratt Ltd., Lund/Bromley, 1993.