

Involutions and representations of the finite orthogonal groups

Student: Julio Brau

Advisors:

Dr. Ryan Vinroot

Dr. Klaus Lux

Spring 2007

Introduction

A linear representation of a group is a way of giving the group a structure of geometric symmetries. It is a very effective way to study groups because it allows us to reduce many of the problems of abstract groups to problems in linear algebra. The present research has the goal of understanding when it is possible to construct an involution model for the finite orthogonal groups. After some work, we have discovered that an involution model does not always exist for $O(n, q)$ and we conjecture that it does so only for $n \leq 5$.

We could effectively write out the sum of the degrees of the irreducible characters of the orthogonal groups as a polynomial in q . To do so we made use of the gaussian binomial coefficients. From writing out the sum of the degrees in this form we can say some things about the polynomial such as its degree, but we would like to be able to say more, such as whether or not it is reducible over \mathbb{Q} , although in specific cases it appears not to be. Throughout our research we made use of the computer algebra system GAP.

1 Representation theory

Definition. A *representation* of a group G is a group homomorphism

$$\pi : G \rightarrow GL_n(\mathbb{C})$$

where $GL_n(\mathbb{C})$ is the group of all invertible $n \times n$ matrices with entries in \mathbb{C} . The *degree* of the representation is n . When $n = 1$ we say that π is a *linear* representation.

Definition. Two representations π and π' are *equivalent* if there exists an invertible matrix T such that $\pi(g) = T^{-1}\pi'(g)T$ for all $g \in G$.

Definition. Let π be a representation of the group G . A *subrepresentation* of π is the restriction of the action of π to a subspace $U \subset V = \mathbb{C}^n$ such that U is invariant under all representation operators $\pi(g)$, i.e. $\pi(g)(U) \subseteq U \forall g \in G$.

Definition. A representation is said to be *irreducible* if there exists no non-trivial invariant subspace. We denote the set of all irreducible representations of a group G by $\text{Irr}(G)$.

Definition. Let π be a representation of a group G . The *character* of π is a function $\chi : G \rightarrow \mathbb{C}$ defined by

$$\chi(g) = \text{tr } \pi(g)$$

where tr denoted the trace of the matrix $\pi(g)$.

Recall that the trace function is well-defined since for two equivalent representations π_1 and π_2 of G , we have that $\pi_1(g) = T^{-1}\pi_2(g)T$ for all $g \in G$ and so consequently

$$\text{tr } \pi_1(g) = \text{tr } T^{-1}\pi_2(g)T = \text{tr } \pi_2(g)$$

for all $g \in G$. Often we will replace the term representation with the term character, for example, we will speak of a linear character, irreducible character, etc. Note also that $\chi(1)$ is just the trace of the identity matrix, so this equals the degree of the representation. A character is part of a more general class of functions of \mathbb{C}^G called *class functions*, which are functions of G that are constant on conjugacy classes. We now recall some basic definitions and results in character theory that we will often use.

Definition. Let G be a group. The *character table* of G is a square array of complex numbers with rows indexed by the inequivalent irreducible characters of G and the columns indexed by the conjugacy classes. The entry in row χ and column K is the value of χ on the conjugacy class K .

$$\begin{array}{c|ccc} & \dots & K & \dots \\ \hline \vdots & & \vdots & \\ \chi & \dots & \chi(K) & \\ \vdots & & & \end{array}$$

Definition. Let χ and ψ be characters of a group G . The *inner product* of χ and ψ is

$$[\chi, \psi] = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)}.$$

Theorem 1 *Let G be a group. The irreducible characters of G form an orthonormal basis for the vector space of all class functions of G with respect to the inner product $[\cdot, \cdot]$.*

Corollary 2 *Let χ be a character of G . Then χ is irreducible if and only if $[\chi, \chi] = 1$.*

2 Induced characters

The following concept provides a helpful method for compute the irreducible characters of a group G .

Definition. Let $H \leq G$ and let χ be a character of H . Then the *induced character* on G is given by

$$\chi^G(g) = \frac{1}{|H|} \sum_{x \in G} \chi^\circ(xgx^{-1}),$$

where χ° is defined by $\chi^\circ(h) = \chi(h)$ if $h \in H$ and $\chi^\circ(y) = 0$ if $y \notin H$.

Note that, in general, an induced irreducible character will not be an irreducible of G , however, we may then decompose that character to find new irreducibles of G . Of great help is the following

Lemma 3 (Frobenius Reciprocity) *Let $H \leq G$ and let ψ be a character of H and χ be a character of G . Then*

$$[\psi, \chi_H] = [\psi^G, \chi].$$

where χ_H is the restriction of χ to the subgroup H .

3 Bilinear and Quadratic forms

Definition. Let V be a vector space over a field F . A *bilinear form* on V is a function $B : V \times V \rightarrow F$ that is linear in each variable, that is, that satisfies

$$\begin{aligned} B(u + v, w) &= B(u, w) + B(v, w); \\ B(u, v + w) &= B(u, v) + B(u, w); \\ B(cu, v) &= cB(u, v); \\ B(u, cv) &= cB(u, v) \end{aligned}$$

for all $u, v, w \in V$ and all $c \in F$. We say then that B is a bilinear form on V .

If B is a bilinear form on V and $P = \{v_1, v_2, \dots, v_n\}$ is a basis for V then the matrix $A = [B(v_i, v_j)]$ is called the matrix of B relative to P . We also say that A is a representing matrix of B . If $u, v \in V$ and $u = \sum_i c_i v_i$ and $v = \sum_i b_i v_i$ then

$$B(u, v) = B\left(\sum_i c_i v_i, \sum_i b_i v_i\right) = \sum_{i,j} c_i B(v_i, v_j) b_j = C^t A B$$

where $C = (c_1, \dots, c_n)^t$ and $B = (b_1, \dots, b_n)^t$. Two matrices A and C of a form B relative to different basis of V are congruent, that is, $A = P^t C P$ for some invertible matrix P . In particular note that $\det A = (\det P)^2 \det C$. Since the determinant of the matrix of the form B depends on the choice of basis for V , we make the following definitions.

Definition. If F is a field, then we denote its multiplicative group of nonzero elements by F^* . Define $F^{\times 2} = \{a^2 : a \in F\}$. If A is a representing matrix of B then the *discriminant* of a bilinear form B is

$$\text{discr}(A) = \begin{cases} 0 & \text{if } \det A = 0 \\ (\det A)F^{\times 2} \in F^*/F^{\times 2} & \text{otherwise.} \end{cases}$$

Note that the discriminant function is well defined.

Definition. A bilinear form B is *nondegenerate* if $\text{discr}(B) \neq 0$.

Definition. A bilinear form B is *symmetric* if $B(u, v) = B(v, u)$ for all $v, u \in V$.

In this paper we will be interested only in nondegenerate symmetric bilinear forms. Given a symmetric bilinear form B on V we may define the *quadratic form* $Q : V \rightarrow F$ by $Q(v) = B(v, v)$. Note that the bilinear form B is also completely determined by the quadratic form Q . We will show that, when the field F is finite, there are exactly two inequivalent nondegenerate quadratic forms. To this end we make the following definitions.

Definition. Let B_1 and B_2 be bilinear forms on spaces V_1 and V_2 , respectively. We say that B_1 and B_2 are *equivalent* if there exists an isometry $\sigma : V_1 \rightarrow V_2$, that is, σ satisfies $B_2(\sigma v, \sigma w) = B_1(v, w)$ for all $v, w \in V_1$.

Proposition 4 *bilinear forms B_1, B_2 on spaces V_1 and V_2 are equivalent if and only if there exists bases for V_1 and V_2 such that $[B_1(v_i, v_j)] = [B_2(v_i, v_j)]$.*

Given a set of vectors $\{v_1, \dots, v_m\}$ we say that the set is orthogonal relative to the form B if $B(v_i, v_j) = 0 \forall i \neq j$.

Theorem 5 *Let B be a symmetric form on a vector space V . Then V has an orthogonal basis $\{v_1, \dots, v_n\}$ relative to which B has representing matrix*

$$A = \begin{pmatrix} b_1 & 0 & \dots & 0 \\ 0 & \ddots & & 0 \\ \vdots & & b_r & \vdots \\ 0 & \dots & & 0 \end{pmatrix},$$

where the $Q(v_i) = b_i \neq 0$.

In the past theorem one may choose v_1 so that b_1 could be any element in the image of Q . Afterwards at each stage we may choose v_i so that b_i can be any element in the image of the restriction of Q to the orthogonal complement of $\langle v_1, \dots, v_{i-1} \rangle$. With this in mind we also have that

Theorem 6 *If B is a nondegenerate symmetric bilinear form on a space V over a finite field F of dimension $n \geq 2$, then there is a basis for V relative to which the representing matrix $A = \text{diag}(1, \dots, 1, d), 0 \neq d \in F$.*

Since in the above theorem $\text{discr}(B) = d \cdot F^{\times 2}$ and $[F^* : F^{\times 2}] = 2$ then there are up to equivalence two nondegenerate symmetric bilinear (quadratic) forms over a space V , one with discriminant $1 \pmod{F^{\times 2}}$ and the other with discriminant $\neq 1 \pmod{F^{\times 2}}$.

4 Orthogonal groups

Let V be a vector space of dimension $n \geq 2$ over a field F with $\text{char } F \neq 2$ having a non-degenerate symmetric bilinear form.

Definition. The *orthogonal group* $O(V)$ consists of all isometries of V , that is,

$$O(V) = \{\tau \in GL(V) : B(\tau u, \tau v) = B(u, v), \text{ for all } u, v \in V\}.$$

Here $GL(V)$ denotes the general linear group of V , which consists of all invertible linear transformations of V . Note that $O(V) \leq GL(V)$. Let $\tau \in O(V)$. Suppose we choose a basis for V , and let T be the matrix representing τ relative to the basis. Then we have that $T^t A T = A$ where A is the matrix representing the form B relative to the basis. Then it follows that

$$(\det T)^2 \cdot \det A = \det A$$

so $\det T = \pm 1$.

When F is a finite field with q elements, the orthogonal group on V is finite and we denote it by $O(n, F_q)$.

Theorem 7 *Let V be a vector space over a finite field F . If n is even, there are exactly two non-isomorphic orthogonal groups over V . When n is odd, there is exactly one orthogonal group over V .*

Proof: First consider the case $n = 2k$. Recall that there are exactly two inequivalent nondegenerate quadratic forms, one with discriminant $1 \pmod{F^{\times 2}}$ and the other with discriminant $\neq 1 \pmod{F^{\times 2}}$. Let d be a nonsquare in F^* . We may choose an orthogonal basis relative to which the forms have representing matrix A given by

1. $A = \text{diag}(1, -1, 1, -1, \dots, 1, -1)$,
2. $A = \text{diag}(1, -1, 1, -1, \dots, 1, -d)$.

The discriminants of these forms are respectively given by $(-1)^k$ and $(-1)^k d \pmod{F^{\times 2}}$. If k is even then $(-1)^k = 1$ is a square and $(-1)^k d$ is a nonsquare. If k is odd then if -1 is a square then $-d$ is a nonsquare and if -1 is a nonsquare then $-d$ is a square. Then we always have that the discriminants

of these forms are square and nonsquare in some order, which implies that these are the two inequivalent forms.

Now suppose $n = 2k + 1$ is odd. Again we may choose basis so that the representing matrices of the forms are given by

$$(3) \quad A = \text{diag}(1, -1, 1, -1, \dots, 1, -1, -1),$$

$$(4) \quad A = \text{diag}(1, -1, 1, -1, \dots, 1, -1, -d).$$

The discriminants of these forms are respectively $(-1)^{k+1}$ and $(-1)^{k+1}d$ (mod $F^{\times 2}$) and by the same analysis as before these are a square and a non-square in some order. However note that if we replace the quadratic form Q by $Q^a(v) = aQ(v)$, then these two forms determine the same orthogonal group. Then if we scale Q by d in case 4 we obtain

$$A = \text{diag}(d, -d, d, -d, \dots, d, -d, -d^2),$$

where $\text{discr}A = (-1)^{k+1}d^{2k+2} \equiv (-1)^{k+1} \pmod{F^{\times 2}}$ which is the discriminant for the form of case 3. Thus these two forms determine the same orthogonal group and so when n is odd we have exactly one orthogonal group. ■

We shall denote the group of type 1 by $O^+(2n, q)$, of type 2 by $O^-(2n, q)$ and of type 3 by $O(2n + 1, q)$.

Theorem 8 *Let F_q be a finite field with $\text{char } F_q \neq 2$. Then*

1. $|O^+(2k, q)| = 2q^{k(k-1)}(q^k - 1) \prod_1^{k-1} (q^{2i} - 1),$
2. $|O^-(2k, q)| = 2q^{k(k-1)}(q^k + 1) \prod_1^{k-1} (q^{2i} - 1),$
3. $|O(2k + 1, q)| = 2q^{k^2} \prod_1^k (q^{2i} - 1).$

Definition. Let π be a representation of the group G . Then π is a *real* representation if we can choose a basis for $V = \mathbb{C}^n$ such that the corresponding matrix representation has image in $GL_n(\mathbb{R})$.

Definition. Let G be a group. A *model* for G is the direct sum of its irreducible characters each appearing with multiplicity one. That is, a model for a group G is

$$\sum_{\chi \in \text{Irr}(G)} \chi.$$

We wish to construct a model for the orthogonal groups by inducing linear characters of the centralizers of involutions in G . In other words, if x_1, x_2, \dots, x_n are a set of representatives of conjugacy classes of order 2 or 1 in G , then we say that an *involution model* of G is a set of linear characters $\{\chi_i\}$ where χ_i is a linear character of $C_G(x_i)$ and

$$\sum_{i=1}^n \text{Ind}_{C_G(x_i)}^G(\chi_i) = \sum_{\chi \in \text{Irr}(G)} \chi$$

Definition. Let G be a group and let χ be a character of G . The *Frobenius-Schur* indicator of χ is

$$\varepsilon(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

This indicator takes the values 1, 0 and -1 (See [4]). The Frobenius-Schur indicator will prove very useful as the following is also true.

Theorem 9 (Frobenius-Schur) *Let $\chi \in \text{Irr}(G)$. Then*

$$\varepsilon(\chi) \neq 0 \iff \chi \text{ is real valued.}$$

Proposition 10 (Frobenius-Schur) *Let G be a finite group such that $\varepsilon(\chi) = 1$ for every irreducible character χ of G . Then*

$$\sum_{\chi \in \text{Irr}(G)} \chi(1) = |\{g \in G \mid g^2 = 1\}|.$$

Theorem 11 (Gow, 1985) *If χ is any irreducible character of*

$$G = \begin{cases} O(2n+1, q) \\ O^+(2n, q) \\ O^-(2n, q) \end{cases}$$

with q odd, then $\varepsilon(\chi) = 1$.

These results imply that in the orthogonal groups the sum of the degrees of the irreducible characters is exactly equal to the number of elements whose square is the identity. Note that since two conjugate elements have the same order, then

$$|\{g \in G \mid g^2 = 1\}| = \sum_{a^2=1} |\text{cc}(a)| = \sum_{a^2=1} \frac{|G|}{|C_G(a)|}.$$

In $GL(n, q)$ there are exactly $n+1$ conjugacy classes of elements whose square is the identity, two of which are I and $-I$, where I denotes the identity matrix. Each conjugacy class has a representative that is a diagonal matrix with a certain number of 1's and -1's on the main diagonal. If the representative has k 1's and $n-k$ -1's then we will say that the conjugacy class represented by $(k, n-k)$. If we consider the $n-1$ conjugacy classes different from I and $-I$, then each of these classes splits into two distinct ones in the orthogonal group, giving us a total of $2n$ classes whose square is the identity. It follows from [6] that the centralizers of involutions in $O^\pm(n, q)$ are products of smaller orthogonal groups. Suppose first that $G = O^+(n, q)$. Wall showed that if C is a centralizer in $GL(n, q)$ of a conjugacy class represented by $(k, n-k)$ and it splits into centralizers C_1 and C_2 in G , then

$$|C_1| = |O^+(k, q) \times O^+(n-k, q)|$$

and

$$|C_2| = |O^-(n-k, q) \times O^-(k, q)|.$$

If $G = O^-(n, q)$ then

$$|C_1| = |O^+(k, q) \times O^-(n-k, q)|$$

and

$$|C_2| = |O^+(n-k, q) \times O^-(k, q)|.$$

Since we know the order of these groups, we may now compute for any pair of specific values of n and q the sum of the degrees of the irreducible characters. For example if we let $G = O^+(2, q)$ then

$$\begin{aligned} \sum_{\chi \in \text{Irr}(G)} \chi(1) &= 2 + \frac{|G|}{|O^+(1, q)||O^+(1, q)|} + \frac{|G|}{|O^-(1, q)||O^-(1, q)|} \\ &= 2 + \frac{2(q-1)}{4} + \frac{2(q-1)}{4} \\ &= q + 1. \end{aligned}$$

Using this same approach we can write a general formula for the sum of the degrees of the irreducibles. After doing some algebra and using the q -binomial coefficients we are able to do this.

Definition. We define the q -binomial coefficients, also called Gaussian binomials, by

$$\binom{m}{r}_q = \frac{(q^m - 1)(q^{m-1} - 1) \cdots (q^{m-r+1} - 1)}{(q - 1)(q^2 - 1) \cdots (q^r - 1)}.$$

Theorem 12 Let $\gamma(q) = \sum_{\chi \in \text{Irr}(G)} \chi(1)$. Then

(i) If $G = O(n, q)$ where $n = 2m + 1$ then

$$\sum_{\chi \in \text{Irr}(G)} \chi(1) = 2 \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} q^{(m - \lfloor k/2 \rfloor)(k+1)} \binom{m}{\lfloor \frac{k}{2} \rfloor}_{q^2}.$$

(ii) If $G = O^+(n, q)$ where $n = 2m$ and m is even, then

$$\begin{aligned} \sum_{\chi \in \text{Irr}(G)} \chi(1) &= \sum_{l=0}^{m-1} q^{2l(m-l-1) + (m-1)} (q^m - 1) \binom{m-1}{l}_{q^2} \\ &\quad + \sum_{l=0}^m q^{2l(m-l)} \binom{m}{l}_{q^2} + q^{\frac{m^2}{2}} \binom{m}{\frac{m}{2}}_{q^2}. \end{aligned}$$

(iii) If $G = O^+(n, q)$ where $n = 2m$ and m is odd, then

$$\begin{aligned} \sum_{\chi \in \text{Irr}(G)} \chi(1) &= \sum_{l=0}^{m-1} q^{2l(m-l-1)+(m-1)} (q^m - 1) \binom{m-1}{l}_{q^2} \\ &+ \sum_{l=0}^m q^{2l(m-l)} \binom{m}{l}_{q^2} + q^{\frac{m^2-1}{2}} (q^m - 1) \binom{m-1}{\frac{m-1}{2}}_{q^2}. \end{aligned}$$

(iv) If $G = O^-(n, q)$ where $n = 2m$ and m is even, then

$$\begin{aligned} \sum_{\chi \in \text{Irr}(G)} \chi(1) &= \sum_{l=0}^{m-1} q^{2l(m-l-1)+(m-1)} (q^m + 1) \binom{m-1}{l}_{q^2} \\ &+ \sum_{l=0}^m q^{2l(m-l)} \binom{m}{l}_{q^2} + q^{\frac{m^2}{2}} \binom{m}{\frac{m}{2}}_{q^2}. \end{aligned}$$

(v) If $G = O^-(n, q)$ where $n = 2m$ and m is odd, then

$$\begin{aligned} \sum_{\chi \in \text{Irr}(G)} \chi(1) &= \sum_{l=0}^{m-1} q^{2l(m-l-1)+(m-1)} (q^m + 1) \binom{m-1}{l}_{q^2} \\ &+ \sum_{l=0}^m q^{2l(m-l)} \binom{m}{l}_{q^2} + q^{\frac{m^2-1}{2}} (q^m - 1) \binom{m-1}{\frac{m-1}{2}}_{q^2}. \end{aligned}$$

Using the fact that the degree of $\binom{m}{k}_{q^2}$ equals $k(2m - k + 1)$ we have the following

Corollary 13 Let $\gamma(q) = \sum_{\chi \in \text{Irr}(G)} \chi(1)$. Then we have that

1. For $O(2k + 1, q)$, $\text{deg}(\gamma) = k(k + 1)$.
2. For $O^\pm(2k, q)$, $\text{deg}(\gamma) = k^2$.

The following GAP code defines a function which takes two inputs, a group G and a subgroup $H \leq G$, and it outputs the multiplicities of the induced linear characters of H to G .

```

indfunction:=function(g,h)
a:=CharacterTable(g);
b:=CharacterTable(h);
lin:=Filtered(Irr(b),x->x[1]=1);
ind:=Induced(b,a,Irr(b));
return List(ind,x->List(Irr(a),y->ScalarProduct(y,x)));
end;

```

Using this function we found an counterexample to there being an involution model for every orthogonal group. For $O(5, q)$ there does not exist an involution model since all of the linear characters of one of the centralizers is never multiplicity free when induced. However, for $n \leq 4$ the induced linear characters appear to always be multiplicity free, so this leads us to believe that $O(n, q)$ does have an involution model for this case. We have then the following

Conjecture. *Let $G = O^\pm(n, q)$ with q odd.*

1. *Let ψ be a linear character of a centralizer of a non-central involution of G . Then ψ^G is multiplicity free if and only if $n \leq 4$.*
2. *G has an involution model if and only if $n \leq 4$.*

Note that if part 1 is true then part 2 would follow. One of the steps in proving this conjecture would be to construct involution models for the orthogonal groups with $n \leq 4$. The following theorems show this for $n = 2$. The proof of the following theorem can be found in [2].

Theorem 14 *$O^+(2, q)$ is dihedral of order $2(q - 1)$ and $O^-(2, q)$ is dihedral of order $2(q + 1)$.*

The proof of the following theorem can be found in [7].

Theorem 15 *The dihedral groups have involution models.*

References

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

- [2] Grove, L. *Classical Groups and Geometric Algebra*. Graduate Studies in Mathematics, Volume 39. American Mathematical Society. 2001.
- [3] Grove, L. *Groups and Characters*. Wiley Interscience. 1997.
- [4] Isaacs, I.M. *Character theory of finite groups*. Academic Press. Pure and Applied Mathematics, No. 69. New York, 1976.
- [5] Sagan, E. Bruce *The Symmetric Group. Representations, Combinatorial Algorithms, and Symmetric Functions*. Graduate Texts in Mathematics. Springer-Verlag New York, 2001.
- [6] Wall, G.E. *On the conjugacy classes in the unitary orthogonal and symplectic groups*. J. Australian. Math. Soc. 3, (1962), 1-62.
- [7] Vinroot, Ryan C. *Involution models of finite Coxeter groups*. To appear in J. Group Theory.