Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 308 (2007) 612–628
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

The number of homomorphisms from finite groups to classical groups

Michael Bate

Christ Church College, Oxford OX1 1DP, UK

Received 6 March 2006

Available online 2 October 2006

Communicated by Jan Saxl

Abstract

We provide upper and lower bounds for the number of completely reducible homomorphisms from a finite group Γ to general linear and unitary groups over arbitrary finite fields, and to orthogonal and symplectic groups over finite fields of odd characteristic.
© 2006 Elsevier Inc. All rights reserved.

Keywords: Finite group; Classical group; Finite field; Completely reducible representation

1. Introduction

Let Γ be a finite group and let k be a finite field. Let K be the algebraic closure of k and suppose that G is one of the linear algebraic groups $\mathrm{GL}_n(K)$, $\mathrm{GO}_n(K)$ or $\mathrm{Sp}_n(K)$; we let V denote the natural n-dimensional KG-module. The finite general linear, unitary, orthogonal and symplectic groups all arise as finite subgroups of these algebraic groups fixed under particular Frobenius morphisms. Let F be such a morphism on G; denote the fixed points of F in G by G^F.

Given a homomorphism $\rho : \Gamma \to G$, we say that ρ is *completely reducible* if V is a completely reducible $K\Gamma$-module via ρ. Let $\mathrm{Hom}_{cr}(\Gamma, G)$ denote the set of completely reducible homomorphisms from Γ to G; note that if $|\Gamma|$ is coprime to the characteristic of K, then $\mathrm{Hom}_{cr}(\Gamma, G) = \mathrm{Hom}(\Gamma, G)$. In this paper we aim to estimate the size of $\mathrm{Hom}_{cr}(\Gamma, G)^F$ by providing upper and lower bounds; we express these bounds in terms of invariants associated to the representation theory of Γ over k and K, and other invariants associated to the order of

E-mail address: bate@maths.ox.ac.uk.

0021-8693/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2006.09.003

the classical group G^F. The approach we take is based on [7], where the case $G = \mathrm{GL}_n(K)$ and $G^F = \mathrm{GL}_n(k)$ is considered. We slightly extend the analysis in [7] by removing the restriction that $|\Gamma|$ and $|k|$ are coprime; the price we pay for this is to have to consider the representation theory of Γ in greater detail.

The paper is set out as follows. We begin by drawing together the basic definitions, results and notation needed in the sequel in Section 2. The material in this section is well known, so we do not give too much detail, but it is necessary to introduce a fair bit of notation in order to be able to state the main results, which we do in Section 3. Most of the remainder of the paper is devoted to proving the main results. The final section provides an example which illustrates a point raised in the main body of the paper.

2. Notation and preliminaries

Throughout the paper, Γ is a finite group, k is a finite field of characteristic p and K is the algebraic closure of k.

2.1. The orders of finite classical groups

In what follows, we need upper and lower bounds for the orders of finite classical groups. These orders are well known, see, for example, [2, 2.9] or [3, Chapter 2]. In order to bound the orders of the groups we are interested in, we need to introduce the (strictly positive) constant

$$\beta := \prod_{i=1}^{\infty} \bigl(1 - 2^{-i}\bigr). \tag{2.1.1}$$

It can be shown that $\beta \geqslant e^{-2}$ (consider the logarithm of the reciprocal of β). The constant β allows us to give the following bounds for the orders of finite classical groups:

$$\begin{aligned}
\beta q^{n^2} &\leqslant \bigl|\mathrm{GL}_n(q)\bigr| \leqslant q^{n^2},\\
\beta q^{\frac{1}{2}n(n+1)} &\leqslant \bigl|\mathrm{Sp}_n(q)\bigr| \leqslant q^{\frac{1}{2}n(n+1)},\\
2\beta q^{\frac{1}{2}n(n-1)} &\leqslant \bigl|\mathrm{GO}_n(q)\bigr| \leqslant 2q^{\frac{1}{2}n(n-1)} \quad \text{(see remark)},\\
\beta\left(\frac{q+1}{q}\right)q^{n^2} &\leqslant \bigl|\mathrm{GU}_n(q)\bigr| \leqslant \left(\frac{q+1}{q}\right)q^{n^2}.
\end{aligned} \tag{2.1.2}$$

Remark. We follow the notation of [3] for classical groups. In addition, when n is even, we use the notation $\mathrm{GO}_n(q)$ to denote either one of $\mathrm{GO}_n^{\pm}(q)$. These bounds are valid for orthogonal groups *in odd characteristic*, with one exception: the group $\mathrm{GO}_2^-(q)$ has order $2(q+1)$, which is greater than the upper bound given. We deal with this exception on a case-by-case basis as it arises. The lower bound is clearly still valid even in this case. Throughout the paper, we only consider orthogonal groups in odd characteristic.

Remark. There are many similar bounds for the orders of finite classical groups in the literature, e.g. see [8, Corollary 15]. The important feature of the bounds we give here is that the upper bounds are free of any constant, except the obvious and necessary factor of 2 for orthogonal

groups. With weaker upper bounds, especially for unitary groups, we would not be able to match the form of our upper and lower bounds in Theorems B, C and D (see Section 3), where the unitary groups play a rôle.

2.2. Frobenius maps and conjugacy

The finite classical groups in this paper all arise as finite subgroups of algebraic groups via Frobenius morphisms. Given an algebraic group G acting on an algebraic variety X, and a Frobenius morphism F on G and X, let G^F (respectively X^F) denote the fixed points of F on G (respectively X). For any $x \in X$, let $C_G(x)$ denote the stabilizer of x in G. If Z is an algebraic group which is stable under F, then we let $H^1(F, Z)$ denote Z modulo the equivalence relation: $x \sim y$ if and only if $x = zyF(z)^{-1}$ for some $z \in Z$. A well-known result of Springer–Steinberg relates G-orbits on X to G^F-orbits on X^F via this *Galois cohomology group*. The following result is taken from [9, I, 2.7].

Theorem 2.2.1. *Let G be a connected linear algebraic group and let F be a Frobenius map on G. Suppose X is an F-stable G-variety on which G acts transitively. Let $x \in X^F$ and set $C = C_G(x)$. Then $(G \cdot x)^F = (G \cdot x) \cap X^F$ consists of one G^F-orbit for every element of $H^1(F, C/C^0)$. In particular, if C is connected, then there is just one G^F-orbit.*

In order to apply this theorem to our analysis, we also need a result originally due to Freudenthal [4, §2, Satz], see also [5, Lemma 1.5]. Given a vector space V and a bilinear form ψ on V, we let $G(V, \psi) = \{g \in \mathrm{GL}(V) \mid \psi(gv, gw) = \psi(v, w) \text{ for all } v, w \in V\}$. When ψ is non-degenerate and symmetric (respectively alternating), then $G(V, \psi)$ is the corresponding orthogonal (respectively symplectic) group.

Theorem 2.2.2 *(Freudenthal). Suppose ψ is a symmetric or alternating bilinear form on a finite-dimensional K-vector space V, where K is an algebraically closed field, not of characteristic 2. Suppose also $x, y \in G = G(V, \psi)$ are such that there exists $g \in \mathrm{GL}(V)$ with $y = g^{-1}xg$. Then there exists $h \in G$ with $y = h^{-1}xh$.*

Remark 2.2.3. We can apply this result as follows. If $\rho, \theta : \Gamma \to G(V, \psi)$ are two representations of the finite group Γ in $G(V, \psi)$ such that there exists $g \in \mathrm{GL}(V)$ with $\theta(x) = g^{-1}\rho(x)g$ for all $x \in \Gamma$, then there exists $h \in G(V, \psi)$ such that $\theta(x) = h^{-1}\rho(x)h$ for all $x \in \Gamma$.

Remark 2.2.4. Theorem 2.2.2 is *not* true in general when K has characteristic 2; for example, conjugacy classes of involutions in symplectic and orthogonal groups are not so well behaved in characteristic 2. This obstruction is one of the main reasons we restrict attention to odd characteristic when dealing with symplectic and orthogonal groups; we do not have a result like that given in Remark 2.2.3 which allows us to control the orbits of representations in such a way.

2.3. Some representation theory

All modules in this paper are left modules. Let V be an n-dimensional $K\Gamma$-module and let $\mathcal{M} = \{M_1, \ldots, M_s\}$ be a basic set of irreducible $K\Gamma$-modules; set $d_i = \dim_K M_i$ for each i. We index the basic set so that M_1 is the trivial $K\Gamma$-module. Let V be an n-dimensional K-

vector space and suppose $\rho : \Gamma \to \mathrm{GL}(V)$ is a completely reducible representation of Γ. We may assume (by conjugating) that V decomposes as a direct sum

$$V = \bigoplus_{i=1}^{s} n_i M_i,$$

where $n_i M_i$ represents the direct sum of M_i with itself n_i times. Note that we have a formula relating the dimensions $n = \sum_{i=1}^{s} n_i d_i$. We shall also need to consider the quantity $\sum_{i=1}^{s} d_i^2$, which is the K-dimension of the socle of the group algebra $K\Gamma$; we let $\varsigma = \sum_{i=1}^{s} d_i^2$ denote this dimension. When the characteristic of K is coprime to $|\Gamma|$, we have $|\Gamma| = \varsigma$.

We shall use the following results, which are [6, Propositions 2.3, 2.4]; note that when we have a tensor product decomposition of a space, say $V = V_1 \otimes V_2$, and groups G_1 and G_2 acting on V_1 and V_2, respectively, we denote the product of G_1 and G_2 acting on the tensor product in the obvious way by $G_1 \otimes G_2$ (this is the notation used in [6]).

Proposition 2.3.1. *Let K be a field and let V be a K-vector space. Let L denote a subgroup of* $\mathrm{GL}(V)$ *which acts completely reducibly and homogeneously on V, with s absolutely irreducible summands of dimension r. Then*

(i) *there is a tensor decomposition $V = V_1 \otimes V_2$, where* $\dim V_1 = r$ *and* $\dim V_2 = s$, *such that* $L \subseteq \mathrm{End}(V_1) \otimes 1$ *and* $C_{\mathrm{GL}(V)}(L) = 1 \otimes \mathrm{GL}(V_2)$;
(ii) $C_{\mathrm{GL}(V)}(C_{\mathrm{GL}(V)}(L)) = \mathrm{GL}(V_1) \otimes 1$;
(iii) *the irreducible KL-submodules of V are precisely the subspaces $V_1 \otimes \langle v \rangle$, where $0 \neq v \in V_2$.*

Proposition 2.3.2. *Let $V = V_1 \otimes V_2$, and for $i = 1, 2$ let G_i be an absolutely irreducible subgroup of* $\mathrm{GL}(V_i)$. *Suppose $V_1 \otimes V_2$ is a self-dual module for $G_1 \otimes G_2$, then V_i is self-dual for G_i, for $i = 1, 2$.*

3. Results

We state our main results in this section for easy reference. Let Γ be a finite group, let k be a finite field of order q and let K denote the algebraic closure of k. Let ς denote the K-dimension of the socle of the group algebra $K\Gamma$; let δ_1 (respectively δ_{-1}) denote the number of isomorphism classes of self-dual $K\Gamma$-modules of symmetric (respectively alternating) type (see Section 5), and let $l = \delta_1 + \delta_{-1}$ denote the number of isomorphism classes of self-dual $K\Gamma$-modules. Given a classical group $H = H(q)$ over k, let $\mathrm{Hom}_{cr}(\Gamma, H)$ denote the set of completely reducible homomorphisms from Γ to H; i.e., the set of $\rho : \Gamma \to H$ such that the natural module for H is a completely reducible $k\Gamma$-module via ρ.

3.1. General linear and unitary groups

Our first two results are:

Theorem A. *Let n be a positive integer and let r denote the remainder when n is divided by ς. Then there exists an absolute constant β and a number $f = f(\varsigma)$, independent of q and n, such that*

$$\beta q^{(n^2-r^2)(1-\varsigma^{-1})} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GL}_n(q)\right)\right| \leqslant f q^{n^2(1-\varsigma^{-1})},$$

for all n and q.

Note that this result reduces to [7, Theorem] when $|\Gamma|$ is coprime to q, so that $\varsigma = |\Gamma|$.

Theorem B. *Let n, r, β and f be as in Theorem* A*, and let λ denote the number of isomorphism classes of $k\Gamma$-modules which admit a non-degenerate Γ-invariant Hermitian form. Then*

$$\beta\left(\frac{q}{q+1}\right)^{\lambda} q^{(n^2-r^2)(1-\varsigma^{-1})} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GU}_n(q)\right)\right| \leqslant f\left(\frac{q}{q+1}\right)^{\lambda} q^{n^2(1-\varsigma^{-1})},$$

for all n and q.

3.2. Orthogonal and symplectic groups

Given a self-dual irreducible $k\Gamma$-module M, we can extend scalars to K and form the self-dual completely reducible $K\Gamma$-module $M^K := M \otimes_k K$. The irreducible summands of M^K are either all self-dual, or none of them is self-dual.

Definition 3.2.1. Let $\chi = \chi(k, \Gamma)$ denote the number of isomorphism classes of self-dual $k\Gamma$-modules M such that the irreducible summands of M^K are not self-dual.

The number χ is a non-negative integer which depends upon Γ and the finite field k; however, if k'/k is an extension of finite fields, then $\chi(k', \Gamma) \leqslant \chi(k, \Gamma)$, so for fixed Γ and a given characteristic, these numbers are bounded above. Also, if k is a splitting field for Γ, then $\chi(k, \Gamma) = 0$.

Given a positive integer n, let r denote the remainder when n is divided by ς. Define Δ_1 and Λ_1, which depend on n, r, ς, δ_1 and δ_{-1}, as follows:

$$\Delta_1 = \frac{1}{2}n^2\left(1 - \frac{1}{\varsigma}\right) - \frac{1}{2}n\left(1 - \frac{(\delta_1 - \delta_{-1})}{\varsigma}\right),$$
$$\Lambda_1 = \frac{1}{2}r^2\left(1 - \frac{1}{\varsigma}\right) - \frac{1}{2}r\left(1 - \frac{(\delta_1 - \delta_{-1})}{\varsigma}\right).$$

The situation for orthogonal groups is complicated by the failure of our generic bounds in Eq. (2.1.2) for the group $\mathrm{GO}_2^-(q)$. Consequently, our next theorem comes in two parts:

Theorem C. *Suppose q is an odd prime power. There exists an absolute constant β and a number $f = f(\varsigma)$, independent of q and n, such that*

(i) *if $\mathrm{GO}_n(q) \neq \mathrm{GO}_2^-(q)$, then*

$$\left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GO}_n(q)\right)\right| \leqslant f q^{\frac{1}{8}l}\left(\frac{q}{q+1}\right)^{\chi} q^{\Delta_1}.$$

In case $\mathrm{GO}_n(q) = \mathrm{GO}_2^-(q)$, *then*

$$\left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GO}_2^-(q)\right)\right| \leqslant f q^{\frac{1}{8}l}\left(\frac{q}{q+1}\right)^{\chi-1} q^{\Delta_1}.$$

(ii) *If* $n/\varsigma < 1$ *or* $n/\varsigma \geqslant 3$, *then*

$$\beta q^{-\Lambda_1}\left(\frac{q}{q+1}\right)^{\chi} q^{\Delta_1} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GO}_n(q)\right)\right|.$$

In case $1 \leqslant n/\varsigma < 3$, *then*

$$\beta q^{-\Lambda_1}\left(\frac{q}{q+1}\right)^{\chi+\delta_1} q^{\Delta_1} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GO}_n(q)\right)\right|.$$

Let n be a positive even integer and let r be the remainder when ς divides $\frac{n}{2}$. Define Δ_{-1} and Λ_{-1}, which depend on n, r, ς, δ_1 and δ_{-1}, as follows:

$$\Delta_{-1} = \frac{1}{2}n^2\left(1 - \frac{1}{\varsigma}\right) + \frac{1}{2}n\left(1 - \frac{(\delta_1 - \delta_{-1})}{\varsigma}\right),$$
$$\Lambda_{-1} = 2r^2\left(1 - \frac{1}{\varsigma}\right) + r\left(1 - \frac{(\delta_1 - \delta_{-1})}{\varsigma}\right).$$

Our final theorem is

Theorem D. *Suppose* q *is an odd prime power. There exists an absolute constant* β *and a number* $f = f(\varsigma)$, *independent of* q *and* n, *such that*

$$\beta q^{-\Lambda_{-1}}\left(\frac{q}{q+1}\right)^{\chi} q^{\Delta_{-1}} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{Sp}_n(q)\right)\right| \leqslant f q^{\frac{1}{8}l}\left(\frac{q}{q+1}\right)^{\chi} q^{\Delta_{-1}}.$$

4. General linear and unitary groups

4.1. Centralizers

Let V be an n-dimensional K-vector space and let $G = \mathrm{GL}(V) \simeq \mathrm{GL}_n(K)$. Let F be a Frobenius morphism on G with fixed point subgroup $G^F \simeq \mathrm{GL}_n(q)$ or $\mathrm{GU}_n(q)$. Let ρ be a completely reducible F-stable homomorphism from Γ to G. Recall that we may assume that V decomposes as a direct sum

$$V = \bigoplus_{i=1}^{s} n_i M_i,$$

where $n_i M_i$ represents the direct sum of M_i with itself n_i times.

The centralizer of $\rho(\Gamma)$ in $\mathrm{GL}(V)$ is isomorphic to the group of units of the endomorphism ring $\mathrm{End}_{K\Gamma}(V)$. By Schur's lemma, we have $\mathrm{End}_{K\Gamma}(V) \simeq \bigoplus_{i=1}^{s} M_{n_i}(K)$, so that

$$C_{\mathrm{GL}(V)}(\rho) \simeq \prod_{i=1}^{s} \mathrm{GL}_{n_i}(K). \tag{4.1.1}$$

This also follows from Proposition 2.3.1. The centralizer is a connected subgroup of $\mathrm{GL}(V)$, so by Theorem 2.2.1, the intersection $G \cdot \rho \cap \mathrm{Hom}_{cr}(\Gamma, G^F)$ forms a single G^F-orbit.

Now $C_{G^F}(\rho) = C_G(\rho)^F$. If $G^F \simeq \mathrm{GL}_n(q)$, then $C_G(\rho)$ is isomorphic to a product of general linear groups over extensions of $\mathbb{F}_q$. Using the bounds for general linear groups from Eq. (2.1.2), we see that

$$\beta^s q^{\sum_{i=1}^{s} n_i^2} \leqslant \left|C_{G^F}(\rho)\right| \leqslant q^{\sum_{i=1}^{s} n_i^2}. \tag{4.1.2}$$

On the other hand, if $G^F \simeq \mathrm{GU}_n(q)$, then $C_G(\rho)$ is isomorphic to a product of general linear and unitary groups over extensions of $\mathbb{F}_{q^2}$. If we let λ denote the number of unitary factors in this centralizer, then our bounds from Eq. (2.1.2) show that

$$\beta^s \left(\frac{q+1}{q}\right)^{\lambda} q^{\sum_{i=1}^{s} n_i^2} \leqslant \left|C_{G^F}(\rho)\right| \leqslant \left(\frac{q+1}{q}\right)^{\lambda} q^{\sum_{i=1}^{s} n_i^2}. \tag{4.1.3}$$

Remark 4.1.4. To see clearly how the centralizer in the unitary case arises, one needs to consider what we are saying about the completely reducible $k\Gamma$-module U defined by the representation $\rho : \Gamma \to \mathrm{GU}_n(q) \subset \mathrm{GL}_n(q^2)$. This module decomposes as a direct sum of irreducible $k\Gamma$-modules $U = \bigoplus_{j=1}^{t} m_j N_j$; moreover, $U^K = V$. Since $\rho(\Gamma) \subseteq \mathrm{GU}_n(q)$, U admits a non-degenerate Hermitian form ψ which is fixed by $\rho(\Gamma)$ (a *Γ-invariant Hermitian form*). Now the restriction of ψ to a summand $m_j N_j$ of U is non-degenerate if and only if the irreducible module N_j also admits a Γ-invariant Hermitian form; it is in this case that we obtain a unitary factor in the centralizer. In the other cases, the summand $m_j N_j$ pairs up with another summand $m_{j'} N_{j'}$ so that the restriction of ψ to $m_j N_j \oplus m_{j'} N_{j'}$ is non-degenerate; moreover, in this case, $\dim_k N_j = \dim_k N_{j'}$ and $m_j = m_{j'}$. Each of these pairs contribute a single general linear factor to the centralizer. The detailed calculation of these centralizers is done by hand in [1], where explicit matrices are written down.

The upshot of this is that the number λ is equal to the number of isomorphism classes of irreducible $k\Gamma$-modules which admit a non-degenerate Γ-invariant Hermitian form.

4.2. Upper bounds

In order to derive our upper bounds we first need to analyze the sum $\sum_{i=1}^{s} n_i^2$ which appears in Eqs. (4.1.2) and (4.1.3). Recall that we also have $\sum_{i=1}^{s} n_i d_i = n$ and $\dim_K \mathrm{soc}\, K\Gamma = \varsigma = \sum_{i=1}^{s} d_i^2$. Following [7], set $t = n\varsigma^{-1}$ and let $r_i = n_i - t d_i$ for each i. Then

$$\begin{aligned}\sum_i n_i^2 &= t^2 \sum_i d_i^2 + 2t \sum_i r_i d_i + \sum_i r_i^2 \\ &= t^2 \varsigma + 2t \left(\sum_i \left(n_i d_i - t d_i^2\right) \right) + \sum_i r_i^2\end{aligned}$$

$$= n^2\varsigma^{-1} + 2t(n - t\varsigma) + \sum_i r_i^2$$

$$= n^2\varsigma^{-1} + \sum_i r_i^2.$$

Each r_i is an integer multiple of ς^{-1}, so that $\sum_i r_i^2 = u\varsigma^{-2}$ for some non-negative integer u. Conversely, given any non-negative integer u, there are no more than $(2\sqrt{u}+1)^s$ s-tuples $(r_1, \ldots, r_s)$ of integer multiples of ς^{-1} such that $\sum_i r_i^2 = u\varsigma^{-2}$. Using the lower bound from (4.1.2), and the upper bound for the order of $\mathrm{GL}_n(q)$ from (2.1.2), we can see that

$$\begin{aligned}\left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GL}_n(q)\right)\right| &\leqslant \sum_u \left(2\sqrt{u}+1\right)^s \beta^{-s} q^{n^2 - n^2\varsigma^{-1} - u\varsigma^{-2}} \\ &\leqslant q^{n^2(1-\varsigma^{-1})} \sum_u \left(2\sqrt{u}+1\right)^\varsigma \beta^{-\varsigma} 2^{-u\varsigma^{-2}},\end{aligned}$$

where the sums are taken over all non-negative integers u. Now the second sum converges and is bounded above by a number $f = f(\varsigma)$ depending only on ς, giving the upper bound

$$\left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GL}_n(q)\right)\right| \leqslant f q^{n^2(1-\varsigma^{-1})}, \tag{4.2.1}$$

for all n, q and all finite groups Γ.

The analysis for unitary groups is almost identical; we just have to use the lower bound from (4.1.3), and the upper bound for unitary groups from (2.1.2). We derive the upper bound in this case

$$\left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GU}_n(q)\right)\right| \leqslant f\left(\frac{q}{q+1}\right)^{\lambda-1} q^{n^2(1-\varsigma^{-1})}, \tag{4.2.2}$$

for all n, q and all finite groups Γ.

4.3. Lower bounds

To derive lower bounds, we construct an explicit F-stable representation from Γ to $G = \mathrm{GL}(V)$ and then work out a lower bound for the size of its G^F-orbit. Following [7], let n be a positive integer, and divide n by ς, giving $n = m\varsigma + r$ for non-negative integers m and r with $0 \leqslant r < \varsigma$. Let $M = \operatorname{soc} K\Gamma$ be the socle of the group algebra $K\Gamma$, which has dimension ς over K; then $M \simeq \bigoplus_{i=1}^s d_i M_i$, where the $M_i \in \mathcal{M}$ are the members of the basic set of $K\Gamma$-modules. Let T be the module formed from r copies of the trivial $K\Gamma$ module M_1. Then form the module $V := mM \oplus T$, which is an n-dimensional $K\Gamma$-module, and let $\rho : \Gamma \to \mathrm{GL}(V)$ denote the corresponding representation of Γ.

The left regular representation is clearly F-stable for any standard Frobenius map F; moreover, the matrix of any $x \in \Gamma$ under this representation is stable under the inverse-transpose map (with the obvious choice of basis). Since $M = \operatorname{soc} K\Gamma$ is the largest semisimple submodule of $K\Gamma$, this shows that M is F-stable for the Frobenius maps we are interested in. Thus, by extension, the representation ρ afforded by V is F-stable, so that $\rho : \Gamma \to G^F$. The module M_1

appears with multiplicity $md_1 + r$ as a summand of V, and $d_1 = 1$; for $i > 1$, $M_i \in \mathcal{M}$ has multiplicity md_i as a summand of V. By Eq. (4.1.2), if $G^F \simeq \mathrm{GL}_n(q)$, then

$$\left|C_{G^F}(\rho)\right| \leqslant q^{\sum_{i=1}^{s} m^2 d_i^2 + 2mr + r^2}.$$

On the other hand, if $G^F \simeq \mathrm{GU}_n(q)$, then Eq. (4.1.3) gives

$$\left|C_{G^F}(\rho)\right| \leqslant \left(\frac{q+1}{q}\right)^{\lambda} q^{\sum_{i=1}^{s} m^2 d_i^2 + 2mr + r^2},$$

where λ is again the number discussed in Remark 4.1.4. In either case we analyze the quantity $\sum_{i=1}^{s} m^2 d_i^2 + 2mr + r^2$, using the facts that $n = m\varsigma + r$ and $\sum_{i=1}^{s} d_i^2 = \varsigma$. Thus

$$\begin{aligned}\sum_{i=1}^{s} m^2 d_i^2 + 2mr + r^2 &= \left(n^2 - 2nr + r^2\right)\varsigma^{-1} + 2\left(nr - r^2\right)\varsigma^{-1} + r^2 \\ &= n^2\varsigma^{-1} + r^2\left(1 - \varsigma^{-1}\right).\end{aligned}$$

We can therefore find the following lower bounds:

$$\beta q^{(n^2-r^2)(1-\varsigma^{-1})} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GL}_n(q)\right)\right|, \tag{4.3.1}$$

and

$$\beta\left(\frac{q}{q+1}\right)^{\lambda-1} q^{(n^2-r^2)(1-\varsigma^{-1})} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GU}_n(q)\right)\right|, \tag{4.3.2}$$

for all n, q and all finite groups Γ.

4.4. Theorems A and B

The inequalities (4.2.1) and (4.3.1) give Theorem A, and (4.2.2) and (4.3.2) give Theorem B.

In [7], it is noted that the bounds for the order of $\mathrm{GL}_n(q)$ given in Eq. (2.1.2) allow us to rewrite our bounds as follows:

$$\beta q^{-r^2(1-\varsigma^{-1})}\left|\mathrm{GL}_n(q)\right|^{1-\varsigma^{-1}} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GL}_n(q)\right)\right| \leqslant f_1\left|\mathrm{GL}_n(q)\right|^{1-\varsigma^{-1}},$$

where f_1 is a slightly modified version of f. We can do the same for the unitary case, obtaining the bounds

$$\begin{aligned}&\beta\left(\frac{q}{q+1}\right)^{\lambda} q^{-r^2(1-\varsigma^{-1})}\left|\mathrm{GU}_n(q)\right|^{1-\varsigma^{-1}} \\ &\quad\leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GU}_n(q)\right)\right| \leqslant f_1\left(\frac{q}{q+1}\right)^{\lambda}\left|\mathrm{GU}_n(q)\right|^{1-\varsigma^{-1}}.\end{aligned}$$

5. Symplectic and orthogonal groups (char $k \neq 2$)

Throughout this section, the characteristic of k (hence K) is odd. We begin by relabeling our basic set $\mathcal{M}$ of $K\Gamma$-modules. Given a $K\Gamma$-module M, we let M^* denote the dual module, and say M is *self-dual* if $M \simeq M^*$ as $K\Gamma$-modules. Further, we say that a self-dual module is of *symmetric* (respectively *alternating*) *type* if the non-degenerate bilinear form corresponding to the isomorphism $M \simeq M^*$ is symmetric (respectively alternating). If M is a self-dual irreducible $K\Gamma$-module, then M is either of symmetric type or of alternating type, but not both. Let δ_1 (respectively δ_{-1}) denote the number of isomorphism classes of self-dual irreducible $K\Gamma$-modules of symmetric (respectively alternating) type, and set $l = \delta_1 + \delta_{-1}$. We index our basic set $\mathcal{M}$ as follows:

$$\mathcal{M} = \{M_1, \dots, M_l, M_{l+1}, M_{l+1}^*, \dots, M_s, M_s^*\},$$

where the first δ_1 modules are self-dual of symmetric type, the next δ_{-1} modules are self-dual of alternating type, and the final $2(s-l)$ modules come in dual pairs as shown.

Let V be a completely reducible n-dimensional $K\Gamma$-module and denote the corresponding representation by $\rho : \Gamma \to \mathrm{GL}(V)$. Suppose ψ is a non-degenerate symmetric or alternating bilinear form on V such that $\psi(\rho(x)v, \rho(x)w) = \psi(v, w)$ for all $v, w \in V$ and $x \in \Gamma$; we say V *admits a Γ-invariant bilinear form ψ*. Let $G = G(V, \psi)$ denote the subgroup of $\mathrm{GL}(V)$ consisting of the isometries of the form ψ. Since ψ is Γ-invariant, we have $\rho : \Gamma \to G$.

Since ψ induces a $K\Gamma$-isomorphism between V and V^*, the multiplicity of each M_i as a summand of V must be the same as the multiplicity of its dual M_i^*. Thus we have

$$V \simeq \bigoplus_{i=1}^{l} n_i M_i \oplus \bigoplus_{i=l+1}^{s} n_i \left(M_i \oplus M_i^*\right),$$

for non-negative integers n_i such that $n = \sum_{i=1}^{l} n_i d_i + \sum_{i=l+1}^{s} 2n_i d_i$. Furthermore, the restriction of ψ to the summands $n_i M_i$ $(1 \leqslant i \leqslant l)$ and $n_i(M_i \oplus M_i^*)$ $(l+1 \leqslant i \leqslant s)$ is non-degenerate.

5.1. Centralizers

First suppose that ψ is a symmetric bilinear form, so that $G \simeq \mathrm{GO}_n(K)$. Fix $1 \leqslant i \leqslant l$, let $W = n_i M_i$ and regard Γ as a subgroup of $\mathrm{GL}(W)$ via the restriction of ρ to W (we abuse notation here and identify Γ with its image under $\rho|_W$). The action of Γ on W is completely reducible and homogeneous, so by Proposition 2.3.1 there exists a tensor decomposition $W = W_1 \otimes W_2$ with $C_{\mathrm{GL}(W)}(\Gamma) = 1 \otimes \mathrm{GL}(W_2)$. The restriction of ψ to W is a non-degenerate symmetric bilinear form on W. Let C denote the subgroup of this centralizer fixing the form ψ. Then C is an irreducible subgroup of $\mathrm{GL}(W_2)$ and $W = W_1 \otimes W_2$ is a self-dual module for $\Gamma \otimes C$. By Proposition 2.3.2, W_2 is self-dual for C. Moreover, if $1 \leqslant i \leqslant \delta_1$, then W and W_1 are self-dual of symmetric type, so that W_2 must also be self-dual of symmetric type. On the other hand, if $\delta_1 + 1 \leqslant i \leqslant l$, then W is of symmetric type and W_1 is of alternating type, so that W_2 must be of alternating type. In the first case, we see that $C \simeq \mathrm{GO}_{n_i}(K)$, and in the second case, we have $C \simeq \mathrm{Sp}_{n_i}(K)$.

Now suppose $l + 1 \leqslant i \leqslant s$, and let $W = n_i(M_i \oplus M_i^*)$. We know that $C_{\mathrm{GL}(W)}(\Gamma) \simeq \mathrm{GL}_{n_i}(K) \times \mathrm{GL}_{n_i}(K)$, and that W is again a self-dual $K\Gamma$-module via the restriction of ψ to W.

This time, since the modules M_i and M_i^* are not isomorphic, the subgroup of this centralizer fixing the form is isomorphic to a single copy of $\mathrm{GL}_{n_i}(K)$ (after choice of a suitable basis with respect to ψ, we have elements $(a, b) \in \mathrm{GL}_{n_i}(K) \times \mathrm{GL}_{n_i}(K)$, and for such an element to fix ψ, we need $b = (a^\top)^{-1}$).

We conclude that

$$C_G(\rho) \simeq \prod_{i=1}^{\delta_1} \mathrm{GO}_{n_i}(K) \times \prod_{i=\delta_1+1}^{l} \mathrm{Sp}_{n_i}(K) \times \prod_{i=l+1}^{s} \mathrm{GL}_{n_i}(K). \tag{5.1.1}$$

An almost identical analysis when ψ is alternating, so that $G \simeq \mathrm{Sp}_n(K)$, yields in this case

$$C_G(\rho) \simeq \prod_{i=1}^{\delta_1} \mathrm{Sp}_{n_i}(K) \times \prod_{i=\delta_1+1}^{l} \mathrm{GO}_{n_i}(K) \times \prod_{i=l+1}^{s} \mathrm{GL}_{n_i}(K). \tag{5.1.2}$$

Now suppose that F is a Frobenius map on G such that $G^F \simeq \mathrm{GO}_n(q)$ when $G \simeq \mathrm{GO}_n(K)$ and $G^F \simeq \mathrm{Sp}_n(q)$ when $G \simeq \mathrm{Sp}_n(K)$. Suppose further that $\rho(\Gamma) \subseteq G^F$. Then $C_{G^F}(\rho) = C_G(\rho)^F$ is isomorphic to a product of orthogonal, symplectic, unitary and general linear groups over extensions of the finite field k. This time, the number of unitary factors is controlled by the number χ introduced in Definition 3.2.1. Again, extensive calculations can be found in [1] which explicitly determine these centralizers; it suffices for our purposes to stick to bounding their orders.

Let $\varepsilon = 1$ when G is orthogonal and $\varepsilon = -1$ when G is symplectic. The bounds from Eq. (2.1.2) give in these cases:

$$\left|C_{G^F}(\rho)\right| \geqslant \beta^s \left(\frac{q+1}{q}\right)^{\chi} q^{\kappa_\varepsilon}, \tag{5.1.3}$$

where we define κ_ε for $\varepsilon = \pm 1$ by

$$\kappa_\varepsilon = \sum_{i=1}^{\delta_1} \frac{1}{2} n_i(n_i - \varepsilon) + \sum_{i=\delta_1+1}^{l} \frac{1}{2} n_i(n_i + \varepsilon) + \sum_{i=l+1}^{s} n_i^2. \tag{5.1.4}$$

5.2. Upper bounds

For ease of exposition, we derive our upper bounds in several steps.

Step 1. Recall that we set $\varepsilon = \pm 1$ depending on whether G is orthogonal or symplectic. We are interested in the quantity κ_ε defined in Eq. (5.1.4). We have the additional equations

$$n = \sum_{i=1}^{l} n_i d_i + \sum_{i=l+1}^{s} 2 n_i d_i, \qquad \varsigma = \sum_{i=1}^{l} d_i^2 + \sum_{i=l+1}^{s} 2 d_i^2.$$

The analysis that follows mimics that for the general linear case but, because of the different factors in the centralizer, we have to be slightly more careful. Let $t = n\varsigma^{-1}$ and set $n_i = t d_i + r_i$ for $1 \leqslant i \leqslant s$. Then

$$
\begin{aligned}
2\kappa_\varepsilon &= \sum_{i=1}^{l} n_i^2 + \sum_{i=l+1}^{s} 2n_i^2 - \varepsilon\left(\sum_{i=1}^{\delta_1} n_i + \sum_{i=\delta_1+1}^{l_2} n_i\right) \\
&= t^2\left(\sum_{i=1}^{l} d_i^2 + \sum_{i=l+1}^{s} 2d_i^2\right) + 2t\left(\sum_{i=1}^{l} r_i d_i + \sum_{i=l+1}^{s} 2r_i d_i\right) + \left(\sum_{i=1}^{l} r_i^2 + \sum_{i=l+1}^{s} 2r_i^2\right) \\
&\quad - \varepsilon t\left(\sum_{i=1}^{\delta_1} d_i\right) + \varepsilon t\left(\sum_{i=\delta_1+1}^{l} d_i\right) - \varepsilon\left(\sum_{i=1}^{\delta_1} r_i\right) + \varepsilon\left(\sum_{i=\delta_1+1}^{l} r_i\right) \\
&= t^2\varsigma - \varepsilon t\delta_1 + \varepsilon t\delta_{-1} + 2t\left(\sum_{i=1}^{l} r_i d_i + \sum_{i=l+1}^{s} 2r_i d_i\right) \\
&\quad + \left(\sum_{i=1}^{\delta_1}\left(r_i^2 - \varepsilon r_i\right) + \sum_{i=\delta_1+1}^{l}\left(r_i^2 + \varepsilon r_i\right) + \sum_{i=l+1}^{s} 2r_i^2\right).
\end{aligned}
$$

Now, re-substituting $r_i = n_i - td_i$, we see that

$$\sum_{i=1}^{l} r_i d_i + \sum_{i=l+1}^{s} 2r_i d_i = n - t\varsigma = 0.$$

To complete our analysis, we first need to look at the remainder term

$$R_\varepsilon := \sum_{i=1}^{\delta_1}\left(r_i^2 - \varepsilon r_i\right) + \sum_{i=\delta_1+1}^{l}\left(r_i^2 + \varepsilon r_i\right) + \sum_{i=l+1}^{s} 2r_i^2. \tag{5.2.1}$$

From Eq. (5.2.1), we can see that

$$
\begin{aligned}
R_\varepsilon + \frac{1}{4}l &= \sum_{i=1}^{\delta_1}\left(r_i^2 - \varepsilon r_i + \frac{1}{4}\right) + \sum_{i=\delta_1+1}^{l}\left(r_i^2 + \varepsilon r_i + \frac{1}{4}\right) + \sum_{i=l+1}^{s} 2r_i^2 \\
&= \sum_{i=1}^{\delta_1}\left(r_i - \frac{\varepsilon}{2}\right)^2 + \sum_{i=\delta_1+1}^{l}\left(r_i + \frac{\varepsilon}{2}\right)^2 + \sum_{i=l+1}^{s} 2r_i^2 \\
&\geqslant 0,
\end{aligned}
\tag{5.2.2}
$$

so that $R_\varepsilon \geqslant -\frac{1}{4}l$.

Suppose, for the moment, that $G^F \neq \mathrm{GO}_2^-(q)$. Then the order of G^F is bounded above by $2q^{\frac{1}{2}n(n-\varepsilon)}$. Thus we can bound the size of the G^F-orbit O_ρ of ρ by

$$|O_\rho| = \left|G^F\right| / \left|C_{G^F}(\rho)\right| \leqslant 2\beta^{-s}\left(\frac{q}{q+1}\right)^{\chi} q^{\frac{1}{2}n(n-\varepsilon)-\kappa_\varepsilon}.$$

Finally, we set

$$\Delta_\varepsilon = \frac{1}{2}n^2\left(1-\frac{1}{\varsigma}\right) - \frac{1}{2}\varepsilon n\left(1-\frac{(\delta_1-\delta_{-1})}{\varsigma}\right), \tag{5.2.3}$$

and note that $s \leqslant \varsigma$ so that $\beta^{-s} \leqslant \beta^{-\varsigma}$. We can therefore bound the size of the orbit of ρ above as follows:

$$|O_\rho| \leqslant 2\beta^{-\varsigma}\left(\frac{q}{q+1}\right)^{\chi} q^{\Delta_\varepsilon - \frac{1}{2}R_\varepsilon}. \tag{5.2.4}$$

In the exceptional case that $G^F = \mathrm{GO}_2^-(q)$, the upper bound for the order of G^F is no longer valid; however, if we write $|G^F| = 2q(\frac{q+1}{q})$, then in this case we can achieve the slightly altered bound

$$|O_\rho| \leqslant 2\beta^{-\varsigma}\left(\frac{q}{q+1}\right)^{\chi-1} q^{\Delta_1 - \frac{1}{2}R_1}. \tag{5.2.5}$$

Step 2. Since $C_G(\rho)$ is no longer connected, each G-orbit may correspond to several G^F-orbits; the number of G^F-orbits is controlled by Theorem 2.2.1. First suppose that G is symplectic, hence connected. The centralizer of ρ has at most δ_{-1} non-connected factors, which gives at most $2^{\delta_{-1}}$ G^F-orbits corresponding to ρ. Note that this number is independent of ρ and, since $\delta_{-1} < \varsigma$, it is bounded above by a function depending only on ς, namely 2^ς.

Now suppose G is orthogonal. Since G is not connected, we cannot apply Theorem 2.2.1 directly. Instead, consider the identity component $G^0 = \mathrm{SO}_n(K)$ of G. The index of $C_{G^0}(\rho)$ in $C_G(\rho)$ is at most 2, so $C_{G^0}(\rho)$ also has at most δ_1 non-connected factors, which gives at most 2^{δ_1} $(G^0)^F$-orbits corresponding to ρ. Now there are two possibilities to consider. Suppose first that the G-orbit of ρ is the same as the G^0-orbit of ρ; then the number of $(G^0)^F$-orbits corresponding to the G^0-orbit of ρ equals the number of G^F-orbits corresponding to the G-orbit of ρ. The other possibility is that the G-orbit of ρ splits into 2 G^0-orbits. In this case, however, the two G^0-orbits can be fused by an F-stable element of $G \setminus G^0$, so the number of $(G^0)^F$-orbits corresponding to ρ still equals the number of G^F-orbits corresponding to ρ. In either case, then, we again get no more than $2^{\delta_1} \leqslant 2^\varsigma$ G^F-orbits corresponding to ρ.

Step 3. Each representation $\rho : \Gamma \to G$ corresponds to a remainder term R_ε given by the formula in Eq. (5.2.1). Since each r_i is an integer multiple of ς^{-1}, the formula for $R_\varepsilon + \frac{1}{4}l$ given in Eq. (5.2.2) shows that $R_\varepsilon + \frac{1}{4}l = \frac{u}{(2\varsigma)^2}$ for some non-negative integer u. Thus we have

$$\begin{aligned}
-\sqrt{u} + \varepsilon\varsigma \leqslant 2\varsigma r_i \leqslant \sqrt{u} + \varepsilon\varsigma \quad &\text{for } 1 \leqslant i \leqslant \delta_1,\\
-\sqrt{u} - \varepsilon\varsigma \leqslant 2\varsigma r_i \leqslant \sqrt{u} - \varepsilon\varsigma \quad &\text{for } \delta_1 + 1 \leqslant i \leqslant l,\\
-\sqrt{\frac{u}{2}} \leqslant 2\varsigma r_i \leqslant \sqrt{\frac{u}{2}} \quad &\text{for } l+1 \leqslant i \leqslant s.
\end{aligned}$$

In particular, there are no more than $(\sqrt{u}+1)^s$ possible s-tuples $(r_1, \ldots, r_s)$ of the correct form giving such a remainder. Since each s-tuple uniquely defines the corresponding s-tuple $(n_1, \ldots, n_s)$, and thus uniquely defines the G-orbit of ρ, by Theorem 2.2.2, this gives an upper

bound for the number of orbits giving such a remainder R_ε. Moreover, since $s \leqslant \varsigma$, we have a bound depending only on u and ς.

Step 4. Suppose that $G^F \neq \mathrm{GO}_2^-(q)$. By Steps 1 and 2, each G-orbit contributes at most $2^{\varsigma+1}\beta^{-\varsigma}(\frac{q}{q+1})^\chi q^{\Delta_\varepsilon - \frac{1}{2}R_\varepsilon}$ representations from Γ to G^F, and Step 3 bounds the number of orbits which can give a particular value of $R_\varepsilon = \frac{u}{(2\varsigma^2)} - \frac{1}{4}l$. Thus

$$\left|\mathrm{Hom}_{cr}\left(\Gamma, G^F\right)\right| \leqslant \sum_u \left(\sqrt{u}+1\right)^\varsigma 2^{\varsigma+1}\beta^{-\varsigma}\left(\frac{q}{q+1}\right)^\chi q^{\Delta_\varepsilon - \frac{u}{8\varsigma^2}+\frac{1}{8}l},$$

where the sum is taken over all non-negative integers u. Bringing out all terms not dependent on u, we obtain an infinite sum $\sum_u(\sqrt{u}+1)^\varsigma q^{-u/8\varsigma^2}$, which converges and is bounded above by a function of ς, independent of n and q. Absorbing all other terms dependent only on ς into a single function $f(\varsigma)$, we obtain the bound

$$\left|\mathrm{Hom}_{cr}\left(\Gamma, G^F\right)\right| \leqslant f(\varsigma)\left(\frac{q}{q+1}\right)^\chi q^{\Delta_\varepsilon+\frac{1}{8}l}. \tag{5.2.6}$$

The remaining case $G^F = \mathrm{GO}_2^-(q)$ gives the same bound, but with χ replaced by $\chi - 1$.

Remark 5.2.7. The factor of $q^{\frac{1}{8}l}$ in these bounds may at first appear to be just an artefact of the proof. However, in Section 6 we provide a simple example which indicates that in general we do need some sort of correcting factor to make the bounds work. We believe that the factor we have included here may be the best one can do in this generality.

5.3. Lower bounds

We find lower bounds in a similar way to those obtained for general linear and unitary groups. We begin by considering orthogonal groups. Let n be a positive integer and write $n = m\varsigma + r$, where M is a non-negative integer and $0 \leqslant r < \varsigma$. Consider the $K\Gamma$-module $M = \mathrm{soc}\, K\Gamma$ and let $V = mM \oplus T$, where T is formed from r copies of the trivial module M_1. We consider the summands of V in turn.

The trivial module appears with multiplicity $m + r$ as a summand of V, and each copy admits an obvious symmetric bilinear form. Similarly, for each $2 \leqslant i \leqslant \delta_1$, the module M_i appears with multiplicity md_i, and each copy of M_i admits a non-degenerate Γ-invariant symmetric bilinear form.

For $\delta_1 < i \leqslant l$, the module M_i appears with multiplicity md_i and, since M_i has alternating type, md_i is even. We therefore have $md_i/2$ pairs of summands $M_i \oplus M_i$, on which we can construct a non-degenerate Γ-invariant symmetric bilinear form using the alternating form admitted by each copy of M_i.

For $l + 1 \leqslant i \leqslant s$, the module $M_i \oplus M_i^*$ appears with multiplicity md_i. Again, each of these summands admits a non-degenerate Γ-invariant symmetric bilinear form (given by a matrix $\left(\begin{smallmatrix} 0 & I \\ I & 0 \end{smallmatrix}\right)$ with respect to a basis of M_i and a dual basis of M_i^*).

Combining all these forms, we see that V admits a non-degenerate Γ-invariant symmetric bilinear form, ψ say. Thus the representation ρ afforded by V is a homomorphism $\rho : \Gamma \to G =$

$G(V,\psi) \simeq \mathrm{GO}_n(K)$. Moreover, by the argument given in Section 4.3, ρ is F-stable for any Frobenius morphism F we are interested in. Thus $\rho : \Gamma \to G^F \simeq \mathrm{GO}_n(q)$.

By our centralizer calculations in Section 5.1,

$$C_G(\rho) \simeq \mathrm{GO}_{m+r}(K) \times \prod_{i=2}^{\delta_1} \mathrm{GO}_{md_i}(K) \times \prod_{i=\delta_1+1}^{l} \mathrm{Sp}_{md_i}(K) \times \prod_{i=l+1}^{s} \mathrm{GL}_{md_i}(K).$$

Suppose, for the moment, that $m \geqslant 3$, so that there are no factors of GO_2^- in $C_{G^F}(\rho)$. Then

$$\left|C_{G^F}(\rho)\right| \leqslant 2^{\delta_1} \left(\frac{q+1}{q}\right)^{\chi} q^{\kappa},$$

where

$$2\kappa = (m+r)(m+r-1) + \sum_{i=2}^{\delta_1} md_i(md_i-1) + \sum_{i=\delta_1+1}^{l} md_i(md_i+1) + \sum_{i=l+1}^{s} 2m^2 d_i^2.$$

Using the facts that $m = (n-r)\varsigma^{-1}$ and $\sum_{i=1}^{l} d_i^2 + \sum_{i=l+1}^{s} 2d_i^2 = \varsigma$, we can rearrange the right-hand side to obtain

$$2\kappa = \frac{n^2}{\varsigma} - \frac{n(\delta_1 - \delta_{-1})}{\varsigma} + r^2\left(1 - \frac{1}{\varsigma}\right) - r\left(1 - \frac{(\delta_1 - \delta_{-1})}{\varsigma}\right).$$

Thus we write

$$\Lambda_1 = \frac{1}{2}r^2\left(1 - \frac{1}{\varsigma}\right) - \frac{1}{2}r\left(1 - \frac{(\delta_1 - \delta_{-1})}{\varsigma}\right),$$

and, using the bound $|G^F| \geqslant 2\beta q^{\frac{1}{2}n(n-1)}$, obtain a lower bound for the size of the G^F-orbit O_ρ of ρ:

$$|O_\rho| \geqslant \beta 2^{1-\delta_1} \left(\frac{q}{q+1}\right)^{\chi} q^{\Delta_1 - \Lambda_1},$$

where Δ_1 is the number defined in Eq. (5.2.3). Now $C_G(\rho)$ has exactly δ_1 non-connected factors, so the G-orbit of ρ corresponds to at least $2^{\delta_1 - 1}$ G^F-orbits, by Theorem 2.2.1; note that we subtract 1 since in order to apply the theorem we must pass to $G^0 \simeq \mathrm{SO}_n(K)$, which has index two in G, and we may lose one non-connected factor. Thus we can multiply our bound by $2^{\delta_1 - 1}$ and obtain the bound

$$\beta\left(\frac{q}{q+1}\right)^{\chi} q^{\Delta_1 - \Lambda_1} \leqslant \left|\mathrm{Hom}_{cr}\big(\Gamma, \mathrm{GO}_n(q)\big)\right|. \tag{5.3.1}$$

Note that if $m = 0$, then $r = n$ and $\Lambda_1 = \Delta_1$, so this bound is also valid in this case. Thus, we are left with the possibility that $m = 1$ or 2. In these cases, we may have up to δ_1 factors of GO_2^- in our centralizer, so that the upper bound for its order is no longer valid. To get round this

problem, we note that $|\mathrm{GO}_2^-(q)| = 2(\frac{q+1}{q})q$, and therefore make our bound slightly smaller by multiplying by $(\frac{q}{q+1})^{\delta_1}$, giving

$$\beta\left(\frac{q}{q+1}\right)^{\chi+\delta_1} q^{\Delta_1-\Lambda_1} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{GO}_n(q)\right)\right|. \tag{5.3.2}$$

We do not provide all the details for the symplectic groups, but note a few key points. This time we have a positive even integer $n = 2n'$, say. Divide n' by ς, so that $n' = m\varsigma + r$, where $0 \leqslant r < \varsigma$, and form the (self-dual) $K\Gamma$-module $V' = mM \oplus T$, where $M = \mathrm{soc}\, K\Gamma$ and T is formed from r copies of the trivial module. Then $V = V' \oplus V'$ is an n-dimensional $K\Gamma$-module, stable under a standard Frobenius map F; moreover, each V' is self-dual of symmetric type, so we can construct a non-degenerate Γ-invariant *alternating* bilinear form on V by taking the form with matrix $\left(\begin{smallmatrix} 0 & \varphi \\ -\varphi & 0 \end{smallmatrix}\right)$, where φ is the matrix of the symmetric form on V'. If we let ρ denote the representation afforded by V, then this time we get $G \simeq \mathrm{Sp}_n(K)$, and

$$C_G(\rho) \simeq \mathrm{Sp}_{2m+2r}(K) \times \prod_{i=2}^{\delta_1} \mathrm{Sp}_{2md_i}(K) \times \prod_{i=\delta_1+1}^{l} \mathrm{GO}_{2md_i}(K) \times \prod_{i=l+1}^{s} \mathrm{GL}_{2md_i}(K).$$

Note that this time, since for $\delta_1 + 1 \leqslant i \leqslant l$ the modules M_i have dimension at least 2 (they admit alternating forms), we do not have to worry about GO_2^- factors in $C_{G^F}(\rho)$. Using our previous calculations as we did for the orthogonal case, we obtain

$$\beta\left(\frac{q}{q+1}\right)^{\chi} q^{\Delta_{-1}-\Lambda_{-1}} \leqslant \left|\mathrm{Hom}_{cr}\left(\Gamma, \mathrm{Sp}_n(q)\right)\right|, \tag{5.3.3}$$

where Δ_{-1} is defined in Eq. (5.2.3) and

$$\Lambda_{-1} = 2r^2\left(1 - \frac{1}{\varsigma}\right) + r\left(1 - \frac{(\delta_1 - \delta_{-1})}{\varsigma}\right).$$

5.4. Theorems C and D

The inequalities (5.2.6), (5.3.1), (5.3.2) and (5.3.3) prove Theorems C and D. Note that in this case it is not possible to rewrite the bounds in terms of the order of the classical group concerned, but the factors of q^{Δ_ε} for $\varepsilon = \pm 1$ compare favorably with these orders. Indeed, in specific cases, e.g. for certain cyclic groups, one could rewrite the bounds in an analogous way to those for general linear and unitary groups.

6. Example

We provide, as promised in Remark 5.2.7, a very simple example to show that the factor of $q^{\frac{1}{8}l}$ in the upper bounds for orthogonal groups is needed. Let $\Gamma = S_3$, the symmetric group on 3 letters, and suppose k is a finite field of order q, where q is an odd prime power such that the group algebra $k\Gamma$ is semisimple. Then $\varsigma = |\Gamma| = 6$. There are up to isomorphism three irreducible $k\Gamma$-modules: the trivial module, which we denote by M_1; the module afforded by the

sign representation, denoted M_2; a two-dimensional irreducible, denoted M_3. These modules are all self-dual of symmetric type, so that $\delta_1 = 3$, $\delta_{-1} = 0$ and $l = 3$.

Let $n = 4$ and let $V = M_1 \oplus M_2 \oplus M_3$ be a four-dimensional representation of Γ. Since each M_i is self-dual, we see that we can view this representation as a homomorphism $\rho : \Gamma \to \mathrm{GO}_4(q)$ (it does not matter whether it is $+$ or $-$ type). Denote the centralizer of ρ in $\mathrm{GO}_4(q)$ by C; then $C \simeq \mathrm{GO}_1(q) \times \mathrm{GO}_1(q) \times \mathrm{GO}_1(q)$. Thus the size of the orbit of ρ is a polynomial in q with largest power q^6.

For this set-up, we can calculate

$$\Delta_1 = \frac{1}{2} \cdot 4^2 \cdot \left(1 - \frac{1}{6}\right) - \frac{1}{2} \cdot 4\left(1 - \frac{(3-0)}{6}\right) = \frac{17}{3} < 6.$$

Thus, as q increases, the size of the orbit of ρ is greater than any fixed multiple of q^{Δ_1}. On the other hand, $\Delta_1 + \frac{1}{8}l > 6$, so that the upper bound given in Theorem B is still valid.

This example shows why we need in general to include the factor of $q^{\frac{1}{8}l}$ in our upper bounds; similar examples are easily constructed for the symplectic case. Note that the representation ρ provides a stronger lower bound in this particular case.

Acknowledgments

The author thanks Gerhard Röhrle and Geoff Robinson for helpful conversations during the early stages of this work. Martin Liebeck and Chris Parker have also provided useful insight, in particular, directing me towards the results I used from [6], which considerably shortened the arguments in Section 5.

References

[1] M. Bate, The number of homomorphisms from finite groups to classical groups, PhD thesis, University of Birmingham, UK, 2006.
[2] R.W. Carter, Finite Groups of Lie type, Conjugacy Classes and Complex Characters, Wiley, New York, 1985.
[3] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups, Clarendon Press, Oxford, 1985.
[4] H. Freudenthal, Elementatteilertheorie der Komplexen Ortogonalen und Symplektischen Gruppen, Indag. Math. 14 (1952) 199–201.
[5] J.C. Jantzen, Nilpotent orbits in representation theory, in: Lie Theory, in: Progr. Math., vol. 228, Birkhäuser Boston, Boston, 2004, pp. 1–211.
[6] M.W. Liebeck, G. Seitz, On the subgroup structure of classical groups, Invent. Math. 134 (1998) 427–453.
[7] M.W. Liebeck, A. Shalev, The number of homomorphisms from a finite group to a general linear group, Comm. Algebra 32 (2004) 657–661.
[8] C.W. Parker, R.A. Wilson, Recognising simplicity in black-box groups, preprint, 2005.
[9] T.A. Springer, R. Steinberg, Conjugacy classes, in: Seminar on Algebraic Groups and Related Finite Groups, in: Lecture Notes in Math., vol. 131, Springer-Verlag, Heidelberg, 1970, pp. 167–266.