The Steinberg lattice of a finite Chevalley group and its modular reduction

Roderick Gow

Mathematics Department, University College, Belfield, Dublin 4, Ireland

1 Introduction

Let p be a prime and let $q = p^a$, where a is a positive integer. Let $G = G(\mathbb{F}_q)$ be a Chevalley group over $\mathbb{F}_q$, with associated system of roots Φ and Weyl group W. Steinberg showed in 1957 that G has an irreducible complex representation whose degree equals the p-part of $|G|$, [11]. This representation, now known as the Steinberg representation, has remarkable properties, which reflect the structure of G, and there have been many research papers devoted to its study. The module constructed in [11] is in fact a right ideal in the integral group ring $\mathbb{Z}G$ of G, and is thus a $\mathbb{Z}G$-lattice, which we propose to call the Steinberg lattice of G. It should be noted that lattices not integrally isomorphic to the Steinberg lattice may also afford the Steinberg representation, and such lattices may differ considerably in their properties compared with the Steinberg lattice.

In this paper, we will describe the G-invariant integral symmetric bilinear form f defined on the Steinberg lattice. Using the linear characters of a Sylow p-subgroup of G, we will find certain elementary divisors of the Gram matrix D of f. These elementary divisors provide information about the composition factors of the Steinberg lattice when it is reduced modulo any prime. In Section 5, we provide two examples to see whether our knowledge of these elementary divisors is sufficient for us to deduce a composition series for the modular reduction of the Steinberg lattice when $G = B_2(\mathbb{F}_q)$. We conclude the paper in Section 6 by showing that our results provide the fullest information about the elementary divisors of D when $G = A_n(\mathbb{F}_q)$, and we formulate a conjecture about the composition factors of the modular reduction of the Steinberg lattice in this case.

2000 *Mathematics Subject Classification* 20C15, 20C20, 20C33

2 The invariant integral symmetric bilinear form

We refer the reader to the book [1] for an exposition of the theory of Chevalley groups. Let Φ^+ denote a set of positive roots in Φ. Given a root r, we will write $r > 0$ if r is positive and $r < 0$ if r is negative. Let Π denote the corresponding set of fundamental roots in Φ^+. G is generated by root subgroups X_r, where r ranges over Φ. The root subgroups X_r, where r ranges over Φ^+, generate a Sylow p-subgroup subgroup U of G, of order q^N, where $N = |\Phi^+|$. Let B denote the normalizer of U in G. The decomposition of G into B,B–double cosets is labelled by the elements of the Weyl group W. Specifically, there are elements n_w of G defined for each element w of W such that G is the disjoint union of the double cosets Bn_wB, as w runs over W. We let U_w^+ denote the subgroup $U \cap (n_w^{-1}Un_w)$ of U. U_w^+ is generated by those root subgroups X_r where $r > 0$ and $w(r) > 0$, and its order is $q^{N-\ell(w)}$, where $\ell(w)$ is the number of positive roots that w maps into negative roots. There is a corresponding subgroup U_w^- of U generated by those root subgroups X_r where $r > 0$ and $w(r) < 0$. U is factorized as a product $U_w^+U_w^-$ of these two subgroups. We also use the homomorphism ε from W onto the group $\{1,-1\}$ of two elements. We have

$$\varepsilon(w) = (-1)^{\ell(w)}$$

and we may identify ε with the determinant function of the natural representation of W.

Consider the element

$$e = \sum_{b\in B} b \sum_{w\in W} \varepsilon(w)n_w,$$

in $\mathbb{Z}G$. The right ideal $e\mathbb{Z}G$ is the Steinberg lattice which we will investigate in this paper. It will be more convenient for our subsequent work to replace the ring $\mathbb{Z}$ by a principal ideal domain R of characteristic 0 which contains a primitive p-th root of unity. We will be more specific about R later. We let I denote the RG-lattice eRG, which we shall call the Steinberg lattice over R. In the case that $p = 2$, we may take $R = \mathbb{Z}$. One of Steinberg's main results, [11, Theorem 1], is that the $|U|$ elements eu, where u runs over the elements of U, form a free basis of I, and this fact enables us to make calculations in I.

There is a natural G-invariant non-degenerate symmetric bilinear form $F : RG \times RG \to R$ given by

$$F(g,h) = \delta_{g,h},$$

where g and h are elements of G, and $\delta_{g,h} = 1$ if $g = h$, $\delta_{g,h} = 0$ otherwise. Restriction of F to $I \times I$ determines a non-degenerate G-invariant symmetric bilinear form, and we shall now evaluate F on the free basis of I just described.

Given $u \in U$, we set

$$c_W(u) = |\{\, w \in W : n_w u n_w^{-1} \in U \,\}|.$$

Thus $c_W(u)$ is the size of a non-empty subset of W, with $c_W(1) = |W|$. In view of our earlier discussion, we can also write

$$c_W(u) = |\{\, w \in W : u \in U_w^+ \,\}|.$$

2.1 Lemma Let u_1 and u_2 be elements of U. Then we have

$$F(eu_1, eu_2) = |B| c_W(u_2 u_1^{-1}).$$

Proof: As F is U-invariant, it suffices to show that $F(e, eu) = |B|c_W(u)$ for $u \in U$. A typical component of eu has the form $bn_w u$, with coefficient ±1. To calculate $F(e, eu)$, we need to know when such an element $bn_w u$ is expressible in the form $b' n_x$, where $b' \in B$ and $x \in W$. We note here that $n_w u \in Bn_x$ if and only if each of the $|B|$ elements $bn_w u$, as b runs over B, is also in Bn_x. This accounts for the $|B|$ factor in our formula for $F(e, eu)$. Suppose now that $n_w u = b' n_x$ for some $b' \in B$ and $x \in W$. Since then $Bn_w B = Bn_x B$, it follows that $w = x$ and thus $n_w u = b' n_w$. As u has p-power order and U is the unique Sylow p-subgroup of B, we deduce that $b' \in U$ and $n_w u n_w^{-1} \in U$. Thus there are $c_W(u)$ elements $w \in W$ for which $Bn_w u = Bn_w$. Since $\varepsilon(w)^2 = 1$, it is now straightforward to see that $F(e, eu) = |B| c_W(u)$. □

We rescale the restriction of F to $I \times I$ to produce a G-invariant symmetric bilinear form $f : I \times I \to R$ by setting

$$f(a, b) = |B|^{-1} F(a, b)$$

for all a and b in I. Let $U = \{u_1, \ldots, u_m\}$, where $m = |U|$. The Gram matrix D, say, of f with respect to the basis eu_i, $1 \le i \le m$, of I has i, j-entry $c_W(u_j u_i^{-1})$. Thus all entries of D are positive integers, and those on the main diagonal equal $|W|$.

Let n be the rank of G. Write the positive roots of G in the form r_i, where $1 \le i \le N$, and take $r_1, \ldots, r_n$ to be the fundamental roots. Let u be an element of U. Following [1, Theorem 5.3.3], we may write, with the usual notation,

$$u = \prod_{i=1}^{N} x_{r_i}(t_i),$$

where the $t_i \in \mathbb{F}_q$. Provided that $t_i \neq 0$ for $1 \leq i \leq n$, the argument of [11, Lemma 3] shows that $c_W(u) = 1$. Thus $q^{N-n}(q-1)^n$ entries of D are equal to 1.

3 Calculations with the linear characters of U

Let U_2 be the subgroup of U generated by the root subgroups X_r, where r is positive but not fundamental. U_2 is a normal subgroup of U and U/U_2 is an elementary abelian p-group of order q^n, [1, Theorem 5.3.3]. In all but a few cases, U_2 is the commutator subgroup U' of U. U' is a proper subgroup of U_2 when $q = 2$ and G is of type G_2, F_4, B_n or C_n for $n \geq 2$, and also when $G = G_2(\mathbb{F}_3)$, [4, Lemma 7]. In the exceptional cases, U/U' has order greater than q^n but it is still elementary abelian, since U is generated by elements of order p. In the non-exceptional cases, any complex linear character λ of U contains X_r in its kernel whenever r is positive but not fundamental.

Let λ be a complex linear character of U. We define the element e_λ of RG by

$$e_\lambda = \sum_{u \in U} \lambda(u) eu.$$

We clearly have

$$e_\lambda x = \lambda(x)^{-1} e_\lambda$$

for all x in U. We now consider the inner product of e_λ with the basis elements of I.

3.1 Lemma Let x be an element of U and λ a complex linear character of U. Then

$$f(ex, e_\lambda) = \lambda(x) \sum_{u \in U} c_W(u) \lambda(u).$$

Proof: We know that

$$f(ex, e_\lambda) = f(e, e_\lambda x^{-1}) = \lambda(x) f(e, e_\lambda).$$

The rest follows from Lemma 2.1. □

We see from Lemma 3.1 that $f(ex, e_\lambda)$ is the product of a p-th root of unity with the fixed quantity

$$\sum_{u\in U} c_W(u)\lambda(u),$$

which we intend to evaluate in terms of known invariants of G.

Given a subset S of G, we let $\sigma(S)$ denote the sum in RG of the elements of S.

3.2 Lemma We have

$$\sum_{u\in U} c_W(u)u = \sum_{w\in W} \sigma(U_w^+)$$

Proof: Given $u \in U$ and $w \in W$, we set

$$c_w(u) = \begin{cases} 1, & \text{if } u \in U_w^+; \\ 0, & \text{otherwise.} \end{cases}$$

It follows from this definition that

$$\sum_{u\in U} c_W(u)u = \sum_{u\in U}\sum_{w\in W} c_w(u)u. \tag{1}$$

Reversing the order of summation in the second sum in (1), we obtain

$$\sum_{u\in U} c_W(u)u = \sum_{w\in W}\sum_{u\in U} c_w(u)u \tag{2}$$

and it follows from the formula for $c_w(u)$ that (2) may be written as

$$\sum_{u\in U} c_W(u)u = \sum_{w\in W} \sigma(U_w^+). \tag{3}$$

3.3 Corollary Let λ be a complex linear character of U and let w be an element of W. Let λ_w denote the restriction of λ to U_w^+ and let 1_w denote the principal character of U_w^+. Then we have

$$\sum_{u\in U} c_W(u)\lambda(u) = \sum_{w\in W} |U_w^+|(\lambda_w, 1_w).$$

Proof: Applying λ to each side of (3), we obtain

$$\sum_{u\in U} c_W(u)\lambda(u) = \sum_{w\in W}\sum_{u\in U_w^+} \lambda(u)$$

and the second sum is clearly

$$\sum_{w\in W} |U_w^+|(\lambda_w, 1_w).$$

□

3.4 Lemma Let λ be a complex linear character of U, whose kernel contains the subgroup U_2, described at the beginning of this section. Let J be the subset of all those fundamental roots r with the property that λ is non-trivial on X_r. Let D_J be the subset of all elements x of W that satisfy $x(J) \leq \Phi^+$. Let w be any element of W. Then $\lambda_w = 1_w$ if and only if $w_0 w \in D_J$, where w_0 is the longest element of W.

Proof: As we noted previously, U_w^+ is generated by those X_r, where $r > 0$ and $w(r) > 0$. Since by our assumption on λ, X_s is in the kernel of λ whenever s is a positive root not in J, it follows that $\lambda_w = 1_w$ if and only if U_w^+ contains no root subgroup X_r with $r \in J$ or equivalently, if and only if all roots in $w(J)$ are negative. Now as the longest element w_0 maps all negative roots into positive roots, it follows that $\lambda_w = 1_w$ precisely when $w_0 w(J) \leq \Phi^+$, in which case $w_0 w \in D_J$, as required. □

3.5 Lemma Let w_1 and w_2 be elements of W with $w_2 = w_0 w_1$, where w_0 is the longest element of W. Then

$$\ell(w_1) + \ell(w_2) = N = |\Phi^+|.$$

Proof: Clearly, for any root $r > 0$, we have $w_2(r) = w_0(w_1(r))$. Since w_0 maps all positive roots into negative roots, and vice versa, $w_2(r)$ is positive if and only if $w_1(r)$ is negative. The result follows. □

Lemma 3.4 implies, using the previous notation, that

$$\sum_{u \in U} c_W(u)\lambda(u) = \sum_{w_0 w \in D_J} q^{N-\ell(w)}$$

and Lemma 3.5 yields that the sum on the right is

$$\sum_{d_J \in D_J} q^{\ell(d_J)}.$$

We now relate the sums above to the lattice of parabolic subgroups of G.

3.6 Theorem Assume the notation of Lemma 3.4. Then we have

$$\sum_{u \in U} c_W(u)\lambda(u) = |G : P_J|,$$

where P_J is the parabolic subgroup of G associated to the subset J of Π.

Proof: Let W_J be the subgroup of W generated by the fundamental reflections w_r, where $r \in J$. By the proof of [1, Theorem 9.4.5], we have

$$\sum_{w \in W} q^{\ell(w)} = \sum_{w' \in W_J} q^{\ell(w')} \sum_{d_J \in D_J} q^{\ell(d_J)}. \tag{4}$$

Now

$$\sum_{w \in W} q^{\ell(w)} = |G : B|. \tag{5}$$

Similarly,

$$\sum_{w' \in W_J} q^{\ell(w')} = |P_J : B|, \tag{6}$$

since the sum on the left of (6) arises from the decomposition of P_J into B,B-double cosets using the elements of W_J to label the double coset representatives. Thus

$$\sum_{u \in U} c_W(u)\lambda(u) = \sum_{d_J \in D_J} q^{\ell(d_J)} = |G : P_J|, \tag{7}$$

as required. □

4 Elementary divisors and modular reduction of the Steinberg lattice

Let $l \neq p$ be a prime divisor of $|G|$. We assume now that R is a local ring of characteristic 0 in which the unique maximal ideal is lR. We continue to assume that R contains a primitive p-th root of unity. We may take R to be the ring of integers in a suitably large unramified extension of finite degree of the field of l-adic numbers. In this case, R/lR is a finite field, K, say, of characteristic l.

Let $\bar{I}$ denote the KG-module I/lI. We refer to $\bar{I}$ as the l-modular reduction of the Steinberg lattice. Given α in R and v in I, we let $\overline{\alpha}$ and $\bar{v}$ denote the images of these elements in R/lR and I/lI, respectively. Similarly, let $\overline{f}$ denote the corresponding G-invariant symmetric bilinear form defined on $\bar{I} \times \bar{I}$ by the formula

$$\overline{f}(\bar{x},\bar{y}) = \overline{f(x,y)}.$$

As we noted in Section 2 that some of the entries of the Gram matrix D of f equal 1, it follows that $\overline{f}$ is not the zero bilinear form.

Since R is a principal ideal ring with unique maximal ideal lR, the theory of the Smith normal form shows that there exist R-bases

$$\{x_1,\dots,x_m\} \text{ and } \{y_1,\dots,y_m\}$$

of I with

$$f(x_i,y_j) = l^{a_i}\delta_{ij},\ 1 \le i,j \le m,$$

where $m = |U|$ and the a_i are non-negative rational integers satisfying

$$0 = a_1 \le a_2 \le \ldots \le a_m$$

(we may take $a_1 = 0$, since l does not divide all the entries of D). Thus, working over R, the elementary divisors of D are

$$l^{a_1}, l^{a_2}, \dots, l^{a_m}.$$

The product of these powers of l is the l-part of $\det D$.

Let ν be the l-adic valuation on R, defined so that $\nu(l^i) = i$. For each integer $k \ge 0$, we define

$$I(k) = \{x \in I : \nu(f(x,y)) \ge k \text{ for all } y \in I\}.$$

It is clear that $I(k)$ is a G-invariant sublattice of I of maximal rank. We now set

$$\overline{I(k)} = (I(k) + lI)/lI$$

and note that $\overline{I(k)}$ is KG-submodule of $\bar{I}$.

4.1 Lemma With the notation above, $\dim \overline{I(k)}$ equals the number of indices i with $a_i \ge k$.

Proof: It is straightforward to check that $I(k)$ has an R-basis consisting of those y_i with $a_i \ge k$, together with those $l^{k-a_j}y_j$, where $a_j < k$. Since $l^{k-a_j}y_j \in lI$ if $a_j < k$, those $\overline{y_i}$ with $a_i \ge k$ form a basis of $\overline{I(k)}$. □

4.2 Corollary The KG-module $\overline{I(k)}/\overline{I(k+1)}$ has dimension equal to the number of indices i with $a_i = k$.

We thus obtain a filtration of $\bar{I}$ by the modules $\overline{I(k)}/\overline{I(k+1)}$ in accordance with the different powers of l that occur among the elementary divisors of D. This filtration seems to have been introduced by Jantzen in [8, Lemma 3].

It is a routine matter to show that there is a G-invariant symmetric bilinear form defined on $\overline{I(k)} \times \overline{I(k)}$ whose radical is $\overline{I(k+1)}$. This implies the following result, whose proof we omit.

4.3 Theorem Provided $\overline{I(k)}/\overline{I(k+1)}$ is non-zero, it is a self-dual KG-module.

Now let λ be a linear character of U of the non-exceptional type described in Lemma 3.4. Let J be the subset of fundamental roots associated to λ and let P_J be the corresponding parabolic subgroup of G. Let $c = \nu(|G : P_J|)$. Lemma 3.1 and Theorem 3.6 show that $e_\lambda \in I(c)$ but $e_\lambda \notin I(c+1)$. Thus $\overline{e_\lambda}$ determines a non-zero one-dimensional KU-submodule in $\overline{I(c)}/\overline{I(c+1)}$. We therefore have the following result.

4.4 Theorem Let $l \neq p$ be a prime divisor of $|G|$. Suppose that there are exactly t different powers of l, say $l^{a_1}, \ldots, l^{a_t}$, that divide $|G : P|$, where P ranges over the lattice of parabolic subgroups containing B. Then $l^{a_1}, \ldots, l^{a_t}$ occur as elementary divisors of D over R and the l-modular reduction of the Steinberg lattice has at least t composition factors for KG.

We can now give a characterization of the socle S of $\bar{I}$ in terms of the elementary divisors of D. Our proof involves showing that S is an irreducible KG-module, a result first proved by Tinberg, [12, Theorem 4.10], in the more general context of a group possessing an unsaturated split (B,N)-pair of characteristic p. In what follows, we denote the principal character of U by 1, and write

$$e_1 = \sum_{u \in U} eu$$

for the corresponding element in RG.

4.5 Theorem Let $l \neq p$ be a prime divisor of $|G|$ and let $\kappa = \nu(|G : B|)$. Let S denote the socle of $\bar{I}$. Then S is an irreducible KG-module and it contains $\overline{e_1}$. Furthermore, the highest power of l that occurs as an elementary divisor over R of D is l^κ, and $\overline{I(\kappa)} = S$. Thus the multiplicity of l^κ as an elementary divisor of D is $\dim S$.

Proof: We will identify $\bar{I}$ as the submodule of KG generated by $\bar{e}$, where $\bar{e}$ is the image of e in KG. We may then also view the elements of $\bar{I}$ as K-linear combinations of expressions of the form $\sigma(B)x$, where $x \in G$ and

$$\sigma(B) = \sum_{b \in B} b.$$

Let M be any non-zero irreducible submodule of $\bar{I}$ and let $s \neq 0$ be an element of M. Then an element of the form $\sigma(B)x$ is present in s with non-zero coefficient γ. Thus $\sigma(B)$ is present in $sx^{-1} \in M$ with coefficient γ. We may write

$$sx^{-1} = \sum_{u \in U} \gamma_u \bar{e}u,$$

where the γ_u are in K. By [11, Theorem 1],

$$\sum_{u \in U} \gamma_u = \gamma.$$

Now setting

$$\sigma(U) = \sum_{u \in U} u,$$

we find that

$$(sx^{-1})\gamma^{-1}\sigma(U) = \gamma^{-1}(\sum_{u \in U} \gamma_u) \sum_{u \in U} \bar{e}u = \sum_{u \in U} \bar{e}u = \overline{e_1} \in M.$$

It follows that M is unique and hence equals S. Thus, S is irreducible and contains $\overline{e_1}$, as required.

We next note that $e_1 \in I(\kappa)$ but $e_1 \notin I(\kappa+1)$. It follows that l^κ is an elementary divisor of D. Let now l^t be the highest power of l that occurs as an elementary divisor of D, and suppose by way of contradiction that $t > \kappa$. Lemma 4.1 implies that $\overline{I(t)}$ is a non-zero submodule of $\bar{I}$. Hence $\overline{I(t)}$ contains S and thus $e_1 \in I(t)$. This is a contradiction. Therefore, $t = \kappa$, as claimed.

Since $\overline{I(\kappa)} \neq 0$, it follows that $S \leq \overline{I(\kappa)}$. Suppose, if possible, that $S \neq \overline{I(\kappa)}$. Now Theorem 4.3 implies that $\overline{I(\kappa)}$ is a self-dual KG-module. Let g denote a G-invariant non-degenerate symmetric bilinear defined on $\overline{I(\kappa)} \times \overline{I(\kappa)}$ (g is derived from f in a straightforward way). Let S_1 be the subspace of $\overline{I(\kappa)}$ defined by

$$S_1 = \{x \in \overline{I(\kappa)} : g(x,S) = 0\}.$$

As S is a KG-submodule and g is G-invariant, it is clear that S_1 is also a KG-submodule, and it is not trivial. Thus we have $S < S_1$. Elementary duality theory implies that

$$\overline{I(\kappa)}/S_1 \cong S^*,$$

where S^* is the dual module of S. We know that $\overline{e_1}$ is a non-zero fixed point of U in S and there is thus a trivial composition factor for U in S^*. Since l does not divide $|U|$, U acts completely reducibly on $\overline{I(\kappa)}$ and it follows that U has a two-dimensional subspace of fixed points. This is a contradiction, since the subspace of fixed points of U in its action on $\bar{I}$ is one-dimensional (recall that $\bar{I}$ is isomorphic as a KU-module to the regular module KU). We deduce that $\overline{I(\kappa)} = S$, as required. □

Theorem 4.5 implies an earlier result of Steinberg, [11, Theorems 2 and 3].

4.6 Corollary Let $l \neq p$ be a prime divisor of $|G|$. Then $\bar{I}$ is an irreducible KG-module if and only if l does not divide $|G : B|$.

Hiss showed in [3] that the trivial KG-module is a composition factor of $\bar{I}$ if and only if l divides $q+1$. Subsequently, Khammash improved this result to show that the socle of $\bar{I}$ is the trivial KG-module if and only if l divides $q+1$, [9]. We will now reprove Khammash's theorem using the methods developed in this paper.

4.7 Theorem The trivial KG-module is a composition factor of $\bar{I}$ if and only if l divides $q+1$. Furthermore, if the trivial module is a composition factor of $\bar{I}$, it occurs exactly once and equals the socle S of $\bar{I}$.

Proof: Suppose that l divides $q+1$. We will show that

$$\bar{e}_1 = (-1)^N \sum_{g \in G} g,$$

where $N = |\Phi^+|$. Let w be any element of W. Given $u_1 \in U_w^+$ and $u_2 \in U_w^-$, set $u = u_1 u_2$. Then $u \in U$ and the coset $Bn_w u$ equals $Bn_w u_2$. Fixing u_2, there are thus $|U_w^+|$ elements $u \in U$ such that $Bn_w u = Bn_w u_2$. Consequently, given any element $b \in B$, the coefficient of $bn_w u_2$ in $\bar{e}_1$ is equal to $\varepsilon(w)|U_w^+| \bmod l$. Since $|U_w^+| = q^{N-l(w)}$, and $\varepsilon(w) = (-1)^{l(w)}$, it follows from the supposition that $q \equiv -1 \bmod l$ that the coefficient of $bn_w u_2$ in $\bar{e}_1$ is $(-1)^N$. However, each element of G is uniquely expressible in the form $bn_w u_2$ by [1, Theorem 8.4.3], and thus it follows that

$$\bar{e}_1 = (-1)^N \sum_{g \in G} g,$$

as stated. We deduce that $\overline{e_1}$ is a non-trivial fixed-point for G in $\bar{I}$ and since S is irreducible, it must be the trivial KG-module.

Conversely, suppose that the trivial KG-module occurs as a composition factor of $\bar{I}$. Let M and M_1 be KG-submodules of $\bar{I}$ with $M_1 < M$ and M/M_1 the trivial KG-module. Since M is a completely reducible KU-module, there exists a KU-submodule M_2 of M such that M_2 is the trivial one-dimensional KU-submodule and $M = M_1 \oplus M_2$. Now as $\bar{I}$ is the regular KU-module, $\overline{e_1}$ spans the unique one-dimensional trivial KU-submodule of $\bar{I}$. It follows that $\overline{e_1} \in M_2$. This implies that $M_1 = 0$. For, if $M_1 \neq 0$, M_1 contains S, since S is irreducible. This is impossible, as we know that $\overline{e_1} \in S \leq M_1$, whereas $\overline{e_1} \notin M_1$. Thus, $M_1 = 0$, as stated, and M is the one-dimensional subspace spanned by $\overline{e_1}$. Consequently, S is the trivial KG-module. Since $\bar{I}$ is a submodule of KG, and KG contains a unique one-dimensional trivial KG-submodule, spanned by the element

$$\sum_{g \in G} g,$$

we must have

$$\overline{e_1} = \alpha \sum_{g \in G} g$$

for some non-zero element α of K. Therefore, from the first part of this proof, it must be the case that

$$\varepsilon(w)|U_w^+| \equiv \varepsilon(w')|U_{w'}^+| \bmod l$$

for all w and w' in W. Setting w equal to any reflection and w' equal to the identity, we obtain

$$-q^{N-1} \equiv q^N \bmod l,$$

which implies that l divides $q+1$, as required. □

5 Two examples of modular reduction of the Steinberg lattice

While Theorem 4.4 tells us about powers of l that occur as elementary divisors of the Gram matrix D, it would also be useful to have some upper bound on their multiplicities. A formula for $\det D$ would provide partial information in this respect. Now D is a specialization of the group matrix of U introduced by Frobenius in his creation of the theory of group characters. We will briefly reformulate parts of Frobenius's theory to show how we may find some integer divisors of $\det D$ and then calculate $\det D$ in one non-trivial case.

Let $T = \{t_1, \dots, t_n\}$ be a finite group of order n. Let $c(t_1)$, …, $c(t_n)$ be any n rational integers labelled by the elements of T. Consider the element

$$t = c(t_1)t_1 + \cdots + c(t_n)t_n$$

in the complex group algebra $\mathbb{C}T$. We define a linear transformation $\tau : \mathbb{C}T \to \mathbb{C}T$ by

$$\tau(x) = tx$$

for all $x \in \mathbb{C}T$. With respect to the group element basis of $\mathbb{C}T$, τ has matrix Δ, say, whose (i, j)-entry is $c(t_j t_i^{-1})$.

The group algebra $\mathbb{C}T$ is a direct sum of minimal left ideals, say

$$\mathbb{C}T = I_1 \oplus \cdots \oplus I_s$$

and under the left regular representation of $\mathbb{C}T$ on itself, each left ideal I_j is an irreducible $\mathbb{C}T$-module and is thus τ-invariant. Let X_j be the irreducible representation of T afforded by I_j. Then, in its action on I_j, τ acts as the linear transformation

$$X_j(t) = c(t_1)X_j(t_1) + \cdots + c(t_n)X_j(t_n).$$

It follows that we can evaluate $\det \Delta$ as a product of the determinants of the linear transformations just considered, since we clearly have

$$\det \Delta = \prod_{j=1}^{s} \det X_j(t).$$

We quote without proof the following result describing properties of the factors in this product.

5.1 Lemma Let $T = \{t_1, \dots, t_n\}$ be a finite group of order n. Let b_1, …, b_n be n rational integers. Let χ be an irreducible complex character of T and let X be a representation of T with character χ. Then

$$\det(b_1 X(t_1) + \cdots + b_n X(t_n))$$

depends only on χ and not on the choice of representation X. It is an algebraic integer in the field $\mathbb{Q}(\chi)$ obtained by adjoining to $\mathbb{Q}$ all the values taken by χ.

In the case of interest to us, we take $T = U$, and $b_i = c_W(u_i)$ for $1 \leq i \leq m = |U|$. Then we see that

$$\det D = \prod_j \det\left(c_W(u_1)X_j(u_1) + \cdots + c_W(u_m)X_j(u_m)\right)^{X_j(1)},$$

where X_j runs through the inequivalent irreducible complex representations of U, and each factor is an algebraic integer. Taking into account the case when X_j has degree 1, we obtain the following result that describes certain factors of $\det D$.

5.2 Corollary Let λ be a complex linear character of U, whose kernel contains the subgroup U_2, described at the beginning of Section 3. Let $J = J(\lambda)$ be the subset of all those fundamental roots r with the property that λ is non-trivial on X_r and let P_J be the parabolic subgroup of G associated to J. Then $\det D$ is divisible by

$$\prod_\lambda |G : P_{J(\lambda)}|,$$

the product being taken over all admissible λ.

It is more complicated to find the contributions to $\det D$ that arise from the irreducible representations of U of degree greater than 1. To illustrate the theory just described, we will evaluate $\det D$ when $G = B_2(\mathbb{F}_q)$, where q is a power of an odd prime p. The following table lists the various irreducible representations of the Sylow p-subgroup U of G and the factors of $\det D$ that correspond to them. We omit details of the calculations, which involve finding explicit matrices for the irreducible representations of U.

degree of representation	number of representations	factor of $\det D$
1	1	$(q+1)^2(q^2+1)$
1	$2(q-1)$	$(q+1)(q^2+1)$
1	$(q-1)^2$	1
q	$(q-1)$	$(q+1)(q^2+1)$
q	$\frac{(q-1)^2}{2}$	$q+1$
q	$\frac{(q^2-1)}{2}$	$(q+1)(q^2+1)$

5.3 Corollary Let $G = B_2(\mathbb{F}_q)$, where q is a power of an odd prime. Then we have

$$\det D = (q+1)^a(q^2+1)^b,$$

where $a = q^3+q$, $b = \dfrac{q(q+1)^2}{2} - 1$.

Using the formula above, we proceed to consider two examples where we try to find a composition series for $\bar{I}$ when $G = B_2(\mathbb{F}_q)$.

5.4 Example $G = B_2(\mathbb{F}_q)$, q odd, l an odd prime divisor of $q+1$.

Let q be a power of an odd prime p, let l be an odd prime divisor of $q+1$ and let $d = \nu(q+1)$. Let $G = B_2(\mathbb{F}_q)$ and let r_1 and r_2 be fundamental roots for a root system of type B_2. Let χ_{st} denote the Steinberg character of G. By the results of [10], there are irreducible l-modular Brauer characters φ_0, φ, φ_s, φ_t and φ_{st} and a positive integer α such that

$$\chi_{st} = \varphi_0 + \alpha\varphi + \varphi_s + \varphi_t + \varphi_{st}$$

on l-regular elements of G. We have $\alpha = 1$ if $l = 3$ and $d = 1$; otherwise, $\alpha = 2$. We may describe these Brauer characters by noting that φ_0 is the principal Brauer character and

$$\varphi(1) = \frac{q(q-1)^2}{2}, \quad \varphi_s(1) = \varphi_t(1) = \frac{q(q^2+1)}{2} - 1.$$

Now there exist real-valued irreducible complex characters χ_s and χ_t of G such that

$$\chi_s = \varphi_0 + \varphi_s, \quad \chi_t = \varphi_0 + \varphi_t$$

on l-regular elements. Since χ_s and χ_t are real-valued, it follows that φ_s and φ_t are real-valued. Furthermore, there is a real-valued irreducible character χ of G such that $\chi = \varphi$ on l-regular elements. Thus φ is real-valued. Now it is known that the restriction to U of χ contains no linear character of U. It follows that the same is true of φ. Finally, it is clear that φ_{st} must also be real-valued.

Let φ_0 correspond to the trivial irreducible KG-module V_0, φ to V_1, φ_s to V_2, φ_t to V_3 and φ_{st} to V_4. Then the V_i are all self-dual, as their Brauer characters are real-valued. It is straightforward to check that the restriction to U of each of χ_s and χ_t contains a linear character λ for which $J = \{r_1\}$

or $\{r_2\}$, and the same must then be true of φ_s and φ_t. Since $|G:P_J| = (q+1)(q^2+1)$ when J is as above, we have $\nu(|G:P_J|) = d$ in this case. It follows that V_2 and V_3 are composition factors of $\overline{I(d)}/\overline{I(d+1)}$, each occurring with multiplicity 1. Furthermore, since $\nu(|G:B|) = 2d$, we know from Theorem 4.5 that l^{2d} occurs with multiplicity 1 as an elementary divisor of D.

We set

$$u = \dim \overline{I(d)}/\overline{I(d+1)}.$$

Then l^d occurs with multiplicity u as an elementary divisor of D. Moreover, since V_2 and V_3 are composition factors of $\overline{I(d)}/\overline{I(d+1)}$, we have

$$u \geq \dim V_2 + \dim V_3 = q(q^2+1) - 2.$$

If we now consider the power of l that divides $\det D$ and the contributions of the elementary divisors l^d and l^{2d} to this power, we obtain the estimate

$$ud + 2d \leq \nu(\det D) = d(q^3+q).$$

Since we also have the inequality

$$ud + 2d \geq d(q^3+q),$$

it follows that $u = q^3+q-2$. Thus, V_2 and V_3 are the only composition factors of $\overline{I(d)}/\overline{I(d+1)}$, and the elementary divisors of D are l^d with multiplicity q^3+q-2 and l^{2d} with multiplicity 1. Theorem 4.3 shows that $\overline{I(d)}/\overline{I(d+1)}$ is a self-dual KG-module and, since V_2 and V_3 are non-isomorphic self-dual KG-modules, it follows in a straightforward way that $\overline{I(d)}/\overline{I(d+1)}$ is the direct sum of V_2 and V_3. The composition factors of $\bar{I}/\overline{I(1)}$ are V_1, with multiplicity α, and V_4 with multiplicity 1. In the case that $\alpha = 1$, $\bar{I}/\overline{I(1)}$ is the direct sum of V_1 and V_4, as both modules are self-dual. Then $\bar{I}$ has a composition series

$$\begin{array}{c} V_1 \oplus V_4 \\ V_2 \oplus V_3 \\ V_0 \end{array}$$

with the trivial module V_0 equal to the socle. When $\alpha = 2$, we have not been able to deduce a composition series for $\bar{I}/\overline{I(1)}$.

5.5 Example $G = B_2(\mathbb{F}_q)$, $q \equiv 1 \bmod 4$, $l = 2$

In this example, we take $l = 2$, $G = B_2(\mathbb{F}_q)$, and we assume that $q \equiv 1 \bmod 4$. Following the notation of our previous example and also that of [13], the results of [13] show that there are 2-modular Brauer characters φ_i, $1 \leq i \leq 6$, and an integer $x \geq 0$ such that

$$\chi_{st} = \varphi_0 + \varphi_1 + \varphi_2 + \varphi_3 + \varphi_4 + \varphi_5 + (2x+1)\varphi_6$$

on 2-regular elements of G. We have

$$\begin{gathered}\varphi_1(1) = \varphi_2(1) = \tfrac{(q-1)^2}{2}(q^2 + q(1-x) + 1)\\ \varphi_4(1) = \varphi_5(1) = \tfrac{q^2-1}{2},\ \varphi_6(1) = \tfrac{q(q-1)^2}{2}\\ \varphi_3(1) = \tfrac{q(q^2+1)}{2} - 1\end{gathered}$$

and φ_0 is the principal Brauer character. Each φ_i is real-valued and corresponds to an irreducible self-dual KG-module, V_i say, for $0 \leq i \leq 6$.

The restriction to U of φ_6 contains no linear character of U. For $1 \leq i \leq 5$, $\varphi_i(1)$ is relatively prime to p and thus the restriction to U of each such φ_i contains a non-trivial linear character. It is straightforward to see that the restriction to U of each of φ_3, φ_4 and φ_5 contains a linear character λ for which $J = \{r_1\}$ or $\{r_2\}$. Since for such a subset J of fundamental roots, $\nu(|G : P_J|) = 2$, it follows that V_3, V_4 and V_5 are all composition factors of $\overline{I(2)}/\overline{I(3)}$. $\overline{I(3)}$ is the socle of $\bar{I}$ and equals the trivial KG-module. The only linear characters that occur in the restriction to U of φ_1 and φ_2 are those for which the corresponding subset J is Π. It follows that V_1 and V_2 are composition factors of $\bar{I}/\overline{I(1)}$.

We set

$$u = \dim \overline{I(1)}/\overline{I(2)}, \quad v = \dim \overline{I(2)}/\overline{I(3)}.$$

Then 2 has multiplicity u as an elementary divisor of D, 2^2 has multiplicity v, and we know from Corollary 4.6 that 2^3 has multiplicity 1. The product of these elementary divisors is the power of 2 dividing $\det D$ and we deduce that

$$u + 2v + 3 = \nu(\det D) = q^3 + q + \frac{q(q+1)^2}{2} - 1.$$

As we know that V_3, V_4 and V_5 are composition factors of $\overline{I(2)}/\overline{I(3)}$, it follows that

$$v \geq \dim V_3 + \dim V_4 + \dim V_5.$$

Furthermore, as V_1 and V_2 occur as composition factors of $\bar{I}$ only in $\bar{I}/\overline{I(1)}$, it follows that V_6 is a composition factor of $\overline{I(1)}/\overline{I(2)}$ if $u > 0$ and of $\overline{I(2)}/\overline{I(3)}$ if $v > \dim V_3 + \dim V_4 + \dim V_5$.

Straightforward inequality estimates using the formula for $\det D$ yield that $u = \dim V_6$ and $v = \dim V_3 + \dim V_4 + \dim V_5$. Thus, since V_3, V_4 and V_5 are non-isomorphic and self-dual,

$$\overline{I(1)}/\overline{I(2)} \cong V_6, \quad \overline{I(2)}/\overline{I(3)} \cong V_3 \oplus V_4 \oplus V_5.$$

The composition factors of $\bar{I}/\overline{I(1)}$ are V_1 and V_2 with multiplicity 1, and V_6 with multiplicity $2x$. In case $x = 0$, which occurs, for example, when $q = 5$, by the tables in [7, p.145], we obtain the composition series

$$\begin{array}{c} V_1 \oplus V_2 \\ V_6 \\ V_3 \oplus V_4 \oplus V_5 \\ V_0 \end{array}$$

We note that this example illustrates that we cannot detect all the elementary divisors of D through the linear characters of U. For we have seen that 2 occurs as an elementary divisor in this case, but U acts on $\overline{I(1)}/\overline{I(2)}$ without one-dimensional invariant subspaces.

6 The modular reduction of the Steinberg lattice when $G = A_n(\mathbb{F}_q)$

The theory of Section 4 gives sufficient conditions for the factors $\overline{I(k)}/\overline{I(k+1)}$ to be non-trivial in terms of the powers of l that divide the numbers $|G : P_J|$. We would have a complete correspondence if we knew that the restriction to U of any irreducible l-modular Brauer character of G contains a linear character of U with non-zero multiplicity, but the examples in Section 5 show that this does not happen in general. As might be anticipated, the situation is under better control when $G = A_n(\mathbb{F}_q)$, since the following theorem is true.

6.1 Theorem Let $G = A_n(\mathbb{F}_q)$ and let M be an irreducible KG-module. Then M contains a one-dimensional KU-submodule.

This theorem is probably well known and a proof of it may be modelled on a corresponding result proved by Gelfand and Graev, [2], in the context of complex representations. We omit the details, as the theorem is not crucial to our further development of the theory.

6.2 Corollary Let $G = A_n(\mathbb{F}_q)$ and let l be a prime divisor of $|G : B|$. Then the powers of l that occur as elementary divisors over R of the Gram matrix D are precisely the powers of l that divide the indices $|G : P|$, where P runs over the set of parabolic subgroups that contain B.

Now the general Chevalley group G described in this paper is realized as a group of automorphisms of a Lie algebra $\mathscr{L}$ over $\mathbb{F}_q$, defined in terms of the root system Φ. G is a normal subgroup of a larger group $\widehat{G}$ of automorphisms of $\mathscr{L}$, described in [1, p.98 and p.118]. It is straightforward to show from the definition of e that $\widehat{G}$ acts on the Steinberg lattice. When $G = A_n(\mathbb{F}_q)$, the larger group $\widehat{G}$ is isomorphic to the projective general linear group $\mathrm{PGL}_{n+1}(\mathbb{F}_q)$ and thus we may consider the Steinberg lattice to be a module for this group. In particular, we may use the tables in [5] to determine the composition factors of the modular reduction of the Steinberg lattice of $\widehat{G}$ for $n \leq 9$. Perusal of these tables suggests that any non-zero quotient $\overline{I(k)}/\overline{I(k+1)}$ is an irreducible $K\widehat{G}$-module. This leads us to formulate a conjecture, as follows.

6.3 Conjecture Let $G = A_n(\mathbb{F}_q)$ and let l be a prime divisor of $|G : B|$. Let $k \geq 0$ be an integer and let $I(k)$ be the corresponding sublattice of I. Then the quotient $\overline{I(k)}/\overline{I(k+1)}$ is either zero or is an irreducible $K\widehat{G}$-module. Equivalently, the number of composition factors of the $K\widehat{G}$-module $\bar{I}$ equals the number of different powers of l that equal the l-part of $|G : P|$, as P ranges over the parabolic subgroups of G.

The fact that the conjecture above is true for certain small values of n allows us to use the dimensions of the composition factors of $\bar{I}$ to obtain an explicit formula for $\det D$ in these cases. For we know the elementary divisors of D in terms of the prime divisors of $|G : P|$, and their multiplicities are provided by the dimensions of the composition factors. We illustrate how this technique may be put into practice by evaluating $\det D$ when $n = 3$, using the tables in [5] for $\mathrm{GL}_4(\mathbb{F}_q)$.

6.4 Theorem Let $G = A_3(\mathbb{F}_q)$. Then we have

$$\det D = (q+1)^a (q^2+1)^b (q^2+q+1)^c,$$

where $a = q^5 + q^3 - q^2 + 1$, $b = q^5 + q^4 - q^2 - q + 1$ and $c = q^4 + q^2 - 1$.

Proof: Let χ_{st} be the Steinberg character of $\widehat{G}$ and let l be a prime divisor of $|G:B|$. We begin with the case that l divides $q+1$ and set $d = \nu(q+1)$. Suppose that l is odd. Then the l-modular decomposition of χ_{st} is given by

$$\chi_{st} = \varphi_0 + \varphi_1 + \varphi_2,$$

where the φ_i are irreducible Brauer characters and φ_0 is the principal Brauer character. We also have

$$\varphi_1(1) = (q^3-1)(q^2+1), \quad \varphi_2(1) = q^2(q^3-1)(q-1).$$

Now φ_0 is associated with the elementary divisor l^{2d}, and φ_1 with the elementary divisor l^d. Thus

$$\nu(\det D) = 2d + d(q^3-1)(q^2+1).$$

Suppose next that $l=2$. The 2-modular decomposition of χ_{st} is described by

$$\chi_{st} = \varphi_0 + \varphi_1 + \varphi_2 + \varphi_3,$$

where φ_0 is the principal Brauer character and

$$\varphi_1(1) = (q^3-1)(q^2+1), \quad \varphi_2(1) = (q^3-1)(q-1).$$

The Brauer characters φ_0, φ_1 and φ_2 are associated to the elementary divisors 2^{2d+1}, 2^{d+1} and 2, respectively. Thus

$$\nu(\det D) = 2d+1+(d+1)(q^3-1)(q^2+1)+(q^3-1)(q-1)$$

when $l=2$.

Next, we let l be an odd prime divisor of q^2+1. Then we have

$$\chi_{st} = \varphi_1 + \varphi_2,$$

where $\varphi_1(1) = q^5+q^4-q^2-q+1$ and

$$\nu(\det D) = \nu(q^2+1)\varphi_1(1).$$

Finally, we let l be a divisor of q^2+q+1. Then we find that

$$\chi_{st} = \varphi_1 + \varphi_2,$$

where $\varphi_1(1) = q^4 + q^2 - 1$, and correspondingly

$$\nu(\det D) = \nu(q^2 + q + 1)\varphi_1(1).$$

This accounts for all prime divisors of $|G : B|$ and it is straightforward to see that the prime factors of $\det D$ which we have found are equivalent to the formula claimed for $\det D$ above. □

Using the same ideas, we have obtained the formula

$$\det D = (q+1)^a(q^2+1)^b(q^2+q+1)^c(q^4+q^3+q^2+q+1)^e,$$

for $G = A_4(\mathbb{F}_q)$, where $a = q^7 + q^5 - q^2 + 1$, $b = q^8 + q^7 - q^3 - q^2 + 1$, $c = q^6 + q^5 - q$ and $e = q^9 + q^8 - 2q^5 + q^2 + q - 1$. The two formulae we have obtained are difficult to interpret combinatorially in the form presented, but we feel that it may be possible to calculate $\det D$ in principle whenever $G = A_n(\mathbb{F}_q)$. We have in mind something in the spirit of the James-Murphy formula for the determinant of the Gram matrix of the integral symmetric bilinear form associated to a Specht lattice, [6]. On the basis of these results and Corollary 5.3, it seems that $\det D$ is a product of factors of the form $\Phi_m(q)$, where $\Phi_m(q)$ denotes the m-th cyclotomic polynomial evaluated at q, and m runs over the degrees of the Weyl group of G.

Acknowledgement. The author is grateful to Fernando Szechtman for a careful reading of the original manuscript.

REFERENCES

1. R. W. Carter, "Simple Groups of Lie Type," John Wiley: London, New York, 1972.

2. I. M. Gelfand and M. I. Graev, Construction of irreducible representations of simple algebraic groups over a finite field, Dokl. Akad. Nauk SSSR **147** (1962), 529-532.

3. G. Hiss, The number of trivial composition factors of the Steinberg module, Arch. Math. (Basel) **54** (1990), 247-251.

4. R. B. Howlett, On the degrees of Steinberg characters of Chevalley groups, Math. Z. **135** (1974), 125-135.

5. G. D. James, The decomposition matrices of $\mathrm{GL}_n(q)$ for $n \leq 10$, Proc. London Math. Soc. **60** (1990), 225-265.

6. G. D. James and G. E. Murphy, The determinant of the Gram matrix for a Specht module, J. Algebra **59** (1979), 222-235.

7. C. Jansen, K. Lux, R. A. Parker and R. A. Wilson, "An Atlas of Brauer characters". The Clarendon Press: Oxford, 1995.

8. J. C. Jantzen, Kontravariante Formen auf induzierten Darstellungen halbeinfacher Lie-Algebren, Math. Ann. **226** (1977), 53-65.

9. A. A. Khammash, On the homological construction of the Steinberg representation, J. Pure Appl. Algebra **87** (1993), 17-21.

10. T. Okuyama and K. Waki, Decomposition numbers of $\mathrm{Sp}(4,q)$, J. Algebra **199** (1998), 544-555.

11. R. Steinberg, Prime power representations of finite linear groups, II, Canad. J. Math. **9** (1957), 347-351.

12. N. B. Tinberg, The Steinberg component of a finite group with a split (B,N)-pair, J. Algebra **104** (1986), 126-134.

13. D. L. White, The 2-decomposition numbers of $\mathrm{Sp}(4,q)$, q odd, J. Algebra **131** (1990), 703-725.