Journal of Combinatorial Theory, Series A **94**, 1–14 (2001)
doi:10.1006/jcta.2000.3118, available online at http://www.idealibrary.com on IDEAL®

Codes Associated with Nondegenerate Quadrics of a Symplectic Space of Even Order

N. S. Narasimha Sastry

Division of Theoretical Statistics and Mathematics, Indian Statistical Institute, 8th Mile, Mysore Road, R. V. College Post, Bangalore 560059, India
E-mail: nsastry@isibang.ac.in

and

Peter Sin[1]

Department of Mathematics, University of Florida, 358 Little Hall, P.O. Box 118105, Gainesville, Florida 32611
E-mail: sin@math.ufl.edu

Communicated by the Managing Editors

Received June 15, 1999

This paper studies the incidence relation between the points and quadrics in the projective space of a symplectic vector space over a field of even order. The 2-rank of the incidence matrix is determined. This is achieved by viewing the code generated by incidence vectors as a module for the symplectic group and applying the 2-modular representation theory of this group. The radical series of this module is also described.

Key Words: incidence matrices; *p*-ranks; designs; quadrics; symplectic group; orthogonal group; representations.

1. INTRODUCTION

Let $q = 2^t$ and let $V(q)$ be a vector space of dimension $2n$, $n \geqslant 2$, defined over the finite field $\mathbb{F}_q$ and endowed with a nonsingular symplectic bilinear form b. Let $P = \mathbb{P}(V(q))$ be the associated projective space. The codes studied here are related to the nondegenerate quadrics of the symplectic geometry of (P, b). Thus, the quadrics of P we consider are those which have quadratic forms f for which b is the associated bilinear form, in other words, b equals the *polarization* $\theta(f)$ of f defined by

$$\theta(f)(v_1, v_2) = f(v_1 + v_2) - f(v_1) - f(v_2), \qquad v_i \in V(q).$$

[1] Supported by NSF Grant DMS9701065.

0097-3165/01 $35.00

It is well known [7, Theorem 6] that this set of quadrics splits into two orbits under the action of the symplectic group G of b: the set of those with Witt index n (i.e., the dimension of a maximal isotropic subspace contained in the quadric is n; these are the so-called *hyperbolic quadrics*) and the set of those with Witt index $n-1$ (these are the so-called *elliptic quadrics*). See [7, 4.1, p. 218].

Let k be a perfect field of characteristic 2 and let k^P be the space of k-valued functions on P. Let $\mathscr{D}$ be the subspace of k^P generated by the characteristic functions of nondegenerate quadrics polarizing to b and of given Witt index. The dimension of $\mathscr{D}$ is equal to the 2-rank of the incidence relation between P and the set of quadrics in question. In this note we find this dimension (Theorem 3.1) and give the structure of $\mathscr{D}$ as a kG-module (Theorem 4.1). By Theorem 3.1, the dimension of $\mathscr{D}$ plus 1 equals the dimension of the k-span $\mathscr{C}$ of the characteristic functions of the hyperplanes of a projective space $\hat{P}$ of dimension $2n$ over $\mathbb{F}_q$ (see [1, Theorem 5.7, p. 180]). We explain this equality in Section 5 by producing a $kO(2n+1, q)$-module homomorphism from $k^{\hat{P}}$ to k^P which maps $\mathscr{C}$ isomorphically to $k1_P \oplus \mathscr{D}$. This together with Theorem 4.1 also gives the $kO(2n+1, q)$-module structure of $\mathscr{C}$.

For the dimensions of codes associated with several incidence systems in the literature, see [1, 4, 11]. The structure of the codes as modules are discussed for fewer cases; see [12, 2, 13] for some recent examples.

2. BACKGROUND RESULTS ON THE REPRESENTATION THEORY OF SYMPLECTIC GROUPS

Let $\bar{k}$ denote an algebraic closure of k. By choosing a symplectic basis $\{e_1, ..., e_n, f_n, ..., f_1\}$ of $V(q)$ such that $b(e_i, f_j) = \delta_{ij}$, we may regard the group $G = \mathrm{Sp}(V(q))$ as the subgroup of $\mathbb{F}_q$-rational points of the algebraic group $\mathrm{Sp}(2n, \bar{k})$. In this section, we put together a few facts about the representations of G needed to prove Theorems 3.1 and 4.1. We note that Lemma 2.1 is the only result from this section which is needed for the proof of Theorem 3.1, in case the reader wishes to skip the rest. As is well known, the representation theory of $\bar{k}G$ is related in many ways to the theory of (rational) representations of $\mathrm{Sp}(2n, \bar{k})$, which has been studied in great detail in [6]. Some of the important basic notions are more general and belong to the representation theory of reductive groups, as described in [10].

Let T be the diagonal subgroup (a maximal torus) in $\mathrm{Sp}(2n, \bar{k})$ and let $X(T)$ denote its character group. Then $X(T)$ is a free abelian group of rank n. As a basis we can take the set $\{\tilde{\omega}_1, ..., \tilde{\omega}_n\}$ where $\tilde{\omega}_i$ maps the diagonal matrix $\mathrm{diag}(t_1, ..., t_n, t_n^{-1}, ..., t_1^{-1})$ to the scalar $t_1 \cdot t_2 \cdots t_i$. This is called the set of *fundamental weights*. The set of nonnegative integral combinations of the fundamental weights are called the *dominant* weights. The isomorphism

classes of simple $\mathrm{Sp}(2n, \bar{k})$-modules are parametrized by the set of dominant weights in the following way. There is a certain ordering on the group $X(T)$ and given a simple $\mathrm{Sp}(2n, \bar{k})$-module there is among its weights (the characters of T which it affords) a unique highest one with respect to this ordering, which characterizes the simple module. The highest weights of simple modules are dominant and each dominant weight λ occurs as the highest weight of a simple module $L(\lambda)$. The simple module $L(0)$ is the trivial module.

The fundamantal weight $\tilde{\omega}_i$ is the highest weight which occurs in ith exterior power of the natural module. (The ith exterior power may not itself be a simple module but it has the composition factor $L(\tilde{\omega}_i)$ with multiplicity one.)

Let e be a positive integer. A dominant weight $\sum_i a_i \tilde{\omega}_i$ is called 2^e-*restricted* if all the coefficients a_i satisfy $0 \leqslant a_i \leqslant 2^e - 1$. Steinberg has proved [15, Theorem 7.4, p. 45] that the restrictions to $\mathrm{Sp}(2n, 2^e)$ of the $2^n e$ simple $\mathrm{Sp}(2n, \bar{k})$-modules with 2^e-restricted highest weights form a complete set of nonisomorphic simple $\bar{k}\mathrm{Sp}(2n, 2^e)$-modules.

Next we recall the celebrated Tensor Product Theorem of Steinberg. This theorem applies to all Chevalley groups and we shall apply it to certain symplectic groups and spin groups. Since a less well known refinement concerning symplectic groups in characteristic 2 will be important for us, we will give here a brief account of both these results as they apply to $\mathrm{Sp}(2n, \bar{k})$.

Let $L(\lambda)$ denote the simple module with highest weight λ and let

$$\lambda = \lambda_0 + 2\lambda_1 + \cdots + 2^r \lambda_r \tag{1}$$

be the 2-adic expression for λ (in which the λ_i are 2-*restricted* weights). Then $L(\lambda)$ has a tensor factorization in the form

$$L(\lambda) \cong L(\lambda_0) \otimes L(\lambda_1)^{(2)} \otimes \cdots \otimes L(\lambda_r)^{(2^r)}. \tag{2}$$

In the above equation the superscript (2^i) denotes the ith-Frobenius twist; if U is a vector space over a field $\mathbb{F}$ of characteristic 2, then $U^{(2^i)}$ is the vector space with the same abelian group structure as U but having scalar multiplication defined by

$$\lambda \circ u = \lambda^{2^{-i}} u \qquad (\lambda \in \mathbb{F}, u \in U).$$

If U is a module for a group, then the matrices which represent the group on $U^{(2^i)}$ are obtained from those for U by raising each matrix entry to its 2^i th power.

The sharper form of the Tensor Product Theorem [15, Theorem 11.1, p. 52] is based on the factorization of the Frobenius endomorphism of $\mathrm{Sp}(2n, \bar{k})$ as the composite of two surjective homomorphisms of algebraic groups,

$$\mathrm{Sp}(2n, \bar{k}) \xrightarrow{\tau} \mathrm{Spin}(2n+1, \bar{k}) \xrightarrow{\sigma} \mathrm{Sp}(2n, \bar{k}). \tag{3}$$

(See [6, Chap. I, Sect. 3] for more details.) These maps are isomorphisms of the underlying abstract groups, but not isomorphisms of algebraic groups. For this reason, the rational represenation theories of these groups are different, though of course closely related.

Now, let λ be a 2-restricted weight. We can write

$$\lambda = \mu + \varepsilon\tilde{\omega}_n, \tag{4}$$

where μ is a combination of the first $n-1$ fundamental weights and $\varepsilon \in \{0, 1\}$. Steinberg's refinement states that accordingly, we have

$$L(\lambda) \cong L(\mu) \otimes L(\varepsilon\tilde{\omega}_n). \tag{5}$$

(See [6, Chap. I, Sect. 4] for more details.) The simple module $L(\tilde{\omega}_n)$ is the so-called *spin* module for $\mathrm{Sp}(2n, \bar{k})$, because it is obtained by composing the map τ in (3) with the spin representation of $\mathrm{Spin}(2n+1, \bar{k})$. It has dimension 2^n.

Let f be a fixed quadratic form on $V(q)$ which has polarization b and let $O(f) \subset G$ be its orthogonal group. We may consider f as a quadratic form on $\bar{k} \otimes_{\mathbb{F}_q} V(q)$ and denote the corresponding orthogonal group by $O(2n, \bar{k})$. Let $\Omega(2n, \bar{k})$ be its commutator subgroup and let $\Omega(f)$ be the commutator subgroup of $O(f)$. The latter two groups are Chevalley groups, for which Steinberg's Tensor Product Theorem (usual form) and the classification of simple modules by highest weights also hold.

LEMMA 2.1. *Let L be a nontrivial simple kG-module. Then $\Omega(f)$ fixes only the zero vector of L. The same is true (a fortiori) of $O(f)$.*

Proof. It suffices to prove the result with k replaced by $\bar{k}$ because $\bar{k} \otimes_k L$ is a semisimple $\bar{k}G$-module. Thus, we assume L is a simple $\bar{k}G$-module. Then L is the restriction to G of a simple $\mathrm{Spin}(2n, \bar{k})$-module $L(\lambda)$, where the highest weight λ is 2^t-restricted. We will consider the restriction of $L(\lambda)$ first to $\Omega(2n, \bar{k})$ and then to $\Omega(f)$. Let λ be written in its 2-adic expression as in (1), and for each i, let

$$\lambda_i = \mu_i + \varepsilon_i\tilde{\omega}_n, \tag{6}$$

as in (4).

By the refined version of the Tensor Product Theorem, we have

$$L(\lambda) \cong \bigotimes_{i=1}^{t-1} L(\mu_i)^{(2^i)} \otimes \bigotimes_{i=0}^{t-1} L(\varepsilon_i\tilde{\omega}_n)^{(2^i)}. \tag{7}$$

We now describe the restrictions of the $L(\mu_i)$ and $L(\tilde{\omega}_n)$ to $\Omega(2n, \bar{k})$. Consider the simply connected algebraic group $\mathrm{Spin}(2n, \bar{k})$ covering $\Omega(2n, \bar{k})$. We label the fundamental weights for this group in the usual way as $\delta_1, ..., \delta_{n-1}, \delta_n$, so that δ_1 corresponds to the natural module for $\Omega(2n, \bar{k})$ and the two weights δ_{n-1} and δ_n correspond to the half-spin modules. The half-spin modules are the two 2^{n-1}-dimensional direct summands of the spin module for $\mathrm{Spin}(2n, \bar{k})$. One should be careful not to confuse this last spin module with the spin module $L(\tilde{\omega}_n)$ for $\mathrm{Spin}(2n, \bar{k})$. The relation between the two is as follows. The restriction of $L(\tilde{\omega}_n)$ from $\mathrm{Spin}(2n, \bar{k})$ to $\Omega(2n, \bar{k})$ is naturally also a module (of dimension 2^n) for the covering group $\mathrm{Spin}(2n, \bar{k})$. This module is not the spin module of $\mathrm{Spin}(2n, \bar{k})$ but rather its first Frobenius twist, as can be seen by weight calculations. Thus,

$$L(\tilde{\omega}_n) \cong L'(2\delta_{n-1}) \oplus L'(2\delta_n), \tag{8}$$

where we use $L'(\delta)$ to denote the simple $\mathrm{Spin}(2n, \bar{k})$-module with highest weight δ.

It is also known that the restriction of $L(\mu_i)$ to $\Omega(2n, \bar{k})$ defines a simple module for $\mathrm{Spin}(2n, \bar{k})$ which has restricted highest weight not involving δ_{n-1} or δ_n. (See [6, Chap. I, Sect. 4]; these μ_i are called τ-restricted there.)

Thus, the first factor $\Pi = \bigotimes_{i=1}^{t-1} L(\mu_i)^{(2^i)}$ from (7) restricts to a simple module of $\Omega(2n, \bar{k})$ whose highest weight is 2^t-restricted and does not involve δ_{n-1} or δ_n. On the other hand, by (8), the restriction of the second factor $\Pi' = \bigotimes_{i=0}^{t-1} L(\varepsilon\tilde{\omega}_n)^{(2^i)}$ is a direct sum of simple modules, each having 2^t-restricted highest weight involving only δ_{n-1} and δ_n.

Therefore, the restrictions of both Π and Π' to $\Omega(f)$ are respectively simple and semisimple and certainly no simple summand of Π' is isomorphic to the dual of Π. Thus, the $\Omega(f)$-fixed points on L are given by

$$L(\lambda)^{\Omega(f)} \cong \mathrm{Hom}_{\bar{k}\Omega(f)}(k, \Pi \otimes \Pi') \cong \mathrm{Hom}_{\bar{k}\Omega(f)}(\Pi^*, \Pi') = 0. \tag{9}$$

The lemma is proved. ∎

3. DIMENSION OF $\mathscr{D}$

In this section we prove our first main result.

THEOREM 3.1. *The subcode $\mathscr{D}$ of k^P generated by the characteristic functions of nondegenerate quadrics of given Witt index polarizing to b is independent of the Witt index and is of dimension $(2n+1)^t$.*

Proof. Recall that, for a finite dimensional vector space U, the symmetric square $S^2(U^*)$ and the exterior square $\bigwedge^2(U^*)$ of the dual U^* of U describe, respectively, the space of all quadratic forms on U and the space of all symplectic bilinear forms on U. Let U be defined over a perfect field $\mathbb{F}$ of characteristic 2. As in Section 2, we shall let $U^{(2^i)}$ denote the ith Frobenius twist of U. For any finite set I of non-negative integers, let U_I denote $\bigotimes_{i\in I} U^{(2^i)}$. We have a short exact sequence

$$0 \to U^{*(2)} \to S^2(U^*) \xrightarrow{\theta} \bigwedge^2(U^*) \to 0 \tag{10}$$

of vector spaces, where θ is the polarization defined above. (See [14, Sect. 1] for all this.) In the above equation the space $U^{*(2)}$ of linear forms, with twisted scalar multiplication, may be identified with the space of squared linear forms as the squaring map defines a canonical vector space isomorphism between these spaces. Likewise, we shall always interpret the space $S^2(U^*)^{(2)}$ of quadratic forms with twisted scalar multiplication as the space of squares of quadratic forms, again through squaring, and we will denote its elements by f^2, where f is a quadratic form. This convention will also be extended to higher powers of 2.

Note that $b \in \bigwedge^2(V(q)^*)$. We shall be interested in the preimage $E(q)$ of $\mathbb{F}_q b$ in $S^2(U^*)$. Thus, we have a nonsplit short exact sequence of modules for the symplectic group G of b:

$$0 \to V(q)^{*(2)} \to E(q) \xrightarrow{\theta} \mathbb{F}_q b \to 0. \tag{11}$$

Fix a nondegenerate quadratic form $f \in E(q)$ on $V(q)$ and let $O(f)$ be its orthogonal group. The maps $v \to b(-, v) \to b(-, v)^2 \to f + b(-, v)^2$ are isomorphisms of the $O(f)$-sets $V(q) \cong V(q)^* \cong V(q)^{*(2)} \cong \theta^{-1}(b)$. Thus, as a $\mathbb{F}O(f)$-module, $E(q) = \mathbb{F}_q \oplus V(q)^{*(2)}$, where the decomposition corresponds to writing $f' \in E(q)$ as $f + v^2$ for $v \in V(q)^*$. Thus (11) splits relative to $O(f)$. But it does not split relative to G.

Let $Q \subset P$ be the quadric corresponding to f and $\mathcal{Q}$ denote the set of all quadrics in P having the same Witt index as Q and polarizing to b.

To prove the theorem, we have to compute the rank of the incidence map

$$\alpha: k^{\mathcal{Q}} \to k^P. \tag{12}$$

We observe that since the theorem concerns the rank of a k-linear map there is no loss in assuming that k contains $\mathbb{F}_q$ as a subfield, so we make this assumption throughout the proof of Theorem 3.1.

Let

$$M(q) = E(q) \otimes E(q)^{(2)} \otimes \cdots \otimes E(q)^{(2^{t-1})} \tag{13}$$

and M, E, and V denote the tensor product of $M(q)$, $E(q)$, and $V(q)$, respectvely, with k over $\mathbb{F}_q$.

We define

$$\beta: k^{\mathcal{Q}} \to M \tag{14}$$

and

$$\gamma: M \to k^P \tag{15}$$

as follows. Let $Q' \in \mathcal{Q}$ be the set of zeros in P of the quadratic form $f' \in E(q)$. Then f' is defined only up to a nonzero element of $\mathbb{F}_q$, but the element $a = f' \otimes f'^2 \otimes \cdots \otimes f'^{2^{t-1}}$ of $M(q)$ depends only on Q'. The element $a \otimes 1_k$ of M is $\beta Q'$. We regard $E(q)^{(2^i)}$ and k^P as spaces of functions from $V(q)$ to $\mathbb{F}_q$ and from P to k, respectively, and define γ as the map that sends the element $(g_0 \otimes g_1^2 \otimes \cdots \otimes g_{t-1}^{2^{t-1}}) \otimes 1_k$ of M to the function $\prod_i g_i^{2^i}$ on P. (Note that the factors $g_i^{2^i}$ of the product do not each, by themselves, define functions on P but the product does.) These are clearly kG-maps. The composite $\gamma \circ \beta$ is not quite α but rather $1_P - \alpha$, where 1_P is the constant function 1 on P. Now $k^P = k1_P \oplus Y_P$, where the subspace Y_P consists of all k-valued functions on P whose values at the points of P sum to zero. Then $1_P - \alpha$ has image in Y_P because members of $\mathcal{Q}$ have odd cardinality (see [9, Theorem 22.5.1, p. 23]); and the image of α is mapped onto the image of $1_P - \alpha$ under the projection onto Y_P. The theorem follows from two facts:

(i) β is surjective and γ is injective.

(ii) 1_P is not in the image of α.

From (i) it is immediate that the image of $1_P - \alpha$ is independent of Witt index and has the claimed dimension. From (ii) it follows that α and $1_P - \alpha$ have the same rank.

We now prove (i). The splitting of (11) relative to $O(f)$ noted above implies that, for $i = 0, 1, 2, ..., t-1$, $E(q)^{(2^i)}$ is the direct sum of $V(q)^{(2^{i+1})}$ and k as $kO(f)$-modules. (Note that $V(q)^{(2^t)} \cong V(q)^{(2^0)} = V(q)$.) So, as $kO(f)$-modules,

$$M \cong \bigoplus_{I \subseteq \{0, ..., t-1\}} V_I. \tag{16}$$

The importance of this is that M is semisimple and multiplicity-free as a $kO(f)$-module. Modules of this kind are easy to work with; to check that a map from such a module is injective it is necessary only to verify that the restriction to each component is nonzero; and to check that a map into such a module is surjective, one merely has to check that the image has nonzero projection into each component.

In the case of the maps β and γ both these conditions are very easy to check. For example, for any nonzero v, the image of $f' = f + v^2$ has nonzero projection onto each factor, so β is surjective.

Finally, we prove (ii). By Lemma 2.1 and Frobenius reciprocity [8, Chap. III, Theorem 2.5], we have for any nontrivial simple kG-module L,

$$\mathrm{Hom}_{kG}(\mathrm{ind}_{O(f)}^{G} k, L) \cong \mathrm{Hom}_{kO(f)}(k, L) = 0, \tag{17}$$

while

$$\mathrm{Hom}_{kG}(\mathrm{ind}_{O(f)}^{G} k, k) \cong \mathrm{Hom}_{kO(f)}(k, k) \cong k. \tag{18}$$

It follows that $k^{\mathscr{D}}$ has a unique maximal submodule, with quotient a one-dimensional trivial module, hence so does the image of α. In particular, the image of α is indecomposable. Since this image is clearly not equal to $k1_P$, it cannot contain $k1_P$, or else it would decompose as the direct sum of $k1_P$ and the intersection with Y_P. This establishes (ii) and completes the proof of the theorem. ∎

4. THE RADICAL SERIES AND THE SOCLE SERIES OF $\mathscr{D}$

The *socle* of a module A, denoted by $\mathrm{soc}A$, is the maximal semisimple submodule of A. The higher socles in the *socle series* (also called the *upper Loewy series*) are then defined recursively by

$$\mathrm{soc}^{i+1} A/\mathrm{soc}^i A = \mathrm{soc}(A/\mathrm{soc}^i A).$$

Dually, the *radical* of A, denoted by $\mathrm{rad}\, A$, is the intersection of all maximal submodules of A, so $A/\mathrm{rad}\, A$ is the maximal semisimple quotient of A. The *radical series* (also known as the *lower Loewy series*) is defined by

$$\mathrm{rad}^{i+1} A = \mathrm{rad}(\mathrm{rad}^i A).$$

The semisimple subquotients $\mathrm{soc}^{i+1} A/\mathrm{soc}^i A$ and $\mathrm{rad}^i A/\mathrm{rad}^{i+1} A$ are called the *layers* of the socle and radical series.

Our second theorem describes the radical and socle layers of the kG-module $\mathscr{D}$. Let $\bar{k}$ be an algebraic closure of k and let $\mathscr{D}_{\bar{k}}$ denote the corresponding code over $\bar{k}$. Then $\mathscr{D}_{\bar{k}} = \bar{k} \otimes_k \mathscr{D}$. Now by [5, 7.9(i), 7.10, and 5.29] a kG-module A is semisimple if and only if $\bar{k} \otimes_k A$ is a semisimple $\bar{k}G$-module.

It follows that the socle and radical layers of the $\bar{k}G$-module $\mathscr{D}_{\bar{k}}$ are simply obtained from those of the kG-module $\mathscr{D}$ by extending scalars to $\bar{k}$. If we have a decomposition of the layers of $\mathscr{D}_{\bar{k}}$ into simple $\bar{k}G$-modules, we

can recover the decomposition of $\mathscr{D}$ into simple kG-modules in the following way. Let A be a layer of $\mathscr{D}$ and suppose $\bar{k} \otimes_k A = \bigoplus_i L_i$. We note that by (16) $\bar{k} \otimes_k \mathscr{D}$ is multiplicity-free so no two L_i are isomorphic. The Galois group Γ of $\bar{k}$ over k acts on $\bar{k} \otimes_k A$ with A as the set of fixed points. Conjugation by Γ permutes the isomorphism classes of simple $\bar{k}G$-modules and so permutes the L_i. If B is a simple kG-summand of A, then $\bar{k} \otimes B$ is invariant under Γ hence equal to the sum of those L_i belonging to a union of orbits. On the other hand the sum of all L_i in a single orbit is a Γ-stable $\bar{k}G$-submodule of $\bar{k} \otimes_k A$ and the Γ-fixed points of this submodule form a kG-submodule of A. Therefore the simple kG-summands of A correspond bijectively with the Γ-orbits on the L_i and are obtained from them by taking the fixed points of Γ on the orbit sums of the L_i.

In this way, we are reduced to the case $k = \bar{k}$, which is what we shall assume in our statement and proof of the next theorem

THEOREM 4.1. *Assume k is algebraically closed. Let $S = \{0, 1, ..., t-1\}$. Then* $\mathrm{rad}^{t+1} \mathscr{D} = 0$, $\mathrm{soc}^{t+1} \mathscr{D} = \mathscr{D}$ *and for* $0 \leqslant i \leqslant t$ *we have*

$$\mathrm{rad}^i \mathscr{D}/\mathrm{rad}^{i+1} \mathscr{D} = \mathrm{soc}^{t+1-i}\mathscr{D}/\mathrm{soc}^{t-i}\mathscr{D} \cong \bigoplus_{I \subseteq S,\ |I| = i} V_I. \tag{19}$$

Proof. Since the kG-modules $\mathscr{D}$ $(= \mathrm{Im}\alpha)$, $\mathrm{Im}(1-\alpha)$ and M are all isomorphic, we choose to work with M. From the definition of $M(q)$ (see (5)), one can see that M has a filtration with semisimple layers as in the statement (take the natural semisimple filtration induced by the composition series of each tensor factor $E^{(2^i)}$). So what requires proof is the nonsplitting of the layers. More precisely, we will prove the following.

Let V_J be a composition factor of M. If $J \neq \varnothing$ and $r \notin J$, then the composition factor V_J appears before $V_{J \cup \{r\}}$ in every descending composition series of M.

Since all composition factors of M occur without multiplicity, this will follow from the existence of a section of M which is a nonsplit extension of V_J by $V_{J \cup \{r\}}$. Without loss, we can assume that $r = 1$. Consider the section of M obtained by taking E in the first tensor factor in the definition of M, V_j in the j-th factor whenever $j \in J$, and k in the other factors. This is certainly an extension of V_J by $V_{J \cup \{1\}}$, so the point is to prove that it does not split. To put it another way, we must prove that if $1 \notin J$ then $E \otimes V_J$ is a nonsplit extension of V_J with $V_{J \cup \{1\}}$. This is then reduced to proving

$$\mathrm{Hom}_{kG}(V_J \otimes V_J, E) = 0, \tag{20}$$

The structure of $V \otimes V$ is described in [6, Chap. I, Sect. 5.4]. To begin with we shall use only the fact that its composition factors are, ignoring multiplicities: k, V_1 and the unique nontrivial composition factor $L = L(\tilde{\omega}_2)$ of $\wedge^2(V)$. It follows that $V_J \otimes V_J$ has a filtration all subquotients of which have the form $L_I \otimes V_{K+1}$, where I and K are disjoint subsets of J and $K+1$ denotes the set $\{k+1 : k \in K\}$. Suppose first $0 \notin J$. Then

$$\mathrm{Hom}_{kG}(L_I \otimes V_{K+1}, V_1) = \mathrm{Hom}_{kG}(L_I, V_{(K \cup \{0\})+1}) = 0. \tag{21}$$

Therefore, if there is a nonzero map from $L_I \otimes V_{K+1}$ to E, then it must be surjective, since E has a unique maximal submodule isomorphic to V_1. Now any module which has E as a quotient also has a trivial quotient. But, except when I and K are both empty we have

$$\mathrm{Hom}_{kG}(L_I \otimes V_{K+1}, k) = \mathrm{Hom}_{kG}(L_I, V_{K+1}) = 0. \tag{22}$$

Furthermore, in the case that I and K are empty it is clear that E is not a homomorphic image of $L_I \otimes V_{K+1}$. We therefore conclude that if $0 \notin J$, there are no (nonzero) kG-maps from any $L_I \otimes V_{K+1}$ to E and hence none from $V_J \otimes V_J$.

So we must consider the case $0 \in J$. We write

$$V_J \otimes V_J = (V \otimes V) \otimes (V_{J \setminus \{0\}} \otimes V_{J \setminus \{0\}}). \tag{23}$$

As above, the module $V_{J \setminus \{0\}} \otimes V_{J \setminus \{0\}}$ has a filtration in which the subquotients have the form $L_I \otimes V_{K+1}$, where I and K are disjoint subsets of $J \setminus \{0\}$. Suppose that I and K are not both empty. Then we obtain

$$\mathrm{Hom}_{kG}(k \otimes L_I \otimes V_{K+1}, k) = \mathrm{Hom}_{kG}(L_I, V_{K+1}) = 0, \tag{24}$$

$$\mathrm{Hom}_{kG}(L \otimes L_I \otimes V_{K+1}, k) = \mathrm{Hom}_{kG}(L_{I \cup \{0\}}, V_{K+1}) = 0, \tag{25}$$

$$\mathrm{Hom}_{kG}(V_1 \otimes L_I \otimes V_{K+1}, k) = \mathrm{Hom}_{kG}(L_{I \cup \{0\}}, V_{(K \cup \{0\})+1}) = 0. \tag{26}$$

From (24), (25), and (26) we see that $\mathrm{Hom}_{kG}((V \otimes V) \otimes L_I \otimes V_{K+1}, E) = 0$, unless $I = K = \varnothing$.

It remains to consider the case $I = K = \varnothing$. Then $(V \otimes V) \otimes L_I \otimes V_{K+1}$ reduces to $V \otimes V$. From the submodule structure of $V \otimes V$ one can see that neither E nor $V^{(2)} \cong \mathrm{soc}(E)$ is a homomorphic image of V. Therefore, $\mathrm{Hom}_{kG}(V \otimes V, E) = 0$. The theorem is proved. ∎

Remark 4.1. The case $n = 2$ of Theorems 3.1 and 4.1 appears as Theorem 13 in [12, p. 493].

5. AN APPLICATION

Let $\hat{V}(q)$ be a $(2n+1)$-dimensional vector space over $\mathbb{F}_q$ and $\hat{P}$ the corresponding projective space. Let g denote a nondegenerate quadratic form on $\hat{V}(q)$ as well as the one induced by it on $\hat{P}$. Let $Q \subset \hat{P}$ be the quadric defined by g and $\langle v \rangle$ be its nucleus [9, Corollary 2, p. 10]. We identify the orthogonal geometry of (Q, g) with the symplectic geometry of (P, b) considered in Section 1 by taking $V(q)$ to be $\hat{V}(q)/\langle v \rangle$ and b to be the symplectic bilinear form induced by g on $\mathbb{P}(V(q))$, the identification being done via the natural map from $\hat{V}(q)$ to $V(q)$. We also identify the orthogonal group $O(g)$ with G, always via this map and talk about $O(g)$-modules. The set $\mathscr{H}$ of hyperplanes of $\hat{P}$ has three $O(g)$-orbits: the set $\mathscr{H}(t)$ of $(q^{2n}-1)/(q-1)$ tangent hyperplanes to Q, the set $\mathscr{H}(e)$ of $\binom{q^n}{2}$ hyperplanes intersecting Q in a nondegenerate elliptic quadric and the set $\mathscr{H}(h)$ of $\binom{(1+q^n)}{2}$ hyperplanes meeting Q in a nondegenerate hyperbolic quadric, see [9, Theorem 22.6.6 (a)(iii), (ii), p. 28, and Theorem 22.9.2, p. 44].

Let $\mathscr{C}(t)$, $\mathscr{C}(e)$, $\mathscr{C}(h)$ denote the $kO(g)$-submodules of $\mathscr{C}$ generated by the characteristic functions of the hyperplanes in $\mathscr{H}(t)$, $\mathscr{H}(e)$, and $\mathscr{H}(h)$, respectively. We have

$$\mathscr{C} = \mathscr{C}(t) + \mathscr{C}(e) + \mathscr{C}(h).$$

We note that $1_{\hat{P}}$, being the sum of characteristic functions on $\hat{P}$ of elements of $\mathscr{H}(t)$, is in $\mathscr{C}(t)$ and so also in $\mathscr{C}$. But it is not in $\mathscr{C}(e) + \mathscr{C}(h)$ because no element of $\mathscr{H}(e) \cup \mathscr{H}(h)$ contains the nucleus.

Let $\mathscr{C}^0$ denote the subcode of $k^{\hat{P}}$ generated by the characteristic functions of complements of hyperplanes of $\hat{P}$. Then,

$$\mathscr{C}(t) = k1_{\hat{P}} \oplus \mathscr{C}^0(t)$$

and

$$\mathscr{C}^0 = \mathscr{C}^0(t) + \mathscr{C}^0(e) + \mathscr{C}^0(h),$$

where $\mathscr{C}^0(t)$, $\mathscr{C}^0(e)$ and $\mathscr{C}^0(h)$ carry their obvious meanings as the subcodes generated by the complements of the three types of hyperplanes.

Consider

$$k^{\hat{P}} \xrightarrow{\eta} k^{Q} \xrightarrow{\zeta} k^{P}, \tag{27}$$

where η is the $O(g)$-module morphism taking a k-valued function on $\hat{P}$ to its restriction to Q and ζ is the isomorphism defined by the identification described above.

PROPOSITION 5.1. (i) $\mathscr{C}(e) = \mathscr{C}(h) \simeq \mathscr{D}$ *as* $kO(g)$*-modules.*

(ii) $\mathscr{C}^0$ *and* $\mathscr{C}(e)$ *are distinct* $kO(g)$*-module complements to* $k1_{\hat{P}}$ *in* $\mathscr{C}$. *However,* $\mathscr{C}^0 = \mathscr{C}^0(e)$.

(iii) $\mathscr{C}^0(t) = \mathrm{soc}(\mathscr{C}^0) = \mathrm{soc}(\mathscr{C}(e))$. *Moreover, this is a simple* $kO(g)$*-module of dimension* $(2n)^t$.

Proof. (i) Since nondegenerate elliptic (respectively, hyperbolic) quadrics in Q are intersections with Q of elements of $\mathscr{H}(e)$ (respectively, $\mathscr{H}(h)$) and they correspond to nondegenerate elliptic (respectively, hyperbolic) quadrics of the symplectic geometry of (P, b), Theorem 3.1 implies that $\zeta \circ \eta$ maps both $\mathscr{C}(e)$ and $\mathscr{C}(h)$ onto $\mathscr{D}$. Since $\dim \mathscr{C} = \dim \mathscr{D} + 1$, the codimension of $\mathscr{C}(e)$ as well as that of $\mathscr{C}(h)$ in $\mathscr{C}$ can be at most one. As noted before their sum does not contain $1_{\hat{P}}$ but $\mathscr{C}$ does. It follows that $\mathscr{C}(e) = \mathscr{C}(h)$ and that

$$\mathscr{C} = k1_{\hat{P}} \oplus \mathscr{C}(e).$$

Furthermore, $1_{\hat{P}}$ is mapped to 1_P. Therefore $\mathscr{C}(e)$ is mapped isomorphically to $\mathscr{D}$.

(ii) These submodules are distinct because $\mathscr{C}^0$ contains words with the nucleus of Q in their supports and $\mathscr{C}(e)$ does not.

Since $\langle 1_{\hat{P}}, \mathscr{C}^0(e) \rangle = \langle 1_{\hat{P}}, \mathscr{C}(e) \rangle = \mathscr{C}$, the codimension of $\mathscr{C}^0(e)$ in $\mathscr{C}$ is 1. So $\mathscr{C}^0 = \mathscr{C}^0(e)$.

(iii) By Theorem 4.1, we know that $\mathrm{soc}(\mathscr{D})$ is a simple module of dimension $(2n)^t$. Since it is nontrivial, this simple submodule is the unique complement to $k1_P$ in the socle of $k1_P \oplus \mathscr{D}$ and hence is equal to the socle of every complement of $k1_P$ in $k1_P \oplus \mathscr{D}$. By the above isomorphism from $\mathscr{C}$ to $k1_P \oplus \mathscr{D}$, we see that $\mathscr{C}$ has a unique nontrivial simple submodule in its socle. This submodule has dimension $(2n)^t$ and is equal to the socle of any complement of $k1_{\hat{P}}$ in $\mathscr{C}$. Thus, all statements will be proved if we show that $\mathscr{C}^0(t)$ is mapped under $\zeta \circ \eta$ to $\mathrm{soc}(\mathscr{D})$. Now the hyperplanes in $\mathscr{H}(t)$ are precisely those which contain the nucleus of Q, so under the identification of the orthogonal geometry of Q with the symplectic geometry of P they correspond to the hyperplanes of P. Therefore, by definition of $\zeta \circ \eta$, the image of $\mathscr{C}^0(t)$ is equal to the subcode of k^P generated by the characteristic functions of the complements of the hyperplanes in P. We must show that this submodule is equal to the socle of $\mathscr{D}$. This fact seems to be known but we will give a proof here along the lines of the proof of Theorem 3.1. Let $\mathscr{H}^*$ denote the set of hyperplanes in P. We must prove that the image of the map

$$\alpha^*: k^{\mathscr{H}^*} \to k^P \tag{28}$$

sending a hyperplane to the characteristic function of its complement is equal to the socle of $\mathscr{D}$. Let the modules M and E be as in the proof of Theorem 3.1. Define

$$\beta^*: k^{\mathscr{H}^*} \to M \tag{29}$$

as follows. A hyperplane H, defined by a linear function v may equally well be regarded as the set of zeros of $v^2 \in V^{*(2)} \subset E$. Then β^* sends H to $v^2 \otimes \cdots \otimes v^{2^t} \in \bigotimes_{i=1}^{t} V^{*(2^i)} \subseteq M$. Finally, let $\gamma: M \to k^P$ be as in (15) of the proof of Theorem 3.1. Then it is straightforward to check that $\gamma \circ \beta^* = \alpha^*$. Since the image of β^* is a simple kG-module and since $\mathscr{D}$ has a unique simple kG-submodule, the proof is complete. ▌

Remark 5.1. Blokhuis and Moorhouse have also proved the injectivity of η on $\mathscr{C}$ [3, Theorem 1.2(i)]. In the same paper they also give the dimension of $\mathscr{C}(t)$. Though $\mathscr{C}(e)$ depends on the quadratic form g polarizing to b, interestingly $\mathscr{C}^0(e)$ does not.

Remark 5.2. For a discussion of the case $n = 1$, see [3, Theorem 1.10]. Note that $C(e) \neq C(h)$ if $n = 1$; in fact the k-ary codes generated by the secant lines, the tangent lines and the external lines of a conic in a Desarguesian plane of order 2^t are all distinct, as a look at the intersection of the conic with the supports of the code words reveals.

ACKNOWLEDGMENT

We take this opportunity to thank the referee for several suggestions which have improved the exposition.

REFERENCES

1. E. F. Assmus, Jr., and J. Key, "Designs and Their Codes," Cambridge Univ. Press, Cambridge, UK, 1992.
2. M. Bardoe and P. Sin, The permutation modules for the action for $GL(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}(\mathbb{F}_q^{n+1})$, *J. London Math. Soc.* **61** (2000), 58–80.
3. A. Blokhuis and G. E. Moorhouse, Some p-ranks related to orthogonal spaces, *J. Algebraic Combin.* **4** (1995), 295–316.
4. A. E. Brouwer and H. A. Wilbrink, Block designs, *in* "Handboook of Incidence Geometry" (F. Buekenhout, Ed.), pp. 349–382, Elsevier, Amsterdam, 1995.
5. C. W. Curtis and I. Reiner, "Methods of Representation Theory, with Applications to Finite Groups and Orders," Vol. I, Wiley–Interscience, New York, 1981.
6. M. F. Dowd and P. Sin, On representations of algebraic groups in characteristic two, *Comm. Algebra* **24** (1996), 2597–2686.

7. R. H. Dye, Interrelations of symplectic and orthogonal groups in characteristic two, *J. Algebra* **59** (1979), 202–221.
8. W. Feit, "The Representation Theory of Finite Groups," North Holland, Amsterdam, 1982.
9. J. W. P. Hirschfeld and J. A. Thas, "General Galois Geometries," Oxford Univ. Press, Oxford/New York, 1991.
10. J. C. Jantzen, "Representations of Reductive Groups," Academic Press, New York, 1987.
11. G. E. Moorhouse, Some p-ranks related to geometric structures, *in* "Mostly Finite Geometries" (N. L. Johnson, Ed.), Lecture Notes in Pure and Appl. Math., Vol. 190, pp. 353–364, Dekker, New York, 1997.
12. N. S. N. Sastry and P. Sin, The code of a regular generalized quadrangle of even order, *Proc. Sympos. Pure Math.* **63** (1998), 485–496.
13. P. Sin, The permutation representation of $Sp(2m, \mathbb{F}_q)$ acting on the vectors of its standard module, preprint.
14. P. Sin and W. Willems, G-invariant quadratic forms, *J. Reine Angew. Math.* **420** (1991), 45–59.
15. R. Steinberg, Representations of algebraic groups, *Nagoya J. Math.* **22** (1963), 33–56.