The Code of a Regular Generalized Quadrangle of Even Order

N. S. Narasimha Sastry
Peter Sin

Introduction

Let $V(q) \cong \mathbb{F}_q^4$ be a 4-dimensional vector space over the field of $q = 2^n$ elements, endowed with a nonsingular symplectic form $\langle -, - \rangle$. Our aim is to study the incidence between the set P of one-dimensional subspaces of $V(q)$ (viewed as points of projective space) and the set L (lines) of isotropic 2-dimensional subspaces. This incidence system is the regular generalized quadrangle of order q. (See [8], p.37 and (5.2.1), p.77.) Let A be the incidence matrix, with rows labelled by the $q^3 + q^2 + q + 1$ points (in any order) and columns labelled by the $q^3 + q^2 + q + 1$ lines (in any order) and entries 0 or 1 according to whether or not the point lies on the line. The matrix A can be considered as a matrix over any commutative ring k and defines an k-linear map between the free k-modules k^L and k^P on L and P respectively, sending $l \in L$ to $\sum_{p \in l} p \in k^P$. The most interesting case is when $k = \mathbb{F}_2$, when we have a natural identification of subsets of P with the elements of $\mathbb{F}_2^P$. The first theorem gives the rank of A in this case. Two fields are involved, the field $\mathbb{F}_q$ defining the geometry and the coefficient field $k = \mathbb{F}_2$. The latter may be replaced by any extension without altering the rank, but the order $q = 2^n$ of the first field is critical. Let $\mathcal{N}$ be the collection of those subsets of $\mathbb{Z}/2n\mathbb{Z}$ which do not have two consecutive elements.

Theorem 1. *Let k be any field of characteristic 2. Then*

$$\begin{aligned} \mathit{rank}\ A &= 1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2n} + \left(\frac{1-\sqrt{17}}{2}\right)^{2n} \\ &= 1 + \sum_{I \in \mathcal{N}} 4^{|I|}. \end{aligned}$$

We shall in fact prove that the rank of A is equal to the second expression. A simple combinatorial proof of the equality of the two expressions is given in the first lemma of [6, Appendix].

This work was done while one of us (NSN) was visiting the university of Florida during 1995-96. He wishes to thank Professor John Thompson for kindly arranging this visit and the department for its kind hospitality and the friendly atmosphere during his stay.

We shall not prove Theorem 1 directly but instead, we shall deduce it from a much stronger result (Theorem 2) for which we need some notation and background results. We shall take k to be an algebraically closed field of characteristic 2 from now on. The group $G = \mathrm{Aut}(V(q), \langle -, - \rangle) \cong \mathrm{Sp}(4, q)$ acts on the sets P and L, preserving the incidence relation. Thus, the map from k^L to k^P defined by A is a map of kG-modules. Denote its image by $\mathcal{C}$. This is the code of the generalized quadrangle. Theorem 1 gives its dimension. It is is well known that the words of minimum weight in this code are precisely the scalar multiples of the columns of A ([3, Theorem 2.8,(b),p.3].]). It is clear that the vector $\mathbf{1} = \sum_{p \in P} p$ spans a trivial kG-submodule of k^P and that the map sending every $p \in P$ to $\mathbf{1}$ is a kG-projection onto this submodule. Thus

$$k^P = k\mathbf{1} \oplus Y_P, \tag{1}$$

where Y_P is the kernel of the projection. It is also immediate from the fact that each point lies on $q+1$ lines that $\mathbf{1} \in \mathcal{C}$. Thus, we have a decomposition

$$\mathcal{C} = k\mathbf{1} \oplus \overline{\mathcal{C}}. \tag{2}$$

We can think of $\overline{\mathcal{C}}$ as the set of codewords of even weight. Theorem 2 below describes the structure of the kG-module $\overline{\mathcal{C}}$ in detail.

We next recall some facts about the simple kG-modules. Let $V = V(q) \otimes_{\mathbb{F}_q} k \cong k^4$ and extend the symplectic form to V. Then G is the subgroup of the algebraic group $\mathrm{Sp}(V) \cong \mathrm{Sp}(4, k)$ fixed by the n-th power of the Frobenius morphism F (which is the map squaring matrix entries of elements in $\mathrm{SL}(4, k)$). It is well known [13, Theorem 28, p.146] that $\mathrm{Sp}(4, k)$ has an endomorphism τ with $\tau^2 = F$. Let S be any $\mathrm{Sp}(4, k)$-module, given by some representation $\phi : \mathrm{Sp}(4, k) \to \mathrm{GL}(S)$. Then for $i \in \mathbb{N}$, we denote by S_i, the vector space S with the "twisted" module structure given by the representation $\phi \circ \tau^i$. Clearly, $S \cong S_{2n}$ as kG-modules, so for kG-modules, we may take the indices in $\mathbb{Z}/2n\mathbb{Z}$. For $I \subseteq \mathbb{Z}/2n\mathbb{Z}$, we set $V_I = \bigotimes_{i \in I} V_i$ (with $V_\emptyset = k$). Then by Steinberg's Tensor Product Theorem [12,§11], the 4^n modules V_I are a complete set of nonisomorphic simple kG-modules. It makes sense to speak of even and odd elements of $\mathbb{Z}/2n\mathbb{Z}$, and so each $I \subseteq \mathbb{Z}/2n\mathbb{Z}$ can be partitioned as $I = I_{\mathrm{odd}} \cup I_{\mathrm{even}}$. We set $h_I = |I_{\mathrm{even}}| - |I_{\mathrm{odd}}|$.

Recall that the *radical* of a module is the largest submodule with semisimple quotient (called the *head*). Iterating, we obtain the *radical series*. Dually, the maximal semisimple submodule is called the *socle* and we have the *socle series*. We are ready to state the main result, from which Theorem 1 follows immediately.

THEOREM 2. *The radical series of $\overline{\mathcal{C}}$ has length $2n+1$. The radical layers are*

$$\operatorname{rad}^j(\overline{\mathcal{C}})/\operatorname{rad}^{j+1}(\overline{\mathcal{C}}) \cong \bigoplus_{\substack{I\in\mathcal{N}\\ h_I+n=j}} V_I \qquad (0\leq j\leq 2n).$$

Moreover, the socle series is the same in the sense that

$$\operatorname{soc}^j(\overline{\mathcal{C}}) = \operatorname{rad}^{2n+1-j}(\overline{\mathcal{C}}).$$

REMARK. Since every composition factor of $\overline{\mathcal{C}}$ has multiplicity 1, it follows that every submodule of $\overline{\mathcal{C}}$ is determined by the isomorphism type of its head.

The proof of Theorem 2 is presented in §1. In §2 we discuss certain subcodes of $\mathcal{C}$ of geometric origin.

§1. The structure of $\mathcal{C}$.

Let G_α and G_β be the stabilizers in G of a point and of a line respectively. We have the decomposition of $G_\alpha = U_\alpha L_\alpha$ as the semidirect product of its unipotent radical U_α with a Levi complement L_α. Further we have

$$L_\alpha \cong \mathrm{SL}(2,q)\times \mathbb{F}_q^\times. \tag{3}$$

The facts we use about $k\,\mathrm{SL}(2,q)$-modules can be found in [1]. The simple $k\,\mathrm{SL}(2,q)$-modules are all obtained as twisted tensor products of the standard 2-dimensional module W; if W_j ($j\in\mathbb{Z}/n\mathbb{Z}$) denotes the twist of this module by the j-th power of the Frobenius map and for $K\subseteq\mathbb{Z}/n\mathbb{Z}$, we set

$$W_K = \bigotimes_{j\in K} W_j,$$

then the W_K are a complete set of nonisomorphic simple $k\,\mathrm{SL}(2,q)$- modules. We fix an isomorphism in (3) and denote by $[a]$ the character $t\mapsto t^a$ of $\mathbb{F}_q^\times$, $a\in\mathbb{Z}/(q-1)\mathbb{Z}$. Then, since U_α acts trivially on all simple kG_α-modules, these modules are of the form

$$W_K\otimes[a] \qquad \text{(outer tensor product)}.$$

For example, the module $W_{\mathbb{Z}/n\mathbb{Z}}\otimes[0]$ is the Steinberg module St_{L_α}; also we will write $[a]$ for $k\otimes[a]$.

At several points later, we need facts about representations of G_α, which we collect in the next lemma.

Lemma 3.

(a) *The restriction of V to G_α is a uniserial module with composition factors (in descending order) $[-1]$, $W \otimes [0]$, $[1]$. The module is semisimple for L_α.*

(b) *The restriction of V_1 to G_α is a nonsplit extension of $W \otimes [-1]$ by $W \otimes [1]$. The module is semisimple for L_α.*

(c) *The group U_α is elementary abelian. This $\mathbb{F}_2 L_\alpha$- module can be given a $\mathbb{F}_q$-vector space structure $R(q)$ so that $R = R(q) \otimes_{\mathbb{F}_q} k$ is isomorphic as a kL_α-module to a nonsplit extension of $W \otimes [1]$ by $[1]$.*

(d) $\mathrm{Ext}^1_{kG_\alpha}(M, [-2]) = 0$ *for* $M \cong [0]$, $W \otimes [1]$ *and* $W \otimes [-1]$.

Proof: Parts (a), (b) and (c) are by direct calculations involving only the standard 4-dimensional matrix representation of G. In (c), to get the $\mathbb{F}_q$-structure, one must choose the isomorphisms between the root subgroups and the additive group of $\mathbb{F}_q$ in a consistent way, so that Z_α acts with the same character (instead of different Galois conjugates of a character) on both composition factors. The 1-cohomology groups for G_α with values in simple modules can all be computed by means of the inflation-restriction sequence [10, Ch. VII.6, Prop. 5 and p.118, Remark]; since we have a semidirect product in which the kernel U_α acts trivially on any simple kG_α-module M, the inflation-restriction sequence takes the form of the short exact sequence:
(4)

$$0 \to H^1(L_\alpha, M) \xrightarrow{\mathrm{inf}} H^1(G_\alpha, M) \xrightarrow{\mathrm{res}} \mathrm{Hom}_{kL_\alpha}\Big(\bigoplus_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_2)} R^{(\sigma)}, M\Big) \to 0.$$

The first term of this sequence is easy to compute given the calculations of all extensions of simple $k\,\mathrm{SL}(2,q)$-modules in [1], and the third term is straightforward to calculate. Thus we obtain the G_α- cohomology. Then (d) follows from the standard isomorphisms (cf. [10, p. 111]):

$$H^1(G_\alpha, [-2]) \cong \mathrm{Ext}^1_{kG_\alpha}(k, [-2]), \qquad \text{etc.} \quad \blacksquare$$

The automorphism τ of G interchanges the two parabolic subgroups G_α and G_β, so that

$$k^L \cong \mathrm{ind}_{G_\beta}^G(k) \cong [\mathrm{ind}_{G_\alpha}^G(k)]_1 \cong (k^P)_1. \tag{5}$$

We set $V_{\mathrm{odd}} = V_{(\mathbb{Z}/2n\mathbb{Z})_{\mathrm{odd}}}$ and $V_{\mathrm{even}} = V_{(\mathbb{Z}/2n\mathbb{Z})_{\mathrm{even}}}$.

The following lemma is a special case of Curtis' theory of modular representations of groups with a split BN-pair [7, 6.6, 6.8].

LEMMA 4.

(a) $\mathrm{soc}(Y_P) \cong \mathrm{head}(Y_P) \cong V_{\mathrm{even}}$.

(b) $\mathrm{soc}(Y_L) \cong \mathrm{head}(Y_L) \cong V_{\mathrm{odd}}$.

PROOF: By (5), it suffices to prove (a). Now k^P, is self-dual, so Y^P is too. Further, all simple kG-modules are self-dual, since V is. Thus, we are reduced to showing that $\mathrm{head}(Y_P) \cong V_{\mathrm{even}}$. By Frobenius reciprocity,

$$\mathrm{Hom}_{kG}(\mathrm{ind}_{G_\alpha}^G(k), V_I) \cong \mathrm{Hom}_{kG_\alpha}(k, V_I) \cong (V_I)^{G_\alpha}.$$

Direct computation shows that the only simple modules V_I on which G_α has a nonzero fixed point are k and V_{even}, and for these the space of fixed points is 1-dimensional. The lemma now follows from (1). ∎

Since $\overline{\mathcal{C}}$ is the image of the kG-map from Y_L to Y_P induced by A, Lemma 4 yields

$$\mathrm{head}(\overline{\mathcal{C}}) \cong V_{\mathrm{odd}} \quad \text{and} \quad \mathrm{soc}(\overline{\mathcal{C}}) \cong V_{\mathrm{even}}. \tag{6}$$

We denote by $[Y : W]_G$ the composition multiplicity of the simple kG-module W in the kG-module Y.

LEMMA 5. $[Y_P : V_{\mathrm{odd}}]_G = 1$.

PROOF: First, we observe that $V_{\mathbb{Z}/2n\mathbb{Z}}$ is the Steinberg module St_G. As is true of all Steinberg modules for groups of Lie type, St_G is projective and its restriction to a parabolic subgroup G_J is the induction to G_J of the Steinberg module of a Levi complement L_J [5, Proposition 6.3.3]. Thus, using Frobenius reciprocity,

$$\begin{aligned}\mathrm{Hom}_{kG}(St_G \otimes V_{\mathrm{even}}, \mathrm{ind}_{G_\alpha}^G(k)) &\cong \mathrm{Hom}_{kG_\alpha}(St_G \otimes V_{\mathrm{even}}, k)\\ &\cong \mathrm{Hom}_{kG_\alpha}(St_G, V_{\mathrm{even}})\\ &\cong \mathrm{Hom}_{kG_\alpha}(\mathrm{ind}_{L_\alpha}^{G_\alpha} St_{L_\alpha}, V_{\mathrm{even}})\\ &\cong \mathrm{Hom}_{kL_\alpha}(St_{L_\alpha}, V_{\mathrm{even}}).\end{aligned}$$

The last space has dimension $[V_{\mathrm{even}} : St_{L_\alpha}]_{L_\alpha}$ because St_{L_α} is projective (hence also injective).

We have $L_\alpha \cong \mathrm{SL}(2,q) \times \mathbb{F}_q^\times$ and the restriction of V to this subgroup is a direct sum of two one-dimensional modules and a two-dimensional simple module, by Lemma 3. Since $St_{L_\alpha} \cong W_{\mathbb{Z}/n\mathbb{Z}} \otimes [0]$, it follows that $[V_{\mathrm{even}} : St_{L_\alpha}]_{L_\alpha} \leq 1$. Next,

$$\begin{aligned}\mathrm{Hom}_{kG}(St_G \otimes V_{\mathrm{even}}, V_{\mathrm{odd}}) &\cong \mathrm{Hom}_{kG}(St_G, V_{\mathrm{even}} \otimes V_{\mathrm{odd}})\\ &= \mathrm{Hom}_{kG}(St_G, St_G) \cong k,\end{aligned}$$

so the projective cover of V_{odd} is a direct summand of $St_G \otimes V_{\text{even}}$. It now follows that $[\text{ind}_{G_\alpha}^G(k) : V_{\text{odd}}]_G \leq 1$ and equality holds by (6), which proves the lemma. ∎

We can now give a module-theoretic characterization of $\overline{\mathcal{C}}$.

LEMMA 6. *Suppose X is a kG-module satisfying the following conditions:*

(a) $\text{head}(X) \cong V_{\text{odd}}$*;*

(b) $\text{soc}(X) \cong V_{\text{even}}$ *and* $[X : V_{\text{even}}]_G = 1$*;*

(c) $\text{Hom}_{kG_\alpha}(X, k) \neq 0$.

Then $X \cong \overline{\mathcal{C}}$.

PROOF: By Frobenius reciprocity, (c) gives a nonzero kG-map from X to k^P. By (a), the image of this map is contained in Y_P and has head isomorphic to V_{odd}. This shows that the image is $\overline{\mathcal{C}}$, for Lemma 5 shows that there is a unique submodule of Y_P with this property and (6) shows that $\overline{\mathcal{C}}$ is one such. Finally, by (b), this map is injective. ∎

We will now construct a module satisfying the hypotheses of Lemma 6. The properties of $\overline{\mathcal{C}}$ stated in Theorem 2 will then be read off by closer examination of the construction itself.

To begin with, we assert that there exists a kG-module E which is uniserial with composition factors (in descending order) V_1, k, V_2. In fact (cf. [11, Lemma 2]) such a module exists as a subquotient of $V \otimes V$. (It is even a module for the algebraic group; it's dual admits a natural description as the quotient of the space of symmetric bilinear forms on V by the 1-dimensional span of the given symplectic form $\langle -, - \rangle$.) We then define $\tilde{X}$ to be the tensor product $\bigotimes_{i=0}^{n-1} E_{2i}$ of all the Galois conjugates of E. We note the following properties of $\tilde{X}$ which follow from its definition. The descending composition series of the tensor factors E_{2i} induce a natural descending filtration on $\tilde{X}$ of length $2n+1$ as follows. If we designate the composition factors of each E_{2i} to be of level 0, 1 and 2 in descending order, then the t-th layer of filtration on $\tilde{X}$ is the direct sum of all the tensor products (involving one composition factor from each E_{2i}) such that the levels of the factors add up to t. We shall call this the *descending tensor filtration*. It is clear that the products formed by taking one composition factor from each E_{2i} are all simple modules. Therefore each layer of this filtration is semisimple. Moreover, the composition factors V_J of $\tilde{X}$ each occur with multiplicity one and have the property that J has no consecutive indices of the form "odd-even". However, there are some in which consecutive indices of the form "even-odd" occur in J.

LEMMA 7. *$\tilde{X}$ has a submodule Z such that the composition factors of Z are precisely those composition factors V_J of $\tilde{X}$ for which J contains consecutive* *indices. In particular, the composition factors of $X = \tilde{X}/Z$ are precisely the V_J with J in the collection $\mathcal{N}$ of subsets not having consecutive indices.*

PROOF: Suppose V_J is a composition of $\tilde{X}$ such that J contains consecutive indices r, $r+1$. Note that r must be even and $n > 1$. Since V_J occurs with composition multiplicity one, there is a unique submodule A of X with $\mathrm{head}(A) \cong V_J$; A can be characterized as the smallest submodule having V_J as a composition factor. The Lemma will follow if we can prove that for every composition factor V_K of A, the set K also contains r and $r+1$. By induction, it is sufficient to consider the composition factors V_K of $\mathrm{rad}(A)/\mathrm{rad}^2(A)$. Suppose that V_K is such a factor. Then $\mathrm{Ext}^1_{kG}(V_J, V_K) \neq 0$. Thus J and K must satisfy the condition for this to hold given by the main theorem in [11], which states:

The space $\mathrm{Ext}^1_{kG}(V_J, V_K)$ is zero unless the symmetric difference of J and K is a singleton $\{i\}$ with $i-1 \notin J \cap K$, in which case it is one-dimesional.

If $J \subseteq K$, or $i \neq r$, $r+1$, we are done. Clearly i cannot be $r+1$. Finally, suppose $i = r$. So $J = K \cup \{r\}$. But since r is even, V_r occurs at level 2 in the tensor factor $E_{2(r-1)}$ of $\tilde{X}$, while k is at level 1. So the composition factor V_J appears in the layer of the tensor filtration on $\tilde{X}$ *below* that in which V_K appears. This contradicts the fact that V_K is a composition factor of A and the lemma is proved. ∎

We shall next prove that $X = \tilde{X}/Z$ has the structure claimed for $\overline{\mathcal{C}}$ in Theorem 2. Up to isomorphism there is a unique nonsplit extension D_i of V_i by the trivial module k (by [11]). The key fact is:

LEMMA 8. *If neither i nor $i-1$ belongs to $J \in \mathcal{N}$ then $D_i \otimes V_J$ is a nonsplit extension of $V_{J\cup\{i\}}$ by V_J.*

PROOF: This follows from the fact that D_i is isomorphic to a submodule of $V_{i-1} \otimes V_{i-1}$, so that $D_i \otimes V_J$ embeds in $V_{i-1} \otimes V_{J\cup\{i-1\}}$. Then since this is a tensor factor of $V_{i-1} \otimes V_{\mathbb{Z}/2n\mathbb{Z}}$, which by [11, Lemma 1] is a projective indecomposable module, hence has simple socle. Therefore $D_i \otimes V_J$ has simple socle and the lemma is proved. ∎

LEMMA 9. *The filtration on X induced by the tensor filtration on $\tilde{X}$ is equal to the radical filtration, and the reversed (ascending) filtration is the socle filtration.*

PROOF: Let $K \in \mathcal{N}$. Suppose that there is an odd index r in K. Then Lemma 8 applies with $J = K \setminus \{r\}$, showing that $D_r \otimes V_{K\setminus\{r\}}$ is indecomposable of length 2. If $r = 2j+1$, then D_r is isomorphic to a quotient of E_j. Let $\tilde{X}_j$ be the tensor product of the other factors, so that $\tilde{X} = E_j \otimes \tilde{X}_j$. Then

$V_{K\setminus\{r\}}$ is a composition factor of $\tilde{X}_j$, since $r+1 \notin K$. Therefore, $D_r \otimes V_{K\setminus\{r\}}$ is isomorphic to a subquotient of $\tilde{X}$. This shows that the unique composition factor V_K of $\tilde{X}$ occurs in a subquotient which is a nonsplit extension of V_K by $V_{K\setminus\{r\}}$. Note that in the tensor filtration of $\tilde{X}$, V_K appears exactly one layer above $V_{K\setminus\{r\}}$. Next suppose there is an even index $s = 2j$ so that $K \cup \{s\}$ is still in $\mathcal{N}$. Then the dual module D_r^* is isomorphic to a submodule of E_{2j-1} and a similar argument to the above shows that V_K occurs in $\tilde{X}$ in a subquotient which is a nonsplit extension of V_K by $V_{K\cup\{r\}}$. Again, we note that $V_{K\cup\{r\}}$ is exactly one layer below V_K in the tensor filtration of $\tilde{X}$. None of what we have said is affected by passing to X. Thus we have shown that if V_K is any composition factor of X then all composition factors of X which can be obtained either by deleting an odd index or by adding an even index appear strictly lower in the radical filtration of X and exactly one layer lower in the filtration induced from the tensor fitration of $\tilde{X}$. It is easy to see that starting with any $K \in \mathcal{N}$, we can reach the set $(\mathbb{Z}/2n\mathbb{Z})_{\mathrm{even}}$ by applying a suitable sequence of these two operations on indices.

Then since the induced filtration has semisimple layers, it follows that the two filtrations are equal. The dual argument shows that the ascending induced filtration is the socle filtration. ∎

Proof of Theorem 2: It remains to show $X \cong \overline{\mathcal{C}}$. The hypotheses (a) and (b) of Lemma 6 are immediate consequences of Lemma 9. We now check condition (c). If we consider E as a kG_α-module, then by parts (a) and (b) of Lemma 3, E has a filtration with subquotients (in descending order) $W\otimes[-1]$, $W\otimes[1]$, k, $[-2]$, $W_1\otimes[0]$, $[2]$, where the last three factors come from a G_α-filtration of $S = \mathrm{soc}_G(E) \cong V_2$. Then by Lemma 3 (d), the nonzero kG_α homomorphism from S to $[-2]$ extends to E. Therefore the induced homomorphism from $\bigotimes_{i=0}^{n-1} S_{2i} \cong V_{\mathrm{even}}$ to $[\sum_{i=0}^{n-1} 2^i(-2)] = [0]$ extends to $\tilde{X} = \bigotimes_{i=0}^{n-1} E_{2i}$. Since the submodule $\bigotimes_{i=0}^{n-1} S_{2i}$ of $\tilde{X}$ maps isomorphically to its image in X, this proves $\mathrm{Hom}_{kG_\alpha}(X, k) \neq 0$. So by Lemma 6, $X \cong \overline{\mathcal{C}}$. ∎

Remark. A closer look at the proof of Lemma 9 shows that the same argument, using lemma 8 will yield the entire submodule structure of $\overline{\mathcal{C}}$. From $J \in \mathcal{N}$ we may obtain other elements of $\mathcal{N}$ by deleting an odd index or by adding an even one so that the resulting set still belongs to $\mathcal{N}$. If $K \in \mathcal{N}$ is obtained from J by a sequence of these two types of operation, then we will write $K \prec J$. This is clearly a partial order with unique maximal element $(\mathbb{Z}/2n\mathbb{Z})_{\mathrm{odd}}$ and unique minimal element $(\mathbb{Z}/2n\mathbb{Z})_{\mathrm{even}}$. Consider the collection of those subsets $\mathcal{X}$ of $\mathcal{N}$ with the property that if $J \in \mathcal{X}$ and $K \prec J$, then $K \in \mathcal{X}$. This collection is partially ordered by inclusion. The argument of Lemma 9 shows that this partially ordered set is lattice-isomorphic to the collection of kG-submodules of $\overline{\mathcal{C}}$.

§2. Some geometric subcodes

Ovoids.

An *ovoid in the 3-dimensional projective space* $\mathbb{P}(V(q)) \cong PG(3,q)$ is a set $\mathcal{O}$ of q^2+1 points, of which no three are collinear. An *ovoid in the symplectic geometry* $\mathcal{W}(q) = (P, L)$ is a set $\mathcal{O}$ of q^2+1 points, such that no two lie on a common (isotropic) line. By a well-known theorem of Segre [9, Theorem III, p.321] (see also [2, Prop. 1 and Remarks, p.138]), the classification of the ovoids of $PG(3,q)$ and those of $\mathcal{W}(q)$ are equivalent problems.

The only known ovoids in $\mathcal{W}(q)$ are the (nondegenerate) *elliptic quadrics* and the *Tits ovoids* [14, n°.5]. An *elliptic quadric* is the set of one-dimensional isotropic subspaces in $V(q)$ for a quadratic form f of Witt index 1 which has the given symplectic form $< -, - >$ as its associated bilinear form. The stabilizer in G of an elliptic quadric is conjugate to a subgroup Ω which has a subgroup of index 2 isomorphic to $\mathrm{SL}(2,q^2) \cong \mathrm{SO}(V(q), f)$. A *Tits ovoid* is the set of self-conjugate points of a polarity of $\mathcal{W}(q)$ which exists only when q is an odd power of 2. When $q > 2$, its stabilizer in G is conjugate to the Suzuki group $Sz = \mathrm{Sp}(4,k)^{\tau^n}$.

The codes $\mathcal{Q}$ and $\mathcal{T}$.

Given a subset X of P, we can consider the sum of its elements as a vector $[X]$ in k^P, and thereby obtain a bijection from the set of all subsets of P to the $\mathbb{F}_2$-span of P in k^P. In [2, Propositions 2 and 3] it was shown that the elements $[\mathcal{O}]$, where $\mathcal{O}$ is either an elliptic quadric or a Tits ovoid, belong to the code $\mathcal{C}$. Let $\mathcal{Q}$ denote the subspace of $\mathcal{C}$ generated by the vectors $[\mathcal{O}]$ for elliptic quadrics, and let $\mathcal{T}$ denote the corresponding space for Tits ovoids. In this section we investigate these subcodes, which are clearly kG-submodules.

Up to isomorphism there is a unique nonsplit extension M_i of the trivial module by V_{i+2}. (The dual of this module was denoted D_{i+2} earlier.) Thus, M is isomorphic to a submodule of the module E defined earlier in the construction of X. Thus in $\tilde{X} = \bigotimes_{i=1}^n E_{2i}$ there is a submodule $\tilde{\mathcal{Q}} = \bigotimes_{i=1}^n M_{2i}$ of dimension 5^n. We also have [11, Lemma 2(b)]

$$M \cong \wedge^2(V_1)/(\wedge^2(V_1))^G. \tag{7}$$

We will describe the structure of $\tilde{\mathcal{Q}}$ and then show that it is isomorphic to $\mathcal{Q}$ as a kG-module. More precisely, we shall show that in the diagram

$$\begin{array}{ccc} \tilde{X} & \longrightarrow & X \cong \overline{\mathcal{C}} \\ & & \uparrow \\ & & \mathcal{C} \end{array} \tag{8}$$

the modules $\tilde{\mathcal{Q}}$ and $\mathcal{Q}$ map isomorphically to the same submodule of $\overline{\mathcal{C}}$.

LEMMA 10.

(a) *The horizontal map in (8) restricts to an isomorphism of $\tilde{\mathcal{Q}}$ with its image.*

(b) *The tensor filtration on $\tilde{X}$ induces the radical filtration (and socle filtration) of $\tilde{\mathcal{Q}}$. Thus, $\tilde{\mathcal{Q}}$ has radical length $n+1$ with*

$$\operatorname{rad}^j(\mathcal{Q})/\operatorname{rad}^{j+1}(\mathcal{Q}) \cong \bigoplus_{\substack{I \in (\mathbb{Z}/2n\mathbb{Z})_{\text{even}} \\ |I|=j}} V_I \qquad (0 \le j \le n).$$

PROOF: Part (a) is clear since $\tilde{\mathcal{Q}}$ has no composition factors in common with the kernel of the map. Part (b) is proved using Lemma 8, exactly as in the proof of Lemma 9. ∎

In view of Lemma 10(a) we identify $\tilde{\mathcal{Q}}$ with its image in $\overline{\mathcal{C}}$ and use the same symbol for both. Let $\overline{\mathcal{Q}}$ denote the image of $\mathcal{Q}$ in $\overline{\mathcal{C}}$.

LEMMA 11. $\tilde{\mathcal{Q}} = \overline{\mathcal{Q}}$.

PROOF: Let T be a cyclic subgroup of order q^2+1 of the stabilizer Ω in G of an elliptic quadric $\mathcal{O}$. First we have that $\overline{\mathcal{C}}^T$ is one-dimensional, either by direct calculation, knowing the composition factors by Theorem 2 or (more geometrically) by [2, Lemma 4]. Second, from Lemma 10 (b) we have $\operatorname{head}(\tilde{\mathcal{Q}}) \cong k$. Since T acts semisimply, these two observations imply that T fixes some nonzero vector in $\tilde{\mathcal{Q}}$, but none in $\operatorname{rad}\tilde{\mathcal{Q}}$. Thus, $\tilde{\mathcal{Q}}$ is the kG-submodule of $\overline{\mathcal{C}}$ generated by the one-dimensional space $\overline{\mathcal{C}}^T$. But it is clear that the image of $[\mathcal{O}]$ in $\overline{\mathcal{C}}$ is a nonzero vector fixed by T. Therefore, $\tilde{\mathcal{Q}}$ is generated by the image of $[\mathcal{O}]$, hence equal to $\overline{\mathcal{Q}}$. ∎

LEMMA 12. *The vertical map in (8) restricts to an isomorphism of $\mathcal{Q}$ to $\overline{\mathcal{Q}}$.*

PROOF: This amounts to checking that $\mathbf{1}$ does not lie in $\mathcal{Q}$. Supose it did. Then we would have $\mathcal{Q} \cong k \oplus \overline{\mathcal{Q}} \cong k \oplus \tilde{\mathcal{Q}}$, using Lemma 11 for the last isomorphism. Then since $\operatorname{head}(\tilde{\mathcal{Q}}) \cong k$, by Lemma 10(b), it would follow that $\dim_k \operatorname{Hom}_{kG}(\mathcal{Q}, k) = 2$. On the other hand $\mathcal{Q}$ is a quotient of the transitive permutation module $\operatorname{ind}_\Omega^G(k)$ with basis consisiting of the set of elliptic quadrics, and by Frobenius reciprocity, $\dim_k \operatorname{Hom}_{kG}(\operatorname{ind}_\Omega^G(k), k) = 1$, so we have a contradiction. ∎

We summarize our results on $\mathcal{Q}$.

Theorem 13. *$\mathcal{Q}$ is a 5^n-dimensional subcode of $\mathcal{C}$ isomorphic as a kG-module to*

$$\bigotimes_{i=0}^{n-1}[\wedge^2(V_1)/(\wedge^2(V_1))^G]_{2i}.$$

It has radical length $n+1$ and the layers of its radical series are those stated for $\tilde{\mathcal{Q}}$ in Lemma 10.

∎

Remark. If we fix an isomorphism $(k^P)_1 \cong k^L$ and identify submodules of $(k^P)_1$ with their images, then the subcode $\mathcal{Q}_1$ of k^L can be described in terms of the incidences of points and lines in $\mathcal{W}(q)$ and the ambient space $\mathbb{P}(V(q))$. Let $\widehat{L}$ denote the set of all lines in $\mathbb{P}(V(q))$ and $k^{\widehat{L}}$ the vector space having this set as basis. The same method used to prove Lemma 4 (see also [7], 6.6, 6.8) yields:

$$k^{\widehat{L}} \cong \langle \mathbf{1} \rangle \oplus Y_{\widehat{L}}, \qquad \mathrm{soc}_{\widehat{G}}(Y_{\widehat{L}}) \cong \mathrm{head}_{\widehat{G}}(Y_{\widehat{L}}) \cong \bigotimes_{i=0}^{n-1}[\wedge^2(V)]^{(i)}, \tag{9}$$

where the superscript (i) indicates twisting by F^i and $\mathbf{1}$ is the sum of all lines.

Consider the following diagram:

$$\begin{tikzcd}
k^{\widehat{L}} \arrow[r, "\widehat{\alpha}"] & k^{P} \arrow[r, "\alpha^*"] \arrow[d, "\widehat{\alpha}^*"'] & k^{L} \\
 & k^{\widehat{L}} \arrow[ur, "\pi"'] &
\end{tikzcd}$$

Here the maps $\widehat{\alpha}$ and $\widehat{\alpha}^*$ are respectively the line-point and point-line incidence maps of $\mathbb{P}(V(q))$. These maps commute with the action of $\widehat{G} = \mathrm{SL}(V(q))$. The map α^* is the point-line incidence map in $\mathcal{W}(q)$ and π is the projection mapping isotropic lines to themselves and nonisotropic lines to 0. These are kG-maps. It is immediate from the definitions that the diagram commutes. We consider first the map $\widehat{\alpha}^* \circ \widehat{\alpha}$. Since $\widehat{G}$ acts as a rank 3 permutation group on $\widehat{L}$, we have $\dim_k \mathrm{End}_{k\widehat{G}}(k^{\widehat{L}}) = 3$, and from (9) one sees that the identity and the maps onto the two simple submodules form a basis for this space. From this it is not hard to see that the image of $\widehat{\alpha}^* \circ \widehat{\alpha}$ must be $\mathrm{soc}_{\widehat{G}}(Y_{\widehat{L}})$. Since the diagram commutes, this shows that

$\mathcal{I} := \mathrm{Im}(\alpha^* \circ \widehat{\alpha}) = \pi(\mathrm{soc}_{\widehat{G}}(Y_{\widehat{L}}))$. We claim

$$\mathcal{I} = \langle \mathbf{1} \rangle \oplus Q_1. \tag{10}$$

It is easy to see that $\langle \mathbf{1} \rangle \subsetneq \mathcal{I}$. The image $\overline{\mathcal{I}}$ of $\mathcal{I}$ in $\overline{\mathcal{C}}$ is therefore a kG-quotient of $\mathrm{soc}_{\widehat{G}}(Y_{\widehat{L}})$ with simple socle equal to V_{even}. Since V_{even} occurs with composition multiplicity 1 in $\bigotimes_{i=0}^{n-1}[\wedge^2(V)]^{(i)}$, there is a unique such quotient, and Lemma 10 shows that it must be isomorphic to $\tilde{\mathcal{Q}}_1$. Thus in particular $\mathrm{head}(\overline{\mathcal{I}}) \cong k$, and we can conclude by the reasoning of Lemma 11 that $\overline{\mathcal{I}}$ is the submodule of $\overline{\mathcal{C}}_1$ generated by $(\overline{\mathcal{C}}_1)^{\tau(T)} = (\overline{\mathcal{C}}^T)_1$, namely, $\overline{\mathcal{Q}}_1$. Now (10) follows. ∎

Assume now that $n > 1$ is odd. Let $\overline{\mathcal{T}}$ denote the image of $\mathcal{T}$ in $\overline{\mathcal{C}}$.

Lemma 14. *Let $\mathcal{S}$ be a Tits ovoid and let Ω be the stabilizer of an elliptic quadric $\mathcal{O}$. Then there exists a cyclic subgroup T of Ω of order q^2+1 for which*

$$\sum_{t \in T} t[\mathcal{S}] = [\mathcal{O}].$$

Proof: We may assume that $\mathcal{S}$ is the Tits ovoid stabilized by Sz. Denote the sum in the statement by $f_T(\mathcal{S})$. Now $Sz \cap \Omega$ contains a cyclic subgroup T' of order $q \pm \sqrt{2q}+1$ and index 4 [4, Theorem 5(a)][1]

The centralizer in G of this subgroup is a cyclic subgroup of Ω of order q^2+1. We take this to be our T. Let $\{\mathcal{S}_j\}_{j=1}^{q \mp \sqrt{2q}+1}$ be the set of distinct images of $\mathcal{S}$ under T. Each $\mathcal{S}_j$ can be further decomposed into T'-orbits $\mathcal{S}'_{jl}$ $(1 \leq l \leq q \mp \sqrt{2q}+1)$. Then, since k has characteristic 2 we have

$$f_T(\mathcal{S}) = \sum_{j=1}^{q \pm \sqrt{2q}+1} \sum_{l=1}^{q \mp \sqrt{2q}+1} [\mathcal{S}'_{jl}].$$

We claim that for each j precisely one of the $\mathcal{S}'_{jl}$ is disjoint from all the other ovoids $\mathcal{S}_{j'}$, while each of the other $\mathcal{S}'_{jl}$ is equal to precisely one $\mathcal{S}'_{j'l}$ for $j' \neq j$. If $j' \neq j$ then $\mathcal{S}_{j'} \cap \mathcal{S}_j$ is a T'-orbit (cf. [4, proof of Theorem 1(b), p.156-157][1]) and if j, j' and j'' are distinct, then the T'-orbits $\mathcal{S}_{j'} \cap \mathcal{S}_j$ and $\mathcal{S}_{j''} \cap \mathcal{S}_j$ are distinct, since T acts semiregularly on $\mathbb{P}(V(q))$. This proves the claim. It follows the weight of $f_T(\mathcal{S})$ is equal to $(q+\sqrt{2q}+1)(q-\sqrt{2q}+1) = q^2+1$. In view of [2, Lemma 4] the only possibilty for $f_T(\mathcal{S})$ is $[\mathcal{O}]$. ∎

---

[1] On p.147 of this paper appears the erroneous statement that there is a single conjugacy class of subgroups isomorphic to $\mathrm{SL}(2,q^2)$ in $\mathrm{Sp}(4,q)$. There are in fact two classes, interchanged by the automorphism τ. The results which we use from this paper remain true however, so long as they are understood as referring to that conjugacy class whose members stabilize elliptic quadrics.

THEOREM 15.

(a) $\mathcal{Q} \subsetneq \mathcal{T}$.

(b) $\overline{\mathcal{T}} \subseteq \mathrm{rad}^n(\overline{\mathcal{C}})$ *but* $\overline{\mathcal{T}} \nsubseteq \mathrm{rad}^{n+1}(\overline{\mathcal{C}})$. *Consequently, the radical length of* $\overline{\mathcal{T}}$ *is* $n+1$.

(c) $\mathcal{T}$ *maps isomorphically to* $\overline{\mathcal{T}}$.

PROOF: (a) Lemma 14 gives the inclusion. To prove that this inclusion is proper, it is enough to show that Sz does not fix any nonzero element of $\mathcal{Q} \cong \tilde{\mathcal{Q}}$. Now each composition factor of $\tilde{\mathcal{Q}}$ remains simple upon restriction to Sz, so $[\tilde{\mathcal{Q}} : k]_{Sz} = 1$. Now $\tilde{\mathcal{Q}}$ has a kG quotient isomorphic to the nonsplit extension M of the trivial module by V_2. This extension does not split for Sz (e.g. using [11, Lemma 2]; here we use $n > 1$). We may therefore conclude that $\tilde{\mathcal{Q}}^{Sz} = 0$. This establishes (a).

(b) We consider the possibilities for simple homomorphic images of $\overline{\mathcal{T}}$. Now $\overline{\mathcal{T}}$ is a homomorphic image of the permutation module $\mathrm{ind}_{Sz}^G(k)$ and if V_J is a simple quotient of the latter then

$$(11) \quad 0 \neq \mathrm{Hom}_{kG}(\mathrm{ind}_{Sz}^G(k), V_J) \cong \mathrm{Hom}_{kSz}(k, V_J) \cong \mathrm{Hom}_{kSz}(V_{J_{\mathrm{even}}}, V_{J_{\mathrm{odd}}}).$$

Now $V \cong V_n$ for Sz, so both $V_{J_{\mathrm{even}}}$ and $V_{J_{\mathrm{odd}}} \cong V_{J_{\mathrm{odd}}+n}$ are simple kSz-modules, by the Tensor Product Theorem [12,§11]. Therefore, in order for (11) to hold, we must have $h_J = |J_{\mathrm{even}}| - |J_{\mathrm{odd}}| = 0$. The only layer of $\overline{\mathcal{C}}$ in which such V_J appear is $\mathrm{rad}^n(\overline{\mathcal{C}})/\mathrm{rad}^{n+1}(\overline{\mathcal{C}})$. It follows that any nonzero image in $\overline{\mathcal{C}}$ of $\mathrm{ind}_{Sz}^G(k)$ is contained in $\mathrm{rad}^n(\overline{\mathcal{C}})$ but not in $\mathrm{rad}^{n+1}(\overline{\mathcal{C}})$. In particular this is true of $\overline{\mathcal{T}}$. The radical length then follows from this and the fact that $\overline{\mathcal{T}}$ contains $\overline{\mathcal{Q}}$.

(c) We must show that $\mathbf{1} \notin \mathcal{T}$. We can argue exactly as in the proof of Lemma 12 (with $\mathcal{T}$ in place of $\mathcal{Q}$ and Sz in place of Ω) as long as we show $\mathrm{Hom}_{kG}(\overline{\mathcal{T}}, k) \neq 0$. To see this, observe that by (a) and (b) $\overline{\mathcal{Q}}$ is contained in $\overline{\mathcal{T}}$ and has nonzero image in $\mathrm{head}(\overline{\mathcal{T}})$, and that $\mathrm{head}(\overline{\mathcal{Q}}) \cong k$. ∎

REFERENCES

1. J. L. Alperin, *Projective modules for* $SL(2, 2^n)$, J. Pure and Applied Algebra **15** (1979), 219-234.
2. B. Bagchi, N.S.N. Sastry, *Even order inversive planes, Generalized quadrangles and codes*, Geom. Dedicata **22** (1987), 137-147.
3. B. Bagchi, N.S.N. Sastry, *Codes associated with Generalized polygons*, Geom. Dedicata **27** (1988), 1-8.
4. B. Bagchi, N.S.N. Sastry, *Intersection pattern of the classical ovoids in symplectic 3-space of even order*, J. Algebra **26** (1989), 147-160.
5. R. W. Carter, "Finite Groups of Lie Type, Conjugacy Classes and Complex Characters," Wiley, Chichester, 1985.

6. L. Chastkofsky, W. Feit, *On the Projective characters in characteristic 2 of the groups $Suz(2^m)$ and $Sp_4(2^n)$*, Publ. Math. I. H. E. S. **51** (1980), 9-35.
7. C. W. Curtis, *Modular representations of finite groups with split BN-pairs*, Springer Lecture Notes **131** (1964), 57-95.
8. S. E. Payne, J. A. Thas, "Finite Generalized Quadrangles," Advanced Publishing Program, Pitman, Boston, London, Melbourne, 1984.
9. B. Segre, *On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two*, Acta Arithm. **5** (1959), 315-332.
10. J-P. Serre, "Local Fields," Graduate Texts in Mathematics, Springer Verlag, Berlin, New York, Heidelberg, 1979.
11. P. Sin, *Extensions of simple modules for $Sp_4(2^n)$ and $Sz(2^n)$*, Bull. Lond. Math. Soc. **24** (1992), 159-164.
12. R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33-56.
13. R. Steinberg, "Lectures on Chevalley Groups," Mimeographed Notes, Yale Univ. Math. dept., New Haven, Conn., 1968.
14. J. Tits, *Ovoides et groupes de Suzuki*, Archiv der Math. **13** (1962), 187-198.

Math.-Stat. Division, Indian Statistical Institute, 8th mile, Mysore Road, R.V. College Post, Bangalore-560059, India
e-mail: nsastry@isibang.ernet.in
Department of Mathematics, University of Florida, Gainesville, FL 32611, USA
e-mail: sin@math.ufl.edu