HIGHER WEIGHTS OF GRASSMANN CODES

SUDHIR R. GHORPADE AND GILLES LACHAUD

Abstract. Using a combinatorial approach to studying the hyperplane sections of Grassmannians, we give two new proofs of a result of Nogin concerning the higher weights of Grassmann codes. As a consequence, we obtain a bound on the number of higher dimensional subcodes of the Grassmann code having the minimum Hamming norm. We also discuss a generalization of Grassmann codes.

Contents

1. Introduction

Let C be linear $[n,k]_q$–code, that is, a k-dimensional subspace of the n-dimensional vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$ with q elements. Given any (linear) subspace D of $\mathbb{F}_q^n$, one defines (cf. [14]) the *Hamming norm* of D as

$$\|D\| = |\{i \in \{1,\dots,n\} : \text{ there exists } v \in D \text{ with } v_i \neq 0\}|.$$

Given $r \geq 1$, the r-th *higher weight* of the code C is defined by

$$d_r = d_r(C) = \min\{\|D\| : D \text{ is a subspace of } C \text{ with } \dim D = r\}.$$

Note that $d_1 = d_1(C)$ is the classical Hamming weight or the minimum distance of C. The notion of higher weights was first introduced by V. Wei in [15] and, besides being a natural generalization of Hamming weights, it has found a number of applications in Cryptography and Coding Theory. For a survey of this topic and a detailed bibliography, we refer to [14].

In this paper, we consider the so called Grassmann codes, which were introduced, and studied in a series of papers (cf. [8]– [12]) by C. Ryan and K. Ryan in the binary

---

Date: December 15, 1998.

1991 *Mathematics Subject Classification.* 11T71, 14M15, 51E20, 94B05, 94B27.

The first author is partially supported by a 'Career Award' grant from AICTE, New Delhi and an IRCC grant from IIT Bombay.

This is an unofficial electronic version of the paper which has appeared in *Coding Theory, Cryptography and Related Areas* (Guanajuato, 1998), J. Buchmann, T. Hoeholdt, H. Stichtenoth and H. Tapia-Recillas Eds., Springer-Verlag, Berlin (2000), pp. 122–131; MR **2001d:**940136. Some of the references have been updated.

case ($q = 2$) and later by D. Nogin [7] in the general case. These codes may be viewed as a generalization of Reed-Muller codes. In [7], Nogin has shown that the higher weights d_r of the Grassmann code $C(\ell, m)$ satisfy the Griesmer-Wei bound for $r \leq \max\{\ell, m-\ell\}+1$. One of the main aims of this paper is to give an alternate, short proof of this result of Nogin. Our approach is based on using the Plücker embedding of the Grassmannian and a classical and elementary result concerning the same. This approach has turned out to be quite fruitful elsewhere in the study of MDS codes (cf. [1]) and it seems conceivable that this may also be helpful in studying a possibly far-reaching generalization of the Grassmann codes that is proposed in Section 5 of this paper. Besides the abovementioned alternate, short proof of Nogin's result, we also indicate how, using a certain combinatorial structure theorem proved in [1], we can obtain a yet another proof. This second proof of Nogin's result on higher weights of Grassmann codes $C(\ell, m)$ is arguably more 'natural' in the sense that, unlike in Nogin's proof and our first proof, one does not have to pass to the dual Grassmannian in order to assume something like $m - \ell \geq \ell$. In fact, this 'natural' proof makes it transparent why a quantity such as "$\max\{\ell, m-\ell\}+1$" should appear, and, moreover, one can also obtain as a corollary, a bound on the number of r-dimensional subcodes of $C(\ell, m)$ with minimum Hamming norm, for $r \leq \max\{\ell, m-\ell\}+1$.

This paper is organized as follows. In Section 2 below, we collect some preliminaries concerning projective systems and Grassmannians. In Section 3, we recall a basic fact about Grassmannians and deduce some results for the number of $\mathbb{F}_q$-rational points of sections of Grassmannians by coordinate hyperplanes. These are applied to give two proofs of Nogin's result on higher weights in Section 4. Finally, in Section 5, we discuss a possible generalization of the Grassmann codes, make a conjecture about the minimum distance of these general codes, and prove a partial result towards this conjecture by using the techniques of Section 3. It may be remarked that the methods used in Sections 3 and 4 are similar to those in [1]. Also, a few results (Corollary 3.3, for example) are analogous to those in [1] but the proofs here are somewhat different. At any rate, it seemed desirable that for an alternate proof which is claimed to be 'short', the exposition here should be reasonably self-contained.

A part of this work was done when the first author was visiting the Institut de Mathématiques de Luminy (IML) in Marseille for a few months during 1997 and 1998. He would like to use this opportunity to thank the IML for its hospitality and the CNRS of France for its support. Thanks are also due to Michael Tsfasman for a number of helpful discussions, and to Hao Chen for his comments on a preliminary version of this paper.

2. Preliminaries

For studying, or even defining, the Grassmann codes, it is convenient to use the language of projective systems due to Tsfasman and Vlăduţ. Thus, we begin by briefly recalling some basic aspects of this terminology. For details, one may refer to [13], [14].

An $[n, k]_q$*–projective system* is a collection of n not necessarily distinct points in the $(k-1)$-dimensional projective space $\mathbb{P}^{k-1}_{\mathbb{F}_q}$ over $\mathbb{F}_q$. It is called *nondegenerate* if these n points are not contained in any hyperplane. Incidentally, a linear

$[n,k]_q$–code $C \subseteq \mathbb{F}_q^n$ is called *nondegenerate* if C is not contained in any coordinate hyperplane. One has a natural notion of equivalence of projective systems as well as of linear codes. There is a natural one-to-one correspondence between the equivalence classes of nondegenerate $[n,k]_q$–projective systems and the equivalence classes of nondegenerate linear $[n,k]_q$–codes. Under this correspondence, if X is an $[n,k]_q$–projective system and C is the corresponding code, then the nonzero codewords of C correspond to hyperplanes in $\mathbb{P}^{k-1}_{\mathbb{F}_q}$ and more generally, subcodes $D \subset C$ of dimension r correspond to (projective) subspaces of codimension r in $\mathbb{P}^{k-1}_{\mathbb{F}_q}$. Consequently, the higher weights of C are given by

$$\begin{aligned} d_r(C) & \\ &= \min\left\{|X \cap \Pi^c| : \Pi \text{ is a projective subspace of codimension } r \text{ in } \mathbb{P}^{k-1}\right\} \\ &= n - \max\left\{|X \cap \Pi| : \Pi \text{ is a projective subspace of codimension } r \text{ in } \mathbb{P}^{k-1}\right\}. \end{aligned}$$

Here Π^c denotes the complement (in $\mathbb{P}^{k-1}_{\mathbb{F}_q}$) of Π.

Nice examples of projective systems can be obtained by considering (the set of $\mathbb{F}_q$-rational points of) projective algebraic varieties defined over $\mathbb{F}_q$. In particular, the Grassmannian over $\mathbb{F}_q$:

$$G_{\ell,m} = G_{\ell,m}(\mathbb{F}_q) = \{W : W \text{ is a subspace of } \mathbb{F}_q^m \text{ with } \dim W = \ell\}$$

defines an $[n,k]_q$–projective system, with

$$n := |G_{\ell,m}(\mathbb{F}_q)| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q := \frac{(q^m-1)(q^m-q)\dots(q^m-q^{\ell-1})}{(q^\ell-1)(q^\ell-q)\dots(q^\ell-q^{\ell-1})} \quad \text{and} \quad k := \binom{m}{\ell}.$$

Note that the above formula for $|G_{\ell,m}(\mathbb{F}_q)|$ is a well-known fact whose proof can be found, for example, in [2]. Here, we use the natural nondegenerate embedding of $G_{\ell,m}(\mathbb{F}_q)$ in $\mathbb{P}^{k-1}_{\mathbb{F}_q}$, called the *Plücker embedding*. This is concretely obtained as follows. Let

$$I(\ell,m) = \{\alpha = (\alpha_1,\dots,\alpha_\ell) \in \mathbb{Z}^\ell : 1 \le \alpha_1 < \dots < \alpha_\ell \le m\}$$

be an indexing set [ordered, say, lexicographically] for the points of $\mathbb{P}^{k-1}(\mathbb{F}_q)$. Given any $\alpha \in I(\ell,m)$ and any $\ell \times m$ matrix $A = (a_{ij})$, let

$$p_\alpha(A) = \alpha\text{–th minor of } A \ := \ \det\left(a_{i\alpha_j}\right)_{1\le i,j\le \ell}.$$

Now, for any $W \in G_{\ell,m}(\mathbb{F}_q)$, we can find a $\ell \times m$ matrix A_W whose rows give a basis of W, and then

$$p(W) = \left(p_\alpha(A_W)\right)_{\alpha \in I(\ell,m)} \in \mathbb{P}^{k-1}_{\mathbb{F}_q}$$

is called the *Plücker coordinate* of W. It is easy to see that this depends only on W and not on the choice of A_W. Moreover, the map $W \mapsto p(W)$ of $G_{\ell,m}(\mathbb{F}_q) \to \mathbb{P}^{k-1}_{\mathbb{F}_q}$ is injective and its image equals the zero locus of certain quadratic polynomials (cf. [4], [5] for details); this map, then, is the *Plücker embedding*. Henceforth, we shall identify W with $p(W)$. It may be remarked that in defining the Plücker embedding, we have tacitly used representations of elements of $\mathbb{F}_q^m$ in terms of the natural basis of $\mathbb{F}_q^m$; if instead, we use another basis to define the 'coordinates', then we have a linear isomorphism (i.e., a collineation) of the ambient space $\mathbb{P}^{k-1}_{\mathbb{F}_q}$, which induces an isomorphism between the two different embeddings of $G_{\ell,m}(\mathbb{F}_q)$.

The nondegenerate linear $[n,k]_q$–code corresponding to the projective system defined by $G_{\ell,m}(\mathbb{F}_q)$ (with its Plücker embedding) is denoted by $C(\ell,m)$ and is called the *Grassmann code*. It may be noted that if $\ell = 1$, then $G_{\ell,m}(\mathbb{F}_q) = \mathbb{P}^{m-1}_{\mathbb{F}_q}$, and thus in this case $C(\ell, m)$ is essentially the Reed-Muller code. On the other hand, if $l = m$, then $G_{\ell,m}(\mathbb{F}_q)$ reduces to a single point. To avoid trivialities, hereafter we shall tacitly assume that $1 \le \ell < m$.

3. Linear Sections of Grassmannians

We begin by stating a classical result on Grassmannians and then prove some auxiliary results concerning sections of the Grassmannian by linear subspaces that are intersections of coordinate hyperplanes. First, we need some notation.

Given any $\alpha \in I(\ell, m)$, we let

$$B_\alpha = \{p \in G_{\ell,m}(\mathbb{F}_q) : p_\alpha = 1\}$$

and

$$C_\alpha = \{\mathbf{t} = (t_{ij}) : \mathbf{t} \text{ an } \ell \times m \text{ matrix over } \mathbb{F}_q \text{ with } t_{i\alpha_j} = \delta_{ij} \text{ for } 1 \le i, j \le \ell\},$$

where δ_{ij} is the usual Kronecker delta. Given any $\gamma_1, \ldots, \gamma_\ell \in \{1, \ldots, m\}$ and any $p \in \mathbb{P}^{k-1}(\mathbb{F}_q)$, we let

$$p_{\gamma_1 \ldots \gamma_\ell} = \begin{cases} 0 & \text{if } \gamma_i = \gamma_j \text{ for some } i \ne j \\ p_\alpha & \text{if there exists a permutation } \sigma \text{ of } \{1, \ldots, \ell\} \\ & \text{such that } \left(\gamma_{\sigma(1)}, \ldots, \gamma_{\sigma(\ell)}\right) = \alpha \in I(\ell, m). \end{cases}$$

The following result appears essentially as Proposition 2 in [5], and is also implicit in [4]. For more motivation and references about this result, see [1].

3.1. Lemma (Basic Cell Lemma). *Fix any $\alpha \in I(\ell, m)$. Then the polynomial maps (or morphisms) $\Phi : B_\alpha \to C_\alpha$ and $\Psi : C_\alpha \to B_\alpha$ defined by*

$$\Phi(p) = (t_{ij}(p)), \quad \text{where} \quad t_{ij}(p) := p_{\alpha_1 \ldots \alpha_{i-1} j \alpha_{i+1} \ldots \alpha_\ell}, \quad \textit{for } 1 \le i \le \ell, \ 1 \le j \le m$$

and

$$\Psi(\mathbf{t}) = (p_\beta), \quad \text{where} \quad p_\beta := \beta\textit{-th minor of } \mathbf{t} = \det\left(t_{i\beta_j}\right)_{1 \le i,j \le \ell}, \quad \text{for } \beta \in I(\ell, m),$$

are bijective and inverses of each other.

Now we introduce the following notation for intersections of the Grassmannian by coordinate hyperplanes. Given any subset Λ of $I(\ell, m)$, we let

$$E_\Lambda = \{p \in G_{\ell,m}(\mathbb{F}_q) : \ p_\alpha = 0 \text{ for all } \alpha \in \Lambda\}.$$

For a "small" subset Λ such as $\{\alpha\}$, $\{\alpha, \beta\}$, $\{\alpha, \beta, \gamma\}$, the corresponding E_Λ would be simply denoted by E_α, $E_{\alpha\beta}$, $E_{\alpha\beta\gamma}$, respectively. By standard conventions, E_Λ equals $G_{\ell,m}(\mathbb{F}_q)$ if Λ is empty.

Given any $\alpha \in I(\ell, m)$, by $\bar{\alpha}$ we shall denote the corresponding set, i.e., $\bar{\alpha} = \{\alpha_1, \ldots, \alpha_\ell\}$. A family $\Lambda \subseteq I(\ell, m)$ will be called *close* if $|\bar{\alpha} \cap \bar{\beta}| = k - 1$ for all $\alpha, \beta \in \Lambda, \ \alpha \ne \beta$.

3.2. Proposition. *Let $\Lambda \subseteq I(\ell, m)$ be a close family of cardinality r. Let $\delta = \ell(m - \ell)$. Then*

$$|E_\Lambda| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q - q^\delta - q^{\delta-1} - \cdots - q^{\delta-r+1}.$$

Proof. We proceed by induction on r. The case when $r = 0$ (i.e., when Λ is empty) is trivial. Assume that $r \geq 1$ and that the result holds for smaller values of r. Fix any $\alpha \in \Lambda$. Since Λ is close, for any $\beta \in \Lambda$ with $\beta \neq \alpha$, there exist unique integers $u = u(\beta)$ and $v = v(\beta)$ such that $1 \leq u \leq \ell$, $1 \leq v \leq m$, $v \notin \bar{\alpha}$ and $\beta = (\alpha_1, \ldots, \alpha_{u-1}, v, \alpha_{u+1}, \ldots, \alpha_\ell)$. Clearly the pairs $(u(\beta), v(\beta))$ are distinct for distinct elements $\beta \in \Lambda$. Moreover, for any $p \in B_\alpha$, and any $\beta \in \Lambda$ with $\beta \neq \alpha$, the β-th minor of $\mathbf{t} = \Phi(p)$ is precisely equal to t_{uv}. Thus it follows from Lemma 3.1 that the set $A_{r-1} = \{p \in G_{\ell,m} : p_\alpha \neq 0 \text{ and } p_\beta = 0 \text{ for all } \beta \in \Lambda \setminus \{\alpha\}\}$ is in bijection with the zero locus of $r-1$ distinct coordinates in ${\mathbb{F}_q}^\delta$, and hence $|A_{r-1}| = q^{\delta-r+1}$. Now note that $E_\Lambda = E_{\Lambda\setminus\{\alpha\}} \setminus A_{r-1}$, and apply the induction hypothesis. □

3.3. Corollary. *Given any $\alpha \in I(\ell,m)$, we have $|E_\alpha| = {m \brack \ell}_q - q^{\ell(m-\ell)}$.*

Proof. Any singleton subset of $I(\ell,m)$ is close. So we can apply Proposition 3.2. □

4. Computation of Higher Weights

In this section, we shall give two proofs of Nogin's result on the determination of certain higher weights d_r of the Grassmann code $C(\ell,m)$. As in Proposition 3.2, we let $\delta = \ell(m-\ell)$. The following result is proved in [7, Thm. 4.1].

4.1. Proposition. $d_1(C(\ell,m)) = q^\delta$.

Remarks. 1. Notice that a weaker version of the above result, namely, the inequality, $d_1 \leq q^\delta$ is an immediate consequence of Corollary 3.3.

2. Nogin's proof of Proposition 4.1 uses the language of Exterior Algebra, and he shows that if $\omega \in \Lambda^{m-\ell}\mathbb{F}_q^m$ is "completely decomposable" then the corresponding hyperplane H_ω is of minimum weight, that is, $|H_\omega^c \cap G_{\ell,m}(\mathbb{F}_q)| = q^\delta$. It may be noted that these completely decomposable hyperplanes are essentially the same as the coordinate hyperplanes $E_\alpha = \{p \in G_{\ell,m}(\mathbb{F}_q) : p_\alpha = 0\}$. Indeed, if a completely decomposable element $\omega = v_1 \wedge \cdots \wedge v_{m-\ell} \in \Lambda^{m-\ell}\mathbb{F}_q^m$ is nonzero, then we can extend $\{v_1, \ldots, v_{m-\ell}\}$ to a basis $\{v_1, \ldots, v_m\}$ of $\mathbb{F}_q^m$. If we use this basis to define the Plücker coordinates, then for any $\omega' \in \Lambda^\ell\mathbb{F}_q^m$, the condition $\omega' \wedge \omega = 0$ (that defines H_ω) corresponds precisely to the condition $p_\alpha = 0$ (that defines E_α) for a uniquely determined α.

3. A change of basis of the ambient space can be viewed as an instance of the natural action of the general linear group $GL_m(\mathbb{F}_q)$ on the Grassmannian $G_{\ell,m}(\mathbb{F}_q)$. (See, for example, [1] for an explicit description of this group action). This action is transitive and thus an 'orbit' of p_α will consist of $|G_{\ell,m}(\mathbb{F}_q)| = {m \brack \ell}_q$ elements. Moreover, the α-th Plücker coordinate p_α is determined only up to multiplication by nonzero elements of $\mathbb{F}_q$. This shows that the number of hyperplanes H in $\mathbb{P}^{k-1}_{\mathbb{F}_q}$ such that $|H \cap G_{\ell,m}(\mathbb{F}_q)| = {m \brack \ell}_q - q^\delta$, or equivalently, the number of minimum weight codewords of the Grassmann code $C(\ell,m)$, is $\geq (q-1){m \brack \ell}_q$. This inequality may be viewed as a weak version of Corollary 4.5 of [7].

We are now ready to state and prove Nogin's main result on higher weights of Grassmann codes.

4.2. Theorem. *For $1 \leq r \leq \max\{\ell, m-\ell\} + 1$, we have*

$$d_r(C(\ell,m)) = q^\delta + q^{\delta-1} + \cdots + q^{\delta-r+1} = q^\delta\left(1 + \frac{1}{q} + \cdots + \frac{1}{q^{r-1}}\right).$$

Proof. It is well-known (cf. [15]) that the higher weights of any linear code satisfy the Griesmer-Wei bound:

$$d_r \geq \sum_{i=0}^{r-1} \left\lceil \frac{d_1}{q^i} \right\rceil .$$

Thus, for the Grassmann code $C(\ell, m)$, we find using Proposition 4.1 that

$$d_r \geq q^\delta + q^{\delta-1} + \cdots + q^{\delta-r+1}.$$

Now, since $G_{\ell,m}$ and $G_{m-\ell,m}$ are isomorphic, we may assume without loss of generality that $(m-\ell) \geq \ell$. Choose any subset λ of $\{1, 2, \ldots, m\}$ of cardinality $\ell - 1$. Given any positive integer r such that $r \leq m - \ell + 1$, we can choose r distinct integers from the complement of λ in $\{1, 2, \ldots, m\}$, and add them to λ to generate a close subset Λ of $I(\ell, m)$ cardinality r. Therefore, by Proposition 3.2 and the description, given in Section 2, of higher weights in terms of projective systems, it follows that

$$d_r \leq q^\delta + q^{\delta-1} + \cdots + q^{\delta-r+1}.$$

This completes the proof. □

For a more 'natural' proof of Proposition 4.2, we shall make use of a 'Structure Theorem for Close Families' that is proved in [1]. It suffices to note only the following consequence of this Structure Theorem, which is also proved in [1].

4.3. Proposition. *For $r \geq 2$, the cardinality $c_r = c_r(\ell, m)$ of the set of close families $\Lambda \subseteq I(\ell, m)$ with $|\Lambda| = r$, is given by*

$$c_r = \binom{m}{r} \left[\binom{m-r}{\ell-1} + \Delta_{2,r} \binom{m-r}{m-\ell-1} \right],$$

where $\Delta_{2,r}$ is the complement of Kronecker delta, which is 0 if $r = 2$ and 1 otherwise.

Henceforth, for $r \geq 1$, we let $c_r = c_r(\ell, m)$ be the integer defined above if $r \geq 2$ and $c_r(\ell, m) = \binom{m}{\ell}$ if $r = 1$. Note that this definition is consistent with the set theoretic description in Proposition 4.3.

4.4. Corollary. *Assume that $1 \leq \ell < m$ and $r \geq 1$. Then*

$$c_r(\ell, m) > 0 \iff r \leq \max\{\ell, m - \ell\} + 1.$$

Proof. Since $l \geq 1$, we have

$$\binom{m-r}{\ell-1} > 0 \iff \ell - 1 \leq m - r \iff r \leq m - \ell + 1.$$

In particular, since $l < m$, we have $c_2(\ell, m) > 0$. Further, since $l < m$, we have

$$\binom{m-r}{m-\ell-1} > 0 \iff m - \ell - 1 \leq m - r \iff r \leq \ell + 1.$$

So the desired result follows from Proposition 4.3 if $r \geq 2$. The case of $r = 1$ is obvious. □

Second Proof of Theorem 4.2. Suppose $1 \leq r \leq \max\{\ell, m - \ell\} + 1$. By Corollary 4.4, there exists a close family $\Lambda \subseteq I(\ell, m)$ of cardinality r. Now Proposition 3.2 implies that

$$d_r \leq q^\delta + q^{\delta-1} + \cdots + q^{\delta-r+1}.$$

The other inequality is obtained, as in the previous proof of Theorem 4.2, from the Griesmer-Wei bound. □

4.5. Corollary. *For $1 \le r \le \max\{\ell, m-\ell\}+1$, the number of r-dimensional subcodes of $C(\ell,m)$ of minimum Hamming norm is at least $c_r(\ell,m)$.*

Proof. The r-dimensional subcodes D of $C(\ell,m)$ of minimum Hamming norm, viz., $\|D\| = d_r = d_r(C(\ell,m))$, are in one-to-one correspondence with projective subspaces Π of $\mathbb{P}^{k-1}_{\mathbb{F}_q}$ of codimension r for which $|G_{\ell,m}(\mathbb{F}_q) \cap \Pi| = n - d_r$. Every close family $\Lambda \subseteq I(\ell,m)$ of cardinality r defines such a projective subspace $\Pi(\Lambda)$, and evidently, $\Pi(\Lambda) \ne \Pi(\Lambda')$ if $\Lambda' \subseteq I(\ell,m)$ is a close family of cardinality r with $\Lambda \ne \Lambda'$. Thus the desired result follows from Proposition 4.3. □

5. A Generalization of the Grassmann code

In this section, we discuss what appears to be a natural and, from the viewpoint of Algebraic Geometry, obvious generalization of Grassmann codes. This is obtained by considering the so called Schubert subvarieties of the Grassmannian. These subvarieties may be described as follows.

Fix any $\alpha = (\alpha_1, \dots, \alpha_\ell) \in I(\ell,m)$. Let $A_1 \subset \cdots \subset A_\ell$ be the canonical partial flag of subspaces of $\mathbb{F}_q^m$ associated to α, given by

$$A_i = \mathrm{span}\{e_1, \dots, e_{\alpha_i}\}, \quad \text{for} \quad i = 1, \dots, \ell$$

where $\{e_1, \dots, e_m\}$ denotes the natural basis of $\mathbb{F}_q^m$. Define the *Schubert variety* in $G_{\ell,m}(\mathbb{F}_q)$ associated to α (or more pedantically, to the above partial flag) by

$$\Omega_\alpha = \Omega_\alpha(\mathbb{F}_q) = \{W \in G_{\ell,m}(\mathbb{F}_q) : \dim(W \cap A_i) \ge i \text{ for } i = 1, \dots, \ell\}.$$

It is well-known (cf. [4], [5]) that Ω_α is a projective algebraic variety. Indeed, if we define for $\beta = (\beta_1, \dots, \beta_\ell)$ and $\beta' = (\beta'_1, \dots, \beta'_\ell)$ in $I(\ell,m)$,

$$\beta \le \beta' \iff \beta_i \le \beta'_i \quad \text{for all } i = 1, \dots, \ell,$$

then we obtain a partial order on $I(\ell,m)$, and as a consequence of the Basic Cell Lemma 3.1, it can be shown (see, for example, [5, Prop. 3]) that

$$\Omega_\alpha(\mathbb{F}_q) = \{p \in G_{\ell,m}(\mathbb{F}_q) : p_\beta = 0 \text{ for all } \beta \not\le \alpha\},$$

and moreover that for any $\beta \le \alpha$, there exists some $p \in \Omega_\alpha(\mathbb{F}_q)$ such that $p_\beta \ne 0$. In fact, the (defining) ideal $I(\Omega_\alpha)$ of Ω_α is generated by the generic Plücker coordinates p_β, for $\beta \not\le \alpha$ and certain quadratic polynomials (cf. [4] for details). It follows that the Plücker coordinates p_β, for $\beta \le \alpha$, do not satisfy any linear relation. Thus if we let

$$k_\alpha = |\{\beta \in I(\ell,m) : \beta \le \alpha\}| \quad \text{and} \quad n_\alpha = |\Omega_\alpha(\mathbb{F}_q)|$$

then $\Omega_\alpha(\mathbb{F}_q)$ gives rise to a nondegenerate $[n_\alpha, k_\alpha]_q$-projective system, via the induced Plücker embedding, and therefore, a linear $[n_\alpha, k_\alpha]_q$-code. This code may be called a *Schubert code* and denoted by $C_\alpha(\ell,m)$.

Notice that if $\alpha = (m-\ell+1, m-\ell+2, \dots, m)$, then $\beta \le \alpha$ for all $\beta \in I(\ell,m)$, and thus $\Omega_\alpha(\mathbb{F}_q) = G_{\ell,m}(\mathbb{F}_q)$. Thus in this case $C_\alpha(\ell,m)$ equals the Grassmann code $C(\ell,m)$.

The following conjecture seems plausible.

5.1. Conjecture (Ghorpade). *The minimum distance* $d_1\left(C_\alpha(\ell,m)\right)$ *of the Schubert code* $C_\alpha(\ell,m)$ *equals* q^{δ_α}, *where*

$$\delta_\alpha = \sum_{i=1}^{\ell}(\alpha_i - i) = \alpha_1 + \cdots + \alpha_\ell - \frac{\ell(\ell+1)}{2}.$$

Notice that if $\alpha = (m-\ell+1, m-\ell+2, \ldots, m)$, then $\delta_\alpha = \ell(m-\ell)$, and in this case, the conjectured equality follows from Proposition 4.1. In the general case, the following inequality can be proved as an application of the Basic Cell Lemma.

5.2. Proposition. $d_1\left(C_\alpha(\ell,m)\right) \le q^{\delta_\alpha}$.

Proof. Identify $\mathbb{P}^{k_\alpha-1}$ as a subset of $\mathbb{P}^{k-1}$ in a natural way. Let $p = p(W) \in B_\alpha \cap \Omega_\alpha(\mathbb{F}_q)$. Then we can choose a basis of W such that the corresponding $\ell\times m$ matrix $A_W = (a_{ij})$ has the property that $a_{ij} = 0$ for $j > \alpha_i$. Now if $\Phi : B_\alpha \to C_\alpha$ is as in Lemma 3.1 and $\mathbf{t} = \Phi(p)$, then using Laplace development for determinants, it is easy to see that $\mathbf{t}_{ij} = 0$ whenever $j > \alpha_i$. Conversely, if $\mathbf{t} \in C_\alpha$ has this property, then it is evident that the subspace corresponding to $p = \Psi(\mathbf{t}) \in G_{\ell,m}(\mathbb{F}_q)$ satisfies the intersection conditions defining $\Omega_\alpha(\mathbb{F}_q)$. It follows that $B_\alpha \cap \Omega_\alpha(\mathbb{F}_q)$ is in one-to-one correspondence with the set

$$\{\mathbf{t} \in C_\alpha : \mathbf{t}_{ij} = 0, \text{ for } 1 \le i \le \ell \text{ and } 1 \le j \le m \text{ with } j > \alpha_i\},$$

which is evidently in bijection with ${\mathbb{F}_q}^{\delta_\alpha}$. Consequently, for the coordinate hyperplane $H_\alpha = \{p \in \mathbb{P}^{k_\alpha-1}_{\mathbb{F}_q} : p_\alpha = 0\}$, we have $|\Omega_\alpha(\mathbb{F}_q) \cap H_\alpha| = n_\alpha - q^{\delta_\alpha}$. This proves the desired inequality. $\square$

Remarks. 1. It may be noted that unlike in the case of Grassmannians, the intersection of the Schubert variety $\Omega_\alpha(\mathbb{F}_q)$ with an arbitrary coordinate hyperplane $H_\beta = \{p \in \mathbb{P}^{k_\alpha-1}_{\mathbb{F}_q} : p_\beta = 0\}$ is not the complement of an affine space unless $\beta = \alpha$. Indeed, this intersection is the complement of a 'determinantal variety' if $\beta \le \alpha$, and it is $\Omega_\alpha(\mathbb{F}_q)$ if $\beta \not\le \alpha$. For some details concerning this, one may refer to [6].

2. The Grassmann variety $G_{\ell,m}$ admits a natural generalization to homogeneous varieties of the form G/P, where G is a nice (say, semisimple) algebraic group and P a maximal parabolic (or more generally, any parabolic) subgroup. Moreover, Schubert subvarieties can also be defined in this general context as the Zariski closures of the corresponding Schubert cells, and these are indexed by the quotients W/W_P of the Weyl group of G by the Weyl group of P. This would of course lead to a further generalization of the Grassmann code.

3. However, before proceeding with further generalizations as indicated above, it may be worthwhile to note that already in the classical case which we have considered here, the Schubert code $C_\alpha(\ell,m)$ is far from well understood. For example, even the basic parameters n_α and k_α are not so easy to describe explicitly, not to mention the entire weight hierarchy. Recently, M. Tsfasman and the first author have looked at these and other related problems, and are able to answer some of them. The details may appear elsewhere.

4. Professor Hao Chen, who came across a preliminary version of this paper, has recently informed us that he is able to prove Conjecture 5.1 for Schubert codes in $G_{2,m}(\mathbb{F}_q)$, that is, in the case of $\ell = 2$.

References

[1] Ghorpade, S. R., Lachaud, G.: Hyperplane sections of Grassmannians and the number of MDS linear codes. Finite Fields Appl. **7** (2001), 468–506.

[2] Goldman, J., Rota, G.-C.: The number of subspaces of a vector space. In: "Recent Progress in Combinatorics" (W. T. Tutte Ed.), pp. 75–84, Academic Press, New York, 1969.

[3] Hirschfeld, J. W. P., Tsfasman, M. A., Vlăduţ, S. G.: The weight hierarchy of higher-dimensional Hermitian codes. IEEE Trans. Inform. Theory **40** (1994) 275–278.

[4] Hodge, W. V. D., Pedoe, D.: "Methods of Algebraic Geometry", Vol. II, Cambridge Univ. Press, Cambridge, 1952.

[5] Kleiman, S. L., Laksov, D.: Schubert Calculus. Amer. Math. Monthly **79** (1972) 1061–1082.

[6] Musili, C.: Applications of standard monomial theory. In: "Proceedings of the Hyderabad Conference on Algebraic Groups", (S. Ramanan, Ed.), pp. 381–406, Manoj Prakashan, Madras (Distributed outside India by the American Math. Society, Providence), 1991.

[7] Nogin, D. Yu.: Codes associated to Grassmannians. In: "Arithmetic, Geometry and Coding theory" (R. Pellikan, M. Perret, S. G. Vlăduţ, Eds.), pp. 145–154, Walter de Gruyter, Berlin/New York, 1996.

[8] Ryan, C. T.: An application of Grassmannian varieties to coding theory. Congr. Numer. **57** (1987) 257–271.

[9] Ryan, C. T. Projective codes based on Grassmann varieties. *Congr. Numer.* **57** (1987) 273–279.

[10] Ryan, C. T.: The weight distribution of a code associated to intersection properties of the Grassmannian variety $G(3,6)$. *Congr. Numer.* **61** (1988) 183–198.

[11] Ryan, C. T., Ryan, K. M.: An application of geometry to the calculation of weight enumerators. *Congr. Numer.* **67** (1988) 77–90.

[12] Ryan, C. T., Ryan, K. M.: The minimum weight of the Grassmann codes $C(k,n)$. Discrete Appl. Math. **28** (1990) 149–156.

[13] Tsfasman M. A., Vlăduţ, S. G.: "Algebraic Geometric Codes", Kluwer, Amsterdam, 1991.

[14] Tsfasman, M. A., Vlăduţ, S. G.: Geometric approach to higher weights. IEEE Trans. Inform. Theory **41** (1995) 1564–1588.

[15] Wei, V. K.: Generalized Hamming weights for linear codes. IEEE Trans. Inform. Theory **37** (1991) 1412–1418.

Department of Mathematics
Indian Institute of Technology Bombay
Powai, Mumbai 400076, India
E-mail address: srg@math.iitb.ac.in
URL: http://www.math.iitb.ac.in/~srg

Équipe "Arithmétique et Théorie de l'Information"
Institut de Mathématiques de Luminy
Luminy Case 907, 13288 Marseille, Cedex 9, France
E-mail address: lachaud@iml.univ-mrs.fr
URL: http://iml.univ-mrs.fr:80/ati/