Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Finite Fields and Their Applications 11 (2005) 684–699
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Schubert varieties, linear codes and enumerative combinatorics

Sudhir R. Ghorpade[a,*,1], Michael A. Tsfasman[b,c,d,2]

[a] *Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India*
[b] *Institut de Mathématiques de Luminy, Case 907, 13288 Marseille, France*
[c] *Independent University of Moscow, Russia*
[d] *Dorbushin Math. Lab., Institute for Information Transmission Problems, Moscow, Russia*

Received 26 May 2003; revised 5 July 2004

Communicated by Oscar Moreno

Available online 3 October 2005

Abstract

We consider linear error correcting codes associated to higher-dimensional projective varieties defined over a finite field. The problem of determining the basic parameters of such codes often leads to some interesting and difficult questions in combinatorics and algebraic geometry. This is illustrated by codes associated to Schubert varieties in Grassmannians, called Schubert codes, which have recently been studied. The basic parameters such as the length, dimension and minimum distance of these codes are known only in special cases. An upper bound for the minimum distance is known and it is conjectured that this bound is achieved. We give explicit formulae for the length and dimension of arbitrary Schubert codes and prove the minimum distance conjecture in the affirmative for codes associated to Schubert divisors.

Keywords: Grassmannian; Linear codes; Minimum distance; Projective system; Schubert variety

[*] Corresponding author. Fax: +91 222 5723480.
E-mail addresses: srg@math.iitb.ac.in (S.R. Ghorpade), tsfasman@iml.univ-mrs.fr (M.A. Tsfasman).

[1] Partially supported by a 'Career Award' grant from AICTE, New Delhi and an IRCC grant from IIT Bombay.

[2] Partially supported by the RFBR Grants 99-01-01204, 02-01-01041 and 02-01-22005.

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2004.09.002

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements, and let n, k be integers with $1 \leqslant k \leqslant n$. The n-dimensional vector space $\mathbb{F}_q^n$ has a norm, called *Hamming norm*, which is defined by

$$\|x\| = |\{i \in \{1, \ldots, n\} : x_i \neq 0\}| \quad \text{for } x \in \mathbb{F}_q^n.$$

More generally, if D is a subspace of $\mathbb{F}_q^n$, the *Hamming norm of D* is defined by

$$\|D\| = |\{i \in \{1, \ldots, n\} : \text{ there exists } x \in D \text{ with } x_i \neq 0\}|.$$

A *linear $[n, k]_q$-code* is, by definition, a k-dimensional subspace of $\mathbb{F}_q^n$. The adjective *linear* will often be dropped since in this paper we only consider linear codes. The parameters n and k are referred to as the *length* and the *dimension* of the corresponding code. If C is an $[n, k]_q$-code, then the *minimum distance $d = d(C)$* of C is defined by

$$d(C) = \min\{\|x\| : x \in C, \ x \neq 0\}.$$

More generally, given any positive integer r, the *rth higher weight $d_r = d_r(C)$* of C is defined by

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

Note that $d_1(C) = d(C)$.

An $[n, k]_q$-code is said to be *nondegenerate* if it is not contained in a coordinate hyperplane of $\mathbb{F}_q^n$. Two $[n, k]_q$-codes are said to be *equivalent* if one can be obtained from another by permuting coordinates and multiplying them by nonzero elements of $\mathbb{F}_q$; in other words, if they are in the same orbit for the natural action of the semidirect product of $(\mathbb{F}_q^*)^n$ and S_n. It is clear that this gives a natural equivalence relation on the set of $[n, k]_q$-codes.

An alternative way to describe codes is via the language of projective systems introduced in [18]. A *projective system* is a (multi)set X of n points in the projective space $\mathbb{P}^{k-1}$ over $\mathbb{F}_q$. We call X *nondegenerate* if these n points are not contained in a hyperplane of $\mathbb{P}^{k-1}$. Two projective systems in $\mathbb{P}^{k-1}$ are said to be *equivalent* if there is a projective automorphism of the ambient space $\mathbb{P}^{k-1}$, which maps one to the other; in other words, if they are in the same orbit for the natural action of $PGL(k, \mathbb{F}_q)$. It is clear that this gives a natural equivalence relation on the set of projective systems of n points in $\mathbb{P}^{k-1}$.

It turns out that a nondegenerate projective system of n points in $\mathbb{P}^{k-1}$ corresponds naturally to a nondegenerate linear $[n, k]_q$-code. Moreover, if we pass to equivalence classes with respect to the equivalence relations defined above, then this correspondence is one-to-one. The minimum distance of the code $C = C_X$ associated to a nondegenerate projective system X of n points in $\mathbb{P}^{k-1}$ admits a nice geometric interpretation in terms of X, namely,

$$d(C_X) = n - \max\left\{|X \cap H| : H \text{ a hyperplane of } \mathbb{P}^{k-1}\right\}.$$

We have a similar interpretation for the rth higher weight $d_r(C_X)$, where the hyperplane H is replaced by a projective subspace of codimension r in $\mathbb{P}^{k-1}$. For more details concerning projective systems, higher weights and a proof of the above mentioned one-to-one correspondence, we refer to [18,19].

The language of projective systems not only explains the close connection between algebraic geometry and coding theory, but also facilitates the introduction of linear codes corresponding to projective algebraic varieties defined over a finite field. A case in point is the Grassmannian $G_{\ell,m} = G_\ell(V)$ of ℓ-dimensional subspaces of an m-dimensional vector space V over $\mathbb{F}_q$. We have the well-known Plücker embedding of the Grassmannian into a projective space (cf. [3,9]), and this embedding is known to be nondegenerate. Considering the ($\mathbb{F}_q$-rational) points of $G_{\ell,m}$ as a projective system, we obtain a q-ary linear code, called the *Grassmann code*, which we denote by $C(\ell, m)$. These codes were first studied by Ryan [14–16] in the binary case and by Nogin [12] in the q-ary case. It is clear that the length n and the dimension k of $C(\ell, m)$ are given by

$$n = \begin{bmatrix} m \\ \ell \end{bmatrix}_q := \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{\ell-1})}{(q^\ell-1)(q^\ell-q)\cdots(q^\ell-q^{\ell-1})} \quad \text{and} \quad k = \binom{m}{\ell}. \tag{1}$$

The minimum distance of $C(\ell, m)$ is given by the following elegant formula due to Nogin [12]:

$$d\left(C(\ell, m)\right) = q^\delta, \quad \text{where} \quad \delta := \ell(m-\ell). \tag{2}$$

In fact, Nogin [12] also determined some of the higher weights of $C(\ell, m)$. More precisely, he showed that for $1 \leqslant r \leqslant \max\{\ell, m-\ell\} + 1$,

$$d_r\left(C(\ell, m)\right) = q^\delta + q^{\delta-1} + \cdots + q^{\delta-r+1}. \tag{3}$$

Alternative proofs of (3) were given in [3], and in the same paper a generalization to Schubert codes was proposed. The Schubert codes are indexed by the elements of the set

$$I(\ell, m) := \{\alpha = (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{Z}^\ell : 1 \leqslant \alpha_1 < \cdots < \alpha_\ell \leqslant m\}.$$

Given any $\alpha \in I(\ell, m)$, the corresponding *Schubert code* is denoted by $C_\alpha(\ell, m)$, and it is the code obtained from the projective system defined by the Schubert variety Ω_α

in $G_{\ell,m}$ with a nondegenerate embedding induced by the Plücker embedding. Recall that Ω_α can be defined by

$$\Omega_\alpha = \{W \in G_{\ell,m} : \dim(W \cap A_{\alpha_i}) \geqslant i \text{ for } i = 1, \ldots, \ell\},$$

where A_j denotes the span of the first j vectors in a fixed basis of V, for $1 \leqslant j \leqslant m$. It was observed in [3] that the length n_α and the dimension k_α of $C_\alpha(\ell, m)$ are abstractly given by

$$n_\alpha = |\Omega_\alpha(\mathbb{F}_q)| \quad \text{and} \quad k_\alpha = |\{\beta \in I(\ell, m) : \beta \leqslant \alpha\}|, \tag{4}$$

where for $\beta = (\beta_1, \ldots, \beta_\ell) \in I(\ell, m)$, by $\beta \leqslant \alpha$ we mean that $\beta_i \leqslant \alpha_i$ for $i = 1, \ldots, \ell$. It was shown in [3] that the minimum distance of $C_\alpha(\ell, m)$ satisfies the inequality

$$d(C_\alpha(\ell, m)) \leqslant q^{\delta_\alpha}, \quad \text{where} \quad \delta_\alpha := \sum_{i=1}^{\ell} (\alpha_i - i) = \alpha_1 + \cdots + \alpha_\ell - \frac{\ell(\ell+1)}{2}.$$

Further, it was conjectured by the first author that, in fact, the equality holds, i.e.,

$$d(C_\alpha(\ell, m)) = q^{\delta_\alpha}. \tag{5}$$

We shall refer to (5) as the *minimum distance conjecture* (for Schubert codes). Note that if $\alpha = (m - \ell + 1, \ldots, m - 1, m)$, then $\Omega_\alpha = G_{\ell,m}$ and so in this case (5) is an immediate consequence of (2).

The minimum distance conjecture has been proved in the affirmative by Chen [1] when $\ell = 2$. In fact, he proves the following. If $\ell = 2$ and $\alpha = (m - h - 1, m)$ [we can assume that α is of this form without any loss of generality], then $d(C_\alpha(2, m)) = q^{\delta_\alpha} = q^{2m-h-4}$, and moreover,

$$n_\alpha = \frac{(q^m - 1)(q^{m-1} - 1)}{(q^2 - 1)(q - 1)} - \sum_{j=1}^{h} \sum_{i=1}^{j} q^{2m-j-2-i}, \text{ and} \tag{6}$$

$$k_\alpha = \frac{m(m-1)}{2} - \frac{h(h+1)}{2}. \tag{7}$$

An alternative proof of the minimum distance conjecture, as well as the weight distribution of codewords in the case $\ell = 2$, was obtained independently by Guerra and Vincenti [7]; in the same paper, they prove also the following lower bound for $d(C_\alpha(\ell, m))$ in the general case:

$$d(C_\alpha(\ell, m)) \geqslant \frac{q^{\alpha_1}(q^{\alpha_2} - q^{\alpha_1}) \cdots (q^{\alpha_\ell} - q^{\alpha_{\ell-1}})}{q^{1+2+\cdots+\ell}} \geqslant q^{\delta_\alpha - \ell}. \tag{8}$$

In an earlier paper, Vincenti [20], partly in collaboration with Guerra, verified the minimum distance conjecture for the unique nontrivial Schubert variety in the Klein quadric $G_{2,4}$, namely $\Omega_{(2,4)}$, and obtained a lower bound which is weaker than (8), and also proved the following formula [3] for the length of $C_\alpha(\ell, m)$.

$$n_\alpha = |\Omega_\alpha(\mathbb{F}_q)| = \sum_{(k_1,\ldots,k_{\ell-1})} \prod_{i=0}^{\ell-1} \begin{bmatrix} \alpha_{i+1} - \alpha_i \\ k_{i+1} - k_i \end{bmatrix}_q q^{(\alpha_i - k_i)(k_{i+1} - k_i)}, \tag{9}$$

where the sum is over all $(\ell-1)$-tuples $(k_1, \ldots, k_{\ell-1})$ of integers with $i \leqslant k_i \leqslant \alpha_i$ and $k_i \leqslant k_{i+1}$ for $1 \leqslant i \leqslant \ell - 1$, and where, by convention, $\alpha_0 = 0 = k_0$ and $k_\ell = \ell$.

We can now describe the contents of this paper. In Section 2 below, we give two formulae for the length n_α of $C_\alpha(\ell, m)$. Of these, the first is very simple and is related to a classical result about the Grassmannians. The other formula is somewhat similar to (9) even though it was obtained independently. The latter formula may be a little more effective in actual computations. Next, in Section 3, we give a determinantal formula for the dimension k_α of $C_\alpha(\ell, m)$ and show that in certain cases this determinant can be evaluated. Moreover, we also give an alternative formula for k_α using the formulae for n_α obtained in the previous section. Finally, in Section 4, we show that the minimum distance and some of the higher weights for the codes corresponding to Schubert divisors, i.e., Schubert varieties of codimension one in the corresponding Grassmannians, can be easily obtained using the results of [3,12]. This shows, in particular, that the minimum distance conjecture is true for all Schubert divisors such as, for instance, the unique nontrivial Schubert variety in the Klein quadric.

As a byproduct of the results in this paper, we see that n_α can be expressed in three distinct ways and k_α in two. This yields curious combinatorial identities, which may not be easy to prove directly.

Some of the main results of this paper, namely, Theorems 4, 7 and 9, were presented during a talk by the first author at the Conference on Arithmetic, Geometry and Coding Theory (AGCT-8) held at CIRM, Luminy in May 2001. The article [6], written for FPSAC-2003, gives an overview (without proofs) of the results in this paper, and it may be referred to for a more leisurely introduction to this paper.

We end this introduction with the following comment. The Grassmannian is a special instance of homogeneous spaces of the form G/P where G is a semisimple algebraic group and P a parabolic subgroup. Moreover, Schubert varieties also admit a generalization in this context. Thus it was indicated in [3] that the Grassmann and Schubert codes can also be introduced in a much more general setting. It turns out, in fact, that the construction of such general codes was already proposed in the binary case by Wolper in an unpublished paper [21]. The general case, however, needs to be better understood and can be a source of numerous interesting problems.

[3] In fact, in [7,20], the Grassmannian and its Schubert subvarieties are viewed as families of projective subspaces of a projective space rather than linear subspaces of a vector space. The two viewpoints are, of course, equivalent. To get (9) from [20, Proposition 15], one has to set $\ell = d + 1$, $\alpha_i = a_{i-1} + 1$ and $k_i = \ell_{i-1} + 1$ for $1 \leqslant i \leqslant \ell$. A similar substitution has to be made to get (8) from [7, Theorem 1.1].

2. Length of Schubert codes

Fix integers ℓ, m with $1 \leqslant \ell \leqslant m$. Let $I(\ell, m)$ be the indexing set with the partial order $\leqslant$ defined in the previous section. For $\beta = (\beta_1, \ldots, \beta_\ell) \in I(\ell, m)$, let

$$\delta_\beta := \sum_{i=1}^{\ell} (\beta_i - i) = \beta_1 + \cdots + \beta_\ell - \frac{\ell(\ell+1)}{2}.$$

Finally, fix some $\alpha \in I(\ell, m)$ and let $C_\alpha(\ell, m)$ be the corresponding Schubert code.

Quite possibly, the simplest formula for the length n_α of $C_\alpha(\ell, m)$ is the one given in the theorem below. This formula is an easy consequence of the well-known cellular decomposition of the Grassmannian, which goes back to Ehresmann [2]. However, it does not seem easy to locate this formula in the literature, and thus, for the sake of completeness, we include here a sketch of the proof.

Theorem 1. *The length n_α of $C_\alpha(\ell, m)$ or, in other words, the number of $\mathbb{F}_q$-rational points of Ω_α, is given by*

$$n_\alpha = \sum_{\beta \leqslant \alpha} q^{\delta_\beta}, \tag{10}$$

where the sum is taken over all $\beta \in I(\ell, m)$ satisfying $\beta \leqslant \alpha$.

Proof. Consider, as in the previous section, the subspaces A_j spanned by the first j basis vectors, for $1 \leqslant j \leqslant m$. Given any $W \in G_{\ell,m}$, the numbers $r_j = \dim W \cap A_j$ have the property[4] that $0 \leqslant r_j - r_{j-1} \leqslant 1$ (where $r_0 = 0$, by convention), and, since $r_m = \ell$, there are exactly ℓ indices where this difference is 1. Thus there is a unique $\beta \in I(\ell, m)$ such that W is in

$$C_\beta := \left\{ L \in G_{\ell,m} : \dim(L \cap A_{\beta_j}) = j \text{ and } \dim(L \cap A_{\beta_j - 1}) = j - 1 \text{ for } 1 \leqslant j \leqslant \ell \right\}.$$

Moreover, for any $L \in C_\beta$, we have: $L \in \Omega_\alpha \Leftrightarrow \beta \leqslant \alpha$. It follows that Ω_α is the disjoint union of C_β as β varies over the elements of $I(\ell, m)$ satisfying $\beta \leqslant \alpha$. Now it suffices to observe that the subspaces in C_β are in natural one-to-one correspondence with $\ell \times m$ matrices (over $\mathbb{F}_q$) with 1 in the (i, β_i)th spot, and zeros to its right as well as below, for $1 \leqslant i \leqslant \ell$. □

It may be argued that even though formula (10) is simple and elegant, it may not be very effective in practice in view of the rather intricate summation involved. For example, if Ω_α is the full Grassmannian $G_{\ell,m}$, then (10) involves $\binom{m}{\ell}$ summands, while

[4] This follows, for example, because the kernel of the map $W \cap A_j \to \mathbb{F}_q$, mapping a vector to its jth coordinate (with respect to the fixed basis of V), is $W \cap A_{j-1}$.

the closed form formula in (1) given by the Gaussian binomial coefficient may be deemed preferable. For an arbitrary $\alpha \in I(\ell, m)$, it is not easy to estimate the number of summands in (10), as may be clear from the results of Section 3. With this in view, we shall now describe another formula for n_α, which is far from being elegant but may also be of some interest. First, we need an elementary definition and a couple of preliminary lemmas.

By a *consecutive block* in an ℓ-tuple $\beta = (\beta_1, \dots, \beta_\ell) \in I(\ell, m)$, we mean an ordered sequence of the form $\beta_i, \dots, \beta_j$ where $1 \leqslant i \leqslant j \leqslant \ell$ and $\beta_{p+1} = \beta_p + 1$ for $i \leqslant p < j$. For example, 3, 4 is a consecutive block in (1, 3, 4, 7) as well as in (1, 3, 4, 5) and in (2, 3, 4, 5). Note that any $\beta \in I(\ell, m)$ always has ℓ consecutive blocks although it may often be regarded as having fewer consecutive blocks.

Lemma 2. *Suppose $\alpha = (\alpha_1, \dots, \alpha_\ell)$ has $u+1$ consecutive blocks*:

$$\alpha = (\alpha_1, \dots, \alpha_{p_1},\ \alpha_{p_1+1}, \dots, \alpha_{p_2},\ \dots,\ \alpha_{p_{u-1}+1}, \dots, \alpha_{p_u},\ \alpha_{p_u+1}, \dots, \alpha_\ell)$$

so that $1 \leqslant p_1 < \cdots < p_u < \ell$ and $\alpha_{p_i+1}, \dots, \alpha_{p_{i+1}}$ are consecutive for $0 \leqslant i \leqslant u$, where by convention, $p_0 = 0$ and $p_{u+1} = \ell$. Then

$$\Omega_\alpha = \{W \in G_{\ell,\alpha_\ell} : \dim(W \cap A_{\alpha_{p_i}}) \geqslant p_i \text{ for } i = 1, \dots, u\}.$$

Proof. As in the proof of Theorem 1, for any $W \in G_{\ell,\alpha_\ell}$, we have $\dim(W \cap A_{j-1}) \geqslant \dim(W \cap A_j) - 1$ for $1 \leqslant j \leqslant m$. Also, $\dim(W \cap A_{\alpha_\ell}) \geqslant \ell$ if and only if W is a subspace of A_{α_ℓ}. The desired result is now clear. □

Given any integers a, b, s, t, we define

$$\lambda(a, b; s, t) = \sum_{r=s}^{t} (-1)^{r-s} q^{\binom{r-s}{2}} \begin{bmatrix} a-s \\ r-s \end{bmatrix}_q \begin{bmatrix} b-r \\ t-r \end{bmatrix}_q .$$

Here, for any $u, v \in \mathbb{Z}$, the Gaussian binomial coefficient $\left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right]_q$ is defined as in (1) when $0 \leqslant v \leqslant u$, and 0 otherwise. Thus, if $a = s = 0$, then $\lambda(a, b; s, t) = \left[\begin{smallmatrix} b \\ t \end{smallmatrix}\right]_q$.

Lemma 3. *Let B be a b-dimensional vector space over $\mathbb{F}_q$ and $G_{t,b} = G_t(B)$ denote the Grassmannian of t-dimensional subspaces of B. Now suppose A is any subspace of B and S is any subspace of A, and we let $a = \dim A$ and $s = \dim S$. Then*

$$|\{T \in G_t(B) : T \cap A = S\}| = \lambda(a, b; s, t).$$

Proof. Let $\mathcal{L}_A$ be the poset of all subspaces of A with the partial order given by inclusion. Define functions $f, g : \mathcal{L}_A \to \mathbb{N}$ by

$$f(S) = |\{T \in G_t(B) : T \cap A = S\}| \quad \text{and} \quad g(S) = |\{T \in G_t(B) : T \cap A \supseteq S\}|.$$

It is clear that for any $S \in \mathcal{L}_A$ with dim $S = s$, we have

$$g(S) = \sum_{\substack{R \in \mathcal{L}_A \\ R \supseteq S}} f(R).$$

On the other hand, for any S as above, we clearly have

$$g(S) = |\{T \in G_t(B) : T \supseteq S\}| = |G_{t-s}(B/S)| = \begin{bmatrix} b-s \\ t-s \end{bmatrix}_q. \tag{11}$$

Hence, by Möbius inversion applied to the poset $\mathcal{L}_A$ and the well-known formula for the Möbius function of $\mathcal{L}_A$ (cf. [17, Chapter 3]), we obtain

$$f(S) = \sum_{\substack{R \in \mathcal{L}_A \\ R \supseteq S}} \mu(S, R) g(R) = \sum_{\substack{R \in \mathcal{L}_A \\ R \supseteq S}} (-1)^{\dim R - \dim S} q^{\binom{\dim R - \dim S}{2}} \begin{bmatrix} b-r \\ t-r \end{bmatrix}_q.$$

Since the terms in the last summation depend only on the dimension of the varying subspace R, we may write it as

$$\sum_{r=s}^{a} |\{R \in \mathcal{L}_A : R \supseteq S \text{ and } \dim R = r\}| (-1)^{r-s} q^{\binom{r-s}{2}} \begin{bmatrix} b-r \\ t-r \end{bmatrix}_q.$$

As in (11), the cardinality of the set appearing in the above summand is readily seen to be $\left[\begin{smallmatrix} a-s \\ r-s \end{smallmatrix}\right]_q$. This yields the desired equality. □

Theorem 4. *Let u and $p_1, \ldots, p_u$ be as in Lemma 2. Then the length n_α of the Schubert code $C_\alpha(\ell, m)$ is given by*

$$n_\alpha = \sum_{s_1=p_1}^{\alpha_{p_1}} \sum_{s_2=p_2}^{\alpha_{p_2}} \cdots \sum_{s_u=p_u}^{\alpha_{p_u}} \prod_{i=0}^{u} \lambda(\alpha_{p_i}, \alpha_{p_{i+1}}; s_i, s_{i+1}) \tag{12}$$

where, by convention, $s_0 = p_0 = 0$ and $s_{u+1} = p_{u+1} = \ell$.

Proof. We use induction on u. If $u = 0$, i.e., if $\alpha_1, \ldots, \alpha_\ell$ are consecutive, then $\Omega_\alpha = G_{\ell,\alpha_\ell}$, and so we know that $n_\alpha = \left[\begin{smallmatrix} \alpha_\ell \\ \ell \end{smallmatrix}\right]_q = \lambda(0, \alpha_\ell; 0, \ell)$. Now suppose that $u \geqslant 1$ and the result holds for all smaller values of u. Then, by Lemma 2, we see that

$$\Omega_\alpha = \coprod_S \{T \in G_{\ell,\alpha_\ell} : T \cap A_{\alpha_{p_u}} = S\},$$

where the disjoint union is taken over the set, say Λ_u, of all subspaces S of $A_{\alpha_{p_u}}$ satisfying $\dim S \geqslant u$ and $\dim S \cap A_{\alpha_{p_i}} \geqslant p_i$ for $1 \leqslant i \leqslant u-1$. Hence, by Lemma 3,

$$n_\alpha = |\Omega_\alpha(\mathbb{F}_q)| = \sum_{s=p_u}^{\alpha_{p_u}} |\{S \in \Lambda_u : \dim\ S = s\}| \lambda(\alpha_{p_u}, \alpha_\ell; s, \ell).$$

But for any s with $p_u \leqslant s \leqslant \alpha_{p_u}$, the set of s-dimensional subspaces in Λ_u is precisely the Schubert variety in $G_{s,\alpha_{p_u}}$ corresponding to the tuple $(\alpha_1, \ldots, \alpha_{p_u})$ with u consecutive blocks. Hence the induction hypothesis applies. □

Remark 5. In the case $\ell = 2$, we obviously have $u \leqslant 1$, and the formula given above becomes somewhat simpler. It is not difficult to verify that this agrees with the formula (6) of Chen [1].

Remark 6. As a consequence of the results in this section, we obtain a purely combinatorial identity which equates the right-hand sides of (9), (10) and (12). It would be an intriguing problem to prove this without invoking Schubert varieties.

3. Dimension of Schubert codes

Let the notation be as in the beginning of the previous section. Our aim is to give an explicit formula for the dimension k_α of the Schubert code $C_\alpha(\ell, m)$. As in the case of Theorem 1, it suffices to appeal to another classical fact about Schubert varieties in Grassmannians, namely, the postulation formula due to Hodge [8]. For our purpose, we use a slightly simpler description of Hodge's formula, which (together with an alternative proof) is given in [5].

Theorem 7. *The dimension k_α of the Schubert code $C_\alpha(\ell, m)$ equals the determinant of the $\ell \times \ell$ matrix whose (i, j)th entry is $\binom{\alpha_j - j + 1}{i - j + 1}$, i.e.,*

$$k_\alpha = \begin{vmatrix} \binom{\alpha_1}{1} & 1 & 0 & \ldots & 0 \\ \binom{\alpha_1}{2} & \binom{\alpha_2 - 1}{1} & 1 & \ldots & 0 \\ \vdots & & & & \vdots \\ \binom{\alpha_1}{\ell} & \binom{\alpha_2 - 1}{\ell - 1} & \binom{\alpha_3 - 2}{\ell - 2} & \ldots & \binom{\alpha_\ell - \ell + 1}{1} \end{vmatrix}. \tag{13}$$

Proof. Recall the abstract description in (4) for the dimension k_α of $C_\alpha(\ell, m)$:

$$k_\alpha = |\{\beta \in I(\ell, m) : \beta \leqslant \alpha\}|.$$

By Hodge Basis Theorem (cf. [5, Theorem 1]), we know that a vector space basis for the tth component, say R_t, of the homogeneous coordinate ring of Ω_α is indexed by the t-tuples $(\beta^{(1)}, \ldots, \beta^{(t)})$ of elements of $I(\ell, m)$ satisfying $\beta^{(1)} \leqslant \cdots \leqslant \beta^{(t)} \leqslant \alpha$. The postulation formula of Hodge gives the Hilbert function $h(t) = \dim R_t$ ($t \in \mathbb{N}$) of this ring. Now, using [5, Lemma 7], we may write

$$h(t) = \det_{1 \leqslant i,j \leqslant \ell} \left(\binom{t + \alpha_j - j}{t + i - j} \right) \qquad \text{for } t \in \mathbb{N}.$$

By putting $t = 1$, we get the desired result. □

Remark 8. In the case $\ell = 2$, we obviously have

$$k_\alpha = \alpha_1(\alpha_2 - 1) - \binom{\alpha_1}{2} = \frac{\alpha_1(2\alpha_2 - \alpha_1 - 1)}{2}$$

and if we write $\alpha = (m - h - 1, m)$, then we retrieve the formula (7) of Chen [1].

The determinant in (13) is not easy to evaluate in general. For example, none of the recipes in the rather comprehensive compendium of Krattenthaler [10] seem to be applicable. The following Proposition shows, however, that in a special case a simpler formula can be obtained.

Theorem 9. *Suppose $\alpha_1, \ldots, \alpha_\ell$ are in an arithmetic progression, i.e., there are $c, d \in \mathbb{Z}$ such that $\alpha_i = c(i-1) + d$ for $i = 1, \ldots, \ell$. Let $\alpha_{\ell+1} = c\ell + d = \ell\alpha_2 + (1-\ell)\alpha_1$. Then*

$$k_\alpha = \frac{\alpha_1}{\ell!} \prod_{i=1}^{\ell-1} (\alpha_{\ell+1} - i) = \frac{\alpha_1}{\alpha_{\ell+1}} \binom{\alpha_{\ell+1}}{\ell}.$$

Proof. If $\alpha_i = c(i-1) + d$ for $i = 1, \ldots, \ell$, then the (i, j)th entry of the transpose of the $\ell \times \ell$ matrix in (13) can be written as

$$\binom{c(i-1) + d - i + 1}{j - i + 1} = \binom{BL_i + A}{L_i + j}, \quad \text{where } B = 1 - c, \;\; L_i = 1 - i \text{ and } A = d.$$

Now we use formula (3.13) in [10, Theorem 26], which says that for an $\ell \times \ell$ matrix whose (i, j)th entry of the form $\binom{BL_i + A}{L_i + j}$ [where A, B can be indeterminates and the L_i's are integers], the determinant is given by

$$\frac{\prod_{1 \leqslant i < j \leqslant \ell} (L_i - L_j)}{\prod_{i=1}^{\ell} (L_i + \ell)!} \prod_{i=1}^{\ell} \frac{(BL_i + A)!}{((B-1)L_i + A - 1)!} \prod_{i=1}^{\ell} (A - Bi + 1)_{i-1},$$

where in the last product we used the shifted factorial notation, viz., $(a)_0 = 1$ and $(a)_t = a(a+1)\cdots(a+t-1)$, for $t \geqslant 1$. Substituting $B = 1-c$, $L_i = 1-i$ and $A = d$ and making elementary simplifications, we obtain the desired formula. □

Remark 10. The simplest case, where the above proposition is applicable is when $\alpha_1, \ldots, \alpha_\ell$ are consecutive, i.e., $c = 1$ and $\alpha_i = d + i - 1$. Notice that in this case, the formula for k_α reduces to $\binom{d+\ell-1}{\ell}$. Of course, this is not surprising since Ω_α is nothing but the smaller Grassmannian $G_{\ell,d+\ell-1}$ in this case. Thus, in this case we also have simpler formulae for n_α and δ_α and the minimum distance conjecture is true. However, even in this simplest case, the evaluation of the determinant in (13) does not seem obvious. Indeed, here it becomes an instance of the Ostrowski determinant $\det\left(\binom{d}{k_i - j}\right)$ if we take $k_i = i + 1$. A formula for such a determinant and the result that it is positive for increasing $\{k_i\}$ was obtained by Ostrowski [13] in 1964. The case when $\{k_i\}$ are consecutive seems to go back to Zeipel in 1865 (cf. [11, Vol. 3, pp. 448–454]).

An alternative formula for the dimension k_α of $C_\alpha(\ell, m)$ can be derived using results of the previous section. To this end, we begin by observing that the dimension k of the q-ary Grassmann code $C(\ell, m)$ does not depend on q, and bears the following relation to the length $n = n(q)$ of $C(\ell, m)$:

$$\lim_{q\to 1} n(q) = k \quad \text{or, in other words,} \quad \lim_{q\to 1} \begin{bmatrix} m \\ \ell \end{bmatrix}_q = \binom{m}{\ell}. \tag{14}$$

Much has been written on this limiting formula in combinatorics literature. For example, a colourful, albeit mathematically incorrect, way to state it would be to say that the (lattice of) subsets of an m-set is the same as the (lattice of) subspaces of an m-dimensional vector space over the field of one element! In the proposition below, we observe that a similar relation holds in the case of Schubert codes, and, then, use this relation to obtain the said alternative formula for k_α.

Proposition 11. *The dimension k_α of the q-ary Schubert code $C_\alpha(\ell, m)$ is independent of q and is related to the length $n_\alpha = n_\alpha(q)$ of $C_\alpha(\ell, m)$ by the formula*

$$\lim_{q\to 1} n_\alpha(q) = k_\alpha. \tag{15}$$

Consequently, if u and $p_1, \ldots, p_u$ be are as in Lemma 2, then

$$k_\alpha = \sum_{s_1=p_1}^{\alpha_{p_1}} \sum_{s_2=p_2}^{\alpha_{p_2}} \cdots \sum_{s_u=p_u}^{\alpha_{p_u}} \prod_{i=0}^{u} \binom{\alpha_{p_{i+1}} - \alpha_{p_i}}{s_{i+1} - s_i}, \tag{16}$$

where, by convention, $s_0 = p_0 = 0$ and $s_{u+1} = p_{u+1} = \ell$.

Proof. The limiting formula (15) follows from the abstract description in (4) of k_α and Theorem 1. Further, (16) will follow from Theorem 4 if we show that for any integer parameters $a, b, s, t,$ we have

$$\lim_{q\to 1} \lambda(a, b; s, t) = \binom{b-a}{t-s}.$$

But, in view of (14), this is equivalent to proving the binomial identity

$$\sum_{j\geqslant 0}(-1)^j\binom{a-s}{j}\binom{b-s-j}{t-s-j} = \binom{b-a}{t-s}.$$

This identity is trivial if $t < s$, and if $t \geqslant s$, it follows easily if, after expanding by the binomial theorem, we compare the coefficients of X^{t-s} in the identity

$$(1-X)^{a-s}(1-X)^{t-b-1} = (1-X)^{a-b+t-s-1}$$

and observe that for any integers M and N, we have $\binom{-N-1}{M} = (-1)^M\binom{N+M}{M}$. □

Remark 12. As a consequence of the results in this section, we obtain a purely combinatorial identity which equates the right-hand sides of (13) and (16). It would be an intriguing problem to prove this without invoking Schubert codes.

While one would like to construct codes having both the *rate* k/n and the *relative distance* d/n as close to 1 as possible, the two requirements are in conflict with each other. For Schubert codes, this conflict manifests itself in a peculiar way:

Corollary 13. *Let $R = R(q)$ and $\Delta = \Delta(q)$ denote, respectively, the rate and the relative distance of the q-ary Schubert code $C_\alpha(\ell, m)$. Then, we have*

$$\lim_{q\to 1} R(q) = 1 \quad \text{and} \quad \lim_{q\to\infty} \Delta(q) = 1.$$

Proof. The limiting formula for the rate is immediate from Proposition 11. As for the relative distance, it suffices to observe that using Theorem 1, we have

$$\lim_{q\to\infty} \frac{U_\alpha(q)}{n_\alpha(q)} = 1 \quad \text{and} \quad \lim_{q\to\infty} \frac{L_\alpha(q)}{n_\alpha(q)} = 1,$$

where $U_\alpha(q) := q^{\delta_\alpha}$ denotes the upper bound (cf. [3, Proposition 4]) for the minimum distance of $C_\alpha(\ell, m)$, while $L_\alpha(q)$ denotes the lower bound given by (8). □

4. Minimum distance conjecture for Schubert divisors

The notation in this section will be as in the Introduction and at the beginning of Section 2. To avoid trivialities, we may tacitly assume that $1 < \ell < m$. Further, we let

$$\theta := (m-\ell+1, m-\ell+2, \dots, m) \quad \text{and} \quad \eta := (m-\ell, m-\ell+2, \dots, m).$$

Note that with respect to the partial order $\leqslant$, defined in the Introduction, θ is the unique maximal element of $I(\ell, m)$ whereas η the unique submaximal element. Moreover, by (4), we have

$$k_\theta = k := \binom{m}{\ell} \text{ and } k_\eta = k-1; \text{ also } \delta_\theta = \delta := \ell(m-\ell) \text{ and } \delta_\eta = \delta - 1.$$

Thus, in view of Theorem 1, we have

$$n_\theta = |\Omega_\theta| = |G_{\ell,m}| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q \quad \text{and} \quad n_\eta = |\Omega_\eta| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q - q^\delta. \tag{17}$$

Indeed, Ω_θ is the full Grassmannian $G_{\ell,m}$, whereas Ω_η is the unique subvariety of $G_{\ell,m}$ of codimension one, which is often referred to as the *Schubert divisor* in $G_{\ell,m}$.

Theorem 14. *If $\eta := (m-\ell, m-\ell+2, \dots, m)$ so that $\delta_\eta = \delta - 1$, then*

$$d_r(C_\eta(\ell, m)) = q^{\delta-1} + q^{\delta-2} + \cdots + q^{\delta-r} \quad \text{for} \quad 1 \leqslant r \leqslant \max\{\ell, m-\ell\}. \tag{18}$$

In particular, $d_1(C_\eta(\ell, m)) = q^{\delta_\eta}$, and so the minimum distance conjecture is valid in this case.

Proof. Let r be a positive integer and $H_\theta = \{p = (p_\beta) \in \mathbb{P}^{k-1} = \mathbb{P}(\wedge^\ell V) : p_\theta = 0\}$ be the hyperplane given by the vanishing of the Plücker coordinate corresponding to θ. Note that $\Omega_\eta = G_{\ell,m} \cap H_\theta$. Now, if Π is a linear subspace of $\mathbb{P}^{k_\eta - 1} = \mathbb{P}(H_\theta)$ of codimension r, then as a linear subspace of $\mathbb{P}^{k-1}$, it is of codimension $r+1$. Therefore,

$$|\Omega_\eta \cap \Pi| = |G_{\ell,m} \cap H_\theta \cap \Pi| = |G_{\ell,m} \cap \Pi| \leqslant |G_{\ell,m}| - d_{r+1}(C(\ell, m)).$$

Hence, in view of (17), if $r \leqslant \max\{\ell, m-\ell\}$, then by (3), we see that

$$d_r(C_\eta(\ell, m)) = |\Omega_\eta| - \max_{\operatorname{codim}\Pi = r} |\Omega_\eta \cap \Pi| \geqslant |\Omega_\eta| - |G_{\ell,m}| + q^\delta + q^{\delta-1} + \cdots + q^{\delta-r}.$$

Thus, to complete the proof it suffices to exhibit a codimension r linear subspace Π of $\mathbb{P}^{k_\eta - 1} = \mathbb{P}(H_\theta)$ such that $|\Omega_\eta \cap \Pi| = |\Omega_\eta| - (q^{\delta-1} + q^{\delta-2} + \cdots + q^{\delta-r})$. To this end, we use the notion of a close family introduced in [3,4], and some results from [3].

First, suppose $m-\ell \geqslant \ell$ so that $r \leqslant m-\ell$. Now let

$$\alpha^{(j)} = (m-\ell+2-j, m-\ell+2, m-\ell+3, \ldots, m), \quad \text{for } j = 1, \ldots, r+1$$

and let $\Lambda = \left\{\alpha^{(1)}, \ldots, \alpha^{(r+1)}\right\}$. Then Λ is a subset of $I(\ell, m)$ and a *close family*[5], in the sense of [3, p. 126]. Note that $\alpha^{(1)} = \theta$ and $\alpha^{(2)} = \eta$. Thus if Π denotes the linear subspace of $\mathbb{P}^{k_\eta - 1} = \mathbb{P}(H_\theta)$ defined by the vanishing of the Plücker coordinates corresponding to $\alpha^{(2)}, \ldots, \alpha^{(r+1)}$, and Π' denotes the linear subspace of $\mathbb{P}^{k-1}$ defined by the vanishing of the Plücker coordinates corresponding to $\alpha^{(1)}, \ldots, \alpha^{(r+1)}$, then $\operatorname{codim} \Pi' = r+1$, and using [3, Proposition 1], we obtain

$$|\Omega_\eta \cap \Pi| = |G_{\ell,m} \cap \Pi'| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q - q^\delta - q^{\delta-1} - \cdots - q^{\delta-r}.$$

Thus, in view of (17), it follows that Π is a subspace of $\mathbb{P}^{k_\eta - 1} = \mathbb{P}(H_\theta)$ of codimension r with the desired property.

On the other hand, suppose $\ell \geqslant m-\ell$. Then we let

$$\alpha^{(j)} = (m-\ell, m-\ell+1, \ldots, m-\widehat{\ell+j}-1, \ldots, m), \quad \text{for } j = 1, \ldots, r+1,$$

where $m-\widehat{\ell+j}-1$ indicates that the element $m-\ell+j-1$ is to be removed. Once again, for $r \leqslant \ell$, $\Lambda = \left\{\alpha^{(1)}, \ldots, \alpha^{(r+1)}\right\}$ is a subset of $I(\ell, m)$ and a close family with $\alpha^{(1)} = \theta$. Hence we can proceed as before and apply [3, Proposition 1] to obtain the desired formula for $d_r(C_\eta(\ell, m))$. □

Remark 15. An obvious analogue of the inductive argument in the above proof seems to fail for Schubert subvarieties of codimension 2 or more. For example, in $G_{3,6}$ the subvariety Ω_α corresponding to $\alpha = (3, 4, 6)$ is of codimension 2. However, Ω_α is not the intersection of $G_{3,6}$ with two Plüker coordinate hyperplanes but with four of them [viz., those corresponding to $(j, 5, 6)$ for $1 \leqslant j \leqslant 4$]. Thus, to determine $d_1(C_\alpha(3, 6))$, we should know $d_5(C(3, 6))$. But we know $d_r(C(3, 6))$ only for $r \leqslant \max\{3, 6-3\}+1 = 4$. The argument will, however, work for Schubert varieties of codimension 2 in $G_{2,m}$ because one of these two varieties will be a lower order Grassmannian while the other is a section by just 3 hyperplanes, and assuming, as we may, that $m > 4$, we can apply formula (3) and some results from [3]. We leave the details to the reader. In any case, we know from the work of Chen [1] and Guerra–Vincenti [7] that the minimum distance conjecture is true when $\ell = 2$.

[5] Two elements $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ and $\beta = (\beta_1, \ldots, \beta_\ell)$ in $I(\ell, m)$ are said to be *close* if they differ in a single coordinate, that is, $|\{\alpha_1, \ldots, \alpha_\ell\} \cap \left\{\beta_1, \ldots, \beta_\ell\right\}| = \ell - 1$. A subset of $I(\ell, m)$ is called a *close family* if any two distinct elements in it are close.

Acknowledgments

A part of this work was done when the first author was visiting the Institut de Mathématiques de Luminy (IML), Marseille during May–June 1999. Partial support for this visit from the Commission on Development and Exchanges (CDE) of the International Mathematical Union (IMU), and the warm hospitality of IML is gratefully acknowledged. Thanks are also due to Gilles Lachaud and Serge Vlăduţ for useful discussions, to Christian Krattenthaler for some helpful correspondence concerning determinant evaluations, and to Lucio Guerra and Rita Vincenti for a week long visit in June 2002 to the University of Perugia during which the first author learned of their recent results. We are also grateful to a vicious landlady, whom we do not name here, and more so to a kind-hearted one, Mme C. Cerisier, whose actions led us to share an apartment in Marseille in June 1996, where this work began.

References

[1] H. Chen, On the minimum distance of Schubert codes, IEEE Trans. Inform. Theory 46 (2000) 1535–1538.

[2] C. Ehresmann, Sur la topologie de certains espaces homogènes, Ann. of Math. (2) 35 (1934) 396–443.

[3] S.R. Ghorpade, G. Lachaud, Higher weights of Grassmann codes, in: Coding Theory, Cryptography and Related Areas (Guanajuato, 1998), Springer, Berlin/Heidelberg, 2000, pp. 122–131.

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

[5] S.R. Ghorpade, A note on Hodge's postulation formula for Schubert varieties, in: Geometric and Combinatorial Aspects of Commutative Algebra (Messina, 1999), Marcel Dekker, New York, 2001, pp. 211–220.

[6] S.R. Ghorpade, M.A. Tsfasman, Classical varieties, codes and combinatorics, in: Proceedings of the 15th International Conference on Formal Power Series and Algebraic Combinatorics, Vadstena, Sweden, 2003.

[7] L. Guerra, R. Vincenti, On the linear codes arising from Schubert varieties, Des. Codes Cryptogr. 33 (2004) 173–180.

[8] W.V.D. Hodge, Some enumerative results in the theory of forms, Proc. Cambridge Philos. Soc. 39 (1943) 22–30.

[9] W.V.D. Hodge, D. Pedoe, Methods of Algebraic Geometry, vol. II, Cambridge University Press, Cambridge, 1952.

[10] C. Krattenthaler, Advanced determinant calculus, Sém. Lothar. Combin. 42 (1999), Article B42q, 67.

[11] T. Muir, The Theory of Determinants in the Historical Order of Development, 4 vols., Macmillan, London, 1906–1923.

[12] D.Yu. Nogin, Codes associated to Grassmannians, in: R. Pellikaan, M. Perret, S.G. Vlăduţ (Eds.), Arithmetic Geometry and Coding Theory (Luminy, 1993), Walter de Gruyter, Berlin/New York, 1996, pp. 145–154.

[13] A.M. Ostrowski, On some determinants with combinatorial numbers, J. Reine Angew. Math. 216 (1964) 25–30.

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

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

[16] C.T. Ryan, K.M. Ryan, The minimum weight of Grassmannian codes $C(k, n)$, Discrete Appl. Math. 28 (1990) 149–156.

[17] R. Stanley, Enumerative combinatorics, vol. I, Wadsworth & Brooks/Cole, Monterey, CA, 1986.

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

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

[20] R. Vincenti, On some classical varieties and codes, Rapporto Technico 20/2000, Dipartimento di Mathematica e Informatica, Universitá degli Studi di Perugia, Italy, 2000.

[21] J. Wolper, Linear Codes from Schubert varieties, Issac Newton Institute of Mathematical Sciences, Cambridge, Preprint No. NI96048, 1996.