CLASSICAL VARIETIES, CODES AND COMBINATORICS

SUDHIR R. GHORPADE AND MICHAEL A. TSFASMAN

1. Introduction

For over two decades, the theory of linear (error correcting) codes has extensive and fruitful interaction with the theory of algebraic curves. The study of linear codes associated to higher dimensional algebraic varieties over finite fields is relatively new. However, given the richness of the geometric objects at our disposal, it promises to play a useful role in coding theory. Moreover, such a study often seems to lead to questions that could also be of interest in combinatorics and algebraic geometry.

In this article we attempt to illustrate these remarks by considering linear codes associated to Schubert varieties in Grassmannians. Our main results are presented here only with a brief idea of proofs; for details, we refer to [7]. To motivate and to give a perspective, we include a quick outline of some background material and known results.

2. Linear Codes and Projective Systems

Let $\mathbb{F}_q$ denote the finite field with q elements, and let n, k be integers with $1 \leq k \leq n$. 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 article 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

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

The first named author was partially supported by the IRCC grant 97IR012 from IIT Bombay. The second named author was partially supported by the RFBR Grants 99-01-01204, 02-01-01041 and 02-01-22005.

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 [21]. 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 $\mathbb{P}^{k-1}$.

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. For more details concerning projective systems and a proof of the above mentioned one-to-one correspondence, we refer to [21] and [22].

3. GRASSMANN CODES AND SCHUBERT CODES

Perhaps the most basic example of a projective algebraic variety over $\mathbb{F}_q$ 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], [11]), 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 [17, 18, 19] in the binary case and by Nogin [14] in the q-ary case. It is clear that the length n and the dimension k of $C(\ell,m)$ are given by

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

The minimum distance of $C(\ell,m)$ is given by the following elegant formula due to Nogin [14]:

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

In fact, Nogin [14] also determined some of the higher weights of $C(\ell,m)$. More precisely, he showed that for $1 \le r \le \max\{\ell, m-\ell\}+1$,

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

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

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

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

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

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

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

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

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

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

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

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 Hao 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 [9]; in the same paper, they prove also the following lower bound for $d(C_\alpha(\ell,m))$ in the general case:

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

In an earlier paper, Vincenti [23], 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[1] 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 $i \leq k_i \leq \alpha_i$ and $k_i \leq k_{i+1}$ for $1 \leq i \leq \ell-1$, and where, by convention, $\alpha_0 = 0 = k_0$ and $k_\ell = \ell$.

Now, we are ready to state our main results.

4. LENGTH OF SCHUBERT CODES

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

---

[1] In fact, in [23] and [9], 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 [23, Prop. 15], one has to set $\ell = d+1$, $\alpha_i = a_{i-1}+1$ and $k_i = \ell_{i-1}+1$ for $1 \leq i \leq \ell$. A similar substitution has to be made to get (8) from [9, Thm. 1.1].

Quite possibly, the simplest formula for the length n_α of $C_\alpha(\ell,m)$ is the one given in the theorem below. This is essentially an easy consequence of the well-known cellular decomposition of the Grassmannian, which goes back to Ehresmann [2].

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*

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

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

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 the closed form formula in (1) for n 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 will be clear from the results in Section 5. 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 some notation.

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 $\begin{bmatrix} u \\ v \end{bmatrix}_q$ is defined as in (1) when $0 \le v \le u$, and 0 otherwise. Thus, if $a = s = 0$, then $\lambda(a,b;s,t) = \begin{bmatrix} b \\ t \end{bmatrix}_q$.

Theorem 2. *Let $\alpha = (\alpha_1, \dots, \alpha_\ell)$ have $u+1$ 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 $1 \le p_1 < \dots < p_u < \ell$ and $\alpha_{p_i+1}, \dots, \alpha_{p_{i+1}}$ are consecutive for $0 \le i \le u$, where by convention, $p_0 = 0$ and $p_{u+1} = \ell$. Then the length n_α of the Schubert code $C_\alpha(\ell,m)$ is given by

$$n_\alpha = \sum_{s_1=p_1}^{\alpha_{p_1}} \sum_{s_2=p_2}^{\alpha_{p_2}} \cdots \sum_{s_u=p_u}^{\alpha_{p_u}} \prod_{i=0}^{u} \lambda(\alpha_{p_i}, \alpha_{p_{i+1}}; s_i, s_{i+1}), \tag{11}$$

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

The key idea in the proof of the above theorem is to use an inductive argument together with Möbius inversion applied to the poset of subspaces of a finite dimensional vector space over $\mathbb{F}_q$, and the well-known formula for the Möbius function of this poset (cf. [20, Ch. 3]).

Remark 3. In the case $\ell = 2$, we obviously have $u \le 1$, and the formula given above becomes somewhat simpler. It is not difficult to verify that this agrees with the formula (6) of Hao Chen [1].

Remark 4. 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 (11). It would be an intriguing problem to prove this without invoking Schubert varieties.

5. Dimension of Schubert codes

Let the notation be as in the beginning of the previous section. An explicit formula for the dimension k_α of the Schubert code $C_\alpha(\ell, m)$ is given by the following

Theorem 5. *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.,*

$$k_\alpha = \begin{vmatrix} \binom{\alpha_1}{1} & 1 & 0 & \dots & 0 \\ \binom{\alpha_1}{2} & \binom{\alpha_2-1}{1} & 1 & \dots & 0 \\ \vdots & & & & \vdots \\ \binom{\alpha_1}{\ell} & \binom{\alpha_2-1}{\ell-1} & \binom{\alpha_3-2}{\ell-2} & \dots & \binom{\alpha_\ell-\ell+1}{1} \end{vmatrix}. \tag{12}$$

The key idea in the proof of this theorem is to use the postulation formula for Schubert varieties in Grassmannians, which goes back to Hodge [10] (see also [5]).

Remark 6. In the case $\ell = 2$, we obviously have

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

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

The determinant in (12) is, in general, not easy to evaluate. For example, none of the recipes in the rather comprehensive compendium of Krattenthaler [12] seems applicable. However, in a special case, a much simpler formula can be obtained.

Theorem 7. *Suppose $\alpha_1, \dots, \alpha_\ell$ are in an arithmetic progression, i.e., there are $c, d \in \mathbb{Z}$ such that $\alpha_i = c(i-1) + d$ for $i = 1, \dots, \ell$. Then*

$$k_\alpha = \frac{\alpha_1}{\alpha_{\ell+1}} \binom{\alpha_{\ell+1}}{\ell}, \quad \text{where} \quad \alpha_{\ell+1} := c\ell + d = \ell\alpha_2 + (1-\ell)\alpha_1.$$

The key idea in the proof of the above theorem is to use formula (3.13) from [12, Thm. 26].

Remark 8. The simplest case where the above Proposition is applicable is when $\alpha_1, \dots, \alpha_\ell$ are consecutive, i.e., $c = 1$ and $\alpha_i = d + i - 1$. Then, the formula for k_α reduces to $\binom{d+\ell-1}{\ell}$. Of course, this is not surprising because in this case Ω_α is nothing but the smaller Grassmannian $G_{\ell, d+\ell-1}$. So, here 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 (12) does not seem obvious. Indeed, 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 [15] in 1964. The case when $\{k_i\}$ are consecutive seems to go back to Zeipel in 1865 (cf. [13, 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 $C(\ell, m)$:

$$\lim_{q\to 1} n(q) = k \quad \text{or, in other words,} \quad \lim_{q\to 1} \begin{bmatrix} m \\ \ell \end{bmatrix}_q = \binom{m}{\ell}. \tag{13}$$

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! It turns out that a similar relation holds in the case of Schubert codes. This can, then, be used to obtain the said alternative formula for k_α:

Proposition 9. *The dimension k_α of the q-ary Schubert code $C_\alpha(\ell, m)$ is independent of q and is related to its length $n_\alpha = n_\alpha(q)$ by the formula*

$$\lim_{q\to 1} n_\alpha(q) = k_\alpha. \tag{14}$$

Consequently, if u and $p_1, \dots, p_u$ be are as in Theorem 2, then

$$k_\alpha = \sum_{s_1=p_1}^{\alpha_{p_1}} \sum_{s_2=p_2}^{\alpha_{p_2}} \cdots \sum_{s_u=p_u}^{\alpha_{p_u}} \prod_{i=0}^{u} \binom{\alpha_{p_{i+1}} - \alpha_{p_i}}{s_{i+1} - s_i}, \tag{15}$$

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

Remark 10. As a consequence of the results in this section, we obtain a purely combinatorial identity which equates the right hand sides of (12) and (15). 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 11. *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*

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

This corollary is a consequence of Proposition 9 together with Theorem 1 and some results from [3].

6. Minimum Distance Conjecture for Schubert Divisors

As remarked earlier, the minimum distance conjecture for the unique nontrivial Schubert variety in the Klein quadric $G_{2,4}$, namely $\Omega_{(2,4)}$, was proved in [23]. The result in [1] and [9] for Schubert varieties in $G_{2,m}$ generalizes this simple example. Another natural generalization is the family of Schubert varieties of codimension one in $G_{\ell,m}$ for arbitrary ℓ and m. It turns out that the conjecture can also be proved, in the affirmative, for this other generalization. However, the general case of the minimum distance conjecture remains open.

Let us, as before, fix integers ℓ, m with $1 \le \ell \le m$, and for any $\beta = (\beta_1, \dots, \beta_\ell) \in I(\ell, m)$, let $\delta_\beta = \sum_{i=1}^{\ell}(\beta_i - i)$. 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 $\le$, defined in Section 3, θ is the unique maximal element of $I(\ell, m)$, whereas η the unique submaximal element. Moreover $\delta_\theta = \delta := \ell(m-\ell)$ and $\delta_\eta = \delta - 1$. Thus, 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 12. *For $1 \le r \le \max\{\ell, m-\ell\}$, we have*

$$d_r\left(C_\eta(\ell, m)\right) = q^{\delta-1} + q^{\delta-2} + \cdots + q^{\delta-r}. \tag{16}$$

In particular, $d\left(C_\eta(\ell, m)\right) = q^{\delta_\eta}$, i.e., the minimum distance conjecture is valid in this case.

The key idea in the proof of this theorem is to use the notion of a close family introduced in [3] and [4], and some results from [3].

7. Related Developments

Just as a Schubert variety is a natural generalization of the Grassmannian, another natural generalization is the variety of partial flags. These are defined as follows. Let V be a vector space of dimension m over $\mathbb{F}_q$. Let $\underline{\ell} = (\ell_1, \dots, \ell_s)$ be a sequence of integers such that $0 < \ell_1 < \cdots < \ell_s < m$. A *partial flag* of dimension $\underline{\ell}$ is a sequence $(V_1, \dots, V_s)$ of subspaces of V such that $V_1 \subset \cdots \subset V_s$ and $\dim V_i = \ell_i$ for $1 \le i \le s$. Let $\mathcal{F}_{\underline{\ell}}(V)$ denote the set of partial flags of dimension $\underline{\ell}$. Note that if $s = 1$, then $\mathcal{F}_{\underline{\ell}}(V)$ is the *Grassmannian* $\mathrm{Gr}_{\ell_1}(V)$. In general, $\mathcal{F}_{\underline{\ell}}(V)$ embeds naturally into a product of Grassmannians, and hence into a product of projective spaces via the Plücker embeddings, and consequently, into a large projective space via the Segre embedding. As such, it is a projective variety defined over $\mathbb{F}_q$ and gives rise to a linear code, which we denote by $C(\underline{\ell}; m)$ or $C(\ell_1, \dots, \ell_s; m)$. The basic parameters n, k and d of this code were determined by Rodier [16] when $s = 2$ and $\underline{\ell} = (1, m-1)$. In effect, he showed:

$$n = \frac{(q^m - 1)(q^{m-1} - 1)}{(q-1)^2}, \quad k = m^2 - 1 \quad \text{and} \quad d = q^{2m-3} - q^{m-2}.$$

It turns out that it is possible to extend the first two results so as to obtain formulae for n and k in the general case. The general formula for n is, in essence, known for many years and can be gleaned, for example, from [6, Sec. 2]. The general formula for k is a little more involved and uses ideas from representation theory. These results about the length and dimension of codes associated to flag varieties are expected to appear in [8]. However, for the minimum distance of these codes, nothing seems to be known, in general, even conjecturally.

Finally, we remark that Grassmannians and flag varieties are 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 generalization in this context. Thus it was indicated in [3] that codes such as 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 [24]. The general case, however, needs to be better understood and can be a source of numerous interesting problems.

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 and G. Lachaud, Higher weights of Grassmann codes, in: "Coding Theory, Cryptography and Related Areas" (Guanajuato, 1998), Springer-Verlag, Berlin/Heidelberg, 2000, pp. 122–131.

[4] S. R. Ghorpade and 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 and G. Lachaud, Number of solutions of equations over finite fields, and a conjecture of Lang and Weil, in: Number Theory and Discrete Mathematics (Chandigarh, 2000), Birkhäuser, Basel, 2002, pp. 269-291.

[7] S. R. Ghorpade and M. A. Tsfasman, Schubert varieties, linear codes and enumerative combinatorics, Prétirage n° 2003-04, Institut de Mathématiques de Luminy, Marseille, 2003.

[8] S. R. Ghorpade, Flag varieties and error correcting codes, in preparation.

[9] L. Guerra and R. Vincenti, On the linear codes arising from Schubert varieties, to appear in: *Des. Codes Cryptogr.*

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

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

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

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

[14] D. Yu. Nogin, Codes associated to Grassmannians, in: "Arithmetic, Geometry and Coding Theory" (Luminy, 1993), Walter de Gruyter, Berlin/New York, 1996, pp. 145–154.

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

[16] F. Rodier, Codes from flag varieties over a finite field, *J. Pure Appl. Algebra* **178** (2003) 203–214.

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

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

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

[20] R. Stanley, "Enumerative combinatorics, Vol. I", Revised Ed., Cambridge Univ. Press, Cambridge, 1997.

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

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

[23] R. Vincenti, On some classical varieties and codes, Proc. Combinatorics 2000 (Gaeta, Italy), to appear in: *Ital. J. Pure Appl. Math.*

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

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`

INSTITUT DE MATHÉMATIQUES DE LUMINY, CASE 907, 13288 MARSEILLE, FRANCE,

AND

INDEPENDENT UNIVERSITY OF MOSCOW,

AND

DORBUSHIN MATH. LAB., INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS, MOSCOW.

E-mail address: `tsfasman@iml.univ-mrs.fr`

URL: `http://www.aha.ru/~tsfasman`