Hyperplane Sections of Grassmannians and the Number of MDS Linear Codes

Sudhir R. Ghorpade*

Department of Mathematics, Indian Institute of Technology, Bombay, Powai, Mumbai 400076, India
E-mail: srg@math.iitb.ac.in

and

Gilles Lachaud

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

Communicated by Michael Tsfasman

Received May 28, 1999; revised July 11, 2000

We obtain some effective lower and upper bounds for the number of (n, k)-MDS linear codes over $\mathbb{F}_q$. As a consequence, one obtains an asymptotic formula for this number. These results also apply for the number of inequivalent representations over $\mathbb{F}_q$ of the uniform matroid, or, alternatively, the number of $\mathbb{F}_q$-rational points of certain open strata of Grassmannians. The techniques used in the determination of bounds for the number of MDS codes are applied to deduce several geometric properties of certain sections of Grassmannians by coordinate hyperplanes.

Key Words: Grassmannians, MDS codes, hyperplane sections, uniform matroids, arcs in projective spaces.

1. INTRODUCTION

Let V be a vector space of dimension n over the finite field $\mathbb{F}_q$ of q elements. Fixing a basis of V, we can represent elements $x \in V$ by their 'coordinates' $(x_1, \ldots, x_n)$, and then we can define a metric, known as the

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

Hamming metric, on V by

$$d(x,y) = \Big| \{i \in \{1,2,\dots,n\} : x_i \neq y_i\} \Big|, \qquad \text{for } x,y \in V.$$

An (n,k)–*linear code* over $\mathbb{F}_q$ is simply a k-dimensional subspace of V. Given such a code C, one defines the *minimal distance* of C to be

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

If $d(C) = t$, then the code C 'corrects' $\lfloor (t-1)/2 \rfloor$ errors. Thus, in Coding Theory, one is often interested in constructing codes C for which $d(C)$ is as large as possible. In general, the minimal distance of any (n,k)-linear code satisfies the Singleton bound (cf. [29]), namely,

$$d(C) \leq n - k + 1.$$

If $d(C) = n - k + 1$, then C is said to be a *Maximum Distance Separable* code, or simply, a *MDS* code.

Let q be a prime power and n, k be any integers such that $1 \leq k \leq n$. We are primarily interested in the following problem.

Problem A: *Determine the number of* (n,k)*-MDS linear codes over* $\mathbb{F}_q$.

It turns out that this problem admits a number of equivalent formulations. For example, in Matroid Theory, one has the notion of a *uniform matroid.* If we let $U_{k,n}$ denote the uniform matroid on n elements (in which any k elements form a base), then Problem A is equivalent to

Problem A$'$: *Determine the number of inequivalent representations over* $\mathbb{F}_q$ *of the uniform matroid* $U_{k,n}$.

For a proof of equivalence of Problem A and Problem A$'$, and some related results, we refer to [42].

As another example, consider the Grassmannian, which is one of the most basic objects in Algebraic Geometry. If we let $G_{k,n}$ denote the Grassmannian (of k-dimensional subspaces of an n-space) along with its canonical Plücker embedding [see Section 2 for details], and if $U(k,n)$ denotes the open stratum of $G_{k,n}$ consisting of those points of $G_{k,n}$ for which *all* the Plücker coordinates are nonzero, then Problem A is equivalent to

Problem A$''$: *Determine the number of* $\mathbb{F}_q$*-rational points of* $U(k,n)$.

It may be noted that, in view of Weil Conjectures, the last problem is essentially equivalent to determining the (ℓ-adic) Betti numbers of $U(k,n)$ and the eigenvalues of the Frobenius endomorphisms on the étale cohomology groups of $U(k,n)$. For details concerning this formulation, we refer to [41].

In a sense, Problem A can be traced back to some classical problems in Finite (Projective) Geometry posed by B. Segre in 1955. To describe these problems, we recall that an *n-arc* in the $(k-1)$–dimensional projective space $\mathbb{P}^{k-1}$ is a set of n points $P_1, \ldots, P_n$ in $\mathbb{P}^{k-1}$ such that no k of them lie in a hyperplane. An n-arc is said to be *complete* if it can not be extended to a $(n+1)$-arc in $\mathbb{P}^{k-1}$. Note that the point set of the rational normal curve, namely $\{P_t : t \in \mathbb{F}_q\} \cup \{P_\infty\}$, where $P_t = (1, t, t^2, \ldots, t^{k-1})$ and $P_\infty = (0, 0, \ldots, 0, 1)$, is a classical example of a complete $(q+1)$-arc. The problems of Segre can now be stated as follows.

S1 For which n, does there exist an n-arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$?

S2 For which k, $k < q$, is every $(q+1)$-arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ the point set of the rational normal curve?

S3 For which n and k, $k < q$, is every n-arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ a subset of the point set of the rational normal curve?

It is not difficult to see that the notion of an n-arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is essentially equivalent to the notion of a (n, k)-MDS linear code. Thus Problem A also admits an equivalent formulation in the language of arcs in projective spaces over finite fields (see, for example, [38, Lem. 4]). To relate Segre's problems to MDS codes, we let

$$\gamma(q) = \gamma(q; k, n) = \text{ the number of } (n, k)\text{-MDS codes over } \mathbb{F}_q\ .$$

Now the connection of Segre's problems with MDS codes is clear from the following observations (cf. [41, Prop. 3.2]).

C1 There exists an n-arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ if and only if $\gamma(q; k, n) > 0$.

C2 If $k < q$, then every $(q+1)$-arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is the point set of the rational normal curve if and only if $\gamma(q; k, q+1) = \gamma(q; 2, q+1) = (q-1)^q (q-2)!$

C3 If $n \leq q+1$ and $k < n-1$, then every n-arc in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ is a subset of the point set of the rational normal curve if and only if $\gamma(q; k, n) = \gamma(q; 2, n) = (q-1)^{n-1}(q-2)(q-3)\cdots(q-n+2)$.

For more on Segre's problems and the known results concerning them, we refer to [6], [7] and [19].

Returning to Problem A, an exact formula for for $\gamma(q; k, n)$ is known only when $k = 2$ (any n) and $k = 3$ (and $n \leq 9$). Since there is a duality for MDS codes (cf. [45, Prop. 4.1]), we have $\gamma(q; k, n) = \gamma(q; n-k, n)$, and in this way a few more values of (n, k) are covered. The known exact formulae are as follows.

(i) $\gamma(q; 1, n) = (q-1)^{n-1}$

(ii) $\gamma(q; 2, n) = (q-1)^{n-1}(q-2)\cdots(q-n+2)$

(iii) $\gamma(q;3,6) = (q-1)^5(q-2)(q-3)(q^2-2q+21)$

(iv) $\gamma(q;3,7) = (q-1)^6\left[(q-3)(q-5)(q^4-20q^3+148q^2-468q) - 30a_1(q)\right]$

(v) $\gamma(q;3,8) = (q-1)^7[(q-5)(q^7-43q^6+788q^5-7937q^4+47097q^3 -162834q^2-299280q-222960)-240(q^2-20q+78)a_1(q)+840b_2(q)]$

(vi) $\gamma(q;3,9) = (q-1)^8[q^{10}-75q^9+2530q^8-50466q^7+657739q^6 -5835825q^5-35563770q^4-146288034q^3+386490120q^2- 588513120q+389442480-1080(q^4-47q^3+807q^2-5921q+15134)a_1(q) +840(9q^2-243q+1684)b_2(q)+30240(-9b_3(q)+9a_2(q)+2a_3(q))]$.

Here, the functions $a_j(q)$, $b_\ell(q)$ appearing in the formulae (iv)–(vi) are defined by $a_j(q) = |\{x \in \mathbb{F}_q : f_j(x) = 0\}|$, where $f_1(x) = x^2+x+1$, $f_2(x) = x^2+x-1$ and $f_3(x) = x^2+1$, and for a prime ℓ, $b_\ell(q) = 1$ if q is a power of ℓ and 0 otherwise.

Of these exact formulae, (i) is trivial, (ii) is easy and (iii) is not difficult to obtain directly. Formulae (iv) and (v) were proved by Glynn [15]. Also, (iv) was proved independently in characteristic 2 by Rolland [38]. Lastly, (vi) was proved a few years ago by Iampolskaia, Skorobogatov and Sorokin [23]. It is clear that the exact formulae become increasingly complicated as n increases even for a small value of k such as $k=3$, and it is perhaps a hopeless task to obtain an exact formula in the general case. In fact, as Skorobogatov [41] has remarked, the work of Mnëv [33] indicates that it may be theoretically impossible to determine $\gamma(q;k,n)$ in general.

Faced with this scenario, we attempt in this paper to do what seems to be the next best thing to obtaining an exact solution of Problem A. Namely, we determine explicit upper and lower bounds for the number $\gamma(q;k,n)$, for any values of n,k and q (see Theorem 5.5 for a precise statement). As a Corollary, one obtains the following asymptotic formula

$$\gamma(q;k,n) = q^\delta + \left[1 - \binom{n}{k}\right] q^{\delta-1} + O\left(q^{\delta-2}\right), \qquad \text{where } \delta = k(n-k).$$

This implies in particular that given any (n,k) with $1 \le k \le n$, there exist (many) MDS codes for sufficiently large q. To get some idea of how closely these bounds approximate $\gamma(q)$, the reader may have a look at the tables in Section 7. It is seen therein that as q increases, our bounds become close to each other and (hence) to the exact value. Thus, these bounds seem fairly effective.

The main idea behind obtaining these bounds is quite simple. We work with the equivalent formulation in terms of the open stratum in Grassmannian (Problem A$''$), and note that to calculate the number of its $\mathbb{F}_q$-rational points, it suffices to determine the number of $\mathbb{F}_q$-rational points of all sections (typically denoted by E_Λ) of the Grassmannian $G_{k,n}$ by arbitrary families Λ of coordinate hyperplanes. Counting the latter is difficult in general, but in some cases we can do it using classical geometric facts about Grassmannians and some combinatorial ramifications thereof. Moreover, in the general case, we can obtain bounds for the number of $\mathbb{F}_q$-rational points of E_Λ, using the Griesmer-Wei bounds for higher weights of linear codes and some work of Nogin [35] about the so called Grassmann codes. The information thus obtained about $|E_\Lambda(\mathbb{F}_q)|$ is applied to yield the bounds for $\gamma(q;k,n)$ via the classical Bonnferroni inequalities.

In the process of counting the number of $\mathbb{F}_q$-rational points of E_Λ, we are led to consider a combinatorial notion of "close" families of subsets of a finite set and prove a Structure Theorem concerning them. This part may perhaps be of interest in itself, and the reader may directly refer to Section 4 for details.

The counting of $|E_\Lambda(\mathbb{F}_q)|$ also paves the way for deducing a number of geometric results concerning the linear sections of Grassmannians by coordinate hyperplanes. This is done mainly using the Grothendieck-Lefschetz Trace Formula and Deligne's Main Theorem ascertaining the validity of Riemann Hypothesis for varieties over finite fields (see Theorem 6.4 for a combined statement) and also using a result on hyperplane sections from [25]. It may be noted that the Schubert varieties in Grassmannians are particular cases of linear sections such as E_Λ. Also, a result of Mnëv [33] shows that up to birational equivalence and a torus action, the linear sections E_Λ are as general as any quasiprojective variety (at least over the reals). Thus, geometric properties of the linear sections E_Λ can be of considerable interest. We are able to prove results concerning the dimension, irreducibility (and, in general, the number of irreducible components), bounds on the dimensions of the singular loci, and in some cases Cohen-Macaulayness and normality, for the linear sections E_Λ when $|\Lambda| \leq 2$. In case Λ is singleton, these results can be recovered from the known results concerning Schubert varieties (although our proofs are different) but when Λ has two elements, the results appear to be new. More generally, when Λ is a "close" family of cardinality > 2, we determine the dimension of E_Λ and show that it has only one top-dimensional irreducible component.

This paper is organized as follows. In the next section, we set up some notation, and collect some preliminaries concerning Grassmannians, MDS codes and elementary facts about counting or estimating the cardinality of finite unions of finite sets. Main lemmas about the cardinality of sections of Grassmannians by coordinate hyperplanes are proved in Section 3. In Section 4, we define the notion of close families and prove basic results concerning them. This section is self-contained and can be read independently of others. Our main results about the bounds on the number of MDS codes are proved in Section 5. Geometric applications of our techniques to linear sections of Grassmannians are given in Section 6, and a reader primarily interested in these geometric results can go directly to this section, referring to the earlier sections only as and when necessary. Finally, in Section 7, we give a number of tables which contain numerical values of the lower and upper bounds for $\gamma(q;k,n)$ together with the exact value (wherever available) for certain 'small' values of (n,k) and q.

2. PRELIMINARIES

We begin with some notation and generalities about Grassmannians. A vector space V of dimension n over the field $\mathbb{F}_q$ of q elements, a basis $\{v_1,\ldots,v_n\}$ of V and an integer k with $1 \le k \le n$ will be kept fixed throughout this paper. We set

$$\delta = k(n-k) \qquad \text{and} \qquad N = \binom{n}{k}.$$

By $G_{k,n}(\mathbb{F}_q)$, or often simply by $G_{k,n}$, we shall denote the Grassmannian consisting of all k–dimensional subspaces of V. It is well-known that $G_{k,n}$ can be naturally embedded in the projective space $\mathbb{P}^{N-1}(\mathbb{F}_q)$. This is known as the *Plücker embedding* and it can be explicitly described as follows. First, let

$$I(k,n) = \{\alpha = (\alpha_1,\ldots,\alpha_k) \in \mathbb{Z}^k : 1 \le \alpha_1 < \ldots < \alpha_k \le n\}.$$

We can, and will, index the points of $\mathbb{P}^{N-1}(\mathbb{F}_q)$ by elements of $I(k,n)$ [ordered, say, lexicographically]. Now, given a k–dimensional subspace W, the 'coordinates' (in terms of $\{v_1,\ldots,v_n\}$) of a basis of W give a $k \times n$ matrix $A = (a_{ij})$ of rank k and the Plücker coordinate associated to W is given by $p = (p_\alpha)_{\alpha \in I(k,n)}$ where

$$p_\alpha = \alpha\text{–th minor of } A \;=\; \det\left(a_{i\alpha_j}\right)_{1 \le i,j \le k}, \qquad \text{for } \alpha \in I(k,n).$$

Note that a different choice of a basis for W results in all p_α's being multiplied by a nonzero scalar, and thus W uniquely determines a point of $\mathbb{P}^{N-1}(\mathbb{F}_q)$. Note also that the above construction is valid if $\mathbb{F}_q$ is replaced by any field F. In case F is an algebraically closed field (for example, the algebraic closure of $\mathbb{F}_q$), then it is well-known that the corresponding Grassmannian $G_{k,n}(F)$ is a nondegenerate, irreducible, nonsingular projective variety in $\mathbb{P}^{N-1}(F)$ of dimension δ (cf. [22]).

Following Andrews [3], we define the q–factorial of a nonnegative integer d by

$$[d]! = (q^d-1)(q^{d-1}-1)\ldots(q-1)$$

and the Gaussian binomial coefficient corresponding to n and k by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]!}{[k]![n-k]!} = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}.$$

It is well-known (and not difficult to prove) that $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$ is precisely the cardinality of the Grassmannian $G_{k,n}(\mathbb{F}_q)$, and $q^{\binom{d}{2}}[d]!$ is the cardinality of the general linear group $GL_d(\mathbb{F}_q)$. (See, for example, [17]). It is also well-known that $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$ is, in fact, a polynomial in q of degree δ with positive integral coefficients; indeed

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{i=0}^{\delta} \nu_i \, q^i$$

where ν_i is the number of partitions of i with at most k parts, each $\leq n-k$, i.e., ν_i equals the cardinality of the following set:

$$\{(\lambda_1, \dots, \lambda_r) \in \mathbb{N}^r : \lambda_1 + \dots + \lambda_r = i, \ r \leq k \text{ and } n-k \geq \lambda_1 \geq \dots \geq \lambda_r \geq 1\}.$$

Alternately, ν_i can be described in terms of paths in a $k \times (n-k)$ rectangle, or topologically (cf. [5, p. 292]) by $\nu_i = \dim H^{2i}(G_{k,n}; \mathbb{C})$. Notice that the sequence $\nu_0, \nu_1, \dots, \nu_\delta$ of the coefficients of $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$ is symmetric, i.e., $\nu_i = \nu_{\delta-i}$ for $0 \leq i \leq \delta$. This follows readily from the combinatorial description (by considering the complement in a $k \times (n-k)$ rectangle of the Young diagram of a partition) or from the topological description (by Poincaré duality). Thus, whenever $1 < k < n-1$, one gets easily the following estimate, which will be useful for us in the sequel.

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^\delta + q^{\delta-1} + 2q^{\delta-2} + O(q^{\delta-3}). \tag{1}$$

We now turn to some preliminaries about MDS codes. Throughout, by a *code* we will mean a linear code. Thus, an (n,k)-code over $\mathbb{F}_q$ is simply a k-dimensional subspace of V. Recall that the *dual* of an (n,k)-code C is the $(n, n-k)$-code $C^\perp$ given by $\{x \in V : \langle x, y \rangle = 0 \text{ for all } y \in C\}$, where $\langle \ \rangle$ is the usual dot product on V w.r.t the basis $\{v_1, \dots, v_n\}$. Let us also recall the following well-known characterization of the minimal distance of a code. This result is implicit in [29] as well as in [36] and [38], and in any case, its proof is a simple exercise in Linear Algebra.

LEMMA 2.1. *Let C be an (n,k)–linear code over $\mathbb{F}_q$ and H be its parity check matrix [i.e., an $(n-k) \times n$ matrix whose rows form a basis of the* *dual of C in V] and d be a positive integer. Then $d = d(C)$ if and only if every set of $d-1$ columns of H is linearly independent and some set of d columns of H is linearly dependent.*

Note that the Singleton inequality $d(C) \leq n - k + 1$ is an immediate consequence of the above Lemma. Further, we have the following corollary, which links MDS codes to Grassmannians.

Corollary 2.2. *Let C be an (n,k)–linear code over $\mathbb{F}_q$ and A be a $k \times n$ matrix whose rows form a basis of C. Then C is an MDS code if and only if all $k \times k$ minors of A are nonzero. Consequently, the number of (n,k)–linear MDS codes over $\mathbb{F}_q$ equals the cardinality of the open stratum $\{p \in G_{k,n}(\mathbb{F}_q) : p_\alpha \neq 0$ for all $\alpha \in I(k,n)\}$ of the Grassmannian.*

Proof. Follows by applying Lemma 2.1 to the dual $C^\perp$ of C and noting that C is an MDS code if and only if $C^\perp$ is. The latter follows, for instance, from Proposition 4.1 of [45]. ▮

Finally, in this section, we will recall some classical facts from Set Theory. Let N be a nonnegative integer. Put

$$[N] = \{1, 2, \ldots, N\} \quad \text{and for } r \in [N], \quad I_r[N] = \{\Lambda \subseteq [N] : |\Lambda| = r\}.$$

Let $A_1, \ldots, A_N$ be finite sets. Given any $\Lambda \subseteq [N]$, let

$$E_\Lambda = \bigcap_{i \in \Lambda} A_i.$$

Given any $r \in [N]$, let

$$e_r = \sum_{\Lambda \in I_r[N]} |E_\Lambda| \quad \text{and} \quad B_r = \sum_{i=1}^{r} (-1)^{i+1} e_i.$$

Proposition 2.3 (Principle of Inclusion and Exclusion).

$$\Big| \bigcup_{i \in [N]} A_i \Big| = B_N = \sum_{i=1}^{N} (-1)^{i+1} e_i.$$

Proposition 2.4 (Bonnferroni Inequalities). *Given any $r \in [N]$, we have*

$$\Big| \bigcup_{i \in [N]} A_i \Big| \leq B_r \quad \textit{if } r \textit{ is odd},$$

and

$$\Big|\bigcup_{i\in[N]} A_i\Big| \geq B_r \quad \textit{if } r \textit{ is even.}$$

REMARK 2.5. These results are very well-known. The inequalities in Proposition 2.4 seem to have first appeared in a paper of Bonnferroni (1936) on Probability and Statistics. For a reference to Bonnferroni's work as well as for a proof of Propositions 2.3 and 2.4, see, for example, [9, §4.1 and 4.7]. It may be tempting to think that the Bonnferroni bounds B_r become better as r increases, that is,

$$B_1 \geq B_3 \geq B_5 \geq \cdots \quad \text{and} \quad B_2 \leq B_4 \leq B_6 \leq \cdots.$$

But this is not true in general. Examples are easy to construct. Roughly speaking, this will be true if the intersections E_Λ are not too large compared to the A_i's. However, one can show that the inequalities above will always hold starting from B_r if $r > \lceil N/2 \rceil$. Indeed, for such r, we have $\binom{N}{r-1} \geq \binom{N}{r}$, and one can find a "contractive surjection" $f : I_{r-1}[N] \to I_r[N]$ (i.e., a surjective map such that $f(\Lambda') \supset \Lambda'$ for all $\Lambda' \in I_{r-1}[N]$). The existence of such a map follows from the Symmetric Chain Decomposition (SCD) of the Boolean lattice (cf. [4, Thm. 1, p. 18]) or, alternatively, as a consequence of Hall's Marriage Theorem (cf. [4, Ex. 7, p. 9]). Now,

$$\begin{aligned}
\sum_{\Lambda'\in I_{r-1}[N]} |E_{\Lambda'}| &= \sum_{\Lambda\in I_r[N]} \sum_{\Lambda'\in f^{-1}(\Lambda)} |E_{\Lambda'}| \\
&\geq \sum_{\Lambda\in I_r[N]} |E_\Lambda||f^{-1}(\Lambda)| \\
&\geq \sum_{\Lambda\in I_r[N]} |E_\Lambda|,
\end{aligned}$$

where the first inequality follows since f is contractive and the second since f is surjective. Thus $e_{r-1} \geq e_r$, and this implies the desired inequalities for the Bonnferroni bounds.

3. HYPERPLANE SECTIONS OF GRASSMANNIANS

We now introduce a variant of a set-theoretic notation used in the previous section, which will be relevant for our purpose. Given any subset Λ of $I(k,n)$, we let

$$E_\Lambda = \{p \in G_{k,n} : \ p_\alpha = 0 \text{ for all } \alpha \in \Lambda\}.$$

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. Given any $\alpha \in I(k,n)$, by $\bar{\alpha}$ we denote the corresponding set, i.e., $\bar{\alpha} = \{\alpha_1,\dots,\alpha_k\}$. Finally, given any point $p = (p_\alpha) \in \mathbb{P}^{N-1}(\mathbb{F}_q)$ and any integers $\gamma_1,\dots,\gamma_k$ between 1 and n, we set

$$p_{\gamma_1\dots\gamma_k} = \begin{cases} 0 & \text{if } \gamma_i = \gamma_j \text{ for some } i \neq j \\ \operatorname{sgn}(\sigma) p_\alpha & \text{if } \gamma_1,\dots,\gamma_k \text{ are distinct and } \sigma \in S_k,\ \alpha \in I(k,n) \\ & \text{are such that } \gamma_{\sigma(i)} = \alpha_i, \text{ for } 1 \le i \le k. \end{cases}$$

In estimating the number of points of the open stratum of Corollary 2.2, the following fundamental lemma about the Grassmannian would be crucial. Briefly, it says that the intersection of $G_{k,n}$ with a basic open subset $U_\alpha = \{p \in \mathbb{P}^{N-1} : p_\alpha \neq 0\}$ is in natural one-to-one correspondence with a cell (i.e., an affine space) of dimension δ. This result is classical and appears, for instance, essentially as Proposition 2 in [24]. It may be noted that although in [24] it is assumed that the ground field is $\mathbb{C}$, the argument therein works for arbitrary ground fields (of any characteristic). A slightly weaker version appears also in the literature on Coding Theory (see, for example, [36], [38], [41]).

Lemma 3.1 (Basic Cell Lemma). *Fix any $\alpha \in I(k,n)$. Let*

$$B_\alpha = \{p \in G_{k,n} : p_\alpha = 1\}$$

and

$$C_\alpha = \{\mathbf{t} = (t_{ij}) \in M_{k,n}(\mathbb{F}_q) : t_{i\alpha_j} = \delta_{ij} \text{ for } 1 \le i,j \le k\},$$

where $M_{k,n}(\mathbb{F}_q)$ denotes the set of all $k \times n$ matrices with entries in $\mathbb{F}_q$ and δ_{ij} denotes the Kronecker delta. Then the polynomial maps (or morphisms) $\Phi : B_\alpha \to C_\alpha$ and $\Psi : C_\alpha \to B_\alpha$ defined by

$$\Phi(p) = (t_{ij}(p)),$$

where for $p \in B_\alpha$,

$$t_{ij}(p) := p_{\alpha_1\dots\alpha_{i-1}j\alpha_{i+1}\dots\alpha_k}, \qquad \text{for } 1 \le i \le k,\ 1 \le j \le n$$

and

$$\Psi(\mathbf{t}) = (p_\beta),$$

where for $\mathbf{t} \in C_\alpha$,

$$p_\beta := \beta\text{-th minor of } \mathbf{t} = \det\left(t_{i\beta_j}\right)_{1\le i,j\le k}, \qquad \text{for } \beta \in I(k,n)$$

are bijective and inverses of each other. In particular, $G_{k,n} \cap U_\alpha$ *is in one-to-one correspondence with* $\mathbb{A}^\delta(\mathbb{F}_q)$*, where* $U_\alpha = \{p \in \mathbb{P}^{N-1} : p_\alpha \neq 0\}$.

COROLLARY 3.2. *Given any* $\alpha \in I(k,n)$*, we have* $|E_\alpha| = \begin{bmatrix} n \\ k \end{bmatrix}_q - q^\delta$.

Proof. With U_α as in Lemma 3.1, we have $E_\alpha = G_{k,n} \setminus (G_{k,n} \cap U_\alpha)$ and $|\mathbb{A}^\delta(\mathbb{F}_q)| = q^\delta$. ▮

COROLLARY 3.3. *Let* $\alpha, \beta \in I(k,n)$ *be distinct and let* $d = k - |\bar\alpha \cap \bar\beta|$ *be the "distance" between them. Then*

$$|E_{\alpha\beta}| = \begin{bmatrix} n \\ k \end{bmatrix}_q - 2q^\delta + q^{\delta - \binom{d+1}{2}}[d]!.$$

In particular, if $|\bar\alpha \cap \bar\beta| = k-1$*, then*

$$|E_{\alpha\beta}| = \begin{bmatrix} n \\ k \end{bmatrix}_q - 2q^\delta - q^{\delta-1}.$$

Proof. Let $A_1 = \{p \in G_{k,n} : p_\alpha \neq 0 \text{ and } p_\beta = 0\}$ and $n_1 = |A_1|$. By Lemma 3.1, we see that $n_1 = |\{\boldsymbol{t} \in C_\alpha : f_\beta(\boldsymbol{t}) = 0\}|$, where C_α is as in Lemma 3.1 and $f_\beta(\boldsymbol{t})$ is the $k \times k$ minor $\det\left(t_{i\beta_j}\right)_{1 \le i,j \le k}$. Now, write

$$\bar\beta \setminus (\bar\alpha \cap \bar\beta) = \{s_1, s_2, \ldots, s_d\} \quad \text{with} \quad s_1 < s_2 < \ldots < s_d.$$

Since $t_{i\alpha_j} = \delta_{ij}$ $(1 \le i,j \le k)$, by expanding the $k \times k$ matrix $\left(t_{i\beta_j}\right)$ suitably, using Laplace development, it follows that

$$f_\beta(\boldsymbol{t}) = \det\left(t_{i\beta_j}\right)_{1 \le i,j \le k} = \pm \det\left(t_{is_j}\right)_{1 \le i,j \le d}.$$

Therefore, the affine variety $\{\boldsymbol{t} \in C_\alpha : f_\beta(\boldsymbol{t}) = 0\}$ is a cone over the complement of $GL_d(\mathbb{F}_q)$ in $\mathbb{F}_q^{d^2}$. Consequently,

$$n_1 = q^{\delta - d^2}\left(q^{d^2} - q^{\binom{d}{2}}[d]!\right) = q^\delta - q^{\delta - \binom{d+1}{2}}[d]!.$$

The desired equality now follows from Corollary 3.2 since $E_{\alpha\beta} = E_\beta \setminus A_1$. ▮

REMARK 3.4. Given any $\alpha, \beta \in I(k,n)$, if $d = k - |\bar\alpha \cap \bar\beta|$ denotes the "distance" between them, then we always have $d \le \min\{k, n-k\}$. Indeed, it is obvious that $d \le k$, and moreover, the relations

$$2k - |\bar\alpha \cap \bar\beta| = |\bar\alpha| + |\bar\beta| - |\bar\alpha \cap \bar\beta| = |\bar\alpha \cup \bar\beta| \le n$$

readily imply that $d \leq n-k$.

In general, the cardinality of E_Λ is very difficult to determine exactly. However, we show below that it can be determined if the elements of Λ are "close" to each other. Moreover, a rather surprising application of Coding Theory shows that the cardinality in the general case is bounded above by that in the "close" case.

LEMMA 3.5. *Let Λ be a subset of $I(k,n)$ of cardinality r. Then*

$$|E_\Lambda| \leq \begin{bmatrix} n \\ k \end{bmatrix}_q - q^\delta - q^{\delta-1} - \ldots - q^{\delta-r+1}.$$

Moreover, if Λ has the property that $|\bar{\alpha} \cap \bar{\beta}| = k-1$, for all $\alpha, \beta \in I(k,n)$, $\alpha \neq \beta$, then the equality holds.

Proof. Since the Plücker embedding $G_{k,n} \hookrightarrow \mathbb{P}^{N-1}(\mathbb{F}_q)$ is nondegenerate, it defines a nondegenerate projective system in the sense of Tsfasman–Vlăduţ (cf. [44], [45]) and therefore (by [45, Theorem 2.1]) a nondegenerate linear $\left(\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q, N\right)$–code. Viewed this way, the higher weights d_r of this code satisfy the following Griesmer–Wei bound (cf. [46]):

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

Moreover, we know from the work of Nogin [35] that the minimum distance d_1 for this code is q^δ. Now, using the equivalence with the language of projective systems (cf. [45]) once again, we find that the difference $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q - d_r$ is given by

$$\max\left\{|G_{k,n} \cap \Pi_r| : \Pi_r \text{ a codimension } r \text{ projective subspace of } \mathbb{P}^{N-1}\right\}.$$

Thus, using the Griesmer–Wei bound with $d_1 = q^\delta$, we see that for any projective subspace Π_r of codimension r in $\mathbb{P}^{N-1}$, we have

$$|G_{k,n} \cap \Pi_r| \leq \begin{bmatrix} n \\ k \end{bmatrix}_q - q^\delta - q^{\delta-1} - \ldots - q^{\delta-r+1}.$$

Now E_Λ is evidently the intersection of $G_{k,n}$ with r coordinate hyperplanes, and hence the first part of the Lemma is proved. Next, suppose Λ has the property that $|\bar{\alpha} \cap \bar{\beta}| = k-1$, for all $\alpha, \beta \in I(k,n)$, $\alpha \neq \beta$. Choose any

$\alpha \in \Lambda$. Using arguments similar to those in the proof of Corollary 3.3 above, we see that for any $p \in G_{k,n}$ and $\beta \in \Lambda \setminus \{\alpha\}$, p_β corresponds to $\pm t_{uv}$ in the correspondence of Lemma 3.1, for a pair $(u,v) \neq (i, \alpha_j)$ for all $1 \le i, j \le k$, which is uniquely determined by β. Moreover, the pairs (u,v) corresponding to distinct elements of $\Lambda \setminus \{\alpha\}$ are distinct. It follows that the set

$$A_{r-1} = \{p \in G_{k,n} : p_\alpha \neq 0 \text{ and } p_\beta = 0 \text{ for all } \beta \in \Lambda \setminus \{\alpha\}\}$$

is in bijection with the zero locus of $r-1$ distinct coordinates in ${\mathbb{F}_q}^\delta$, and thus $|A_{r-1}| = q^{\delta - r + 1}$. The desired equality follows by induction on r since $E_\Lambda = E_{\Lambda \setminus \{\alpha\}} \setminus A_{r-1}$. ▮

Remark 3.6. For a more leisurely proof of the above Lemma as well as for an application of these ideas to the study of the so called Grassmann codes, see [13].

4. CLOSE FAMILIES OF k-SUBSETS

In this section, we shall prove some set-theoretic and combinatorial results, which, together with Corollary 3.3 and Lemma 3.5, would be useful in estimating the number of MDS codes. We shall find it convenient to use 'subsets' instead of 'sequences'. Accordingly, we consider $I_k[n]$ instead of $I(k,n)$. Recall that for any integer j, we let

$$I_j[n] = \{A : A \text{ is a subset of } [n] \text{ with } |A| = j\}$$

and that $[n]$ denotes the set of first n positive integers. As in Axiomatic Set Theory, for a given $\Lambda \subseteq I_k[n]$, the intersection of all $A \in \Lambda$ will be denoted by $\cap\Lambda$.

A family $\Lambda \subseteq I_k[n]$ will be called *close* if

$$|A \cap B| = k-1 \quad \text{for all } A, B \in \Lambda, \ A \neq B.$$

Basic examples of close families can be obtained by considering either of the following two types.

Definition 4.1. Let $\Lambda \subseteq I_k[n]$ be a nonempty family with $|\Lambda| = r$. We say that

(i) Λ is of *Type I* if there exists $S \in I_{k-1}[n]$ and $T \subseteq [n] \setminus S$ with $|T| = r$ such that

$$\Lambda = \{S \cup \{t\} : t \in T\}.$$

(ii) Λ is of *Type II* if there exists $S \in I_{k-r+1}[n]$ and $T \subseteq [n] \setminus S$ with $|T| = r$ such that

$$\Lambda = \{S \cup T \setminus \{t\} : t \in T\}.$$

REMARK 4.1. With notation as in the Definition above, observe that if Λ is of Type I or of Type II, then $\cap\Lambda$ is equal to S; in particular,

$$|\cap \Lambda| = \begin{cases} k-1 & \text{if } \Lambda \text{ is of Type I} \\ k-r+1 & \text{if } \Lambda \text{ is of Type II}. \end{cases}$$

It follows that if $r > 2$, the class of Type I families is disjoint from the class of Type II families. If $r = 2$, these two classes coincide. If $r = 1$, any $\Lambda \subseteq I_k[n]$ with $|\Lambda| = r$ is of Type I as well as of Type II.

The following characterization of close families is reminiscent of results in Extremal Set Theory or the Theory of Block Designs. However, we were unable to find it in the relevant literature.

THEOREM 4.2 (Structure Theorem for Close Families). *Let $\Lambda \subseteq I_k[n]$ with $|\Lambda| = r \geq 2$. Then Λ is close if and only if Λ is either of Type I or of Type II.*

Proof. It is obvious that if Λ is of Type I or Type II, then Λ is close. Conversely, suppose Λ is close. We proceed by induction on r. The case of $r = 2$ is trivial. Suppose $r = 3$. Write $\Lambda = \{A, B, C\}$ and let $t_B, t_C \in A$ and $j_B, j_C \in [n] \setminus A$ be the unique elements such that

$$B = (A \setminus \{t_B\}) \cup \{j_B\} \quad \text{and} \quad C = (A \setminus \{t_C\}) \cup \{j_C\}.$$

If $t_B = t_C$, then Λ is clearly of Type I, whereas if $t_B \neq t_C$, then $|B \cap C| = k - 1$ implies that $j_B = j_C$, and consequently, Λ is of Type II.

Now suppose $r > 3$ and that the result holds for smaller values of r. Fix any $A \in \Lambda$ and let

$$\Lambda' = \Lambda \setminus \{A\}, \quad S' = \cap\Lambda' \quad \text{and} \quad S = \cap\Lambda.$$

By induction hypothesis, we are in either of the two cases below.

Case 1. Λ' is of Type I.

Here, $|S'| = k - 1$, and thus for $S = S' \cap A$, we have $k - 2 \leq |S| \leq k - 1$. Suppose, if possible, $|S| = k - 2$. Now since $r > 3$, we can find distinct sets $B_1, B_2, B_3 \in \Lambda'$ and distinct elements $t_1, t_2, t_3 \in [n] \setminus S'$ such that $B_i = S' \cup \{t_i\}$ for $i = 1, 2, 3$. Since $|B_i \cap A| = k - 1 > k - 2 = |S' \cap A|$, we must have $t_i \in A$ for $i = 1, 2, 3$. But then $|A| \geq k + 1$, which is a contradiction. Therefore, $|S| = k - 1$ and so Λ must be of Type I.

Case 2. Λ' is of Type II.

Here, $|S'| = k - r + 2$, and there exists $T' \subseteq [n] \setminus S'$ with $|T'| = r - 1$ such that $\Lambda' = \{S' \cup T' \setminus \{t'\} : t' \in T'\}$. Thus, for $S = S' \cap A$, we have $k - r + 1 \leq |S| \leq k - r + 2$. In any case, since $r > 3$, there exists $t'_1 \in T'$ such that $t'_1 \in A$. Let $B_1 = S' \cup T' \setminus \{t'_1\}$. Suppose, if possible, $|S| = k - r + 2$. Then $S' = S \subseteq A$ and since $|A| = k$, there exists $t'_2 \in T'$ such that $t'_2 \notin A$. Let $B_2 = S' \cup T' \setminus \{t'_2\}$. Now $|B_1 \cap A| = k - 1$ implies that $T' \setminus \{t'_2\} \subseteq A$. But then $|B_2 \cap A| = k$, which is a contradiction. Therefore, $|S| = k - r + 1$. So there is a unique $s' \in S'$ such that $S = S' \setminus \{s'\}$. Now $|B_1 \cap A| = k - 1$ implies that $T' \subseteq A$, and thus $S' \cup T' \setminus \{s'\} = A$. It follows that if we let $T = T' \cup \{s'\}$, then $T \subseteq [n] \setminus S$, $|T| = r$ and $\Lambda = \{S \cup T \setminus \{t\} : t \in T\}$. Thus Λ is of Type II.

This completes the proof. ▌

REMARK 4.3. It may be remarked that subfamilies Λ of $I_k[n]$ are sometimes referred to as k-uniform hypergraphs or simply, as hypergraphs (see, for example [4]). Indeed, if $k = 2$, then these are essentially the same as simple graphs (i.e., finite graphs without loops or multiple edges). In the case of $k = 2$, the 'Structure Theorem' above is equivalent to an elementary result in Graph Theory that if a connected simple graph G has the property that any two edges are incident, then G is either a star or a triangle.

As a consequence of the 'Structure Theorem' above, we can calculate the cardinality of close families of a given size. In the sequel, we shall tacitly use the following elementary identities of binomial coefficients; for a proof of these, one may refer to [12, Lem. 3.1 (iv) and Lem. 3.2].

Given any integers a, b, c with $a \geq 0$, we have

$$\binom{a}{b}\binom{a-b}{c} = \binom{a}{c}\binom{a-c}{a-b-c} = \binom{a}{a-b-c}\binom{b+c}{b}.$$

COROLLARY 4.4. *Given any integer $r \geq 1$, let $c_r = c_r(k,n)$ denote the cardinality of all close families in $I_k[n]$ of cardinality r. Then*

$$c_r = \begin{cases} N & \text{if } r = 1 \\ \binom{n}{r}\binom{n-r}{k-1} & \text{if } r = 2 \\ \binom{n}{r}\left[\binom{n-r}{k-1} + \binom{n-r}{n-k-1}\right] & \text{if } r \geq 3\ . \end{cases}$$

Proof. The case of $r = 1$ is trivial. For $r \geq 2$, the number of $\Lambda \subseteq I_k[n]$ of Type I is clearly equal to

$$\binom{n}{k-1}\binom{n-k+1}{r} = \binom{n}{r}\binom{n-r}{n-k+1-r}$$

whereas the number of $\Lambda \subseteq I_k[n]$ of Type II is clearly equal to

$$\binom{n}{k-r+1}\binom{n-k+r-1}{r} = \binom{n}{r}\binom{n-r}{n-k-1}.$$

Thus, in view of Remark 4.1, the desired result follows from Theorem 4.2. ▌

REMARK 4.5. It would be interesting to determine the structure and consequently or otherwise, the cardinality of the set of families $\Lambda \subseteq I_k[n]$ of k-subsets of $[n]$ such that $|\Lambda| = r$ and any two distinct elements of Λ are at "distance" d from each other (i.e., $|A \cap B| = k-d$ for $A, B \in \Lambda,\ A \neq B$). The above two results correspond to the case of $d = 1$ while the Proposition below corresponds to the case of $r = 2$. It may be remarked that a variant of this general problem wherein one replaces the condition "distance d" by "distance $\leq d$" (i.e., $|A \cap B| \geq k - d$ for all $A, B \in \Lambda$) is much studied in the literature. For example, the well-known Erdös-Ko-Rado Theorem (cf. [4, p. 45]) is related to the case $d = k - 1$ of the latter problem.

PROPOSITION 4.6. *Let d be an integer with $1 \leq d \leq k$ and $\lambda_d = \lambda_d(k,n)$ be the number of 2-element subsets $\{A, B\}$ of $I_k[n]$ such that $|A \cap B| = k-d$. Then*

$$\lambda_d = \frac{1}{2}\binom{n}{k}\binom{n-k}{d}\binom{k}{d} = \frac{N}{2}\binom{n-k}{d}\binom{k}{d}.$$

Proof. Choosing an ordered pair (A, B) with $A, B \in I_k[n]$ and $|A \cap B| = k - d$ is equivalent to choosing any $k - d$ elements of $[n]$, and then any d

elements from the rest, and finally, any d elements from the remaining $n-(k-d)-d$ integers. Hence, the number of such ordered pairs is equal to

$$\binom{n}{k-d}\binom{n-k+d}{d}\binom{n-k}{d} = \binom{n}{n-k}\binom{k}{d}\binom{n-k}{d}.$$

For subsets instead of ordered pairs, we have to divide by 2. ▌

Remark 4.7. With notations as in the two results above, we have:

1. $\lambda_d = 0$ if $d > \min\{k, n-k\}$.
2. $\displaystyle\sum_{d=1}^{\min\{k,n-k\}} \lambda_d = \binom{N}{2}$.
3. $c_2 = \lambda_1$.

These identities follow easily from the formulae obtained above or alternatively, from the set-theoretic descriptions of c_r and λ_d and the observation in Remark 3.4.

5. BOUNDS FOR THE NUMBER OF MDS CODES

In this section, we shall prove our main results concerning estimates for

$$\gamma(q) = \gamma(q;k,n) = \text{ the number of } (n,k)\text{-MDS codes over } \mathbb{F}_q\,.$$

It is trivial to check that if $k = n$, then $\gamma(q) = 1$. Moreover, using the well-known duality between MDS codes and their duals (cf. [45, Prop. 4.1]), we clearly have $\gamma(q;k,n) = \gamma(q;n-k,n)$. Thus using Corollary 2.2, we can easily see that

$$\gamma(q;1,n) = \gamma(q;n-1,n) = (q-1)^{n-1}.$$

With this in view, we shall tacitly assume throughout this section that $1 < k < n-1$.

Following Section 3, we will consider hyperplane sections E_Λ for $\Lambda \subseteq I(k,n)$. As a variant of the notation used in Section 2, we define for any $r \geq 1$,

$$e_r(q) = e_r(q;k,n) = \sum_{|\Lambda|=r} |E_\Lambda|,$$

where the sum is over all subfamilies $\Lambda \subseteq I(k,n)$ of cardinality r. We set, by convention,

$$e_0(q) = e_0(q;k,n) = |G_{k,n}(\mathbb{F}_q)| = \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

We also define for any $r \geq 0$,

$$\mathcal{B}_r(q) = \mathcal{B}_r(q;k,n) = \sum_{i=0}^{r} (-1)^i e_i(q).$$

Note that for $r > N = \binom{n}{k}$, we have $e_r(q) = 0$ and $\mathcal{B}_r(q) = \mathcal{B}_N(q)$.

LEMMA 5.1. $\gamma(q) = \mathcal{B}_N(q) = \sum_{r=0}^{N} (-1)^r e_r(q)$. *Moreover, for any* $r \geq 0$, $\mathcal{B}_{2r+1}(q) \leq \gamma(q) \leq \mathcal{B}_{2r}(q)$.

Proof. By Corollary 2.2, we have

$$\gamma(q) = \Big| G_{k,n}(\mathbb{F}_q) \setminus \bigcup_{\alpha \in I(k,n)} E_\alpha \Big| = \begin{bmatrix} n \\ k \end{bmatrix}_q - \Big| \bigcup_{\alpha \in I(k,n)} E_\alpha \Big|.$$

Thus the desired result follows from Proposition 2.3 and Proposition 2.4. ▮

Now recall that for any $r \geq 1$, we have defined in Section 4 the function $c_r = c_r(k,n)$. Also for any integer d with $1 \leq d \leq k$, we have defined the function $\lambda_d = \lambda_d(k,n)$. It may be noted that c_r and λ_d are explicitly computable from the formulae given in Corollary 4.4 and Proposition 4.6. We set $c_0 = 1$. Observe that as a consequence of Theorem 4.2, it is readily seen that for $r \geq 0$,

$$c_r(k,n) = 0 \text{ if and only if } r > \max\{k, n-k\} + 1. \qquad (2)$$

It may be noted that the last assertion can also be derived from Corollary 4.4 (cf. [13]).

We define another explicit function by putting for any $r \geq 0$,

$$\epsilon_r(q) = \epsilon_r(q;k,n) = \begin{bmatrix} n \\ k \end{bmatrix}_q - q^\delta - q^{\delta-1} - \cdots - q^{\delta-r+1}.$$

Note that $\epsilon_0(q) = e_0(q) = \left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$. More generally, we have the following relation between $\epsilon_r(q)$ and $e_r(q)$.

LEMMA 5.2. *For $0 \le r \le N$, we have: $c_r \epsilon_r(q) \le e_r(q) \le \binom{N}{r} \epsilon_r(q)$.*

Proof. The upper bound follows from the first assertion in Lemma 3.5 while the lower bound follows from the second assertion in Lemma 3.5. ▮

PROPOSITION 5.3. *With notations as above, we have the following.*
(i) $\mathcal{B}_0(q) = e_0(q) = {n \brack k}_q$. *And asymptotically,*

$$\mathcal{B}_0(q) = q^\delta + q^{\delta-1} + 2q^{\delta-2} + O\left(q^{\delta-3}\right).$$

(ii) $\mathcal{B}_1(q) = e_0(q) - e_1(q)$ *is given by*

$$\mathcal{B}_1(q) = Nq^\delta + (1-N){n \brack k}_q = Nq^\delta + (1-N)\prod_{j=0}^{k-1} \frac{q^n - q^j}{q^k - q^j}$$

and asymptotically, it is given by

$$\mathcal{B}_1(q) = q^\delta + (1-N)q^{\delta-1} + (2-2N)q^{\delta-2} + O\left(q^{\delta-3}\right).$$

(iii) $\mathcal{B}_2(q) = e_0(q) - e_1(q) + e_2(q)$ *is equal to*

$$\left[N - 2\binom{N}{2}\right] q^\delta + \left[1 - N + \binom{N}{2}\right] {n \brack k}_q + \sum_{d=1}^{\min\{k,n-k\}} \lambda_d q^{\delta - \binom{d+1}{2}} [d]!$$

and asymptotically, it is given by

$$\mathcal{B}_2(q) = q^\delta + (1-N)q^{\delta-1} + \left[2 - 2N + \binom{N}{2}\right] q^{\delta-2} + O\left(q^{\delta-3}\right).$$

Proof. The first assertion is trivial and the asymptotic formula in (i) has already been noted in Section 2. For (ii), note that

$$e_1(q) = \sum_{\alpha \in I(k,n)} |E_\alpha| = \sum_{\alpha \in I(k,n)} \left({n \brack k}_q - q^\delta \right) = N {n \brack k}_q - Nq^\delta,$$

where the second equality follows from Corollary 3.2. The asymptotic formula for $\mathcal{B}_2(q)$ follows from (i). Lastly, in view of Remark 3.4, we have

$$e_2(q) = \sum_{\substack{\{\alpha,\beta\} \subseteq I(k,n) \\ \alpha \ne \beta}} |E_{\alpha\beta}| = \sum_{d=1}^{\min\{k,n-k\}} \sum_{\substack{\{\alpha,\beta\} \subseteq I(k,n) \\ |\alpha \cap \beta| = k-d}} |E_{\alpha\beta}|$$

$$= \sum_{d=1}^{\min\{k,n-k\}} \lambda_d \left(\begin{bmatrix} n \\ k \end{bmatrix}_q - 2q^\delta + q^{\delta - \binom{d+1}{2}} [d]! \right)$$

where the last equality follows from Corollary 3.3 and Proposition 4.6. The desired formulae for $\mathcal{B}_2(q)$ follow from above in view of Remark 4.7. Moreover, if $d > 1$, then we have

$$q^{\delta - \binom{d+1}{2}} [d]! = q^\delta - q^{\delta-1} - q^{\delta-2} + O\left(q^{\delta-3}\right).$$

In view of (1) and Remark 4.7, this yields the asymptotic formula for $\mathcal{B}_2(q)$. ▮

Definitions 5.4. Given any $s \geq 0$, we define $\widetilde{L}_s(q) = \widetilde{L}_s(q; k, n)$ and $\widetilde{U}_s(q) = \widetilde{U}_s(q; k, n)$ by

$$\widetilde{L}_s(q) = \sum_{r=0}^{s} c_{2r} \epsilon_{2r}(q) - \sum_{r=1}^{s+1} \binom{N}{2r-1} \epsilon_{2r-1}(q)$$

and

$$\widetilde{U}_s(q) = \sum_{r=0}^{s} \binom{N}{2r} \epsilon_{2r}(q) - \sum_{r=0}^{s} c_{2r-1} \epsilon_{2r-1}(q).$$

Further, we define $L_s(q) = L_s(q; k, n)$ by $L_0(q) = \mathcal{B}_1(q)$ and for $s \geq 1$,

$$L_s(q) = \mathcal{B}_2(q) + \sum_{r=2}^{s} c_{2r} \epsilon_{2r}(q) - \sum_{r=2}^{s+1} \binom{N}{2r-1} \epsilon_{2r-1}(q)$$

and $U_s(q) = U_s(q; k, n)$ by $U_0(q) = \mathcal{B}_0(q)$, $U_1(q) = \mathcal{B}_2(q)$ and for $s \geq 2$,

$$U_s(q) = \mathcal{B}_2(q) + \sum_{r=2}^{s} \binom{N}{2r} \epsilon_{2r}(q) - \sum_{r=2}^{s} c_{2r-1} \epsilon_{2r-1}(q).$$

Finally, we define

$$\begin{aligned} \widetilde{L}(q) &= \widetilde{L}(q; k, n) = \max\left\{ \widetilde{L}_s(q) : 0 \leq s \leq \lfloor (N-1)/2 \rfloor \right\}; \\ \widetilde{U}(q) &= \widetilde{U}(q; k, n) = \min\left\{ \widetilde{U}_s(q) : 0 \leq s \leq \lfloor N/2 \rfloor \right\}, \end{aligned}$$

and

$$\begin{aligned} L(q) &= L(q; k, n) = \max\left\{ L_s(q) : 0 \leq s \leq \lfloor (N-1)/2 \rfloor \right\}; \\ U(q) &= U(q; k, n) = \min\left\{ U_s(q) : 0 \leq s \leq \lfloor N/2 \rfloor \right\}. \end{aligned}$$

THEOREM 5.5. *We have the following lower and upper bounds for the number $\gamma(q) = \gamma(q; k, n)$ of all (n,k)-MDS linear codes over $\mathbb{F}_q$.*

(i) *For $0 \le s \le \lfloor (N-1)/2 \rfloor$, we have*

$$\widetilde{L}_s(q) \le L_s(q) \le \gamma(q).$$

(ii) *For $0 \le s \le \lfloor N/2 \rfloor$, we have*

$$\gamma(q) \le U_s(q) \le \widetilde{U}_s(q).$$

(iii) *Lastly, we have*

$$\widetilde{L}(q) \le L(q) \le \gamma(q) \le U(q) \le \widetilde{U}(q).$$

Proof. Given any $s \ge 0$, by Lemma 5.1, we have $\gamma(q) \ge \mathcal{B}_{2s+1}(q)$. In particular, $\gamma(q) \ge \mathcal{B}_1(q) = L_0(q) = \widetilde{L}_0(q)$. Now if $1 \le s \le \lfloor (N-1)/2 \rfloor$, or equivalently, if $1 \le 2s+1 \le N$, then by Lemma 5.2,

$$\begin{aligned} \mathcal{B}_{2s+1}(q) &= \mathcal{B}_2(q) + \sum_{r=2}^{s} e_{2r}(q) - \sum_{r=2}^{s+1} e_{2r-1}(q) \\ &\ge \mathcal{B}_2(q) + \sum_{r=2}^{s} c_{2r}\epsilon_{2r}(q) - \sum_{r=2}^{s+1} \binom{N}{2r-1} \epsilon_{2r-1}(q). \end{aligned}$$

Thus $\mathcal{B}_{2s+1}(q) \ge L_s(q)$. Likewise, Lemma 5.2 implies that

$$\mathcal{B}_2(q) \ge c_0\epsilon_0(q) - N\epsilon_1(q) + c_2\epsilon_2(q)$$

and thus $L_s(q) \ge \widetilde{L}_s(q)$. This proves (i). Assertion (ii) is similarly proved, and (iii) is an immediate consequence of (i) and (ii). ▮

COROLLARY 5.6. *For any given parameters (n,k) with $1 \le k \le n$, there exist (n,k)-MDS linear codes over $\mathbb{F}_q$ for sufficiently large q. In fact, $\gamma(q; k, n) > 0$ whenever $q \ge N = \binom{n}{k}$.*

Proof. Indeed, by Lemma 5.3 (ii), we have

$$L_0(q) = \mathcal{B}_1(q) = q^\delta + (1-N)q^{\delta-1} + O\left(q^{\delta-2}\right).$$

Since the coefficient of q^δ is positive, it follows that $L_0(q) > 0$ for sufficiently large q. Hence, by Theorem 5.5 (i), $\gamma(q) > 0$ for q sufficiently large. The last assertion follows by looking at $L_0(q)$ more carefully. Thus, we write,

$$L_0(q) = Nq^\delta + (1-N)\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{i=0}^{\delta} \nu_i q^i - \sum_{i=0}^{\delta-1} N\nu_i q^i = 1 + \sum_{i=0}^{\delta-1} \nu_i (q-N) q^i$$

where ν_i denotes the coefficient of q^i in the polynomial expansion of the Gaussian binomial coefficient $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$. As remarked in Section 2, each ν_i is positive, and thus the last expression above is ≥ 1 if $q \geq N$. ∎

Remark 5.7. The last assertion in the above Corollary appears to give a partial answer to the first problem of B. Segre. However, the bound $N = \binom{n}{k}$ is not optimal, in general; this may be seen easily from the existence of the Reed-Solomon codes. However, the proof of Corollary 5.6 also shows that as soon as $q > N$, there is an abundance of MDS codes for the corresponding parameters.

Theorem 5.8. *The number $\gamma(q) = \gamma(q; k, n)$ of all (n, k)-MDS linear codes over $\mathbb{F}_q$ is asymptotically equal to*

$$\gamma(q) = q^\delta + \left[1 - \binom{n}{k}\right] q^{\delta-1} + O\left(q^{\delta-2}\right).$$

Proof. By Lemma 5.3, both $L_0(q) = \mathcal{B}_1(q)$ and $U_1(q) = \mathcal{B}_2(q)$ are asymptotically given by

$$q^\delta + (1-N)q^{\delta-1} + O\left(q^{\delta-2}\right).$$

Now by Theorem 5.5, $L_0(q) \leq \gamma(q) \leq U_1(q)$ for all q. This implies the desired formula. ∎

Remark 5.9. It may be worthwhile to write down explicitly some of the lower bounds and upper bounds given by Theorem 5.5. For example, $L_s(q)$ for $s = 0$ gives the following lower bound for $\gamma(q)$:

$$\binom{n}{k} q^{k(n-k)} + \left[1 - \binom{n}{k}\right] \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}$$

while $U_s(q)$ for $s = 0$ gives the 'trivial upper bound'

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}.$$

A simpler, and slightly less trivial, upper bound can be obtained as a direct consequence of the Basic Cell Lemma. Namely,

$$\gamma(q; n, k) \leq q^{k(n-k)}.$$

To see this, note that by Corollary 2.2, $\gamma(q) \leq |G_{k,n}(\mathbb{F}_q) \setminus E_\alpha|$, for any $\alpha \in I(k, n)$, and then use Corollary 3.2. We leave it to the reader to work out more special cases of the bounds in Theorem 5.5 and to observe that in a few cases, some simplifications in the defining expressions can be made.

6. GEOMETRIC APPLICATIONS

Let F be an algebraically closed field. Consider the Grassmannian $G_{k,n}(F)$ of all k-dimensional subspaces of the n-dimensional vector space F^n over F. Let $\{v(1), \ldots, v(n)\}$ be the standard F-basis of F^n. As noted before, $G_{k,n}(F)$ is a projective algebraic variety of $\mathbb{P}_F^{N-1}$, which is defined over $\mathbb{Z}$ (and hence over $\mathbb{F}_q$ for any prime power q). We are interested in the geometry of the closed subvarieties

$$E_\Lambda(F) = \{p = (p_\gamma) \in G_{k,n}(F) : p_\gamma = 0 \text{ for all } \gamma \in \Lambda\}$$

where $\Lambda \subseteq I(k, n)$. Note that classical Schubert varieties $\Omega_\alpha(F)$ of $G_{k,n}(F)$ are particular cases of $E_\Lambda(F)$. Indeed, given $\alpha = (\alpha_1, \ldots, \alpha_k) \in I(k, n)$, the corresponding Schubert variety $\Omega_\alpha(F)$ is given by

$$\Omega_\alpha(F) = \{W \in G_{k,n}(F) : \dim (W \cap A_i) \geq i \text{ for } i = 1, \ldots, k\},$$

where $A_i = \operatorname{span}\{v(\alpha_1), \ldots, v(\alpha_i)\}$ for $1 \leq i \leq k$. Further, if we consider the 'Bruhat order' on $I(k, n)$ defined by

$$\beta \leq \beta' \Longleftrightarrow \beta_i \leq \beta'_i \quad \text{for all } i = 1, \ldots, k,$$

where $\beta = (\beta_1, \ldots, \beta_k)$ and $\beta' = (\beta'_1, \ldots, \beta'_k)$ are arbitrary elements of $I(k, n)$, then, in terms of the Plücker coordinates, we have

$$\Omega_\alpha(F) = \{p = (p_\gamma) \in G_{k,n}(F) : p_\beta = 0 \text{ for all } \beta \in I(k, n) \text{ with } \beta \not\leq \alpha\}.$$

It is well-known (cf. [22]) that $\Omega_\alpha(F)$ are irreducible algebraic varieties and

$$\dim \Omega_\alpha(F) = \sum_{i=1}^{k} \alpha_i - \frac{k(k+1)}{2}.$$

Note that the Grassmannian $G_{k,n}(F)$ is a particular case of $\Omega_\alpha(F)$ with $\alpha = (n-k+1, n-k+2, \dots, n)$. In particular, $\dim G_{k,n}(F) = \delta = k(n-k)$.

Lastly, recall that we have a natural transitive action of $\mathrm{GL}_n(F)$ on the Grassmannian $G_{k,n}(F)$, given by $(g, W) \mapsto W'$, where $W' \in G_{k,n}(F)$ is obtained from $g \in \mathrm{GL}_n(F)$ and $W \in G_{k,n}(F)$ by considering a $k \times n$ matrix C whose rows form a basis of W and letting W' be the subspace spanned by the rows of Cg. Alternatively, we can view $G_{k,n}(F)$ as the quotient $\mathrm{GL}_n(F)/P_k$, where P_k is the parabolic subgroup of $\mathrm{GL}_n(F)$ consisting of invertible matrices $g = (g_{ij})$ such that $g_{ij} = 0$ whenever $1 \le j \le k < i \le n$; now $\mathrm{GL}_n(F)$ acts naturally on this quotient and thus on $G_{k,n}(F)$. In particular, $G_{k,n}(F)$ is a homogeneous space.

Lemma 6.1. *For any $\alpha \in I(k,n)$, $E_\alpha(F)$ is isomorphic to a Schubert variety in $G_{k,n}(F)$. In particular, $E_\alpha(F)$ is an irreducible variety, and moreover the dimension of $E_\alpha(F)$ is $\delta - 1$.*

Proof. By the homogeneity of $G_{k,n}(F)$, it is clear that $E_\alpha(F)$ is isomorphic to $E_\theta(F)$, for any $\theta \in I(k,n)$. Take $\theta = (n-k+1, n-k+2, \dots, n-1, n)$. Then θ is the 'maximal element' of $I(k,n)$ w.r.t. the Bruhat order and if $\eta = (n-k, n-k+2, \dots, n-1, n)$, then: $\beta \not\le \eta \Leftrightarrow \beta = \theta$, for any $\beta \in I(k,n)$. Hence $\Omega_\eta(F) = E_\theta(F)$. Therefore $E_\theta(F)$, and consequently any $E_\alpha(F)$ is irreducible. The assertion about the dimension of $E_\alpha(F)$ follows easily from the formula for the dimension of Schubert varieties. ▮

Remarks 6.2. (i) It may be noted that the sections E_α and E_θ appearing in the above proof are not only isomorphic but also *isotopic* in the sense that there is an automorphism of the ambient space $\mathbb{P}_F^{N-1}$ (in fact, a collineation, i.e., a projective linear isomorphism), which leaves $G_{k,n}(F)$ invariant and maps $E_\alpha(F)$ onto $E_\theta(F)$. Indeed, let $g \in \mathrm{GL}_n(F)$ be the matrix corresponding to a permutation of the basis $\{v(1), \dots, v(n)\}$ in such a way that $v(\alpha_i) \mapsto v(\theta_i)$ for $1 \le i \le k$. Then the compound matrix C_g [which, by definition, is the $N \times N$ matrix, with rows and columns indexed by the elements of $I(k,n)$, whose (β,γ)-th entry is the $k \times k$ minor $\det \left(g_{\beta_i \gamma_j}\right)_{1 \le i,j \le k}$, where $\beta, \gamma \in I(k,n)$] is nonsingular and gives the desired collineation.

(ii) It is well-known (see, for example, [34, Thm. 4.1]) that if $\boldsymbol{t} = \{t_\beta : \beta \in I(k,n)\}$ is the set of coordinate functions on $G_{k,n}(F)$, then the vanishing ideal of $\Omega_\alpha(F)$ in the homogeneous coordinate ring $R = F[\boldsymbol{t}]$ of $G_{k,n}(F)$ is precisely the ideal J_α generated by $\{t_\beta : \beta \not\le \alpha\}$. In particular, the ring R/J_α is reduced. Note that if $\alpha = \eta = (n-k, n-k+2, \dots, n-1, n)$, then the ideal of $\Omega_\eta(F)$ in R is (t_θ). Hence, from the previous remark, we see that the ideal of $E_\alpha(F)$ in R is (t_α) and the ring $R/(t_\alpha)$ is reduced.

We shall now try to study more general linear sections E_Λ of the Grassmannian $G_{k,n}$. We begin by proving a useful fact about sections by close families as a nice application of the Structure Theorem.

LEMMA 6.3. *Let $\boldsymbol{P} = \{P_\gamma : \gamma \in I(k,n)\}$ be a family of N independent indeterminates over F and $S = F[\boldsymbol{P}]$ denote the corresponding polynomial ring. Let $Q = I(G_{k,n})$ denote the (vanishing) ideal of $G_{k,n}$ in S. If Λ is a close subset of $I(k,n)$, then the ideal $I_\Lambda = Q + (P_\gamma : \gamma \in \Lambda)$ generated by Q and the indeterminates corresponding to Λ, is a radical ideal. In particular, the linear section E_Λ is also the scheme-theoretic intersection of $G_{k,n}$ and the linear subvariety defined by the vanishing of the P_γ's for $\gamma \in \Lambda$.*

Proof. The case when Λ is empty is trivial. If $|\Lambda| = 1$, then $E_\Lambda = E_\alpha$ for some $\alpha \in I(k,n)$ and the result follows from Lemma 6.1 and Remark 6.2 (ii). Assume that $|\Lambda| = r \geq 2$. By Theorem 4.2, Λ is of Type I or Type II. If Λ is of Type I, then by suitably permuting the basis elements $v(1), \dots, v(n)$ of F^n [which, as in Remark 6.2 (i), would give a collineation of $\mathbb{P}_F^{N-1}$ leaving $G_{k,n}(F)$ invariant; or algebraically, an automorphism of S which leaves Q invariant], we may assume that Λ equals

$$\Lambda_{\mathrm{I}} = \{(n-k+1-j, n-k+2, n-k+3, \dots, n) : 0 \leq j \leq r-1\}.$$

On the other hand, if Λ is of Type II, then a suitable permutation of the basis elements would permit us to assume that Λ equals

$$\Lambda_{\mathrm{II}} = \left\{(n-k, n-k+1, \dots, \widehat{n-k+j}, \dots, n) : 0 \leq j \leq r-1\right\},$$

where $\widehat{n-k+j}$ indicates that $n-k+j$ is deleted. Note that both Λ_{I} and Λ_{II} are *upwards closed* w.r.t the Bruhat order in the sense that if U denotes any one of them, then

$$\alpha' \in U,\ \beta' \in I(k,n) \text{ and } \alpha' \leq \beta' \Longrightarrow \beta' \in U.$$

Therefore from [34, Thm. 4.4], it follows that I_Λ is a radical ideal. ∎

We shall now show how one can quickly obtain some interesting geometric information about some of the linear sections E_Λ if we use the results of Section 3 together with powerful results in Algebraic Geometry for varieties over finite fields. For simplicity, we shall assume henceforth that the ground field F is an algebraic closure of a finite field $\mathbb{F}_q$ of characteristic p. It is clear of course that all the varieties considered in this section (such as $E_\Lambda(F)$) are defined over $\mathbb{F}_q$ or for that matter over the prime subfield $\mathbb{F}_p$. Now that F is fixed, we may simply write $G_{k,n}$, E_α, etc., in place of $G_{k,n}(F)$, $E_\alpha(F)$, etc., in the remainder of this section.

We state below a weak version of the Grothendieck-Lefschetz Trace Formula, coupled with Deligne's Main Theorem concerning the so called Riemann hypothesis for varieties over finite fields.

THEOREM 6.4. *Let X be a projective algebraic variety defined over $\mathbb{F}_q$, and let $\bar{X} = X \otimes F$ denote the corresponding variety over the algebraic closure F of $\mathbb{F}_q$. Let $\dim \bar{X} = d$. Then there exist integers b_i, for $0 \le i \le 2d$, and algebraic integers ω_{ij}, for $0 \le i \le 2d$, $1 \le j \le b_i$, such that*

$$|\omega_{ij}| \le q^{i/2} \quad \text{for } 0 \le i \le 2d,\ 1 \le j \le b_i,$$

and for any $m \ge 1$, we have

$$|X(\mathbb{F}_{q^m})| = \sum_{i=0}^{2d} (-1)^i \sum_{j=1}^{b_i} \omega_{ij}^m\,;$$

in particular,

$$|X(\mathbb{F}_{q^m})| \le \sum_{i=0}^{2d} b_i (q^m)^{i/2}.$$

Further, if $\bar{X}$ is irreducible, then for any $m \ge 1$, we have

$$|X(\mathbb{F}_{q^m})| \;=\; (q^m)^d + \sum_{i=0}^{2d-1} (-1)^i \sum_{j=1}^{b_i} \omega_{ij}^m \;\le\; (q^m)^d + \sum_{i=0}^{2d-1} b_i (q^m)^{i/2}.$$

REMARK 6.5. The numbers ω_{ij} are the eigenvalues of the (geometric) Frobenius endomorphism on the étale cohomology spaces $H^i(\bar{X}) = H^i(\bar{X}, \mathbb{Q}_\ell)$ of $\bar{X}$, where ℓ is a prime different from p. The assertion about the absolute values of ω_{ij} may be stated more precisely by saying that each ω_{ij} is pure of weight $\le i/2$. Recall that a number $\omega \in \overline{\mathbb{Q}}_\ell$ is said to be *pure* of weight r if ω is an algebraic integer and $|\iota(\omega)| = q^{r/2}$ for any embedding ι of $\overline{\mathbb{Q}}_\ell$ in $\mathbb{C}$. And $H^i(\bar{X})$ is said to be *pure* of weight i if all the eigenvalues of the Frobenius endomorphism on $H^i(\bar{X})$ are pure of weight i. It is known that if X is nonsingular, then each $H^i(\bar{X})$ is pure of weight i. For a more general and more detailed description of the above Theorem, see [14], [32], and/or the original sources referred therein.

COROLLARY 6.6. *Let X be a projective algebraic variety defined over $\mathbb{F}_q$, and let $\bar{X} = X \otimes F$ denote the corresponding variety over F. If $\dim \bar{X} = d$,* *then the limit*

$$\lim_{m\to\infty} \frac{|X(\mathbb{F}_{q^m})|}{q^{md}}.$$

exists and is equal to the number of irreducible components of $\bar{X}$ *of dimension* d.

Proof. Let

$$\bar{X} = Y_1 \cup \ldots \cup Y_b \cup Y_{b+1} \cup \ldots \cup Y_{b+c}$$

be an irredundant decomposition of $\bar{X}$ into irreducible subvarieties, where $Y_1, \ldots, Y_b$ are of dimension d and $Y_{b+1}, \ldots, Y_{b+c}$ are of dimension $< d$. Since the decomposition is irredundant, it follows that for $r > 1$ and $1 \leq i_1 < \ldots < i_r \leq b + c$, the intersection $Y_{i_1} \cap \cdots \cap Y_{i_r}$ is of dimension $< d$. Now by Proposition 2.3, we see that $|X(\mathbb{F}_{q^m})|$ equals

$$\sum_{i=1}^{b} |Y_i(\mathbb{F}_{q^m})| + \sum_{j=1}^{c} |Y_{b+j}(\mathbb{F}_{q^m})| - \sum_{1\leq i<j\leq b+c} |Y_i(\mathbb{F}_{q^m}) \cap Y_j(\mathbb{F}_{q^m})| + \cdots.$$

Dividing by q^{md} and taking limit as $m \to \infty$, the desired result follows readily from Theorem 6.4. ▮

Remark 6.7. As noted in [14, Proof of Prop. 3.3], we have, in general, that for any scheme X of dimension d, the number of irreducible components of dimension d is equal to the dimension of the $(2d)$-th étale cohomology space of $\bar{X}$.

Theorem 6.8. *Suppose* $1 < k < n-1$. *Let* $\Lambda \subseteq I(k,n)$ *be a family such that* $|\Lambda| \geq 2$. *Then we have the following.*

(i) *If* Λ *is close, then* $\dim E_\Lambda = \delta - 2$.

(ii) *If* Λ *is close and* $|\Lambda| = 2$, *then* E_Λ *has exactly two irreducible components of dimension* $\delta - 2$,

(iii) *If* Λ *is close and* $|\Lambda| > 2$, *then* E_Λ *has exactly one irreducible component of dimension* $\delta - 2$.

(iv) *If* Λ *is not close and* $|\Lambda| = 2$, *then* E_Λ *has exactly one irreducible component of dimension* $\delta - 2$.

Proof. Let $r = |\Lambda|$. Since $r \geq 2$, we can find two distinct elements α and β in Λ. Assume that either Λ is close or $|\Lambda| = 2$. In case Λ is close, by

Lemma 3.5, we have

$$|E_\Lambda(\mathbb{F}_q)| = \begin{bmatrix} n \\ k \end{bmatrix}_q - q^\delta - q^{\delta-1} - \ldots - q^{\delta-r+1} \tag{3}$$

whereas if Λ is not close and $|\Lambda| = 2$, then $d = k - |\bar{\alpha} \cap \bar{\beta}| > 1$ and by Corollary 3.3, we have

$$|E_{\alpha\beta}(\mathbb{F}_q)| = \begin{bmatrix} n \\ k \end{bmatrix}_q - 2q^\delta + q^{\delta - \binom{d+1}{2}}[d]!. \tag{4}$$

Also recall that by Corollary 3.2, we have

$$|E_\alpha(\mathbb{F}_q)| = \begin{bmatrix} n \\ k \end{bmatrix}_q - q^\delta. \tag{5}$$

Now using the asymptotic description for $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$ as in Section 2, and the asymptotic description for $q^{\delta - \binom{d+1}{2}}[d]!$ appearing in the proof of Proposition 5.3, we see that

$$|E_\Lambda(\mathbb{F}_q)| = bq^{\delta-2} + O\left(q^{\delta-3}\right) \tag{6}$$

where

$$b = \begin{cases} 1 & \text{if } |\Lambda| > 2 \text{ and } \Lambda \text{ is close,} \\ 1 & \text{if } |\Lambda| = 2 \text{ and } \Lambda \text{ is not close,} \\ 2 & \text{if } |\Lambda| = 2 \text{ and } \Lambda \text{ is close.} \end{cases}$$

It is clear that each of the identities (3), (4), (5) and (6) are valid with q replaced by q^m for any $m \geq 1$. Hence we see that E_Λ is a proper subvariety of E_α. By Lemma 6.1, the latter is irreducible of dimension $\delta - 1$, and therefore, if we let $e = \dim E_{\alpha\beta}$, then $e \leq \delta - 2$. Moreover, if $e < \delta - 2$, then from Theorem 6.4 we see that $|E_\Lambda(\mathbb{F}_{q^m})|/q^{me}$ is unbounded as $m \to \infty$. But this contradicts Corollary 6.6. Thus, $e = \delta - 2$. The remaining assertions concerning the number of irreducible components of dimension $\delta - 2$ follow from (6) in view of Corollary 6.6. ▮

In the case of E_Λ, where Λ is close and $|\Lambda| = 2$, we can sharpen the result in Theorem 6.8 (ii) using the following algebro-geometric result. Recall that a projective algebraic variety is said to be *arithmetically Cohen-Macaulay* if its homogeneous coordinate ring is Cohen-Macaulay.

THEOREM 6.9. *Suppose $1 < k < n - 1$. Let $\alpha, \beta \in I(k, n)$ be such that $|\bar{\alpha} \cap \bar{\beta}| = k - 1$. Then the projective variety $E_{\alpha\beta}$ is arithmetically Cohen-Macaulay. In particular, $E_{\alpha\beta}$ is Cohen-Macaulay and equidimensional.*

Proof. Let $\boldsymbol{P} = \{P_\gamma : \gamma \in I(k,n)\}$, $S = F[\boldsymbol{P}]$ and $Q = I(G_{k,n})$ be as in Lemma 6.3. Further, let $I = I(E_\alpha)$ and $J = I(E_{\alpha\beta})$ denote, respectively, the ideals of E_α and $E_{\alpha\beta}$ in S. By Lemma 6.1 and the arithmetic Cohen-Macaulayness of Schubert varieties (cf. [21], [27] or [34]), we see that the homogeneous coordinate ring $A = S/I$ of E_α is a Cohen-Macaulay domain of dimension δ. Moreover, by Theorem 6.8, it follows that the homogeneous coordinate ring $B = S/J$ of $E_{\alpha\beta}$ is of dimension $\delta - 1$. Also, in view of Remark 6.2 (ii), Lemma 6.3 and Hilbert's Nullstellensatz, we have $I = (Q, P_\alpha)$ and $J = (I, P_\beta)$.

The arithmetic Cohen-Macaulayness of the projective variety $E_{\alpha\beta}$ (or equivalently, the Cohen-Macaulayness of S/J) now follows from one of several 'routine' arguments using the fact that S/I is Cohen-Macaulay, $J = (I, P_\beta)$ and $\dim S/J = \dim S/I - 1$. We outline below one such argument for the sake of completeness. Let h_β denote the image of P_β in $A = S/I$. Then $B = S/J$ is isomorphic to $\bar{A} = A/(h_\beta)$. Now let $\mathfrak{m}$ be a maximal ideal of A containing h_β and $\overline{\mathfrak{m}}$ be the corresponding maximal ideal of $\bar{A}$. Since A is Cohen-Macaulay, it is universally catenary (cf. [30, Thm. 33]), and thus (using, for example, the observations in [30, Sec. 14.B]), it follows that the localizations $A_\mathfrak{m}$ and $\bar{A}_{\overline{\mathfrak{m}}}$ are of dimensions δ and $\delta - 1$ respectively and the former is Cohen-Macaulay. In particular, h_β is a regular element in $A_\mathfrak{m}$ and by [30, Thm. 30], it can be extended to a maximal regular sequence $h_\beta, f_2, \ldots, f_\delta$ of $A_\mathfrak{m}$. Consequently, $\bar{f}_2, \ldots, \bar{f}_\delta$ is a regular sequence of $\bar{A}_{\overline{\mathfrak{m}}}$. Therefore $\bar{A}_{\overline{\mathfrak{m}}}$ is Cohen-Macaulay. This shows that $E_{\alpha\beta}$ is arithmetically Cohen-Macaulay. The remaining assertions are consequences of standard facts in Commutative Algebra (see, for example, [30, Sec. 16]). ∎

REMARK 6.10. The irreducibility and arithmetic Cohen-Macaulayness of E_α can also be derived using arguments similar to those in the proofs of Theorem 6.8 and Theorem 6.9. In other words, we can first use Corollary 3.2 and Theorem 6.4 to determine the dimension and the number of top-dimensional irreducible components of E_α, and secondly, we can use the connection with Schubert varieties [in effect, just the 'Basis Theorem'] only to the extent of deducing the observation in Remark 6.2 (ii) that the ideal of E_α in R is (t_α). In this way, one can avoid Lemma 6.1 and using some results from [21], [27] or [34].

COROLLARY 6.11. *Suppose $1 < k < n - 1$. Let $\alpha, \beta \in I(k,n)$ be such that $|\bar{\alpha} \cap \bar{\beta}| = k - 1$. Then the projective variety $E_{\alpha\beta}(F)$ has exactly two irreducible components, each of dimension $\delta - 2$.*

Proof. Follows from Theorem 6.8 and Theorem 6.9. ∎

It turns out that the results of Section 3 can be used not only to get information about the dimension of the hyperplane sections E_Λ and of their irreducible components, but also to derive interesting facts concerning the singularities of these hyperplane sections. To this end, we shall use the following result, which is proved in [25, Prop. 3.2]. We use this opportunity to remark a small correction in [25, Prop. 3.2], namely that $\#X_{Z(f)}(\mathbb{F}_q)$ should be replaced by $q\,\#X_{Z(f)}(\mathbb{F}_q)$ on two occasions in the statement of the said proposition. Indeed, the proof of [25, Prop. 3.2] is valid only if this correction is made.

PROPOSITION 6.12. *Let X be an irreducible projective variety in $\mathbb{P}_F^{N-1}$ of dimension d defined over $\mathbb{F}_q$, f be a homogeneous polynomial in N variables with coefficients in $\mathbb{F}_q$, H be subscheme of $\mathbb{P}_F^{N-1}$ corresponding to the principal ideal generated by f, and let E^* be the scheme-theoretic intersection of X and H. Let $\sigma(f) = \dim \operatorname{Sing} E^*$ denote the dimension of the singular locus of E^* and let E be the algebraic set (i.e., the reduced subscheme) associated to E^*. Then there exists a constant $B_0 = B_0(f, X)$, independent of q such that*

$$\Big| q|E(\mathbb{F}_q)| - |X(\mathbb{F}_q)| \Big| \leq B_0(f, X) q^{(d+\sigma(f)+2)/2}.$$

REMARK 6.13. From Lemma 6.3 and the proof of Theorem 6.9, it is clear that if $\{\alpha, \beta\}$ is close, then the scheme theoretic intersection of E_α with the hyperplane H_β corresponding to the ideal (P_β) is reduced and equals $E_{\alpha\beta}$.

COROLLARY 6.14. *Given any $\alpha \in I(k,n)$, we have* $\dim \operatorname{Sing} E_\alpha \geq \delta - 4$, *or equivalently, the codimension of* $\operatorname{Sing} E_\alpha$ *in* E_α *is* ≤ 3.

Proof. The case when $k = 1$ or $k \geq n-1$ is trivial. Thus we may assume that $1 < k < n$. From Corollary 3.2 and the asymptotic description for $\begin{bmatrix} n \\ k \end{bmatrix}_q$ given in Section 2, we have

$$|E_\alpha(\mathbb{F}_q)| = \begin{bmatrix} n \\ k \end{bmatrix}_q - q^\delta = q^{\delta-1} + 2q^{\delta-2} + O\left(q^{\delta-3}\right).$$

Applying Proposition 6.12 with $X = G_{k,n}(F)$ and $f = P_\alpha$ and noting that

$$q\left(q^{\delta-1} + 2q^{\delta-2} + \cdots\right) - \left(q^\delta + q^{\delta-1} + 2q^{\delta-2} + \cdots\right) = q^{\delta-1} + O\left(q^{\delta-2}\right),$$

we get $\delta - 1 \leq (\delta + \sigma(f) + 2)/2$, which implies that $\sigma(f) \geq \delta - 4$. Hence from Lemma 6.1 and the fact that E_α is reduced (cf. Remark 6.2 (ii)), it follows that $\operatorname{codim} \operatorname{Sing} E_\alpha \leq 3$. ▮

Remark 6.15. In fact, a more precise result than that given by the above Corollary is known. Indeed, by Lemma 6.1, we know that E_α is isomorphic to the Schubert variety $\Omega_\eta(F)$ in $G_{k,n}(F)$, where $\eta = (n-k, n-k+2, \ldots, n-1, n)$, Now, thanks to the work of Lascoux [28], Svanes [43], and Lakshmibai-Weymann [26], the structure of the singular locus of all Schubert varieties in Grassmannians is well understood. Thus, for example, from [26, Thm. 5.3], we can easily see that $\operatorname{Sing} \Omega_\eta(F) = \Omega_{\eta'}(F)$, where $\eta' = (n-k-1, n-k, n-k+3, \ldots, n-1, n)$. In particular, from the dimension formula noted at the beginning of this section and in view of the proof of Lemma 6.1, we obtain that $\dim \operatorname{Sing} E_\alpha = \dim \Omega_{\eta'}(F) = 2(n-k-2) + (k-2)(n-k) = \delta - 4$, and thus $\operatorname{codim} \operatorname{Sing} E_\alpha = 3$. This shows, in particular, that E_α has no singularities in codimension 1, and since, as noted in the proof of Theorem 6.9, it is Cohen-Macaulay, it follows from Serre's criterion of normality, that E_α is a normal variety. It may be remarked that the normality of arbitrary Schubert varieties is known in general from the work of Andersen [2], Ramanan-Ramanathan [37] and Seshadri [40] (see also [31] for a short proof). However, in the case of more general hyperplane sections E_Λ, which may not be Schubert varieties, very little seems to be known in the literature. In the case of $E_{\alpha\beta}$, where $\{\alpha, \beta\}$ is close, the following Corollary gives some results that our methods would yield.

Corollary 6.16. *Suppose* $1 < k < n-1$. *Let* $\alpha, \beta \in I(k,n)$ *be such that* $|\bar{\alpha} \cap \bar{\beta}| = k-1$. *Then* $\dim \operatorname{Sing} E_{\alpha\beta} = \delta - 3$, *or equivalently, the codimension of* $\operatorname{Sing} E_{\alpha\beta}$ *in* $E_{\alpha\beta}$ *is* 1. *In particular,* $E_{\alpha\beta}$ *is not a normal variety.*

Proof. By Lemma 6.1 we know that E_α is an irreducible projective variety with $\dim E_\alpha = \delta - 1$. Now in view of Corollary 3.2 and Corollary 3.3, by applying Proposition 6.12 with $X = E_\alpha$ and $f = P_\beta$ it follows that there is a constant B_0 independent of q such that

$$\left| q\left(2q^{\delta-2} + \cdots\right) - \left(q^{\delta-1} + 2q^{\delta-2} + \cdots\right) \right| \leq B_0 q^{(\delta-1+\sigma(f)+2)/2}.$$

Consequently, $\delta - 1 \leq (\delta + \sigma(f) + 1)/2$, and therefore $\sigma(f) \geq \delta - 3$. On the other hand, by Remark 6.13, the scheme theoretic intersection $E^*_{\alpha\beta}$ of E_α and the hyperplane H_β corresponding to (P_β) is reduced, and thus it has no singularities in codimension 0 (see, for example, [11, Ex. 11.10, p. 266]). Hence $E^*_{\alpha\beta} = E_{\alpha\beta}$ and $\sigma(f) \leq \dim E_{\alpha\beta} - 1 = \delta - 3$. Thus $\operatorname{codim} \operatorname{Sing} E_{\alpha\beta} = 1$. Now since $E_{\alpha\beta}$ has singularities in codimension 1, Serre's criterion of normality implies that it can not be a normal variety. ▌

In contrast to the linear section $E_{\alpha\beta}$ by a close family of two coordinate hyperplanes, we shall show that in the case of families $\{\alpha, \beta\}$ which are not close, the variety $E_{\alpha\beta}$ is much better behaved.

THEOREM 6.17. *Suppose $1 < k < n-1$. Let $\alpha, \beta \in I(k,n)$ be such that $|\bar{\alpha} \cap \bar{\beta}| < k-1$. Let H_β denote the hyperplane in $\mathbb{P}_F^{N-1}$ defined by $\{P_\beta = 0\}$, and let $E^*_{\alpha\beta}$ denote the scheme theoretic intersection of E_α and H_β. Then we have the following.*

(i) $\dim \operatorname{Sing} E^*_{\alpha\beta} \geq \delta - 5$. *In other words,* $\operatorname{codim} \operatorname{Sing} E^*_{\alpha\beta} \leq 3$.

(ii) *$E^*_{\alpha\beta}$ is arithmetically Cohen-Macaulay. In particular, it is Cohen-Macaulay and equidimensional.*

(iii) *$E_{\alpha\beta}$ is an irreducible variety.*

Proof. To prove (i), we proceed as in the proof of Corollary 6.16. Thus, we first note that E_α is irreducible of dimension $\delta - 1$. Now, using Corollary 3.2, Corollary 3.3, the asymptotic description for $q^{\delta - \binom{d+1}{2}}[d]!$ appearing in the proof of Proposition 5.3, and Proposition 6.12, we see that there is a constant B_0 independent of q such that

$$\left| q\left(q^{\delta-2} + 3q^{\delta-3} + \cdots\right) - \left(q^{\delta-1} + 2q^{\delta-2} + \cdots\right) \right| \leq B_0 q^{(\delta-1+\sigma(f)+2)/2}.$$

Consequently, $\delta - 2 \leq (\delta + \sigma(f) + 1)/2$, and therefore $\sigma(f) \geq \delta - 5$. Next, to prove (ii), we let $S = F[\boldsymbol{P}]$ and Q be as in Lemma 6.3 so that $R = S/Q$ is the homogeneous coordinate ring of $G_{k,n}$. Write $R = F[\boldsymbol{t}]$, where $\boldsymbol{t} = \{t_\gamma : \gamma \in I(k,n)\}$ and t_γ denotes the image of P_γ in R. Let J^* be the ideal of R generated by t_α and t_β. Since E_α and H_β are both reduced, it follows that the homogeneous coordinate ring of $E^*_{\alpha\beta}$ is isomorphic to R/J^*. Since J^* and $\sqrt{J^*}$ have the same set of minimal primes, it follows from Hilbert's Nullstellensatz that $\dim E^*_{\alpha\beta} = \dim E_{\alpha\beta} = \delta - 2$. Now R is Cohen-Macaulay (cf. [21]) and J^* is an ideal of codimension 2 and is generated by two elements. Hence, by [11, Prop. 18.13], we can conclude that R/J^* is Cohen-Macaulay. This proves (ii). In particular $E^*_{\alpha\beta}$ is equidimensional. But we know from Theorem 6.8 (iv) that $E_{\alpha\beta}$ has exactly one irreducible component of dimension $\delta - 2$. This implies that $\sqrt{J^*}$ is prime and thus $E_{\alpha\beta}$ is irreducible. ▌

REMARK 6.18. It appears likely that if $\{\alpha, \beta\} \subseteq I(k,n)$ is not close, then $E^*\alpha\beta$ is reduced (so that $E^*_{\alpha\beta} = E_{\alpha\beta}$) and $\dim \operatorname{Sing} E_{\alpha\beta} = \delta - 5$; this would then imply that $E_{\alpha\beta}$ is Cohen-Macaulay and normal. In any case, it is clear already that the geometry of $E_{\alpha\beta}$ seems to depend a lot on the combinatorial condition as to whether or not $\{\alpha, \beta\}$ is close.

Examples 6.19. Finally, in this section, we work out two examples, which nicely illustrate some of the results proved above.

1. Consider $G_{2,4}$, which is the simplest nontrivial Grassmannian. This is a hypersurface in $\mathbb{P}^5$ of dimension $\delta = 4$ and is defined by the equation

$$P_{12}P_{34} - P_{13}P_{24} + P_{14}P_{23} = 0.$$

Suppose $\alpha = (1,2)$. Then $E_\alpha = G_{2,4} \cap \{P_{12} = 0\}$ is like a projective cylinder over the affine cone defined by an equation of the form $xw - yz = 0$. Thus E_α is clearly irreducible of dimension 3; indeed, the ideal of E_α is like the principal ideal $(xw - yz)$ in the polynomial ring $F[x,y,z,w,u]$, and this ideal is clearly a prime ideal of height 1. Moreover the point defined by $P_{12} = P_{13} = P_{24} = P_{14} = P_{23} = 0$ and $P_{34} = 1$ is the only singular point of E_α and thus $\dim \operatorname{Sing} E_\alpha = 0$ as is to be expected. Next, if $\beta = (1,3)$, then $\{\alpha, \beta\}$ is a close family and $E_{\alpha\beta}$ is the union of the two planes Π_1 and Π_2 defined by $P_{12} = P_{13} = P_{14} = 0$ and $P_{12} = P_{13} = P_{23} = 0$ respectively. So, $\dim E_{\alpha\beta} = 2$ and $E_{\alpha\beta}$ has two irreducible components of dimension 2. Moreover, the singular locus of $E_{\alpha\beta}$ is the line formed by the intersections of Π_1 and Π_2. Thus $\dim \operatorname{Sing} E_{\alpha\beta} = 1$, as is to be expected. Finally, if $\gamma = (1,4)$, then $\Lambda = \{\alpha, \beta, \gamma\}$ is a close family of maximum possible cardinality and the corresponding E_Λ is isomorphic to $\mathbb{P}^2$ so that it is irreducible of dimension $\delta - 2$. It may be noted that if we take a family such as $\Lambda' = \{(1,2),(1,3),(3,4)\}$, which is not close, then $E_{\Lambda'}$ is isomorphic to a union of two $\mathbb{P}^1$'s and thus it is reducible of dimension $< \delta - 2$. On the other hand, if we let $\theta = (3,4)$ and we take the 2-element family $\{\alpha, \theta\}$, which is not close then $E_{\alpha\theta}$ is the determinantal hypersurface in $\mathbb{P}^4$ given by an equation of the form $xw - yz = 0$. Thus $E_{\alpha\theta}$ is irreducible (and Cohen-Macaulay) of dimension 2.

2. Consider $G_{2,5}$, which is a subvariety of $\mathbb{P}^9$ of dimension $\delta = 6$. It is not difficult to see that the following 5 quadratic relations determine $G_{2,5}$.

$$\begin{aligned}
P_{12}P_{34} - P_{13}P_{24} + P_{14}P_{23} &= 0;\\
P_{12}P_{45} - P_{14}P_{25} + P_{15}P_{24} &= 0;\\
P_{12}P_{35} - P_{13}P_{25} + P_{15}P_{23} &= 0;\\
P_{13}P_{45} - P_{14}P_{35} + P_{15}P_{34} &= 0;\\
P_{23}P_{45} - P_{24}P_{35} + P_{25}P_{34} &= 0.
\end{aligned}$$

Suppose $\alpha = (1,2)$ and $\beta = (1,3)$. Consider $E_{\alpha\beta} = G_{2,5} \cap \{P_{12} = P_{13} = 0\}$. Then from the above quadratic relations, we see that for any $p \in E_{\alpha\beta}$, we must have $p_{23} = 0$ or $p_{14} = p_{15} = 0$. It follows that $E_{\alpha\beta} = V^{(1)} \cup V^{(2)}$ where $V^{(1)}$ and $V^{(2)}$ are subvarieties of $\mathbb{P}^9$ defined by

$$V^{(1)} = \{P_{12} = P_{13} = P_{14} = P_{15} = 0 = P_{23}P_{45} - P_{24}P_{35} + P_{25}P_{34}\}$$

and

$$\begin{aligned} V^{(2)} = \{P_{12} = P_{13} = P_{23} = 0 \ &= P_{14}P_{25} - P_{15}P_{24} \\ &= P_{14}P_{35} - P_{15}P_{34} = P_{24}P_{35} - P_{25}P_{34}\}. \end{aligned}$$

It is clear that $V^{(1)}$ is isomorphic to $G_{2,4}$ and thus it is irreducible of dimension 4. Further, $V^{(2)}$ is isomorphic to a cylinder [since P_{45} is free] over a determinantal variety in $\mathbb{P}^5$ defined by an ideal of the form

$$I_2\left(\begin{bmatrix} x & y & z \\ u & v & w \end{bmatrix}\right)$$

that is generated by the 2×2 minors of a generic 2×3 matrix. It is well-known (cf. [8, Prop. 1.1]) therefore that the projective variety in $\mathbb{P}^5$ corresponding to the ideal above is irreducible and has dimension $4 - 1 = 3$. Therefore, $V^{(2)}$ is also irreducible, and $\dim V^{(2)} = 3 + 1 = 4$. So, the assertions (i) and (ii) of Theorem 6.8 are verified. Next, let $\gamma = (1,4)$, and consider $E_{\alpha\beta\gamma}$. As in the case of $E_{\alpha\beta}$, we can easily see that for any $p \in E_{\alpha\beta\gamma}$, we must have $p_{15} = 0$ or $p_{23} = p_{24} = p_{25} = 0$. It follows that $E_{\alpha\beta\gamma}$ is the union of two subvarieties, one isomorphic to $G_{2,4}$ and the other isomorphic to $\mathbb{P}^3$. It may be noted that in this case $E_{\alpha\beta\gamma}$ is reducible of dimension 4 but it has only one irreducible component of dimension 4. Finally, consider $\Lambda = \{(1,2), (1,3), (1,4), (1,5)\}$, which is a close family of maximum possible cardinality. Then E_Λ is isomorphic to $G_{2,4}$, which is irreducible of dimension 4.

Note that if in $G_{2,5}$, we consider a 2-element family which is not close such as $\{\alpha, \theta\}$, where $\theta = (3,4)$, then, the corresponding $E_{\alpha\theta}$ turns out to be a projective variety in $\mathbb{P}^8$ defined by an ideal of the form

$$I_2\left(\begin{bmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & \end{bmatrix}\right)$$

that is generated by the 2×2 minors of a ladder shaped subset of a generic 3×3 matrix. It may be remarked that such *ladder determinantal varieties* have recently been of interest and one knows that in general, they are irreducible (cf. [1, Thm. 20.16.4]), arithmetically Cohen-Macaulay (cf.

[18, Cor. 4.10]) and projectively normal (cf. [10, Prop. 3.3]). Also, from [18, Cor. 4.7] it can be seen that the dimension of $E_{\alpha\theta}$ is 4. This confirms some of the results of Theorem 6.8 and Theorem 6.17 in the particular case of the linear section $E_{\alpha\theta}$ of $G_{2,5}$.

We remark that the above decompositions of $E_{\alpha\beta}$ (say) into irreducible components can be used to compute directly the number of $\mathbb{F}_q$-rational points of $E_{\alpha\beta}$. It is interesting and instructive, especially in the second example, to do so and compare with the formula given by Corollary 3.3.

7. TABLES

In this section, we give some numerical data to compare, wherever possible, the lower bound $L(q) = L(q; k, n)$ and the upper bound $U(q) = U(q; k, n)$ for the number $\gamma(q) = \gamma(q; k, n)$ of all (n, k)-MDS linear codes over $\mathbb{F}_q$. It will be seen that the bounds quickly become better as q increases. Of course, the MDS codes may not always exist for a given set of parameters and in such a case the lower bound $L(q)$ is usually negative. In fact, we can easily avoid these negative values and, in view of Remark 5.9, also make a minor improvement in the upper bound $U(q)$ by replacing $L(q)$ and $U(q)$ by $\hat{L}(q)$ and $\hat{U}(q)$, respectively, where the latter are defined by $\hat{L}(q) = \max\{L(q),\ 0\}$ and $\hat{U}(q) = \min\{U(q),\ q^{\delta}\}$. However, in practice $L(q)$ quickly becomes positive and $U(q)$ quickly becomes smaller than q^{δ}.

		$(n, k) = (5, 2)$
$q = 2$	$L(q) =$	-755
	$\gamma(q) =$	0
	$U(q) =$	155
$q = 8$	$L(q) =$	-116945
	$\gamma(q) =$	72030
	$U(q) =$	250180
$q = 32$	$L(q) =$	752269015
	$\gamma(q) =$	803463270
	$U(q) =$	834446500
$q = 128$	$L(q) =$	4083938982775
	$\gamma(q) =$	4097278095750
	$U(q) =$	4104293323300
$q = 512$	$L(q) =$	17696499789458935
	$\gamma(q) =$	17699930414237190
	$U(q) =$	17701667866691620
$q = 2048$	$L(q) =$	73462400307624392695
	$\gamma(q) =$	73463279573643761670
	$U(q) =$	73463720623898435620
$q = 8192$	$L(q) =$	301899332435640416395255
	$\gamma(q) =$	301899557593636585365510
	$U(q) =$	301899670263342869807140

		$(n,k)=(6,2)$
$q=2$	$L(q)=$	-5274
	$\gamma(q)=$	0
	$U(q)=$	651
$q=32$	$L(q)=$	587426008626
	$\gamma(q)=$	697406118360
	$U(q)=$	773487190971
$q=512$	$L(q)=$	4592733883143010903026
	$\gamma(q)=$	4594689536371003677720
	$U(q)=$	4595715252586834081371
$q=8192$	$L(q)=$	20247738819037735639138726461426
	$\gamma(q)=$	20247771753930719892728171053080
	$U(q)=$	20247788696637052969529490759771

		$(n,k)=(6,3)$
$q=2$	$L(q)=$	-16265
	$\gamma(q)=$	0
	$U(q)=$	1395
$q=32$	$L(q)=$	12924803540365
	$\gamma(q)=$	18854872557090
	$U(q)=$	23274288377355
$q=512$	$L(q)=$	2327775159087185688779245
	$\gamma(q)=$	2329516639604540539808130
	$U(q)=$	2330369613207389653784235
$q=8192$	$L(q)=$	165768039589972820570950606406918125
	$\gamma(q)=$	165768509822290080011242807140458370
	$U(q)=$	165768733035888981455839539456467115

		$(n,k) = (7,3)$
$q = 2$	$L(q) =$	-258214
	$\gamma(q) =$	0
	$U(q) =$	11811
$q = 128$	$L(q) =$	14123647489168989269978846
	$\gamma(q) =$	14763973216014483920056080
	$U(q) =$	15093570758315423135537841
$q = 2048$	$L(q) =$	5354042033282754906723825686066392657886
	$\gamma(q) =$	5354784455399714241650925286098021465360
	$U(q) =$	5355088314817274002456447976702416620081

		$(n,k) = (8,3)$
$q = 2$	$L(q) =$	-3508517
	$\gamma(q) =$	0
	$U(q) =$	97155
$q = 128$	$L(q) =$	22859051508168206183682487379017
	$\gamma(q) =$	26143755283265696967345957437040
	$U(q) =$	27818370911486822148299133905997
$q = 512$	$L(q) =$	38858929850431024228647936374271440818633
	$\gamma(q) =$	39096878508416888436124942798204100945520
	$U(q) =$	39186366672436705546578090425688010235853

		$(n,k) = (9,3)$
$q = 2$	$L(q) =$	-43386809
	$\gamma(q) =$	0
	$U(q) =$	788035
$q = 128$	$L(q) =$	29035501732844392930104338279237572141
	$\gamma(q) =$	43680038826242120201491233198224596320
	$U(q) =$	51566850324744464560126628177426264779

We can also consider the case when $(n,k) = (10,3)$, where no exact formula is known but the lower and upper bounds can still be computed. If we compute these as q runs over powers of 2, we don't get any interesting information till $q = 64$ because for $q \leq 32$, $L(q)$ is negative while $U(q)$ is positive. Later, however $L(q)$ is a fairly large positive integer, and, the difference between $L(q)$ and $U(q)$ becomes relatively small. For instance, the first four digits of $L(q)$ and $U(q)$ are identical, for $q = 2048$. This time we avoid making a table since the numbers involved are quite huge.

Finally, we remark that the tables above have been prepared using MATHEMATICA. A more extensive data is also available. Anyone interested in this data and/or a copy of the relevant MATHEMATICA programs, may send an e-mail to the first author.

ACKNOWLEDGMENT

This research was partly supported by the Indo-French Mathematical Research Program of the Centre National de la Recherche Scientifique (CNRS) of France and the National Board for Higher Mathematics (NBHM) of India, and we thank these organizations for their support. We would also like to express our warm gratitude to Robert Rolland, Alexeï Skorobogatov, Murali Srinivasan and Michael Tsfasman for a number of helpful discussions, and to Sameer D'Costa for writing the Mathematica programs to generate the tables in Section 7.

REFERENCES

1. S. S. Abhyankar, "Enumerative Combinatorics of Young Tableaux", Marcel Dekker, New-York, 1988.
2. H. H. Andersen, Schubert varieties and Demazure's character formula, *Invent. Math.* **79** (1985), 611–618.
3. G. E. Andrews, "Theory of Partitions", Encyclopedia of Mathematics and its Applications, Vol. 2, Addison-Wesley, Reading, Mass., 1976.
4. B. Bollobás, "Combinatorics : set systems, hypergraphs, families of vectors, and combinatorial probability", Cambridge Univ. Press, Cambridge, 1986.
5. R. Bott and L. W. Tu, "Differential forms in Algebraic Topology", Springer-Verlag, New York, 1980.
6. A. Blokhuis, A. A. Bruen and J. A. Thas, Arcs in $PG(n,q)$, MDS-codes, and three fundamental problems of B. Segre—some extensions, *Geom. Dedicata* **35** (1991), 1–11.
7. A. A. Bruen, J. A. Thas and A. Blokhuis, On M.D.S. codes, arcs in $PG(n,q)$ with q even, and a solution of three fundamental problems of B. Segre, *Invent. Math.* **92** (1988), 441–459.
8. W. Bruns and U. Vetter, "Determinantal Rings", Lecture Notes in Math., Vol. 1327, Springer-Verlag, Berlin, 1988.
9. L. Comtet, "Advanced Combinatorics", D. Reidel, Dordrecht-Holland, 1974.
10. A. Conca, Ladder determinantal rings, . *J. Pure and Appl. Algebra* **98** (1995), 119–134.

11. D. Eisenbud, "Commutative Algebra with a view towards Algebraic Geometry", Grad. Texts in Math., Vol. 150, Springer-Verlag, New-York, 1995.
12. S. R. Ghorpade, Young multitableaux and higher dimensional determinants, *Adv. Math.* **121** (1996), 167–195.
13. S. R. Ghorpade and G. Lachaud, Higher weights of Grassmann codes, *in* "Coding Theory, Cryptography and Related Areas" (J. Buchmann, T. Hoeholdt, H. Stichtenoth, H. Tapia-Recillas, Eds.), pp. 122-131, Springer-Verlag, Berlin/Heidelberg, 2000.
14. S. R. Ghorpade and G. Lachaud, Étale cohomology, Lefschetz theorems, and number of points of singular varieties over finite fields, Prétirage n° 99-13 (45 pp.), Institut de Mathématiques de Luminy, Marseille, France, 1999.
15. D. Glynn, Rings of geometries, II, *J. Combin. Theory Ser. A* **49** (1988), 26–66.
16. J. M. Goethals, A polynomial approach to linear codes, *Philips Research Reports* **24** (1969), 145–159.
17. J. Goldman and G.-C. Rota, 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.
18. J. Herzog and N. V. Trung, Gröbner bases and multiplicity of determinantal and pfaffian ideals, *Adv. Math.* **96** (1992), 1–37.
19. J. W. P. Hirschfeld and J. A. Thas, "General Galois Geometries", Oxford Univ. Press, Oxford, 1991.
20. J. W. P. Hirschfeld, M. A. Tsfasman, and S. G. Vlăduţ, The weight hierarchy of higher-dimensional Hermitian codes, *IEEE Trans. Inform. Theory* **40** (1994), 275–278.
21. M. Hochster, Grassmannians and their Schubert subvarieties are arithmetically Cohen-Macaulay, *J. Algebra* **25** (1973), 40–57.
22. W. V. D. Hodge and D. Pedoe, "Methods of Algebraic Geometry, Vol. II", Cambridge Univ. Press, Cambridge, 1952.
23. A. I. Iampolskaia, A. N. Skorobogatov, and E. A. Sorokin, Formula for the number of $[9,3]$ MDS codes, *IEEE Trans. Inform. Theory* **41** (1995), 1667–1671.
24. S. L. Kleiman and D. Laksov, Schubert Calculus, *Amer. Math. Monthly* **79** (1972), 1061–1082.
25. G. Lachaud, Number of points of linear codes defined on algebraic varieties, *in* "Arithmetic, Geometry and Coding theory" (R. Pellikan, M. Perret, S. G. Vlăduţ, Eds.), pp. 77–104, Walter de Gruyter, Berlin/New York, 1996.
26. V. Lakshmibai and J. Weyman, Multiplicity of points on a Schubert variety in a miniscule G/P, *Adv. Math.* **84** (1990), 179–208.
27. D. Laksov, The arithmetic Cohen-Macaulay character of Schubert schemes, *Acta. Math.* **129** (1972), 1–9.
28. A. Lascoux, "Polynôme symétriques, Foncteurs de Schur et Grassmanniennes", Thèse, Université de Paris VII, 1977.
29. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error Correcting Codes", North Holland, Amsterdam, 1977.
30. H. Matsumura, "Commutative Algebra", 2nd Ed., Benjamin/Cummings, Reading, Mass., 1980.
31. V. B. Mehta and V. Srinivas, Normality of Schubert varieties, *Amer. J. Math.* **109** (1987), 987–989.

32. J. S. Milne, "Étale cohomology", Princeton Math. Series vol. 33, Princeton University Press, Princeton, 1980.

33. N. E. Mnëv, On manifolds of combinatorial types of projective configurations and convex polytopes, *Soviet Math. Doklady* **32:1** (1985), 335–337.

34. C. Musili, Postulation formula for Schubert varieties, *J. Indian Math. Soc.* **36** (1972), 143–171.

35. D. Yu. Nogin, 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.

36. U. Oberst and A. Dür, A constructive characterization of all optimal linear codes, *in*, "Seminaire d'Algebre" (P. Dubriel, M. P. Malliavin, Eds.), Lecture Notes in Math., Vol. 1146, pp. 176–213, Springer–Verlag, Berlin, 1985.

37. S. Ramanan and A. Ramanathan, Projective normality of flag varieties and Schubert varieties, *Invent. Math.* **79** (1985), 217–224.

38. R. Rolland, The number of MDS [7,3] codes on finite fields of characteristic 2, *Appl. Algebra Engrg. Comm. Comput.* **3** (1992), 301–310.

39. R. Rolland and A. N. Skorobogatov, Dénombrement de configurations dans le plan projectif, *in* "Arithmetic, Geometry and Coding theory" (R. Pellikan, M. Perret, S. G. Vlăduţ, Eds.), pp. 199–207, Walter de Gruyter, Berlin/New York, 1996.

40. C. S. Seshadri, Line bundles on Schubert varieties, *in* "Vector Bundles on Algebraic Varieties" (Papers presented at the Bombay Colloquium, 1984), pp. 495–528, Oxford Univ. Press, Bombay, 1987.

41. A. N. Skorobogatov, Linear codes, strata of Grassmannians and the problems of Segre, *in* "Coding Theory and Algebraic Geometry" (H. Stichtenoth and M. A. Tsfasman, Eds.), Lecture Notes in Math., Vol. 1518, pp. 210–223, Springer–Verlag, Berlin, 1992.

42. A. N. Skorobogatov, On the number of representations of matroids over finite fields, *Des. Codes Cryptogr.* **9** (1996), 215–226.

43. T. Svanes, Coherent cohomology on Schubert subschemes of flag schemes and applications, *Adv. Math.* **14** (1974), 369–453.

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

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

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