Finite Fields and Their Applications 76 (2021) 101905

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Higher Grassmann codes

Mahir Bilen Can[a,*], Roy Joshua[b], G.V. Ravindra[c]

[a] *Tulane University, New Orleans, LA, United States of America*
[b] *The Ohio State University, Columbus, OH, United States of America*
[c] *University of Missouri-St. Louis, St. Louis, MO, United States of America*

A R T I C L E I N F O

Article history:
Received 12 September 2020
Received in revised form 12 April 2021
Accepted 6 July 2021
Available online 13 August 2021
Communicated by S. Rybakov

MSC:
94B27
94B05
14M15
14G05

Keywords:
Grassmann codes
Projective systems
Parameters of a code

A B S T R A C T

We compute the parameters of the linear codes that are associated with *all* projective embeddings of Grassmann varieties.

1. Introduction

Throughout the paper $\mathbb{F}_q$ will denote the finite field with q elements, where q is a power of a prime number, p. Moreover, we will restrict to schemes of finite type defined over such

* Corresponding author.
E-mail addresses: mahirbilencan@gmail.com (M.B. Can), joshua.1@math.osu.edu (R. Joshua), girivaru@gmail.com (G.V. Ravindra).

https://doi.org/10.1016/j.ffa.2021.101905
1071-5797/

a finite field. Let X denote the Grassmann variety of l-dimensional subspaces of a fixed m-dimensional vector space V. One way to obtain the projective variety structure on X is via the Plücker embedding $\mathbf{p}: X \hookrightarrow \mathbb{P}^{\binom{m}{l}-1}$. The corresponding Grassmann code is obtained by evaluating sections of the line bundle on X obtained as the restriction of the canonical line bundle on $\mathbb{P}^{\binom{m}{l}-1}$ at the $\mathbb{F}_q$-rational points on X. Originally introduced by Ryan in [16], and investigated by Ryan and Ryan in [17], the Grassmann codes are natural generalizations of the well-known Reed-Müller codes (see, for example, [13]). A significant advantage in efficiency is gained by considering these geometric codes. Indeed, already in the case of projective spaces, the performance of the projective Reed-Müller codes, compared to the classical generalized Reed-Müller codes, are much better [11, Section 3]. The parameters for a general Grassmann code over $\mathbb{F}_q$ was computed later in [14], with much of these calculations later extended to some other important subvarieties of Grassmannians [5,6] as well as to some other partial flag varieties [15] (see [7] also).

In the present context, by a *projective embedding* of an algebraic variety or a scheme X, we mean a closed immersion of X into a projective space $\mathbb{P}^m$ in the sense of [8, §3, Chapter II]. One may consider many other projective embeddings of the Grassmannian other than the Plücker embedding. For example, let $\iota : Gr(l, V) \to \mathbb{P}((\bigwedge^l V)^{\otimes r})$ denote the projective embedding of $Gr(l, V)$ that is obtained by composing the diagonal Plücker embedding with the r-fold Segre embedding of $\prod^r \mathbb{P}(\bigwedge^l V)$. The resulting code is obtained by evaluating the global sections of the restriction of the canonical line bundle on the corresponding projective space to the Grassmannian, at the $\mathbb{F}_q$-rational points of the Grassmannian. *The goal of the present paper is to explicitly determine the parameters of all such codes obtained from the Grassmannian. This is part of a larger effort to compute parameters of codes produced from the large class of algebraic varieties called projective spherical varieties, which contain as special cases the class of all projective embeddings of Grassmannians, flag varieties as well as toric varieties.*

It may be also worth pointing out that [11, Theorem 2] had considered such higher dimensional embeddings of the projective space and computed the parameters of the resulting Reed-Muller codes. More precisely, when $l = 1$, the Grassmann variety $Gr(l, V)$ is equal to the projective space of lines in V, that is, $\mathbb{P}(V) \cong \mathbb{P}^{m-1}$. In this case we get the projective Reed-Müller codes; for every $r \in \mathbb{N}$, the relevant embedding is provided by the r-th symmetric power of V. The parameters of such codes were determined by Lachaud in [11, Theorem 2]. Thus the results of the present paper may be also viewed as an extension of [11] to all Grassmannians. This also explains why we chose the title of our paper as the *Higher Grassmann Codes*; we consider higher dimensional projective spaces to embed the Grassmann variety, such as via the composition of the diagonal Plücker embedding with the Segre embedding.

Let x denote a variable, and let a be a positive integer. Then the *a-th rising factorial of* x, denoted by $x^{(a)}$, is the product $x^{(a)} = x(x+1)\cdots(x+a-1)$.

Let q denote a power of a prime number p. It is convenient to denote by $[m]_q$ the polynomial $1+q+\cdots+q^{m-1} = \frac{q^m-1}{q-1}$, which is often called the *q-analog of* m since its evaluation at $q = 1$ is m. The q-factorial of m is defined by $[m]_q! := [m]_q[m-1]_q\cdots[2]_q[1]_q$.

As convention, we set $[0]_q := 1$. For $l \in \{0, \ldots, m\}$, the q-binomial coefficient $\begin{bmatrix} m \\ l \end{bmatrix}_q$ is defined by

$$\begin{bmatrix} m \\ l \end{bmatrix}_q := \frac{[m]_q!}{[m-l]_q![l]_q!}.$$

It is well-known that, if q is a power of a prime number, then $\begin{bmatrix} m \\ l \end{bmatrix}_q$ is the $\mathbb{F}_q$-rational points of the Grassmann variety of l-dimensional subspaces of an m-dimensional vector space. Also, there is an elementary combinatorial interpretation of $\begin{bmatrix} m \\ l \end{bmatrix}_q$ in terms of partitions of integers.

Moreover, one may recall the following standard terminology used in coding theory. A k-dimensional vector subspace W in an n-dimensional vector space V defined over $\mathbb{F}_q$ is called an *$[n, k, d]_q$-code*. Here, d is defined as the minimum of the distances between distinct elements of W; the distance is defined by the number of coordinates where two vectors differ from each other. The integer n is often called the *length of the code*, and k is called the *dimension of the code*.

Let $\{e_1, \ldots, e_n\}$ denote the standard basis for $\mathbb{F}_q^n$, and let $x_1, \ldots, x_n$ denote the corresponding coordinate functionals on $\mathbb{F}_q^n$. An $[n, k, d]_q$-code $W \subset \mathbb{F}_q^n$ is said to be *nondegenerate* if W is not contained in any of the following coordinate hypersurfaces:

$$H_i := \{v \in \mathbb{F}_q^n : \ x_i(v) = 0\} \cong \mathbb{F}_q^{m-1} \qquad (i \in \{1, \ldots, n\}).$$

In the language of [21], there is a 1-1 correspondence between the set of equivalence classes of nondegenerate $[n, l, d]_q$-codes and the set of equivalence classes of projective $[n, k, d]_q$-systems, which are defined as follows.

Let X be an algebraic variety with n $\mathbb{F}_q$-rational points. Let $\varphi : X \to \mathbb{P}^{m-1}$ be an embedding, and let $x_1, \ldots, x_n$ denote the images of the $\mathbb{F}_q$-rational points of X in $\mathbb{P}^{m-1}$. Let E denote the $\mathbb{F}_q$-vector space $\mathbb{F}_q^m$, and let $y_1, \ldots, y_n$ denote (arbitrary) liftings of $x_1, \ldots, x_n$ to $E \setminus \{0\}$ in the given order. Then we get an evaluation map on the linear forms of E,

$$\begin{aligned} \mathrm{ev} : E^* &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(y_1), \ldots, f(y_n)). \end{aligned} \tag{1.1}$$

The image of ev, denoted by C, is the *projective $[n, k, d]_q$-system* associated with φ. Note that the length of C is n, its dimension is $k = m - \dim \ker(\mathrm{ev})$, and its minimum distance is given by

$$d = \min\{|X(\mathbb{F}_q)| - |X(\mathbb{F}_q) \cap \ker(f)| : \ f \in E^* \ \text{ and } \ X(\mathbb{F}_q) \not\subset \ker(f)\}.$$

Example 1.2. As before, let V be an m dimensional vector space over $\mathbb{F}_q$. The points in the image of the Plücker embedding $\mathbf{p} : Gr(l, V) \to \mathbb{P}^{\binom{m}{l}-1}$ can be viewed as projective

$[n, k, d]_q$-systems, where $n = \begin{bmatrix} m \\ l \end{bmatrix}_q$ and $k = \binom{m}{l}$. These projective systems (or rather the codes corresponding to these projective systems) are called the *(classical) Grassmann codes.*

Adopting the above notation, we now present a special case of our main theorem, which is recorded as Theorem 4.1 in the sequel.

Theorem 1.3. *Let $\iota : Gr(l, V) \to \mathbb{P}((\bigwedge^l V)^{\otimes r})$ denote the projective embedding of $Gr(l, V)$ that is obtained by composing the diagonal Plücker embedding with the r-fold Segre embedding of $\prod^r \mathbb{P}(\bigwedge^l V)$. If C is the projective $[n, k, d]_q$-system corresponding to ι, then for every sufficiently large prime characteristic $p > 0$, the parameters of C satisfy the following conditions:*

1. $n = \begin{bmatrix} m \\ l \end{bmatrix}_q = \frac{[m]_q [m-1]_q \cdots [m-l+1]_q}{[1]_q [2]_q \cdots [l]_q}$,
2. $k = \frac{m^{(r)} (m-1)^{(r)} \cdots (m-l+1)^{(r)}}{1^{(r)} 2^{(r)} \cdots l^{(r)}}$,
3. $q^{l(m-l)} - rq^{l(m-l)-1} \leq d \leq q^{l(m-l)} - (r-1)q^{l(m-l)-1}$.

We know that the upper bound for the minimum distance is achieved for $r = 1$ by [14] as well as for $l = 1$ by [11]. We conjecture that the upper bound is always achieved. Note that as a polynomial in q, the leading term of n in Theorem 1.3 is $q^{l(m-l)}$. Also, the coefficient of $q^{l(m-l)-1}$ in n is 1. (We will justify these statements in Section 2 by using a simple, well-known combinatorial argument.) Then the leading term of the difference $n - d$ is given by $rq^{l(m-l)-1}$. It follows that, if we fix r, then for every sufficiently big q, the difference $n - d$ is greater than k. In other words, our codes satisfy the Singleton bound for sufficiently large values of q. Let us point out that there is an effective way, due to Jantzen, to check how small the characteristic p can be in order for our theorem to hold; it is explained in Remark 2.10.

Next, we want to point out some facts about the parameters of our codes. First of all, for $r > 1$, it is easy to see by an inductive argument that the dimensions of our codes are all greater than $\binom{m}{l}$, which is the dimension of Grassmann codes obtained from the Plücker embedding as shown in [14]. On the other hand, it is already apparent from the $r = 2$ case of Theorem 1.3 that our codes may have smaller minimum distance compared to the ordinary Grassmann codes ($r = 1$). Nevertheless, as $q \to \infty$, the dominating term of the minimum distance of our code is also given by $q^{l(m-l)}$. Therefore, on finite fields with big characteristic exponents, our codes become more advantageous compared to the ordinary Grassmann codes.

The paper is structured as follows. In Section 2, we setup our notation, and we review some basic representation theory and algebraic geometry facts regarding Grassmann and Schubert varieties. In Section 3, we analyze the Białynicki-Birula decomposition of $Gr(l, V)$ in relation with that of $\mathbb{P}(\bigwedge^l V)$. In Section 4, we prove our main result by giving a lower bound for the dimension of C for small prime characteristics. By applying Weyl's dimension formula to calculate this lower bound, we conclude our paper by proving Theorem 1.3 in Section 4.1.

Acknowledgments. At the time of writing this paper, the first author was partially supported by a grant from Louisiana Board of Regents (no. 555596). The authors thank the referees for their careful reading of the paper and for their constructive comments.

2. Preliminaries

In this section we will introduce the most basic objects and notation for our paper. We recall that we will restrict to schemes of finite type defined over a fixed finite field $\mathbb{F}_q$.

For a positive integer $m \in \mathbb{Z}$, we will use the notation $[m]$ to denote the finite set $\{1, \dots, m\}$. For $l \in [m]$, the set of all l-element subsets of $[m]$ is denoted by $\binom{[m]}{l}$. We view $\binom{[m]}{l}$ as a chain, where the total order is given by the lexicographic ordering. More precisely, we view the elements of $\binom{[m]}{l}$ as increasing sequences of l-tuples of integers from $[m]$, and we order them lexicographically. The lexicographic order on $\binom{[m]}{l}$ will be denoted by $\preceq$. In particular, whenever $\binom{[m]}{l}$ appears as an indexing set of some vector, we always assume that its elements are ordered according to $\preceq$. We will refer to an element of $\binom{[m]}{l}$ as an l-subset.

An *integer partition of* m is a non-increasing sequence of positive numbers $\lambda = (\lambda_1, \dots, \lambda_s)$ such that $\sum_{i=1}^{s} \lambda_i = m$. The *Young diagram of* λ is a top-left justified arrangement of the boxes with λ_i boxes in the i-th row. For example, the Young diagram of the integer partition $\lambda = (7, 3, 3, 2, 1)$ of 16 is shown in Fig. 2.1.

The coefficient of the monomial q^a in $\begin{bmatrix} m \\ l \end{bmatrix}_q$ is given by the number of integer partitions of a whose Young diagram fit into an $l \times (m - l)$ grid [20, Proposition 1.7.3]. This well-known combinatorial fact is a direct consequence of the decomposition of the Grassmann variety $Gr(l, \mathbb{F}_q^m)$ into Schubert cells, which we will review in the sequel. By abuse of notation, let us use $\lambda \subseteq l \times (m - l)$ to indicate that the Young diagram of the integer partition λ fits inside the $l \times (m-l)$ grid. Then we have the following polynomial identity which summarizes our discussion:

$$\begin{bmatrix} m \\ l \end{bmatrix}_q = 1 + \sum_{\lambda \subseteq l \times (m-l)} q^{\#\text{ of boxes in } \lambda}.$$

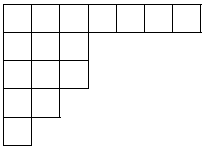

Fig. 2.1. The Young diagram of $(7, 3, 3, 2, 1)$.

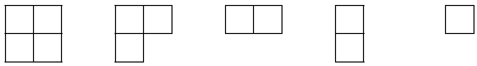

Fig. 2.2. The Young diagrams of the integer partitions whose Young diagram fits in a 2×2 grid.

Thus, the coefficients of the monomials $q^{l(m-l)}$ and $q^{l(m-l)-1}$ in $\begin{bmatrix} m \\ l \end{bmatrix}_q$ are equal to 1. In particular, the leading term of $\begin{bmatrix} m \\ l \end{bmatrix}_q$ is $q^{l(m-l)}$. We used this fact to justify (in the introduction) the fact that our codes in Theorem 4.1 satisfy the Singleton bound.

Example 2.1. Let $m = 4$, $l = 2$. Then, there are 5 integer partitions whose Young diagram fits into 2×2 grid. We depicted the Young diagrams of these integer partitions in Fig. 2.2.

It follows from the list of Young diagrams in Fig. 2.2 that

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = 1 + q + 2q^2 + q^3 + q^4.$$

We finish this subsection by introducing another commonly used notation. The multiplicative group of nonzero entries in $\mathbb{F}_q^\times$ will be denoted by $\mathbb{G}_m$.

2.1. The Grassmann varieties

Let K be a field. Let $\mathbf{SL}_m$ denote the group of $m \times m$ matrices with determinant 1 with entries from K. The diagonal maximal torus in $\mathbf{SL}_m$, denoted by $\mathbf{T}_m$, is a split torus. The Borel subgroup of upper triangular matrices in $\mathbf{SL}_m$, denoted by $\mathbf{B}_m$, contains $\mathbf{T}_m$. We denote by $X(\mathbf{T}_m)$ the group of rational characters of $\mathbf{T}_m$, and the dual of $X(\mathbf{T}_m)$, that is $\mathrm{Hom}_{\mathbb{Z}}(X(\mathbf{T}_m), \mathbb{Z})$, is denoted by $Y(\mathbf{T}_m)$. The nondegenerate bilinear pairing between $X(\mathbf{T}_m)$ and $Y(\mathbf{T}_m)$ will be denoted by $\langle , \rangle$. The Weyl group of $\mathbf{SL}_m$ is isomorphic to S_m, the symmetric group of permutations of the set $[m]$. It acts on $\mathbf{T}_m$ by conjugation, hence, it acts on the groups $X(\mathbf{T}_m)$ and $Y(\mathbf{T}_m)$. However, the pairing $\langle , \rangle$ is S_m-invariant. The root system of the pair $(\mathbf{SL}_m, \mathbf{T}_m)$ will be denoted by R. Explicitly, it is given by the set of vectors $R = \{\varepsilon_i - \varepsilon_j : \ 1 \leq i, j \leq m\}$, where $\{\varepsilon_1, \dots, \varepsilon_m\}$ is the standard basis for the m-dimensional Euclidean $\mathbb{Q}$-vector space. The system of positive roots determined by $\mathbf{B}_m$, denoted by R^+, is given by $R^+ = \{\varepsilon_i - \varepsilon_j : \ 1 \leq i < j \leq m\}$. The subset of simple roots in R^+ will be denoted by S; it is given by $S = \{\alpha_i : \ \alpha_i = \varepsilon_i - \varepsilon_{i+1}, \ 1 \leq i \leq m-1\}$. The duals of the basis vectors α_i $(1 \leq i \leq m-1)$ are denoted by $\alpha_i^\vee$, and the *fundamental weights* ϖ_i $(1 \leq i \leq m-1)$ are defined by equations $\langle \varpi_i, \alpha_j^\vee \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$ for $\alpha_j \in S$. Note that the i-th fundamental weight ϖ_i is the highest weight vector of the i-th fundamental representation $\wedge^i k$ of $\mathbf{SL}_m$. The submonoid generated by ϖ_i $(1 \leq i \leq m-1)$ in $X(\mathbf{T}_m)$, denoted by $X(\mathbf{T}_m)_+$, is the *monoid of dominant weights*. Then we have,

$$X(\mathbf{T}_m)_+ = \{\lambda \in X(\mathbf{T}_m) : \ \langle \lambda, \alpha_i^\vee \rangle \geq 0 \text{ for every } \alpha_i \in S\}.$$

$$\begin{tikzcd} & (\bigwedge^l V) \setminus \{0\} \arrow[d] \\ \mathbf{p}: Gr(l,V) \arrow[r] & \mathbb{P}^{\binom{m}{l}-1} \end{tikzcd}$$

Fig. 2.3. The Plücker coordinates of $Gr(l,V)$ come from the coordinates on $\bigwedge^l V$.

It is well-known that for every finite dimensional irreducible representation W of $\mathbf{SL}_m$, there is a unique dominant weight $\lambda \in X(\mathbf{T}_m)_+$ called the *highest weight of* W, see [10, Chapter II.2]. In other words, simple $\mathbf{SL}_m$-modules are parametrized by the elements of $X(\mathbf{T}_m)_+$.

Since it is the point of departure for our paper, we will briefly review the definition of the Plücker embedding. Let V be an m-dimensional vector space. We fix a basis $\{e_1, \dots, e_m\}$ of V. Note that an l-dimensional subspace M of V can be identified with an $l \times m$ matrix $A = A(M)$, where the rank of A is l. Indeed the rows of such a matrix span an l-dimensional vector subspace; two such matrices A_1, A_2 span the same vector subspace if and only if there exists $g \in \mathbf{GL}_l$ such that $A_1 = gA_2$.

Let $\mathbf{Mat}_{l,m}$ denote the space of $l \times m$ matrices (over a field) and let $\mathbf{Mat}^0_{l,m}$ denote the Zariski open subset consisting of rank l matrices. Then $\mathbf{GL}_l$ acts by the left matrix multiplication on $\mathbf{Mat}^0_{l,m}$, and the quotient is precisely the Grassmann variety $Gr(l,V)$. In this interpretation, the elements of $Gr(l,V)$ are the equivalence classes of matrices $[A]$ where $A \in \mathbf{Mat}^0_{l,m}$. The *Plücker embedding of* $Gr(l,V)$ is defined by $\mathbf{p}: Gr(l,V) \to \mathbb{P}^{\binom{m}{l}-1}$, $[A] \mapsto (\det A_I)_{I \in \binom{[m]}{l}}$, where A_I is the $l \times l$-minor of A determined by the columns indexed by I.

Finally, let us point out the fact that $Gr(l,V)$ is a homogeneous space for $\mathbf{SL}_m$ as well as for $\mathbf{GL}_m$:

$$Gr(l,V) \cong \mathbf{SL}_m/\mathrm{Stab}_{\mathbf{SL}_m}(\langle e_1, \dots, e_l \rangle) \cong \mathbf{GL}_m/\mathrm{Stab}_{\mathbf{GL}_m}(\langle e_1, \dots, e_l \rangle).$$

Here, $\langle e_1, \dots, e_l \rangle$ is the l-dimensional subspace spanned by $e_1, \dots, e_l$ in V.

2.2. Projective embeddings of $Gr(l,V)$

Let V denote the m-dimensional K-vector space K^m with the standard basis $\{e_1, \dots, e_m\}$. The l-th fundamental representation of $\mathbf{SL}_m$ is given by the l-th exterior power of V. It is well-known that the Picard group of $Gr(l,V)$ is generated by the ample line bundle $\mathcal{L}(\varpi_l)$.

The dual of the space of global sections, that is $H^0(Gr(l,V), \mathcal{L}(\varpi_l))^*$, is isomorphic to $\wedge^l V$. Therefore, the Plücker coordinates on $Gr(l,V)$ are given by the restrictions of the coordinate functions on the affine space $\mathbb{A}^{\binom{m}{l}} \cong \wedge^l V$.

Next, we will consider the space of global sections of the line bundle $\mathcal{L}(r\varpi_l)$, where r is a positive integer. Since $\mathcal{L}(r\varpi_l)$ is very ample, it gives a closed embedding,

$$\tau_r: \; Gr(l,V) \hookrightarrow \mathbb{P}(H^0(Gr(l,V), \mathcal{L}(r\varpi_l))^*). \tag{2.2}$$

The analogs of Plücker coordinates for (2.2) are called the *standard monomials*. In this section, we will compute the parameters of the codes that we will construct from (2.2). Since the underlying idea of computations is the same for every $r > 1$, we will present the simplest case, that is $r = 2$.

To identify the projective space in (2.2), we first embed $Gr(l, V)$ into $\mathbb{P}^s \times \mathbb{P}^s$, where $s = \binom{m}{l} - 1$; this embedding is given by the composition of the diagonal embedding of $Gr(l, V)$ into $Gr(l, V) \times Gr(l, V)$ followed by the doubled Plücker embedding. Then we use the Segre embedding to embed the doubled projective space into a bigger projective space. We denote the morphism defined by these compositions by ι. In summary, we have the following diagram:

$$\iota : Gr(l, V) \xrightarrow{\text{diag}} Gr(l, V) \times Gr(l, V) \xrightarrow{\mathbf{p}\times\mathbf{p}} \mathbb{P}^s \times \mathbb{P}^s \xrightarrow{\text{Segre}} \mathbb{P}^{s^2+2s}. \tag{2.3}$$

We will describe explicitly the image of (2.3).

Let M be a point from $Gr(l, V)$, and let $(m_1, m_2, \dots, m_{s+1})$ denote its image under the Plücker embedding. Then we have

$$\begin{aligned} \iota :\ M &\overset{\text{diag}}{\longmapsto} (M, M) \overset{(\mathbf{p},\mathbf{p})}{\longmapsto} ((m_1, \dots, m_{s+1}), (m_1, \dots, m_{s+1})) \\ &\overset{\text{Segre}}{\longmapsto} (m_i m_j)_{\substack{i=1,\dots,s+1 \\ j=1,\dots,s+1}}. \end{aligned} \tag{2.4}$$

Equivalently, $(m_i m_j)_{\substack{i=1,\dots,s+1 \\ j=1,\dots,s+1}}$ is the point that is represented by the tensor product $M \otimes M$ in $\mathbb{P}(\bigwedge^l V \otimes \bigwedge^l V)$.

We will show that ι is very useful for understanding the embedding (2.2). We proceed with some general remarks.

Let G be a connected reductive group, and let B be a Borel subgroup. Let P be a standard parabolic subgroup, that is, P is a parabolic subgroup and $B \subset P$. We assume that all of these (sub)groups are defined over $K := \mathbb{F}_q$.

There is a canonical projection map $\pi : G/B \to G/P$, and for every locally free sheaf $\mathcal{S}$ on G/P, there is an isomorphism

$$H^0(G/P, \mathcal{S}) \xrightarrow{\sim} H^0(G/B, \pi^*\mathcal{S}). \tag{2.5}$$

In our special case, if P is the maximal parabolic subgroup in $G = \mathbf{SL}_m$ corresponding to the fundamental weight ϖ_l, and B is the Borel subgroup $\mathbf{B}_m$, then we have the isomorphism

$$H^0(G/P, \mathcal{L}(r\varpi_l)) \xrightarrow{\sim} H^0(G/B, \pi^*\mathcal{L}(r\varpi_l)) \tag{2.6}$$

for every $r \in \mathbb{Z}_+$. Therefore, as far as our embedding (2.2) concerned, we can work with the $\mathbf{SL}_m$ module $H^0(G/B, \pi^*\mathcal{L}(r\varpi_l))$. To be precise, we will work with the dual of this module.

Definition 2.7. Let T be a maximal torus such that $T \subset B$. For every $\lambda \in X(T)$, we will use the abbreviation $H^0(r\varpi_l) := H^0(G/P, \mathcal{L}(r\varpi_l))$. If λ is a dominant weight from $X(T)_+$, then the G-module, $V(\lambda) := H^0(-w_0\lambda)^*$, where w_0 is the longest element of the Weyl group W, is called the *Weyl module associated with* λ.

We have several remarks in order.

Remark 2.8. The formal characters of $V(\lambda)$ and $H^0(\lambda)$ are always equal, see [10, Chapter II.2.13].

Remark 2.9. In characteristic 0, Weyl modules give irreducible representations of G, and furthermore, $V(\lambda)$ is isomorphic to $H^0(\lambda)$. However, in characteristic $p \neq 0$, they (the Weyl modules) are in general non-simple. Nevertheless, the isomorphism $V(\lambda) \cong H^0(\lambda)$ holds if $V(\lambda)$ is simple. This follows from [10, Chapter II.6, Proposition 6.16]. In this case, we can compute the dimension of $V(\lambda)$ via Weyl character formula, see [10, Chapter II.5, Corollary 5.11]. Since this is a formal computation, it can be performed over $\mathbb{Z}$ (hence over $\mathbb{C}$) as well.

Remark 2.10. For every field K and positive integer $m \in \mathbb{N}$, the exterior powers $\bigwedge^l K^m$ $(1 \leq l \leq m)$ are simple $\mathbf{SL}_m$-modules, see [10, Chapter II.2.15]. More generally, (over a finite field $K = \mathbb{F}_q$) there is an explicit characterization of the weights λ such that $V(\lambda)$ is simple, see [9, pg. 113]. It goes as follows: Let p denote the characteristic of K, and let ρ denote the weight $\varpi_1 + \cdots + \varpi_{m-1}$. Then $V(\lambda)$ is simple over K if and only if for each positive root $\alpha = \varepsilon_i - \varepsilon_j \in R^+$ with $1 \leq i < j \leq m$ the following property holds: Let $\langle \lambda + \rho, \alpha^\vee \rangle = ap^s + bp^{s+1}$, where a, b, s are nonnegative integers such that $0 < a < p$. Then there should exist $\beta_0, \beta_1, \ldots, \beta_b \in R^+$ with $\langle \lambda + \rho, \beta_i^\vee \rangle = p^{s+1}$ for $1 \leq i \leq b$ and $\langle \lambda + \rho, \beta_0^\vee \rangle = ap^s$ with $\alpha = \sum_{i=0}^b \beta_i$ and with $\alpha - \beta_0 \in R$. Equivalently, there exist integers $i = i_0 < i_1 < \cdots < i_b < i_{b+1} = j$ such that $\{\beta_i : \ 0 \leq i \leq b\} = \{\varepsilon_{i_v} - \varepsilon_{i_{v+1}} : \ 0 \leq v \leq b\}$ and $\beta_0 \in \{\varepsilon_i - \varepsilon_{i_1}, \varepsilon_{i_b} - \varepsilon_j\}$. Notice that for every sufficiently big prime number, we have $b = s = 0$, hence, $\langle \lambda + \rho, \alpha^\vee \rangle = a < p$. In this case, all of the subsequent conditions automatically hold. Therefore, $V(\lambda)$ is a simple $\mathbf{SL}_m(K)$-module. This observation is exploited in the paper [2] as well.

2.3. Schubert varieties in $Gr(l, V)$

Let G be an algebraic group, and let B be a Borel subgroup of G. Let G/P be a projective homogeneous space, where P is a parabolic subgroup such that $B \subseteq P$. To a large extent, the geometry and the topology of G/P is determined by its Schubert subvarieties. By definition, a *Schubert variety in* G/P is the Zariski closure of a B-orbit in G/P. In the case of Grassmann varieties, they can be defined quite explicitly.

For a subset $J \subset [m]$, we will denote by E_J the subspace $\langle e_j : \ j \in J \rangle$. In particular, we will denote by $E_{[j]}$ $(j \in [m])$ the subspace $\langle e_1, \ldots, e_j \rangle$. Let $I = \{i_1, \ldots, i_l\}$ be an element of $\binom{[m]}{l}$. The *Schubert cell associated with* I *in* $Gr(l, V)$ is the affine space

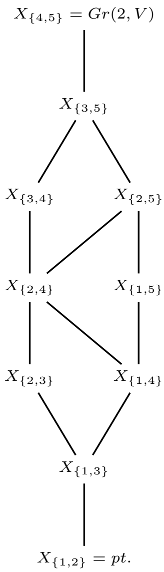

Fig. 2.4. The Grassmann variety $Gr(2, V)$ and its Schubert varieties, where $\dim_k V = 5$.

$$C_I := \{W \in Gr(l, V) :\ \dim(W \cap E_{[j]}) = |I \cap [j]| \text{ for every } j \in [m]\}. \tag{2.11}$$

It is not difficult to verify that if $I \neq I'$, then $C_I \cap C_{I'} = \emptyset$. It is also not difficult to check that the union of all Schubert cells is equal to $Gr(l, V)$. The decomposition

$$Gr(l, V) = \bigsqcup_{I \in \binom{[m]}{l}} C_I \tag{2.12}$$

is called the *Bruhat-Chevalley decomposition* of $Gr(l, V)$.

The Zariski closure of C_I in $Gr(l, V)$, called the *Schubert variety associated with* I, is given by

$$X_I := \overline{C_I} = \{W \in Gr(l, V) :\ \dim(W \cap E_{[j]}) \geq |I \cap [j]| \text{ for every } j \in [m]\}.$$

The intersection ring (the Chow ring) of $Gr(l, V)$ is completely determined by the classes of Schubert varieties. For $I = \{i_1, \dots, i_l\}, J = \{j_1, \dots, j_l\}$ from $\binom{[m]}{l}$, the inclusion relationship between X_I and X_J is given by the entry-wise comparisons:

$$X_I \subseteq X_J \iff i_r \leq j_r \text{ for every } r \in [l]. \tag{2.13}$$

We have an example of the Hasse diagram of this partial order in Fig. 2.4.

Remark 2.14. It is not difficult to check from (2.13) that the Schubert cell $C_{\{m-l+1, m-l+2, \dots, m\}}$ is open and dense in $Gr(l, V)$, and that, there is a unique one-codimensional Schubert subvariety X' in $Gr(l, V)$. The indexing set of X' is given by

$\{m-l, m-l+2, m-l+3, \dots, m\}$. This divisor of $Gr(l,V)$ is precisely the intersection of the image of the Plücker embedding (Fig. 2.3) with the hypersurface of $\mathbb{P}(\bigwedge^l V)$ that is given by the vanishing of the last coordinate variable with respect to $\preceq$. This remark will be justified in Section 4.

2.4. Tsfasman-Serre theorem

In this section, to simplify our notation and to be consistent with our references, we will denote by π_m the q-analog of $m+1$, where q is a power of a prime number. In other words, we set

$$\pi_m := [m+1]_q = \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q .$$

If X is a variety defined over $\mathbb{F}_q$, then by $X(\mathbb{F}_q)$ we will denote the set of $\mathbb{F}_q$-rational points of X.

As we mentioned before in our discussion of the Grassmann varieties, π_m is the cardinality of the projective space $\mathbb{P}^m(\mathbb{F}_q)$. The following theorem about the number of zeros of a homogeneous polynomial on a projective space was originally conjectured by Tsfasman; it was first proved by Serre [18] and then by Sørensen [19]. More recently, Datta and Ghorpade [3] found a conceptual proof of it.

Theorem 2.15. *Let P be a nonzero homogeneous polynomial of degree r from $\mathbb{F}_q[x_0, \dots, x_m]$. If $r \leq q+1$, then*

$$|\{x \in \mathbb{P}^m(\mathbb{F}_q) : \; P(x) = 0\}| \leq rq^{m-1} + \pi_{m-2}. \tag{2.16}$$

Remark 2.17. Let $a_1, \dots, a_r$ be distinct elements of $\mathbb{F}_q$. If $r \leq q$, then it is easy to check that the polynomial

$$G_r(x_0, \dots, x_m) := (x_1 - a_1 x_0) \cdots (x_1 - a_r x_0)$$

has exactly $rq^{m-1} + \pi_{m-2}$ zeros in $\mathbb{P}^m(\mathbb{F}_q)$. Likewise, it is easy to check that the polynomial

$$g_r(x_1, \dots, x_m) = (x_1 - a_1) \cdots (x_1 - a_r),$$

has exactly rq^{m-1} zeros in $\mathbb{A}^m(\mathbb{F}_q)$. It is well-known that this is the maximum of the number of $\mathbb{F}_q$-rational points on a hypersurface of degree r in $\mathbb{A}^m(\mathbb{F}_q)$, [12, Theorem 6.13].

3. Some helpful lemmas

In this section, K denotes a finite field with q elements; all of our algebraic groups are defined over K.

Let s denote $\binom{m}{l} - 1$, and let $\{F_1, \dots, F_{s+1}\}$ denote the standard basis for $\bigwedge^l V$; if $r \in \{1, \dots, s+1\}$ corresponds to the subset $I = \{i_1, \dots, i_l\} \in \binom{[m]}{l}$, then F_r is given by $F_r = e_{i_1} \wedge \cdots \wedge e_{i_l}$. Let $x_1, \dots, x_{s+1}$ denote the corresponding Plücker coordinate functionals on $\bigwedge^l V$. Thus, $x_r = F_r^*$ for $r \in \{1, \dots, r+1\}$. Then the coordinate functionals on $\mathbb{P}(\bigwedge^l V \otimes \bigwedge^l V)$ are given by $x_i \otimes x_j$, $i, j \in \{1, \dots, s+1\}$.

As we mentioned before, we know from Nogin's work that the minimum distance on $Gr(l, V)$ is given by

$$d = |\{M \notin H_v : M \in Gr(l, V)\}| = q^{l(m-l)}, \tag{3.1}$$

where v is any completely decomposable vector from $\bigwedge^{m-l} V \cong (\bigwedge^l V)^*$, and H_v is the hypersurface defined by $H_v = \{w \in \bigwedge^l V : \ w \wedge v = 0\}$ (see [14, Theorem 2, Proposition 3]). Here, a vector $v \in \bigwedge^{m-l} V$ is said to be *completely decomposable* if there exist $m - l$ vectors $u_1, \dots, u_{m-l} \in V$ such that $v = u_1 \wedge \cdots \wedge u_{m-l}$. It is easy to check that the Plücker coordinate functions are completely decomposable. In the sequel, we will not distinguish between $\bigwedge^{m-l} V$ and $(\bigwedge^l V)^*$.

We set v to be the last Plücker coordinate function with respect to $\preceq$, that is, $v := x_{s+1}$. Let us write $[H_v]$ for the projectivization of H_v, that is, the image of H_v under the canonical projection $(\bigwedge^l V) \setminus \{0\} \to \mathbb{P}(\bigwedge^l V)$. Then $[H_v] \cap Gr(l, V)$ is the unique Schubert divisor of $Gr(l, V)$. Thus we have the following alternative description of d:

$$\begin{aligned} d &= |\{M \in Gr(l, V) : \ x_{s+1}(M) \neq 0\}| \\ &= \begin{bmatrix} m \\ l \end{bmatrix}_q - |\{M \in Gr(l, V) : \ x_{s+1}(M) = 0\}|. \end{aligned} \tag{3.2}$$

It follows from our discussion in Subsection 2.3 that d is the number of K-rational points on the open the subset $\{M \in Gr(l, V) : \ x_{s+1}(M) \neq 0\}$. From a similar vein, we will compute the minimum distance of the embedding $Gr(l, V) \hookrightarrow \mathbb{P}(H^0(r\varpi_l)^*)$. The main "novel ingredient" of our computation is the fact that the geometry of a higher twisting of the Plücker embedding is essentially determined by the cellular decomposition of the relevant projective space.

The action of $\mathbf{GL}_m$ on V induces an action on $\bigwedge^l V$. Let $\lambda : \mathbb{G}_m \to \mathbf{T}_m$ denote the one-parameter subgroup defined by

$$\lambda(t) = \operatorname{diag}(t^{v_0}, \dots, t^{v_{n-1}}), \tag{3.3}$$

where $v_0, \dots, v_{m-1}$ are integers such that $v_i = 2^{v_{i+1}}$ for $i \in \{0, \dots, m-2\}$. By λ, we get an action of $\mathbb{G}_m$ on $\mathbb{P}(\bigwedge^l V)$:

$$t \cdot [A] := [\lambda(t) \cdot A] \qquad (t \in \mathbb{G}_m,\ A \in \bigwedge^l V). \tag{3.4}$$

Warning: The notation $[A]$ indicates that we are taking the image of the vector A under the projection $\bigwedge^l V \setminus \{0\} \to \mathbb{P}(\bigwedge^l V)$. This should not be confused with $[m]$, which stands for the set $\{1, \dots, m\}$. We trust that this clash of notation will not cause any confusion for the reader.

Lemma 3.5. *The fixed point set of the action of $\mathbb{G}_m$ is given by $\mathbb{P}(\bigwedge^l V)^{\mathbb{G}_m} = \{[F_1], \dots, [F_{s+1}]\}$.*

Proof. Let $[(a_0, \dots, a_s)]$ be a point in $\mathbb{P}(\bigwedge^l V)$, and let $t \in \mathbb{G}_m$. Then we have

$$t \cdot [(a_0, \dots, a_s)] = [(t^{\sum_{i=0}^{l-1} v_i} a_0, \dots, t^{\sum_{i=m-l}^{m-1} v_i} a_s)] \qquad (t \in \mathbb{G}_m). \tag{3.6}$$

The way that we chose the positive integers $v_0, \dots, v_{m-1}$ ensures that the exponents of t in on the right hand side of (3.6) are strictly decreasing from left to right. It follows that

$$[(a_0, \dots, a_s)] \neq [(t^{\sum_{i=0}^{l-1} v_i} a_0, \dots, t^{\sum_{i=m-l}^{m-1} v_i} a_s)],$$

unless all but one of the coordinates is zero. Therefore, the fixed point set of the $\mathbb{G}_m$-action is given by $\{[(1,0,\dots,0)], [(0,1,0,\dots,0)], \dots, [(0,\dots,0,1)]\}$, which is precisely our standard basis $\{F_1, \dots, F_{s+1}\}$. $\square$

For $i \in \{1, \dots, s+1\}$, the subvariety

$$F_i^+ := \{(a_1, \dots, a_i, 1, 0, \dots, 0) :\ a_1, \dots, a_i \in K\} \subset \mathbb{P}(\bigwedge^l V) \tag{3.7}$$

is called the *plus-cell corresponding to F_i*; it is isomorphic to the affine space K^i. Since $\mathbb{P}(\bigwedge^l V) = \bigsqcup_{i=0}^m F_i^+$, the plus-cell decomposition is a cellular decomposition of $\mathbb{P}(\bigwedge^l V)$ in the sense of algebraic topology.

Clearly, the Grassmann variety $Gr(l, V)$ in $\mathbb{P}(\bigwedge^l V)$ is stable under the action (3.4), and furthermore, every fixed point of λ is contained in $Gr(l, V)$. It follows that the intersections of the plus-cells (3.7) with $Gr(l, V)$ give the plus-cell decomposition of $Gr(l, V)$.

Next, we will prove that this plus-cell decomposition of the Grassmann variety agrees with its Bruhat-Chevalley decomposition, (2.12).

Lemma 3.8. *Let $r \in \{0, \dots, s\}$ correspond to the subset $I \in \binom{[m]}{l}$ with respect to $\preceq$. Then $F_r^+ \cap Gr(l, V)$ is equal to the Schubert cell C_I.*

Proof. The Plücker embedding is a $\mathbf{GL}_m$-equivariant morphism. Let $\mathbf{B}_m$ denote the Borel subgroup of upper triangular matrices in $\mathbf{GL}_m$. On one hand we have that C_I is the $\mathbf{B}_m$-orbit of F_r [1, Proposition 1.1.3]. On the other hand, we see that the $\mathbf{B}_m$-orbit of $[(0,\dots,0,1,0,\dots,0)]$, where 1 appears in the r-th position, is given by F_r^+. Indeed, the action of $\mathbf{B}_m$ on $\mathbb{P}(\bigwedge^l V)$ is obtained from the first fundamental representation of $\mathbf{GL}_m$ on $V \cong K^m$, whereby, $\mathbf{B}_m \cdot e_r = \langle e_1,\dots,e_r\rangle$. Since the nonzero Plücker coordinate functions on F_r^+ are the ones that correspond to the l-subsets $J \in \binom{[m]}{l}$ such that $J \preceq I$, we see the $\mathbf{B}_m$-orbit of F_r in $\mathbb{P}(\bigwedge^l V)$ is contained in F_r^+. In particular, we see that $F_r^+ \cap Gr(l,V) = \mathbf{B}_m \cdot F_r$. This finishes the proof of our lemma. $\square$

We now justify Remark 2.14.

Corollary 3.9. *The unique Schubert divisor $X_{\{m-l,m-l+2,\dots,m\}}$ is equal the intersection of $Gr(l,V)$ with the hypersurface $\{x_{s+1}=0\}$ of $\mathbb{P}(\bigwedge^l V)$.*

Proof. As we already pointed out in Remark 2.14, the uniqueness of the one-codimensional Schubert subvariety is easy to check from the Bruhat-Chevalley order (2.13). The Plücker coordinate function x_{s+1} corresponds to the subset $\{m-l+1,\dots,m\}$ which is maximal with respect to $\preceq$. In other words, by Lemma 3.8, $\{x_{s+1}\neq 0\}\cap Gr(l,V)$ is the open Schubert cell in $Gr(l,V)$. Therefore, its complement, also called the *boundary*, is $\mathbf{B}_m$-stable. In particular, the boundary of the open cell is a union of Schubert subvarieties. Since there is a unique codimension one Schubert subvariety (hence, all other proper Schubert subvarieties are contained in this one), the boundary is equal to $X_{\{m-l,m-l+2,\dots,m\}}$ as claimed. But the complement is equal to the intersection $\{x_{s+1}=0\}\cap Gr(l,V)$. This finishes the proof of our claim. $\square$

4. The main theorem

Recall that the dimension of an algebraic geometric $[n,k,d]_q$-code C on a projective variety $X \hookrightarrow \mathbb{P}^r$ is given by the “dimension” of the image of the evaluation map $\mathrm{ev}: E^* \to \mathbb{F}_q^n$, that is, $l = m - \dim\ker(\mathrm{ev})$. Here, we view E^* as the vector space homogeneous linear forms on $\mathbb{P}^r = \mathbb{P}(E)$. If the projective embedding of X is E is an equivariant embedding with respect to an action of an affine group G, then the kernel of the evaluation map has the structure of a finite dimensional G-module. In the case of Grassmann codes that we discussed earlier (Example 1.2), the Plücker embedding of $Gr(l,V)$ is given by the $\mathbf{SL}_m$-representation $\bigwedge^l V$, which is well-known to be a simple $\mathbf{SL}_m$-module, hence, the corresponding evaluation map is injective. This is essentially the reason why one does not need to mention anything further about l; it is simply the dimension of the irreducible representation $\bigwedge^l V$. However, for all other projective embeddings of $Gr(l,V)$, the kernel of the evaluation map is not trivial since the corresponding $\mathbf{SL}_m$-module may not be simple. In general, the simpleness of the corresponding Weyl module strongly depends on the characteristic of the base field $\mathbb{F}_q$.

We are now ready to prove our main theorem.

Theorem 4.1. *Let C denote the projective $[n,k,d]$-system associated with the closed embedding obtained from the composition*

$$\iota: \ Gr(l,V) \longrightarrow \mathbb{P}(\prod^{r}(\wedge^l V)) \ \longrightarrow \mathbb{P}((\bigwedge^l V)^{\otimes r}).$$

Then the parameters of C satisfy

1. $n = \begin{bmatrix} m \\ l \end{bmatrix}_q$,
2. $q^{l(m-l)} - rq^{l(m-l)-1} \leq d \leq q^{l(m-l)} - (r-1)q^{l(m-l)-1}$,
3. $\dim soc_{\mathbf{SL}_m}(H^0(r\varpi_l)) \leq k \leq \dim H^0(r\varpi_l)$,

where $soc_{\mathbf{SL}_m} H^0(r\varpi_l)$ is the unique simple submodule of $H^0(r\varpi_l)$. Moreover, the upper bound for k is achieved if $H^0(r\varpi_l)$ is a simple $\mathbf{SL}_m$-module.

Before we give the proof of our main theorem, we have a remark in order.

Remark 4.2. First, let us point out that if the characteristic of the underlying field is big enough, then $H^0(r\varpi_l)$ is a simple $\mathbf{SL}_m$-module. In this case, we have $k = \dim H^0(r\varpi_l)$. As we will show in the sequel, the dimension of $H^0(r\varpi_l)$ can be calculated by the well-known Weyl dimension formula. These observations show that Theorem 1.3 follows from Theorem 4.1 when p is sufficiently big.

Secondly, even if $H^0(r\varpi_l)$ is not simple, in lower ranks, the formal character of $\mathrm{soc}_{\mathbf{SL}_n}(H^0(r\varpi_l))$, hence its dimension, is not so difficult to compute; see [10, Chapter II.8].

Proof. By our discussion from Subsection 2.2, the image of ι is contained in the projective subspace $\mathbb{P}(H^0(r\varpi_l)^*)$ in $\mathbb{P}((\bigwedge^l V)^{\otimes r})$; for $r = 2$, the corresponding embedding of $Gr(l,V)$ is explicitly given by the assignment (2.4). The case of an arbitrary $r \in \mathbb{N}$ is a straightforward generalization of this special case. Also, we already know that the number of $\mathbb{F}_q$-rational points of $Gr(l,V)$ is $\begin{bmatrix} m \\ l \end{bmatrix}_q$. This is the length of our code. We now proceed to compute the minimum distance.

Let $\mathcal{O}_{\mathbb{P}((\bigwedge^l V)^{\otimes r})}(1)$ denote the first Serre twist of the structure sheaf of $\mathbb{P}((\bigwedge^l V)^{\otimes r})$. The pullback of this line bundle under the Segre embedding is equal to the r-fold tensor product $\mathcal{O}_{\mathbb{P}(\bigwedge^l V)}(1) \boxtimes \cdots \boxtimes \mathcal{O}_{\mathbb{P}(\bigwedge^l V)}(1)$. The restriction of this product to the diagonal, which is isomorphic to $\mathbb{P}(\bigwedge^l V)$, is given by the multiplication of the sections of the factors; it lands in $\mathcal{O}_{\mathbb{P}(\bigwedge^l V)}(r)$. Therefore, we notice that a degree one hypersurface in $\mathbb{P}((\bigwedge^l V)^{\otimes r})$ determines a degree r hypersurface in $\mathbb{P}(\bigwedge^l V)$. Since our goal is to compute the minimum distance, we will work with the hypersurfaces in $\mathbb{P}((\bigwedge^l V)^{\otimes r})$ having the highest number of $\mathbb{F}_q$-rational points. Therefore, in light of Remark 2.17, we will consider the following degree r polynomial:

$$P := x_{s+1}(x_{s+1} - b_1 x_s)\cdots(x_{s+1} - b_{r-1}x_s) \in \mathbb{F}_q[x_{i_1}\cdots x_{i_r} :\ 1 \le i_1 \le \cdots \le i_r \le s+1], \tag{4.3}$$

where $b_1, \ldots, b_{r-1}$ are distinct nonzero elements of $\mathbb{F}_q$. In particular, the number of $\mathbb{F}_q$-rational points of the hypersurface $U_P := \{P = 0\}$ in $\mathbb{P}(\bigwedge^l V)$ is equal to $rq^{s-1} + \pi_{s-2}$.

Next, we intersect U_P with the Grassmann $Gr(l, V)$; we will determine the number of $\mathbb{F}_q$-rational points of the intersection. In other words, we want to determine the number

$$|\{M \in Gr(l, V) :\ (x_{s+1}(x_{s+1} - b_1 x_s)\cdots(x_{s+1} - b_{r-1}x_s))(M) = 0\}|. \tag{4.4}$$

We split our analysis of the defining equation in (4.4) into three major cases:

1. $x_{s+1}(M) = x_s(M) = 0$ and $M \in Gr(l, V)$;
2. $x_{s+1}(M) = 0$, $x_s(M) \neq 0$ and $M \in Gr(l, V)$;
3. $x_{s+1}(M) \neq 0$, $((x_{s+1} - b_1 x_s)\cdots(x_{s+1} - b_{r-1}x_s))(M) = 0$, and $M \in Gr(l, V)$.

In the first case, that is $\{M \in \mathbb{P}(\bigwedge^l V) :\ x_{s+1}(M) = x_s(M) = 0\} \cap Gr(l, V)$, we get every point M from $Gr(l, V)$ which is not contained in the Schubert cells of codimension ≤ 1. Since $Gr(l, V)$ has a unique Schubert divisor, we see that

$$|\{M \in \mathbb{P}(\bigwedge^{l} V) :\ x_{s+1}(M) = x_s(M) = 0\} \cap Gr(l, V)| = \begin{bmatrix} m \\ l \end{bmatrix} - q^{l(m-l)} - q^{l(m-l)-1}.$$

In the second case, we get precisely the codimension one Schubert cell in $Gr(l, V)$, which has $q^{l(m-l)-1}$ elements. Finally, in the third case, the intersection

$$\{M \in \mathbb{P}(\bigwedge^{l} V) :\ x_{s+1}(M) \neq 0,\ ((x_{s+1} - b_1 x_s)\cdots(x_{s+1} - b_{r-1}x_s))(M) = 0\} \cap Gr(l, V)$$

is a hypersurface in the dense Bruhat cell of $Gr(l, V)$. Since the defining equation of this hypersurface is given by $(x_{s+1}(M) - b_1 x_s)\cdots(x_{s+1}(M) - b_{r-1}x_s) = 0$, where $x_{s+1}(M) \neq 0$, and b_i's are distinct elements from $\mathbb{F}_q$, this hypersurface has exactly $(r-1)q^{l(m-l)-1}$ $\mathbb{F}_q$-rational points, see Remark 2.17. Thus, we see that the total number of zeros of the homogeneous polynomial $x_{s+1}(x_{s+1} - b_1 x_s)\cdots(x_{s+1} - b_{r-1}x_s)$ on $Gr(l, V)$ is given by

$$\begin{aligned} &\left(\begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} - q^{l(m-l)-1}\right) + q^{l(m-l)-1} + (r-1)q^{l(m-l)-1} \\ &= \begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} + (r-1)q^{l(m-l)-1}. \end{aligned}$$

It follows that an upper bound for the minimum distance on $Gr(l, V)$ in $\mathbb{P}((\bigwedge^l V)^{\otimes r})$ is given by

$$\begin{bmatrix} m \\ l \end{bmatrix}_q - \left(\begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} + (r-1)q^{l(m-l)-1} \right) = q^{l(m-l)} - (r-1)q^{l(m-l)-1}. \tag{4.5}$$

Next, we will prove our formula for the lower bound for the minimum distance. To this end, let Q be a homogeneous degree r polynomial from $\mathbb{F}_q[x_1, \dots, x_{s+1}]$ such that the intersection $H_Q \cap Gr(l, V)$ attains the maximum number of $\mathbb{F}_q$-rational points among all such intersections. Here, H_Q denotes the hypersurface in $\mathbb{P}(\bigwedge^l V)$ defined by Q. It follows that the intersection of H_Q with the open cell of $Gr(l, V)$ is nonempty. We assume that this intersection attains the maximum number $rq^{l(m-l)-1}$, see Remark 2.17. Under these assumptions, we see that

$$|H_Q \cap Gr(l, V)|_{\mathbb{F}_q} \leq rq^{l(m-l)-1} + \begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)}, \tag{4.6}$$

where $\begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)}$ is the number of $\mathbb{F}_q$-rational points in the complement of the open cell in the Grassmannian. Since (4.6) is an upper bound for the number of zeros of Q on $Gr(l, V)$ over $\mathbb{F}_q$, a lower bound for the minimum distance is given by

$$\begin{bmatrix} m \\ l \end{bmatrix}_q - \left(\begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} + rq^{l(m-l)-1} \right) = q^{l(m-l)} - rq^{l(m-l)-1}. \tag{4.7}$$

By combining (4.5) and (4.7), we obtain the following inequalities for the minimum distance,

$$q^{l(m-l)} - rq^{l(m-l)-1} \leq d \leq q^{l(m-l)} - (r-1)q^{l(m-l)-1}. \tag{4.8}$$

It remains to compute the dimension of our code. Since the image of ι is contained in $\mathbb{P}((H^0(Gr(l, V), \mathcal{L}(r\varpi_l))^*)$, the image of the evaluation map $\text{ev} : ((\bigwedge^l V)^{\otimes r})^* \to \mathbb{F}_q^n$ agrees with the image of the (restricted) evaluation map $\text{ev} : H^0(r\varpi_l)^* \to \mathbb{F}_q^n$. On one hand, if $H^0(r\varpi_l)$ is a simple $\mathbf{SL}_m$-module, then so is $H^0(r\varpi_l)^*$. In this case, the kernel of the evaluation map is trivial, hence, $k = \dim H^0(r\varpi_l)$. On the other hand, if our finite dimensional module $H^0(r\varpi_l)$ is not simple, then it is not guaranteed that the kernel of the evaluation map is trivial. Nevertheless, it is always true that the sum of all simple submodules, namely, the socle of $H^0(r\varpi_l)$, is not contained in the kernel. Indeed, it is well-known that $\text{soc}_{\mathbf{SL}_m} H^0(r\varpi_l)$ is simple [10, Corollary II.2.3], so, if it were contained in the kernel, then the evaluation map has to map the whole vector space to 0, which would be absurd. This argument shows that the dimension of the evaluation map is at least as big as $\dim \text{soc}_{\mathbf{SL}_m} H^0(r\varpi_l)$. Hence, the proof of our assertion is finished. □

We conclude this subsection by a remark that expands on the last part of the proof of our Theorem 4.1. Let λ denote the (dominant) weight $r\varpi_l$. We assume that $H^0(\lambda)$ is a simple $\mathbf{SL}_m$-module. Then, as we pointed out before in Remark 2.9, the Weyl module $V(\lambda)$ is isomorphic to $H^0(\lambda)$. Since $V(\lambda)$ is generated, as an $\mathbf{SL}_m$-module, by a B-stable

1	1	2	2	5
2	2	3	4	
3	4	5		

Fig. 4.1. A semistandard Young tableau of shape $(5,4,3)$.

line of weight λ [10, Ch. II, Lemma 2.13], we see that the $\mathbf{SL}_m$-orbit of a nonzero vector in the socle of $H^0(\lambda)^*$ generates the whole module. In our case, the $\mathbf{SL}_m$-orbit of a nonzero vector on such a line is isomorphic to $Gr(l,V)$. (This fact is also well-known, [10, Ch II, §2.16].) Thus, the projective space on $H^0(\lambda)^*$ is spanned by the image of the embedding of our Grassmann variety.

4.1. Weyl's character and dimension formulas

Let $\lambda = r\varpi_l$ ($r \in \mathbb{N}$) be a dominant weight for $\mathbf{SL}_m$. As we mentioned before, assuming that $H^0(r\varpi_l)$ is simple, its character and dimension can be computed as if we are working over the field of complex numbers. In particular, in this case we can apply the well-known combinatorics of Young tableaux. The purpose of this subsection is to briefly explain how this methodology works. A general reference for this material is [4].

Recall that the monoid of dominant weights for $(\mathbf{SL}_m, \mathbf{B}_m, \mathbf{T}_m)$ is generated by the fundamental weights ϖ_i $(1 \le i \le m-1)$. Let $a_1\varpi_1 + \cdots + a_{m-1}\varpi_{m-1} \in X(\mathbf{T}_m)_+$ be a dominant weight for some nonnegative integers $a_i \in \mathbb{N}$ $(1 \le i \le m-1)$, and set $\lambda_m := 0$. Then the sequence $\lambda = (\lambda_1, \ldots, \lambda_m)$ defined by the equations,

$$\lambda_i - \lambda_{i+1} = a_i \quad \text{for } i \in [m-1]$$

is an integer partition, that is, $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_m$. Clearly, if we are given λ, then we can solve these equations for a_i's as well. In other words, there is a one-to-one correspondence between the integer partitions and the dominant weights for the special linear groups. In light of this bijection, $a_1\varpi_1 + \cdots + a_{m-1}\varpi_{m-1} \leftrightsquigarrow \lambda$, hereafter, for the sake of brevity, let us denote by $W(\lambda)$ the simple module $H^0(Gr(l,V), \mathcal{L}(a_1\varpi_1 + \cdots + a_{m-1}\varpi_{m-1}))^*$.

Let $\lambda = (\lambda_1, \ldots, \lambda_m)$ be an integer partition. Recall that the Young diagram of λ is a top-left justified arrangement of the boxes with λ_i boxes in the i-th row. A *semistandard Young tableau of shape* λ (or, an *SSYT of shape* λ, for short) is a filling of the boxes of the Young diagram of shape λ with positive integers that is weakly increasing in every row and strictly increasing in every column. For example, in Fig. 4.1, we have an SSYT of shape $(5,4,4)$. Let T be an SSYT of shape λ. Let us define the *weight of* T as the monomial $x^T := x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}$, where the integer i_j $(1 \le j \le k)$ appears in T n_j times. Then the character of a simple $\mathbf{SL}_m(\mathbb{C})$-module $W(\lambda)$ is given by the *Schur function* $s_\lambda(x_1, \ldots, x_m)$ which is defined as the weight generating function of all SSYT of shape λ,

$$s_\lambda(x_1, \ldots, x_m) = \sum_{\text{T: SSYT of shape } \lambda} x^T.$$

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)
(2, 1)	(2, 2)	(2, 3)	(2, 4)	
(3, 1)	(3, 2)	(3, 3)		

Fig. 4.2. The coordinates of the boxes of $(5, 4, 3)$.

0	1	2	3	4
−1	0	1	2	
−2	−1	0		

7	6	5	3	1
5	4	3	1	
3	2	1		

Fig. 4.3. The contents and the hook lengths of the boxes of $(5, 4, 3)$.

In particular, by specializing the variables x_i $(1 \leq i \leq n)$ to 1, we get the dimension of $W(\lambda)$,

$$\dim W(\lambda) = \#\text{ SSYT of shape } \lambda \text{ filled with entries from } \{1, \dots, m\}.$$

This number can be calculated in a combinatorial way by the *hook length formula*. To explain this formula, we first put coordinates on the boxes of the Young diagram of $\lambda = (\lambda_1, \dots, \lambda_m)$ by identifying it with the set $\{(i, j) : \; j \in [\lambda_i], \; i \in [m]\}$. For example, the coordinates of the integer partition $(5, 4, 3)$ are depicted in Fig. 4.2.

The *content* of a box $u = (i, j)$ in the Young diagram of λ is defined as $c(u) := j - i$. The *hook length of* u, denoted by $h(u)$ is defined as the number of boxes directly to the right of u and directly below u, counting u itself once. In Fig. 4.3, the diagram on the left shows the contents and the diagram on the right shows the hook lengths of the boxes of λ.

In this notation we have the following concrete form of the Weyl's dimension formula,

$$s_\lambda(1, \dots, 1) = \prod_{u \in \text{Young diagram of } \lambda} \frac{m + c(u)}{h(u)}. \tag{4.9}$$

Example 4.10. Let V be a three dimensional vector space over $\mathbb{C}$. Let $l = 2$. In this case, the partition corresponding to the dominant weight ϖ_l is $\lambda = (1, 1)$, and therefore, we have the following SSYT tableaux for the irreducible representation $W(\lambda) \cong H^0(Gr(2, V), \mathcal{L}(\varpi_2))$:

$$\begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline \end{array} \qquad \begin{array}{|c|}\hline 1 \\ \hline 3 \\ \hline \end{array} \qquad \begin{array}{|c|}\hline 2 \\ \hline 3 \\ \hline \end{array}$$

Note that, corresponding to each SSYT of shape λ, there is a Plücker coordinate function. For the tableaux in the above example, the Plücker coordinate functions are given by p_{12}, p_{13}, and p_{23}. In particular, we have

$$\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & 2 \\ \hline \end{array} \quad \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 3 & 3 \\ \hline \end{array} \quad \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & 3 \\ \hline \end{array} \quad \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 3 \\ \hline \end{array} \quad \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 3 \\ \hline \end{array} \quad \begin{array}{|c|c|}\hline 2 & 2 \\ \hline 3 & 3 \\ \hline \end{array}$$

Fig. 4.4. The set of SSYT of shape $(2,2)$ with entries from $\{1,2,3\}$.

$$\dim W(\lambda) = \dim H^0(Gr(2,V), \mathcal{L}(\varpi_2)) = 3.$$

Example 4.11. We preserve our notation from Example 4.10. The partition corresponding to $2\varpi_2$ is given by $\lambda = (2,2)$. Thus, the SSYT's corresponding to the "Plücker coordinates" of the embedding for the line bundle $\mathcal{L}(2\varpi_2)$ are listed in Fig. 4.4. In particular, we see that $H^0(Gr(2,\mathbb{C}^3), \mathcal{L}(2\varpi_2))$ is six dimensional. Of course, we can get the same count by using formula in (4.9).

Before we describe an application of this combinatorics to our main theorem, let us point out, by our running example, that for every sufficiently big characteristic $p > 0$, the $\mathbf{SL}_m(\mathbb{F}_q)$-module $H^0(r\omega_l)$ is simple.

Example 4.12. For $\mathbf{SL}_3$, ρ denotes $\varpi_1 + \varpi_2$. Then $2\varpi_2 + \rho = \varpi_1 + 3\varpi_2$. By definition, the fundamental dominant weight ϖ_i is the dual of the coroot $\alpha_i^\vee$. Therefore, we have

$$\begin{aligned} \langle \varpi_1 + 3\varpi_2, \alpha_1^\vee \rangle &= 1, \\ \langle \varpi_1 + 3\varpi_2, \alpha_2^\vee \rangle &= 3, \\ \langle \varpi_1 + 3\varpi_2, (\alpha_1+\alpha_2)^\vee \rangle &= 4. \end{aligned}$$

Now by Remark 2.10, we see that for every prime characteristic $p \geq 5$, the $\mathbf{SL}_3(\mathbf{F}_q)$-module $W(\lambda)$ is simple.

Corollary 4.13. *For every sufficiently big prime characteristic p, the dimension of the code C defined in Theorem 4.1 is given by*

$$\dim H^0(r\varpi_l) = \frac{\prod_{i=0}^{l-1}(m-i)^{(r)}}{\prod_{i=1}^{l}(i)^{(r)}}. \tag{4.14}$$

Proof. Thanks to Remark 2.10, we know that for every sufficiently big prime characteristic, the $\mathbf{SL}_m$-module $H^0(r\omega_l)$ is simple. Theorem 4.1 implies that the dimension of our code is given by the Weyl's dimension formula. The integer partition $\lambda = (\lambda_1, \ldots, \lambda_m)$ that corresponds to the dominant weight $r\varpi_l$ is given by

$$\lambda_1 = \cdots = \lambda_l = r \;\text{ and }\; \lambda_j = 0 \;\text{ for } j \in \{l+1, \ldots, m\}.$$

The contents and the hook lengths of the boxes of λ are depicted in Fig. 4.5.

To finish the proof, we will use the formula in (4.9) by using the content and hook length tableaux that are shown in (4.5). To keep track of the products, we multiply

0	1	2	$\cdots$	$r-1$
-1	0	1	$\cdots$	$r-2$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$-(l-1)$	$-(l-2)$	$-(l-3)$	$\cdots$	$-(l-r)$

$l+r-1$	$l+r-2$	$l+r-3$	$\cdots$	l
$l+r-2$	$l+r-2$	$l+r-3$	$\cdots$	$l-1$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
r	$r-1$	$r-2$	$\cdots$	1

Fig. 4.5. The contents and the hook lengths of the boxes of $(r,\dots,r,0,\dots,0)$.

the entries row-by-row, from top-to-bottom. We multiply the entries of the rows of the content tableau from left-to-right:

$$\begin{aligned}
&\text{Row 1}: m\cdot(m+1)\cdots(m+r-1)=m^{(r)},\\
&\text{Row 2}: (m-1)\cdot m\cdots(m+r-2)=(m-1)^{(r)},\\
&\qquad\vdots\\
&\text{Row l}\ : (m-(l-1))\cdot(m-(l-2))\cdots(m-(l-r))=(m-(l-1))^{(r)}.
\end{aligned}$$

Thus, the numerator of the hook length formula is given by $\prod_{i=0}^{l-1}(m-i)^{(r)}$. For the hook length tableau, we multiply the entries of the rows from right-to-left:

$$\begin{aligned}
&\text{Row 1}: l\cdot(l+1)\cdots(l+r-1)=l^{(r)},\\
&\text{Row 2}: (l-1)\cdot l\cdots(l+r-2)=(l-1)^{(r)},\\
&\qquad\vdots\\
&\text{Row l}\ : 1\cdot 2\cdots r=(1)^{(r)}.
\end{aligned}$$

Then the denominator of the hook length formula is given by $\prod_{i=0}^{l-1}(1+i)^{(r)}$. This finishes the proof of our corollary. □

Proof of Theorem 1.3. In light of Remark 2.10, we choose a sufficiently large prime characteristic p so that $H^0(r\omega_l)$ is a simple $\mathbf{SL}_m$-module. Then the dimension k of our code is equal to $\dim H^0(r\omega_l)$. Hence, our theorem follows from Theorem 4.1 and Corollary 4.13. □

Example 4.15. We consider the embedding associated with the highest weight $2\varpi_3$ of the Grassmann variety $Gr(3,\mathbb{F}_q^5)$, where the characteristic of $\mathbb{F}_q$ is sufficiently large so that $H^0(2\varpi_3)$ is a simple $\mathbf{SL}_5$-module. Then the parameters of our code are given by

$$\begin{aligned}
n&=\begin{bmatrix}5\\3\end{bmatrix}_q=\frac{[5]_q[4]_q[3]_q}{[3]_q[2]_q[1]_q}=1+q+2q^2+2q^3+2q^4+q^5+q^6,\\
k&=\frac{5^{(2)}4^{(2)}3^{(2)}}{1^{(2)}2^{(2)}3^{(2)}}=\frac{5\cdot6\cdot4\cdot5\cdot3\cdot4}{1\cdot2\cdot2\cdot3\cdot3\cdot4}=50,
\end{aligned}$$

and

$$q^6 - 2q^5 \leq d \leq q^6 - q^5.$$

Note that, if $q > 3$, then $n - d$ is significantly bigger than $k = 50$.

References

[1] Michel Brion, Lectures on the geometry of flag varieties, in: Topics in Cohomological Studies of Algebraic Varieties, in: Trends Math., Birkhäuser, Basel, 2005, pp. 33–85.

[2] Roger W. Carter, George Lusztig, On the modular representations of the general linear and symmetric groups, Math. Z. 136 (1974) 193–242.

[3] Mrinmoy Datta, Sudhir R. Ghorpade, On a conjecture of Tsfasman and an inequality of Serre for the number of points of hypersurfaces over finite fields, Mosc. Math. J. 15 (4) (2015) 715–725.

[4] William Fulton, Young Tableaux, London Mathematical Society Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997, with applications to representation theory and geometry.

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

[6] Sudhir R. Ghorpade, Michael A. Tsfasman, Schubert varieties, linear codes and enumerative combinatorics, Finite Fields Appl. 11 (4) (2005) 684–699.

[7] Søren Have Hansen, Error-correcting codes from higher-dimensional varieties, Finite Fields Appl. 7 (4) (2001) 531–552.

[8] Robin Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York-Heidelberg, 1977.

[9] Jens Carsten Jantzen, Darstellungen halbeinfacher algebraischer Gruppen und zugeordnete kontravariante Formen, Bonner Math. Schr. 67 (1973), v+124.

[10] Jens Carsten Jantzen, Representations of Algebraic Groups, second edition, Mathematical Surveys and Monographs, vol. 107, American Mathematical Society, Providence, RI, 2003.

[11] Gilles Lachaud, The parameters of projective Reed-Muller codes, Discrete Math. 81 (2) (1990) 217–221.

[12] Rudolf Lidl, Harald Niederreiter, Finite Fields, second edition, Encyclopedia of Mathematics and Its Applications., vol. 20, Cambridge University Press, Cambridge, 1997, with a foreword by P. M. Cohn.

[13] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes. II, North-Holland Mathematical Library, vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[14] D.Yu. Nogin, Codes associated to Grassmannians, in: Arithmetic, Geometry and Coding Theory, Luminy, 1993, De Gruyter, Berlin, 1996, pp. 145–154.

[15] F. Rodier, Codes from flag varieties over a finite field, J. Pure Appl. Algebra 178 (2) (2003) 203–214.

[16] Charles Ryan, An application of Grassmannian varieties to coding theory, in: Sixteenth Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Man., 1986, vol. 57, 1987, pp. 257–271.

[17] Charles T. Ryan, Kevin M. Ryan, The minimum weight of the Grassmann codes $C(k, n)$, Discrete Appl. Math. 28 (2) (1990) 149–156.

[18] Jean-Pierre Serre, Lettre à M. Tsfasman, (Luminy, 1989), Journées Arithmétiques 198–200 (1991) 11, 351–353.

[19] Anders Bjært Sørensen, Projective Reed-Muller codes, IEEE Trans. Inf. Theory 37 (6) (1991) 1567–1576.

[20] Richard P. Stanley, Enumerative Combinatorics, vol. 1, second edition, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012.

[21] Michael Tsfasman, Serge Vlăduţ, Dmitry Nogin, Algebraic Geometric Codes: Basic Notions, Mathematical Surveys and Monographs, vol. 139, American Mathematical Society, Providence, RI, 2007.