Finite Fields and Their Applications 89 (2023) 102211

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Higher Grassmann codes II

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*

ARTICLE INFO

Article history:
Received 24 April 2022
Received in revised form 29 December 2022
Accepted 28 March 2023
Available online xxxx
Communicated by Gary L. Mullen

MSC:
94B27
14G50
14M15
94B05

Keywords:
Higher Grassmann codes
Parameters of a code

ABSTRACT

We compute the parameters of the linear codes that are associated with higher dimensional projective embeddings of Grassmannian when the degree exceeds the number of elements of the finite field. We investigate various dimension formulas for the projective Reed-Müller codes. We show that the duals of higher Grassmann codes are given by higher Grassmann codes or their simple extensions.

1. Introduction

In this article, we continue our work [1] on the higher Grassmann codes, which are defined as follows. Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a power

* 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.2023.102211

of a prime number. For positive integers l and m such that $l \leq m$, let V denote the vector space $\overline{\mathbb{F}}_q^m$, where $\overline{\mathbb{F}}_q$ stands for an algebraic closure of $\mathbb{F}_q$. Let $Gr(l,V)$ denote the Grassmann variety of l-dimensional subspaces of V. 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 Segre embedding of $\prod_{i=1}^r \mathbb{P}(\bigwedge^l V)$. The *$r$-th order (higher) Grassmann code* is the code determined by the projective system corresponding to ι. Note that an r-th order projective Reed-Müller code can be regarded as an r-th order Grassmann code.

In [1], we found the parameters of higher Grassmann codes under the assumption that $2 \leq r < q-1$. For the *classical case*, that is, when $r = 1$, the parameters of Grassmann codes were studied previously; Ryan and Ryan detailed the binary case in [12], and the parameters of the q-ary case were determined by Nogin, [9]. In the present article, we further relax the assumption on r to the interval

$$1 \leq r \leq (q-1)(\dim Gr(l,V)) - 1.$$

Note that this is the true upper bound to get interesting codes. Once the degree of our code exceeds the critical number $(q-1)\dim Gr(l,V) - 1$, we do not get any new codewords since all codewords are obtained by evaluating the polynomials at $\mathbb{F}_q$-rational points. Indeed, if a variable x appears with a degree bigger than $q-1$ in a polynomial function, then that power of x can be reduced modulo $x^q - x$ without changing the value of the polynomial function.

A significant portion of this article is about the extension of our earlier results from [1] to the Grassmann codes of arbitrary order. The methods of [1] do not readily apply to the extended setting for several reasons. First of all, for the minimum distance calculations, we have to work with a higher dimensional space of functions. As a result, the bounds on the minimum distances of the extended codes are different than the ones that we presented in [1]. Secondly, for the dimension calculations, our previous representation theoretic approach does not directly apply. Indeed, for $r \in \{1, \dots, q-1\}$, we can always choose a sufficiently large q to ensure that the corresponding r-th order Grassmann code is a simple $\mathbf{SL}_m(\mathbb{F}_q)$-module. Then we can use the well-known Weyl character formula to compute its dimension. However, if r is in the range $\{q-1, q, \dots, \dim Gr(l,V) - 1\}$, then our code may not be a simple $\mathbf{SL}_m(\mathbb{F}_q)$-module anymore. To obtain the dimension formula, we have to first prove a technical result that is akin to a weak form of Hilbert's nullstellensatz for the $\mathbb{F}_q$-rational points of a Grassmann variety (Theorem 4.9). Only after this we could use important determinantal formulas that go back to MacMahon [8] combined with the deep algebro-combinatorial techniques of Rota [11] to calculate the dimension of a higher Grassmann code (Theorem 5.3). In this regard, the first main result of our article is an elaboration of the dimension formula for the projective Reed-Müller codes. We provide two formulations of the dimension in two different expressions in Propositions 3.5 and 3.9. The reason why we had to deal with this issue in the first place is that, these computations, especially the one in Proposition 3.9, hold keys to a formula for the dimension of a higher Grassmann code. We should also mention that our dimension formulas are new even for the projective Reed-Müller codes.

Let C denote the r-th order Grassmann code. Another major result of our article is a duality result, that is Theorem 7.4. Roughly speaking, it states that the dual of C is either another higher Grassmann code, or an extension of a higher Grassmann code by an all-1 codeword. An important consequence of this result is that every higher Grassmann code is self-orthogonal. This can be seen as a generalization of the duality properties of the projective Reed-Müller codes. Our duality theorem readily enables us to apply the results of the present paper along with some rather well-known techniques such as the Calderbank-Shore-Steane method to produce quantum codes from the higher Grassmann codes. This will be explored in a separate paper.

We are now ready to give a brief outline of our paper. In the next preliminaries section we setup our notation. In Section 3, we analyze some dimension formulas for the projective Reed-Müller codes. In Section 4, we describe our weak $\mathbb{F}_q$-nullstellensatz for the set of $\mathbb{F}_q$-rational points, $Gr(l, V)(\mathbb{F}_q)$. Section 5 is devoted to the dimension computations. The main result of Section 6 is Theorem 6.2, which describes the bounds for the minimum distance of a Grassmann code of degree ν. These bounds are natural extensions of the bounds that we found in our first paper [1, Theorem 1.3, part 3]. Finally, our main duality theorem is proven in Section 7.

Acknowledgment

The first author was partially supported by a grant from the Louisiana Board of Regents (contract no. LEQSF(2021-22)-ENH-DE-26). The third author was partially supported by a grant from the Simons Foundation (Award ID: 830817, GVR). The authors would like to thank the referee for carefully reading the earlier draft and providing valuable suggestions that improved the present version.

2. Preliminaries and notation

Throughout this text, $\mathbb{Z}_+$ will stand for the set of all positive integers. Let $n \in \mathbb{Z}_+$. Let $v \in \mathbb{F}_q^n$. The *Hamming weight* of v, denoted by $||v||$, is the number of nonzero coordinates of v. In this paper, by an $[n, k, d]$*-code over* $\mathbb{F}_q$ we mean a k-dimensional subspace $C \subseteq \mathbb{F}_q^n$ such that

$$d = \min\{||v|| : \quad v \text{ is a nonzero vector in } C\}.$$

Let $\langle , \rangle$ denote the standard dot product on $\mathbb{F}_q$. Let C be an $[n, k, d]$ code over $\mathbb{F}_q$. The *dual of* C is the code defined by

$$C^\perp := \{v \in \mathbb{F}_q^n : \ \langle v, w\rangle = 0 \ \text{ for all } w \in C\}.$$

The length and dimension of $C^{\perp}$ are given by n and $n-k$, respectively. The code that is defined as the linear span of the union $\{\mathbf{1}_n\} \cup C$ in $\mathbb{F}_q^n$ will be denoted by $\overline{C}$. Although it is not a standard name, we will call $\overline{C}$ the *all-one vector extension of* C.

Let X be a variety defined over $\mathbb{F}_q$. The set of $\mathbb{F}_q$-rational points of X is denoted by $X(\mathbb{F}_q)$. To relax our notation, whenever the underlying field is apparent from the context, we write $|X|$ to denote the number of $\mathbb{F}_q$-rational points of X. We fix the following letters throughout our paper:

n : the length of an unspecified code,
k : the dimension of an unspecified code,
d : the minimum distance of an unspecified code,
d : the dimension of the Grassmann variety, $Gr(l, V)$, where $V = \mathbb{F}_q^m$,
e : the dimension of the projective space, $\mathbb{P}(\bigwedge^l V)$.

Then, in the notation of the introduction, we have, $\mathsf{d} := l(m-l)$ and $\mathsf{e} := \binom{m}{l} - 1$.

Let $a \in \mathbb{Z}_+$, and let x be a variable. The *a-th rising factorial of x*, denoted by $x^{(a)}$, is the product $x^{(a)} = x(x+1)\cdots(x+a-1)$. The set $\{1, \ldots, a\}$ is denoted by $[a]$. The polynomial $1 + q + \cdots + q^{a-1}$, denoted by $[a]_q$, is called the *q-analog* of a. Note that $[a]_q = \frac{q^a-1}{q-1}$. We set $[0]_q := 1$. The product $[1]_q[2]_q \cdots [a]_q$, called the *q-factorial of a*, is denoted by $[a]_q!$. Let $\{a, b\} \subset \mathbb{N}$. The *$q$-binomial coefficient* is defined by

$$\begin{bmatrix} a \\ b \end{bmatrix}_q := \begin{cases} \frac{[a]_q!}{[a-b]_q![b]_q!} & \text{if } a \geq b, \\ 0 & \text{if } a < b. \end{cases}$$

Let α be a finite sequence of nonnegative integers. If the sum of the parts of α is equal to m, then α is called a *weak composition of* m. For example $(1, 3, 0, 2)$ is a weak composition of 6. If a weak composition of m has no 0 entries then, it is called a *composition of* m. An *(integer) partition of* m is a composition of m with nonincreasing parts. When we want to emphasize that a given sequence is a composition of m, we will write $\alpha \vDash m$.

Let $\mathbf{B}_m(\overline{\mathbb{F}}_q)$ denote the Borel subgroup of all upper triangular matrices in $\mathbf{SL}_m(\overline{\mathbb{F}}_q)$. A *Schubert variety* in $Gr(l, V)$ is the Zariski closure of a $\mathbf{B}_m(\overline{\mathbb{F}}_q)$-orbit. The *boundary* of a Schubert variety in $Gr(l, V)$ is the complement of the open Borel subgroup in that Schubert variety. In particular, the boundary of $Gr(l, V)$, denoted by $\partial Gr(l, V)$, is the unique one codimensional Schubert variety in $Gr(l, V)$.

It is well-known that the Schubert subvarieties of $Gr(l, V)$ are indexed by the integer partitions whose Young diagrams fit into the $l \times (m-l)$ rectangle. In this correspondence, the unique 0-dimensional Schubert variety is indexed by the integer partition of 0, whose Young diagram is the empty set. The boundary of $Gr(l, V)$ corresponds to the Schubert variety indexed by the partition $(m-l, m-l, \ldots, m-l, m-l-1)$.

Example 2.1. Let V be a four dimensional vector space. Let $l = 2$. There are five positive dimensional Schubert varieties. They are indexed by the integer partitions whose Young

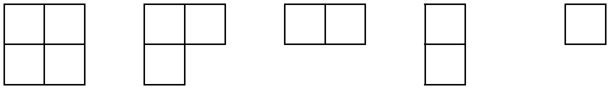

Fig. 2.1. The Young diagrams of the integer partitions whose Young diagram fits in a 2×2 grid.

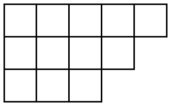

Fig. 2.2. The Young diagram of $(5, 4, 3)$.

diagram fits into 2×2 grid (Fig. 2.1). Then $\partial Gr(2, V)$ corresponds to the Young diagram of $(2, 1)$.

Let α and β be two integer partitions. If the Young diagram of α is contained in the Young diagram of β, then we will write $\alpha \leq \beta$. This order on the integer partitions whose Young diagrams fit into $l \times (m - l)$ grid is called the *Bruhat-Chevalley order*. It has an important geometric interpretation. Let X_α and X_β denote the Schubert varieties corresponding to the partitions α and β. Then we have

$$\alpha \leq \beta \iff X_\alpha \subseteq X_\beta. \tag{2.2}$$

Following [10], we denote the partial order defined in (2.2) by $\mathbf{A}_{m-1}(l)$.

Let $\gamma = (\gamma_1, \ldots, \gamma_s)$ be a composition. The *diagram of* γ is a top-left justified array of boxes, where the i-th row of the array has γ_i boxes for $i \in \{1, \ldots, s\}$. Likewise, let $\lambda = (\lambda_1, \ldots, \lambda_s)$ be an integer partition. The *Young diagram of* λ is a top-left justified array of boxes, where the i-th row of the array has λ_i boxes for $i \in \{1, \ldots, s\}$. To given an example, we depict the Young diagram of the partition $\lambda = (5, 4, 3)$ in Fig. 2.2.

Let K be a field. Let $K[x_1, \ldots, x_m]$ be a polynomial ring over K with m variables. The *support* of a monomial $x_{i_1}^{a_{i_1}} x_{i_2}^{a_{i_2}} \cdots x_{i_r}^{a_{i_r}} \in K[x_1, \ldots, x_m]$, where $a_{i_1}, \ldots, a_{i_r}$ are positive integers, is the set of variables $\{x_{i_1}, \ldots, x_{i_r}\}$. By allowing 0 as an exponent, let us write $x_{i_1}^{a_{i_1}} x_{i_2}^{a_{i_2}} \cdots x_{i_r}^{a_{i_r}}$ in the form $x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$. Then we can identify the sequence of exponents, $(a_1, \ldots, a_m)$, as a weak composition with m parts. To determine the count of the monomials of total degree r, we add $(1, \ldots, 1)$ to $(a_1, \ldots, a_m)$. Then we get a monomial of total degree $r + m$ whose support is $\{x_1, \ldots, x_m\}$. These monomials are in one-to-one correspondence with the compositions of $m + r$ with m parts. Therefore, the number of monomials of degree r in m variables is $\binom{m+r-1}{m-1}$. For details of this composition counting, see [15, pg. 18].

In the sequel, the notation of modular arithmetic will be used. Let q be a power of a prime number. Let r be a positive integer. When we write $t \equiv r \mod q - 1$ for some $t \in \mathbb{Z}$, we mean that $t - r$ is divisible by $q - 1$. When we write $t = r \mod q - 1$, we mean that $t \in \{0, \ldots, q - 1\}$, and t is the remainder of division of r by $q - 1$.

3. Projective Reed-Müller codes

Let $m \in \mathbb{Z}_+$. For $\nu \in \mathbb{Z}_+$, we denote by $\mathbb{F}_q[x_0, \dots, x_m]_h^\nu$ the set of all homogeneous polynomials of degree ν from $\mathbb{F}_q[x_0, \dots, x_m]$. By adding 0 to $\mathbb{F}_q[x_0, \dots, x_m]_h^\nu$, we obtain a vector space of dimension $\binom{m+\nu}{\nu}$. Let $P_1, \dots, P_n$ be the list of all $\mathbb{F}_q$-rational points of $\mathbb{P}^m$. Then we have

$$n = |\mathbb{P}^m| = [m+1]_q.$$

The *projective Reed-Müller code of degree* ν *over* $\mathbb{F}_q$, denoted $PC_\nu(m, q)$, is defined as follows:

$$PC_\nu(m, q) := \{(F(P_1), \dots, F(P_n)) \in \mathbb{F}_q^n : \ F(x_0, \dots, x_n) \in \mathbb{F}_q[x_0, \dots, x_m]_h^\nu\}. \quad (3.1)$$

For $\nu \in [q-2]$, the parameter of the projective Reed-Müller codes of degree ν were first determined by Lachaud in [7]. For $\nu \geq q-1$, the parameters are determined by Sorensen [14] except for the dimension formula which we proceed to explain.

In [14, Theorem 1], Sorensen stated the following formula for the dimension of $PC_r(m, q)$:

$$\dim PC_\nu(m, q) = \sum_{\substack{0 < t \leq \nu \text{ s.t.} \\ t \equiv \nu \mod q-1}} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t - jq + m}{t - jq} \right). \quad (3.2)$$

We claim that this dimension formula is not correct. We will use a well-known identity that is obtained by the “finite differences” formalism.

Lemma 3.3. *Let K be a field. Let $P(x) \in K[x]$ be a polynomial of the form $P(x) := a_0 + a_1 x + \cdots + a_e x^e$. Then we have*

$$\sum_{j=0}^{e} (-1)^j \binom{e}{j} P(j) = (-1)^e e! a_e.$$

Proof. Our assertion is stated (in a different notation) in [4, pg 190]. $\square$

Let $P(x) \in \mathbb{Q}[x]$ be the polynomial defined by

$$P(x) := \frac{(t - xq)(t - xq - 1) \cdots (t - xq - (m-1))}{m!}.$$

For every integer $j \in \mathbb{N}$, we have

$$P(j) = \binom{t - jq + m}{m} = \binom{t - jq + m}{t - jq}.$$

We now apply Lemma 3.3 to $P(x)$. Since $\deg P(x) = m$, we find

$$\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} P(j) = 0. \tag{3.4}$$

The identity in (3.4) shows that the r.h.s. of Soresen's formula (3.2) is always 0. The correct formula for $\dim PCR_\nu(m,q)$ is given in our proposition.

Proposition 3.5. *The dimension of the projective Reed-Müller code of degree ν is given by*

$$\dim PCR_\nu(m,q) = \sum_{\substack{t \in [\nu] \\ t \equiv \nu \mod q-1}} \sum_{i=0}^{\lfloor t/q \rfloor} (-1)^i \binom{m+1}{i} \binom{m+t-iq}{m}.$$

Proof. Let us compute the cardinality of the set

$$\left\{ x_0^{i_0} x_1^{i_1} \cdots x_m^{i_m} \;:\; \begin{array}{c} i_0 + \cdots + i_m = t \text{ and,} \\ 0 \le i_j \le q-1 \text{ for } j \in \{0,\dots,m\} \end{array} \right\} \tag{3.6}$$

as follows. The elements (3.6) are in one-to-one correspondence with the weak compositions of t with at most $m+1$ parts, and each part less than q. Let $N(t, m+1, q-1)$ denote the cardinality of this set. Then we have

$$[x^t](1 + x + \cdots + x^{q-1})^{m+1} = N(t, m+1, q-1), \tag{3.7}$$

where $[x^a]h(x)$ ($a \in \mathbb{N}$, $h(x)$ is a polynomial) stands for the coefficient of x^a in $h(x)$. By using the binomial theorem and a related generating series [4, eqn. (5.56)], we notice that

$$\begin{aligned} (1 + x + \cdots + x^{q-1})^{m+1} &= (1 - x^q)^{m+1} \frac{1}{(1-x)^{m+1}} \\ &= \left(\sum_{i=0}^{m+1} (-1)^i \binom{m+1}{i} (x^q)^i \right) \left(\sum_{i=0}^{\infty} \binom{m+i}{i} x^i \right). \end{aligned} \tag{3.8}$$

For $r \in \mathbb{N}$, let a_r denote the number defined by

$$a_r := \begin{cases} (-1)^i \binom{m+1}{i} & \text{if } r = iq \text{ for some } i \in \{0,\dots,m+1\}, \\ 0 & \text{otherwise.} \end{cases}$$

Then the coefficient of x^t in the product (3.8) is given by $\sum_{r=0}^{t} a_r \binom{m+t-r}{m}$. It is now easily seen that $t/q < m+1$, and that

$$\sum_{r=0}^{t} a_r \binom{m+t-r}{m} = \sum_{i\in\{0,\ldots,\lfloor t/q\rfloor\}} (-1)^i \binom{m+1}{i}\binom{m+t-iq}{m}.$$

This finishes the proof of our assertion. $\square$

Next, we recompute $\dim PCR_\nu(m,q)$ with an eye towards a similar computation for the Grassmann case. In fact, the inner sum in our reformulation will be used later.

Proposition 3.9. *The dimension of the projective Reed-Müller code of degree ν is given by*

$$\dim PCR_\nu(m,q) = \sum_{\substack{t\,\in\,[\nu]\\ t\,\equiv\,\nu \mod q-1}} \sum_{e=1}^{\min\{t,m+1\}} \binom{m+1}{e} \left(\sum_{j=1}^{\lfloor \frac{t-e}{q-1} \rfloor} (-1)^j \binom{e}{j} \binom{t-1-(q-1)j}{e-1} \right).$$

Proof. We compute the cardinality of the set

$$\left\{ x_0^{i_0} x_1^{i_1} \cdots x_m^{i_m} \ : \ \begin{array}{c} i_0+\cdots+i_m = t \text{ and,} \\ 0 \le i_j \le q-1 \text{ for } j\in\{0,\ldots,m\} \end{array} \right\}$$

by first fixing the variables that we use. Let $e \in \{1,\ldots,\min\{m+1,t\}\}$, and choose e variables from $x_0,\ldots,x_m$. This can be done in $\binom{m+1}{e}$ many different ways. We proceed with the harmless assumption that our chosen variables are $x_1,\ldots,x_e$. Next, we determine the number of monomials of the form $x_1^{i_1}\cdots x_e^{i_e}$, where $\sum_{j=1}^{e} i_j = t$ and $1 \le i_j \le q-1$ for $j\in\{1,\ldots,e\}$. The set of all such monomials is in bijection with the set of compositions,

$$\{(\gamma_1,\ldots,\gamma_e) \vDash t : \ 1 \le \gamma_j \le q-1 \ \text{ for all } j \in \{1,\ldots,e\}\}.$$

Let $g(t,e,q-1)$ denote the cardinality of the set in the previous line. The generating series of $g(t,e,q-1)$ is easily seen to be

$$\sum_{t\ge e} g(t,e,q-1)x^t = (x+x^2+\cdots+x^{q-1})^e = x^e \frac{(1-x^{q-1})^e}{(1-x)^e}.$$

By manipulating the power series as before, we see that

$$g(t,e,q-1) = \sum_{j=0}^{\lfloor \frac{t-e}{q-1} \rfloor} (-1)^j \binom{e}{j} \binom{t-1-(q-1)j}{e-1}. \tag{3.10}$$

Since e varies in $\{1,\ldots,\min\{m+1,t\}\}$, by combining our counts, we finish the proof of our assertion. $\square$

4. The Nullstellensatz for Grassmannians

Our goal in this section is to prove a 'theorem of zeros' for $Gr(l,V)(\mathbb{F}_q)$. First, we present several preparatory observations. We begin with a simple remark.

Remark 4.1. Let $c \in \mathbb{F}_q$. Let S be a nonempty subset of $\mathbb{A}^s(\mathbb{F}_q)$. We claim that if $|S|$ is a power of q, then the equality $\sum_{a\in S} c = 0$ holds. Indeed, obviously, we have $\sum_{a\in S} c = |S|c$. Since $\mathbb{F}_q$ is an abelian group of order q, we have $|S|c = 0$ in $\mathbb{F}_q$. As a consequence of this simple observation, we see that if S is an affine subspace (of positive dimension) of $\mathbb{A}^s(\mathbb{F}_q)$, then $\sum_{a\in S} c = 0$ holds.

The *homogeneous coordinate ring* R of $Gr(l,V)$ is the $\overline{\mathbb{F}}_q$-algebra generated by the Plücker coordinates of $Gr(l,V)$. It has a natural grading that is given by the degree. The graded pieces are spanned by their standard monomials in the Plücker coordinates [13, Proposition 1.3.6]. In other words, if $\mathcal{O}_{Gr(l,V)}$ denotes the structure sheaf of $Gr(l,V)$, then R can be identified with $\bigoplus_{r\geq 0} H^0(Gr(l,V),\mathcal{O}_{Gr(l,V)}(r))$, where $H^0(Gr(l,V),\mathcal{O}_{Gr(l,V)}(r))$ corresponds to the r-th graded piece spanned by the degree r monomials in the Plücker variables. In turn, the Plücker variables are the coordinates of the affine space $\mathbb{A}^{\mathsf{e}+1}(\overline{\mathbb{F}}_q)$, that is, $\bigwedge^l \overline{\mathbb{F}}_q^m$. It is not difficult to check that the set of $\mathbb{F}_q$-rational points of the vector space $\bigwedge^l \overline{\mathbb{F}}_q^m$ is $\bigwedge^l \mathbb{F}_q^m$. Therefore, the Plücker coordinates are the coordinates of the affine space $\bigwedge^l \mathbb{F}_q^m$ as well.

Proposition 4.2. *Let r be a positive integer of the form $r = a(q-1)$, where $a \in [\mathsf{d}]$. If F is an element of $H^0(Gr(l,V),\mathcal{O}_{Gr(l,V)}(r))$, then we have*

$$\sum_{a\in Gr(l,V)(\mathbb{F}_q)} F(a) = 0.$$

Proof. If $Gr(l,V)$ is a projective space, then, our claim follows from [14, Lemma 1]. We proceed with the assumption that $Gr(l,V)$ is not a projective space. In particular, it is not $\mathbb{P}^1$. Since $H^0(Gr(l,V),\mathcal{O}_{Gr(l,V)}(r))$ is spanned as a vector space by the standard monomials of degree r, it suffices to prove our claim for a single standard monomial. Let M be a standard monomial of the form,

$$M := p_{\alpha(i_1)}^{a_1} p_{\alpha(i_2)}^{a_2} \cdots p_{\alpha(i_s)}^{a_s} \in H^0(Gr(l,V),\mathcal{O}_{Gr(l,V)}(r)) \qquad (\alpha(i_1) > \cdots > \alpha(i_s)), \tag{4.3}$$

where the exponents are positive integers such that $\sum_{j=1}^{s} a_j = r$. We will use induction on r, where the base case is given by $r = q-1$.

After choosing a suitable one-parameter subgroup (in a way that we discussed in [1, Section 3]), we may assume that the vanishing set of the Plücker coordinate $p_{\alpha(i_1)}$ is the boundary of $Gr(l,V)$. Equivalently, we may assume that $\alpha(i_1) = \alpha(\mathsf{e})$. Hence, we proceed with the assumption that M vanishes on the boundary $\partial Gr(l, V)$. Let us first analyze the possibility that $M = p_{\alpha(\mathsf{e})}^{a(q-1)}$. In this case, the only values of M are 0 or 1. In fact, since $p_{\alpha(\mathsf{e})}$ vanishes precisely on the boundary of $Gr(l, V)$, we have $p_{\alpha(\mathsf{e})} = 1$ on the affine open cell of $Gr(l, V)$. Thus, by Remark 4.1, we see that $\sum_{a \in C_{\alpha(\mathsf{e})}} M(a) = 0$. We now proceed with the general case that M has more than one Plücker variables in it. In this case, by setting $p_{\alpha(\mathsf{e})} = 1$, we obtain a standard monomial of lower degree, that is, $\tilde{M} = p_{\alpha(i_2)}^{a_2} \cdots p_{\alpha(i_s)}^{a_s}$. If $\sum_{j=2}^{s} a_j$ is divisible by $q - 1$, then we apply our induction hypothesis to conclude that

$$\sum_{P \in Gr(l,V)} M(P) = \sum_{P \in Gr(l,V) \setminus \partial Gr(l,V)} \tilde{M}(P) = 0.$$

If $\sum_{j=2}^{s} a_j$ is not divisible by $q - 1$, then we apply [2, Lemma 1.6] to conclude the same identity. Notice that these two cases also take care of the base case, where $r = q - 1$. □

4.1. Affine $\mathbb{F}_q$-Nullstellensatz and its consequences

Notation 4.4. Let $x_\bullet$ be a list of variables, $x_\bullet := (x_1, \dots, x_s)$. Let $F(x_\bullet)$ be a polynomial from $\mathbb{F}_q[x_\bullet]$. We denote by $\bar{F}(x_\bullet)$ the polynomial obtained from $F(x_\bullet)$ by reducing it modulo $x_i^q - x_i$ for $i \in \{1, \dots, s\}$. In other words, $\bar{F}(x_\bullet)$ is obtained from $F(x_\bullet)$ by replacing in every monomial of $F(x_\bullet)$ every factor of the form $x_i^{t_i}$, where $t_i = a(q-1)+b$ such that $b \in [q-1]$, with x_i^b. We will call $\bar{F}(x_\bullet)$ the *reduced form* of $F(x_\bullet)$.

Let us abbreviate the list of Plücker coordinates $p_{\alpha(0)}, \dots, p_{\alpha(\mathsf{e})}$ to $p_\bullet$. Let $F(p_\bullet)$ be a polynomial of the form

$$F(p_\bullet) := \sum c_{i_0 i_1 \dots i_\mathsf{e}} p_{\alpha(0)}^{i_0} p_{\alpha(1)}^{i_1} \cdots p_{\alpha(\mathsf{e})}^{i_\mathsf{e}} \in \mathbb{F}_q[p_\bullet],$$

where some of the exponents might be 0. We will denote by $\bar{F}(p_\bullet)$ the reduced form of $F(p_\bullet)$ as defined in Notation 4.4.

Let Γ_q denote the ideal of $\mathbb{F}_q[p_\bullet]$ that is generated by the polynomials $p_{\alpha(i)}^q - p_{\alpha(i)}$ for $i \in \{0, \dots, \mathsf{e}\}$. The proof of the following lemma is easy.

Lemma 4.5. *Let $F(p_\bullet)$ be an element of $\mathbb{F}_q[p_\bullet]$. If $\bar{F}(p_\bullet)$ is not the zero polynomial, then $\bar{F} \notin \Gamma_q$.*

Proof. Let us assume that $\bar{F} \in \Gamma_q$. Since the degree of Plücker variable in the reduced polynomial $\bar{F}(p_\bullet)$ is at most $q-1$, $\bar{F}(p_\bullet)$ must be the zero polynomial. This finishes the proof. □

Adapting it to our notation, we now state a finite field analog of the "theorem of zeros." A modern proof of this useful result can be found in Ghorpade's article [3].

Theorem 4.6. *(Affine $\mathbb{F}_q$-Nullstellensatz) Let $H, H_1, \ldots, H_s$ be polynomials from $\mathbb{F}_q[p_\bullet]$ such that H vanishes at every common zero of $H_1, \ldots, H_s$. Then we have*

(1) *there exist polynomials $G_1, \ldots, G_s$ in $\mathbb{F}_q[p_\bullet]$ and $\gamma \in \Gamma_q$ such that*

$$H = G_1 H_1 + \cdots + G_s H_s + \gamma. \tag{4.7}$$

(2) *H vanishes at all points of $\bigwedge^l \mathbb{F}_q$ if and only if $H \in \Gamma_q$.*

It is easy to see that (2) follows from (1). We will use the following consequence of the Affine $\mathbb{F}_q$-Nullstellensatz.

Lemma 4.8. *Let I be the vanishing ideal in $\mathbb{F}_q[p_\bullet]$ of a (closed) set $V \subset \bigwedge^l \mathbb{F}_q^m$. If $\{H_1, \ldots, H_s\}$ is a set of generators for I, then so is the following union:*

$$\{\overline{H}_1, \ldots, \overline{H}_s\} \cup \{p_{\alpha(j)}^q - p_{\alpha(j)} : \ j = 0, \ldots, \mathsf{e}\}.$$

In particular, F vanishes on a (closed) set $V \subseteq \bigwedge^l \mathbb{F}_q^m$ if and only if so does $\bar{F}$.

Proof. Let N be a positive integer such that $N \geq q$. Then we have

$$p_{\alpha(j)}^N = (p_{\alpha(j)}^q - p_{\alpha(j)}) p_{\alpha(j)}^{N-q} + p_{\alpha(j)}^{N-(q-1)}.$$

By using induction, we see from this observation that any polynomial $F \in I$ can be written in the form $\bar{F} + \gamma$, where γ is an element of Γ_q. Since the inclusion $\Gamma_q \subseteq I$ is always true, we see that F vanishes on V if and only if $\bar{F}$ vanishes on V. The proof now follows. □

Let us consider the canonical quotient map,

$$\pi : \left(\bigwedge^l \overline{\mathbb{F}}_q^m \right) \setminus \{0\} \longrightarrow \mathbb{P} := \mathbb{P}(\bigwedge^l \overline{\mathbb{F}}_q^m).$$

The closure of the preimage $\pi^{-1}(Gr(l, V))$ in $\bigwedge^l \overline{\mathbb{F}}_q^m$ will be denoted by $\mathbf{C}Gr(l, V)$. In our next result, we will denote by $[P]$ the point in $\mathbb{P}$ that is represented by a nonzero vector P in $\bigwedge^l V$. Let F be a homogeneous polynomial in the Plücker variables. When we write $F([P])$ we actually mean the evaluation of $F(p_\bullet)$ at the point P; it is defined up to a scalar multiple of P but we are only interested in whether $F(P) = 0$ or not. We are now ready to state and prove an analog of $\mathbb{F}_q$-Nullstellensatz for the homogeneous coordinate ring of a Grassmann variety.

Theorem 4.9. *Let F be an $\mathbb{F}_q$-rational section from $H^0(Gr(l, V), \mathcal{O}_{Gr(l,V)}(r))$. If $F([P]) = 0$ for all $[P] \in Gr(l, V)$, then $\bar{F} = 0$. Conversely, if $\bar{F} = 0$, then $F([P]) = 0$ for all $[P] \in Gr(l, V)$.*

Proof. By the definition of the homogeneous coordinate ring R of $Gr(l,V)$, a nonzero element of R cannot vanish at all points of $Gr(l,V)$. In particular, if an element $F \in H^0(Gr(l,V), \mathcal{O}_{Gr(l,V)}(r))$ has the property that $F([P]) = 0$ for every $[P] \in Gr(l,V)$, then F must be the zero element of R. Of course, this implies that $\bar{F} = 0$. Conversely, if $\bar{F} = 0$, then, by Lemmas 4.5 and 4.8, we have $F(P) = 0$ for every P in the cone $\mathbf{C}Gr(l,V)$. Since F is homogeneous, we have $F([P]) = 0$ for every $[P] \in Gr(l,V)$. This finishes the proofs of our assertions. $\square$

5. The dimension of a higher Grassmann code

In Section 3, we presented two formulas for the dimension of a projective Reed-Müller code. In this section, we present a similar calculation for the dimensions of higher Grassmann codes. Our approach has its roots in Proposition 3.9. The underlying idea is the following: we first count the number of supports of the relevant standard monomials, and then we count the possible exponents that we can place on the variables of the supports. The latter calculation has been made in the proof of Proposition 3.9 but the first calculation requires a completely novel approach. To this end, we begin with providing some useful algebraic definitions regarding the poset $\mathbf{A}_{m-1}(l)$.

Let P be a finite poset. Let K be a field. The *incidence algebra* of P over K, denoted $I(P,K)$, is the K-algebra of all functions $f : \mathrm{Int}(P) \to K$, where $\mathrm{Int}(P)$ is the set of all intervals of P. The addition of functions is defined, as usual, by the pointwise addition, and the multiplication is defined by

$$(fg)(s,u) = \sum_{s \le t \le u} f(s,t)g(t,u).$$

Let $[s,u]$ be a nonempty interval from P. If $[s,u]$ has only two elements, then we say that u covers s in P. A *chain* in $[s,u]$ is a strictly increasing sequence of elements from $[s,u]$. A *multichain* in $[s,u]$ is a weakly increasing sequence of elements from $[s,u]$. The *length* of a (multi)chain is defined as the number of entries of the sequence minus one. A *maximal chain* is a chain that is not a part of another chain in $[s,u]$. If $t_0 < t_1 < \cdots < t_r$ is a chain in P, then the integer r is called the *length* of the chain. The poset P is said to be a *graded*, if every maximal chain in P has the same length. In this case, there is a unique function $\ell : P \to \mathbb{N}$, called the *rank function*, such that $\ell(x) = 0$ for every minimal element $x \in P$, and $\ell(u) = \ell(s) + 1$ if u covers s in P.

If P has a unique minimal (resp. maximal) element, then we denote it by $\hat{0}$ (resp. by $\hat{1}$). Now we proceed with the assumption that P is a finite graded poset with $\hat{0}$ and $\hat{1}$. Furthermore, we assume that P has at least two elements (hence $\hat{0} \neq \hat{1}$). For $a \in \{i \in \mathbb{Z} : \ i \ge 2\}$, let $Z(P,a)$ denote the number of multichains of the form $\hat{0} \le t_1 \le t_2 \le \cdots \le t_{a-1} \le \hat{1}$ in P. We call $Z(P,a)$ the *zeta polynomial of* P. This name is justified with the fact [15, Proposition 3.12.1 a.] that $Z(P,a)$ is indeed a polynomial function of a. A closely related function, called the *zeta function of* P, is defined as follows:

$$\zeta(s,u) = \begin{cases} 1 & \text{if } s \le u, \\ 0 & \text{otherwise.} \end{cases}$$

It is not difficult to check that, for $s \le u$, $\zeta^r(s,u)$ is the number of multichains of the form $s = s_0 \le s_1 \le \cdots \le s_r = u$. In particular, we see that $\zeta^a(\hat{0},\hat{1}) = Z(P,a)$ for every $a \in \{i \in \mathbb{Z} :\ i \ge 2\}$.

Note that the zeta function is actually an element of the incidence algebra, $I(P,K)$. The identity element of $I(P,K)$ is the function $\delta : \mathrm{Int}(P) \to K$ defined by

$$\delta(s,u) = \begin{cases} 1 & \text{if } s = u, \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to check that

$$(\zeta - \delta)(s,u) = \begin{cases} 1 & \text{if } s < u, \\ 0 & \text{otherwise.} \end{cases}$$

Hence, $(\zeta-\delta)^r(s,u)$ gives the number of chains $s = s_0 < s_1 < \cdots < s_r = u$ of length r from s to u.

Proposition 5.1. *Let $h(r,m,l)$ denote the number of chains $\alpha(i_1) > \alpha(i_2) > \cdots > \alpha(i_r)$ of length r from $\hat{0}$ to $\hat{1}$ in $\mathbf{A}_{m-1}(l)$. Then $h(r,m,l)$ is given by the following equivalent formulas:*

1. $h(r,m,l) = \sum_{c=0}^{r} (-1)^{r-c} \binom{r}{c} \det \left[\binom{m-l+c}{i-j+c} \right]_{1 \le i,j \le m-l}$,
2. $h(r,m,l) = \sum_{c=0}^{r} (-1)^{r-c} \binom{r}{c} \prod_{i=1}^{m-l} \prod_{j=1}^{c} \prod_{s=1}^{m-l} \frac{i+j+s-1}{i+j+s-2}$.

Proof. We expand the function $(\zeta-\delta)^r$ in the incidence algebra of $\mathbf{A}_{m-1}(l)$,

$$(\zeta - \delta)^r = \sum_{c=0}^{r} \binom{r}{c} \zeta^c (-\delta)^{r-c} = \sum_{c=0}^{r} \binom{r}{c} \zeta^c (-1)^{r-c}.$$

Then we evaluate this expansion on the interval $[\hat{0},\hat{1}]$:

$$\begin{aligned}(\zeta-\delta)^r(\hat{0},\hat{1}) &= \sum_{c=0}^{r} (-1)^{r-c} \binom{r}{c} \zeta^c(\hat{0},\hat{1}) \\ &= \sum_{c=0}^{r} (-1)^{r-c} \binom{r}{c} Z(\mathbf{A}_{m-1}(l), c).\end{aligned}$$

But we know from [15, Exercise 149] that $Z(\mathbf{A}_{m-1}(l), c) = \det \left[\binom{m-l+c}{i-j+c} \right]_{1 \le i,j \le m-l}$. The following identity is well-known:

$$\det\left[\binom{a+b}{a+i-j}\right]_{1\le i,j\le r} = \prod_{i=1}^{r}\prod_{j=1}^{a}\prod_{s=1}^{b}\frac{i+j+s-1}{i+j+s-2}. \tag{5.2}$$

This particular identity can be proved by using the plane partition identities developed by MacMahon in [8]. Alternatively, one can use certain recurrences to prove it. This is explained in [6, Section 2.3]. If we set $a = c$ and $b = r = m - l$ in (5.2), then we see that

$$Z(\mathbf{A}_{m-1}(l), c) = \prod_{i=1}^{m-l}\prod_{j=1}^{c}\prod_{s=1}^{m-l}\frac{i+j+s-1}{i+j+s-2}.$$

This finishes the proof of our proposition. $\square$

We are now ready to present our dimension count for the higher Grassmann codes. Recall that in the proof of Proposition 3.9, in line (3.10), we found a formula for the number of positive exponents that we can place on e variables so that the resulting monomial has degree t:

$$g(t, e, q-1) = \sum_{j=0}^{\lfloor \frac{t-e}{q-1} \rfloor} (-1)^j \binom{e}{j}\binom{t-1-(q-1)j}{e-1}.$$

Now by using Proposition 5.1, we obtain the main result of this section.

Theorem 5.3. *Let $C_{Gr(l,V)}(\nu)$ denote the q-ary degree ν Grassmann code on $Gr(l, V)$. If $\nu < (q-1)\mathsf{d}$, then the dimension of $C_{Gr(l,V)}(\nu)$ is given by the formula*

$$\dim C_{Gr(l,V)}(\nu) = \sum_{\substack{t \in [\nu] \\ t \equiv \nu \mod q-1}} \sum_{r=1}^{\min\{t,\mathsf{d}\}} h(r, m, l) g(t, r, q-1),$$

where

$$h(r, m, l) = \sum_{c=0}^{r} (-1)^{r-c}\binom{r}{c}\prod_{i=1}^{m-l}\prod_{j=1}^{c}\prod_{s=1}^{m-l}\frac{i+j+s-1}{i+j+s-2},$$

and

$$g(t, r, q-1) = \sum_{j=0}^{\lfloor \frac{t-r}{q-1} \rfloor} (-1)^j \binom{r}{j}\binom{t-1-(q-1)j}{r-1}.$$

Proof. Let M be a standard monomial of degree ν. If the exponent of a Plücker variable in M is greater than $q-1$, then we can reduce this monomial without changing its values. Therefore, the dimension of our code is equal to the number of reduced standard monomials. Indeed, we claim that these standard monomials are linearly independent. Otherwise, we find a linear combination of them that is equal to zero. But thanks to our $\mathbb{F}_q$-Nullstellensatz Theorem 4.9, this is not possible.

We now proceed to calculate the number of reduced standard monomials of degree t, where $t \in [\nu]$ and $t \equiv \nu \mod q-1$. As we mentioned at the beginning of this subsection, first, we count the number of supports of these standard monomials. The number of supports with r Plücker variables in them is given by $h(r,m,l)$ of Proposition 5.1. Next, we count the number ways of placing positive exponents, which add up to t, on the variables of our support. This number is found in the proof of Proposition 3.9, in line (3.10). Now our result follows at once by combining these two counts. □

6. The minimum distance of a higher Grassmann code

In this section, we present bounds on the minimum distance of a higher Grassmann code.

The following restatement of a result of Kasami, Lin, and Peterson will be useful for our purposes.

Lemma 6.1. *Let $Z_f = \{w \in \mathbb{A}^N(\mathbb{F}_q) : f(w) = 0\}$ be a hypersurface in $\mathbb{A}^N(\mathbb{F}_q)$, where $f \in \mathbb{F}_q[x_1, \ldots, x_N]$ is a polynomial such that $\deg f = r(q-1) + s$ with $0 \leq s < q-1$. Then we have $|Z_f| \leq q^N - (q-s)q^{N-r-1}$.*

Proof. The proof is a direct consequence of [5, Theorem 5] and the correspondence between the linear $[n,k,d]_q$ codes and the $[n,k,d]_q$-systems as explained in [16, Proposition 1.1.4]. □

Theorem 6.2. *Let $C_{Gr(l,V)}(\nu)$ denote the q-ary degree ν Grassmann code on $Gr(l,V)$. Let r and s be the nonnegative integers defined by $\nu - 1 = r(q-1) + s$, where $0 \leq s < q-1$. If $\nu < (q-1)\mathsf{d}$, then the minimum distance of $C_{Gr(l,V)}(\nu)$ is bounded as follows:*

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

Proof. The idea of the proof is similar to the idea of the proof of [1, Theorem 4.1, Part 2.], where we assumed that $\nu < q-1$. We proceed with the assumption that $q-1 \leq \nu < (q-1)\mathsf{d}$.

It follows from the argument we had in the second paragraph of the proof of [1, Theorem 4.1] that our problem of finding the minimum distance for $C_{Gr(l,V)}(\nu)$ is equivalent to the problem of determining the number of $\mathbb{F}_q$-rational points of the intersection of $Gr(l,V)$ with a degree ν hypersurface in $\mathbb{P}(\bigwedge^l V) \cong \mathbb{P}^{\mathsf{e}}$. Note that, since r and s are defined by $\nu - 1 = r(q-1) + s$, we have $1 \leq r < \mathsf{d}$. Note also that we always have the strict inequality, $\mathsf{d} < \mathsf{e}$. Let $x_0, \ldots, x_{\mathsf{e}}$ denote the Plücker coordinates of $\mathbb{P}(\bigwedge^l V)$. For our upper bound, we consider the following homogeneous polynomial of degree ν:

$$F := x_{r+1} \prod_{j=1}^{s} (x_{r+1} - b_j x_r) \prod_{i=0}^{r-1} (x_{r+1}^{q-1} - x_i^{q-1}), \tag{6.3}$$

where $b_i \in \mathbb{F}_q \setminus \{0\}$ and $b_i \neq b_j$ for every $\{i, j\} \subset \{1, \dots, s\}$ such that $i \neq j$. We will analyze the $\mathbb{F}_q$-rational points of the intersection $\{F = 0\} \cap Gr(l, V)$ in $\mathbb{P}(\bigwedge^l V) \cong \mathbb{P}^{\mathsf{e}}$.

First, we choose an appropriate one-parameter subgroup of $\mathbf{SL}_n(\overline{\mathbb{F}}_q)$ such that the boundary of $Gr(l, V)$ is given by the intersection $\{x_{r+1} = 0\} \cap Gr(l, V)$, and the additional equation $x_r = 0$ gives a Borel subgroup stable divisor in $\partial Gr(l, V)$, denoted by Z. We now analyze the zeros of (6.3) following the steps:

1. $M \in Gr(l, V)$ such that $x_{r+1}(M) = x_r(M) = 0$;
2. $M \in Gr(l, V)$ such that $x_{r+1}(M) = 0$ and $x_r(M) \neq 0$;
3. $M \in Gr(l, V)$ such that $x_{r+1}(M) \neq 0$, $x_r(M) \neq 0$, but

$$\left(\prod_{j=1}^{s} (x_{r+1} - b_j x_r) \prod_{i=0}^{r-1} (x_{r+1}^{q-1} - x_i^{q-1}) \right) (M) = 0.$$

In the first case, that is, $\{M \in \mathbb{P}(\bigwedge^l V) : \ x_{r+1}(M) = x_r(M) = 0\} \cap Gr(l, V)$, F is zero on every point of Z. The count of $\mathbb{F}_q$-rational points of Z is well-known:

$$|Z| = \begin{bmatrix} m \\ l \end{bmatrix} - q^{l(m-l)} - q^{l(m-l)-1}.$$

In the second case, F is zero on the complement of Z in $\partial Gr(l, V)$. This count is also well-known,

$$|\partial Gr(l, V) \setminus Z| = q^{l(m-l)-1}.$$

Finally, in the third case, the set

$$\{M \in Gr(l, V) : \ x_{r+1}(M) {\neq} 0, x_r(M) {\neq} 0, \ \left(\prod_{j=1}^{s} (x_{r+1} - b_j x_r) \prod_{i=0}^{r-1} (x_{r+1}^{q-1} {-} x_i^{q-1}) \right) (M) {=} 0\} \tag{6.4}$$

is the intersection of an open set with a hypersurface in the affine space $Gr(l, V) \setminus \partial Gr(l, V) \cong \mathbb{A}^{l(m-l}$. To work with the coordinates on this affine space, we set $x_{r+1} = 1$.

$$G := \prod_{j=1}^{s} (1 - b_j x_r) \prod_{i=0}^{r-1} (1 - x_i^{q-1}) = 0 \qquad (x_r \neq 0).$$

This polynomial is zero in $\mathbb{A}^{l(m-l)}(\mathbb{F}_q)$ unless

$$x_r \neq b_j^{-1} \qquad \text{for } j \in \{1, \ldots, s\}, \tag{6.5}$$

$$x_i = 0 \qquad \text{for } i \in \{0, \ldots, r-1\}. \tag{6.6}$$

But there are exactly $(q-1-s)q^{l(m-l)-r-1}$ points satisfying (6.5) and (6.6). Hence, the vanishing set of G in $\{x_r \neq 0\} \cap \mathbb{A}^{l(m-l)}(\mathbb{F}_q)$ contains $q^{l(m-l)} - (q-1-s)q^{l(m-l)-r-1}$ points. Now, by combining our findings, we see that the total number of zeros of the homogeneous polynomial F on $Gr(l,V)$ is given by

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

Equivalently, we have

$$|\{F=0\} \cap Gr(l,V)| = \begin{bmatrix} m \\ l \end{bmatrix}_q - (q-1-s)q^{l(m-l)-r-1}.$$

Therefore, an upper bound for the minimum distance of Grassmann code of order ν is given by

$$\begin{bmatrix} m \\ l \end{bmatrix}_q - \left(\begin{bmatrix} m \\ l \end{bmatrix}_q - (q-1-s)q^{l(m-l)-r-1} \right) = (q-1-s)q^{l(m-l)-r-1}. \tag{6.7}$$

Next, we will provide a lower bound for the minimum distance. To this end, let Q be a homogeneous degree ν polynomial from $\mathbb{F}_q[x_1, \ldots, x_{s+1}]$ 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. Since we want to find the extremities, in light of Lemma 6.1, we assume generously that this intersection attains the maximum number $q^{l(m-l)} - (q-s)q^{l(m-l)-r-1}$ on this open cell. We assume also that H_Q contains the boundary $\partial Gr(l,V)$. Note that $|\partial Gr(l,V)| = \left[\begin{smallmatrix} m \\ l \end{smallmatrix}\right]_q - q^{l(m-l)}$. Hence, under our assumptions, we see that

$$\begin{aligned} |H_Q \cap Gr(l,V)| &\leq q^{l(m-l)} - (q-s)q^{l(m-l)-r-1} + \begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} \\ &= \begin{bmatrix} m \\ l \end{bmatrix}_q - (q-s)q^{l(m-l)-r-1}. \end{aligned} \tag{6.8}$$

Since (6.8) 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

$$\begin{bmatrix} m \\ l \end{bmatrix}_q - \left(\begin{bmatrix} m \\ l \end{bmatrix}_q - (q-s)q^{l(m-l)-r-1} \right) = q^{l(m-l)-r} - sq^{l(m-l)-r-1}. \tag{6.9}$$

By combining (6.7) and (6.9), we finish the proof of our assertion. □

7. The dual of a higher Grassmann code

In his results about the dual of a projective Reed-Müller code, Sorensen makes use of the following lemma:

Lemma 7.1. *([14, Lemma 6]) Let $d(t,m,q)$ denote the number of monomials of the form $x_0^{i_0}\cdots x_m^{i_m}$ with $0\le i_j\le q-1$, and $\sum_{j=0}^m i_j = x$. If $0\le s<q-1$, then the following properties hold:*

1. $d(t,m,q)=d((m+1)(q-1)-t,m,q)$,
2. $\sum_{\substack{t\,<\,(m\,+\,1)(q\,-\,1)\\ t\,=\,s \mod q\,-\,1}} d(t,m,q)=\sum_{\substack{0\,<\,t\,\le\,(m\,+\,1)(q\,-\,1)\\ t\,=\,s \mod q\,-\,1}} d(t,m,q)=\frac{q^{m+1}-1}{q-1}$.

We have an analogous result for the Grassmannian $Gr(l,V)$. For $\nu\in\{0,1,\dots,(q-1)\mathsf{d}\}$, let $\kappa(\nu)$ denote the number of standard monomials $p_{\alpha(j_1)}^{i_1}\cdots p_{\alpha(j_r)}^{i_r}$ such that $\sum_{j=1}^r i_j=\nu$ and $i_j\in\{0,\dots,q-1\}$ for all $j\in\{1,\dots,r\}$.

Lemma 7.2. *The numbers $\kappa(\nu)$ satisfy the following properties:*

(1) $\kappa(\nu)=\kappa((q-1)\mathsf{d}-\nu)$.
(2) *If r is a nonnegative integer such that $0\le r<q-1$, then we have*

$$\sum_{\substack{\nu\,\in\,[(q\,-\,1)\mathsf{d}]\\ \nu\,=\,r\quad \mod q\,-\,1}}\kappa(\nu)=\begin{bmatrix} m\\ l\end{bmatrix}_q.$$

Proof. The map $p_{\alpha(0)}^{i_0}\cdots p_{\alpha(\mathsf{e})}^{i_{\mathsf{e}}}\mapsto p_{\alpha(0)}^{q-1-i_0}\cdots p_{\alpha(\mathsf{e})}^{q-1-i_{\mathsf{e}}}$ gives a bijection between the standard monomials of degree ν and the standard monomials of degree $(q-1)\mathsf{d}-\nu$ whose variables have exponents at most $q-1$. Hence, the proof of (1) follows.

For (2), we already know from Lemma 7.1 that if there are no restrictions on the supports of the monomials $p_{\alpha(0)}^{i_0}\cdots p_{\alpha(\mathsf{e})}^{i_{\mathsf{e}}}$, then there are $\frac{q^{\mathsf{e}+1}-1}{q-1}$ monomials of the form $p_{\alpha(0)}^{i_0}\cdots p_{\alpha(\mathsf{e})}^{i_{\mathsf{e}}}$ with $\sum_{j=1}^r i_j=\nu$ and $i_j\in\{0,\dots,q-1\}$ for all $j\in\{1,\dots,r\}$. In other words, such monomials are in bijection with the $\mathbb{F}_q$-rational points of the projective space $\mathbb{P}$. The additional condition of *standardness*, that is,

$$\alpha(j_1)>\cdots>\alpha(j_r)$$

gives the points that are contained in the image of $Gr(l,V)(\mathbb{F}_q)$ in the set of $\mathbb{F}_q$-rational points of $\mathbb{P}(\bigwedge^l V)$. Our assertion follows from this observation. □

Remark 7.3. The inner sum in Theorem 5.3, that is, $\sum_{r=1}^{\min\{t,\mathsf{d}\}} h(r,m,l)g(t,r,q-1)$ is equal to $\kappa(t)$. In other words, we have the following formula

$$\dim C_{Gr(l,V)}(\nu) = \sum_{\substack{t \in [\nu] \\ t \equiv \nu \mod q-1}} \kappa(t).$$

We are now ready to describe the duals of the higher Grassmann codes. The proof of our result is similar to the Sorensen's proof of the corresponding result [14, Theorem 2] for the projective Reed-Müller codes.

Theorem 7.4. *Let $\nu \in [(q-1)\mathsf{d}-1]$. Let $C_{Gr(l,V)}(\nu)$ denote the q-ary degree ν Grassmann code on $Gr(l,V)$. If μ is defined by the equation $\mu := (q-1)(\mathsf{d}-1)-\nu$, then we have Then the dual of $C_{Gr(l,V)}(\nu)$ is given by one of the following two cases:*

$$C_{Gr(l,V)}(\nu)^{\perp} = \begin{cases} C_{Gr(l,V)}(\mu) & \text{if } \nu \neq 0 \mod (q-1), \\ \\ \overline{C_{Gr(l,V)}(\mu)} & \text{if } \nu = 0 \mod (q-1). \end{cases}$$

Proof. We begin with the assumption that $\nu \neq 0 \mod q-1$.

Recall that the length of a higher Grassmann code (of some degree) on $Gr(l,V)$ is $n = \begin{bmatrix} m \\ l \end{bmatrix}_q$. Let $F(p_\bullet)$ and $G(p_\bullet)$ be two homogeneous polynomials in Plücker coordinates viewed as $\mathbb{F}_q$-rational sections in $H^0(Gr(l,V), \mathcal{O}_{Gr(l,V)}(\nu))$ and $H^0(Gr(l,V), \mathcal{O}_{Gr(l,V)}(\mu))$, respectively. The codewords corresponding to $F(p_\bullet)$ and $G(p_\bullet)$ are given by the vectors $(F(P_1), \dots, F(P_n))$ and $(G(P_1), \dots, G(P_n))$ in $\mathbb{F}_q^n$, respectively. The inner product of these two vectors is given by the sum of the values of the homogeneous polynomial $(FG)(p_\bullet)$. Clearly, the degree of $(FG)(p_\bullet)$ is $(q-1)(\mathsf{d}-1)$. Thus, by Proposition 4.2, we know that $\sum_{P \in Gr(l,V)(\mathbb{F}_q)} (FG)(P) = 0$. In other words, the inner product of the codewords of $F(p_\bullet)$ and $G(p_\bullet)$ are orthogonal. Hence, we proved the inclusion $C_{Gr(l,V)}(\nu)^{\perp} \supseteq C_{Gr(l,V)}(\mu)$. We proceed to prove the opposite inclusion.

In light of Remark 7.3, we calculate the following sum:

$$\dim C_{Gr(l,V)}(\nu) + \dim C_{Gr(l,V)}(\mu) = \left(\sum_{\substack{t \in [\nu] \\ t \equiv \nu \mod q-1}} \kappa(t) \right) + \left(\sum_{\substack{t \in [\mu] \\ t \equiv \mu \mod q-1}} \kappa(t) \right). \tag{7.5}$$

Let us consider the remainders of ν and μ modulo $q-1$. In other words, by using their ordinary divisions, we write $\nu = a_\nu(q-1) + b_\nu$ and $\mu = a_\mu(q-1) + b_\mu$, where $\{b_\mu, b_\nu\} \subset [q-2]$ and $\{a_\mu, a_\nu\} \subset \mathbb{Z}_+$. The first summation on the right hand side of (7.5) is given by

$$\sum_{\substack{t \in [\nu] \\ t \equiv \nu \mod q-1}} \kappa(t) = \kappa(\nu) + \kappa(\nu - (q-1)) + \cdots + \kappa(\nu - a_\nu(q-1)). \tag{7.6}$$

We want to understand how the second summation in (7.5) completes (7.6). Since $\mu+\nu = (q-1)(\mathsf{d}-1)$, we have $(q-1)(\mathsf{d}-1) < \nu + (a_\mu+1)(q-1) < (q-1)\mathsf{d}$. At the same time we have

$$\begin{aligned}\sum_{\substack{t \in [\mu] \\ t \equiv \mu \mod q-1}} \kappa(t) &= \kappa(\mu)+\kappa(\mu-(q-1))+\cdots+\kappa(\mu-a_\mu(q-1)) \\ &= \kappa((q-1)(\mathsf{d}-1)-\nu)+\cdots+\kappa((q-1)(\mathsf{d}-1)-\nu-a_\mu(q-1)) \\ &= \kappa((q-1)+\nu)+\cdots+\kappa(\nu+(a_\mu+1)(q-1)) \qquad \text{(by Lemma 7.2 (1))}.\end{aligned}$$

By adding (7.6) to the last sum we found, we see that (7.5) is given by

$$\begin{aligned}\dim C_{Gr(l,V)}(\nu)+\dim C_{Gr(l,V)}(\mu) &= \kappa(b_\nu)+\kappa(b_\nu+(q-1))+\cdots+\kappa(\nu+(a_\mu+1)(q-1)) \\ &= \begin{bmatrix} m \\ l \end{bmatrix}_q \qquad \text{(by Lemma 7.2 (2))}. \end{aligned} \tag{7.7}$$

Since the dimension of the dual of $C_{Gr(l,V)}(\nu)$ is given by $\begin{bmatrix} m \\ l \end{bmatrix}_q - \dim C_{Gr(l,V)}(\nu)$, which is equal to $\dim C_{Gr(l,V)}(\mu)$ by (7.7), we conclude that $C_{Gr(l,V)}(\nu)^\perp = C_{Gr(l,V)}(\mu)$.

We now proceed with the assumption that $\nu = 0 \mod q-1$. In this case, by using similar arguments as in the previous case, we find that $\dim C_{Gr(l,V)}(\nu) + \dim C_{Gr(l,V)}(\mu) = \begin{bmatrix} m \\ l \end{bmatrix}_q - 1$. Notice that although $\nu = 0 \mod (q-1)$, ν cannot be exactly 0 since $\nu \in [(q-1)\mathsf{d}-1]$. Hence, the higher Grassmann code $C_{Gr(l,V)}(\mu)$ does not contain the all-one vector $\mathbf{1}_n$, viewed as the evaluation of the constant polynomial 1 at all points of $Gr(l,V)(\mathbb{F}_q)$. Therefore, the dimension of the all-one extended code $\overline{C_{Gr(l,V)}(\mu)}$ is $1+\dim C_{Gr(l,V)}(\mu)$. In particular, we have the following identity for the sum of the dimensions:

$$\dim C_{Gr(l,V)}(\nu) + \overline{\dim C_{Gr(l,V)}(\mu)} = \begin{bmatrix} m \\ l \end{bmatrix}_q. \tag{7.8}$$

Now, as in the previous case, let

$$F(p_\bullet) \in H^0(Gr(l,V), \mathcal{O}_{Gr(l,V)}(\nu)) \quad \text{and} \quad G(p_\bullet) \in H^0(Gr(l,V), \mathcal{O}_{Gr(l,V)}(\mu))$$

be two $\mathbb{F}_q$-rational sections. Since the degree of $(FG)(p_\bullet)$ is $(q-1)(\mathsf{d}-1)$, we see from Proposition 4.2 that $\sum_{P\in Gr(l,V)(\mathbb{F}_q)}(FG)(P) = 0$. At the same time, by using Proposition 4.2 once more, we see also that $(F(P_1),\dots,F(P_n))\cdot a\mathbf{1}_n = 0$ for all $a \in \mathbb{F}_q$. It follows that $\mathbf{a}\cdot\mathbf{b} = 0$ for every $\mathbf{a} \in C_{Gr(l,V)}(\nu)$ and for every $\mathbf{b} \in \overline{C_{Gr(l,V)}(\mu)}$. Hence, in light of (7.8), we see that $\overline{C_{Gr(l,V)}(\mu)}$ is the dual of the code $C_{Gr(l,V)}(\nu)$. This finishes the proof of our theorem. □

Data availability

No data was used for the research described in the article.

References

[1] Mahir Bilen Can, Roy Joshua, G.V. Ravindra, Higher Grassmann codes, Finite Fields Appl. 76 (2021) 101905.
[2] P. Delsarte, J.-M. Goethals, F.J. MacWilliams, On generalized Reed-Muller codes and their relatives, Inf. Control 16 (1970) 403–442.
[3] Sudhir R. Ghorpade, A note on Nullstellensatz over finite fields, in: Contributions in Algebra and Algebraic Geometry, in: Contemp. Math., vol. 738, Amer. Math. Soc., Providence, RI, 2019, pp. 23–32.
[4] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, Concrete mathematics, in: A Foundation for Computer Science, second edition, Addison-Wesley Publishing Company, Reading, MA, 1994.
[5] Tadao Kasami, Shu Lin, W. Wesley Peterson, New generalizations of the Reed-Muller codes. I. Primitive codes, IEEE Trans. Inf. Theory IT-14 (1968) 189–199.
[6] C. Krattenthaler, Advanced determinant calculus, vol. 42, in: The Andrews Festschrift, Maratea, 1998, 1999, B42q.
[7] Gilles Lachaud, The parameters of projective Reed-Muller codes, Discrete Math. 81 (2) (1990) 217–221.
[8] Percy A. MacMahon, Combinatory Analysis, vols. I, II (Bound in One Volume), Dover Phoenix Editions, Dover Publications, Inc., Mineola, NY, 2004, Reprint of it An Introduction to Combinatory Analysis (1920) and it Combinatory Analysis, vols. I, II (1915, 1916).
[9] D.Yu. Nogin, Codes associated to Grassmannians, in: Arithmetic, Geometry and Coding Theory, Luminy, 1993, De Gruyter, Berlin, 1996, pp. 145–154.
[10] Robert A. Proctor, Bruhat lattices, plane partition generating functions, and minuscule representations, Eur. J. Comb. 5 (4) (1984) 331–350.
[11] Gian-Carlo Rota, On the foundations of combinatorial theory. I. Theory of Möbius functions, Z. Wahrscheinlichkeitstheor. Verw. Geb. 2 (1964) 340–368.
[12] Charles T. Ryan, Kevin M. Ryan, The minimum weight of the Grassmann codes $C(k, n)$, Discrete Appl. Math. 28 (2) (1990) 149–156.
[13] C.S. Seshadri, Introduction to the Theory of Standard Monomials, second edition, Texts and Readings in Mathematics, vol. 46, Hindustan Book Agency, New Delhi, 2014.
[14] Anders Bjært Sørensen, Projective Reed-Muller codes, IEEE Trans. Inf. Theory 37 (6) (1991) 1567–1576.
[15] Richard P. Stanley, Enumerative Combinatorics. Volume 1, second edition, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012.
[16] Michael Tsfasman, Serge Vlăduţ, Dmitry Nogin, Algebraic Geometric Codes: Basic Notions, Mathematical Surveys and Monographs, vol. 139, American Mathematical Society, Providence, RI, 2007.