Enumerative Coding for Line Polar Grassmannians with applications to codes

Ilaria Cardinali[a,*], Luca Giuzzi[b]

[a] *Department of Information Engineering and Mathematics, University of Siena, Via Roma 56, I-53100, Siena, Italy*

[b] *DICATAM - Section of Mathematics, University of Brescia, Via Branze 53, I-25123, Brescia, Italy*

Abstract

A k-polar Grassmannian is a geometry having as pointset the set of all k-dimensional subspaces of a vector space V which are totally isotropic for a given non-degenerate bilinear form μ defined on V. Hence it can be regarded as a subgeometry of the ordinary k-Grassmannian. In this paper we deal with orthogonal line Grassmannians and with symplectic line Grassmannians, i.e. we assume $k = 2$ and μ to be a non-degenerate symmetric or alternating form. We will provide a method to efficiently enumerate the pointsets of both orthogonal and symplectic line Grassmannians. This has several nice applications; among them, we shall discuss an efficient encoding/decoding/error correction strategy for line polar Grassmann codes of either type.

Keywords: Enumerative Coding, Polar Grassmannian, Linear Code.
2010 MSC: 14M15, 94B27, 94B05

1. Introduction

Let V be a vector space of dimension n over a field $\mathbb{K}$. For any $k < n$, the k–Grassmannian $\mathcal{G}_{n,k}$ of V is the geometry whose pointset $\mathcal{P}(\mathcal{G}_{n,k})$ consists of the k-dimensional subspaces of V and whose lines are the sets of the form

$$\ell_{X,Y} := \{Z \colon X < Z < Y \colon \dim Z = k\}$$

where X and Y are two subspaces of V with $\dim(X) = k - 1$ and $\dim(Y) = k + 1$. Incidence is containment. It is well known that $\mathcal{G}_{n,k}$ can be embedded, as an algebraic variety $\mathbb{G}_{n,k}$, into the projective space $\mathrm{PG}(\bigwedge^k V)$, by means of the Plücker embedding e_k. More precisely, e_k maps the k-vector subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of V to the point $\langle v_1 \wedge v_2 \wedge \cdots \wedge v_k\rangle$ of $\mathrm{PG}(\bigwedge^k V)$ (see [13, Chapter VII] and [14, Chapter XVI] for details).

In this paper we assume $\mathbb{K}$ to be a finite field $\mathbb{F}_q$ of order q. A basic problem is to construct an enumerator for the points of $\mathcal{G}_{n,k}$, that is a bijection $\iota : \mathcal{P}(\mathcal{G}_{n,k}) \to \{0, 1, \ldots, N-1\}$, where $N := \begin{bmatrix} n \\ k \end{bmatrix}_q$ is the number of points of $\mathcal{G}_{n,k}$. This has been studied extensively, see [26], because of its relevance to applications. In particular, Grassmannians defined over finite fields have been used in coding theory to construct linear projective codes [23, 24] and network codes [17]. In general, it is not convenient to implement a Grassmann code by naïvely providing a generator matrix, as the number of columns is large; so, a point enumerator ι provides an efficient way to

*Corresponding author.
Email addresses: ilaria.cardinali@unisi.it (Ilaria Cardinali), luca.giuzzi@unibs.it (Luca Giuzzi)

uniquely identify subspaces corresponding to given positions. Several algorithms for enumerating the points of Grassmannians have been proposed; see [18, 26]. We point out that, apart from their usefulness for coding theory, these algorithms also have independent geometric interest.

The present paper is concerned with the problem outlined above, focusing on the case of line polar Grassmannians of either orthogonal or symplectic type. These are proper subgeometries of line Grassmannians having as pointset the set of lines of a vector space V which are totally isotropic for a given non-degenerate symmetric or alternating form. We shall determine a method to enumerate these lines, following the basic approach of [8]. In general, the case of polar Grassmannians is more involved than that of ordinary k-Grassmannians, as there are some requirements imposed on the subspaces which have to be fulfilled; thus, a careful use of linear algebra (combined with combinatorial techniques) is necessary in order to get a reasonably efficient representation. We shall also examine in detail the computational complexity of the proposed algorithms.

Our algorithms will then be applied to polar Grassmann codes of either orthogonal or symplectic type. These codes have been introduced respectively in [2] and in [3] as linear codes arising from the Plücker embedding of polar Grassmannians of orthogonal or symplectic type. Some bounds on their minimum distance have been obtained: it has been proved in [4] for q odd and in [5] for q even that if $k = 2$ then the minimum distance of a line orthogonal Grassman code is $q^{4n-5} - q^{3n-4}$; the minimum distance of a line symplectic Grassman code is $q^{4n-5} - q^{2n-3}$ (see [3]).

We shall set the notation in Section 1.1 and recall some notions about polar Grassmann codes in Section 1.2. The organization of the paper and the main results are outlined in Section 1.3.

1.1. Notation

Let $V := V(2n+1, q)$ be a vector space of dimension $2n+1$ over a finite field $\mathbb{F}_q$ and let $\mathfrak{q} : V \to \mathbb{F}_q$ be a non-degenerate quadratic form. The k-orthogonal Grassmannian $\Delta_{n,k}$ is a point-line geometry whose points are all the totally $\mathfrak{q}$-singular k-subspaces of V and whose lines are the sets either of the form

$$\ell_{X,Z} := \{Y \in \mathcal{G}_{2n+1,k} : X < Y < Z\} \text{ for } k < n,$$

where $\dim X = k-1$, $\dim Z = k+1$ and Z is totally $\mathfrak{q}$-singular or of the form

$$\ell_X := \{Y : X < Y < X^{\perp \mathfrak{q}}, \dim Y = n, Y \text{ totally singular } \} \text{ for } k = n,$$

with $\dim X = n-1$ and $X^{\perp \mathfrak{q}}$ the space orthogonal to X with respect to the bilinear form $\mathfrak{b}$ associated with $\mathfrak{q}$. Incidence is defined in the natural way.

Likewise, denote by $\overline{V} := V(2n, q)$ a vector space of dimension $2n$ over a finite field $\mathbb{F}_q$ and consider a non-degenerate alternating bilinear form $\mathfrak{s} : \overline{V} \times \overline{V} \to \mathbb{F}_q$. The k-symplectic Grassmannian $\overline{\Delta}_{n,k}$ has as points all totally $\mathfrak{s}$-isotropic k-spaces of $\overline{V}$ and as lines the sets of the form

$$\ell_{X,Z} = \{Y \in \mathcal{G}_{2n,k} : X < Y < Z\} \text{ for } k < n,$$

with $\dim X = k-1$, $\dim Z = k+1$ and Z totally $\mathfrak{s}$-isotropic or

$$\ell_X = \{Y : X < Y, \dim Y = n, Y \text{ totally isotropic}\} \text{ for } k = n,$$

with $\dim X = n-1$.

By construction, any point of $\Delta_{n,k}$ is also a point of $\mathcal{G}_{2n+1,k}$ and any point of $\overline{\Delta}_{n,k}$ is also a point of $\mathcal{G}_{2n,k}$.

Consider the embeddings $\varepsilon_k := e_k|_{\Delta_{n,k}}$ and $\overline{\varepsilon}_k := e_k|_{\overline{\Delta}_{n,k}}$ induced by the Plücker embedding e_k on the polar Grassmannians of orthogonal and symplectic type. In particular, $\varepsilon_k(\Delta_{n,k})$ is a subvariety of $\mathbb{G}_{2n+1,k}$ and $\overline{\varepsilon}_k(\overline{\Delta}_{n,k})$ is a subvariety of $\mathbb{G}_{2n,k}$. We summarize what is known about these embeddings. We warn the reader that we shall always use vector dimensions.

Theorem 1.1 ([6]). *Let $\varepsilon_k : \Delta_{n,k} \to \mathrm{PG}(\bigwedge^k V)$ be the restriction of the Plücker embedding to the orthogonal polar Grassmannian $\Delta_{n,k}$ and let $W_{n,k} := \langle \varepsilon_k(\Delta_{n,k}) \rangle$. Then,*

- *For $k < n$, ε_k is projective and*

$$\dim W_{n,k} = \begin{cases} \binom{2n+1}{k} & \text{if } \mathrm{char}(\mathbb{F}) \text{ odd} \\ \binom{2n+1}{k} - \binom{2n+1}{k-2} & \text{if } \mathrm{char}(\mathbb{F}) = 2. \end{cases}$$

- *For $k = n$, $\varepsilon_n : \Delta_{n,n} \to \mathrm{PG}(W_{n,n})$ maps lines into conics.*

Theorem 1.2 ([9, 21]). *Let $\overline{\varepsilon}_k : \Delta_{n,k} \to \mathrm{PG}(\bigwedge^k V)$ be the restriction of the Plücker embedding to the symplectic polar Grassmannian $\overline{\Delta}_{n,k}$ and let $\overline{W}_{n,k} := \langle \overline{\varepsilon}_k(\overline{\Delta}_{n,k}) \rangle$. Then,*

- *$\overline{\varepsilon}_k : \overline{\Delta}_{n,k} \to \mathrm{PG}(\bigwedge^k V)$ is projective and $\dim(\overline{W}_{n,k}) = \binom{2n}{k} - \binom{2n}{k-2}$.*

1.2. Polar Grassmann Codes

Throughout the paper, we shall denote by N the length of a linear code and by K its dimension; as before, lower case letters n and k shall be used to represent the parameters of the associated Grassmannians.

A q-ary code $\mathcal{C}$ of length N and dimension K is called *projective* if the columns of its generator matrix are the coordinates of N distinct points in $\mathrm{PG}(K-1, q)$. Conversely, given a set of N distinct points $\Omega = \{P_1, \ldots, P_N\}$ in $\mathrm{PG}(W)$ we call *projective code induced by* Ω any linear code $\mathcal{C}(\Omega)$ generated by a matrix G whose columns consist of the coordinates of the points in Ω with respect to some reference system. We have $K = \dim\langle\Omega\rangle$. Clearly, $\mathcal{C}(\Omega)$ is defined only up to code equivalence, but in the rest of this paper we shall speak, with a slight abuse of notation, of *the* code induced by Ω; see [27] for more details.

The close correspondence between hyperplane sections of Ω and the weights of the codewords of $\mathcal{C}(\Omega)$ is a basic result of the theory of projective codes. In particular, hyperplanes of $\mathrm{PG}(W)$ having maximal proper intersection with Ω are associated with codewords of minimum weight.

The projective codes $\mathcal{C}_{n,k}$ arising from the pointset $e_k(\mathcal{G}_{n,k}) \subseteq \mathrm{PG}(\bigwedge^k V)$ are called Grassmann codes. They have been introduced in [23, 24] as a generalization of Reed-Muller codes of the first order and have been widely investigated ever since: both their monomial automorphism groups and minimum weights are well understood, see [10, 11, 12, 15, 19, 25]. Codes associated with subsets of Grassmannians have also been studied; see, for instance [1]. We point out that Grassmannians can also be used to obtain Tanner codes; see [20].

All these codes have a fairly low rate; as such, in order to be efficiently implemented, it is paramount to provide some encoding and decoding algorithms acting locally on the components. To this aim, in [26] an enumerative coding scheme for Grassmannians is considered and some efficient algorithms are presented; see also [18].

Starting with [2] we have been considering linear codes arising from the Plücker embedding of polar Grassmannians of either orthogonal or symplectic type. In particular, in [2] a new family of linear codes related to the Plücker embedding of polar orthogonal Grassmannians $\Delta_{n,k}$ has been introduced and some bounds on its minimum distance have been determined.

In close analogy to orthogonal polar Grassmann codes, in [3] we introduced symplectic polar Grassmann codes, that is codes arising from the Plücker embedding of a symplectic Grassmannian.

Either family of polar Grassmann codes can be obtained from a Grassmann code $\mathcal{C}_{2n+1,k}$ or $\mathcal{C}_{2n,k}$ by just deleting all the columns corresponding respectively to k–spaces which are non-singular with respect to $\mathfrak{q}$ or non-isotropic with respect to $\mathfrak{s}$ — as such they can be regarded in a natural way as punctured versions of $\mathcal{C}_{2n+1,k}$ or $\mathcal{C}_{2n,k}$. We summarize in the following theorems what is currently known about the parameters of these codes.

Theorem 1.3 ([2],[4],[5]). *The known parameters $[N, K, d]$ of $\mathcal{P}_{n,k} := \mathcal{C}(\Delta_{n,k})$ are*

(n,k)	N	K	d	*Reference*
$1 \le k < n$	$\prod_{i=0}^{k-1} \frac{q^{2(n-i)}-1}{q^{i+1}-1}$	$\binom{2n+1}{k}$	$d \ge \widetilde{d}(q,n,k)$	*[2]*
$(3,3)$	$(q^3+1)(q^2+1)(q+1)$	35	$q^2(q-1)(q^3-1)$	*[2]*
$(n,2)$	$\frac{(q^{2n}-1)(q^{2n-2}-1)}{(q-1)(q^2-1)}$	$(2n+1)n$	$q^{4n-5}-q^{3n-4}$	*[4]*

q odd

(n,k)	N	K	d	*Reference*
$1 \le k < n$	$\prod_{i=0}^{k-1} \frac{q^{2(n-i)}-1}{q^{i+1}-1}$	$\binom{2n+1}{k} - \binom{2n+1}{k-2}$	$d \ge \widetilde{d}(q,n,k)$	*[2]*
$(3,3)$	$(q^3+1)(q^2+1)(q+1)$	28	$q^5(q-1)$	*[2]*
$(n,2)$	$\frac{(q^{2n}-1)(q^{2n-2}-1)}{(q-1)(q^2-1)}$	$(2n+1)n-1$	$q^{4n-5}-q^{3n-4}$	*[5]*

q even

$$\widetilde{d}(q,n,k) := (q+1)(q^{k(n-k)}-1)+1$$

Theorem 1.4 ([3]). *The known parameters $[N, K, d]$ of $\mathcal{W}_{n,k} := \mathcal{C}(\overline{\Delta}_{n,k})$ are*

(n,k)	N	K	d	*Reference*
$1 < k \le n$	$\prod_{i=0}^{k-1}(q^{2n-2i}-1)/(q^{i+1}-1)$	$\binom{2n}{k} - \binom{2n}{k-2}$		*[3]*
$(n,2)$	$\frac{(q^{2n}-1)(q^{2n-2}-1)}{(q-1)(q^2-1)}$	$n(2n-1)-1$	$q^{4n-5}-q^{2n-3}$	*[3]*
$(3,3)$	$(q^3+1)(q^2+1)(q+1)$	14	q^6-q^4	*[3]*

1.3. Organization of the paper and Main Results

In Section 2 we recall the notion of prefix enumeration and describe counting algorithms for the points of both $\Delta_{n,2}$ and $\overline{\Delta}_{n,2}$. In particular, in § 2.2 we consider the number of totally $\mathfrak{q}$-singular lines of V spanned by vectors with a prescribed prefix, while in § 2.3 we investigate the totally $\mathfrak{s}$-isotropic lines of $\overline{V}$. The complexity of the prefix enumerators is discussed in § 2.2.3.

Theorem 1.5. *For an orthogonal line Grassmannian, the computational complexity for determining the number of points whose representation begins with a prescribed prefix is $O(n^2)$.*

For a symplectic line Grassmannian, the computational complexity for determining the number of points whose representation begins with a prescribed prefix is $O(n)$.

These results are used in Section 3 to present an enumerative coding scheme according to the approach of [8]. In § 3.1 we analyze the overall complexity of our enumerative encoding scheme.

Theorem 1.6. *The computational complexity of the point enumerator of an orthogonal line Grassmannian is $O(q^2n^3)$. The computational complexity of the point enumerator of a symplectic line Grassmannian is $O(q^2n^2)$.*

Section 4 is dedicated to applications of the scheme introduced in Section 3 to orthogonal and symplectic line polar Grassmann codes. We propose some encoding/decoding and error correction strategies which act locally on the components of the codewords.

2. Prefix enumeration

In this section we shall present an algorithm to count the number of points of a line polar Grassmannian whose representation satisfies certain conditions. This will be essential for the enumerative encoding algorithm of Section 3.

2.1. Preliminaries

In order to simplify the exposition, in this section we shall slightly alter the notation introduced in Section 1.1. For $\varepsilon = 0, 1$, let $V^\varepsilon := V(2n+\varepsilon, q)$ be a vector space of dimension $2n+\varepsilon$ over $\mathbb{F}_q$ and let B_ε be a fixed basis of V^ε. So, according to Section 1.1, $V^0 := \overline{V}$ and $V^1 := V$. Up to projectivities, there is exactly one class of non-degenerate quadratic forms on V^1; hence, it is not restrictive to choose the following quadratic form $\mathfrak{q}$:

$$\mathfrak{q}(\mathbf{x}) = x_1^2 + \sum_{i=1}^{n} x_{2i}x_{2i+1}, \tag{1}$$

where $x = (x_i)_{i=1}^{2n+1}$. The associated bilinear form $\mathfrak{b}$ is

$$\mathfrak{b}(x, y) := 2x_1y_1 + \sum_{i=1}^{n} \left(x_{2i}y_{2i+1} + y_{2i}x_{2i+1}\right),$$

where $x = (x_i)_{i=1}^{2n+1}$, $y = (y_i)_{i=1}^{2n+1}$. Note that, for q even, the form $\mathfrak{b}$ is alternating and degenerate, while for q odd $\mathfrak{b}$ is non-degenerate and symmetric. We will denote by $\mathcal{Q}$ the non-degenerate parabolic quadric of $\mathrm{PG}(V)$ defined by $\mathfrak{q}$.

If $\varepsilon = 0$, consider the following non-degenerate symplectic form $\mathfrak{s} : \overline{V} \times \overline{V} \to \mathbb{F}_q$,

$$\mathfrak{s}(x, y) = \sum_{i=1}^{n} (x_{2i-1}y_{2i} - y_{2i-1}x_{2i}) \tag{2}$$

where $x = (x_i)_{i=1}^{2n}$, $y = (y_i)_{i=1}^{2n}$. We will denote by $\mathcal{W}$ the non-degenerate symplectic polar space of $\mathrm{PG}(\overline{V})$ defined by $\mathfrak{s}$.

Recall that a $(2 \times t)$-matrix G is said to be in *Hermite normal form* or in *row reduced echelon form* (RREF, in brief) if it is in row-echelon form, the leading non-zero entry of each row is 1 and all entries above a leading entry are 0. For each line ℓ of $\mathrm{PG}(V^\varepsilon)$, there are two uniquely determined vectors $X, Y \in \mathbb{F}_q^{2n+\varepsilon}$ such that $\ell = \langle X, Y\rangle$ and $G_\ell := \begin{pmatrix} X \\ Y \end{pmatrix}$ is a $2 \times (2n+\varepsilon)$-matrix in RREF. We call G_ℓ the *representation* of ℓ.

We remind that a line $\ell = \langle X, Y\rangle$ of $\mathrm{PG}(V^1)$ is said to be *totally* $\mathfrak{q}$*-singular* if $\mathfrak{q}(X) = \mathfrak{q}(Y) = 0 = \mathfrak{b}(X, Y)$. Likewise, a line $\ell = \langle X, Y\rangle$ of $\mathrm{PG}(V^0)$ is *totally* $\mathfrak{s}$*-isotropic* if $\mathfrak{s}(X, Y) = 0$.

Denote by $\mathcal{M}_{2,t}$ the set of all $(2 \times t)$-matrices over $\mathbb{F}_q$ and also let

$$\mathcal{M}_2^\varepsilon := \bigcup_{t=0}^{2n+\varepsilon} \mathcal{M}_{2,t}.$$

with $\varepsilon \in \{0, 1\}$ and $\mathcal{M}_{2,0} := \{\emptyset\}$.

Table 1: Useful numbers

Ξ	$\lvert\Xi\rvert_1 := \lvert\{\text{points of } \Xi\}\rvert$	$\lvert\Xi\rvert_2 := \lvert\{\text{lines of } \Xi\}\rvert$
$\mathrm{PG}(v,q)$	$\frac{(q^{v+1}-1)}{q-1}$	$\frac{(q^v-1)(q^{v+1}-1)}{(q^2-1)(q-1)}$
$Q(2v,q)$	$\frac{(q^{2v}-1)}{q-1}$	$\frac{(q^{2v-1}-1)(q^{2v}-1)}{(q^2-1)(q-1)}$
$Q^+(2v-1,q)$	$\frac{(q^v-1)(q^{v-1}+1)}{q-1}$	$\frac{(q^{2v-2}-1)(q^v-1)(q^{v-1}+1)}{(q^2-1)(q-1)}$
$W(2v-1,q)$	$\frac{q^{2v}-1}{q-1}$	$\frac{(q^{2v}-1)(q^{2v-2}-1)}{(q-1)(q^2-1)}$

For $1 \le t \le 2n+\varepsilon$, let $S_t = \begin{pmatrix} A_t \\ B_t \end{pmatrix} \in \mathcal{M}_2^\varepsilon$ with $A_t := (\alpha_1, \alpha_2, \ldots, \alpha_t)$ and $B_t := (\beta_1, \beta_2, \ldots, \beta_t)$ and put $\widehat{A} := (A_t, x_{t+1}, x_{t+2}, \ldots, x_{2n+\varepsilon})$ and $\widehat{B} := (B_t, y_{t+1}, y_{t+2}, \ldots, y_{2n+\varepsilon})$.

Then we say that S_t is the *t-prefix* or the *t-leading part* of the $2 \times (2n+\varepsilon)$-matrix $\begin{pmatrix} \widehat{A} \\ \widehat{B} \end{pmatrix}$. The *length* of S_t is the number t of its columns.
We shall also define the following two vectors of V^ε: $A := (A_t, 0, \ldots, 0)$ and $B := (B_t, 0, \ldots, 0)$.

Definition 2.1. Let

- $n_{\mathfrak{q}} : \mathcal{M}_2^1 \times \mathbb{N} \to \mathbb{N}$ be the function sending any $(S_t, n) \in \mathcal{M}_2^1 \times \mathbb{N}$ to the number of totally $\mathfrak{q}$-singular lines of $\mathrm{PG}(2n,q)$ whose representation in RREF has prefix S_t;
- $n_{\mathfrak{s}} : \mathcal{M}_2^0 \times \mathbb{N} \to \mathbb{N}$ be the function sending any $(S_t, n) \in \mathcal{M}_2^0 \times \mathbb{N}$ to the number of totally $\mathfrak{s}$-isotropic lines of $\mathrm{PG}(2n-1,q)$ whose representation in RREF has prefix S_t.

If S_t is not in RREF, we have $n_{\mathfrak{q}}(S_t, n) = 0$ and $n_{\mathfrak{s}}(S_t, n) = 0$ for any $n \in \mathbb{N}$. Henceforth, we shall always silently assume that S_t is given in RREF.

Definition 2.2. We say that a $(2 \times r)$-matrix

$$S_r = \begin{pmatrix} \alpha_1 & \ldots & \alpha_t & \ldots & \alpha_r \\ \beta_1 & \ldots & \beta_t & \ldots & \beta_r \end{pmatrix}$$

is in *t-Row Echelon Form* (in brief t-REF) if one of the following two conditions holds

a) $\alpha_t = \beta_t = 0$ and S_r is in RREF, or

b) $\alpha_t = 0$ or $\beta_t = 0$ but $(\alpha_t, \beta_t) \neq (0,0)$, S_r is in row-echelon form and the leading non-zero entry in each row is 1.

Note that, in general, a matrix in t-REF is not in RREF. Indeed, given a $(2 \times r)$-matrix S in RREF, if either $\alpha_t = 0$ or $\beta_t = 0$, then S is already also in t-REF; otherwise, when $\beta_t \neq 0$, we can always subtract from the first row of S the second row multiplied by $\lambda = \alpha_t \beta_t^{-1} (\neq 0)$ to get a new matrix

$$S' = \begin{pmatrix} \alpha_1 - \lambda\beta_1 & \ldots & 0 & \ldots & \alpha_r - \lambda\beta_r \\ \beta_1 & \ldots & \beta_t & \ldots & \beta_r \end{pmatrix} \text{ in } t\text{-REF}. \tag{3}$$

It is now easy to see that, for any line ℓ and any $1 \le t \le 2n+\varepsilon$, there exists exactly one matrix in t-REF whose rows span ℓ.

For $q = 2^s$ denote by $\mathrm{Tr}_2(x)$ the absolute trace of $x \in \mathbb{F}_q$, that is $\mathrm{Tr}_2(x) := \sum_{i=0}^{s-1} x^{2^i}$.

2.2. Enumerating orthogonal Grassmannians

In this section we shall compute the enumerating function $n_{\mathfrak{q}}$ introduced in Definition 2.1. If S_t $(1 \leq t \leq 2n+1)$ is not in RREF, then $n_{\mathfrak{q}}(S_t, n) = 0$ for all n. Suppose now $(S_t, n) \in \mathcal{M}_2^1 \times \mathbb{N}$ with $S_t \in \mathcal{M}_{2,t}^1$ in RREF. The value $n_{\mathfrak{q}}(S_t, n)$ is the number of solutions in the unknowns x_i and y_i, $i = t+1, \ldots, 2n+1$, of the system of quadratic equations

$$\begin{cases} \mathfrak{q}(\widehat{A}) = 0 \\ \mathfrak{q}(\widehat{B}) = 0 \\ \mathfrak{b}(\widehat{A}, \widehat{B}) = 0. \end{cases} \tag{4}$$

The first step of the algorithm is to transform S_t in t-REF, see Definition 2.2.

We will distinguish two cases, depending on the parity of t. These cases will not be fully independent: as it will be seen, our algorithm for t even requires some computations with some auxiliary prefixes of odd length and, likewise, some cases with a prefix of odd length are dealt with by reducing to different cases where the prefix has an even number of columns. In any case, as the analysis shall show, this will not lead to an infinite recursion and will ultimately provide the correct value without explicitly solving (4).

2.2.1. Even t

If $t = 0$, then $n_{\mathfrak{q}}(\emptyset, n) = \frac{(q^{2n-1}-1)(q^{2n}-1)}{(q^2-1)(q-1)}$ is the number of the (totally singular) lines of $\mathcal{Q}$; see Table 1. For $t > 0$ even, System (4) can be explicitly written as follows.

$$\begin{cases} \alpha_1^2 + \sum_{i=1}^{t/2-1} \alpha_{2i}\alpha_{2i+1} + \alpha_t x_{t+1} + \sum_{i=t/2+1}^{n} x_{2i}x_{2i+1} = 0 \\ \beta_1^2 + \sum_{i=1}^{t/2-1} \beta_{2i}\beta_{2i+1} + \beta_t y_{t+1} + \sum_{i=t/2+1}^{n} y_{2i}y_{2i+1} = 0 \\ 2\alpha_1\beta_1 + \alpha_t y_{t+1} + \beta_t x_{t+1} + \sum_{i=1}^{t/2-1} (\alpha_{2i}\beta_{2i+1} + \alpha_{2i+1}\beta_{2i}) + \sum_{i=t/2+1}^{n} (x_{2i}y_{2i+1} + x_{2i+1}y_{2i}) = 0. \end{cases} \tag{5}$$

We will compute the number of solutions of the system (5) in the unknowns x_i, y_i, for $t+1 \leq i, j \leq 2n+1$. We distinguish several cases.

A.1) $\boxed{\alpha_t = 0 \text{ and } \beta_t \neq 0.}$ The second and third equations of (5) are linear in respectively y_{t+1} and x_{t+1} and the coefficient of y_{t+1} is non-zero. So, for any choice of $(y_{t+2}, \ldots, y_{2n+1}) \in \mathbb{F}_q^{2n-t}$, the value of y_{t+1} is uniquely determined; there are q^{2n-t} possibilities. Similarly, the third equation directly provides the value of x_{t+1} once $x_{t+2}, \ldots, x_{2n+1}$, satisfying the first equation, are given. Hence, there remains to study the number of solutions of the first equation, which can be written as

$$\mathfrak{q}(A) + \sum_{i=t/2+1}^{n} x_{2i}x_{2i+1} = 0. \tag{6}$$

As S_t is in t-REF, we have $A_t = (\alpha_1, \ldots, \alpha_{t-1}, 0) \neq \mathbf{0}$; i.e. there is $i < t$ such that $\alpha_i \neq 0$. Since $B_t = (\beta_1, \ldots, \beta_t) \neq \mathbf{0}$, any vector solution of (6), with arbitrary choices of $y_{t+2}, \ldots, y_{2n+1}$ gives different lines. Call $\widehat{\eta_0}(A)$ the number of solutions of (6). If $\mathfrak{q}(A) = 0$, then $\widehat{\eta_0}(A)$ is the number of vectors $(x_{t+2}, \ldots, x_{2n+1}) \in \mathbb{F}_q^{2n-t}$ satisfying

$\mathfrak{q}^+(x_{t+2},\ldots,x_{2n+1})=0$ where

$$\mathfrak{q}^+(x_{t+2},\ldots,x_{2n+1}) := \sum_{i=t/2+1}^{n} x_{2i}x_{2i+1}.$$

Hence $\widehat{\eta_0}(A)$ is $(q-1)$ times the number of points of a hyperbolic quadric $\mathcal{Q}^+$ in $\mathrm{PG}(2n-t-1,q)$. If $\mathfrak{q}(A)\neq 0$, then $\widehat{\eta_0}(A)$ is the number of vectors $(x_{t+2},\ldots,x_{2n+1})\in\mathbb{F}_q^{2n-t}$ such that

$$\mathfrak{q}^+(x_{t+2},\ldots,x_{2n+1}) = -\mathfrak{q}(A).$$

If q is odd, then the form $\mathfrak{q}^+$ has the same quadratic character as $-\mathfrak{q}(A)$ for half of the points of $\mathrm{PG}(2n-t-1,q)$ not in $\mathcal{Q}^+$; each of these points contributes 2 vector solutions of (6). The points with quadratic character different from that of $-\mathfrak{q}(A)$ do not contribute any solution. Thus, $\widehat{\eta_0}(A) := \eta_0(\mathfrak{q}(A))$, where

$$\eta_0(c) := \begin{cases} (q-1)|Q^+(2n-t-1,q)|_1+1 & \text{if } c=0 \\ 2\cdot\frac{1}{2}\left(|\mathrm{PG}(2n-t-1,q)|_1-|Q^+(2n-t-1,q)|_1\right) & \text{if } c\neq 0, \end{cases} \tag{7}$$

that is, by Table 1:

$$\eta_0(c) = \begin{cases} (q-1)\cdot\frac{(q^{n-t/2}-1)(q^{n-t/2-1}+1)}{q-1}+1 & \text{if } c=0 \\ \frac{q^{2n-t}-1}{q-1}-\frac{(q^{n-t/2}-1)(q^{n-t/2-1}+1)}{q-1} & \text{if } c\neq 0. \end{cases}$$

For q even, an analogous argument, where we consider the absolute trace $\mathrm{Tr}_2(\mathfrak{q}(A))$ of $\mathfrak{q}(A)$ instead of its quadratic character, leads to the same formula (7).

Finally,

$$n_{\mathfrak{q}}(S_t,n) = \underbrace{|\{\text{solutions to (6)}\}|}_{\text{possibilities for } x_{t+2},\ldots,x_{2n+1}} \times \underbrace{q^{2n-t}}_{\substack{\text{possibilities for} \\ y_{t+2},\cdots,y_{2n+1}}} = \eta_0(\mathfrak{q}(A))\cdot q^{2n-t}.$$

A.2) $\boxed{\alpha_t\neq 0 \text{ and } \beta_t=0.}$ This case is analogous to A.1 with the roles of the first and the second equation reversed. The only difference is for $B=\mathbf{0}$. Indeed,

A.2.1) for $B\neq\mathbf{0}$ and $\beta_t=0$, we argue exactly as in A.1 and $n_{\mathfrak{q}}(S_t,n)=\eta_0(\mathfrak{q}(B))\cdot q^{2n-t}$.

A.2.2) for $B=\mathbf{0}$ we first count the number of points of the hyperbolic quadric having equation $\mathfrak{q}^+(y_{t+2},\ldots,y_{2n+1}) := y_{t+2}y_{t+3}+\ldots+y_{2n}y_{2n+1}=0$. Let $\ell=\langle\widehat{A},\widehat{B}\rangle$ be any line with $\widehat{B}$ given by the previous equation and denote by $i>t$ the index of the first non-zero component y_i of $\widehat{B}$. Then, $\begin{pmatrix}\widehat{A}-x_iy_i^{-1}\widehat{B}\\ \widehat{B}\end{pmatrix}$ is the representative matrix of ℓ in RREF. In particular, $x_i=0$ and the t-prefix of this matrix is the same as that of $\begin{pmatrix}\widehat{A}\\ \widehat{B}\end{pmatrix}$. So, there are q^{2n-t-1} possibilities for $x_{t+1},\ldots,x_{2n+1}$. Thus,

$$n_{\mathfrak{q}}(S_t,n) := \frac{q^{2n-t-1}}{q-1}(q^{n-t/2}-1)(q^{n-t/2-1}+1).$$

A.3) $\boxed{\alpha_t = \beta_t = 0.}$ In this case the matrix $G = \begin{pmatrix} \widehat{A} \\ \widehat{B} \end{pmatrix}$ has the form

$$G = \begin{pmatrix} \alpha_1 & \dots & \alpha_{t-1} & 0 & x_{t+1} & \dots x_{2n+1} \\ \beta_1 & \dots & \beta_{t-1} & 0 & y_{t+1} & \dots y_{2n+1} \end{pmatrix}.$$

As the coefficients of x_{t+1} and y_{t+1} in the equations of (5) are both zero, the system (5) is formally the same as the system defined by

$$G' = \begin{pmatrix} \alpha_1 & \dots & \alpha_{t-1} & x_{t+2} & \dots x_{2n+1} \\ \beta_1 & \dots & \beta_{t-1} & y_{t+2} & \dots y_{2n+1} \end{pmatrix}.$$

We shall call "reduced" this new system, where the unknowns x_{t+1} and y_{t+1} have been removed. It is straightforward to see that for each solution of the reduced system there are q^2 solutions of (5), being x_{t+1} and y_{t+1} arbitrary. Note that the number of solutions of the reduced system is $n_{\mathfrak{q}}(S_{t-1}, n-1)$ where

$$S_{t-1} := \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} \end{pmatrix}.$$

We now consider three subcases:

A.3.1) $\boxed{A_t = B_t = \mathbf{0}.}$ In this case, $n_{\mathfrak{q}}(S_t, n)$ is the number of lines contained in the parabolic quadric $\mathcal{Q}$ defined by $\mathfrak{q}$ and in the subspace Π of codimension t described by the equations

$$x_1 = 0, x_2 = 0, \dots, x_t = 0.$$

As $\mathcal{Q}' := \Pi \cap \mathcal{Q}$ is a cone of vertex $W = (\overbrace{0, 0, \dots, 0}^{t}, 1, 0, \dots, 0)$ and basis the hyperbolic quadric $\mathcal{Q}^+$ of $\mathrm{PG}(2n-t-1, q)$ with equation

$$\begin{cases} x_1 = x_2 = \dots = x_t = 0 \\ x_{t+2}x_{t+3} + x_{t+4}x_{t+5} + \dots + x_{2n}x_{2n+1} = 0, \end{cases}$$

we have $n_{\mathfrak{q}}(S_t, n) = \sigma q^2 + |\mathcal{Q}^+|_1$, where $\sigma = |\mathcal{Q}^+|_2$ is the number of lines of $\mathcal{Q}^+$; see Table 1.

A.3.2) $\boxed{A_t \neq \mathbf{0} \text{ and } B_t = \mathbf{0}.}$ In this case, $n_{\mathfrak{q}}(S_t, n) := q^2 n_{\mathfrak{q}}(S_{t-1}, n-1) + \sigma_1$, where σ_1 corresponds to the number of solutions of (5) which do not arise from solutions of the reduced system. This happens only if the second row of G' is null, but the second row of G is not. That is,

$$G = \begin{pmatrix} A_t & 0 & x_{t+2} & \dots & x_{2n+1} \\ \mathbf{0} & 1 & 0 & \dots & 0 \end{pmatrix}.$$

Thus, $\sigma_1 = \eta_0(\mathfrak{q}(A))$, see (7).

A.3.3) $\boxed{A_t \neq \mathbf{0} \text{ and } B_t \neq \mathbf{0}.}$ In this case, $n_{\mathfrak{q}}(S_t, n) = q^2 n_{\mathfrak{q}}(S_{t-1}, n-1)$ and we apply a recursive argument (see Case B.1 in § 2.2.2).

Recall that $A_t = \mathbf{0}$ and $B_t \neq \mathbf{0}$ cannot occur as the matrix S_t is in t-REF.

Computing the value of $n_{\mathfrak{q}}(S_t, n)$ when $(\alpha_t, \beta_t) = (0, 0)$ has thus been reduced to determining $n_{\mathfrak{q}}(S_{t-1}, n-1)$, where the number of columns of S_{t-1} is odd and the number of unknowns is $2n - t$.

2.2.2. Odd t

For t odd System (4) can be explicitly written as follows.

$$\begin{cases} \alpha_1^2 + \sum_{i=1}^{(t-1)/2} \alpha_{2i}\alpha_{2i+1} + \sum_{i=(t+1)/2}^{n} x_{2i}x_{2i+1} = 0 \\ \beta_1^2 + \sum_{i=1}^{(t-1)/2} \beta_{2i}\beta_{2i+1} + \sum_{i=(t+1)/2}^{n} y_{2i}y_{2i+1} = 0 \\ 2\alpha_1\beta_1 + \sum_{i=1}^{(t-1)/2} (\alpha_{2i}\beta_{2i+1} + \alpha_{2i+1}\beta_{2i}) + \sum_{i=(t+1)/2}^{n} (x_{2i}y_{2i+1} + x_{2i+1}y_{2i}) = 0. \end{cases} \tag{8}$$

As in Section 2.1, let $S_t = \begin{pmatrix} A_t \\ B_t \end{pmatrix}$ be in RREF with $A_t = (\alpha_1, \dots, \alpha_t)$ and $B_t = (\beta_1, \dots, \beta_t)$. We first replace the $(2 \times t)$-matrix S_t with the $2 \times (t+1)$-matrix $S_{\gamma,\delta}$ obtained from S_t by adding the column $\begin{pmatrix} \gamma \\ \delta \end{pmatrix}$, with $\gamma, \delta \in \mathbb{F}_q$, i.e. $S_{\gamma,\delta} = \begin{pmatrix} A_t & \gamma \\ B_t & \delta \end{pmatrix}$. By Definition 2.1, $n_{\mathfrak{q}}(S_{\gamma,\delta}, n) = 0$ if $S_{\gamma,\delta}$ is not in RREF. Hence

$$n_{\mathfrak{q}}(S_t, n) = \sum_{(\gamma,\delta)\in\mathbb{F}_q^2} n_{\mathfrak{q}}(S_{\gamma,\delta}, n).$$

We distinguish several cases.

B.1) $\boxed{A_t \neq \mathbf{0} \text{ and } B_t \neq \mathbf{0}.}$ We need to compute the values $n_{\mathfrak{q}}(S_{\gamma,\delta}, n)$ where $S_{\gamma,\delta}$ has an even number $t+1$ of columns. More precisely,

$$n_{\mathfrak{q}}(S_t, n) = \sum_{\substack{(\gamma,\,\delta)\,\in\,\mathbb{F}_q^2 \\ \gamma\,\neq\,0\,\neq\,\delta}} n_{\mathfrak{q}}(S_{\gamma,\delta}, n) + \sum_{\gamma\in\mathbb{F}_q\setminus\{0\}} n_{\mathfrak{q}}(S_{\gamma,0}, n) + \sum_{\delta\in\mathbb{F}_q\setminus\{0\}} n_{\mathfrak{q}}(S_{0,\delta}, n) + n_{\mathfrak{q}}(S_{0,0}, n).$$

B.1.1) $\boxed{\sum_{\substack{(\gamma,\,\delta)\,\in\,\mathbb{F}_q^2 \\ \gamma\,\neq\,0\,\neq\,\delta}} n_{\mathfrak{q}}(S_{\gamma,\delta}, n).}$ Put $\lambda = \delta^{-1}\gamma$. We have $n_{\mathfrak{q}}(S_{\gamma,\delta}, n) = n_{\mathfrak{q}}(S_{t+1}, n)$ where

$$S_{t+1} := \begin{pmatrix} \alpha_1 - \lambda\beta_1 & \dots & \alpha_t - \lambda\beta_t & 0 \\ \beta_1 & \dots & \beta_t & \delta \end{pmatrix}.$$

As S_{t+1} is in $(t+1)$-REF, we are lead back to Case A.1 of § 2.2.1. Thus,

$$n_{\mathfrak{q}}(S_{t+1}, n) = q^{2n-t-1}\eta_1(c),$$

with $\eta_1(c)$ the number of solutions of the equation $\mathfrak{q}(A - \lambda B) = 0$, as λ varies in $\mathbb{F}_q \setminus \{0\}$. If $c := \mathfrak{q}(A - \lambda B)$, then (see also (7))

$$\eta_1(c) := \begin{cases} (q-1)|Q^+(2n-t-2, q)|_1 + 1 & \text{for } c = 0 \\ |\mathrm{PG}(2n-t-2, q)|_1 - |Q^+(2n-t-2, q)|_1 & \text{for } c \neq 0, \end{cases} \tag{9}$$

that is, by Table 1:

$$\eta_1(c) = \begin{cases} (q-1)\cdot\frac{(q^{n-(t+1)/2}-1)(q^{n-(t+3)/2}+1)}{q-1} + 1 & \text{if } c = 0 \\ 2\cdot\frac{1}{2}\left(\frac{q^{2n-t-1}-1}{q-1} - \frac{(q^{n-(t+1)/2}-1)(q^{n-(t+3)/2}+1)}{q-1}\right) & \text{if } c \neq 0. \end{cases}$$

We have

$$c = \mathfrak{q}(A) - \lambda\mathfrak{b}(A,B) + \lambda^2\mathfrak{q}(B). \tag{10}$$

Let now ξ be the number of non-zero solutions of (10) in the unknown λ. The possible values assumed by ξ are outlined in Table 2 for q odd and in Table 3 for q even. For q odd, the symbols $\square$ and $\not\square$ represent respectively the set of all non-zero square elements and the set of non-square elements in $\mathbb{F}_q$. Hence,

Table 2: Number ξ of solutions of $\mathfrak{q}(A) - \lambda\mathfrak{b}(A,B) + \lambda^2\mathfrak{q}(B) = 0$ for q odd.

$\mathfrak{q}(A)$	$\mathfrak{b}(A,B)$	$\mathfrak{q}(B)$	Δ	ξ
0	0	0	0	$q-1$
0	$\neq 0$	$\neq 0$	$*$	1
0	0	$\neq 0$	0	0
0	$\neq 0$	0	$*$	0
$\neq 0$	0	0	$*$	0
$\neq 0$	$\neq 0$	0	$*$	1
$\neq 0$	Any	$\neq 0$	$\square$	2
$\neq 0$	Any	$\neq 0$	0	1
$\neq 0$	Any	$\neq 0$	$\not\square$	0

$$\Delta := \mathfrak{b}(A,B)^2 - 4\mathfrak{q}(A)\mathfrak{q}(B).$$

$*$ means that there are no conditions on Δ.

Table 3: Number ξ of solutions of $\mathfrak{q}(A) + \lambda\mathfrak{b}(A,B) + \lambda^2\mathfrak{q}(B) = 0$ for q even.

$\mathfrak{q}(A)$	$\mathfrak{b}(A,B)$	$\mathfrak{q}(B)$	Θ	ξ
0	0	0	$*$	$q-1$
0	$\neq 0$	$\neq 0$	$*$	1
0	0	$\neq 0$	$*$	0
0	$\neq 0$	0	$*$	0
$\neq 0$	0	0	$*$	0
$\neq 0$	$\neq 0$	0	$*$	1
$\neq 0$	0	$\neq 0$	$*$	1
$\neq 0$	$\neq 0$	$\neq 0$	0	2
$\neq 0$	$\neq 0$	$\neq 0$	1	0

$$\Theta := \mathrm{Tr}_2\left(\frac{\mathfrak{q}(A)\mathfrak{q}(B)}{\mathfrak{b}(A,B)^2}\right).$$

$*$ means that there are no conditions on Θ or Θ does not exist.

$$\sum_{\substack{(\gamma,\,\delta)\,\in\,\mathbb{F}_q^2 \\ \gamma\neq 0\neq\delta}} n_{\mathfrak{q}}(S_{\gamma,\delta},n) = \underbrace{(q-1)}_{\text{cases for }\delta}\, q^{2n-t-1}\Big(\underbrace{\xi\eta_1(0)}_{\substack{\text{first eq.}\\ \text{homogeneous}}} + \underbrace{(q-1-\xi)\eta_1(1)}_{\substack{\text{first eq.}\\ \text{nonhomogeneous}}}\Big).$$

B.1.2) $\boxed{\sum_{\gamma\in\mathbb{F}_q\setminus\{0\}} n_{\mathfrak{q}}(S_{\gamma,0},n) + \sum_{\delta\in\mathbb{F}_q\setminus\{0\}} n_{\mathfrak{q}}(S_{0,\delta},n).}$ Suppose $\gamma = 0$ and $\delta \neq 0$. Arguing as in Case A.1 of § 2.2.1, we see that $n_{\mathfrak{q}}(S_{0,\delta},n) = n_{\mathfrak{q}}(S_{0,1},n)$ for any $\delta \neq 0$. Hence,

$$\sum_{\gamma\in\mathbb{F}_q\setminus\{0\}} n_{\mathfrak{q}}(S_{\gamma,0},n) = (q-1)n_{\mathfrak{q}}(S_{0,1},n),$$

where the factor $n_{\mathfrak{q}}(S_{0,1},n)$ can be directly computed as in Case A.1.
The case $\gamma \neq 0$ and $\delta = 0$ is analogous to case A.2.1; hence,

$$\sum_{\delta\in\mathbb{F}_q\setminus\{0\}} n_{\mathfrak{q}}(S_{0,\delta},n) = (q-1)n_{\mathfrak{q}}(S_{1,0},n).$$

B.1.3) $\boxed{n_{\mathfrak{q}}(S_{0,0},n).}$ In this case, $n_{\mathfrak{q}}(S_{0,0},n) = q^2 n_{\mathfrak{q}}(S_t,n-1)$ as x_{t+2} and y_{t+2} may be chosen arbitrarily and $n_{\mathfrak{q}}(S_t,n-1)$ is the number of solutions of the system associated with

$$G' = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t & x_{t+3} & \dots & x_{2n+1} \\ \beta_1 & \beta_2 & \dots & \beta_t & y_{t+3} & \dots & y_{2n+1} \end{pmatrix}.$$

B.2) $\boxed{A_t = B_t = \mathbf{0}.}$ An argument analogous to Case A.3.1 of § 2.2.1 shows that we have to determine the number of lines of a hyperbolic quadric $\mathcal{Q}^+$ in $\mathrm{PG}(2n-t,q)$ with equation

$$x_{t+1}x_{t+2} + \ldots + x_{2n}x_{2n+1} = 0;$$

we refer to Table 1 for the actual value.

B.3) $\boxed{A_t \neq \mathbf{0} \text{ and } B_t = \mathbf{0}.}$ In this case all the $2 \times (t+1)$-matrices $S_{\gamma,\delta}$ are of the form

$$S_{\gamma,\delta} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_t & \gamma \\ 0 & 0 & \ldots & 0 & \delta \end{pmatrix}.$$

When $S_{\gamma,\delta}$ is taken in $(t+1)$-REF, either $\delta = 1$ and $\gamma = 0$ or $\delta = 0$ and γ is arbitrary. Note that for any solution of the first equation of (8) there are $q-1$ vector solutions of the second equation yielding the same line. In this case,

$$n_{\mathfrak{q}}(S_t, n) = n_{\mathfrak{q}}(S_{0,1}, n) + \sum_{\gamma \in \mathbb{F}_q \setminus \{0\}} n_{\mathfrak{q}}(S_{\gamma,0}, n) + n_{\mathfrak{q}}(S_{0,0}, n).$$

B.3.1) $\boxed{n_{\mathfrak{q}}(S_{0,1}, n).}$ We can compute $n_{\mathfrak{q}}(S_{0,1}, n)$ using the same approach as in Case A.1.

B.3.2) $\boxed{\sum_{\gamma \in \mathbb{F}_q \setminus \{0\}} n_{\mathfrak{q}}(S_{\gamma,0}, n).}$ We have $S_{\gamma,0} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_t & \gamma \\ 0 & 0 & \ldots & 0 & 0 \end{pmatrix}$. With an approach similar to Case A.2.2 we see that

$$n_{\mathfrak{q}}(S_{\gamma,0}, n) = n_{\mathfrak{q}}(S_{1,0}, n) = q^{2n-t-2} \cdot \frac{(q^{n-(t+1)/2} - 1)(q^{n-(t+3)/2} + 1)}{q-1}.$$

Hence, this case contributes $q^{2n-t-2}(q^{n-(t+1)/2} - 1)(q^{n-(t+3)/2} + 1)$ to $n_{\mathfrak{q}}(S_t, n)$.

B.3.3) $\boxed{n_{\mathfrak{q}}(S_{0,0}, n).}$ We need to compute $n_{\mathfrak{q}}(S_{0,0}, n)$, i.e. the number of solutions of the following system in the unknowns $x_{t+2}, \ldots, x_{2n+1}, y_{t+2}, \ldots, y_{2n+1}$:

$$\begin{cases} \mathfrak{q}(A) + 0x_{t+2} + x_{t+3}x_{t+4} + \ldots + x_{2n}x_{2n+1} = 0 \\ 0y_{t+2} + y_{t+3}y_{t+4} + \ldots + y_{2n}y_{2n+1} = 0 \\ 0y_{t+2} + x_{t+2}0 + x_{t+3}y_{t+4} + x_{t+4}y_{t+3} + \ldots + x_{2n+1}y_{2n} = 0. \end{cases} \tag{11}$$

We shall refer to the system in the unknowns $x_{t+3}, \ldots, x_{2n+1}, y_{t+3}, \ldots, y_{2n+1}$ obtained from (11) by removing the unknowns x_{t+2} and y_{t+2} as the "reduced" one. With arguments similar to those of Case A.3.2 we see that each solution of the reduced system corresponds to q^2 solutions of (11). However, there are also solutions of (11) not arising from the reduced system. These solutions correspond to cases in which $y_{t+2} \neq 0$ and $y_{t+3} = \cdots = y_{2n+1} = 0$; that is, the representative matrix of the totally singular lines considered in these cases is

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_t & 0 & 0 & x_{t+3} & \ldots & x_{2n+1} \\ 0 & 0 & \ldots & 0 & 0 & 1 & 0 & \ldots & 0 \end{pmatrix};$$

there are $\eta_1(\mathfrak{q}(A))$ possibilities; see (9). Hence,

$$n_{\mathfrak{q}}(S_{0,0}, n) = q^2 n_{\mathfrak{q}}(S_t, n-1) + \eta_1(\mathfrak{q}(A)).$$

The case $A = \mathbf{0}$ and $B \neq \mathbf{0}$ cannot happen according to the convention we adopted.

The above arguments provide a complete description of how to compute the function $n_{\mathfrak{q}}(S_t, n)$ for any $S_t \in \mathcal{M}_2^1$ and $n \in \mathbb{N}$. We summarize the details of the algorithm in Table 4.

Table 4: Enumerator for Orthogonal Line Grassmannians

$S_t = \begin{pmatrix} A_t \\ B_t \end{pmatrix}$	t	Case	$n_{\mathfrak{q}}(S,n)$	Complexity
$\emptyset$	0		$\frac{(q^n-1)(q^{n+1}-1)}{(q^2-1)(q-1)}$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & 0 \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & \beta_t \end{pmatrix}$ $\beta_t \neq 0$	Even	$A.1$	$q^{2n-t}\eta_0(\mathfrak{q}(A))$	$O(t)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & 0 \end{pmatrix}$ $\alpha_t \neq 0$ $(\beta_1,\dots,\beta_{t-1}) \neq \mathbf{0}$	Even	$A.2.1$	$q^{2n-t}\eta_0(\mathfrak{q}(B))$	$O(t)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ $\alpha_t \neq 0$	Even	$A.2.2$	$\frac{q^{2n-t-1}}{q-1}(q^{n-t/2}-1)(q^{n-t/2-1}+1)$	$O(1)$
$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$	Even	$A.3.1$	$\sigma q^2 + (q^{n-t/2}-1)(q^{n-t/2-1}+1)$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ $(\alpha_1,\dots,\alpha_{t-1}) \neq \mathbf{0}$	Even	$A.3.2$	$q^2 n_{\mathfrak{q}}^O(S_{t-1},n-1) + \eta_0(\mathfrak{q}(A))$; with $n_{\mathfrak{q}}^O(S_{t-1},n-1)$ as in Case $B.3$	$O(n^2)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & 0 \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & 0 \end{pmatrix}$ $(\alpha_1,\dots,\alpha_{t-1}) \neq \mathbf{0}$ $(\beta_1,\dots,\beta_{t-1}) \neq \mathbf{0}$	Even	$A.3.3$	$q^2 n_{\mathfrak{q}}^O(S_{t-1},n-1)$; with $n_{\mathfrak{q}}^O(S_{t-1},n-1)$ as in Case $B.1$	$O(n^2)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & \beta_t \end{pmatrix}$ $(\alpha_1,\dots,\alpha_{t-1},\alpha_t) \neq \mathbf{0}$ $(\beta_1,\dots,\beta_{t-1},\beta_t) \neq \mathbf{0}$	Odd	$B.1$	$q^{2n-t-1}\eta_1(c) + (q-1)n_{\mathfrak{q}}^E(S_{0,1},n) +$ $(q-1)n_{\mathfrak{q}}^E(S_{1,0},n)) + q^2 n_{\mathfrak{q}}^O(S_t,n-1)$; with $n_{\mathfrak{q}}^E(S_{0,1},n)$ as in Case $A.1$ and $n_{\mathfrak{q}}^E(S_{1,0},n)$ as in Case $A.2.1$.	$O(n^2)$
$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$	Odd	$B.2$	$\frac{(q^{2n-t-1}-1)(q^{n-(t-1)/2}-1)(q^{n-(t-3)/2}+1)}{(q^2-1)(q-1)}$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ 0 & 0 & \dots & 0 \end{pmatrix}$ $(\alpha_1,\dots,\alpha_t) \neq \mathbf{0}$	Odd	$B.3$	$n_{\mathfrak{q}}^E(S_{0,1},n) + n_{\mathfrak{q}}^E(S_{1,0},n) +$ $q^2 n_{\mathfrak{q}}^E(S_t,n-1) + \eta_1(\mathfrak{q}(A))$; with $n_{\mathfrak{q}}^E(S_{0,1},n)$ as in Case $A.1$ and $n_{\mathfrak{q}}^E(S_{1,0},n)$ as in Case $A.2.2$.	$O(n^2)$

For the meaning of the symbols and the constants, see the relevant Cases A.x and B.x. in § 2.2.1 and § 2.2.2.

2.2.3. Complexity

We now analyze the complexity of the algorithm described in § 2.2.1 and § 2.2.2.

Given a $(2\times t)$-matrix $S_t = \begin{pmatrix} A_t \\ B_t \end{pmatrix}$ in RREF and $n \in \mathbb{N}$, we shall denote by $n_{\mathfrak{q}}^E(S_t, n)$ the output of the algorithm with t even (see § 2.2.1) and by $n_{\mathfrak{q}}^O(S_t, n)$ the output with t odd (see § 2.2.2). We will write $\kappa(n_{\mathfrak{q}}(S_t, n))$ for the number of multiplications required to compute $n_{\mathfrak{q}}(S_t, n)$. The complexity of the various steps of the algorithm will now be examined.

STEP 1. If $S_0 = \emptyset$ or we are in the hypotheses of cases A.2.2, A.3.1 or B.2, then we can provide the value of $n_{\mathfrak{q}}(S_t, n)$ by directly applying a formula with fixed complexity $O(1)$; see also Table 4.

STEP 2. Otherwise, transform S_t in t-REF; this requires t products and t sums.

STEP 3. If t is even, compute $n_{\mathfrak{q}}^E(S_t, n)$; otherwise compute $n_{\mathfrak{q}}^O(S_t, n)$.

Clearly,

$$\kappa(n_{\mathfrak{q}}(S_t, n)) \leq t + \max\{\kappa(n_{\mathfrak{q}}^E(S_t, n)), \kappa(n_{\mathfrak{q}}^O(S_t, n))\}.$$

We shall now analyze in detail $\kappa(n_{\mathfrak{q}}^E(S_t, n))$ and $\kappa(n_{\mathfrak{q}}^O(S_t, n))$.

- $\boxed{n_{\mathfrak{q}}^E(S_t, n).}$

  1. If S_t is as in Case A.1, then we need to evaluate $\mathfrak{q}(A)$; this requires t products and t sums; thus it has complexity $O(t)$. Likewise, under the assumptions of A.2.1, the complexity to determine $n_{\mathfrak{q}}(S_t, n)$ is $O(t)$.
  2. If S_t satisfies the hypotheses of A.3.2 or A.3.3, we need to consider the complexity of $n_{\mathfrak{q}}^O(S_{t-1}, n-1)$ where S_{t-1} is a $2 \times (t-1)$-matrix obtained from S_t by deleting its last column. Then we need to consider a case of odd length $n_{\mathfrak{q}}^O(S_{t-1}, n-1)$. As it will be shown below, the complexity here is at most $O(n^2)$.

- $\boxed{n_{\mathfrak{q}}^O(S_t, n).}$ We claim that

$$\kappa(n_{\mathfrak{q}}^O(S_t, n)) \leq 3t + \kappa(n_{\mathfrak{q}}^O(S_t, n-1)). \tag{12}$$

  By Cases B.1 and B.3, computing $n_{\mathfrak{q}}^O(S_t, n)$ requires to determine the values of $n_{\mathfrak{q}}^E(S_{\gamma,\delta}, n)$ for $(\gamma, \delta) = (0, 1)$, $(\gamma, \delta) = (1, 0)$ and $\gamma \neq 0 \neq \delta$ (Case B.1)) and the value of $n_{\mathfrak{q}}^O(S_t, n-1)$ (Case B.3). The first three cases have already been shown to have complexity at most $O(t)$. Hence, the claim follows.

  Observe that $\kappa(n_{\mathfrak{q}}^O(S_t, \frac{t-1}{2})) = 3\frac{t-1}{2}$, since, in this case, we just need to check if the line spanned by A and B is totally singular. Note that $n_{\mathfrak{q}}^O(S_t, \frac{t-1}{2})$ is the number of totally singular lines of $\mathrm{PG}(t-1, q)$ whose representative matrix is S_t. Clearly, this number is 1 if the line spanned by the rows of S_t is singular and 0 otherwise. By recursively applying (12), since $t \leq 2n+1$, we have

$$\begin{aligned}\kappa(n_{\mathfrak{q}}^O(S_t, n)) \leq 3t + \kappa(n_{\mathfrak{q}}^O(S_t, n-1)) + O(1) \leq 6t + \kappa(n_{\mathfrak{q}}^O(S_t, n-2)) + O(1) \leq \dots \\ \leq 3 \sum_{i=1}^{n-(t+1)/2} t + \kappa(n_{\mathfrak{q}}^O(S_t, \frac{t-1}{2})) + O(1) \leq O(n^2).\end{aligned}$$

In summary, the complexity of the algorithm to determine $n_{\mathfrak{q}}(S_t, n)$ is $O(n^2)$. This proves Theorem 1.5 for the orthogonal line Grassmannian.

2.3. Enumerating Symplectic Grassmannians

Following Definition 2.1, given any $S_t = \begin{pmatrix} A_t \\ B_t \end{pmatrix} \in \mathcal{M}_2^0$, where $A_t = (\alpha_1, \ldots, \alpha_t)$, $B_t = (\beta_1, \ldots, \beta_t)$, $1 \leq t \leq 2n$, denote by $n_{\mathfrak{s}}(S_t, n)$ the number of totally $\mathfrak{s}$-isotropic lines of $\mathrm{PG}(2n-1, q)$ spanned by $\widehat{A} = (\alpha_1, \ldots, \alpha_t, x_{t+1}, \ldots, x_{2n})$ and $\widehat{B} = (\beta_1, \ldots, \beta_t, y_{t+1}, \ldots, y_{2n})$ as $x_{t+1}, \ldots, x_{2n}, y_{t+1}, \ldots, y_{2n}$ vary. Also, put $A = (A_t, 0, \ldots, 0)$ and $B = (B_t, 0, \ldots, 0)$. We remind that S_t is assumed to be in RREF. (Otherwise, $n_{\mathfrak{s}}(S_t, n) = 0$). In this section we compute $n_{\mathfrak{s}}(S_t, n)$, with an approach similar to that of Section 2.2. We have to determine the number of solutions of the equation $\mathfrak{s}(\widehat{A}, \widehat{B}) = 0$ in the unknowns x_i, y_i for $t+1 \leq i \leq 2n$, see Definition 2.2. The first step of the algorithm is to transform S_t in t-REF using (3).

Let $\mathfrak{s}'$ be the alternating form induced by the restriction of $\mathfrak{s}$ to the subspace of $\overline{V}$ of equation $x_1 = x_2 = \cdots = x_t = 0$. We distinguish two subcases.

2.3.1. Even t

There are three possibilities:

C.1) $\boxed{A_t = B_t = \mathbf{0}.}$ In this case, $n_{\mathfrak{s}}(S_t, n)$ is the number of totally $\mathfrak{s}'$-isotropic lines in a subspace $\mathrm{PG}(2n-t-1, q)$. Thus (see Table 1),

$$n_{\mathfrak{s}}(S_t, n) = \frac{(q^{2n-t}-1)(q^{2n-t-2}-1)}{(q-1)(q^2-1)}.$$

C.2) $\boxed{A_t \neq \mathbf{0},\ B_t = \mathbf{0}.}$ In this case, the representative matrix of the lines we consider has the form

$$G = \begin{pmatrix} \alpha_1 & \ldots & \alpha_t & x_{t+1} & \ldots & x_{2n} \\ 0 & \ldots & 0 & y_{t+1} & \ldots & y_{2n} \end{pmatrix}.$$

Suppose $Y = (y_{t+1}, \ldots, y_{2n})$ is a given non-null vector with leading coefficient $y_i = 1$, $i > t$. There are $\frac{q^{2n-t}-1}{q-1}$ choices for Y. For any such Y we count the number of vectors $X = (x_{t+1}, \ldots, x_{2n})$ with $x_i = 0$ such that $\mathfrak{s}'(X, Y) = 0$: this amounts to q^{2n-t-2}. Hence,

$$n_{\mathfrak{s}}(S_t, n) = q^{2n-t-2}\frac{q^{2n-t}-1}{q-1}.$$

C.3) $\boxed{A_t \neq \mathbf{0},\ B_t \neq \mathbf{0}.}$ We distinguish two subcases, according to the value of $\mathfrak{s}(A, B)$.

C.3.1) $\boxed{\mathfrak{s}(A, B) = 0.}$ In this case we count the number of pairs of vectors (X, Y) with $X, Y \in \mathbb{F}_q^{2n-t}$ and $\mathfrak{s}'(X, Y) = 0$. If $X = \mathbf{0}$, then there are q^{2n-t} different choices for Y such that $\mathfrak{s}'(X, Y) = 0$. If $X \neq \mathbf{0}$, there are q^{2n-t-1} choices for Y such that $\mathfrak{s}'(X, Y) = 0$. Thus,

$$n_{\mathfrak{s}}(S_t, n) = q^{2n-t-1}(q^{2n-t}-1) + q^{2n-t}. \tag{13}$$

C.3.2) $\boxed{\mathfrak{s}(A, B) \neq 0.}$ Let $X = (x_{t+1}, \ldots, x_{2n})$ be a fixed non-null vector. There are $q^{2n-t}-1$ choices for such X. We count the number of vectors $Y = (y_{t+1}, \ldots, y_{2n})$ such that $\mathfrak{s}'(X, Y) = -\mathfrak{s}(A, B)$. This is a linear equation in the unknowns $y_{t+1}, \ldots, y_{2n}$; hence, there are q^{2n-t-1} choices for Y. Thus,

$$n_{\mathfrak{s}}(S_t, n) = (q^{2n-t}-1)q^{2n-t-1}. \tag{14}$$

2.3.2. Odd t

When t is odd, we first replace the matrix $S_t = \begin{pmatrix} A_t \\ B_t \end{pmatrix} \in \mathcal{M}_a^0$, with a $2 \times (t+1)$-matrix $S_{\gamma,\delta} := \begin{pmatrix} A_t & \gamma \\ B_t & \delta \end{pmatrix}$ obtained from S_t by adding the column $\begin{pmatrix} \gamma \\ \delta \end{pmatrix}$, with $\gamma, \delta \in \mathbb{F}_q$. By Definition 2.1, $n_{\mathfrak{s}}(S_{\gamma,\delta}, n) = 0$ if $S_{\gamma,\delta}$ is not in RREF. Hence

$$n_{\mathfrak{s}}(S_t, n) = \sum_{(\gamma,\delta)\in\mathbb{F}_q^2} n_{\mathfrak{s}}(S_{\gamma,\delta}, n).$$

We distinguish three subcases.

D.1) $\boxed{A_t = B_t = \mathbf{0}.}$ In this case, $n_{\mathfrak{s}}(S_t, n)$ is the number of lines contained in the symplectic polar space $\mathcal{W}$ defined by $\mathfrak{s}$ and in the subspace Π of codimension t described by the equations

$$x_1 = 0, x_2 = 0, \ldots, x_t = 0.$$

As $\Pi \cap \mathcal{W}$ is a degenerate symplectic polar space with radical of dimension 1, we have $n_{\mathfrak{s}}(S_t, n) = \sigma q^2 + |\mathcal{W}'|_1$, where $\mathcal{W}'$ is a non-degenerate symplectic polar space in $\mathrm{PG}(2n - t - 2, q)$ and $|\mathcal{W}'|_1$ and $\sigma := |\mathcal{W}'|_2$ are respectively the number of points and lines of $\mathcal{W}'$; see Table 1.

D.2) $\boxed{A_t \neq \mathbf{0},\ B_t = \mathbf{0}.}$ In this case the only matrices in RREF are $S_{\gamma,0}$ with $\gamma \in \mathbb{F}_q$ and $S_{0,1}$. Thus,

$$n_{\mathfrak{s}}(S_t, n) = \sum_{\gamma\in\mathbb{F}_q} n_{\mathfrak{s}}(S_{\gamma,0}, n) + n_{\mathfrak{s}}(S_{0,1}, n).$$

By Case C.2 of § 2.3.1, $n_{\mathfrak{s}}(S_{\gamma,0}, n) = n_{\mathfrak{s}}(S_{0,0}, n)$ for all $\gamma \in \mathbb{F}_q$; thus,

$$n_{\mathfrak{s}}(S_t, n) = q n_{\mathfrak{s}}(S_{0,0}, n) + n_{\mathfrak{s}}(S_{0,1}, n),$$

where $n_{\mathfrak{s}}(S_{0,1}, n)$ is computed in Case C.3 of § 2.3.1 (and $n_{\mathfrak{s}}(S_{0,0}, n)$ is computed in Case C.2).

D.3) $\boxed{A_t \neq \mathbf{0}, B_t \neq \mathbf{0}.}$ There are two possibilities.

D.3.1) $\boxed{\alpha_t = \beta_t = 0.}$ In this case, the matrix $S_{\gamma,\delta}$ has the form

$$S_{\gamma,\delta} = \begin{pmatrix} \alpha_1 & \ldots & \alpha_{t-1} & 0 & \gamma \\ \beta_1 & \ldots & \beta_{t-1} & 0 & \delta \end{pmatrix}$$

and it is in t-REF (as S_t is in t-REF). Observe that the number of lines admitting a representative matrix in t-REF whose $(t+1)$-prefix is $S_{\gamma,\delta}$ can be computed as in Case C.3.1 or C.3.2 of § 2.3.1 according as $\mathfrak{s}(A, B) = 0$ or $\mathfrak{s}(A, B) \neq 0$, but does not depend on the choice of γ and δ. Thus,

$$n_{\mathfrak{s}}(S_t, n) = q^2 n_{\mathfrak{s}}(S_{t-1}, n).$$

D.3.2) $\boxed{(\alpha_t, \beta_t) \neq (0, 0).}$ Let $A_\gamma = (\alpha_1, \ldots, \alpha_t, \gamma, 0, \ldots, 0)$ and $B_\delta = (\beta_1, \ldots, \beta_t, \delta, 0, \ldots, 0)$. Clearly,

$$\mathfrak{s}(A_\gamma, B_\delta) = \alpha_1\beta_2 - \alpha_2\beta_1 + \cdots + \alpha_t\delta - \beta_t\gamma.$$

As (α_i, β_i) for $i = 1, \ldots, t$ are all given and $(\alpha_t, \beta_t) \neq (0, 0)$, $\mathfrak{s}(A_\gamma, B_\delta) = 0$ is a non-trivial linear equation in the unknowns γ and δ. Hence, there are exactly q

values of (γ, δ) such that $\mathfrak{s}(A_\gamma, B_\delta) = 0$. For each of these values we have, by Case C.3.1, $q^{2n-t-2}(q^{2n-t-1}-1)+q^{2n-t-1}$ distinct lines to take into account. For the remaining q^2-q values of (γ, δ), such that $\mathfrak{s}(A_\gamma, B_\delta) \neq 0$, we have, by Case C.3.2, $(q^{2n-t-1}-1)q^{2n-t-2}$ distinct lines. Consequently,

$$n_{\mathfrak{s}}(S_t, n) = q^{4n-2t-1}.$$

2.3.3. Complexity

Given a $(2 \times t)$-matrix S_t in RREF and $n \in \mathbb{N}$, the computational complexity of the algorithm to determine $n_{\mathfrak{s}}(S_t, n)$ is $O(n)$. This can be immediately seen by analyzing the steps presented in the previous sections. For the convenience of the reader we summarize the various cases, depending on the structure of S_t, together with their complexity, in Table 5. This proves Theorem 1.5 for symplectic line Grassmannians.

3. Enumerative coding

In this section, following the approach of [8], we construct enumerators for the points of $\Delta_{n,2}$ and $\overline{\Delta}_{n,2}$ using the functions $n_{\mathfrak{q}}$ and $n_{\mathfrak{s}}$ introduced in Section 2. We shall present the full details for the orthogonal Grassmannian $\Delta_{n,2}$; the symplectic case is entirely analogous.

Fix a total order $\preceq$ on the vectors of $\mathbb{F}_q^2$ and write $A \prec B$ if and only if $A \preceq B$ and $A \neq B$. Let ℓ be a totally $\mathfrak{q}$-singular line of V and $G_\ell = (G_1, \ldots, G_{2n+1})$ be its $2 \times (2n+1)$-representative matrix (in RREF), where $G_i \in \mathbb{F}_q^2$ is the i-th column of G_ℓ. For any $j \leq 2n+1$ and $X \in \mathbb{F}_q^2$, let $S_j^X := (G_1, \ldots, G_{j-1}, X)$ be the $(2 \times j)$-matrix comprising the first $j-1$ columns of G_ℓ and whose last column is X.

Let $\mathbb{I} = \{0, \ldots, N-1\}$, with $N = |\Delta_{n,2}|_1$ (see Table 1) and define

$$\iota : \begin{cases} \Delta_{n,2} \to \mathbb{I} \\ \ell \mapsto \iota(G_\ell) := \displaystyle\sum_{j=1}^{2n+1} \sum_{X \prec G_j} n_{\mathfrak{q}}(S_j^X, n). \end{cases} \tag{15}$$

The order $\prec$ defined on the vectors of $\mathbb{F}_q^2$ can be extended to matrices of order $2 \times (2n+1)$ lexicographically; that is $G \ll H$ if and only if there exists $i \in \{1, \ldots, 2n+1\}$ such that $\forall j < i : G_j = H_j$ and $G_i \prec H_i$. By the proof of Theorem 3.1 we see that $G \ll H$ if and only if $\iota(G) < \iota(H)$.

We say that a vector $X \in \mathbb{F}_q^2$ is *allowable in position j for* $(G_1, \ldots, G_{j-1})$ if and only if $n_{\mathfrak{q}}(S_j^X, n) > 0$, i.e. $(G_1, \ldots, G_{j-1}, X, X_{j+1}, \ldots, X_{2n+1})$ represents a totally $\mathfrak{q}$-singular line for at least one choice of $X_{j+1}, \ldots, X_{2n+1}$.

Theorem 3.1. *The index function ι defined in* (15) *is a bijection.*

Proof. As $|\Delta_{n,2}|_1 = |\mathbb{I}|$, it is enough to show that ι is injective. Let

$$\begin{aligned} G &= (G_1, G_2, \ldots, G_{i-1}, G_i, \ldots, G_{2n+1}); \\ H &= (H_1, H_2, \ldots, H_{i-1}, H_i, \ldots, H_{2n+1}). \end{aligned}$$

We will show that if $G \ll H$, then $\iota(G) < \iota(H)$. Suppose $G_i \prec H_i$ and $G_s = H_s \ \forall s < i$. Define

$$\begin{aligned} \iota^{\prec}(G) := \{(X_1, \ldots, X_{2n+1}) : X_1 \prec G_1\} \cup \{(G_1, X_2, \ldots, X_{2n+1}) : X_2 \prec G_2\} \cup \ldots \\ \ldots \cup \{(G_1, G_2, \ldots, G_{2n}, X_{2n+1}) : X_{2n+1} \prec G_{2n+1}\}. \end{aligned} \tag{16}$$

Table 5: Enumerator for Symplectic Line Grassmannians

$S = \begin{pmatrix} A_t \\ B_t \end{pmatrix}$	t	Case	$n_{\mathfrak{s}}(S, n)$	Complexity
$\emptyset$	0		$\frac{(q^{2n-1}-1)(q^{2n-2}-1)}{(q^2-1)(q-1)}$	$O(1)$
$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$	Even	$C.1$	$\frac{(q^{2n-t}-1)(q^{2n-t-2}-1)}{(q^2-1)(q-1)}$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq 0$	Even	$C.2$	$q^{2n-t-2}\frac{q^{2n-t}-1}{q-1}$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_t \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_t) \neq \mathbf{0}$ $\mathfrak{s}(A, B) = 0$	Even	$C.3.1$	$q^{2n-t-1}(q^{2n-t}-1) + q^{2n-t}$	$O(t)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_t \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_t) \neq \mathbf{0}$ $\mathfrak{s}(A, B) \neq 0$	Even	$C.3.2$	$(q^{2n-t}-1)q^{2n-t-1}$	$O(t)$
$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$	Odd	$D.1$	$\frac{(q^{2n-t-1}-1)^2}{(q-1)(q^2-1)}$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq 0$	Odd	$D.2$	$qn^E_{\mathfrak{s}}(S_{0,0}, n) + n^E_{\mathfrak{s}}(S_{0,1}, n)$ with $n^E_{\mathfrak{s}}(S_{0,0}, n)$ as in Case $C.2$ and $n^E_{\mathfrak{s}}(S_{0,1}, n)$ as in Cases $C.3.1$ or $C.3.2$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & 0 \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_{t-1}) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_{t-1}) \neq \mathbf{0}$	Odd	$D.3.1$	$q^2 n^E_{\mathfrak{s}}(S_{t-1}, n)$ with $n^E_{\mathfrak{s}}(S_{t-1}, n)$ as in Cases $C.3.1$ or $C.3.2$	$O(t)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_t \end{pmatrix}$ $(\alpha_1, \dots, \alpha_{t-1}) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_{t-1}) \neq \mathbf{0}$ $(\alpha_t, \beta_t) \neq (0, 0)$	Odd	$D.3.2$	$q^{4n-2t-1}$	$O(1)$

For the meaning of the symbols and the constants, see the relevant Cases C.x and D.x. in § 2.3.1 and § 2.3.2.

In (16) and throughout this proof, the elements of the sets are all matrices in RREF representing totally $\mathfrak{q}$-singular lines. Clearly, if $G_1 = H_1, \ldots, G_{i-1} = H_{i-1}$ and $G_i \prec H_i$ for some columns $H_1, \ldots, H_i$, then

$$G \in \{(G_1, \ldots, G_{i-1}, X_i, X_{i+1}, \ldots, X_{2n+1}) : X_i \prec H_i\};$$

in particular, $G \in \iota^{\prec}(H)$. Furthermore, if $G \in \iota^{\prec}(H)$, then $\iota^{\prec}(G) \subset \iota^{\prec}(H)$. Suppose $Y := (Y_1, \ldots, Y_{2n+1}) \in \iota^{\prec}(G)$. Then, there exists j such that $Y_1 = G_1, \ldots, Y_{j-1} = G_{j-1}$ and $Y_j \prec G_j$.

- If $j < i$, then $Y_1 = G_1 = H_1, \ldots, Y_{j-1} = G_{j-1} = H_{j-1}$ and $Y_j \prec H_j = G_j$; thus $Y \in \iota^{\prec}(H)$.
- If $j = i$, then $Y_i \prec G_i \prec H_i$ and $Y \in \{(G_1, \ldots, G_{i-1}, X_i, X_{i+1}, \ldots, X_{2n+1}) : X_i \prec H_i\}$; thus $Y \in \iota^{\prec}(H)$.
- If $j > i$, then $Y_i = G_i \prec H_i$; thus,

  $$Y \in \{(G_1, \ldots, G_{i-1}, X_i, X_{i+1}, \ldots, X_{2n+1}) : X_i \prec H_i\};$$

  consequently, $Y \in \iota^{\prec}(H)$.

As $G \in \iota^{\prec}(H)$ but $G \notin \iota^{\prec}(G)$, the above inclusions are proper. We now show that $\iota(G) = |\iota^{\prec}(G)|$. Note that

$$|\{(G_1, G_2, \ldots, G_{i-1}, X_i, X_{i+1}, \ldots X_{2n+1}) : X_i \prec G_i\}| = \sum_{X_i \prec G_i} |\{(G_1, G_2, \ldots, G_{i-1}, X_i, X_{i+1}, \ldots X_{2n+1})\}| = \sum_{X_i \prec G_i} n_{\mathfrak{q}}((G_1, \ldots, G_{i-1}, X_i), n).$$

Furthermore, as the sets in (16) are disjoint,

$$\begin{aligned} |\iota^{\prec}(G)| &= |\{(X_1, \ldots, X_{2n+1}) : X_1 \prec G_1\}| + |\{(G_1, X_2, \ldots, X_{2n+1}) : X_2 \prec G_2\}| + \cdots \\ &\quad + |\{(G_1, G_2, \ldots, G_{2n}, X_{2n+1}) : X_{2n+1} \prec G_{2n+1}\}| = \\ &\sum_{X_1 \prec G_1} n_{\mathfrak{q}}((X_1), n) + \sum_{X_2 \prec G_2} n_{\mathfrak{q}}((G_1\, X_2), n) + \ldots + \sum_{X_{2n+1} \prec G_{2n+1}} n_{\mathfrak{q}}((G_1\, G_2\, \ldots\, G_{2n}\, X_{2n+1}), n) = \\ &= \sum_{i=1}^{2n+1} \sum_{X_i \prec G_i} n_{\mathfrak{q}}((G_1, \ldots, G_{i-1}, X_i), n) = \iota(G). \end{aligned}$$

To conclude, observe that for any two distinct lines represented by matrices G and H in RREF we have either $G \in \iota^{\prec}(H)$ or $H \in \iota^{\prec}(G)$. The former yields $\iota^{\prec}(G) \subset \iota^{\prec}(H)$, whence $\iota(G) < \iota(H)$; the latter yields, in an entirely analogous way, $\iota(G) > \iota(H)$. In any case $G \neq H$ gives $\iota(G) \neq \iota(H)$ and ι is injective. □

Given an index $i \in \mathbb{I}$, the following theorem characterizes each column G_k, $1 \leq k \leq 2n+1$, of the representative matrix G_ℓ of a totally singular line ℓ as the maximum allowable vector of $\mathbb{F}_q^2$ for the given value of i and k. This theorem is crucial to invert the enumerative function ι.

Theorem 3.2. *Suppose $G = (G_1, \ldots, G_{2n+1})$ represents a totally singular line ℓ and let $\iota(\ell) = i$. Let also for any $k = 1, \ldots, 2n+1$,*

$$\theta(G_{\leq k}) := \sum_{X \prec G_k} n_{\mathfrak{q}}(S_k^X, n), \qquad i_k := i - \sum_{j=1}^{k-1} \theta(G_{\leq j}).$$

Then G_k is the maximum vector of $\mathbb{F}_q^2$ with respect to the order $\prec$ such that $\theta(G_{\leq k}) \leq i_k$.

Proof. Define

$$\Theta(G_{\leq k}) := \{(G_1, \ldots, G_{k-1}, X, \ldots) \in \iota^{\prec}(G) : X \prec G_k\},$$
$$\Lambda(G_{\leq k}) := \{(G_1, \ldots, G_{k-1}, Y, \ldots) \in \iota^{\prec}(G) : Y \preceq G_k\}.$$

Then,

$$\Lambda(G_{\leq 1}) = \{(Y, \ldots) \in \iota^{\prec}(G) : Y \preceq G_1\} = \iota^{\prec}(G).$$

We have

$$|\Theta(G_{\leq k})| = \sum_{X \prec G_k} n_{\mathfrak{q}}(S_k^X, n) = \theta(G_{\leq k}).$$

On the other hand, for $k > 1$ we can write

$$\Lambda(G_{\leq k}) = \iota^{\prec}(G) \setminus \big(\{(X_1, \ldots) : X_1 \prec G_1\} \cup \{(G_1, X_2, \ldots) : X_2 \prec G_2\} \cup \cdots$$
$$\cdots \cup \{(G_1, G_2, \ldots, G_{k-2}, X_{k-1}, \ldots) : X_{k-1} \prec G_{k-1}\}\big) = \iota^{\prec}(G) \setminus \bigcup_{j=1}^{k-1} \Theta(G_{\leq j}).$$

Thus,

$$|\Lambda(G_{\leq k})| = \iota(G) - \sum_{j=1}^{k-1} \theta(G_{\leq j}) = i_k.$$

We distinguish two cases:

- $k = 1$. By way of contradiction, suppose G_1 is not maximum and $\theta(G_{\leq 1}) \leq i_1 = i$. Then, there is an element $G_1' \in \mathbb{F}_q^2$, with $G_1 \prec G_1'$ and $\theta(G_{\leq 1}') \leq i$. By construction, $\Lambda(G_{\leq 1}) \subset \Theta(G_{\leq 1}')$. Observe that $G \in \Theta(G_{\leq 1}')$ but $G \notin \Lambda(G_{\leq 1})$. Thus, the inclusion is proper. Moving to the cardinalities we have

  $$i = |\Lambda(G_{\leq 1})| < |\Theta(G_{\leq 1}')| = \theta(G_{\leq 1}') \leq i,$$

  a contradiction.

- $k > 1$. Suppose that the thesis holds for $j \leq k$ but not for $j = k + 1$, i.e. all G_j for $j \leq k$ are maximum such that $\theta(G_{\leq j}) \leq i_j$ and G_{k+1} is not the maximum element such that $\theta(G_{\leq k+1}) \leq i_{k+1}$. Then, as before, there is a G_{k+1}' such that $G_{k+1} \prec G_{k+1}'$ with $\theta(G_{\leq k+1}') \leq i_{k+1}$. For any $Y \preceq G_{k+1}$ we have $Y \prec G_{k+1}'$; thus, the following holds

  $$\Lambda(G_{\leq k+1}) = \{(G_1, \ldots, G_k, Y, \ldots) \in \iota^{\prec}(G) : Y \preceq G_{k+1}\} \subset$$
  $$\subset \{(G_1, \ldots, G_k, X, \ldots) \in \iota^{\prec}(G) : X \prec G_{k+1}'\} = \Theta(G_{\leq k+1}').$$

  Furthermore, as $G \in \Theta(G_{\leq k+1}')$ but $G \notin \Lambda(G_{\leq k+1})$, the above inclusion is proper. Thus,

  $$i_{k+1} = |\Lambda(G_{\leq k+1})| < |\Theta(G_{\leq k+1}')| = \theta(G_{\leq k+1}') \leq i_{k+1},$$

  a contradiction.

□

In Table 6 we show in detail the procedure arising from Theorem 3.2 to efficiently invert the function ι. Observe that the check $n_{\mathfrak{q}}(S_k^Y, n) > 0$ is necessary, as each column G_k must be allowable and columns which are allowable in a given position k may not be allowable in position $k - 1$ or vice-versa.

Table 6: Inverse of ι

Require: $i \in \{0, \dots, N-1\}$
  $i_1 \leftarrow 1$
  for $k = 1, \dots, 2n+1$ **do**
    $M \leftarrow \{Y \colon \sum_{X \prec Y} n_{\mathfrak{q}}(S_k^X, n) \leq i_k \text{ and } n_{\mathfrak{q}}(S_k^Y, n) > 0\}$
    $G_k \leftarrow \max M$
    $\theta(G_{\leq k}) \leftarrow \sum_{X \prec G_k} n_{\mathfrak{q}}(S_k^X, n)$;
    $i_{k+1} \leftarrow i_k - \theta(G_{\leq k})$;
  end for
  return $G = (G_1, \dots, G_k, \dots, G_{2n+1})$

3.1. Complexity

We now estimate the actual cost of the enumerative encoding presented in this section. In the orthogonal case, to evaluate ι we need to compute at most $q^2 - 1$ values of $n_{\mathfrak{q}}(S_j^X, n)$ for any $j = 1, \dots, 2n+1$ as X varies in $\mathbb{F}_q^2$. So, the overall complexity turns out to be $O(q^2 n^3)$. Conversely, given an index $i \in \mathbb{I}$, recovering the corresponding line $\ell = \iota^{-1}(i)$ requires to test at most $q^2 - 1$ vectors $X \in \mathbb{F}_q^2$ for each column of G; thus, the cost is once more $O(q^2 n^3)$. In the symplectic case, the same arguments give a complexity of $O(q^2 n^2)$ for enumerative enconding.

The computational complexity of the enumerative algorithm for the orthogonal and symplectic Grassmannians are summarized in Theorem 1.6.

4. Application to polar Grassmann codes

We now apply the enumeration techniques discussed in the previous sections to efficiently implement the polar Grassmann codes $\mathcal{P}_{n,2}$ and $\mathcal{W}_{n,2}$. We refer to Section 1.2 for the definition and some basics about these codes.

We shall focus the discussion on the case of orthogonal polar Grassmann codes, while we will only point out the adjustements to be made for the symplectic case $\mathcal{W}_{n,2}$, as the arguments in the two cases are very similar.

4.1. Encoding

As in Section 2.2, let V be a vector space of dimension $2n+1$ over $\mathbb{F}_q$ and fix a basis $B := (e_1, \dots, e_{2n+1})$ of V.

It is well known that the dual $(\bigwedge^k V)^*$ of the vector space $\bigwedge^k V$ is isomorphic to $\bigwedge^{2n+1-k} V$. We recall the following universal property of the k^{th}-exterior power of a vector space.

Theorem 4.1 ([22, Theorem 14.23]). *Let V, U be two vector spaces over the same field. A map $f : V^k \longrightarrow U$ is alternating k–linear if and only if there is a linear map $\zeta : \bigwedge^k V \longrightarrow U$ with $\zeta(v_1 \wedge v_2 \wedge \cdots \wedge v_k) = f(v_1, v_2, \dots, v_k)$. The map ζ is uniquely determined.*

By Theorem 4.1, for $k = 2$, any linear functional ζ on $\bigwedge^2 V$ corresponds to a bilinear alternating form on V; hence it can be represented by an antisymmetric $(2n+1) \times (2n+1)$-matrix $M = (\mathfrak{m}_{ij})_{i,j=1}^{2n+1}$ whose entries are $\mathfrak{m}_{ij} = \zeta(e_i \wedge e_j)$. With a slight abuse of notation, for any $\ell \in \Delta_{2,n}$ write $\zeta(\ell) := \zeta(G_1^\ell \wedge G_2^\ell)$, where G_1^ℓ and G_2^ℓ are the two rows of the representative matrix G_ℓ of ℓ in RREF. Clearly, we also have $\zeta(\ell) = G_1^\ell M {G_2^\ell}^T$. Let $\mathcal{P}_{n,2}$ be the line orthogonal Grassman $[N, K, d]$-code as in Theorem 1.3.

Definition 4.1. Let $\psi\colon \mathbb{F}_q^K \to \mathcal{P}_{n,2}$ be the function mapping any message $(m_i)_{i=1}^K \in \mathbb{F}_q^K$ to the codeword $(c_{i+1})_{i=0}^{N-1} \in \mathcal{P}_{n,2}$ where

$$c_{i+1} := \zeta(\iota^{-1}(i)) = G_1^{(i)} M G_2^{(i)T},$$

the function ι is defined in (15), $G_1^{(i)}$ and $G_2^{(i)}$ are the rows of the representative matrix G_{ℓ_i} in RREF of the line $\ell_i := \iota^{-1}(i)$ and ζ is the bilinear alternating form with matrix $M := M_0 - M_0^T$ with respect to B, with

- for q odd:

$$M_0 = \begin{pmatrix} 0 & m_1 & m_2 & \dots & m_{2n} \\ 0 & 0 & m_{2n+1} & \dots & m_{4n-1} \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & m_{n(2n+1)} \\ 0 & \dots & \dots & 0 & 0 \end{pmatrix}$$

  and

- for q even:

$$M_0 = \begin{pmatrix} 0 & m_1 & m_2 & & \dots & m_{2n} \\ 0 & 0 & m_{2n+1} & & \dots & m_{4n-1} \\ \vdots & & \ddots & & \ddots & \vdots \\ 0 & 0 & \dots & 0 & m_{n(2n+1)-2} & m_{n(2n+1)-1} \\ 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & \dots & \dots & 0 & 0 & 0 \end{pmatrix}.$$

Clearly, ψ is a linear function.

Theorem 4.2. *The function ψ introduced in Definition 4.1 is an encoding for $\mathcal{P}_{n,2}$.*

Proof. We need to prove that ψ is injective. We first point out that, by Definition 4.1, a codeword $\mathbf{c} \in \mathcal{P}_{n,2}$ is associated with a message $\mathbf{m}$ if the positions $c_{i+1},\ 0 \le i \le N-1$, of $\mathbf{c}$ are the values assumed on the lines of $\Delta_{n,2}$ by the linear functional $\zeta \in (\bigwedge^2 V)^*$ defined by $\mathbf{m}$. In order to make more explicit the link between codewords $\mathbf{c}$ and linear functionals ζ, we shall write $\mathbf{c}_\zeta$.

Suppose that q is odd. Then $\mathcal{P}_{n,2} = \bigwedge^2 V$ (see [6]). A codeword $\mathbf{c}_\zeta$ is null if and only if the functional ζ is identically null on $\bigwedge^2 V$. Indeed, since $\langle \varepsilon_2(\Delta_{n,2}) \rangle = \bigwedge^2 V$, there exist some positions $i_1+1, \dots, i_{n(2n+1)}+1$ of $\mathbf{c}_\zeta$ such that $B' := (\iota^{-1}(i_j))_{j=1}^{n(2n+1)}$ is a basis of $\bigwedge^2 V$. If $\mathbf{c}_\zeta = \mathbf{0}$, then ζ is zero on all the elements of B'. Hence, by linearity, ζ is the null functional. This proves that ψ is injective.

Suppose that q is even. Now $\langle \varepsilon_2(\Delta_{n,2}) \rangle$ is a hyperplane W of $\bigwedge^2 V$ (see [6]). By Definition 4.1, any non-null codeword $\mathbf{c}_\zeta$ is associated with a message $\mathbf{m} \in \mathbb{F}_q^K$ which is in correspondence with a linear functional $\zeta \in (\bigwedge^2 V)^*$ which is not identically null on W. By [7], $W = \ker \zeta_0$ with

$$\zeta_0\colon \bigwedge^2 V \to \mathbb{F}_q, \quad \zeta_0((u_{ij})_{1 \le i < j \le 2n+1}) := u_{23} + u_{45} + \dots + u_{2n,2n+1}$$

where u_{ij} are the Plücker coordinates of vectors in $\bigwedge^2 V$ with respect to the basis $(e_i \wedge e_j)_{1 \le i < j \le 2n+1}$.

Given any message $\mathbf{m} = (m_1, \dots, m_{n(2n+1)-1}) \in \mathbb{F}_q^K$, by Definition 4.1, the antisymmetric matrix M defined by $\mathbf{m}$ has $\mathfrak{m}_{2n,2n+1} = 0$.

Let $\zeta \in (\bigwedge^2 V)^*$ be the functional associated with $\mathbf{m}$ by means of the bilinear alternating form defined by M. Observe that the functional $\zeta|_W$ induced by the restriction of ζ to W is null if and only if ζ is proportional to ζ_0. By construction, we have $\zeta(e_{2n} \wedge e_{2n+1}) = 0$. We are now ready to prove that the function $\psi : \mathbb{F}_q^K \to \mathcal{P}_{n,2}$ is injective. Indeed, if $\mathbf{m}_1$ and $\mathbf{m}_2$ are messages inducing two forms ζ_1 and ζ_2 and such that $\psi(\mathbf{m}_1) = \psi(\mathbf{m}_2)$, then $\zeta' = \zeta_1 - \zeta_2$ is null on W. So, ζ' must be proportional to ζ_0. However, $(\zeta_1 - \zeta_2)(e_{2n} \wedge e_{2n+1}) = 0$, while $\zeta_0(e_{2n} \wedge e_{2n+1}) = 1$. So, the only possibility is that $\zeta_1 - \zeta_2$ is the null functional on $\bigwedge^2 V$, i.e. $\mathbf{m}_1 = \mathbf{m}_2$. □

A straightforward counting argument provides the following relationship between the components of $\mathbf{m}$ and the entries $\mathfrak{m}_{ij}$ of M with $1 \leq i < j \leq 2n+1$:

$$\mathfrak{m}_{ij} = m_{2n(i-1)+j-\frac{i^2-i}{2}-1}. \tag{17}$$

So, we can directly determine each component of $\mathbf{c}$ using just $\mathbf{m}$ without having to resort to the generator matrix of the code.

The case of symplectic Grassmann codes $\mathcal{W}_{n,2}$ is entirely analogous to what we proposed for $\mathcal{P}_{n,2}$ for q even. Definition 4.1 remains the same if we write $\mathcal{W}_{n,2}$ in place of $\mathcal{P}_{n,2}$, $\binom{2n}{k} - 1$ in place of $\binom{2n+1}{k} - 1$ for K and we consider q arbitrary. The only further difference in Theorem 4.2 is that $\langle \varepsilon_k(\overline{\Delta}_{n,2}) \rangle = \ker(\zeta_0)$ with

$$\zeta_0 \colon \bigwedge^2 V \to \mathbb{F}_q, \quad \zeta_0((u_{ij})_{1 \leq i < j \leq 2n+1}) := u_{12} + u_{34} + \cdots + u_{2n-1,2n},$$

where u_{ij} are the Plücker coordinates of vectors in $\bigwedge^2 V$.

4.2. Decoding

We address now the problem of recovering the original message $\mathbf{m}$ once a codeword $\mathbf{c}$ has been given. Here we shall assume that no error occurred; how to perform error correction shall be discussed in the next section. Clearly, by Section 4.1, recovering $\mathbf{m}$ is equivalent to reconstructing the antisymmetric matrix M associated with $\mathbf{m}$.

In general, polar Grassmann codes are not systematic, nor there are entries in $\mathbf{c}$ corresponding exactly to the values $\mathfrak{m}_{ij}$ in M. None the less, it is possible to provide a list of lines yielding information positions in $\mathbf{c}$ such that the values $\mathfrak{m}_{ij}$ can be easily determined.

Theorem 4.3. *Let $\mathbf{c}$ be a codeword of $\mathcal{P}_{n,2}$ and $M = (\mathfrak{m}_{ij})_{1 \leq i,j \leq 2n+1}$ be the antisymmetric matrix associated with the message $\mathbf{m}$ mapped to $\mathbf{c}$ using the encoding ψ. Suppose that the pair (i,j) with $1 \leq i < j \leq 2n+1$ is in one of the following types:*

Type I: $i \geq 2$ even and $j \geq i+2$ or i odd and $j \geq i+1$;

Type II: $i \geq 2$ even and $j = i+1$;

Type III: $i = 1$ and $j > i$.

Then the following holds:

- *If (i,j) is of Type I then $\mathfrak{m}_{ij} = c_{\iota(\ell_{i,j})+1}$ where $\ell_{i,j} := \langle e_i, e_j \rangle$.*
- *If (i,j) is of Type II then $\mathfrak{m}_{ij}$ can be obtained by solving a system of 2 linear equations in 2 unknowns for q odd and a single linear equation for q even.*
- *If (i,j) is of Type III then $\mathfrak{m}_{ij}$ can be obtained by solving a linear equation.*

Proof. If (i,j) is of Type I, the thesis is straightforward. If (i,j) is of Type II, we distinguish two cases according to whether q is odd or even.

Suppose q odd. Consider two lines $\ell^1 := \langle e_i + e_{i+3}, e_{i+1} - e_{i+2}\rangle$ and $\ell^2 := \langle e_i - e_{i+3}, e_{i+1} + e_{i+2}\rangle$ and call $c_x := c_{\iota(\ell^1)+1}$, $c_y := c_{\iota(\ell^2)+1}$ the corresponding entries of $\mathbf{c}$. Then we have

$$\begin{cases} \mathfrak{m}_{i,i+1} - \mathfrak{m}_{i,i+2} - \mathfrak{m}_{i+1,i+3} + \mathfrak{m}_{i+2,i+3} = c_x \\ \mathfrak{m}_{i,i+1} + \mathfrak{m}_{i,i+2} + \mathfrak{m}_{i+1,i+3} - \mathfrak{m}_{i+2,i+3} = c_y \end{cases}.$$

The entries $\mathfrak{m}_{i+1,i+3}$ and $\mathfrak{m}_{i,i+2}$ correspond to indexes of Type I; thus they can be read off $\mathbf{c}$ directly. The remaining unknowns $\mathfrak{m}_{i,i+1}$ and $\mathfrak{m}_{i+2,i+3}$ can now be recovered by solving a system in two unknowns. Observe that this operation has fixed complexity $O(1)$.

Suppose q even. Recall that, in this case, $\mathfrak{m}_{2n,2n+1} = 0$. Consider the line $\ell := \langle e_i + e_{2n}, e_{i+1} + e_{2n+1}\rangle$ and let $c_x = c_{\iota(\ell)+1}$. We get

$$\mathfrak{m}_{i,i+1} + \mathfrak{m}_{i,2n+1} + \mathfrak{m}_{i+1,2n} = c_x.$$

As $\mathfrak{m}_{i,2n+1}$ and $\mathfrak{m}_{i+1,2n}$ correspond to indexes of Type I, this gives the value of $\mathfrak{m}_{i,i+1}$.

Suppose $(i,j) = (1,j)$ is of Type III. If $j > 3$, we consider the line $\ell = \langle e_1 - e_2 + e_3, e_j\rangle$. A straightforward computation shows that the corresponding entry $c_z := c_{\iota(\ell)+1}$ is

$$\mathfrak{m}_{1j} - \mathfrak{m}_{2j} + \mathfrak{m}_{3j} = c_z$$

and both $(2,j)$ and $(3,j)$ are of Type I; thus we just have to solve this equation. As for the remaining coefficients $\mathfrak{m}_{12}$ and $\mathfrak{m}_{13}$, we use the entries corresponding to $\ell^{12} = \langle e_1 - e_4 + e_5, e_2\rangle$ and $\ell^{13} = \langle e_1 - e_4 + e_5, e_3\rangle$. □

Theorem 4.3 shows that it is possible to extract any component of the message $\mathbf{m}$ from a codeword $\mathbf{c}$ with complexity $O(1)$. As such, the complexity to recover the whole of $\mathbf{m}$ is $O(n^2)$.

In the symplectic case, the same arguments as in Theorem 4.3 lead to the following.

Theorem 4.4. *Let $\mathbf{c}$ be a codeword of $\mathcal{W}_{n,2}$ and $M = (\mathfrak{m}_{ij})_{1\le i,j\le 2n+1}$ be the antisymmetric matrix associated with the message $\mathbf{m}$ mapped to $\mathbf{c}$ using the encoding ψ. Suppose that the pair (i,j) with $1 \le i < j \le 2n+1$ is in one of the following types:*

Type I: $i \ge 1$ odd and $j \ge i+2$ or i even and $j \ge i+1$;

Type II: $i \ge 1$ odd and $j = i+1$;

Then the following holds:

- *If (i,j) is of Type I then $\mathfrak{m}_{ij} = c_{\iota(\ell_{i,j})+1}$ where $\ell_{i,j} := \langle e_i, e_j\rangle$.*
- *If (i,j) is of Type II then $\mathfrak{m}_{ij}$ can be obtained by solving one linear equation.*

4.3. Error correction

Locally decodable codes have received much attention in recent years; see [28, 29] for some surveys. In general, a code is *locally decodable* if it is able to recover a given component m_i of a message $\mathbf{m}$ with probability larger than $1/2$ querying just a fixed number of components r_j of the received vector $\mathbf{r}$ — this, clearly, under the assumption that not too many errors have occurred; see [16].

In this section we shall introduce an algorithm to reconstruct a correct information position using only some local information.

Let $\mathbf{r} = (r_{i+1})_{i=0}^{N-1} \in \mathbb{F}_q^N$ be a received vector; by the arguments in Section 4.1, $\mathbf{r}$ is a codeword $\mathbf{c}$ if and only if there exists $\zeta \in (\bigwedge^2 V)^*$, such that $r_{i+1} = \zeta(G_1^\ell \wedge G_2^\ell)$ for any $0 \leq i \leq N-1$ where $\ell = \langle G_1^\ell, G_2^\ell \rangle$ and $\ell = \iota^{-1}(i)$. As in § 4.1, we shall write $r_{i+1} := \zeta(\ell)$.

Fix now a position $i+1$ and consider the totally singular line $\ell = \iota^{-1}(i)$. Let

$$\Sigma_\ell := \{\pi : \ell \subseteq \pi \subseteq \mathcal{Q}, \dim \pi = 3\}$$

be the set of all totally singular planes of $\mathcal{Q}$ containing ℓ (we remind that we have always used vector dimension throughout the paper, but we adopt projective terminology when speaking of geometric objects). The restriction ζ_π of ζ to each plane π determines by Theorem 4.1 a degenerate alternating bilinear form which we shall still denote by the same symbol. Clearly, in absence of errors, all the forms ζ_π, as π varies in Σ_ℓ, must agree on ℓ. The overall number of totally singular planes containing a given fixed line ℓ is $|\Sigma_\ell| = \frac{q^{2n-4}-1}{q-1}$; this is also the total number of different forms ζ_π we can consider.

Let $0 < \varepsilon \leq |\Sigma_\ell|$ be a parameter denoting the number of planes of Σ_ℓ we want to use and consider the following error correction strategy:

1. Choose $\varepsilon \leq |\Sigma_\ell|$ planes at random in Σ_ℓ.
2. For each of the chosen planes, say π, let p, q, s be three distinct lines of π different from ℓ forming a triangle and recover the alternating bilinear form ϕ^π such that $\phi^\pi(p) = r_{\iota(p)+1}$, $\phi^\pi(q) = r_{\iota(q)+1}$, $\phi^\pi(s) = r_{\iota(s)+1}$. This corresponds to solving a linear system of 3 equations in 3 unknowns.
3. If all forms ϕ^π are such that $\phi^\pi(\ell) = r_{\iota(\ell)+1}$, then we claim that the value $r_{\iota(\ell)+1}$ is correct and set $c_{\iota(\ell)+1} = r_{\iota(\ell)+1}$; otherwise, take $c_{\iota(\ell)+1}$ as the value assumed by the majority of the forms ϕ^π, as π varies in Σ_ℓ, when evaluated on ℓ.

The same correction strategy can be implemented for polar symplectic Grassmann codes, by considering totally isotropic planes instead of totally singular ones.

Acknowledgments

This research was performed within the activity of GNSAGA of INdAM (Italy) whose support both authors acknowledge.

[1] P. Beelen, S. R. Ghorpade, and T. Høholdt. Duals of affine Grassmann codes and their relatives. *IEEE Trans. Inform. Theory*, 58(6):3843–3855, 2012.

[2] I. Cardinali and L. Giuzzi. Codes and caps from orthogonal Grassmannians. *Finite Fields Appl.*, 24:148–169, 2013.

[3] I. Cardinali and L. Giuzzi. Minimum distance of symplectic Grassmann codes. *Linear Algebra Appl.*, 488:124–134, 2016.

[4] I. Cardinali, L. Giuzzi, K. V. Kaipa, and A. Pasini. Line polar Grassmann codes of orthogonal type. *J. Pure Appl. Algebra*, 220(5):1924–1934, 2016.

[5] I. Cardinali, L. Giuzzi, Minimum distance of Line Orthogonal Grassmann codes in even characteristic *preprint*, arXiv:1605.09333.

[6] I. Cardinali and A. Pasini. Grassmann and Weyl embeddings of orthogonal Grassmannians. *J. Algebraic Combin.*, 38(4):863–888, 2013.

[7] I. Cardinali and A. Pasini. Embeddings of line-Grassmannians of polar spaces in Grassmann varieties. In *Groups of exceptional type, Coxeter groups and related geometries*, volume 82 of *Springer Proc. Math. Stat.*, pages 75–109. Springer, New Delhi, 2014.

[8] T. M. Cover. Enumerative source encoding. *IEEE Trans. Information Theory*, IT-19(1):73–77, 1973.

[9] B. De Bruyn. Some subspaces of the kth exterior power of a symplectic vector space. *Linear Algebra Appl.*, 430(11-12):3095–3104, 2009.

[10] S. R. Ghorpade and K. V. Kaipa. Automorphism groups of Grassmann codes. *Finite Fields Appl.*, 23:80–102, 2013.

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

[12] S. R. Ghorpade, A. R. Patil, and H. K. Pillai. Decomposable subspaces, linear sections of Grassmann varieties, and higher weights of Grassmann codes. *Finite Fields Appl.*, 15(1):54–68, 2009.

[13] W. V. D. Hodge and D. Pedoe. *Methods of algebraic geometry. Vol. I.* Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1994. Book I: Algebraic preliminaries, Book II: Projective space, Reprint of the 1947 original.

[14] W. V. D. Hodge and D. Pedoe. *Methods of algebraic geometry. Vol. II.* Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1994. Book III: General theory of algebraic varieties in projective space, Book IV: Quadrics and Grassmann varieties, Reprint of the 1952 original.

[15] K. V. Kaipa and H. K. Pillai. Weight spectrum of codes associated with the Grassmannian $G(3, 7)$. *IEEE Trans. Inform. Theory*, 59(2):986–993, 2013.

[16] J. Katz and L. Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 80–86 (electronic). ACM, New York, 2000.

[17] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.

[18] Y. Medvedeva. Fast enumeration for grassmannian space. In *Problems of Redundancy in Information and Control Systems (RED), 2012 XIII International Symposium on*, pages 48–52. IEEE, 2012.

[19] D. Y. Nogin. Codes associated to Grassmannians. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pages 145–154. de Gruyter, Berlin, 1996.

[20] F. Piñero. *An algebraic approach to graph codes.* PhD thesis, Technical University of Denmark, 2014.

[21] A. A. Premet and I. D. Suprunenko. The Weyl modules and the irreducible representations of the symplectic group with the fundamental highest weights. *Comm. Algebra*, 11(12):1309–1342, 1983.

[22] S. Roman. *Advanced linear algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2008.

[23] C. Ryan. An application of Grassmannian varieties to coding theory. *Congr. Numer.*, 57:257–271, 1987. Sixteenth Manitoba conference on numerical mathematics and computing (Winnipeg, Man., 1986).

[24] C. T. Ryan. Projective codes based on Grassmann varieties. *Congr. Numer.*, 57:273–279, 1987. Sixteenth Manitoba conference on numerical mathematics and computing (Winnipeg, Man., 1986).

[25] C. T. Ryan and K. M. Ryan. The minimum weight of the Grassmann codes $C(k, n)$. *Discrete Appl. Math.*, 28(2):149–156, 1990.

[26] N. Silberstein and T. Etzion. Enumerative coding for Grassmannian space. *IEEE Trans. Inform. Theory*, 57(1):365–374, 2011.

[27] M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[28] S. Yekhanin. *Locally Decodable Codes and Private Information Retrival Schemes*. Information Security and Cryptography Texts and Monographs. Springer, New York, 2010.

[29] S. Yekhanin. Locally decodable codes: a brief survey. In *Coding and cryptology*, volume 6639 of *Lecture Notes in Comput. Sci.*, pages 273–282. Springer, Heidelberg, 2011.