Implementing Line-Hermitian Grassmann codes

Ilaria Cardinali and Luca Giuzzi

February 5, 2019

Abstract

In [6] we introduced line Hermitian Grassmann codes and determined their parameters. The aim of this paper is to present (in the spirit of [4]) an algorithm for the point enumerator of a line Hermitian Grassmannian which can be usefully applied to get efficient encoders, decoders and error correction algorithms for the aforementioned codes.

Keywords: Hermitian variety, Polar Grassmannian, Projective Code, Point Enumerator.
MSC(2010): 14M15, 94B27, 94B05.

1 Introduction

Let V be a vector space of dimension K over a (finite) field $\mathbb{K}$ and suppose Ω to be a *projective system* of $\mathrm{PG}(V)$ of order N, that is a set of N distinct points of $\mathrm{PG}(V)$ such that $\dim\langle\Omega\rangle = \dim(V)$. An *enumerator* for Ω is a bijection $\iota : \Omega \to \{0, 1, \dots, N-1\}$ which can be efficiently computed and inverted (i.e. with complexity which is $O(\log|\Omega|)$ or less).

Enumerators are interesting because of their relevance to applications, as they provide an efficient way to represent and access the elements of a (ordered) list, without requiring a large amount of storage.

For example, take Ω as the point-set of a k-Grassmann variety, hence the elements in Ω are the k-dimensional vector subspaces of V. Then, a (point) enumerator for Ω is a bijective function that maps any k-dimensional subspace to an integer $i \in \{0, 1, \dots, |\Omega| - 1\}$ in a way that can be computed and inverted with efficiency.

This plays a key role in the implementation of Grassmann codes (see [14]), since it makes possible to encode messages without requiring to explicitly write the full generator matrix of the code, a process which would be very expensive both computationally and in terms of storage; see also Section 6.

In the present paper we shall be concerned with point enumerators of line Hermitian Grassmannians (see [6]). In this way, we continue a project started in [4] where we introduced point enumerators for line polar Grassmannians of orthogonal [7, 5] and symplectic type [3].

Before stating our main results, we shall recall the definition of Hermitian Grassmannians and set the notation in Section 1.1; next, in Section 1.2, we shall provide some basics about polar Grassmann codes. The organization of the paper and the main results are outlined in Section 1.3.

1.1 Hermitian Grassmannians and their embeddings

Assume $\mathbb{K} = \mathbb{F}_{q^2}$ to be a finite field of order q^2 and let $V := V(m, \mathbb{K})$ be an m-dimensional vector space over $\mathbb{K}$ and $k \in \{1, \dots, m-1\}$. Let $\mathcal{G}_{m,k}$ be the k-Grassmannian of the projective space $\mathrm{PG}(V)$, that is the point–line geometry whose points are the k-dimensional subspaces of V and whose lines are the sets

$$\ell_{W,T} := \{X : W \leq X \leq T, \dim X = k\}$$

with $\dim W = k-1$ and $\dim T = k+1$.

Let $e_k : \mathcal{G}_{m,k} \to \mathrm{PG}(\bigwedge^k V)$ be the Plücker (or Grassmann) embedding of $\mathcal{G}_{m,k}$, which maps any arbitrary k–dimensional subspace $X = \langle v_1, v_2, \dots, v_k \rangle$ of V to the point $e_k(X) := [v_1 \wedge v_2 \wedge \cdots \wedge v_k]$ of $\mathrm{PG}(\bigwedge^k V)$. Note that lines of $\mathcal{G}_{m,k}$ are mapped onto (projective) lines of $\mathrm{PG}(\bigwedge^k V)$. The dimension $\dim(e_k)$ of the embedding e_k is defined as the vector dimension of the subspace spanned by its image. It is well known that $\dim(e_k) = \binom{m}{k}$.

The image $e_k(\mathcal{G}_{m,k})$ of the Plücker embedding is a projective variety of $\mathrm{PG}(\bigwedge^k V)$, called *Grassmann variety* and denoted by $\mathbb{G}(m, k)$.

Suppose now that V is equipped with a non-degenerate Hermitian form η of Witt index n (hence either $m = 2n+1$ or $m = 2n$).

The *Hermitian k-Grassmannian* induced by η is defined for $k = 1, \dots, n$ as the geometry having as points the totally η–isotropic subspaces of V of dimension k and as lines

- for $k < n$, the sets of the form

  $$\ell_{W,T} := \{X : W \leq X \leq T, \dim X = k\}$$

  with T totally η–isotropic and $\dim W = k-1$, $\dim T = k+1$.

- for $k = n$, the sets of the form

  $$\ell_W := \{X : W \leq X, \dim X = n, X \text{ totally } \eta\text{–isotropic}\}$$

  with $\dim W = n-1$.

We will denote a Hermitian k-Grassmannian either by the symbol $\mathcal{H}_{n,k}$ when we do not want to mention the parity of m or by the symbols $\mathcal{H}_{n,k}^{even}$ (for $m = 2n$) respectively $\mathcal{H}_{n,k}^{odd}$ (for $m = 2n + 1$) when the parity of m plays a significant role.

Clearly, for $k = 1, \dots, n$, the point-set of $\mathcal{H}_{n,k}$ is always a subset of that of $\mathcal{G}_{m,k}$. If $k = 1$, $\mathcal{H}_{n,1}$ (also denoted $\mathcal{H}_n$ or $\mathcal{H}_m$) stands for a Hermitian polar space of rank n and if $k = n$, $\mathcal{H}_{n,n}$ is usually called *Hermitian dual polar space of rank n*. Let $\varepsilon_{n,k} := e_k|_{\mathcal{H}_{n,k}}$ be the restriction of the Plücker embedding e_k of $\mathcal{G}_{m,k}$ to the Hermitian k-Grassmannian $\mathcal{H}_{n,k}$. The map $\varepsilon_{n,k}$ is an embedding of $\mathcal{H}_{n,k}$ called *Plücker (or Grassmann) embedding* of $\mathcal{H}_{n,k}$ in $\mathrm{PG}(\bigwedge^k V)$; its dimension has been proved to be $\dim(\varepsilon_{n,k}) = \binom{\dim(V)}{k}$ for $\dim(V)$ even and k arbitrary by Blok and Cooperstein [1] and for $\dim(V)$ arbitrary and $k = 2$ by Cardinali and Pasini [8]. Consider now the following projective system of $\mathrm{PG}(\bigwedge^k V)$:

$$\mathbb{H}_{n,k} := \varepsilon_{n,k}(\mathcal{H}_{n,k}) = \{\varepsilon_{n,k}(X) \colon X \text{ point of } \mathcal{H}_{n,k}\} \subset \mathrm{PG}(\bigwedge^k V). \tag{1}$$

Note that if $k = 2$ and $n > 2$ then $\varepsilon_{n,2}$ maps lines of $\mathcal{H}_{n,2}$ onto projective lines of $\mathrm{PG}(\bigwedge^2 V)$, independently of the parity of $\dim(V)$, i.e. the embedding is *projective*. Otherwise, if $n = k = 2$ and $m = \dim(V) = 5$ then the lines of $\mathcal{H}_{2,2}^{odd}$ are mapped onto Hermitian curves, while if $m = \dim(V) = 4$ then lines of $\mathcal{H}_{2,2}^{even}$ are mapped onto Baer sublines of $\mathrm{PG}(\bigwedge^2 V)$. In the latter case $\mathbb{H}_{2,2}^{even} \cong Q^-(5, q)$ is contained in a proper subgeometry, defined over the subfield $\mathbb{F}_q$, of $\mathrm{PG}(\bigwedge^2 V)$.

1.2 Line Hermitian Grassmann codes

Given a projective system Ω of $\mathrm{PG}(V)$ of order N, where $\dim(V) = K$, we can construct a $[N, K]$-linear code $\mathcal{C}(\Omega)$ associated to Ω as a code whose generator matrix is the $(K \times N)$-matrix whose columns are vector representatives of the points of Ω; see [18]. There is a well-known relationship between the maximum number of points of Ω lying in a hyperplane of $\mathrm{PG}(V)$ and the minimum Hamming distance $d_{\min}$ of $\mathcal{C}(\Omega)$, namely

$$d_{\min} = N - \max_{\substack{\Pi \leq \mathrm{PG}(V) \\ \mathrm{codim}(\Pi) = 1}} |\Pi \cap \Omega| .$$

The case in which Ω is the point-set of a Grassmann variety $\mathbb{G}(m, k)$ has been extensively studied; see e.g. [15, 16, 17, 14, 11, 10, 12]. In this case the associated codes $\mathcal{C}(\Omega)$ are called *Grassman codes.*

In a series of papers we have investigated codes arising from a proper subvariety Ω of $\mathbb{G}(m, k)$; more precisely when Ω is the image under the Plücker embedding of a polar line Grassmannian; see [2, 7, 5] for the orthogonal case and [3] for the symplectic case. Following the same approach of [2], we defined in [6] *Hermitian Grassmann codes* as those projective codes arising from the Plücker embedding of a Hermitian Grassmannian (see Equation (1)) and we determined their minimum distance, also characterizing the words of minimum weight.

In particular, for line Hermitian Grassmann codes, i.e. taking $k = 2$, we proved in [6] the following.

Theorem 1. *A line Hermitian Grassmann code defined by a non–degenerate Hermitian form on a vector space $V(m, q^2)$ is a $[N, K, d_{\min}]$-linear code where*

$$N = \frac{(q^m + (-1)^{m-1})(q^{m-1} - (-1)^{m-1})(q^{m-2} + (-1)^{m-3})(q^{m-3} - (-1)^{m-3})}{(q^2-1)^2(q^2+1)};$$

$$K = \binom{m}{2};$$

$$d_{\min} = \begin{cases} q^{4m-12} - q^{2m-6} & \textit{if } m = 4, 6\ . \\ q^{4m-12} & \textit{if } m \geq 8 \textit{ is even.} \\ q^{4m-12} - q^{3m-9} & \textit{if } m \textit{ is odd.} \end{cases}$$

1.3 Organization of the paper and Main Results

In Section 2 we recall the notion of *prefix enumeration* and provide counting algorithms for the points of $\mathcal{H}_{n,2}$. In Sections 3 and 4 we compute the number of totally η-singular lines of V spanned by vectors with a prescribed prefix. The complexity of the prefix enumerators is discussed in Section 5, where we prove our main result.

Main Theorem

(i) The computational complexity for the number of points of a line Hermitian Grassmannian of $V(m, q^2)$, whose representation begins with a prescribed prefix, is $O(m^2)$.

(ii) The computational complexity for a point enumerator of a line Hermitian Grassmannian of $V(m, q^2)$ is $O(q^4m^3)$.

Section 6 is dedicated to applications of the scheme introduced in Sections 3 and 4 to line Hermitian Grassmann codes. We also propose some encoding/decoding and error correction strategies which act locally on the components of the codewords.

2 Preliminaries

2.1 Point enumerator: notation and basics

Let $\mathfrak{A}$ be an alphabet equipped with a total order relation $\prec$ and let $\mathcal{O} \subseteq \mathfrak{A}^m$ be a set of m-uples with entries in $\mathfrak{A}$. For any $\omega \in \mathcal{O}$ and $t \leq m$ a non-negative integer, we define the *prefix of length* t or t*-prefix* of ω as the t-uple of the first t-entries of ω. If $\alpha = (\alpha_1, \dots, \alpha_t) \in \mathfrak{A}^t$ and $\beta = (\beta_1, \dots, \beta_s) \in \mathfrak{A}^s$, we shall write $\alpha|\beta$ to refer to the $(t+s)$-uple $(\alpha, \beta) = (\alpha_1, \dots, \alpha_t, \beta_1, \dots, \beta_s) \in \mathfrak{A}^{t+s}$ and say that $\alpha|\beta$ is the *concatenation of* α *and* β. If $t = 0$ then $\alpha = \emptyset$ and we let $\emptyset|\beta = \beta$. Accordingly, α is *the* t*-prefix* of $\alpha|\beta$.

Given $\alpha = (\alpha_i)_{i=1}^t \in \mathfrak{A}^t$, $1 \leq t \leq m$, define $\mathcal{O}^\alpha$ as the set all the concatenations $\alpha|\beta \in \mathcal{O}$ where β varies in $\mathfrak{A}^{m-t}$, i.e.

$$\mathcal{O}^\alpha := \{\alpha|\beta \in \mathcal{O} \colon \beta \in \mathfrak{A}^{m-t}\} = \{\omega \in \mathcal{O} \colon \omega_i = \alpha_i, \forall i = 1, \dots, t\}.$$

Put also

$$\mathcal{O}^\emptyset := \mathcal{O} \text{ and } \mathfrak{A}^0 = \emptyset.$$

Suppose the following function is given

$$\psi : \begin{cases} \bigcup_{t=0}^m \mathfrak{A}^t \to \{0, \dots, |\mathcal{O}|\} \\ \\ \alpha \to |\mathcal{O}^\alpha| \end{cases} \tag{2}$$

Clearly $\psi(\alpha) = 0$ if and only if there is no word in $\mathcal{O}$ with prefix α and $\psi(\alpha) = |\mathcal{O}|$ if and only if all words in $\mathcal{O}$ have α as prefix.

For any $\omega \in \mathcal{O}$ and $i \leq m$ write $\omega_{\leq i} := (\omega_1, \dots, \omega_i)$ for the i-prefix of ω and let $\mathbb{I} = \{0, 1, \dots, |\mathcal{O}| - 1\}$. Note that $\omega_{\leq 0} = \emptyset$ and, for $x \in \mathfrak{A}$, $\psi(\omega_{\leq 0}|x) := \psi(x)$.

The function ι defined by

$$\iota : \begin{cases} \mathcal{O} \to \mathbb{I} \\ \iota(\omega) := \displaystyle\sum_{j=1}^m \sum_{\substack{x \in \mathfrak{A}; \\ x \prec \omega_j.}} \psi(\omega_{\leq j-1}|x). \\ \end{cases} \tag{3}$$

is an enumerator for the set $\mathcal{O}$ and given any two elements $\omega, \omega' \in \mathcal{O}$ we have $\iota(\omega) < \iota(\omega')$ if and only if ω precedes ω' in the lexicographic ordering of $\mathfrak{A}^m$ induced by $\prec$. See [9] where such a function was first introduced and also [5] for the details of its injectivity. The inverse of the function ι can be computed as described in Table 1; see [5, Theorem 3.1] for the details of the proof.

Table 1: Inverse of ι

```
Require: $i \in \mathbb{I}$
  $i_1 \leftarrow 1$
  $\omega \leftarrow []$
  for $k = 1, \dots, m$ do
      $M \leftarrow \{y \in \mathfrak{A}\colon \psi(\omega_{\leq k-1}|y) > 0$ and $\sum_{x \prec y} \psi(\omega_{\leq k-1}|x) \leq i_k\}$
      $\omega \leftarrow \omega|(\max M)$
      $i_{k+1} \leftarrow i_k - \sum_{x \prec \omega_k} \psi(\omega_{\leq k-1}|x);$
  end for
  return $\omega$
```

2.2 Notation

In this section we shall apply to the case of line Hermitian Grassmannians, what we introduced in general in Section 2.1. Before defining the analogue of the function ψ (see Equation (2)) we need to recall a few more notions and explain what we mean by *representation* of a given line.

Let $V = V(m, q^2)$ be a vector space of dimension m over $\mathbb{F}_{q^2}$ and let B be a given basis of V. We will always write the coordinates of vectors with respect to B.

Up to projectivities, there is exactly one class of non-degenerate Hermitian forms on V. So, without loss of generality, we can take for m odd the form η to be

$$\eta_m(X, Y) := x_1^q y_1 + x_2^q y_3 + x_3^q y_2 + \cdots + x_{m-1}^q y_m + x_m^q y_{m-1} \tag{4}$$

where $X = (x_i)_{i=1}^m$, and $Y = (y_i)_{i=1}^m$. Accordingly, the points X of the Hermitian polar space $\mathcal{H}_m$ defined by η_m satisfy the following equation

$$x_1^{q+1} + \mathrm{Tr}(\sum_{i=1}^{(m-1)/2} x_{2i}^q x_{2i+1}) = 0,$$

where $\mathrm{Tr}(x) := x + x^q$ is the trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$.

For m even, we will regard the vector space V_m as the m-dimensional vector subspace of $V_{m+1} := V(m + 1, q^2)$ of equation $x_1 = 0$ and the Hermitian form defined on V_m will be the restriction of the form η_{m+1} defined above for the case of odd dimension to $V_m \times V_m$, i.e. $\eta_m(X, Y) := \eta_{m+1}|_{V_m \times V_m}(X, Y)$. Accordingly, if m is even, the polar space $\mathcal{H}_m$ has as points and lines, the points and lines of $\mathcal{H}_{m+1}$ which are fully contained in the hyperplane of equation $x_1 = 0$. Hence, $\mathcal{H}_n^{even} = \mathcal{H}_n^{odd} \cap V_m$.

We shall denote by μ_m, respectively N_m, the number of points, respectively the number of lines, of $\mathcal{H}_m \subseteq \mathrm{PG}(m - 1, q^2)$ (independently from the parity of m). It is well known that

$$\mu_m := \frac{(q^m + (-1)^{m-1})(q^{m-1} - (-1)^{m-1})}{(q^2-1)} \text{ and } N_m := \frac{\mu_m \mu_{m-2}}{q^2+1}. \tag{5}$$

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.

The points of $\mathcal{H}_m$ will be represented as vectors normalized on the left, i.e. whose first non-zero entry is 1. For them the *alphabet* consists of the elements of $\mathbb{F}_{q^2}$ where $\prec$ is an arbitrary total order relation defined on it satisfying the condition: $\forall y \in \mathbb{F}_{q^2} \setminus \{0\} : 0 \prec y$.

The elements of a line Hermitian Grassmannian, i.e. the points of $\mathcal{H}_{n,2}$, are the totally singular lines $\ell \subseteq \mathrm{PG}(m-1, q^2)$ for η. Clearly each of them admits a unique representation in *row-reduced echelon form* (RREF), i.e. for each line ℓ of $\mathrm{PG}(V)$ regarded as a point of $\mathcal{H}_{n,2}$, there are two uniquely determined vectors $X, Y \in \mathbb{F}_{q^2}^m$ such that $\ell = \langle X, Y \rangle$ and $G_\ell := \begin{pmatrix} X \\ Y \end{pmatrix}$ is a $(2 \times m)$-matrix in RREF. We call G_ℓ the *representation* of ℓ.

For example, the representation of a line $\ell = \langle X, Y \rangle$ is a matrix of the form $G_\ell := \begin{pmatrix} 0 & \cdots & 0 & 1 & \cdots & * & \cdots & * & 0 & * & \cdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & 1 & * & \cdots \end{pmatrix}$ where $*$ denotes an arbitrary element of the field. (The unicity of the vectors $(0, \cdots, 0, 1, \cdots, *, \cdots, *, 0, *, \cdots)$ and $(0, \cdots, 0, 0, \cdots, 0, \cdots, 0, 1, *, \cdots)$ as representatives of ℓ is ensured by Gaussian elimination).

With a slight abuse of notation we shall say that a point (resp. a line) has prefix α if its representation with respect to the basis B has prefix α. Clearly, when m is even we can identify the points of the polar space $\mathcal{H}_m$ with those of $\mathcal{H}_{m+1}$ having prefix 0, while the lines of $\mathcal{H}_m$ correspond to the lines of $\mathcal{H}_{m+1}$ with prefix $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

Recall that, in the case of lines, the alphabet $\mathfrak{A}$ consists of all column vectors in $\mathbb{F}_{q^2}^2$ of the form $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ with $\alpha, \beta \in \mathbb{F}_{q^2}$. With a slight abuse of notation, we shall denote the order induced lexicographically on $\mathbb{F}_{q^2}^2$ by $\prec$ with the same symbol $\prec$, so that

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \prec \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \Leftrightarrow (\alpha \prec \gamma) \text{ or } ((\alpha = \gamma) \text{ and } \beta \prec \delta).$$

Under the assumptions we made above, since $\mathcal{H}_n^{even} = \mathcal{H}_n^{odd} \cap V_m$, for all points $p \in \mathcal{H}_n^{even}$ and $p' \in \mathcal{H}_n^{odd} \setminus \mathcal{H}_n^{even}$ we have $\iota(p) < \iota(p')$. Likewise, for any two lines $\ell \in \mathcal{H}_{n,2}^{even}$ and $\ell' \in \mathcal{H}_{n,2}^{odd} \setminus \mathcal{H}_{n,2}^{even}$ (where $\ell = \ell' \cap V_m$) we also have $\iota(\ell) < \iota(\ell')$. This implies that, we can define point and line enumerators for the polar spaces $\mathcal{H}_n^{even}$

as the restriction of the corresponding point and line enumerators for the polar spaces $\mathcal{H}_n^{odd}$. So, in the remaining part of the paper, we shall only explicitly deal with enumerators for $\mathcal{H}_n^{odd}$, i.e. assume m to be odd.

3 Point enumerators

For any t-uple $D_t = (d_i)_{i=1}^t$, $t \leq m$, denote by $\theta(D_t)$ the number of points of $\mathcal{H}_m$ having D_t as prefix, i.e.

$$\theta(D_t) := |\{[D_t|X_{m-t}] \colon [D_t|X_{m-t}] \text{ is a point of } \mathcal{H}_m\}|.$$

In this section we will explain how to explicitly compute the point counting function θ.

We suppose m is odd.

- if D_t is not normalized on the left, then return 0;
- if t is odd, there are two possible subcases:
  1. $\boxed{D_t = \mathbf{0}}$. Then the number of points whose representation begins with D_t is exactly the same as the number of points of a Hermitian variety $\mathcal{H}_{m-t}$; so return
     $$\boxed{\theta(D_t) = \mu_{m-t}}.$$
  2. $\boxed{D_t \neq \mathbf{0}}$. Let $s = (q^2-1)\mu_{m-t} + 1$ be the number of vectors contained in a non-degenerate Hermitian variety in $\mathrm{PG}(V_{m-t})$ and
     (a) if $\eta_t(D_t, D_t) = 0$, then return s;
     (b) if $\eta_t(D_t, D_t) \neq 0$, then let $X \in V(m-t, q^2)$ such that $\eta_{m-t}(X,X) \neq 0$. Then there are $q+1$ values of λ such that $\eta_{m-t}(\lambda X, \lambda X) = -\eta_t(D_t, D_t)$ since the equation $\lambda^{q+1} = \frac{-\eta_t(D_t,D_t)}{\eta_{m-t}(X,X)}$ has exactly $q+1$ solutions. In other words, for each point X not in $\mathcal{H}_{m-t}$ (by convention the points of $\mathcal{H}_{m-t}$ are represented by vectors normalized on the left) there are $q+1$ vectors $Y \in V(m-t, q^2)$ such that $D_t|Y$ is a point of $\mathcal{H}_m$. So, return $(q^{2(m-t)} - s)/(q-1)$.

     In summary,
     $$\boxed{\theta(D_t) = \begin{cases} s & \text{if } \eta_t(D_t,D_t) = 0 \\ (q^{2(m-t)} - s)/(q-1) & \text{if } \eta_t(D_t,D_t) \neq 0 \end{cases}}.$$
- if t is even, there are three possible subcases:

1. $\boxed{D_t = \mathbf{0}}$. In this case we return the number of points whose $(t+1)$-th entry is 0 plus the number of points whose $(t+1)$-th entry is 1 and use the arguments of the previous cases; so

$$\boxed{\theta(D_t) = \theta(D_t|0) + \theta(D_t|1)}.$$

2. $\boxed{D_t \neq \mathbf{0} \text{ and } d_t = 0}$. In this case we need to compute the number of vectors whose representation begins with D_t; observe that this number does not depend on the value of the entry in position $t+1$, since we have

$$d_1^{q+1} + \mathrm{Tr}(d_2^q d_3 + \cdots + 0^q x_{t+1} + \cdots) = 0$$

so, this is q^2 times the number of points with odd prefix $D_t|0$. So,

$$\boxed{\theta(D_t) = q^2 \theta(D_t|0)}.$$

3. $\boxed{D_t \neq \mathbf{0} \text{ and } d_t \neq 0}$. In this case we have to count the number of vector solutions of

$$d_1^{q+1} + \mathrm{Tr}(d_2^q d_3 + \cdots d_{t-2}^q d_{t-1}) + \mathrm{Tr}(d_t^q x_{t+1}) + \mathrm{Tr}(x_{t+2}^q x_{t+3} + \cdots + x_{m-1}^q x_m) = 0.$$

For any choice of $x_{t+2}, \dots, x_m$ there are q possibilities for x_{t+1} such that

$$\mathrm{Tr}(d_t^q x_{t+1}) = -d_1^{q+1} - \mathrm{Tr}(d_2^q d_3 + \cdots d_{t-2}^q d_{t-1}) - \mathrm{Tr}(x_{t+2}^q x_{t+3} + \cdots + x_{m-1}^q x_m).$$

So, in this case, we return

$$\boxed{\theta(D_t) = q \cdot q^{2(m-t-1)}}.$$

It is straightforward to see that to compute the function $\theta(D_t)$ where D_t is a prefix of length $t \leq m$ requires at worst to evaluate $\eta_t(D_t, D_t)$, that is to perform t products and t conjugations. So,

Lemma 2. *The computational complexity of the function θ is $O(t) \leq O(m)$.*

4 Line Enumerators

Let ℓ be a line of $\mathcal{H}_m$ with prefix D_t of length t $(\leq m)$. More explicitly, put $D_t := \begin{pmatrix} A_t \\ B_t \end{pmatrix}$ where $A_t := (a_i)_{i=1}^t$, $B_t := (b_i)_{i=1}^t$, and define $\hat{A} := (A_t, x_{t+1}, \dots, x_m)$ and $\hat{B} := (B_t, y_{t+1}, \dots, y_m)$ so that $\ell = \langle \hat{A}, \hat{B} \rangle$. Take D_t in RREF form and denote by $\psi(D_t)$ the number of lines in $\mathcal{H}_m$ whose representation in RREF begins with D_t. Define $\psi^E(D_t)$ and $\psi^O(D_t)$ as follows:

$$\psi(D_t) =: \begin{cases} \psi^E(D_t) & \text{if } t \text{ is even} \\ \psi^O(D_t) & \text{if } t \text{ is odd.} \end{cases}$$

In this section we will compute $\psi(D_t)$ with some recursive formulas. To this aim, we need to determine the number of solutions of the following system of equations:

$$\begin{cases} \eta_m(\hat{A}, \hat{A}) = 0 \\ \eta_m(\hat{B}, \hat{B}) = 0 \\ \eta_m(\hat{A}, \hat{B}) = 0 \end{cases} . \tag{6}$$

We shall distinguish two cases, depending on the parity of t.

4.1 Even prefix t

It $t = 0$ then $\psi(D_0) = \psi^E(\emptyset)$ is clearly the number of lines of $\mathcal{H}_m$.
If $t > 0$ system (6) can be written as

$$\begin{cases} a_1^{q+1} + \mathrm{Tr}(a_2^q a_3 + \cdots + a_{t-2}^q a_{t-1}) + \mathrm{Tr}(a_t^q x_{t+1}) + \\ \qquad\qquad + \mathrm{Tr}(x_{t+2}^q x_{t+3} + \cdots + x_{m-1}^q x_m) = 0 \\ b_1^{q+1} + \mathrm{Tr}(b_2^q b_3 + \cdots + b_{t-2}^q b_{t-1}) + \mathrm{Tr}(b_t^q y_{t+1}) + \\ \qquad\qquad + \mathrm{Tr}(y_{t+2}^q y_{t+3} + \cdots + y_{m-1}^q y_m) = 0 \\ a_1^q b_1 + a_2^q b_3 + a_3^q b_2 + \cdots + a_{t-2}^q b_{t-1} + a_{t-1}^q b_{t-2} + a_t^q y_{t+1} + x_{t+1}^q b_t + \\ \qquad x_{t+2}^q y_{t+3} + x_{t+3}^q y_{t+2} + \cdots + x_{m-1}^q y_m + x_m^q y_{m-1} = 0 \end{cases} \tag{7}$$

or, equivalently, as

$$\begin{cases} \eta_m(A_t|0^{m-t}, A_t|0^{m-t}) + \mathrm{Tr}(a_t^q x_{t+1}) + \mathrm{Tr}(x_{t+2}^q x_{t+3} + \cdots + x_{m-1}^q x_m) = 0 \\ \eta_m(B_t|0^{m-t}, B_t|0^{m-t}) + \mathrm{Tr}(b_t^q y_{t+1}) + \mathrm{Tr}(y_{t+2}^q y_{t+3} + \cdots + y_{m-1}^q y_m) = 0 \\ \eta_m(A_t|0^{m-t}, B_t|0^{m-t}) + a_t^q y_{t+1} + x_{t+1}^q b_t + x_{t+2}^q y_{t+3} + x_{t+3}^q y_{t+2} + \\ \qquad\qquad + \cdots + x_{m-1}^q y_m + x_m^q y_{m-1} = 0. \end{cases} \tag{8}$$

Note that the matrix $D_t = \begin{pmatrix} A_t \\ B_t \end{pmatrix}$, provided as input of the algorithm, is always supposed to be in RREF. Our goal is now to compute the number of lines whose representation in RREF begins with D_t. To do that it is convenient to replace in (8) the generators $(A_t, x_{t+1}, \ldots, x_m)$ and $(B_t, y_{t+1}, \ldots, y_m)$ of ℓ with two other generators in such a way that at least one of them has the t-th component equal to zero. This is always possible: indeed, if $a_t = 0$ or $b_t = 0$, then we do nothing; otherwise, if, for instance $b_t \neq 0$, we replace the spanning vectors $(A_t, x_{t+1}, \dots, x_m)$ and $(B_t, y_{t+1}, \dots, t_m)$ of ℓ with the vectors $(A_t, x_{t+1}, \dots, x_m) - \frac{a_t}{b_t}(B_t, y_{t+1}, \dots, y_m)$ and $(B_t, y_{t+1}, \dots, y_m)$ respectively. This new prefix $\begin{pmatrix} A_t - \frac{a_t}{b_t} B_t \\ B_t \end{pmatrix}$ of ℓ may not be in RREF but this is not influent for our purposes.

The following cases need to be considered.

(E1) $\boxed{t = 0}$. All lines in $\mathcal{H}_m$ have prefix $\emptyset$; thus,

$$\boxed{\psi^E(\emptyset) = N_m}.$$

(E2) $\boxed{A_t = \mathbf{0} = B_t}$. The lines with prefix D_t correspond to the lines contained in the degenerate Hermitian variety embedded in a vector space of dimension $m - t$ satisfying the following equations

$$(x_t^q x_{t+1} + x_{t+1}^q x_t + x_{t+2}^q x_{t+3} + x_{t+3}^q x_{t+2} + \cdots + x_{m-1}^q x_m = 0) \wedge (x_t = 0).$$

Hence

$$\boxed{\psi^E(D_t) := \mu_{m-t-1} + q^4 N_{m-t-1}}.$$

(E3) $\boxed{a_t \neq 0 \text{ and } B_t = \mathbf{0}}$. For any choice of X_{m-t} such that $\eta_m(A_t|X_{m-t}, A_t|X_{m-t}) = 0$, there are μ_{m-t-1} points Y_{m-t} such that $\langle A_t|X_{m-t}, 0_t|Y_{m-t}\rangle$ is a line of $\mathcal{H}_m$. Since $\begin{pmatrix} A_t & X_{m-t} \\ 0_t & Y_{m-t} \end{pmatrix}$ and $\begin{pmatrix} A_t & X_{m-t} - \alpha Y_{m-t} \\ 0_t & Y_{m-t} \end{pmatrix}$ represent the same line for all $\alpha \in \mathbb{F}_{q^2}$, any line is represented q^2 distinct times. So, we get

$$\psi^E(D_t) = \frac{1}{q^2} \mu_{m-t-1} \theta(A_t).$$

Using the value provided by point 3 of case even in Section 3 for $\theta(A_t)$, this gives

$$\boxed{\psi^E(D_t) := q^{2m-2t-3} \mu_{m-t-1}}.$$

(E4) $\boxed{a_t = 0 \text{ and } b_t \neq 0}$. For any fixed vector $Y = (B_t|y_{t+1}|Y')$ with prefix B_t such that $\eta_m(B_t|y_{t+1}|Y', B_t|y_{t+1}|Y') = 0$ and any choice of $X' = (x_{t+2}, \dots, x_m)$ such that the vector $(A_t|0|X')$ satisfies $\eta_m(A_t|0|X', A_t|0|X') = 0$, the third equation of System (8) uniquely determines x_{t+1}. Hence for any value of $(x_{t+2}, \cdots, x_m)$ and $(y_{t+1}, \cdots, y_m)$ satisfying the first and the second equation of System (8), the third equation provides only one solution of x_{t+1}; so the number of solutions of the system can be computed by only considering the first two equations. The number of solutions of the second equation is $\theta(B_t)$, where we recall from Section 3 that $\theta(B_t)$ is the number of points of $\mathcal{H}_m$ having B_t as prefix. As for the first equation, since $a_t = 0$, we have $\theta(A_t|0) = \theta(A_t|\alpha)$ for any $\alpha \in \mathbb{F}_{q^2}$. Hence, the number of solutions of the first equation is $\theta(A_t|0)$. Since

$$\theta(A_t) = \sum_{\alpha\in\mathbb{F}_{q^2}} \theta(A_t|\alpha) = \sum_{\alpha\in\mathbb{F}_{q^2}} \theta(A_t|0) = q^2\theta(A_t|0),$$

we have $\theta(A_t|0) = \frac{1}{q^2}\theta(A_t)$. It follows that $\psi^E(D_t) = \theta(A_t|0)\theta(B_t)$; hence

$$\boxed{\psi^E(D_t) := \frac{1}{q^2}\theta(A_t)\theta(B_t)}.$$

(E5) $\boxed{a_t \neq 0 \text{ and } B_t \neq \mathbf{0}}$. Since $a_t \neq 0$ we necessarily have $b_t = 0$. This case is analogous to the previous one so

$$\boxed{\psi^E(D_t) = \frac{1}{q^2}\theta(A_t)\theta(B_t)}.$$

(E6) $\boxed{a_t = b_t = 0 \text{ and } A_t \neq \mathbf{0} \neq B_t}$. By System (7), the set of lines of $\mathcal{H}_m$ with (even) prefix $D_t = \begin{pmatrix} A_t \\ B_t \end{pmatrix}$ is the same as the disjoint union of the sets of lines with (odd) prefix $D'_{t+1} = \begin{pmatrix} A_t|\alpha \\ B_t|\beta \end{pmatrix}$ as α and β vary in $\mathbb{F}_{q^2}$. Hence

$$\psi^E(D_t) = \sum_{\alpha,\beta\in\mathbb{F}_{q^2}} \psi^O\left(\begin{pmatrix} A_t|\alpha \\ B_t|\beta \end{pmatrix}\right).$$

Observe that

$$\psi^O\left(\begin{pmatrix} A_t|\alpha \\ B_t|\beta \end{pmatrix}\right) = \psi^O\left(\begin{pmatrix} A_t|0 \\ B_t|0 \end{pmatrix}\right)$$

for any $\alpha, \beta \in \mathbb{F}_{q^2}$. So,

$$\boxed{\psi^E(D_t) := q^4\psi^O\left(\begin{pmatrix} A_t|0 \\ B_t|0 \end{pmatrix}\right)}.$$

The function ψ^O shall be analyzed in the next section.

(E7) $\boxed{a_t = b_t = 0 \text{ and } A_t \neq \mathbf{0} = B_t}$. In this case $\eta_{t+1}(A_t|\alpha, A_t|\alpha) = \eta_{t+1}(A_t|0, A_t|0)$ and $\eta_{t+1}(A_t|\alpha, \mathbf{0}|0) = 0$ for all $\alpha \in \mathbb{F}_{q^2}$. So, in particular,

$$\psi^O\left(\begin{pmatrix} A_t|\alpha \\ \mathbf{0}\,|0 \end{pmatrix}\right) = \psi^O\left(\begin{pmatrix} A_t|0 \\ \mathbf{0}\,|0 \end{pmatrix}\right)$$

for any $\alpha \in \mathbb{F}_{q^2}$. Thus

$$\boxed{\psi^E(D_t) :=} \sum_{\alpha \in \mathbb{F}_{q^2}} \psi^O\left(\begin{pmatrix} A_t|\alpha \\ \mathbf{0}\,|0 \end{pmatrix}\right) + \psi^O\left(\begin{pmatrix} A_t|0 \\ \mathbf{0}\,|1 \end{pmatrix}\right) =$$

$$= \boxed{q^2\psi^O\left(\begin{pmatrix} A_t|0 \\ \mathbf{0}\,|0 \end{pmatrix}\right) + \psi^O\left(\begin{pmatrix} A_t|0 \\ \mathbf{0}\,|1 \end{pmatrix}\right)}.$$

4.2 Odd prefix t

In this section we shall examine the case in which t is odd. System (6) can be written as

$$\begin{cases} a_1^{q+1} + \mathrm{Tr}(a_2^q a_3 + \cdots + a_{t-1}^q a_t) + \mathrm{Tr}(x_{t+1}^q x_{t+2} + \cdots + x_{m-1}^q x_m) = 0 \\ b_1^{q+1} + \mathrm{Tr}(b_2^q b_3 + \cdots + b_{t-1}^q b_t) + \mathrm{Tr}(y_{t+1}^q y_{t+2} + \cdots + y_{m-1}^q y_m) = 0 \\ a_1^q b_1 + a_2^q b_3 + a_3^q b_2 + \cdots + a_{t-1}^q b_t + a_t^q b_{t-1} + \\ \qquad\qquad + x_{t+1}^q y_{t+2} + x_{t+2}^q y_{t+1} + \cdots + x_{m-1}^q y_m + x_m^q y_{m-1} = 0 \end{cases} \tag{9}$$

or, equivalently, as

$$\begin{cases} \eta_t(A_t, A_t) + \mathrm{Tr}(x_{t+1}^q x_{t+2} + \cdots + x_{m-1}^q x_m) = 0 \\ \eta_t(B_t, B_t) + \mathrm{Tr}(y_{t+1}^q y_{t+2} + \cdots + y_{m-1}^q y_m) = 0 \\ \eta_t(A_t, B_t) + x_{t+1}^q y_{t+2} + x_{t+2}^q y_{t+1} + \cdots + x_{m-1}^q y_m + x_m^q y_{m-1} = 0. \end{cases} \tag{10}$$

The following cases need to be considered.

(O1) $\boxed{t = m}$ Then either $D_m = \begin{pmatrix} A_m \\ B_m \end{pmatrix}$ represents a line $\ell = \langle A_m, B_m \rangle$ of $\mathcal{H}_m$ or not; so we have

$$\boxed{\psi^O(D_m) := \begin{cases} 1 & \text{if } \eta_m(A_m, B_m) = \eta_m(A_m, A_m) = \eta_m(B_m, B_m) = 0 \\ 0 & \text{otherwise} \end{cases}}.$$

(O2) $\boxed{A_t = \mathbf{0} = B_t}$. The lines with prefix D_t correspond to the lines contained in a non-degenerate Hermitian variety embedded in a vector space of dimension $m-t$ satisfying the following equation

$$x_{t+1}^q x_{t+2} + x_{t+2}^q x_{t+1} + \cdots + x_{m-1}^q x_m = 0.$$

Hence

$$\boxed{\psi^O(D_t) := N_{m-t}}.$$

(O3) $\boxed{A_t \neq \mathbf{0} \text{ and } B_t = \mathbf{0}}$ Then

$$\psi^O(D_t) := \sum_{\alpha\neq 0} \psi^E\left(\begin{pmatrix} A_t|\alpha \\ \mathbf{0}\,|0 \end{pmatrix}\right) + \psi^E\left(\begin{pmatrix} A_t|0 \\ \mathbf{0}\,|1 \end{pmatrix}\right) +$$
$$+\sum_{\alpha} \psi^O\left(\begin{pmatrix} A_t|0|\alpha \\ B_t|0|0 \end{pmatrix}\right) + \psi^O\left(\begin{pmatrix} A_t|0|0 \\ B_t|0|1 \end{pmatrix}\right).$$

(a) Observe that
$$\psi^E\left(\begin{pmatrix} A_t|\alpha \\ \mathbf{0}\,|0 \end{pmatrix}\right) = \psi^E\left(\begin{pmatrix} A_t|1 \\ \mathbf{0}\,|0 \end{pmatrix}\right)$$
for any $\alpha \neq 0$; so, the first contribution is
$$\sum_{\alpha\neq 0} \psi^E\left(\begin{pmatrix} A_t|\alpha \\ \mathbf{0}\,|0 \end{pmatrix}\right) = (q^2-1)\psi^E\left(\begin{pmatrix} A_t|1 \\ \mathbf{0}\,|0 \end{pmatrix}\right)$$

(b) Also
$$\psi^O\left(\begin{pmatrix} A_t|0|\alpha \\ \mathbf{0}\,|0|0 \end{pmatrix}\right) = \psi^O\left(\begin{pmatrix} A_t|0|0 \\ \mathbf{0}\,|0|0 \end{pmatrix}\right)$$
for any α; so the third contribution is
$$\sum_{\alpha} \psi^O\left(\begin{pmatrix} A_t|0|\alpha \\ B_t|0|0 \end{pmatrix}\right) = q^2\psi^O\left(\begin{pmatrix} A_t|0|0 \\ \mathbf{0}\,|0|0 \end{pmatrix}\right).$$

It follows that

$$\boxed{\begin{aligned}\psi^O(D_t) :=\ & (q^2-1)\psi^E\left(\begin{pmatrix} A_t|1 \\ \mathbf{0}\,|0 \end{pmatrix}\right) + \psi^E\left(\begin{pmatrix} A_t|0 \\ \mathbf{0}\,|1 \end{pmatrix}\right) + \\ & +q^2\psi^O\left(\begin{pmatrix} A_t|0|0 \\ \mathbf{0}\,|0|0 \end{pmatrix}\right) + \psi^O\left(\begin{pmatrix} A_t|0|0 \\ B_t|0|1 \end{pmatrix}\right).\end{aligned}}$$

(O4) $\boxed{B_t \neq \mathbf{0}}$ Then

$$\psi^O(D_t) := \sum_{\alpha\neq 0\neq\beta} \psi^E\left(\begin{pmatrix} A_t|\alpha \\ B_t|\beta \end{pmatrix}\right) + \sum_{\alpha\neq 0} \psi^E\left(\begin{pmatrix} A_t|\alpha \\ B_t|0 \end{pmatrix}\right) + \\ + \sum_{\beta\neq 0} \psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|\beta \end{pmatrix}\right) + \psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|0 \end{pmatrix}\right).$$

In order to determine the various contributions, for $A_t, B_t \in V(t, q^2)$, define

$$\zeta(A_t, B_t) := \sum_{\alpha\neq 0\neq\beta} \psi^E\left(\begin{pmatrix} A_t|\alpha \\ B_t|\beta \end{pmatrix}\right).$$

Lemma 3.

$$\zeta(A_t, B_t) = (q^2-1)\theta(B_t|1)[\xi(A_t, B_t)s + (q^2-1-\xi(A_t,B_t))\frac{q^{2m-2t-4}-s}{q-1}]$$

where $\xi(A_t, B_t)$ is the number of values $\lambda \in \mathbb{F}_{q^2}$ with $\lambda \neq 0$ such that

$$\eta_m(A_t - \lambda B_t|0^{m-t}, A_t - \lambda B_t|0^{m-t}) = 0$$

and $s = (q^2-1)\mu_{m-t-2} + 1$.

Proof. Since

$$\psi^E\left(\begin{pmatrix} A_t|\alpha \\ B_t|\beta \end{pmatrix}\right) = \psi^E\left(\begin{pmatrix} A_t - \lambda_{\alpha,\beta}B_t | \alpha - \lambda_{\alpha,\beta}\beta \\ B_t \quad | \quad \beta \end{pmatrix}\right)$$

for any choice of scalars $\lambda_{\alpha,\beta} \in \mathbb{F}_{q^2}$,

$$\zeta(A_t, B_t) := \sum_{\alpha\neq 0\neq\beta} \psi^E\left(\begin{pmatrix} A_t - \lambda_{\alpha,\beta}B_t | \alpha - \lambda_{\alpha,\beta}\beta \\ B_t \quad | \quad \beta \end{pmatrix}\right).$$

Put $\lambda_{\alpha,\beta} := \alpha\beta^{-1}$. Then,

$$\zeta(A_t, B_t) := \sum_{\alpha\neq 0\neq\beta} \psi^E\left(\begin{pmatrix} A_t - \alpha\beta^{-1}B_t | 0 \\ B_t \quad |\beta \end{pmatrix}\right).$$

Since α is an arbitrary non-zero element, for each value of β, $\lambda_{\alpha,\beta} := \alpha\beta^{-1}$ assumes all possible non-zero values — so, with a change of variable, we get

$$\zeta(A_t, B_t) := \sum_{\lambda\neq 0\neq\beta} \psi^E\left(\begin{pmatrix} A_t - \lambda B_t | 0 \\ B_t \quad |\beta \end{pmatrix}\right).$$

Finally, observe that for $\beta \neq 0$,

$$\psi^E\left(\begin{pmatrix} A_t - \lambda B_t | 0 \\ B_t \quad | \beta \end{pmatrix}\right) = \psi^E\left(\begin{pmatrix} A_t - \lambda B_t | 0 \\ B_t \quad | 1 \end{pmatrix}\right).$$

Hence

$$\zeta(A_t, B_t) := (q^2 - 1) \sum_{\lambda \neq 0} \psi^E\left(\begin{pmatrix} A_t - \lambda B_t | 0 \\ B_t \quad | 1 \end{pmatrix}\right).$$

Now, since the $(t+1)$-entry in the second row is non-zero, by case (E4) analyzed in Section 4.1,

$$\psi^E\left(\begin{pmatrix} A_t - \lambda B_t | 0 \\ B_t \quad | 1 \end{pmatrix}\right) = \frac{1}{q^2}\theta(A_t - \lambda B_t | 0)\theta(B_t | 1)$$

and

$$\zeta(A_t, B_t) = \frac{q^2 - 1}{q^2}\theta(B_t | 1) \sum_{\lambda \neq 0} \theta(A_t - \lambda B_t | 0).$$

On the other hand, by Section 3 case 2 of even prefix,

$$\theta(A_t - \lambda B_t | 0) = q^2 \theta(A_t - \lambda B_t | 0 | 0),$$

so,

$$\frac{1}{q^2}\theta(A_t - \lambda B_t | 0) = \begin{cases} s & \text{if } \eta_t(A_t - \lambda B_t, A_t - \lambda B_t) = 0 \\ \dfrac{(q^2)^{(m-t-2)} - s}{q - 1} & \text{if } \eta_t(A_t - \lambda B_t, A_t - \lambda B_t) \neq 0, \end{cases}$$

where $s := (q^2 - 1)\mu_{m-t-2} + 1$. Since $\xi(A_t, B_t)$ is the number of values $\lambda \in \mathbb{F}_{q^2}$ with $\lambda \neq 0$ and $\eta_m(A_t - \lambda B_t | 0^{m-t}, A_t - \lambda B_t | 0^{m-t}) = 0$, we have

$$\begin{aligned} \zeta(A_t, B_t) = (q^2 - 1)\theta(B_t | 1)(\xi(A_t, B_t)s + (q^2 - 1 - \xi(A_t, B_t))\tfrac{q^{2m-2t-4} - s}{q-1}) = \\ = (q^2 - 1)q^{2m-2t-3}(\xi(A_t, B_t)s + (q^2 - 1 - \xi(A_t, B_t))\tfrac{q^{2m-2t-4} - s}{q-1}). \end{aligned}$$

□

We now compute $\xi(A_t, B_t)$.

Lemma 4. *We have*

$$\xi(A_t, B_t) := \begin{cases} q^2 - 1 & \textit{if } \eta_t(A_t, A_t) = \eta_t(B_t, B_t) = \eta_t(A_t, B_t) = 0 \\ q - 1 & \textit{if } \eta_t(A_t, A_t) = \eta_t(B_t, B_t) = 0 \neq \eta_t(A_t, B_t) \\ 0 & \textit{if } \eta_t(A_t, B_t) = 0 = \eta_t(A_t, A_t)\eta_t(B_t, B_t) \\ q + 1 & \textit{if } \eta_t(A_t, B_t) = 0, \eta_t(A_t, A_t)\eta_t(B_t, B_t) \neq 0 \\ q & \textit{if } \eta_t(A_t, B_t) \neq 0, \eta_t(A_t, A_t)\eta_t(B_t, B_t) = 0 \\ 1 & \textit{if Equation (11) satisfied} \\ q + 1 & \textit{otherwise} \end{cases}$$

where for $\eta_t(B_t, B_t) \neq 0$, let

$$\delta := \frac{\eta_t(A_t, B_t)^q}{\eta_t(B_t, B_t)}$$

and consider

$$\delta^{q+1}\eta_t(B_t, B_t) - \delta\eta_t(A_t, B_t) - \delta^q\eta_t(B_t, A_t) + \eta_t(A_t, A_t) = 0. \tag{11}$$

Proof. The value $\xi(A_t, B_t)$ is precisely the number of intersections different from $\{A_t, B_t\}$, of the line $\ell_{AB} := \langle A_t, B_t\rangle$ with a Hermitian variety $\mathcal{H}_t$ defined by the form η_t. We distinguish several cases:

(a) $\eta_t(A_t, A_t) = \eta_t(B_t, B_t) = 0$. Then either the line ℓ_{AB} is totally isotropic, i.e. $\eta_t(A_t, B_t) = 0$; hence there are $q^2 - 1$ points on ℓ_{AB} different from A_t and B_t and $\xi(A_t, B_t) := q^2 - 1$ or the line ℓ_{AB} meets $\mathcal{H}_t$ in a Baer subline, hence $\xi(A_t, B_t) = q - 1$.

(b) $\eta_t(A_t, B_t) = 0$ and $(\eta_t(A_t, A_t) \neq 0$ or $\eta_t(B_t, B_t) \neq 0)$. Then

i. $\eta_t(A_t, A_t) = 0 \neq \eta_t(B_t, B_t)$, then the line ℓ_{AB} is tangent to $\mathcal{H}_t$ in A_t but not totally isotropic; so it meets $\mathcal{H}_t$ only in A_t and, consequently,

$$\xi(A_t, B_t) = 0;$$

the case $\eta_t(A_t, A_t) \neq 0 = \eta_t(B_t, B_t)$ is entirely analogous;

ii. $\eta_t(A_t, A_t) \neq 0 \neq \eta_t(B_t, B_t)$; then $A_t, B_t \notin \mathcal{H}_t$ and B_t is in the polar hyperplane of A_t. In this case the line ℓ_{AB} meets $\mathcal{H}_t$ in a Baer subline, hence there are $(q + 1)$ points, all different from A_t and B_t, so

$$\xi(A_t, B_t) = q + 1.$$

(c) $\eta_t(A_t, B_t) \neq 0$. Then

i. if $\eta_t(A_t, A_t) = 0$ or $\eta_t(B_t, B_t) = 0$, then the line ℓ_{AB} meets $\mathcal{H}_t$ in $q + 1$ points, one of them being A_t (or B_t); so

$$\xi(A_t, B_t) = q.$$

ii. If $\eta_t(A_t, A_t) \neq 0 \neq \eta_t(B_t, B_t)$, then observe that since $A_t, B_t \notin \mathcal{H}_t$ the line ℓ_{AB} is tangent to $\mathcal{H}_t$ if, and only if the equation

$$\eta_t(A_t - \lambda B_t, A_t - \lambda B_t) = 0 \tag{12}$$

admits a solution with multiplicity $q + 1 > 1$. Expanding Equation (12), we have

$$\lambda^{q+1}\eta_t(B_t, B_t) - \lambda^q\eta_t(B_t, A_t) - \lambda\eta_t(A_t, B_t) + \eta_t(A_t, A_t) = 0,$$

and its derivative in λ is

$$\lambda^q \eta_t(B_t, B_t) - \eta_t(A_t, B_t) = 0. \tag{13}$$

So, let

$$\delta := \frac{\eta_t(A_t, B_t)^q}{\eta_t(B_t, B_t)}.$$

We have that ℓ_{AB} is tangent to $\mathcal{H}_t$ if and only if (11) is satisfied. This gives the last two possible values for $\xi(A_t, B_t)$.

□

Corollary 5. *The complexity of the function $\zeta(A_t, B_t)$ is $O(t) \leq O(m)$.*

Proof. In order to determine $\zeta(A_t, B_t)$ we need to evaluate the point enumerator $\theta(B_t|1)$, which has complexity $O(m)$, and the function $\xi(A_t, B_t)$. It is straightforward to see from Lemma 4 that evaluating $\xi(A_t, B_t)$ requires to compute three sesquilinear products, each of them involving t products and t conjugations. So the complexity of $\xi(A_t, B_t)$ is also $O(t) \leq O(m)$. □

Observe that

$$\psi^E\left(\begin{pmatrix} A_t|\alpha \\ B_t|0 \end{pmatrix}\right) = \psi^E\left(\begin{pmatrix} A_t|1 \\ B_t|0 \end{pmatrix}\right)$$

for any $\alpha \neq 0$; so

$$\sum_{\alpha\neq 0} \psi^E\left(\begin{pmatrix} A_t|\alpha \\ B_t|0 \end{pmatrix}\right) = (q^2-1)\psi^E\left(\begin{pmatrix} A_t|1 \\ B_t|0 \end{pmatrix}\right)$$

On the other hand,

$$\psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|\beta \end{pmatrix}\right) = \psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|1 \end{pmatrix}\right)$$

for any $\beta \neq 0$; so

$$\sum_{\beta\neq 0} \psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|\beta \end{pmatrix}\right) = (q^2-1)\psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|1 \end{pmatrix}\right)$$

Finally,

$$\psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|0 \end{pmatrix}\right) = \sum_{\alpha,\beta} \psi^O\left(\begin{pmatrix} A_t|0|\alpha \\ B_t|0|\beta \end{pmatrix}\right);$$

on the other hand

$$\psi^O\left(\begin{pmatrix} A_t|0|\alpha \\ B_t|0|\beta \end{pmatrix}\right) = \psi^O\left(\begin{pmatrix} A_t|0|0 \\ B_t|0|0 \end{pmatrix}\right),$$

so

$$\psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|0 \end{pmatrix}\right) = q^4\psi^O\left(\begin{pmatrix} A_t|0|0 \\ B_t|0|0 \end{pmatrix}\right).$$

It follows that

$$\boxed{\begin{aligned} \psi^O(D_t) \quad &:= \zeta(A_t, B_t) + (q^2-1)\Bigg(\psi^E\left(\begin{pmatrix} A_t|0 \\ B_t|1 \end{pmatrix}\right) + \psi^E\left(\begin{pmatrix} A_t|1 \\ B_t|0 \end{pmatrix}\right)\Bigg) + \\ &\quad q^4\psi^O\left(\begin{pmatrix} A_t|0|0 \\ B_t|0|0 \end{pmatrix}\right). \end{aligned}}$$

5 Proof of the Main Theorem

We now estimate the complexity of the line enumerator given by the function ι described by Equation (3) in Section 2.1 and complete the proof of our main theorem. By definition, in order to evaluate $\iota(\ell)$ for a given line ℓ we need to compute the value of the function ψ defined in Section 4 for at most q^4m different inputs (recall that the alphabet $\mathfrak{A}$ in this case is $\mathbb{F}_{q^2}^2$). So we can state that the complexity of ι is at most q^4m times the complexity of ψ. We can now proceed to analyze the function ψ step by step. We refer to the labels in Section 4.1 and 4.2, as well as to Table 2 for the various cases.

- In case (E1), i.e. $t = 0$, as well as in cases (E2), (E3) and (O2), the number $\psi(D_t)$ depends only on the length t. So, the complexity is $O(1)$.
- In case (O1), i.e. $t = m$, $\psi(D_m)$ is either 1 or 0 according as $D_m = \begin{pmatrix} A \\ B \end{pmatrix}$ represents a totally isotropic line $\ell = \langle A, B\rangle$ or not. To check whether this is the case we need to evaluate $\eta_m(A, A)$, $\eta_m(B, B)$ and $\eta_m(A, B)$. This requires $3m$ products as well as $3m$ conjugations; so the overall complexity of this case is $O(m)$.
- In cases (E4) and (E5) we need to evaluate the number of totally isotropic points whose normalized coordinates begin with either A or B, i.e. the functions $\theta(A)$ and $\theta(B)$. By Lemma 2, the complexity of θ is $O(m)$; consequently the complexity of this case is also $O(m)$.

- The value of $\psi^E(D_t)$ in cases (E6) and (E7) is a function of $\psi^O(D'_{t+1})$ where D'_{t+1} is as in cases (O3) or (O4). More in detail, the complexity of case (E6) is the same as the complexity of case (O4), while the complexity of case (E7) is the same as the sum of the complexities of cases (O3) and (O4).
- The computation of $\psi^O(D_t)$ in both cases (O3) and (O4) requires to compute the value of $\psi^E(D_{t+1})$ in cases of the form (E3), (E4) or (E5) and then evaluate functions of the form $\psi^O(D_{t+2})$ with suitable prefixes of length $t+2$. We have already seen that the complexity of cases (E3), (E4) or (E5) is at most $O(m)$.

  If $t+2=m$, then $\psi^O(D_{t+2})$ is of type (O1) and has also complexity $O(m)$, so, for $t=m-2$ the overall complexity of both (O3) and (O4) is $O(m)$.

  Suppose now $t=m-2i$ with $1 \le i \le \lfloor m/2 \rfloor$. The complexity of the function $\zeta(A_t, B_t)$ occurring in case (O4) is $O(m)$, see Corollary 5.

  In any case, the complexity of $\psi^O(D_{m-2i})$ is the sum of $O(m)$ and the complexity of $\psi^O(D_{m-2i+2})$. In turn, the complexity of $\psi^O(D_{m-2i+2})$ is $O(m)$ plus the complexity of $\psi^O(D_{m-2i+4})$. After i steps, the complexity of $\psi^O(D_{m-2i})$ is i times the complexity of $\psi^O(D_m)$. Since $i=O(m)$, we see that the total complexity for cases (O3) and (O4) is at most $O(m^2)$.

The above argument shows that the maximum complexity of the function ψ is $O(m^2)$. So, the complexity of ι is $O(q^4m^3)$.

□

6 Applications

In this section we propose an application of the enumerator ι defined in (3) and studied in Sections 3 and 4 for the encoding and decoding of Line Hermitian Grassmann codes. We refer to [6] for more details on these codes. As seen in Section 1.2, the generator matrix of a line Hermitian Grassmann code consists of a $(K \times N)$-matrix whose columns are vector representatives for the points of the variety $\mathbb{H}_{n,2}$ (see (1)).

The way to implement such codes relies on the possibility to easily handle the point-set of $\mathbb{H}_{n,2}$.

For each codeword $\mathbf{c}$ there is a linear functional $\omega : \bigwedge^2 V \to \mathbb{F}_{q^2}$ such that

$$\mathbf{c} = (\omega(P_1), \dots, \omega(P_n))$$

where $P_1, \dots, P_N$ are the points of $\mathbb{H}_{n,2}$. It is well known that the linear functionals $\bigwedge^2 V \to \mathbb{F}_{q^2}$ correspond to alternating bilinear forms on V; see [6].

This motivates the scheme we propose in the following sections to encode, decode and correct linear Hermitian Grassmann codes.

Table 2: Enumerator for Hermitian Line Grassmannians

$D_t = \begin{pmatrix}A_t\\B_t\end{pmatrix}$	t	Case	$\psi(S)$	Complexity
$\emptyset$	$t=0$	(E1)	N_m	$O(1)$
$\begin{pmatrix}a_1a_2\cdots a_m\\b_1\,b_2\cdots b_m\end{pmatrix}$	$t=m$	(O1)	$\begin{cases}1 & \text{if } \eta_m(A_m,B_m)=\eta_m(A_m,A_m)\\ & \quad =\eta_m(B_m,B_m)=0\\0 & \text{otherwise}\end{cases}$	$O(m)$
$\begin{pmatrix}00\cdots 00\\00\cdots 00\end{pmatrix}$	Even	(E2)	$\mu_{m-t-1}+q^4N_{m-t-1}$	$O(1)$
$\begin{pmatrix}a_1a_2\cdots a_{t-1}a_t\\0\;\;0\cdots\;\;0\;\;\;0\end{pmatrix}$ $a_t\neq 0$	Even	(E3)	$q^{2m-2t-3}\mu_{m-t-1}$	$O(1)$
$\begin{pmatrix}a_1a_2\cdots a_{t-1}\,0\\b_1\,b_2\cdots b_{t-1}\,b_t\end{pmatrix}$ $b_t\neq 0$	Even	(E4)	$\frac{1}{q^2}\theta(A_t)\theta(B_t)$	$O(m)$
$\begin{pmatrix}a_1a_2\cdots a_{t-1}a_t\\b_1\,b_2\cdots b_{t-1}\;0\end{pmatrix}$ $a_t\neq 0, B_t\neq \mathbf{0}$	Even	(E5)	$\frac{1}{q^2}\theta(A_t)\theta(B_t)$	$O(m)$
$\begin{pmatrix}a_1a_2\cdots a_{t-1}0\\b_1\,b_2\cdots b_{t-1}0\end{pmatrix}$ $A_t\neq \mathbf{0}\neq B_t$	Even	(E6)	$q^4\psi^O\begin{pmatrix}A_t\vert 0\\B_t\vert 0\end{pmatrix}$	$O(m^2)$
$\begin{pmatrix}a_1a_2\cdots a_{t-1}0\\0\;\;0\cdots\;\;0\;\;0\end{pmatrix}$ $A_t\neq \mathbf{0}$	Even	(E7)	$q^4\psi^O\begin{pmatrix}A_t\vert 0\\\mathbf{0}\;\vert 0\end{pmatrix}+\psi^O\begin{pmatrix}A_t\vert 0\\\mathbf{0}\;\vert 1\end{pmatrix}$	$O(m^2)$
$\begin{pmatrix}00\cdots 00\\00\cdots 00\end{pmatrix}$	Odd	(O2)	N_{m-t}	$O(1)$
$\begin{pmatrix}a_1a_2\cdots a_t\\0\;\;0\cdots 0\end{pmatrix}$ $A_t\neq \mathbf{0}$	Odd	(O3)	$(q^2-1)\psi^E\begin{pmatrix}A_t\vert 1\\\mathbf{0}\;\vert 0\end{pmatrix}+\psi^E\begin{pmatrix}A_t\vert 0\\\mathbf{0}\;\vert 1\end{pmatrix}+$ $q^2\psi^O\begin{pmatrix}A_t\vert 0\vert 0\\\mathbf{0}\;\vert 0\vert 0\end{pmatrix}+\psi^O\begin{pmatrix}A_t\vert 0\vert 0\\\mathbf{0}\;\vert 0\vert 1\end{pmatrix}$	$O(m^2)$
$\begin{pmatrix}a_1a_2\cdots a_t\\b_1\,b_2\cdots b_t\end{pmatrix}$ $A_t\neq \mathbf{0}\neq B_t$	Odd	(O4)	$\zeta(A_t,B_t)+(q^2-1)\Bigg(\psi^E\begin{pmatrix}A_t\vert 1\\B_t\vert 0\end{pmatrix}+$ $\psi^E\begin{pmatrix}A_t\vert 0\\B_t\vert 1\end{pmatrix}\Bigg)+q^4\psi^O\begin{pmatrix}A_t\vert 0\vert 0\\B_t\vert 0\vert 0\end{pmatrix}$	$O(m^2)$

The function $\zeta(A_t,B_t)$ is computed in Lemma 3 and Lemma 4.

6.1 Encoding and decoding

Assume m odd and let $B := (e_1, \dots, e_m)$ a basis of $V(m, q^2)$ such that the sesquilinear form η has Equation (4). Our arguments apply also when m is even, and $V(m, q^2)$ is the hyperplane of equation $x_1 = 0$ embedded in $V(m+1, q^2)$. Let also $K = \binom{m}{2}$ and suppose $\mathbf{w} = (w_1, \dots, w_K)$ to be a message. Using the enumerator ι, we define the i-th component c_i of a codeword $\mathbf{c} = (c_1, \dots, c_N)$ representing $\mathbf{w}$ as

$$c_i := \omega_{\mathbf{w}}(A_{i-1}, B_{i-1}) := A_{i-1} W B_{i-1}^T$$

where $\begin{pmatrix} A_{i-1} \\ B_{i-1} \end{pmatrix} = \iota^{-1}(i-1)$ represents the i–th element $\ell = \langle A_{i-1}, B_{i-1} \rangle$ of the polar Grassmannian $\mathcal{H}_{n,2}$ and $W = W_0 - W_0^T$ is the antisymmetric matrix obtained from

$$W_0 = \begin{pmatrix} 0 & w_1 & w_2 & \dots & w_{m-1} \\ & 0 & w_m & \dots & w_{2m-3} \\ & & \ddots & & \vdots \\ & & & 0 & w_K \\ & & & & 0 \end{pmatrix}$$

representing the alternating bilinear form $\omega_{\mathbf{w}}$ induced by $\mathbf{w}$ with respect to the basis B. Note that W is precisely the Gram matrix of the alternating bilinear form $\omega_{\mathbf{w}}$.

For $1 \leq i < j \leq m$, denote by $\mathfrak{w}_{ij}$ the entry in W_0 in position (i, j). Then

$$\mathfrak{w}_{ij} := w_{\frac{(i-1)(2n-i)}{2} + j - i}.$$

Denote by $\varphi : \mathbb{F}_{q^2}^K \to \mathbb{F}_{q^2}^N$ the function mapping a message $\mathbf{w}$ to the corresponding codeword $\mathbf{c}$.

Lemma 6. *The function $\varphi : \mathbb{F}_{q^2}^K \to \mathbb{F}_{q^2}^N$ is linear.*

Proof. Let $\mathbf{w}$ and $\mathbf{w}'$ be two messages and $\mathbf{c}$ and $\mathbf{c}'$ be the corresponding codewords. Let also $\mathbf{c}'' = \alpha\mathbf{c} + \beta\mathbf{c}'$ and $\mathbf{w}'' = \alpha\mathbf{w} + \beta\mathbf{w}'$ for $\alpha, \beta \in \mathbb{F}_{q^2}$. Then

$$c_i'' = \alpha c_i + \beta c_i' = \alpha A_{i-1} W B_{i-1}^T + \beta A_{i-1} W' B_{i-1}^T = A_{i-1}(\alpha W + \beta W') B_{i-1}^T,$$

so $\varphi(\alpha\mathbf{w} + \beta\mathbf{w}') = \alpha\varphi(\mathbf{w}) + \beta\varphi(\mathbf{w}')$ and φ is linear. □

Given a codeword $\mathbf{c} = (c_i)_{i=1}^N$ we now show how to uniquely extract the entries $\mathfrak{w}_{ij}$ with $i < j$ of W_0 from $\mathbf{c}$ with constant complexity $O(1)$; clearly, this is equivalent to determine the message $\mathbf{w} = (w_i)_{i=1}^K$.

Theorem 7. *Suppose m to be odd. Let $\mathbf{c}$ be a codeword and $W = (\mathfrak{w}_{ij})_{1\leq i,j\leq 2n+1}$ be the antisymmetric matrix associated with the message $\mathbf{w}$ mapped to $\mathbf{c}$ using the function φ. Suppose that the pair (i,j) with $1 \leq i < j \leq m$ 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 $\mathfrak{w}_{ij} = c_{\iota(\ell_{i,j})+1}$ where $\ell_{i,j} := \langle e_i, e_j\rangle$.*
- *If (i,j) is of Type II then $\mathfrak{w}_{ij}$ can be obtained by solving a system of 2 linear equations in 2 unknowns.*
- *If (i,j) is of Type III then $\mathfrak{w}_{ij}$ can be obtained by solving a linear equation.*

Proof. If (i,j) is of Type I then the line $\ell_{i,j} := \langle e_i, e_j\rangle$ is totally isotropic for the Hermitian form η; furthermore $\omega_{\mathbf{w}}(e_i, e_j) = \mathfrak{w}_{ij}$ and we are done.

Suppose (i,j) is of Type II with $i < 2n$. Let σ be an element of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\sigma^q + \alpha\sigma + \beta = 0$ with $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$. Consider two lines $\ell := \langle e_i + (\alpha\sigma + \beta)e_{i+3}, \sigma e_{i+1} + e_{i+2}\rangle$ and $\ell^q := \langle e_i + (\alpha\sigma^q + \beta)e_{i+3}, \sigma^q e_{i+1} + e_{i+2}\rangle$. It is straightforward to see that both lines are totally isotropic, so they correspond to two components in the codeword $\mathbf{c}$; call them respectively $c_x := c_{\iota(\ell)+1}$ and $c_y := c_{\iota(\ell^q)+1}$. Then we have

$$\begin{cases} \sigma\mathfrak{w}_{i,i+1} + \mathfrak{w}_{i,i+2} - \sigma(\alpha\sigma + \beta)\mathfrak{w}_{i+1,i+3} - (\alpha\sigma + \beta)\mathfrak{w}_{i+2,i+3} = c_x \\ \sigma^q\mathfrak{w}_{i,i+1} + \mathfrak{w}_{i,i+2} - \sigma^q(\alpha\sigma^q + \beta)\mathfrak{w}_{i+1,i+3} - (\alpha\sigma^q + \beta)\mathfrak{m}_{i+2,i+3} = c_y. \end{cases} \tag{14}$$

The entries $\mathfrak{w}_{i+1,i+3}$ and $\mathfrak{w}_{i,i+2}$ correspond to indexes of Type I; thus they can be read off $\mathbf{c}$ directly. We are left with a linear system of two equations in the unknowns $\mathfrak{w}_{i,i+1}$ and $\mathfrak{w}_{i+2,i+3}$. Since

$$\det\begin{pmatrix} \sigma & -(\alpha\sigma + \beta) \\ \sigma^q & -(\alpha\sigma^q + \beta)\end{pmatrix} = \beta(\sigma^q - \sigma) \neq 0,$$

this linear system admits a unique solution and can be solved with complexity $O(1)$. In particular, for $(i,j) = (2n-2, 2n-1)$ we obtain also the value $\mathfrak{w}_{2n,2n+1}$ for the pair $(i,j) = (2n, 2n+1)$.

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

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

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

Corollary 8. *Suppose m to be even. Let $\mathbf{c}$ be a codeword and $W = (\mathfrak{w}_{ij})_{1\leq i,j\leq 2n+1}$ be the antisymmetric matrix associated with the message $\mathbf{w}$ mapped to $\mathbf{c}$ using the encoding φ. Suppose that the pair (i, j) with $1 \leq i < j \leq m$ is in one of the following types:*

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

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

Then the following holds:

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

Proof. For m even, we can regard the Hermitian polar space $\mathcal{H}_m$ as the hyperplane section of $\mathcal{H}_{m+1}$ with respect to the hyperplane $x_1 = 0$. By renumbering the indexes, we can write the form inducing $\mathcal{H}_n$ as $\eta(x, y) = x_1 y_2^q + \cdots$ instead of $x_1 y_1^q + x_2 y_3^q + \cdots, x_1 = y_1 = 0$. The corollary now follows from the previous theorem.

□

Corollary 9. *The map $\varphi : \mathbb{F}_{q^2}^K \to \mathbb{F}_{q^2}^N$ is injective.*

Proof. Suppose $\varphi(\mathbf{w}) = \mathbf{0}$; by the proof of Theorem 7, all indexes $\mathfrak{w}_{ij}$ of Type I must be 0. Also, for indexes of Type II System (14) becomes

$$\begin{cases} \sigma\mathfrak{w}_{i,i+1} - (\alpha\sigma + \beta)\mathfrak{w}_{i+2,i+3} = 0 \\ \sigma^q\mathfrak{w}_{i,i+1} - (\alpha\sigma^q + \beta)\mathfrak{w}_{i+2,i+3} = 0 \end{cases}$$

whose only solution is $\mathfrak{w}_{i,i+1} = \mathfrak{w}_{i+2,i+3} = 0$. Finally, entries of Type III must satisfy $\mathfrak{w}_{1j} = 0$ for all j.

The case m even is entirely analogous and can be proven using Corollary 8. □

By Lemma 6 and Corollary 9, φ is a linear encoding.

6.2 Error correction

First of all, observe that in order to recover the original message sent $\mathbf{w} = (w_1, \ldots, w_K)$ it is enough to guarantee that the entries of a received vector $\mathbf{r} \in \mathbb{F}_{q^2}^N$ needed to obtain the elements $\mathfrak{w}_{ij}$ of Theorem 7 and Corollary 8, are correct. This could be implemented using standard techniques from coding theory, e.g. syndrome decoding, see [13, Chapter 1], but such an approach would be very inefficient in the case of (polar) Grassmann codes, since the parity check matrix is huge.

A different, more viable, approach is what we proposed in [4] for line polar Grassmann codes of either orthogonal or symplectic type and we here extend to the Hermitian case. Suppose r_x is an entry in the received vector $\mathbf{r}$ which we want to insure to be correct. So, we take the line $\ell = \langle A_{x-1}, B_{x-1} \rangle$ with index $\iota(\ell) = x - 1$ and consider the pencil Π_ℓ of all the totally singular planes passing through ℓ.

For each $\pi \in \Pi_\ell$ choose 3 non-concurrent lines r, s, t of π different from ℓ. Observe that the values of $r_{\iota(r)+1}$ $r_{\iota(s)+1}$ and $r_{\iota(t)+1}$ are sufficient to reconstruct the restriction of the alternating form $\omega_{\mathbf{w}}$ to π, say ω^π. If $\omega^\pi(A_{x-1}, B_{x-1}) = r_x$ for a sufficient number of planes, then we can assume that the received value r_x is correct. Otherwise, we replace r_x with the majority of the values $\omega^\pi(A_{x-1}, B_{x-1})$ assumes as π varies in Π_ℓ. We leave to a future work a detailed analysis of the performance of this error correcting algorithm.

Acknowledgments

Both authors are affiliated with GNSAGA of INdAM (Italy) whose support they acknowledge.

References

[1] R. J. Blok and B. N. Cooperstein. The generating rank of the unitary and symplectic Grassmannians. *J. Combin. Theory Ser. A*, 119(1):1–13, 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 and L. Giuzzi. Enumerative coding for line polar Grassmannians with applications to codes. *Finite Fields Appl.*, 46:107–138, 2017.

[5] I. Cardinali and L. Giuzzi. Minimum distance of line orthogonal Grassmann codes in even characteristic. *J. Pure Appl. Algebra*, 222(10):2975–2988, 2018.

[6] I. Cardinali and L. Giuzzi. Line Hermitian Grassmann codes and their parameters. *Finite Fields Appl.*, 51: 407–432, 2018.

[7] 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.

[8] 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.

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

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

[11] 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.

[12] 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.

[13] F. J. MacWilliams and N. J. A. Sloane *The theory of error-correcting codes.* North Holland Publishing Co., 1977.

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

[15] 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).

[16] 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).

[17] 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.

[18] 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.

Authors' addresses:

Ilaria Cardinali
Department of Information Engineering
and Mathematics
University of Siena
Via Roma 56, I-53100, Siena, Italy
ilaria.cardinali@unisi.it

Luca Giuzzi
D.I.C.A.T.A.M.
Section of Mathematics
University of Brescia
Via Branze 43, I-25123, Brescia, Italy
luca.giuzzi@unibs.it