Research Article

Open Access

Jesús Carrillo–Pacheco* and Fausto Jarquín –Zárate

A family of low density matrices in Lagrangian–Grassmannian

<https://doi.org/10.1515/spma-2018-0019>

Received October 18, 2017; accepted April 26, 2018

Abstract: The aim of this paper is twofold. First, we show a connection between the Lagrangian–Grassmannian variety geometry defined over a finite field with q elements and the q –ary Low–Density Parity–Check codes. Second, considering the Lagrangian–Grassmannian variety as a linear section of the Grassmannian variety, we prove that there is a unique linear homogeneous polynomials family, up to linear combination, such that annuls the set of its rational points.

Keywords: Lagrangian–Grassmannian variety, general theory of matrices, the low–density parity–check codes

MSC: 14M15, 15B34, 94B05

1 Introduction

The Lagrangian–Grassmannian variety (LG–variety) $L(n, 2n)$ parametrizes the set of all maximal isotropic subspaces of a symplectic vector space E of dimension $2n$ over arbitrary field $\mathbb{F}$. In [1] it was given for the first time a set of linear homogeneous polynomials $\Pi_{\alpha_{rs}}$ such that $L(n, 2n) = G(n, 2n) \cap Z(\Pi_{\alpha_{rs}})$, where $G(n, 2n)$ denote the Grassmannian variety, i.e., the linear section as a set of zeros of $\Pi_{\alpha_{rs}}$. In this paper we prove that there is $\Pi_{\alpha_{rs}}$ a unique linear homogeneous polynomials family, up to linear combination, such that annuls the set of its rational points.

On the other hand, in [4] it was shown that the linear functionals $\Pi_{\alpha_{rs}}$ can be grouped into a special type of Boolean matrices (matrices with components ones or zeros), with this we have Boolean matrices in the geometry of LG–variety. In this article, we emphasize that these matrices have importance by themselves, that is, they can be considered from the beginning and then study their properties. With this in mind, we show a connection between the LG–variety geometry defined on a finite field with q elements and the q –ary Low–Density Parity–Check codes, i.e., we give a way to build regular and irregular LDPC–codes in LG–variety. More precisely, we give the construction of two families of Boolean $\mathbb{F}_q$ –matrices ($(0, 1)$ –matrix in any field) and we prove that they are families of low density matrices. Specifically, for each n integer number, is constructed an irregular q –ary Low–Density Parity–Check code from $r = \lfloor \frac{n+2}{2} \rfloor$ regular q –ary Low–Density Parity–Check codes, where $\lfloor x \rfloor$ denote the greatest integer less than or equal to x . With this construction it is very possible to obtain coding and decodification algorithms of the irregular LDPC–code from coding and decodification algorithms of the regular LDPC–codes.

The paper is organized as follows. In section 2 we give the construction of two special classes of $(0, 1)$ –matrices $\mathcal{L}_k$ and B which are key in the development of the work and we characterize when these matrices has maximum rank whenever its coefficients are considered in any field, see Theorem 6. In section 3 we see that

*Corresponding Author: **Jesús Carrillo–Pacheco:** Academia de Matemáticas, Universidad Autónoma de la Ciudad de México, 09390. Ciudad de México, México, E-mail: jesus.carrillo@uacm.edu.mx

Fausto Jarquín–Zárate: Academia de Matemáticas, Universidad Autónoma de la Ciudad de México, 09390. Ciudad de México, México, E-mail: fausto.jarquin@uacm.edu.mx

the $(0, 1)$ -matrices $\mathcal{L}_k$ and B are associated with the q -ary Low-Density Parity-Check codes (LDPC-codes). In section 4 we proof that there is a unique linear homogeneous polynomials family, up to linear combination, such that annuls the set of its rational points, see Theorem 16. We also show that using the matrices $\mathcal{L}_k$ and the rule to construct the matrix B we can give a matrix invariant to each symplectic vector space of finite dimension.

2 Construction of a class $(0, 1)$ -matrices.

Let $A = (a_{ij})$ be an $n \times m$ matrix with coefficients in arbitrary field $\mathbb{F}$. If every entry $a_{ij} \in \{0, 1\}$, then A is called $(0, 1)$ -matrix (or a *Boolean matrix*). In this section we give the construction of a special class of $(0, 1)$ -matrices which are key in the development of this work.

Throughout this paper I_s will denote the $s \times s$ identity matrix, and we denote by $C_b^a = \binom{a}{b}$ a binomial coefficient. For any integer $s \geq 1$, write $\mathbf{s} = (1, \dots, 1)$ a row matrix with s entries equal to 1. For arbitrary integer $k \geq 1$ define the $(k+1) \times C_2^{k+1}$ matrix A_k^0 as

$$A_k^0 = \begin{pmatrix} \boxed{k} & & & & & \\ & \boxed{k-1} & & & & \\ & & \ddots & & & \\ & & \dots & \boxed{3} & & \\ & & \dots & & \boxed{2} & \\ & & \dots & & & \boxed{1} \\ I_k & I_{k-1} & \dots & I_3 & I_2 & I_1 \end{pmatrix},$$

where $I_k, I_{k-1}, \dots, I_3, I_2, I_1$ are the corresponding identity matrices and the non-marked spaces on the upper right blocks are filled-in with zeroes. Now consider the following $(1+k+C_2^{k+1}) \times C_2^{k+1}$ matrix given by adding an identity matrix of size C_2^{k+1} in the bottom part of the above A_k^0 matrix, that is the matrix

$$A_k^0(I_{C_2^{k+1}}) = \begin{pmatrix} \boxed{k} & & & & & \\ & \boxed{k-1} & & & & \\ & & \ddots & & & \\ & & \dots & \boxed{3} & & \\ & & \dots & & \boxed{2} & \\ & & \dots & & & \boxed{1} \\ I_k & I_{k-1} & \dots & I_3 & I_2 & I_1 \\ \hline & & & & & I_{C_2^{k+1}} \end{pmatrix}.$$

Next, define the block stepped matrix A_k^1 by joining the matrices $A_k^0(I_{C_2^{k+1}})$ side-by-side and aligning the bottoms of the corresponding identity matrices, that is

$$A_k^1 = A_k^0(I_{C_2^{k+1}}) \sqcup A_{k-1}^0(I_{C_2^k}) \sqcup \dots \sqcup A_2^0(I_{C_2^2}) \sqcup A_1^0(I_{C_2^2}),$$

where $\sqcup$ means joining together side-by-side and aligning the bottoms of the corresponding identity matrices and filling the non-marked spaces on the upper right blocks with zeroes. Notice that this is a matrix of size

$$(k+1+C_2^{k+1}) \times (C_2^{k+1} + C_2^k + \dots + C_2^3 + C_2^2) = (k+1+C_2^{k+1}) \times C_3^{k+2}.$$

Then, define the matrix $A_k^1(I_{C_3^{k+2}})$ obtained by adding the identity matrix $I_{C_3^{k+2}}$ to the bottom of A_k^1 . Thus, $A_k^1(I_{C_3^{k+2}})$ is a matrix of size $(k+1+C_2^{k+1}+C_3^{k+2}) \times C_3^{k+2}$. We iterate these constructions to obtain matrices

$A_k^2, A_k^3, \dots, A_k^m, \dots$ and $A_k^2(I_{C_4^{k+3}}), A_k^3(I_{C_5^{k+4}}), \dots, A_k^m(I_{C_{m+2}^{k+m+1}}), \dots$. Explicitly, for any integer $\ell \geq 0$ the matrix $A_k^{\ell+1}$ is given by

$$A_k^{\ell+1} = A_k^\ell \left(I_{C_{\ell+2}^{k+\ell+1}} \right) \sqcup A_{(k-1)}^\ell \left(I_{C_{\ell+2}^{k+\ell}} \right) \sqcup \dots \sqcup A_2^\ell \left(I_{C_{\ell+2}^{\ell+3}} \right) \sqcup A_1^\ell \left(I_{C_{\ell+2}^{\ell+2}} \right),$$

where, as before, $\sqcup$ means joining together side-by-side and aligning the bottoms of the corresponding identity matrices, and filling the non-marked spaces on the upper right blocks with zeroes.

2.1 A special class of $(0, 1)$ -matrices $\mathcal{L}_k$

Assume that $n \geq 4$ is an even integer and consider all even integers m such that $4 \leq m \leq n$. For $k = 2$, choose a $(0, 1)$ -matrix $\mathcal{L}_2$ of size $1 \times C_n^{2n}$ having two entries equal to 1 and the remaining ones equal to 0. Now, for $k = (m+2)/2$, let $\mathcal{L}_k$ be the $(0, 1)$ -matrix given by

$$\mathcal{L}_k = A_k^{k-3},$$

where we observe that its number of rows is

$$1 + C_1^k + C_2^{k+1} + \dots + C_{k-3}^{2k-4} + C_{k-2}^{2k-3} = C_{k-2}^{2k-2} = C_{(m-2)/2}^m,$$

and its number of columns is

$$C_{k-2}^{2k-3} + C_{k-2}^{2k-4} + \dots + C_{k-2}^{k-1} + C_{k-2}^{k-2} = C_{k-1}^{2k-2} = C_{m/2}^m.$$

Remark 1. The $(0, 1)$ -matrix $\mathcal{L}_k$ has $k = (m+2)/2$ ones in each row, and has $k-1$ ones in each column. Also it is easy to see that the matrix $\mathcal{L}_{k-1}$ it is immersed in $\mathcal{L}_k$.

2.2 The $(0, 1)$ -matrix B

Here given an integer n and considering its parity, we give a rule $\mathcal{R}$ to construct a matrix B , diagonal by block of order $\binom{2n}{n-2} \times \binom{2n}{n}$. Explicitly, $\mathcal{R}_1$ refers to the rule for n even number and $\mathcal{R}_2$ refers to the rule for n odd number.

Rule 1) $\mathcal{R}_1$: For $n \geq 4$ even integer, $r_1 = (n+2)/2$ and $1 \leq k \leq r_1 - 2$. We define the following set of indices

$$M_k = \{(a_1, \dots, a_{2k}) : a_i + a_j \neq 2n+1, 1 \leq a_1 < \dots < a_{2k} \leq 2n\},$$

and $m_k = |M_k|$ denotes the number of elements of M_k . Then we define a matrix B of order $\binom{2n}{n-2} \times \binom{2n}{n}$ diagonal by blocks as follows

$$B = \mathcal{L}_{r_1} \oplus \bigoplus_{i=1}^{m_1} \mathcal{L}_{r_1-1}^i \oplus \dots \oplus \bigoplus_{i=1}^{m_{r_1-2}} \mathcal{L}_2^i$$

that is

$$B = \begin{pmatrix} \boxed{\mathcal{L}_{r_1}} & & & & & & \\ & \boxed{\mathcal{L}_{r_1-1}} & & & & & \\ & & \ddots & & & & \\ & & & 0 & & & \\ & & & & \boxed{\mathcal{L}_{r_1-1}} & & \\ & & & & & \ddots & \\ & & & & & & \boxed{\mathcal{L}_2} \\ & & & & & & & \ddots \\ & & & & & & & & \boxed{\mathcal{L}_2} \end{pmatrix},$$

where $\mathcal{L}_{k+1}^i \cong \mathcal{L}_{k+1}$ (are equivalent) for $1 \leq k \leq r_1 - 2$ and $1 \leq i \leq m_k$ with $1 \leq t \leq r_1 - 2$.

Rule 2) $\mathcal{R}_2$: For $n \geq 5$ odd integer, $r_2 = (n+1)/2$ and $1 \leq k \leq r_2 - 3$. We define the following set of indices

$$N_k = \{(a_1, \dots, a_{2k+1}) : a_i + a_j \neq 2n+1, 1 \leq a_1 < \dots < a_{2k+1} \leq 2n\},$$

and $n_k = |N_k|$ denotes the number of elements of N_k . Then we define a matrix B of order $\binom{2n}{n-2} \times \binom{2n}{n}$ diagonal by blocks as follows

$$B = \mathcal{L}_{r_2}^{\{n\}} \oplus \bigoplus_{i=1}^{n_1} \mathcal{L}_{r_2-1}^i \oplus \dots \oplus \bigoplus_{i=1}^{n_{r_2-3}} \mathcal{L}_2^i$$

where $\mathcal{L}_{r_2}^{\{n\}} := \mathcal{L}_{r_2} \oplus \dots \oplus \mathcal{L}_{r_2}$ n -times and $\mathcal{L}_{k+1}^\ell \cong \mathcal{L}_{k+1}$ (are equivalent) for $1 \leq k \leq r_2 - 2$ and $1 \leq \ell \leq n_t$ with $1 \leq t \leq r_2 - 3$, that is

$$B = \begin{pmatrix} \boxed{\mathcal{L}_{r_2}} & & & & & \\ & \ddots & & & & \\ & & \boxed{\mathcal{L}_{r_2}} & & & 0 \\ & 0 & & \boxed{\mathcal{L}_{r_2-1}} & & \\ & & & & \ddots & \\ & & & & & \boxed{\mathcal{L}_{r_2-1}} \\ & & & & & & \ddots \\ & & & & & & & \boxed{\mathcal{L}_2} \\ & & & & & & & & \ddots \\ & & & & & & & & & \boxed{\mathcal{L}_2} \end{pmatrix}.$$

Example 2. If $m = 4$, then $k = \frac{4+2}{2} = 3$. By definition

$$\mathcal{L}_3 = A_3^0 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Example 3. If $m = 6$, then $k = \frac{6+2}{2} = 4$. Using the definition

$$\mathcal{L}_4 = A_4^1 = A_4^0(I_{C_2^5}) \sqcup A_3^0(I_{C_2^4}) \sqcup A_2^0(I_{C_2^3}) \sqcup A_1^0(I_{C_2^2})$$

that is

$$\mathcal{L}_4 = \begin{pmatrix} \boxed{A_4^0} & & & & \\ & \boxed{A_3^0} & & & \\ & & \boxed{A_2^0} & & \\ & & & \boxed{1} & \\ & & & \boxed{1} & \\ I_{10} & I_6 & I_3 & \boxed{1} & \end{pmatrix}.$$

Remark 4. Note that the matrix B is of combinatorial construction based over the sets M_k and N_k .

Remark 5. It is well known that an invariant of a matrix is its rank, a natural question is, what are the values of the rank (B) and rank ($\mathcal{L}_k$) when its coefficients are considered in an arbitrary field $\mathbb{F}$?

In this regard we have the following

Theorem 6. Let $n \geq 4$ be a positive integer and $r = \lfloor \frac{n+2}{2} \rfloor$, where $\lfloor x \rfloor$ denote the greatest integer less than or equal to x . Then the following conditions are equivalent:

- 1) $\text{Rank}(\mathcal{L}_k) = C_{\frac{m-2}{2}}^m$ where $k = \lfloor \frac{m+2}{2} \rfloor$ and $2 \leq m \leq 2r-2$, i.e., has maximum rank.
 2) $\text{rank}(B) = C_{n-2}^{2n}$, i.e., has maximum rank.
 3) $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) \geq r$.

Proof. (1) $\Leftrightarrow$ (2) By definition B is a diagonal blocks matrix, then B has maximum rank if and only if each $\mathcal{L}_k$ has maximum rank.

(1) $\Rightarrow$ (3) Induction over k . For $k = 2$ tautologically fulfilled. If $k = 3$ then

$$\mathcal{L}_3 \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & -2 & -2 & -2 \end{pmatrix},$$

which implies $\text{rank}(\mathcal{L}_3) = 4$ if and only if $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) \geq 3$. Recall $k = \lfloor \frac{m+2}{2} \rfloor$ with $2 \leq m \leq 2r-2$, then our induction hypothesis is: if $\text{rank}(\mathcal{L}_k)$ is maximum then $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) \geq r-1$, for all $2 < k \leq r-1$. Suppose $\text{rank}(\mathcal{L}_r) = C_{\frac{n-2}{2}}^n$ is maximum. By Remark 1 we have $\mathcal{L}_{k-1}$ it is immersed in the matrix $\mathcal{L}_k$ for all $3 \leq k \leq r$ and by induction hypothesis we have that $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) \geq r-1$. Note that $\mathcal{L}_r$ it is of order $C_{\frac{n-2}{2}}^n \times C_{\frac{n}{2}}^n$, we define the matrix $(\mathcal{L}_r)^T$ of order $(C_{\frac{n-2}{2}}^n - 1) \times C_{\frac{n}{2}}^n$ removing from the matrix $\mathcal{L}_r$ the first row. We now define the following matrix

$$\begin{pmatrix} r-1 & \cdots & r-1 \\ (\mathcal{L}_r)^T \end{pmatrix},$$

using the fact that $\mathcal{L}_r$ has $r-1$ ones in each column (see Remark 1) and by elementary operations of matrices (adding all the rows to the first row) we have

$$\mathcal{L}_r \sim \begin{pmatrix} r-1 & \cdots & r-1 \\ (\mathcal{L}_r)^T \end{pmatrix}.$$

Since $\mathcal{L}_r$ has maximum rank and by induction hypothesis $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) \geq r-1$, then $r-1 \neq 0$ thus we obtain that $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) \geq r$.

(3) $\Rightarrow$ (1) Suppose $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) > r-1$. Applying elementary row operations on $\mathcal{L}_r$, it is easy to see that

$$\mathcal{L}_r \sim \left(\begin{array}{c|c} Id & R \\ \hline 0, \dots, 0 & r-1, \dots, r-1 \end{array} \right) =: \overline{\mathcal{L}_k}$$

where $R = (R_{ij})$ it is a matrix of order $(C_{\frac{n-2}{2}}^n - 1) \times (C_{\frac{n}{2}}^n - (C_{\frac{n-2}{2}}^n - 1))$, denote by $K = C_{\frac{n-2}{2}}^n - 1$ and $J = C_{\frac{n}{2}}^n - (C_{\frac{n-2}{2}}^n - 1)$. Let $N = C_{\frac{n-2}{2}}^n$ and $\{R_1, \dots, R_N\}$ the set of N -array rows $\overline{\mathcal{L}_k}$. Let $\alpha_1, \dots, \alpha_N$ scalars such that $\alpha_1 R_1 + \dots + \alpha_N R_N = 0$ is a linear combination. We have that

$$\begin{aligned} \alpha_1 R_1 + \dots + \alpha_N R_N &= (\alpha_1, 0, \dots, 0, \alpha_1 R_{11}, \alpha_1 R_{12}, \dots, \alpha_1 R_{1J}) + \\ &\quad (0, \alpha_2, 0, \dots, 0, \alpha_2 R_{21}, \alpha_2 R_{22}, \dots, \alpha_2 R_{2J}) + \\ &\quad \vdots \quad \quad \quad \vdots \\ &\quad (0, \dots, 0, \alpha_i, 0, \dots, 0, \alpha_i R_{i1}, \alpha_i R_{i2}, \dots, \alpha_i R_{iJ}) + \\ &\quad \vdots \quad \quad \quad \vdots \\ &\quad (0, \dots, 0, \alpha_{N-1}, \alpha_{N-1} R_{N-11}, \alpha_{N-1} R_{N-12}, \dots, \alpha_{N-1} R_{N-1J}) + \\ &\quad (0, \dots, 0, \alpha_N(r-1), \alpha_N(r-1), \dots, \alpha_N(r-1)) = \\ &\quad (\alpha_1, \dots, \alpha_{N-1}, \sum_{i=1}^{N-1} \alpha_i R_{i1} + (r-1)\alpha_N, \sum_{i=1}^{N-1} \alpha_i R_{i2} + (r-1)\alpha_N, \end{aligned}$$

$$\dots, \sum_{i=1}^{N-1} \alpha_i R_{i,N-1} + (r-1)\alpha_N = (0, 0, \dots, 0),$$

thus $\alpha_1 = \alpha_2 = \dots = \alpha_{N-1} = 0$, this is $\sum_{i=1}^{N-1} \alpha_j R_{1i} + (r-1)\alpha_N = 0$ for all $j = 1, \dots, N-1$ which implies $(r-1)\alpha_N = 0$, that is to say $\alpha_N = 0$. Therefore $\{R_1, \dots, R_N\}$ is a set linearly independent for $1 \leq N \leq C_{\frac{n-2}{2}}^n$. $\square$

The following example clarify the construction of the matrix B and notation of Theorem 6.

Example 7. For $n = 7$ and $r = \lfloor \frac{7+2}{2} \rfloor = 4$, we have

$$B = \mathcal{L}_4^{\{7\}} \oplus \bigoplus_{i=1}^{301} \mathcal{L}_3^i \oplus \bigoplus_{i=1}^{693} \mathcal{L}_2^i.$$

Thus, in B there are 7 submatrices $\mathcal{L}_4$, 301 submatrices $\mathcal{L}_3$ and 693 submatrices $\mathcal{L}_2$, that is,

$$B = \begin{pmatrix} \boxed{\mathcal{L}_4} & & & & & & 0 \\ & \ddots & & & & & \\ & & \boxed{\mathcal{L}_4} & & & & \\ & & & \boxed{\mathcal{L}_3} & & & \\ 0 & & & & \ddots & & \\ & & & & & \boxed{\mathcal{L}_3} & \\ & & & & & & \boxed{\mathcal{L}_2} \\ & & & & & & \ddots \\ & & & & & & & \boxed{\mathcal{L}_2} \end{pmatrix}$$

Also a direct calculation shows that

$\#(\mathbb{F})$	$\text{char}(\mathbb{F})$	$\text{rank}(\mathcal{L}_3)$	$\text{rank}(\mathcal{L}_4)$	$\text{rank}(B)$
∞	0	4	15	2002
2	2	3	10	1666
3	3	4	14	1995
2^2	2	3	10	1666
$q \geq 5$	p	4	15	2002

Keep the notation of Theorem 6, note that $\text{rank}(B) = C_5^{14} = 2002$ iff $\text{rank}(\mathcal{L}_4) = C_2^6 = 15$ and $\text{rank}(\mathcal{L}_3) = C_1^4 = 4$ iff $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) \geq \lfloor \frac{7+2}{2} \rfloor = 4$. That is B , $\mathcal{L}_4$ and $\mathcal{L}_3$ has maximum rank iff $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) = p \geq 4$.

Remark 8. If the matrix B and $\mathcal{L}_k$ has coefficients in any field $\mathbb{F}$, then the values of its ranks depends on $\text{char}(\mathbb{F})$.

3 LDPC codes associated with matrices $\mathcal{L}_k$ and B

A H matrix is called *Low Density Matrix* if containing mostly 0's and relatively few 1's, the *density* d of the matrix H is the quotient of the total number of ones in the matrix H between the order of the matrix. Let $\mathbb{F}_q$ be a finite field with q elements and q is a power of a prime number p . A q -ary Low-Density Parity-Check code (LDPC-code) is block code of length N , given by the null space over $\mathbb{F}_q$ of a sparse parity-check matrix H over $\mathbb{F}_q$. An LDPC-code is *regular* if the sparse parity-check matrix has in each column a fixed number i of 1's and each row a fixed number j of 1's, and the parameters of regular LDPC-code are (N, i, j) where N, i, j are as above. It is said to be *irregular* LDPC-code, if it is not regular. The Low-Density Parity-Check (LDPC)

codes are a type of linear code whose main characteristic is that its Parity Checking Matrix is scattered i.e., it is a binary matrix that has few ones and many zeros, see [6].

Throughout this section we keep the notation of section 2. The matrix $\mathcal{L}_k$ has order $C_{\frac{m-2}{2}}^m \times C_{\frac{m}{2}}^m$ and the quantity of ones in the matrix $\mathcal{L}_k$ is given by $kC_{\frac{m-2}{2}}^m$, the density d of ones in $\mathcal{L}_k$ is given by

$$d = \frac{kC_{\frac{m-2}{2}}^m}{(C_{\frac{m-2}{2}}^m)(C_{\frac{m}{2}}^m)} = \frac{k}{C_{\frac{m}{2}}^m} = \frac{\lfloor \frac{m+2}{2} \rfloor}{C_{\frac{m}{2}}^m}.$$

Clearly

$$\lim_{m \rightarrow \infty} \frac{\lfloor \frac{m+2}{2} \rfloor}{C_{\frac{m}{2}}^m} = 0.$$

Thus we have demonstrate the following.

Lemma 9. Let $2 \leq m \leq n$ be and $k = \lfloor \frac{m+2}{2} \rfloor$. Then the matrices $\mathcal{L}_k$ are low density matrix.

Theorem 10. The matrices $\mathcal{L}_k$ with $k = \lfloor \frac{m+2}{2} \rfloor$, $2 \leq m \leq n$ and $r = \lfloor \frac{n+2}{2} \rfloor$ are matrices checking parity of a regular LDPC code with parameters $(C_m^{2m}, k-1, k)$, and has $C_{\frac{m}{2}}^m - C_{\frac{m-2}{2}}^m$ information digits for all $2 \leq k \leq r$ iff $\text{char}(\mathbb{F}_q) \geq r$.

Proof. The code $C_{\mathcal{L}_k} = \{x : \mathcal{L}_k \cdot x^T = 0\}$ have matrix $\mathcal{L}_k$ as parity check matrix, by the Lemma 9, $\mathcal{L}_k$ it is low density matrix, then $C_{\mathcal{L}_k}$ is a regular LDPC code (see Remark 1). By Theorem 6 we obtain $\mathcal{L}_k$ has maximum rank iff $\text{char}(\mathbb{F}_q) \geq r$. $\square$

Proposition 11. With the notation of subsection 2.2, B is a low density matrix.

Proof. Since the direct sum of low-density matrices is low density, the result is followed by Lemma 9. $\square$

Theorem 12. The matrix B is parity check matrix of a irregular LDPC codes with parameters $(C_n^{2n}, r-1, r)$, the code has $C_{\frac{n}{2}}^n - C_{\frac{n-2}{2}}^n$ information digits iff $\text{char}(\mathbb{F}_q) \geq r$.

Proof. It follows from the Proposition 11 and Theorem 6. $\square$

Remark 13. Note that the dimension of the q -ary Low-Density Parity–Check codes $C_{\mathcal{L}_k}$ and C_B depend strongly of the characteristics of the field.

Remark 14. For each n integer number, is constructe an irregular q -ary Low–Density Parity–Check code from $r = \lfloor \frac{n+2}{2} \rfloor$ regular q -ary Low–Density Parity–Check codes. With this construction it is very possible to obtain coding and decodification algorithms of the irregular LDPC–code from coding and decodification algorithms of the regular LDPC–codes.

4 A characterization of the linear homogeneous polynomials that annuls the rational points LG-variety

If we assign an appropriate coordinate system we can show that each row of the matrix B can be seen as a linear functional of type (1), see below. In this section we will show, as a main result, that these linear functional are unique, up to linear combination, such that annul the Lagrangian–Grassmannian variety.

In the sequel $E = (E, \langle \cdot, \cdot \rangle)$ will be a symplectic vector space i.e., E is a $2n$ -dimensional vector space over $\mathbb{F}_q$ and $\langle \cdot, \cdot \rangle$ is a symplectic form on E . The Grassmannian $G(n, 2n)$ is an algebraic variety and can be embedded in a projective space $\mathbb{P}^{c-1}$ where $c = \binom{2n}{n}$, by the Plücker embedding. A subspace W of E is said

to be isotropic if $\langle x, y \rangle = 0$ for all $x, y \in W$. The Lagrangian-Grassmannian (LG), parameterizes to all the maximal isotropic subspaces of a symplectic vector space i.e.,

$$L(n, 2n) = \{U \leq E : U \text{ is isotropic and } \dim_{\mathbb{F}_q} U = n\}.$$

By choosing a basis $v_1, \dots, v_n$ for each $W \in G(n, 2n)$ and sending this basis to (the equivalence class of) $v_1 \wedge \dots \wedge v_n \in \mathbb{P}(\wedge^n E)$ to have the following description of the Grassmannian

$$G(n, 2n) = \{v_1 \wedge \dots \wedge v_n \in \mathbb{P}(\wedge^n E) : v_1, \dots, v_n \text{ are linearly independent}\}$$

and hence the Lagrangian-Grassmannian is given by

$$L(n, 2n) = \{v_1 \wedge \dots \wedge v_n \in G(n, 2n) : \langle v_i, v_j \rangle = 0, 1 \leq i < j \leq n\}.$$

For integers $k < m$ define the set

$$I(k, m) = \{\alpha = (\alpha_1, \dots, \alpha_k) : 1 \leq \alpha_1 < \dots < \alpha_k \leq m\}.$$

Let $\alpha = (\alpha_1, \dots, \alpha_k) \in I(k, m)$, we define the support of α as the set

$$\text{supp}(\alpha) = \{\alpha_1, \dots, \alpha_k\}.$$

Remark 15. Throughout this paper, we must consider $\alpha = (\alpha_1, \dots, \alpha_k) \in I(k, m)$ means to a permutation on the indices of α .

Now, for $\alpha = (\alpha_1, \dots, \alpha_k) \in I(k, m)$ write

$$\begin{aligned} w_\alpha &:= w_{\alpha_1} \wedge \dots \wedge w_{\alpha_k}, \\ w_{\alpha_{rs}} &:= w_{\alpha_1} \wedge \dots \wedge \widehat{w}_{\alpha_r} \wedge \dots \wedge \widehat{w}_{\alpha_s} \wedge \dots \wedge w_{\alpha_k}, \end{aligned}$$

where $\widehat{a}$ means that the corresponding term is omitted.

For $w \in \wedge^k E$ written in Plücker coordinates as $w = \sum_{\alpha \in I(k, m)} P_\alpha w_\alpha$, and for $\alpha_{st} \in I(k-2, m)$ define the linear polynomials which we call *symplectic linear relations* given by

$$\Pi_{\alpha_{st}} := \sum_{i=1}^k c_{i, \alpha_{rs}, 2n-i+1} X_{i, \alpha_{rs}, 2n-i+1}, \quad (1)$$

$$\text{with } c_{i, \alpha_{rs}, 2n-i+1} = \begin{cases} 1 & \text{if } |\text{supp}\{i, \alpha_{rs}, 2n-i+1\}| = k, \\ 0 & \text{otherwise,} \end{cases}$$

where $\text{supp}(\beta) = \{\beta_1, \dots, \beta_k\}$ for $\beta = (\beta_1, \dots, \beta_k) \in I(k, m)$.

In the rest of this section we consider $m = 2n$ and $k = n-2$. Below we define the contraction mapping $f : \wedge^n E \rightarrow \wedge^{n-2} E$ as $v_1 \wedge \dots \wedge v_n \mapsto \sum_{1 \leq r < s \leq n} \langle v_r, v_s \rangle v_{rs}$. It is shown in [1, Section 3] that

$$L(n, 2n) = G(n, 2n) \cap \mathbb{P}(\ker f).$$

Moreover $w \in \ker f$ if and only if $\sum_{i=1}^n P_{i\alpha_{rs} 2n-i+1} = 0$ for all $\alpha_{rs} \in I(n, 2n)$, where $P_{i\alpha_{st}(2n-i+1)} := P_{i\alpha_1 \dots \widehat{\alpha_r} \dots \widehat{\alpha_s} \dots \alpha_n(2n-i+1)}$ is element in $\mathbb{F}$.

With this notation, the generators of $\ker f$ are the polynomials $\Pi_{\alpha_{st}}$, with $\alpha_{rs} \in I(k-2, m)$. On the other hand, if $w = \sum_{\alpha \in I(k, m)} P_\alpha w_\alpha \in \mathbb{P}(\wedge^k E)$, then $w \in G(n, E)$ if and only if for each pair of successions $1 \leq \alpha_1 < \dots < \alpha_{k-1} \leq m$ and $1 \leq \beta_1 < \dots < \beta_{k-1} \leq m$ the Plücker coordinate of w satisfy the quadratic relation see [5, Section 4].

$$\sum_{i=1}^{k+1} (-1)^i P_{\alpha_1 \dots \alpha_{k-1} \beta_i} P_{\beta_1 \beta_2 \dots \widehat{\beta_i} \dots \beta_{k+1}} = 0,$$

where the index $\widehat{\beta}_i$ means that the corresponding term is omitted. The quadratic equation

$$Q_{\alpha'\beta'} = \sum_{i=1}^{k+1} X_{\alpha_1 \dots \alpha_{k-1} \beta_i} X_{\beta_1 \beta_2 \dots \widehat{\beta}_i \dots \beta_{k+1}} \quad (2)$$

where $\alpha' \in I(k-1, m)$ and $\beta' \in I(k+1, m)$ are called *Plücker relation (quadratic)*.

So have characterization of $L(n, 2n)$, as the common zeros of the quadratic polynomials $Q_{\alpha'\beta'}$ and the symplectic linear relations $\Pi_{\alpha_{rs}}$, that is

$$L(n, 2n) = \mathbb{Z}\langle Q_{\alpha'\beta'}, \Pi_{\alpha_{rs}} \rangle \quad (3)$$

where $\alpha' \in I(n-1, 2n)$, $\beta' \in I(n+1, 2n)$ and $\alpha_{rs} \in I(n-2, 2n)$.

Theorem 16. *With the above notation, the are unique linear homogeneous polynomials h in the dual space $(\wedge^n E)^*$ that vanish over the set of $\mathbb{F}_q$ -rational points $L(n, 2n)(\mathbb{F}_q)$ are linear combinations of*

$$\{\Pi_{\alpha_{rs}} : \alpha_{rs} \in I(n-2, 2n)\}.$$

Proof. By induction on n , assume first that $n = 2$. Then,

$$I(2, 4) = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$$

and notice that $\{e_{12}, e_{13}, e_{24}, e_{34}\} \subseteq L(2, 4)(\mathbb{F}_q)$ since they are totally decomposable and isotropic. Now, if $h \in (\wedge^2 E)^*$ vanishes on $L(2, 4)(\mathbb{F}_q)$, then $L(2, 4)(\mathbb{F}_q) \subseteq Z(h, \Pi)$, where $\Pi = X_{14} + X_{23}$. Suppose that $h = A_{12}X_{12} + A_{13}X_{13} + A_{14}X_{14} + A_{23}X_{23} + A_{24}X_{24} + A_{34}X_{34}$. Since $h(L(2, 4)(\mathbb{F}_q)) = 0$, then $h = A_{14}X_{14} + A_{23}X_{23}$. By [2], $w = (1, 0, 1, -1, 0, 1) \in L(2, 4)(\mathbb{F}_q)$ and thus $h(w) = A_{14} - A_{23} = 0$, that is $A_{14} = A_{23} =: A$, and consequently $h = A(X_{14} + X_{23}) = A\Pi$, show the case $n = 2$.

Now, our induction hypothesis is: For all $k < n$, every $h \in (\wedge^k E)^*$ such that $L(k, 2k)(\mathbb{F}_q) \subseteq Z(h, \Pi_{\alpha_{rs}} : \alpha_{rs} \in I(k-2, 2k))$, must be of the form $h = \sum A_{\alpha_{rs}} \Pi_{\alpha_{rs}}$, for $\alpha_{rs} \in I(k-2, 2k)$. Assume that $h \in (\wedge^n E)^*$ and $L(n, 2n)(\mathbb{F}_q) \subseteq Z(h, \Pi_{\alpha_{rs}} : \alpha_{rs} \in I(n-2, 2n))$. If $h \in \langle \Pi_{\alpha_{rs}} : \alpha_{rs} \in I(n-2, 2n) \rangle$, we finish the proof. Otherwise, write $h = \sum_{\alpha \in I(n, 2n)} A_{\alpha} X_{\alpha}$, with $A_{\bar{\alpha}} \neq 0$, where $\bar{\alpha} = (\bar{\alpha}_1, \dots, \bar{\alpha}_k, \dots, \bar{\alpha}_n) \in I(n, 2n)$ is a fixed index and $\bar{\alpha}_k$ is chosen arbitrarily and without loss of generality we can suppose that $1 \leq \bar{\alpha}_k \leq n$. Then usual basis e_{α} of $\wedge^n E$, for $\alpha \in I(n, 2n)$, can be written as

$$\mathcal{B} = \{e_{(\beta, \bar{\alpha}_k)} : \beta \in I(n-1, 2n-2), \{\bar{\alpha}_k, 2n - \bar{\alpha}_k + 1\} \not\subseteq \text{supp}(\beta)\} \cup \{e_{\alpha} : \alpha \in \Phi^c\}$$

where $\Phi = \{(\beta, \bar{\alpha}_k) \in I(n-1, 2n-2) : \{\bar{\alpha}_k, 2n - \bar{\alpha}_k + 1\} \not\subseteq \text{supp}(\beta)\}$ and $\Phi^c = \{\alpha \in I(n, 2n) : \{\bar{\alpha}_k, 2n - \bar{\alpha}_k + 1\} \subseteq \text{supp}(\alpha)\}$. Then,

$$h = \sum_{(\beta, \bar{\alpha}_k) \in \Phi} A_{(\beta, \bar{\alpha}_k)} X_{(\beta, \bar{\alpha}_k)} + \sum_{\alpha \in \Phi^c} A_{\alpha} X_{\alpha}.$$

Let

$$h' = \sum_{(\beta, \bar{\alpha}_k) \in \Phi} A_{(\beta, \bar{\alpha}_k)} X_{(\beta, \bar{\alpha}_k)} \quad \text{and} \quad h'' = \sum_{\alpha \in \Phi^c} A_{\alpha} X_{\alpha},$$

where clearly $h', h'' \in (\wedge^n E)^*$ and $h = h' + h''$. Let ℓ be the isotropic line generated by $e_{\bar{\alpha}_k}$ and let $U(\ell) = \{L \in L(n, 2n) : \ell \subseteq L\}$. We may identify $U(\ell)$ with the Lagrangian-Grassmannian $L(n-1, \ell^{\perp}/\ell) \simeq L(n-1, 2n-2)$. Consider the map

$$- \wedge e_{\bar{\alpha}_k} : \wedge^{n-1} E \rightarrow \wedge^n E$$

given by wedging with $e_{\bar{\alpha}_k}$ on basis elements and then extending linearly. Composing this map with the contraction $f : \wedge^n E \rightarrow \wedge^{n-2} E$, explicitly we have, for $\sum_{\beta \in I(n-1, 2n-2)} p_{\beta} e_{\beta} \in \wedge^{n-1} E$,

$$\wedge \left(\sum_{\beta \in I(n-1, 2n-2)} p_{\beta} e_{\beta} \right) \wedge e_{\bar{\alpha}_k} = \sum_{\beta \in I(n-1, 2n-2)} p_{(\beta, \bar{\alpha}_k)} (e_{\beta} \wedge e_{\bar{\alpha}_k})$$

$$= \sum_{\beta \in I(n-1, 2n-2)} p_{(\beta, \bar{\alpha}_k)} e_{(\beta, \bar{\alpha}_k)} =: w \in \wedge^n E,$$

where the $\bar{\alpha}_k$ in the sums satisfy that $\bar{\alpha}_k \notin \text{supp}(\beta)$, clearly $L(n-1, \ell^\perp/\ell) = -\wedge e_{\bar{\alpha}_k}(L(n-1, 2(n-1)))$. Applying f we obtain

$$\begin{aligned} f(w) &= \sum_{\beta \in I(n-1, 2n-2)} p_{(\beta, \bar{\alpha}_k)} f(e_{(\beta, \bar{\alpha}_k)}) \\ &= \sum_{\beta \in I(n-1, 2n-2)} p_{(\beta, \bar{\alpha}_k)} \left(\sum_{1 \leq r < s \leq n} \langle e_{\alpha_r}, e_{\alpha_s} \rangle e_{(\beta, \bar{\alpha}_k)_{rs}} \right) \\ &= \sum_{1 \leq r < s \leq n} \left(\sum_{1 \leq \varphi_1 < \varphi_2 \leq n} p_{(\beta_{rs}, \bar{\alpha}_k)_{\varphi_1 \varphi_2}} \langle e_{\varphi_1}, e_{\varphi_2} \rangle \right) e_{(\beta_{rs}, \bar{\alpha}_k)}. \end{aligned}$$

Now, if $w \in \text{Im}(-\wedge e_{\bar{\alpha}_k}) \cap \ker f$, since the $e_{(\beta, \bar{\alpha}_k)_{rs}}$ are linearly independent, we must have that

$$\sum_{1 \leq \varphi_1 < \varphi_2 \leq n} p_{((\beta_{rs}, \bar{\alpha}_k)_{\varphi_1 \varphi_2})} \langle e_{\varphi_1}, e_{\varphi_2} \rangle = 0,$$

where $\langle e_{\varphi_1}, e_{\varphi_2} \rangle = 1$ if and only if $\varphi_1 + \varphi_2 = 2n+1$, that is if $\varphi_1 = i$, then $\varphi_2 = 2n-i+1$. Hence, the previous sum is $\sum_{i=1}^n p_{(i, (\beta_{rs}, \bar{\alpha}_k), 2n-i+1)} = 0$ for all $\beta_{rs} \in I(n-3, 2n-2)$, again for $\bar{\alpha}_k \notin \text{supp}(\beta_{rs})$, up to a permutation on the indexes. Therefore, $w \in L(n-1, \ell^\perp/\ell)$ satisfies the linear relations $\sum_{i=1}^n X_{(i, (\beta_{rs}, \bar{\alpha}_k), 2n-i+1)} = 0$, for all $\beta_{rs} \in I(n-3, 2n-2)$. Put $\Pi_{(\beta_{rs}, \bar{\alpha}_k)} := \sum_{i=1}^n X_{(i, (\beta_{rs}, \bar{\alpha}_k), 2n-i+1)}$. Clearly,

$$\{\Pi_{(\beta_{rs}, \bar{\alpha}_k)} : 1 \leq r < s \leq n, \beta_{rs} \in I(n-3, 2n-2)\} \subseteq \{\Pi_{\alpha_{rs}} : \alpha_{rs} \in I(n-2, 2n)\},$$

$$h'(L(n-1, \ell^\perp/\ell)(\mathbb{F}_q)) = h(U(\ell)(\mathbb{F}_q)) = 0,$$

and by the induction hypothesis

$$h' = \sum_{\beta \in I(n-1, 2n-2)} A_{(\beta, \bar{\alpha}_k)} X_{(\beta, \bar{\alpha}_k)} \in \langle \Pi_{\alpha_{rs}} : \alpha_{rs} \in I(n-2, 2n) \rangle,$$

where $\bar{\alpha}_k \notin \text{supp}(\beta)$ and $h' \neq 0$. Hence, applying the same process to h'' we have that $h'' = h'_1 + h'_2$ with $h'_1 \in \langle \Pi_{\alpha_{rs}} : \alpha_{rs} \in I(n-2, 2n) \rangle$. This process must finish in a finite number of steps. $\square$

Keep the above notation

$$\{Q_{\alpha', \beta'}\} \cup \{\Pi_{\alpha_{rs}}\} \quad (4)$$

where $\alpha' \in I(n-1, 2n)$, $\beta' \in I(n+1, 2n)$ and $\alpha_{rs} \in I(n-2, 2n)$, we call it set of *canonical equations* of Lagrangian-Grassmannian variety.

Example 17. The purpose of this example is to show how the matrix B is constructed from the linear homogeneous polynomials $\Pi_{\alpha_{rs}}$.

For $n = 6$ and $r = \lfloor \frac{6+2}{2} \rfloor = 4$ we have for the Lagrangian-Grassmannian $L(6, 12) = G(6, 12) \cap \mathbb{P}(\ker f)$. Let $P_i = (i, 13-i)$ for $i = 1, 2, \dots, 6$, $\Sigma_6 = \{P_1, P_2, \dots, P_6\}$, and $C_2(\Sigma_6)$ the set of all combinations of 6 objects taken 2 at a time. For $1 \leq \alpha_1 < \alpha_2 \leq 12$ such that $\alpha_1 + \alpha_2 \neq 13$, we define the following set

$$\Sigma\{\alpha_1, \alpha_2\} = \{(\alpha_1, \alpha_2, P_i) \mid i + \alpha_j \neq 13, \alpha_j + 13 - i \neq 13, j = 1, 2\}.$$

Now, for $1 \leq \alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 \leq 12$ such that $\alpha_i + \alpha_j \neq 13$, define

$$\Sigma\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{(\alpha_1, \alpha_2, \alpha_3, \alpha_4) : \alpha_i + \alpha_j \neq 13 \text{ with } 1 \leq i, j \leq 4\}.$$

then

$$I(4, 12) = C_2(\Sigma_6) \cup \left(\bigcup_{\substack{1 \leq \alpha_1 < \alpha_2 \leq 12 \\ \alpha_1 + \alpha_2 \neq 13}} \Sigma\{\alpha_1, \alpha_2\} \right) \cup \left(\bigcup_{\substack{1 \leq \alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 \leq 12 \\ \alpha_i + \alpha_j \neq 13}} \Sigma\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \right).$$

Moreover the matrix associated with the systems $\{\Pi_{\alpha_{rs}} : \alpha_{rs} \in \mathcal{C}_2(\Sigma_6)\}, \{\Pi_{\alpha_{rs}} : \alpha_{rs} \in \Sigma\{\alpha_1, \alpha_2\}\}$ and $\{\Pi_{\alpha_{rs}} : \alpha_{rs} \in \Sigma\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}\}$ are $\mathcal{L}_4, \mathcal{L}_3^{(\alpha_1, \alpha_2)} \cong \mathcal{L}_3$ for $1 \leq \alpha_1 < \alpha_2 \leq 12$ such that $\alpha_1 + \alpha_2 \neq 13$ and $\mathcal{L}_2^{(\alpha_1, \alpha_2, \alpha_3, \alpha_4)} \cong \mathcal{L}_2$ for $1 \leq \alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 \leq 12$ such that $\alpha_i + \alpha_j \neq 13$ respectively. Then

$$B = \mathcal{L}_4 \oplus \left(\bigoplus_{\substack{1 \leq \alpha_1 < \alpha_2 \leq 12 \\ \alpha_1 + \alpha_2 \neq 13}} \mathcal{L}_3^{(\alpha_1, \alpha_2)} \right) \oplus \left(\bigoplus_{\substack{1 \leq \alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 \leq 12 \\ \alpha_i + \alpha_j \neq 13}} \mathcal{L}_2^{(\alpha_1, \alpha_2, \alpha_3, \alpha_4)} \right)$$
$$= \begin{pmatrix} \boxed{\mathcal{L}_4} & & & & & \\ & \boxed{\mathcal{L}_3} & & & & \\ & & \ddots & & & \\ & & & \boxed{\mathcal{L}_3} & & \\ & & 0 & & \boxed{\mathcal{L}_2} & \\ & & & & & \ddots \\ & & & & & & \boxed{\mathcal{L}_2} \end{pmatrix},$$

where there are 60 submatrices $\mathcal{L}_3$, and 240 submatrices $\mathcal{L}_2$.

Remark 18. In the previous example, we can see that the matrix B associated to the set of linear homogeneous polynomials $\{\Pi_{\alpha_{rs}} \mid \alpha_{rs} \in I(4, 12)\}$ is composed of blocks of matrices $\mathcal{L}_4, \mathcal{L}_3$ and $\mathcal{L}_2$, this fragmentation is due to the fact that $I(4, 12)$ is expressed as a disjoint partition. Following the order of ideas, in general, for each n integer number, the set $I(n - 2, 2n)$ can be expressed as a disjoint partition and each part of this partition is associated with a subset of $\{\Pi_{\alpha_{rs}} \mid \alpha_{rs} \in I(n - 2, 2n)\}$, with this we obtain a description of the linear section of $L(n, 2n)$, all the details can be found in [4].

4.1 An invariant of a symplectic vector space

We define $\mathcal{A}(n) = (\mathcal{R}, \mathcal{L}_r, \dots, \mathcal{L}_2)$ an array of matrices, where $\mathcal{R}$ is the rule that allows to construct the matrix B as in section 2.2. Let E be a symplectic vector space of dimension $2n$ and denote by $[E]$ the class of symplectomorphism vector spaces to the symplectic vector space E .

Then the correspondence given by

$$\psi : [E] \mapsto \mathcal{A}(n)$$

satisfies the following.

Proposition 19. *ψ is an injective function.*

Proof. If (E_1, Ω_1) and (E_2, Ω_2) are two vector spaces symplectic morphisms, then $2n_1 = 2n_2$, that is $n_1 = n_2$ and $\mathcal{A}(n_1) = (\mathcal{R}_{n_1}, \mathcal{L}_{r_1}, \dots, \mathcal{L}_2) = (\mathcal{R}_{n_2}, \mathcal{L}_{r_2}, \dots, \mathcal{L}_2) = \mathcal{A}(n_2)$, this means that there is an invariant under symplectic morphisms. Suppose $\psi([E_1]) = \mathcal{A}(n_1) = \mathcal{A}(n_2) = \psi([E_2])$, then $r_1 = \lfloor \frac{n_1+2}{2} \rfloor = \lfloor \frac{n_2+2}{2} \rfloor = r_2$ which implies $n_1 = n_2$ or $n_2 = n_1 + 1$. If $n_1 = n_2$, then $E_1 \cong E_2$ (symplectic), because if $(W_1, \overline{W_1}), (W_2, \overline{W_2})$ are decompositions symplectic of E_1 and E_2 respectively, then each isomorphism $W_1 \cong W_2$ extends to a symplectic morphism f , i.e., $E_1 \cong E_2$. If $n_2 = n_1 + 1$, we obtain $\mathcal{R}_{n_1} \neq \mathcal{R}_{n_2}$, that is $\mathcal{A}(n_1) \neq \mathcal{A}(n_2)$. $\square$

Remark 20. We can say that $A(n) = (\mathcal{R}, \mathcal{L}_r, \dots, \mathcal{L}_2)$ is an invariant of a symplectic vector space of dimension $2n$. It follows from the content of the work, using $A(n) = (\mathcal{R}, \mathcal{L}_r, \dots, \mathcal{L}_2)$ we can construct: matrix B , LDPC codes and see to the LG-variety as $L(n, 2n) = G(n, 2n) \cap \mathbb{P}(\ker B)$.

Acknowledgement: We thank the anonymous referee for the careful reading of the manuscript. His/her remarks improved the presentation of the article. The authors were supported by Laboratorio de Cifrado y Codificación de la Información (LCCI) of Universidad Autónoma de la Ciudad de México (SLT-UACM).

References

- [1] J. Carrillo-Pacheco and F. Zaldivar, *On Lagrangian-Grassmannian Codes*, Designs, Codes and Cryptography 60 (2011) 291–268.
- [2] J. Carrillo-Pacheco, G. Vega, and F. Zaldivar. *The Weight Distribution of a Family of Lagrangian-Grassmannian Codes*, Lecture Notes on Computer Science, Vol. 9084 Springer Verlag (2015), 240–246.
- [3] J. Carrillo-Pacheco and F. Zaldivar, *On Codes over $FFN(1, q)$ -Projective Varieties*, Advances in Mathematics of Communications 10 No. 2 (2016) 209–220.
- [4] J. Carrillo-Pacheco, F. Jarquín-Zárate, M. Velasco-Fuentes and F. Zaldivar, *An Explicit Description in Terms of Plücker Coordinates of the Lagrangian-Grassmannian*. Submitted. Preprint: arXiv:1601.07501.
- [5] I. R. Shafarevich, *Basic Algebraic Geometry 1*, Second Edition, Springer-Verlag, 1994.
- [6] R.G. Gallager, *Low Density Parity Check Codes*, Monograph, MIT Press Retrieved August 7, 2013.