UNIVERSIDAD AUTÓNOMA METROPOLITANA

UNIDAD IZTAPALAPA

Casa abierta al tiempo

DIVISIÓN CIENCIAS BÁSICAS e INGENIERÍA

Posgrado en Ciencias

”Códigos Lagrangianos-Grassmannianos”

TESIS PARA OBTENER EL GRADO DE DOCTOR EN CIENCIAS (MATEMÁTICAS)

Que presenta: Jesús Carrillo Pacheco

MATRICULA: 206180460
jesus.carrillo2357@gmail.com
ORCI: 0000-0003-1555-4367

DIRECTOR

Dr. Felipe de Jesús Zaldívar Cruz

JURADO

PRESIDENTE

DR. XAVIER GOMEZ MONT

VOCAL

DR. MARIO PINEDA RUELAS

VOCAL

DR. PEDRO LUIS DEL ANGEL RODRIGUEZ

VOCAL

DR. GERARDO VEGA HERNÁNDEZ

SECRETARIO

DR. FELIPE DE JESÚS ZALDÍVAR CRUZ

México. D. F. 18 de Noviembre de 2011

Índice general

Capítulo 1

Resumen

Usando la variedad Lagrangianna-Grassmanniana, una variedad algebraica suave de dimensión $\frac{n(n+1)}{2}$ que parametriza subespacios isotropicos de dimensión n en un espacio vectorial simpléctico de dimensión $2n$ construimos una nueva clase de códigos lineales generados por esta variedad los códigos Lagrangiannos-Grassmannianos. También calculamos explicitamente la longitud de la palabra, una fórmula para la dimensión y una cota superior para la distancia mínima en terminos de la dimensión de la variedad Lagrangianna-Grassmanniana. Damos una relación entre los pesos grandes del código Lagrangianno-Grassmanniano y los pesos grandes del código de Grassmann. Desmostramos ademas que el código Lagrangianno-Grassmanniano como el código de Schubert son casos particulares de códigos inducidos por variedades proyectivas las cuales son la intersección de una variedad proyectiva arbitraria y una variedad lineal.

Introducción

El problema central de la Teoria de Codigos es como trasmitir información traves de un canal poco fiable, es decir aquel canal que tiene la posibilidad de que el mensaje llege alterado. En este caso se dice que el canal tiene ruido.[en]tendiendo por ruido no sólo lo que nos impide oir con claridad cuando se establece una conexión defectuosa, sino cualquier otra que dificulte la correcta recepción del mensaje.

En 1950 Hamming publicó su artículo [14] sobre códigos de detección y corrección de errores, lo que provocó el uso del código de Hamming en muchos de los nuevos computadores y creo una nueva rama de la teoría de la información, la Teoría de Códigos.

En 1960 R. C. Bose y D. K. Chaudhuri [2] propusieron una clase de códigos correctores de errores múltiples . Estos códigos correctores son conocidos como códigos BCH (por las iniciales de los autores). También en 1960, I. S. Reed y G. Solomon [23] publicaron un esquema de codificación que usa todo el potencial de los códigos de bloque. Los códigos Reed-Solomon que han sido muy utilizados por la NASA, para la trasmisión de la información en las misiones espaciales.

La introducción en los años 70 por Goppa [7] de una nueva construcción de códigos linales a partir de curvas algebraicas lisas (llamados códigos geométricos Goppa o códigos álgebro-geometricos) cambio por completo el panorama de investigación en el terreno de la teoría de códigos correctores de errores; por un lado, la codificación de dichos códigos parecía sencilla, y por otro sus parámetros podían ser fácilmente controlables a partir de la fórmulas clásicas de la geometría algebraica, sin embargo, a pesar del interés que suscito el estudio de los códigos geométricos de Goppa desde su origen, no pudieron encontrarse algoritmos eficientes para su decodificación hasta finales de los años 80, gracias a sucesivos trabajos de Justesen et al., Skorobogatov y Vladut, y Porter. No obstante, los códigos algebro-geometricos apenas han sido implementadas en la práctica por los ingenieros debido a la profundidad matemática de las ideas subyacentes.

Por este motivo, los matemáticos estan haciendo actualmente una descripción de este tipo de códigos y de su tratamiento práctico mediante una aproximación más elemental. Por otra parte, aunque los parámetros de los códigos algebro-geometricos son mucho mejores que los clásicos en sentido asintótico (es decir, para códigos de longitud arbitrariamente grande), las aplicaciones técnicas no se han visto aún en la práctica de sustituir los que actualmente se utilizan por otros de mayor longitud sin que se dispare simúltaneamente el coste y la tasa de error. Como contrapartida, los códigos clásicos que actualmente se utilizan tienen una decodificación bastante más rápida y efectiva.

Ejemplos de códigos algebro-geometricos definidos por objetos geometricos de dimensión grande son los códigos de Grassmann y los códigos de Schubert. En el primer caso conocemos todos los parámetros del código, en particular su distancia mínima esta dada en terminos de la dimensión de la varieadad de Grassmann;

para los códigos de Schubert, la distancia mínima es acotada en terminos de la dimensión de la correspondiente variedad y se conjetura que debe ser dada también en terminos de la dimensión. Los códigos de Grassmann fueron construidos en 1990 por C.T. Ryan y K. M. Ryan para el caso binario [25], [26], [27] y en 1996 por D. Yu Nogin [22] para el caso de potencias primas. Códigos de Schubert, son una generalización de los códigos de Grassmann, fueron introducidos por Ghorpade y Lachaud en 1998 como códigos asociados a un sistema proyectivo definidos por la variedad de Schubert, y ellos dan una cota superior para la distancia mínima con una conjetura para su valor actual [8] y [9]. Ver también [11], [12], [15], [16], [17] y [24], para recientes investigaciones, donde se enfatiza en la determinación de los pesos grandes de los códigos lineales asociados a estas variedades.

1.1. Teoría algebraica de códigos

En esta sección damos resultados generales y bien conocidos de la teoría de códigos lineales ver [18]. Sea F_q un campo fínito. En terminos matemáticos, un código lineal es la imagen $C = \phi(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$ de un monomorfismo lineal (es decir trasformación lineal inyectiva) $\phi : \mathbb{F}_q^k \to \mathbb{F}_q^n$. De la definición vemos que la codificación esta dado por la transformación lineal ϕ.

En el mismo orden de ideas la decodificación puede verse como una función lineal $\theta : \mathbb{F}_q^n \to \mathbb{F}_q^k$ tal que $\theta \circ \phi$ es la identidad en $\mathbb{F}_q^k$.

Así de lo anterior diremos que C es un $[n,k]_q$-código lineal si C es un código lineal cuya longitud de palabra es n y cuya dimensión, como subespacio vectorial de $\mathbb{F}_{||}^{\ltimes}$ es k.

Definición 1.1. Una *matriz generadora* G de un $[n,k]_q$-código lineal C es una matriz de orden $k \times n$ cuyos k renglones son linealmente independientes

Si u es un vector información de longitud k, podemos establecer la regla de codificación como

$$c = uG$$

El mismo código puede ser descrito por diferentes matrices generadoras. Las operaciónes elementales de renglones de matrices no cambia el código, pero la matriz G modificada representa una forma diferente de codificación. Dado que G tiene rango k, nosotros podemos obtener una forma conveniente de G por operaciones en renglones de tal modo k columnas formen una $k \times k$ matriz identidad. Podemos suponer que esta matriz puede elegirse tomando las primeras k columnas y escribir la matriz generadora

$$G = (I, A)$$

a esta forma le llamamos la forma estándar de G.

Definición 1.2. Una matriz *Paridad de Chequeo* H para un $[n,k]_q$-código C es una $(n-k) \times n$ matriz cuyos renglones son linealmente independientes.

Así si G es una matriz generadora para el código C y H es una matriz paridad de chequeo, nosotros tenemos que $GH^T = 0$ donde 0 es a $k \times (n-k)$ matriz de ceros. De la forma estándar de G encontramos que H es de la forma

$$H = (-A^T, I)$$

donde I ahora es una matriz identidad de orden $(n-k) \times (n-k)$.

Definición 1.3. Sea H una matriz Paridad de Chequeo para un $[n,k]_q$-código C y sea r un vector de $\mathbb{F}^{\ltimes}$, entonces el *sindrome*, $s = syn(r)$, esta dado por

$$s = Hr^T$$

Ahora note que si la palabra recibida, es $r = c + e$,donde c es una palabra de C y e es un vector error, entonces

$$s = H(c+e)^T = He^T$$

El término sindrome se refiere al hecho de que s en la palabra recibida. La palabra no contribuye al sindrome, y para una palabra libre de error tenemos que $s = 0$.

Se sigue de la definición de arriba que los renglones de H son ortogonales a las palabras de C. El código generado por los renglones de H es llamado el código dual $C^{\perp}$, definido por

$$C^{\perp} = \{x \in F^n : x \cdot c = 0 : para : todo : c \in C\}$$

1.2. Distancia Mínima y peso mínimo.

En orden para determinar la capacidad de corregir errores de un $[n,k]_q$-código lineal C introducimos los siguientes conceptos usuales.

Definición 1.4. El *peso de Hamming* de una palabra $x \in C$, denotado por $w_H(x)$ es igual al número de coordenadas diferentes de cero en x. En ocasiones el peso de Hamming se le llama simplemente peso.

La *distancia de Hamming* entre dos palabras x e y, denotada por $d_H(x,y)$ es el número de coordenadas donde ellas difieren. Como para el peso de Hamming la distancia de Hamming es simplemente llamada distancia y normalmente se suprime el subindice H de la definición.

No es dificil ver que

$$\begin{aligned} &d_H(x,y) = 0 si y solo si x = y \\ &d_H(x,y) = d_H(y,x) \\ &d_H(x,y) \leq d_H(x,z) + d_H(z,y) \end{aligned}$$

Así d_H cumple las propiedades de una distancia, en particular la tercer propiedad es la desigualdad del triángulo. Con esta distancia el espacio vectorial produce un espacio metrico.

Definición 1.5. La *distancia mínima* de un código, d es la distancia mínima entre cada pareja de palabras diferentes. Decimos que C es un $[n, k, d]$-código lineal cuando C es de longitud n, de dimensión k y distancia mínima d.

Así para poder calcular la distancia mínima tendríamos que calcular la distancia de todos los pares de palabras, pero para códigos lineales esto no tiene que ser necesario ya que tenemos el resultado siguiente:

Lema 1.6. *En un $[n, k]_q$-código C la distancia mínima es igual al peso mínimo de las palabras diferentes de cero*

DEMOSTRACIÓN. Claramente $w(x) = d(0, x)$ así que $d(x, y) = w(x - y)$. Sea c la palabra de peso mínimo, entonces $w(c) = d(0, c)$ y dado que 0 es una palabra tenemos que $d_{min} \leq w_{min}$. En el otro lado, si c_1 y c_2 son palabras en la distancia mínima, tenemos que $d(c_1, c_2) = w(c_1 - c_2)$ y dado que $c_1 - c_2$ es también una palabra y tenemos que $w_{min} \leq d_{min}$. Combinando ambos resultados y tenemos lo que deseamos

□

Teorema 1.7. *Un $[n, k]_q$-código corrige t errores si y sólo si $t < \frac{d}{2}$*

DEMOSTRACIÓN. Supongamos que $t < \frac{d}{2}$ y que tenemos dos palabras c_i y c_j y dos vectores de error e_1 y e_2 de peso $\leq t$ tal que $c_i + e_1 = c_j + e_2$. Entonces $c_i - c_j = e_2 - e_1$ pero $w(e_2 - e_1) = w(c_i - c_j) \leq 2t < d$, contradiciendo el hecho de que el peso mínimo es d. Por otro lado supongamos que $t \geq 2$ y sea c una palabra con peso d. Cambia $t + 1$ bit's diferentes de cero a cero para obtener la un vector y. Entonces $d(0, y) \leq d - (t + 1) \leq t$ y $d(c, y) \leq t$ pero $0 + y = c + (y - c)$ así que el código no corrige t errores

□

Lema 1.8. *Sea C un $[n, k]_q$-código y H una matriz paridad de chequeo para C. Entonces si j columnas de H son linealmente dependientes, C contiene una palabra con elementos diferentes de cero en alguna de las posiciones correspondientes, y si C contiene una palabra de peso j, entonces existen j columnas linealmente linealmente dependientes de H*

DEMOSTRACIÓN. Se sigue directamente de la definición de la multiplicación de matrices, dado que dada una palabra c del código tenemos que $Hc^T = 0$

□

Lema 1.9. *Sea C un $[n, k]_q$-código con matriz paridad de chequeo H. La distancia mínima de C es igual al número mínimo de columnas linealmente dependientes de H*

DEMOSTRACIÓN. Se sigue de manera inmediata del lema y teorema anteriores

□

1.3. Sistemas proyectivos no degenerados

Los conceptos de sistema proyectivo (en este trabajo a este tipo de sistemas les llamamos sistemas proyectivos no degenerados) y demas que se desarrollan en esta sección se presentan en el librode Tsfasman y Vladut []. La noción de código lineal puede ser reformulado usando los conceptos siguientes. Como antes sea $F = F_q$ un campo fínito, con q una potencia de un primo p y sea E un F_q-espacio vectorial, y sea $\mathbb{P}(\mathbb{E})$ el espacio proyectivo inducido por E.

Definición 1.10. Un $[n, k, d]_q$-sistema proyectivo es una familia fínita, sin ordenar, $\chi = \{P_1, ..., P_n\}$ de puntos de $\mathbb{P}(\mathbb{E})$ la cual no esta en ningún hiperplano H de $\mathbb{P}(\mathbb{E})$. Sus parámetros $[n, k, d]$ se definen como sigue: $n = |\chi|$, $k = dim\mathbb{P}(E) + 1$ y $d = n - max\{|\chi \cap H| : H\ es\ Hiperplano\ de\ \mathbb{P}(\mathbb{E})\}$

Dos $[n, k, d]_q$-sistemas proyectivos $\chi \subset \mathbb{P}(\mathbb{E})$ y $\chi' \subset \mathbb{P}(\mathbb{E}')$ son llamados equivalentes si y sólo si existe un isomorfismo $\mathbb{P}(\mathbb{E}) \cong \mathbb{P}(\mathbb{E}')$ que mapea χ sobre χ'

Llamamos a un código lineal degenerado $C \subset F_q^n$ si y sólo si $C \subset F_q^{n-1} \subset F_q^n$, donde F_q^{n-1} es el subespacio de vectores que tienen cero en alguna posición fija.

Teorema 1.11. *Sea $k \geq 1$ y $d \geq 1$. Existe una correspondencia uno-uno entre el conjunto de clases de equivalencia de los $[r, k, d]_q$-códigos lineales no degenerados y el conjunto de clases de equivalencia de los $[r, k, d]_q$-sistemas proyectivos*

DEMOSTRACIÓN. Dado un sistema proyectivo no degenerado $\chi \subset \mathbb{P}(E)$ le asociamos por evaluación un código lineal no degenerado definido por $C_\chi := \{(f(P_1), \ldots, f(P_r)) : f \in E^*\}$. Para veer que esta asignación no depende del representante se han $\chi = \{P_1, \ldots, P_r\} \subset \mathbb{P}(E)$ y $\chi' = \{P'_1, \ldots, P'_r\} \subset \mathbb{P}(E')$ dos sistemas proyectivos no degenerados y sean C_χ y $C_{\chi'}$ sus códigos lineales asociados. Entonces χ es equivalente a χ' si y sólo si existe (ρ_{ij}) para todo $i, j \in \{1, 2, \ldots, n\}$ si y sólo si $(\rho_{ij})G_\chi = G_{\chi^\chi}$ matrices generadoras de los códigos C_χ y $C_{\chi'}$ respectivamente si y sólo si C_χ es equivalente por permutaciones al código $C_{\chi'}$. Así esta asignación no depende del representante. Para probar que es una biyección basta demostrar que para cada C código lineal no degenerado existe un sistema proyectivo χ no degenerado tal que C es equivalente por permutaciones a C_χ. Sea C un $[r, k]$-código lineal no degerado y sea

$$G = \begin{pmatrix} v_{1,1} & v_{1,2} & , \ldots , & v_{1,r} \\ v_{2,1} & v_{2,2} & , \ldots , & v_{2,r} \\ \vdots & \vdots & \vdots & \vdots \\ v_{k,1} & v_{k,2} & , \ldots , & v_{k,r} \end{pmatrix}$$

una matriz generadora del código C. Denotamos por $\overline{v}_i := \{v_{i,1}, \ldots, v_{r,1}\}$ los vectores renglón de G y sea $P_j := [v_{1,j}, \ldots, v_{k,j}]$ para cada $j = 1. \ldots, r$ los r puntos del espacio proyectivo de dimensión $k-1$. El conjunto $\chi = \{P_1, \ldots, P_r\}$ es un sistema proyectivo no degenrado por ser $\overline{v}_i$ una base de C. Además por la forma como definimos el sistema proyectivo χ definimos facilmente que las matrices generadoras G y G_χ son iguales y luego entonces C es equivalente por permutación al código C_χ. □

Definición 1.12. Sea χ un sistema proyectivo no degenerado no degenerado en $\mathbb{P}(E)$. Denotamos por C_χ el código lineal no degerado inducido por χ. Claramente $C_\chi := \{(f(P_1), \ldots, f(P_r)) : f \in E^*\}$

1.4. Variedades proyectivas

Sea $\mathbb{F}$ un campo arbitrario y denotamos por $\mathbb{P}^n$ al espacio proyectivo de dimensión n sobre el campo $\mathbb{F}$. Sea T un conjunto de polinomios en $n+1$ variables con coeficientes en $\mathbb{F}$. Definimos al conjunto cero de T como

$$Z\langle T\rangle = \{x \in \mathbb{P}^n : f(x) = 0 \, para \, cada \, f \in T\}$$

Un subconjunto Y de $\mathbb{P}^n$ es un conjunto algebraico si existe un conjunto T de polinomios homogeneos en $n+1$ variables con coeficientes en $\mathbb{F}$ tal que $Y = Z\langle T\rangle$.

Definición 1.13. Una variedad algebraica proyectiva o simplemente variedad ws un conjunto algebraico irreducible, con la topología de Zariski, en el espacio proyectivo $\mathbb{P}^n$. Una hipersuperficie definida por un polinomio lineal homogéneo es llamado hiperplano.

Observación 1.14. Recordemos algunos hechos bien conocidos en geometría algebraica.
a) Las siguientes condiciones son equivalentes para una variedad Y en $\mathbb{P}^n$:

i) $I(Y)$ esta generado por polinomios lineales.

ii) Y puede ser escrito como intersección de hiperplanos.

En este caso decimos que Y es una Variedad Lineal en $\mathbb{P}^n$.

b) Si Y es una variedad lineal de dimensión r en $\mathbb{P}^n$, entonces $I(Y)$ es minimamente por $n-r$ polinomios lineales.

c) Sean Y y Z variedades lineales en $\mathbb{P}^n$, con $dimY = r$ y $dimZ = s$. Si $r+s-n \geq 0$ entonces $Y \bigcap Z \neq \emptyset$. Además si $Y \bigcap Z \neq \emptyset$, entonces $Y \bigcap Z$ es una variedad lineal de dimensión mayor o igual a $r+s-n$.

Proposición 1.15. *Todo hiperplano proyectivo es maximal, es decir no existe variedad lineal, distinta de H y de $\mathbb{P}(E)$ que contenga completamente a H. Además la parte $\{a, H\}$ de $\mathbb{P}(E)$, constituida por un hiperplano H y un punto $a \in \mathbb{P}(E)$ que no esta en H, engendra a todo el espacio $\mathbb{P}(E)$*

DEMOSTRACIÓN. Sea $\pi : E \to P$ la proyección natural y sea H un hiperplano de $\mathbb{P}(E)$. Entonces por definición $\pi^{-1}(H)$ es un hiperplano en el espacio vectorial en E, por consiguiente máximal en E y así para cualquier subespacio

vectorial V de E tal que $\pi^{-1}(H) \subseteq V$ se tiene que $V = \pi^{-1}(H)$ pero esto implica que $V = E$ □

1.5. La variedad de Grassmann

Sea E un espacio vectorial de dimensión $m \geq 2$ sobre el campo $\mathbb{F}$. Sea $1 \leq n \leq m$ algún entero, sea $I(n,m) : (a_1, \ldots, a_n) \in \mathbb{Z}^n : 1 \leq a_1 <, \ldots, a_n \leq m\}$. Entonces la *Grassmanniana* o *variedad de Grassmann* se define el conjunto de todos los subespacios n-dimensionales W de E ver [] es decir

$$G(n,m) = \{W : W \; es \; subespacio \; de \; E \; de \; dimension \; n\}$$

Se puede encajar $G(n,m)$ en el espacio proyectivo $\mathbb{P}(\bigwedge^n E)$ via la inclusión de Plücker como sigue, sea W un n-subespacio vectorial de E que tiene como base $\{v_1, \ldots, v_n\}$,

$$\varphi : G(n,m) \longrightarrow \mathbb{P}(\wedge^n E)$$
$$\varphi(W) = v_1 \wedge, \cdots, \wedge v_n$$

Se puede demostrar que φ esta bien definido y es una inclusión no degerada. Para cada W en $G(n,m)$, las coordenadas de Plücker de $\varphi(W)$ son las coordenadas en la base $\{e_\alpha : \alpha \in I(n,m)\}$ donde $e_\alpha = e_{\alpha_1} \wedge, \ldots, \wedge e_{\alpha_n}$ así

$$\varphi(W) = \sum_{\alpha \in I(n,m)} p_\alpha e_\alpha$$

donde los coeficientes $p_\alpha \in \mathbb{F}$.

Sea $W \in G(n,m)$ y sea $\{v_1, ..., v_n\}$ una base para este espacio vectorial y sea $v_j = \sum_{i=1}^m a_{ij} e_i$, entonces las coordenadas de Plücker estan dadas por los $\binom{m}{n}$ menores maximales de la matriz $(a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$.

Se puede demostrar que$G(n,m)$ es una variedad algebraica definida por polinomios cuadricos llamadas relaciones de Plücker ver []. La grassmanniana $G(n,m)$ puede ser cubierta por conjuntos abiertos isomorfos a los espacios afines $\mathbb{A}^{n(m-n)}$ y así tenemos que $dim(G(n,m)) = n(m-n)$

1.6. Número de puntos de $G(n,m)(\mathbb{F}_q)$

Let F un campo perfecto. El grupo de Galois $\Gamma := Gal(\overline{F}/F)$ actuab en $(\mathbb{P}^m(\overline{F})$ como sigue: para $\sigma \in \Gamma$ y $(a_0 :, a_1 :, ..., : a_m) \in \mathbb{P}^{>}(\overline{\neg})$ definimos

$$\sigma[a_0 :, a_1 :, ..., : a_m] = [\sigma(a_0) :, \sigma(a_1) :, ..., : \sigma(a_m)]$$

esta acción esta bien definida y se tiene que:

Lema 1.16. *El grupo de Galois $\Gamma = Gal(\overline{F}/F)$ actua en $\mathbb{P}^m(\overline{F})$ y los puntos fijos son precisamente los puntos en $\mathbb{P}^m(F)$*

DEMOSTRACIÓN. Supongamos que para cada $\sigma \in \Gamma$ se tiene que

$$\sigma[a_0 :, a_1 :, ..., : a_m] = [a_0 :, a_1 :, ..., : a_m]$$

entonces existe un escalar λ_σ tal que $\sigma(a_i) = \lambda_\sigma a_i$ para cada $i = 0, \ldots, n$. Sin perdida de generalidad podemos suponer que $a_0 \neq 0$ entonces para $i = 0, \ldots, n$ tenemos

$$\frac{\sigma(a_0) \cdot a_i}{a_0}$$

Consecuentemente para cada $\sigma \in \Gamma$ tenemos que

$$\frac{a_1}{a_0} = \sigma(\frac{a_i}{a_0})$$

esto significa que $\frac{a_i}{a_0} \in F$. Esto implica que

$$[a_0 : \ldots : a_n] = [1 : \frac{a_1}{a_0} : \ldots : \frac{a_1}{a_n}] \in \mathbb{P}^m(F)$$

Entonces el grupo de Galois $\Gamma = Gal(\overline{F}/F)$ actua en $\mathbb{P}^m(\overline{F})$ y los puntos fijos son precisamente los puntos $\mathbb{P}^m(F)$ □

La acción del grupo de Galois Γ en es espacio $\mathbb{P}^m(\overline{F})$ se restringe a una acción en la Grassmanniana correspondiente como sigue. Para comenzar y sin perdida de generalidad podemos suponer que el espacio vectorial E es $(\overline{F})^n$. La Grassmanniana $G(n,m)$ es la colección de todos los subespacios n-dimensionales de $(\overline{F})^n$ y Γ actua en $G(n,m)$ como sigue: para $W \in G(n,m)$ y $\sigma \in \Gamma$ definimos

$$\sigma(W) = \{\sigma[x_1, ..., x_n] : [x_1, ..., x_n] \in W\}$$

donde $\sigma[x_1, ..., x_n] = [\sigma(x_1), ..., \sigma(x_n)]$.

Podemos pensar a $G(n,m)$ como encajado en el espacio proyectivo $\mathbb{P}^n = \mathbb{P}(\bigwedge^n E)$ vía la inclusión de Plücker y podemos considerar la acción de Γ en $G(n,m)$ como la acción inducidad por la acción en el espacio proyectivo. Note que estas dos acciones Γ en $G(n,m)$ son Γ equivalentes. Decimos que $W \in G(n,m)$ es Γ invariante si $\sigma(W) = W$ para todo $\sigma \in \Gamma$.

Lema 1.17. *$W \in G(n,m)$ es Γ es Γ invariante si y sólo si W tiene una base $\{v_1, ..., v_n\}$ con cada $v_i \in F^n$*

DEMOSTRACIÓN. Claramente si el subespacio W tiene una base $\{v_1, ..., v_n\}$ con cada $w_i \in F^m$ entonces Wes Γ-invariante. Ahora sea W un subespacio n-dimensional de E generado por los vectores $\{v_1, ..., v_n\}$ tal que $\sigma(W) = W$, para cada $\sigma \in \Gamma$ y cada $i = 1, 2, \ldots, n$

$$\sigma(w_i) = w_i$$

Como $\sigma(W) = W$ existe $A(\sigma) \in GL(n, \overline{F})$ tal que

$$\sigma \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = A(\sigma) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

Entonces tenemos

$$A(\sigma\tau)\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \sigma[\tau \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}] = \sigma[A(\tau) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}]$$

$$= \sigma[A(\sigma)]\sigma \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \sigma[A(\tau)]A(\sigma) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}]$$

entonces $A(\sigma\tau) = [\sigma A(\tau)]A(\sigma)$ consecuentemente existe $B \in GL(n, \overline{F})$ tal que $B = (\sigma B)A(\sigma)$
Ahora sea

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = B \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

Entonces tenemos

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = B \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = (\sigma B) \cdot A(\sigma) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = (\sigma B) \cdot \sigma \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

$$\sigma[B \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}] = \sigma \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$

Así para todo $\sigma \in \Gamma$, $\sigma(w_i) = w_i$, $i = 1, \ldots, n$ lo cual implica que W tiene una base $\{w_1, w_2, \ldots, w_n\}$ con $w_i \in F^n$. □

Ahora usaremos esto para calcular la cardinalidad de $G(n, m)(\mathbb{F}_{11})$

Proposición 1.18. *El número de puntos de $G(n, m)(\mathbb{F}_q)$ esta dado por*

$$|G(n, m)(\mathbb{F}_q)| = \frac{f(n)}{f(d) \cdot f(n-d) \cdot q^{d(n-d)}}$$

donde $f(n)(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$

DEMOSTRACIÓN. Sea $\mathbb{F} = \mathbb{F}_q$, entoncers tenemos que

$$|G(n, m)(\mathbb{F})| = |[[G(n, m)(\overline{\mathbb{F}})]]^{\Gamma}|$$

el cual es el número de espacios n-dimensionales de $(\overline{\mathbb{F}}))^m$ que son los σ-invariantes. Sea J que denota la colección de todas las ordenadas $\{v_1, \ldots, v_n\}$ con cada $v_i \in$

$(\overline{\mathbb{F}}))^m$. Entonces J define un subconjunto abierto de $((\overline{\mathbb{F}}))^m)^n$ por el lema anterior se sigue que para calcular el número de subespacios los cuales son σ-invariantes uno puede calcular el número de elemnstos de J y contar cuantas bases ordenadas diferentes dan lugar al mismo elemento de $G(n,m)$. La cardinalidad de $G(n,m(\mathbb{F}_q))$ esta dada por el cociente

$$|G(n,m(\mathbb{F}_q))| = \frac{\text{número de puntos de J}}{\text{número de bases ordenadas para cada U}}$$

Ahora para encontrar J tenemos que el grupo lineal general $GL(n,\mathbb{F}) = Aut(\mathbb{F}^m)$ actúa naturalmente en J y la acción es transitiva. El estabilizador de $X = \{e_1,\ldots,e_n\}$ tiene bloque de matrices de la forma

$$\begin{pmatrix} I_n, & * \\ 0, & GL(m-n,\mathbb{F}) \end{pmatrix}$$

De aquí

$$|J| = \frac{GL(n,\mathbb{F})}{|stabX|} = \frac{1}{q^{n(m-n)}} \cdot \frac{GL(n,\mathbb{F})}{GL(m-n,\mathbb{F})}$$

Entonces tenemos que

$$\begin{aligned} |GL(n,\mathbb{F})| &= \frac{|GL(n,\mathbb{F})|}{|GL(n,\mathbb{F})| \cdot |GL(m-n,\mathbb{F})| \cdot q^{n(m-n)}} \\ &= \frac{f(m)}{f(m) \cdot f(m-n) \cdot q^{n(m-n)}} \end{aligned}$$

donde $f(m) = (q^m-1)(q^m-q)\cdots(q^m-q^{m-1})$. □

Definición 1.19. Definimos erl q-factorial de un entero no negativo d por

$$[d]! = (q^d-1)(q^{d-1}-1)\cdots(q-1)$$

y el coeficiente binomial Gaussiano correspondiente a los enteros m y n por

$$\binom{m}{n} = \frac{[m]!}{[n]![m-n]!} = \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{n-1})}{q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}$$

Teorema 1.20. *El número de puntos de $G(n,m)(\mathbb{F}_q)$ esta dada por la fórmula*

$$|G(n,m)(\mathbb{F}_q)| = \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{n-1})}{q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}$$

DEMOSTRACIÓN. Por la proposición anterior tenemos que

$$|G(n,m)(\mathbb{F}_q)| = \frac{f(m)}{f(n) \cdot f(m-n) \cdot q^{n(m-n)}}$$

donde $f(m) = (q^m-1)(q^m-q)\cdots(q^m-q^{n-1})$ entonces multiplicando y dividiendo por $q^{n(m-n)}$ tenemos que

$$|G(n,m)(\mathbb{F}_q)| = \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-n+1}-1)}{(q^n-1)(q^{n-1}-1)\cdots(q-1)}$$

Luego entonces

$$|GL(n,\mathbb{F})| = \frac{[m]!}{[n]![m-n]!} = \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{n-1})}{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}$$

y así hemos demostrado el teorema. □

Capítulo 2

Códigos álgebro-geométricos de Grassmann

En esta sección damos una construcción general de códigos geométricos, cuando tomamos variedades algebraicas proyectivas con buenas propiedades geométricas y consideramos esta construcción en el conjunto de todos los puntos racionales. Los códigos resultantes reflejan estas propiedades est6as propiedades geométricas en sus parámetros. También si reinterpretamos esta construcción en la variedad de Grassmann recobramos los códigos clásicos de Grassmann y Schubert.
Sea F_q un campo finito, E un F_q-espacio vectorial de dimensión fínita y $\mathbb{P}(\mathbb{E})$ el espacio proyectivo inducido por E.

Definición 2.1. Un *Sistema Proyectivo no degenado* es un conjunto de puntos $\chi = \{P_1, ..., P_r\}$ del espacio proyectivo $\mathbb{P}(\mathbb{E})$ no completamente contenido en ningún hiperplano H de $\mathbb{P}(\mathbb{E})$. Los parámetros $[r, k, d]_q$ del sistema proyectivo χ están definidos por $r = |\chi|$, $k = \dim \mathbb{P}(E)$ y

$$d = |\chi| - max\{|\chi \cap H| : H\ es\ un\ hiperplano\ de\ \mathbb{P}(\mathbb{E})\}$$

El concepto de sistema proyectivo se desarrolla en [] capitulo !, sección 1.3. Llamemos a un código lineal $C \subseteq \mathbb{F}_q^r$ degenerado si y sólo si $C \subseteq \mathbb{F}_q^{r-1} \subseteq \mathbb{F}_q^r$, donde $\mathbb{F}_q^{r-1}$ es el subespacio de vectores que tienen cero en alguna posición fija. Es bien sabido que si $k \geq 1$ y $d \geq 1$, entonces existe una correspondencia uno-uno entre el conjunto de clases de equivalencia de los $[r, k, d]_q$-códigos lineales no degenerados y el conjunto de clases de equivalencia de los $[r, k, d]_q$-sistemas proyectivos ver el teorema 2.12 .

Lema 2.2. *Sea* $\chi := \{P_1, ..., P_r\}$ *una familia fínita de puntos de* $\mathbb{P}(\mathbb{E})$. *Sea* $K := \{h \in E^* : h(P_1) = \cdots = h(P_r) = 0\}$. *También sea* $V := \{x \in E :\ h(x) = 0 para todo h \in K\}$. *Entonces* $\mathbb{P}(\mathbb{V})$ *es la subvariedad lineal más pequeña de* $\mathbb{P}(\mathbb{E})$ *que contiene a* χ

DEMOSTRACIÓN. Supongamos que *H* es una subvariedad lineal de $\mathbb{P}(\mathbb{E})$ tal que $\chi \subseteq H$ y $H \subseteq \mathbb{P}(\mathbb{V})$. Entonces $H = \bigcap_{i=1}^t H_i$ es la intersección de hiperplanos H_i de $\mathbb{P}(\mathbb{E})$, esto significa que existe $h_i \in E^*$ tal que $H_i = Z\langle h_i \rangle$ para cada $i = 1, ..., t$. Por lo tanto tenemos que $H = z\langle h_1, ..., h_t \rangle$. Por estar $\chi \subseteq H$, $h_i(P_1) = ... = h_i(P_r) = 0$ para todo $i = 1, ..., t$, esto implica que $h_i \in K$, sea entonces $h_i = \sum_{i=1}^t \alpha_i k_i$ es una combinación lineal con coeficientes $\alpha_i \in F$. Sea $x \in \mathbb{P}(\mathbb{V})$ un elemento arbitrario entonces es fácil ver que $h_i(x) = 0$ para todo $i = 1, ..., t$, así que $x \in Z\langle h_1, ...h_t \rangle$ y en consecuencia $\mathbb{P}(\mathbb{V}) \subseteq Z\langle h_1, ..., h_t \rangle = H$

□

Note que en la última parte de la prueba tenemos que $\mathbb{P}(\mathbb{V}) = Z\langle h_1, ..., h_t\rangle$ si $h_1, ..., h_t$ es una base de K.

Corolario 2.3. *Con la notación de arriba, χ es un sistema proyectivo no degenerado en $\mathbb{P}(\mathbb{V})$*

DEMOSTRACIÓN. Si H es un hiperplano de $\mathbb{P}(\mathbb{V})$ tal que $\chi \subseteq H$, entonces existe $h \in E^*$ tal que $H = Z\langle h_1, ..., h_k, h\rangle$ la cual es una subvariedad lineal más pequeña que $\mathbb{P}(\mathbb{V})$. Lo cual contradice al lema anterior □

Sea C_χ el código lineal no degenerado inducido por el sistema proyectivo χ en $\mathbb{P}(\mathbb{V})$. Entonces su longitud es igual a cardinalidad de χ y que su dimensión es $dim C_\chi = dim V$ (véase 2.11)

Sea E un espacio vectorial de dimensión fínita sobre un campo fínito $F = F_q$. Si X es una variedad algebraica sobre $\overline{F}$ la cerradura algebraica del campo fínito $\mathbb{F}$. Supongamos que $\chi := \{P_1, \ldots, P_r\}$ es el conjunto de sus $\mathbb{F}_q$

$X = Z\langle f_1, ..., f_M, g_1 ... g_N\rangle$ con f_i polinomios homogeneos de grado ≥ 2 los g_j de grado uno con coeficientes en F. Como arriba $K := \{h \in E^* : h(P_1) = \cdots = h(P_r) = 0\}$ y $V := \{x \in E :\ h(x) = 0\, para\, todo\, h \in K\}$.

Lema 2.4. *Para V y g_j como arriba, $\mathbb{P}(\mathbb{V}) = Z\langle g_1 ... g_N\rangle$*

DEMOSTRACIÓN. Del lema 2.2 tenemos que $\mathbb{P}(\mathbb{V}) \subseteq Z\langle g_1 ... g_N\rangle$. Nosotros usamos subindices para denotar donde consideramos el ideal de polinomios. Por ejemplo I_F o $I_{\overline{F}}$, donde $\overline{F}$ es la cerradura algebraica de F. Ahora si $h_1, ..., h_s$ es una base de K, entonces $h_j(P) = 0$ para todo $P \in \chi$, se sigue que
$Z\langle f_1, ..., f_M, g_1, ..., g_N\rangle \subseteq Z < h_j >$ para todo j. Consecuentemente
$h_j \in I(Z\langle h_j\rangle) \subseteq I(Z\langle f_1, ..., f_M, g_1, ..., g_N\rangle) = \sqrt{\langle f_1, ..., f_M, g_1, ..., g_N\rangle}_F$
y dado que $\langle f_1, ..., f_M, g_1, ..., g_N\rangle_F \subseteq \langle f_1, ..., f_M, g_1, ..., g_N\rangle_{\overline{F}}$
entonces $h_j^t \in \langle f_1, ..., f_M, g_1, ..., g_N\rangle_{\overline{F}}$
para algún t entero positivo, y dado que X es una variedad algebraica tenemos que $h_j \in \langle f_1, ..., f_M, g_1, ..., g_N\rangle_{\overline{F}}$. Entonces $h_j \in \langle g_1, ..., g_N\rangle_{\overline{F}}$, así que $h_j = \sum \alpha_i g_i$ con $\alpha_i \in \overline{F}$. Para cada $x \in Z\langle g_1, ..., g_N\rangle$ implica $h_j(x) = \sum_{i=1}^N \alpha_i g_i(x) = 0$ para todo $j = 1, ..., s$ consecuentemente $Z\langle g_1, ..., g_N\rangle \subseteq \mathbb{P}(\mathbb{V})$. Por lo tanto $Z\langle g_1, ..., g_N\rangle = \mathbb{P}(\mathbb{V})$. □

Es inmediato que:

Corolario 2.5. *Sea V y g_i como en el lema 2.4 entonces $V = \{x \in E : g_1(x) = , ..., = g_N(x) = 0\}$*

□

Y también

Corolario 2.6. *Si F_q es un campo finito y E es un espacio vectorial de dimensión finita sobre F_q y si $\chi = \{P_1, ..., P_r\} \subseteq \mathbb{P}(\mathbb{E})$ es un conjunto fínito de puntos no contenidos en ningún hiperplano entonces $K = 0$ y para el código asociado C_χ, tenemos que $dim C_\chi = dim E^*$*

□

2.1. Códigos Grassmann

Para un m-espacio vectorial E, denotamos por $G(n, m)$ el conjunto de subespacios vectoriales de dimensión n de E. La Grassmanniana $G(n, m)$ es una variedad algebraica de dimensión $n(m - n)$ y puede ser encajada en el espacio proyectivo $\mathbb{P}\left(\bigwedge^n E\right)$, donde $\bigwedge^n E$ es el álgebra de Grassmann generada por el espacio vectorial E, mediante la inclusión de Plücker. Por elegir una base $v_1, ...v_n$ para cada $W \in G(n, m)$ y mandar esta base a $v_1 \wedge ... \wedge v_n \in \bigwedge^n E$, uno tiene entonces la siguiente descripción para la variedad Grassmanniana

$$G(n, m) = \{v_1 \wedge ... \wedge v_n \in \bigwedge^n E : v_1, ..., v_n \, son \, linealmente \, independientes\}$$

Si además F_q es un campo fínito entonces $G(n, m)$ es un conjunto fínito $\{P_1, ..., P_r\}$ de puntos del espacio proyectivo $\mathbb{P}\left(\bigwedge^n E\right)$, donde $\binom{m}{n}_q$ al coeficiente binomial Gaussiano, ver definición 2.20 y teorema 2.21.

Lema 2.7. *Sea F_q un campo fínito entonces $G(n, m)$ es un sistema proyectivo en $\mathbb{P}\left(\bigwedge^n E\right)$*

DEMOSTRACIÓN. Supongamos que existe H hiperplano en $\mathbb{P}\left(\bigwedge^n E\right)$ tal que $G(n, m) \subseteq H$, entonces existe $h \in \left(\bigwedge^n E\right)^*$ lineal homogeneo tal que $H = Z\langle h\rangle$ y $Z\langle f_1, ..., f_M\rangle \subseteq Z\langle h\rangle$, así que $h \in (\sqrt{\langle f_1, ..., f_M\rangle})_{F_q}$ y esto implica la existencia de algun $s > 0$ tal que $h^s \in \langle f_1, ..., f_M\rangle_{F_q} \subseteq \langle f_1, ..., f_M\rangle_{\overline{F}_q}$ y donde $\overline{F}_q$ es la cerradura algebraica de F_q, así tenemos entonces que $h \in \langle f_1, ..., f_M\rangle_{\overline{F}_q}$ por ser $G(n, m)$ variedad algebraica irreducible, pero esto es una contradicción ya que h es un polinomio lineal homogéneo □

Sea F_q un campo fínito, denotemos por $C(n, m)$ el código lineal no degenerado inducido por el sistema proyectivo $G(n, m)$ en $\mathbb{P}(\mathbb{E})$. Como es usual en la literatura a $C(n, m)$ le llamamos el código de Grassmann.

Corolario 2.8. *Sea F_q un campo fínito y sea $C(n, m)$ el código de Grassmann, entonces $dim C(n, m) = \binom{m}{n}$*

DEMOSTRACIÓN. Esto es una fácil consecuencia del corolario 3.6 y lema 3.1 de arriba. □

Resumiendo concluimos que si F_q es un campo fínito, la cardinalidad de $G(n,m)$ es igual al coieficiente binomial Gaussiano

$$|G(n,m)| = \binom{m}{n}_q$$

y que $\dim C(n,m) = \binom{m}{n}$. También Ryan (1990) y Nogin (1996) demuestran que si F_q es un campo fínito entonces la distancia mínima $d = d_{C(n,m)}$ del código de Grassmann es igual a $d = q^{n(m-n)}$, ver [25], [26], [27] y [22]. así podemos concluir el siguiente corolario.

Corolario 2.9. *El código de Grassmann es un* $(n,k,d)_q$*-código donde* $n = \binom{m}{n}_q$, $k = \binom{m}{n}$ *y* $d = q^{n(m-n)}$

□

2.2. Códigos de Schubert

Como antes sea $\mathbb{P}(\mathbb{E})$ el espacio proyectivo inducido por el espacio vectorial de dimensión n sobre el campo F_q.

La variedad de Grassman $G(n,m)$ parametriza los subespacios vectoriales de dimensión n de E. Denotamos un punto de $\mathbb{P}(\mathbb{E})$ por $\overline{x}$, donde x denota un vector distinto de cero. Si $w = v_0 \wedge ... \wedge v_n$ el correspondiente subespacio $L(w) = \langle \overline{x}_0, ..., \overline{x}_n \rangle$.

Sea $A_0 \subset A_1 \subset \cdots \subset A_n$ una bandera de espacios lineales in $\mathbb{P}^n = \mathbb{P}(\mathbb{E})$, estrictamente creciente, cuya secuencia de dimensiones denotamos por $\alpha = (a_0, ...a_n)$. La variedad de Schubert $\Omega(\alpha)$ es una subvariedad de la variedad de Grassmann, cuyos puntos corresponden a los subespacios L tal que $dim L \cap A_i \geq i$ para cada i. La variedad de Schubert es esencialmente independiente de la bandera especificada de subespacios de una dimensión dada, hasta un automorfismo lineal de la Grassmanniana.

Supongamos que $\Omega(\alpha) = \{P_1, ..., P_r\}$ como un conjunto de puntos del espacio proyectivo $\mathbb{P}\left(\bigwedge^n E\right)$ bajo la inclusión de Plücker, entonces definimos un código lineal no degenerado $C(\alpha)$ inducido por el sistema proyectivo $\Omega(\alpha)$ de puntos de la variedad de Schubert en el espacio proyectivo $\mathbb{P}(\mathbb{V})$, donde $V = \{x \in E :$ h(x)=0 para todo $h \in K\}$ y $K = \{h \in (\bigwedge E)^* : h(P_1) = \cdots = h(P_r) = 0\}$ ver lema 3.2. Al código lineal $C(\alpha)$ le llamaremos código de Schubert.

Se demuestra en [8] que la longitud n_α y la dimensión k_α de C_α son abstratamente dados por $n_\alpha = |\Omega(\alpha)|$ y $k_\alpha = |\{\beta \in I(n,m) : \beta \leq \alpha\}|$ donde para $\beta = (\beta_1, ..., \beta_n) \in I(n,m)$ entendemos que $\beta \leq \alpha$ si y sólo si $\beta_i \leq \alpha_i$ para $i = 1, ..., n$. Se demuestra también que la distancia mínima $d = d(C(\alpha))$vsatisface la desigualdad $d \leq q^{\delta_\alpha}$ donde $\delta_\alpha = \sum_{i=1}^n (\alpha_i - i) = \alpha_1 + \cdots + \alpha_n - \frac{n(n+1)}{2}$. Además se conjetura que la igualdad debe cumplirse.

2.3. Códigos algebro-geometricos de intersección

Sea E un esapcio vectorial de dimesión finita sobre un campo finito $\mathbb{F} = \mathbb{F}_2$. Si χ es una varieadad proyectiva sobre $\overline{\mathbb{F}}$ una cerradura lagebraica de $\mathbb{F}$. Supongamos que $\chi := \{P_1, \ldots, P_r\}$ es el conjunto de todos sus $\mathbb{F}_q$-puntos racionales. Sea Y una variedad proyectiva y V un subespacio vectorial de E, tal que $X = Y \cap \mathbb{F}(V)$

Definición 2.10. Si X, V y χ son como arriba entonces al código C_χ es llamado código álgebro-geométrico de intersección

Proposición 2.11. *El código de Schubet $C(\alpha)$ es un código algebro-geometrico de intersección*

DEMOSTRACIÓN. Sea $V := \{L \in \bigwedge^n E : L_\beta = 0 \text{para todo} \beta \not\leq \alpha\}$. Se demuestra en la sección 5 de [8] que $\Omega(\alpha) = G(n, m) \cap \mathbb{P}(V)$, así que C_α es un código geometrico de intersección. □

Capítulo 3

Códigos Lagrangianos-Grassmannianos

En este capťulo construimos los códigos Lagrangianos-Grassmannianos, calculamos la longitud de la palabra, damos una fórmula en coordenadas de Plüker que nos permite determinar la dimensión y establecemos una cota superior para la distancia mímima en términos de la dimensión de la variedad Lagrangianna-Grassmanniana, establecemos una relación entre los pesos grandes de los códigos Lagrangiannos-Grassmannianos y los pesos del código de Grassmann.

3.1. La variedad Lagrangianna-Grassmanniana

Definición 3.1. Sea E un espacio vectorial sobre un campo F. Una *forma simpléctica*

$$\langle , \rangle : E \times E :\longrightarrow F$$

es una forma bilineal antisimetrica y no degenerada que satisface

$$\langle w, w\rangle = 0 \, para \, todo \, w \in E$$

$$\langle w', w\rangle = 0 \, para \, todo \, w' \in E$$

entonces $w = 0$. Un espacio vectorial $(E, \langle , \rangle)$ es llamado *espacio vectorial simpléctico* si esta equipado con una forma simplética $\langle , \rangle$

Teorema 3.2. *Un espacio vectorial simpléctico E es necesariamente de dimensión par y si existe una base $v_1, ..., v_n, v'_1, ..., v'_n$ de E tal que*

$$\langle v_i, v_j\rangle = \langle v'_i, v'_j\rangle = 0$$

y

$$\langle v_i, v'_j\rangle = \delta_{ij}$$

es llamada base estándar. Con tal elección una forma simplética puede ser descrita para $x, y \in E$, donde $x = (x_1, ..., x_{2n})$ y $y = (y_1, ..., y_{2n})$ como

$$\langle x, y\rangle = \sum_{i=1}^{n} [(x_i \cdot y_{2n+1-i}) - (x_{2n+1-i} \cdot y_i)]$$

DEMOSTRACIÓN. es fácil ver que este es un pairing alternante no-degenrado en E. La forma anterior en E llamada la *forma simpléctica estándar*

□

Definición 3.3. Sea E un espacio vectorial simpléctico, con forma simpléctica $\langle , \rangle$. Decimos que $W \in G(n, 2n)$ es *isotropico* si y sólo si $\langle x, y\rangle = 0$ para todo $x, y \in W$

Definición 3.4. La *Lagrangianna-Grassmanniana* se define como

$$L(n, 2n) = \{W \in G(n, 2n) : W \; es \; isotropico\}$$

Se puede demostrar que $L(n, 2n)$ es una subvariedad proyectiva de $G(n, 2n)$ de dimensión $\frac{n(n+1)}{2}$.

Definición 3.5. Sean E_1, E_2 dos espacios vectoriales simplécticos. Sea $\phi : E_1 \longrightarrow E_2$ un mapeo lineal. Llamamos a ϕ un *mapeo simpléctico* si para todo $w, w' \in E_1$

$$\langle \phi(w), \phi(w')\rangle = \langle w, w'\rangle$$

Supongamos ahora que $E_1 = E_2 = E$ con la misma forma simplética. Si $\phi : E \longrightarrow E$ es algún mapeo simpléctico entonces es un automorfismo de E. La colección de todos los automorfismos de$E$ es un grupo bajo la composición llamado *grupo simpléctico* de $(E, \langle , \rangle)$ denotado por $Sp(E)$, Si $E = F_q^{2n}$ con la forma simpléctica estandar, denotamos a este grupo como $Sp_{2n}(F_q) \subset GL(2n, F_q)$. Si definimos

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

se puede verificar que una matriz $A \in GL(2n, F_q)$ deja la forma estándar invariante si y sólo si $A^T JA = J$ donde, A^T denota la matriz transpuesta de A. Así

$$Sp_{2n}(F_q) = \{A \in GL(2n, F_q) : A^T JA = J\}$$

3.2. El número de puntos en $L(n, 2n)(F_q)$

Usando el teorema de Witt, tenemos que el grupo simpléctico $Sp_{2n}(F_q)$ actua transitivamente en el conjunto de todos los subespacios simpécticos de $G(n, 2n)(F_q)$ es decir en la Lagrangianna-Grassmnniana. En otras palabras dados W_1, W_2 en $L(n, 2n)$ existe $\phi \in Sp(E)$ tal que

$$\phi(W_1) = W_2$$

En virtud de lo antes dicho tenemos que

$$|L(n, 2n)(F_q)| = \frac{|Sp_{2n}(F_q)|}{|StabW|}$$

donde $StabW$ es el estabilizador de $W \in L(n, 2n)$

Para encontrar $|Sp_{2n}(F_q)|$ usamos el siguiente resultado de álgebra lineal.

Lema 3.6. *Si f es una forma simpléctica en un $2n$-espacio vectorial E sobre un campo de q elementos entonces el número de pares $\{u, v\}$ tal que $f(u, v) = \langle u, v\rangle = 1$ es $(q^{2n} - 1)q^{2n-1}$*

Para una demostración ver [28].

Proposición 3.7. *El número de puntos de $Sp_{2n}(F_q)$ esta dado por la siguiente formula*

$$|Sp_{2n}(F_q)| = q^{n^2}\prod_1^n (q^i-1)(q^i+1)$$

DEMOSTRACIÓN. Dada una forma simpléctica f en un espacio vectorial E de dimensión $2n$ por resultados estándar existe una base simpléctica $\{v_1, v_2, ..., v_{2n}\}$ para E tal que $\langle v_i, v_{i+n}\rangle = 1$ para todo $i = 1, ..., n$ y $\langle v_i, v_j\rangle = 0$ para $|i-j| \neq n$.

Usando el lema anterior el numero de pares $\{\theta v_1, \theta v_{1+n}\}$ tal que $\langle \theta v_1, \theta v_{1+n}\rangle = 1$ es $(q^{2n}-1)q^{2n-1}$. Así que elegimos $\{\theta v_1, \theta v_{1+n}\}$ para que $\{\theta v_i\}$ sea una base simpléctica el numero de pares $\{\theta v_2, \theta v_{2+n}\}$ tal que $\langle \theta v_2, \theta v_{2+n}\rangle = 1$ es igual a $(q^{(2n-2)-1})(q^{2n-2}-1)$ y así sucesivamente. Finalmente el número de pares $\{\theta v_n, \theta v_{2n}\}$ tal que $\langle \theta v_n, \theta v_{2n}\rangle = 1$ es igual a $q(q^2-1)$. Así tenemos que $|Sp_{2n}(F_q)| = \prod_1^n (q^{2i}-1)q^{2i-1} = q^{n^2}\prod_1^n (q^{2i}-1) = q^{n^2}\prod_1^n (q^i-1)(q^i+1)$ □

Lema 3.8. *Sea E un espacio vectorial simpléctico de dimensión $2n$.*

Sea $u_1, ..., u_n, v_1, ..., v_n$ la base estándar de E tal que $\langle u_i, u_j\rangle = \langle v_i, v_j\rangle = 0$ y $\langle u_i, v_j\rangle = \delta_{ij}$. El grupo simpléctico $Sp_{2n}(F_q)$ actua transitivamente en $L(n,2n)(F_q)$ y el número de elementos en el estabilizador para $W = \langle u_1, u_2, ..., u_n\rangle$ esta dado por la fórmula

$$|Stab(W)(F_q)| = q^{\frac{n(n+1)}{2}} q^{\frac{n(n-1)}{2}} \prod_1^n (q^i-1)$$

DEMOSTRACIÓN. Primero note que si $\begin{pmatrix} A & B \\ D & C \end{pmatrix} \in Stab(W)$ entonces D tiene que ser cero.

Sea $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \in Stab(W)$. Si tiene que estar en $Sp(2n)$ debemos tener

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

que es

$$\begin{pmatrix} 0 & A^TC \\ -C^TA & B^TC - C^TB \end{pmatrix} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

Así tenemos que $C = (A^{-1})^T$ y $B^TC = C^TB$, es decir C^TB es una matriz simétrica. Así M es de la forma

$$M = \begin{pmatrix} A & AS \\ 0 & (A^{-1})^T \end{pmatrix}$$

para alguna matriz simétrica S de orden $n \times n$. Sea M_n^{Sym} el grupo de matrices simetricas de orden $n \times n$.

Consideremos los mapeos $\phi_1 : GL(n) \longrightarrow Sp(2n)$ y $\phi_2 : M_n^{Sym} \longrightarrow Sp(2n)$ dados por $\phi_1(A) = \begin{pmatrix} A & 0 \\ 0 & (A^{-1})^T \end{pmatrix}$ y $\phi_2(S) = \begin{pmatrix} I & S \\ 0 & I \end{pmatrix}$.

Entonces ϕ_1 y ϕ_2 son homomorfismos tal que
$\phi_1(A)\phi_2(S) = \begin{pmatrix} A & 0 \\ 0 & (A^{-1})^T \end{pmatrix} \begin{pmatrix} I & S \\ 0 & I \end{pmatrix} = \begin{pmatrix} A & AS \\ 0 & (A^{-1})^T \end{pmatrix}$ Tenemos entonces $Im(\phi_1) \cap Im(\phi_2) = I$. Puede verificarse que $Stab(W)$ es el producto semidirecto de $GL(n)$, el $n \times n$ grupo lineal general, y M_n^{Sym}, el grupo de matrices de orden $n \times n$ simétricas . Consecuentemente tenemos, que

$$|Stab(W)(F_q| = |M_n^{Sym}(F_q)| \cdot |GL(n)(F_q)| = q^{\frac{n(n+1)}{2}} \prod_{i=0}^{n-1}(q^n - q^i)$$

$$= q^{\frac{n(n+1)}{2}} q^{\frac{n(n-1)}{2}} \prod_{i=0}^{n-1}(q^i - 1)$$

□

Proposición 3.9. *El número de puntos en $L(n, 2n)(F_q)$ es dado por*

$$|L(n, 2n)(F_q)| = \prod_{i=1}^{n}(1 + q^i)$$

DEMOSTRACIÓN. La prueba se sigue inmediatamente de la proposición 4.8 y del lema 4.9. Tenemos entonces

$$|L(n, 2n)(F_q)| = \frac{|Sp_{2n}(F_q)|}{|GL(n)(F_q)| \cdot |S_n(F_q)|}$$

$$= \frac{q^{n^2} \prod_{i=1}^{n}(q^i - 1)(q^i + 1)}{q^{\frac{n(n+1)}{2}} q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1)} = \prod_{i=1}^{n}(1 + q^i)$$

□

Definición 3.10. Si E un espacio vectorial simpléctico y $\bigwedge^n E$ el álgebra exterior de E, definimos el mapeo lineal f definido de la siguiente manera

$$f : \bigwedge^{n} E \longrightarrow \bigwedge^{n-2} E$$

$$v_1 \wedge ... \wedge v_n \longmapsto \sum_{1 \leq r < s \leq n} \langle v_r, v_s \rangle v_1 \wedge ... \wedge \widehat{v_r} \wedge ... \wedge \widehat{v_s} ... \wedge v_n$$

donde $\widehat{v}$ significa que el correspondiente término es omitido.

Sea V al nucleo de f y denotemos por $\mathbb{P}(\mathbb{V})$ la proyectivización de V. Entonces $\mathbb{P}(\mathbb{V})$ es un subconjunto cerrado irreducible (bajo la inclusión de Plücker) en $\mathbb{P}\left(\bigwedge^n E\right)$, y $\mathbb{P}(\mathbb{V}) = Z\langle g_1, ..., g_N\rangle$ es el conjunto cero de una familia de polinomios lineales homogeneos $g_1, ..., g_N$, podemos suponer que los g_i son un conjunto minimal de generadores.

Lema 3.11. $L(n, 2n) = G(n, 2n) \bigcap \mathbb{P}(\mathbb{V})$

DEMOSTRACIÓN. Claramente $L(n, 2n) \subseteq G(n, 2n) \cap \mathbb{P}(\mathbb{E})$. Para la otra inclusión, si $w \in G(n, 2n) \cap \mathbb{P}(\mathbb{E})$, entonces w es la clase de equivalencia de $v_1 \wedge ... \wedge v_n$ con $v_1, ...v_n$ linealmente independientes y $f(w) = 0$, que es

$$f(w) = \sum_{1 \leq r < s \leq n} \langle v_r, v_s\rangle v_1 \wedge ... \wedge \widehat{v_r} \wedge ... \wedge \widehat{v_s} \wedge ... \wedge v_n = 0$$

y así $\langle v_r, v_s\rangle = 0$ para todo $1 \leq r < s \leq n$ □

Ahora, dado que $\mathbb{P}(\mathbb{V}) = Z\langle g_1, ..., g_N\rangle$ con g_i una familia minimal de polinomios lineales homogeneos, y dado que la Grassmanniana es la intersección de cuadricas, digamos $G(n, 2n) = Z\langle f_1, ..., f_M\rangle$, entonces

$$L(n, 2n) = Z\langle f_1, ..., f_M, g_1, ..., g_N\rangle$$

3.3. Código Lagrangianno-Grassmanniano

Ya que F_q es un campo finito entonces la variedad algebraica $L(n, 2n)$ es un conjunto finito $\{P_1, ..., P_r\}$ de puntos en el espacio proyectivo $\mathbb{P}\left(\bigwedge^n E\right)$, entonces por corolario 2.3 es un sistema proyectivo no degenerado en $\mathbb{P}(\mathbb{V})$

Definición 3.12. $C_{L(n,2n)}$ el código lineal no degenerado asociado a la Lagrangiana-Grassmanniana $L(n, 2n)$ sobre el campo F_q fínito y le llamamos *código Lagrangiano-Grassmanniano*. Aquí la dimensión del código es $dimV$, para $V = kerf$, y la longitud de la palabra es $|L(n, 2n)| = \prod_{i=1}^{n}(1 + q^i)$ y la distancia mínima es

$$d = |L(n, 2n)| - max\{|H \cap L(n, 2n)| : \ H \ es \ un \ hiperplano \ de \ \mathbb{P}(\mathbb{V})\}$$

A continuación mostramos que una cota superior para esta distancia es $q^{n(n+1)/2}$. Desde luego denotemos por $I(n, 2n) = \{(\alpha_1, ..., \alpha_n) \in \mathbb{Z}^{\,n} : 1 \leq \alpha_1 <, ..., < \alpha_n \leq 2n\}$

y para $\alpha = (\alpha_1, ..., \alpha_n) \in I(n, 2n)$, denotemos por $e_\alpha := e_{\alpha_1} \wedge, ..., \wedge e_{\alpha_n}$ la base estándar para $\bigwedge^n E$, donde $e_1, ..., e_{2n}$ es una base de E. Sea $\Lambda_\alpha = \{w \in L(n, 2n) : p_\alpha = 0\}$, donde p_α es el coeficiente correspondiente en coordenadas de Plücker de w en la base estándar $\{e_\alpha : \alpha \in I(n, 2n)\}$ para $\Lambda^n E$

Sea $W \in L(n, 2n)$ sea

$$L_{W,0} := \{W' \in L(n, 2n) : dim(W' \cap W) = 0\}$$

Sean U, W elementos de $L(n, 2n)$ tal que $E \cong U \oplus W$ y si $U^* = Hom_F(U, F)$ es el dual de U, usando el isomorfismo $W \simeq U^*$ dado por $w \longmapsto \langle w, -\rangle : U \longrightarrow F$ y fijando un splitting $E \simeq U \bigoplus U^*$ tenemos una correspondencia uno-a-uno

$$L_{W,0} \longleftrightarrow Hom^{sym}(U, U^*)$$

donde $Hom^{sym}(U, U^*)$ es el espacio de mapeos lineales $f : U \longrightarrow U^*$ tal que $f = f^*$ identificando $f^* : U^{**} \simeq U \longrightarrow U^*$. Se sigue que para $F = F_q$

$$|L_{W,0}| = q^{n(n+1)/2}$$

.

Sea $L^c_{w,0} = \{W' \in L(n, 2n) : dim(W' \cap W > 0)\}$ el complemento de $L_{W,0}$. Si $L \in L^c_{W,0}$ y $\{l_1, ..., l_n\}$ es una base de L, entonces $(l_1\wedge, ..., \wedge l_n) \wedge (v_1\wedge, ..., \wedge v_n) = 0$ dado por otro lado que el conjunto $\{l_1, ..., l_n, v_1, ..., v_n\}$ deben ser linealmente independientes en E . Pero entonces, para $x \in L \cap W$ no cero si nosotros escribimos en la base de L como $x = \sum a_i l_i$,y en la base de W como $x = \sum b_i v_i$ con al menos un coeficiente diferente de cero y así $0 = \sum a_i l_i - \sum b_i v_i$, lo cual es una contradicción. Consecuentemente $(l_1 \wedge \cdots \wedge l_n) \wedge (v_1 \wedge \cdots \wedge v_n) = 0$. Ahora extendemos el conjunto $\{v_1, ..., v_n\}$ a una base $\{v_1, ..., v_n, v_{n+1}, ..., v_{2n}\}$ de E y usamos esta base para definir coordenadas de Plücker para $l_1 \wedge \cdots \wedge l_n = \sum_{\alpha \in I(n,2n)} p_\alpha(v_{\alpha_1} \wedge \cdots \wedge v_{\alpha_n})$. Se sigue que $(l_1 \wedge \cdots \wedge l_n) \wedge (v_1 \wedge \cdots \wedge v_n) = \sum_{\alpha \in I(n,2n)} p_\alpha(v_{\alpha_1} \wedge \cdots \wedge v_{\alpha_n}) \wedge (v_1 \wedge \cdots \wedge v_n) = p_{(n+1,...,2n)}(v_{n+1} \wedge \cdots \wedge v_{2n}) \wedge (v_1 \wedge \cdots \wedge v_n) = 0$ y esto implica que $p_{(n+1,...,2n)} = 0$ lo cual significa que $L^c_{W,0} \subseteq \Lambda_{(n+1,...,2n)}$ y así $\Lambda^c_{(n+1,...,2n)} \subseteq L_{W,0}$, nosotros hemos probado que:

Lema 3.13. $\Lambda^c_{(n+1,...,2n)} \subseteq L_{W,0}$

DEMOSTRACIÓN. Se sigue inmediatamente de arriba □

Obserbe ahora que $L(n, 2n) = \Lambda_{(n+1,...,2n)} \cup \Lambda^c_{(n+1,...,2n)}$ y que $|\Lambda^c_{(n+1,...,2n)}| = |L(n, 2n)| - |\Lambda_{(n+1,...,2n)}|$.

Proposición 3.14. *Para la distancia mínima d del código Lagrangiano-Grassmanniano $C_{L(n,2n)}$ nosotros tenemos que $d \leq q^{n(n+1)/2}$*

DEMOSTRACIÓN. Por defición $d = |L(n, 2n)| - max\{|H \cap L(n, 2n)| : H \text{ es un hiperplano de } \mathbb{P}(\mathbb{V})\} \leq |L(n, 2n)| - |\Lambda_{(n+1,...,2n)}| = |\Lambda^c_{(n+1,...,2n)}|$ y por las obserevaciones previas y lema se sigue que $|\Lambda^c_{(n+1,...,2n)}| \leq |L_{W,0}| = q^{n(n+1)/2}$ □

Ejemplo: Sea $F = F_2$ es fácil que $L(2, 4)$ es una hipersuperficie de $\mathbb{P}^{\not 4}$ generada cuadrica (una variante de la cuadrica de Klein):

$$x_{12}x_{34} - x_{13}x_{24} + x_{14}^2 = 0$$

y también que

$$\begin{aligned} L(2,4)(F_2) = \{&(10000), (00001), (01000), (00010), (11000), \\ &(00011), (10010), (01001), (11011), (10101), (01110), \\ &(11101), (10111), (01111), (11110)\} \end{aligned}$$

ii) La siguiente matriz de orden 10×15

$$H := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

del código Lagrangiano grassmanniano $C_{L(2,4)}(F_2)$

iii) Usando el teorema que establece que: La distancia mínima de un código es igual al número mínimo de columnas linealmente dependientes de H la matriz de paridad de chequeo ver lemma 2.10 y el inciso (ii) anterior tenemos que la distancia mínima d de $C_{L(2,4)}(F_2)$ es igual a 6 y así para este caso vemos que la desigualdad es estricta en la proposición 3.14 de arriba.

3.4. Geometría del espacio V

Elegimos una base $\{e_1, ..., e_{2n}\}$ de el espacio simpléctico E tal que

$$\langle e_i, e_j \rangle = \begin{cases} 1 & si\ j = 2n + 1 - i\,, \\ 0 & en\ otro\ caso \end{cases}$$

para el mapeo lineal $f : \bigwedge^n E \longrightarrow \bigwedge^{n-2} E$ de la definición 4.9 . Escribimos $w \epsilon \wedge^n E$ en coordenadas de Plücker $w = \sum_{\alpha \epsilon I(n,2n)} p_\alpha e_\alpha$ donde

$$e_\alpha := e_{\alpha_1} \wedge ... \wedge e_{\alpha_n}$$

entonces aplicando f y usando la siguiente notación

$$e_{\alpha_{rs}} := e_{\alpha_1} \wedge ... \wedge \widehat{e_{\alpha_r}} \wedge ... \widehat{e_{\alpha_r}} \wedge ... \wedge e_{\alpha_n}$$

para $1 \leq r < s <\leq n$

$$\sigma(e_{\alpha_{rs}}) := \sigma(e_{\alpha_1}) \wedge ... \wedge \widehat{\sigma}(e_{\alpha_r}) \wedge ... \widehat{\sigma}(e_{\alpha_r}) \wedge ... \wedge \sigma(e_{\alpha_n})$$

vemos que

$$\begin{aligned} f(w) &= \sum_{\alpha \epsilon I(n,2n)} p_\alpha f(e_\alpha) \\ &= \sum_{\alpha \epsilon I(n,2n)} p_\alpha (\sum_{1 \leq r < s \leq n} < e_{\alpha_r}, e_{\alpha_s} > e_{\alpha_{rs}}) \\ &= \sum_{1 \leq r < s \leq n} (\sum_{1 \leq \beta_1 < \beta_2 \leq n} (sgn(\sigma) p_{\sigma(\alpha_{rs})\sigma(\beta_1)\sigma(\beta_2)} < e_{\beta_1}, e_{\beta_2} >)) e_{\alpha_{rs}} \end{aligned}$$

donde σ es una permutación de $\{\alpha_1, ..., \widehat{\alpha_r}, ..., \widehat{\alpha_s}, ..., \alpha_n, \beta_1, \beta_2\}$ tal que

$(\sigma(\alpha_1), ..., \widehat{\sigma}(\alpha_r), ..., \widehat{\sigma}(\alpha_s)..., \sigma(\alpha_n), \sigma(\beta_1), \sigma(\beta_2)) \epsilon I(n, 2n)$.
Denotamos por V el kernel de f.

Lema 3.15. *$w \epsilon V$ si y sólo si $\sum_{i=1}^{n}, a_{i,\alpha_1,...,\alpha_{(n-2)},2n-i+1} p_{i,\alpha_1,...,\alpha_{n-2},2n-i+1} = 0$ para todo $1 \leq \alpha_1 < \cdots < \alpha n - 2 \leq 2n$ y*

$$a_{i,\alpha_1,...,\alpha_{n-2},2n-i+1} = \begin{cases} 1 & si\ |i, \alpha_1, ..., \alpha_{n-2}, 2n-i+1| = n \\ 0 & en\ otro\ caso \end{cases}$$

DEMOSTRACIÓN. $w \epsilon V$ si y sólo si

$\sum_{1 \leq \beta_1 < \beta_2 \leq n} sgn(\sigma) p_{\sigma(\alpha_{rs})\sigma(\beta_1)\sigma(\beta_2)} < e_{\beta_1}, e_{\beta_2} >= 0$

para todo $1 \leq \alpha_1 < ... < \widehat{\alpha_r} < ... < \widehat{\alpha_s} < ... \leq \alpha_n$ y σ como arriba, y dado que $\{e_i\}_1^n$ es una base simpléctica tenemos que

$\sum_{1 \leq \beta_1 < \beta_2 \leq n} sgn(\sigma) p_{\sigma(\alpha_{rs})\sigma(\beta_1)\sigma(\beta_2)} < e_{\beta_1}, e_{\beta_2} >=$
$= \sum_{i=1}^{n} sgn(\sigma) a_{\alpha_{rs}} p_{\sigma(\alpha_{rs})\sigma(i)\sigma(2n-i+1)} \langle e_i, e_{2n-i+1} \rangle = 0$ donde $a_{\alpha_{rs}}$ como en la proposición, y reordenando los indices de p usando la permutación inversa σ^{-1} el resultado se sigue.

□

Para $1 \leq \alpha_1 <, ..., < \alpha_{n-2} \leq 2n$ y $a_{i,\alpha_1,...,\alpha_{n-2},2n-i+1}$ como en el lema anterior, considere los siguientes polinomios lineales y los hiperplanos en $\mathbb{P}\left(\bigwedge^n E\right)$ definido por estos

$$\Pi_{\alpha_1,\alpha_2,...,\alpha_{n-2}} = \sum_{i=1}^{n} a_{i,\alpha_1,...,\alpha_{n-2},2n-i+1} X_{i,\alpha_1,...,\alpha_{n-2},2n-i+1}$$

donde $X_\alpha \in F_q[X_\alpha]_{\alpha \in I(n,2n)}$ una variable en el anillo de polinomios indicado.

Corolario 3.16. $V = \{w \epsilon \wedge^n E : \Pi_{\alpha_1,\alpha_2,...,\alpha_{n-2}}(x) = 0\ para\ todo\ 1 \leq \alpha_1 \leq \alpha_2, ..., \leq \alpha_{n-2} \leq 2n\}$

DEMOSTRACIÓN. Se sigue facilmente del corolario 2.5 arriba.

□

Ejemplos:

En los siguiente ejemplos E es un espacio vectorial simpléctico de dimensión $2n$ con $\{e_1, e_2, ..., e_{2n}\}$ una base simpléctica ver (1) de esta notas.

1) Si $n = 2$ entonces claramente $f : \wedge^2 E \to \wedge^0 E \cong F$ es suprayectivo y así $dimV = 5$

2)Si $n = 3$ entonces es fácil probar directamente que $f : \wedge^3 E \to \wedge^1 E \cong E$ es suprayectivo y así $dimV = 14$

3) Si $n = 4$ entonces V es la solución del siguiente sistema de ecuaciones el cual escribimos explicitamente:

$$
\begin{aligned}
&X_{1278} + X_{1368} + X_{1458} = 0\\
&X_{1278} + X_{2367} + X_{2457} = 0\\
&X_{1368} + X_{2367} + X_{3456} = 0\\
&X_{1458} + X_{2457} + X_{3456} = 0\\
&X_{1236} + X_{1245} = 0\\
&X_{1237} - X_{1345} = 0\\
&X_{1247} + X_{1346} = 0\\
&X_{1257} + X_{1356} = 0\\
&X_{1267} - X_{1456} = 0\\
&X_{1367} + X_{1457} = 0\\
&X_{1238} + X_{2345} = 0\\
&X_{1248} - X_{2346} = 0\\
&X_{1258} - X_{2356} = 0\\
&X_{1268} + X_{2456} = 0\\
&X_{2368} + X_{2458} = 0\\
&X_{1348} + X_{2347} = 0\\
&X_{1358} + X_{2357} = 0\\
&X_{1378} + X_{3457} = 0\\
&X_{2378} - X_{3458} = 0\\
&X_{1468} + X_{2467} = 0\\
&X_{1478} - X_{3467} = 0\\
&X_{2478} + X_{3468} = 0\\
&X_{1568} + X_{2567} = 0\\
&X_{1578} - X_{3567} = 0\\
&X_{2578} + X_{3568} = 0\\
&X_{1678} + X_{4567} = 0\\
&X_{2678} - X_{4568} = 0\\
&X_{3678} + X_{4578} = 0
\end{aligned}
$$

podemos observar que este sistema es de 28×70 y las 24 ecuaciones con sólo 2 variables todas son linealmente independientes ya que ninguna variable se repite.

Por otro lado el subsistema de 4 ecuaciones (con tres variables cada una), tiene la siguiente forma:

$$A_1 + A_2 + A_3 = 0$$

$$A_1 + A_4 + A_5 = 0$$
$$A_2 + A_4 + A_6 = 0$$
$$A_3 + A_5 + A_6 = 0$$

usando operaciones elementales de matrices tenemos que

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \sim ... \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & -2 & -2 & -2 \end{pmatrix}$$

Claramente si $CharF = 2$ entonces el rango de nuestro sistema es 27 y si $CharF \neq 2$ entonces el rango es 28. En el primer caso f no es un epimorfismo y en el segundo f si es epimorfismo.

3.5. Otra construcción de V

Sea n entero positivo y sea $W \in G(n, 2n)$, también consideremos una base fija $v_1, v_2, ..., v_n$ del espacio W donde $v_i := (w_{i,1}, w_{i,2}, ..., w_{i,2n})$ con $w_{i,j}$ elementos del campo. Denotamos por G_W la matriz de orden $n \times 2n$ usando los vectores básicos de la base fija, así:

$$G_W := (w_{ij})$$

A continuación definimos la función

$$P_{i \sqcup (2n-i+1)}$$

del anillo de matrices de orden $n \times (n-2)$ al campo F tal que

$$x := \begin{pmatrix} a_{1,1} & a_{1,2} & ... & a_{1,(n-2)} \\ a_{2,1} & a_{2,2} & ... & a_{2,(n-2)} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ a_{n,1} & a_{n,2} & ... & a_{n,(n-2)} \end{pmatrix} \mapsto P_{i \sqcup (2n-i+1)}(x)$$

donde

$$P_{i \sqcup (2n-i+1)}(x) := det \begin{pmatrix} w_{1,i} & a_{1,1} & a_{1,2} & ... & a_{1,(n-2)} & w_{1,(2n-i+1)} \\ w_{2,i} & a_{2,1} & a_{2,2} & ... & a_{2,(n-2)} & w_{2,(2n-i+1)} \\ . & . & . & ... & . & . \\ . & . & . & ... & . & . \\ . & . & . & ... & . & . \\ w_{n,i} & a_{n,1} & a_{n,2} & ... & a_{n,(n-2)} & w_{n,(2n-i+1)} \end{pmatrix}$$

Con lo anterior definimos la función :

$$\Psi_W : M_{n\times(n-2)} \longrightarrow \mathbb{F}$$

tal que

$$\Psi_W(x) = \sum_{i=1}^{n} P_{i\sqcup(2n-i+1)}(x)$$

Sea D una matriz de orden $k \times n$, el k-menor obtenido de la matriz D por mantener

sólo los elementos pertenecientes a renglones con sufijos $r_1, ..., r_k$ y columnas con sufijos $s_1, ..., s_k$ es denotado por

$$D(r_1, ..., r_k|s_1, ..., s_k)$$

Definición 3.17. El *cofactor* o *complemento algebraico* $\widetilde{D}(r_1, ..., r_k|s_1, ..., s_k)$ del menor $D(r_1, ..., r_k|s_1, ..., s_k)$ en un determinante D es definido como

$$\widetilde{D}(r_1, ..., r_k|s_1, ..., s_k) = (-1)^{r_1+...+r_k+s_1+...+s_k} D(r_{k+1}, ..., r_n|s_{k+1}, ..., s_n)$$

donde $r_{k+1}, ..., r_n$son los $(n-k)$ números entre 1,...,n diferentes de $r_1, ..., r_k$ y los otros $s_{k+1}, ..., s_n$ son los números entre 1,...,n diferentes de $s_1, ..., s_k$

Para comodida del lector enunciamos sin prueba el teorema de expanción de Laplace.

Teorema 3.18. *(de expanción de Laplace) Sea D un determinante de orden n , y sea $r_1, ..., r_k$ enteros tal que $1 \leq k < n$ y $1 \leq r_1 < ... < r_k \leq n$. Entonces*

$$D = \sum_{1\leq u_1<...<u_k\leq n} D(r_1, ..., r_k|u_1, ..., u_k)\widetilde{D}(r_1, ..., r_k|u_1, ..., u_k)$$

Sean $a := 1+2+...+(n-2)$ y $b(r, s) := (-1)^{a+(1+2+...+\widehat{r}+...+\widehat{s}+...n)}$ (donde $\widehat{r}$ y $\widehat{s}$ son omitidos de la suma) y $1 \leq r < s \leq n$.

Aquí x^T denota la matriz transpuesta del elemento $x\epsilon M_{n\times(n-2)}$ y los determinantes

$$D_{x^T}(r_1, ..., r_k|u_1, ..., \widehat{u_r}, ...\widehat{u_s}, ..., u_k)$$

y

$$\widetilde{D}_{x^T}(r_1, ..., r_k|u_1, ..., \widehat{u_r}, ...\widehat{u_s}, ..., u_k)$$

se interpretan de acuerdo a la notación de la sección (6.2) aplicados a la matriz de orden $n \times n$ que resulta de aplicar $P_{i\sqcup(2n-i+1)}$ al elemento x.

Lema 3.19. *Sea $n \geq 2$ entero positivo y sea $W\epsilon G(n, 2n)$ entonces*

$$\Psi_W(x) = (-1)^{n-2} \sum_{1\leq r<s\leq n} b(r, s)\langle v_r, v_s\rangle D_{x^T}(1, 2, ..., (n-2)|1, 2, ...\widehat{r}, ..., \widehat{s}, ..., n)$$

(donde $\widehat{r}$ y $\widehat{s}$ son omitidos) para todo $x\epsilon M_{n\times(n-2)}$

DEMOSTRACIÓN. Por definición tenemos:

$$P_{i\sqcup(2n-i+1)}(x) = (-1)^{(n-2)} det \begin{pmatrix} a_{1,1} & a_{2,1} & ... & a_{n,1} \\ a_{1,2} & a_{2,2} & ... & a_{n,2} \\ . & . & ... & . \\ . & . & ... & . \\ . & . & ... & . \\ a_{1,(n-2)} & a_{2,(n-2)} & ... & a_{n,(n-2)} \\ w_{1,i} & w_{2,i} & ... & w_{n,i} \\ w_{1,(2n-i+1)} & w_{2,(2n-i+1)} & ... & w_{n,(2n-i+1)} \end{pmatrix}$$

$= (-1)^{(n-2)} \sum_{1\leq u_1<...<u_{n-2}\leq n} D_{x^T}(1,...,(n-2)|u_1,...,u_{n-2})$

$\cdot \widetilde{D}(1,...,(n-2)|u_1,...,u_{n-2}) =$

$$= (-1)^{(n-2)}\{b(1,2) det \begin{pmatrix} w_{1,i} & w_{2,i} \\ w_{1,(2n-i+1)} & w_{2,(2n-i+1)} \end{pmatrix} D_{x^T}(1,...,(n-2)|3,...,n)$$

$$+b(1,3) det \begin{pmatrix} w_{1,i} & w_{3,i} \\ w_{1,(2n-i+1)} & w_{3,(2n-i+1)} \end{pmatrix} D_{x^T}(1,2,...,(n-2)|2,4,5,...,n)+$$

$$+...+$$

$$b((n-1),n) det \begin{pmatrix} w_{(n-1),i} & w_{n,i} \\ w_{(n-1),(2n-i+1} & w_{n,(2n-i+1)} \end{pmatrix} D_{x^T}(1,2,...,(n-2)|1,2,...,(n-2))\}$$

Así por definición tenemos que:

$$\Psi_W(x) = \sum_{i=1}^{n} P_{i\sqcup(2n-i+1)}(x) =$$

$$= (-1)^{n-2} b(1,2)\{\sum_{i=1}^{n} det \begin{pmatrix} w_{1,i} & w_{2,i} \\ w_{1,(2n-i+1)} & w_{2,(2n-i+1)} \end{pmatrix}\} D_{x^T}(1,2,...,(n-2)|3,4,...,n)+$$

$$+(-1)^{(n-2)}b(1,3)\{\sum_{i=1}^{n} det\begin{pmatrix} w_{1,i} & w_{3,i} \\ w_{1,(2n-i+1)} & w_{3,(2n-i+1)} \end{pmatrix}\}D_{x^T}(1,2,...,(n-2)|2,4,,5,...,n)+$$

$$+...+$$

$$+(-1)^{(n-2)}b((n-1),n)\{\sum_{i=1}^{n} det\begin{pmatrix} w_{(n-1),i} & w_{n,i} \\ w_{(n-1),(2n-i+1)} & w_{n,(2n-i+1)} \end{pmatrix}\}D_{x^T}(1,2,...,(n-2)|1,2,...,(n-2)) =$$

$$= (-1)^{n-2}b(1,2)\langle v_1,v_2\rangle D_{x^T}(1,2,...,(n-2)|3,4,...,n)+$$

$$+(-1)^{n-2}b(1,3)\langle v_1,v_3\rangle D_{x^T}(1,2,...,n|2,4,5,...,n)+$$

$$+\ldots+$$

$$+(-1)^{n-2}b(n-1,n)\langle v_{n-1},v_n\rangle D_{x^T}(1,2,...,(n-2)|1,2,...,(n-2)) = 0$$

Por lo tanto tenemos que

$$\Psi_W(x) = (-1)^{n-2}\sum_{1\leq r<s\leq n} b(r,s)\langle v_r,v_s\rangle D_{x^T}(1,2,...,(n-2)|1,2,...\widehat{r},...,\widehat{s},...,n)$$

(donde $\widehat{r}$ y $\widehat{s}$ son omitidos) para todo $x\epsilon M_{n\times(n-2)}$

□

Lema 3.20. *Para cada $1 \leq r < s \leq n$ existe un elemento $x_{\alpha\beta}$ en $M_{n\times(n-2)}$ tal que*

$$D_{x^T}(r_1,...,r_k|u_1,...,\widehat{u_r},...\widehat{u_s},...,u_k) = \begin{cases} 1 & si\ r=\alpha\ y\ s=\beta \\ 0 & en\ otro\ caso \end{cases}$$

DEMOSTRACIÓN. $x_{\alpha\beta}$ es la matriz de orden $n \times (n-2)$ tal que las columnas

$$\begin{pmatrix} x_{1\alpha} \\ x_{2\alpha} \\ \cdot \\ \cdot \\ \cdot \\ x_{n\alpha} \end{pmatrix} y \begin{pmatrix} x_{1\beta} \\ x_{2\beta} \\ \cdot \\ \cdot \\ \cdot \\ x_{n\beta} \end{pmatrix}$$

de la matriz $x_{\alpha\beta}$ son columnas de ceros. En las otras $n-2$ colunas acomodamos la matriz identidad de orden $(n-2) \times (n-2)$. Es fácil ver que esta matriz cumple la afirmación del lema. □

Teorema 3.21. *Sea* $W \epsilon G(n, 2n)$ *entonces* $W \epsilon L(n, 2n)$ *si y sólo si* $\Psi_W(x) = 0$ *para todo* $x \epsilon M_{n\times(n-2)}$

DEMOSTRACIÓN. Esto es consecuencia inmediata de los lemas de 3.19 y 3.20 □

El Teorema anterior puede expresarse, como la siguiente fórmula en coordenadas de Plücker :

$$P_{1\sqcup 2n} + P_{2\sqcup(2n-1)} + ... + P_{n\sqcup(n+1)} = 0$$

3.6. Código Lagrangiano-Grassmanniano de una Variedad de Schubert

Sea $F = F_q$ un campo fínito y E un F-espacio vectorial simpléctico de dimensión $2n$, $L(n, 2n)$ la variedad Lagrangiana-Grassmanniana como en la seción 3.1 de este documento.

Definición 3.22. Sea $W : 0 \subset W_1 \subset W_2 \subset \cdots \subset W_n \subset E$ una bandera fija de subespacios isotrópicos de E tal que $dim W_i = i$ para todo $i = 1, 2, ..., n$. Tal bandera es llamada *Bandera Isotropica* de E

Aquí W_n es subespacio isotrópico de dimensión n así que $W_n \in L(n, 2n)$.En otras palabras, una bandera isotrópica completa no es otra cosa que un subespacio $W_n \in L(n, 2n)$ junto con una bandera completa de subespacios de W_n. Note que cada bandera isotrópica $W : 0 \subset W_1 \subset W_2 \subset \cdots \subset W_n \subset E$ puede ser completada a una bandera completa en E por poner $W_{n+i} = W_{n-i}^{\perp}$ para todo $1 \leq i \leq n$.

Definición 3.23. Sea $\lambda = (\lambda_1, ..., \lambda_n) \in I(n, 2n)$. Sea $W : 0 \subset W_1 \subset W_2 \subset \cdots \subset W_n \subset E$ una bandera isotrópica completa de E. Con respecto a esta partición λ definimos la *variedad de Schubert* en el caso de la Lagrangiana-Grassmanniana como

$$L(n, 2n)_\lambda := \{W \in L(n, 2n) : dim(W \cap W_{n+1-\lambda_i}) \geq i, 1 \leq i \leq l(\lambda)\}$$

donde $l(\lambda) = |\{p \in: \lambda_p \neq 0\}|$.

Se sabe que $L(n, 2n)_\lambda$ es una subvariedad proyectiva de $L(n, 2n)$ de codimensión $|\lambda| := \sum_{p=1}^{l} \lambda_p$ en $\mathbb{P}(\bigwedge^{\kappa} \mathbb{E})$ bajo la inclusión de Plücker.

Sea $r = r(\lambda) := |L(n, 2n)_\lambda|$ el cual es fínito por ser F_q fínito. Supongamos que $L(N, 2n)_\lambda = \{P_1, ..., P_r\}$ una familia de r representantes, hasta proporcionalidad, en $\mathbb{P}(\bigwedge^{\kappa} \mathbb{E})$.

Sea $K = \{h \in (\bigwedge^n E)^* : h(P_1) = \cdots h(P_r) = 0\}$

y sean

$V = \{w \in \bigwedge^n E : h(w) = 0 \, para \, todo \, h \in K\}$ como en la sección 2.

Entonces $L(n, 2n)_\lambda$ es un sistema proyectivo no degenerado en $\mathbb{P}(\mathbb{V})$ y sea $C_{L(n,2n)_\lambda}$ el código lineal no degenerado asociado a este sistema lineal no proyectivo.

-

3.7. Pesos grandes para el código $C_{L(n,2n)}$

Si el campo es $F = F_q$ fínito entonces sean $\chi_{G(n,2n)}$ y $\chi_{L(n,2n)}$ los sistemas proyectivos generados por la variedad de Grassmann y la variedad Lagrangiana-Grassmanniana, respectivamente, bajo la inclusión de Plücker y sean $C(n, 2n)$ y $C_{L(n,2n)}$ los códigos lineales no degenarados inducidos (bajo la inclusión de Plücker) por las variedades algebraicas $G(n, 2n)$ y $L(n, 2n)$ respectivamente.

Para un entero no negativo r consideremos las secciones lineales $H \bigcap G(n, 2n)$ y $H \bigcap L(n, 2n)$ de la variedad de Grassman y de la variedad Lagrangiana-Grassmsnniana, por una subvariedad lineal H de codimensión r en $\mathbb{P}\,(\bigwedge^n E)$ y de $\mathbb{P}(\mathbb{V})$ respectivamente.

Definimos el r-peso grande del código de Grassmann y del código Lagrangiano Grassmanniano $d_r(C(n, 2n))$ y $d_r(C_{L(n,2n)})$, respectivamente por:

a) $|G(n, 2n)| - max_{H \leq \mathbb{P}(\wedge^{\kappa} \mathbb{E})}\{|H \bigcap G(n, 2n)| : codimH = r\}$

b) $|L(n, 2n)| - max_{H \leq \mathbb{P}(\mathbb{V})}\{|L(n, 2n) \bigcap H| : codimH = r\}$

Es bien conocido que $d_r(C(l, m-l)) \geq q^\delta + ... + q^\delta - r + 1$ donde $\delta = n(2n-n)$ y si r es pequeño o más precisamente, cuando $r \leq max\{l, m-l\}$ entonces $d_r(C(l, m-l)) = q^\delta + ... + q^\delta - r + 1$

Sea H hiperplano de codimensión r en $\mathbb{P}(\mathbb{V})$ entonces H es un hiperplano de codimensión R(con $R > r$), en $\mathbb{P}(\wedge^{\kappa}\mathbb{E})$.

Sea H un hiperplano de $\mathbb{P}(\mathbb{V})$ de codimensión r entonces:

$$|L(n,2n) \bigcap H| = |G(n,2n) \bigcap \mathbb{P}(\mathbb{V}) \bigcap \mathbb{H}| = |G(n,2n) \bigcap H|$$

Esto implica que

$$max_{H \leq \mathbb{P}(\mathbb{V})}\{|L(n,2n) \bigcap H| : codimH = r\}$$

$$= max_{H \leq \mathbb{P}(\mathbb{V})}\{|G(n,2n) \bigcap H| : codimH = r\}$$

$$\leq max_{H \leq \mathbb{P}(\wedge^{\kappa}\mathbb{E})}\{|G(n,2n) \bigcap H| : codimH = R\}$$

$$|L(n,2n)| - max_{H \leq \mathbb{P}(\wedge^{\kappa}\mathbb{E})}\{|G(n,2n) \bigcap H| : codimH = R\}$$

$$\leq |L(n,2n)| - max_{H \leq \mathbb{P}(\mathbb{V})}\{|L(n,2n) \bigcap H| : codimH = r\}$$

De lo anterior podemos comcluir el siguiente teorema

$|L(n,2n)| - |G(n,2n)| + |G(n,2n)| - max_{H \leq \mathbb{P}(\wedge^{\kappa}\mathbb{E})}\{|G(n,2n) \bigcap H| : codimH = R\} \leq d_r(C_{L(n,2n)})$

$$|L(n,2n)| - |G(n,2n)| + d_R(C(n,2n)) \leq d_r(C_{L(n,2n)})$$

De lo anterior podemos concluir el siguiente teorema

Teorema 3.24. $|L(n,2n)| - |G(n,2n)| + d_R(C(n,2n)) \leq d_r(C_{L(n,2n)})$

□

Corolario 3.25. $|L(n,2n)| - |G(n,2n)| + d_R(C(n,2n)) \leq d_r(C_{L(n,2n)}) \leq |L(n,2n)| - \dim V + r$
donde $R = \binom{2n}{n} - \dim V + r$ *y* $|G(n,2n)| = \binom{2n}{n}_q$

Ahora siguiendo la sección 5 de [8], fijamos un conjunto $T(n,2n) = \{W - 1, \ldots, W_t\}$ de representantes en $\bigwedge^n E$ correspondiente a los puntos de $G(n,2n)$. Dado un subespacio S de $\bigwedge^n E$, nosotros ponemos $g(S) = |S \cap T(n,2n)|$ y sea

$$g_r(n,2n) = max\{g(S) : \text{S es subespacio de codimensión r de } \bigwedge^n E\}$$

Consideremos el mapeo lineal f y $V = \ker f$, entonces $|L(n,2n)| = g(V)$ y es inmediato que $g(V) \leq g_r(n,2n)$ para $r = \binom{2n}{n} - \dim V$. Consecuentemente por el corolario 17 de [8] obtenemos

$$d_r(C_{L(n,2n)}) = |G(n,2n)| - g_r(n,2n) \leq |G(n,2n)| - g_r(V) = |G(n,2n)| - |L(n,2n)|$$

y con esto hemos probado la siguiente proposición.

Proposición 3.26. *Si* $1 \leq r \leq \binom{2n}{n}$, *entonces* $d_r(C(n,2n)) \leq |G(n,2n)| - |L(n,2n)|$

□

También siguiendo [8] podemos determinar el número máximo de puntos en las secciones lineales H de $L(n,2n)$ para subvariedades lineales $H \subseteq \mathbb{P}(\bigwedge^n E)$ de codimensión r. Este problema puede trasladarse al mismo problema para la variedad de Grassmann como sigue: Sea H la subvariedad lineal de codimensión r del espacio proyectivo $\mathbb{P}(V) = Z\langle g_1, \ldots, g_N\rangle$. Podemos calcular el número de puntos en la intersección $H \cap L(n,2n)$. Así hemos probado la siguiente proposición

Proposición 3.27. *Si* Λ *es una familis cerrada de* $I(n,2n)$ *con* k *elementos entonces* $|H_\Lambda \cap L(n,2n)| \leq \binom{2n}{n}_q - q^{n^2} - \cdots q^{n^2-k-1}$

□

3.8. Ejemplos

A) Si $F = F_q$ y $r = 1$ entonces tenemos que:
$R = 2$ y $|L(2,4)| - |G(2,4)| + d_2(C(2,4)) \leq d_1(C_{L(2,4)})$

$(1+q)(1+q^2) + (q^4+q^3) \leq \frac{(q^4-1)(q^4-q)}{(q^2-1)(q^2-q)} + d_1(C_{L(2,4)})$
$(1+q)(1+q^2) \leq 2q^2 + q + 1 + d_1(C_{L(2,4)})$
$(1+q)(1+q^2) \leq (q+1)^2 + q^2 - q + d_1(C_{L(2,4)})$
$(1+q)(q^2-q) \leq q^2 - q + d_1(C_{L(2,4)})$
$q^3 - q \leq q^2 - q + d_1(C_{L(2,4)})$
Así hemos obtenido una cota inferior para la distacia minima:

$q^3 - q^2 \leq d_1(C_{L(2,4)})$

Sea Λ_{14} la intersección de $L(n,2n)$ con el hiperplano coordenado

$$H_{14} := Z < x_{14} >$$

la ecuación homogenea de esta intersección es

$$x_{12}x_{34} - x_{13}x_{24} - x_{14}^2 = 0 \; y \; x_{14} = 0$$

así que $\Lambda_{14} = \{(P_{12}, P_{13}, P_{14}, P_{24}, P_{34}) \epsilon L(n,2n) : P_{14} = 0\}$

Claramente $\Lambda_{14} = L(n,2n) \bigcap Z < x_{14} >$ es una hipersuperficie dada por la ecuación

$$x_{12}x_{34} - x_{13}x_{24} = 0$$

entonces existe una correspondencia uno-uno;

$$\mathbb{P} \times \mathbb{P} \leftrightarrow \Lambda_{14}$$

(Por la inclusión de Segre) dada por la correspondencia

$$[[a:b] : [c:d]] \mapsto (ac, ad, bc, bd)$$

Si $F = F_q$ entonces $|\Lambda_{14}| = |\mathbb{P} \times \mathbb{P}| = (1+q)^2$

$|\Lambda_{14}| \leq max\{|L(2,4) \bigcap H| : H\ hiperplano\ de\ \mathbb{P}(V)\ de\ codimension\ 1\}$ $d = |L(2,4)| - max\{|L(2,4)| \bigcap H| : H\ hiperplano\ de\ \mathbb{P}(V)\ de\ codimension\ 1\}$ $\leq |L(2,4)| - |\Lambda_{14}| = (1+q)(1+q)^2 - (1+q)^2 = q^3 - q$ Así acotamos inferior y superior la distancia mínima

$$q^3 - q^2 \leq d \leq q^3 - q$$

En general, para $C_{L(n,2n)}$ podemos dar una cota inferior para la distancia mínima $d = d_1$;

B) Como segunda aplicación tenemos en general, una cota inferior para la distancia mínima $d = d_1$ del código Lagrangiano-Grassmanniano $C_{L(n,2n)}$ en terminos de pesos grandes del código de Grassmann $G(n, 2n)$

Corolario 3.28. $|L(n,2n)| - |G(n,2n)| + d_R(C(n,2n)) \leq d_1(C_{L(n,2n)})$ *donde* $R = dim \bigwedge^n(E) - dimV + 1$

DEMOSTRACIÓN. Es consecuencia del teorema 3.23. □

Proposición 3.29. *El código Lagrangiano-Grassmanniano* $C_{L(n,2n)}$ *es un código ágebro-geométrico de intersección.*

DEMOSTRACIÓN. Se sigue directamente del lema 3.10 □

Capitulo 4

Conclusiones y Perspectivas

3.9. Conclusiones

Estas pueden enumerarse de la siguiente manera:
1) Los códigos algebro-geoetricos de intersección son una generalización de los códigos de Schubert y los códigos Lagrangiannos-Grassmannianos.
2) La dimensión del código Lagrangianno-Grassmanniano puede calcularse algoritmicamente.
3) Existe una relación entre los pesos grandes del código de Grassmann y el código Lagrangiano-Grassmanniano.

3.10. Perspectivas

Las perspectivas pueden enumerarse de la siguiente manera:
1) Demostrar que en los códigos algebro-geoetricos de intersección que resultan de tomar todos los puntos racionales de la intersección de una variedad proyectiva y una variedad lineal, que sea ademas el cociente de la acción de un grupo el cual actua transitivamente, pueden calcularse de manera canónica; la longitud de las palabras y la dimensión del código.
2) Determinar los parametros básicos del código Lagrangiano-Grassmanniano de una variedad de Schubert. 3) Demostrar que el código Lagrangiano-Grassmanniano de una variedad de Schubet es una genralización del código Lagranggiano-Grassmanniano.
4) Estudiar el comportamiento de los pesos grandes de los códigos algebro-geometricos de intersección.

Bibliografía

1. R. Bernt, *An introduction to Symplectic Geometry* amer. Math Soc. Providence (1998)
2. $ay - Chaud4ed4$ Bose. R. C. and Ray-Chaudhuri D. K. .^{o}n a class of error-correcting binary group codesÏnformation and Control, 1960, 68-79.
3. $34wnskirop$ J. Buczynski "Properties of Legendrian Subvarieties of Projective Space "Geometria Dedicata 118, 2006, 87-103.
4. $resvcrt$ J. Carrillo-Pacheco and F. Zaldivar .^{o}n Lagrangian-Grassmannian Codes", Designs, Codes and Criptography DOI 10.1007/s10623-010-9434-4
5. $tfdc543ed$ J. Carrillo-Pacheco and F. Zaldivar "Higher Weights of Lagrangian-Grassmannian Codes.^{En}viado (2010)
6. Cornell, G., Silverman, J. (Eds.), *Arithmetic Geometry*. Springer-Verlag, New York, (1986).
7. Deligne, P. et al, SGA 4 1/2: *Cohomologie étale*. Lecture Notes in Mathematics **569**, Springer-Verlag, Berlin, 1977.
8. Freitag, E., Kiehl, R., *Étale Cohomology and the Weil Conjecture*. Springer-Verlag, Berlin, 1988.
9. Fulton W., *Algebraic Curves*. Addison-Wesley, Reading (1989).
10. Greenberg, M. and Harper, J., *Algebraic Topology, A First Course*. Addison-Wesley, Reading, 1980.
11. Grothendieck, A., Dieudonne, J., *Eléments de Géometrie Algébrique* I. Publ. Math. IHES **4**, (1960).
12. Grothendieck, A., Dieudonne, J., *Eléments de Géometrie Algébrique* IV. Publ. Math. IHES **32**, (1967).
13. Grothendieck, A., Sur quelques points d'algèbre homologique, *Tôhoku Math. J.* **9** (1957), 119-221.
14. Guillemin V., Pollack A., *Topología diferencial*. Sociedad Matemática Mexicana, México, 2003.
15. Hartshorne, R., *Algebraic Geometry*. Springer-Verlag, New York, 1977.
16. Lütkebohmert, W., On compactification of schemes. *Manuscripta Math.* **80** (1993), 95-111.
17. McLane, S., *Categories for the Working Mathematician*. Springer-Verlag, Berlin, 1979.
18. Milne, J., *Étale Cohomology*. Princeton University Press. Princeton, 1980.
19. Milne, J., *Lectures on étale cohomology*. v2.10 (20 de mayo 2008).
20. Milne J., *Abelian Varieties.* v2.00 (17 de marzo 2008).

21. Mumford, D., *Abelian Varieties.* Oxford University Press (1970).
22. Mumford, D., *The Red Book of Varieties and Schemes*. Springer-Verlag, Berlin, 1999.
23. Murre, J. P., *An Introduction to Grothendieck's Theory of the Fundamental Group.* Tata Institute of Fundamental Research, Bombay (1967).
24. Nagata, M., Imbedding of an abstract variety in a complete variety. *J. Math. Kyoto Univ*. **2** (1962), 1-10.
25. Nagata, M., A generalization of the imbedding problem of an abstract variety in a complete variety. *J. Math. Kyoto Univ*. **3** (1963), 89-102.
26. Shatz, S., *Profinite Groups, Arithmetic, and Geometry*. Annals of Math. Studies 67, Princeton University Press, Princeton, 1972.
27. Silverman J. H., *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York (1986).
28. Tamme, G., *Introduction to Étale Cohomology*. Springer-Verlag, Berlin, 1989.
29. Zaldívar, F., *Cohomología de Galois de campos locales*. Sociedad Matematica Mexicana, México, 2001.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE DISERTACIÓN PÚBLICA

No. 00018
Matrícula: 206180460

CODIGOS
LAGRANGIANOS-GRASSMANNIANOS

En México, D.F., se presentaron a las 12:00 horas del día 18 del mes de noviembre del año 2011 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. XAVIER GOMEZ MONT
DR. MARIO PINEDA RUELAS
DR. PEDRO LUIS DEL ANGEL RODRIGUEZ
DR. GERARDO VEGA HERNANDEZ
DR. FELIPE DE JESUS ZALDIVAR CRUZ

JESUS CARRILLO PACHECO
ALUMNO

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron a la presentación de la Disertación Pública cuya denominación aparece al margen, para la obtención del grado de:

DOCTOR EN CIENCIAS (MATEMATICAS)

DE: JESUS CARRILLO PACHECO

y de acuerdo con el artículo 78 fracción IV del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

REVISÓ

LIC. JULIO CESAR DE LARA ISASSI
DIRECTOR DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JOSE ANTONIO DE LOS REYES HEREDIA

PRESIDENTE

DR. XAVIER GOMEZ MONT

VOCAL

DR. MARIO PINEDA RUELAS

VOCAL

DR. PEDRO LUIS DEL ANGEL RODRIGUEZ

VOCAL

DR. GERARDO VEGA HERNANDEZ

SECRETARIO

DR. FELIPE DE JESUS ZALDIVAR CRUZ