CÓDIGOS GEOMÉTRICOS

LUCAS MONTERO

Resumen. En este artículo veremos como las curvas algebraicas nos permiten construir códigos correctores con propiedades positivas.

Índice

1. Introducción 1
2. Convenciones y hechos preliminares 2
3. Códigos 5
4. Códigos Geométricos 9
Referencias 13

1. Introducción

El estudio de teoría de códigos está principalmente centrado en corregir los errores introducidos a los mensajes al pasar por un canal con ruido", en este informe consideraremos los códigos conocidos como códigos de bloques ya que las palabras son bloques de dígitos de un largo uniforme.

Se han estudiado diversas formas de corregir errores ocasionados por el ruido de los medios de transmisión, una de estas formas que se verá en este informe es la de matrices de "parity-check"que checkean si las palabras pertenecen o no a un código y es posible hacer algunas correcciones menores de ser necesario, pero este tipo de códigos no son los mejores siempre, tomemos por ejemplo la comunicación satelital que presenta una comunicación demasiado cara como para permitirse enviar mensajes más de una vez y es muy lenta, otra forma más adecuada a este ejemplo que no se verá en este trabajo es la de códigos de repetición que utiliza la repetición de cada dígito una n cantidad de veces, esto permite corregir errores grandes pero los mensajes se vuelven demasiado pesados y la comunicación muy lenta para otros propósitos.

Es por esto que en este trabajo además se estudiarán los códigos geométricos que ofrecen una alta flexibilidad a la hora de escoger entre el tamaño de los mensajes y la capacidad correctiva de estos.

Aunque la teoría de códigos está bien establecida desde hace décadas, presenta un problema grave con las herramientas convencionales de álgebra, el tiempo de decodificación de palabras y determinación de la distancia mínima entre palabras son problemas NP-completos, esto quiere decir que no existe un algoritmo eficiente conocido hasta la fecha que permita resolverlos en un tiempo polinomial, es por esto que estudiar códigos utilizando herramientas poco convencionales como la geometría algebraica ya que le proporcionan a los códigos propiedades especiales que influyen en una decodificación más eficiente.

Una de las herramientas más importantes es el teorema de Riemman-Roch [2.32], que provee a los códigos de estas deseadas propiedades especiales, además es importante destacar que es teóricamente posible construir una secuencia de códigos geométricos con parámetros mejores que lo que se creía posible con el álgebra convencional, incluso antes de que se desarrollaron estos códigos se creía que estos límites eran insuperables.

Estructura del artículo. Para este informe vamos a recordar lo básico de curvas algebraicas en la sección de hechos preliminares, ahí partiremos de topología de Zariski [2.1] hasta llegar al teorema de Riemman-Roch [2.32], luego se verá un resumen sobre las nociones básicas de códigos hasta lo más importante, los códigos de Reed-Solomon [3.22], una vez visto esto partiremos cambiando las estructuras clásicas de los códigos de Reed-Solomon por variedades algebraicas con la primera construcción de códigos geométricos [4.1], luego de esto construiremos

tres códigos más que utilicen las estructuras de geometría algebraica y veremos algunas de sus propiedades para terminar en ejemplos y ejercicios de estos códigos.

2. Convenciones y hechos preliminares

2.1. Convención. Asumimos que K es algebraicamente cerrado y X es irreducible, para todas las curvas consideraremos que son proyectivas, suaves y absolutamente irreducibles sobre un cuerpo finito $\mathbb{F}_q$

2.2. Hechos preliminares.

Definición 2.1. Sea X un conjunto y sea $\tau = \{U_i\}_{i\in I}$ una familia de subconjuntos de X, diremos que τ es una **topología** si cumple lo siguiente:

1. $\emptyset, X \in \tau$
2. $\forall J \subseteq I : \{U_i\}_{i\in J} \in \tau$
3. $\forall U_1, U_2 \in \tau : U_1 \cap U_2 \in \tau$

llamaremos a estos subconjuntos de X **abiertos** y a sus complementos les diremos **cerrados**.

Por otra parte, llamaremos a esta topología una **topología de Zariski** cuando X es un cuerpo y diremos que $U \subseteq X$ es abierto si existe un polinomio no nulo con coeficientes en X tal que no se anula para ningún elemento de U.

Definición 2.2. Un **prehaz** F en X consiste en

1. $\forall\, U \subseteq X$ abierto, $\exists F(U)$
2. Para toda inclusión de abiertos $U \hookrightarrow V$, una aplicación de restricción:

$$\begin{aligned} \mathrm{r}_{V,U} : F(V) &\longrightarrow F(U) \\ s &\longmapsto s|_U \end{aligned}$$

tal que si existen $U \hookrightarrow V \hookrightarrow W$ son inclusiones y sus restricciones conmutan, es decir $\mathrm{r}_{W,U} = \mathrm{r}_{V,U} \circ \mathrm{r}_{W,V}$ y $\mathrm{r}_{U,U} = \mathrm{Id}$.

Definición 2.3. Sea X un cuerpo algebraicamente cerrado y F prehaces de este cuerpo, diremos que un **germen** es una clase de equivalencia de pares de la forma (f, U) que contiene a todas las funciones $f \in F(U)$ tales que $f_1(x) = f_2(x)\, \forall\, x \in U$ con U una vecindad abierta de x, luego el conjunto de gérmenes en x se le llama **tallo**.

Definición 2.4. Sea F un prehaz de grupos abelianos en X, decimos que F es un **haz** si cumple con las siguientes condiciones $\forall\, U \subseteq X$

1. Pegado: Si $U = \cup_{i\in I} U_i$ cubrimiento de abiertos, si $s_i \in F(U_i)$ son secciones tales que $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j} = s_i\, \forall\, i, j \in I$
2. Unicidad: Si $U = \cup U_i$ cubrimiento abierto y $s \in F(s)$ una sección, entonces $s|_{U_i} = 0$.

Definición 2.5. Sea K un cuerpo y V un espacio vectorial sobre K con una operación bilineal extra de $V \times V \to A$ que denotaremos por *cdot*, ahora llamaremos a V un **K-algebra** si cumple las siguientes propiedades $\forall\, x, y, z \in V$ y $\forall\, a, b \in K$:

1. $(x + y) \cdot z = x \cdot z + y \cdot z$
2. $z \cdot (x + y) = z \cdot x + z \cdot y$
3. $(ax) \cdot (by) = (ab)(x \cdot y)$

Definición 2.6. Sea $S \subseteq K[p]$ un conjunto de polinomios, la *variedad* definida por S es el conjunto

$$V(S) = \{a \in K^r : f(a) = 0, \quad \forall f \in S\}$$

Definición 2.7. Sea K un cuerpo, denotaremos al conjunto K^n de la topología de Zariski y de un haz de K-álgebras llamado el haz de funciones regulares, el correspondiente espacio anillado lo llamaremos **espacio afín** y lo denotaremos por $\mathbb{A}^n(K)$

Definición 2.8. Sea $V \cong K^{n+1}$ un espacio vectorial, el **espacio proyectivo** $\mathbb{P}(V) \cong \mathbb{P}^n$ es la variedad algebraica cuyos puntos corresponden a rectas vectoriales en V, es decir clases de equivalencia de n-tuplas de la forma $(\lambda v_0, \lambda v_1, \ldots, \lambda v_n)$ donde no todos los v_i sean nulos y $\lambda \in K$

Observación 2.9. Notar que existe un incrustamiento natural de $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$.

Observación 2.10. Recordando de (2.1), los cerrados en un espacio afín sería el conjunto de ceros que comparten un conjunto de polinomios con coeficientes en K, es decir si X cerrado en $\mathbb{A}^n$ entonces

$$X = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n | f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0\}$$

Definición 2.11. Un abierto U dentro de un cerrado X tal que $X \cong \mathbb{P}^n$ lo llamaremos un conjunto **cuasiproyectivo**, además diremos que es **reducible** si existe un par de cerrados no vacíos dentro de U tales que $U = U_1 \cup U_2$, de no ser el caso diremos que es **irreducible**, ahora un conjunto cuasiproyectivo irreducible lo llamaremos una **variedad cuasiproyectiva**

Definición 2.12. Sea $f \in \mathbb{F}[x, y]$ una variedad irreducible, diremos un punto de la forma $(P_1, P_2, 0)$ en la clausura proyectiva de f un **punto al infinito**.

Ejemplo 2.13. Notemos que $\mathbb{A}^1 - \{0\}$ es una variedad cuasiproyectiva ya que no existe un conjunto de polinomios que se anulen en todos los puntos entonces es abierta y por lo tanto no puede ser proyectiva.

Definición 2.14. Sea X una variedad, decimos que que la **dimensión** de X, denotada $\dim(X)$, es el entero más grande tal que existe una cadena estrictamente decreciente de variedades $X = X_0 \subset \cdots \subset X_n \neq \emptyset$, con X_i un cerrado en X_{i-1} para $i = 1, \ldots, n$. Si Y es un cerrado en X entonces podemos definir la **codimensión** de Y en X, denotada $\operatorname{codim}_X(Y) = \dim(X) - \dim(Y)$

Definición 2.15. Sea $X \subseteq \mathbb{P}^n$ una variedad cuasiproyectiva, sean $F, G \in K[T_0, \ldots, T_n]$ polinomios del mismo grado en coordenadas homogéneas en $\mathbb{P}^n$, y sea $G(P) \neq 0$ para algún $P \in X$, decimos que la fracción $F/G \in K[T_0, \ldots, T_n]$ define una **función racional**.

Definición 2.16. Un mapeo nacional f de una variedad $X \subseteq \mathbb{P}^m$ a $\mathbb{A}^n$ está dado por una n-tupla $(f_1, \ldots, f_n)$ con $f_i \in K(X)$, y decimos que $f = (f_1, \ldots, f_n)$. Si toda f_i es regular en $p \in X$ entonces llamaremos a f **regular** en P, si f regular en todo punto de X la llamaremos simplemente regular.

Definición 2.17. Sea $P \in X$, el conjunto racional de funciones que son regulares en P es denotado como $\mathscr{O}_P$, es claro que $\mathscr{O}_P$ es un anillo y lo llamaremos el **anillo local** de P

Observación 2.18. Es de vital importancia notar que $\mathscr{O}_P$ posee un único ideal maximal m_P formado por $f \in \mathscr{O}_P \,|\, f(P) = 0$

Además $\mathscr{O}_P/m_P = K$, luego podemos decir que m_P/m_P^2 es un K-espacio vectorial y llamaremos a su dual $\theta_P = (m_P/m_P^2)^*$ es llamado el **espacio tangente** a X en P.

Por último notemos que $\dim(X) \leq \dim_K(\theta_P) \leq n$.

Definición 2.19. Un punto P es llamado **suave** si $\dim(X) = \dim_K(\theta_P)$, si todos los puntos de X son suaves entonces X es llamada una **variedad suave** o **sin singularidades**.

Definición 2.20. Sea X una variedad, una familia de espacios vectoriales es un mapa regular $f : \epsilon \to X$ tal que para cualquier $P \in X$ su **fibra** sería $\overline{\epsilon}_P = f^{-1}(P)$ es un espacio vectorial sobre K.

Definición 2.21. Una variedad cuasiproyectiva de dimensión 1 la llamaremos **curva cuasiproyectiva** y lla llamaremos simplemente **curva** a las que su subvariedad cerrada sea un punto, y diremos que es **completa** si la curva es cerrada $\mathbb{P}^n$.

Proposición 2.22. *Una curva X tiene una cantidad finita de puntos singulares.*

Proposición 2.23. *Sea $X \subseteq \mathbb{P}^n$ una curva y $P \in X$ suave, luego $dim_K(\theta_P) = n - 1$*

Teorema 2.24. *Dos curvas suaves completas son isomorfas $\Leftrightarrow$ son birracionalmente isomorfas.*

Definición 2.25. Sea $f = x^{q+1} + y^{q+1} + 1 = 0$ sobre $\mathbb{F}_{q^2}$ es llamada una **curva q-Hermitiana**, la clausura proyectiva definida por $\overline{f} = X^{q+1} + Y^{q+1} + Z^{q+1}$ tiene $q + 1$ puntos al infinito, más aún podemos definir $Z = 0, Y = 1$ entonces $X^{q+1} + 1 = 0$ que tiene $q + 1$ raíces, sean $\omega_1, \ldots, \omega_{q+1}$ las raíces, luego $(\omega_i, 1, 0) \in \overline{f}$.

Definición 2.26. Sea $f : X \to Y$ una función racional no constante (**dominante**), ya que $f^* : K(Y) \to K(X)$ es una incrustación, llamaremos a la división $[K(X) : f^*(K(Y))]$ el **grado** de f y lo denotaremos como $\deg(f)$.

Definición 2.27. Sea X una curva completa suave sobre K, un **divisor** D de X es una suma formal $\sum a_P \cdot P$ con $P \in X$, $a_P \in \mathbb{Z}$.
El conjunto $\{P \in X \mid a_P \neq 0\}$ lo llamaremos **soporte** de D y lo denotamos $\mathrm{Supp}(X)$
Denotaremos como $\mathrm{Div}(X)$ al conjunto de divisores de X, el cual es un grupo abeliano si podemos sumar y restar divisores, sean $A = \sum_P a_P \cdot P$ y $B = \sum_P b_P \cdot P$

$$A \pm B = \sum_P (a_P \pm b_P) \cdot P$$

Ahora el mapa $\mathrm{Div}(X) \to \mathbb{Z}$ es sobreyectivo y denotaremos su kernel como $\mathrm{Div}^0(X)$.

Si $a_P \geq 0 \, \forall \, P \in X$ llamaremos al divisor $D = \sum_P a_P \cdot P$ **divisor efectivo** y lo denotaremos como $D \geq 0$, más aún, si $D \neq 0$ lo llamamos **positivo** y denotaremos al conjunto de divisores efectivos como $\mathrm{Div}^+(X)$, esta definición induce un orden parcial en $\mathrm{Div}(X)$, este es que $A \geq B$ si $A - B \in \mathrm{Div}^+(X)$

Definición 2.28. Sea $f \in K(X)^*$ luego definimos al **divisor de principal** como $(f) = \sum \mathrm{ord}_P(f) \cdot P$, ahora el conjunto de divisores principales lo denotaremos por $P(X)$, el cual es un subgrupo de $\mathrm{Div}(X)$, más aún $P(X) \subseteq \mathrm{Div}^0(X)$ y definiremos $Cl(X) = \mathrm{Div}(X)/P(X)$ y $Cl^0(X) = \mathrm{Div}^0(X)/P(X)$.

Definición 2.29. Sea D un divisor en X, definimos el **espacio asociado** a D como

$$L(D) = \{f \in K^*(X) \mid (f) + D \geq 0\} \cup \{0\}$$

y denotaremos su dimensión como $\ell(D)$

Definición 2.30. Sea $M \neq 0$ un subespacio de $L(D)$, el conjunto de divisores efectivos de la forma $(f) + D$ con $f \in M - \{0\}$ es llamado **sistema lineal** y lo denotaremos como $|M|$, si $|M| = L(D)$ entonces es llamado un **sistema lineal completo** y es denotado como $|D|$.

Definición 2.31. Sea $P \in X$ y sea $f \in \mathscr{O}_P$, definimos a $d_P(f)$ como la imagen de $f - f(P) \in m_P$ en m_P/m_P^2 y lo llamaremos el **diferencial** de f en P.

Sea U un abierto de X y sea $f \in K[U]$, sea $\varphi[U]$ el conjunto de los mapas φ tales que toman $P \in U$ y los envían a un $\varphi(P) \in m_P/m_P^2$, cualquier $f \in K[U]$ define un $df \in \varphi[U]$ por $(df)(P) = d_P(f)$, llamaremos a este φ una **forma diferencial regular** en U si para todo $P \in U$ existe una vecindad abierta V de P en U tal que $\varphi|_V$ cae en el $K[V]$-submodulo $\sum_{f \in K[V]} K[V] \cdot df$ de $\varphi[V]$, denotaremos al $K[U]$-modulo como $\Omega[U]$

Para todo $P \in X$ existe un abierto U que contiene a P tal que $\omega = f \cdot dt \in \Omega[U]$ para $f \in K(X)$, donde $t - t(P)$ es un parámetro local para cualquier $P \in U$, se sigue que para cualquier $\omega \neq 0$ existe un cubrimiento de abiertos $\{U_i\}$ de X tal que $\omega|_{U_i} = f_i \cdot dt_i$ para cualquier i, como $f_i \cdot dt_i = f_j \cdot dt_j$ en $U_i \cap U_j$, $t_i - t_i(q)$ y $t_j - t_j(q)$ siendo parametros locales de $q \in U_i \cap U_j$; vemos que f_i/f_j , $f_j/f_i \in (K[U_i \cap U_j])^*$, luego $\{U_i, f_i\}$ es un divisor asociado a ω, como $\omega' = f \cdot \omega$ vemos que $(\omega') = (f) + (\omega)$, entonces la clase $K = K_X$ de equivalencia de (ω) no depende de la elección de ω, es llamada **clase canónica** de X.

Teorema 2.32. *Sea X una curva suave completa, $K = K_X$ su clase canónica, entonces $\forall \, D \in Div(X)$*

$$\ell(D) - \ell(K - D) = deg(D) - g + 1$$

donde g un automorfismo de X.

Definición 2.33. Sea X una curva suave completa, entonces existe una única variedad abeliana que denotaremos por J_X tal que cumple las siguientes propiedades

1. J_X isomorfa a $\mathrm{Div}(X)/P(X)$ como grupo.
2. El mapa $i_{P_0} : X \to J_X$ es regular para cualquier $P_0 \in X$.
3. Para cualquier mapa $\varphi : X \to A$ donde A es una variedad abeliana tal que $\varphi(P_0$ es el elemento neutral de A, existe un morfismo de variedades abelianas $\lambda : J_X \to A$ con $\varphi = \lambda \circ i_{P_0}$.

   Llamaremos a esta variedad J_X como el **Jacobiano** de X y llamaremos a la dimensión del jacobiano de X el **género** de X y lo denotaremos como $g(X)$.

Definición 2.34. Sea X una curva suave completa de género 1 la llamaremos **elíptica** y si tiene género 2 la llamaremos **hiperelíptica**.

3. Códigos

Definición 3.1. Sea A un conjunto finito de elementos, el cual llamaremos **alfabeto**, el conjunto $A^n = A \times \dots A$ está dotado de una distancia interna $d(a,b)$ con $a, b \in A^n$ definida como:

$$d((a_1, \dots, a_n), (b_1, \dots, b_n)) = |\{i = a_i \neq b_i\}|$$

la cual llamaremos la **métrica de Hamming**, también llamaremos a $q = |A|$ la **cardinalidad del alfabeto**.

Definición 3.2. Cualquier $C \subseteq A^n$ no nulo se conoce como un **código de largo** n (se puede usar q-ary code para especificar la cadinalidad del alfabeto), la cardinalidad de C es $M = |C| \in \mathbb{N}$ y el el logaritmo de la cardinalidad $k = log_q|C| \in \mathbb{R}$, ahora definimos la **distancia mínima entre palabras** de C como:

$$d = \min\{d(a,b) \,|\, a, b \in C, a \neq b\}$$

Definición 3.3. Un código con n, k, d y q se le conoce como un $[n,k,d]_q$**-code**, los elementos de C se les conocen como **vectores** y los componentes de estos vectores se les conocen como **coordenadas** o **posiciones**

Definición 3.4. Otros parámetros útiles son, la **tasa** $R = k/n$, la **distancia mínima relativa** $\delta = d/n$

Observación 3.5. Notar que $0 < R < 1$ y $0 < \delta < 1$

Definición 3.6. Si $A = \mathbb{F}_q$ un cuerpo finito con $q = p^m$ con p primo, un **código lineal** es un código C de largo n que es un subespacio lineal de $\mathbb{F}_q^n$.

Observación 3.7. Para un código lineal $k = \dim(C)$, $d = \min\{||a|| \,|\, a \in C, a \neq 0\}$ donde $||a|| = |\{i \,|\, a_i \neq 0\}|$ el cual se le llama el **peso** de a.

Definición 3.8. Sea C un código lineal, luego cualquier elección de bases de C se puede ver como una incrustación $C : \mathbb{F}_q^k \hookrightarrow \mathbb{F}_q^n$, el cual denotaremos de la misma forma que el código, ahora la matriz de esta transformación la llamaremos la **matriz generadora del código**, por otra parte podemos construir la siguiente secuencia exacta

$$0 \longrightarrow \mathbb{F}_q^k \xrightarrow{C} \mathbb{F}_q^n \xrightarrow{H} \mathbb{F}_q^{n-k} \longrightarrow 0$$

Donde H es sobreyectiva y $\ker(H) = C$, luego a la matriz de H la denotaremos como la **parity-check matrix del código** C.

Observación 3.9. Notar que la forma en la que la matriz H chequea los elementos de C al cumplir $H \cdot c = 0$ con $c \in C$

Ejercicio 3.10. Sea C un código lineal con la siguiente parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Encontrar una palabra con peso mínimo y encontrar los parámetros de C.

Solución: Primero veamos que las palabras satisfacen $Hc^T = 0$, luego las 6 columnas de la derecha de H son el complemento de las 6 de la izquierda, luego la suma de la primera y la última columna es el vector sólo de 1, de la misma forma las siguientes hacia el centro de la matriz van formando el vector de sólo unos, luego la suma de las primeras dos columnas con las ultimas dos columnas debe ser cero y eso corresponde con la siguiente palabra de peso 4

$$(1,1,0,0,0,0,0,0,0,0,1,1)$$

Otra palabra de peso 4 correspondiente a la dependencia lineal de las primeras 6 columnas es

$$(0,1,1,0,1,1,0,0,0,0,0,0)$$

Luego es fácil ver que no existen palabras con un peso menor a 4.

Por último, es fácil observar que la dimensión del código es 12, la distancia mínima de palabra es 4 y que $n-k=6$ entonces $k=6$ por lo tanto C es un $[12,6,4]_q$-code

Definición 3.11. Diremos que dos códigos lineales C y C' son **equivalentes** si existe un automorfismo lineal A tal que $C'=A(C)$, donde $A\in\mathscr{A}$ con $\mathscr{A}$ el grupo de automorfismos lineales de $\mathbb{F}_q^n$, el subgrupo $\mathrm{Aut}(C)\subseteq\mathscr{A}$ lo llamaremos el **grupo de automorfismos de** C, además el grupo $\mathscr{A}$ que es representado por matrices monomiales (es decir que todas sus filas y columnas contienen al menos un elemento no nulo) es isomorfo al producto semi directo de $(\mathbb{F}_q^*)^n$ y S_n, por último podemos ver que $|\mathscr{A}|=(q-1)^n\cdot n!$.

Ejercicio 3.12. Sea C un código lineal sobre $\mathbb{Z}_3$ con la siguiente parity-check matrix

$$H=\begin{bmatrix}0&0&0&1&0&1\\0&0&2&0&1&0\\0&1&2&2&0&0\\1&0&1&2&0&0\end{bmatrix}$$

Encontrar los parámetros de C

Solución: Notemos que permutando las columnas de una parity-chack matrix podemos obtener un código equivalente, luego tenemos

$$H'=\begin{bmatrix}0&0&0&1&0&1\\0&0&1&0&2&0\\0&1&0&0&2&2\\1&0&0&0&1&2\end{bmatrix}$$

Luego es evidente que no se pueden encontrar 3 o menos columnas linealmente independientes de H', luego el código es un $[6,2,4]_3$.

Definición 3.13. Podemos redefinir los códigos lineales de una forma conveniente, sea V un espacio vectorial sobre $\mathbb{F}_q$, un $[n,k,d]_q$-system es una familia ordenada de puntos $\mathcal{P}$ en V tales que $\mathcal{P}$ no se encuentra dentro de un hiperplano. Los parámetros del sistema se definen de la siguiente forma $n=|\mathcal{P}|$, $k=\dim(V)$, $d=n-\max_H|\mathcal{P}\cap H|\geq 1$

Observación 3.14. De la misma forma que se definieron los códigos equivalentes 3.11, se pueden definir los códigos equivalentes usando la nueva definición **??** usando isomorfismos de espacios vectoriales.

Proposición 3.15. *Existe una función inyectiva entre el conjunto de clases de $[n,k,d]_q$-system y $[n,k,d]_q$-code (lineales).*

Demostración: Sea V^* el dual de V y digamos que $(V^*)^*=V$, sea $\mathcal{P}=(P_1,\dots,P_n)$, tomemos una función $\varphi:V^*\longrightarrow\mathbb{F}_p^n$ definida por $\varphi(x)=(\varphi_1(x),\dots,\varphi_n(x))$, donde $\varphi_i(x)=x(P_i)$.

Es fácil ver que φ es inyectiva, sea $C=\mathrm{Im}(\varphi)$, y de igual forma $C\subseteq\mathbb{F}_q^n$, luego $V=C^*$.

Definición 3.16. Sea $\mathbb{P}=\mathbb{P}(V)$ un espacio proyectivo sobre $\mathbb{F}_q$, un **sistema proyectivo** es una familia ordenada de puntos $\mathcal{P}$ en $\mathbb{P}$ que no pertenece a un hiperplano proyectivo, abusando del lenguaje diremos que $\mathcal{P}\subseteq\mathbb{P}$. Los parámetros los definiremos como $n=|\mathcal{P}|$, $k=\dim(\mathbb{P})+1$, $d=n-\max_H|\mathcal{P}\cap H|\geq 1$. Igual que en los sistemas definidos anteriormente diremos que dos sistemas proyectivos son equivalentes si existe un isomorfismo proyectivo $\mathbb{P}\simeq\mathbb{P}'$ que tome $\mathcal{P}$ y entregue $\mathcal{P}'$. Denotaremos a los sistemas proyectivos de la misma forma que los sistemas definidos antes, es decir $[n,k,d]_q$-system.

Definición 3.17. Sea $C\subset\mathbb{F}_q^n$, diremos que el código es **degenerado** si $C\subseteq\mathbb{F}_q^{n-1}$, donde $\mathbb{F}_q^{n-1}$ es el subespacio de vectores con 0 en alguna posición fija.

Proposición 3.18. *Existe una función inyectiva entre el conjunto de clases de $[n,k,d]_q$-system proyectivos y $[n,k,d]_q$-code no degenerados.*

Definición 3.19. Presentemos la última definición de códigos, un **sistema dual** es una familia ordenada de puntos Q en un espacio lineal W (con multiplicidades) que no pertenece a un hiperplano, los parámetros serían $n=|Q|$, $k=n-\dim(W)$, d es la mínima cantidad de vectores linealmente independientes en Q (en particular si Q incluye multiplicidades entonces $d\leq 2$).

Teorema 3.20. *Existe una función inyectiva entre el conjunto de clases de equivalencia de clases de sistemas duales y códigos lineales, y también entre la clase de equivalencia de sistemas proyectivos duales y códigos lineales no degenerados.*

Ejemplo 3.21. Para todo n existen tres simples códigos que se consideran triviales, estos son

1. $[n, n, 1]_q$-code con $C_1 = \mathbb{F}_q^n$, llamado el código **trivial**, este código se compone de todos los puntos posibles en nuestro cuerpo finito, el valor de k es n por definición y la distancia entre palabras es 1.
2. $[n, n-1, 2]_q$-code con $C_2 = \{(v_1, \ldots, v_n) \in \mathbb{F}_q^n \mid \sum v_i = 0, \forall\, i = 1, \ldots, n\}$ llamado el código **parity-check**, en donde la distancia entre palabras debe ser de a lo menos 2 ya que de lo contrario no se puede cumplir la condición del código.
3. $[n, 1, n]_q$-code $C_2 = \{(v, \ldots, v) \in \mathbb{F}_q^n \mid v \in \mathbb{F}_q\}$ llamado el código de **repetición**, donde la distancia entre palabras es máxima.

Definición 3.22. Sea $\mathcal{P} = \{P_1, \cdot, P_n\} \subseteq \mathbb{F}_q$, tomemos el espacio lineal $L(a)$ de polinomios con coeficientes en $\mathbb{F}_q$ tal que $\dim(L(a)) = a+1$, es decir que los polinomios tienen grado a lo más a, es necesario que $n > a$, ahora tomemos $f(x) \in L(a)$ tal que no es nulo y no se anula para todo $P \in \mathcal{P}$, más aún, este $f(x)$ debe tener a lo más a raíces en $\mathcal{P}$, luego la evaluación:

$$\begin{aligned} \mathrm{Ev}_{\mathcal{P}} : L(a) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) \end{aligned}$$

es inyectiva (sólo para $n > a$) y su imagen es un código en $\mathbb{F}_q^n$ que llamaremos **código de Reed-Solomon**, además lo denotaremos como $[n, a+1, n-a]_q$-code

Observación 3.23. Notar que los parámetros de los códigos de Reed-Solomon cumplen la condición de $k+d = n+1$ la cual es bastente buena, incluso no puede ser mejor, y la condición de $k = a+1$ puede ser libremente tomada entre 1 y n; además estos códigos son incrustaciones, es decir, $L(a) \subseteq L(a+1)$. Lamentablemente estos códigos no pueden exceder el largo q pero utilizando curvas algebraicas podremos extender este largo.

Definición 3.24. Diremos que un código es **cíclico** si $\forall\, (c_0, c_1, \ldots, c_{n-1}) \in C, \exists (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.

Definición 3.25. Sea X una curva de género 0 sobre $\mathbb{F}_q$, llamaremos al código construido con esta curva un **código de género 0** y sus parámetros son los siguientes

1. $n \leq q+1$
2. $d = 1, \ldots, n$
3. $k = n+1-d$

Definición 3.26. La **función de distribución del peso** de un código C está definida por $A_i = \#\{a \in C | \omega(a) = i\}$, con $1 \leq i \leq n$ y la escribimos como

$$W_C(X) = \sum_{i=1}^{n} A_i X^i \in \mathbb{Z}[X]$$

notar que la distancia mínima de palabra es el entero positivo más pequeño tal que $A_d \neq 0$

Definición 3.27. Un **código de Hamming** es un código tal que $n = q-1$ donde $q = 2^m$ para algún $m \geq 2$, luego el código

$$C \subseteq \mathbb{F}_2[T]/(T^{q-1} - 1)$$

es el ideal generado por el mínimo polinomio $f_\alpha(T) \in \mathbb{F}_2[T]$ de $\alpha \in \mathbb{F}_q^*$ donde α es un generador del grupo multiplicativo $\mathbb{F}_q^*$

Teorema 3.28. *Sea C un código de Hamming, luego es un $[n, n-m, 3]_q$-code binario y cíclico, es decir que tiene un largo $q-1$, dimensión $q-1-m$ y distancia mínima 3*

Demostración: Usaremos el teorema de Delsarte [5] para obtener

$$C^\perp = \{Tr(\lambda x)_{x \in \mathbb{F}_q^*} | \lambda \in \mathbb{F}_q\}$$

La cual se relaciona con los $\lambda \in \mathbb{F}_q$ de la curva con género cero

$$Y^2 - Y = \lambda X$$

veamos que la cardinalidad de $C^{\perp}$ es q y la distribución de su peso está dada, para $\lambda = 0$ obtenemos la palabra cero de peso cero y por $\lambda \neq 0$ se obtiene una palabra de peso $q/2$ como λx recorre todos los elementos de $\mathbb{F}_q$, la identidad de MacWilliams [5] nos dice que

$$W_C(X) = \frac{1}{q}\left((1+X)^{q-1} + (q-1)(1-X)^{q/2}(1+X)^{q/2-1}\right)$$

luego el número de palabras en C de peso i están dadas por

$$A_i = \frac{1}{q}\left(\binom{q-1}{i} + (q-1)(-1)^{\frac{i+1}{2}}\binom{q/2-1}{i/2}\right)$$

en particular $A_1 = A_2 = 0$ y $A_3 = (q-1)(q-2)/6$, entonces la mínima distancia entre palabras es 3.

Ejemplo 3.29. Sea un código de hamming $[7,4]$ binario y cíclico con generador binomial $g(x) = a + x + x^3$, ahora C tiene una distribución de peso $A_0 = 1, A_3 = A_4 = 7, A_7 = 1$, luego $\mathrm{Aut}(C)$ es un grupo de klein de orden 168.

Observación 3.30. Notemos que no es necesario escribir la distancia mínima de palabra para un código de hamming, luego los denotaremos como $[n,k]$-code

Ejercicio 3.31. Consideremos el $[7,4]$-code con la siguiente matriz de parity-check

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

encontrar una palabra de peso 3 y encontrar la palabra original si tenemos$(1\,0\,1\,0\,0\,1\,?)$, $(1\,0\,0\,?\,0\,1\,?)$ y $(1\,0\,0\,?\,?\,?\,0)$

Solución:
Primero, recordemos que $Hc^T = 0$, luego

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} = \begin{bmatrix} c_1 + c_4 + c_6 + c_7 = 0 \\ c_2 + c_4 + c_5 + c_6 = 0 \\ c_3 + c_5 + c_6 + c_7 = 0 \end{bmatrix}$$

luego escogiendo podemos tomar la palabra $c = (1\,0\,0\,0\,1\,1\,0)$, ahora usemos este mismo procedimiento con las palabras desconocidas

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ x \end{bmatrix} = \begin{bmatrix} 1+1+x = 0 \Rightarrow x = 0 \\ 1+1 = 0 \\ 1+1+x = 0 \end{bmatrix}$$

entonces la primera palabra era $(1\,0\,1\,0\,0\,1\,0)$, luego la segunda

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ x \\ 0 \\ 1 \\ y \end{bmatrix} = \begin{bmatrix} 1+x+1+y = 0 \\ x+1 = 0 \Rightarrow x = 1 \\ 1+y = 0 \Rightarrow y = 1 \end{bmatrix}$$

entonces la segunda palabra desconocida es $(1\,0\,0\,1\,0\,1\,1)$, ahora para la tercera

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ x \\ y \\ z \\ 0 \end{bmatrix} = \begin{bmatrix} 1+x+z=0 \Rightarrow z=1 \\ x+y+z=0 \Rightarrow y=1 \\ y+z=0 \Rightarrow x=0 \end{bmatrix}$$

luego la tercera palabra desconocida es $(1\,0\,0\,0\,1\,1\,0)$

4. Códigos Geométricos

Construcción 4.1. Sea X una curva tal que $X(\mathbb{F}_q) \neq \emptyset$, sea $\mathcal{P} \subset X(\mathbb{F}_q)$, $|\mathcal{P}| = n$, $D \in \mathrm{Div}(X)$, además sea $\mathrm{Supp}(D) \cap \mathcal{P} = \emptyset$, consideremos el mapa:

$$\begin{aligned} \mathrm{Ev}_{\mathcal{P}} : L(D) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) \end{aligned}$$

Donde $\mathcal{P} = \{P_1, \ldots, P_n\}$, Obtenemos el código C= $\mathrm{Ev}_{\mathcal{P}}(L(D))$, usaremos la notación:

$$C = (X, \mathcal{P}, D)_L$$

Podemos suponer que escogemos D tal que $f \in L(D)$ tiene a lo más b ceros en $\mathbb{F}_q$-puntos de la curva X.
Si $n > b$ entonces $\mathrm{Ev}_{\mathcal{P}}$ es una incrustación y

$$\begin{aligned} k &= \ell(D) \\ d &\geq n - b \end{aligned}$$

Tomando el teorema de Riemman-Roch es posible estimar los parámetros de C con el siguiente teorema:

Teorema 4.2. *Sea X una curva de género g y sea $0 \leq deg(D) = a < n = |\mathcal{P}|$. Entonces $C = (X, \mathcal{P}, D)_L$ es un $[n, k, d]_q$-code con*

$$\begin{aligned} k &\leq a - g + 1 \\ d &\leq n - a \end{aligned}$$

Demostración: Tomemos $D = D_1 - D_2$, luego $D_1, D_2 \geq 0$, Una función no nula $f \in L(D)$ tiene a los más $a_1 = \deg(D_1)$ polos y y a lo menos $a_2 = \deg(D_2)$ ceros en $\mathrm{Supp}(D)$, ya que $D + (f)_0 - (f)_\infty \geq 0$, entonces el número de sus ceros fuera de $\mathrm{Supp}(D)$ es a lo más $a_1 - a_2 = a$.

Hemos supuesto que $a < n$, entonces tenemos que $EV_{\mathcal{P}}(f) \neq 0$ para toda $f \neq 0$, es decir $EV_{\mathcal{P}}$ es un encrustamiento.

Por último $EV_{\mathcal{P}}(f)$ tiene al menos $(n - a)$ coordenadas no nulas, entonces:

$$d \geq n - a$$

Por otro lado $C = EV_{\mathcal{P}}(L(D)) \backsimeq L(D)$ es decir:

$$k = \ell(D) \geq a - g + 1$$

de acuerdo al teorema de Riemman-Roch. ■

Ejemplo 4.3. Sea $X = \mathbb{P}^1$, $D = a \cdot \infty$, entonces $L(D)$ es un espacio de polinomios de grado a lo más a, si para $\mathcal{P}$ tomamos todos los $\mathbb{F}_q$-puntos de $\mathbb{P}^1$ excepto por ∞, es decir que $\mathcal{P} = \mathbb{F}_q$, entonces podemos construir un $[q, a + 1.q - a]_q$-code, el cual es de hecho un código de Reed-Solomon.

Construcción 4.4. Asumamos X es una curva y sea $\mathcal{P} = P_1, \ldots, P_n$ y $\mathbf{P} = P_1 + \cdots + P_n \in \mathrm{Div}(X)$, consideremos el espacio de formas diferenciales:

$$\Omega(\mathbf{P} - D) = \{\omega \in \Omega(X)^* | (\omega) + \mathbf{P} - D \geq 0\} \cup \{0\}$$

Es decir, este espacio posee una apropiada multiplicidad de 0 en el soporte de D y a lo más polos simples en los puntos P_i con $i = 1, \ldots, n$.

Recordemos que para cualquier punto P en X y para cualquier forma no nula de $\omega \in \Omega(X)$ referencia, se define un residuo $\mathrm{Res}_P(\omega)$, es claro que para $P \in X(\mathbb{F}_q)$ y ω definido sobre $\mathbb{F}_q$ tenemos que $\mathrm{Res}_P(\omega) \in \mathbb{F}_q$, entonces tenemos el siguiente mapa:

$$\begin{aligned} \mathrm{Res}_{\mathcal{P}} : \Omega(\mathbf{P} - D) &\longrightarrow \mathbb{F}_q^n \\ \omega &\longmapsto (\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_2}(\omega)) \end{aligned}$$

El cual define un código $C = \mathrm{Res}_{\mathcal{P}}(\Omega(\mathbf{P} - D))$ y lo escribimos como $C = (X, \mathcal{P}, D)_\Omega$

Con el siguiente teorema podemos demostrar que $C = (X, \mathcal{P}, D)_\Omega$ es un $[n, k, d]_q$-code

Teorema 4.5. *Sea X una curva de género g y sea $2g - 2 < a$ y $\mathcal{P} \cap Supp(D) = \emptyset$. Entonces $C = (X, \mathcal{P}, D)_\Omega$ es un $[n, k, d]_q$-code con*

$$\begin{aligned} k \leq & n - a + g - 1 \\ d \leq & a - 2g + 2 \end{aligned}$$

Demostración: Sea K un divisor canónico, $\deg(K) = 2g - 2$, entonces

$$\begin{aligned} \Omega(\mathbf{P} - D) &\backsimeq L(K + \mathbf{P} - D) \\ \dim(\Omega(\mathbf{P} - D)) &= \ell(K + \mathbf{P} - D) \\ &\geq (2g - 2 + n - a) - g + 1 \\ &= n - a + g - 1 \end{aligned}$$

Ahora para cualquier forma diferencial de ω tenemos que

$$\begin{aligned} K \sim (\omega) &= (\omega)_0 - (\omega)_\infty \\ \Rightarrow 2g - 2 = \deg(K) &= \deg((\omega)_0) - \deg((\omega)_\infty) \end{aligned}$$

Ahora asumamos que $D = D_1 - D_2$ con $D_1, D_2 \geq 0$, $\mathrm{Supp}(D_1) \cap \mathrm{Supp}(D_2) = \emptyset$, si $\omega \in \Omega(\mathbf{P} - D)$ entonces $(\omega_0) \geq D_1$, luego

$$\deg((\omega)_\infty) = \deg((\omega)_0) - 2g + 2 \geq a - 2g + 2 + \deg(D_2)$$

Es decir la forma ω tiene al menos $a - 2g + 2$ polos fuera del $\mathrm{Supp}(D_2)$. Ya que $\mathcal{P} \cap \mathrm{Supp}(D) = \emptyset$, entonces estos polos están en los puntos $P_i \in \mathcal{P}$, luego los polos son de orden 1 y $\mathrm{Res}_{P_i}(\omega) \neq 0 \Leftrightarrow \mathrm{Supp}((\omega)_\infty)$.

Suponemos que $a > 2g - 2$, entonces $\mathrm{Res}_{\mathcal{P}}(\omega) \neq 0 \; \forall \; \omega \neq 0$, es decir que $\mathrm{Res}_{\mathcal{P}}$ es un incrustamiento.

Además el número de coordenadas no nulas es a lo más $a - 2g + 2$, la dimensión $k = \dim(\Omega(\mathbf{P} - D))$ está ya estimada más arriba. ■

Observación 4.6. Para los códigos $C = (X, \mathcal{P}, D)_L$ existe una construcción elemental de alargamiento que hace posible prescindir de la condición $\mathrm{Supp}(D) \cap \mathcal{P} = \emptyset$.

Sea X una curva, $\mathcal{P} \subset X(\mathbb{F}_q)$, $|\mathcal{P}| = n$, $D = D' + D''$, $\mathrm{Supp}(D') \cap \mathcal{P} = \emptyset$, $\mathrm{Supp}(D'') \subset \mathcal{P}$, $\forall \; Q_i \in \mathrm{Supp}(D'')$ escoger un parámetro local t_i.
Si $D'' = \sum_{i=1}^{s} b_i \cdot Q_i$ entonces $\forall \; f \in L(D)$ la función $t_i^{b_i} \cdot f$ es regular en Q_i, luego podemos considerar el mapeo:

$$\begin{aligned} \text{Ev'}_{\mathcal{P}} : L(D) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_r), t_1^{b_1} \cdot f(Q_1), \ldots, t_s^{b_s} \cdot f(Q_s)) \end{aligned}$$

donde $\{P_1, \ldots, P_r\} = \mathcal{P} - \mathrm{Supp}(D'')$, el código $C' = \text{Ev'}(L(D))$, el cual denotamos como $(X, \mathcal{P}, D)'$, es un alargamiento de $(X, \mathcal{P}', D)_L$, donde $\mathcal{P}' = \mathcal{P} - \mathrm{Supp}(D'')$, por s posiciones correspondientes a los puntos de $\mathrm{SUpp}(D'') = \mathrm{Supp}(D) \cap \mathcal{P}$.
Los parámetros de C' satisfacen el teorema (4.2)

Construcción 4.7. Sea X una variedad proyectiva suave sobre $\mathbb{F}_q$, $\mathscr{L}$ un fibrado en X definido sobre $\mathbb{F}_q$ y $H^0(\mathscr{L})$ el espacio de sus secciones, sea $\mathcal{P} = \{P_1, \dots, P_n\} \subset X(\mathbb{F}_q)$.
Es imposible construir un mapeo de $H^0(\ell)$ a $\mathbb{F}_q^n$ evaluando puntos (como se hizo en (**??**) ya que el valor de una sección puede no estar bien definido en algún punto, pero el conjunto de anulación de una sección en un punto sí está bien definido, el cual es bastante cercano a lo que queremos, luego tenemos el mapeo natural:

$$H^0(\mathscr{L}) \longrightarrow \oplus_{i=1}^n \bar{\mathscr{L}}_{P_i}$$

donde $\bar{\mathscr{L}}_{P_i}$ es la fibra de $\mathscr{L}$ en el punto P_i, es decir un espacio vectorial unidimensional en $\mathbb{F}_q$, el cual fija una trivialización arbitraria en las fibras $\bar{\mathscr{L}}_{P_i}$, es decir un isomorfismo $\bar{\mathscr{L}}_{P_i} \backsimeq \mathbb{F}_q$, el cual es equivalente a tomar un vector no nulo en cada $\bar{\mathscr{L}}_{P_i}$, por último obtenemos el siguiente diagrama:

$$\begin{array}{ccc} \mathrm{Germ}_{\mathcal{P}} : H^0(\mathscr{L}) & & \\ & \searrow & \\ \downarrow & & \\ \oplus_{i=1}^n \bar{\mathscr{L}}_{P_i} & \xrightarrow{\sim} & \mathbb{F}_q^n \end{array}$$

y consideramos a $C = \mathrm{Germ}_{\mathcal{P}} : H^0(\mathscr{L})$ nuestro código y lo denotamos como $C = (X, \mathcal{P}, \mathscr{L})_H$

Luego, de igual forma que en las construcciones anteriores veamos un teorema para estimar los parámetros.

Teorema 4.8. *Sea X una curva de género g y sea $0 \leq deg(\mathscr{L}) = a < n = |\mathcal{P}|$. Entonces $C = (X, \mathcal{P}, \mathscr{L})_H$ es un $[n, k, d]_q$-code con*

$$\begin{aligned} k \leq & a - g + 1 \\ d \leq & n - a \end{aligned}$$

Demostración: Para toda sección no nula $s \in H^0(\mathscr{L})$, el divisor D de sus ceros pertenece a la clase de divisores correspondiente al fibrado $\mathscr{L}$, entonces el total de números de ceros de s es igual a a (si contamos las multiplicidades), y el numero de ceros pertenecientes a $\mathcal{P}$ es a lo más a, luego $d \geq n - a$, si $a < n$ entonces el mapa $\mathrm{Germ}_{\mathcal{P}}$ es un incrustamiento y $k = H^0(\mathscr{L}) \geq a - g + 1$ por el teorema de Riemman-Roch. ■

Corolario 4.9. *Sea X una curva de género g sobre $\mathbb{F}_q$ y sea $N = |X(\mathbb{F}_q)| > g - 1$, entonces $\forall\, n = g+1, \dots, N$ y $\forall\, k = 1, \dots, n - g$ existe un código lineal $[n, k, d]_q$-code cuyos parámetros satisfacen*

$$k + d = n - g + 1$$

Demostración: Tomemos el conjunto $\mathcal{P} = \{P_1, \dots, P_n\} \subseteq X(\mathbb{F}_q)$ y un fibrado $\mathscr{L} \in \mathrm{Pin}(X)$ de grado $a = k + g - 1$, $g - 1 < a < n$ por el teorema (4.8) tenemos que los parámetros de $C' = (X, \mathcal{P}, \mathscr{L})_H$ cumplen las siguientes condiciones

$$\begin{aligned} k' \leq & a - g + 1 \\ d' \leq & n - a \end{aligned}$$

Utilizamos el lemma (lemma de codigos) tenemos que podemos construir un $[n, k, d]_q$-code C con $d = n - a$, es decir $k + d = n - g + 1$. ■

Ejercicio 4.10. Probar que si $\mathcal{P} \cap \mathrm{Supp}(D) = \emptyset$ entonces la trivialización produce un código $(X, \mathcal{P}, \mathscr{L})_H$ coincidente con $X, \mathcal{P}, D)_L$, ¿cuál es la relación entre $(X, \mathcal{P}, \mathscr{L})_H$ y $X, \mathcal{P}, D)'$ para $\mathrm{Supp}(D) \cap \mathcal{P} \neq \emptyset$?.

Proposición 4.11. *Sea $X \subset \mathbb{P}^m$ una curva y sea $N = |X(\mathbb{F}_q)|$, para cualquier n tal que $N \geq n >$ máx$\{m, deg(X)\}$ entonces existe un código no degenerado $[n, k, d]_q$-code con $k = m + 1$ y $d \geq n - deg(X)$*

Ahora vamos a traducir la construcción (4.7) a otro lenguaje.

Construcción 4.12. Si una variedad X es dada junto a una incrustación proyectiva $X \subset \mathbb{P}^m$ luego cualquier elección de $\mathcal{P} \subseteq X(\mathbb{F}_q)$, tal que $|\mathcal{P}| > m$ y $\mathcal{P}$ no pertenece a un hiperplano, entrega una proyección $[n, k, d]_q$-system con $n = |\mathcal{P}|$, $k = m + 1$, $d = n -$ máx$\{|H \cap \mathcal{P}|\}$, el máximo siendo tomado sobre todos los $\mathbb{F}_q$-hyperplanes $H \subset \mathbb{P}^m$.
Para una curva X (dada por la incrustación), su grado es definido por el número de $\bar{\mathbb{F}}_q$-points (contando las

multiplicidades) en su intersección con un hiperplano arbitrario, en cualquier caso tenemos que $\max_H\{|H \cap \mathcal{P}|\} \leq \deg(X)$, luego por (4.11) podemos hacer lo siguiente.
Sea X una variedad y $\mathscr{L}$ un fibrado en él, el fibrado $\mathscr{L}$ corresponde a un mapeo

$$\varphi_{\mathscr{L}} : X \longrightarrow \mathbb{P}(H^0(\mathscr{L})) \backsimeq \mathbb{P}^{h^0(\mathscr{L})-1}$$

para un sistema proyectivo $[n, k, d]_q$-system, tomemos un subconjunto $\mathcal{P} \subseteq X(\mathbb{F}_q)$ mapeado a $\mathbb{P}(H^0(\mathscr{L}))$ (si algunos puntos están pegados se cuentan con sus multiplicidades correspondientes), luego $n = |\mathcal{P}|$, $k = h^0(\mathscr{L})$. El inverso de las imágenes de una sección de un hiperplano de $\mathbb{P}(H^0(\mathscr{L}))$ son divisores efectivos D pertenecientes a la clase de $\mathscr{L}$, entonces $d = n - \max_D\{|D \cap \mathcal{P}|\}$.
Consideramos ahora el caso de curvas, si X es una curva de genero g y $a = \deg(\mathscr{L})$, entonces $k = h^0(\mathscr{L}) \geq a - g + 1$, más aún $|D(\mathbb{F}_q)| \leq \deg(D) = a$, es decir, $d \geq n - a$, así tenemos una construcción lineal de $[n, k, d]_q$-code denotado como $C = (X, \mathcal{P}, \mathscr{L})_P$.

Ejercicio 4.13. Probar que $(X, \mathcal{P}, \mathscr{L})_H$ y $(X, \mathcal{P}, \mathscr{L})_P$ son equivalentes.

Ejercicio 4.14. Sea $\mathbb{F}_4 = \{0, 1, a, a + 1\}$, C definido por $y^2z + yz^2 + x^3$, es decir $F = \frac{\mathbb{F}_q[x,y,z]}{(y^2z+yz^2+x^3)}$, encontrar la distancia mínima entre palabras

Solución: Los puntos racionales serían $[(0, 0, 1), (0, 1, 0), (0, 1, 1), (1, a, 1), (1, a+1, 1), (a, a, 1), (a, a+1, 1), (a+1, a, 1), (a + 1, a + 1, 1)]$, luego la matriz generadora del código será

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & a+1 & a & a+1 & a & 0 \\ 0 & 0 & 1 & 1 & a & a & a+1 & 0 \\ 0 & 0 & a & a+1 & a+1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & a+1 & a+1 & a & 0 \end{bmatrix}$$

luego la suma de la tercera y quinta fila es (00001110) por lo que $d = 3$.

Observación 4.15. Es importante destacar para los códigos de género 0 que $\mathbb{F}_q$ es $\mathbb{F}_q$-isomorfo a la linea proyectiva $\mathbb{P}^1$.

Definición 4.16. Sea X una curva de género 1, llamaremos al código construido con esta curva **código elíptico**, los cuales existen para cualquier $n \leq N_q(1)$, con $N_q(1)$ es el máximo número de $\mathbb{F}_q$-points posibles en una curva de género 1, para $q = p^m$ tenemos que

$$N_q(1) = \begin{cases} q + \lceil 2\sqrt{q} \rceil, & \text{si } p | \lceil 2\sqrt{q} \rceil, \text{ y } m \geq 3 \text{ es impar} \\ q + \lceil 2\sqrt{q} \rceil + 1, & \text{caso contrario} \end{cases}$$

Ejercicio 4.17. Sea $C : f = YZ - X^2 = 0$ sobre $\mathbb{F}_7$ una curva suave con género 0 y puntos racionales $P_i = (i, i^2, 1)$ para $i = 0, 1, \ldots, 6$ y $Q = (0, 1, 0)$ un punto al infinito, encontrar la matriz parity-check del código.

Solución: Sea $x = X/Z$ y $L(mQ)$ es espacio vectorial generado por x^i con $i = 0, 1, \ldots, m$, entonces sea $B = P_0 + \cdots + P_6$, entonces la matriz será

$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ x(p_0) & x(p_1) & x(p_2) & \ldots & 2x(p_6) \\ x^2(p_0) & x^2(p_1) & x^2(p_2) & \ldots & x^2(p_6) \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ x^m(p_0) & x^m(p_1) & x^m(p_2) & \ldots & x^m(p_6) \end{bmatrix}$$

Y se evalúa en

$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & 2 & \ldots & 6 \\ 0 & 1 & 2^2 & \ldots & 6^2 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 1 & 2^m & \ldots & 6^m \end{bmatrix}$$

Ejercicio 4.18. Sea $C : f = X^3 + Y^2Z + YZ^2$ una curva suave con género 1, tiene 9 puntos racionales y uno al infinito $Q = (0, 1, 0)$, encontrar la parity-check matrix.

Solución: Tomemos B como la suma de todos los puntos racionales menos el infinito; el código posee una distancia mínima de $d^* = a - (2g - 2) = a$, luego sea $a = 5$ para que soporte errores de 2 dígitos, el rango sería $8 - a + 1 - 1 = 3$, tenemos $L(5Q) = \langle 1, x, y, x^2, xy\rangle$, tomemos $\mathbb{F}_4 := \mathbb{F}_2[\omega]$ con $\omega^2 + \omega + 1 = 0$, luego

$$P_1 = (0, 0, 1) \quad P_2 = (0, 0, 1) \quad P_3 = (1, \omega, 1) \quad P_4 = (1, \omega^2, 1)$$
$$P_5 = (\omega, \omega, 1) \quad P_6 = (\omega, \omega^2, 1) \quad P_7 = (\omega^2, \omega, 1) \quad P_8 = (\omega^2, \omega^2, 1)$$

Luego la matriz sería

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ x(P_1) & x(P_2) & \dots & x(P_8) \\ y(P_1) & y(P_2) & \dots & y(P_8) \\ x^2(P_1) & x^2(P_2) & \dots & x^2(P_8) \\ xy(P_1) & xy(P_2) & \dots & xy(P_8) \end{bmatrix}$$

evaluando tenemos

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 0 & 1 & \omega & \omega^2 & \omega & \omega^2 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & \omega^2 & \omega^2 & \omega & \omega \\ 0 & 0 & \omega & \omega^2 & \omega^2 & 1 & 1 & \omega \end{bmatrix}$$

Referencias

[1] Ravi Vakil, *The Rising Sea: Foundations of Algebraic Geometry*, Preprint (2017).
[2] Tsfasman & Vladut, *Algebraic-Geometric Codes*, (1991).
[3] Carlos Munuera & Fernando Torres, *Sobre Curvas Algebraicas Y Códigos Correctores.*
[4] Zhuo Jia Dai , *Algebraic Geometric Coding Theory*, (2006).
[5] Norman E. Hurt , *Code Theory and Algebraic Geometry*, (2006).

Departamento de Matemática, Universidad Técnica Federico Santa María, Santiago, Chile.
Email address: lucas.montero.14@sansano.usm.cl