UNIVERSIDAD
DE GRANADA

Facultad de Ciencias

E.T.S. de Ingenierías Informática y de Telecomunicación

Doble Grado en Ingeniería Informática y Matemáticas

TRABAJO DE FIN DE GRADO

Algoritmo de Peterson-Gorenstein-Zierler para códigos cíclicos sesgados

[25 de febrero de 2020 a las 11:01 – 1.0]

Presentado por

José María Martín Luque

Tutorizado por

Gabriel Navarro Garulo

Curso académico 2019–2020

ÍNDICE GENERAL

RESUMEN

Resumen.

SUMMARY

Summary.

INTRODUCCIÓN

El padre de la teoría de la información Claude Shannon. El libro *Mathematical Theory of Cryptography* (1945) y su ampliación posterior, *Mathematical Theory of Communication* (1948)

Francis Bacon ya afirmó en el año 1623 que únicamente son necesarios dos símbolos para codificar toda la comunicación.

> La transposición de dos letras en cinco emplazamientos bastará para dar 32 diferencias [y] por este arte se abre un camino por el que un hombre puede expresar y señalar las intenciones de su mente, a un lugar situado a cualquier distancia, mediante objetos ... capaces solo de una doble diferencia. (Dyson, 2015, p. 30)

Bla bla bla

Parte I

PARTE DE PRUEBA

1

PRELIMINARES

En este capítulo se detallan algunos conceptos básicos de Álgebra que son necesarios para la comprensión más adelante de la teoría de códigos. Según (Cohn, 1982) y (Cohn, 1989) y el libro de Jacobson.

1.1 ANILLOS

DEFINICIÓN 1.1.1. Un *anillo* es un conjunto junto a dos operaciones: la suma (+) y la multiplicación (·), que verifican las siguientes propiedades.

- Propiedad asociativa:

$$(x + y) + z = x + (y + z), \qquad (xy)z = x(yz).$$

- Propiedad conmutativa para la suma:

$$x + y = y + x.$$

- Existencia de elemento neutro:

$$x + 0 = x, \qquad x1 = x.$$

- Existencia de elemento inverso para la suma:

$$x + (-x) = 0.$$

- Propiedad distributiva para la multiplicación sobre la suma:

$$x(y + z) = xy + xz.$$

Si un anillo verifica la propiedad conmutativa para la multiplicación, es decir, $xy = yx$, se dice que es un *anillo conmutativo*.

Dos anillos son *isomorfos* si hay un *isomorfismo* entre ellos, es decir, existe una biyección que preserva todas las operaciones. Decimos que los anillos isomorfos son idénticos, pues intrínsecamente son iguales.

En cualquier anillo R se verifica que $0x = x0 = 0$ para todo $x \in R$, ya que $x0 = x(0 + 0) = x0 + x0$, de donde concluimos que $x0 = 0$ e igualmente, $0x = 0$.

El *anillo trivial* es aquel que solo tiene un elemento. Necesariamente entonces $1 = 0$, pero este es el único caso en el que ocurre. Supongamos que $1 = 0$. Entonces, para cada elemento x del anillo se tiene que $x = x1 = x0 = 0$, luego tiene un único elemento.

Un elemento a de un anillo se dice que es *invertible* si existe un elemento a' en el anillo tal que $aa' = a'a = 1$. A este elemento, que es único lo llamamos *elemento inverso* de a y lo denotamos por a^{-1}. El elemento 0 no puede tener inverso porque ya hemos visto que siempre que se multiplique por él se obtiene el 0. Los anillos en los que todo elemento distinto de 0 es invertible se llaman *anillos de división*.

DEFINICIÓN 1.1.2 (SUBANILLO). Un subconjunto S de un anillo R se denomina *subanillo* si S es cerrado bajo las operaciones de suma y producto de R y forma un anillo con estas operaciones.

DEFINICIÓN 1.1.3 (IDEAL). Un subconjunto J de un anillo R se denomina *ideal* si J es un subanillo de R y para todo $a \in J$ y $r \in R$ se verifica que $ar \in J$ y $ra \in J$.

EJEMPLO 1.1.4.

- Sea R el cuerpo $\mathbb{Q}$ de números racionales. Entonces, el conjunto $\mathbb{Z}$ de los enteros es un subanillo de $\mathbb{Q}$ pero no es un ideal porque, por ejemplo, $1 \in \mathbb{Z}, 1/2 \in \mathbb{Q}$, pero $1/2 \cdot 1 = 1/2 \notin \mathbb{Z}$.
- Sea R un anillo conmutativo, $a \in R$ y sea $J = \{ra : r \in R\}$. Entonces, J es un ideal.

DEFINICIÓN 1.1.5. Sea R un anillo conmutativo. Un ideal J de R se dice que es *principal* si existe un elemento $a \in R$ tal que $J = (a) = \{ra : r \in R\}$.

Dado un elemento del anillo distinto de cero, podemos clasificarlo en dos tipos. Sea $a \neq 0$. Si existe $b \neq 0$ tal que ab o ba es cero, entonces a es un elemento *divisor de cero*, y en caso contrario, un elemento *regular*.

Un anillo no trivial sin divisores de cero se dice que es *entero*, un anillo entero conmutativo se denomina *dominio de integridad*.

Una propiedad importante de los elementos regulares es la ley de cancelación.

PROPOSICIÓN 1.1.6. *Si c es un elemento regular de un anillo R entonces para cada $a, b \in R$, tales que $ca = cb$ o bien $ac = bc$, se tiene que $a = b$.*

DEFINICIÓN 1.1.7. Sea R un anillo. La *característica* del anillo es el menor natural n tal que $n1 = 0$. Si no existe tal número, la característica del anillo es 0.

1.2 CUERPOS FINITOS

DEFINICIÓN 1.2.1. Un *cuerpo* es un anillo de división conmutativo. Se dice que un cuerpo es *finito* si tiene un número finito de elementos, al que llamamos *orden* del cuerpo.

Sea F un cuerpo. Un subconjunto K de F que es por sí mismo un cuerpo bajo las operaciones de F se denomina *subcuerpo* de F. También podemos decir que F es una extensión de K.

De hecho todas las nociones que hemos definido para anillos (característica, ...) son válidas para los cuerpos, pues un cuerpo no deja de ser un anillo.

TEOREMA 1.2.2. *Todo cuerpo F tiene al menos un subcuerpo P, el subcuerpo primo de F que está contenido en cada subcuerpo de F. O bien F tiene característica 0 y $P \cong \mathbb{Q}$ o bien F tiene característica p, un número primo, y entonces $P \cong \mathbb{F}_p$.*

Mención especial merecen los cuerpos finitos.

Un cuerpo con un número finito de elementos se denomina *cuerpo finito* o *cuerpo de Galois*, por su descubridor.

Sea V un espacio vectorial n-dimensional sobre $\mathbb{F}_p$, el cuerpo de p elementos. Si $u_1, \dots, u_n$ es una base de V, entonces cada elemento de V se escribe de forma única en la forma $\sum \alpha_i u_i$, donde $\alpha_i \in \mathbb{F}_p$. Como cada coeficiente puede tener hasta p valores distintos, obtenemos un total de p^n elementos.

LEMA 1.2.3. *Un espacio vectorial n-dimensional sobre $\mathbb{F}_p$ tiene p^n elementos.*

Todo cuerpo finito F tiene claramente característica p en virtud del teorema 1.2.2 y su subcuerpo primo es $\mathbb{F}_p$.

1.3 ANILLOS DE POLINOMIOS

Para cualquier anillo R podemos definir un anillo de polinomios en x con coeficientes en x.

Trabajaremos con anillos de polinomios en cuerpos finitos.

Denotamos el anillo de le los polinomios con coeficientes en $\mathbb{F}_q$ por $\mathbb{F}_q[x]$. Es un anillo conmutativo con las operaciones habituales de suma y multiplicación de polinomios. De hecho, es un dominio de integridad.

Un polinomio en $\mathbb{F}_q[x]$ viene dado por $f(x) = \sum_{i=0}^{n} a_i x^i$, donde a_i son los coeficientes del término de grado i y pertenecen a $\mathbb{F}_q$.

El grado de un polinomio es el mayor grado de cualquier término con coeficiente distinto de cero.

PROPOSICIÓN 1.3.1. *Grado de sumas y productos*

El coeficiente del término de mayor grado se denomina *coeficiente líder*.

Un polinomio es *mónico* si su coeficiente líder es 1. Sean $f(x)$ y $g(x)$ polinomios en $\mathbb{F}_q[x]$. Decimos que $f(x)$ *divide a* $g(x)$, denotado por $f(x)|g(x)$, si existe un polinomio $h(x) \in \mathbb{F}_q[x]$ tal que $g(x) = f(x)h(x)$. El polinomio $f(x)$ se llama *divisor* o *factor* de $g(x)$. El *máximo común divisor* de $f(x)$ y $g(x)$, siendo al menos uno de ellos distinto de cero, es el polinomio mónico de $\mathbb{F}_q[x]$ de mayor grado que divida tanto a $f(x)$ como a $g(x)$. Lo denotamos por $\text{mcd}(f(x), g(x))$. Dos polinomios son *primos relativos* si su máximo común divisor es 1.

TEOREMA 1.3.2. *Sean $f(x)$ y $g(x)$ polinomios de $\mathbb{F}_q[x]$, siendo $g(x)$ distinto de cero.*

1. *Existen polinomios únicos, $h(x), r(x) \in \mathbb{F}_q[x]$ tales que*

$$f(x) = g(x)h(x) + r(x), \quad \textit{donde } \operatorname{gr} r(x) < \operatorname{gr} g(x) \textit{ o } r(x) = 0.$$

2. *Si $f(x) = g(x)h(x) + r(x)$, entonces*

$$\text{mcd}(f(x), g(x)) = \text{mcd}(g(x), r(x)).$$

Un polinomio no constante $f(x) \in \mathbb{F}_q[x]$ es *irreducible sobre* $\mathbb{F}_q$ si no es posible factorizarlo como producto de dos polinomios de $\mathbb{F}_q[x]$ de grado menor.

TEOREMA 1.3.3. *Sea $f(x)$ un polinomio no constante. Entonces,*

$$f(x) = p_1(x)^{a_1} p_2(x)^{a_2} \dots p_k(x)^{a_k},$$

donde cada $p_i(x)$ es irreducible, los polinomios $p_i(x)$ son únicos salvo producto por escalares y los elementos a_i son únicos.

Esto nos dice que $\mathbb{F}_q[x]$ es lo que se conoce como *dominio de factorización única*. Pero es además un dominio de ideales principales.

Demostración. □

Para construir un cuerpo de característica p comenzamos con un polinomio $f(x) \in \mathbb{F}_q[x]$ que es irreducible sobre $\mathbb{F}_q$ y que tiene grado m. Usando el algoritmo de euclides podemos demostrar que el anillo cociente dado por $\mathbb{F}_p[x]/(f(x))$ es un cuerpo, y de hecho, un cuerpo finito con $q = p^m$ elementos.

Demostración. □

Cada elemento de dicho anillo cociente es una clase lateral de la forma $g(x) + (f(x))$, donde $g(x)$ es único y tiene grado ocmo mucho $m - 1$.

Escribiremos cada clase lateral como un vector en $\mathbb{F}_p^m$ siguiendo la correspondencia:

$$g_{m-1}x^{m-1} + g_{m-2}x^{m-2} + \cdots + g_1x + g_0 + (f(x)) \iff g_{m-1}g_{m-2}\cdots g_1g_0.$$

Esta notación de vectorial nos permite realizar la suma en el cuerpo utilizando la suma habitual de los vectores. Multiplicar es una tarea a priori más complicada. Para multiplicar $g_1(x)+(f(x))$ por $g_2(x)+(f(x))$ primero utilizamos al algoritmo de división para escribir

$$g_1(x)g_2(x) = f(x)h(x) + r(x),$$

donde como sabemos o bien $\operatorname{gr} r(x) \leq m - 1$ o bien $r(x) = 0$. Puesto que estamos en el anillo cociente $\mathbb{F}_p[x]/(f(x))$ nos queda

$$(g_1(x) + (f(x)))(g_2(x) + (f(x))) = r(x) + (f(x)).$$

Esta notación es engorrosa, por lo que habitualmente operaremos en α en vez de en x suponiendo que $f(\alpha) = 0$. Así, $g_1(\alpha)g_2(\alpha) = r(\alpha)$. En consecuencia, multiplicamos los polinomios en α de la forma habitual y utilizamos la ecuación $f(\alpha) = 0$ para reducir las potencias de α de grado mayor a $m - 1$ a polinomios en α de grado menor que m.

El conjunto $\{0\alpha^{m-1} + 0\alpha^{m-2} + \cdots + 0\alpha + a_0 \mid a_0 \in \mathbb{F}_p\} = \{a_0 \mid a_0 \in \mathbb{F}_p\}$ es el subcuerpo primo de $\mathbb{F}_q$.

Decimos que obtenemos $\mathbb{F}_q$ a partir de $\mathbb{F}_p$ yuxtaponiendo una raíz α de $f(x)$ a $\mathbb{F}_p$. Esta raíz viene dada formalmente por $\alpha = x + (f(x))$ en el anillo cociente $\mathbb{F}_p[x]/(f(x))$. Por tanto, ya hemos visto antes que $g(x)+(f(x)) = g(\alpha)$ y $f(\alpha) = f(x+(f(x))) = f(x)+(f(x)) = 0+(f(x))$.

Un polinomio irreducible sobre $\mathbb{F}_p$ de grado m es *primitivo* si tiene una raíz que es un elemento primitivo de $\mathbb{F}_q = \mathbb{F}_{p^m}$. Puede probarse que existen polinomios irreducibles de cualquier grado.

TEOREMA 1.3.4. *Para cualquier primo p y cualquier entero positivo m, existe un cuerpo finito, único salvo isomorfismos, con $q = p^m$ elementos.*

1.4 AUTOMORFISMOS

2

FUNDAMENTOS DE TEORÍA DE CÓDIGOS

La teoría de códigos (...). Las definiciones y los resultados comentados en esta sección seguirán lo descrito en (Huffman & Pless, 2003, pp. 1-48) y (Podestá, 2006).

2.1 CÓDIGOS LINEALES

Vamos a comenzar nuestro estudio con los códigos lineales, pues son los más sencillos de comprender. Consideremos el espacio vectorial de todas las n-tuplas sobre el cuerpo finito $\mathbb{F}_q$, al que denotaremos en lo que sigue como $\mathbb{F}_q^n$. A los elementos $(a_1, \dots, a_n)$ de $\mathbb{F}_q^n$ los notaremos usualmente como $a_1 \cdots a_n$.

DEFINICIÓN 2.1.1. Un (n, M) *código* $\mathcal{C}$ sobre el cuerpo $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ de tamaño M. A los elementos de $\mathcal{C}$ los llamaremos *palabras codificadas* —o *codewords* en inglés—.

Es necesario añadir más estructura a los códigos para que sean de utilidad.

DEFINICIÓN 2.1.2. Decimos que un código $\mathcal{C}$ es un código *lineal de longitud n y rango k* —abreviado como $[n, k]$ *lineal*— si dicho código es un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k.

Un código lineal $\mathcal{C}$ tiene q^k palabras codificadas.

DEFINICIÓN 2.1.3. Una *matriz generadora* para un $[n, k]$ código $\mathcal{C}$ es una matriz $k \times n$ cuyas filas conforman una base de $\mathcal{C}$.

Veamos un ejemplo de matriz generadora. Consideremos la matriz $G = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right) \in \mathcal{M}_{2\times 3}(\mathbb{F}_2)$. Dicha matriz genera un $[3, 2]$ código binario, pues dado (x_1, x_2), se tiene que

$$(x_1, x_2)\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = (x_1, x_1 + x_2, x_2),$$

y por tanto este código codifica de la forma

$$00 \longrightarrow 000, \quad 01 \longrightarrow 011, \quad 10 \longrightarrow 110, \quad 11 \longrightarrow 101.$$

DEFINICIÓN 2.1.4. Para cada conjunto k de columnas independientes de una matriz generadora G el conjunto de coordenadas correspondiente se denomina *conjunto de información* para un código $\mathcal{C}$. Las $r = n - k$ coordenadas restantes se llaman *conjunto redundante*, y el número r, la *redundancia* de $\mathcal{C}$.

Si las primeras k coordenadas forman un conjunto de información el código tiene una única matriz generadora de la forma $[I_k \mid A]$, donde I_k es la matriz identidad $k \times k$ y A es una matriz $k \times r$. Esta matriz generadora se dice que está en *forma estándar*.

Como un código lineal $\mathcal{C}$ es un subespacio de un espacio vectorial, podemos calcular el ortogonal a dicho subespacio, obteniendo lo que llamaremos el *código dual* $\mathcal{C}^\perp$.

DEFINICIÓN 2.1.5. El *código dual* $\mathcal{C}^\perp$ de un código $\mathcal{C}$ viene dado por

$$\mathcal{C}^\perp = \left\{ x \in \mathbb{F}_q^n \,:\, x \cdot c = 0 \quad \forall c \in \mathcal{C} \right\}.$$

DEFINICIÓN 2.1.6. Sea $\mathcal{C}$ un $[n,k]$ código lineal. Una matriz H se dice que es *matriz de paridad* si es una matriz generadora de $\mathcal{C}^\perp$.

PROPOSICIÓN 2.1.7. *Sea H la matriz de paridad de un $[n,k]$ código lineal $\mathcal{C}$. Entonces,*

$$\mathcal{C} = \left\{ x \in \mathbb{F}_q^n \,:\, xH^T = 0 \right\} = \left\{ x \in F_q^n \,:\, Hx^T = 0 \right\}.$$

Demostración. Sea $c \in \mathcal{C}$ una palabra codificada. Sabemos que la podemos expresar como $c = uG$, donde $u \in \mathbb{F}_q^k$ y G es la matriz generadora de $\mathcal{C}$. Tenemos entonces que $cH^T = uGH^T$ y como $GH^T = 0$ —por ser H matriz generadora del subespacio ortogonal $\mathcal{C}$— se tiene que

$$\mathcal{C} \subset S_H = \left\{ x \in \mathbb{F}_q^n \,:\, Hx^T = 0 \right\},$$

que es el espacio solución de un sistema de $n - k$ ecuaciones con n incógnitas y de rango $n - k$. Como $\dim(S_H) = n - (n - k) = k = \dim L$, concluimos que

$$L = S_H = \left\{ x \in \mathbb{F}_q^n \,:\, Hx^T = 0 \right\}. \qquad \square$$

El resultado anterior, junto a la definición anterior, nos conducen al siguiente teorema.

TEOREMA 2.1.8. *Si $G = [I_k \mid A]$ es una matriz generadora para un $[n,k]$ código $\mathcal{C}$ en forma estándar entonces $H = [-A \mid I_{n-k}]$ es una matriz de paridad para $\mathcal{C}$.*

Un código se dice *autoortogonal* cuando $\mathcal{C} \subseteq \mathcal{C}^\perp$, y *autodual* cuando $\mathcal{C} = \mathcal{C}^\perp$.

2.1.1 *Distancias y pesos*

DEFINICIÓN 2.1.9. La *distancia de Hamming* $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y})$ entre dos vectores $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ se define como el número de coordenadas en las que difieren $\boldsymbol{x}$ e $\boldsymbol{y}$.

TEOREMA 2.1.10. *La función de distancia* $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y})$ *verifica las siguientes propiedades.*

1. *No negatividad:* $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) \geq 0$ *para todo* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$.
2. $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = 0$ *si y solo si* $\boldsymbol{x} = \boldsymbol{y}$.
3. *Simetría:* $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{d}(\boldsymbol{y}, \boldsymbol{x})$ *para todo* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$.
4. *Desigualdad triangular:* $\mathrm{d}(\boldsymbol{x}, \boldsymbol{z}) \leq \mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) + \mathrm{d}(\boldsymbol{y}, \boldsymbol{z})$ *para todo elemento* $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbb{F}_q^n$.

La *distancia (mínima)* de un código $\mathcal{C}$ es la menor distancia posible entre dos palabras codificadas distintas. Es importante a la hora de determinar la capacidad de corrección de errores del código $\mathcal{C}$, pues como veremos más tarde, a mayor distancia mínima, mayor número de errores en el código se pueden corregir.

DEFINICIÓN 2.1.11. El *peso de Hamming* $\mathrm{wt}(\boldsymbol{x})$ de un vector $\boldsymbol{x}$ es el número de coordenadas distintas de cero de $\boldsymbol{x}$.

TEOREMA 2.1.12. *Si* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$, *entonces* $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{wt}(\boldsymbol{x} - \boldsymbol{y})$. *Si* $\mathcal{C}$ *es un código lineal, la distancia mímina es igual al peso mínimo de las palabras codificadas de* $\mathcal{C}$ *distintas de cero.*

Como consecuencia de este teorema —para códigos lineales— la distancia mínima también se llama *peso mínimo* del código. Si el peso mínimo d de un $[n, k]$ código es conocida, nos referiremos a él como un $[n, k, d]$ código.

DEFINICIÓN 2.1.13. Sea $A_i(\mathcal{C})$ —que abreviaremos A_i— el número de palabras codificadas de peso i en $\mathcal{C}$. Para cada $0 \leq i \leq n$, la lista A_i se denomina *distribución de peso* o *espectro de peso* de $\mathcal{C}$.

EJEMPLO 2.1.14. Sea $\mathcal{C}$ el código binario con matriz generadora

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Dado (x_1, x_2, x_3), se tiene que

$$(x_1, x_2, x_3)\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} = (x_1, x_1, x_2, x_2, x_3, x_3),$$

y por tanto este código codifica de la forma

$$000 \longrightarrow 000000, \quad 001 \longrightarrow 000011, \quad 010 \longrightarrow 001100, \quad 011 \longrightarrow 001111,$$

$$100 \longrightarrow 110000, \quad 101 \longrightarrow 110011, \quad 110 \longrightarrow 111100, \quad 111 \longrightarrow 111111.$$

Luego la distribución de peso de $\mathcal{C}$ es $A_0 = A_6 = 1$ y $A_2 = A_4 = 3$. Usualmente solo se listan los A_i que son distintos de cero.

TEOREMA 2.1.15. *Sea $\mathcal{C}$ un $[n, k, d]$ código sobre $\mathbb{F}_q$. Entonces,*

1. $A_0(\mathcal{C}) + A_1(\mathcal{C}) + \cdots + A_n(\mathcal{C}) = q^k$.
2. $A_0(\mathcal{C}) = 1$ *y* $A_1(\mathcal{C}) = A_2(\mathcal{C}) = \cdots = A_{d-1}(\mathcal{C}) = 0$.

TEOREMA 2.1.16. *Sea $\mathcal{C}$ un código lineal con matriz de paridad H. Si $\boldsymbol{c} \in \mathcal{C}$, las columnas de H que se corresponden con coordenadas no nulas de $\boldsymbol{c}$ son linealmente independientes. Recíprocamente, si entre w columnas de H existe una relación de dependencia lineal con coeficientes no nulos, entonces hay una palabra codificada en $\mathcal{C}$ de peso w cuyas coordenadas no nulas se corresponden con dichas columnas.*

COROLARIO 2.1.17. *Un código lineal tiene peso mínimo d si y solo si su matriz de paridad tiene un conjunto de d columnas linealmente dependientes pero no tiene un conjunto de $d-1$ columnas linealmente dependientes.*

2.2 EJEMPLOS DE CÓDIGOS

2.2.1 *Códigos de Hamming*

Consideremos una matriz $r \times (2^r - 1)$ cuyas columnas son los números $1, 2, 3, \ldots, 2^{r-1}$ escritos en binario. Dicha matriz es la matriz de paridad de un $[n = 2^{r-1}, k = n-r]$ código binario. A los códigos de esta forma los llamaremos códigos de Hamming de longitud $n = 2^{r-1}$ y los denotamos por $\mathcal{H}_r$ o $\mathcal{H}_{2,r}$.

Como las columnas son distintas y no dula, la distancia es al menos 3 por el corolario 2.1.17. Además, como las columnas correspondientes a los números $1, 2, 3$ son linealmente independientes, la distancia mínima

es 3 por el mismo corolario. Podemos decir por tanto que los códigos de Hamming $\mathcal{H}_r$ son $[2^{r-1}, 2^{r-1-r}, 3]$ códigos binarios.

Podemos generalizar esta definición y definir los códigos de Hamming $\mathcal{H}_{q,r}$ sobre un cuerpo finito arbitrario $\mathbb{F}_q$. Para $r \geq 2$ un código $\mathcal{H}_{q,r}$ tiene matriz de paridad $H_{q,r}$, cuyas columnas están compuestas por un vector no nulo por cada uno de los subespacios de dimensión 1 de $\mathbb{F}_q^r$. Hay $(q^r - 1)/(q - 1)$ subespacios de dimensión 1, por lo que $\mathcal{H}_{q,r}$ tiene longitud $n = (q^r - 1)/(q - 1)$, dimensión $n - r$ y redundancia r. Como todas las columnas son independientes unas de otras, $\mathcal{H}_{q,r}$ tiene peso mínimo al menos 3. Si sumamos dos vectores no nulos de dos subespacios unidimensionales distintos obtenemos un vector no nulo de un tercer subespacio unidimensional, por lo que $\mathcal{H}_{q,r}$ tiene peso mínimo 3. Cuando $q = 2$, $\mathcal{H}_{2,r}$ es el código $\mathcal{H}_r$.

2.3 CÓDIGOS CÍCLICOS

Un código lineal $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ es *cíclico* si para cada vector $\boldsymbol{c} = c_0 \dots_{n-2} c_{n-1}$ en $\mathcal{C}$, el vector $c_{n-1}c_0 \dots c_{n-2}$ –obtenido a partir de $\boldsymbol{c}$ haciendo desplazando cíclicamente las coordenadas, llevando $i \mapsto i + 1$ mód n– también está en $\mathcal{C}$. Pensamos en la posición de las coordenadas de forma cíclica, al llegar a $n - 1$ comienzas de nuevo en 0. Al hablar de coordenadas consecutivas siempre tendremos en cuenta esta ciclicidad.

Cuando trabajemos con códigos cíclicos representaremos las palabras codificadas como polinomios. Hay una biyección entre el vector $\boldsymbol{c} = c_0c_1 \dots c_{n-1}$ en $\mathbb{F}_q$ y los polinomios de forma $c(x) = c_0 + c_1x + \dots c_{n-1}x^{n-1}$ en $\mathbb{F}_q[x]$ de grado al menos $n - 1$. Obsérvese que dado $c(x)$ descrito como antes, $xc(x) = c_{n-1}x^n + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}$, que equivaldría a representar la palabra codificada $\boldsymbol{c}$ desplazada una posición a la derecha si x^n fuese igual a 1.

Formalmente, el hecho de que un código $\mathcal{C}$ sea invariante bajo un desplazamiento cíclico implica que si $c(x)$ está en $\mathcal{C}$, también lo está $xc(x)$, siempre que multipliquemos módulo $x^n - 1$. Esto nos sugiere que el contexto para estudiar códigos cíclicos es el anillo cociente $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1)$.

Por tanto, bajo la correspondencia vectores-polinomios que hemos descrito antes, los códigos cíclcos son ideales de $\mathcal{R}_n$, y los ideales de $\mathcal{R}_n$ son códigos cíclicos. En consecuencias, el estudio de los códigos cíclicos en $\mathbb{F}_q^n$ es equivalente al estudio de los ideales en $\mathcal{R}_n$, que depende de la factorización de $x^n - 1$.

2.3.1 *Factorización de $x^n - 1$*

Existen dos posibilidades: o bien $x^n - 1$ tiene factores irreducibles repetidos, o no.

Para factorizar $x^n - 1$ sobre $\mathbb{F}_q$ es útil considerar la extensión de cuerpos $\mathbb{F}_{q^t}$ de $\mathbb{F}_q$ que contenga todas sus raíces. $\mathbb{F}_{q^t}$ debe contener una enésima raíz primitiva de la unidad, que ocurre cuando $n \mid (q^t - 1)$ por el teorema...

2.3.2 .

Vamos a ver que hay una correspondencia biyectiva entre los códigos cíclicos en $\mathcal{R}_n$ y los polinomios mónicos divisores de $x^n - 1$.

Teorema 2.3.1. *Sea $\mathcal{C}$ un ideal de $\mathcal{R}_n$, es decir, un código cíclico de longitud n. Entonces:*

1. *Existe un único polinomio mónico $g(x)$ de grado mínimo en $\mathcal{C}$.*
2. *El polinomio descrito en 1 genera $\mathcal{C}$, es decir, $\mathcal{C} = \langle g(x) \rangle$.*
3. *El polinomio descrito en 1 verifica que $g(x) \mid x^n - 1$.*

Sea $k = n - \operatorname{gr} g(x)$ y sea $g(x) = \sum_{i_0}^{n-k} g_i x^i$, donde $g_{n-k} = 1$. Entonces:

4. *Se verifica que*

$$\mathcal{C} = \langle g(x) \rangle = \{ f(x)g(x) \,:\, \operatorname{gr} f(x) < k \}.$$

5. *El conjunto $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ es una base de $\mathcal{C}$ y $\mathcal{C}$ tiene dimensión k.*
6. *La matriz G dada por*

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & \cdots & g_{n-k} & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_{n-k} & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & & \ddots & 0 \\ 0 & 0 & \ldots & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_{n-k} \end{bmatrix},$$

donde cada fila es un desplazamiento cíclico de la fila previa, es una matriz generadora de $\mathcal{C}$.

7. *Si α es una raíz enésima primitiva de la unidad en alguna extensión de cuerpos de $\mathbb{F}_q$ entonces*

$$g(x) = \prod_s M_{\alpha^s}(x),$$

siendo el producto sobre un subconjunto de representantes de las clases q-ciclotómicas módulo n.

Demostración. Veamos la demostración apartado por apartado.

1. Supongamos que $\mathcal{C}$ contiene dos polinomios mónicos distintos, $g_1(x)$ y $g_2(x)$, de grado mínimo r. Entonces, $g_1(x) - g_2(x)$ es un polinomio no nulo de grado menor que r, lo que es absurdo. Existe por tanto un único polinomio de grado mínimo r en $\mathcal{C}$, como queríamos.

2. Como $g(x) \in \mathcal{C}$ y $\mathcal{C}$ es un ideal, tenemos que $\langle g(x)\rangle \subset \mathcal{C}$. Por otra parte, dado $p(x) \in \mathcal{C}$ el algoritmo de división nos da elementos $q(x), r(x)$ tales que $p(x) = q(x)g(x) + r(x)$, de forma que o bien $r(x) = 0$ o bien $\operatorname{gr} r(x) < \operatorname{gr} g(x)$. Como podemos expresar $r(x)$ de la forma $r(x) = p(x) - q(x)g(x) \in \mathcal{C}$ y tiene grado menor que $\operatorname{gr} g(x)$, al ser este último de grado mínimo necesariamente ha de darse que $r(x) = 0$. Por tanto, $p(x) = q(x)g(x) \in \langle g(x)\rangle$ y $\mathcal{C} \subset \langle g(x)\rangle$. En consecuencia, $\langle g(x)\rangle = \mathcal{C}$.

3. Por el algoritmo de división, al dividir $x^n - 1$ por $g(x)$ tenemos $x^n - 1 = q(x)g(x) + r(x)$. De nuevo, o bien $r(x) = 0$ o bien $\operatorname{gr} r(x) < \operatorname{gr} g(x)$. Como en $\mathcal{R}_n$ se tiene que $x^n - 1 = 0 \in \mathcal{C}$, necesariamente $r(x) \in \mathcal{C}$. Esto supone una contradicción, a menos que $r(x) = 0$. En consecuencia, $g(x) \mid x^n - 1$.

4. El ideal generado por $g(x)$ es $\langle g(x)\rangle = \{f(x)g(x) : f(x) \in \mathcal{R}_n\}$. Queremos ver que podemos restringir los polinomios $f(x)$ a aquellos que tengan grado menor que k. Por 3 sabemos que $x^n - 1 = h(x)g(x)$ para algún polinomio $h(x)$ de grado $k = n - \operatorname{gr} g(x)$. Dividimos entonces $f(x)$ por este polinomio $h(x)$ y por el algoritmo de división obtenemos $f(x) = q(x)h(x) + r(x)$, donde $\operatorname{gr} r(x) < \operatorname{gr} h(x) = k$. Entonces, tenemos

$$\begin{aligned} f(x)g(x) &= q(x)h(x)g(x) + r(x)g(x) \\ &= q(x)(x^n - 1) + r(x)g(x), \end{aligned}$$

luego $f(x)g(x) = r(x)g(x)$, y como ya hemos visto que $\operatorname{gr} r(x) < k$, tenemos lo que buscábamos.

5. A partir de (4) tenemos que el conjunto

$$\{g(x), xg(x), \dots, x^{k-1}g(x)\}$$

genera $\mathcal{C}$, y como es linealmente independiente, forma una base de $\mathcal{C}$. Esto demuestra también que la dimensión de $\mathcal{C}$ es k.

6. La matriz G es matriz generadora de $\mathcal{C}$ pues

$$\{g(x), xg(x), \dots, x^{k-1}g(x)\}$$

es una base de $\mathcal{C}$.

7. TODO.

□

Este teorema nos muestra que existe un polinomio mónico $g(x)$ que divide a $x^n - 1$ y genera $\mathcal{C}$. Vamos a ver a continuación que dicho polinomio es único.

COROLARIO 2.3.2. *Sea $\mathcal{C}$ un código cíclico en $\mathcal{R}_n$ distinto de cero. Son equivalentes:*

1. *El polinomio $g(x)$ es el polinomio mónico de menor grado en $\mathcal{C}$.*
2. *Podemos expresar $\mathcal{C}$ como $\mathcal{C} = \langle g(x) \rangle$, $g(x)$ es mónico y $g(x) \mid (x^n - 1)$.*

Demostración. Que (1) implica (2) ya lo hemos probado en el teorema 2.3.1. Veamos que partiendo de (2) obtenemos (1). Sea $g_1(x)$ el polinomio mónico de menor grado en $\mathcal{C}$. Por el teorema 2.3.1, $g_1(x) \mid g(x)$ en $\mathbb{F}_q[x]$ y $\mathcal{C} = \langle g_1(x) \rangle$. Como $g_1(x) \in \mathcal{C} = \langle g(x) \rangle$, podemos expresar $g_1(x) = g(x)a(x)$ mód $x^n - 1$, luego tenemos que $g_1(x) = g(x)a(x) + (x^n - 1)b(x)$ en $\mathbb{F}_q[x]$. Por otro lado, como $g(x) \mid (x^n - 1)$, tenemos que $g(x) \mid g(x)a(x) + (x^n - 1)b(x)$, o lo que es lo mismo, que $g(x) \mid g_1(x)$. En consecuencia, como $g_1(x)$ y $g(x)$ son ambos mónicos y dividen el uno al otro en $\mathbb{F}_q[x]$, son necesariamente iguales. □

A este polinomio lo llamamos *polinomio generador* del código cíclico $\mathcal{C}$. Por el corolario anterior, este polinomio es tanto el polinomio mónico en $\mathcal{C}$ de grado mínimo como el polinomio mónico que divide a $x^n - 1$ y genera a $\mathcal{C}$. Existe por tanto una correspondencia biunívoca entre los códigos cíclicos distintos de cero y los divisores de $x^n - 1$ distintos de $x^n - 1$. Para extender dicha correspondencia entre todos los códigos cíclicos en $\mathcal{R}_n$ y todos los divisores mónicos de $x^n - 1$ definimos como polinomio generador del código cíclico $\{\mathbf{0}\}$ el polinomio $x^n - 1$. Esta correspondencia biyectiva nos conduce al siguiente corolario.

COROLARIO 2.3.3. *El número de códigos cíclicos en $\mathcal{R}_n$ es 2^m, donde m es el número de clases q-ciclotómicas módulo n. Es más, las dimensiones de los códigos cíclicos en $\mathcal{R}_n$ son todas sumas de tamaños de las clases q-ciclotómicas módulo n.*

Demostración. □

El siguiente resultado nos muestra la relación entre dos polinomios generadores cuando un código es subcódigo de otro.

COROLARIO 2.3.4. *Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ códigos cíclicos sobre $\mathbb{F}_q$ con polinomios generadores $g_1(x)$ y $g_2(x)$, respectivamente. Entonces, $\mathcal{C}_1 \subset \mathcal{C}_2$ si y solo si $g_2(x) \mid g_1(x)$.*

2.3.3 *Codificación y decodificación de códigos cíclicos*

Los códigos cíclicos son más sencillos de decodificar que otros tipos de códigos debido a su estructura adicional. Vamos a ver a continuación tres tipos de codificación de códigos cíclicos. Consideraremos un código cíclico $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ con polinomio generador $g(x)$ de grado $n-k$, por lo que $\mathcal{C}$ tiene dimensión k.

CODIFICACIÓN NO-SISTEMÁTICA Esta forma de codificación está basada en la técnica natural de codificación que describimos en la sección ( ). Sea G la matriz generadora obtenida a partir de los desplazamientos de $g(x)$ descrita en el teorema 2.3.1. Dado el mensaje $\mathbf{m} \in \mathbb{F}_q^k$, lo codificamos como la palabra codificada $\mathbf{c} = \mathbf{m}G$. De igual forma, si $m(x)$ y $c(x)$ son los polinomios en $\mathbb{F}_q[x]$ asociados a $\mathbf{m}$ y $\mathbf{c}$, entonces $c(x) = m(x)g(x)$.

CODIFICACIÓN SISTEMÁTICA En este método, dado un mensaje

CODIFICACIÓN SISTEMÁTICA USANDO EL CÓDIGO DUAL

EJEMPLO 2.3.5. Sea $\mathcal{C}$ un código cíclico de longitud 15 con polinomio generador $g(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$. Vamos a ver su codificación con los tres métodos descritos.

2.4 ALGORITMO DE PETERSON-GORENSTEIN-ZIERLER

BIBLIOGRAFÍA

Dyson, G. (2015). *La catedral de Turing: los orígenes del universo digital*. OCLC: 904326706. Barcelona: Debate.

Cohn, P. M. (1982). *Algebra* (2nd ed.). New York: Wiley.

Cohn, P. M. (1989). *Algebra Vol. 2* (2nd ed., reprint with corr.). OCLC: 832519027. New York: Wiley.

Huffman, W. C. & Pless, V. (2003). *Fundamentals of error-correcting codes*. doi:10.1017/CBO9780511807077

Podestá, R. (2006). *Introducción a la Teoría de Códigos Autocorrectores*. Universidad Nacional de Córdoba. Recuperado desde https://www.famaf.unc.edu.ar/documents/940/CMat35-3.pdf