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

[23 de diciembre de 2019 a las 13:37 – 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.

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

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

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

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* $\mathrm{wt}(\mathbf{x})$ de un vector $\mathbf{x}$ es el número de coordenadas distintas de cero de $\mathbf{x}$.

TEOREMA 2.1.12. *Si* $\mathbf{x},\mathbf{y}\in\mathbb{F}_q^n$, *entonces* $\mathrm{d}(\mathbf{x},\mathbf{y})=\mathrm{wt}(\mathbf{x}-\mathbf{y})$. *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* $A_1(\mathcal{C}) = A_2(\mathcal{C}) = \cdots = A_{d-1}(\mathcal{C}) = 0$.

2.2 CÓDIGOS CÍCLICOS

2.3 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