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

[1 de noviembre de 2019 a las 19:11 – 1.0]

Presentado por

José María Martín Luque

Tutorizado por

Gabriel Navarro Garulo

Curso académico 2019–2020

ÍNDICE GENERAL

RESUMEN

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

SUMMARY

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit

blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

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

I

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).

1.1 MONOIDES

Definición 1.1.1. Un *monoide* es un conjunto S con un elemento e y una aplicación $\mu : S^2 \to S$ tal que si $\mu(x, y)$ es el resultado de aplicar μ a la pareja de elementos $x, y \in S$, se verifican:

1. $\mu(x, \mu(y, z)) = \mu(\mu(x, y), z)$ para todo $x, y, z \in S$.
2. $\mu(e, x) = \mu(x, e) = x$ para todo $x \in S$.

Obsérvese que, por definición, un monoide siempre tiene al menos un elemento. A la aplicación μ que actúa sobre parejas de elementos se le llama *operación binaria* y al elemento e, elemento neutro de μ.

1.2 ANILLOS

Definición 1.2.1. Un *anillo*.

2

FUNDAMENTOS DE TEORÍA DE CÓDIGOS

La teoría de códigos tal y cual. Las definiciones aquí ... según 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

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

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. 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 2.1.6. *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 nos conduce

TEOREMA 2.1.7. *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 $\mathcal{C}$.*

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