II Encuentro Matemático del Caribe

Universidad Tecnológica de Bolívar & Universidad del Sinú Seccional Cartagena

Septiembre 09 - 12, 2020, Cartagena de Indias - Colombia

Decodificación mediante el uso de líderes de clase en códigos lineales binarios

Tipo: ponencia

John H. Castillo.* Lisbeth Delgado.**

Resumen

Palabras & frases claves: Código lineal, líderes de clase, algoritmo.

1. Introducción

Un $[n, k]$ código lineal binario es k-subespacio de $\mathbb{F}_2^n$. Un elemento de un código lineal se denomina una palabra código. La distancia de Hamming, $d_H(\mathbf{x}, \mathbf{y})$, entre dos vectores $\mathbf{x} = (x_1 \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ es el número de entradas en las que difieren, equivalentemente ,

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|.$$

Para $\mathbf{x} \in \mathbb{F}_2^n$, el peso de Hamming de $\mathbf{x}$ se define como $w_H(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0})$. La distancia mínima $d(C) = d$ de un código lineal se define como el peso mínimo entre todas las palabras código no nulas, en este caso se denomina un $[n, k, d]$ código lineal binario. Una matriz generadora para un $[n, k]$ código C es una matriz G de tamaño $k \times n$, cuyas filas forman una base para C. Entonces el código C puede ser visto como

$$C = \{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_2^k\}. \tag{1}$$

*Universidad de Nariño, San Juan de Pasto, Colombia, e-mail: jhcastillo@udenar.edu.co

**Universidad del Cauca, Popayán, Colombia, e-mail: lddelgado@unicauca.edu.co

Para un $[n, k]$-código lineal binario, el proceso de decodificación consiste en construir una tabla con 2^{n-k} entradas en lugar de una de 2^n entradas (todas las palabras de $\mathbb{F}_2^n$). Se debe tener en cuenta que con este proceso las distintas clases laterales del código forman una partición de $\mathbb{F}_2^n$ en 2^{n-k} conjuntos de tamaño 2^k. Para la construcción de esta tabla, se busca una matriz H de control de paridad del código $\mathcal{C}$, la cual es una matriz generadora para el código dual de $\mathcal{C}$. Entonces para un vector $y \in \mathbb{F}_2^n$ su síndrome se define como $(y) = Hy^T \in \mathbb{F}_2^{n-k}$. Cuando el síndrome de la palabra es 0 el vector $y \in \mathcal{C}$, esto proporciona una forma de detectar si una palabra pertenece o no al código. Es más se puede demostrar que existe una correspondencia uno a uno entre las clases laterales de $\mathcal{C}$ y los valores de los síndromes. Sea v una palabra transmitida y sea w la palabra recibida, de esto resulta un patrón de error e tal que $e = w - v \in w + \mathcal{C}$. Entonces $w - e = v \in \mathcal{C}$, así el patrón de error e y la palabra recibida w están en la misma clase lateral del código $\mathcal{C}$.

El procedimiento de decodificación por distancia mínima de una palabra en un código lineal $\mathcal{C}$ se realiza de la siguiente manera. Se recibe la palabra w, se elige una palabra e de menor peso en la clase lateral $w + \mathcal{C}$ y se concluye que $v = w - e$ es la palabra transmitida. Para esto es necesario construir la tabla que se mencionó anteriormente, la cual se conoce como arreglo estándar o arreglo Slepiano, y en el que se requiere encontrar los líderes de clases laterales. Se resalta que el único líder de clase que pertenece al código C es el vector cero. En general, toda clase lateral de peso a lo más $t = \lfloor (d-1)/2 \rfloor$ tiene un único líder.

De esta forma, para llevar acabo este proceso de decodificación, para un código lineal binario dado, es necesario construir algoritmos que permitan el cálculo del conjunto de líderes de clase de forma eficiente. Este problema ya ha sido ampliamente estudiado; recientemente en el artículo "Computing coset leaders and leader codewords of binary codes"[1]. En este artículo los autores presentan una forma de adaptar las ideas presentadas en [4, Section 11.7] para determinar la distribución de pesos del conjunto de líderes de clase, el radio de Newton y el radio de cubrimiento, parámetros considerados entre los más importantes y estudiados para un código lineal, ver [3, Chap. 1, Sec. 5].

En esta ponencia presentamos los conceptos matemáticos necesarios para implementar algoritmos en `SageMath` [5] para decodificar palabras recibidas en un código lineal mediante el uso del arreglo estándar.

Agradecimiento

Este trabajo es parcialmente financiado por *Vicerrectoría de Investigaciones e Interacción Social* de la Universidad de Nariño.

Referencias

[1] Borges-Quintana, M., Borges-Trenard, M. A., Márquez-Corbella, I. and Martínez-Moro, E. Computing coset leaders and leader codewords of binary codes *Journal of Algebra and its Applications*, 2015. DOI: 10.1142/S0219498815501285.

[2] Ling, S. and Xing, C. *Coding Theory: A First Course*. Cambridge University Press, Cambridge, 2004.

[3] MacWilliams, F. J. and Sloane, N. J. A. *The Theory of Error-Correcting Codes*, 1977.

[4] Pless, V. and Huffman, W. C. *Fundamentals of error-correcting codes*. Cambridge University Press, New York, 2003.

[5] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 9.0), 2020, https://www.sagemath.org.