PO-06 APLICACIONES A LA TEORÍA DE CÓDIGOS

Adriana Alexandra Albarracín Mantilla
Magister en Matemáticas, docente Escuela de Matemáticas
Universidad Industrial de Santander
adrialba@matematicas.uis.edu.co

RESUMEN

En esta charla se aplicará el tema de espacios vectoriales a la teoría de la codificación, examinando las formas de codificar un mensaje y decodificarlo después de que el ruido lo ha distorsionado. Posteriormente se ilustrará con algunos ejemplos.

Palabras Claves.Teoría de códigos, espacios vectoriales.

ABSTRACT

In this talk we present some applications of vector spaces theory to the Coding Theory. We exhibit many ways of coding and decoding information for the reliable transmission over a noisy chanel. Some examples are given.

Key Words. Coding theory, vector spaces.

Introducción

La Teoría de códigos nace en 1948 y su aplicación inmediata consiste en la detección y corrección de errores de un mensaje que ha sido transmitido a través de un canal interferido por el ruido.

El inicio de la Teoría de Códigos se da con la publicación del artículo A Mathematical Theory of Comunication en Bell Systems Technical Journal, de C.E Shannon, posteriormente aparecen los trabajos de Richard Hamming y Maral Golay en los cuales muestran métodos de detección y corrección de errores de un mensaje que ha sido transmitido a través de un canal interferido por el ruido.

Más adelante, en 1982, M.A Tsfasman S.G, Vladut y Th. Zink construyen una familia de códigos buenos, con los cuales se obtiene la solución al problema fundamental de la teoría de códigos en términos probabilísticos.

Dado que los mensajes transmitidos desde la voz humana hasta los datos recibidos de un satélite en general son vulnerables al ruido, se busca preservar la información que es transmitida, a través de un canal discreto y sin memoria que es afectado por el ruido, para ello, se considera la información presentada como una secuencia larga de símbolos pertenecientes a un conjunto finito cualquiera llamado alfabeto.

El proceso de codificación más conocido es el de codificación por bloques que consiste en dividir la información por bloques de *k* símbolos que se conocen como símbolos de información. El proceso de codificación se realiza agregando una cierta cantidad de símbolos extras, llamados símbolos

redundantes, que convierten el bloque inicial de *k* símbolos en un bloque de *n* símbolos, esto debe responder a un método estructurado que permita detectar, y corregir los errores presentados. Si el receptor del mensaje conoce la técnica con la cual se codifica, puede verificar si hubo cambios durante la transmisión del mensaje inicial. En el proceso de decodificación, se pueden recuperar los primeros *k* símbolos de información aunque al receptor le haya llegado una n-upla.

El código que detecta errores, recibe el nombre de corrección de error.

Supongamos que se desea enviar el mensaje 1011. Para codificar 1011, se agrega una cola binaria y así, si 1011 se codifica 10111 y se distorsionara a 00111, se detecta que hubo un error pues no hay una cantidad par de unos, a esta clave o código de detección de error se le llama comprobación de paridad.

Si 1011 se codifica como 10111011 y se recibe 00111011, podemos verificar que se han cometido dos errores si hubiese ocurrido un error, estaría en la posición 1. Este esquema de codificado no es eficiente.

Códigos Lineales

Sea F_q el campo con q elementos. Se dice que *C* es un código lineal sobre el alfabeto F_q si es un subespacio lineal de F_q^n. Los elementos de *C* reciben el nombre de palabras código, *n* denota la longitud del código y *k* la dimensión de *C* como espacio vectorial sobre F_q. Así el código *C* sobre F_q es un *[n,k]* código q-ario.

2.1 Definición: Una matriz generadora *G* de un *[n,k]* código q-ario, es una matriz $k \times n$, donde las filas conforman una base para C.

Si *G* es una matriz generadora de *C* entonces $C = \{uG : u \in F_q^{\,k}\}$.

2.2 Definición: Dos códigos son equivalentes si sus matrices generadoras son equivalentes.

2.3 Definición: La distancia de Hamming sobre F_q^n es la función *h* definida por

$h(a,b) = |\{i : a_i \neq b_i\}|$, para $a = (a_1, a_2, .., a_n)$ y $b = (b_1, b_2, ..., b_n) \in F_q^{\,n}$.(1)

2.4 Definición: La distancia mínima *d* de un código lineal $C \neq 0$ está dada por

$d := mín\{h(a,b) : a,b \in C, a \neq b\}$, (2)

Un *[n, k]* código q-ario con distancia mínima se denota por *[n,k,d]* -código q-ario. Los valores *n, k* y *d*, se conocen como parámetros fundamentales de un código lineal. El parámetro *d* determina la capacidad de un código para detectar y corregir errores, como lo establece el siguiente resultado:

2.5 Teorema: Un *[n,k,d]* código q-ario puede:

1. Detectar a lo sumo *d-1* errores.

2. Corregir a lo sumo $\left[\left|\frac{d-1}{2}\right|\right]$ errores.

Códigos de Hamming

Estos códigos corrigen errores únicos, y fueron encontrados por Marce Golay y Richard Hamming, en la década de los cincuenta.

Para cada *r> 0*, el código de Hamming q-ario $H_q(r)$ es un *[n, n-r, 3]* código q-ario con $n = \frac{q^r - 1}{q - 1}$.

Note que *r=n-k*, representa el número de símbolos de control de paridad del código. Su construcción se hace especificando una matriz de control de paridad *H* y puesto que la distancia mínima es *3*, se puede probar que cualquier par de columnas de *H*, deben ser linealmente independientes.

Los códigos que alcanzan la igualdad *k+d=n+1* son óptimos en cuanto a capacidad correctora y se conocen como códigos *MDS*(Códigos de Máxima Distancia Separable).

El problema fundamental de la teoría de códigos es encontrar la mayor cantidad de palabras código que pueda tener un código, dado *n* y *d.*

Ejercicios de Aplicación

1. Codifique el mensaje ATTACK NOW, utilizando la matriz invertible $M = \begin{bmatrix} -3 & 4 \\ -1 & 2 \end{bmatrix}$.

2. Sean $F_q=Z_2$ y $H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$ sobre Z_2, la matriz de comprobación de paridad para el código N_H (espacio nulo de *H*). Encuentre la matriz generadora del código de Hamming.

3. Si se reciben los mensajes *1010101* y *1100111* codificados con Hamming y se supone que a lo más existe un error en cada transmisión, determine los mensajes originales.

4. Sea $g(x) = \min(\alpha, F_2) = x^3 + x + 1$ con $\alpha \in F_2^{\,3}$.Determine la matriz de control de paridad para $H_2^{\,3}$.

Referencias bibliográficas

H. Stichtenoth (1993). Algebraic Function Fields and Codes, Berlin: Springer-Verlag.

Nakos, G., & Joiner D. (1991). Álgebra Lineal con Aplicaciones, México: Thomson.

Vera P., (1982). Introduction to the theory of error correcting codes, New York: Wiley.

Wesley P. (1961). Error correcting codes, Cambridge: MIT Press.