Algunas conexiones entre códigos lineales binarios y grafos

John H. Castillo
jhcastillo@udenar.edu.co
Universidad de Nariño, San Juan de Pasto, Colombia

Seminario MAPI Online
Mayo 2021

Un $[n, k]$ código lineal binario es un 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 $C = \{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_2^k\}$.

Un grafo finito G con n vértices es una pareja (V, E) donde $V = \{1, \ldots, n\}$ es el conjunto de vértices y $E \subseteq V \times V$ es el conjunto de aristas. Si $(i, j) \in E$ o $(j, i) \in E$ se dice que i y j son vecinos. La matriz de adyacencia $A_G = (a_{ij})$ es una matriz de tamaño $n \times n$ simétrica tal que $a_{ij} = 1$ si $i \in N(j)$ y $a_{ij} = 0$ en caso contrario.

En esta charla presentaremos algunas conexiones que existen entre la teoría de códigos y la teoría de grafos.