
SEMINARIO

Rodrigo San-José

Universidad de Valladolid

Pesos de Hamming generalizados de códigos decrecientes

Abstract:

Los pesos de Hamming generalizados (GHWs) de un código lineal son una generalización de la distancia mínima que tiene múltiples aplicaciones en criptografía y códigos cuánticos. Por ejemplo, determinan la cantidad de información que puede ser extraída cuando usamos el código en un canal intervenido de tipo II (wire-tap channel of type II), tienen aplicaciones en funciones t-resilientes y pueden usarse para obtener mejores cotas en el tamaño de la lista en algoritmos de decodificación en lista. Los pesos de Hamming generalizados relativos (RGHWs), estrechamente relacionados con los GHWs, determinan la seguridad de los esquemas de compartición de secretos lineales y la capacidad correctora de códigos cuánticos. Esto ha motivado varios trabajos recientes sobre los GHWs y RGHWs de familias clásicas de códigos.

La cota de la huella permite acotar el número de puntos racionales de una variedad en términos de la huella del ideal que la define. En esta charla, revisaremos cómo se puede utilizar la cota de la huella para derivar los GHWs de los códigos cartesianos decrecientes, y luego veremos cómo mejorar esta cota en el caso de los códigos norma-traza decrecientes. Esta cota mejorada es ajustada, es decir, proporciona los GHWs de los códigos norma-traza decrecientes y, en particular, da los GHWs de los códigos hermíticos. También veremos cómo utilizar estos resultados para construir códigos cuánticos impuros con parámetros excelentes.

Este es un trabajo conjunto con Eduardo Camps-Moreno, Hiram H. López y Gretchen L. Matthews.

Seminario IMUVA, Edificio LUCIA
7 de Marzo de 2025 (12:00)
Organiza: GIR SINGACOM

