V Encuentro Conjunto de la Real Sociedad Matemática Española (RSME) y la Sociedad Matemática Mexicana (SMM)

14-18 de junio de 2021

Centro de Investigación en Matemáticas (CIMAT), Guanajuato, México (virtual)
https://rsmeysmm.eventos.cimat.mx/node/1409

Programa de la Sesión Especial

Teoría Algebraica de Códigos

Conferenciantes: María Bras Amoro (URV), Eduardo Campos Moreno (IPN) , Elías García Claro (UAM) , Delio Jaramillo-Velez (CINVESTAV), Irene Márquez Corbella (ULL), Juan Jacobo Simón Pinero (UM), Rafael Villareal Rodríguez (CINVESTAV).

Organizadores: Edgar Martínez-Moro (UVA) y Yuriko Pitones Amaro (CIMAT)

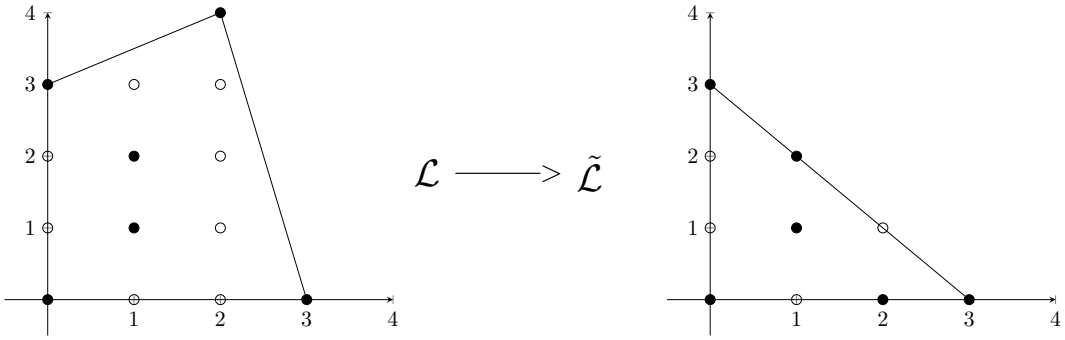

Figura: Dr. Rafael Heraclio Villarreal, Códigos de Evaluación

Programa (Jueves, 17 de junio de 2021)

- 12:00-13:00 (GTM-5) / 19:00-20:00 (GTM +2):
  - Dr. Rafael Heraclio Villarreal: *Códigos de Evaluación*.

- 13:00-14:00 (GTM-5) / 20:00-21:00 (GTM +2):

  Preguntas y discusión sobre las conferencias grabadas:
  - Dra. María Bras Amorós : *The Isometry-Dual Property for one-point andtwo-point AG Codes*.
  - M.C. Eduardo Campos : *Introducción a códigos polares*.
  - Dr. Elías García Claro: *Sobre códigos de grupo de dimensión fácilmente calculable y MDS*.
  - M.C. Delio Jaramillo-Velez: *Pesos generalizados de Hamming de ciertos códigos de tipo Reed-Muller*.
  - Dra. Irene Márquez Corbella: *Códigos afines con gran dimensión cuyo cuadrado tiene una distancia mínima designada*.
  - Dr. Juan Jacobo Simón Pinero: *El Algoritmo de Berlekamp-Massey-Sakata*.

Títulos y resúmenes

- Dra. María Bras Amorós (Universidad de Rovira i Virgili)
  Título: *The Isometry-Dual Property for one-point andtwo-point AG Codes*.
  Resumen: A flag of codes $C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_s \subseteq \mathbb{F}_{q^n}$ is said to satisfy the *isometry-dual property* if there exists $\mathbf{x} \in (\mathbb{F}_q^*)^n$ such that the code C_i is $\mathbf{x}$-isometric to the dual code $C_{s-i}^{\perp}$ for all $i = 0, \ldots, s$. For P and Q rational places in a function field $\mathcal{F}$, we investigate the existence of isometry-dual flags of codes in the families of two-point algebraic geometry codes

  $$C_{\mathcal{L}}(D, a_0P + bQ) \subsetneq C_{\mathcal{L}}(D, a_1P + bQ) \subsetneq \cdots \subsetneq C_{\mathcal{L}}(D, a_sP + bQ),$$

  where the divisor D is the sum of pairwise different rational places of $\mathcal{F}$ and P, Q are not in $supp(D)$. We characterize those sequences in terms of b for general function fields. We then apply the result to the broad class of Kummer extensions $\mathcal{F}$ defined by affine equations of the form $y^m = f(x)$, for $f(x)$ a separable polynomial of degree r, where $\gcd(r, m) = 1$.

  Work joint to Alonso S. Castellanos and Luciane Quoos.

- M. C. Eduardo Campos (Escuela Superior de Física y Matemáticas del IPN)
  Título: *Introducción a códigos polares*.
  Resumen: El problema de codificación de canal consiste en buscar esquemas para transmitir información a través de un medio ruidoso y detectar y corregir posibles errores introducidos por él. Shannon probó que estos esquemas existen pero su demostración no sugiere una forma de construirlos. Los códigos polares son la primera herramienta teórica que nos garantiza la construcción de un esquema que satisface las condiciones del teorema de Shannon sobre ciertos canales. En esta plática, introduciremos los conceptos básicos de teoría de la información y de teoría de códigos para comprender el enunciado del teorema de Shannon y los códigos polares como ejemplo de un código que lo satisface.

- Dr. Elías García Claro (Universidad Autónoma Metropolitana- Iztapalapa)
  Título: *Sobre códigos de grupo de dimensión fácilmente calculable y MDS*.
  Resumen: Un código de grupo es un ideal de un álgebra de un grupo finito sobre un campo finito (con estructura de espacio métrico con la métrica de Hamming). Si un código de grupo está generado por un idempotente y su dimensión es menor o igual a la característica del campo sobre el que está definido, se dice que este es de dimensión fácilmente calculable, o ECD (easily computable dimension) por sus siglas en Inglés. La cota de Singleton establece que si existe un $[n, k, d]$-código lineal, d es menor o igual a $n - k + 1$. Aquellos códigos que alcanzan dicha cota son llamados códigos MDS. La conjetura-MDS establece que los códigos MDS tienen longitud acotada superiormente por términos del tamaño del campo. Durante la presentación se introducirán los códigos ECD, y se presentará una relación que existe entre estos y los códigos MDS.

- M.C. Delio Jaramillo-Velez (CINVESTAV)
  Título: *Pesos generalizados de Hamming de ciertos códigos de tipo Reed-Muller*.
  Resumen: Mostraremos como obtener los pesos generalizados de cierta familia de códigos de tipo Reed-Muller a partir de la fórmula de los pesos generalizados de códigos afines cartesianos, dada por P. Beelen y M. Datta en 2018. Finalmente dado un conjunto proyectivo determinamos los pesos generalizados de códigos de tipo Veronese y de sus códigos duales en términos de los pesos generalizados de su correspondiente códigos de tipo Reed-Muller proyectivo.

- Dra. Irene Márquez Corbella (Universidad de la Laguna)
  Título: *Códigos afines con gran dimensión cuyo cuadrado tiene una distancia mínima designada*.
  Resumen: Dado un código lineal $\mathcal{C}$ se define como su cuadrado $\mathcal{C}^2$ al código generado por los productos componente a componente de dos elementos de $\mathcal{C}$. Nuestro objetivo en esta charla es responder a la siguiente pregunta: ¿qué familia de códigos afines verifican a la vez que $\mathcal{C}$ tiene una dimensión alta mientras que $\mathcal{C}^2$ tiene una distancia mínima designada? El método que vamos a proponer recibe como entrada un entero positivo d y construye un código $\mathcal{C}$ tal que la distancia mínima de C^2 sea mayor o igual que d y la dimensión de $\mathcal{C}$ sea mayor que la correspondiente familia de códigos Reed-Muller pesados que satisfacen la primera condición.

  Trabajo conjunto con Ignacio García Marco y Diego Ruano.

- Dr. Juan Jacobo Simón Pinero (Universidad de Murcia)
  Título: *El Algoritmo de Berlekamp-Massey-Sakata*.
  Resumen: Resumen: El algoritmo de Berlekamp-Massey-Sakata (aBMS) es una generalización a dos variables del algoritmo de Berlekamp-Massey que consiste en, dada una sucesión periódica en un cuerpo finito, encontrar la fórmula de recurrencia y el polinomio que la generan. En el caso de dos variables, consiste en encontrar una base de Gröebner para determinar el sistema de recurrencias lineales.

  Existen muchos métodos de descodificación basados en este algoritmo; entre otros, la descodificación por localizador que se aplica en códigos abelianos y algebraicogeométricos.

  En esta plática, vamos a mostrar un panorama sobre su funcionamiento y comentaremos algunas de nuestras aportaciones en un trabajo conjunto con José Joaquín Bernal. Entre otras, cabe mencionar la siguiente: para una tabla de orden (o bien, doblemente periódica) $r_1 \times r_2$, obtenida por una fórmula polinomial (por síndromes) que tiene $t \leq \min\{\lfloor \frac{r_1}{2} \rfloor, \lfloor \frac{r_2}{2} \rfloor\}$ términos, existe un conjunto mínimo de índices sobre el que basta ejecutar el algoritmo para obtener la base de Gröebner, garantizando que el proceso terminará en, a lo más, $\frac{t^2+7t}{2} - 1$ pasos.

- Dr. Rafael Heraclio Villarreal (Centro de Estudios Avanzados del Instituto Politécnico Nacional)
  Título: *Códigos de Evaluación*.
  Resumen: Introduciremos los códigos de evaluación estándar y presentaremos un teorema de dualidad que relaciona códigos de tipo Reed-Muller con sus duales.

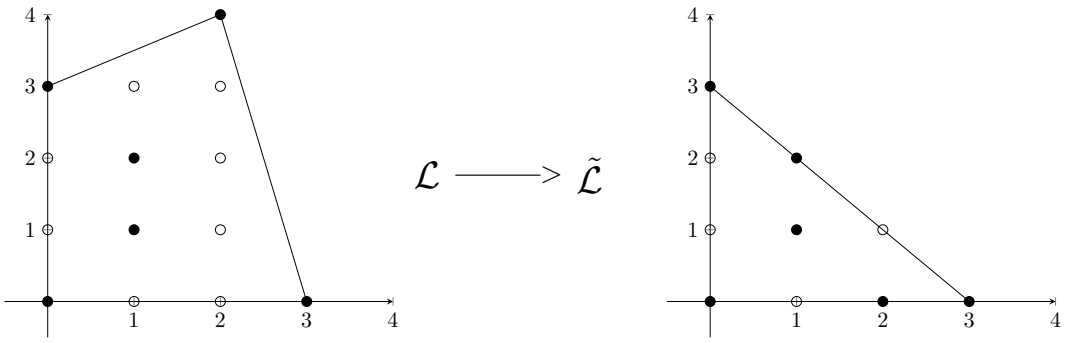

Figure 1: Puntos enteros que definen un código de evaluación $\mathcal{L}_X$ y los puntos que definen su código estándar $\widetilde{\mathcal{L}}_X$.