

# CURSO DE POSGRADO: TEORÍA DE CÓDIGOS SOBRE CUERPOS Y ANILLOS

RICARDO PODESTÁ

*Primer Cuatrimestre de 2011*

La siguiente es una propuesta de curso de posgrado de 60 horas del Doctorado en Matemática.

## REQUISITOS

Se requiere un cierto manejo de álgebra y aritmética en general, cubiertos por las materias: Álgebra I, Álgebra II y Estructuras Algebraicas de la Licenciatura en Matemática (espacios vectoriales, algebra lineal, congruencias, polinomios, cocientes de polinomios, anillos, cuerpos, ideales, morfismos).

El curso está pensado en 3 bloques y está basado en los libros de Huffman-Pless (Capítulos 1, 2, 3, 4, 5, 6, 7, 12 y 13) y Roman (Capítulos 4, 5, 6, 7, 8).

## PROGRAMA TENTATIVO

Entre corchetes los temas adicionales en caso de haber tiempo.

### Parte 1. Conceptos básicos.

*Capítulo 1: Generalidades de códigos.* Códigos y sus parámetros. Pesos y distancias. Tipos de códigos. Ejemplos: códigos triviales, de repetición, de peso par, de suma par, ISBN, EAN-13. Objetivos de la teoría. Codificación y decodificación. Detección y corrección de errores. Construcciones de códigos a partir de otros dados. Equivalencia de códigos. Grupo de Automorfismos. Cotas básicas: Singleton, Hamming, Gilbert-Varshamov, Griesmer. Códigos perfectos y de máxima distancia de separación (MDS).

*Capítulo 2: Códigos lineales.* Códigos lineales. Matrices generadora y de paridad. Códigos duales y autoduales. Decodificación por síndrome. Familias de códigos: de Hamming, simplex, de Golay binarios y ternarios, de Reed-Muller (binarios). El algebra de grupo  $\mathbb{C}[\mathbb{F}_q]$  y caracteres. Enumeradores de peso e identidades de MacWilliams. Polinomios de Krawtchouk. [Códigos no lineales: Kerdock, Preparata, Nordstrom-Robinson, Goethals.]

*Capítulo 3: Cuerpos finitos.* Extensiones de cuerpos. Los cuerpos finitos  $\mathbb{F}_q$ . Subcuerpos. El grupo multiplicativo  $\mathbb{F}_q^*$ . Elementos primitivos. Construcciones de cuerpos finitos. Automorfismo de Frobenius y traza. Códigos de traza y de restricción. Teorema de Delsarte.

### Parte 2. Conceptos intermedios.

*Capítulo 4: Polinomios sobre cuerpos finitos.* Polinomios irreducibles sobre  $\mathbb{F}_q$ . El cuerpo de descomposición de un polinomio. Polinomios minimales. El número de polinomios irreducibles sobre  $\mathbb{F}_q$ . El orden de un polinomio. Raíces de la unidad sobre  $\mathbb{F}_q$ . Factorización de  $x^n - 1$  sobre  $\mathbb{F}_q$ . Conjuntos ciclotómicos. Polinomios ciclotómicos  $\Phi_n(x)$  y propiedades. Criterio de irreducibilidad de  $\Phi_n(x)$  sobre  $\mathbb{F}_q$ .

*Capítulo 5: Códigos cíclicos.* Definición y generalizaciones. Códigos cíclicos como ideales de polinomios. Polinomio generador y de control de paridad. Duales. Códigos de Hamming y de Golay como cíclicos, criterios. Generador idempotente de un código cíclico. Códigos cíclicos primitivos. Multiplicadores. Códigos cíclicos definidos por raíces de la unidad. Distancia mínima: polinomios de Mattson-Solomon y cota de BCH. Métodos de codificación. Decodificación de Meggit. Códigos afinmente invariantes.

*Capítulo 6. Familias de códigos cíclicos.* Códigos de Bose-Chadhuri-Hoquenhem (BCH). Códigos BCH primitivos y BCH “*narrow-sense*”. Códigos BCH binarios. Decodificación de códigos BCH (algoritmos de Peterson-Gorenstein-Zierler, Berlekamp-Massey, Sugiyama y Sudan-Guruswami). Polinomio localizador de errores y las “*key-equations*”. Códigos de Reed-Solomon (RS). [Códigos duádicos.] Códigos de residuos cuadráticos (QR).

### Parte 3: Conceptos avanzados.

*Capítulo 7. Códigos cíclicos generalizados y códigos geométricos.* Códigos de evaluación. Códigos RS y BCH como códigos de evaluación. Códigos alternantes y de Goppa clásicos. Códigos de Reed-Solomon generalizados (GRS). Códigos vía residuos. Códigos de Reed-Muller generalizados (GRM). Espacio afín  $\mathbb{A}^n(\mathbb{F}_q)$  y proyectivo  $\mathbb{P}^n(\mathbb{F}_q)$ . Curvas algebraicas. Códigos sobre curvas. [Códigos de Goppa, geométricos y generalizaciones.]

*Capítulo 8: Códigos sobre anillos.* Códigos  $\mathbb{Z}_4$ -lineales. Mapa de Gray. Pesos de Lee, de Hamming y Euclideo y distancias asociadas. Enumeradores de pesos asociados. Enumeradores de peso generalizados. Códigos binarios a partir de códigos lineales sobre  $\mathbb{Z}_4$ . Códigos cíclicos sobre  $\mathbb{Z}_4$ . Factorización de  $x^n - 1$  sobre  $\mathbb{Z}_4$ . Lemma de Hensel. El paper de Hammons-Kumar-Calderbank-Sloane-Solé y la relación entre los códigos Kerdock-Preparata. Anillos de Galois. Códigos sobre anillos de Galois.

### REFERENCIAS

Seguiremos los siguientes libros:

- W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, 2003.
- S. Roman, *Coding and Information Theory*, 1992.

Otras fuentes de referencia

- R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, 1994.
- J. H. van Lint, *Introduction to Coding Theory*, 1982.
- W. C. Huffman, V. Pless (editores), *Handbook of coding theory I y II*, 1998.
- S. A. Stepanov, *Codes on Algebraic Curves*, 1999.
- M. Tsfasman, S. Vladut, D. Nogin, *Algebraic Geometric Codes*, 2007.
- Zhe-Xian Wan, *Lectures on finite fields and Galois rings*, 2003.