EXP-UNC: 0061383/2018

TÍTULO: Teoría de códigos algebraicos		
AÑO: 2019	**CUATRIMESTRE:** primero	**N° DE CRÉDITOS:** 3
CARGA HORARIA: 65 horas.		
CARRERA/S: Doctorado en Matemática		

FUNDAMENTOS

La Teoría de Códigos es parte de la Teoría de la Información inaugurada por Claude Shannon en 1948. Al enviar mensajes por canales de transmisión, siempre existen errores debidos a ruidos, interferencias, etc. Además del diseño de canales con buenas propiedades de transmisión, que es tarea de los ingenieros, se pretende minimizar los errores a partir del diseño de buenos códigos. El objetivo básico de la teoría es que el código utilizado para codificar el mensaje original pueda ser capaz de detectar y corregir la mayor cantidad de errores posibles. El diseño y estudio de dichos códigos es el área de la teoría de códigos autocorrectores. El estudio de familias de códigos con buenos parámetros y algoritmos eficientes de codificación y decodificación son parte central de la teoría.

La teoría se basa en técnicas de álgebra lineal sobre cuerpos finitos para los códigos lineales. Para los códigos cíclicos se utilizan polinomios, ciclotomía, teoria de cuerpos. Existen muchas conexiones con objetos combinatorios como diseños, arreglos, grafos regulares, esquemas de asociación, geometrías finitas, etc. Códigos más avanzados utilizan anillos finitos en lugar de cuerpos finitos. Existen también mucha interrelación con la teoría de números (códigos residuos cuadráticos, uso de curvas elípticas para determinación de espectros, relación entre lattices y códigos y las formas modulares asociadas..) Todo esto forma parte de la teoría algebraica de códigos, en contrapartida con la teoría de los códigos geométricos que utilizan curvas algebraicas para definir los códigos y que no será tratado aquí.

OBJETIVOS

Los objetivos generales del curso son:
- Introducir al alumno a la teoría de códigos.
- Mostrar la conexión con otras áreas (combinatoria, álgebra conmutativa, teoría de números)
- Que el alumno aprenda a trabajar con cuerpos finitos, sus construcciones y propiedades, y la de los polinomios irreducibles sobre cuerpos finitos. Aprender a trabajar con conjuntos y polinomios ciclotómicos.
- Que el alumno se familiarice con las familias de códigos más importantes y reconozca sus propiedades más salientes. Por ejemplo: 1) Lineales (Hamming, Golay, Reed-Muller), 2) Cíclicos (BCH, Reed-Solomon, QR), 3) códigos más generales (Goppa, alternantes, sobre anillos).
- Identificar códigos con propiedades especiales como códigos MDS, códigos perfectos, códigos autoduales.
- Que el alumno conozca los resultados más importantes de la teoría como el Teorema de Delsarte, Identidades de MacWilliams, Teorema de Gleason, etc.

EXP-UNC: 0061383/2018

PROGRAMA

Unidad 1: CÓDIGOS LINEALES

CAPÍTULO 1: GENERALIDADES DE CÓDIGOS. Códigos lineales y no lineales. Parámetros principales y relativos. Longitud, dimensión, distancia, pesos. Cotas. Ejemplos. Operaciones y construcciones. Codificacion y decodificacion. Equivalencias de códigos.

CAPÍTULO 2: CÓDIGOS LINEALES. Matrices generadoras y de paridad. Códigos duales. Cotas (Singleton, Hamming, Gilbert-Varshamov, Griesmer). Códigos de Hamming y de Golay. Códigos de Reed-Muller. Códigos especiales (autoduales, MDS; perfectos). [Decodificacion por síndrome].

CAPÍTULO 3: ESPECTRO DE CÓDIGOS LINEALES. Pesos, distribución y espectro. Caracteres. Polinomios enumeradores de peso. Identidades de MacWilliams. Polinomios de Krawtchouk.

Unidad 2: CUERPOS FINITOS Y POLINOMIOS

CAPÍTULO 4: CUERPOS FINITOS. Extensiones de cuerpos. Cuerpos finitos. Caracterización. Subcuerpos. Grupo multiplicativo. Clausura algebraica. Automorfismo de Frobenius. Funciones norma y traza. Teorema restricción/dualidad/traza de Delsarte.

CAPÍTULO 5: POLINOMIOS SOBRE CUERPOS FINITOS Y CICLOTOMÍA. Polinomios irreducibles y minimales. Número de polinomios irreducibles. Orden de un polinomio. Raíces de la unidad sobre Fq. Conjuntos ciclotómicos. Factorización de x^n-1 sobre Fq. Polinomios ciclotómicos. Criterio de irreducibilidad de polinomios ciclotómicos

Unidad 3: CÓDIGOS CÍCLICOS

CAPÍTULO 6: Definición y ejemplos. Códigos cíclicos como ideales de anillos de polinomios. Polinomio generador y de chequeo, duales. Códigos de Hamming y Golay como cíclicos. Ceros de códigos cíclicos. Idempotentes. Códigos cíclicos primitivos, multiplicadores. Cota de BCH para la distancia mínima. Métodos de decodificación (Meggit). Códigos afínmente invariantes.

CAPITULO 7 - FAMILIAS DE CÓDIGOS CÍCLICOS

Códigos BCH primitivos. Códigos BCH en sentido estrecho.Códigos BCH binarios. Códigos Decodificación de BCH's (algoritmos de PGZ, BM, S y SG). Códigos de Reed-Solomon (RS). Códigos de residuos cuadráticos (QR). [Códigos de Melas y Zetterberg].

Unidad 4: OTROS CÓDIGOS

CAPITULO 8. OTROS CÓDIGOS. Códigos de evaluación (BCH y RS). Códigos alternantes. Códigos de Goppa clásicos (racionales). Códigos RS generalizados (GRS-codes). Códigos no lineales famosos: Nordstrom-Robinson, Kerdock, Preparata. [Códigos de Goethals]

CAPITULO 9: CÓDIGOS SOBRE ANILLOS. Códigos Z4-lineales. Mapa de Gray. Distancias de Lee, Hamming y Euclídea. Enumeradores de pesos. Códigos binarios a partir de Z4-códigos lineales. Códigos cíclicos sobre Z4. Factorización de x^n-1 sobre Z4, lema de Hensel. [El paper HKCSS'94].

EXP-UNC: 0061383/2018

PRÁCTICAS
Resolución de ejercicios prácticos que serán discutidos entre todos. Entrega de ejercicios resueltos.

BIBLIOGRAFÍA
BIBLIOGRAFIA BASICA [1] W. Cary Huffman, Vera Pless. Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, 2003. [2] F. J. MacWilliams, N. J. A. Sloane. The theory of error-correcting codes I & II. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. [3] Steven Roman. Coding and information theory. Graduate Texts in Mathematics, 134. Springer-Verlag, New York, 1992. BIBLIOGRAFIA COMPLEMENTARIA [4] Peter Cameron, Jacob van Lint. Designs, graphs, codes and their links. London Mathematical Society student texts, Cambridge University, 1996 [5] Wolfgang Ebeling. Lattices and codes: a course partially based on lectures by Hirzebruch. Advanced lectures in mathematics. Vieweg, 2002 [6] Rudolf Lidl, Harald Niederreiter. Introduction do finite fields and their applications. Cambridge University, 1994 [7] Rudolf Lidl, Harald Niederreiter. Finite Fields. Cambridge University, 1997. [8] Gary Mullen, Daniel Panario. Handbook of finite fields [9] Gabriele Nebe, Eric Rains, Neil Sloane. Self-dual codes and invariant theory. Berlin, Springer, 2006.

MODALIDAD DE EVALUACIÓN
REGULARIDAD: Asistencia regular a clase (80%) + entrega de ejercicios resueltos. APROBACION: Proyecto: estudio de un tema y exposición oral del mismo. Examen escrito (podría ser take-home) y examen oral.

REQUERIMIENTOS PARA EL CURSADO
El curso es autocontenido, pero se requiere manejo de álgebra y en menor medida de combinatoria. Contenidos de las materias Álgebra I, II y III y Estructuras algebraicas de Licenciatura en Matemática de la FAMAF.