



Propuesta de Trabajo Fin de Grado en Matemáticas (curso 2021-2022)

Responsable de tutorización: Francisco Javier Lobillo Borrero
Departamento: Álgebra
Correo electrónico: jlobillo@ugr.es

Responsable de cotutorización:
Departamento:
Correo electrónico:

(Rellenar sólo en caso de que la propuesta esté realizada a través de un estudiante)
Estudiante que propone el trabajo: Cristian Pozo González

Título del trabajo: Códigos Goppa

Tipología del trabajo (marcar una o varias de las siguientes casillas):

Materias del grado relacionadas con el trabajo: Álgebra I y III, Geometría I y II, Álgebra Conmutativa Computacional, Teoría de Números y Criptografía.

Descripción y resumen de contenidos:

Introducidos por V. D. Goppa en 1970, son códigos lineales que generalizan algunos BCH en sentido estricto y pueden verse como códigos subcuerpo de algunos códigos de Reed-Solomon Generalizados (GRS). A su vez, son el elemento inicial de otra familia de códigos definidos mediante curvas algebraicas proyectivas. Son a su vez importantes por ser la familia de códigos utilizados en el criptosistema de McEliece.

En este Trabajo de Fin de Grado se estudiarán los códigos Goppa, sus parámetros y algoritmos de decodificación eficientes.

Actividades a desarrollar:

Códigos lineales y cota de Gilbert–Varshamov.
Códigos cíclicos y códigos BCH.
Códigos de evaluación y códigos GRS.
Códigos Goppa.
Algoritmo de Sugiyama.
Códigos Goppa y cota de Gilbert–Varshamov.

<i>Objetivos matemáticos planteados</i>
Descripción de los Códigos Goppa.
Relación de los códigos Goppa con los códigos BCH y GRS.
Decodificación eficiente de los códigos Goppa.
Estudio de la cota de Gilbert–Varshamov asintótica para códigos lineales.
Relación de los códigos Goppa con la cota de Gilbert–Varshamov.

Bibliografía para el desarrollo matemático de la propuesta:

[1] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2010.

[2] V. D. Goppa. *Geometry and Codes*. *Mathematics and its applications*, 24. (Soviet series). Springer Science+Business Media, 1988.

Otras referencias (si procede):

Firma del estudiante
(solo para trabajos propuestos por estudiantes)

Firma del responsable de tutorización
(solo para trabajos propuestos por estudiantes)

Firma del responsable de cotutorización
(solo para trabajos propuestos por estudiantes)

En, Granada, a 12 de Mayo de 2021