CURSO DE DOCTORADO

Flavio Salizzoni

Max Planck Institute for Mathematics in the Sciences, Alemania

The Hilbert regularity in Coding theory and Cryptography

Abstract:

The aim of the course is to show how well-known objects in commutative algebra emerge naturally in the context of coding theory and cryptography. In particular, the focus will be on the Hilbert function and its regularity.

In the first part of the course, we will show that the sequence of dimensions of the Schur powers of a linear code coincides is determined by the Hilbert function of the set of projective points associated with the code. This sequence is an invariant of the code and allows us to distinguish between non-equivalent codes. We will briefly discuss the consequences of these results in code-based cryptography.

In the second part of the course, we will focus on multivariate cryptography. After a brief introduction to the topic, we will prove how the Hilbert regularity can be used to bound from above the complexity of solving a system of polynomial equations.

Se celebrará en 4 sesiones:

-Lunes 6 de octubre de 12:00 a 14:00
-Viernes 10 de octubre de 10:00 a 12:00
-Miércoles 15 de octubre de 12:00 a 14:00
-Viernes 17 de octubre de 10:00 a 12:00

Registro (gratuito pero necesario): https://eventos.uva.es/go/hilbert-coding

Aula A125 (seminario de Álgebra), Facultad de Ciencias
Lunes 6 de Octubre de 2025 (12:00)
Organiza: GIR SINGACOM