Universidad Complutense de Madrid
Facultad de Ciencias Matemáticas
Departamento de Algebra

Teléfono: 91 394 45 70, Fax: 91 394 46 62
Correo electrónico: Algebra@mat.ucm.es

SEMINARIO DE GEOMETRÍA ALGEBRAICA

Jueves, 30 de noviembre de 2017, **13:00**, Seminario 238

Iván Blanco-Chacón

University College, Dublín

Impartirá la conferencia

Rank metric codes and and zeta functions

Resumen.

In [1], I. Duursma introduced the zeta function of an error correcting code over $\mathbb{F}_q$ with respect to the Hamming distance. It is the generating function for a family of weight enumerator polynomials and, as with zeta functions of curves over finite fields, its zeros encode essential information of the object, in this case, the code: the sum of the reciprocal roots of the zeta function, up to a sign, provides an upper-bound for the minimal distance, which dictates the correcting capacity of the code. Finer information on special families of codes (divisible, self-dual) can be extracted from the zeta function and an analogue of the Riemann Hypothesis is expected to occur for relevant families. Recently, in [2], we have introduced a zeta function for error correcting codes with respect to the rank-metric distance. We have found similar upper bounds as in the Hamming setting, although some new phenomena appear. Rank metric codes appear in random-network coding and distributed storage and are being extensively studied also from the point of view of code-based cryptography. In our talk, after recalling some definitions on Hamming/rank-metric codes, we will discuss the works [1] and [2]. Although some knowledge in basic error-correcting theory will help, the only pre-requisite to follow the talk is a good knowledge of linear algebra, so students are very welcome.

References [1] Duursma I.: From weight enumerators to zeta functions. Discret. Appl. Math. 111(12), 5573 (2001).

[2] Blanco-Chacón I., Byrne E., Duursma I., Sheekey J.: Rank metric codes and zeta functions. Des. Codes Cryptogr. 2017 (to appear)