gazteak RSME 2025

AL10

Coding Theory

Teoría de Códigos

Organizers **Organizadores** **Antolatzaileak**

Iván Bailera Martín
(Centro Univ. de la Defensa, Zaragoza)

Helena Martín Cruz
(IMAC & Universitat Jaume I)

Rodrigo San José Rubio
(IMUVa, Universidad de Valladolid)

Carlos Vela Cabello
(Universität St. Gallen)

Description **Descripción** **Deskribapena**

Information theory corresponds to a branch of mathematics and computer science that studies the transmission and processing of data. In this session, we will primarily focus on applications related to coding theory. These include computer science (code-based cryptography, data compression), electrical engineering (communication and coding theory), biology (DNA sequences), and physics (quantum computing and communication), among others. The session also includes applications from other areas to coding theory, such as lattice theory, finite geometries, algebraic geometry, commutative algebra, etc.

La teoría de la información corresponde a una rama de las matemáticas y de la computación que estudia la transmisión y el procesamiento de datos. En esta sesión nos interesaremos principalmente en las aplicaciones relacionadas con la teoría de códigos. Estas incluyen a las ciencias de la computación (criptografía basada en códigos, compresión de datos), la ingeniería eléctrica (teoría de la comunicación y codificación), la biología (secuencias de ADN) y la física (computación y comunicación cuántica), entre otras. La sesión también contempla aplicaciones de otras áreas a teoría de códigos, como pueden ser la teoría de retículos, geometrías finitas, geometría algebraica, álgebra conmutativa, etc.

MSC Codes **Códigos MSC** **MSC Kodeak**

94-06

(primary)

94B05; 94B35; 81P70

(secondary)

Slots **Bloques** **Blokeak**

2.A (Aula 0.7); 2.B (Aula 0.7); 2.C (Aula 0.7)

QR Code **Código QR** **QR Kodea**

Session Schedule **Horario de la Sesión** **Saioaren Ordutegia**

J16 | 11:00-11:20 | 0.7
Computational Study of Binary Group Codes of Small Lengths
Beatriz García García (Universidad de Oviedo)

J16 | 11:30-11:50 | 0.7
Distributed matrix multiplication using multivariate polynomials
Adrián Fidalgo-Díaz (University of Valladolid)

J16 | 12:00-12:20 | 0.7
Computational Private Information Retrieval Protocol with Codes over Rings
Seyma Bodur (Universidad de Valladolid)

J16 | 12:30-12:50 | 0.7
Consistent flag codes
Miguel Ángel Navarro-Pérez (University Carlos III of Madrid)

J16 | 16:30-16:50 | 0.7
Using classical codes for quantum fault-tolerant computing
Rodrigo San-José (Universidad de Valladolid)

J16 | 17:00-17:20 | 0.7
On direct product group codes and associated quantum codes
Miguel Sales Cabrera (Universitat d'Alacant)

J16 | 17:30-17:50 | 0.7
Error-correcting codes on higher dimensional varieties
Daniel Camazón Portela (University of Almería & Institute of Mathematics of the University of Valladolid)

V17 | 9:00-9:20 | 0.7
On $\mathbb{Z}_{p^s}$-additive simplex codes
Sergi Sánchez Aragón (Universitat Autònoma de Barcelona)

V17 | 9:30-9:50 | 0.7
Geometry of Rank Metric Codes over Rings
Markel Epelde (UPV/EHU)

V17 | 10:00-10:20 | 0.7
Skew Recursive Linear Sequences and Skew Codes
Tamar Mesablishvili (University of Granada)

Thursday 16	**Jueves 16**	**Osteguna 16**
11:00-11:20	**11:00-11:20**	**11:00-11:20**
[Room 0.7]	**[Aula 0.7]**	**[Gela 0.7]**

Computational Study of Binary Group Codes of Small Lengths

Beatriz García García
(Universidad de Oviedo)

Technological advances yield the need to develop quantum-resistant cryptosystems such as, for instance, the development of McEliece-type cryptosystems. In this direction, the study of group codes is interesting, being also the the construction of quantum codes another motivation for such a study. In this work, an exhaustive study of binary group codes with small lengths is carried out. It will allow to improve the knowledge of both algebraic and computational properties of the group code family.

Joint work with Consuelo Martínez López and Ignacio Fernández Rúa.

Thursday 16	**Jueves 16**	**Osteguna 16**
11:30-11:50	**11:30-11:50**	**11:30-11:50**
[Room 0.7]	**[Aula 0.7]**	**[Gela 0.7]**

Distributed matrix multiplication using multivariate polynomials

Adrián Fidalgo-Díaz
(University of Valladolid)

When running a distributed algorithm, the slowest of the worker nodes that perform the computation limits the speed of the execution. This justifies the need for designing distributed algorithms that do not require to gather the results from all the nodes, just the first of them that respond. Considering the slower nodes as erasures, this turns out to be a job for coding-theory. In this work, we tackle this problem using multivariate polynomials (in a Reed-Muller and hyperbolic codes fashion).

Joint work with Umberto Martínez-Peñas.

Thursday 16 | **Jueves 16** | **Osteguna 16**
12:00-12:20 | **12:00-12:20** | **12:00-12:20**
[Room 0.7] | **[Aula 0.7]** | **[Gela 0.7]**

Computational Private Information Retrieval Protocol with Codes over Rings

Seyma Bodur
(Universidad de Valladolid)

A Private Information Retrieval (PIR) protocol protects user's privacy. Computational privacy is one of the approaches that ensures security by preventing the database administrator from determining the file index with reasonable computational resources. We present a computational PIR scheme using codes over rings that utilize the coding theory perspective of Holzbaur, Hollanti, and Wachter-Zeh, and resists the attack presented by Bordage and Lavauzelle.

Joint work with Edgar Martínez-Moro and Diego Ruano.

Thursday 16 | **Jueves 16** | **Osteguna 16**
12:30-12:50 | **12:30-12:50** | **12:30-12:50**
[Room 0.7] | **[Aula 0.7]** | **[Gela 0.7]**

Consistent flag codes

Miguel Ángel Navarro-Pérez
(University Carlos III of Madrid)

A constant dimension code is a set of subspaces with the same dimension and a flag code is a set of flags (nested sequences of subspaces) with the same increasing sequence of dimensions.
Associated with any flag code, there is a family of constant dimension codes, the projected codes, whose parameters are related to the ones of the given flag code. In this talk, we introduce consistent flag codes, whose parameters are completely determined by the projected codes and study their properties.

Joint work with Clementa Alonso-González.

Thursday 16	**Jueves 16**	**Osteguna 16**
16:30-16:50	**16:30-16:50**	**16:30-16:50**
[Room 0.7]	**[Aula 0.7]**	**[Gela 0.7]**

Using classical codes for quantum fault-tolerant computing

Rodrigo San-José
(Universidad de Valladolid)

One of the main open problems for quantum fault-tolerant computing is the implementation of non-Clifford gates, particularly the T gate. Motivated by this, CSS-T were introduced as CSS codes which support a transversal T gate. In this talk, we show how to check if a CSS code is CSS-T using the Schur product, and we construct CSS-T codes from cyclic codes. We also study triorthogonal codes, which are a particular case of CSS-T codes that implements the T gate on the logical qubits.

Joint work with Eduardo Camps-Moreno, Hiram H. López, Gretchen L. Matthews, Diego Ruano and Ivan Soprunov.

arXiv:2312.17518

Thursday 16	**Jueves 16**	**Osteguna 16**
17:00-17:20	**17:00-17:20**	**17:00-17:20**
[Room 0.7]	**[Aula 0.7]**	**[Gela 0.7]**

On direct product group codes and associated quantum codes

Miguel Sales Cabrera
(Universitat d'Alacant)

Group codes, which are linear codes viewed as left ideals in a group algebra, are studied when this algebra is semisimple. The talk focuses on group codes where the group is a direct product of cyclic and dihedral groups, showing that, in some cases, they achieve optimal distance for their dimension. Additionally, quantum CSS codes will be constructed from these classical codes, which are crucial for quantum computing.

Joint work with Xaro Soler-Escrivà and Víctor Sotomayor.

Thursday 16	**Jueves 16**	**Osteguna 16**
17:30-17:50	**17:30-17:50**	**17:30-17:50**
[Room 0.7]	**[Aula 0.7]**	**[Gela 0.7]**

Error-correcting codes on higher dimensional varieties

Daniel Camazón Portela
(University of Almería & Institute of Mathematics of the University of Valladolid)

Tsfasman and Vlăduţ suggested the use of higher dimensional varieties to construct AG-codes, but the number of works in this sense does not equal that of curves or surfaces. Our aim is to go one step further the work of S. Hansen and study AG-codes on projective bundles over D-L surfaces. To obtain bounds on the parameters, we use intersection theory and the fact that, for some standard D-L surfaces, all their rational points are distributed on the irreducible components of a divisor Di.

Joint work with Juan Antonio López Ramos.

Friday 17	**Viernes 17**	**Ostirala 17**
9:00-9:20	**9:00-9:20**	**9:00-9:20**
[Room 0.7]	**[Aula 0.7]**	**[Gela 0.7]**

On $\mathbb{Z}_{p^s}$-additive simplex codes

Sergi Sánchez Aragón
(Universitat Autònoma de Barcelona)

$\mathbb{Z}_{p^s}$-additive codes are subgroups of $\mathbb{Z}_{p^s}^n$ where p is prime and $s \geq 1$. We consider recursive constructions of $\mathbb{Z}_{p^s}$-additive simplex codes of type α and β, which are a generalization over $\mathbb{Z}_{p^s}$ of the already known $\mathbb{Z}_{2^s}$-additive simplex codes. In this work, we show the fundamental parameters of these codes, as well as their complete weight distributions for the Hamming and homogeneous weights.

joint work with Cristina Fernández-Córdoba and Mercè Villanueva.

Friday 17	**Viernes 17**	**Ostirala 17**
9:30-9:50	**9:30-9:50**	**9:30-9:50**
[Room 0.7]	**[Aula 0.7]**	**[Gela 0.7]**

Geometry of Rank Metric Codes over Rings

Markel Epelde
(UPV/EHU)

In 1985, Gabidulin introduced the rank metric over finite fields. In 2022, Alfarano et al. studied the relations between this metric and the Hamming metrics. This metric has been generalized to rings in several papers, such as the Cardinal Rank. Based on support theory, in this talk we study the constructions of rank metrics over rings using ranked lattices, we classify those metrics and show some of their properties. Finally, we show their relations with the equivalent Hamming-like metrics.

Joint work with Alessandro Neri.

Friday 17	**Viernes 17**	**Ostirala 17**
10:00-10:20	**10:00-10:20**	**10:00-10:20**
[Room 0.7]	**[Aula 0.7]**	**[Gela 0.7]**

Skew Recursive Linear Sequences and Skew Codes

Tamar Mesablishvili
(University of Granada)

We explore the relationship between the skew and classical recursive linear sequences, formulate the Massey agreement theorem for skew linear recursive sequences and derive a condition under which the cyclic and acyclic complexities is the same. We also introduce a family of MDS codes with respect to skew-linear complexity, and compare such codes with other families of skew codes we encounter in the literature.

Joint work with José Gómez-Torrecillas.