UNIVERSITÀ POLITECNICA DELLE MARCHE

Dipartimento Ingegneria Informazione

Seminar Announcement

January 27, 2026, 10:00 – 11:00, Room 160-2

GROUP CODES AND LDOI CODES

Fabian Ricardo Molina Gomez, Universidad de Oviedo

Abstract

The advent of quantum computing poses a serious threat to many classical public-key cryptosystems, motivating the development of post-quantum cryptography. Within this setting, code-based cryptography stands out as a well-established and secure approach, encouraging the study of new families of structured linear codes. In this talk, we focus on group codes, namely linear codes that can be realized as two-sided ideals of group algebras over finite fields. Their algebraic structure has been extensively studied and, in the semisimple case, admits a description in terms of central idempotents. This viewpoint provides effective algebraic and computational tools for decoding and motivates further developments. Inspired by LDPC codes, we introduce LDOI (Low-Density Orthogonal Idempotent) group codes, defined by orthogonal idempotents of small weight. In the case of the binary field, this low-density condition gives rise to sparse parity-check–like matrices. When the associated adjacency matrix is binary, the minimum distance can be determined very easily, and efficient decoding can be achieved using a Bit-Flipping–type algorithm. Finally, we present explicit constructions of LDOI group codes with binary adjacency matrices. Restricting to abelian groups, we use 2-cyclotomic classes to construct low-weight orthogonal idempotents. Under suitable arithmetic conditions—for certain primes—we guarantee the desired sparsity. Examples, limitations, and directions for future research are discussed.

Bio

Fabián Molina holds a Bachelor's degree in Mathematics from the University of Tolima (Colombia) and a Doctorate in Mathematics and Statistics from the University of Oviedo (Spain). His work focuses on group algebras and two-sided ideals, particularly their role as group codes in the semisimple case, with applications in coding theory and cryptography.

For further information, contact:

Paolo Santini p.santini@univpm.it, Marco Baldi: m.baldi@univpm.it