

Construction of QC-LDPC Codes with Girth g from the Hermite Normal Form of a Matrix

Anthony Gomez-Fonseca

University of Notre Dame

The problem of determining the existence of a protograph-based QC-LDPC code with girth g and shortest blocklength for a prescribed protograph has been investigated in the literature. In some of these works, the goal was to obtain an algebraic expression for the blocklength in terms of the dimensions of the biadjacency matrix of the protograph and a lifting factor N . An algebraic expression has been found for N when $g > 4$ is desired in the case of the fully-connected (all-ones) protograph but only lower bounds for the cases with larger girth. Computer search has been used in most cases to determine the exact value for N that gives the shortest blocklength for a particular protograph. In this talk, we present a promising connection between the lifting factor N (and therefore the blocklength of a QC-LDPC code) and the product of the pivots of the Hermite normal form of a matrix constructed from certain substructures in the protograph called tailless backtrackless closed (TBC) walks.

In Special Session 2 on Coding Theory at the Mathematical Congress of the Americas 2025.