An Algebraic Approach to Coding Theory

Hiram H. López, Virginia Tech, Blacksburg, VA – 24061

Abstract

Coding theory plays a fundamental role in the reliable transmission and storage of information, enabling communication systems to detect and correct errors in the presence of noise. More recently, error-correcting codes have become increasingly important in cryptography, particularly in developing schemes believed to be secure against attacks by quantum computers.

Evaluation codes are defined by evaluating families of functions at a prescribed set of points. In this talk, we explore how the vanishing ideal of the point set plays a central role in determining the fundamental parameters of an evaluation code, such as its length, dimension, and minimum distance. When the points possess additional algebraic structure-such as Cartesian point sets or the rational points of the Hermitian curve-the associated ideal becomes an even more powerful tool, enabling the computation of further invariants, including the dual code and generalized Hamming weights. We also examine the connection between the permutation group of the code and the functions and point sets from which it is constructed, highlighting the interplay among algebraic geometry, coding theory, and symmetry.

Keywords: cryptography, quantum computing, vanishing ideal, Hamming weight, algebraic geometry.