On varieties and codes defined by quadratic equations

Ruud Pellikaan

We will review the work on algebraic geometry codes \( C = C_L(X, P, E) \) that have a unique representation \((X, P, E)\), where \( X \) is an algebraic curve, \( P \) is an \( n \)-tuple of mutually distinct points and \( E \) is a divisor. See [1, 2, 4, 5]. As a consequence algebraic geometry codes with certain parameters are not secure for the code based McEliece public crypto system.

One of the key ingredients of these results is the classical fact that certain curves embedded in projective space are defined by quadratic equations. We consider generalizations to higher dimensional varieties [6] and order domains [3] and their corresponding codes.

Keywords: McEliece public crypto system, algebraic geometry codes

References


1Department of Mathematics and Computing Science
Technical University of Eindhoven
g.r.pellikaan@tue.nl