Minimal codewords of certain evaluation codes

Rati Ludhani*[1,2] and Alain Couvreur[3,2]

[1]Centre Inria de Saclay – Institut National de Recherche en Informatique et en Automatique – France
[2]Laboratoire dínformatique de l´cole polytechnique [Palaiseau] – Centre National de la Recherche Scientifique, Ecole Polytechnique, Centre National de la Recherche Scientifique : UMR7161 – France
[3]Centre Inria de Saclay – Institut National de Recherche en Informatique et en Automatique – France

Résumé

Minimal codewords of a linear code reveal its important structural properties and are required, for instance, in secret-sharing schemes and certain decoding algorithms. A nonzero codeword is said to be minimal if its support does not properly contain the support of any other nonzero codeword. Determining minimal codewords of a general linear code is NP-hard, so one typically exploits the specific structure of a given code. Here, we consider this problem for projective Reed–Muller (PRM) codes of order 2.
PRM codes of order 2 are linear codes obtained by evaluating quadratic forms over a finite field F at the F-rational points of the corresponding projective space. To characterize their minimal codewords, we reduce the problem to the following geometric and combinatorial question: given two F-quadrics such that the F-rational points of one are contained in the other, can they differ? Note that for F-linear spaces of the same dimension, these are always same. Our main result is that for absolutely irreducible quadrics, containment of F-rational points implies same quadrics almost always. In this talk, we present a complete answer to this question, thereby classifying the minimal codewords of PRM codes of order 2.
Collaboration with Alain Couvreur.

*Intervenant