Decomposing Linear Codes over Finite Fields using Permutation Groups[1]

Stefka Bouyuklieva

Faculty of Mathematics and Informatics,
St. Cyril and St. Methodius University of Veliko Tarnovo, Bulgaria

stefka@ts.uni-vt.bg

A linear $[n, k]$ code C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field of q elements. We say that two codes C_1 and C_2 of the same length over $\mathbb{F}_q$ are equivalent provided there is a monomial matrix M and an automorphism γ of the field such that $C_2 = C_1 M\gamma$. The set of coordinate permutations that map the code C to itself forms a group, called the permutation automorphism group of C and denoted by $PAut(C) < \mathrm{S}_n$. Two more groups can be considered - the monomial automorphism group $MAut(C)$, and the group $\Gamma Aut(C)$ consisting of the maps of the form $M\gamma$, that map C to itself.

Let $(u, v) : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an inner product in the linear space $\mathbb{F}_q^n$. If C is an $[n, k]$ linear code, then its orthogonal complement $C^\perp = \{u \in \mathbb{F}_q^n : (u, v) = 0 \ \forall v \in C\}$ is a linear $[n, n-k]$ code. If $C = C^\perp$, C is termed self-dual.

The purpose of this talk is to present the structure of the linear codes over a finite field with q elements that have permutation automorphisms of prime order. Methods to construct and classify self-dual codes under the assumption that they have an automorphism of a given prime order are given in [1, 2]. These methods are extended to linear codes with permutation and monomial automorphisms over larger fields

References

[1] W.C.Huffman, Decomposing and shortening codes using automorphisms, *IEEE Trans. Inform. Theory* **32** (1986) 833-836.

[2] V.Y.Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Theory* 33 (1987) 77-82.

[1]This research was supported, in part, by the Bulgarian (NSF) contract KP-06 N 32/1 of 07.12.2019.