Construction and enumeration for self-dual cyclic codes of even length over $F_{2^m}+uF_{2^m}$

曹永林教授

山东理工大学

The class of self-dual codes is an interesting topic in coding theory duo to their connections to other fields of mathematics such as lattices, cryptography, invariant theory, block designs, etc. In many instances, self-dual codes over a finite field have been found by constructing self-dual codes over an extension ring of the field. Let F_{2^m} be a finite field of 2^m elements, $R=F_{2^m}+uF_{2^m}$ ($u^2=0$) and *s, n* be positive integers such that *n* is odd. We give an explicit representation for every self-dual cyclic code over the finite chain ring *R* of length $2^s n$ and provide an efficient calculation method to obtain all distinct codes. Moreover, we obtain a clear formula to count the number of all these self-dual cyclic codes. As an application, self-dual and 2-quasi-cyclic codes over F_{2^m} of length $2^{s+1}n$ can be obtained from self-dual cyclic code over R of length of length $2^s n$ and by a Gray map preserving orthogonality and distances from R onto $F_{2^m}{}^2$.