Finite Fields and Their Applications 43 (2017) 123–140

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A class of binary cyclic codes with generalized Niho exponents

Yuan Chen [a,b], Nian Li [a,c,1], Xiangyong Zeng [a,b,*,2]

[a] *Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan 430062, PR China*
[b] *State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093), PR China*
[c] *Department of Informatics, University of Bergen, N-5020 Bergen, Norway*

A R T I C L E   I N F O

Article history:
Received 20 April 2016
Received in revised form 26 September 2016
Accepted 26 September 2016
Available online xxxx
Communicated by Gary McGuire

MSC:
11T71
94B15
11L03

Keywords:
Niho exponent
Cyclic code
Weight distribution
Exponential sum

A B S T R A C T

In this paper, a class of binary cyclic codes with three generalized Niho-type nonzeros is introduced. Based on some techniques in solving certain equations over finite fields, the proposed cyclic codes are shown to have six nonzero weights and the weight distribution is also completely determined.

* Corresponding author at: Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan 430062, PR China.
E-mail address: xiangyongzeng@aliyun.com (X. Zeng).

[1] N. Li is supported by the Norwegian Research Council.
[2] X. Zeng is supported by the National Natural Science Foundation of China (No. 61170257).

http://dx.doi.org/10.1016/j.ffa.2016.09.005

1. Introduction

Niho exponents were originally introduced by Niho who investigated the cross correlation between an m-sequence and its decimations [14]. In the past decades Niho's this pioneering work has become one of the most cited works in the theory of m-sequences and coding theory. As applications of Niho exponents, the reader is referred to [4,7,13,14] for the constructions of sequence families with low correlation by using an m-sequence and its Niho-type decimations, referred to [1,5,6,8,10,16] for the constructions of Bent functions and permutation polynomials from Niho exponents, and referred to [2,9,11] for the constructions of cyclic codes with few Niho-type nonzeros.

In recent papers [17] and [18], the authors studied several families of cyclic codes with arbitrarily many generalized Niho-type nonzeros, and determined their weight distributions. A cyclic code is said to have k nonzeros (or zeros) if its parity-check (or generator) polynomial has k irreducible factors over the underlying field, and we usually say that a cyclic code has k nonzeros $\alpha_1, \alpha_2, \cdots, \alpha_k$ if α_i is a root of the i-th irreducible factor for $i = 1, 2, \cdots, k$ respectively. To determine the weight distribution of cyclic codes, it's usual to solve certain equations over finite fields and then determine the power moment identities. The coefficient matrix of the system of equations to be solved in [17] (or [18]) has a particular form, i.e., the exponent of the variables in each column varies consecutively either from $-t$ to t or from $-2t+1$ to $2t-1$ with gap 2 for some positive integer t (see (18), (19), (22), (23) in [17]). The matrix in such a form behaves like a Vandermonde matrix whose rank can be easily determined. This enabled the authors in [17] (or [18]) can obtain the first $2t$ power moment identities and then determine the weight distribution of the cyclic codes therein. Motivated by this observation, in this paper we consider a new class of cyclic codes with generalized Niho-type nonzeros and the property that the corresponding coefficient matrix of the system of equations do not behave like a Vandermonde matrix. Note that the above mentioned coefficient matrix and the generalized Niho-type nonzeros of the cyclic code are in one-to-one correspondence. Thus, our approach to this problem is then to obtain a new coefficient matrix by adding one row into a Vandermonde matrix, where the exponent of the added row has gap 2 with that of the last row in the employed Vandermonde matrix (see (A.1) for example). It will be seen that it is much more difficult to determine the number of solutions to the system of equations with such a coefficient matrix, even though it is very close to being a Vandermonde matrix. By using this idea, a class of cyclic codes with three generalized Niho-type nonzeros is proposed in this paper, and the weight distribution is completely determined based on some techniques in solving equations over finite fields. It is surprising that our problem has close relation with the Zetterberg codes [15].

The rest of this paper is organized as follows. Section 2 recalls some basic concepts and results on the cyclotomic cosets of the generalized Niho exponents. Section 3 proposes a class of binary cyclic codes with three generalized Niho-type nonzeros and determines their weights. Section 4 deduces the first five power moment identities. Section 5 de-