Finite Fields and Their Applications 24 (2013) 45–54

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Quasi-cyclic NMDS codes

Hongxi Tong *,[1], Yang Ding [2]

Department of Mathematics, Shanghai University, Shanghai, 200444, PR China

ARTICLE INFO

Article history:
Received 20 September 2012
Received in revised form 9 April 2013
Accepted 27 May 2013
Available online 13 June 2013
Communicated by W. Cary Huffman

MSC:
94B05
94B15
14H05
14H37
14H52

Keywords:
Cyclic codes
Quasi-cyclic codes
NMDS codes
Elliptic curves
Elliptic function fields
Algebraic geometry codes

ABSTRACT

Quasi-cyclic (QC) codes constitute a remarkable generalization of cyclic codes, and near-MDS (NMDS) codes are a family of codes obtained by weakening the restrictions of MDS codes. In this paper, we consider the QC NMDS codes by combining these two concepts. By choosing some elliptic curves with many rational points, we give a construction of QC NMDS codes based on the action of an elliptic curve automorphism on the rational points of the curve. Moreover, we calculate explicit example over finite fields of characteristic 2, 3, 5 or 7.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q. Let C be an $[n,k,d]$ linear code over $\mathbb{F}_q$. The Singleton bound states a relationship among n, k and d: $d \leqslant n-k+1$. So the Singleton defect of C is defined by $s(C)=n-k+1-d$, $s(C)\geqslant 0$. If $s(C)=0$, C is called an MDS code. MDS codes have very good properties and are important. For example Reed–Solomon codes are MDS.

* Corresponding author.
E-mail addresses: tonghx@shu.edu.cn (H. Tong), dingyang@shu.edu.cn (Y. Ding).

[1] The work of the first author is supported by a grant of “The First-Class Discipline of Universities in Shanghai”.

[2] The work of the second author is supported by the National Natural Science Foundation of China (11201286).

1071-5797/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ffa.2013.05.008

If $s(C) = 1$, C is called an almost MDS (AMDS) code [3]. If $s(C) = s(C^{\perp}) = 1$, C is called a near-MDS (NMDS) code, where $C^{\perp}$ is the dual of C.

Let C be an $[n, k, n-k]$ AMDS code over $\mathbb{F}_q$, if $n > k + q$, then C is an NMDS code [4].

The ternary Golay codes and the quaternary quadratic residue [11,6,5] code are NMDS codes. NMDS codes have been investigated in [1,2,5,13]. The existence of an $[n, k, n-k]_q$ NMDS code C is equivalent to the existence of a set S of points in $PG(k-1, q)$ having the following properties:

a) any $k-1$ points from S generate a hyperplane in $PG(k-1, q)$;
b) there exist k points lying on a hyperplane;
c) every $k+1$ points from S generate $PG(k-1, q)$.

And they correspond to

a) $s(C^{\perp}) \leqslant 1$;
b) $s(C) \neq 0$;
c) $s(C) \leqslant 1$,

respectively.

Especially, every $[n, 3, n-3]$ NMDS code is equivalent to $(n, 3)$-arc in $PG(2, q)$.

Let C be a linear code with length lm over $\mathbb{F}_q$. Let

$$c = (c_{0,0}, c_{0,1}, \ldots, c_{0,l-1}, c_{1,0}, \ldots, c_{1,l-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,l-1})$$

denote a codeword in C. Then

$$c' = (c_{m-1,0}, \ldots, c_{m-1,l-1}, c_{0,0}, c_{0,1}, \ldots, c_{0,l-1}, \ldots, c_{m-2,0}, \ldots, c_{m-2,l-2}, c_{m-2,l-1}) \in C.$$

C is called a QC code over $\mathbb{F}_q$ of length lm and index l, and m is called the co-index of C. $R = \mathbb{F}_q[x]/(x^m - 1)$ is the ring of q-ary polynomials module $x^m - 1$. The map $\phi : \mathbb{F}_q^{l,m} \to R^l$ defined by

$$\phi(c) = \big(c_0(x), c_1(x), \ldots, c_{l-1}(x)\big)$$

where $c_j(x) = c_{0,j} + c_{1,j}x + \cdots + c_{m-1,j}x^{m-1} \in R$. Let $\phi(C)$ denote the image of C under ϕ. Then ϕ induces a one-to-one correspondence between the set of QC codes of index l and length lm over $\mathbb{F}_q$ and the set of R-linear codes of length l over R.

Let $m_1, m_2, \ldots, m_l$ be positive integers and set $R_i = \mathbb{F}_q[x]/(x^{m_i} - 1)$. Any $\mathbb{F}_q[x]$-submodule of the $\mathbb{F}_q[x]$-module $R' := R_1 \times R_2 \times \cdots \times R_l$ is called a generalized quasi-cyclic (GQC) code of block length $(m_1, m_2, \ldots, m_l)$ and $\mathbb{F}_q$-length $\sum_{i=1}^{l} m_i$ over $\mathbb{F}_q$ [6,9–12].

This paper is organized as follows. In preliminaries, we give some basic facts on elliptic curves and elliptic function fields. Then we give our results on automorphisms of elliptic curves, and we can construct some QC NMDS codes from these elliptic curves. In the last, we will obtain many QC NMDS codes over finite fields with characteristic 2, 3, 5, and 7.

2. Preliminaries

Let E/K be an elliptic curve which is given by a Weierstrass equation

$$C\colon Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$