Finite Fields and Their Applications 23 (2013) 8–34

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Cyclic codes from cyclotomic sequences of order four

Cunsheng Ding

Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

ARTICLE INFO

Article history:
Received 27 December 2012
Revised 26 March 2013
Accepted 28 March 2013
Available online 17 April 2013
Communicated by Arne Winterhof

MSC:
94B15
94B05
05B50

Keywords:
Almost difference sets
Cyclic codes
Cyclotomy
Difference sets
Sequences

ABSTRACT

Cyclic codes are a subclass of linear codes and have a lot of applications in consumer electronics, data transmission technologies, broadcast systems, and computer applications as they have efficient encoding and decoding algorithms. In this paper, three cyclotomic sequences of order four are employed to construct a number of classes of cyclic codes over GF(q) with prime length. Under certain conditions lower bounds on the minimum weight are developed. Some of the codes obtained are optimal or almost optimal. In general, the codes constructed in this paper are very good. Some of the cyclic codes obtained in this paper are closely related to almost difference sets and difference sets.

1. Introduction

Let q be a power of a prime p. A linear $[n, \kappa, d]$ code over GF(q) is a κ-dimensional subspace of $\mathrm{GF}(q)^n$ with minimum (Hamming) nonzero weight d.

A linear $[n, \kappa]$ code $\mathcal{C}$ over the finite field GF(q) is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. By identifying any vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{GF}(q)^n$ with

$$c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in \mathrm{GF}(q)[x]/\left(x^n - 1\right),$$

E-mail address: cding@ust.hk.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.03.006

any code $\mathcal{C}$ of length n over GF(q) corresponds to a subset of $\mathrm{GF}(q)[x]/(x^n-1)$. The linear code $\mathcal{C}$ is cyclic if and only if the corresponding subset in $\mathrm{GF}(q)[x]/(x^n-1)$ is an ideal of the ring $\mathrm{GF}(q)[x]/(x^n-1)$.

Note that every ideal of $\mathrm{GF}(q)[x]/(x^n-1)$ is principal. Let $\mathcal{C}=\langle g(x)\rangle$, where the generator $g(x)$ of the ideal has the least degree. Then $g(x)$ is called a *generator polynomial* and $h(x)=(x^n-1)/g(x)$ is referred to as a *parity-check polynomial* of $\mathcal{C}$.

A vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{GF}(q)^n$ is said to be *even-like* if $\sum_{i=0}^{n-1} c_i = 0$, and is *odd-like* otherwise. The minimum weight of the even-like codewords, respectively the odd-like codewords of a code is the minimum even-like weight, denoted by d_{even}, respectively the minimum odd-like weight of the code, denoted by d_{odd}.

The error correcting capability of cyclic codes may not be as good as some other linear codes in general. However, cyclic codes have many applications in storage and communication systems because they have efficient encoding and decoding algorithms [6–8,15,23]. For example, Reed–Solomon codes have found important applications from deep-space communication to consumer electronics. They are prominently used in consumer electronics such as CDs, DVDs, Blu-ray Discs, in data transmission technologies such as DSL & WiMAX, in broadcast systems such as DVB and ATSC, and in computer applications such as RAID 6 systems.

Cyclic codes have been studied for decades and a lot of progress has been made (see [3,17,20] for further references). The total number of cyclic codes over GF(q) and their constructions are closely related to cyclotomic cosets modulo n, and thus many areas of number theory. The objective of this paper is to construct cyclic codes over GF(q) with length n and generator polynomial

$$\frac{x^n-1}{\gcd(\Lambda(x), x^n-1)} \tag{1}$$

where

$$\Lambda(x)=\sum_{i=0}^{n-1} \lambda_i x^i \in \mathrm{GF}(q)[x]$$

and $\lambda^\infty = (\lambda_i)_{i=0}^{\infty}$ is a sequence of period n over GF(q). Throughout this paper, we call the cyclic code $\mathcal{C}_\lambda$ with the generator polynomial of (1) the *code defined by the sequence* λ^∞, and the sequence λ^∞ the *defining sequence* of the cyclic code $\mathcal{C}_\lambda$. By properly selecting the sequence λ^∞ over GF(q) related to certain combinatorial designs, we will construct cyclic codes over GF(q) with good parameters.

2. Preliminaries

In this section, we present basic notations and results of combinatorial designs, cyclotomy, sequences, and cyclic codes that will be employed in subsequent sections.

2.1. Difference sets and almost difference sets

Let $(A,+)$ be an abelian group of order n. Let C be a k-subset of A. The set C is an (n,k,λ) *difference set* of A if $d_C(w)=\lambda$ for every nonzero element w of A, where $d_C(w)$ is the *difference function* defined by $d_C(w)=|C\cap(C+w)|$, here and hereafter $C+w := \{c+w\colon\ c\in C\}$. Detailed information on difference sets can be found in [2].

Let $(A,+)$ be an abelian group of order n. A k-subset C of A is an (n,k,λ,t) *almost difference set* of A if $d_C(w)$ takes on λ altogether t times and $\lambda+1$ altogether $n-1-t$ times when w ranges over all the nonzero elements of A. The reader is referred to [1] for information on almost difference sets.

Difference sets and almost difference sets are closely related to sequences with only a few autocorrelation values, and are related to some of the codes constructed in this paper.