Discrete Mathematics 321 (2014) 76–89

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Binary cyclic codes from explicit polynomials over GF(2^m)[☆]

Cunsheng Ding[a], Zhengchun Zhou[b,*]

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

[b] School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China

ARTICLE INFO

Article history:
Received 14 August 2013
Received in revised form 18 December 2013
Accepted 23 December 2013
Available online 8 January 2014

Keywords:
Polynomials
Permutation polynomials
Cyclic codes
Linear span
Sequences

ABSTRACT

Cyclic codes are a subclass of linear codes and have applications in consumer electronics, data storage systems, and communication systems as they have very efficient encoding and decoding algorithms. In this paper, monomials and trinomials over finite fields with even characteristic are employed to construct a number of families of binary cyclic codes. Lower bounds on the minimum weight of some families of the cyclic codes are developed. The minimum weights of other families of the codes constructed in this paper are determined. The dimensions of the codes are flexible. Some of the codes presented in this paper are optimal or almost optimal in the sense that they meet some bounds on linear codes. Open problems regarding binary cyclic codes from monomials and trinomials are also presented.

1. Introduction

Let q be a power of a prime p. A linear $[n, k, d]$ code over GF(q) is a k-dimensional subspace of GF$(q)^n$ with minimum Hamming distance d. A linear $[n, k]$ 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 $\sum_{i=0}^{n-1} c_i x^i \in \mathrm{GF}(q)[x]/(x^n - 1)$, 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 $\mathrm{GF}(q)[x]/(x^n - 1)$. It is well known that every ideal of $\mathrm{GF}(q)[x]/(x^n - 1)$ is principal. Let $\mathcal{C} = (g(x))$ be a cyclic code, where $g(x)$ is monic and has the smallest degree. Then $g(x)$ is called the *generator polynomial* and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check* polynomial of $\mathcal{C}$.

Cyclic codes have wide applications in storage and communication systems because they afford efficient encoding and decoding algorithms [5,12,27]. Cyclic codes have been studied for decades and a lot of progress has been made (see for example, [3,4,9–11,13,16,14,17,18,22,21,25,24,26,28,30]). The total number of cyclic codes over GF(q) and their constructions are closely related to q-cyclotomic cosets modulo n, and thus many topics of number theory. One way of constructing cyclic codes over GF(q) of length n is to use the generator polynomial

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

[☆] C. Ding's research was supported by The Hong Kong Research Grants Council, Proj. No. 601013. Z. Zhou's research was supported by the Natural Science Foundation of China under Grants 61201243 and 61373009, and the application fundamental research plan project of Sichuan Province under Grant 2013JY0167, and the open research fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2013D10. Z. Zhou is also with National Mobile Communications Research Laboratory, Southeast University.

* Corresponding author.
E-mail addresses: cding@ust.hk (C. Ding), zzc@home.swjtu.edu.cn (Z. Zhou).

0012-365X/$ – see front matter © 2014 Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.disc.2013.12.020

where

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

and $s^\infty = (s_i)_{i=0}^\infty$ is a sequence of period n over GF(q). Throughout this paper, we call the cyclic code $\mathcal{C}_s$ with the generator polynomial of (1) the *code defined by the sequence* s^∞, and the sequence s^∞ the *defining sequence* of the cyclic code $\mathcal{C}_s$.

One basic question is whether good cyclic codes can be constructed with this approach. It turns out that the code $\mathcal{C}_s$ could be an optimal or almost optimal linear code if the sequence s^∞ is properly designed [6].

In this paper, several types of monomials and trinomials over GF(2^m) will be employed to construct a number of classes of binary cyclic codes. Lower bounds on the minimum weight of some classes of the cyclic codes are derived, in some cases we determine the exact minimal distance. The dimensions of the codes of this paper are flexible. Some of the codes obtained in this paper are optimal or almost optimal as they meet certain bounds. Several open problems regarding cyclic codes from monomials and trinomials are also presented in this paper.

The first motivation of this study is that some of the codes constructed in this paper could be optimal or almost optimal. The second motivation is the simplicity of the constructions of these cyclic codes that may lead to efficient encoding and decoding algorithms.

2. Preliminaries

In this section, we present basic notations and results of q-cyclotomic cosets, highly nonlinear functions, and sequences that will be employed throughout the paper.

2.1. Some notations fixed throughout this paper

Throughout this paper, we adopt the following notations unless otherwise stated:

- $q = 2$, m is a positive integer, $r = q^m$, and $n = r - 1$.
- $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is the usual ring of integers modulo n.
- α is a generator of GF$(r)^*$, and $m_a(x)$ is the minimal polynomial of $a \in$ GF(r) over GF(q).
- $\mathbb{N}_q(x)$ is a function defined by $\mathbb{N}_q(i) = 0$ if $i \equiv 0 \pmod q$ and $\mathbb{N}_q(i) = 1$ otherwise, where i is any nonnegative integer.
- Tr(x) is the trace function from GF(r) to GF(q).
- By Database we mean the collection of the tables of best linear codes known maintained by Markus Grassl at http://www.codetables.de/.

2.2. The linear span and minimal polynomial of periodic sequences

Let $s^\infty = (s_i)_{i=0}^\infty$ be a sequence of period L over GF(q). A polynomial $c(x) = \sum_{i=0}^{\ell} c_i x^i$ over GF(q), where $c_0 = 1$, is called a *characteristic polynomial* of s^∞ if

$$-c_0 s_i = c_1 s_{i-1} + c_2 s_{i-2} + \cdots + c_l s_{i-\ell} \quad \text{for all } i \geq \ell.$$

The characteristic polynomial of smallest degree is called the *minimal polynomial* of s^∞, and denoted by $\mathbb{M}_s(x)$. The degree of the minimal polynomial is referred to as the *linear span* or *linear complexity* of s^∞. Since we require the constant term of any characteristic polynomial to be 1, the minimal polynomial of any periodic sequence s^∞ is to be unique. In addition, any characteristic polynomial must be a multiple of the minimal polynomial. It should be noticed that in some references the reciprocal of $\mathbb{M}_s(x)$ is called the minimal polynomial of the sequence s^∞ (see [1,15]).

There are a few ways to determine their linear span and minimal polynomials of a periodic sequence. One of them is given in the following lemma [8, p. 87, Theorem 5.3].

Lemma 1. *Let s^∞ be a sequence of period L over* GF(q). *Define $S^L(x) = \sum_{i=0}^{L-1} s_i x^i \in$* GF($q$)[$x$]. *Then the minimal polynomial $\mathbb{M}_s(x)$ of s^∞ is given by*

$$\frac{x^L - 1}{\gcd(x^L - 1, S^L(x))} \tag{2}$$

and the linear span $\mathbb{L}_s$ of s^∞ is given by $L - \deg(\gcd(x^L - 1, S^L(x)))$.

It is well known that any sequence s^∞ over GF(q) of period $q^m - 1$ has a unique expansion of the form [15, p. 87]

$$s_t = \sum_{i=0}^{q^m-2} c_i \alpha^{it}, \quad \text{for all } t \geq 0. \tag{3}$$

An alternative way to compute the linear span and minimal polynomial of $\mathbb{M}_s(x)$ is based on (3) and a result in [1].

Lemma 2. *Let s^∞ be a sequence over* GF(q) *of period $q^m - 1$ with the expansion in* (3). *Let the index set be $I = \{i | c_i \neq 0\}$, then the minimal polynomial $\mathbb{M}_s(x)$ of s^∞ is $\mathbb{M}_s(x) = \prod_{i \in I}(1 - \alpha^i x)$, and the linear span of s^∞ is $|I|$.*