Finite Fields and Their Applications 34 (2015) 1–19

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

LCD codes over finite chain rings

Xiusheng Liu, Hualu Liu

School of Mathematics and Physics, Hubei Polytechnic University, Huangshi, Hubei 435003, China

ARTICLE INFO

Article history:
Received 27 May 2014
Received in revised form 28 November 2014
Accepted 13 January 2015
Available online 28 January 2015
Communicated by W. Cary Huffman

MSC:
11T71
94B05

Keywords:
Finite chain rings
Complementary dual codes
Generator matrices

ABSTRACT

A linear code with a complementary-dual (an LCD code) is defined to be a linear code C satisfying $C \cap C^{\perp} = \{0\}$. We provide a necessary condition for an LCD linear code C over a finite chain ring. Under suitable conditions, we give a sufficient condition under which a linear code C over a finite chain ring is LCD. In particular, we derive a necessary and sufficient condition for free linear codes over a finite chain ring to be LCD. We also give a characterization of LCD codes over principal ideal rings.

1. Introduction

A linear code with a complementary-dual (which is abbreviated to LCD code) was defined in [10] to be a linear code C satisfying $C \cap C^{\perp} = \{0\}$. In the same paper, Massey showed that asymptotically good LCD codes exist, and provided applications of LCD codes such as they provide an optimum linear coding solution for the two-user binary adder channel.

E-mail addresses: lxs6682@163.com (X. Liu), hwlulu@163.com (H. Liu).

http://dx.doi.org/10.1016/j.ffa.2015.01.004
1071-5797/

Dinh established the algebraic structures in terms of generator polynomial of all repeated-root constacyclic codes of length $3p^s$, $4p^s$, $6p^s$ over $\mathbb{F}_{p^m}$. Using these structures, constacyclic LCD codes of such lengths were also characterized (see [1,3,2]). Yang and Massy in [15] showed that a necessary and sufficient condition for a cyclic code of length n over finite fields to be an LCD code is that the generator polynomial $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ as in $x^n - 1$. In [13], Sendrier indicated that linear codes with complementary-duals meet the asymptotic Gilbert–Varshamov bound. Esmaeili and Yari in [6] studied complementary-dual quasi-cyclic codes. Necessary and sufficient conditions for certain classes of quasi-cyclic codes to be LCD codes were obtained [6].

The purpose of this paper is to examine linear codes with complementary duals over finite chain rings. The necessary background materials on finite chain rings are given in Section 2. Section 3 contains the main results of this paper. We provide a necessary condition for an LCD linear code C over a finite chain ring (see Theorem 3.4). An example is exhibited to show that the converse of Theorem 3.4, in general, does not hold. Under suitable conditions, we give a sufficient condition under which a given linear code C over a finite chain ring is LCD. In particular, we derive a necessary and sufficient condition for free linear codes over a finite chain ring to be LCD. In Section 4, we give a characterization of LCD codes over principal ideal rings (PID).

2. Preliminaries

We begin with some definitions and properties about finite chain rings (see [9]). Let R be a finite commutative ring with identity. A nonempty subset $C \subseteq R^n$ is called a *linear code* of length n over R if it is an R-submodule of R^n. Throughout this paper, all codes are assumed to be linear.

A commutative ring is called a *chain ring* if the lattice of all its ideals is a chain. It is well known that if R is a finite chain ring, then R is a principal ideal ring and has a unique maximal ideal $\langle\gamma\rangle = R\gamma = \{r\gamma \mid r \in R\}$. Its chain of ideals is

$$R = \langle\gamma^0\rangle \supset \langle\gamma^1\rangle \supset \cdots \supset \langle\gamma^{t-1}\rangle \supset \langle\gamma^t\rangle = \{0\}.$$

The integer t is called the *nilpotency index* of $\langle\gamma\rangle$. Note that the quotient $R/\langle\gamma\rangle$ is a finite field $\mathbb{F}_q$, where q is a power of a prime p. There is a natural homomorphism from R onto $\mathbb{F}_q = R/\langle\gamma\rangle$, i.e.,

$$^{-} : R \longrightarrow \mathbb{F}_q = R/\langle\gamma\rangle, \quad r \mapsto r + \langle\gamma\rangle = \bar{r}, \quad \text{for any } r \in R.$$

We need the following lemma (see [5]).

Lemma 2.1. *Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$. Let $V \subset R$ be a set of representatives for the equivalence classes of R under congruence modulo γ. Then*