Finite Fields and Their Applications 50 (2018) 138–153

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Constructions of optimal LCD codes over large finite fields

Lin Sok [a,b], Minjia Shi [c,a,d,*], Patrick Solé [e]

[a] *School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China*
[b] *Department of Mathematics, Royal University of Phnom Penh, 12156 Phnom Penh, Cambodia*
[c] *Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, Anhui University, No.3 Feixi Road, Hefei, Anhui, 230039, China*
[d] *National Mobile Communications Research Laboratory, Southeast University, China*
[e] *CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France*

ARTICLE INFO

Article history:
Received 31 May 2017
Received in revised form 14 September 2017
Accepted 15 November 2017
Available online xxxx
Communicated by W. Cary Huffman

MSC:
94B05
94B15

Keywords:
Orthogonal matrices
Complementary dual codes
Matrix product codes
Optimal codes

ABSTRACT

In this paper[1], we prove existence of optimal complementary dual codes (LCD codes) over large finite fields. We also give methods to generate orthogonal matrices over finite fields and then apply them to construct LCD codes. Construction methods include random sampling in the orthogonal group, code extension, matrix product codes and projection over a self-dual basis.

* Corresponding author.
E-mail addresses: sok.lin@rupp.edu.kh (L. Sok), smjwcl.good@163.com (M. Shi), sole@enst.fr (P. Solé).

[1] This paper was presented in part at the International Conference on Coding Theory, Cryptography and Related Topics, Shandong University of Technology, Zibo, April 7–11, 2017.

https://doi.org/10.1016/j.ffa.2017.11.007
1071-5797/

1. Introduction

Linear codes with complementary duals, which we refer to as LCD codes, were introduced by Massey in [19]. They give an optimum linear coding solution for the two user binary adder channel. They are also used in counter measures to passive and active side channel analyses on embedded crypto-systems, see [5] for a detailed description. It is known from [20] that LCD codes are asymptotically good.

Dougherty et al. [8] constructed binary LCD codes using orthogonal matrices, self-dual codes, combinatorial designs and Gray map from codes over a family of non chain rings of characteristic 2. Liu et al. [16] characterized matrix product linear complementary dual (MPLCD) codes and gave their constructions from orthogonal-like matrices. Using generalized Reed–Solomon codes, the authors of [4] and [13] proved the existence of optimal LCD codes over finite fields with some conditions on lengths and the field sizes. The problem of existence of q-ary $[n, k]$ MDS LCD codes has completely been solved by Carlet et al. [6] for the Euclidean case.

Recently, in the paper [21], MDS self-dual codes over large prime fields have been constructed from orthogonal matrices and from the generalized method of [1]. It is important to note that a single orthogonal matrix gives rise to several LCD codes, by a different choice of basis.

From the existence of MDS self-dual codes for example in [9,14] as well as from MDS self-orthogonal codes, we construct MDS LCD codes with certain lengths. We also generalize the constructions [21] of orthogonal matrices from prime fields to arbitrary finite fields and afterwards we give explicit constructions of LCD and MPLCD codes. Short LCD codes are constructed from orthogonal-like matrices by randomly sampling elements in the orthogonal group and from code extension by two symbols while the long ones are constructed from matrix product codes and from projection over a self-dual basis. Many optimal, almost MDS and MDS codes over different fields are obtained.

The paper is organized as follows: Section 2 gives preliminaries for LCD codes. Section 3 proves the existence of LCD codes of certain lengths and also gives method to construct and to extend an LCD code. In Section 4 we present numerical results of some optimal codes, almost MDS and MDS LCD codes over different large fields.

2. Preliminaries

A *linear* $[n, k]$ *code* C *of length* n over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. An element in C is called a *codeword*. The (Hamming) weight $\mathrm{wt}(\mathbf{x})$ of a vector $\mathbf{x} = (x_1, \ldots, x_n)$ is the number of non-zero coordinates in it. The *minimum distance (*or *minimum weight)* $d(C)$ of C is $d(C) := \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$. The *Euclidean inner product* of $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbb{F}_q^n$ is $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$. The *dual* of C, denoted by $C^{\perp}$ is the set of vectors orthogonal to every codeword of C under the Euclidean inner product. A linear code C is called linear complementary dual (*LCD*) if $C \cap C^{\perp} = \{0\}$.