Finite Fields and Their Applications 42 (2016) 67–80

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Quasi-cyclic complementary dual codes

Cem Güneri [a,*], Buket Özkaya [a], Patrick Solé [b,c]

[a] Sabancı University, FENS, 34956 İstanbul, Turkey
[b] CNRS, LTCI, University of Paris-Saclay, 75 013 Paris, France
[c] Mathematics Department, King Abdulaziz University, Jeddah, Saudi Arabia

ARTICLE INFO

Article history:
Received 28 September 2015
Received in revised form 9 May 2016
Accepted 10 July 2016
Available online 22 July 2016
Communicated by Chaoping Xing

MSC:
94B05
11T71

Keywords:
Quasi-cyclic code
LCD code
Dual code

ABSTRACT

Linear complementary dual codes are linear codes that intersect with their dual trivially. Quasi-cyclic codes that are complementary dual are characterized and studied by using their concatenated structure. Some asymptotic results are derived. Hermitian linear complementary dual codes are introduced to that end and their cyclic subclass is characterized. Constructions of quasi-cyclic complementary dual codes from codes over larger alphabets are given.

1. Introduction

Linear complementary codes (LCD) are linear codes that intersect with their dual trivially. This concept was introduced by Massey, following an Information Theoretic motivation [12]. It was rediscovered more recently in [2] from Boolean masking considerations, of interest in embarked cryptography. The two main results so far in the theory

* Corresponding author.
E-mail addresses: guneri@sabanciuniv.edu (C. Güneri), buketo@sabanciuniv.edu (B. Özkaya), sole@enst.fr (P. Solé).

http://dx.doi.org/10.1016/j.ffa.2016.07.005

of LCD codes are the characterization of the cyclic subclass [17] and the asymptotic goodness [15]. In the present work we consider the more general subclass of quasi-cyclic complementary dual codes (QCCD). This was partially studied in [3] where special attention to one-generator family was put. We use the duality driven Chinese Remainder Theorem (CRT) decomposition championed in [9,10] and more recently in [5–7]. Since that decomposition was useful to study self-dual quasi-cyclic codes it is natural to consider it again for studying LCD codes. While [2] only considers binary codes, we have q-ary codes which are useful in several ways. In particular we generalize in the case of q a square the cyclic subclass characterization of [11]. We also use this extra flexibility for deriving new constructions of LCD codes by base field descent. Last, but not least, we need a Hermitian version of Massey's work [11,12] to use in the duality driven CRT in order to show that long QCCD codes are good (Corollary 3.8). This is the main result of this paper. Some numerical examples show that the codes are also good in finite length. Some are even optimal as linear codes as Table 2 shows.

The material is organized as follows. Section 2 recalls the CRT set-up, on which Section 3 is built to derive its asymptotic results. Section 4 is dedicated to the Hermitian inner product. Section 5 considers special constructions, in particular from trace orthogonal bases.

2. Background on quasi-cyclic codes

In the whole paper q denotes a prime power and $\mathbb{F}_q$ the finite field of that order. A linear code over $\mathbb{F}_q$ is called a **quasi-cyclic** (QC) code of index ℓ if it is closed under shifting codewords by ℓ units, and ℓ is the smallest positive integer with this property. So, cyclic codes amount to the special case $\ell = 1$. It is well-known that the index of a QC code divides its length. So, we let C be a QC code of length $m\ell$, index ℓ over $\mathbb{F}_q$. If we let $R := \mathbb{F}_q[x]/\langle x^m - 1\rangle$, then the code C can be viewed as an R-module in R^ℓ ([9, Lemma 3.1]).

As in [9], assume the following factorization into irreducible polynomials in $\mathbb{F}_q[x]$

$$x^m - 1 = g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*, \tag{2.1}$$

where g_i's are self-reciprocal and h_j^* denotes the reciprocal of h_j. Let ξ be a primitive mth root of unity over $\mathbb{F}_q$. Assume that $g_i(\xi^{u_i}) = 0$ and $h_j(\xi^{v_j}) = 0$ (for all i, j). Then we also have $h_j^*(\xi^{-v_j}) = 0$. By the Chinese Remainder Theorem (CRT), R decomposes as

$$\left(\bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle g_i\rangle\right) \oplus \left(\bigoplus_{j=1}^{t}\Big(\mathbb{F}_q[x]/\langle h_j\rangle \oplus \mathbb{F}_q[x]/\langle h_j^*\rangle\Big)\right)$$
$$= \left(\bigoplus_{i=1}^{s} \mathbb{F}_q(\xi^{u_i})\right) \oplus \left(\bigoplus_{j=1}^{t}\Big(\mathbb{F}_q(\xi^{v_j}) \oplus \mathbb{F}_q(\xi^{-v_j})\Big)\right).$$