Finite Fields and Their Applications 47 (2017) 183–202

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Structure and performance of generalized quasi-cyclic codes

Cem Güneri [a,*], Ferruh Özbudak [c], Buket Özkaya [a], Elif Saçıkara [a], Zahra Sepasdar [d], Patrick Solé [b]

[a] *Sabancı University, Istanbul, Turkey*
[b] *CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France*
[c] *Middle East Technical University, Ankara, Turkey*
[d] *Department of Pure Mathematics, Ferdowsi University of Mashhad, Iran*

A R T I C L E I N F O

Article history:
Received 29 November 2016
Received in revised form 14 June 2017
Accepted 17 June 2017
Available online xxxx
Communicated by W. Cary Huffman

MSC:
94B60
94B65
11T71

Keywords:
GQC codes
QC codes
LCD codes
Self-dual codes

A B S T R A C T

Generalized quasi-cyclic (GQC) codes form a natural generalization of quasi-cyclic (QC) codes. They are viewed here as mixed alphabet codes over a family of ring alphabets. Decomposing these rings into local rings by the Chinese Remainder Theorem yields a decomposition of GQC codes into a sum of concatenated codes. This decomposition leads to a trace formula, a minimum distance bound, and to a criteria for the GQC code to be self-dual or to be linear complementary dual (LCD). Explicit long GQC codes that are LCD, but not QC, are exhibited.

* Corresponding author.
E-mail address: guneri@sabanciuniv.edu (C. Güneri).

http://dx.doi.org/10.1016/j.ffa.2017.06.005

1. Introduction

Quasi-cyclic codes (QC) have been known for more than fifty years. They have been shown to be asymptotically good, which is in marked contrast with the subclass of cyclic codes. Even in short length (less than a hundred) they contain more optimal codes than cyclic codes. Still, their structure is more complex than that of cyclic codes. A general approach to study QC codes is to decompose it into shorter component codes. A decomposition based on the Chinese Remainder Theorem (CRT) is given in [9], whereas a concatenated decomposition is provided in [8]. It has been observed that these two decompositions are essentially the same ([6]).

In recent years a super class of quasi cyclic codes has appeared: generalized quasi-cyclic codes ([5,13]). Up to coordinate permutation a QC code is equivalent to a linear code with block circulant generator matrix. More specifically, the circulant blocks will have the same size, namely the co-index m. The idea of Generalized Quasi-Cyclic (GQC) codes is to relax this requirement to allow blocks of different sizes. The immediate benefit is to construct codes whose lengths are not multiple of the index. For instance a GQC code might very well have prime length. The CRT decomposition has been extended to GQC codes at the price of a more complicated notation ([5]).

The aim of this paper is twofold. First, we aim to extend the structural theory of [9] to GQC codes, a program partially done in [5]. In particular the trace formula of [9] is extended to GQC codes. Concatenated description of GQC codes is presented and the results for QC codes in [6,8] are extended to GQC codes. Moreover, multilevel (generalized) concatenated description of GQC codes is obtained, which yields a minimum distance bound for GQC codes, extending Jensen's bound for QC codes. Let us note that there is a minimum distance bound on GQC codes due to Esmaeili and Yari ([5]) but it only applies to one generator GQC codes. Our bound applies to all GQC codes. Criteria for self-duality bearing on the component codes are given. In a recent paper [7], a similar criterion for a QC code to intersect its dual trivially (LCD code as Linear Complementary Dual) was derived. This criterion is generalized here to GQC codes.

Next, we study the asymptotic performance of GQC codes. Explicit long GQC codes that are LCD, but not QC, are exhibited. These codes have only finitely many distinct co-indices in the spirit of [11], but have a length going to infinity. The proof rests on the existence of families of good QC codes that are LCD [7].

The material is organized as follows. The next section collects the necessary definitions and notations. Section 3 develops the concatenated structure and a trace expression. Section 4 derives the minimum distance bound. Section 5 derives criteria for self-duality and LCDness. Asymptotic results are given in Section 6. Section 7 concludes the article and points out directions for future research.