

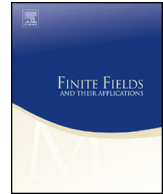


ELSEVIER

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On normalized generating sets for GQC codes over \mathbb{Z}_2 [☆]Sunghan Bae ^a, Pyung-Lyun Kang ^b, Chengju Li ^{c,*}^a Department of Mathematics, Korea Advanced Institute of Science and Technology, Daejeon, 34141, Republic of Korea^b Department of Mathematics, Chungnam National University, Daejeon, 34134, Republic of Korea^c Shanghai Key Laboratory of Trustworthy Computing, School of Computer Science and Software Engineering, East China Normal University, Shanghai, 200062, China

ARTICLE INFO

Article history:

Received 23 February 2016

Received in revised form 7 August 2016

Accepted 24 November 2016

Available online 11 January 2017

Communicated by Chaoping Xing

MSC:

94B05

94B15

11T71

13M99

Keywords:

Binary codes

Generalized quasi-cyclic codes

Dual codes

ABSTRACT

Let r_i be positive integers and $R_i = \mathbb{Z}_2[x]/\langle x^{r_i} - 1 \rangle$ for $1 \leq i \leq \ell$. Denote $\mathcal{R} = R_1 \times R_2 \times \cdots \times R_\ell$. Generalized quasi-cyclic (GQC) code \mathcal{C} of length $(r_1, r_2, \dots, r_\ell)$ over \mathbb{Z}_2 can be viewed as $\mathbb{Z}_2[x]$ -submodule of \mathcal{R} . In this paper, we investigate the algebraic structure of \mathcal{C} by presenting its normalized generating set. We also present a method to determine the normalized generating set of the dual code of \mathcal{C} , which is derived from the normalized generating set of \mathcal{C} .

© 2016 Elsevier Inc. All rights reserved.

[☆] The second author is supported by CNU research fund and the third author is supported by the NSFC-Zhejiang Joint Fund for the Integration of Industrialization and Informatization (No. U1509219) and the Fundamental Research Funds for the Central Universities (No. 56XZA15002).

* Corresponding author.

E-mail addresses: shbae@kaist.ac.kr (S. Bae), plkang@cmu.ac.kr (P.-L. Kang), lichengju1987@163.com (C. Li).

1. Introduction

Cyclic codes can be efficiently encoded using shift registers and have rich algebraic structures for efficient decoding, which explain their significant role in both the theory of error-correcting codes and engineering.

Classical cyclic codes of length n over a finite field \mathbb{F}_q , which can be viewed as ideals of $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$, were extensively investigated [10,11]. Codes over finite rings have been studied since the early 1970's. Hammons et al. [9] showed that certain good nonlinear binary codes can be constructed from cyclic codes over \mathbb{Z}_4 via Gray map. Since then, a lot of progresses on the study of codes over finite rings have been made [1,2,4,6,7]. As a generation of cyclic code, generalized quasi-cyclic (GQC) code and quasi-cyclic code over finite fields or finite rings have been studied [3,5,8,12–15] and employed to construct low-density parity-check codes.

Let \mathbb{Z}_2 be the ring of integers modulo 2, r_i positive integers, and $R_i = \mathbb{Z}_2[x]/\langle x^{r_i} - 1 \rangle$ for $1 \leq i \leq \ell$. Denote $\mathcal{R} = R_1 \times R_2 \times \cdots \times R_\ell$. A GQC code \mathcal{C} of length $(r_1, r_2, \dots, r_\ell)$ over \mathbb{Z}_2 can be viewed as a $\mathbb{Z}_2[x]$ -submodule of \mathcal{R} .

- It is well-known that \mathcal{C} is a binary cyclic code if $\ell = 1$.
- When $\ell = 2$, \mathcal{C} is called a \mathbb{Z}_2 -double cyclic code. The algebraic structures of \mathcal{C} and its dual code were presented in [3].
- When $\ell = 3$, \mathcal{C} is called a \mathbb{Z}_2 -triple cyclic code. The minimal generating set of \mathcal{C} and the relations between \mathcal{C} and its dual code were determined in some special cases [13].

Recently, Matsui [12] presented a complete theory of generator polynomial matrix of GQC code \mathcal{C} and a relation formula of the generator polynomial matrices between \mathcal{C} and \mathcal{C}^\perp , where \mathcal{C}^\perp is the dual code of \mathcal{C} . We refer the reader to [12] for more information on GQC code. In this paper, for any positive integer ℓ , we investigate the algebraic structure of GQC code \mathcal{C} by presenting its normalized generating set. We also present a method to determine the relationship between a normalized generating set of \mathcal{C} and that of \mathcal{C}^\perp . It will be seen that our method is more concrete because a normalized generating set of \mathcal{C}^\perp can be explicitly determined if a normalized generating set of \mathcal{C} is given.

The rest of this paper is organized as follows. In Section 2, we investigate the algebraic structure of the GQC code \mathcal{C} over \mathbb{Z}_2 . In Section 3, we present a method to determine a normalized generating set of \mathcal{C}^\perp , which is derived from a normalized generating set of \mathcal{C} . In Section 4, we conclude this paper.

2. GQC codes over \mathbb{Z}_2

Suppose that r_i are positive integers for $1 \leq i \leq \ell$. Let \mathcal{C} be a binary linear code of length $n = r_1 + r_2 + \cdots + r_\ell$. We call \mathcal{C} a GQC code of length $(r_1, r_2, \dots, r_\ell)$ over \mathbb{Z}_2 if

$$\mathbf{c} = (c_{1,0}, c_{1,1}, \dots, c_{1,r_1-1} | \cdots | c_{\ell,0}, c_{\ell,1}, \dots, c_{\ell,r_\ell-1}) \in \mathcal{C}$$

Download English Version:

<https://daneshyari.com/en/article/5771596>

Download Persian Version:

<https://daneshyari.com/article/5771596>

[Daneshyari.com](https://daneshyari.com)