Finite Fields and Their Applications 34 (2015) 280–304

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On generator and parity-check polynomial matrices of generalized quasi-cyclic codes

Hajime Matsui

Toyota Technological Institute, 2-12-1 Hisakata, Tempaku, Nagoya, Aichi 468-8511, Japan

A R T I C L E I N F O

Article history:
Received 6 August 2014
Received in revised form 27 December 2014
Accepted 12 February 2015
Available online 3 March 2015
Communicated by Xiang-dong Hou

MSC:
94B05
11T71
05E20

Keywords:
Error-correcting codes
Extended Euclidean algorithm
Bézout's identity
Automorphism group
Circulant matrix
Gröbner basis
Buchberger's algorithm

A B S T R A C T

Generalized quasi-cyclic (GQC) codes have been investigated as well as quasi-cyclic (QC) codes, e.g., on the construction of efficient low-density parity-check codes. While QC codes have the same length of cyclic intervals, GQC codes have different lengths of cyclic intervals. Similarly to QC codes, each GQC code can be described by an upper triangular generator polynomial matrix, from which the systematic encoder is constructed. In this paper, a complete theory of generator polynomial matrices of GQC codes, including a relation formula between generator polynomial matrices and parity-check polynomial matrices through their equations, is provided. This relation generalizes those of cyclic codes and QC codes. While the previous researches on GQC codes are mainly concerned with 1-generator case or linear algebraic approach, our argument covers the general case and shows the complete analogy of QC case. We do not use Gröbner basis theory explicitly in order that all arguments of this paper are self-contained. Numerical examples are attached to the dual procedure that extracts one from each other. Finally, we provide an efficient algorithm which calculates all generator polynomial matrices with given cyclic intervals.

E-mail address: matsui@toyota-ti.ac.jp.

http://dx.doi.org/10.1016/j.ffa.2015.02.003
1071-5797/© 2015 Elsevier Inc. All rights reserved.

1. Introduction

Many researches have been done on quasi-cyclic (QC) codes [3,4,14,16–19,25]. Classical cyclic codes including ubiquitous Reed–Solomon codes correspond to a special case of QC codes. Some class of low-density parity-check (LDPC) codes is investigated as QC codes [7,8,11,12,15].

Each QC code is characterized by its generator matrix or parity-check matrix which is a combination of circulant matrices with the same number of columns. Another way to represent QC codes is the use of polynomial matrices [14,26]. Each QC code has its own generator polynomial matrix, which is upper triangular, and its own parity-check polynomial matrix, which is lower triangular. These polynomial matrices of a QC code have polynomial entries with a fixed bound of degree.

On the other hand, a class of generalized quasi-cyclic (GQC) codes is also remarkable, in a sense that many efficient LDPC codes are not contained in QC codes but are contained in GQC codes [29,31]. A GQC code is equivalent to a linear code with a non-trivial automorphism group, where its cyclic subgroup is fixed [9]. Many of algebraic geometry codes, especially Hermitian codes, are GQC codes because these codes have non-trivial automorphisms [6,20,21]. A subclass of finite geometry codes, especially projective geometry codes, is not QC codes but GQC codes, and there are many high performance LDPC codes in GQC codes [13,29]. Thus, many researches have been also done for GQC codes recently [2,5,27].

GQC codes are usually discussed in terms of submodules over polynomial rings. The generator matrix and parity-check matrix of a GQC code viewed as a linear code can be represented by a combination of circulant matrices with different numbers of columns. Similarly to QC codes, a GQC code can also be represented by a polynomial matrix, which has polynomial entries with differently fixed bounds of degree in general. These properties of GQC codes are shown in [30], where their proofs require Gröbner basis theory on modules [1].

In this paper, we provide elementarily a complete theory of GQC codes. Background knowledge of this paper is required only on linear codes, cyclic codes, and basic polynomial arithmetic over finite fields. We show that each GQC code is described by a generator polynomial matrix $G = (g_{i,j})$ of the form

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{l,l} \end{pmatrix}, \tag{1}$$

namely, an $l \times l$ upper triangular polynomial matrix with $g_{i,j} \in \mathbb{F}_q[x]$, that satisfies the following equation, which is called the identical equation of G,

$$AG = \operatorname{diag}\left[x^{n_1} - 1, \ldots, x^{n_l} - 1\right], \tag{2}$$