DOCTORATE
THESIS MONITORING COMMITTEE PERIODIC EVALUATION REPORT

Student's	
Institute Registered	Graduate School of Natural and Applied Sciences
Department	Mathematics (English)
Program	PhD
Student ID Number	13565006
Full Name	Sümeyra BEDİR
TMC meeting place-date	03.11.2017
Periodic Evaluation Term	☐ May-June 20.. ☒ Nov-Dec 2017
Periodic Evaluation Number	☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5 ☐ 6 ☐ 7
THESIS TITLE	Vectorial Cyclic Codes And Their Structure
Does the content correspond to the Thesis proposal?	☐ YES ☐ NO
EVALUATION OF THE THESIS STUDY	☐ Successful ☐ Unsuccessful ☐ by unanimious votes ☐ by majority of votes

THESIS MONITORING COMMITTEE MEMBERS			
	Appellation, Full Name	Department/ University	Date-Signature
Thesis Advisor	Prof. Dr. Bayram Ali ERSOY	Department of Mathematics/ Yıldız Technical University	
Committee Member	Prof. Dr. A. Göksel AĞARGÜN	Department of Mathematics/ Yıldız Technical University	
Committee Member	Prof. Dr. Ünsal TEKİR	Department of Mathematics/ Marmara University	

Additional Document: Student's Report

NOTE: The thesis committee members who have additional personal remarks may specify them with a report.

ON GENERATOR AND PARITY-CHECK POLYNOMIAL MATRICES OF GENERALIZED QUASI-CONSTACYCLIC CODES

Sümeyra Bedir
Thesis Report-4

1 Introduction

This study is based on the following article;

- Matsui, H. "On Generator and Parity-check Polynomial Matrices of Generalized Quasi-cyclic Codes", Finite Fields and Their Applications 34 (2015):280-304.

In this work, 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. As the author noted; "Background knowledge of this paper is required only on linear codes, cyclic codes and basic polynomial arithmetic over finite fileds."

We extended this work to the constacyclic case, namely; we showed that the facts and the theory for the quasi-cyclic codes obtained from cyclic components, also hold for quasi-codes obtained from constacyclic components. We are trying to prove a similar fact for quasi-cyclic codes obtained from pseudo-cyclic components.

Matsui shows that each GQC code obtained from l cyclic components, can be described by an upper triangular generator matrix $G = (g_{i,j} \in F_q[x])$ of the form

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{l,l} \end{bmatrix}_{lxl}$$

which satisfies the identical equation of G;

$$AG = diag[x^{n_1} - 1, \ldots, x^{n_l} - 1]$$

where $A = (a_{i,j})$ is another upper triangular $l \times l$ polynomial matrix. This identical equation generalizes a cyclic code's $ag = x^n - 1$ for its generator polynomial g, to the quasi-cyclic case.

Further, he generalizes the well known fact $h = x^{\deg h} a(x^{-1})$ for the dual of a cyclic code to the dual of the quasi-cycic code obtained from cyclic components (GQC). He shows that the generator poynomial matrix for the dual GQC code (which is the parity-check polynomial matrix for the GQC code) can be calculated from the matrix A.

1.1 Definitions and Algorithms

1.1.1 Generator Polynomial Matrix of GQC Codes

Definition 1 *Let C be a GQC code, and let $G = (g_{i,j})$ be an lxl matrix whose entriees are in $F_q[x]$ and whose rows are codewords of C. If $g_{i,j} = 0$ for all $1 \leq i, j \leq l$ with $i > j$, namely, G is of the form*

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{l,l} \end{bmatrix}_{lxl}$$

*and moreover, for all $1 \leq i \leq l$, $g_{i,i}$ has the minimum degree among all codewords of the form $(0, \ldots, 0, c_i, \ldots, c_l) \in C$ with $c_i \neq 0$, then we call G a **generator polynomial matrix** of C.If $g_{i,i}$ is monic for all $1 \leq i \leq l$ and G satisfies $\deg g_{i,j} < \deg g_{j,j}$ for all $1 \leq i \neq j \leq l$, then we say that G is **reduced.***

1.1.2 Parity-check Polynomial Matrix of GQC Codes

Definition 2 *Let C be a GQC code, and let $H = (h_{i,j})$ be an lxl matrix whose entriees are in $F_q[x]$ and whose rows are codewords of $C^{\perp}$. If $h_{i,j} = 0$ for all $1 \leq i, j \leq l$ with $i < j$, namely, H is of the form*

$$H = \begin{bmatrix} h_{1,1} & 0 & \cdots & 0 \\ h_{2,1} & h_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ h_{l,1} & h_{l,2} & \cdots & h_{l,l} \end{bmatrix}_{lxl}$$

*and moreover, for all $1 \leq i \leq l$, $h_{i,i}$ has the minimum degree among all codewords of the form $(c_1, \ldots, c_i, 0, \ldots, 0) \in C^{\perp}$ with $c_i \neq 0$, then we call H a **parity-check polynomial matrix** of C.If $h_{i,i}$ is monic for all $1 \leq i \leq l$ and H satisfies $\deg h_{i,j} < \deg h_{j,j}$ for all $1 \leq i \neq j \leq l$, then we say that H is **reduced.***

For each GQC code, the reduced generator polynomial matrix is uniquely determined, and moreover, the reduced parity-check polynomial matrix is also uniquely determined. From any generator polynomial matrix and parity-check polynomial matrix, we can obtain the reduced ones by elementary row operations of polynomial matrices.

1.1.3 Buchberger's Algorithm for GQC Codes

The algorithm for obtaining the reduced generator polynomial matrix from a generator matrix G of a GQC code is described as follows;

We start with the polynomial representaion

$$G' = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,l} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ c_{k,1} & \cdots & 0 & c_{k,l} \end{bmatrix}_{kxl}$$

where $c_{i,j} \in F_q[x]$ for $1 \leq i \leq k$ and $1 \leq j \leq l$. Let c_i denote the i^{th} row of G' for $1 \leq i \leq k$. In this algorithm, the following manipulations of the polynomial matrix are carried out inductively.

1. If $c_{1,1} = \cdots = c_{k,1} = 0$, then set $c_1 = (x^{n_1} - 1, 0, \ldots, 0)$ and stop. If $c_{1,1} \neq 0$ and $c_{2,1} = \cdots = c_{k,1} = 0$, then stop.

2. By exchanging c_1 for another row of $c_2, \ldots c_k$ if it is required, we can assume that $c_{1,1}$ has the minimum degree among nonzero $c_{1,1}, \ldots c_{k,1}$.

3. Compute $p_i, r_i \in F_q[x]$ such that $c_{i,1} = p_i c_{1,1} + r_i$ with $\deg r_i < \deg c_{1,1}$ for all $2 \leq i \leq k$ and replace c_i with $c_i - p_i c_1$ for all $2 \leq i \leq k$, and go to step 1.

After the above manipulations, $c_1 = (c_{1,1}, \ldots, c_{1,l})$ is denoted by $g_1 = (g_{1,1}, \ldots, g_{1,l})$ and then we have $g_{1,1} = \gcd(c_{1,1}, \ldots, c_{k,1})$ from the initial matrix G'.

Now, G' is converted to;

$$G'' = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & c_{2,2} & \cdots & c_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & c_{k,2} & \cdots & c_{k,l} \end{bmatrix}_{kxl}$$

where $c_{i,j}$ in G'' is generally unequal to $c_{i,j}$ in G'.

Next, we apply the above manipulation to the submatrix;

$$\begin{bmatrix} c_{2,2} \cdots c_{2,l} \\ \ddots \ \ddots \ \vdots \\ c_{k,2} \cdots c_{k,l} \end{bmatrix}$$

and continuing recursively we obtian the reduced form G.

1.2 The Duality Theorem

As a consequence of the fact that upper triangular matrices over the quotient field of $F_q[x]$ form a group, the matrix A satisfying the equation

$$AG = diag[x^{n_1} - 1, \ldots, x^{n_l} - 1]$$

is also an upper triangular matrix.

The Duality Theorem

Theorem 3 *Let $G = (g_{i,j})$ be the reduced generator polynomial matrix of a GQC code C, and let A be the polynomial matrix which satisfies $AG = diag[x^{n_1}-1, \ldots, x^{n_l}-1]$. Then*

$$H = \begin{bmatrix} x^{\deg a_{1,1}} a_{1,1}^{<n_1>} & 0 & \cdots & 0 \\ x^{\deg a_{2,2}} a_{1,2}^{<n_1>} & x^{\deg a_{2,2}} a_{2,2}^{<n_2>} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ x^{\deg a_{l,l}} a_{1,l}^{<n_1>} & x^{\deg a_{l,l}} a_{2,1}^{<n_2>} & \cdots & x^{\deg a_{l,l}} a_{l,l}^{<n_l>} \end{bmatrix}_{lxl}$$

where each $a_{i,j}^{<\omega>}$ is the polynomial with coefficient vector as the first row of transpose of the circulant matrix obtained from $a_{i,j}$, and each column i of H is considered modulo $x^{n_i} - 1$.

2 Our Studies

2.1 Application of the Theory to the Constacyclic Case

The proof of the main theorem above was relying mainly on the well-known fact below;

$$x^{n_i} - 1 | x^N - 1 \iff n_i | N.$$

In order to make use of this fact in the consept of constacyclic codes we prove the following corollary;

Corollary 4 $x^{n_i}-\alpha_i|x^N-1$ *if and only if* $N=\operatorname{lcm}(n_1,\dots,n_l).\operatorname{lcm}(ord(\alpha_1),\dots,ord(\alpha_l))$, *where* $\alpha_i\in F_q$.

Proof. We have

$$\begin{aligned}
& (x^{n_i}-\alpha_i)(\alpha_i^{-1}+\alpha_i^{-2}x^{n_i}+\cdots+\alpha_i^{-ord(\alpha_i)}x^{n_i ord(\alpha_i)}) \\
= \; & x^{n_i ord(\alpha_i)}-1 \\
\Longleftrightarrow \; & (x^{n_i}-\alpha_i)|(x^{n_i ord(\alpha_i)}-1)\dots\dots\dots(*)
\end{aligned}$$

We also have

$$\begin{aligned}
& n_i ord(\alpha_i)|\operatorname{lcm}(n_1,\dots,n_l).\operatorname{lcm}(ord(\alpha_1),\dots,ord(\alpha_l)) \\
\Leftrightarrow \; & (x^{n_i ord(\alpha_i)}-1)|(x^{\operatorname{lcm}(n_1,\dots,n_l).\operatorname{lcm}(ord(\alpha_1),\dots,ord(\alpha_l))}-1)\dots.(**)
\end{aligned}$$

By $(*)$ and $(**)$,

$$\Longleftrightarrow x^{n_i}-\alpha_i|x^N-1$$

■

Another base concept to implement is the definition of $a_{i,j}^{<\omega>}$ and the modulo $x^\omega-1$ from the duality theorem.

The implementations should consider the fact that we use constacyclic shift instead of cyclic shift.

So we define $a_{i,j}^{<\omega>}$ as follows, for simplicity we denote $a_{i,j}$ simply by a.

Definition 5 *Let* $a\in F_q[x]$ *with* $\deg a<\omega$ *have the extended coefficient vector* $(a_0,a_1,\dots,a_{\omega-1})$. *The coefficient vector of* $a^{<\omega>}$ *is the first row of transpose of the* $\alpha^{-1}-twistulant$ *matrix of* a.

In this case; $\alpha^{-1}-twistulant$ *matrix of* a *is*

$$\begin{bmatrix}
a_0 & a_1 & \cdots & a_{\omega-1} \\
\alpha^{-1}a_{\omega-1} & a_0 & \cdots & a_{\omega-2} \\
\alpha^{-1}a_{\omega-2} & \alpha^{-1}a_{\omega-1} & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
\alpha^{-1}a_1 & \cdots & \alpha^{-1}a_{\omega-1} & a_0
\end{bmatrix}$$

so $a^{<\omega>}=a_0+\alpha^{-1}a_{\omega-1}x+\alpha^{-1}a_{\omega-2}x^2+\cdots+\alpha^{-1}a_1x^{\omega-1}$.

We also implemented the following fact to the constacyclic case;

$$AG=diag[x^{n_1}-1,\dots,x^{n_l}-1]$$

This time we should have

$$AG = diag[x^{n_1} - \alpha_1, \ldots, x^{n_l} - \alpha_l]$$

where each constacyclic component i, is $\alpha_i - constacyclic$.

When we look back at the parity-check matrix

$$H = \begin{bmatrix} x^{\deg a_{1,1}} a_{1,1}^{<n_1>} & 0 & \cdots & 0 \\ x^{\deg a_{2,2}} a_{1,2}^{<n_1>} & x^{\deg a_{2,2}} a_{2,2}^{<n_2>} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ x^{\deg a_{l,l}} a_{1,l}^{<n_1>} & x^{\deg a_{l,l}} a_{2,1}^{<n_2>} & \cdots & x^{\deg a_{l,l}} a_{l,l}^{<n_l>} \end{bmatrix}_{lxl}$$

the i^{th} column is considered modulo $x^{n_i} - 1$.

To implement this fact to the constacyclic case, we should be careful that we are talking about the dual code, so we consider each column i modulo $x^{n_i} - \alpha_i^{-1}$.

The Duality Theorem for Constacyclic Case

Theorem 6 *Let $G = (g_{i,j})$ be the reduced generator polynomial matrix of a generalized quazi constacyclic code C, and let A be the polynomial matrix which satisfies $AG = diag[x^{n_1} - \alpha_1, \ldots, x^{n_l} - \alpha_l]$. Then*

$$H = \begin{bmatrix} x^{\deg a_{1,1}} a_{1,1}^{<n_1>} & 0 & \cdots & 0 \\ x^{\deg a_{2,2}} a_{1,2}^{<n_1>} & x^{\deg a_{2,2}} a_{2,2}^{<n_2>} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ x^{\deg a_{l,l}} a_{1,l}^{<n_1>} & x^{\deg a_{l,l}} a_{2,1}^{<n_2>} & \cdots & x^{\deg a_{l,l}} a_{l,l}^{<n_l>} \end{bmatrix}_{lxl}$$

where each $a_{i,j}^{<\omega>}$ is the polynomial with coefficient vector as the first row of transpose of the $\alpha_i^{-1} - twistulant$ matrix obtained from $a_{i,j}$, and each column i of H is considered modulo $x^{n_i} - \alpha_i$.