Bull. Korean Math. Soc. **59** (2022), No. 6, pp. 1557–1565
https://doi.org/10.4134/BKMS.b210891
pISSN: 1015-8634 / eISSN: 2234-3016

GLIFT CODES OVER CHAIN RING AND NON-CHAIN RING $R_{e,s}$

Elif Segah Oztas

Abstract. In this paper, Glift codes, generalized lifted polynomials, matrices are introduced. The advantage of Glift code is "distance preserving" over the ring $\mathcal{R}$. Then optimal codes can be obtained over the rings by using Glift codes and lifted polynomials. Zero divisors are classified to satisfy "distance preserving" for codes over non-chain rings. Moreover, Glift codes apply on MDS codes and MDS codes are obtained over the ring $\mathcal{R}$ and the non-chain ring $\mathcal{R}_{e,s}$.

1. Introduction

Lifted polynomials were firstly introduced in [7]. In [7], lifted polynomials defined over F_{16} to generate reversible codes. And a version of the lifted polynomial (4^k-lifted polynomial) solves the DNA reversibility problem introduced in [7], by using double DNA bases over F_{16}. Moreover, these codes generated by lifted polynomials can satisfy that having optimal bound. Then, computational complexity to find optimal codes is shorted by using lifted polynomials. For example, let C be a code over F_{16} and its parameter is $[n, k, d]$. Computational steps or loops to get the generator matrix are approximately 15^{nk}. However, by using lifted polynomials, computational steps to obtain lifted polynomials are approximately 15^y where y is the number of non-zero coefficients of the polynomial. Lifted polynomials were extended to F_{256} in [8]. These polynomials and a kind of version of them help to obtain optimal code and solve the DNA reversibility problem by using DNA 4-bases. In literature, lifted polynomials are defined in limited structures that are limited by the degree of base polynomials ([7, 8]). For example, let $g(x) \in F_4[x]$ and $\deg g(x) = t$. The degree of the lifted form of the polynomial is also t. Definition of the lifted polynomial is different from some kind of lift operation named lifted code etc. in literature [4, 5]. In [1–3] they use a p-adic structure or finite fields for lift operation that are different from the method presented here.

Received December 9, 2021; Revised March 30, 2022; Accepted May 2, 2022.
2020 *Mathematics Subject Classification.* Primary 94B05, 94B60, 94B65.
Key words and phrases. Glift codes, lifted polynomials, lifted matrices, optimal codes, lifted MDS codes, distance preserving, zero divisor classification.

In this study, the degree of the general lifted form of the polynomial has extended as $t \leq n$ where n is the length of code. Glift codes are introduced that are generated by lifted polynomials and lifted matrices. Glift codes preserve the hamming distance over the ring after lifting operation because of the property of the ring $\mathcal{R}$ (chain-ring or that has one maximal ideal). Then some properties of codes are preserved as satisfying the Griesmer bound, become MDS code, distance, dimension, free rows of generator matrix, etc. When Glift codes are applied in the codes over a non-chain ring, the problem "distance preserving" has appeared. A form of lifted polynomials and classification of zero-divisors of the non-chain ring $\mathcal{R}_{e,s}$ are introduced to solve "distance preserving". Moreover, Glift codes also preserve the property of MDS codes over non-chain rings.

In Section 2, we give some background. In Section 3, the definitions of generalized lifted polynomials, lifted matrices and Glift codes are introduced. In Section 4, the special case of lifted polynomials, matrices are defined and the zero divisors are classified to solve the problem "distance preserving" of Glift codes over $\mathcal{R}_{e,s}$.

2. Background

In this section basic definition are given.

The following map is used for converting from polynomials to codewords (or word or vector) over a ring R.

For each word $(c_0, c_1, \ldots, c_{n-1}) \in R^n$, the polynomial $g(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ is associated and $c_i \in R$.

$$\Phi : R[x]/(x^n - 1) \to R^n$$
$$g(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \mapsto g = (c_0, c_1, \ldots, c_{n-1}).$$

Let $g(x) \in R[x]/(x^n - 1)$ and $\deg g(x) = t$. Spanning set for $g(x)$ is

$$S_g = \{g(x), xg(x), \ldots, x^{n-t-1}g(x)\}$$

over R. $\langle S_g \rangle$ is a set that generated by S_g.

$$\langle S_g \rangle = \{r_0 g(x) + r_1 x g(x) + \cdots + r_{n-t-1}x^{n-t-1}g(x)\},$$

where $r_i \in R$, $0 \leq i \leq n - t - 1$.

The Hamming distance $d(c', c'') = |\{0 \leq i \leq n-1 : c'_i \neq c''_i\}|$ for $c', c'' \in R^n$. Linear code over finite field F is a subvector space. In a ring R, a subset $C \subset R^n$ is a code with length of n. C is a linear code length of n over R if C is an R-submodule over R^n. If the rank of code C is equal to free rank, it is named as free R-submodule or free linear code over R.

3. Generalization of lifted polynomials, lifted matrices and glift codes

Let $\mathcal{R}$ be a ring (chain-ring or the ring that has one maximal ideal) that is generated by using finite field F. Then characteristics are equal as $char(\mathcal{R}) = char(F)$. Let $\mathbf{R}$ be an extension of a ring $\mathcal{R}$. Then $char(\mathcal{R}) = char(\mathbf{R})$.

Definition 1 (General lifted form of polynomials)**.** Let $g(x) = a_0 + a_1x + \cdots + a_tx^t \in \mathcal{R}[x]$ be a base polynomial for lifted forms, $\deg g(x) = t$ and designed length be n where $t \leq n$. General lifted form of $g(x)$ (or lifted polynomial of $g(x)$) over $\mathbf{R}$ for length n is

$$g^{\lambda}(x) = \sum_{i=0}^{n-1} \begin{cases} b_ix^i,\ b_i \in U_{\mathbf{R}}, & a_i \in U_{\mathcal{R}}, \\ b_ix^i,\ b_i \in Z_{\mathbf{R}}, & a_i \in Z_{\mathcal{R}}, \end{cases}$$

where $U_{\mathbf{R}}$ is a set of units in $\mathbf{R}$, $Z_{\mathbf{R}}$ is a set of zero and zero divisors in $\mathbf{R}$ and $g^{\lambda}(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$.

Definition 2. Let $g(x)$ be a polynomial over a ring. Weight of unit term is defined as $W_u(g(x)) =$ number of coefficients that are unit. Weight of zero and zero divisor term is defined as $W_z(g(x)) =$ number of coefficients that are zero or zero divisor. And $W_u(g(x)) + W_z(g(x)) = \deg g(x) + 1$.

Example 3.1. Let $g(x) = 1 + 3x + 4x^3 + 2x^5 \in \mathbb{Z}_8[x]$. Then, $g(x) = 1 + 3x + 0x^2 + 4x^3 + 0x^4 + 2x^5$. $W_u(g(x)) = 2$ and $W_z(g(x)) = 4$.

Number of lifted polynomials from $\mathcal{R}$ to $\mathbf{R}$ for one base polynomial $g(x)$ is $N_{\lambda} = |U_{\mathbf{R}}|^{W_u(g(x))} \cdot |Z_{\mathbf{R}}|^{W_z(g(x))+n-\deg g(x)-1}$.

Example 3.2. Let $g(x) = (1 + u) + x^3$ be a base polynomial for lifting from $\mathcal{R}_1 = F_2[u]/\langle u^2\rangle$ to $\mathbf{R}_1 = F_4[u, v]/\langle u^2, v^2\rangle$ and let 6 be designed length. Some of lifted polynomials over $\mathbf{R}_1$ are as follows:

- $g_1^{\lambda}(x) = 1 + v + (1 + u)x^3 + ux^4$
- $g_2^{\lambda}(x) = 1 + v + (1 + u)x^3 + ux^4 + uvx^5$
- $g_3^{\lambda}(x) = 1 + uvx + (1 + u)(1 + v)x^3 + +vx^5$
- $g_4^{\lambda}(x) = 1 + ux + vx^2 + x^3 + uvx^4 + vx^5$

Definition 3. Let $g^{\lambda}(x)$ be a lifted polynomial of $g(x)$ from $\mathcal{R}$ to $\mathbf{R}$, $\deg g(x) = t$ and length is n. Lifted spanning set of $g^{\lambda}(x)$ is

$$S_{g^{\lambda}} = \{g^{\lambda}(x), xg^{\lambda}(x), \ldots, x^{n-t-1}g^{\lambda}(x)\}.$$

A lot of lifted polynomials can be generated by using a base polynomial according to Definition 1.

Then, the lifted spanning set can be extended as following definition.

Definition 4. Let $\mathcal{L}_g = \{g_j^{\lambda}(x) : 0 < j \leq N_{\lambda}\}$ be a family of lifted polynomials of $g(x)$ from $\mathcal{R}$ to $\mathbf{R}$, $\deg g(x) = t$ and length is n. General lifted spanning set is

$$GS_{g^{\lambda}} = \{g_{h_0}, xg_{h_1}, x^2g_{h_2}, \ldots, x^{n-t-1}g_{h_{n-t-1}}\},$$

where $g_{h_i} \in \mathcal{L}_g$ ($h_i \in \{1, \ldots, N_\lambda\}$).

Example 3.3. Let $g(x) = 1 + u + x^3$ be a base polynomial for lifting from $\mathcal{R}_1 = F_2[u]/\langle u^2\rangle$ to $\mathbf{R}_1 = F_4[u, v]/\langle u^2, v^2\rangle$ and let 6 be designed length. Let choose some of lifted polynomials over $\mathbf{R}_1$ as follows:

- $g_0^\lambda(x) = 1 + v + (1 + u)x^3 + ux^4$
- $g_1^\lambda(x) = 1 + v + (1 + u)x^3 + ux^4 + uvx^5$
- $g_2^\lambda(x) = 1 + uvx + (1 + u)(1 + v)x^3 + +vx^5$

General lifted spanning set is

$$GS_{g^\lambda} = \{g_0, xg_1, x^2g_2\}.$$

Definition 5. Let G be a generator matrix of code C over $\mathcal{R}$. Let components of G be shown as (a_{ij}). Lifted generator matrix is $G_\lambda = (b_{ij})$

$$(b_{ij}) = \begin{cases} b_{ij} \in U_{\mathbf{R}}, & a_{ij} \in U_{\mathcal{R}}, \\ b_{ij} \in Z_{\mathbf{R}}, & a_{ij} \in Z_{\mathcal{R}}, \end{cases}$$

over $\mathbf{R}$.

Example 3.4. Let $G = \left[\begin{smallmatrix} 1 & 0 & u \\ 0 & 1 & u+1 \end{smallmatrix}\right]$ be a generator matrix for lifting from $\mathcal{R}_1 = F_2[u]/\langle u^2\rangle$ to $\mathbf{R}_1 = F_4[x]/\langle u^2, v^2\rangle$. A lifted generator matrix over $\mathbf{R}_1$ is $G_\lambda = \left[\begin{smallmatrix} v+1 & u & uv \\ u(v+1) & (u+1)(v+1) & 1 \end{smallmatrix}\right]$.

Definition 6. Let C be a code generated by S_{g^λ}, GS_{g^λ} or G_λ over $\mathbf{R}$. $C = \langle S_{g^\lambda}\rangle$ ($C = \langle GS_g^\lambda\rangle$ or $C = \langle G_\lambda\rangle$) is called as Glift code.

Theorem 3.5. *Let C be an $[n, k, d]$ code over F and generated by generator matrix G. Then $C' = \langle G_\lambda\rangle$ is an $[n, k, d]_{\mathcal{R}}$ Glift code over $\mathcal{R}$ and C' is also a linear free code over $\mathcal{R}$.*

Proof. If G is linearly independent, then the set G_λ is also linearly independent and generates a free code according to Definition 5. □

Theorem 3.6. *Let $g(x)$ be a base polynomial for the lifted polynomials from a finite field F to $\mathcal{R}$ and $char(\mathcal{R}) = char(F)$. Let elements of S_g be linear independent and $|S_g| = k$. Then $C' = \langle S_{g^\lambda}\rangle$ and $C'' = \langle GS_{g^\lambda}\rangle$ are $[n, k, d]_{\mathcal{R}}$ Glift codes over $\mathcal{R}$ if $C = \langle S_g\rangle$ is an $[n, k, d]$ linear code over F. Moreover, C' and C'' are free linear codes over $\mathcal{R}$.*

Proof. Note that d is created by coefficient of $g(x)$ and all coefficients are elements of F when $C = \langle S_g\rangle$ is an $[n, k, d]$ linear code over F. Let $g^\lambda(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ be a lifted polynomial over $\mathcal{R}$. According to Definition 1, some coefficients of $g^\lambda(x)$ are zero divisors. An element that exists in maximal ideal, can annihilate all zero divisors over $\mathcal{R}$. The units of $\mathcal{R}$ are not affected by these multiplication operators and do not become a zero. And elements of S_g are linearly independent then the set S_{g^λ} is also linearly independent and generates a free linear code according to Definition 1. As a result, hamming distance is preserved over $\mathcal{R}$ by using Glift code and lifted polynomials. □

Theorem 3.5 and Theorem 3.6 satisfy the preserving the distance by using Glift codes. Glift code is also suitable for lifting all linear code, the cyclic codes and MDS codes because the structure of Glift code and these codes have determined dimensions. Become MDS code is preserved over the ring because Glift codes preserve the dimension and distance. Protecting "the become cyclic code" is still an open problem.

Corollary 3.7. *Let $g(x)$ be a base polynomial for the lifted polynomials from a finite field F to $\mathcal{R}$, $char(\mathcal{R}) = char(F)$ and $g(x) \mid (x^n - 1)$ over F. Then $C' = \langle S_{g^\lambda} \rangle$ and $C'' = \langle GS_{g^\lambda} \rangle$ are $[n, k, d]_{\mathcal{R}}$ Glift codes over $\mathcal{R}$ and $C = \langle g(x) \rangle$ is an $[n, k, d]$ cyclic code over F. Moreover, C' and C'' are free linear codes over $\mathcal{R}$.*

Example 3.8. Let $g(x) = 1 + x + x^3 \mid x^7 - 1$ be a polynomial over F_2 and $S_g = \{g(x), xg(x), x^2g(x), x^3g(x)\}$. Then $C = \langle S \rangle$ is a $[7, 4, 3]_{F_2}$ cyclic code over F_2. Let lifted polynomial of $g(x)$ be $g^\lambda = 1 + (1 + u)x + ux^2 + x^3 + ux^5$ and $S_{g^\lambda} = \{g^\lambda(x), xg^\lambda(x), x^2g^\lambda(x), x^3g^\lambda(x)\}$. Then $\mathcal{C} = \langle S_{g^\lambda} \rangle$ is a $[7, 4, 3]_{\mathcal{R}_1}$ Glift code and it is also a free linear code over $\mathcal{R}_1 = F_2[u]/\langle u^2 \rangle$. Moreover, $\mathcal{C}$ satisfies the Griesmer bound over rings [9].

Corollary 3.9. *Let C be an $[n, k, d]$ MDS code over F and generated by generator matrix G. Then C' is an $[n, k, d]_{\mathcal{R}}$ Glift code over $\mathcal{R}$ and $C' = \langle G_\lambda \rangle$. Moreover, C' is also an MDS code over $\mathcal{R}$ because it is a free linear code.*

4. Glift codes over non-chain ring $\mathcal{R}_{e,s}$

In [6], the non-cain ring $R_{k,s} = \mathbb{F}_{4^{2k}}[u_1, \ldots, u_s]/\langle u_1^2 - u_1, \ldots, u_s^2 - u_s \rangle$ are introduced, decomposed and the elements are generated by using idempotents. Moreover a method to find the idempotents is introduced in [6]. In this section, the ring $\mathcal{R}_{e,s} = \mathbb{F}_{2^e}[u_1, \ldots, u_s]/\langle u_1^2 - u_1, \ldots, u_s^2 - u_s \rangle$ is considered. The method for finding idempotents in $\mathcal{R}_{e,s}$ is the same as that for finding them in $R_{k,s}$ in [6] because the rings have same characteristic.

The Glift codes are generated by lifted polynomials or lifted matrices as seen in Section 3. In Glift codes that are lifted from a finite field to a chain ring, determining the distance is satisfied by one maximal ideal of chain ring. In a non-chain ring, this is not possible to determine the distance over the non-chain ring by using Glift codes with a lifted polynomial. In this section, classifying of zero divisors, z-lifted polynomials, and z-lifted matrices are introduced to solve the problem of protecting the distance over $\mathcal{R}_{e,s}$.

Theorem 4.1. *Let $I = \{I_i\}$ be a set of 2^s elements of $\mathcal{R}_{e,s}$, where I_i is idempotent and $0 \le i \le 2^s - 1$. If*

(i) $I_i^2 = I_i$,

(ii) $I_iI_j = 0$ *for* $i \neq j$ *and* $0 \le i, j \le 2^s - 1$,

(iii) $\sum_{i=0}^{2^s-1} I_i = 1$,

then $\mathcal{R}_{e,s} = I_0\mathbb{F}_{2^e} \oplus I_1\mathbb{F}_{2^e} \oplus \cdots \oplus I_{2^s-1}\mathbb{F}_{2^e}$.

Theorem 4.2. *Let $E = \{0, 1, \ldots, 2^s-1\}$. In $\mathcal{R}_{e,s}$, zero divisors of class $T \subset E$ is*

$$Z(T) = \{\sum_{i\in D} a_i I_i \mid a_i \in F_{2^e}, D = E \setminus T, T \neq \emptyset\} \setminus \{0\},$$

where I_i is an idempotent element of $\mathcal{R}_{e,s}$.

Proof. All elements of sets of $Z(T)$ can be annihilated as the following set

$$Ann_{\mathcal{R}_{e,s}}(Z(T)) = \bigcup_{T'\in\mathcal{P}(T)\setminus\{\emptyset\}} Z(T'),$$

where a $T \neq \emptyset$ and $\mathcal{P}$ shows the power set. Then the defined set $Z(T)$ includes the zero divisors. □

Example 4.3. The idempotent set I for the ring $\mathcal{R}_{4,3} = F_{16}[u_1, u_2, u_3]/\langle u_1^2 - u_1, u_2^2 - u_2, u_3^2 - u_3\rangle$ is

$$\begin{aligned}
I_0 &= u_1u_2u_3,\\
I_1 &= (u_1+1)u_2u_3,\\
I_2 &= u_1(u_2+1)u_3,\\
I_3 &= u_1u_2(u_3+1),\\
I_4 &= (u_1+1)(u_2+1)u_3,\\
I_5 &= (u_1+1)u_2(u_3+1),\\
I_6 &= u_1(u_2+1)(u_3+1),\\
I_7 &= (u_1+1)(u_2+1)(u_3+1),
\end{aligned}$$

given in Example 2 in [6]. Elements of $\mathcal{R}_{4,3}$ are defined as $a_0I_0 + a_1I_1 + a_2I_2 + a_3I_3 + a_4I_4 + a_5I_5 + a_6I_6 + a_7I_7$ where $a_i \in F_{16}$ and $0 \le i \le 7$. Some sets of zero divisors are listed as follows:

class T	$Z(T)$
$T = \{0\}$	$Z(\{0\}) = Z(T) = \{a_1I_1 + a_2I_2 + a_3I_3 + a_4I_4 + a_5I_5 + a_6I_6 + a_7I_7 \mid a_i \in F_{16}$ and $0 \le i \le 7\}$
$T = \{0,1\}$	$Z(\{0,1\}) = \{a_2I_2 + a_3I_3 + a_4I_4 + a_5I_5 + a_6I_6 + a_7I_7 \mid a_i \in F_{16}$ and $0 \le i \le 7\}$
$T = \{2\}$	$Z(\{2\}) = \{a_0I_0 + a_1I_1 + a_3I_3 + a_4I_4 + a_5I_5 + a_6I_6 + a_7I_7 \mid a_i \in F_{16}$ and $0 \le i \le 7\}$
$T = \{0,1,3,5,7\}$	$Z(T) = \{a_2I_2 + a_4I_4 + a_6I_6 \mid a_i \in F_{16}$ and $0 \le i \le 7\}$

Number of zero divisors of set $Z(T) = \{a_2I_2 + a_4I_4 + a_6I_6\}$ is $16^3 - 1$ where $T = \{0, 1, 3, 5, 7\}$.

Definition 7. Let $g(x) = a_0 + a_1x + \cdots + a_tx^t \in F_{2^e}[x]$ be a base polynomial for lifted forms, $\deg g(x) = t$ and designed length be n where $t \le n$. A z-lifted form (z-lifted polynomial) of $g(x)$ over $\mathcal{R}_{e,s}$ for length n is

$$g^{Z(T)\lambda}(x) = \sum_{i=0}^{n-1} \begin{cases} b_i x^i,\ b_i \in U_{\mathcal{R}_{e,s}}, & a_i \neq 0, \\ b_i x^i,\ b_i \in Z(T) \text{ or } b_i = 0, & a_i = 0, \end{cases}$$

where $U_{\mathcal{R}_{e,s}}$ is a set of units in $\mathcal{R}_{e,s}$, and $Z(T)$ is a set of zero divisors of class T in $\mathcal{R}_{e,s}$ and $g^{Z(T)\lambda}(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$.

Definition 8. Let G be a generator matrix of code C over F_{2^e}. Let components of G be shown as (a_{ij}). A z-lifted generator matrix is $G_{Z(T)\lambda} = (b_{ij})$:

$$(b_{ij}) = \begin{cases} b_{ij} \in U_{\mathcal{R}_{e,s}}, & a_{ij} \neq 0, \\ b_{ij} \in Z(T_i) \text{ or } b_i = 0, & a_{ij} = 0, \end{cases}$$

where $U_{\mathcal{R}_{e,s}}$ is a set of units in $\mathcal{R}_{e,s}$, and $Z(T_i)$ is a set of zero divisors of class T in $\mathcal{R}_{e,s}$.

According to Definition 8, all zero in same row have to lift zero divisors that are in same class of zero divisor $Z(T_i)$.

Theorem 4.4. *Let $\alpha = \alpha_0 I_0 + \alpha_1 I_1 + \cdots + \alpha_{2^s-1} I_{2^s-1} \in \mathcal{R}_{e,s}$ where $\alpha_i \in F_{2^e}$ and I_i $(i \in \{1, \ldots, 2^s - 1\})$ is an idempotent, and let $g^{Z(T)\lambda}$ be a z-lifted polynomial of $g(x)$ over $\mathcal{R}_{e,s}$ where $g(x) \in F_{2^e}[x]$. Then $C' = \langle GS_{g^{Z(T)\lambda}} \rangle$ is an $[n,k,d]_{\mathcal{R}_{e,s}}$ Glift code over $\mathcal{R}_{e,s}$ if $C = \langle S_g \rangle$ is an $[n,k,d]$ linear code over F_{2^e}. Moreover, C' is a free linear code over $\mathcal{R}$.*

Proof. There is no one element of a maximal ideal that makes zero by multiplying all elements. Then all zero divisors are classified and the definition of special lifted polynomial as a z-lifted polynomial is introduced in Definition 7. d is preserved over the ring $\mathcal{R}_{e,s}$, because, according to Definition 7. Then all annihilators for zero divisor among coefficients are separated and classified by using Theorem 4.2. □

We have:

Corollary 4.5. *$C' = \langle GS_{g^{Z(T)\lambda}} \rangle$ is an $[n,k,d]_{\mathcal{R}_{e,s}}$ Glift code and MDS code over $\mathcal{R}_{e,s}$ if $C = \langle S_g \rangle$ is an MDS $[n,k,d]$ linear code over F_{2^e}.*

Theorem 4.6. *Let $\alpha = \alpha_0 I_0 + \alpha_1 I_1 + \cdots + \alpha_{2^s-1} I_{2^s-1} \in \mathcal{R}_{e,s}$ where $\alpha_i \in F_{2^e}$ and I_i $(i \in \{1, \ldots, 2^s - 1\})$ is an idempotent, and let $G_{Z(T)\lambda}$ be a z-lifted generator matrix of G over $\mathcal{R}_{e,s}$ where G is a generator matrix of a code C over F_{2^e}. Then $C' = \langle G_{Z(T)\lambda} \rangle$ (zeros of each row of $G_{Z(T)\lambda}$ can be included in different $Z(T)$ class) is an $[n,k,d]_{\mathcal{R}_{e,s}}$ Glift code over $\mathcal{R}_{e,s}$ if $C = \langle G \rangle$ is an $[n,k,d]$ linear code over F_{2^e}. Moreover, C' is a linear free code over $\mathcal{R}_{e,s}$.*

Proof of Theorem 4.6 is similar as that of Theorem 4.4.

We have:

Corollary 4.7. *$C' = \langle G_{Z(T)\lambda} \rangle$ is an $[n,k,d]_{\mathcal{R}_{e,s}}$ Glift code and MDS code over $\mathcal{R}$ if $C = \langle G_\lambda \rangle$ is an MDS $[n,k,d]$ linear code over F_{2^e}.*

Example 4.8. Let G be a generator matrix of code C over F_8:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & w^3 & w^4 & w^6 & w^4 & w^3 \\ 0 & 1 & 0 & w^3 & w^2 & w & w & w^2 & w^3 \\ 0 & 0 & 1 & w^3 & w^4 & w^6 & w^4 & w^3 & 1 \end{bmatrix}$$

Then C is a $[9,3,7]_{F_8}$ MDS code.

The idempotent set I for the ring $\mathcal{R}_{3,2} = F_8[u_1,u_2]/\langle u_1^2 - u_1, u_2^2 - u_2\rangle$ is

$$\begin{aligned} I_0 &= u_1u_2, \\ I_1 &= (u_1+1)u_2, \\ I_2 &= u_1(u_2+1), \\ I_3 &= (u_1+1)(u_2+1). \end{aligned}$$

Let $Z(T_1) = \{a_1I_1 + a_3I_3 \mid a_1, a_3 \in F_8\}$ where $T_1 = \{0,2\}$ and $Z(T_2) = \{a_0I_0 + a_1I_1 \mid a_0, a_1 \in F_8\}$ where $T_2 = \{2,3\}$. Let us choose

$$G_{Z(T)\lambda} = \begin{bmatrix} 1 & wI_1 & w^4I_1 + w^2I_3 & 1 & w^3 & w^4 & w^6 & w^4 & w^3 \\ 0 & I_0 + I_1 + I_2 + I_3 & I_1 & w^3 & w^2 & w & w & w^2 & w^3 \\ 0 & I_0 + w^5I_1 & 1 & w^3 & w^4 & A & w^4 & w^3 & 1 \end{bmatrix}$$

(where $A = w^6I_0 + w^4I_1 + I_2 + I_3$) where zero components of $G_{Z(T)\lambda}[1]$ that is the first row of $G_{Z(T)\lambda}$ are chosen from $Z(T_1)$, other zero component are chosen from $Z(T_2)$. These choosing operations are applied according to Definition 8. An important point that is all zeros of a row should be chosen from the same $Z(T)$. Then, $C' = \langle G_{Z(T)\lambda}\rangle$ is a $[9,3,7]_{\mathcal{R}_{3,2}}$ Glift code and MDS code over non-chain ring $\mathcal{R}_{3,2}$.

5. Conclusion

In this study, generalized lifted polynomials, lifted matrices are introduced over the rings. Also, Glift codes are introduced over $\mathcal{R}$. Glift codes use lifted polynomials and lifted matrices to generate free linear codes over $\mathcal{R}$. Hamming distance is preserved by Glift codes over $\mathcal{R}$. Then, it helps to generate optimal codes that satisfy Griesmer bound over the ring $\mathcal{R}$. However, Glift codes generated by lifted polynomials or lifted matrices can't preserve the distance over non-chain ring $\mathcal{R}_{e,s}$. Zero divisors of $\mathcal{R}_{e,s}$ are classified and z-lifted polynomials, z-lifted matrices are introduced to use in Glift codes. Then, "distance preserving" is solved by Glift codes generated by z-lifted polynomials, z-lifted matrices.

References

[1] R. L. Bouzara, K. Guenda, and E. Martinez-Moro, *Lifted codes and lattices from codes over finite chain rings*, arXiv:2007.05871.

[2] S. T. Dougherty, S. Y. Kim, and Y. H. Park, *Lifted codes and their weight enumerators*, Discrete Math. **305** (2005), no. 1-3, 123–135. https://doi.org/10.1016/j.disc.2005.08.004

[3] S. T. Dougherty, H. Liu, and Y. H. Park, *Lifted codes over finite chain rings*, Math. J. Okayama Univ. **53** (2011), 39–53.

[4] A. Guo and S. Kopparty, *List-decoding algorithms for lifted codes*, IEEE Trans. Inform. Theory **62** (2016), no. 5, 2719–2725. https://doi.org/10.1109/TIT.2016.2538766

[5] A. Guo, S. Kopparty, and M. Sudan, *New affine-invariant codes from lifting*, in ITCS'13—Proceedings of the 2013 ACM Conference on Innovations in Theoretical Computer Science, 529–539, ACM, New York, 2013.

[6] F. Gursoy, E. S. Oztas, and Bahattin Yildiz, *Reversible DNA codes over a family of non-chain rings* $R_{k,s}$, arXiv:1711.02385.

[7] E. S. Oztas and I. Siap, *Lifted polynomials over* F_{16} *and their applications to DNA codes*, Filomat **27** (2013), no. 3, 459–466. https://doi.org/10.2298/FIL1303459O

[8] E. S. Oztas and I. Siap, *On a generalization of lifted polynomials over finite fields and their applications to DNA codes*, Int. J. Comput. Math. **92** (2015), no. 9, 1976–1988. https://doi.org/10.1080/00207160.2014.930449

[9] K. Shiromoto and L. Storme, *A Griesmer bound for linear codes over finite quasi-Frobenius rings*, Discrete Appl. Math. **128** (2003), no. 1, 263–274. https://doi.org/10.1016/S0166-218X(02)00450-X

Elif Segah Oztas
Department of Mathematics
Karamanoglu Mehmetbey University
Karaman, Turkey
Email address: elifsegahoztas@gmail.com