mathematics

Article

Construction of Quantum Codes over the Class of Commutative Rings and Their Applications to DNA Codes

Shakir Ali [1,*], Amal S. Alali [2], Elif Segah Oztas [3] and Pushpendra Sharma [1]

[1] Department of Mathematics, Faculty of Science, Aligarh Muslim University, Aligarh 202002, India
[2] Department of Mathematical Sciences, College of Science, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[3] Department of Mathematics, Kamil Ozdag Science Faculty, Karamanoglu Mehmetbey University, Karaman 70100, Türkiye
* Correspondence: shakir.ali.mm@amu.ac.in or drshakir1971@gmail.com

Abstract: Let k, m be positive integers and $\mathbb{F}_{2^m}$ be a finite field of order 2^m of characteristic 2. The primary goal of this paper is to study the structural properties of cyclic codes over the ring $S_k = \frac{\mathbb{F}_{2^m}[v_1,v_2,\ldots,v_k]}{\langle v_i^2-\alpha_i v_i, v_i v_j - v_j v_i\rangle}$, for $i, j = 1, 2, 3, \ldots, k$, where α_i is the non-zero element of $\mathbb{F}_{2^m}$. As an application, we obtain better quantum error correcting codes over the ring S_1 (for $k = 1$). Moreover, we acquire optimal linear codes with the help of the Gray image of cyclic codes. Finally, we present methods for reversible DNA codes.

Keywords: Kronecker product; cyclic codes; Gray map; quantum codes; DNA codes

MSC: 94B05; 94B15; 94B60; 92D20; 17D92

check for updates

Citation: Ali, S.; Alali, A.S.; Oztas, E.S.; Sharma, P. Construction of Quantum Codes over the Class of Commutative Rings and Their Applications to DNA Codes. *Mathematics* **2023**, *11*, 1430. https://doi.org/10.3390/math11061430

Academic Editors: Alexei Kanel-Belov and Alexei Semenov

Received: 16 February 2023
Revised: 8 March 2023
Accepted: 9 March 2023
Published: 15 March 2023

1. Introduction

Quantum codes are used in both quantum computing and quantum communication in order to protect the information from channel noise that may occur during transmission. From that point, the development of classical cyclic codes into quantum error-correcting codes and their generalizations began to accelerate. Shor [1] initially developed quantum-error-correcting codes in 1995. Steane [2] developed the structural features of straightforward quantum-error-correcting codes a year later, in 1996. After two years, Calderbank et al. [3] developed a revolutionary method for constructing quantum-error-correcting codes from classical-error-correcting codes. Many effective quantum errors correcting codes with dual or self-orthogonal contained properties have been constructed using classical cyclic codes over the finite field $\mathbb{F}_q$. Using cyclic codes of odd length, Qian [4] constructed quantum error correcting codes for the first time on the finite non-chain ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$. Later, a great deal of study was conducted on quantum codes that were constructed from cyclic codes, constacyclic codes, and skew constacyclic codes over a non-chain ring with odd characteristics (see for references [5–8]). In 2014, Cengellenmis et al. [9] provided the structure of codes over the ring $\frac{\mathbb{F}_2[v_1,v_2,\ldots,v_k]}{\langle v_i^2=v_i, v_i v_j = v_j v_i\rangle}$ by using a Gray map. After that in 2018, Zheng et al. [10] gave the generator polynomial of constacyclic codes over the ring $\frac{\mathbb{F}_{p^m}[u_1,u_2,\ldots,u_k]}{\langle u_i^2=u_i, u_i u_j = u_j u_i\rangle}$ and also provided the structural properties of linear codes over this ring. Additionally, several quantum codes with even characteristics were constructed over the finite ring (see for references [11–13]). Over a finite non-chain ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ with $u^2 = u$, Islam and Prakash [14] recently obtained some new quantum and LCD codes. This inspires us to explore the properties of cyclic codes over a ring $S_k = \frac{\mathbb{F}_{2^m}[v_1,v_2,\ldots,v_k]}{\langle v_i^2-\alpha_i v_i, v_i v_j - v_j v_i\rangle}$, for $i, j = 1, 2, 3, \ldots, k$, where α_i is the non-zero elements of $\mathbb{F}_{2^m}$. In [15], Adleman calculated the NP-complete problem in the test tube in the 1990s. This experiment encouraged me to start heavily the studies that are the union of mathematics and DNA strings. DNA strings had to have a proper distance (difference) between them to prevent wrong connections in Aldeman's experiment. Then researchers found a proper connection to solve this problem by using error correction codes. The main idea for the solution is generating reversible complement DNA codes with proper distance. Firstly, methods of generating reversible DNA codes were given by [16–18]. Because the side of complement is easier than creating the reversible DNA codes. In [19], double DNA bases are used, but they delete half of the DNA double base of each element in the code. Thus, they do not use double DNA bases in DNA codes. If the algebraic structure has four elements then reversible codes can map to DNA codes directly. Because, the number of DNA bases is four which are (A) adenine, (G) guanine, (T) thymine, and (C) cytosine. However, if an algebraic structure has more than four elements, the reversibility problem arises. The first use of double DNA bases in DNA codes was presented by [20]. Moreover, the reversibility problem was presented and solved in [20]. The reversibility problem can be explained in algebraic structures that have more than four elements. In the algebraic structure, each element corresponds to DNA multiple bases. For example, Let us consider a ring R and $|R| = 16$. Each element corresponds to DNA double bases (or 2 bases). Let $(a,b,c)\ inR^3$ correspond to (AT,GT,CA) $(ATGTCA)$. Reverse of (a,b,c) is $(a,b,c)^r = (c,b,a)$. Furthermore, (c,b,a) corresponds (CA,GT,AT). However, the reverse of (AT,GT,CA) cannot correspond to the (CA,GT,AT). Reverse of (AT,GT,CA) is (AC,TG,TA). In short, the reversibility problem is that we can not obtain the reverse of DNA correspondence by using the reverse of a vector.

In this work, we explore the structural properties of cyclic codes over the ring $S_k = \frac{\mathbb{F}_{2^m}[v_1,v_2,\ldots,v_k]}{\langle v_i^2-\alpha_i v_i, v_iv_j-v_jv_i\rangle}$ and introduce methods to solve the reversibility problem over $\mathbb{S}_k^t = \frac{\mathbb{F}_{4^{2t}}[v_1,v_2,\ldots,v_k]}{\langle v_i^2-v_i, v_iv_j-v_jv_i\rangle}$. First, we create a technique to create the idempotents of $\mathbb{S}_k^t$ by using a binary numeral system. Thus, we can arrange the idempotents to solve the reversibility problem with DNA correspondence tables over F_4^{2t}. After that, we present the methods to generate reversible and reversible DNA codes. The methods enable us to create DNA codes that do not need to be cyclic codes or skew cyclic codes over $\mathbb{S}_k^t$. This design satisfies to generate more DNA codes by using one source polynomial. This is important for real DNA strings to correspond to the codes. In [21], They found some codewords corresponding to a real DNA string with an error over Z_4. They used long computational processes to find codewords that correspond to real DNA strings with an error. We can create codes and codewords that correspond to real DNA strings by the presented methods in this paper with proper computational processes.

The structure of this paper is as follows. In Section 2, we give some fundamental definitions, define a Gray map over the ring S_k, and explore the structure of linear codes and their dual over the ring S_k. In Section 3, we look into the cyclic codes decomposition, their dual on the ring S_k, and their corresponding generators. We also provide the necessary and sufficient conditions for cyclic codes to contain their duals. In Section 4, we provide some examples of better quantum codes and with the help of the Gray image of cyclic code, we also obtain optimal codes over $S_1 (k = 1)$. Moreover, in Section 5, we present methods to generate DNA codes with flexible designs as applications for DNA codes.

2. Preliminaries

First, we consider that $\mathbb{F}_{2^m}$ is a Galois field of order 2^m of a characteristic 2, and m is a positive integer. For a positive integer k, let us consider that $S_k = \frac{\mathbb{F}_{2^m}[v_1,v_2,\ldots,v_k]}{\langle v_i^2-\alpha_i v_i, v_iv_j-v_jv_i\rangle}$, for $i,j = 1,2,3,\ldots,k$, where α_i is the non-zero element of $\mathbb{F}_{2^m}$. We begin our discussion with some basic definitions:

(i) The Hamming distance between two vectors $\mathbf{x} = x_1 \ldots x_n$ and $\mathbf{y} = y_1 \ldots y_n$ is the number of places where they differ, and is denoted by $d(\mathbf{x},\mathbf{y})$.

(ii) The Hamming weight of a vector $\mathbf{x} = x_1x_2 \ldots x_n$ is the number of nonzero x_i and is denoted by $wt(\mathbf{x})$.

(iii) Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, the Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$ is defined as $\mathbf{x} \cdot \mathbf{y} = x_0 y_0 + x_1 y_1 + \ldots + x_{n-1} y_{n-1}$.
(iv) Each element of code C is referred to as a codeword and a code of length n over R is said to be linear if it is an R-submodule of R^n.
(v) A code C is said to be self-dual if $C = C^{\perp}$, self-orthogonal if $C \subseteq C^{\perp}$ and dual containing if $C^{\perp} \subseteq C$.
(vi) A linear code C is said to be linear complementary dual or in short LCD if $C \cap C^{\perp} = \{\mathbf{0}\}$, where $C^{\perp}$ is the dual code of C.
(vii) A linear code C of length n over R is said to be a cyclic code if every cyclic shift of a codeword c in C is again a codeword in $\mathcal{C}$, i.e., if $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathcal{C}$, then its cyclic shift $\delta(\mathbf{c}) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$, where the operator δ is known as cyclic shift.
(viii) A linear code C is said to be reversible if $\mathbf{c}^r = (c_{n-1}, c_{n-2}, \ldots, c_0) \in C$ whenever $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in C$.
(ix) Let C be a linear code of length n over R. Then C is called complement if for any $\mathbf{z} = (z_0, z_1, \ldots, z_{n-1}) \in C, \mathbf{z}^c = (\overline{z_0}, \overline{z_1}, \ldots, \overline{z_{n-1}}) \in C$, reversible-complement if for any $\mathbf{z} \in C, \mathbf{z}^{rc} \in C$.
(x) Let C be a code of length n over R. Then C (or the DNA correspondence of C) is called a reversible (reversible complement) DNA code if the DNA correspondence of C satisfies the properties of being reversible (reversible compliment).
(xi) It is important to note that the set of n-fold tensor product $(\mathcal{H}^q)^{\otimes n} = \mathcal{H}^q \otimes \mathcal{H}^q \otimes \ldots \otimes \mathcal{H}^q$ (n- times) is the Hilbert space with dimension q^n and that $\mathcal{H}^q$ is the Hilbert space with dimension q, where $\mathcal{H}$ is the complex field. A quantum code of length n over the field $\mathbb{F}_q$ (q is a power of prime.) is denoted by $[[n, k, d]]_q$, where k is the dimension and d is the minimum distance. We know that each quantum code satisfies the singleton bound, i.e., $n - k + 2 \geq 2d$. A quantum code is said to be MDS (maximum distance separable) if $n - k + 2 = 2d$. A quantum code $[[n, k, d]]_q$ is better than the other quantum code $[[n', k', d']]_q$ if any one or both the following conditions hold:
  (a) $\frac{k}{n} > \frac{k'}{n'}$, where $d = d'$ (larger code rate with same distance).
  (b) $d > d'$ where $\frac{k}{n} = \frac{k'}{n'}$ (larger distance with the same code rate).

Lemma 1 (CSS Construction [22])**.** *If C is an $[n, k, d]$ linear code of length n with $C^{\perp} \subseteq C$ over $\mathbb{F}_q$, then there exists a quantum error correcting code with parameters $[[n, 2k - n, d]]_q$ over $\mathbb{F}_q$.*

Lemma 2 ([3])**.** *A cyclic code C of length n with generator polynomial $g(x)$ over $\mathbb{F}_q$ that contains its dual if and only if*

$$x^n - 1 \equiv 0(mod g(x) g^*(x)),$$

where $g^*(x)$ is the reciprocal polynomial of $g(x)$.

Further, with the help of the Kronecker product, we define the Gray map over S_k. Kronecker product has the following properties:
(i) $(P \otimes Q)^{-1} = P^{-1} \otimes Q^{-1}$ for matrices $P = (p_{ij})_{m \times m}$ and $Q = (q_{i'j'})_{n \times n}$.
(ii) $(P \otimes Q) \otimes C = P \otimes (Q \otimes C)$ for arbitrary matrices P, Q and C.
(iii) $(P \otimes Q)^T = P^T \otimes Q^T$, where P^T and Q^T represent the transpose of matrices P and Q, respectively.

The Kronecker product of matrices P and Q is the $pm \times qn$ block matrix

$$P \otimes Q = \begin{bmatrix} p_{11}Q & p_{12}Q & \cdots & p_{1n}Q \\ p_{21}Q & p_{22}Q & \cdots & p_{2n}Q \\ \cdots & \cdots & \cdots & \cdots \\ p_{m1}Q & p_{m2}Q & \cdots & p_{mn}Q \end{bmatrix}$$

where $P = (p_{ij})$ is an $m \times n$ matrix and $Q = (q_{i'j'})$ is a $p \times q$ matrix. More specifically,

$$P \otimes Q = \begin{bmatrix} p_{11}q_{11} & p_{11}q_{12} & \cdots & p_{11}q_{1q} & \cdots & \cdots & p_{1n}q_{11} & p_{1n}q_{12} & \cdots & p_{1n}q_{1q} \\ p_{11}q_{21} & p_{11}q_{22} & \cdots & p_{11}q_{2q} & \cdots & \cdots & p_{1n}q_{21} & p_{1n}q_{22} & \cdots & p_{1n}q_{2q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{11}q_{p1} & p_{11}q_{p2} & \cdots & p_{11}q_{pq} & \cdots & \cdots & p_{1n}q_{p1} & p_{1n}q_{p2} & \cdots & p_{1n}q_{pq} \\ \vdots & \vdots & \vdots & \vdots & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \ddots & \vdots & \vdots & & \vdots \\ p_{m1}q_{11} & p_{m1}q_{12} & \cdots & p_{m1}q_{1q} & \cdots & \cdots & p_{mn}q_{11} & p_{mn}q_{12} & \cdots & p_{mn}q_{1q} \\ p_{m1}q_{21} & p_{m1}q_{22} & \cdots & p_{m1}q_{2q} & \cdots & \cdots & p_{mn}q_{21} & p_{mn}q_{22} & \cdots & p_{mn}q_{2q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{m1}q_{p1} & p_{m1}q_{p2} & \cdots & p_{m1}q_{pq} & \cdots & \cdots & p_{mn}q_{p1} & p_{mn}q_{p2} & \cdots & p_{mn}q_{pq} \end{bmatrix}$$

for $1 \leq i \leq m, 1 \leq j \leq n, 1 \leq i' \leq p, 1 \leq j' \leq q$.

The ring $S_k = \frac{\mathbb{F}_{2^m}[v_1, v_2, \ldots, v_k]}{\langle v_i^2 - \alpha_i v_i, v_i v_j - v_j v_i \rangle}$ and the ring S_k can also be expressed as $\mathbb{F}_{2^m} + \mathbb{F}_{2^m} v_1 + \mathbb{F}_{2^m} v_2 + \mathbb{F}_{2^m} v_1 v_2 + \ldots + \mathbb{F}_{2^m} v_1 v_2 \ldots v_k$ such that $v_i^2 = \alpha_i v_i, v_i v_j = v_j v_i$ for $i, j = 1, 2, 3, \ldots, k$. S_k is a finite commutative ring. Next, let us consider that $\mathcal{T}$ be the power set of $\{1, 2, 3, .., k\}$. Henceforth, every element $s \in S_k$ can be uniquely expressed as $s = \sum_{T \in \mathcal{T}} \beta_T v_T$ for some $\beta_T \in \mathbb{F}_q, T \in \mathcal{T}, v_T = \prod_{i \in T} v_i$ and $v_\phi = 1$. Let $e_i^k \in \{v_T \in \mathcal{T}, v_\phi = 1\}$ and also $e_i^k \neq e_j^k$, where $i \neq j$ and $i, j = 1, 2, 3, \ldots, 2^k$.

We take $k = 1$, then $S_1 = \mathbb{F}_{2^m} / \langle v_1^2 - \alpha_1 v_1 \rangle$. The ring S_1 can be expressed as $S_1 = \mathbb{F}_{2^m} + v_1 \mathbb{F}_{2^m}$ such that $v_1^2 = \alpha_1 v_1$. Henceforth, the basis of S_1 is the $\{1, v_1\}$. Let $e_1^1 = 1, e_2^1 = v_1$. For the ring S_k, using Kronecker Product, the bases of S_k can be written as

$$(e_1^k, e_2^k, \ldots, e_{2^k}^k) = (1, v_k) \otimes (e_1^{k-1}, e_2^{k-1}, \ldots, e_{2^{k-1}}^{k-1}), \tag{1}$$

where $(e_1^1, e_2^1) = (1, v_1)$. Further, we obtain the set of an orthogonal set of idempotents of the ring S_k such that $\zeta_i^k = \prod_{j=1}^{k} \Delta_j$, where $\Delta_j \in \{\frac{v_j}{\alpha_j}, \frac{\alpha_j - v_j}{\alpha_j}\}$ and $\zeta_i^k \neq \zeta_j^k$ for $i, j = 1, 2, 3, \ldots, 2^k$. It is easily to see that

$$\sum_{i=1}^{2^k} \zeta_i^k = 1, (\zeta_i^k)^2 = \zeta_i^k, \zeta_i^k \zeta_j^k = 0 \,(for\, i \neq j),$$

where $i, j = 1, 2, 3, \ldots, 2^k$. Therefore, the set $\{\zeta_i^k | i = 1, 2, \ldots, 2^k\}$ is also a basis of the ring S_k. Again, we take $k = 1$, then $\zeta_1^1 = \frac{v_1}{\alpha_1}, \zeta_2^1 = \frac{\alpha_1 - v_1}{\alpha_1}$. Similarly as in (1), we have

$$(\zeta_1^k, \zeta_2^k, \ldots, \zeta_{2^k}^k) = (\frac{v_k}{\alpha_k}, \frac{\alpha_k - v_k}{\alpha_k}) \otimes (\zeta_1^{k-1}, \zeta_2^{k-1}, \ldots, \zeta_{2^{k-1}}^{k-1}),$$

where $(\zeta_1^1, \zeta_2^1) = (\frac{v_1}{\alpha_1}, \frac{\alpha_1 - v_1}{\alpha_1})$.

With the help of Chinese Remainder Theorem, we write

$$S_k = S_k \zeta_1^k \oplus S_k \zeta_2^k \oplus \ldots \oplus S_k \zeta_{2^k}^k = \mathbb{F}_{2^m} \zeta_1^k \oplus \mathbb{F}_{2^m} \zeta_2^k \oplus \ldots \oplus \mathbb{F}_{2^m} \zeta_{2^k}^k.$$

Every element s in S_k has the unique representation $s = \sum_{i=1}^{2^k} \beta_i e_i^k = \sum_{i=1}^{2^k} \gamma_i^k \zeta_i^k$, where $\beta_i, \gamma_i^k \in \mathbb{F}_{2^m}$ and $i = 1, 2, \ldots, 2^k$. Now, we define a Gray map:

$$\Theta_k : S_k \longrightarrow \mathbb{F}_{2^m}^{2^k}$$

is defined by

$$\Theta_k(s) = \Theta_k(\sum_{i=1}^{2^k} \beta_i e_i^k) = (\beta_1, \beta_2, \dots, \beta_{2^k}) A_{2^k}. \tag{2}$$

In above described Gray map, $A_{2^k} \in GL_{2^k}(\mathbb{F}_{2^m})$ is a matrix and $GL_{2^k}(\mathbb{F}_{2^m})$ is the linear group of all $2^k \times 2^k$ invertible matrices over the field $\mathbb{F}_{2^m}$ such that $A_{2^k} A_{2^k}^T = \epsilon I_{2^k \times 2^k}$, where $A_{2^k}^T$ is the transpose of A_{2^k}, $I_{2^k \times 2^k}$ is an identity matrix of order 2^k and $\epsilon \in \mathbb{F}_{2^m} \backslash \{0\}$. In order to make our representation easier, we write $(\beta_1, \beta_2, \dots, \beta_{2^k})(A_{2^k}) = (\gamma_1^k, \gamma_2^k, \dots, \gamma_{2^k}^k)$. Above described Gray map can easily be extended to S_k^n as

$$\Theta_k : S_k^n \longrightarrow \mathbb{F}_{2^m}^{2^k n}$$

and is defined as

$$\Theta_k(s_0, s_1, \dots, s_{n-1}) = (\gamma_{i,j}^k)_{1 \leq i \leq 2^k, 1 \leq j \leq n-1}.$$

We denote each $s_j = \sum\limits_{i=1}^{2^k} \beta_{i,j} e_i^k$. Henceforth

$$\Theta_k(s_j) = (\beta_{1,j}, \beta_{2,j}, .., \beta_{2^k,j})(A_{2^k}) = (\gamma_{1,j}^k, \gamma_{2,j}^k, \dots, \gamma_{2^k,j}^k),$$

where $\beta_{i,j} \in \mathbb{F}_{2^m}, i = 1, 2, 3, \dots, 2^k$ and $j = 1, 2, \dots, n-1$.

When we take $k = 1$, we can define the Gray map in a similar way as (2)

$$\Theta_1(S_1) \longrightarrow \mathbb{F}_{2^m}^2$$

defined map $\Theta_1(\beta_1 e_1^1 + \beta_2 e_2^1) = \Theta_1(\beta_1 + \beta_2 v_1) = (\beta_1, \beta_2) A_2$, $A_2 \in GL_2(\mathbb{F}_{2^m})$ is a matrix and $GL_2(\mathbb{F}_{2^m})$ is the linear group of all 2×2 invertible matrices over the field $\mathbb{F}_{2^m}$ such that $A_2 A_2^T = \epsilon I_{2\times 2}$, where A_2^T is the transpose of A_2, $I_{2\times 2}$ is an identity matrix of order 2 and $\epsilon \in \mathbb{F}_{2^m} \backslash \{0\}$.

The Lee weight of every element $s = \sum\limits_{i=1}^{2^k} \beta_i e_i^k$ of the ring S_k is defined as $w_L(s) = w_H(\Theta_k(s)) = w_H(\gamma_1^k, \gamma_2^k, \dots, \gamma_{2^k}^k)$. Let C be a linear code of length n over S_k. It can be easily seen that $\Theta_k(C)$ is a linear code of length $2^k n$ over $\mathbb{F}_{2^m}$. Any linear code C of length n over S_k, we state

$$C_j = \{\mathbf{x_j} \in \mathbb{F}_{2^m}^n | \sum_{i=1}^{2^k} \zeta_i^k \mathbf{x_i} \in C, \mathbf{x_i} \in \mathbb{F}_{2^m}^n,\ i \neq j \, and \, 1 \leq i \leq 2^k\},$$

where $j = 1, 2, \dots, 2^k$. Then C_j is a linear code of length n over $\mathbb{F}_{2^m}$, for $j = 1, 2, 3, \dots, 2^k$. Next, let us consider that B_i is the linear code over $\mathbb{F}_{2^m}$, where $i = 1, 2, \dots, 2^k$. We denote $B_1 \oplus B_2 \oplus \dots \oplus B_{2^k} = \{b_1 + b_2 + \dots + b_{2^k} | b_i \in B_i, 1 \leq i \leq 2^k\}$ and similarly we define the product as $B_1 \otimes B_2 \otimes \dots \otimes B_{2^k} = \{(b_1, b_2, \dots, b_{2^k}) | b_i \in B_i, 1 \leq i \leq 2^k\}$. Hence, a linear code C of length n over S_k can be easily seen that $C = \oplus_{i=1}^{2^k} \zeta_i^k C_i = \zeta_1^k C_1 \oplus \zeta_2^k \oplus \dots \oplus \zeta_{2^k}^k C_{2^k}$. A matrix is called generator matrix of C if the rows of the matrix generates C. Let G_i be the generator matrix for the code C_i, for $i = 1, 2, 3, \dots, 2^k$. Then a generator matrix for the code C is

$$G = \begin{bmatrix} \zeta_1^k G_1 \\ \zeta_2^k G_2 \\ . \\ . \\ . \\ \zeta_{2^k}^k G_{2^k} \end{bmatrix}$$

and a generator matrix of $\Theta_k(C)$ is

$$\Theta_k(G) = \begin{bmatrix} \Theta_k(\zeta_1^k G_1) \\ \Theta_k(\zeta_2^k G_2) \\ \cdot \\ \cdot \\ \cdot \\ \Theta_k(\zeta_{2^k}^k G_{2^k}) \end{bmatrix}.$$

3. Main Results

In this section, we discuss some results on the Gray map, and structural properties of cyclic codes over S_k and with the help of CSS-construction, we prove some results on quantum error correcting codes.

3.1. Results on the Gray Map

In this section, we describe some results on the Gray map.

Proposition 1. *The Gray map Θ_k is a linear, bijective and distance-preserving map from (R_k^n, d_L) to $(\mathbb{F}_{2^m}^{2^k n}, d_H)$, where $d_L = d_H$.*

Proof. Suppose $\mathbf{c_1}, \mathbf{c_2} \in S_k$. It can be easily seen that

$$\Theta_k(\mathbf{c_1} + \mathbf{c_2}) = \Theta_k(\mathbf{c_1}) + \Theta_k(\mathbf{c_2}).$$

Now, we take $\delta \in \mathbb{F}_{2^m}$, then

$$\Theta_k(\delta \mathbf{c_1}) = \delta \Theta_k(\mathbf{c_1}).$$

So, Θ_k is a map linear-preserving. Now, we will prove that Θ_k is a bijection.

Then, we have

$$\begin{aligned} \Theta_k(\mathbf{c_1}) &= \Theta_k(\mathbf{c_2}) \\ \Theta_k(\sum_{i=1}^{2^k} \beta_i e_i^k) &= \Theta_k(\sum_{i=1}^{2^k} \delta_i e_i^k) \\ (\beta_1, \beta_2, \ldots, \beta_{2^k}) A_{2^k} &= (\delta_1, \delta_2, \ldots, \delta_{2^k}) A_{2^k} \end{aligned}$$

where $\beta_i, \delta_i \in \mathbb{F}_{2^m}$ for $1 \leq i \leq 2^k$. This implies that

$$\beta_1 = \delta_1, \ldots, \beta_{2^k} = \delta_{2^k}.$$

Then $c_1 = c_2$. Henceforth, Θ_k is one-one. Take any $(\beta_1, \beta_2, \ldots, \beta_{2^k}) A_{2^k} \in \mathbb{F}_{2^m}^{2^k}$, then there exists a corresponding element $\mathbf{c_1} \in S_k$ such that $\Theta_k(\mathbf{c_1}) = (\beta_1, \ldots, \beta_{2^k})$. Therefore, Θ_k is onto. Hence, Θ_k is a bijective map.

Furthermore, we have

$$\begin{aligned} d_L(\mathbf{c_1}, \mathbf{c_2}) &= w_L(\mathbf{c_1} - \mathbf{c_2}) \\ &= w_H(\Theta_k(\mathbf{c_1} - \mathbf{c_2})) \\ &= w_H(\Theta_k(\mathbf{c_1}) - \Theta_k(\mathbf{c_2})) \\ &= d_H(\Theta_k(\mathbf{c_1}), \Theta_k(\mathbf{c_2})). \end{aligned}$$

Hence, Θ_k is a distance-preserving map. □

Proposition 2. *Let C be a linear code of length n over S_k. Then $|\Theta_k(C^\perp)| = |\Theta_k(C)^\perp|$ and $\Theta_k(C)$ is self-orthogonal if and only if C is self-orthogonal. Furthermore, $\Theta_k(C)$ is self-dual if and only if C is self-dual.*

Proof. Suppose two elements $\mathbf{s}, \mathbf{t}$ in S_k such that

$$\mathbf{s} = (s_0, s_1, \ldots, s_{n-1})$$

$$\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}),$$

where $s_j = \sum_{i=1}^{2^k} p_{i,j}\zeta_i^k, t_j = \sum_{i=1}^{2^k} r_{i,j}\zeta_i^k$ for $i = 1, 2, 3, \ldots, 2^k, j = 1, 2, \ldots, n-1$ and $p_{i,j}, r_{i,j} \in \mathbb{F}_{2^m}$. Next, let us consider that $\mathbf{s} \cdot \mathbf{t} = 0$. Then, we obtain

$$\begin{aligned} \sum_{i=1}^{n-1} s_j t_j &= 0 \\ \Longrightarrow \sum_{j=0}^{n-1} (\sum_{i=0}^{2^k} p_{i,j}\zeta_i^k)(\sum_{i=0}^{2^k} r_{i,j}\zeta_i^k) &= 0. \end{aligned}$$

Since $(\zeta_i^k)^2 = \zeta_i^k$, we have

$$\sum_{j=0}^{n-1} \sum_{i=0}^{2^k} p_{i,j} r_{i,j} \zeta_i^k = \sum_{i=0}^{2^k} \sum_{j=0}^{n-1} p_{i,j} r_{i,j} \zeta_i^k = 0.$$

Therefore,

$$\sum_{j=0}^{n-1} p_{i,j} r_{i,j} = 0,$$

where $i = 1, 2, \ldots, 2^k$. Furthermore,

$$\begin{aligned} \Theta_k(\mathbf{s})\Theta_k(\mathbf{t}) &= \sum_{j=0}^{n-1} \sum_{i=0}^{2^k} p_{i,j} r_{i,j} \\ &= \sum_{i=0}^{2^k} \sum_{j=0}^{n-1} p_{i,j} r_{i,j} \\ &= 0. \end{aligned}$$

This implies that,

$$\Theta_k(C^\perp) \subseteq \Theta_k(C)^\perp.$$

Since Θ_k is a bijection, then $|\Theta_k(C^\perp)| = |\Theta_k(C)^\perp|$. Hence, $\Theta_k(C^\perp) = \Theta_k(C)^\perp$. Now, C is self-orthogonal if and only if $C \subseteq C^\perp$. Henceforth, $\Theta_k(C) \subseteq \Theta_k(C^\perp) = \Theta_k(C)^\perp$ if and only if $\Theta_k(C)$ is self-orthogonal. In the same way, C is self-dual if and only if $\Theta_k(C)$ is self-dual. □

Proposition 3. *Let $C = \oplus_{i=1}^{2^k} \zeta_i^k C_i$ be a linear code of length n over S_k. Then,*

(i) $\Theta_k(C) = C_1 \otimes C_2 \otimes \ldots \otimes C_{2^k}$ *as well as* $|C| = |C_1||C_2| \ldots |C_{2^k}|$.

(ii) $C^\perp = \oplus_{i=1}^{2^k} \zeta_i^k C_i^\perp$*, Moreover, each C_i is self-orthogonal if and only if C is self-orthogonal as well as each C_i is self-dual if and only if C is self-dual.*

Proof.

(i) Let us suppose that $\mathbf{w} = (\gamma^k_{1,0}, \gamma^k_{1,1}, \ldots, \gamma^k_{1,n-1}, \gamma^k_{2,0}, \gamma^k_{2,1}, \ldots, \gamma^k_{2,n-1}, \ldots, \gamma^k_{2^k,0}, \gamma^k_{2^k,1}, \ldots, \gamma^k_{2^k,n-1}) \in \Theta_k(C)$ and $s_j = \sum_{i=1}^{2^k} \gamma^k_{i,j}\zeta^k_i$, where $j = 0, 1, 2, \ldots, n-1$. Hence, $\mathbf{s} = (s_0, s_1, \ldots, s_{n-1}) \in C$, but Θ_k is bijective map, $(\gamma^k_{i,0}, \gamma^k_{i,1}, \ldots, \gamma^k_{i,n-1}) \in C_i$, where $i = 1, 2, \ldots, 2^k$. With the help of definition of C_i, $\mathbf{w} \in C_1 \otimes C_2 \otimes \ldots \otimes C_{2^k}$. Hence, $\Theta_k(C) \subseteq C_1 \otimes C_2 \otimes \ldots \otimes C_{2^k}$.
On the other hand, let $\mathbf{w} = (\gamma^k_{1,0}, \gamma^k_{1,1}, \ldots, \gamma^k_{1,n-1}, \gamma^k_{2,0}, \gamma^k_{2,1}, \ldots, \gamma^k_{2,n-1}, \ldots, \gamma^k_{2^k,0}, \gamma^k_{2^k,1}, \ldots, \gamma^k_{2^k,n-1}) \in C_1 \otimes C_2 \otimes \ldots \otimes C_{2^k}$, then $(\gamma^k_{i,0}, \gamma^k_{i,1}, \ldots, \gamma^k_{i,n-1}) \in C_i$, where $i = 1, 2, \ldots, 2^k$. We select $s_j = \sum_{i=1}^{2^k} \gamma^k_{i,j}\zeta^k_i$, where $j = 0, 1, \ldots, n-1$. Then, $\mathbf{s} = (s_0, s_1, \ldots, s_{n-1}) \in C$ and $\Theta_k(\mathbf{s}) = \mathbf{w}$. Therefore, $\mathbf{w} \in \Theta_k(C)$. Hence, $C_1 \otimes C_2 \otimes \ldots \otimes C_{2^k} \subseteq \Theta_k(C)$. Furthermore, the map Θ_k is bijective, then $|C| = |\Theta_k(C)|$. Consequently, $|C| = |C_1 \otimes C_2 \otimes \ldots \otimes C_{2^k}| = |C_1||C_2| \ldots |C_{2^k}|$.

(ii) Let us consider $U_j = \{\mathbf{r_j} \in \mathbb{F}^n_{2^m} | \sum_{i=1}^{2^k} \zeta^k_i \mathbf{r_i} \in C^\perp, for\ some\ \mathbf{r_i} \in \mathbb{F}^n_{2^m}, i \neq j \& 1 \leq i, j \leq 2^k\}$. Then $C^\perp$ can be uniquely expressed as $C^\perp = \zeta^k_1 U_1 \oplus \zeta^k_2 U_2 \oplus \ldots \oplus C^k_{2^k}$. Since, $U_1 = \{\mathbf{r_1} \in \mathbb{F}^n_{2^m} | \sum_{i=1}^{2^k} \zeta^k_i \mathbf{r_i} \in C^\perp, for\ some\ \mathbf{r_i} \in \mathbb{F}^n_{2^m}, i \neq 1 \& 1 \leq i \leq 2^k\}$. Evidently, $C_1 U_1 = 0$, hence $U_1 \subseteq C_1^\perp$. Next, let us consider that $\mathbf{c_1} \in C_1^\perp$, then $\mathbf{c_1 x_1} = 0$ for any $\mathbf{c} = \sum \zeta^k_i \mathbf{x_i} \in C$. Therefore, $\zeta^k_1 \mathbf{c_1 c} = \zeta^k_1 \mathbf{c_1 x_1} = 0$ and this implies that $\zeta^k_1 \mathbf{c_1} \in C^\perp$. We have $\mathbf{c_1} \in U_1$, with the help of unique representation of $C^\perp$, so $C_1^\perp \subseteq U_1$. In this similar way, we can show that $C_j^\perp = U_j^\perp$, where $j = 2, 3, \ldots, 2^k$. Thus, we arrive at $C^\perp = \oplus_{i=1}^{2^k} \zeta^k_i C_i^\perp$. Furthermore, $C \subseteq C^\perp$ if and only if C is self-orthogonal. Then, we have,

$$\zeta^k_1 C_1 \oplus \ldots \oplus \zeta^k_{2^k} C_{2^k} \subseteq \zeta^k_1 C_1^\perp \oplus \ldots \oplus \zeta^k_{2^k} C_{2^k}^\perp \iff C_i \subseteq C_i^\perp,$$

where $i = 1, 2, \ldots, 2^k$. In a similar way, we can easily see that C is self-dual if and only if each C_i is self-dual.

□

Proposition 4. *Let $C = \oplus_{i=1}^{2^k} \zeta^k_i C_i$ be a linear code having the parameters $[n, k, d_L]$ over S_k. Then $\Theta_k(C)$ is a linear code with parameters $[2^k n, \sum_{i=1}^{2^k} k_i, d_H]$ over $\mathbb{F}_{2^m}$, where $i = 1, 2, 3, \ldots, 2^k$ and $d_L = d_H$.*

3.2. Cyclic Codes over S_k

We begin this section with some important results on cyclic codes over S_k.

Theorem 1. *Let $C = \oplus_{i=1}^{2^k} \zeta^k_i C_i$ be a linear code of length n over S_k. Then C is a cyclic code of length n over S_k if and only if each C_i is a cyclic code over $\mathbb{F}_{2^m}$, where $i = 1, 2, \ldots, 2^k$.*

Proof. Let C be a linear code of length n over S_k. Take any codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$, here $c_j = \sum_{i=1}^{2^k} \zeta^k_i c_{i,j}$, $i = 1, 2, \ldots, 2^k$ and $j = 1, 2, \ldots, n-1$. Next, let us consider that $\mathbf{y_1}, \mathbf{y_2}, \ldots, \mathbf{y_{2^k}}$ are in $C_1, C_2, \ldots, C_{2^k}$, respectively, where $\mathbf{y_i} = (c_{i,0}, c_{i,1}, \ldots, c_{i,n-1}) \in C_i$. Since C is a cyclic code over S_k, we have $\delta(\mathbf{c}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$, where $\delta(\mathbf{c})$ is the cyclic shift of $\mathbf{c}$. Henceforth, $\delta(\mathbf{c})$ is in C if and only if $\delta(\mathbf{y_i}) = (c_{i,n-1}, c_{i,0}, \ldots, c_{i,n-2}) \in C_i$, where $i = 1, 2, 3, \ldots, 2^k$. Thus, C is a cyclic code of length n over S_k if and only if each C_i is a cyclic code over $\mathbb{F}_{2^m}$. $\square$

Theorem 2. *Let $C = \oplus_{i=1}^{2^k} \zeta_i^k C_i$ be a cyclic code of length n over S_k and $g_i(x)$ be the monic generator polynomial of C_i, where each $g_i(x)$ divides $x^n - 1$. Then,*

(i) $C = \langle g_1(x)\zeta_1^k, g_2(x)\zeta_2^k, \ldots, g_{2^k}(x)\zeta_{2^k}^k \rangle$ *as well as* $|C| = 2^{m^{2^k n - \sum_{i=1}^{2^k} deg(g_i(x))}}$.

(ii) $C = \langle g(x) \rangle$*, where* $g(x) = \sum_{i=1}^{2^k} g_i(x)\zeta_i^k$ *divides* $(x^n - 1)$.

Proof.

(i) In view of Theorem 1, each C_i is a cyclic code of length n over $\mathbb{F}_{2^m}$, where $i = 1, 2, \ldots, 2^k$. However, C is a cyclic code over S_k and it is given that $g_i(x)$ is the monic generator polynomial of C_i, i.e., $C_i = \langle g_i(x) \rangle \subseteq \frac{\mathbb{F}_{2^m}[x]}{\langle x^n - 1 \rangle}$. Hence, $C = \langle g_1(x)\zeta_1^k, g_2(x)\zeta_2^k, \ldots, g_{2^k}(x)\zeta_{2^k}^k \rangle$ and also the map Θ is bijective, then $|\Theta(C)| = |C|$. By Proposition 3, we conclude that

$$\begin{aligned} |C| &= |C_1||C_2| \ldots |C_{2^k}| \\ &= (2^m)^{n - deg(g_1(x))} \ldots (2^m)^{n - deg(g_{2^k}(x))} \\ &= (2^m)^{2^k n - \sum_{i=1}^{2^k} deg(g_i(x))}. \end{aligned}$$

(ii) By part (i), $C = \langle g_1(x)\zeta_1^k, g_2(x)\zeta_2^k, \ldots, g_{2^k}(x)\zeta_{2^k}^k \rangle$. Next, we consider that $D = g_1(x)\zeta_1^k + g_2(x)\zeta_2^k + \ldots + g_{2^k}(x)\zeta_{2^k}^k$. It is clearly that $D \subseteq C$. However, $(\zeta_i^k)^2 = \zeta_i^k$ and $\zeta_i^k \zeta_j^k = 0$, where $i, j = 1, 2, \ldots, 2^k$ and $i \neq j$. Hence $g_i(x)\zeta_i^k = (g_1(x)\zeta_1^k + \ldots + g_{2^k}(x)\zeta_{2^k}^k)\zeta_i^k$. This shows that $C \subseteq D$. Now, from the above discussion, we conclude that $C = D$, where $f(x) = \sum_{i=1}^{2^k} g_i(x)\zeta_i^k$. It is given that monic generator polynomial of C_i is $g_i(x)$, where $i = 1, 2, \ldots, 2^k$. Henceforth, $g_i(x)$ divides $x^n - 1$ such that $x^n - 1 = h_i(x)g_i(x)$ this implies that $(x^n - 1)\zeta_i^k = h_i(x)g_i(x)\zeta_i^k$, where $i = 1, 2, \ldots, 2^k$.

$$\begin{aligned} x^n - 1 &= x^n(\sum_{i=1}^{2^k} \zeta_i^k) - (\sum_{i=1}^{2^k} \zeta_i^k) = \sum_{i=1}^{2^k} (x^n - 1)\zeta_i^k \\ &= \sum_{i=1}^{2^k} h_i(x)g_i(x)\zeta_i^k = (\sum_{i=1}^{2^k} h_i(x)\zeta_i^k)(\sum_{i=1}^{2^k} g_i(x)\zeta_i^k) \\ &= (\sum_{i=1}^{2^k} h_i(x)\zeta_i^k) g(x). \end{aligned}$$

Hence, $g(x)$ divides $x^n - 1$. This completes the proof.

$\square$

Corollary 1. *Let $C = \oplus_{i=1}^{2^k} \zeta_i^k C_i$ be a cyclic code of length n over S_k. Then $C^\perp = \oplus_{i=1}^{2^k} \zeta_i^k C_i^\perp$ is also a cyclic code of length n over S_k.*

3.3. Quantum Codes

In quantum computing and communication, quantum codes are employed to shield quantum information from noise into the channel during transmission. One of the noteworthy developments in code construction is the construction of quantum error-correcting codes from classical error-correcting codes. The construction of quantum error-correcting codes from classical error-correcting codes was done by Calderbank et al. [3]. In this section, using the CSS(Calderbank-Shor-Steane) construction [22], we obtain quantum codes from dual-containing cyclic codes. In comparison to already existing quantum codes, we are able to construct superior quantum codes. Moreover, using a necessary and sufficient condition over the finite fields in [3], we are able to determine the necessity for cyclic codes to contain their duals over S_k. Our first result gives the necessary and sufficient conditions for cyclic codes to contain their duals.

Theorem 3. *Let $C = \oplus_{i=1}^{2^k} \zeta_i^k C_i$ be a cyclic code of length n over S_k, where $g_i(x)$ is the generator polynomial of C_i and $i = 1, 2, \ldots, 2^k$. Then,*

(i) *$C^\perp \subseteq C$ if and only if $C_i^\perp \subseteq C_i$, where $i = 1, 2, \ldots, 2^k$.*

(ii) *$C^\perp \subseteq C$ if and only if $x^n - 1 \equiv 0(mod g_i(x) g_i^*(x))$, where $g_i^*(x)$ is the reciprocal polynomial of $g_i(x)$.*

Proof.

(i) First, let us consider that $C^\perp \subseteq C$. This implies that $\oplus_{i=1}^{2^k} \zeta_i^k C_i^\perp \subseteq \oplus_{i=1}^{2^k} \zeta_i^k C_i$. However, C_i is a linear code such that $\zeta_i^k C_i \equiv C(mod \zeta_i^k)$, we get $C_i^\perp \subseteq C_i$, where $i = 1, 2, \ldots, 2^k$. Conversely, let us consider that $C_i^\perp \subseteq C_i$, where $i = 1, 2, \ldots, 2^k$. This shows that $C^\perp = \oplus_{i=1}^{2^k} \zeta_i^k C_i^\perp \subseteq \oplus_{i=1}^{2^k} \zeta_i^k C_i = C$.

(ii) Let $C^\perp \subseteq C$, by using part (i), $C_i^\perp \subseteq C_i$, where $i = 1, 2, \ldots, 2^k$. Now, by Lemma 2, $x^n - 1 \equiv (mod g_i(x) g_i^*(x))$, where $g_i^*(x)$ denotes the reciprocal of $g_i(x)$. Conversely, let us consider that $x^n - 1 \equiv (mod g_i(x) g_i^*(x))$, where $g_i^*(x)$ denotes the reciprocal of $g_i(x)$ and $i = 1, 2, \ldots, 2^k$. Hence, by Lemma 2, we have $C_i^\perp \subseteq C_i$, where $i = 1, 2, \ldots, 2^k$. Application of part (i) yields that $C^\perp \subseteq C$.

□

Theorem 4. *Let $C = \oplus_{i=1}^{2^k} \zeta_i^k C_i$ be a cyclic code of length n over S_k and its Gray image having the parameters $[2^k n, \sum_{i=1}^{2^k} k_i, d_H]$, where $i = 1, 2, \ldots, 2^k$. Then,*

(i) *If $C^\perp \subseteq C$, then there exists a quantum code $[[2^k n, \sum_{i=1}^{2^k} k_i - 2^k n, d_H]]_{2^m}$ over $\mathbb{F}_{2^m}$.*

(ii) *If $x^n - 1 \equiv 0(mod g_i(x) g_i^*(x))$, where $g_i^*(x)$ is the reciprocal polynomial of $g_i(x)$, and $i = 1, 2, 3, \ldots, 2^k$, then there exists a quantum code $[[2^k n, 2\sum_{i=1}^{2^k} k_i - 2^k n, d_H]]_{2^m}$ over $\mathbb{F}_{2^m}$.*

Proof.

(i) First, let us consider that $C^\perp \subseteq C$. By Proposition 2, $\Theta_k(C^\perp) = \Theta_k(C)^\perp$, $\Theta_k(C)^\perp \subseteq \Theta_k(C)$. Hence, $\Theta_k(C)$ is a dual containing linear code over $\mathbb{F}_{2^m}$. By Lemma 1, there exists a quantum code $[[2^k n, 2\sum_{i=1}^{2^k} k_i - 2^k n, d_H]]_{2^m}$ over $\mathbb{F}_{2^m}$.

(ii) Let us consider that $x^n - 1 \equiv 0(mod g_i(x) g_i^*(x)$ for $i = 1, 2, 3, \ldots, 2^k$, where g_i^* denotes the reciprocal polynomial of $g_i(x)$. By Theorem 3 part (ii), $C^\perp \subseteq C$, by using part (i), there exists a quantum code $[[2^k n, 2\sum_{i=1}^{2^k} k_i - 2^k n, d_H]]_{2^m}$ over $\mathbb{F}_{2^m}$.

□

4. Applications

In this section, we obtain a number of optimal linear codes from the Gray images of cyclic codes over S_1(for $k = 1$). Additionally, we obtain quantum codes over S_1 that are better than the ones found in some recent references [23,24] by using dual-containing cyclic codes. The Magma computation system is used to complete all of the computations in these examples [25].

Example 1. *Let $n = 8, m = 1$ and $S_1 = \mathbb{F}_2[u_1]/\langle u_1^2 - u_1\rangle$. Then, we have,*

$$x^8 - 1 = (x+1)^8 \in \mathbb{F}_2[x].$$

Take

$$\begin{aligned} g_1(x) &= (x+1) \\ g_2(x) &= (x+1)^5. \end{aligned}$$

Hence, C is a cyclic code of length 8 over S_1. By Proposition 4, the Gray image $\Theta_1(C)$ has parameters $[16, 10, 4]$ over $\mathbb{F}_2$. This code is optimal according to the database [26].

Example 2. *Let $n = 28, m = 2$, $\alpha_1 = 1$ and $S_1 = \mathbb{F}_{2^2}[u_1]/\langle u_1^2 - u_1\rangle$. Then, we have,*

$$x^{28} - 1 = (x+1)^4(x^3+x+1)^4(x^3+x^2+1)^4 \in \mathbb{F}_4[x].$$

Take

$$\begin{aligned} g_1(x) &= (x+1)(x^3+x+1)^3 \\ g_2(x) &= (x+1)^2. \end{aligned}$$

Hence, C is a cyclic code of length 28 over S_1. Then, by the Proposition 4, the Gray image $\Theta_1(C)$ has parameters $[56, 44, 4]$ over $\mathbb{F}_4$. However, $x^{28} - 1 \equiv 0(mod g_i(x)g_i^*(x))$, where $i = 1, 2$. With the help of Theorem 3, $C^\perp \subseteq C$. Hence, by Theorem 4, there exists a quantum code with parameters $[[56, 32, 4]]_4$. The code has the same minimum distance but a larger code rate than the previous known quantum code $[[56, 16, 4]]_4$ existing in [23].

In Tables 1 and 2, we write the coefficients of generator polynomials in decreasing order, for example, we write 1021 to represent the polynomial $x^3 + 2x + 1$. In Table 1, we obtain optimal linear codes with the help of the Gray image of cyclic codes and also in Table 2, we obtain quantum codes. In Table 2, it is noted that our obtained codes $[[n, k, d]]_{2^m}$ are better than the existing quantum codes $[[n', k', d']]_{2^m}$ collected from different references mentioned there.

Table 1. Gray images of cyclic codes of length n over S_1.

m	n	$g_1(x)$	$g_2(x)$	$\Theta_1(C)$	*Remarks*
1	4	11	11	$[8, 6, 2]_2$	*optimal*
1	2	11	11	$[4, 2, 2]_2$	*optimal*
1	8	101	110011	$[16, 9, 4]_2$	*optimal*
1	12	11	101101	$[24, 18, 4]_2$	*optimal*
1	14	101	111001	$[28, 21, 4]_2$	*optimal*
1	15	111	1100111001	$[30, 19, 6]_2$	*optimal*
2	8	11	110011	$[16, 10, 4]_4$	...
2	9	11	110ww	$[18, 13, 3]_4$	...

Table 2. Quantum codes from cyclic codes over S_1.

m	n	$g_1(x)$	$g_2(x)$	$\Theta_1(C)$	$[[n,k,d]]_{2^m}$	$[[n',k',d']]_{2^m}$
2	7	1011	1101	$[14,8,3]$	$[[14,2,3]]_{2^2}$	...
2	11	1	$1w^2 11w1$	$[22,17,5]$	$[[22,12,5]]_{2^2}$	...
2	28	11100101001	101	$[56,44,4]$	$[[56,32,4]]_{2^2}$	$[[56,16,4]]_{2^2}$ [23]
3	12	11	11	$[24,22,2]$	$[[24,20,2]]_{2^3}$	$[[21,15,2]]_{2^3}$ [24]
4	14	11	11110011	$[28,20,4]$	$[[28,12,4]]_{2^4}$	$[[28,4,3]]_{2^4}$ [24]
4	19	$1w^5 0w^5 w^5 w^{10} w^{10} 0w^{10} 1$	$1w^5 0w^5 w^5 w^{10} w^{10} 0w^{10} 1$	$[38,20,7]$	$[[38,2,7]]_{2^4}$	...
4	22	11	$11w^{10} w^{10} 1111w^9 w^9 11$	$[44,33,6]$	$[[44,22,6]]_{2^4}$	$[[35,5,3]]_{2^4}$ [24]
4	29	$1w^7 w^6 w^3 w^{12} w^9 w^{13} 1$	$1w^7 w^6 w^3 w^{12} w^9 w^{13} 1$	$[58,44,6]$	$[[58,30,6]]_{2^4}$	...
4	41	$1w^{10} w^2 w^8 w^{10} 1$	$1w^{10} w^2 w^8 w^{10} 1$	$[82,72,4]$	$[[82,62,4]]_{2^4}$	...

5. DNA Codes Over $\mathbb{S}_k^t$

In this section, $\mathbb{S}_k^t = \frac{\mathbb{F}_{4^{2t}}[v_1,v_2,\ldots,v_k]}{\langle v_i^2 - v_i, v_iv_j - v_jv_i \rangle}$ that a special case of S_k is considered. We use $\mathbb{S}_k^t$ to obtain reversible DNA codes because the number of DNA bases is 4. Here, we present methods to generate reversible DNA codes and reversible complement DNA codes. In [27–30], there are more computational or limited operations to generate the DNA codes. Furthermore, ref. [27] applies a method that is more similar to the generator method of the coterm polynomials as in [31]. Here, the presented methods satisfy the more flexibility and variety to obtain the DNA codes rather than the method of [27–30]. In this section, we present a method that is more efficient than [29] for obtaining the idempotents. We define the structure of idempotents as follows.

We define κ to determine idempotent structure according to indices of related idempotents. κ gives the set of places of non-zero digits in a binary number that is a correspondence to an integer.

$$\kappa(r) = \kappa(r = (b_n \ldots b_2b_1)_2) = \{i | b_i \neq 0\},$$

where $r \in Z^+ \cup \{0\}$. For example, $\kappa(19) = \kappa(19 = (10011)_2) = \{1,2,5\}$.

Definition 1. *The idempotent form of* $\mathbb{S}_k^t$*:*

$$I_j = \begin{cases} v_i + 1, & \text{if } i \in \kappa(j) \\ v_i, & \text{if } i \notin \kappa(j) \end{cases}$$

Example 3. *Let us create the set of idempotents over* $\mathbb{S}_3^t$*. According to Definition 1, idempotents are:*

$$\begin{aligned}
I_0 &= v_1v_2v_3, \\
I_1 &= (v_1+1)v_2v_3, \\
I_2 &= v_1(v_2+1)v_3, \\
I_3 &= (v_1+1)(v_2+1)v_3, \\
I_4 &= v_1v_2(v_3+1), \\
I_5 &= (v_1+1)v_2(v_3+1), \\
I_6 &= v_1(v_2+1)(v_3+1), \\
I_7 &= (v_1+1)(v_2+1)(v_3+1).
\end{aligned}$$

Each elements $r \in \mathbb{S}_k^t$ is expressed by $r = a_0 I_0 + a_1 I_1 + \ldots + a_{2^k-1} I_{2^k-1}$ where $a_1, \ldots, a_{2^k-1} \in \mathbb{F}_{4^{2k}}$. Because of $\mathbb{S}_k^t = I_0\mathbb{F}_{4^{2t}} \oplus I_1\mathbb{F}_{4^{2t}} \oplus \ldots \oplus I_{2^k-1}\mathbb{F}_{4^{2t}}$. By using the structure $\mathbb{S}_k^t = I_0\mathbb{F}_{4^{2t}} \oplus I_1\mathbb{F}_{4^{2t}} \oplus \ldots \oplus I_{2^k-1}\mathbb{F}_{4^{2t}}$ for element of $\mathbb{S}_k^t$, we use the Gray map as follows:

$$\begin{aligned} \varphi : \mathbb{S}_k^t &\longrightarrow \mathbb{F}_{4^{2t}}^{2^k} \\ \alpha &\longrightarrow (\alpha_0, \alpha_1, \ldots, \alpha_{2^k-1}). \end{aligned}$$

This Gray map is a one-to-one and onto map. It can be extended to n-tuples coordinate-wise.

We use the following automorphism to satisfy the DNA reversibility over $\mathbb{S}_k^t$.

$$\begin{aligned} \theta : &\mathbb{S}_k^t \longrightarrow \mathbb{S}_k^t \\ &a \longrightarrow a^{4^t} \;\; \forall a \in \mathbb{F}_{4^{2t}}, \\ &v_i \longrightarrow v_i + 1 \;\; \forall i \in \{1, \ldots, k\}. \end{aligned}$$

We use DNA correspondences for each element of $\mathbb{F}_{4^{2t}}$ that are given in [20,32].

Lemma 3. *$\theta(I_j) = I_{2^k-1-j}$ $\forall$ $j \in \{0, 1, \ldots, 2^k - 1\}$ where I_j are idempotents of $\mathbb{S}_k^t$, $(j \in \{0, 1, \ldots, 2^k - 1\})$.*

Theorem 5. *DNA reverse of $\varphi(\beta)$ is $\varphi(\theta(\beta))$ where $\beta \in \mathbb{S}_k^t$.*

Proof of Lemma 3 and Theorem 5 is similar to Lemma 1 and Theorem 3 in [29].

The following example shows that θ reverses an element's DNA correspondence.

Example 4. *DNA 2-bases correspondence for elements of $\mathbb{F}_{16}$ is given by Table-1 in [20]. An algorithm to generate the general form of Table-1 is given by [32]. A special property of Table-1 is the fourth power of each element in $\mathbb{F}_{16}$ maps to the DNA 2-bases that are reverses of each other. The general form of this property satisfies by 4^tth power of elements in $\mathbb{F}_{4^{2t}}$.*

Let us consider the ring $\mathbb{S}_2^1$. Let α be a primitive element of $\mathbb{F}_{16}$ and $\beta = \alpha^3 I_0 + \alpha^7 I_1 + \alpha I_2 + \alpha^6 I_3 \in \mathbb{S}_2^1$. Then, $\varphi(\beta) = (\alpha^3, \alpha^7, \alpha, \alpha^6)$. Let τ maps each element of the field to DNA correspondence and it can be extended n-tuple structures. By using Table-1 ([20]), the corresponding DNA 2-bases is

$$\begin{aligned} \tau(\alpha^3, \alpha^7, \alpha, \alpha^6) &= (\tau(\alpha^3), \tau(\alpha^7), \tau(\alpha), \tau(\alpha^6)) \\ &= (AG, GT, AT, AC). \end{aligned}$$

Also,

$$\begin{aligned} \theta(\beta) &= \alpha^9 I_0 + \alpha^4 I_1 + \alpha^{13} I_2 + \alpha^{12} I_3 \\ &\Rightarrow \varphi(\theta(\beta)) = (\alpha^9, \alpha^4, \alpha^{13}, \alpha^{12}) \\ &\Rightarrow \tau(\theta(\beta)) = (\alpha^9, \alpha^4, \alpha^{13}, \alpha^{12}) = (CA, TA, TG, GA). \end{aligned}$$

Thus, $\varphi(\beta)$ and $\varphi(\theta(\beta))$ are DNA reverses of each other.

We can consider the φ for n-coordinates, also. For $\mathbf{c} = (c_0, \ldots, c_{n-2}, c_{n-1}) \in \mathbb{S}_k^t$ we have DNA correspondence of $\mathbf{c}$ as $\varphi(\mathbf{c}) = (\varphi(c_0), \ldots, \varphi(c_{n-2}), \varphi(c_{n-1}))$. Then, the DNA reverse of $\varphi(\mathbf{c})$ is $\varphi(\theta(c)^r) = (\varphi(\theta(c_{n-1})), \varphi(\theta(c_{n-2})), \ldots, \varphi(\theta(c_0)))$ where $\theta(\mathbf{c}) = (\theta(c_0), \ldots, \theta(c_{n-2}), \theta(c_{n-1}))$. We will define a θ-lifted and ρ-lifted which are special forms of General lifted [33] polynomials that are generated by using a polynomial over a base field of the rings. These polynomials will be used to generate reversible DNA codes.

Let $h(x) = b_0 + b_1 x + \ldots + b_s x^s$ be a polynomial over $\mathbb{S}_k^t$. $h(x)$ is called as palindromic polynomial if $b_i = b_{s-i}$ $\forall$ $i \in \{0, 1, \ldots, s\}$.

Definition 2. *Let $g(x) = b_0 + b_1x + \ldots + b_sx^s$ be a palindromic polynomial over $\mathbb{F}$ (finite field) and $g(x)|(x^n-1)$ over $\mathbb{F}$. A θ-lifted polynomial of $g(x)$ is denoted by $g^\theta(x) \in R$ and the ring R that is an extended from $\mathbb{F}$.*

$$g^\theta(x) = \sum_{i=0}^{\lfloor \frac{s}{2} \rfloor} \begin{cases} \beta_i x^i + \theta(\beta_i)x^{s-i}, \beta \in U(R) & , b_i \neq 0 \\ \beta_i x^i + \theta(\beta_i)x^{s-i}, \beta \in Z(R) & , b_i = 0 \end{cases} \tag{3}$$

and a ρ-lifted polynomial of $g(x)$ is denoted by $g^\rho(x) \in R$

$$g^\rho(x) = \sum_{i=0}^{\lfloor \frac{s}{2} \rfloor} \begin{cases} \beta_i x^i + \beta_i x^{s-i}, \beta \in U(R) & , b_i \neq 0 \\ \beta_i x^i + \beta_i x^{s-i}, \beta \in Z(R) & , b_i = 0 \end{cases} \tag{4}$$

where $Z(R)$ is a set of zero and zero divisors, and $U(R)$ is a set of units of R.

We define the following definition of the generator set to generate the reversible DNA codes.

Definition 3. *Let $h(x) = b_0 + b_1x + \ldots + b_sx^s$ be a polynomial over $\mathbb{S}_k^t$. θ-generator set for $h(x)$ for a code length of n is*

$$S_\theta(h(x)) = \left\{ t(x) \middle| \begin{cases} t(x) = x^i h(x) & , i \mod 2 = 0 \\ t(x) = x^i \theta(h(x)) & , i \mod 2 = 1 \end{cases} \right\} \text{ where } i \in \{0, 1, \ldots, n-1-s\}$$

and $\theta(h(x)) = \theta(b_0) + \theta(b_1)x + \ldots + \theta(b_s)x^s$.

In short, $S_\theta(h(x)) = \{h(x), x\theta(h(x)), x^2h(x), x^3\theta(h(x)), x^4h(x), \ldots\}$.

Theorem 6. *Let $g(x)$ be a palindromic polynomials dividing $x^n - 1$ (n is even) over $\mathbb{F}_{4^{2t}}$ with degree s.*

(i) If s is even, C is generated by $S_\theta(g^\rho(x))$
(ii) If s is odd, C is generated by $S_\theta(g^\theta(x))$

and $\varphi(C)$ is a reversible DNA code and C is a linear free code over $\mathbb{S}_k^t$.

Proof. Order of θ is 2 then $\theta^2(\beta) = \beta$ or $\theta^2(g(x)) = g(x)$. $\varphi(\beta \sum_i x^i \theta^i(g'(x)))$ determines the DNA correspondence of the codewords that are called DNA codewords. Reverses of DNA codewords are denoted as follows

$$\varphi(\beta \sum_i x^i \theta^i(g'(x)))^r = \varphi(\theta(\beta) \sum_i x^{n-s-1-i} \theta^{n-s-1-i}(g'(x))),$$

where $i \in \{0, 1, \ldots, n-s-1\}$ and $g'(x) = g^\theta(x)$(or $g'(x) = g^\rho(x)$). This show that each DNA codewords have its reverse in the code C. Then $\varphi(C)$ is a reversible DNA code. Each lifting operator protects the being the unit element of $\mathbb{S}_k^t$. Thus, C is a linear free code, and each generator set is linearly independent. □

Corollary 2. *Let C be a linear free code and $\varphi(C)$ be a DNA code. If C has the codeword $(\mathbf{I}, \mathbf{I}, \ldots, \mathbf{I})$ where $\mathbf{I} = I_0 + I_1 + \ldots + I_{2^k-1}$ then $\varphi(C)$ is a reversible complement DNA code.*

Corollary 3. *Let $g(x)$ be a palindromic polynomials dividing $x^n - 1$ (n is even) over $F_{4^{2t}}$ and $C =< S_\theta(g(x)) >$. If $\mathcal{I} = \mathbf{I} + \mathbf{I}x + \ldots + \mathbf{I}x^n$ is added to the generator set as $C' =< S_\theta(g(x)) \cup \mathcal{I} >$ then $\varphi(C')$ is a reversible complement DNA code.*

6. Conclusions

In this study, we generated the optimal linear codes over S_1 utilizing the algebraic structural properties of cyclic codes over S_1. In addition, we have provided a number of quantum codes $[[n,k,d]]_q$ are better than the existing quantum codes $[[n^{'}, k^{'}, d^{'}]]_q$ collected from difference references mentioned there. Skew cyclic codes can be used to extend this work. We also find the quantum codes over S_2, S_3 and so on with the same method on taking $k = 2, 3, \ldots$. Moreover, the method of generating the reversible and the reversible complement DNA codes is presented as applications of DNA codes. It satisfies an advantage which is the variety of DNA codes. Then, the determination of the distance between codes and DNA correspondence is an open problem.

Author Contributions: All authors made equal contributions. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Princess Nourah bint Abdulrahman University grant number-PNURSP2023R231.

Data Availability Statement: Data sharing is not applicable as no datasets were generated or analyzed during the current study.

Acknowledgments: The authors extend their appreciation to Princess Nourah bint Abdulrahman University (PNU), Riyadh, Saudi Arabia for funding this research under Researchers Supporting Project Number (PNURSP2023R231).

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

1. Shor, P.W. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A* **1995**, *52*, 2493–2496. [CrossRef]
2. Steane, A.M. Simple quantum error correcting codes. *Phys. Rev. A* **1996**, *54*, 4741–4751. [CrossRef] [PubMed]
3. Calderbank, A.R.; Rains, E.M.; Shor, P.M.; Sloane, N.J.A. Quantum error-correction via codes over $GF(4)$. *IEEE Trans. Inf. Theory* **1998**, *44*, 1369–1387. [CrossRef]
4. Qian, J.; Ma, W.; Gou, W. Quantum codes from cyclic codes over finite ring. *Int. J. Quantum Inf.* **2009**, *7*, 1277–1283. [CrossRef]
5. Bag, T.; Upadhyay, A.K.; Ashraf, M.; Mohammad, G. Quantum code from cyclic code over the ring $\mathbb{F}_p/\langle u^3 - u\rangle$. *Asian-Eur. J. Math.* **2020**, *13*, 2050008. [CrossRef]
6. Ashraf, M.; Mohammad, G. Quantum codes over Fp from cyclic codes over $\mathbb{F}_p[u,v]/\langle u^2-1, v^3-v, uv-vu\rangle$. *Cryptogr. Commun.* **2019**, *11*, 325–335. [CrossRef]
7. Gao, Y.; Gao, J.; Fu, F.W. Quantum codes from cyclic codes over the ring $\mathbb{F}_q + v_1\mathbb{F}_q + \ldots + v_r\mathbb{F}_q$. *Appl. Algebra Eng. Commun. Comput.* **2019**, *30*, 161–174. [CrossRef]
8. Islam, H.; Prakash, O.; Verma, R.K. Quantum codes from the cyclic codes over $\mathbb{F}_P[v,w]/\langle v^2-1, w^2-1, vw-wv\rangle$. *Springer Proc. Math. Stat.* **2019**, *307*, 67–74. [CrossRef]
9. Cengellenmis, Y.; Dertli, A.; Dougherty, S.T. Codes over an infinite family of rings with a Gray map. *Des. Codes Cryptogr.* **2014**, *72*, 559–580. [CrossRef]
10. Zheng, X.; Kong, B. Constacyclic codes over $\mathbb{F}_{p^m}[u_1, u_2, \ldots, u_k]\backslash\langle u_i^2 = u_i, u_iu_j = u_ju_i\rangle$. *Open Math.* **2018**, *16*, 490–497. [CrossRef]
11. Dertli, A.; Cengellenmis, Y.; Eren, S. On quantum codes obtained from cyclic codes over A_2. *Int. J. Quantum Inf.* **2015**, *13*, 1550031. [CrossRef]
12. Kai, X.; Zhu, S. Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. *Int. J. Quantum Inf.* **2011**, *9*, 689–700. [CrossRef]
13. Qian, J. Quantum codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. *J. Inf. Compt. Sci.* **2013**, *10*, 1715–1722. [CrossRef]
14. Islam, H.; Prakash, O. New Quantum and LCD Codes over Finite Fields of Even Characteristic. *Def. Sci. J.* **2021**, *71*, 656–661. [CrossRef]
15. Adleman, L. Molecular computation of solutions to combinatorial problems. *Science* **1994**, *266*, 1021–1024. [CrossRef]
16. Abulraub, T.; Ghrayeb, A.; Nian Zeng, X. Construction of cyclic codes over $GF(4)$ for DNA computing. *J. Frankl. Inst.* **2006**, *343*, 448–457. [CrossRef]
17. Siap, I.; Abulraub, T.; Ghrayeb, A. Similarity cyclic DNA codes over rings. In Proceedings of the International Conference on Bioinformatics and Biomedical Engineering, Shanghai, China, 16–18 May 2008.
18. Siap, I.; Abulraub, T.; Ghrayeb, A. Cyclic DNA codes over the ring $\mathbb{F}_2[u]/(u^2-1)$ based on the deletion distance. *J. Franklin Inst.* **2009**, *346*, 731–740. [CrossRef]
19. Yildiz, B.; Siap, I. Cyclic codes over $\mathbb{F}_2[u]/(u^4-1)$ and applications to DNA codes. *Comput. Math. Appl.* **2012**, *63*, 1169–1176. [CrossRef]
20. Oztas, E.S.; Siap, I. Lifted polynomials over $\mathbb{F}_{16}$ and their applications to DNA Codes. *Filomat* **2013**, *27*, 459–466. [CrossRef]
21. Faria, L.C.B.; Rocha, A.S.L.; Kleinschmidt, J.H.; Silva-Filho, M.C.; Bim, E.; Herai, R.H.; Yam-agishi, M.E.B.; Palazzo, R., Jr. Is a genome a codeword of an error-correcting code? *PLoS ONE* **2012**, *7*, e36644. [CrossRef]
22. Grassl, M.; Beth, T. On optimal quantum codes. *Int. J. Quantum Inf.* **2004**, *2*, 55–64. [CrossRef]
23. Ozen, M.; Cem, E.F.; Ince, H. Quantum codes from cyclic codes over $\mathbb{F}_4 + v\mathbb{F}_4$. *J. Appl. Math. Inform.* **2016**, *34*, 397–404. [CrossRef]

24. Grassl, M.; Beth, T. Quantum BCH codes. In Proceedings of the Proceedings X. International Symposium on Theoretical Electrical Engineering, Magdeburg, Germany, 6–9 September 1999; pp. 207–212. arXiv:quant-ph/9910060.
25. Bosma, W.; Cannon, J. *Handbook of Magma Functions*; University of Sydney: Sydney, Australia, 1995.
26. Grassl, M. Code Tables: Bounds on the Parameters of Various Types of Codes. Available online: http://www.codetables.de/ (accessed on 20 April 2021).
27. Cengellenmis, Y.; Dertli, A.; Dougherty, S.T.; Korban, A.; Sahinkaya, S.; Ustun, D. Reversible G-codes over the ring $F_{j,k}$ with applications to DNA codes. *Adv. Math. Commun.* 2021, *Early access*. [CrossRef]
28. Cengellenmis, Y.; Aydin, N.; Dertli, A. Reversible DNA codes from skew cyclic codes over a ring of order 256. *J. Algebra Comb. Discret. Struct. Appl*. **2021**, *8*, 1–8.
29. Gursoy, F.; Oztas, E.S.; Yildiz, B. Reversible DNA codes over a family of non-chain rings $R_{k,s}$. *arXiv* **2017**, arXiv:1711.02385.
30. Cengellenmis, Y.; Dertli, A. On the skew cyclic codes and the reversibility problem for DNA 4-Bases. *Math. Comput. Sci.* **2020**, *14*, 431–435. [CrossRef]
31. Oztas, E.S.; Yildiz, B.; Siap, I. A novel approach for constructing reversible codes and applications to DNA codes over the ring $\mathbb{F}_2[u]/(u^{2k}-1)$. *Finite Fields Appl.* **2017**, *46*, 217–234. [CrossRef]
32. Oztas, E.S.; Siap, I. On a generalization of lifted polynomials over finite fields and their applications to DNA codes. *Int. J. Comput. Math. Vol.* **2015**, *92*, 1976–1988. [CrossRef]
33. Oztas, E.S. Glift codes over chain ring and non-chain ring $R_{e,s}$. *Bull. Korean Math. Soc.* **2022**, *59*, 1557–1565. [CrossRef]