Kong and Zheng *EPJ Quantum Technology* (2023) 10:3
https://doi.org/10.1140/epjqt/s40507-023-00160-7

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH

Open Access

Quantum codes from constacyclic codes over S_k

Bo Kong[1*] and Xiying Zheng[2*]

*Correspondence: kongbo666@163.com; zxyccnu@163.com
[1] School of Statistics and Mathematics, Henan Finance University, Zhengzhou, 450046, Henan, China
[2] Faculty of Engineering, Huanghe Science and Technology College, Zhengzhou, 450063, Henan, China

Abstract

Let $S_k = \mathbb{F}_q[u_1, u_2, \ldots, u_k]/\langle u_i^3 = u_i, u_iu_j = u_ju_i = 0\rangle$, where $1 \leq i,j \leq k$, $q = p^m$, p is an odd prime. First, we define two new Gray maps ϕ_k and φ_k, and study their Gray images. Further, we determine the structure of constacyclic codes and their dual codes, and give a necessary and sufficient conditions of constacyclic codes to contain their duals. Finally, we obtain some new quantum codes over $\mathbb{F}_q$ by using CSS construction, and compare the constructed codes better than the existing literature.

MSC: 94B05; 94B15; 94B60

Keywords: Constacyclic codes; Quantum codes; Gray map; Dual-containing codes; CSS construction

1 Introduction

In recent years, quantum theory and technology has become a popular research in the field of information, the research progress of some mathematical problems plays a key role in the study of quantum error correction problems. Calderbank et al. [1] gave a way to construct quantum error correcting codes from classical error correcting codes, constructing quantum error correcting codes is a systematic and effective mathematical method by using constacyclic codes. There are a lot of works about constacyclic codes over finite fields and finite rings [2–10] and many good quantum codes constructed by using cyclic codes over finite rings [11–14]. Currently, some authors have obtained quantum codes from constacyclic codes over finite non-chain ring. Wang et al. [15] studied quantum codes over $\mathbb{F}_q$ from Hermitian dual-containing constacyclic codes over $\mathbb{F}_{q^2} + v\mathbb{F}_{q^2}$. Prakash et al. [16] obtained quantum codes from skew constacyclic codes over a class of non-chain rings $R_{e,q} = \mathbb{F}_q[u]/\langle u^e - 1\rangle$ by applying the CSS construction. Ashraf et al. [17] constructed quantum codes from $\mathbb{F}_qR_1R_2$-cyclic codes and introduced a Gray map to find some new and better quantum codes over $\mathbb{F}_p$. Dertli and Cengellenmis [18] studied quantum codes from constacyclic codes over the finite ring $u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, Islam and Prakash [19] constructed quantum codes from $\lambda = (\lambda_1 + u\lambda_2 + v\lambda_3)$-constacyclic codes over a class of finite commutative non-chain rings $\mathbb{F}_q[u,v]/\langle u^2 - \gamma u, v^2 - \delta v, uv = vu = 0\rangle$.

Due to the strong motivation discussed above, we construct some new quantum codes by studying the structure of constacyclic codes over a finite non-chain ring. The major two contributions of this paper are as follows.

1. In general, it is difficult to determine the structure of constacyclic codes over a finite non-chain ring, we study the structure of λ-constacyclic codes and their dual codes over the ring S_k, and give a necessary and sufficient conditions of dual-containing constacyclic codes.
2. As an application, we obtain some new quantum codes from constacyclic codes over S_k by using CSS construction and compare these codes better than the existing codes that appeared in some recent references.

2 Preliminaries

Let $S_k = \mathbb{F}_q[u_1, u_2, \ldots, u_k]/\langle u_i^3 = u_i, u_iu_j = u_ju_i = 0\rangle$, where $q = p^m$ and p is an odd prime. The ring S_k is a commutative and Frobenius ring with identity but not local, and the cardinality of S_k is $q^{(2k+1)}$.

Let $e_1 = \frac{u_1^2+u_1}{2}$, $e_2 = \frac{u_1^2-u_1}{2}, \ldots, e_{2k-1} = \frac{u_k^2+u_k}{2}$, $e_{2k} = \frac{u_k^2-u_k}{2}$, $e_{2k+1} = 1-u_1^2-u_2^2-\cdots-u_k^2$, where $e_ie_j = 0$, when $i \neq j$, and $e_i^2 = e_i$, when $i = 1, 2, \ldots, 2k+1$, and $1 = e_1 + e_2 + \cdots + e_{2k+1}$. By the Chinese Remainder Theorem we can get that

$$S_k = e_1S_k \oplus e_2S_k \oplus \cdots \oplus e_{2k+1}S_k.$$

$\forall r \in S_k$, r can be expressed uniquely as $r = r_1e_1 + r_2e_2 + \cdots + r_{2k+1}e_{2k+1}$, where $r_i \in \mathbb{F}_q$, $i = 1, 2, \ldots, 2k+1$.

By the definition above, it can be easily seen that S_k is a principal ideal ring but not a chain ring, which has $2k+1$ maximal ideals. For any element $(\lambda_1e_1 + \lambda_2e_2 + \cdots + \lambda_{2k+1}e_{2k+1})$ of S_k, $(\lambda_1e_1 + \lambda_2e_2 + \cdots + \lambda_{2k+1}e_{2k+1})$ is a unit if and only if $\lambda_1, \lambda_2, \ldots, \lambda_{2k+1}$ are units over $\mathbb{F}_q$.

If C is a code of length n over S_k, then C is a subset of S_k^n. C is a linear code of length n over S_k if and only if C is an S_k-submodule of S_k^n.

For any unit $\lambda \in S_k$, a code C is called a λ-constacyclic code of length n over S_k if and only if C is invariant under constacyclic shift operator $\sigma_\lambda : S_k^n \to S_k^n$ by

$$\sigma_\lambda(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2}).$$

When $\lambda = 1$, C is a cyclic code, when $\lambda = -1$, C is a negacyclic code.

If C is a linear code of length n over S_k, the dual code of C is defined as

$$C^\perp = \{x \mid \forall y \in C, x \cdot y = 0\},$$

where $x \cdot y = \sum_{i=0}^{n-1} x_iy_i$, $x = (x_0, x_1, \ldots, x_{n-1}) \in S_k^n$, $y = (y_0, y_1, \ldots, y_{n-1}) \in S_k^n$.

3 Gray maps

Let A be an $n \times n$ matrix, such that $AA^T = \lambda E_n$, where A^T denotes the transpose of the matrix A, E_n is the identity matrix of order n, $\lambda \in \mathbb{F}_q$ and $\lambda \neq 0$.

Definition 1 We define a Gray map $\phi_k : S_k \to \mathbb{F}_q^{2k+1}$ by $r \mapsto (r_1, r_2, \ldots, r_{2k+1})$, where $r = r_1e_1 + r_2e_2 + \cdots + r_{2k+1}e_{2k+1}$.

And ϕ_k can be expanded as:

$$\begin{aligned}\phi_k : S_k^n &\to \mathbb{F}_q^{(2k+1)n}\\ (a_0, a_1, \dots, a_{n-1}) &\mapsto \bigl(a^{(1)}A, a^{(2)}A, \dots, a^{(2k+1)}A\bigr),\end{aligned}$$

where

$$a_j = a_{1,j}e_1 + a_{2,j}e_2 + \cdots + a_{2k+1,j}e_{2k+1} \in S_k, \quad j = 0, 1, 2, \dots, n-1,$$

and

$$a^{(i)} = (a_{i,0}, a_{i,1}, \dots, a_{i,n-1}), \quad i = 1, 2, \dots, 2k+1.$$

When the Gray map is defined as ϕ_k, the Gray weight of $a \in S_k$ is defined as $w_G(a) = w_H(\phi_k(a))$, where $w_H(\phi_k(a))$ denotes the Hamming weight of $\phi_k(a)$.

The Gray weight of a vector $r = (x_1, x_2, \dots, x_n) \in S_k^n$ is defined as $w_G(r) = \sum_{i=1}^n w_G(x_i)$, the Gray distance of $x, y \in S_k^n$ is given by $d_G(x, y) = w_G(x - y)$, and the minimum Gray distance of C is defined as

$$d_G(C) = \min\bigl\{d_G(x - y), x, y \in C, x \neq y\bigr\}.$$

Lemma 1 *ϕ_k is both a bijection and a distance preserving linear map from S_k^n to $\mathbb{F}_q^{(2k+1)n}$.*

Proof Let $a = (a_0, a_1, \dots, a_{n-1}) \in S_k^n$, $b = (b_0, b_1, \dots, b_{n-1}) \in S_k^n$, $l \in \mathbb{F}_q$, where $a_j = a_{1,j}e_1 + a_{2,j}e_2 + \cdots + a_{2k+1,j}e_{2k+1} \in S_k$, $b_j = b_{1,j}e_1 + b_{2,j}e_2 + \cdots + b_{2k+1,j}e_{2k+1} \in S_k$, $j = 0, 1, 2, \dots, n-1$, $a^{(i)} = (a_{i,0}, a_{i,1}, \dots, a_{i,n-1})$, $b^{(i)} = (b_{i,0}, b_{i,1}, \dots, b_{i,n-1})$, $i = 1, 2, \dots, 2k+1$.

Then

$$\begin{aligned}\phi_k(a + b) &= \phi_k(a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1})\\ &= \bigl(\bigl(a^{(1)} + b^{(1)}\bigr)A, \bigl(a^{(2)} + b^{(2)}\bigr)A, \dots, \bigl(a^{(2k+1)} + b^{(2k+1)}\bigr)A\bigr)\\ &= \bigl(a^{(1)}A, a^{(2)}A, \dots, a^{(2k+1)}A\bigr) + \bigl(b^{(1)}A, b^{(2)}A, \dots, b^{(2k+1)}A\bigr)\\ &= \phi_k(a) + \phi_k(b),\end{aligned}$$

$$\begin{aligned}\phi_k(la) &= \phi_k(la_0, la_1, \dots, la_{n-1})\\ &= (la_0A, la_1A, \dots, la_{n-1}A)\\ &= l\bigl(a^{(1)}A, a^{(2)}A, \dots, a^{(2k+1)}A\bigr)\\ &= l\phi_k(a).\end{aligned}$$

So ϕ_k is linear.

$\forall a, b \in S_k^n$, suppose $\phi_k(a) = \phi_k(b)$, then

$$\bigl(a^{(1)}A, a^{(2)}A, \dots, a^{(2k+1)}A\bigr) = \bigl(b^{(1)}A, b^{(2)}A, \dots, b^{(2k+1)}A\bigr).$$

Because A is an invertible matrix, we have

$$\left(a^{(1)},a^{(2)},\dots,a^{(2k+1)}\right)=\left(b^{(1)},b^{(2)},\dots,b^{(2k+1)}\right),$$

so $a=b$, ϕ_k is an injection.

As

$$\left|S_k^n\right|=\left|\mathbb{F}_q^{(2k+1)n}\right|=q^{(2k+1)n},$$

so ϕ_k is a bijection.

$\forall a,b\in S_k^n$, then

$$\begin{aligned}
&a-b=(a_0-b_0,a_1-b_1,\dots,a_{n-1}-b_{n-1}),\\
&\phi_k(a-b)=\left(\left(a^{(1)}-b^{(1)}\right)A,\left(a^{(2)}-b^{(2)}\right)A,\dots,\left(a^{(2k+1)}-b^{(2k+1)}\right)A\right)=\phi_k(a)-\phi_k(b),\\
&d_G(a,b)=w_G(a-b)=w_H\left(\phi_k(a-b)\right)=w_H\left(\phi_k(a)-\phi_k(b)\right)=d_H\left(\phi_k(a),\phi_k(b)\right).
\end{aligned}$$

So ϕ_k is a distance preserving map from S_k^n to $\mathbb{F}_q^{(2k+1)n}$. $\square$

By Lemma 1 and the definition of ϕ_k, we can have the following lemma.

Lemma 2 *Let C be a linear code of length n over S_k^n and the minimal Gray distance of C is d, then $\phi_k(C)$ is a $[(2k+1)n,l,d]$ linear code over $\mathbb{F}_q$, where $l=\log_q|C|$.*

Let B be a $(2k+1)\times(2k+1)$ matrix, such that $BB^T=\lambda E_{2k+1}$, where B^T denotes the transpose of the matrix B, E_{2k+1} is the identity matrix of order $2k+1$, $\lambda\in\mathbb{F}_q$ and $\lambda\neq 0$. $\forall r=r_1e_1+r_2e_2+\cdots+r_{2k+1}e_{2k+1}\in S_k$, the vector form of r is written as $r=(r_1,r_2,\dots,r_{2k+1})$.

Definition 2 We define a Gray map $\varphi_k: S_k\to\mathbb{F}_q^{2k+1}$ by $r\mapsto rB$.

And φ_k can be expanded as

$$\begin{aligned}
\varphi_k: S_k^n&\to\mathbb{F}_q^{(2k+1)n}\\
(a_0,a_1,\dots,a_{n-1})&\mapsto(a_0B,a_1B,\dots,a_{n-1}B),
\end{aligned}$$

where $a_i=a_{1,i}e_1+a_{2,i}e_2+\cdots+a_{2k+1,i}e_{2k+1}\in S_k$, $i=0,1,2,\dots,n-1$.

When the Gray map is defined as φ_k, the Gray weight of $a\in S_k$ is defined as $w_G(a)=w_H(\varphi_k(a))$, where $w_H(\varphi_k(a))$ denotes the Hamming weight of $\varphi_k(a)$.

The Gray weight of a vector $r=(x_1,x_2,\dots,x_n)\in S_k^n$ is defined as $w_G(r)=\sum_{i=1}^n w_G(x_i)$, the Gray distance of $x,y\in S_k^n$ is given by $d_G(x,y)=w_G(x-y)$, and the minimum Gray distance of C is defined as

$$d_G(C)=\min\left\{d_G(x-y),x,y\in C,x\neq y\right\}.$$

Lemma 3 *φ_k is both a bijection and a distance preserving linear map from S_k^n to $\mathbb{F}_q^{(2k+1)n}$.*

Proof Let $a,b \in S_k^n$, where $a = (a_0,a_1,\dots,a_{n-1})$, $b = (b_0,b_1,\dots,b_{n-1})$, $l \in \mathbb{F}_q$. Then

$$\begin{aligned}\varphi_k(a+b) &= \varphi_k(a_0+b_0,a_1+b_1,\dots,a_{n-1}+b_{n-1})\\ &= \big((a_0+b_0)B,(a_1+b_1)B,\dots,(a_{n-1}+b_{n-1})B\big)\\ &= (a_0B,a_1B,\dots,a_{n-1}B)+(b_0B,b_1B,\dots,b_{n-1}B)\\ &= \varphi_k(a)+\varphi_k(b),\end{aligned}$$

$$\begin{aligned}\varphi_k(la) &= \phi_k(la_0,la_1,\dots,la_{n-1}) = (la_0B,la_1B,\dots,la_{n-1}B)\\ &= l(a_0B,a_1B,\dots,a_{n-1}B)\\ &= l\phi_k(a).\end{aligned}$$

So φ_k is linear.

$\forall a,b \in S_k^n$, suppose $\varphi_k(a) = \varphi_k(b)$, then

$$(a_0B,a_1B,\dots,a_{n-1}B) = (b_0B,b_1B,\dots,b_{n-1}B).$$

Because B is an invertible matrix, we have $a = (a_0,a_1,\dots,a_{n-1}) = (b_0,b_1,\dots,b_{n-1}) = b$, φ_k is an injection.

As

$$\left|S_k^n\right| = \left|\mathbb{F}_q^{(2k+1)n}\right| = q^{(2k+1)n},$$

so φ_k is a bijection.

$\forall a,b \in S_k^n$, then

$$\begin{aligned}&a-b = (a_0-b_0,a_1-b_1,\dots,a_{n-1}-b_{n-1}),\\ &\varphi_k(a-b) = \big((a_0-b_0)B,(a_1-b_1)B,\dots,(a_{n-1}-b_{n-1})B\big) = \varphi_k(a)-\varphi_k(b),\\ &d_G(a,b) = w_G(a-b) = w_H\big(\varphi_k(a-b)\big) = w_H\big(\varphi_k(a)-\varphi_k(b)\big) = d_H\big(\varphi_k(a),\varphi_k(b)\big).\end{aligned}$$

So φ_k is a distance preserving map from S_k^n to $\mathbb{F}_q^{(2k+1)n}$. □

By Lemma 3 and the definition of φ_k, we can have the following lemma.

Lemma 4 *Let C be a linear code of length n over S_k^n and the minimal Gray distance of C is d, then $\varphi_k(C)$ is a $[(2k+1)n,l,d]$ linear code over $\mathbb{F}_q$, where $l = \log_q|C|$.*

4 Constacyclic codes over S_k

Let C be a linear code of length n over S_k and define

$$C_j = \left\{x_j \in \mathbb{F}_q^n \,\middle|\, \sum_{i=1}^{2k+1} x_ie_i \in C, x_i \in \mathbb{F}_q^n\right\},\quad j = 1,2,\dots,2k+1,$$

then, $C_1,C_2,\dots,C_{2k+1}$ are linear codes of length n over $\mathbb{F}_q$.

Moreover, the linear code C of length n over S_k can be represented as

$$C = \bigoplus_{j=1}^{2k+1} e_j C_j.$$

Let G_j be the Generator matrices of C_j, then the Generator matrix of C is

$$G = \begin{bmatrix} e_1 G_1 \\ e_2 G_2 \\ \cdots \\ e_{2k+1} G_{2k+1} \end{bmatrix}.$$

Definition 3 We define a quasi-cyclic shift on $(\mathbb{F}_q^n)^{2k+1}$,

$$\begin{aligned}
&\psi_{2k+1}(a_{1,0}, a_{1,1} \cdots, a_{1,n-1}, a_{2,0}, a_{2,1} \cdots, a_{2,n-1},\\
&\quad \cdots, a_{2k+1,0}, a_{2k+1,1} \cdots, a_{2k+1,n-1})\\
&\quad = \bigl(\sigma(a_{1,0}, a_{1,1} \cdots, a_{1,n-1}), \sigma(a_{2,0}, a_{2,1} \cdots, a_{2,n-1}),\\
&\quad \cdots, \sigma(a_{2k+1,0}, a_{2k+1,1} \cdots, a_{2k+1,n-1})\bigr).
\end{aligned}$$

Proposition 1 *Let σ be the cyclic shift operator on S_k^n, let ψ_{2k+1} be the quasi-cyclic shift on $(\mathbb{F}_q^n)^{2k+1}$ defined as above. Then $\phi_k \sigma = \psi_{2k+1} \phi_k$.*

Proof Let $(a_0, a_1, \ldots, a_{n-1}) \in S_k^n$, where $a_j = a_{1,j}e_1 + a_{2,j}e_2 + \cdots + a_{2k+1,j}e_{2k+1} \in S_k$, $j = 0, 1, 2, \ldots, n-1$, $a^{(i)} = (a_{i,0}, a_{i,1}, \ldots, a_{i,n-1})$, $i = 1, 2, \ldots, 2k+1$.

$$\begin{aligned}
&\phi_k(a_0, a_1, \ldots, a_{n-1}) = \bigl(a^{(1)}A, a^{(2)}A, \ldots, a^{(2k+1)}A\bigr),\\
&\sigma(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}, a_0, \ldots, a_{n-2}).
\end{aligned}$$

If we apply ϕ_k, we can have

$$\begin{aligned}
\phi_k\bigl(\sigma(a_0, a_1, \ldots, a_{n-1})\bigr) &= \phi_k(a_{n-1}, a_0, \ldots, a_{n-2})\\
&= \bigl((a_{1,n-1}, a_{1,0}, \ldots, a_{1,n-2})A, (a_{2,n-1}, a_{2,0}, \ldots, a_{2,n-2})A,\\
&\quad \cdots, (a_{2k+1,n-1}, a_{2k+1,0}, \ldots, a_{2k+1,n-2})A\bigr).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\psi_{2k+1}\bigl(\phi_k(a_0, a_1, \ldots, a_{n-1})\bigr) &= \psi_{2k+1}\bigl(a^{(1)}A, a^{(2)}A, \ldots, a^{(2k+1)}A\bigr)\\
&= \bigl(\sigma\bigl(a^{(1)}A\bigr), \sigma\bigl(a^{(2)}A\bigr), \ldots, \sigma\bigl(a^{(2k+1)}A\bigr)\bigr)\\
&= \bigl((a_{1,n-1}, a_{1,0}, \ldots, a_{1,n-2})A,\\
&\quad (a_{2,n-1}, a_{2,0}, \ldots, a_{2,n-2})A,\\
&\quad \cdots, (a_{2k+1,n-1}, a_{2k+1,0}, \ldots, a_{2k+1,n-2})A\bigr)\\
&= \phi_k\bigl(\sigma(a_0, a_1, \ldots, a_{n-1})\bigr).
\end{aligned}$$

Thus $\phi_k \sigma = \psi_{2k+1} \phi_k$. □

Proposition 2 *Let σ and ψ_{2k+1} be defined as above, then a linear code C of length n over S_k is a cyclic code if and only if $\phi_k(C)$ is a quasi cyclic code of index $2k+1$ of length $(2k+1)n$ over $\mathbb{F}_q$.*

Proof If C is a cyclic code of length n over S_k. Then $\sigma(C) = C$. We can have $\phi_k(\sigma(C)) = \phi_k(C)$.

By Proposition 1,

$$\phi_k\bigl(\sigma(C)\bigr) = \psi_{2k+1}\bigl(\phi_k(C)\bigr) = \phi_k(C).$$

So, $\phi_k(C)$ is a quasi-cyclic code of index $2k+1$ of length $(2k+1)n$ over $\mathbb{F}_q$.

Conversely, suppose $\phi_k(C)$ is a quasi-cyclic code of index $2k+1$ of length $(2k+1)n$ over $\mathbb{F}_q$, then $\psi_{2k+1}(\phi_k(C)) = \phi_k(C)$.

By Proposition 1, we have $\psi_{2k+1}(\phi_k(C)) = \phi_k(\sigma(C)) = \phi_k(C)$.

Since ϕ_k is a bijective linear map, so $\sigma(C) = C$. □

Theorem 1 *Let $\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1}$ be a unit of S_k. Let $C = \bigoplus_{j=1}^{2k+1} e_j C_j$ be a linear code of length n over S_k, then C is a $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$-constacyclic code over S_k if and only if C_i is a λ_i-constacyclic code over $\mathbb{F}_q$, where $i = 1, 2, \ldots, 2k+1$.*

Proof $\forall c_i = (c_{i,0}, c_{i,1}, \ldots, c_{i,n-1}) \in C_i$, where $i = 1, 2, \ldots, 2k+1$.

$$c = e_1 c_1 + e_2 c_2 + \cdots + e_{2k+1} c_{2k+1} = \left(\sum_{i=1}^{2k+1} e_i c_{i,0}, \sum_{i=1}^{2k+1} e_i c_{i,1}, \ldots, \sum_{i=1}^{2k+1} e_i c_{i,n-1}\right) \in C.$$

$\forall \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1} \in S_k$, it's easy to know that $\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1} \in S_k$ is a unit if and only if $\lambda_i \neq 0$, that is, λ_i is a unit over $\mathbb{F}_q$, where $i = 1, 2, \ldots, 2k+1$.

If C_i is a λ_i-constacyclic code over $\mathbb{F}_q$, $i = 1, 2, \ldots, 2k+1$, then

$$\sigma_{\lambda_i}(c_i) = \sigma_{\lambda_i}(c_{i,0}, c_{i,1}, \ldots, c_{i,n-1}) = (\lambda_i c_{i,n-1}, c_{i,0}, \ldots, c_{i,n-2}) \in C_i,$$

and

$$\begin{aligned}
&\sigma_{\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1}}(c) \\
&\quad = \left((\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1}) \sum_{i=1}^{2k+1} e_i c_{i,n-1}, \sum_{i=1}^{2k+1} e_i c_{i,0}, \ldots, \sum_{i=1}^{2k+1} e_i c_{i,n-2}\right) \\
&\quad = e_1 \sigma_{\lambda_1}(c_1) + e_2 \sigma_{\lambda_2}(c_2) + \cdots + e_{2k+1} \sigma_{\lambda_{2k+1}}(c_{2k+1}) \in C.
\end{aligned}$$

So C is a $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$-constacyclic code over S_k.

Conversely, if C is a $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$-constacyclic code over S_k, we have

$$\sigma_{\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1}}(c) = e_1 \sigma_{\lambda_1}(c_1) + e_2 \sigma_{\lambda_2}(c_2) + \cdots + e_{2k+1} \sigma_{\lambda_{2k+1}}(c_{2k+1}) \in C.$$

So $\sigma_{\lambda_i}(c_i) \in C_i$, C_i is a λ_i-constacyclic code over $\mathbb{F}_q$, $i = 1, 2, \ldots, 2k+1$. □

Theorem 2 *Let* $C = \bigoplus_{j=1}^{2k+1} e_jC_j$ *be a* $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1}e_{2k+1})$*-constacyclic code of length* n *over* S_k*, then* $C = \langle e_1g_1(x) + e_2g_2(x) + \cdots + e_{2k+1}g_{2k+1}(x)\rangle$*, where* g_i *is the generator polynomial of* C_i*,* $i = 1, 2, \ldots, 2k + 1$*.*

Proof Let $C = \bigoplus_{j=1}^{2k+1} e_jC_j$ be a $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1}e_{2k+1})$-constacyclic n over S_k, by Theorem 1, we get that C_i is a λ_i-constacyclic code over $\mathbb{F}_q$, $i = 1, 2, \ldots, 2k + 1$.

Because the generator polynomial of C_i is $g_i(x)$, $i = 1, 2, \ldots, 2k + 1$. Then

$$C = \bigl\langle e_1g_1(x), e_2g_2(x), \ldots, e_{2k+1}g_{2k+1}(x)\bigr\rangle.$$

Let $C' = \langle e_1g_1(x) + e_2g_2(x) + \cdots + e_{2k+1}g_{2k+1}(x)\rangle$. So $C' \subseteq C$.

Because $e_i[e_1g_1(x) + e_2g_2(x) + \cdots + e_{2k+1}g_{2k+1}(x)] = e_ig_i(x), i = 1, 2, \ldots, 2k + 1$. So $C \subseteq C'$.

So, we have $C = C'$, and the generator polynomial of C is

$$g(x) = e_1g_1(x) + e_2g_2(x) + \cdots + e_{2k+1}g_{2k+1}(x).$$

Because $g_i(x)$ is the generator polynomial of C_i, g_i divides $x^n - \lambda_i$, $i = 1, 2, \ldots, 2k + 1$. Let $g_i(x)f_i(x) = x^n - \lambda_i$, $i = 1, 2, \ldots, 2k + 1$.

Then

$$\begin{aligned}&\bigl[e_1g_1(x) + e_2g_2(x) + \cdots + e_{2^k}g_{2k+1}(x)\bigr]\bigl[e_1f_1(x) + e_2f_2(x) + \cdots + e_{2k+1}f_{2k+1}(x)\bigr]\\ &\quad = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1}e_{2k+1}.\end{aligned}$$

So

$$e_1g_1(x) + e_2g_2(x) + \cdots + e_{2k+1}g_{2k+1}(x) \mid x^n - (\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1}e_{2k+1}). \qquad \square$$

Theorem 3 *Let* $C = \bigoplus_{j=1}^{2k+1} e_jC_j$ *be a linear code of length* n *over* S_k*, let* $C_j^\perp$ *be the dual code of* C_j*, then* $C^\perp = \sum_{j=1}^{2k+1} e_jC_j^\perp$*, where* $j = 1, 2, \ldots, 2k + 1$*.*

Proof Let $\tilde{C} = \bigoplus_{j=1}^{2k+1} e_jC_j^\perp$, $\forall x = \sum_{j=1}^{2k+1} e_jx_j \in C$, $\forall \tilde{x} = \sum_{j=1}^{2k+1} e_j\tilde{x}_j \in \tilde{C}$, where $x_j \in C_j$, $\tilde{x}_j \in C_j^\perp$.

Since $x_j\tilde{x}_j = 0$, it follows that $x \cdot \tilde{x} = \sum_{j=1}^{2k+1}(x_j\tilde{x}_j)e_j = 0$.

So, $\tilde{C} \subseteq C^\perp$.

Since $|C||C^\perp| = |S_k|^n$, we have

$$|\tilde{C}| = \prod_{j=1}^{2k+1} \bigl|C_j^\perp\bigr| = \prod_{j=1}^{2k+1} \frac{q^n}{|C_j|} = \frac{|S_k|^n}{|C|} = \bigl|C^\perp\bigr|.$$

So

$$C^\perp = \tilde{C}. \qquad \square$$

Theorem 4 *Let* $C = \bigoplus_{j=1}^{2k+1} e_jC_j$ *be a* $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1}e_{2k+1})$*-constacyclic code of length* n *over* S_k*, then*

$$C^\perp = \bigl\langle e_1f_1^*(x) + e_2f_2^*(x) + \cdots + e_{2k+1}f_{2k+1}^*(x)\bigr\rangle, \bigl|C^\perp\bigr| = q^{(\sum_{i=1}^{2k+1}\deg(g_i))},$$

$f_i^*(x)$ is the reciprocal polynomial of $f_i(x) = (x^n - \lambda_i)/g_i(x)$ which is defined as $f_i^*(x) = x^{\deg(f_i)} f_i(x^{-1})$, where g_i is the generator polynomial of C_i, $i = 1, 2, \dots, 2k+1$.

Proof Let $C_i = \langle g_i(x)\rangle$ be a λ_i-constacyclic code of length n over $\mathbb{F}_q$, $i = 1, 2, \dots, 2k+1$. $\forall x = (x_0, x_1, \dots, x_{n-1}) \in C_i^\perp$, $\forall y = (y_0, y_1, \dots, y_{n-1}) \in C_i$, then $\sigma_{\lambda_i}^{n-1}(y) = (\lambda_i y_1, \lambda_i y_2, \dots, \lambda_i y_{n-1}, y_0) \in C_i$, and

$$\begin{aligned} 0 = x \cdot \sigma_{\lambda_i}^{n-1}(y) &= \lambda_i x_0 y_1 + \lambda_i x_1 y_2 + \cdots + \lambda_i x_{n-2} y_{n-1} + x_{n-1} y_0 \\ &= \lambda_i \bigl(x_0 y_1 + x_1 y_2 + \cdots + x_{n-2} y_{n-1} + \lambda_i^{-1} x_{n-1} y_0\bigr) \\ &= \lambda_i \sigma_{\lambda_i^{-1}}(x) \cdot y. \end{aligned}$$

So, $\sigma_{\lambda_i^{-1}}(x) \in C_i^\perp$, $C_i^\perp$ is a λ_i^{-1}-constacyclic code over $\mathbb{F}_q$.

Let $\tilde{C}_i = \langle f_i^*(x)\rangle$,

$$\begin{aligned} f_i^*(x) g_i^*(x) &= x^{\deg(f_i)} f_i\bigl(x^{-1}\bigr) x^{\deg(g_i)} g_i\bigl(x^{-1}\bigr) \\ &= x^{\deg(f_i)} \bigl(x^{-n} - \lambda_i\bigr)/g_i\bigl(x^{-1}\bigr) x^{\deg(g_i)} g_i\bigl(x^{-1}\bigr) \\ &= 1 - x^n \lambda_i = -\lambda_i \bigl(x^n - \lambda_i^{-1}\bigr) \end{aligned}$$

we have $f_i^*(x) \mid (x^n - \lambda_i^{-1})$, so $\tilde{C}_i \subseteq C_i^\perp$.

Because $|\tilde{C}_i| = q^{n-\deg f_i^*} = q^{\deg g_i} = \frac{q^n}{|C_i|} = |C_i^\perp|$, we have $C_i^\perp = \tilde{C}_i = \langle f_i^*(x)\rangle$, $i = 1, 2, \dots, 2k+1$.

By Theorem 3, $C^\perp = \sum_{j=1}^{2k+1} e_j C_j^\perp$, we have $|C^\perp| = \prod_{j=1}^{2k+1} |C_j^\perp| = q^{(\sum_{i=1}^{2k+1} \deg(g_i))}$, and we can get the form of $C^\perp$ is

$$C^\perp = \bigl\langle e_1 f_1^*(x), e_2 f_2^*(x), \dots, e_{2k+1} f_{2k+1}^*(x)\bigr\rangle.$$

Let $\tilde{C}' = \langle e_1 f_1^*(x) + e_2 f_2^*(x) + \cdots + e_{2k+1} f_{2k+1}^*(x)\rangle$. Then $\tilde{C}' \subseteq C^\perp$.

Because

$$e_i\bigl[e_1 f_1^*(x), e_2 f_2^*(x), \dots, e_{2k+1} f_{2k+1}^*(x)\bigr] = e_i f_i^*(x), \quad i = 1, 2, \dots, 2k+1.$$

So $C^\perp \subseteq \tilde{C}'$.

We have

$$C^\perp = \tilde{C}' = \bigl\langle e_1 f_1^*(x) + e_2 f_2^*(x) + \cdots + e_{2k+1} f_{2k+1}^*(x)\bigr\rangle. \qquad \square$$

5 Quantum codes from constacyclic codes over S_k

Theorem 5 *Let C be a linear code of length n over S_k, then*

$$\phi_k(C)^\perp = \phi_k\bigl(C^\perp\bigr), \qquad \varphi_k(C)^\perp = \varphi_k\bigl(C^\perp\bigr).$$

Proof Let $a = (a_0, a_1, \dots, a_{n-1}) \in C$, $b = (b_0, b_1, \dots, b_{n-1}) \in C^\perp$, where $a_j = a_{1,j} e_1 + a_{2,j} e_2 + \cdots + a_{2k+1,j} e_{2k+1}$, $b_j = b_{1,j} e_1 + b_{2,j} e_2 + \cdots + b_{2k+1,j} e_{2k+1} \in S_k$, $j = 0, 1, 2, \dots, n-1$, $a^{(i)} = (a_{i,0}, a_{i,1}, \dots, a_{i,n-1})$, $b^{(i)} = (b_{i,0}, b_{i,1}, \dots, b_{i,n-1})$, $i = 1, 2, \dots, 2k+1$.

Then

$$a \cdot b = \sum_{j=0}^{n-1} a_j b_j = \sum_{j=0}^{n-1} \sum_{i=1}^{2k+1} a_{i,j} b_{i,j} e_i = \sum_{i=1}^{2k+1} a^{(i)} {b^{(i)}}^T e_i = 0.$$

So

$$a^{(i)} {b^{(i)}}^T = 0, \quad i = 1, 2, \dots, 2k+1.$$

Since

$$\phi_k(a) = \left(a^{(1)}A, a^{(2)}A, \dots, a^{(2k+1)}A\right), \qquad \phi_k(b) = \left(b^{(1)}A, b^{(2)}A, \dots, b^{(2k+1)}A\right).$$

It follows that

$$\begin{aligned}\phi_k(a) \cdot \phi_k(b) &= \phi_k(a)\phi_k(b)^T \\ &= \sum_{i=1}^{2k+1} a^{(i)} A A^T {b^{(i)}}^T = \sum_{i=1}^{2k+1} a^{(i)} \lambda E_n {b^{(i)}}^T \\ &= \lambda \sum_{i=1}^{2k+1} a^{(i)} {b^{(i)}}^T = 0.\end{aligned}$$

So we have

$$\phi_k\left(C^\perp\right) \subseteq \phi_k(C)^\perp.$$

As ϕ_k is a bijection, and

$$|C| = \left|\phi_k(C)\right|.$$

Then

$$\left|\phi_k\left(C^\perp\right)\right| = \frac{q^{(2k+1)n}}{|C|} = \frac{q^{(2k+1)n}}{|\phi_k(C)|} = \left|\phi_k(C)^\perp\right|.$$

So

$$\phi_k(C)^\perp = \phi_k\left(C^\perp\right).$$

Let

$$c = (c_1, c_2, \dots, c_n) \in C, \qquad d = (d_1, d_2, \dots, d_n) \in C^\perp,$$

then

$$\varphi_k(c) = (c_1 B, c_2 B, \dots, c_n B), \qquad \varphi_k(d) = (d_1 B, d_2 B, \dots, d_n B).$$

The vector forms of c_i and d_i are respectively

$$c_i = (c_{i1}, c_{i2}, \dots, c_{i(2k+1)}), \qquad d_i = (d_{i1}, d_{i2}, \dots, d_{i(2k+1)}), \quad i = 1, 2, \dots, n.$$

Then

$$\begin{aligned}\varphi_k(c) \cdot \varphi_k(d) &= \varphi_k(c)\varphi_k(d)^T \\ &= \sum_{i=1}^{n} c_i B B^T d_i^T = \sum_{i=1}^{n} c_i \lambda E_{2k+1} d_i^T = \lambda \sum_{i=1}^{n} c_i d_i^T = 0.\end{aligned}$$

So we have

$$\varphi_k\bigl(C^\perp\bigr) \subseteq \varphi_k(C)^\perp.$$

As φ_k is a bijection, and

$$|C| = \bigl|\varphi_k(C)\bigr|.$$

Then

$$\bigl|\varphi_k\bigl(C^\perp\bigr)\bigr| = \frac{q^{(2k+1)n}}{|C|} = \frac{q^{(2k+1)n}}{|\varphi_k(C)|} = \bigl|\varphi_k(C)^\perp\bigr|.$$

Therefore,

$$\varphi_k(C)^\perp = \varphi_k\bigl(C^\perp\bigr).$$

□

Theorem 6 *Let $C = \bigoplus_{j=1}^{2k+1} e_j C_j$ be a linear code of length n over S_k, then C is a self-orthogonal code over S_k if and only if C_j is a self-orthogonal code over $\mathbb{F}_q$, if C is a self-orthogonal code over S_k, then $\phi_k(C)$ and $\varphi_k(C)$ are self-orthogonal codes over $\mathbb{F}_q$, where $j = 1, 2, \dots, 2k + 1$.*

Proof By using Theorem 1, we have $C \subseteq C^\perp$ if and only if $C_j \subseteq C_j^\perp$, so C is a self-orthogonal code over S_k if and only if C_j is a self-orthogonal code over $\mathbb{F}_q$, where $j = 1, 2, \dots, 2k + 1$.

Let C be a self-orthogonal code, $\forall a = (a_0, a_1, \dots, a_{n-1})$, $b = (b_0, b_1, \dots, b_{n-1}) \in C$, $a_j = a_{1,j}e_1 + a_{2,j}e_2 + \cdots + a_{2k+1,j}e_{2k+1}$, $b_j = b_{1,j}e_1 + b_{2,j}e_2 + \cdots + b_{2k+1,j}e_{2k+1} \in S_k$, $j = 0, 1, 2, \dots, n-1$, $a^{(i)} = (a_{i,0}, a_{i,1}, \dots, a_{i,n-1})$, $b^{(i)} = (b_{i,0}, b_{i,1}, \dots, b_{i,n-1})$, $i = 1, 2, \dots, 2k + 1$.

Then

$$a \cdot b = \sum_{j=0}^{n-1} a_j b_j = \sum_{j=0}^{n-1} \sum_{i=1}^{2k+1} a_{i,j} b_{i,j} e_i = \sum_{i=1}^{2k+1} a^{(i)} {b^{(i)}}^T e_i = 0.$$

So,

$$a^{(i)} {b^{(i)}}^T = 0, \quad i = 1, 2, \dots, 2k + 1.$$

It follows that

$$\begin{aligned}\phi_k(a)\cdot\phi_k(b) &= \phi_k(a)\phi_k(b)^T \\ &= \sum_{i=1}^{2k+1} a^{(i)}AA^T{b^{(i)}}^T = \sum_{i=1}^{2k+1} a^{(i)}\lambda E_n {b^{(i)}}^T = \lambda\sum_{i=1}^{2k+1} a^{(i)}{b^{(i)}}^T = 0.\end{aligned}$$

So $\phi_k(C)$ is a self-orthogonal code over $\mathbb{F}_q$.

Let $c = (c_1, c_2, \ldots, c_n) \in C$, $d = (d_1, d_2, \ldots, d_n) \in C$, then

$$\varphi_k(c) = (c_1B, c_2B, \ldots, c_nB), \qquad \varphi_k(d) = (d_1B, d_2B, \ldots, d_nB).$$

$$c_i = c_{i,1}e_1 + c_{i,2}e_2 + \cdots + c_{i,2k+1}e_{2k+1} \in S_k,$$

$$d_i = d_{i,1}e_1 + d_{i,2}e_2 + \cdots + d_{i,2k+1}e_{2k+1} \in S_k,$$

where $i = 1, 2, \ldots, n$.

The vector forms of c_i and d_i are respectively

$$c_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,2k+1}), \qquad d_i = (d_{i,1}, d_{i,2}, \ldots, d_{i,2k+1}), \quad i = 1, 2, \ldots, n.$$

Since C is a self-orthogonal code,

$$c\cdot d = \sum_{j=1}^{n} c_j d_j = \sum_{i=1}^{n}\sum_{j=1}^{2k+1} c_{i,j}d_{i,j}e_i = \sum_{i=1}^{2k+1} c_i {d_i}^T e_i = 0.$$

So,

$$c_i {d_i}^T = 0, \quad i = 1, 2, \ldots, 2k+1.$$

Then,

$$\begin{aligned}\varphi_k(c)\cdot\varphi_k(d) &= \varphi_k(c)\varphi_k(d)^T \\ &= \sum_{i=1}^{n} c_i BB^T d_i^T = \sum_{i=1}^{n} c_i\lambda E_{2k+1} d_i^T = \lambda\sum_{i=1}^{n} c_i d_i^T = 0.\end{aligned}$$

So $\varphi_k(C)$ is a self-orthogonal code over $\mathbb{F}_q$. □

Lemma 5 *Let C be a constacyclic code over $\mathbb{F}_q$, the generator polynomial is $g(x)$. Then, C contains its dual code if and only if $x^n - \lambda \equiv 0 (\bmod\, g(x)g^*(x))$, where $g^*(x)$ is the reciprocal polynomial of $g(x)$, $\lambda = \pm 1$.*

Proof Let $C^\perp = \langle f^*(x)\rangle$ be the dual code of C, where $f(x) = (x^n - \lambda)/g(x)$, $\lambda = \pm 1$. C contains its dual code if and only if there exists $h(x) \in \mathbb{F}_q[x]$, such that $f^*(x) = g(x)h(x)$ if and only if $g^*(x)g(x) = \frac{\lambda(x^n-\lambda^{-1})}{f^*(x)}g(x) = \frac{\lambda(x^n-\lambda^{-1})}{g(x)h(x)}g(x) = \frac{\lambda(x^n-\lambda)}{h(x)}$ if and only if $(x^n - \lambda) = \lambda^{-1}g^*(x)g(x)h(x) \equiv 0(\bmod g(x)g^*(x))$. □

Theorem 7 (CSS construction, [20]) *Let $C_1 = [n, k_1, d_1]q$ and $C_2 = [n, k_2, d_2]q$ be linear codes over $\mathbb{F}_q$, with $C_2^\perp \subseteq C_1^\perp$. Let $d = \min(d_1, d_2)$, then there exists a quantum error-correcting code C with parameters $C = [[n, k_1 + k_2 - n, \geq d]]_q$. In particular, if $C_1^\perp \subseteq C_1$, then there exists a quantum error-correcting code $C = [[n, 2k_1 - n, \geq d_1]]_q$.*

Theorem 8 *Let $C = \bigoplus_{j=1}^{2k+1} e_j C_j$ be a $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$-constacyclic code of length n over S_k, where $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$ is a unit in S_k. Then $C^\perp \subseteq C$ if and only if $x^n - \lambda_i \equiv 0(\bmod g_i(x)\tilde{g}_i(x))$, where g_i is the generator polynomial of C_i, $\tilde{g}_i(x) = \frac{1}{g_i(0)} g_i^*(x) = \frac{1}{g_i(0)} x^{\deg g_i} g_i(x^{-1})$, $i = 1, 2, \ldots, 2k + 1$.*

Proof If $x^n - \lambda_i \equiv 0(\bmod g_i(x)\tilde{g}_i(x))$, by Lemma 5, we have $C_i^\perp \subseteq C_i$, $i = 1, 2, \ldots, 2k + 1$, then $e_i C_i^\perp \subseteq e_i C_i$, so $C^\perp = \bigoplus_{j=1}^{2k+1} e_j C_j^\perp \subseteq \bigoplus_{j=1}^{2k+1} e_j C_j = C$.

Conversely, let $C^\perp \subseteq C$, then $C^\perp = \bigoplus_{j=1}^{2k+1} e_j C_j^\perp \subseteq \bigoplus_{j=1}^{2k+1} e_j C_j = C$, we have $C_i^\perp \subseteq C_i$, by Lemma 5, we have $x^n - \lambda_i \equiv 0(\bmod g_i(x)\tilde{g}_i(x))$ $i = 1, 2, \ldots, 2k + 1$. □

By using Lemma 5 and Theorem 8, we can have the following corollary.

Corollary 1 *Let $C = \bigoplus_{j=1}^{2k+1} e_j C_j$ be a $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$-constacyclic code of length n over S_k, where $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$ is a unit in S_k. Then $C^\perp \subseteq C$ if and only if $C_i^\perp \subseteq C_i$, where C_i is a λ_i-constacyclic code of length n over $\mathbb{F}_q$, $\lambda_i = \pm 1$, $i = 1, 2, \ldots, 2k + 1$.*

By using Theorem 7 and Theorem 8 we can have the following theorems.

Theorem 9 *Let $C = \bigoplus_{j=1}^{2k+1} e_j C_j$ be a $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$-constacyclic code of length n over S_k. Let C_i be a λ_i-constacyclic code of length n over $\mathbb{F}_q$, $C_i^\perp \subseteq C_i$, where $\lambda_i = \pm 1$, $i = 1, 2, \ldots, 2k + 1$, then $C^\perp \subseteq C$ and there exists a quantum error-correcting code with parameters $[[(2k + 1)n, 2l - (2k + 1)n, \geq d]]_q$, where d is the minimum Gray weight of code C, and l is the dimension of the linear code $\phi_k(C)$.*

Theorem 10 *Let $C = \bigoplus_{j=1}^{2k+1} e_j C_j$ be a $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k+1} e_{2k+1})$-constacyclic code of length n over S_k. Let C_i be a λ_i-constacyclic code of length n over $\mathbb{F}_q$, $C_i^\perp \subseteq C_i$, where $\lambda_i = \pm 1$, $i = 1, 2, \ldots, 2k + 1$, then $C^\perp \subseteq C$ and there exists a quantum error-correcting code with parameters $[[(2k + 1)n, 2l - (2k + 1)n, \geq d]]_q$, where d is the minimum Gray weight of code C, and l is the dimension of the linear code $\varphi_k(C)$.*

Example 1 Let

$$B = \begin{bmatrix} 1 & -2 & 2 & 0 & 0 \\ -2 & 1 & 2 & 0 & 0 \\ 2 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix},$$

$S_2 = \mathbb{F}_5[u_1, u_2]/\langle u_1^3 = u_1, u_2^3 = u_2, u_1 u_2 = u_2 u_1 = 0\rangle$, $e_1 = \frac{u_1^2 + u_1}{2}$, $e_2 = \frac{u_1^2 - u_1}{2}$, $e_3 = \frac{u_2^2 + u_2}{2}$, $e_4 = \frac{u_2^2 - u_2}{2}$, $e_5 = 1 - u_1^2 - u_2^2$, when $n = 30$,

$$x^{30} + 1 = (x + 2)^5 (x + 3)^5 (x^2 + 2x + 4)^5 (x^2 + 3x + 4)^5,$$

$$x^{30} - 1 = (x + 1)^5 (x + 4)^5 (x^2 + x + 1)^5 (x^2 + 4x + 1)^5 \quad \text{in } \mathbb{F}_5(x).$$

Let C be a $(1-2u_2^2)$-constacyclic code of length 30 over S_2 with generator polynomial $e_1g_1(x)+e_2g_2(x)+e_3g_3(x)+e_4g_4(x)+e_5g_5(x)$, where $g_1 = x+1$, $g_2 = x+4$, $g_3 = x+2$, $g_4 = x+3$, $g_5 = x+1$, then $x^n-1 \equiv 0(\mathrm{mod} g_i(x)\tilde{g}_i(x))$, when $i = 1,2,5$, $x^n+1 \equiv 0(\mathrm{mod} g_i(x)\tilde{g}_i(x))$, when $i = 3,4$. By using Theorem 8, we have $C^{\perp} \subseteq C$ and $\phi_2(C)$ is a linear code over $\mathbb{F}_5$ with parameters $[150,145,2]$. By Theorem 9, we know that there is a quantum error correcting code with parameters $[[150,140,\geq 2]]_5$.

Example 2 Let

$$B = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & -1 & -1 & 0 \\ 1 & -1 & 1 & -1 & 0 \\ 1 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix},$$

$S_2 = \mathbb{F}_7[u_1,u_2]/\langle u_1^3 = u_1, u_2^3 = u_2, u_1u_2 = u_2u_1 = 0\rangle$, $e_1 = \frac{u_1^2+u_1}{2}$, $e_2 = \frac{u_1^2-u_1}{2}$, $e_3 = \frac{u_2^2+u_2}{2}$, $e_4 = \frac{u_2^2-u_2}{2}$, $e_5 = 1-u_1^2-u_2^2$, when $n = 15$,

$$\begin{aligned} x^{15}-1 &= (x+3)(x+5)(x+6)(x^4+x^3+x^2+x+1) \\ &\quad \times (x^4+2x^3+4x^2+x+2)(x^4+4x^3+2x^2+x+4), \\ x^{15}+1 &= (x+1)(x+2)(x+4)(x^4+3x^3+2x^2+6x+4) \\ &\quad \times (x^4+5x^3+4x^2+6x+2)(x^4+6x^3+x^2+6x+1). \end{aligned}$$

Let C be a $(1-2u_1^2-u_2^2)$-constacyclic code of length 15 over S_2 with generator polynomial $e_1g_1(x)+e_2g_2(x)+e_3g_3(x)+e_4g_4(x)+e_5g_5(x)$, where $g_1 = x^4+3x^3+2x^2+6x+4$, $g_2 = x^4+5x^3+4x^2+6x+2$, $g_3 = g_4 = x^4+6x^3+x^2+6x+1$, $g_5 = x^4+x^3+x^2+x+1$. By using Theorem 8, we have $C^{\perp} \subseteq C$ and $\varphi_2(C)$ is a linear code over $\mathbb{F}_7$ with parameters $[85,65,4]$. By Theorem 10, we know that there is a quantum error correcting code with parameters $[[85,45,\geq 4]]_7$.

Example 3 Let

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix},$$

$n = 3$ and $S_1 = \mathbb{F}_7[u_1]/\langle u_1^3 = u_1\rangle$, $e_1 = \frac{u_1^2+u_1}{2}$, $e_2 = \frac{u_1^2-u_1}{2}$, $e_3 = 1-u_1^2$, $x^3+1 = (x+1)(x+2)(x+4)$, $x^3-1 = (x+3)(x+5)(x+6)$.

Let C be a $(2u_1^2-1)$-constacyclic code of length 3 over S_1 with generator polynomial $e_1g_1(x)+e_2g_2(x)+e_3g_3(x)$, where $g_1 = x+3$, $g_2 = x+5$, $g_3 = x+4$. By Theorem 8, we have $C^{\perp} \subseteq C$, and $\phi_1(C)$ is a linear code over $\mathbb{F}_7$ with parameters $[9,6,2]$. By Theorem 9, we know that there is a quantum error correcting code with parameters $[[9,3,\geq 2]]_7$.

In Table 1, we provide some new quantum codes $[[n,l,d]]_q$ (in the sixth column) and compare the constructed codes $[[n',l',d']]_q$ (in the seventh column) better (by means of larger code rate or larger distance) than the existing references [13, 16, 17]. Further, the

Table 1 New Quantum codes over S_k

n	k	$(\lambda_1,\dots,\lambda_{2k+1})$	$\langle g_1(x),\dots,g_{2k+1}(x)\rangle$	$\varphi_k(C)$	$[[n,l,d]]_q$	$[[n',l',d']]_q$
8	1	$(1,1,-1)$	$(112,112,1022)$	$[24,16,3]$	$[[24,8,\geq 3]]_3$	$[[24,8,2]]_3$ [13]
24	1	$(1,1,1)$	$(1101,11,11)$	$[72,67,3]$	$[[72,62,\geq 3]]_3$	$[[72,48,2]]_3$ [13]
26	1	$(1,1,1)$	$(101102,121,121)$	$[78,66,4]$	$[[78,54,\geq 4]]_3$	$[[78,48,4]]_3$ [17]
12	1	$(1,1,1)$	$(1111,11,11)$	$[36,31,4]$	$[[36,26,\geq 4]]_3$	$[[36,24,3]]_3$ [17]
28	1	$(1,1,1)$	$(1111,11,11)$	$[84,79,4]$	$[[84,75,\geq 4]]_7$	$[[84,72,3]]_7$ [17]
16	1	$(1,1,1)$	$(1\omega^2\omega^3\omega^5,1\omega^2,1\omega^2)$	$[48,43,3]$	$[[48,38,\geq 3]]_9$	$[[48,30,3]]_9$ [16]

first column represents the length n, the second column is parameter k for S_k, the third column gives the value of units $(\lambda_1,\dots,\lambda_{2k+1})$, the fourth column gives the generator polynomials $\langle g_1(x),\dots,g_{2k+1}(x)\rangle$, where $g_i(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ is denoted by $a_na_{n-1}\cdots a_1a_0$, e.g., 112 represents the polynomial x^2+x+2, the fifth column gives parameters of $\varphi_k(C)$.

6 Conclusion

In this paper, we study the structure of constacyclic codes over the non-chain rings $S_k=\mathbb{F}_q[u_1,u_2,\dots,u_k]/\langle u_i^3=u_i,u_iu_j=u_ju_i=0\rangle$, and apply the CSS construction on Gray images of dual containing constacyclic codes to obtain some new quantum codes improving the existing codes that appeared in some recent references.

Acknowledgements
The authors would like to thank the referees and the editor for their careful reading the paper and valuable comments and suggestions, which improved the presentation of this manuscript.

Funding
This work was supported by the Key Technologies Research and Development Program of Henan Province (No. 212102210573) and Zhengzhou Special Fund for Basic Research and applied basic research (No. ZZSZX202111).

Availability of data and materials
All data generated or analysed during this study are included in this published article.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
We agree to publication in the Journal.

Competing interests
The authors declare no competing interests.

Author contributions
All authors have read and agreed to the published version of the manuscript.

Publisher's Note

Received: 11 June 2022 Accepted: 25 January 2023 Published online: 06 February 2023

References

1. Calderbank AR, Rains EM, Shor PM et al. Quantum error correction via codes over *GF*(4). IEEE Trans Inf Theory. 1998;44:1369–87. https://doi.org/10.1109/18.681315.
2. Chen B, Dinh HQ, Liu H. Repeated-root constacyclic codes of length $2l^mp^n$. Finite Fields Appl. 2015;33:137–59. https://doi.org/10.1016/j.ffa.2014.11.006.
3. Chen B, Liu H. Constructions of cyclic constant dimension codes. Des Codes Cryptogr. 2018;86:1267–79. https://doi.org/10.1007/s10623-017-0394-9.
4. Li J, Gao J, Fu FW et al. $\mathbb{F}_qR$-Linear skew constacyclic codes and their application of constructing quantum codes. Quantum Inf Process. 2020;19:193. https://doi.org/10.1007/s11128-020-02700-x.

5. Dinh HQ, Kewat PK, Kushwaha S et al. Constacyclic codes of length p^s over $\mathbb{F}_{p^m}/\langle u^2, v^2, uv - vu\rangle$. Discrete Math. 2020;343:111890. https://doi.org/10.1016/j.disc.2020.111890.
6. Kumar R, Bhaintwal M. A class of constacyclic codes and skew constacyclic codes over $\mathbb{Z}_{2^s} + u\mathbb{Z}_{2^s}$ and their gray images. J Appl Math Comput. 2021;66:111–28. https://doi.org/10.1007/s12190-020-01425-5.
7. Zheng X, Kong B. Cyclic codes and $\lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv$-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$. Appl Math Comput. 2017;306:86–91. https://doi.org/10.1016/j.amc.2017.02.017.
8. Zheng X, Kong B. Constacyclic codes over $\mathbb{F}_{p^m}[u_1, u_2, \ldots, u_k]/\langle u_i^2 = u_i, u_iu_j = u_ju_i\rangle$. Open Math. 2018;16:490–7. https://doi.org/10.1515/math-2018-0045.
9. Kong B, Zheng X, Ma H. The depth spectrums of constacyclic codes over finite chain rings. Discrete Math. 2015;338:256–61. https://doi.org/10.1016/j.disc.2014.09.013.
10. Liu HW, Liu JG. On σ-self-orthogonal constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Adv Math Commun. 2022;16:643–65. https://doi.org/10.3934/amc.2020127.
11. Dertli A, Cengellenmis Y, Eren S. On quantum codes obtained from cyclic codes over A_2. Int J Quantum Inf. 2015;13:1550031. https://doi.org/10.1142/S0219749915500318.
12. Gao Y, Gao J, Fu FW. Quantum codes from cyclic codes over the ring $\mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_r\mathbb{F}_q$. Appl Algebra Eng Commun Comput. 2019;30:161–74. https://doi.org/10.1007/s00200-018-0366-y.
13. Islam H, Prakash O. Quantum codes from the cyclic codes over $\mathbb{F}_p[u,v,w]/\langle u^2-1, v^2-1, w^2-1, uv-vu, vw-wv, wu-uw\rangle$. J Appl Math Comput. 2019;60:625–35. https://doi.org/10.1007/s12190-018-01230-1.
14. Rani S, Verma RK, Prakash O. Quantum codes from repeated-root cyclic and negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m}$. Int J Theor Phys. 2021;60:1299–327. https://doi.org/10.1007/s10773-021-04757-5.
15. Wang Y, Kai X, Sun Z et al. Quantum codes from Hermitian dual-containing constacyclic codes over $\mathbb{F}_{q^2} + v\mathbb{F}_{q^2}$. Quantum Inf Process. 2021;20:122. https://doi.org/10.1007/s11128-021-03052-w.
16. Prakash O, Islam H, Patel S et al. New quantum codes from skew constacyclic codes over a class of non-chain rings $\mathbb{R}_{e,q}$. Int J Theor Phys. 2021;60:3334–52. https://doi.org/10.1007/s10773-021-04910-0.
17. Ashra M, Khan N, Mohammad G. Quantum codes from cyclic codes over the mixed alphabet structure. Quantum Inf Process. 2022;21:180. https://doi.org/10.1007/s11128-022-03491-z.
18. Dertli A, Cengellenmis Y. Quantum codes obtained from some constacyclic codes over a family of finite rings $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p$. Math Comput Sci. 2020;14:437–41. https://doi.org/10.1007/s11786-019-00426-3.
19. Islam H, Prakash O. New quantum codes from constacyclic and additive constacyclic codes. Quantum Inf Process. 2020;19:319. https://doi.org/10.1007/s11128-020-02825-z.
20. Ketkar A, Klappenecker A, Kumar S et al. Nonbinary Stabilizer Codes Over Finite Fields. IEEE Trans Inf Theory. 2006;52:4892–914. https://doi.org/10.1109/TIT.2006.883612.