Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 8(10): 24075–24086.
DOI: 10.3934/math.20231227
Received: 01 June 2023
Revised: 26 July 2023
Accepted: 31 July 2023
Published: 09 August 2023

Research article

Quantum codes from σ-dual-containing constacyclic codes over $\Re_{l,k}$

Xiying Zheng[1], **Bo Kong**[2,*] **and Yao Yu**[1,3]

[1] Faculty of Engineering, Huanghe Science and Technology College, Zhengzhou 450063, China
[2] School of Statistics and Mathematics, Henan Finance University, Zhengzhou 450046, China
[3] School of Electrical Information, Zhengzhou University of Light Industry, Zhengzhou 450002, China

* **Correspondence:** Email: kongbo666@163.com.

Abstract: Let $\Re_{l,k} = \mathbb{F}_{p^m}[u_1, u_2, \cdots, u_k]/\langle u_i^l = u_i, u_i u_j = u_j u_i = 0\rangle$, where p is a prime, l is a positive integer, $(l-1) \mid (p-1)$ and $1 \le i, j \le k$. First, we define a Gray map $\phi_{l,k}$ from $\Re_{l,k}^n$ to $\mathbb{F}_{p^m}^{((l-1)k+1)n}$, and study its Gray image. Further, we study the algebraic structure of σ-self-orthogonal and σ-dual-containing constacyclic codes over $\Re_{l,k}$, and give the necessary and sufficient conditions for λ-constacyclic codes over $\Re_{l,k}$ to satisfy σ-self-orthogonal and σ-dual-containing. Finally, we construct quantum codes from σ-dual-containing constacyclic codes over $\Re_{l,k}$ using the CSS construction or Hermitian construction and compare new codes our obtained better than the existing codes in some recent references.

Keywords: quantum codes; σ-self-orthogonal; σ-dual-containing; constacyclic codes; CSS construction; Hermitian construction
Mathematics Subject Classification: 94B05, 94B15

1. Introduction

Constructing quantum codes is an important subject in the quantum information. The CSS construction and the Hermitian construction were introduced to construct quantum codes from classical error-correcting codes in [1–4]. Constructing quantum codes needs Euclidean dual-containing or Hermitian dual-containing codes with respect to the Euclidean or Hermitian inner product using the CSS construction or Hermitian construction. Fan and Zhang [5] introduced the Galois inner products to generalize the Euclidean inner product and the Hermitian inner product. In [6], Hermitian LCD λ-constacyclic codes over $\mathbb{F}_q$ were addressed by studying the Galois inner product. Galois hulls of linear codes over finite fields were addressed by studying the Galois dual in [7]. In [8], σ-self-orthogonal constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ were studied by generalizing the notion of self-orthogonal codes to σ-self-orthogonal codes over an arbitrary finite ring. Fu and Liu [9] extended constacyclic codes to obtain Galois self-dual codes.

Now, many quantum codes have been constructed by studying the algebraic structure of cyclic and constacyclic codes over finite fields, finite chain rings and finite non-chain ring. Huang et al. [10] constructed quantum codes from Hermitian dual-containing codes by applying the Hermitian construction. In [11], some quantum codes were obtained from constacyclic over $\mathbb{F}_q[u,v]/\langle u^2-\gamma u, v^2-\delta v, uv=vu=0\rangle$ by using the CSS construction. Gowdhaman et al. [12] studied the the structure of cyclic and λ-constacyclic codes over $\frac{\mathbb{F}_p[u,v]}{\langle v^3-v, u^3-u, uv-vu\rangle}$ and constructed quantum codes over $\mathbb{F}_p$ using the CSS construction. Islam and Prakash [13] obtained quantum codes from cyclic codes over a finite non-chain ring $\mathbb{F}_q[u,v]/\langle u^2-\alpha u, v^2-1, uv-vu\rangle$ using the CSS construction. Kong and Zheng obtained some quantum codes from constacyclic codes over $\mathbb{F}_q[u_1,u_2,\cdots,u_k]/\langle u_i^3=u_i, u_iu_j=u_ju_i\rangle$ [14] and $\mathbb{F}_q[u_1,u_2,\cdots,u_k]/\langle u_i^3=u_i, u_iu_j=u_ju_i=0\rangle$ [15] using the CSS construction. As an application, Galois inner product can be applied in the constructions of quantum codes. Some entanglement-assisted quantum codes were obtained from Galois dual codes in [16–18].

Motivated by these works, we define a new non-chain ring $\Re_{l,k}$ by generalizing [15] and study the algebraic structure of σ-self-orthogonal and σ-dual-containing constacyclic codes over $\Re_{l,k}$ based on the σ-inner product. Then, we give the necessary and sufficient conditions for λ-constacyclic codes over $\Re_{l,k}$ to satisfy σ-self-orthogonal and σ-dual-containing. Finally, we obtain some new quantum codes from σ-dual-containing constacyclic codes over $\Re_{l,k}$ using the CSS construction or Hermitian construction and compare these codes better with the existing codes that appeared in some recent papers.

2. Preliminaries

Let R be a finite commutative ring, I is an ideal of R and I is generated by one element, then I is called a principal ideal. If all the ideas of R are principal, R is called a principal ideal ring. If R has a unique maximal ideal, R is called a local ring. If the ideals of R are linearly ordered by inclusion, R is called a chain ring.

Let $\Re_{l,k}=\mathbb{F}_{p^m}[u_1,u_2,\cdots,u_k]/\langle u_i^l=u_i, u_iu_j=u_ju_i=0\rangle$, where p is a prime, l is a positive integer, $(l-1)\mid(p-1)$ and $1\le i,j\le k$. It is a commutative non-chain ring with $p^{m(l-1)k+m}$ elements. Since $(l-1)\mid(p-1)$, then

$$u_i^l-u_i=(u_i-\alpha_1)(u_i-\alpha_2)\cdots(u_i-\alpha_l),$$

where $\alpha_i\in\mathbb{F}_{p^m}$ for $i=1,2,\cdots,l$.

Let

$$\varsigma_{ij}=\frac{(u_j-\alpha_1)\cdots(u_j-\alpha_{i-1})(u_j-\alpha_{i+1})\cdots(u_j-\alpha_l)}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_l)},$$

where $2\le i\le l$ and $1\le j\le k$.

We can get that $\sum_{ij}\varsigma_{ij}=1$, $\varsigma_{ij}^2=\varsigma_{ij}$ and $\varsigma_{ij}\varsigma_{i'j'}=0$, where $(i,j)\neq(i',j')$.

Let $e_1=\varsigma_{21}, e_2=\varsigma_{22},\cdots,e_k=\varsigma_{2k},\cdots,e_{(l-1)k}=\varsigma_{lk}, e_{(l-1)k+1}=\varsigma_{11}$. Let $s=(l-1)k+1$, thus, $1=e_1+e_2+\cdots+e_s$, $e_i^2=e_i$ and $e_ie_j=0$, where $i\neq j$ and $i,j=1,2,\cdots,s$. By the Chinese Remainder Theorem, then

$$\Re_{l,k}=\bigoplus_{j=1}^{s}e_j\Re_{l,k}=\bigoplus_{j=1}^{s}e_j\mathbb{F}_{p^m}.$$

For any element $r \in \Re_{l,k}$, it can be expressed uniquely as

$$r = r_1e_1 + r_2e_2 + \cdots + r_se_s,$$

where $r_i \in \mathbb{F}_{p^m}$ for $i = 1, 2, \cdots, s$.

Let $\mathrm{Aut}(\Re_{l,k})$ be the ring automorphism group of $\Re_{l,k}$. If $\sigma \in \mathrm{Aut}(\Re_{l,k})$, then we can get a bijective map

$$\Re_{l,k}^n \to \Re_{l,k}^n,$$
$$(a_0, a_1, \cdots, a_{n-1}) \mapsto (\sigma(a_0), \sigma(a_1), \cdots, \sigma(a_{n-1})).$$

Let $a = (a_0, a_1, \cdots, a_{n-1})$ and $b = (b_0, b_1, \cdots, b_{n-1}) \in \Re_{l,k}^n$, the σ-inner product [8] of a, b is defined as

$$\langle a, b\rangle_\sigma = a_0\sigma(b_0) + a_1\sigma(b_1) + \cdots + a_{n-1}\sigma(b_{n-1}).$$

When $\Re_{l,k} = \mathbb{F}_{p^m}$ and σ is the identity map of $\mathbb{F}_{p^m}$, then σ-inner product is the Euclidean inner product. When $\Re_{l,k} = \mathbb{F}_{p^m}$ and m is even, $\forall a \in \mathbb{F}_{p^m}$, if $\sigma(a) = a^{p^{\frac{m}{2}}}$, then σ-inner product is the Hermitian inner product. When $\Re_{l,k} = \mathbb{F}_{p^m}$ and $\forall a \in \mathbb{F}_{p^m}$, $\sigma(a) = a^{p^l}$, $0 \le l \le m-1$, then σ-inner product is the Galois inner product [5].

When $\langle a, b\rangle_\sigma = 0$, a and b are called σ-orthogonal, for any code C over $\Re_{l,k}$, the σ-dual code of C is defined as

$$C^{\perp_\sigma} = \{x | \langle x, y\rangle_\sigma = 0, \forall y \in C\}.$$

If $C \subseteq C^{\perp_\sigma}$, C is σ-self-orthogonal, if $C^{\perp_\sigma} \subseteq C$, C is σ-dual-containing, and if $C = C^{\perp_\sigma}$, C is σ-self-dual.

Let θ_t be an automorphism of $\mathbb{F}_{p^m}$, θ_t: $\mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ defined by $\theta_t(a) = a^{p^t}$, where $0 \le t \le m-1$. We can define the automorphism of $\Re_{l,k}$ as follows:

$$\sigma : \Re_{l,k} \to \Re_{l,k},$$
$$\sum_{j=1}^{s} a_je_j \mapsto \sum_{j=1}^{s} e_ja_j^{p^t}.$$

Let $c = (c_0, c_1, \cdots, c_{n-1}) \in \Re_{l,k}^n$ and λ be a unit of $\Re_{l,k}$, then the constacyclic shift δ_λ of c is defined as $\delta_\lambda(c) = (\lambda c_{n-1}, c_0, \cdots, c_{n-2})$. If $\delta_\lambda(C) = C$, C is called a λ-constacyclic code of length n over $\Re_{l,k}$. In particular, when $\lambda = 1$, C is called cyclic code and negative cyclic code when $\lambda = -1$.

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{r-1}x^{r-1} + x^r$ be a monic polynomial, the reciprocal polynomial of $f(x)$ is denoted by $f^*(x) = x^r f(x^{-1})$.

Each codeword $(a_0, a_1, \cdots, a_{n-1}) \in \Re_{l,k}^n$ can be represented by a polynomial $a_0+a_1x+\cdots+a_{n-1}x^{n-1} \in \Re_{l,k}[x]/\langle x^n - \lambda\rangle$,

$$\psi : \Re_{l,k}^n \to \Re_{l,k}[x]/\langle x^n - \lambda\rangle,$$
$$(a_0, a_1, \cdots, a_{n-1}) \mapsto a_0 + a_1x + \cdots + a_{n-1}x^{n-1}.$$

In polynomial representation, a λ-constacyclic code of length n over $\Re_{l,k}$ is defined as an ideal of $\Re_{l,k}[x]/\langle x^n - \lambda\rangle$.

We define a Gray map $\phi_{l,k} : \Re_{l,k} \to \mathbb{F}_{p^m}^s$ by $a = \sum_{i=1}^{s} a_i e_i \mapsto (a_1, a_2, \cdots, a_s)$, and we extend $\phi_{l,k}$ as

$$\phi_{l,k} : \Re_{l,k}^n \to \mathbb{F}_{p^m}^{sn},$$
$$(a_0, a_1, \cdots, a_{n-1}) \mapsto (a_{1,0}, \cdots, a_{1,n-1}, a_{2,0}, \cdots, a_{2,n-1}, \cdots, a_{s,0}, \cdots, a_{s,n-1}),$$

where $a_i = a_{1,i}e_1 + a_{2,i}e_2 + \cdots + a_{s,i}e_s \in \Re_{l,k}$, $i = 0, 1, \cdots, n-1$.

$\forall r \in \Re_{l,k}$, the Gray weight of r is defined as $w_G(r) = w_H(\phi_{l,k}(r))$, where $w_H(\phi_{l,k}(r))$ is the Hamming weight of the image of r under $\phi_{l,k}$.

$\forall x = (x_1, x_2, \cdots, x_n), y = (y_1, y_2, \cdots, y_n) \in \Re_{l,k}^n$, the Gray weight of $x - y$ is defined as $w_G(x - y) = \sum_{i=1}^{n} w_G(x_i - y_i)$, the Gray distance of x, y is defined as $d_G(x, y) = w_G(x - y)$, and the Gray distance of C is defined as $d_G(C) = \min\{d_G(a, b), a, b \in C, a \neq b\}$.

For a linear code C of length n over $\Re_{l,k}$. Let

$$C_j = \{x_j \in \mathbb{F}_{p^m}^n \mid \sum_{i=1}^{s} x_i e_i \in C, x_i \in \mathbb{F}_{p^m}^n\},$$

where $j = 1, 2, \cdots, s$.

Then, $C_1, C_2, \cdots, C_s$ are linear codes of length n over $\mathbb{F}_{p^m}$, $C = \bigoplus_{j=1}^{s} e_j C_j$ and $|\ C\ | = \prod_{j=1}^{s} |\ C_j\ |$.

Lemma 2.1. *An element* $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_s e_s) \in \Re_{l,k}$ *is a unit in* $\Re_{l,k}$ *if and only if* λ_i *is a unit in* $\mathbb{F}_{p^m}$ *for* $i = 1, 2, \cdots, s$.

Proof. This proof is the same as Lemma 3.1 in [14]. □

3. λ-constacyclic codes over $\Re_{l,k}$

In this section, let $\lambda = \sum_{j=1}^{s} \lambda_j e_j$ be a unit in $\Re_{l,k}$, then $\lambda^{-1} = \sum_{j=1}^{s} \lambda_j^{-1} e_j$, where $s = (l-1)k + 1$, $\lambda_j \in \mathbb{F}_{p^m}^*$ for $j = 1, 2, \cdots, s$.

Lemma 3.1. *(See [8]) Let R be a finite commutative Frobenius ring with identity,* $\sigma, \widetilde{\sigma} \in \mathrm{Aut}(R)$ *and C be a liner code of length n over R, then*

(1) $C^{\perp_\sigma}$ *is a linear code over R.*

(2) $C^{\perp_\sigma} = \sigma^{-1}(C^{\perp})$ *and* $|\ C\ ||\ C^{\perp_\sigma}\ |=|\ R\ |^n$.

(3) $(C^{\perp_\sigma})^{\perp_{\widetilde{\sigma}}} = \widetilde{\sigma}^{-1}\sigma^{-1}(C)$.

Theorem 3.1. $C = \bigoplus_{j=1}^{s} e_j C_j$ *is a* λ*-constacyclic code of length n over* $\Re_{l,k}$ *if and only if* C_j *is a* λ_j*-constacyclic code of length n over* $\mathbb{F}_{p^m}$ *for* $j = 1, 2, \cdots, s$.

Proof. This proof is the same as Theorem 1 in [15]. □

Theorem 3.2. *Let* $C = \bigoplus_{j=1}^{s} e_j C_j$ *be a linear code of length n over* $\Re_{l,k}$*. Then* $C^{\perp_\sigma} = \sum_{j=1}^{s} e_j C_j^{\perp_\sigma}$*, where* $C_j^{\perp_\sigma}$ *is the* σ *dual code of* C_j *for* $j = 1, 2, \cdots, s$.

Proof. Let $\tilde{C} = \sum_{j=1}^{s} e_j C_j^{\perp_\sigma}$, $\forall x = \sum_{j=1}^{s} e_j x_j \in C$ and $\forall \tilde{x} = \sum_{j=1}^{s} e_j \tilde{x}_j \in \tilde{C}$, then

$$\langle x, \tilde{x} \rangle_\sigma = \sum_{j=1}^{s} (x_j \sigma(\tilde{x}_j)) e_j = 0,$$

where $x_j \in C_j$, $\tilde{x}_j \in C_j^{\perp_\sigma}$.

So

$$\tilde{C} \subseteq C^{\perp_\sigma}.$$

For $\Re_{l,k}$ is a Frobenius ring, by Lemma 3.1,

$$| C || C^{\perp_\sigma} |=| \Re_{l,k} |^n .$$

Hence

$$| \tilde{C} |= \prod_{j=1}^{s} | C_j^{\perp_\sigma} |= \prod_{j=1}^{s} \frac{p^{mn}}{| C_j |} = \frac{| \Re_{l,k} |^n}{| C |} =| C^{\perp_\sigma} | .$$

So

$$C^{\perp_\sigma} = \tilde{C} = \sum_{j=1}^{s} e_j C_j^{\perp_\sigma}.$$

□

Theorem 3.3. *Let $C = \bigoplus_{j=1}^{s} e_j C_j$ be a λ-constacyclic code of length n over $\Re_{l,k}$. Then $C^{\perp_\sigma} = \sum_{j=1}^{s} e_j C_j^{\perp_\sigma}$ is a $\sigma(\lambda^{-1})$-constacyclic code of length n over $\Re_{l,k}$, and $C_j^{\perp_\sigma}$ is a $\sigma(\lambda_j^{-1})$-constacyclic code over $\mathbb{F}_{p^m}$ for $j = 1, 2, \cdots, s$.*

Proof. Let $C = \bigoplus_{j=1}^{s} e_j C_j$ be a λ-constacyclic code of length n over $\Re_{l,k}$. $\forall x = (x_0, x_1, \cdots, x_{n-1}) \in C^{\perp_\sigma}$ and $\forall y = (y_0, y_1, \cdots, y_{n-1}) \in C$, then

$$\delta_\lambda^{n-1}(y) = (\lambda y_1, \lambda y_2, \cdots, \lambda y_{n-1}, y_0) \in C$$

and

$$\delta_{\sigma(\lambda^{-1})}(x) = (\sigma(\lambda^{-1}) x_{n-1}, x_0, \cdots, x_{n-2}).$$

We can get that

$$\begin{aligned} 0 &= \langle x, \delta_\lambda^{n-1}(y) \rangle_\sigma \\ &= \sigma(\lambda) x_0 \sigma(y_1) + \sigma(\lambda) x_1 \sigma(y_2) + \cdots + \sigma(\lambda) x_{n-2} \sigma(y_{n-1}) + x_{n-1} \sigma(y_0) \\ &= \sigma(\lambda)(x_0 \sigma(y_1) + x_1 \sigma(y_2) + \cdots + x_{n-2} \sigma(y_{n-1}) + \sigma(\lambda^{-1}) x_{n-1} \sigma(y_0)). \end{aligned}$$

So

$$\langle \delta_{\sigma(\lambda^{-1})}(x), y \rangle_\sigma = \sigma(\lambda^{-1}) x_{n-1} \sigma(y_0) + x_0 \sigma(y_1) + \cdots + x_{n-2} \sigma(y_{n-1}) = 0.$$

We have $\delta_{\sigma(\lambda^{-1})}(x) \in C^{\perp_\sigma}$, so $C^{\perp_\sigma}$ is a $\sigma(\lambda^{-1})$-constacyclic code.

By Lemma 2.1, $\lambda^{-1} = \lambda_1^{-1} e_1 + \lambda_2^{-1} e_2 + \cdots + \lambda_s^{-1} e_s$, it implies that $C^{\perp_\sigma}$ is a $\sigma(\lambda^{-1})$-constacyclic code of length n over $\Re_{l,k}$. By Theorem 3.1, we can have $C_j^{\perp}$ is a $\sigma(\lambda_j^{-1})$-constacyclic code over $\mathbb{F}_{p^m}$ for $j = 1, 2, \cdots, s$. □

Theorem 3.4. *Let $C = \bigoplus_{j=1}^{s} e_j C_j$ be a λ-constacyclic code of length n over $\Re_{l,k}$, then there exists a polynomial $g(x) \in \Re_{l,k}[x]$ such that $C = \langle g(x) \rangle$, where $g(x) = \sum_{j=1}^{s} e_j g_j(x)$ is the divisor of $x^n - \lambda$, $g_j(x) \in \mathbb{F}_{p^m}[x]$ is the generator polynomial of λ_j-constacyclic over C_j, and $g_j(x)$ divides $x^n - \lambda_j$ for $j = 1, 2, \cdots, s$.*

Proof. This proof is the same as Theorem 2 in [15]. □

Corollary 3.1. *Let $C = \langle g(x)\rangle$ be a λ-constacyclic code of length n over $\Re_{l,k}$. Then $C^{\perp_\sigma} = \langle\sum_{j=1}^{s} e_j\sigma^{-1}(f_j^*(x))\rangle$ and $|C^{\perp_\sigma}| = p^{m\sum_{j=1}^{s}\deg(g_j)}$, where $f_j(x)g_j(x) = x^n - \lambda_j$, $j = 1, 2, \cdots, s$.*

Proof. Let $C_j^{\perp} = \langle f_j^*(x)\rangle$. By Lemma 3.1, Theorem 3.3 and Theorem 3.4, we can have

$$C_j^{\perp_\sigma} = \sigma^{-1}(C_j^{\perp}) = \langle\sigma^{-1}(f_j^*(x))\rangle$$

and

$$C^{\perp_\sigma} = \sum_{j=1}^{s} e_j C_j^{\perp_\sigma},$$

where $j = 1, 2, \cdots, s$.

Then

$$|C^{\perp_\sigma}| = \prod_{j=1}^{s} |C_j^{\perp_\sigma}| = \prod_{j=1}^{s} |C_j^{\perp}| = p^{m\sum_{j=1}^{s}\deg(g_j)}$$

and $C^{\perp_\sigma}$ has the form

$$C^{\perp_\sigma} = \langle e_1\sigma^{-1}(f_1^*(x)), \cdots, e_s\sigma^{-1}(f_s^*(x))\rangle.$$

Let

$$\tilde{D} = \langle\sum_{j=1}^{s} e_j\sigma^{-1}(f_j^*(x))\rangle,$$

it is easy to see that, $\tilde{D} \subseteq C^{\perp}$.

On the other hand, for $j = 1, 2, \cdots, s$,

$$e_j\sum_{j=1}^{s} e_j\sigma^{-1}(f_j^*(x)) = e_j\sigma^{-1}(f_j^*(x)).$$

Thus $C^{\perp_\sigma} \subseteq \tilde{D}$, it implies that,

$$C^{\perp_\sigma} = \tilde{D} = \langle\sum_{j=1}^{s} e_j\sigma^{-1}(f_j^*(x))\rangle.$$

□

Theorem 3.5. *Let $C = \bigoplus_{j=1}^{s} e_jC_j$ be a λ-constacyclic code of length n over $\Re_{l,k}$, then C is a σ-self-orthogonal code over $\Re_k$ if and only if $C_1, C_2, \cdots, C_s$ are σ-self-orthogonal codes over $\mathbb{F}_{p^m}$.*

Proof. By Theorem 3.2, $C^{\perp_\sigma} = \sum_{j=1}^{s} e_jC_j^{\perp_\sigma}$, so $C \subseteq C^{\perp_\sigma}$ if and only if $C_j \subseteq C_j^{\perp_\sigma}$, it implies that C is a σ-self-orthogonal code over $\Re_{l,k}$ if and only if $C_1, C_2, \cdots, C_s$ are σ-self-orthogonal codes over $\mathbb{F}_{p^m}$. □

Lemma 3.2. *Let C be a λ-constacyclic code of length n over $\mathbb{F}_{p^m}$, its generator polynomial is $g(x)$. Then C is a σ-self-orthogonal code if and only if $f(x)\sigma^{-1}(f^*(x))$ is the divisor of $x^n - \lambda$, $\lambda = \pm 1$, where $f^*(x)$ is the generator polynomial of $C^{\perp}$.*

Proof. We can assume that $\sigma(\lambda^{-1}) = \lambda$.

Since C is a λ-constantcyclic code of length n over $\mathbb{F}_{p^m}$, and $C^{\perp_\sigma}$ is a $\sigma(\lambda^{-1})$-constantcyclic code of length n over $\mathbb{F}_{p^m}$, so C is a σ-self-orthogonal code must satisfy the condition $C \subseteq C^{\perp_\sigma}$.

Let $C^\perp = \langle f^*(x)\rangle$, where $f(x)g(x) = (x^n - \lambda)$ and $\lambda = \pm 1$. $C^{\perp_\sigma} = \sigma^{-1}(C^\perp) = \langle \sigma^{-1}(f^*(x))\rangle$, C is a σ-self-orthogonal code if and only if there exists a polynomial $h(x) \in \mathbb{F}_{p^m}[x]$, such that $\sigma^{-1}(f^*(x))h(x) = g(x)$, if and only if $f(x)\sigma^{-1}(f^*(x))h(x) = f(x)g(x) = (x^n - \lambda)$ if and only if $f(x)\sigma^{-1}(f^*(x))$ is the divisor of $x^n - \lambda$. □

By Theorem 3.5 and Lemma 3.2, it is easy to get the following theorem.

Theorem 3.6. *Let $C = \bigoplus_{j=1}^{s} e_j C_j$ be a λ-constacyclic code of length n over $\mathfrak{R}_{l,k}$, then C is a σ-self-orthogonal code over $\mathfrak{R}_{l,k}$ if and only if $f_j(x)\sigma^{-1}(f_j^*(x))$ is the divisor of $x^n - \lambda_j$, where $f_j^*(x)$ is the generator polynomial of $C_j^\perp$ and $\sigma(\lambda_j^{-1}) = \lambda_j$ for $j = 1, 2, \cdots, s$.*

4. Quantum codes from σ-dual-containing constacyclic codes over $\mathfrak{R}_{l,k}$

Theorem 4.1. *Let $C = \bigoplus_{j=1}^{s} e_j C_j$ be a linear code of length n over $\mathfrak{R}_{l,k}$, which order $\mid C \mid = p^{mk'}$ and the minimum Gray distance of C is d_G, where $s = (l-1)k + 1$. Then $\phi_{l,k}(C)$ is a linear code $[sn, k', d_G]$ and $\phi_{l,k}(C)^{\perp_\sigma} = \phi_{l,k}(C^{\perp_\sigma})$. If C is a σ-self-orthogonal code over $\mathfrak{R}_{l,k}$, then $\phi_{l,k}(C)$ is a σ-self-orthogonal code over $\mathbb{F}_{p^m}$. Specifically, if C is a σ-self-dual code over $\mathfrak{R}_{l,k}$, then $\phi_{l,k}(C)$ is a σ-self-dual code over $\mathbb{F}_{p^m}$.*

Proof. By the definition of $\phi_{l,k}$, it is easy to know that $\phi_{l,k}$ is both a distance preserving map and a linear map from $\mathfrak{R}_{l,k}^n$ to $\mathbb{F}_q^{sn}$, it implies that $\phi_{l,k}(C)$ is a linear code $[sn, k', d_G]$.

If C is a σ-self-orthogonal code, $\forall x = \sum_{j=1}^{s} e_j x_j \in C$, $\forall y = \sum_{j=1}^{s} e_j y_j \in C$, where $x_j, y_j \in \mathbb{F}_{p^m}^n$, because $C \subseteq C^{\perp_\sigma}$, so the σ-inner product of x, y is $\langle x, y\rangle_\sigma = \sum_{j=1}^{s} e_j \langle x_j, y_j\rangle_\sigma = 0$, which implies $\langle x_j, y_j\rangle_\sigma = 0$, so

$$\langle \phi_{l,k}(x), \phi_{l,k}(y)\rangle_\sigma = \sum_{j=1}^{s} \langle x_j, y_j\rangle_\sigma = 0.$$

So $\phi_{l,k}(C)$ is a σ-self-orthogonal code over $\mathbb{F}_{p^m}$.

Let $a = (a_0, a_1, \cdots, a_{n-1}) \in C$ and $b = (b_0, b_1, \cdots, b_{n-1}) \in C^{\perp_\sigma}$, where $a_j = \sum_{i=1}^{s} a_{i,j} e_i$ and $b_j = \sum_{i=1}^{s} b_{i,j} e_i \in \mathfrak{R}_{l,k}$ for $j = 0, 1, 2, \cdots, n-1$, $a^{(i)} = (a_{i,0}, a_{i,1}, \cdots, a_{i,n-1})$ and $b^{(i)} = (b_{i,0}, b_{i,1}, \cdots, b_{i,n-1})$ for $i = 1, 2, \cdots, s$.

Then

$$\langle a, b\rangle_\sigma = \sum_{j=0}^{n-1} \langle a_j, b_j\rangle_\sigma = \sum_{j=0}^{n-1} \sum_{i=1}^{s} e_i \langle a_{i,j}, b_{i,j}\rangle_\sigma = \sum_{i=1}^{s} e_i \langle a^{(i)}, b^{(i)}\rangle_\sigma = 0.$$

So $\langle a^{(i)}, b^{(i)}\rangle_\sigma = 0$ for $i = 1, 2, \cdots, s$.

Since $\phi_{l,k}(a) = (a^{(1)}, a^{(2)}, \cdots, a^{(s)})$ and $\phi_{l,k}(b) = (b^{(1)}, b^{(2)}, \cdots, b^{(s)})$. It follows that

$$\langle \phi_{l,k}(a), \phi_{l,k}(b)\rangle_\sigma = \sum_{i=1}^{s} \langle a^{(i)}, b^{(i)}\rangle_\sigma = 0.$$

So we have

$$\phi_{l,k}(C^{\perp_\sigma}) \subseteq \phi_{l,k}(C)^{\perp_\sigma}.$$

As $\phi_{l,k}$ is a bijection, and $| C |=| \phi_{l,k}(C) |$.
Then

$$| \phi_{l,k}(C^{\perp_\sigma}) |=| \phi_{l,k}(C^{\perp}) |= \frac{p^{msn}}{| C |} = \frac{p^{msn}}{| \phi_{l,k}(C) |} =| \phi_{l,k}(C)^{\perp} |=| \phi_{l,k}(C)^{\perp_\sigma} | .$$

We have

$$\phi_{l,k}(C)^{\perp_\sigma} = \phi_{l,k}(C^{\perp_\sigma}).$$

Suppose C is a σ-self-dual code and $C = C^{\perp_\sigma}$, then

$$\phi_{l,k}(C)^{\perp_\sigma} = \phi_{l,k}(C^{\perp_\sigma}) = \phi_{l,k}(C).$$

Therefore, $\phi_{l,k}(C)$ is a σ-self-dual code over $\mathbb{F}_{p^m}$. □

Lemma 4.1. *Let C be a λ-constacyclic code of length n over $\mathbb{F}_{p^m}$, whose generator polynomial is $g(x)$. Then, C is a σ-dual-containing code if and only if $x^n - \lambda$ is the divisor of $\sigma^{-1}(f^*(x))f(x)$, where $f^*(x)$ is the generator polynomial of $C^{\perp}$ and $\sigma(\lambda^{-1}) = \lambda$.*

Proof. Let $C^{\perp} = \langle f^*(x)\rangle$, where $f(x)g(x) = (x^n - \lambda)$ and $\sigma(\lambda^{-1}) = \lambda$. Then $C^{\perp_\sigma} = \sigma^{-1}(C^{\perp}) = \langle\sigma^{-1}(f^*(x))\rangle$, so C is a σ-dual-containing code if and only if there exists a polynomial $h(x) \in \mathbb{F}_{p^m}[x]$, such that $\sigma^{-1}(f^*(x)) = h(x)g(x)$, if and only if $\sigma^{-1}(f^*(x))f(x) = h(x)g(x)f(x) = h(x)f(x)g(x) = h(x)(x^n - \lambda)$ if and only if $x^n - \lambda$ is the divisor of $\sigma^{-1}(f^*(x))f(x)$. □

Theorem 4.2. *(CSS construction [4]) Let $C = [n, k, d]$ be a linear codes over $\mathbb{F}_q$ with $C^{\perp} \subseteq C$, then there exists a quantum code $[[n, 2k - n, d]]_q$.*

Theorem 4.3. *(Hermitian construction [4]) Let $C = [n, k, d]$ be a linear code over $\mathbb{F}_{q^2}$ with $C^{\perp_H} \subseteq C$, then there exists a quantum code $[[n, 2k - n, d]]_q$.*

By Lemma 4.1 and Theorem 3.3, we can have the following theorem.

Theorem 4.4. *Let $C = \bigoplus_{j=1}^{s} e_jC_j$ be a λ-constacyclic code of length n over $\Re_{l,k}$, where $s = (l-1)k+1$. Then $C^{\perp_\sigma} \subseteq C$ if and only if $x^n - \lambda_j$ is the divisor of $\sigma^{-1}(f_j^*(x))f_j(x)$, where $\sigma(\lambda_j^{-1}) = \lambda_j$ and $f_j^*(x)$ is the generator polynomial of $C_j^{\perp}$ for $j = 1, 2, \cdots, s$.*

By Lemma 4.1 and Theorem 4.4, we can have the following corollary and theorem.

Corollary 4.1. *Let $C = \bigoplus_{j=1}^{s} e_jC_j$ be a λ-constacyclic code of length n over $\Re_{l,k}$. Then $C^{\perp_\sigma} \subseteq C$ if and only if $C_j^{\perp_\sigma} \subseteq C_j$ for $j = 1, 2, \cdots, s$.*

Theorem 4.5. *Let $C = \bigoplus_{j=1}^{s} e_jC_j$ be a a λ-constacyclic code of length n over $\Re_{l,k}$, C_j is λ_j-constacyclic code over $\mathbb{F}_{p^m}$ and $C_j^{\perp_\sigma} \subseteq C_j$, where $s = (l - 1)k + 1$, $\sigma(\lambda_j^{-1}) = \lambda_j$ for $j = 1, 2, \cdots, s$. Then $\phi_{l,k}(C)^{\perp_\sigma} \subseteq \phi_{l,k}(C)$. If θ_t is the identity map of $\mathbb{F}_{p^m}$, then there exists a quantum code $[[sn, 2k' - sn, d_G]]_{p^m}$. If m is even, $\forall a \in \mathbb{F}_{p^m}$, then $\sigma(a) = a^{p^{\frac{m}{2}}}$, then there exists a quantum code $[[sn, 2k' - sn, d_G]]_{p^{m/2}}$, where d_G is the minimum Gray weight of code C, and k' is the dimension of the linear code $\phi_{l,k}(C)$.*

Proof. Let $C_j^{\perp_\sigma} \subseteq C_j$ and $\sigma(\lambda_j^{-1}) = \lambda_j$. By Corollary 4.1, we have $C^{\perp_\sigma} \subseteq C$, so $\phi_{l,k}(C^{\perp_\sigma}) \subseteq \phi_{l,k}(C)$. By Theorem 4.1, $\phi_{l,k}(C)^{\perp_\sigma} = \phi_{l,k}(C^{\perp_\sigma})$, therefore $\phi_{l,k}(C)^{\perp_\sigma} \subseteq \phi_{l,k}(C)$, and by Theorem 4.1, $\phi_{l,k}(C)$ is a linear code $[sn, k', d]$.

If θ_t is the identity map of $\mathbb{F}_{p^m}$, so σ-inner product is the Euclidean inner product, by Theorem 4.2, there exists a quantum code $[[sn, 2k' - sn, d_G]]_{p^m}$.

If m is even, $\forall a \in \mathbb{F}_{p^m}$, then $\sigma(a) = a^{p^{\frac{m}{2}}}$, so σ-inner product is the Hermitian inner product. By Theorem 4.3, there exists a quantum code $[[sn, 2k' - sn, d_G]]_{p^{m/2}}$. □

Example 4.1. *Let $n = 8$ and $\Re_{2,2} = \mathbb{F}_{17}[u_1, u_2]/\langle u_1^2 = u_1, u_2^2 = u_2, u_1u_2 = u_2u_1 = 0\rangle$. In $\mathbb{F}_{17}[x]$,*

$$x^8 - 1 = (x + 1)(x + 2)(x + 4)(x + 8)(x + 9)(x + 13)(x + 15)(x + 16),$$
$$x^8 + 1 = (x + 3)(x + 5)(x + 6)(x + 7)(x + 10)(x + 11)(x + 12)(x + 14).$$

If θ_t is the identity map of $\mathbb{F}_{p^m}$, then σ-inner product is the Euclidean inner product. Let C be an $(e_1 + e_2 + (-1)e_3)$-constacyclic code of length 8 over $\Re_{2,2}$. Let $g(x) = e_1g_1 + e_2g_2 + e_3g_3$ be the generator polynomial of C, where $g_1(x) = (x + 2)(x + 4)(x + 8), g_2(x) = g_3(x) = (x + 3)$, then $C_1 = \langle g_1(x)\rangle$ is a cyclic code of length 8 over $\mathbb{F}_{17}$, $C_2 = \langle g_2(x)\rangle$ and $C_3 = \langle g_3(x)\rangle$ are negacyclic codes of length 8 over $\mathbb{F}_{17}$.

By Theorem 4.1, $\phi_{2,2}(C)$ is a linear code over $\mathbb{F}_{17}$ with parameters $[24, 19, 4]$. By Theorem 4.5, we have $C^\perp \subseteq C$, we get a quantum code $[[24, 14, 4]]_{17}$.

Example 4.2. *Let $n = 45$ and $\Re_{2,2} = \mathbb{F}_5[u_1, u_2]/\langle u_1^2 = u_1, u_2^2 = u_2, u_1u_2 = u_2u_1 = 0\rangle$. In $\mathbb{F}_5[x]$,*

$$x^{45} - 1 = (x^2 + x + 1)^5(x + 4)^5(x^6 + x^3 + 1)^5,$$
$$x^{45} + 1 = (x^2 + 4x + 1)^5(x + 1)^5(x^6 + 4x^3 + 1)^5.$$

Let C be an $(e_1 + (-1)e_2 + (-1)e_3)$-constacyclic code of length 45 over $\Re_{2,2}$. Let $g_1(x) = x^2 + x + 1$, $g_2(x) = g_3(x) = x + 1$, then $C_1 = \langle g_1(x)\rangle$ is a cyclic code of length 45, $C_2 = \langle g_2(x)\rangle$ and $C_3 = \langle g_3(x)\rangle$ are negacyclic codes of length 45 over $\mathbb{F}_5$.

By Theorem 4.1, $\phi_{2,2}(C)$ is a linear code over $\mathbb{F}_5$ with parameters $[135, 131, 3]$. By Theorem 4.5, we have $C^\perp \subseteq C$, we can get a quantum code $[[135, 127, 3]]_5$, which has larger dimension than $[[135, 63, 3]]_5$ in [12].

Example 4.3. *Let $n = 30$ and $\Re_{2,2} = \mathbb{F}_5[u_1, u_2]/\langle u_1^2 = u_1, u_2^2 = u_2, u_1u_2 = u_2u_1 = 0\rangle$. In $\mathbb{F}_5[x]$,*

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

Let C be an $(e_1 + (-1)e_2 + (-1)e_3)$-constacyclic code of length 30 over $\Re_{2,2}$. Let $g_1(x) = x^2 + x + 1$, $g_2(x) = g_3(x) = x + 3$, then $C_1 = \langle g_1(x)\rangle$ is a cyclic code of length 30, $C_2 = \langle g_2(x)\rangle$ and $C_3 = \langle g_3(x)\rangle$ are negacyclic codes of length 30 over $\mathbb{F}_5$.

By Theorem 4.1, $\phi_{2,2}(C)$ is a linear code over $\mathbb{F}_5$ with parameters $[90, 86, 3]$. By Theorem 4.5, we have $C^\perp \subseteq C$, we get a quantum code $[[90, 82, 3]]_5$, which has larger dimension than $[[90, 68, 3]]_5$ in [11].

Example 4.4. *Let $n = 8$ and $\Re_{1,2} = \mathbb{F}_9[u_1]/\langle u_1^2 = u_1\rangle$, $\sigma(a) = a^3$. In $\mathbb{F}_9[x]$,*

$$x^8 - 1 = (x + 1)(x + w)(x + w^2)(x + w^3)(x + 2)(x + w^5)(x + w^6)(x + w^7).$$

Let C be an $(e_1 + e_2)$-constacyclic code of length 8 over $\Re_{1,2}$. Let $g_1(x) = (x + w)(x + w^2)$ and $g_2(x) = x + w^3$, then $C_1 = \langle g_1(x)\rangle$ and $C_2 = \langle g_2(x)\rangle$ are cyclic codes of length 8 over $\mathbb{F}_9$.

By Theorem 4.1, $\phi_{1,2}(C)$ is a linear code over $\mathbb{F}_9$ with parameters $[16, 13, 3]$. By Theorem 4.5, we have $C^{\perp_\sigma} \subseteq C$, we can get a quantum code $[[16, 10, 3]]_3$ satisfying $n - k + 2 - 2d = 2$.

In Table 1, we provide some new quantum codes (in the eighth column) and compare the existing codes (in the ninth column) better (by means of larger code rate or larger distance) than [11–13]. Further, the fifth column gives the value of units $(\lambda_1, \cdots, \lambda_s)$, the sixth column gives the generator polynomials $\langle g_1(x), \cdots, g_s(x)\rangle$, where $g_i(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is denoted by $a_n a_{n-1} \cdots a_1 a_0$, e.g., "11" represents the polynomial "$x^2 + x$", the seventh column gives parameters of $\phi_{l,k}(C)$.

Table 1. New quantum codes from σ-dual-containing constacyclic codes over $\Re_{l,k}$.

p^m	n	k	l	$(\lambda_1, \cdots, \lambda_s)$	$\langle g_1(x), \cdots, g_s(x)\rangle$	$\phi_{l,k}(C)$	New codes	Existing codes
5	60	2	2	$(1, 1, -1)$	$(11, 13, 10301)$	$[180, 174, 3]$	$[[180, 168, 3]]_5$	$[[180, 166, 3]]_5$ [11]
5	33	2	2	$(1, -1, -1)$	$(124114, 114431, 114431)$	$[99, 84, 5]$	$[[99, 69, 5]]_5$	$[[99, 9, 5]]_5$ [12]
5	93	2	2	$(1, 1, -1)$	$(1014, 1014, 1011)$	$[279, 270, 3]$	$[[279, 261, 3]]_5$	$[[279, 225, 3]]_5$ [12]
17	45	2	2	$(1, -1, -1)$	$(15(13)81, 146(16)1, 146(16)1$	$[135, 123, 5]$	$[[135, 111, 5]]_{17}$	$[[135, 63, 3]]_{17}$ [12]
3	48	2	2	$(1, 1, 1)$	$(1211011, 11, 11)$	$[144, 136, 4]$	$[[144, 128, 4]]_3$	$[[144, 36, 3]]_3$ [12]
5	44	2	2	$(1, 1, 1)$	$(114431, 134411, 134411)$	$[132, 117, 5]$	$[[132, 102, 5]]_5$	$[[132, 92, 4]]_3$ [13]
5	48	2	2	$(1, 1, 1)$	$(12, 13, 13)$	$[144, 141, 2]$	$[[144, 138, 2]]_5$	$[[144, 136, 2]]_5$ [13]
9	14	1	2	$(1, -1)$	$(1ww^7 2, 1w)$	$[28, 24, 4]$	$[[28, 20, 4]]_9$	$[[28, 10, 4]]_9$ [13]

5. Conclusions

In this article, we construct quantum codes by studying the algebraic structure of σ-self-orthogonal constacyclic codes over a new finite non-chain ring $\Re_{l,k}$, and our results will enrich the code sources of constructing quantum codes. As an application, we obtain some new quantum codes from σ-dual-containing constacyclic codes over $\Re_{l,k}$ using the CSS construction or Hermitian construction and compare these codes better with the existing codes that appeared in some recent references.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was supported in part by the Zhengzhou Special Fund for Basic Research and Applied Basic Research under Grant ZZSZX202111, in part by the Postgraduate Education Reform and Quality Improvement Project of Henan Province under Grant YJS2023JD6, and in part by the Soft Science Research Project of Henan Province under Grant 232400411122.

We 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.

Conflict of interest

We declare no conflicts of interest.

References

1. A. R. Calderbank, P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A*, **54** (1996), 1098–1105. https://doi.org/10.1103/PhysRevA.54.1098

2. A. M. Steane, Simple quantum error-correcting codes, *Phys. Rev. A*, **54** (1996), 4741–4751. https://doi.org/10.1103/PhysRevA.54.4741

3. A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inf. Theory*, **44** (1998), 1369–1387. https://doi.org/10.1109/ISIT.1997.613213

4. A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inf. Theory*, **52** (2006), 4892–4914. https://doi.org/10.1109/TIT.2006.8836123

5. Y. Fan, L. Zhang, Galois self-dual constacyclic codes, *Des. Codes Cryptogr.*, **84** (2017), 473–492. https://doi.org/10.1007/s10623-016-0282-8

6. X. Liu, Y. Fan, H. Liu, Galois LCD codes over finite fields, *Finite Fields Appl.*, **49** (2018), 227–242. https://doi.org/10.1016/j.ffa.2017.10.001

7. H. Liu, X. Pan, Galois hulls of linear codes over finite fields, *Des. Codes Cryptogr.*, **88** (2020), 241–255. https://doi.org/10.1007/s10623-019-00681-2

8. H. Liu, J. Liu, On σ-self-orthogonal constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Adv. Math. Commun.*, **16** (2022), 643–665. https://doi.org/10.3934/amc.2020127

9. Y. Fu, H. Liu, Galois self-dual extended duadic constacyclic codes, *Disc. Math.*, **346** (2023), 113167. https://doi.org/10.1016/j.disc.2022.113167

10. S. Huang, S. Zhu, J. Li, Three classes of optimal Hermitian dual-containing codes and quantum codes, *Quantum Inf. Process.*, **22** (2023), 45. https://doi.org/10.1007/s11128-022-03791-4

11. H. Islam, O. Prakash, New quantum codes from constacyclic and additive constacyclic codes, *Quantum Inf. Process.*, **19** (2020), 319. https://doi.org/10.1007/s11128-020-02825-z

12. K. Gowdhaman, C. Mohan, D. Chinnapillai, J. Gao, Construction of quantum codes from λ-constacyclic codes over the ring $\frac{\mathbb{F}_p[u,v]}{\langle v^3-v,u^3-u,uv-vu\rangle}$, *J. Appl. Math. Comput.*, **65** (2021), 611–622. https://doi.org/10.1007/s12190-020-01407-7

13. H. Islam, O. Prakash, Construction of LCD and new quantum codes from cyclic codes over a finite non-chain ring, *Cryptogr. Commun.*, **14** (2022), 59–73. https://doi.org/10.1007/s12095-021-00516-9

14. B. Kong, X. Zheng, Non-binary quantum codes from constacyclic codes over $\mathbb{F}_q[u_1, u_2, \cdots, u_k]/\langle u_i^3 = u_i, u_i u_j = u_j u_i\rangle$, *Open Math.*, **20** (2022), 1013–1020. https://doi.org/10.1515/math-2022-0459

15. B. Kong, X. Zheng, Quantum codes from constacyclic codes over S_k, *EPJ Quantum Technol.*, **10** (2023), 3. https://doi.org/10.1140/epjqt/s40507-023-00160-7

16. X. Liu, L. Yu, P. Hu, New entanglement-assisted quantum codes from k-Galois dual codes, *Finite Fields Appl.*, **55** (2019), 21–32. https://doi.org/10.1016/j.ffa.2018.09.001

17. X. Liu, H. Liu, L. Yu, New EAQEC codes constructed from Galois LCD codes, *Quantum Inf. Process.*, **19** (2020), 20. https://doi.org/10.1007/s11128-019-2515-z

18. H. Li, An open problem of k-Galois hulls and its application, *Disc. Math.*, **346** (2023), 113361. https://doi.org/10.1016/j.disc.2023.113361