IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 12, 2020, accepted October 20, 2020, date of publication October 23, 2020, date of current version November 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3033326

Quantum Codes Obtained From Constacyclic Codes Over a Family of Finite Rings $\mathbb{F}_p[u_1, u_2, \ldots, u_s]$

HAI Q. DINH[1,2], TUSHAR BAG[3], SACHIN PATHAK[3], ASHISH KUMAR UPADHYAY[3], AND WARATTAYA CHINNAKUM[4]

[1]Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[2]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[3]Department of Mathematics, IIT Patna, Patna 801103, India
[4]Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Chiang Mai 50200, Thailand

Corresponding author: Hai Q. Dinh (dinhquanghai@tdtu.edu.vn)

This work was supported in part by the Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Thailand. The work of Tushar Bag and Sachin Pathak was supported by the University Grant Commission (UGC), Government of India.

ABSTRACT In this article, we construct some MDS quantum error-correcting codes (QECCs) from classes of constacyclic codes over $R_s = \mathbb{F}_p + u_1\mathbb{F}_p + \cdots + u_s\mathbb{F}_p$, $u_i^2 = u_i$, $u_iu_j = u_ju_i = 0$, for odd prime p and $i, j = 1, 2, \ldots, s$, $i \neq j$. Many QECCs with improved parameters than the existing ones in some of the earlier papers are provided. We present a set of idempotent generators of the ring R_s, and using that we define linear codes, determine all units, and study constacyclic codes over this ring. Among others, we study dual containing constacyclic codes over R_s and construct (non-binary) QECCs. An algorithm to construct QECCs from dual containing constacyclic codes over R_s is obtained that can provide many quantum codes.

INDEX TERMS Cyclic codes, negacyclic codes, constacyclic codes, quantum codes.

I. INTRODUCTION

The classical error-correcting codes are built in our classical computers and digital network to relay information and correct errors that exist in the information during transmission. While the question of factorizing a number to its primes is quickly accomplished for small numbers, it requires months of computing power with large numbers, even with the best computers around. Quantum computers that operate with quantum mechanics concepts have the potential to simulate things much better than the classical models. When working on it, a quantum machine is believed to be able to solve a problem faster than our traditional computers. In the future, quantum computers would dominate the main field for this reason instead of classical computers. Quantum computers can mark the application of error-correcting codes as one of the key reasons for this efficacy. Quantum error-correcting codes (QECCs) play an important role in quantum computing and quantum commutation.

The associate editor coordinating the review of this manuscript and approving it for publication was Faissal El Bouanani.

The theory of the classical error-correcting codes has differences from the theory of QECCs. For example, the theory of classical error-correcting codes began in 1948 with Shannon's paper, [34]. However the theory of QECCs began in 1995 with Shor's paper [35]. Shor constructed the maiden QECC in 1995. Then in the next year 1996, Steane [37] studied properties of simple QECC. Following the work of Calderbank *et al.* [11], researches in QECCs took a major move forward. According to this work, it is enough to find classical codes, which contain their duals in order to obtain the QECCs. Later, Ashikmin and Knill generalized these results to a non binary case [4]. After that, many good QECCs have been constructed by using the cyclic and constacyclic codes over finite fields. Working over finite rings, researchers have constructed QECCs with better parameters [1]–[3], [5], [6], [8], [21]–[23], [25], [26], [28], [32], [33], [36]. Very recently, Bag *et al.* [7] studied the dual containing property of constacyclic and skew constacyclic codes over finite rings and constructed new non binary QECCs from their studies.

Motivated by these works, in this article, we study Γ-constacyclic codes over the ring $R_s = \mathbb{F}_p + u_1\mathbb{F}_p + \cdots + u_s\mathbb{F}_p$, for odd prime p with $u_i^2 = u_i, u_iu_j = u_ju_i = 0$, and

$i, j = 1, 2, \ldots, s, i \neq j$. As an application of this study, we construct QECCs from Γ-constacyclic codes over the ring R_s. This article is organized as follows. In Section 2, we give some definitions and linear codes construction over this ring R_s, which are represented by means of $s+1$ p-ary codes. In Section 3, we discuss some properties of Γ-constacyclic codes over R_s. In Section 4, we study a dual-containing property for Γ-constacyclic codes over R_s and construct QECCs from them. It is observed that, our constructed QECCs have better parameters than the existing ones appeared in the literature over $\mathbb{F}_p$, for odd prime p. We also construct some MDS QECCs from this study.

II. PRELIMINARIES

Consider the ring $R_s = \mathbb{F}_p + u_1\mathbb{F}_p + \cdots + u_s\mathbb{F}_p$, where p is an odd prime and $u_i^2 = u_i$, $u_iu_j = u_ju_i = 0$, for $i, j = 1, 2, \ldots, s$; $i \neq j$. It is a commutative Frobenius ring with p^{s+1} elements.

Recall that, a linear code C over R_s of length n is a R_s-submodule of R_s^n. Elements of C are called codeword. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$. A linear code C is said to be a λ-constacyclic code of length n over R_s if $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ then $\Psi(\mathbf{c}) := (\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in C$, where Ψ is the λ-constacyclic shift operator. When $\lambda = 1$, a constacyclic code is called a cyclic code, and a negacyclic code if $\lambda = -1$. By identifying each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ with a polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ in $R_s[x]/\langle x^n - \lambda\rangle$ we can say, a linear code C is a λ-constacyclic code of length n over R_s if and only if it is an ideal of the ring $R_s[x]/\langle x^n - \lambda\rangle$. Constacyclic codes over finite fields and finite commutative Frobenious rings have been studied extensively by many authors (see, e.g., [12]–[20], [31].)

Let $e_0 = 1 - u_1 - u_2 - \cdots - u_s$ and $e_j = u_j$, for $j = 1, 2, \ldots, s$. Then it is easy to check that $e_0 + e_1 + \cdots + e_s = 1$, $e_ie_j = 0$ and $e_i^2 = e_i$, where $i, j = 0, 1, 2, \ldots, s$ and $i \neq j$. Then $\{e_0, e_1, \ldots, e_s\}$ forms a nonzero pairwise orthogonal idempotent set of R_s. Thus, $R_s = e_0R_s \oplus e_1R_s \oplus \cdots \oplus e_sR_s$.

Any element $r \in R_s = \mathbb{F}_p + u_1\mathbb{F}_p + \cdots + u_s\mathbb{F}_p$ is of the form $a_0 + u_1a_1 + u_2a_2 + \cdots + u_sa_s$, and can be expressed as

$$\begin{aligned} r &= a_0 + u_1a_1 + u_2a_2 + \cdots + u_sa_s \\ &= (1 - u_1 - u_2 - \cdots - u_s)a_0 + u_1(a_0 + a_1) \\ &\quad + u_2(a_0 + a_2) + \cdots + u_s(a_0 + a_s) \\ &= e_0b_0 + e_1b_1 + \cdots + e_sb_s, \end{aligned}$$

where $a_j \in \mathbb{F}_p; j = 0, 1, \ldots, s$ such that $b_0 = a_0$ and $b_j = a_0 + a_j$, for $j = 1, 2, \ldots, s$. Therefore, any $r \in R_s$ can be expressed uniquely as $r = e_0b_0 + e_1b_1 + \cdots + e_sb_s$, for $b_0, b_1, \ldots, b_s \in \mathbb{F}_p$.

Let $M \in GL_{s+1}(\mathbb{F}_p)$ such that $MM^t = \lambda I_{s+1}$, where M^t denotes the transpose of the matrix M, I_{s+1} denotes the identity matrix of order $s+1$ and λ be a non-zero element of $\mathbb{F}_p$. We define a Gray map

$$\Phi : R_s \longrightarrow \mathbb{F}_p^{s+1}, \quad \text{given as} \quad \Phi(r) = (b_0, b_1, \ldots, b_s)M.$$

We can extend this Gray map component-wise from R_s^n to $\mathbb{F}_p^{n(s+1)}$ such that

$$(r_0, r_1, \ldots, r_{n-1}) \mapsto (\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{n-1})M,$$

where $r_i = e_0b_{0,i} + e_1b_{1,i} + \cdots + e_sb_{s,i} \in R_s$, and $\mathbf{b}_i = (b_{0,i}, b_{1,i}, \ldots, b_{s,i}) \in \mathbb{F}_p^{s+1}$, for $i = 0, 1, \ldots, n-1$. We define the Lee weight of r as $w_L(r) = w_H(\Phi(r))$, and the Lee weight of $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1}) \in R_s^n$ is defined as $w_L(\mathbf{r}) = \sum_{i=0}^{n-1} w_L(r_i)$. The Lee distance between $\mathbf{r}$ and $\mathbf{r}' \in R_s^n$ is defined by $d_L(\mathbf{r}, \mathbf{r}') = w_L(\mathbf{r} - \mathbf{r}') = w_H(\Phi(\mathbf{r} - \mathbf{r}'))$. The minimum Lee distance of C is defined as $d_L = d_L(C) = \min\{d_L(\mathbf{r}, \mathbf{r}') \mid \mathbf{r} \neq \mathbf{r}'\}$. It is easy to see that, this Gray map Φ is a $\mathbb{F}_p$-linear distance preserving map from R_s^n to $\mathbb{F}_p^{(s+1)n}$. By the bijectivity of the Gray map, it is readily follows that, $\Phi(C)$ is a $[(s+1)n, k, d_H]$ linear code over $\mathbb{F}_p$, where $d_L = d_H$ and k is the dimension of $\Phi(C)$.

The Euclidean inner product of $\mathbf{r}$ and $\mathbf{r}'$ in R_s^n is defined as $\mathbf{r} \cdot \mathbf{r}' = r_0r_0' + r_1r_1' + \cdots + r_{n-1}r_{n-1}'$. The dual code $C^\perp$ is defined as $C^\perp = \{\mathbf{r} \in R_s^n \mid \mathbf{r} \cdot \mathbf{r}' = 0, \ \forall\, \mathbf{r}' \in C\}$. A code C is called a dual-containing code if $C^\perp \subseteq C$.

We denote

$$\begin{aligned} D_0 \oplus D_1 \oplus \cdots \oplus D_s &= \{d_0 + d_1 + \cdots + d_s \mid \\ &\qquad d_j \in D_j, j = 0, 1, \ldots, s\}. \\ D_0 \otimes D_1 \otimes \cdots \otimes D_s &= \{(d_0, d_1, \cdots, d_s) \mid \\ &\qquad d_j \in D_j, j = 0, 1, \ldots, s\}. \end{aligned}$$

Let C be a linear code of length n over R_s. We define

$$\begin{aligned} C_0 &= \{\mathbf{b}_0 \in \mathbb{F}_p^n \mid e_0\mathbf{b}_0 + e_1\mathbf{b}_1 + \cdots + e_s\mathbf{b}_s \in C; \\ &\quad \mathbf{b}_j \in \mathbb{F}_p^n,\ j = 1, 2, \ldots, s\}, \\ C_1 &= \{\mathbf{b}_1 \in \mathbb{F}_p^n \mid e_0\mathbf{b}_0 + e_1\mathbf{b}_1 + \cdots + e_s\mathbf{b}_s \in C; \\ &\quad \mathbf{b}_j \in \mathbb{F}_p^n,\ j = 0, 2, \ldots, s\}, \\ &\quad \cdots\cdots\cdots \\ C_s &= \{\mathbf{b}_s \in \mathbb{F}_p^n \mid e_0\mathbf{b}_0 + e_1\mathbf{b}_1 + \cdots + e_s\mathbf{b}_s \in C; \\ &\quad \mathbf{b}_j \in \mathbb{F}_p^n, j = 0, 1, 2, \ldots, s-1\}, \end{aligned}$$

Here C_j are linear codes of length n over $\mathbb{F}_p$, for $j = 0, 1, 2, \ldots, s$. So a linear code C over R_s can be expressed as $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_sC_s$.

Lemma 2.1 ([25]): Let λ be a non-zero element of $\mathbb{F}_p$. If there is a non-trivial dual-containing λ-constacyclic code over $\mathbb{F}_p$, then $\lambda = \pm 1$.

We define $H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$ (n-times) to be the n-fold tensor product of the Hilbert space H of dimension q over the complex number $\mathbb{C}$. Then $H^{\otimes n}$ is a Hilbert space of dimension q^n. A quantum code of length n and dimension k over $\mathbb{F}_q$ is defined to be a Hilbert subspace of $H^{\otimes n}$ having dimension q^k. A quantum code with length n, dimension k and minimum distance d over $\mathbb{F}_q$ is denoted by $[[n, k, d]]_q$.

The parameters of quantum codes always satisfy the quantum Singleton bound: $2d \leq n - k + 2$. A quantum code that attains the equality in the Singleton bound is called a maximum distance separable (MDS) quantum code.

The CSS construction and the dual containing property will take the main role in our construction of QECCs.

Theorem 2.2 (CSS Construction [11]): Let C_1 and C_2 be $[n, k_1, d_1]$ and $[n, k_2, d_2]$ linear codes over $\mathbb{F}_q$, respectively, with $C_2^{\perp} \subseteq C_1$, and let $d = \min\{d_1, d_2\}$. Then there exists a QECC with parameters $[[n, k_1 + k_2 - n, d]]_q$. In particular, if $C_1^{\perp} \subseteq C_1$, then there exists a QECC with parameters $[[n, 2k_1 - n, d_1]]_q$.

III. Γ-CONSTACYCLIC CODES OVER R_s

Note that

$$\begin{aligned}\Gamma &= \lambda_0 + u_1\lambda_1 + u_2\lambda_2 + \cdots + u_s\lambda_s \\ &= e_0\lambda_0 + \sum_{j=1}^{s} e_j(\lambda_0 + \lambda_j).\end{aligned}$$

Proposition 3.1: Γ is a unit of R_s if and only if λ_0 and $(\lambda_0 + \lambda_j), j = 1, 2, \ldots, s$, are units in $\mathbb{F}_p$. In particular, when Γ is a unit of R_s, its inverse is

$$\Gamma^{-1} = \lambda_0^{-1} + u_1(\lambda_0 + \lambda_1)^{-1} + u_2(\lambda_0 + \lambda_2)^{-1} + \cdots + u_s(\lambda_0 + \lambda_s)^{-1}.$$

Proof: Suppose Γ is a unit in R_s, then there exists an element $\Lambda = e_0\delta_0 + e_1\delta_1 + e_2\delta_2 + \cdots + e_s\delta_s \in R_s$ such that $\Gamma \cdot \Lambda = 1$, where

$$\begin{aligned}\Gamma \cdot \Lambda &= (e_0\lambda_0 + \sum_{j=1}^{s} e_j(\lambda_0 + \lambda_j)) \cdot (\sum_{i=0}^{s} e_i\delta_i) \\ &= e_0\lambda_0\delta_0 + e_1\delta_1(\lambda_0 + \lambda_1) + \cdots + e_s\delta_s(\lambda_0 + \lambda_s).\end{aligned}$$

On the other hand,

$$\begin{aligned}1 &= (1 - u_1 - u_2 - \cdots - u_s) + u_1 + u_2 + \cdots + u_s \\ &= e_0 + e_1 + e_2 + \cdots + e_s.\end{aligned}$$

Comparing the coefficients of $e_j, j = 0, 1, \ldots, s$, from $\Gamma \cdot \Lambda = 1$, we get we get $\lambda_0\delta_0 = 1$ and $\delta_j(\lambda_0 + \lambda_j) = 1$, for $j = 1, 2, \ldots, s$. Thus, λ_0 and $(\lambda_0 + \lambda_j)$ are units in $\mathbb{F}_p$, where $j = 1, 2, \ldots, s$, and $\delta_0 = \lambda_0^{-1}$, $\delta_j = (\lambda_0 + \lambda_j)^{-1}$.

Conversely, suppose that λ_0 and $(\lambda_0 + \lambda_j), j = 1, 2, \ldots, s$, are units in $\mathbb{F}_p$. Then there are δ'_j in $\mathbb{F}_p$ such that $\lambda_0\delta'_0 = 1$ and $(\lambda_0 + \lambda_j)\delta'_j = 1$, implying $e_0\lambda_0\delta'_0 = e_0$ and $e_j(\lambda_0 + \lambda_j)\delta'_j = e_j$, for $j = 1, 2, \ldots, s$.

Take $\Gamma' = e_0\delta'_0 + e_1\delta'_1 + e_2\delta'_2 + \cdots + e_s\delta'_s \in R_s$. Then

$$\begin{aligned}\Gamma \cdot \Gamma' &= e_0\lambda_0\delta'_0 + e_1(\lambda_0 + \lambda_1)\delta'_1 + \cdots + e_s(\lambda_0 + \lambda_s)\delta'_s \\ &= e_0 + e_1 + \cdots + e_s = 1,\end{aligned}$$

Therefore, Γ is a unit in R_s. □

Theorem 3.2: Let $C = \oplus_{j=0}^{s} e_jC_j$ be a linear code of length n over R_s and Γ be a unit in R_s. Then C is a Γ-constacyclic code of length n over R_s if and only if C_0 is a λ_0-constacyclic code and C_j are $(\lambda_0 + \lambda_j)$-constacyclic codes of length n over $\mathbb{F}_p$, for $j = 1, 2, 3, \ldots, s$.

Proof: Suppose C is a Γ-constacyclic code of length n over R_s. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$, where $c_i = e_0c_{0,i} + e_1c_{1,i} + \cdots + e_sc_{s,i}$, such that $c_{j,i} \in \mathbb{F}_p$ for $i = 0, 1, \ldots, n-1$ and $j = 0, 1, 2, \ldots, s$. Then for $j = 0, 1, 2, \ldots, s$, we have $(c_{j,0}, c_{j,1}, \ldots, c_{j,n-1}) \in C_j$. Since C is a Γ-constacyclic code of length n over R_s,

$$\Psi(\mathbf{c}) = (\Gamma c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Note that

$$\begin{aligned}\Gamma c_{n-1} &= (e_0\lambda_0 + e_1(\lambda_0 + \lambda_1) + \cdots + e_s(\lambda_0 + \lambda_s)) \\ &\quad \times (e_0c_{0,n-1} + e_1c_{1,n-1} + \cdots + e_sc_{s,n-1}) \\ &= e_0\lambda_0c_{0,n-1} + \sum_{j=1}^{s} e_j(\lambda_0 + \lambda_j)c_{j,n-1}.\end{aligned}$$

We get

$$\begin{aligned}\Psi(\mathbf{c}) &= e_0(\lambda_0c_{0,n-1}, c_{0,0}, \ldots, c_{0,n-2}) \\ &\quad + \sum_{j=1}^{s} e_j((\lambda_0 + \lambda_j)c_{j,n-1}, c_{j,0}, \ldots, c_{j,n-2}).\end{aligned}$$

Hence, $(\lambda_0\ c_{0,n-1}, c_{0,0}, \ldots, c_{0,n-2}) \in C_0$ and $((\lambda_0 + \lambda_j)c_{j,n-1}, c_{j,0}, \ldots, c_{j,n-2}) \in C_j$, for $j = 1, 2, \ldots, s$. Therefore, C_0 is a λ_0-constacyclic code and C_j are $(\lambda_0 + \lambda_j)$-constacyclic codes of length n over $\mathbb{F}_p$, for $j = 1, 2, \ldots, s$, respectively.

Conversely, suppose C_0 is a λ_0-constacyclic code and C_j are $(\lambda_0 + \lambda_j)$-constacyclic codes of length n over $\mathbb{F}_p$, for $j = 1, 2, 3, \ldots, s$. Then following the above notations, we get $(\lambda_0\ c_{0,n-1}, c_{0,0}, \ldots, c_{0,n-2}) \in C_0$ and $((\lambda_0 + \lambda_j)c_{j,n-1}, c_{j,0}, \ldots, c_{j,n-2}) \in C_j$, for $j = 1, 2, \ldots, s$. Note that,

$$\begin{aligned}&e_0(\lambda_0c_{0,n-1}, c_{0,0}, \ldots, c_{0,n-2}) \\ &\quad + \sum_{j=1}^{s} e_j((\lambda_0 + \lambda_j)c_{j,n-1}, c_{j,0}, \ldots, c_{j,n-2}) = \Psi(\mathbf{c}).\end{aligned}$$

Then by the direct sum decomposition of C, we get $\Psi(\mathbf{c}) \in C$, for any $c \in C$. Hence, C is a Γ-constacyclic code of length n over R_s. □

Properties of cyclic codes over finite fields have been discussed in [29, Theorem 12.9]. Extending those discussion for constacyclic codes over finite fields, we have the following theorem.

Theorem 3.3: Let C_j be a λ-constacyclic code of length n over $\mathbb{F}_p$. Then there exists a unique monic polynomial (generator polynomial) $f_j(x) \in \mathbb{F}_p[x]/\langle x^n - \lambda\rangle$ such that $C_j = \langle f_j(x)\rangle$ and $f_j(x) \mid (x^n - \lambda)$. Moreover, the dimension of C_j is $k_j = n - \deg(f_j(x))$, with $\{f_j(x), xf_j(x), \cdots, x^{k_j-1}f_j(x)\}$ as a basis set.

Theorem 3.4: Let $C = \oplus_{j=0}^{s} e_jC_j$ be a Γ-constacyclic code of length n over R_s. Then $C = \langle e_0f_0(x) + e_1f_1(x) + \cdots + e_sf_s(x)\rangle$, where $f_j(x)$ are the generator polynomials of C_j, for $j = 0, 1, \ldots, s$.

IV. DUAL CONTAINING Γ-CONSTACYCLIC CODES OVER R_s AND QECCs CONSTRUCTION

Recall that for codes of length n over a finite field $\mathbb{F}$, the code $C = \mathbb{F}^n$ is always a dual-containing code, as $C^{\perp} = \{0\}$. This code $C = \mathbb{F}^n$ is called a trivial dual containing code over $\mathbb{F}$. For Γ-constacyclic codes over R_s, we say that $C = \oplus_{j=0}^{s} e_j C_j$ is a non-trivial dual containing code if at least one C_j is non-trivial over $\mathbb{F}_p$, for $j = 0, 1, \ldots, s$. It is easy to see that the Hamming distance of any trivial code is 1. In this section we will show the existence of such non-trivial dual-containing Γ-constacyclic codes over R_s. Note that, when M is an identity matrix, we get $\Phi(C) = \otimes_{j=0}^{s} C_j, j = 0, 1, \ldots, s$ and $d_L(C) = d_H(\Phi(C)) = d_H(\otimes_{j=0}^{s} C_j) = \min\{d_H(C_j) \mid j = 0, 1, \ldots, s\}$. Thus, if at least one C_j is trivial, then $d_L(C) = 1$. To avoid these cases, we will consider the cases where all the C_j are non-trivial, where $j = 0, 1, \ldots, s$.

Proposition 4.1: Let C be a Γ-constacyclic code over R_s, where $\Gamma = (\lambda_0 + u_1\lambda_1 + u_2\lambda_2 + \cdots + u_s\lambda_s)$. If there is a non-trivial dual containing Γ-constacyclic code of length n over R_s, then $\Gamma \in \{\pm 1, \pm(1 - 2u_{j_1}), \pm(1 - 2u_{j_1} - 2u_{j_2}), \cdots, \pm(1 - 2u_{j_1} - 2u_{j_2} - \cdots - 2u_{j_s})\}$, where $1 \leq j_i \leq s$ and $j_i < j_{i+1}$ for $i = 1, 2, \ldots, s$.

Proof: We prove this result for $s = 2$ and the rest can be done in a similar fashion. Let C be a non-trivial dual containing Γ-constacyclic code over R_2, where $\Gamma = (\lambda_0 + u_1\lambda_1 + u_2\lambda_2)$.

As $C^\perp \subseteq C$, we get $e_0 C_0^\perp \oplus e_1 C_1^\perp \oplus e_2 C_2^\perp \subseteq e_0 C_0 \oplus e_1 C_1 \oplus e_2 C_2$. Considering modulo e_j, we get $C_j^\perp \subseteq C_j$, $j = 0, 1, 2$. By Theorem 3.2, C_0 is λ_0-constacyclic code and C_j are $(\lambda_0 + \lambda_j)$-constacyclic codes of length n over $\mathbb{F}_p$, for $j = 1, 2$. By Lemma 2.1, we get $\lambda_0, \lambda_0 + \lambda_1, \lambda_0 + \lambda_2 = \pm 1$.

Take $\lambda_0 = 1$. Then

1) If $\lambda_0 + \lambda_1 = 1$ and $\lambda_0 + \lambda_2 = 1$, then $\lambda_1 = \lambda_2 = 0$, implying $\Gamma = 1$.
2) If $\lambda_0 + \lambda_1 = 1$ and $\lambda_0 + \lambda_2 = -1$, then $\lambda_1 = 0, \lambda_2 = -2$, implying $\Gamma = 1 - 2u_2$.
3) If $\lambda_0 + \lambda_1 = -1$ and $\lambda_0 + \lambda_2 = 1$, then $\lambda_1 = -2, \lambda_2 = 0$, implying $\Gamma = 1 - 2u_1$.
4) If $\lambda_0 + \lambda_1 = -1$ and $\lambda_0 + \lambda_2 = -1$, then $\lambda_1 = \lambda_2 = -2$, implying $\Gamma = 1 - 2u_1 - 2u_2$.

Similarly, if we take $\lambda_0 = -1$, we will get $\Gamma = -(1 - 2u_1 - 2u_2), -(1 - 2u_1), -(1 - 2u_2), -1$, respectively. Thus, $\Gamma \in \{\pm 1, \pm(1 - 2u_1), \pm(1 - 2u_2), \pm(1 - 2u_1 - 2u_2)\}$. ☐

Remark 4.2: Using the values of Γ from Proposition 4.1, we have the following observations:

- If $\Gamma = 1$, then by Theorem 3.2, C_j are cyclic codes over $\mathbb{F}_p$ for $j = 0, 1, \ldots, s$.
- If $\Gamma = -1$, then by Theorem 3.2, C_j are negacyclic codes over $\mathbb{F}_p$ for $j = 0, 1, \ldots, s$.
- If $\Gamma = 1 - 2u_{j_1}$, then by Theorem 3.2, C_{j_1} is a negacyclic code and C_{j_l} are cyclic codes over $\mathbb{F}_p$ for $1 \leq j_1 \leq s$, $l \neq 1$.
- If $\Gamma = -1 + 2u_{j_1}$, then by Theorem 3.2, C_{j_1} is a cyclic code and C_{j_l} are negacyclic codes over $\mathbb{F}_p$ for $1 \leq j_1 \leq s$, $l \neq 1$.

. . . .

- If $\Gamma = 1 - 2u_{j_1} - 2u_{j_2} - \cdots - 2u_{j_s}$, then by Theorem 3.2, C_0 is a cyclic code and C_{j_i} are negacyclic codes over $\mathbb{F}_p$, where $1 \leq j_i \leq s$ and $j_i < j_{i+1}$ for $i = 1, 2, \ldots, s$.
- If $\Gamma = -1 + 2u_{j_1} + 2u_{j_2} + \cdots + 2u_{j_s}$, then by Theorem 3.2, C_0 is a negacyclic code and C_{j_i} are cyclic codes over $\mathbb{F}_p$, where $1 \leq j_i \leq s$ and $j_i < j_{i+1}$ for $i = 1, 2, \ldots, s$.

Remark 4.3: In Proposition 4.1, we discussed only non-trivial dual-containing Γ-constacyclic codes over R_s, considering all C_j are non-trivial, where $j = 0, 1, \ldots, s$. Here we discuss how Γ will look like, if not all C_j are non-trivial.

- Suppose only one C_j is non-trivial and others are trivial.
  - Consider C_0 is non-trivial and $C_j, j = 1, 2, \ldots, s$ are trivial.
  - Consider $C_j, j \neq 0$ is non-trivial and C_i are trivial, where $i \neq j, i = 0, 1, \ldots, s$.
- Suppose only two C_j are non-trivial and other are trivial.
  - Consider C_0 and C_j are non-trivial and C_i are trivial, where $i \neq j, i = 1, \ldots, s$.
  - Consider $C_i (i \neq 0)$ and $C_j (j \neq 0)$ are non-trivial and C_k are trivial, where $k \neq i, k \neq j$ and $k = 0, 1, \ldots, s$.
- . . . .
- Suppose all but one C_j are non-trivial and one copy of $C_i, i \neq j$ is trivial.

Remark 4.4: We can derive the explicit forms of Γ for the cases in Remark 4.3. Here we show two derivations, and the rest can be done similarly.

- One C_j is non-trivial and all others are trivial.
  Case I: Consider C_0 is non-trivial and $C_j, j = 1, 2, \ldots, s$, are trivial. Then $\lambda_0 = \pm 1$ and as $C_j = \mathbb{F}_p^n$, we take $\lambda_0 + \lambda_j = \eta_j$, where η_j are non-zero elements of $\mathbb{F}_p$ for $j = 1, 2, \ldots, s$. Thus, when $\lambda_0 = 1$, we get
  $$\Gamma = 1 + (\eta_1 - 1)u_1 + (\eta_2 - 1)u_2 + \cdots + (\eta_s - 1)u_s,$$
  or, when $\lambda_0 = -1$, we get
  $$\Gamma = -1 + (\eta_1 + 1)u_1 + (\eta_2 + 1)u_2 + \cdots + (\eta_s + 1)u_s.$$
  Case II: Consider $C_j, j \neq 0$ is non-trivial and C_i are trivial, where $i \neq j, i = 0, 1, \ldots, s$. Then $\lambda_0 + \lambda_j = \pm 1$ and as C_i are trivial, for $i \neq j, i = 0, 1, \ldots, s$, then $\lambda_0 = \eta_0$ and $\lambda_0 + \lambda_i = \eta_i$, where η_i are non-zero elements of $\mathbb{F}_p$ for $i \neq j, i = 0, 1, \ldots, s$. This implies $\lambda_j = \pm 1 - \eta_0$ and $\lambda_i = \eta_i - \eta_0$. Thus,
  $$\begin{aligned}\Gamma = \eta_0 &+ (\eta_1 - \eta_0)u_1 + (\eta_2 - \eta_0)u_2 + \cdots \\ &+ (\eta_{j-1} - \eta_0)u_{j-1} + (1 - \eta_0)u_j \\ &+ (\eta_{j+1} - \eta_0)u_{j+1} + \cdots + (\eta_s - \eta_0)u_s,\end{aligned}$$
  or
  $$\begin{aligned}\Gamma = \eta_0 &+ (\eta_1 - \eta_0)u_1 + (\eta_2 - \eta_0)u_2 + \cdots \\ &+ (\eta_{j-1} - \eta_0)u_{j-1} - (1 + \eta_0)u_j \\ &+ (\eta_{j+1} - \eta_0)u_{j+1} + \cdots + (\eta_s - \eta_0)u_s,\end{aligned}$$

- One C_j is trivial and all others are non-trivial.
  Case I: Consider C_0 is trivial and $C_j, j = 1, 2, \ldots, s$ are non-trivial. Then $\lambda_0 = \eta_0$ and $\lambda_0 + \lambda_j = \pm 1$, for a non-zero element η_0 of $\mathbb{F}_p$ and $j = 1, 2, \ldots, s$. Therefore, $\lambda_j = 1 - \eta_0$ or $-1 - \eta_0$. Hence,
  $$\Gamma = \eta_0 + (1-\eta_0)u_1 + (1-\eta_0)u_2 + \cdots + (1-\eta_0)u_s,$$
  or
  $$\Gamma = \eta_0 + (-1-\eta_0)u_1 + (-1-\eta_0)u_2 + \cdots + (-1-\eta_0)u_s.$$
  Case II: Consider $C_j, j \neq 0$ is trivial and C_i are non-trivial, for $i \neq j$ and $i = 0, 1, \ldots, s$. Then $\lambda_j = \eta_j$, $\lambda_0 = \pm 1$ and $\lambda_0 + \lambda_i = \pm 1$, for $i \neq j, i = 0, 1, \ldots, s$. If $\lambda_0 = 1$, we get $\lambda_i = 0$ or 2, and if $\lambda_0 = -1$, we get $\lambda_i = 0$ or -2. Thus, for
  1) $\lambda_0 = 1, \lambda_j = \eta_j$ and $\lambda_i = 0$, for $i \neq j, i = 0, 1, \ldots, s$. Therefore,
  $$\Gamma = 1 + \eta_j u_j.$$
  2) $\lambda_0 = 1, \lambda_j = \eta_j$ and $\lambda_i = 2$, for $i \neq j, i = 0, 1, \ldots, s$. Therefore,
  $$\Gamma = 1 + 2u_1 + 2u_2 + \cdots + \eta_j u_j + \cdots + 2u_s.$$
  3) $\lambda_0 = -1, \lambda_j = \eta_j$ and $\lambda_i = 0$, for $i \neq j, i = 0, 1, \ldots, s$. Therefore,
  $$\Gamma = -1 + \eta_j u_j.$$
  4) $\lambda_0 = -1, \lambda_j = \eta_j$ and $\lambda_i = -2$, for $i \neq j, i = 0, 1, \ldots, s$. Therefore,
  $$\Gamma = -1 - 2u_1 - 2u_2 + \cdots + \eta_j u_j + \cdots - 2u_s.$$

Lemma 4.5: [11] *Let C_j be a λ-constacyclic code of length n with generator polynomial $f_j(x)$ over $\mathbb{F}_p$. Then C_j contains its dual code if and only if $x^n - \lambda \equiv 0 \pmod{f_j(x)\, f_j^*(x)}$, where $\lambda = \pm 1$ and $f_j^*(x)$ is the reciprocal polynomial of $f_j(x)$, for $j = 0, 1, \ldots, s$.*

Using Lemma 4.5, we can easily show that, the code C of length n over R_s contains its dual if and only if $x^n - \lambda_0 \equiv 0 \pmod{f_0(x) f_0^*(x)}$ and $x^n - (\lambda_0 + \lambda_j) \equiv 0 \pmod{f_j(x) f_j^*(x)}$, where $\lambda_0 = \pm 1 = \lambda_0 + \lambda_j$ for $j = 1, 2, \ldots, s$.

Proposition 4.6: Let $C = \oplus_{j=0}^{s} e_j C_j$ be a linear code of length n over R_s and Φ be the Gray map. Then $\Phi(C^\perp) = \Phi(C)^\perp$.

Proof: Let $\mathbf{a} = e_0\mathbf{a}_0 + e_1\mathbf{a}_1 + \cdots + e_s\mathbf{a}_s \in C$ and $\mathbf{b} = e_0\mathbf{b}_0 + e_1\mathbf{b}_1 + \cdots + e_s\mathbf{b}_s \in C^\perp$. Hence,
$$\mathbf{a}\cdot\mathbf{b} = e_0\mathbf{a}_0\mathbf{b}_0 + e_1\mathbf{a}_1\mathbf{b}_1 + \cdots + e_s\mathbf{a}_s\mathbf{b}_s = 0.$$
It is easy to see that, R_s is a $(s+1)$-dimensional vector space over $\mathbb{F}_p$.

Note that, each element of R_s can be written as a linear combination of the idempotents, thus the idempotent set $\{e_0, e_1, \ldots, e_s\}$ spans R_s.

To see the linear independence of this set, consider
$$c_0e_0 + c_1e_1 + \cdots + c_se_s = 0.$$
Now, multiplying both sides by e_j, we get $c_je_j^2 = 0$ implying $c_j = 0$, for $j = 0, 1, \ldots, s$. Hence, $\{e_0, e_1, \ldots, e_s\}$ forms a basis set.

Thus, $\mathbf{a}\cdot\mathbf{b} = e_0\mathbf{a}_0\mathbf{b}_0 + e_1\mathbf{a}_1\mathbf{b}_1 + \cdots + e_s\mathbf{a}_s\mathbf{b}_s = 0$ implies $\mathbf{a}_0\mathbf{b}_0 = \mathbf{a}_1\mathbf{b}_1 = \cdots = \mathbf{a}_s\mathbf{b}_s = 0$.

Now consider
$$\Phi(\mathbf{a})\cdot\Phi(\mathbf{b}) = \lambda^2(\mathbf{a}_0\mathbf{b}_0 + \mathbf{a}_1\mathbf{b}_1 + \cdots + \mathbf{a}_s\mathbf{b}_s).$$
We have $MM^t = \lambda^2 I_{s+1}$, thus $\Phi(\mathbf{a})\cdot\Phi(\mathbf{b}) = 0$ implying $\Phi(\mathbf{b}) \in \Phi(C)^\perp$, as $\Phi(\mathbf{a}) \in \Phi(C)$. Therefore, $\Phi(C^\perp) \subseteq \Phi(C)^\perp$. Also Φ is a bijection, so $|\Phi(C^\perp)| = |\Phi(C)^\perp|$. Hence, $\Phi(C^\perp) = \Phi(C)^\perp$. □

Theorem 4.7: Let $C = \oplus_{j=0}^{s} e_j C_j$ be a Γ-constacyclic code of length n over R_s. If $C^\perp \subseteq C$, then there exists a QECC with parameters $[[(s+1)n,\ 2k-(s+1)n,\ d_H]]_p$, where d_H denotes the minimum Hamming distance and k denotes the dimension of the code $\Phi(C)$.

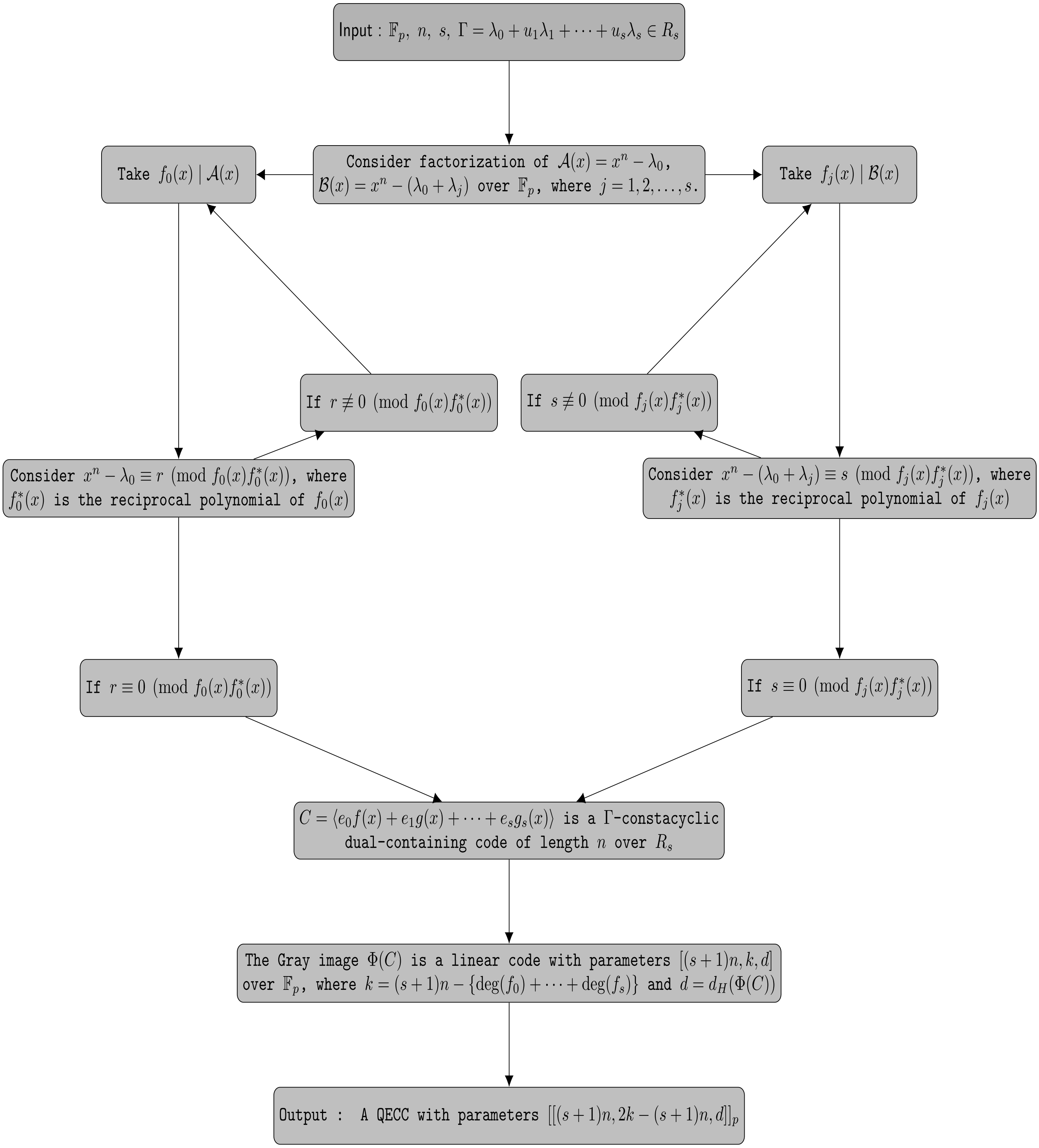
Proof: Let $\mathbf{a} \in \Phi(C^\perp) = \Phi(C)^\perp$, so $\mathbf{a} \in \phi(C)^\perp$. As $\mathbf{a} \in \Phi(C^\perp)$, there exists $\mathbf{a}' \in C^\perp$ such that $\mathbf{a} = \Phi(\mathbf{a}')$. Since $C^\perp \subseteq C$, so $\mathbf{a}' \in C$. Thus $\mathbf{a} = \Phi(\mathbf{a}') \in \Phi(C)$, which implies $\Phi(C)^\perp \subseteq \Phi(C)$. As $\Phi(C)$ is a linear code with parameters $[(s+1)n, k, d_H]$ over $\mathbb{F}_p$, by Theorem 2.2, there exists a QECC with parameters $[[(s+1)n,\ 2k-(s+1)n,\ d_H]]_p$. □

We present an algorithm to construct QECCs from Γ-constacyclic codes over R_s. This algorithm runs through all product of factor $f_i(x)$ to work on those satisfying the conditions of Lemma 4.5, for $i = 0, 1 \ldots, s$.

In this article, we aim to construct better QECCs than the existing ones appeared in the literature over $\mathbb{F}_p$, for odd prime p. The examples and the tables are computed using MAGMA Software [9], [10]. In the following examples and tables, we write coefficients in the decreasing order, for example we use $(1(12)04)^5$ to denote a polynomial $(x^3 + 12x^2 + 4)^5$.

In Tables 1, we present some QECCs with better parameters from our study of cyclic ($\Gamma = 1$) codes over R_1. Although such codes in Table 1 are better than codes in recent papers [3], [8], [25]–[28], they have low Hamming distance. We proceed to improve the parameters in Table 1 to have better parameters, specifically better Hamming distance. We end up with Table 2 of much better codes. In Table 3, we present some MDS QECCs constructed from our study of Γ-constacyclic codes over R_1.

In Tables 2 and 3, the first column shows the distances, second column denotes the unit Γ, the third and fourth columns represent the coefficients of the generator polynomials in decreasing order. In fifth and sixth columns we present the parameters of the Gray images and the constructed QECCs. The seventh column of Table 3, shows the corresponding existing QECCs. For Tables 1, 2 and 3, we consider
$$M = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad \text{such that } MM^t = 2I_2.$$



In Tables 1, 2 and 3, we consider the ring R_1 and the idempotent set $\{e_0, e_1\}$ of this ring. For a fixed n, we take $f_j(x) \mid (x^n - \lambda)$ such that $C = \langle e_0 f_0(x) + e_1 f_1(x) \rangle$, where $C_j = \langle f_j(x) \rangle$ for $j = 0, 1$. Suppose G_j are the generator matrices of C_j, then the generator matrix of C and $\Phi(C)$ are

$$G = \begin{pmatrix} e_0 G_0 \\ e_1 G_1 \end{pmatrix} \quad \text{and} \quad \Phi(G) = \begin{pmatrix} \Phi(e_0 G_1) \\ \Phi(e_1 G_1) \end{pmatrix}.$$

Thus, $\Phi(C)$ is a linear code over $\mathbb{F}_q$ with length $2n$ with generator matrix $\Phi(G)$. Now using MAGMA Software we compute the corresponding Hamming distance and the dimension of $\Phi(C)$.

Example 4.8: Suppose $s = 2, p = 5$ and $n = 44$. Consider $\Gamma = 1$, then $\lambda_0 = 1$ and $\lambda_1 = \lambda_2 = 0$. Let C be a Γ-constacyclic code over R_2. Then by Theorem 3.2, C_j are cyclic

TABLE 1. QECCs constructed from cyclic codes over R_1.

n	$f_0(x)$	$f_1(x)$	$\Phi(C)$	QECCs	Existing QECCs
8	15	18	$[16, 14, 2]$	$[[16, 12, 2]]_{13}$	$[[16, 10, 2]]_{13}$ (ref. [8])
30	12	13	$[60, 58, 2]$	$[[60, 56, 2]]_7$	$[[60, 54, 2]]_7$ (ref. [28])
36	11	12	$[72, 70, 2]$	$[[72, 68, 2]]_3$	$[[72, 66, 2]]_3$ (ref. [28])
40	11	11	$[80, 78, 2]$	$[[80, 76, 2]]_5$	$[[80, 72, 2]]_5$ (ref. [26])
45	14	14	$[90, 88, 2]$	$[[90, 86, 2]]_5$	$[[90, 84, 2]]_5$ (ref. [25])
56	13	12	$[112, 110, 2]$	$[[112, 108, 2]]_5$	$[[112, 104, 2]]_5$ (ref. [27])
60	11	12	$[120, 118, 2]$	$[[120, 116, 2]]_3$	$[[120, 114, 2]]_3$ (ref. [28])
75	14	14	$[150, 148, 2]$	$[[150, 146, 2]]_5$	$[[150, 144, 2]]_5$ (ref. [3])
84	16	15	$[168, 166, 2]$	$[[168, 164, 2]]_7$	$[[168, 162, 2]]_7$ (ref. [27])

TABLE 2. QECCs constructed from Γ-constacyclic codes over R_1.

n	Γ	$f_0(x)$	$f_1(x)$	$\Phi(C)$	QECCs	Existing QECCs
6	$-1+2u_1$	119	16(12)	$[12, 8, 5]$	$[[12, 4, 5]]_{13}$	$[[12, 4, 3]]_{13}$ (ref. [27])
9	$1-2u_1$	13032	12024	$[18, 10, 5]$	$[[18, 2, 5]]_7$	$[[18, 2, 3]]_7$ (ref. [30])
15	$-1+2u_1$	1173	1547	$[30, 24, 5]$	$[[30, 18, 5]]_{11}$	$[[30, 10, 5]]_{11}$ (ref. [30])
18	$-1+2u_1$	101	11011	$[36, 30, 3]$	$[[36, 24, 3]]_3$	$[[36, 10, 3]]_3$ (ref. [24])
18	$-1+2u_1$	12	100600(12)	$[36, 29, 4]$	$[[36, 22, 4]]_3$	$[[36, 20, 3]]_{13}$ (ref. [30])
18	$1-2u_1$	1304(12)	12024	$[36, 28, 5]$	$[[36, 20, 5]]_3$	$[[36, 8, 4]]_{13}$ (ref. [30])
21	$-1+2u_1$	11	10212	$[42, 37, 4]$	$[[42, 32, 4]]_7$	$[[42, 12, 4]]_7$ (ref. [24])
33	$1-2u_1$	124114	12013444241	$[66, 51, 4]$	$[[66, 36, 4]]_5$	$[[66, 6, 2]]_5$ (ref. [3])
33	-1	11011	121242121	$[66, 54, 5]$	$[[66, 42, 5]]_{11}$	$[[66, 36, 4]]_{11}$ (ref. [24])
24	$1-2u_1$	12	139	$[48, 45, 3]$	$[[48, 42, 3]]_{17}$	$[[48, 36, 3]]_{17}$ (ref. [27])
24	$1-2u_1$	12	145(12)	$[48, 44, 4]$	$[[48, 40, 4]]_{17}$	$[[48, 30, 4]]_{17}$ (ref. [27])
26	$-1+2u_1$	1515	132(11)(10)(12)	$[52, 44, 5]$	$[[52, 36, 5]]_{13}$	$[[52, 26, 4]]_{13}$ (ref. [24])
30	$-1+2u_1$	1042104	120034	$[60, 49, 5]$	$[[60, 38, 5]]_5$	$[[60, 36, 3]]_5$ (ref. [24])
39	$1-2u_1$	10110222	11022011011	$[78, 61, 6]$	$[[78, 44, 6]]_3$	$[[78, 42, 3]]_3$ (ref. [3])
48	1	12	11361	$[96, 91, 4]$	$[[96, 86, 4]]_7$	$[[96, 78, 3]]_7$ (ref. [8])
60	1	1121	10112	$[120, 113, 4]$	$[[120, 106, 4]]_5$	$[[120, 96, 3]]_5$ (ref. [25])
66	$-1+2u_1$	1132	114431	$[132, 124, 4]$	$[[132, 116, 4]]_5$	$[[132, 72, 2]]_5$ (ref. [3])
105	1	131	1022201	$[210, 202, 3]$	$[[210, 194, 3]]_5$	$[[210, 150, 2]]_5$ (ref. [3])

codes over $\mathbb{F}_5$, where $j = 0, 1, 2$.

$$\begin{aligned} x^{44} - 1 = &(11)(12)(13)(14)(111212)(114431)\\ &\times(121232)(124114)(131333)(134411)\\ &\times(141313)(144134) \in \mathbb{F}_5[x]. \end{aligned}$$

Let $f_0(x) = 12$, $f_1(x) = 12$ and $f_2(x) = 114431$. Then $C_j = \langle f_j(x)\rangle, j = 0, 1, 2$ are cyclic codes of length 44 over $\mathbb{F}_5$. Note that, $f_j(x)f_j^*(x)$ divides $x^{44}-1$, for $j = 0, 1, 2$. Therefore, by Lemma 4.5, we get $C_j^{\perp} \subseteq C_j$, for $j = 0, 1, 2$. Thus, C is a Γ-constacyclic code over R_2 with generator polynomial $(e_0f_0(x) + e_1f_1(x) + e_2f_2(x))$, and its Gray image $\Phi(C)$ is a linear code with parameters [132, 125, 3] over $\mathbb{F}_5$.

Consider

$$M = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ -2 & 2 & -1 \end{pmatrix}.$$

TABLE 3. MDS QECCs constructed from Γ-constacyclic codes over R_1.

n	Γ	$f_0(x)$	$f_1(x)$	$\Phi(C)$ (MDS)	MDS QECCs
3	-1	12	14	$[6, 4, 3]$	$[[6, 2, 3]]_7$
5	-1	13	15	$[10, 8, 3]$	$[[10, 6, 3]]_{11}$
5	1	129	18	$[10, 7, 4]$	$[[10, 4, 4]]_{11}$
5	$-1 + 2u_1$	199	1(10)5	$[10, 6, 5]$	$[[10, 2, 5]]_{11}$
6	$1 - 2u_1$	19	1(11)	$[12, 10, 3]$	$[[12, 8, 3]]_{13}$
6	$1 - 2u_1$	1(10)	1(12)9	$[12, 9, 4]$	$[[12, 6, 4]]_{13}$
6	$1 - 2u_1$	16(12)	1(12)9	$[12, 8, 5]$	$[[12, 4, 5]]_{13}$
6	$1 - 2u_1$	16(12)	13(11)5	$[12, 7, 6]$	$[[12, 2, 6]]_{13}$
8	$-1 + 2u_1$	1(11)	1(13)	$[16, 14, 3]$	$[[16, 12, 3]]_{17}$
8	$-1 + 2u_1$	17	15(15)	$[16, 13, 4]$	$[[16, 10, 4]]_{17}$
8	$1 - 2u_1$	1(11)8	12(16)	$[16, 12, 5]$	$[[16, 8, 5]]_{17}$
8	$1 - 2u_1$	129	14(12)(10)	$[16, 11, 6]$	$[[16, 6, 6]]_{17}$
8	$1 - 2u_1$	1(14)5(13)	1(16)(10)3	$[16, 10, 7]$	$[[16, 4, 7]]_{17}$
8	$1 - 2u_1$	1354	154(12)1	$[16, 9, 8]$	$[[16, 2, 8]]_{17}$
9	1	18	1(14)	$[18, 16, 3]$	$[[18, 14, 3]]_{19}$
9	$1 - 2u_1$	1(12)	12(11)	$[18, 15, 4]$	$[[18, 12, 4]]_{19}$
9	$1 - 2u_1$	129	117	$[18, 14, 5]$	$[[18, 10, 5]]_{19}$
9	$1 - 2u_1$	146	12(10)(11)	$[18, 13, 6]$	$[[18, 8, 6]]_{19}$
9	$-1 + 2u_1$	1(13)(14)7	11(12)(18)	$[18, 12, 7]$	$[[18, 6, 7]]_{19}$
9	$-1 + 2u_1$	1(15)3(18)6	121(12)	$[18, 11, 8]$	$[[18, 4, 8]]_{19}$
9	$-1 + 2u_1$	11(12)95	12(10)(15)4	$[18, 10, 9]$	$[[18, 2, 9]]_{19}$
11	-1	12	13	$[22, 20, 3]$	$[[22, 18, 3]]_{23}$
11	1	15	112	$[22, 19, 4]$	$[[22, 16, 4]]_{23}$
11	$1 - 2u_1$	112	1(11)(12)	$[22, 18, 5]$	$[[22, 14, 5]]_{23}$
11	$-1 + 2u_1$	11(13)	12(11)(14)	$[22, 17, 6]$	$[[22, 12, 6]]_{23}$

Note that, $MM^t = 9I_3$. Hence, by Theorem 4.7, we obtain a QECC with parameters $[[132, 118, 3]]_5$, which has better parameters than $[[132, 92, 3]]_5$ appeared in [2]. □

Example 4.9: Suppose $s = 3, p = 5$ and $n = 3$. Consider $\Gamma = 1 - 2u_1 - 2u_2 - 2u_3$, then $\lambda_0 = 1, \lambda_1 = -2, \lambda_2 = -2$ and $\lambda_3 = -2$. Let C be a Γ-constacyclic code over R_3. Then by Theorem 3.2, C_0 is a cyclic code and $C_j,\ j = 1, 2, 3$ are negacyclic codes over $\mathbb{F}_{23}$.

$$x^{23} - 1 = (1(22))^{23} \in \mathbb{F}_{23}[x].$$

Let $f_0(x) = 1(22)$. Then $C_0 = \langle f_0(x)\rangle$ is a cyclic code of length 23 over $\mathbb{F}_{23}$.

$$x^{23} + 1 = (11)^{23} \in \mathbb{F}_{23}[x].$$

Let $f_1(x) = f_2(x) = 11$ and $f_3(x) = 1331$. Then $C_i = \langle f_i(x)\rangle$ are negacyclic codes of length 23 over $\mathbb{F}_{23}$, for $i = 1, 2, 3$. Thus, C is a Γ-constacyclic code over R_3 with generator polynomial $(e_0f_0(x) + e_1f_1(x) + e_2f_2(x) + e_3f_3(x))$, and its Gray image $\Phi(C)$ is a linear code with parameters $[92, 86, 4]$ over $\mathbb{F}_{23}$.

Note that, $f_0(x)f_0^*(x)$ divides $x^{23} - 1$ and $f_i(x)f_i^*(x)$ divides $x^{23} + 1$ for $i = 1, 2, 3$. Therefore, by Lemma 4.5, we get $C_j^{\perp} \subseteq C_j$, for $j = 0, 1, 2, 3$.

Consider

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Note that, $MM^t = 4I_4$. Hence, by Theorem 4.7, we obtain a QECC with parameters $[[92, 80, 4]]_{23}$, which has better parameters than $[[90, 78, 3]]_{23}$ appeared in [24]. □

Remark 4.10: Note that in Table 3, the Gray images are actually the MDS linear codes constructed from the Γ-constacyclic codes over R_1. □

Remark 4.11: Construction of QECCs from Γ-constacyclic codes is a better choice than construction of QECCs from cyclic codes. In case of QECCs from cyclic codes, our only option is to consider Γ as 1, but for QECCs construction from Γ-constacyclic codes, we will have more choices of Γ. As an example, if we consider the ring R_1, we can choose Γ from the set $\{-1, 1, 1-2u_1, -1+2u_1\}$ instead of only 1. □

V. CONCLUSION

In this article, we construct QECCs by studying Γ-constacyclic codes over the finite ring $R_s = \mathbb{F}_p + u_1\mathbb{F}_p + \cdots + u_s\mathbb{F}_p$, for odd prime p and $u_i^2 = u_i$, $u_iu_j = u_ju_i = 0$, where $i, j = 1, 2, \ldots, s$; $i \neq j$. We decompose the ring R_s by a set of orthogonal idempotents. Units of this ring are determined, and using those, Γ-constacyclic codes over R_s are studied. We also discuss the dual-containing Γ-constacyclic codes over this ring. A necessary and sufficient condition for Γ-constacyclic codes over R_s to contain their duals is provided. For better understanding of this study, we provide examples of constructed QECCs, whose parameters are better than recent ones in the literature. We also present an algorithm to construct QECCs from Γ-constacyclic codes over the finite ring R_s. For future study, it would be interesting to consider more on the complexity of our algorithm, and develop detailed encoding and decoding schemes. With the algebraic structure obtained in our paper, we believe other constructions, such as the Hermitian construction, can be employed to construct good quantum codes over small fields.

ACKNOWLEDGMENT

The authors are grateful to the anonymous reviewers who have given them helpful comments to improve the manuscript.

REFERENCES

[1] M. Ashraf and G. Mohammad, "Construction of quantum codes from cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$," *Int. J. Inf. Coding Theory*, vol. 3, no. 2, pp. 137–144, 2015.

[2] M. Ashraf and G. Mohammad, "Quantum codes from cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$," *Quantum Inf. Process*, vol. 15, no. 10, pp. 4089–4098, 2016.

[3] M. Ashraf and G. Mohammad, "Quantum codes over $\mathbb{F}_p$ from cyclic codes over $\mathbb{F}_p[u, v]/\langle u^2 - 1, v^3 - v, uv - vu\rangle$," *Cryptogr. Commun.*, vol. 11, no. 2, pp. 325–335, 2019.

[4] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.

[5] T. Bag, A. K. Upadhyay, M. Ashraf, and G. Mohammad, "Quantum codes from cyclic codes over the ring $\mathbb{F}_p[u]/\langle u^3 - u\rangle$," *Asian-Eur. J. Math.*, vol. 13, no. 1, 2020, Art. no. 2050008.

[6] T. Bag, A. Dertli, Y. Cengellenmis, and A. K. Upadhyay, "Application of constacyclic codes over the semi local ring $\mathbb{F}_p^m + v\mathbb{F}_p^m$," *Indian J. Pure Appl. Math.*, vol. 51, no. 1, pp. 265–275, 2020.

[7] T. Bag, H.Q. Dinh, A.K. Upadhyay, R. Bandi, and W. Yamaka, "Quantum codes from skew constacyclic codes over the ring $\mathbb{F}_q[u, v]/\langle u^2 - 1, v^2 - 1, uv - vu\rangle$," *Discrete Math.*, vol. 343, no. 3, 2020, Art. no. 111737.

[8] T. Bag, H. Q. Dinh, A. K. Upadhyay, and W. Yamaka, "New non-binary quantum codes from cyclic codes over product rings," *IEEE Commun. Lett.*, vol. 24, no. 3, pp. 486–490, Mar. 2020.

[9] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," *J. Symbolic Comput.*, vol. 24, nos. 3–4, pp. 235–265, Sep. 1997.

[10] W. Bosma, J. Cannon, C. Fieker, and A. Steel, Eds., *Handbook of Magma Functions*. Sydney, NSW, Australia: Univ. of Sydney, School of Mathematics and Statistics, 2013, pp. 1–5488.

[11] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[12] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, J. Gao, and S. Sriboonchitta, "Constacyclic codes of length np^s over $\mathbb{F}_p^m + u\mathbb{F}_p^m$," *Adv. Math. Commun.*, vol. 12, pp. 231–262, 2018.

[13] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, J. Gao, and S. Sriboonchitta, "A class of repeated-root constacyclic codes over $\mathbb{F}_p^m[u]/\langle u^e\rangle$ of type 2," *Finite Fields Appl.*, vol. 55, pp. 238–267, Jan. 2019.

[14] Y. Cao, Y. Cao, H. Q. Dinh, and S. Jitman, "An explicit representation and enumeration for self-dual cyclic codes over F2m+uF2m of length 2s," *Discrete Math.*, vol. 342, no. 7, pp. 2077–2091, Jul. 2019.

[15] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, J. Gao, and S. Sriboonchitta, "A class of linear codes of length 2 over fnite chain rings," *J. Algebra Appl.*, vol. 19, Jun. 2020, Art. no. 2050103.

[16] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, and F. Ma, "Construction and enumeration for self-dual cyclic codes of even length over $\mathbb{F}_2^m + u\mathbb{F}_2^m$," *Finite Fields Appl.*, vol. 61, Jan. 2020, Art. no. 101598.

[17] Y. Cao, Y. Cao, H. Q. Dinh, F.-W. Fu, and P. Maneejuk, "On matrix-product structure of repeated-root constacyclic codes over finite fields," *Discrete Math.*, vol. 343, no. 4, Apr. 2020, Art. no. 111768.

[18] Y. Cao, Y. Cao, H. Q. Dinh, R. Bandi, F. Fu, "An explicit representation and enumeration for negacyclic codes of length $2^k n$ over $\mathbb{Z}_4 + u\mathbb{Z}_4$," *Adv. Math. Commun.*, vol. 61, Jan. 2020, Art. no. 101598.

[19] Y. Cao, Y. Cao, H. Q. Dinh, T. Bag, and W. Yamaka, "Explicit representation and enumeration of repeated-root $(\delta^2 + \alpha u^2)$-constacyclic codes over $\mathbb{F}_2^m[u]/\langle u^2\lambda$," *IEEE Access*, vol. 8, pp. 55550–55562, 2020.

[20] Y. Cao, Y. Cao, H. Q. Dinh, and S. Jitman, "An efficient method to construct self-dual cyclic codes of length p^s over $\mathbb{F}_p^m + u\mathbb{F}_p^m$," *Discrete Math.*, vol. 343, no. 6, Jun. 2020, Art. no. 111868.

[21] A. Dertli, Y. Cengellenmis, and S. Eren, "On quantum codes obtained from cyclic codes over A_2," *Int. J. Quantum Inf.*, vol. 13, no. 03, Apr. 2015, Art. no. 1550031.

[22] A. Dertli, Y. Cengellenmis, and S. Eren, "Some results on the linear codes over the finite ring $\mathbb{F}_2 + v_1\mathbb{F}_2 + \cdots + v_r\mathbb{F}_2$," *Int. J. Quantum Inf.*, vol. 14, no. 1, Feb. 2016, Art. no. 1650012.

[23] A. Dertli, Y. Cengellenmis, and S. Eren, "On the linear codes over the ring R_p," *Discrete Math. Algorithm. Appl.*, vol. 8, no. 2, 2016, Art. no. 1650036.

[24] L. Diao, J. Gao and J. Lu, "Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes," *Adv. Math. Commun.*, vol. 14, no. 4, p. 555, 2020, doi: 10.3934/amc.2020029.

[25] H. Q. Dinh, T. Bag, A. K. Upadhyay, M. Ashraf, G. Mohammad, and W. Chinnakum, "Quantum codes from a class of constacyclic codes over finite commutative rings," *J. Algebra Appl.*, vol. 19, no. 12, Dec. 2020, Art. no. 2150003.

[26] H. Q. Dinh, T. Bag, A. K. Upadhyay, R. Bandi, and W. Chinnakum, "On the structure of cyclic codes over $\mathbb{F}_qRS$ and applications in quantum and LCD codes constructions," *IEEE Access*, vol. 8, no. 1, pp. 18902–18914, 2020.

[27] Y. Gao, J. Gao, and F. W. Fu, "Quantum codes from cyclic codes over the ring $\mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_r\mathbb{F}_q$," *Applicable Algebra Eng., Commun. Comput.*, vol. 30, pp. 161–174, Jul. 2019, doi: 10.1007/s00200-018-0366-y.

[28] J. Gao and Y. Wang, "u-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ and their applications of constructing new non-binary quantum codes," *Quantum Inf. Process*, vol. 17, no. 4, pp. 1–19, 2018.

[29] R. Hill, *A First Course in Coding Theory*. Oxford, U.K.: Clarendon, 1986.

[30] M. E. Koroglu and I. Siap, "Quantum codes from a class of constacyclic codes over group algebras," *Malaysian J. Math. Sci.*, vol. 11, no. 2, pp. 289–301, 2017.

[31] Y. Liu, M. Shi, H. Q. Dinh, and S. Sriboonchitta, "Repeated-root constacyclic codes of length $3l^mp^s$," *Adv. Math. Commun.*, vol. 14, pp. 359–378, Jan. 2020.

[32] F. Ma, J. Gao, and F. W. Fu, "Constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and their applications of constructing new non-binary quantum codes," *Quantum Inf. Process*, vol. 17, no. 6, pp. 1–19, 2018.

[33] J. Qian, W. Ma, and W. Guo, "Quantum codes from cyclic codes over finite ring," *Int. J. Quantum Inf.*, vol. 7, no. 6, pp. 1277–1283, Sep. 2009.

[34] C. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423 and 623–656, 1948.
[35] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 1, pp. 2493–2496, 1995.
[36] A. K. Singh, S. Pattanayek, and P. Kumar, "On quantum codes from cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$," *Asian-Eur. J. Math.*, vol. 11, no. 1, 2018, Art. no. 1850009.
[37] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 6, pp. 4741–4751, Dec. 1996.

HAI Q. DINH received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from Ohio University, USA, in 1998, 2000, and 2003, respectively. After his graduation, he worked one year as a Visiting Professor at North Dakota State University, USA. Since 2004, he has been working at Kent State University, USA, as a tenured Professor of Mathematics. He is currently a Professor of Applied Mathematics with the Department of Mathematical Sciences, Kent State University. His research interests include algebra and coding theory. Since 2004, he has been publishing more than 100 articles at high level SCI(E) research journals, such as *Journal of Algebra*, *Journal of Pure and Applied Algebra*, IEEE Transactions on Information Theory, IEEE Communications Letters, *Finite Fields and Their Applications*, *Applicable Algebra in Engineering, Communication and Computing*, and *Discrete Applied Mathematics*. He has been a well-known invited/keynote speaker at numerous international conferences and mathematics colloquium. Other than universities in the U.S., he also gave many honorary tutorial lectures at international universities in China, Indonesia, Kuwait, Mexico, Singapore, Thailand, and Vietnam.

TUSHAR BAG received the B.Sc. degree from the Ramakrishna Mission Vidymandira under the University of Calcutta, the M.Sc. degree from IIT Kanpur, India, and the Ph.D. degree from the Department of Mathematics, IIT Patna, India. His main research interests include algebraic coding theory and codes over rings. Till now he has published 16 articles.

SACHIN PATHAK received the B.Sc. degree from Agra University, in 2012, and the M.Sc. degree in mathematics from IIT Kanpur, in 2015. He is currently a Research Scholar with the Department of Mathematics, IIT Patna. He is working in the field of algebraic coding theory.

ASHISH KUMAR UPADHYAY received the B.Sc. and M.Sc. degrees in mathematics from the University of Allahabad, India, and the Ph.D. degree from the Indian Institute of Science, in 2005. He is currently working as an Associate Professor at the Department of Mathematics, IIT Patna. His research interests include algebraic coding theory and algebraic topology.

WARATTAYA CHINNAKUM is currently an Assistant Professor with the Faculty of Economics, Chiang Mai University. She is a member of the Centre of Excellence in Econometrics. She works on the macroeconomic theory, economic development, econometrics, and economic for public policy. Her research interests include coding theory, economic development, financial econometrics, and tourism economics.