ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.12, 11097–11108
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.12.90

QUANTUM PRODUCT CODES OVER THE RING $\mathbb{F}_p + u\mathbb{F}_p$

G. KARTHICK, M. CRUZ, C. DURAIRAJAN, AND GIULIANO G. LA GUARDIA[1]

ABSTRACT. In this paper, we investigate properties of (classical) cyclic codes over the finite ring $\mathcal{S} = \mathbb{F}_p + u\mathbb{F}_p$, where $u^2 = u$, p is a prime and $\mathbb{F}_p$ is the finite field with p elements. We define a Gray map and show that it preserves distances (Lee - Hamming) as well as orthogonality. We then utilize these cyclic codes to construct quantum codes over $\mathbb{F}_p$ by means of the well-known Calderbank-Shor-Steane (CSS) construction. Some of the quantum codes presented here have parameters better than the ones available in the literature.

1. INTRODUCTION

In the last two decades, many researches have focused attention in the construction of quantum codes with good or even optimal parameters; see for example the works [3, 5, 7–9, 11, 15, 16]. One of the main techniques utilized by researchers to construct quantum codes is the CSS construction [3, 12]. The first manner to apply the CSS construction is utilizing Euclidean dual-containing (classical) linear codes; the second one is to consider a pair of nested linear codes. The classical codes used in the CSS construction are codes over finite fields.

As it is natural, techniques of construction of quantum codes derived from (classical) codes over finite rings were presented more recently in the literature [1, 4, 6, 13, 14]. In [1], Bag et al. constructed p-ary quantum codes derived from cyclic codes over $\mathbb{F}_p$ and also $\mathbb{F}_pS_l$, where $p \neq 2$ is a prime, l is a positive

[1]*corresponding author*

2020 *Mathematics Subject Classification.* 81Q99.

Key words and phrases. cyclic codes, codes over rings, product codes.

integer such that $l|(p-1)$, $I_l = \{i \in \mathbb{Z} : i|(p-1), i \leq l\}$, $S_l = \prod_{i \in I_l} R_i$ and $R_i = \mathbb{F}_p[u]/\langle u^{i+1} - u\rangle$. In [4], Gao presented quantum codes over $\mathbb{F}_q$ derived from cyclic codes over the non-chain ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, where $q = p^t$, p prime, $3|(p-1)$ and $v^4 = v$. Dinh et al. [6] investigated the structure of the ring $R = \mathbb{F}_p[u]/\langle u^{i+1} - u\rangle$, where $p \neq 2$ is a prime. As an application, they generated quantum codes over $\mathbb{F}_p$ derived from cyclic and negacyclic codes over R. Ozen et al. [13] studied the structure of the ring $\mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$, where $u^2 = 1$, $v^2 = 1$ and $uv = vu$, which allowed the construction of ternary quantum codes from cyclic codes over this ring. In [14], Qian et al. constructed binary quantum codes from cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$.

In this paper we first investigate the structure of cyclic codes over the ring $\mathcal{S} = \mathbb{F}_p + u\mathbb{F}_p$, where $u^2 = u$. We show how to represent a code C over $\mathcal{S}$ in terms of its component codes C_i, which are codes over $\mathbb{F}_p$. We then define a Gray that preserves distances (Lee - Hamming) as well as orthogonality. After this, we utilize the component codes C_i to obtain p-ary quantum codes by means of the CSS construction.

The paper is organized as follows. In Section (2) we investigate the structure of cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$. We also define a Gray which preserves distances and orthogonality. In Section (3) we utilize the results of the previous section to obtain quantum codes over $\mathbb{F}_p$. Some of these new codes are better than the ones available in the literature. Section (4) presents a code comparison, i.e., we compare the parameters of our codes with the ones exhibited in the literature. Finally, in Section (5), the final remarks are drawn.

2. Codes Over Product Rings

Let us consider the finite non-chain ring $\mathcal{S} = \mathbb{F}_p + u\mathbb{F}_p$, where $u^2 = u$. For more details about theory of finite rings we refer the reader to the textbooks [2, 10].

We write

$$\mathcal{R} = (\mathbb{F}_p + u\mathbb{F}_p) \times \cdots \times (\mathbb{F}_p + u\mathbb{F}_p) = \{(a_1 + ub_1 \mid a_2 + ub_2 \mid \ \ldots \ \mid a_t + ub_t)\},$$

where $a_i, b_i \in \mathbb{F}_p$ and t is a positive integer.

Definition 2.1. *Let $\gamma = n_1 + \cdots + n_t$ be a positive integer. A code $C \subseteq \mathcal{S}^{n_1} \times \mathcal{S}^{n_2} \times \ldots \times \mathcal{S}^{n_t} = \mathcal{R}^\gamma$ over $\mathcal{S}$ of length γ is a nonempty subset of $\mathcal{R}^\gamma$. A linear code C over $\mathcal{S}$ of length γ is an $\mathcal{S}$-submodule of $\mathcal{R}^\gamma$.*

From the Chinese Remainder Theorem, if one considers the idempotent $v_1 = u$ and $v_2 = 1 - u$ ($v_1 + v_2 = 1, v_1 v_2 = 0$), it follows that $\mathcal{S} = v_1\mathcal{S} \oplus v_2\mathcal{S} \cong v_1\mathbb{F}_p + v_2\mathbb{F}_p$. Thus, every element in $v \in \mathcal{S}$ can be uniquely written as $v = av_1 + bv_2$, where $a, b \in \mathbb{F}_p$. We define a Gray map as follows:

$$\varphi_1 : \mathcal{S} \to \mathbb{F}_p^2$$
$$\varphi_1(av_1 + bv_2) = (a, b),$$

which is utilized to define the extension map on $\mathcal{R}$ given by

$$\varphi_2 : \mathcal{R} \to \mathbb{F}_p^{2t}$$
$$\varphi_2(a_1v_1 + b_1v_2 \mid a_2v_1 + b_2v_2 \mid \ \ldots \ \mid a_tv_1 + b_tv_2) = (a_1, b_1, a_2, b_2, \ldots, a_t, b_t).$$

This map can be defined to γ-length ($\gamma = n_1 + \ldots + n_t$) in a natural way:

$$\varphi : \mathcal{R}^\gamma \to \mathbb{F}_p^{2\gamma},$$
$$\begin{aligned}
&\varphi(((a_1^{(1)}, a_2^{(1)}, \ldots, a_{n_1}^{(1)})v_1 + (b_1^{(1)}, b_2^{(1)}, \ldots, b_{n_1}^{(1)})v_2 \\
&|(a_1^{(2)}, a_2^{(2)}, \ldots, a_{n_2}^{(2)})v_1 + (b_1^{(2)}, b_2^{(2)}, \ldots, b_{n_2}^{(2)})v_2| \ldots \\
&|(a_1^{(t)}, a_2^{(t)}, \ldots, a_{n_t}^{(t)})v_1 + (b_1^{(t)}, b_2^{(t)}, \ldots, b_{n_t}^{(t)})v_2)) \\
=&(a_1^{(1)}, a_2^{(1)}, \ldots, a_{n_1}^{(1)}, b_1^{(1)}, b_2^{(1)}, \ldots, b_{n_1}^{(1)}, \\
&a_1^{(2)}, a_2^{(2)}, \ldots, a_{n_2}^{(2)}, b_1^{(2)}, b_2^{(2)}, \ldots, b_{n_2}^{(2)}, \\
&\ldots, a_1^{(t)}, a_2^{(t)}, \ldots, a_{n_t}^{(t)}, b_1^{(t)}, b_2^{(t)}, \ldots, b_{n_t}^{(t)}).
\end{aligned}$$

Let $\mathcal{A}$ be a ring and consider an element $\mathbf{v} \in \mathcal{A}^n$. The Hamming weight $w_H(\mathbf{v})$ of $\mathbf{v}$ is defined as the number of nonzero coordinates of $\mathbf{v}$. The Hamming distance $d_H(\mathbf{v}, \mathbf{w})$ between $\mathbf{v}, \mathbf{w} \in \mathcal{A}^n$ is defined as $d_H(\mathbf{v}, \mathbf{w}) = w_H(\mathbf{v} - \mathbf{w})$.

Definition 2.2. *Let $v \in \mathcal{S}$. The Lee weight w_L on $\mathcal{S}$ is defined by $w_L(v) = w_H(\varphi_1(v))$. The Lee weight of a vector $\boldsymbol{v} \in \mathcal{R}^\gamma$ is the sum of the Lee weights of its coordinates.*

The next result shows important properties of the Gray map.

Theorem 2.1. *The Gray map φ is a weight preserving $\mathbb{F}_p$-linear map from (R^γ, Lee weight) to ($\mathbb{F}_p^{2\gamma}$, Hamming weight).*

Proof. It is immediate to show that φ is bijective and $\mathbb{F}_p$-linear. Since φ is linear we have $d_L(x', x'') = w_L(x' - x'') = w_H(\varphi(x' - x'')) = w_H(\varphi(x') - \varphi(x'')) = d_H(\varphi(x'), \varphi(x''))$. Therefore, φ is a weight preserving $\mathbb{F}_p$-linear map. □

If A_i, $i \in \{1,2\}$, are two linear codes, we define $A_1 \oplus A_2 = \{a_1 + a_2 \mid a_1 \in A_1, a_2 \in A_2\}$ and $A_1 \otimes A_2 = \{(a_1, a_2) \mid a_1 \in A_1, a_2 \in A_2\}$. Let C be a linear code over $\mathcal{S}$ of length n. Let us consider

$$C_1 = \{m_1 \in \mathbb{F}_p^n \mid v_1 m_1 + v_2 m_2 \in C\},$$

$$C_2 = \{m_2 \in \mathbb{F}_p^n \mid v_1 m_1 + v_2 m_2 \in C\}.$$

The codes C_1 and C_2 are $\mathbb{F}_p$-linear. It is easy to see that any cyclic code C over $\mathcal{S}$ can be represented as $C = C_1 v_1 \oplus C_2 v_2$ and $\varphi(C) = C_1 \otimes C_2$.

Let $\mathbf{v} \in \mathcal{R}^\gamma$. In order to facilitate the definition of a cyclic code $C \subseteq \mathcal{R}^\gamma$ over $\mathcal{S}$ we view a vector $\mathbf{v} = ((a_1^{(1)}, a_2^{(1)}, \ldots, a_{n_1}^{(1)})v_1 + (b_1^{(1)}, b_2^{(1)}, \ldots, b_{n_1}^{(1)})v_2 | (a_1^{(2)}, a_2^{(2)}, \ldots, a_{n_2}^{(2)})v_1 + (b_1^{(2)}, b_2^{(2)}, \ldots, b_{n_2}^{(2)})v_2 \mid \ldots | (a_1^{(t)}, a_2^{(t)}, \ldots, a_{n_t}^{(t)})v_1 + (b_1^{(t)}, b_2^{(t)}, \ldots, b_{n_t}^{(t)})v_2)$ in the form

$\mathbf{v} = (a_1^{(1)}v_1 + b_1^{(1)}v_2, a_2^{(1)}v_1 + b_2^{(1)}v_2, \ldots, a_{n_1}^{(1)}v_1 + b_{n_1}^{(1)}v_2, a_1^{(2)}v_1 + b_1^{(2)}v_2, a_2^{(2)}v_1 + b_2^{(2)}v_2, \ldots, a_{n_2}^{(2)}v_1 + b_{n_2}^{(2)}v_2, \ldots, a_1^{(t)}v_1 + b_1^{(t)}v_2, a_2^{(t)}v_1 + b_2^{(t)}v_2, \ldots, a_{n_t}^{(t)}v_1 + b_{n_t}^{(t)}v_2)$.

Definition 2.3. *A code $C \subseteq \mathcal{R}^\gamma$ over $\mathcal{S}$ is cyclic if C is closed under the cyclic shift map, i.e., for every* $\mathbf{c} = (a_1^{(1)}v_1 + b_1^{(1)}v_2, a_2^{(1)}v_1 + b_2^{(1)}v_2, \ldots, a_{n_1}^{(1)}v_1 + b_{n_1}^{(1)}v_2, a_1^{(2)}v_1 + b_1^{(2)}v_2, a_2^{(2)}v_1 + b_2^{(2)}v_2, \ldots, a_{n_2}^{(2)}v_1 + b_{n_2}^{(2)}v_2, \ldots, a_1^{(t)}v_1 + b_1^{(t)}v_2, a_2^{(t)}v_1 + b_2^{(t)}v_2, \ldots, a_{n_t}^{(t)}v_1 + b_{n_t}^{(t)}v_2) \in C$ *one has* $\tau(a_1^{(1)}v_1 + b_1^{(1)}v_2, a_2^{(1)}v_1 + b_2^{(1)}v_2, \ldots, a_{n_1}^{(1)}v_1 + b_{n_1}^{(1)}v_2, a_1^{(2)}v_1 + b_1^{(2)}v_2, a_2^{(2)}v_1 + b_2^{(2)}v_2, \ldots, a_{n_2}^{(2)}v_1 + b_{n_2}^{(2)}v_2, \ldots, a_1^{(t)}v_1 + b_1^{(t)}v_2, a_2^{(t)}v_1 + b_2^{(t)}v_2, \ldots, a_{n_t}^{(t)}v_1 + b_{n_t}^{(t)}v_2) =$
$= (a_{n_t}^{(t)}v_1 + b_{n_t}^{(t)}v_2, a_1^{(1)}v_1 + b_1^{(1)}v_2, a_2^{(1)}v_1 + b_2^{(1)}v_2, \ldots, a_{n_1}^{(1)}v_1 + b_{n_1}^{(1)}v_2, a_1^{(2)}v_1 + b_1^{(2)}v_2, a_2^{(2)}v_1 + b_2^{(2)}v_2, \ldots, a_{n_2}^{(2)}v_1 + b_{n_2}^{(2)}v_2, \ldots, a_1^{(t)}v_1 + b_1^{(t)}v_2, a_2^{(t)}v_1 + b_2^{(t)}v_2, \ldots, a_{n_t-1}^{(t)}v_1 + b_{n_t-1}^{(t)}v_2) \in C$.

A code $C \subseteq \mathcal{R}^\gamma = \mathcal{S}^{n_1} \times \mathcal{S}^{n_2} \times \cdots \times \mathcal{S}^{n_t}$ can be represented as $(C_1|C_2|\ldots|C_t)$, where $C_i \subseteq \mathcal{S}^{n_i}$, and each code C_i can be viewed as $C_{i,n_i}v_1 \oplus C'_{i,n_i}v_2$. In the case of cyclic codes we can also represent the codewords as polynomials by means of the linear map $T : \mathcal{R}^\gamma \longrightarrow \mathcal{R}^\gamma[x] = \frac{\mathcal{S}[x]}{\langle x^{n_1}-1\rangle} \times \frac{\mathcal{S}[x]}{\langle x^{n_2}-1\rangle} \times \cdots \times \frac{\mathcal{S}[x]}{\langle x^{n_t}-1\rangle}$ given by $T(((a_0^{(1)}, a_1^{(1)}, \ldots, a_{n_1-1}^{(1)})v_1 + (b_0^{(1)}, b_1^{(1)}, \ldots, b_{n_1-1}^{(1)})v_2 | (a_0^{(2)}, a_1^{(2)}, \ldots, a_{n_2-1}^{(2)})v_1 + (b_0^{(2)}, b_1^{(2)}, \ldots, b_{n_2-1}^{(2)})v_2 | \ldots | (a_0^{(t)}, a_1^{(t)}, \ldots, a_{n_t-1}^{(t)})v_1 + (b_0^{(t)}, b_1^{(t)}, \ldots, b_{n_t-1}^{(t)})v_2)) = ((a_0^{(1)} + a_1^{(1)}x + \ldots + a_{n_1-1}^{(1)}x^{n_1-1})v_1 + (b_0^{(1)} + b_1^{(1)}x + \ldots + b_{n_1-1}^{(1)}x^{n_1-1})v_2 | (a_0^{(2)} + a_1^{(2)}x + \ldots + a_{n_2-1}^{(2)}x^{n_2-1})v_1 + (b_0^{(2)} + b_1^{(2)}x + \ldots + b_{n_2-1}^{(2)}x^{n_2-1})v_2 \mid \ldots | (a_0^{(t)} + a_1^{(t)}x + \ldots + a_{n_t-1}^{(t)}x^{n_t-1})v_1 + (b_0^{(t)} + b_1^{(t)}x + \ldots + b_{n_t-1}^{(t)}x^{n_t-1})v_2)$.

Multiplication is defined as follows:

$$x \star (f_1(x)|f_2(x)|\ldots|f_t(x)) = (xf_1(x)|xf_2(x)|\ldots|xf_t(x)).$$

It is clear that $\mathcal{R}^\gamma[x]$ is an $\mathcal{S}[x]$-module under the multiplication $\star$.

Definition 2.4. *Let* $\boldsymbol{u} = ((a_1^{(1)}, a_2^{(1)}, \ldots, a_{n_1}^{(1)})v_1 + (b_1^{(1)}, b_2^{(1)}, \ldots, b_{n_1}^{(1)})v_2 | (a_1^{(2)}, a_2^{(2)}, \ldots, a_{n_2}^{(2)})v_1 + (b_1^{(2)}, b_2^{(2)}, \ldots, b_{n_2}^{(2)})v_2 \ | \ldots | (a_1^{(t)}, a_2^{(t)}, \ldots, a_{n_t}^{(t)})v_1 + (b_1^{(t)}, b_2^{(t)}, \ldots, b_{n_t}^{(t)})v_2)$ *and* $\boldsymbol{v} = ((c_1^{(1)}, c_2^{(1)}, \ldots, c_{n_1}^{(1)})v_1 + (d_1^{(1)}, d_2^{(1)}, \ldots, d_{n_1}^{(1)})v_2 | (c_1^{(2)}, c_2^{(2)}, \ldots, c_{n_2}^{(2)})v_1 + (d_1^{(2)}, d_2^{(2)}, \ldots, d_{n_2}^{(2)})v_2 | \ldots | (c_1^{(t)}, c_2^{(t)}, \ldots, c_{n_t}^{(t)})v_1 + (d_1^{(t)}, d_2^{(t)}, \ldots, d_{n_t}^{(t)})v_2)$ *be two vectors in* $\mathcal{R}^\gamma$. *An inner product on* $\mathcal{R}^\gamma$ *is defined as*

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \left[\sum_{i=1}^{n_1} (a_i^{(1)} c_i^{(1)}) + \sum_{i=1}^{n_2} (a_i^{(2)} c_i^{(2)}) + \ldots + \sum_{i=1}^{n_t} (a_i^{(t)} c_i^{(t)}) \right] v_1 + \\ + \left[\sum_{i=1}^{n_1} (b_i^{(1)} d_i^{(1)}) + \sum_{i=1}^{n_2} (b_i^{(2)} d_i^{(2)}) + \ldots + \sum_{i=1}^{n_t} (b_i^{(t)} d_i^{(t)}) \right] v_2.$$

In the following results we show that the structures of C_1 and C_2 are maintained for C and vice-versa.

Theorem 2.2. *The code* $C = v_1 C_1 \oplus v_2 C_2$ *is a cyclic code over* $\mathcal{S}$ *of length* n *if and only if* C_1 *and* C_2 *are cyclic codes over* $\mathbb{F}_p$ *of length* n.

Proof. The proof follows directly from the fact that the shift operator applied to C produces that same effect than the corresponding shift operators applied in C_1 and C_2. □

Theorem 2.3. *The code* $C \subseteq \mathcal{R}^\gamma$ *is a cyclic code over* $\mathcal{S}$ *if and only if* $C_{i,n_i} \subseteq \mathbb{F}_p^{n_i}$ *are cyclic codes over* $\mathbb{F}_p$ *for all* i.

Proof. The idea of the proof is the same as the proof of Theorem 2.2. □

Theorem 2.4. *If* C *is a cyclic code over* $\mathcal{S}$ *then* $C = \langle v_1 f_1(x), v_2 f_2(x) \rangle$, *where* $f_i(x)$ *is the generator polynomial for* C_i, $i = 1, 2$.

Proof. Since $C = v_1 C_1 \oplus v_2 C_2$ and the code C is cyclic, it follows from Theorem 2.2 that C_i is also cyclic. Hence $C = v_1 \langle f_1(x) \rangle + v_2 \langle f_2(x) \rangle$, which implies $C \subseteq \langle v_1 f_1(x), v_2 f_2(x) \rangle$. On the other hand, if $g(x) \in \langle v_1 f_1(x), v_2 f_2(x) \rangle$, i.e., $g(x) = g_1(x) v_1 \ f_1(x) + g_2(x) v_2 f_2(x)$, then $g(x) \in v_1 C_1 \oplus v_2 C_2 = C$, which implies $C = \langle v_1 f_1(x), v_2 f_2(x) \rangle$. □

Theorem 2.5. *Let* $C = v_1 C_1 \oplus v_2 C_2$ *be a cyclic code over* $\mathcal{S}$ *of length* n. *If* $f_i(x)$ *is a generator polynomial of* C_i *for* $i = 1, 2$, *then the polynomial* $f(x) = v_1 f_1(x) + v_2 f_2(x)$ *generates* C *and divides* $x^n - 1$.

Proof. Let $f(x) = v_1 f_1(x) + v_2 f_2(x)$. Since $v_1 v_2 = 0$ and both v_1, v_2 are idempotents, it follows that $v_i f_i(x) = v_i f(x)$ for $i = 1, 2$, which implies $v_i f_i(x) \in \langle f(x) \rangle$. Thus $C = \langle f(x) \rangle$, where $f_i(x) | (x^n - 1)$ for $i = 1, 2$. This implies that there exist $g_i(x) \in \mathbb{F}_p[x]/\langle x^n - 1 \rangle$ such that $f_i(x) g_i(x) = x^n - 1$ for $i = 1, 2$. Since $v_1 + v_2 = 1$ and $v_i f_i(x) g_i(x) = v_i(x^n - 1)$, it follows that $f_1(x) g_1(x) v_1 + f_2(x) g_2(x) v_2 = x^n - 1$. Because $v_i f_i(x) = v_i f(x)$ for $i = 1, 2$, we have $[g_1(x) v_1 + g_2(x) v_2] f(x) = x^n - 1$, i.e., $f(x) | (x^n - 1)$, as required. □

Theorem 2.6. *If C is a cyclic code over $\mathcal{S}$ then also is its dual code $C^\perp$.*

Proof. It is easy to see that $C^\perp = v_1 C_1^\perp \oplus v_2 C_2^\perp$. From Theorem 2.2, it follows that C_1 and C_2 are cyclic codes over $\mathbb{F}_p$; hence, $C_1^\perp$ and $C_2^\perp$ are also cyclic. Again, from Theorem 2.2, it follows that $C^\perp$ is cyclic. □

The following result is well-known in the literature. Since we do not find its proof we present it here for completeness.

Theorem 2.7. *A linear cyclic code $C = \langle f(x) \rangle$ contains its dual code if and only if $x^n - 1 \equiv 0 \ (mod f(x) f^*(x))$, where $f^*(x)$ is the reciprocal polynomial of $f(x)$.*

Proof. Assume that $C^\perp \subseteq C$, i.e., $f(x) | h^*(x)$, where $h^*(x)$ is the reciprocal polynomial of $h(x) = (x^n - 1)/f(x)$. Then there exists a polynomial $t(x) \in \mathbb{F}_q[x]$ such that $h^*(x) = f(x) t(x)$ which implies $f^*(x)[h^*(x) - f(x)t(x)] = 0$. This means that $x^n - 1 = f(x)h(x) = f^*(x) f(x) t^*(x)$, i.e., $x^n - 1 \equiv 0 \ (\text{mod} f(x) f^*(x))$.

Conversely, suppose that $x^n - 1 \equiv 0 \ (\text{mod} f(x) f^*(x))$, i.e., there exists $q(x) \in \mathbb{F}_q[x]$ such that $x^n - 1 = q(x) f(x) f^*(x)$. Hence $f^*(x) h^*(x) = q^*(x) f^*(x) f(x)$, where $h^*(x)$ is the reciprocal polynomial of $h(x) = (x^n - 1)/f(x)$. This implies that $f(x) | h^*(x)$, i.e., $C^\perp \subseteq C$. □

Theorem 2.8. *Let $C = \langle v_1 f_1(x), v_2 f_2(x) \rangle$ be a cyclic code over $\mathcal{S}$ of length n. Then $C^\perp \subseteq C$ if and only if $x^n - 1 \equiv 0 \ (mod f_i(x) f_i^*(x))$ for $i = 1, 2$.*

Proof. This is immediate from the equality $C^\perp = v_1 C_1^\perp \oplus v_2 C_2^\perp$. □

Corollary 2.1. *Let $C = v_1 C_1 \oplus v_2 C_2$ be a cyclic code over $\mathcal{S}$ of length n. Let $f_i(x)$ be the generator polynomial of C_i, $i = 1, 2$, and $f_i^\perp(x)$ be the generator for $C_i^\perp$, $i = 1, 2$, where $C_i^\perp$ are the components of $C^\perp$. Then $f_i(x) | f_i^\perp(x)$ if and only if $f(x) | f^\perp(x)$, where $f(x) = v_1 f_1(x) + v_2 f_2(x)$ and $f^\perp(x) = v_1 f_1^\perp(x) + v_2 f_2^\perp(x)$.*

Theorem 2.9. *Let $C \subseteq \mathcal{R}^\gamma$ be a cyclic code over $\mathcal{S}$. Then C contains its dual code if and only if $C_i \subseteq \mathcal{S}^{n_i}$ also contains its dual code for all i.*

Proof. Assume that $C_i^\perp \subseteq C_i$ for all i. Define $\bar{C}_1 = (C_1|0|\ldots|0), \bar{C}_2 = (0|C_2|\ldots|0)$, $\ldots, \bar{C}_t = (0|0|\ldots|C_t)$. Since $\bar{C}_i^\perp \subseteq \bar{C}_i$ for all i, it then follows that $(C_1^\perp|C_2^\perp|\ldots|C_t^\perp) \subseteq (C_1|C_2|\ldots|C_t)$, i.e., $C^\perp \subseteq C$. Conversely, if $C^\perp \subseteq C$ then $(C_1^\perp|C_2^\perp|\ldots|C_t^\perp) \subseteq (C_1|C_2|\ldots|C_t)$, which implies $C_i^\perp \subseteq C_i$. □

Corollary 2.2. *Let $C \subseteq \mathcal{R}^\gamma$ be a linear code. Then C contains its dual code if and only if C_{i,n_i} and C'_{i,n_i} contain its dual code over $\mathbb{F}_p^{n_i}$ for all $i \in 1, 2, \ldots, t$.*

Proof. The proof follows directly from Theorems 2.8 and 2.9. □

Corollary 2.3. *Let $C^\perp = v_1C_1^\perp \oplus v_2C_2^\perp$ be a cyclic code. If $h_i(x)$ is a generator polynomial for $C_i^\perp$, $i = 1, 2$, then the polynomial $h(x) = v_1h_1(x) + v_2h_2(x)$ is a generator of $C^\perp$ and divides $x^n - 1$.*

Theorem 2.10. *If $C \subseteq \mathcal{R}^\gamma$ is a linear code over $\mathcal{S}$ then $\varphi(C)$ is a linear code over $\mathbb{F}_p$ and $|C| = |\varphi(C)|$. Moreover, $\varphi(C^\perp) = [\varphi(C)]^\perp$.*

Proof. It is easy to see that the linearity of C implies the linearity of $\varphi(C)$. The equality $|C| = |\varphi(C)|$ follows since φ is bijective.

Let $\mathbf{c}^\perp = ((c_1^{(1)}, c_2^{(1)}, \ldots, c_{n_1}^{(1)})v_1 + (d_1^{(1)}, d_2^{(1)}, \ldots, d_{n_1}^{(1)})v_2|(c_1^{(2)}, c_2^{(2)}, \ldots, c_{n_2}^{(2)})v_1 + (d_1^{(2)}, d_2^{(2)}, \ldots, d_{n_2}^{(2)})v_2|, \ldots, |(c_1^{(t)}, c_2^{(t)}, \ldots, c_{n_t}^{(t)})v_1 + (d_1^{(t)}, d_2^{(t)}, \ldots, d_{n_t}^{(t)})v_2) \in C^\perp$. Then, for all $\mathbf{c} = ((a_1^{(1)}, a_2^{(1)}, \ldots, a_{n_1}^{(1)})v_1 + (b_1^{(1)}, b_2^{(1)}, \ldots, b_{n_1}^{(1)})v_2|(a_1^{(2)}, a_2^{(2)}, \ldots, a_{n_2}^{(2)})v_1 + (b_1^{(2)}, b_2^{(2)}, \ldots, b_{n_2}^{(2)})v_2\ |, \ldots, |(a_1^{(t)}, a_2^{(t)}, \ldots, a_{n_t}^{(t)})v_1 + (b_1^{(t)}, b_2^{(t)}, \ldots, b_{n_t}^{(t)})v_2) \in C$ we have

$$\langle \mathbf{c}, \mathbf{c}^\perp \rangle = \left[\sum_{i=1}^{n_1} (a_i^{(1)} c_i^{(1)}) + \sum_{i=1}^{n_2} (a_i^{(2)} c_i^{(2)}) + \ldots + \sum_{i=1}^{n_t} (a_i^{(t)} c_i^{(t)}) \right] v_1 + \left[\sum_{i=1}^{n_1} (b_i^{(1)} d_i^{(1)}) + \sum_{i=1}^{n_2} (b_i^{(2)} d_i^{(2)}) + \ldots + \sum_{i=1}^{n_t} (b_i^{(t)} d_i^{(t)}) \right] v_2 = 0.$$

This means that

$$\sum_{i=1}^{n_1} (a_i^{(1)} c_i^{(1)}) + \sum_{i=1}^{n_2} (a_i^{(2)} c_i^{(2)}) + \ldots + \sum_{i=1}^{n_t} (a_i^{(t)} c_i^{(t)}) = 0$$

and

$$\sum_{i=1}^{n_1} (b_i^{(1)} d_i^{(1)}) + \sum_{i=1}^{n_2} (b_i^{(2)} d_i^{(2)}) + \ldots + \sum_{i=1}^{n_t} (b_i^{(t)} d_i^{(t)}) = 0.$$

This implies that $\varphi(\mathbf{c})\varphi(\mathbf{c}^{\perp}) = 0$, i.e., $\varphi(C^{\perp}) \subseteq [\varphi(C)]^{\perp}$. To show that the equality holds we count the number os elements of these codes, showing that $|\varphi(C^{\perp})| = |[\varphi(C)]^{\perp}|$. We know that $|C^{\perp}| = \prod_{i=1}^{t} |C_i^{\perp}| = \prod_{i=1}^{t} p^{2n_i - k_i - k_i'}$, where k_i, k_i' are the dimensions of the $\mathbb{F}_p$-linear codes C_{i,n_i} and C'_{i,n_i}, respectively. Since φ is bijective one has $|\varphi(C^{\perp})| = \prod_{i=1}^{t} p^{2n_i - k_i - k_i'}$. On other hand we have $|\varphi(C)| = |C| = \prod_{i=1}^{t} p^{k_i + k_i'}$, hence $|[\varphi(C)]^{\perp}| = p^{2\gamma - \sum_{i=1}^{t} k_i - \sum_{i=1}^{t} k_i'}$. Therefore, $|\varphi(C^{\perp})| = |[\varphi(C)]^{\perp}|$, which implies $\varphi(C^{\perp}) = [\varphi(C)]^{\perp}$. □

Corollary 2.4. *Let $C \subseteq \mathcal{R}^{\gamma}$ be a linear code over $\mathcal{S}$. If C is a dual-containing code then also is $\varphi(C)$.*

3. The New Quantum Codes

We begin this section by recalling the concept of quantum codes. For more details with respect to this topic, the reader can consult [3, 7, 12].

Let q be a prime power. Recall that an q-ary $((n, K, d))_q$ quantum code C is an K-dimensional vector subspace of Hilbert space $(\mathbb{C}^q)^{\otimes n}$ which can correct up to $\lfloor (d-1)/2 \rfloor$ errors. If $K = q^k$ we write $[[n, k, d]]_q$. Let us recall the well known Calderbank-Shor-Steane (CSS) quantum code construction.

Theorem 3.1. *(CSS Construction) [3, 7, 12] Let C_1 and C_2 be two classical linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively, with $C_2^{\perp} \subseteq C_1$. Then there exists an $[[n, k_1 + k_2 - n, d]]_q$ stabilizer code, where $d = \min\{wt(c) \mid c \in (C_1 \setminus C_2^{\perp}) \bigcup (C_2 \setminus C_1^{\perp})\}$. In particular, if $C_1^{\perp} \subseteq C_1$ then there exists an $[[n, 2k_1 - n, d' \geq d_1]]_q$ quantum code.*

Applying the CSS construction we show the main result of this section.

Theorem 3.2. *Let $\gamma = n_1 + n_2 + \ldots + n_t$ and $C \subseteq \mathcal{R}^{\gamma}$ be a cyclic code over $\mathcal{S}$. If $C^{\perp} \subseteq C$ then there exists an $[[2\gamma, 2k - 2\gamma, d_L]]_p$ quantum code, where d_L and k denote respectively the Lee weight and the dimension of the code $\varphi(C)$.*

Proof. Since $C_i^{\perp} \subseteq C_i$ for all i, it follows from Theorem 2.9 that $C^{\perp} \subseteq C$. By Corollary 2.4, the code $\varphi(C)$ also contains it dual code. Applying the CSS construction to $\varphi(C)$ one has an $[[2\gamma, 2k - 2\gamma, d_L]]_p$ code, as required. □

In the sequence we show how to apply Theorem 3.2 in order to construct new quantum codes.

Example 1. *Let* $p = 5$ *and* $n_1 = 15, n_2 = 10$ *and* $n_3 = 8$*; we then have*

$$\begin{aligned}\mathcal{R}_\gamma =& \frac{\mathcal{S}[x]}{\langle x^{15}-1\rangle} \times \frac{\mathcal{S}[x]}{\langle x^{10}-1\rangle} \times \frac{\mathcal{S}[x]}{\langle x^{8}-1\rangle} \\ f_{1,n_1}(x) =& x+4, f'_{1,n_1}(x) = x+4, f'_{2,n_2}(x) = x+4, \\ f'_{2,n_2}(x) =& x+4, f_{3,n_3}(x) = x+2, f'_{3,n_3}(x) = x+2,\end{aligned}$$

where f_{i,n_i} *and* f'_{i,n_i} *are the generators for* C_{i,n_i} *and* C'_{i,n_i}*, respectively. Therefore, we obtain a code* $\varphi(C)$ *with parameters* $[66, 60, 2]_5$*. From the CSS construction, an* $[[66, 54, 2]]_5$ *quantum code is obtained, which is better than the* $[[66, 52, 2]]_5$ *code shown in Ref. [1].*

Example 2. *Let* $p = 7$ *and* n_1 *and* $n_2 = 24$*; define*

$$\frac{\mathcal{S}[x]}{\langle x^{24}-1\rangle} \times \frac{\mathcal{S}[x]}{\langle x^{24}-1\rangle}$$

$$\begin{aligned}f_{1,n_1}(x) = x^3+5x+4, f'_{1,n_1}(x) = x^3+5x+4, \\ f'_{2,n_2}(x) = x^3+5x+4, f'_{2,n_2}(x) = x^3+5x+4,\end{aligned}$$

where f_{i,n_i} *and* f'_{i,n_i} *are the generators for* C_{i,n_i} *and* C'_{i,n_i}*, respectively. We know that* $C^\perp \subseteq C$*. The code* $\varphi(\mathcal{C})$ *has parameters* $[96, 84, 3]_7$*; from the CSS construction one has an* $[[96, 72, 3]]_7$ *code, which is better than the* $[[96, 60, 3]]_7$ *code shown in Ref. [6].*

Example 3. *Let us now consider that* $p = 5$*,* n_1 *and* $n_2 = 20$*, i.e.,*

$$\frac{\mathcal{S}[x]}{\langle x^{20}-1\rangle} \times \frac{\mathcal{S}[x]}{\langle x^{20}-1\rangle}$$

$$\begin{aligned}f_{1,n_1}(x) = x^4+4x^3+4x^2+4x+3, f'_{1,n_1}(x) = x^4+4x^3+4x^2+4x+3, \\ f_{2,n_2}(x) = x^4+4x^3+4x^2+4x+3, f'_{2,n_2}(x) = x^4+4x^3+4x^2+4x+3,\end{aligned}$$

where f_{i,n_i} *and* f'_{i,n_i} *are the generators for* $\mathcal{C}_{i,n_i}$ *and* $\mathcal{C}'_{i,n_i}$*, respectively. Proceeding similarly as in the previous examples we obtain an* $[[80, 56, 3]]_5$ *code, which is better that the* $[[80, 54, 3]]_5$ *code, exhibited in Ref. [1].*

Example 4. *Let* $p = 5$*,* $n_1 = 15$*,* $n_2 = n_3 = 10$ *and* $n_4 = 11$*, i.e.,*

$$\frac{\mathcal{S}[x]}{\langle x^{15}-1\rangle} \times \frac{\mathcal{S}[x]}{\langle x^{10}-1\rangle} \times \frac{\mathcal{S}[x]}{\langle x^{10}-1\rangle} \times \frac{\mathcal{S}[x]}{\langle x^{11}-1\rangle}$$

$$f_{1,n_1}(x) = x^4 + 4x^3 + 4x + 1, \quad f'_{1,n_1}(x) = x^4 + 4x^3 + 4x + 1,$$
$$f_{2,n_2}(x) = x^3 + x^2 + 4x + 4, \quad f'_{2,n_2}(x) = x^3 + x^2 + 4x + 4,$$
$$f_{3,n_3}(x) = x^3 + x^2 + 4x + 4, \quad f'_{3,n_3}(x) = x^3 + x^2 + 4x + 4,$$
$$f_{4,n_4}(x) = x^5 + 2x^4 + 4x^3 + x^2 + x + 4,$$
$$f'_{4,n_4}(x) = x^5 + 2x^4 + 4x^3 + x^2 + x + 4,$$

where f_{i,n_i} and f'_{i,n_i} are the generators for $\mathcal{C}_{i,n_i}$ and $\mathcal{C}'_{i,n_i}$, respectively. Proceeding similarly as above we get an $[[92, 32, 3]]_5$.

If we consider $p = 5$, $n_1 = 15$ and $n_2 = 8$ we have an $[[46, 18, 3]]$ quantum code.

4. Code Comparison

In this section we compare the parameters of some codes constructed here with the ones available in the literature. The parameters of our codes are computed by utilizing the software MAGMA. In Table (4), n, n_1 and n_2 denote the lengths of the codes C, C_{i,n_i}, C'_{i,n_i}, respectively. The corresponding polynomial is represented by writing its coefficients; for instance, the polynomial $x^2 + 1$ is written as 101.

The criterion of comparison is the usual ones: if the quantum codes have same length and minimum distance, the better is one whose dimension is higher. According with such usual criterion, we can be seen in Table (4) that the new $[[120, 112, 2]]_3$ code is better than the $[[120, 110, 2]]_3$ code shown in Ref. [13]. Our $[[60, 52, 2]]$ code is much better than the $[[60, 24, 2]]$ code available in Ref. [4]. Additionally, the new $[[92, 24, 5]]_3$ code is comparable with the $[[92, 4, 8]]_3$ code exhibited in Ref. [13].

n	n_1	n_2	$f_{i,n_1} = f'_{i,n_1}$	$f_{i,n_2} = f'_{i,n_2}$	$[n, k, d]$	New	Existing
84	18	24	12	11	$[80, 76, 2]$	$[[84, 72, 2]]_3$	
120	33	27	12	12	$[120, 116, 2]$	$[[120, 112, 2]]_3$	$[[120, 110, 2]]_3$ [13]
60	21	9	13	13	$[60, 56, 2]$	$[[60, 52, 2]]$	$[[60, 24, 2]]$ [4]
90	22	23	11122212212	111220101002	$[90, 48, 7]$	$[[90, 6, 7]]_3$	
92	35	11	1221210120101	112102	$[92, 58, 5]$	$[[92, 24, 5]]_3$	$[[92, 4, 8]]_3$ [13]

5. Final Remarks

We have shown several results concerning cyclic codes over the ring $\mathbb{F}_p + v\mathbb{F}_p$. Applying the Gray map defined here, we have utilized great part of such results

in order to construct quantum codes derived from the product of $\mathbb{F}_p + v\mathbb{F}_p$. Some of these new codes are better than the ones displayed in the literature. As future works, it will be interesting to investigate structures of different finite rings and, consequently, the possibility of construction of quantum codes with good parameters.

REFERENCES

[1] T. BAG, H. Q. DINH, A. K. UPADHYAY, W. YAMAKA: *New non-binary quantum codes from cyclic codes over product rings*, IEEE Commun. Lett., **24**(3) (2020), 486–490.

[2] G. BINI, F. FLAMINI: *Finite Commutative Rings and their Applications*, Springer Science+Business Media New York, 2002.

[3] A. R. CALDERBANK, E. M. RAINS, P. W. SHOR, N. J. A. SLOANE: *Quantum error correction via codes over $GF(4)$*, IEEE Trans. Inform. Theory, **44**(4) (1998), 1369–1387.

[4] J. GAO: *Quantum codes from cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$*, Int. J. Quantum Inf., **13**(8) (2015), art.no.1550063.

[5] D. GOTTESMAN: *Class of quantum error-correcting codes saturating the quantum Hamming bound*, Phys. Rev. A, **54** (1996), 1862–1868.

[6] H. Q. DINH, T. BAG, A. K. UPADHYAY, M. ASHRAF, G. MOHAMMAD, W. CHINNAKUM: *Quantum codes from a class of constacyclic codes over finite commutative rings*, J. Algebra Appl., **19**(12) (2020), art.no. 2150003.

[7] A. KETKAR, A. KLAPPENECKER, S. KUMAR, P. K. SARVEPALLI: *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory, **52**(11) (2006), 4892–4914.

[8] G. G. LA GUARDIA: *Constructions of new families of nonbinary quantum codes*, Phys. Rev. A., **80** (2009), 042331:1–11.

[9] G. G. LA GUARDIA, F. R. F. PEREIRA: *Good and asymptotically good quantum codes derived from algebraic geometry*, Quantum Inform. Processing, **16** (2017), 1–12.

[10] B. R. MCDONALD: *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1974.

[11] C. MUNUERA, W. TENORIO, F. TORRES: *Quantum error-correcting codes from algebraic geometry codes of castle type*, **15** (2016), 4071–4088.

[12] M. A. NIELSEN, I. L. CHUANG: *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[13] M. OZEN, N. T. OZZAIN, H. INCE: *Quantum codes from cyclic codes over $\mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$*, **766** (2016), 12–20.

[14] J. QIAN, W. MA, W. GUO: *Quantum codes from cyclic codes over finite ring*, Int. J. Quantum Inform., **7**(6) (2009), 1277–1283.

[15] E. M. RAINS: *Nonbinary quantum codes*, IEEE Trans. Inform. Theory, **45**(6) (1999), 1827–1832.

[16] A. STEANE: *Enlargement of Calderbank-Shor-Steane quantum codes*, IEEE Trans. Inform. Theory, **45**(7) (1999), 2492–2495.

Department of Mathematics
Bharathidasan University
Tiruchirappalli-24, Tamilnadu, India.
Email address: karthimath123@bdu.ac.in

Department of Mathematics, Bishop Heber College
Bharathidasan University
Tiruchirappalli-17, Tamilnadu, India
Email address: cruzmohan@gmail.com

Department of Mathematics
Bharathidasan University
Tiruchirappalli-24, Tamilnadu, India
Email address: cdurai66@bdu.ac.in

Department of Mathematics
State University of Ponta Grossa
Campus Uvaranas - Av. General Carlos Cavalcanti
4748 - 84030-900, Ponta Grossa-PR-Brazil
Email address: gguardia@uepg.br