Quantum Information Processing (2019) 18:365
https://doi.org/10.1007/s11128-019-2476-2

Quantum codes from codes over the ring $\mathbb{F}_q + \alpha\mathbb{F}_q$

Murat Güzeltepe[1] · Mustafa Sarı[2]

Received: 27 May 2019 / Accepted: 4 October 2019 / Published online: 28 October 2019

Abstract

In this paper, we aim to obtain quantum error correcting codes from codes over a nonlocal ring $R_q = \mathbb{F}_q + \alpha\mathbb{F}_q$. We first define a Gray map φ from R_q^n to $\mathbb{F}_q^{2n}$ preserving the Hermitian orthogonality in R_q^n to both the Euclidean and trace-symplectic orthogonality in $\mathbb{F}_q^{2n}$. We characterize the structure of cyclic codes and their duals over R_q and derive the condition of existence for cyclic codes containing their duals over R_q. By making use of the Gray map φ, we obtain two classes of q-ary quantum codes. We also determine the structure of additive cyclic codes over R_{p^2} and give a condition for these codes to be self-orthogonal with respect to Hermitian inner product. By defining and making use of a new map δ, we construct a family of p-ary quantum codes.

Keywords Quantum codes · Cyclic codes · Gray map

1 Introduction

Quantum error correcting codes(QECC) are useful tool in quantum computation and communication to detect and correct the quantum errors while quantum information is transferred via quantum channel. While it is initially supposed that there is no way to quantum computation and communication due to the difficulties such as decoherence destroying the information of qubits having a superposition, encoding one qubit to nine qubits, the first quantum code called Shor code [16] encourages the researchers in overcoming this problem and deriving a systematic construction for QECC. In [3] and [17], respectively, Shor et al. and Steane, as independence of each other, discover a systematic way to construct QECC which are called CSS code. It is no longer enough to consider two classical linear codes over $GF(2)$ which are nested for constructing binary QECC. Gottesman [6] comes up with an outstanding notion that aims to detect and correct the quantum errors for QECC by considering their stabilizer groups that

✉ Murat Güzeltepe
mguzeltepe@sakarya.edu.tr

[1] Department of Mathematics, Sakarya University, 54187 Sakarya, Turkey

[2] Department of Mathematics, Yıldız Technical University, Istanbul, Turkey

are subgroups of Pauli matrices group on binary qubits. In [4], it is shown that it is equivalent finding additive codes over $GF(4)$ which are self-orthogonal with respect to certain trace inner product to finding binary stabilizer QECC. By redefining the Pauli matrices on qubits over higher alphabets, the results given in [4] are generalized to stabilizer QECC over $\mathbb{F}_q$ in [2,10]. In [10], the finding stabilizer codes of length n over $\mathbb{F}_q$ is transformed into at first the finding additive codes of length $2n$ over $\mathbb{F}_q$ which are self-orthogonal with respect to trace-alternating form and then the finding additive codes of length n over $\mathbb{F}_{q^2}$ which are self-orthogonal with respect to trace-symplectic form. It is also shown that for a linear code over $\mathbb{F}_{q^2}$, its dual with respect to trace-alternating form is equal to its dual with respect to Hermitian inner product, whence paves the way for many further researches, some of which are [1,5,9,18]. Next, Kai et al. [9] consider the quantum codes constructed via the Hermitian dual containing negacyclic codes which are a class of constacyclic codes. The study [5] also provides the construction of quantum codes via a certain class of constacyclic codes containing Hermitian duals. In this study, instead of the classical linear codes over $\mathbb{F}_{q^2}$ including their Hermitian duals, we consider the linear codes over $\mathbb{F}_q$ containing their Euclidean and trace-symplectic duals as the Gray images of certain codes over a nonlocal ring R_q(will be defined later).

This paper includes six sections organized as follows: Section 2 gives to the readers some basic definitions and notations which they need in next sections. Section 3 introduces a Gray map $\varphi : R_q^n \to \mathbb{F}_q^{2n}$ which preserves both Euclidean and trace-symplectic orthogonality in $\mathbb{F}_q^{2n}$. Section 4 studies the cyclic codes and their Hermitian duals (defined in Sect. 2). It also illustrates some quantum codes obtained from cyclic codes over R_5 of length 9 and 11. Section 5 aims to find a condition for additive cyclic codes over $R_q, q = p^2$, to contain their Hermitian duals. Introducing a map $\delta : R_{p^2}^n \to \mathbb{F}_p^{4n}$ preserving the orthogonality, it also gives some quantum code examples obtained from additive cyclic codes over R_5 of length 11. Section 6 concludes the paper.

2 Preliminaries

Let $\mathbb{F}_q$ be a finite field having q elements, where q is a prime power. A code of length n over $\mathbb{F}_q$ is a nonempty subset of $\mathbb{F}_q^n$. A subspace of $\mathbb{F}_q^n$ is a linear code of length n over $\mathbb{F}_q$ and so a linear code has a dimension k. The Hamming weight $w_H(x)$ of a vector $x = (x_0, x_1, \ldots, x_{n-1})$ is the number of nonzero coordinates of the vector x. The Hamming distance $d_H(x, y)$ between two vectors $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ is the Hamming weight of the vector $x - y$. For $u = \left(\beta_1\ \beta_2 \cdots \beta_n\right),\ v = \left(\gamma_1\ \gamma_2 \cdots \gamma_n\right) \in R_q^n$, consider $x_t + iy_t$ with $|x_t| + |y_t|$ minimum. Then, the Mannheim distance between these word u and v is defined as

$$d_M(u,\ v) = \sum_{t=1}^{n} (|x_t| + |y_t|).$$

An element of a code is called codeword. The (minimum) Hamming distance $d_H(C)$ of a code C is defined as the minimum Hamming distance between two distinct codewords in the code C. Also, the Mannheim distance $d_M(C)$ of a code C can be defined in the similar way. $[n, k, d]_q$ and $[n, k, d_M]_q$ codes refer to linear codes of length n over $\mathbb{F}_q$ and R_q having dimension k and Hamming distance d and Mannheim distance d_M, respectively. Recall that the Euclidean inner product $\langle x, y\rangle$ of two vectors $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ is $\langle x, y\rangle = \sum_{i=0}^{n-1} x_i y_i$. The set $C^{\perp} = \{y \in \mathbb{F}_q^n : \langle x, y\rangle = 0,\ \forall x \in C\}$ is called the Euclidean dual of the code C.

Define $\mathbb{C}^{q^n} = \mathbb{C}^q \otimes \mathbb{C}^q \cdots \otimes \mathbb{C}^q$, where $\mathbb{C}^q$ is q-dimensional complex vector space. An $((n, M, d))_q$ quantum code is defined as a subspace with M generators of $\mathbb{C}_q^n$ such that it can detect $d - 1$ errors but not some d errors. If specially $M = q^k$, such a quantum code is denoted by $[[n, k, d]]_q$. The following two theorems show that there is a strong relation between codes over $\mathbb{F}_q$ and quantum error correcting codes.

Theorem 1 ([10] CSS Code Construction) *Suppose that C and C_1 are two $[n, k, d]_q$ and $[n, k_1, d_1]_q$ codes, respectively, such that $C_1 \subseteq C$. Then, there exists a $[[n, k - k_1, d']]_q$ quantum error correcting code, where*

$$d' = \min\left\{w_H(x) : x \in (C - C_1) \cup \left(C_1^{\perp} - C^{\perp}\right)\right\} \geq \min\left\{d, d_1^{\perp}\right\} \tag{1}$$

and $d_1^{\perp} = d_H(C_1^{\perp})$. If, particularly, the code C contains its Euclidean dual, then there exists a $[[n, 2k - n, d']]_q$ quantum error correcting code, where

$$d' = \min\{w_H(x) : x \in C - C^{\perp}\} \geq d. \tag{2}$$

Define the trace $tr : \mathbb{F}_q \to \mathbb{F}_p$, $tr(x) = x + x^p + \cdots + x^{p^{m-1}}$, where $q = p^m$. The trace-symplectic inner product of two vectors (x, y) and (x', y') of $\mathbb{F}_q^{2n}$ is given in [10] as follows:

$$\left\langle (x, y), (x', y')\right\rangle_s := tr\left(\langle x', y\rangle - \langle x, y'\rangle\right). \tag{3}$$

The set $C^{\perp_s} = \{y \in \mathbb{F}_q^{2n} : \langle x, y\rangle_s = 0,\ \forall x \in C\}$ is called the trace-symplectic dual of the code C. Recall that the symplectic weight of a vector (x, y) in $\mathbb{F}_q^{2n}$ is $w_s(x, y) = n - |\{i : x_i = 0 \text{ and } y_i = 0\}|$.

Theorem 2 [10] *Suppose that C is an additive code over $\mathbb{F}_q$ of length $2n$ such that $|C| = q^{n-k}$, $C \subseteq C^{\perp_s}$ and $w_s\left(C^{\perp_s} - C\right) = d$. Then, there exists a $[[n, k, d]]_q$ quantum error correcting code.*

Theorem 2 says that it is necessary to find an additive code over $\mathbb{F}_q$ containing its trace-symplectic dual to construct a quantum code.

For an $[[n, k, d]]_q$ quantum code, the relation $n + 2 \geq k + 2d$, called quantum Singleton bound, is an analog to the Singleton bound for classical linear codes over finite fields [11,15]. An $[[n, k, d]]_q$ quantum code is called a quantum MDS(QMDS) code if it holds the Singleton bound for quantum codes.

Let p be a prime such that $p = a^2 + b^2$ for some positive integers a and b and let $\mathbb{F}_q$ be a finite field having q elements, where q is a positive power of p. We denote R_q

to be $R_q=\mathbb{F}_q+\alpha\mathbb{F}_q$, where $\alpha=a+bi$. Then, R_q is a nonlocal commutative ring with identity and its nontrivial ideals are $\langle\alpha\rangle$ and $\langle\alpha^*\rangle$, where $\alpha^*=a-bi$. It is easily seen that $R_q=\langle\alpha\rangle\oplus\langle\alpha^*\rangle$ and $|\langle\alpha\rangle|=|\langle\alpha^*\rangle|=q$. Thus, since $\langle\alpha\rangle=\{k\alpha:k\in\mathbb{F}_q\}$ and $\langle\alpha^*\rangle=\{k\alpha^*:k\in\mathbb{F}_q\}$, every element r of the ring R_q is written uniquely as

$$k_1\alpha+k_2\alpha^* \tag{4}$$

for some $k_1,k_2\in\mathbb{F}_q$.

A code C of length n over R_q is a nonempty subset of R_q^n. A linear code C of length n over R_q is a submodule of R_q-module R_q^n. Any linear code over R_q is a permutation-equivalent to a code having the following generator matrix:

$$G_{(k_1+k_2+k_3)\times n}=\begin{pmatrix} I_{k_1} & \alpha^*B_1 & \alpha A_1 & \alpha A_1+\alpha^*B_2 & \alpha A_3+\alpha^*B_3 \\ 0 & \alpha I_{k_2} & 0 & \alpha A_4 & 0 \\ 0 & 0 & \alpha^* I_{k_3} & 0 & \alpha^*B_4 \end{pmatrix}, \tag{5}$$

where I_{k_i} is a $k_i\times k_i$ identity matrix and the matrices A_i and B_i are over $\mathbb{F}_q$. Note that for a code C with the generator matrix $G_{(k_1+k_2+k_3)\times n}$, the size $|C|$ of C is equal to $q^{2k_1+k_2+k_3}$.

For an element $r=x+y\alpha$ in R, $r^*=x+y\alpha^*$. Let $x=(x_0,x_1,\ldots,x_{n-1})$ and $y=(y_0,y_1,\ldots,y_{n-1})$ be two vectors in R_q^n. Define Hermitian inner product $\langle x,y\rangle_h$ of the vectors x and y as $\langle x,y\rangle_h:=x_0y_0^*+x_1y_1^*+\cdots+x_{n-1}y_{n-1}^*$. Hermitian dual $C^{\perp_h}$ of a code C over R_q of length n is the set

$$C^{\perp_h}=\{y\in R_q^n:\langle x,y\rangle_h=0,\ \forall x\in C\}. \tag{6}$$

Note that $C^{\perp_h}$ is also linear if C is linear, and $|C||C^{\perp_h}|=|R_q^n|$. A code C is called Hermitian self-orthogonal code if $C\subseteq C^{\perp_h}$.

3 A gray map from R_q^n to $\mathbb{F}_q^{2n}$

We define the Gray map $\varphi:R_q^n\to\mathbb{F}_q^{2n}$ as

$$\varphi(r_0,r_1,\ldots,r_{n-1})=(-y_0b,\ldots,-y_{n-1}b,x_0+y_0a,\ldots,x_{n-1}+y_{n-1}a), \tag{7}$$

where $r_i=x_i+y_i\alpha$ for all $i\in\{0,1,\ldots,n-1\}$.

The Lee weight $w_L(r)$ of an element $r\in R_q$ is $w_H(\varphi(r))$. The Lee weight $w_L(x)$ of a vector $x=(x_0,x_1,\ldots,x_{n-1})\in R_q^n$ is $w_L(x)=\sum_{i=0}^{n-1}w_L(x_i)$. The Lee distance $d_L(x,y)$ between two vectors x and y in R_q^n is defined to be $d_L(x,y)=w_L(x-y)$. The following theorem is direct.

Theorem 3 *The Gray map φ is an $\mathbb{F}_q$-linear and distance-preserving map from (R_q^n,d_L) to $(\mathbb{F}_q^{2n},d_H)$.*

For two elements $r_1 = x_1 + y_1\alpha$ and $r_2 = x_2 + y_2\alpha$ of the ring R_q, suppose that $r_1 \perp_h r_2$. This implies that

$$x_1x_2 + (x_1y_2 + x_2y_1)\,a = 0 \tag{8}$$

and

$$(x_2y_1 - x_1y_2)\,b = 0 \tag{9}$$

We have the following theorem:

Theorem 4 *Let C be a code of length n over R_q. If C contains its Hermitian dual, $\psi(C)$ contains its dual with respect to both usual inner product and trace-symplectic inner product.*

Proof It is sufficient to prove only for $n = 1$. Assume that $r_1 \perp_h r_2$. See that

$$\begin{aligned}\langle \psi(r_1), \psi(r_2) \rangle &= y_1y_2b^2 + (x_1y_2 + x_2y_1)\,a + x_1x_2 + y_1y_2a^2 \\ &= (x_1y_2 + x_2y_1)\,a + x_1x_2.\end{aligned}$$

Equation 8 implies that $\langle \psi(r_1), \psi(r_2) \rangle = 0$. For the second,

$$\begin{aligned}\langle \psi(r_1), \psi(r_2) \rangle_s &= \operatorname{tr}\left(-(x_1 + y_1a)\,y_2b + (x_2 + y_2a)\,y_1b\right) \\ &= \operatorname{tr}\left((x_2y_1 - x_1y_2)\,b\right).\end{aligned}$$

By Equation 9, $\operatorname{tr}((x_2y_1 - x_1y_2)\,b) = 0$ and so proof is completed. □

Combining Theorems 1, 3 and 4, we give:

Corollary 1 *If C is a linear code over R_q having the generator matrix $G_{(k_1+k_2+k_3)\times n}$ and containing its Hermitian dual, then there exists an $[[2n, 2(2k_1 + k_2 + k_3 - n), d \geq d_L]]_q$ quantum error correcting code, where d_L is the minimum Lee distance of the code C.*

It is worth to note that for a vector $x \in R_q^n$, $w_H(x) = w_s(\varphi(x))$ and so the (minimum) Hamming weight of the nonzero codewords in a code C over R_q is equal to the minimum symplectic weight of the nonzero codewords in $\varphi(C)$. We also have the following from Theorems 1 and 4.

Corollary 2 *If C is a linear code over R_q having the generator matrix $G_{(k_1+k_2+k_3)\times n}$ and containing its Hermitian dual, then there exists a $[[n, 2k_1 + k_2 + k_3 - n, d \geq d_H]]_q$ quantum error correcting code, where d_H is the minimum Hamming distance of the code C.*

4 Quantum codes from cyclic codes over R_q

A linear code C over $\mathbb{F}_q$(resp. R_q) is called cyclic if its right cyclic shift of every codeword is also a codeword. Recall that there is a one-to-one correspondence between cyclic codes of length n over $\mathbb{F}_q$ and the ideals of the quotient ring $\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$. Since every ideal of $\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$ is principal, $C=\langle g(x)\rangle$ for some monic polynomial $g(x)\in\frac{F_q[x]}{\langle x^n-1\rangle}$, where $g(x)$ is called generator polynomial of C and divides x^n-1. Similar to the case over $\mathbb{F}_q$, a cyclic code over R_q of length n is an ideal in $\frac{R_q[x]}{\langle x^n-1\rangle}$. Hence, we need to investigate the ideal structure of $\frac{R_q[x]}{\langle x^n-1\rangle}$.

Equation 4 implies that for every vector $x\in R_q^n$, there exits uniquely vectors $x_1,x_2\in\mathbb{F}_q^n$ such that $x=\alpha x_1+\alpha^* x_2$. This leads to a characterization of linear and cyclic codes of length n over R_q.

Theorem 5 *A linear code C over R_q of length n is of the form $C=\alpha C_1\oplus\alpha^*C_2$, where C_1 and C_2 are linear codes over $\mathbb{F}_q$ of length n. If the code C is a cyclic code, then C_1 and C_2 are cyclic codes over $\mathbb{F}_q$.*

We now are ready to give exact characterization for cyclic codes over R_q.

Theorem 6 *Every cyclic code C over R_q of length n has the form $C=\langle\alpha g_1(x)+\alpha^* g_2(x)\rangle$ for some polynomials $g_1(x)$ and $g_2(x)$ in $\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$ which divide x^n-1. Moreover, $|C|=q^{2n-\sum_{i=1}^{2}\deg g_i(x)}$.*

Proof By Theorem 5, $C=\alpha C_1+\alpha^*C_2$ for some cyclic codes $C_1=\langle g_1(x)\rangle$ and $C_2=\langle g_2(x)\rangle$ of length n, where $g_i(x)$ divides x^n-1 for $i=1,2$. Then, $C=\langle\alpha g_1(x),\alpha^* g_2(x)\rangle$. Set $J=\langle\alpha g_1(x)+\alpha^* g_2(x)\rangle$. Clearly, $J\subseteq C$. For reverse inclusion, see that $\alpha^2=2a\alpha$ and $(\alpha^*)^2=2a\alpha^*$. This implies that $\alpha(\alpha g_1(x)+\alpha^* g_2(x))=\alpha^2 g_1(x)=2a\alpha g_1(x)\in J$ and $\alpha^*(\alpha g_1(x)+\alpha^* g_2(x))=(\alpha^*)^2 g_2(x)=2a\alpha^* g_2(x)\in J$. Hence, $\alpha g_1(x)$ and $\alpha^* g_2(x)$ are included in J and $J=C$. The size of C is clear. □

To construct quantum error correcting codes via cyclic codes over R_q, we need the condition that cyclic codes over R_q contain their Hermitian dual. We begin to determine the structure of Hermitian dual code of a cyclic code over R_q. Note that $h(x)=\frac{x^n-1}{g(x)}$ is called check polynomial of a cyclic code $C=\langle g(x)\rangle$ over $\mathbb{F}_q$ of length n and $h^R(x)=x^{\deg h(x)}h(x^{-1})$.

Theorem 7 *Suppose $C=\alpha C_1\oplus\alpha^*C_2$ is a cyclic code over R_q of length n. Then, $C^{\perp_h}=\langle\alpha h_2^R(x)+\alpha^* h_1^R(x)\rangle$, where $h_1(x)$ and $h_2(x)$ are check polynomials of C_1 and C_2, respectively.*

Proof Set $J=\langle\alpha h_2^R(x)+\alpha^* h_1^R(x)\rangle$. Let $C_i=\langle g_i(x)\rangle$ for $i=1,2$. Since $C=\langle\alpha g_1(x)+\alpha^* g_2(x)\rangle$, the definition of Hermitian inner product forces that proving the following equality is necessary.

$$\begin{aligned}&\left(\alpha g_1(x)+\alpha^* g_2(x)\right)\left(\alpha h_2(x)+\alpha^* h_1(x)\right)^*\\&\quad=\left(\alpha g_1(x)+\alpha^* g_2(x)\right)\left(\alpha h_1(x)+\alpha^* h_2(x)\right)\\&\quad=\alpha^2 g_1(x)h_1(x)+\alpha\alpha^*\left(g_1(x)h_2(x)+g_2(x)h_1(x)\right)+\left(\alpha^*\right)^2 g_2(x)h_2(x)=0\end{aligned}$$

Hence, $(\alpha h_2(x)+\alpha^* h_1(x))^R=\alpha h_2^R(x)+\alpha^* h_1^R(x)\in C^{\perp_h}$ and $J\subseteq C^{\perp_h}$. Since $|J||C|=|R_q^{2n}|$, $J=C^{\perp_h}$. □

Note that $x^n - 1$ has no multiple roots over $\mathbb{F}_q$ if $(n, q) = 1$. Then, there exists an n^{th} root β of unity in some field extension of $\mathbb{F}_q$. This fact enables to describe a cyclic code of length n and generator polynomial $g(x)$ with respect to its defining set $Z = \{i : g(\beta^i) = 0,\ i \in \{0, 1, \dots, n-1\}\}$. Denote $Z^{-1} = \{-i \bmod n : i \in Z\}$. Recall that the defining set of $g^R(x)$ is Z^{-1} if the defining set of $g(x)$ is Z. In the following theorem, equivalent conditions for a cyclic code over R_q to contain its Hermitian dual are derived.

Theorem 8 *Let $(n, q) = 1$. Let C_i be a cyclic code of length n and generator polynomial $g_i(x)$ over $\mathbb{F}_q$ and let Z_i be defining set of C_i for $i = 1, 2$. Suppose that $C = \alpha C_1 + \alpha^* C_2$. The following are equivalent:*

1. $C^{\perp_h} \subseteq C$,
2. $C_2^{\perp} \subseteq C_1$,
3. $C_1^{\perp} \subseteq C_2$,
4. $x^n - 1 \equiv 0 \left(\bmod g_1(x)\, g_2^R(x)\right)$,
5. $x^n - 1 \equiv 0 \left(\bmod g_1^R(x)\, g_2(x)\right)$,
6. $Z_1 \cap Z_2^{-1} = \emptyset$,
7. $Z_1^{-1} \cap Z_2 = \emptyset$.

Proof It is easy to see that the conditions (2), (3), (4), (5), (6) and (7) are equivalent from definitions and so it is enough to prove (1)⇔(4). Since $C = \alpha C_1 + \alpha^* C_2$, Theorem 7 implies that $C^{\perp_h} = \alpha C_2^{\perp} \oplus \alpha^* C_1^{\perp}$. So, if $C^{\perp_h} \subseteq C$, then $C_2^{\perp} \subseteq C_1$ and $C_1^{\perp} \subseteq C_2$. Thus, $g_1(x) | h_2^R(x)$ and $g_2(x) | h_1^R(x)$. Say $h_2^R(x) = g_1(x) f(x)$. Since $g_2^R(x)\, h_2^R(x) = -(x^n - 1)$, we get $g_2^R(x)\, g_1(x)\, f(x) = -(x^n - 1)$.

For the other side, if $x^n - 1 \equiv 0 \bmod (g_1(x) g_2^R(x))$, then $g_2^R(x) \big| h_1(x)$ and so $g_2(x) | h_1^R(x)$. This means that $C_1^{\perp} \subseteq C_2$ and $C_2^{\perp} \subseteq C_1$, which completes the proof. □

The following is immediate from Theorem 8.

Corollary 3 *Let C be a cyclic code over $\mathbb{F}_q$ containing its dual and let $C' = \alpha C \oplus \alpha^* C$. Then, C' is a cyclic code over R_q containing its Hermitian dual.*

Corollary 1 is rearranged for cyclic codes containing its Hermitian dual as follows:

Corollary 4 *Let $C = \alpha C_1 \oplus \alpha^* C_2 = \langle \alpha g_1(x) + \alpha^* g_2(x) \rangle$ be a cyclic code over R_q of length n and $(n, q) = 1$. If one of the conditions given in Theorem 8 is satisfied, then there exists a $[\![2n, 2(n - \sum_{i=1}^{2} deg(g_i(x))), d \geq d_L]\!]_q$ quantum error correcting code, where d_L is the minimum Lee weight of the cyclic code C and $g_i(x)$ is generator polynomial of C_i.*

Furthermore, Corollary 2 is rearranged for cyclic codes containing its Hermitian dual as follows:

Corollary 5 *Let $C = \alpha C_1 \oplus \alpha^* C_2 = \langle \alpha g_1(x) + \alpha^* g_2(x) \rangle$ be a cyclic code over R_q of length n and $(n, q) = 1$. If one of the conditions given in Theorem 8 is satisfied, then there exists a $[\![n, n - \sum_{i=1}^{2} deg(g_i(x)), d \geq d_H]\!]_q$ quantum error correcting code, where d_H is the minimum Hamming weight of the cyclic code C and $g_i(x)$ is generator polynomial of C_i.*

Table 1 All nontrivial cyclic codes over R_5 of length 9 containing its Hermitian dual and QECC1 and QECC2 obtained by Corollaries 4 and 5 (respectively) in Example 1

$g_1(x)$	$g_2(x)$	Gray image	QECC1	QECC2
f_2	f_3	$[18, 10, 4]_5$	$[[18, 2, 4]]_5$	$[[9, 1, \geq 2]]_5$
f_2	f_1	$[18, 11, 4]_5$	$[[18, 4, 4]]_5$	$[[9, 2, \geq 2]]_5$
f_2	$f_1 f_3$	$[18, 9, 4]_5$	$[[18, 0, 4]]_5$	$[[9, 0, \geq 2]]_5$
f_3	f_2	$[18, 10, 4]_5$	$[[18, 2, 4]]_5$	$[[9, 1, \geq 2]]_5$
f_3	f_1	$[18, 15, 2]_5$	$[[18, 12, 2]]_5$	$[[9, 6, \geq 2]]_5^*$
f_3	$f_1 f_2$	$[18, 9, 4]_5$	$[[18, 0, 4]]_5$	$[[9, 0, \geq 2]]_5$
$f_2 f_3$	f_1	$[18, 9, 4]_5$	$[[18, 0, 4]]_5$	$[[9, 0, \geq 2]]_5$
f_1	f_2	$[18, 11, 4]_5$	$[[18, 4, 4]]_5$	$[[9, 2, \geq 2]]_5$
f_1	f_3	$[18, 15, 2]_5$	$[[18, 12, 2]]_5$	$[[9, 6, \geq 2]]_5^*$
f_1	$f_2 f_3$	$[18, 9, 4]_5$	$[[18, 0, 4]]_5$	$[[9, 0, \geq 2]]_5$
$f_1 f_2$	f_3	$[18, 9, 4]_5$	$[[18, 0, 4]]_5$	$[[9, 0, \geq 2]]_5$
$f_1 f_3$	f_2	$[18, 9, 4]_5$	$[[18, 0, 4]]_5$	$[[9, 0, \geq 2]]_5$
1	f_1	$[18, 17, 2]_5$	$[[18, 16, 2]]_5^*$	$[[9, 8, \geq 1]]_5^*$
1	f_2	$[18, 12, 2]_5$	$[[18, 6, 2]]_5$	$[[9, 3, \geq 1]]_5$
1	f_3	$[18, 16, 2]_5$	$[[18, 14, 2]]_5$	$[[9, 7, \geq 1]]_5$
1	$f_1 f_2$	$[18, 11, 2]_5$	$[[18, 4, 2]]_5$	$[[9, 2, \geq 1]]_5$
1	$f_1 f_3$	$[18, 15, 2]_5$	$[[18, 12, 2]]_5$	$[[9, 6, \geq 1]]_5$
1	$f_2 f_3$	$[18, 10, 2]_5$	$[[18, 2, 2]]_5$	$[[9, 1, \geq 1]]_5$
f_1	1	$[18, 17, 2]_5$	$[[18, 16, 2]]_5^*$	$[[9, 8, \geq 1]]_5^*$
f_2	1	$[18, 12, 2]_5$	$[[18, 6, 2]]_5$	$[[9, 3, \geq 1]]_5$
f_3	1	$[18, 16, 2]_5$	$[[18, 14, 2]]_5$	$[[9, 7, \geq 1]]_5$
$f_1 f_2$	1	$[18, 11, 2]_5$	$[[18, 4, 2]]_5$	$[[9, 2, \geq 1]]_5$
$f_1 f_3$	1	$[18, 15, 2]_5$	$[[18, 12, 2]]_5$	$[[9, 6, \geq 1]]_5$
$f_2 f_3$	1	$[18, 10, 2]_5$	$[[18, 2, 2]]_5$	$[[9, 1, \geq 1]]_5$

Example 1 Let $x^9 - 1 = f_1 f_2 f_3$ over $\mathbb{F}_5$, where $f_1 = x + 4$, $f_2 = 1 + x^3 + x^6$ and $f_3 = 1 + x + x^2$. All nontrivial cyclic codes over R_5 of length 9 containing its Hermitian dual and quantum error correcting codes(QECC) obtained by Corollaries 4 and 5 are represented in Table 1.

Example 2 Let $x^{11} - 1 = f_1 f_2 f_3$ over $\mathbb{F}_5$, where $f_1 = x + 4$, $f_2 = 4 + x + x^2 + 4x^3 + 2x^4 + x^5$ and $f_3 = 4 + 3x + x^2 + 4x^3 + 4x^4 + x^5$. All nontrivial cyclic codes over R_5 of length 11 containing its Hermitian dual and quantum error correcting codes(QECC) obtained by Corollaries 4 and 5 are represented in Table 2.

Remark 1 The quantum codes having the parameters marked with "*" in Tables 1 and 2 are QMDS codes.

Table 2 All nontrivial cyclic codes over R_5 of length 11 containing its Hermitian dual and QECC1 and QECC2 obtained by Corollaries 4 and 5 (respectively) in Example 2

$g_1(x)$	$g_2(x)$	Gray image	QECC1	QECC2
f_3	f_3	$[22, 12, 5]_5$	$[[22, 2, 5]]_5$	$[[11, 1, \geq 5]]_5$
f_3	f_1	$[22, 16, 4]_5$	$[[22, 10, 4]]_5$	$[[11, 5, \geq 2]]_5$
f_3	$f_1 f_3$	$[22, 11, 6]_5$	$[[22, 0, 6]]_5$	$[[11, 0, \geq 5]]_5$
f_2	f_2	$[22, 12, 5]_5$	$[[22, 2, 5]]_5$	$[[11, 1, \geq 5]]_5$
f_2	f_1	$[22, 16, 4]_5$	$[[22, 10, 4]]_5$	$[[11, 5, \geq 2]]_5$
f_2	$f_1 f_2$	$[22, 11, 6]_5$	$[[22, 0, 6]]_5$	$[[11, 0, \geq 5]]_5$
$f_2 f_3$	f_1	$[22, 11, 4]_5$	$[[22, 0, 4]]_5$	$[[11, 0, \geq 2]]_5$
f_1	f_3	$[22, 16, 4]_5$	$[[22, 10, 4]]_5$	$[[11, 5, \geq 2]]_5$
f_1	f_2	$[22, 16, 4]_5$	$[[22, 10, 4]]_5$	$[[11, 5, \geq 2]]_5$
f_1	$f_2 f_3$	$[22, 11, 4]_5$	$[[22, 0, 4]]_5$	$[[11, 0, \geq 2]]_5$
$f_1 f_3$	f_3	$[22, 11, 6]_5$	$[[22, 0, 6]]_5$	$[[11, 0, \geq 5]]_5$
$f_1 f_2$	f_2	$[22, 11, 6]_5$	$[[22, 0, 6]]_5$	$[[11, 0, \geq 5]]_5$
1	f_1	$[22, 21, 2]_5$	$[[22, 20, 2]]_5^*$	$[[11, 10, \geq 1]]_5^*$
1	f_2	$[22, 17, 2]_5$	$[[22, 12, 2]]_5$	$[[11, 6, \geq 1]]_5$
1	f_3	$[22, 17, 2]_5$	$[[22, 12, 2]]_5$	$[[11, 6, \geq 1]]_5$
1	$f_1 f_2$	$[22, 16, 2]_5$	$[[22, 10, 2]]_5$	$[[11, 5, \geq 1]]_5$
1	$f_1 f_3$	$[22, 16, 2]_5$	$[[22, 10, 2]]_5$	$[[11, 5, \geq 1]]_5$
1	$f_2 f_3$	$[22, 12, 2]_5$	$[[22, 2, 2]]_5$	$[[11, 1, \geq 1]]_5$
f_1	1	$[22, 21, 2]_5$	$[[22, 20, 2]]_5^*$	$[[11, 10, \geq 1]]_5^*$
f_2	1	$[22, 17, 2]_5$	$[[22, 12, 2]]_5$	$[[11, 6, \geq 1]]_5$
f_3	1	$[22, 17, 2]_5$	$[[22, 12, 2]]_5$	$[[11, 6, \geq 1]]_5$
$f_1 f_2$	1	$[22, 16, 2]_5$	$[[22, 10, 2]]_5$	$[[11, 5, \geq 1]]_5$
$f_1 f_3$	1	$[22, 16, 2]_5$	$[[22, 10, 2]]_5$	$[[11, 5, \geq 1]]_5$
$f_2 f_3$	1	$[22, 12, 2]_5$	$[[22, 2, 2]]_5$	$[[11, 1, \geq 1]]_5$

5 Quantum codes from additive cyclic codes over R_q

This section is devoted to obtaining quantum error correcting codes via additive cyclic codes over R_q for $q = p^2$. An additive cyclic code C over R_q means that C is closed under addition and cyclic shift of a codeword in C is again a codeword in C. In other words, an additive cyclic code of length n over R_q is an additive subgroup in the quotient group $\frac{R_q[x]}{\langle x^n - 1\rangle}$ which is closed under multiplication by x. Making use of technique used in Theorem 14 in [4], we first characterize the structure of additive cyclic codes over R_q for $q = p^2$ and then study self-orthogonality condition for these codes which are needed to construct quantum error correcting codes.

Lemma 1 *Let $q = p^2$ be for a prime p and the set $\{1, w\}$ be a polynomial basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. An additive cyclic code over $\mathbb{F}_q$ of length n is of the form $\langle g(x) + wp(x), wa(x)\rangle$ for some polynomials $g(x), p(x), a(x) \in \mathbb{F}_p[x]$. Furthermore, $g(x)$ and $a(x)$ divide $x^n - 1 \pmod{p}$ and $|C| = p^{2n - \deg g(x) - \deg a(x)}$.*

Proof Consider the map $\phi : \mathbb{F}_q \to \mathbb{F}_p$ mapping an element $a+bw$ to a and extend it to the map $\mu : \frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle} \to \frac{\mathbb{F}_p[x]}{\langle x^n-1\rangle}$, $\sum c_i x^i \to \sum \phi(c_i)\, x^i$. Then, μ is an onto $\mathbb{F}_p[x]$-module homomorphism. If C is an additive cyclic code over $\mathbb{F}_q$, then the image of C under μ is an ideal in $\frac{F_p[x]}{\langle x^n-1\rangle}$ and so has a generator $g(x)$ dividing $x^n-1 \pmod p$. Define the set $J = \left\{a(x) \in \frac{F_p[x]}{\langle x^n-1\rangle} : wa(x) \in Ker\mu\right\}$. It is immediate that J is an ideal in $\frac{F_p[x]}{\langle x^n-1\rangle}$ and so $Ker\mu = \langle a(x)\rangle$ for some polynomial $a(x) | x^n - 1 \pmod p$. Since C is generated by the polynomials $a(x)$ and some inverse of $g(x)$, $C = \langle g(x) + wp(x), wa(x)\rangle$ for some polynomial $p(x) \in \mathbb{F}_p[x]$. The remaining is clear. □

The following theorem characterizes the structure of additive cyclic codes over R_{p^2}. The proof is similar to the proofs of Theorems 6 and 7, so we omit it here.

Theorem 9 *An additive cyclic code C over R_{p^2} of length n is of the form $C = \alpha C_1 \oplus \alpha^* C_2$ for some additive cyclic codes C_1 and C_2 of length n over $\mathbb{F}_q$. Hence,*

$$C = \left\langle \alpha\left(g_1(x) + wp_1(x)\right), \alpha w a_1(x), \alpha^*\left(g_2(x) + wp_2(x)\right), \alpha^* w a_2(x)\right\rangle, \quad (10)$$

where $g_i(x), a_i(x) | x^n - 1 \pmod p$.

Next theorem investigates the duals of additive cyclic codes over R_{p^2} and gives a condition for additive cyclic codes which are Hermitian self-orthogonal.

Theorem 10 *Let $C = \alpha C_1 \oplus \alpha^* C_2$ be an additive cyclic code over R_{p^2} of length n. Then, $C^{\perp_h} = \alpha C_2^{\perp} \oplus \alpha^* C_1^{\perp}$. Moreover, C is Hermitian self-orthogonal with respect to Hermitian dual if and only if $C_1 \subseteq C_2^{\perp}$.*

Proof Set $J = \alpha C_2^{\perp} \oplus \alpha^* C_1^{\perp}$. It is easy to check that $J \subseteq C^{\perp_h}$. Since $|J||C| = |R_{p^2}^n|$, $J = C^{\perp_h}$. The second part is immediate. □

Letting $C_i = \langle g_i(x) + wp_i(x), wa_i(x)\rangle$ for $i \in \{1,2\}$ be an additive cyclic code over $\mathbb{F}_{p^2}$, we seek the circumstance for $C_1 \subseteq C_2^{\perp}$.

Lemma 2 *$C_1 \subseteq C_2^{\perp}$ if and only if the following hold:*

1. $g_1(x)\, g_2\left(x^{n-1}\right) + bp_1(x)\, p_2\left(x^{n-1}\right) \equiv 0 \pmod{x^n - 1}$,
2. $g_1(x)\, p_2\left(x^{n-1}\right) + p_1(x)\, g_2\left(x^{n-1}\right) \equiv 0 \pmod{x^n - 1}$,
3. $g_1(x)\, a_2\left(x^{n-1}\right) \equiv 0 \pmod{x^n - 1}$,
4. $p_1(x)\, a_2\left(x^{n-1}\right) \equiv 0 \pmod{x^n - 1}$,
5. $a_1(x)\, g_2\left(x^{n-1}\right) \equiv 0 \pmod{x^n - 1}$,
6. $a_1(x)\, p_2\left(x^{n-1}\right) \equiv 0 \pmod{x^n - 1}$,
7. $a_1(x)\, a_2\left(x^{n-1}\right) \equiv 0 \pmod{x^n - 1}$,

where b is a nonresidue mod p.

Proof Note that $x^2 - b$ is an irreducible polynomial over $\mathbb{F}_p$ if b is a nonresidue mod p. So we can assume that $w^2 = b$. See that the inner product of the vectors corresponding to the polynomials $g_1(x) + wp_1(x)$ and $x^j(g_2(x) + wp_2(x))$ for $j \in \{0, 1, \ldots, n-1\}$ are the coefficient of x^j in the polynomial $(g_1(x) + wp_1(x))x^j (g_2(x^{n-1}) + wp_2(x^{n-1}))$. This fact implies that 1 and 2 hold. The proofs of the remaining are similar. □

By considering the images of additive cyclic codes over R_{p^2} under the Gray map φ , one fails to get p-ary quantum error correcting codes since φ carries elements of R_{p^2} to vectors in $\mathbb{F}^2_{p^2}$. We therefore need a new map to obtain p-ary quantum error correcting codes by using Theorem 2. Let $\{1, w\}$ be a polynomial basis of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$. Note that every element $x \in \mathbb{F}_{p^2}$ can be written uniquely as $x = x_1 + wx_2$ for some $x_1, x_2 \in \mathbb{F}_p$. Define the map $\sigma : R_{p^2} \to \mathbb{F}_p^4$ as

$$\sigma(x + y\alpha) = (y_2, y_1 + y_2, x_2 + y_2, x_1 + x_2 + y_1 + y_2) \tag{11}$$

and extend it to the map $\delta : R^n_{p^2} \to \mathbb{F}_p^{4n}$ as

$$\begin{aligned}&(r_0, \ldots, r_{n-1})\\ &\quad \to (y_{0,2}, y_{0,1} + y_{0,2}, \ldots, y_{n-1,2}, y_{n-1,1} + y_{0,2}, x_{0,2} + y_{0,2}, x_{0,1} + x_{0,2}\\ &\qquad + y_{0,1} + y_{0,2}, \ldots, x_{n-1,2} + y_{n-1,2}, x_{n-1,1} + x_{n-1,2} + y_{n-1,1} + y_{n-1,2}),\end{aligned}$$

where $r_i = x_{i,1} + x_{i,2} + (y_{i,1} + y_{i,2})w$ for some $x_{i,1}, x_{i,2}, y_{i,1} y_{i,2} \in \mathbb{F}_p$. Before stating that the δ-images of two vectors over R_{p^2} which are perpendicular to each other with respect to Hermitian inner product are so with respect to trace-symplectic inner product, we note that if $r_1 \perp_h r_2$ for two elements $r_1 = x + y\alpha$ and $r_2 = u + v\alpha$ in R_{p^2}, by Eq. 9, we further get

$$y_1u_2 + y_2u_1 - (x_1v_2 + x_2v_1) = 0 \tag{12}$$

and

$$y_1u_1 - x_1v_1 + w^2(y_2u_2 - x_2v_2) = 0. \tag{13}$$

In this case, we also observe that

$$\begin{aligned}\langle \delta(r_1), \delta(r_2)\rangle_s &= \operatorname{tr}(x_1v_2 + x_2v_1 - (y_1u_2 + y_2u_1))\\ &\quad + \operatorname{tr}(x_1v_1 - y_1u_1 + 2(x_2v_2 - y_2u_2))\end{aligned}$$

and Eq. 12 implies that

$$\langle \delta(r_1), \delta(r_2)\rangle_s = \operatorname{tr}(x_1v_1 - y_1u_1 + 2(x_2v_2 - y_2u_2)). \tag{14}$$

Then, $\langle \delta(r_1), \delta(r_2)\rangle_s$ vanishes by Eq. 13 if $w^2 \equiv 2 \pmod p$. This is possible only when 2 is a nonresidue mod p, otherwise the polynomial $x^2 - 2$ is reducible over $\mathbb{F}_p$ and so the set $\{1, w\}$ does not form a basis for $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$. We hence have:

Table 3 Some nontrivial additive cyclic codes over R_{25} of length 11 which are Hermitian self-orthogonal and some QECC over $\mathbb{F}_5$ of length 22 obtained by Corollary 6 in Example 3

$g_1(x)$	$p_1(x)$	$a_1(x)$	$g_2(x)$	$p_2(x)$	$a_2(x)$	QECC
0	0	$f_1 f_2$	f_2	f_2	$f_2 f_3$	$[[22, 10, 2]]_5$
0	0	$f_1 f_2$	f_2	f_2	$f_1 f_2$	$[[22, 6, 2]]_5$
0	0	$f_1 f_2$	f_2	$f_2 f_3$	0	$[[22, 16, 1]]_5$
$f_1 f_2$	0	0	$f_2 f_3$	0	f_2	$[[22, 10, 1]]_5$
$f_1 f_2$	0	0	0	0	$f_2 f_3$	$[[22, 16, 1]]_5$
$f_1 f_2$	$f_1 f_2$	0	0	0	0	$[[22, 17, 1]]_5$
f_1	$f_1 f_2$	f_1	$f_2 f_3$	$f_2 f_3$	0	$[[22, 6, 2]]_5$
f_1	f_1	$f_1 f_2$	$f_2 f_3$	0	$f_2 f_3$	$[[22, 5, 2]]_5$
f_1	1	$f_1 f_2$	0	0	0	$[[22, 7, 1]]_5$

Theorem 11 *Let p be an odd prime which can be written $a^2 + b^2$ for some $a, b \in \mathbb{Z}$ and $p \equiv 3\,or\,5 \pmod 8$. Suppose that $\{1, w\}$ is a polynomial basis of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, where $w^2 = 2$. If C is an additive code over R_{p^2} containing its Hermitian dual, then $\delta(C)$ is a linear code over $\mathbb{F}_p$ containing its trace-symplectic dual.*

Proof Since $p \equiv 3\,or\,5 \pmod 8$, 2 is a nonresidue $\bmod\, p$ and so the polynomial $x^2 - 2$ is irreducible over $\mathbb{F}_p$. By the above observation and Eq. 13, proof is over. □

Theorems 2 and 11 together imply:

Corollary 6 *Let p be an odd prime which can be written $a^2 + b^2$ for some $a, b \in \mathbb{Z}$ and $p \equiv 3\,or\,5 \pmod 8$. Suppose that $\{1, w\}$ is a polynomial basis of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, where $w^2 = 2$. Let $C = \alpha C_1 \oplus \alpha^* C_2$ be a cyclic code over R_{p^2} of length n, where for $i = 1, 2$, $C_i = \langle g_i(x) + w p_i(x), a_i(x) \rangle$. If the conditions given in Lemma 2 are satisfied, then there exists a $[[2n, 2n - k, d]]_p$ quantum error correcting code, where $k = \sum_{i=1}^{2} \deg g_i + \deg a_i$ and d is the minimum symplectic weight in $\delta(C)^{\perp_s} - \delta(C)$.*

Example 3 Let $x^{11} - 1 = f_1 f_2 f_3$ over $\mathbb{F}_5$, where $f_1 = x + 4$, $f_2 = 4 + x + x^2 + 4x^3 + 2x^4 + x^5$ and $f_3 = 4 + 3x + x^2 + 4x^3 + 4x^4 + x^5$. Table 3 illustrates what we discuss in this section by giving some examples of quantum error correcting codes over F_5 obtained by Hermitian self-orthogonal additive cyclic codes over R_{25} of length 11.

Example 4 Let $q = 29$, $\alpha = 5 + 2i$ and $x^{31} - 1 = f_1 f_2 f_3 f_4$. With help of MAGMA and under the conditions of Theorem 8, some nontrivial quantum code parameters of length 31 over R_{29} are given in Table 4.

Example 5 Let $q = 13$, $\alpha = 3 + 2i$. Satisfying the conditions given in Corollary 4 and using the software programme Mathematica, we obtain a $[[8, 0, 4]]_{13}$ quantum code from a classical code C over R_{13}. Also, this classical code C is an extremal self-dual code over R_{13}. The generator matrix G of the classical code C is

Table 4 Some nontrivial quantum codes over R_{29} of length 31 which are Hermitian self-orthogonal and some QECC over $\mathbb{F}_{29}$ of length 62 obtained by Theorem 8 in Example 4

$g_1(x)$	$g_2(x)$	QECC1	QECC2
$f_1 f_2$	f_3	$[[62, 20, \geq 8]]_{29}$	$[[31, 10, 8]]_{5+2i}$
$f_2 f_3$	f_4	$[[62, 2, \geq 8]]_{29}$	$[[31, 1, 8]]_{5+2i}$
$f_2 f_3$	$f_1 f_4$	$[[62, 0, \geq 9]]_{29}$	$[[31, 0, 9]]_{5+2i}$

Table 5 Using the software programme Mathematica and the method given in this paper, some new quantum codes with respect to the Mannheim metric over R_{13} of length 5, 6, 8 are given

The generator matrix G	QECC
$G = \begin{pmatrix} 1 & 0 & 9\alpha & 6\alpha & 9+11\alpha \end{pmatrix}$	$[[5, 3, 10]]_{3+2i}$
$G = \begin{pmatrix} 1 & 0 & 9\alpha & 6\alpha & 9+11\alpha \\ 5\alpha & 1 & 5+10\alpha & 11\alpha & 12+9\alpha \\ 12\alpha & 8+3\alpha & 1 & 11\alpha & 5 \end{pmatrix}$	$[[5, 1, 15]]_{3+2i}$
$G = \begin{pmatrix} 1 & 0 & 3+6\alpha & 3+6\alpha & 5+10\alpha & 4+6\alpha \\ 0 & 1 & 6+12\alpha & 7+\alpha & 2\alpha & 1+3\alpha \\ 9+5\alpha & 9+5\alpha & 1 & 8\alpha & 9\alpha & 12+9\alpha \\ 12+11\alpha & 5+10\alpha & 2+4\alpha & 1 & 7\alpha & 7+11\alpha \\ 9\alpha & 9+5\alpha & 9+5\alpha & 12\alpha & 1 & 3+4\alpha \end{pmatrix}$	$[[6, 4, 12]]_{3+2i}$
$G = \begin{pmatrix} 1 & 0 & 9+5\alpha & 12\alpha & 2\alpha & 12+5\alpha \\ 0 & 1 & 10+7\alpha & 3\alpha & 10\alpha & 12+3\alpha \\ 9+5\alpha & 9+5\alpha & 1 & 8\alpha & 9\alpha & 12+9\alpha \\ 12+11\alpha & 5+10\alpha & 2+4\alpha & 1 & 7\alpha & 7+11\alpha \end{pmatrix}$	$[[6, 2, 15]]_{3+2i}$
$G = \begin{pmatrix} 1 & 0 & 11\alpha & 12\alpha & 2+4\alpha & 9+11\alpha \\ 0 & 1 & 8+3\alpha & 11\alpha & 8\alpha & 7+5\alpha \\ 4+8\alpha & 0 & 0 & 5+10\alpha & 12\alpha & 9+11\alpha \end{pmatrix}$	$[[6, 0, 15]]_{3+2i}$
$G = \begin{pmatrix} 1 & 12+11\alpha & 8\alpha & 2\alpha & 12 & 8+7\alpha & 10+5\alpha & 3+12\alpha \\ 12\alpha & 1 & 5+10\alpha & 11\alpha & 2+6\alpha & 1+9\alpha & 2+8\alpha & 6+7\alpha \\ 5\alpha & 9\alpha & 1 & 8+3\alpha & 11+8\alpha & 2 & 11+\alpha & 12+6\alpha \\ \alpha & 1 & 11+\alpha & 1 & 11+4\alpha & 9+3\alpha & 7+10\alpha & 8+6\alpha \end{pmatrix}$	$[[8, 0, 24]]_{3+2i}$

$$G = \begin{pmatrix} 1 & 12+11\alpha & 8\alpha & 2\alpha & 12 & 8+7\alpha & 10+5\alpha & 3+12\alpha \\ 12\alpha & 1 & 5+10\alpha & 11\alpha & 1+6\alpha & 1+9\alpha & 2+8\alpha & 6+7\alpha \\ 5\alpha & 9\alpha & 1 & 8+3\alpha & 11+8\alpha & 2 & 11+\alpha & 12+6\alpha \\ \alpha & 1 & 11+\alpha & 1 & 11+4\alpha & 9+3\alpha & 7+10\alpha & 8+6\alpha \end{pmatrix}.$$

Using the Gray image of this code, we obtain a quantum code with the parameters $[[16, 0, \geq 6]]$ over $\mathbb{F}_{13}$ (Table 5). The generator matrix of the Gray image of the code C is

$$G^{'} = \begin{pmatrix} 0 & 4 & 10 & 9 & 0 & 12 & 3 & 2 & 1 & 6 & 11 & 6 & 12 & 3 & 12 & 0 \\ 2 & 0 & 6 & 4 & 1 & 8 & 10 & 12 & 10 & 1 & 9 & 7 & 6 & 2 & 0 & 1 \\ 3 & 8 & 0 & 7 & 10 & 0 & 11 & 1 & 2 & 1 & 1 & 4 & 9 & 2 & 1 & 4 \\ 11 & 0 & 11 & 0 & 5 & 7 & 6 & 1 & 3 & 1 & 1 & 1 & 10 & 5 & 11 & 0 \\ 12 & 7 & 2 & 7 & 1 & 10 & 1 & 0 & 0 & 4 & 10 & 9 & 0 & 12 & 3 & 2 \\ 3 & 12 & 4 & 6 & 7 & 11 & 0 & 12 & 2 & 0 & 6 & 4 & 1 & 8 & 10 & 12 \\ 11 & 12 & 12 & 9 & 4 & 11 & 12 & 9 & 3 & 8 & 0 & 7 & 10 & 0 & 11 & 1 \\ 10 & 12 & 12 & 12 & 3 & 8 & 2 & 0 & 11 & 0 & 11 & 0 & 5 & 7 & 6 & 1 \end{pmatrix}.$$

Using the software programme MAGMA, it can easily be checked that this [16, 8, 6] classical linear code is an extremal self-dual code over $\mathbb{F}_{13}$.

For the benefit of readers, some of these programs can be found in [7,8].

6 Quantum logical gates and quantum teleportation in quantum channel over R_q

In this section, we define quantum logical gates based on Pauli spin matrices, for example Hadamard gate, for quantum codes given in Sects. 4 and 5 for $q = p$. Using these gates, we encode qubits in quantum channel over R_p.

6.1 Quantum logical gates and basis vectors over R_q

We can consider a quantum system with p-dimensional state space. For the basis vectors, bra-ket notations are used in general. For p-ary quantum state space, the basis vectors are denoted by

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{p\times 1}, |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}_{p\times 1}, \ldots, |p-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}_{p\times 1}.$$

To define the basis for q-ary quantum state space, we need tensor product. The tensor product $\otimes$ is usual tensor product, namely $|a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_n\rangle = |a_1 a_2 \cdots a_n\rangle$. Let $u = (a_1, \ldots, a_n)$ be a vector in a vector space. Thereafter, $|u\rangle$ denotes $|u_1 u_2 \cdots u_n\rangle$.

Let the set $P = \{I, X, Z, Y\}$ denote the well-known Pauli spin matrices. Here, for example, X is known quantum *NOT* gate that it can flip a quantum bit (shortly qubit). More information can be found in ([13], pp.13–20).

Definition 1 [10,14] Let the set $P_p = \{I, X_a, Z_a, Y_a\}$ be the Pauli spin matrices for p-ary quantum state space. The quantum NOT gate X and quantum gate Z were given by

$$(X_i)_{s,t} = \delta_{t,(s+i \pmod{p})}, \quad (Z_i)_{s,t} = \xi^{i.s \pmod{p}} \delta_{s,t},$$

respectively. Here, $\delta_{s,t}$ denotes the Kronecker delta function and $0 \le s, t \le p-1$. The Hadamard gate is defined as

$$H_p = \frac{1}{\sqrt{p}} \left(a_{s,t}\right), \quad a_{s,t} = \xi^{(s-1)(t-1) \pmod{p}}, \quad 1 \le s, t \le p.$$

These gates act on the quantum state $|a_1\rangle$ as

$$X_a\,|a_1\rangle = |a_1 + a \pmod{p}\rangle\,,\; Z_a\,|a_1\rangle = \xi^{Tr(aa_1)}\,|a_1\rangle\,,\; Y_a = X_a Z_a,$$

where $\xi = e^{2\pi i/p}$. Lastly, the Hadamard gate for q-ary quantum state space was constructed by

$$H_q = \frac{1}{\sqrt{q}} \left(\underbrace{H_p \otimes \cdots \otimes H_p}_{m \text{ times}} \right).$$

For example, let $p = 5$. Then,

$$H_p = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \xi & \xi^2 & \xi^3 & \xi^4 \\ 1 & \xi^2 & \xi^4 & \xi & \xi^3 \\ 1 & \xi^3 & \xi & \xi^4 & \xi^2 \\ 1 & \xi^4 & \xi^3 & \xi^2 & \xi \end{pmatrix}.$$

Note that $H_p H_p^{\dagger} = H_p^{\dagger} H_p = I_p$, where $H_p^{\dagger}$ denotes the conjugate transpose of H_p and I_p denotes the identity matrix in p dimensions. In light of the above facts, we now define basis vectors and quantum logical gates for a p-ary quantum state space over R_p.

Definition 2 Let $r = r_1 + r_2\alpha$ be an element of R_p and let $X_{r_1}, X_{r_2}, Z_{r_1}$ and Z_{r_2} denote the quantum gates given in Definition 1. We define quantum gates $X_r^{'}$ and $Z_r^{'}$ over R_p as

$$X_r^{'} = X_{r_1} \otimes X_{r_2}, \quad Z_r^{'} = Z_{r_1} \otimes Z_{r_2},$$

respectively. Also, we define Hadamard gate $H_p^{'}$ for R_p as

$$H_p^{'} = H_p \otimes H_p.$$

Example 6 Let $\alpha = 2 + i$, that is, $p = 5$. There are 25 quantum $X_r^{'}$ gates and 25 quantum $Z_r^{'}$ gates for $R_5 = \mathbb{F}_5 + \alpha\mathbb{F}_5$. Using the above method, we now give some of them:

$$X_1^{'} = X_1 \otimes X_0 = \begin{bmatrix} 0_5 & I_5 & 0_5 & 0_5 & 0_5 \\ 0_5 & 0_5 & I_5 & 0_5 & 0_5 \\ 0_5 & 0_5 & 0_5 & I_5 & 0_5 \\ 0_5 & 0_5 & 0_5 & 0_5 & I_5 \\ I_5 & 0_5 & 0_5 & 0_5 & 0_5 \end{bmatrix}_{25\times 25},$$

where 0_5 denotes 5×5 zero matrix and

$$X_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}_{5\times 5}.$$

Note $1 = 1 + 0.\alpha$, that is, $r_1 = 1$, $r_2 = 0$, and $X_0 = I_5$.

Another quantum NOT gate $X_\alpha^{'}$ for R_5 is

$$X_\alpha^{'} = \begin{bmatrix} X_1 & 0_5 & 0_5 & 0_5 & 0_5 \\ 0_5 & X_1 & 0_5 & 0_5 & 0_5 \\ 0_5 & 0_5 & X_1 & 0_5 & 0_5 \\ 0_5 & 0_5 & 0_5 & X_1 & 0_5 \\ 0_5 & 0_5 & 0_5 & 0_5 & X_1 \end{bmatrix}_{25\times 25},$$

$$Z_1^{'} = Z_1 \otimes Z_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \xi & 0 & 0 & 0 \\ 0 & 0 & \xi^2 & 0 & 0 \\ 0 & 0 & 0 & \xi^3 & 0 \\ 0 & 0 & 0 & 0 & \xi^4 \end{bmatrix} \otimes I_5,$$

$$= \begin{bmatrix} I_5 & 0_5 & 0_5 & 0_5 & 0_5 \\ 0_5 & \xi I_5 & 0_5 & 0_5 & 0_5 \\ 0_5 & 0_5 & \xi^2 I_5 & 0_5 & 0_5 \\ 0_5 & 0_5 & 0_5 & \xi^3 I_5 & 0_5 \\ 0_5 & 0_5 & 0_5 & 0_5 & \xi^4 I_5 \end{bmatrix}_{25\times 25}$$

The Hadamard gate $H_p^{'}$ acts on the state $|0\rangle$ as

$$\begin{aligned} H_p^{'} |0\rangle = {} & |0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |\alpha\rangle \\ & + |2\alpha\rangle + |3\alpha\rangle + |4\alpha\rangle + |1+\alpha\rangle + |2+\alpha\rangle + |3+\alpha\rangle \\ & + |4+\alpha\rangle + |1+2\alpha\rangle + |2+2\alpha\rangle + |3+2\alpha\rangle + |4+2\alpha\rangle + |1+3\alpha\rangle \\ & + |2+3\alpha\rangle + |3+3\alpha\rangle + |4+3\alpha\rangle + |1+4\alpha\rangle + |2+4\alpha\rangle + |3+4\alpha\rangle \\ & + |4+4\alpha\rangle . \end{aligned}$$

The number of basis vector for quantum codes defined over R_5 is 25, namely

$$\begin{aligned} & |0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, \\ & |\alpha\rangle, |1+\alpha\rangle, |2+\alpha\rangle, |3+\alpha\rangle, |4+\alpha\rangle, \\ & |1+2\alpha\rangle, |2+2\alpha\rangle, \ldots, |4+4\alpha\rangle . \end{aligned}$$

Using the above NOT gates $X_1^{'}$ and $X_{\alpha}^{'}$, we define some of these basis vectors as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{25\times 1},$$

$$|1\rangle = X_1^{'}\,|0\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1\ (21th\ \text{component}) \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{25\times 1},$$

$$|2\rangle = X_1^{'}\,|1\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1\ (16th\ \text{component}) \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{25\times 1},$$

$$|\alpha\rangle = X_{\alpha}^{'}\,|0\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1\ (5th\ \text{component}) \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{25\times 1},$$

$$|1+\alpha\rangle = X_1^{'} \otimes \left(X_{\alpha}^{'}\,|0\rangle\right).$$

It is clear that we obtain all basis vectors, using the above method since $|r_1 + r_2\alpha\rangle = X_{r_1}^{'} \otimes \left(X_{r_2\alpha}^{'}\,|0\rangle\right)$ and $|r_2\alpha\rangle = \underbrace{X_{\alpha}^{'} \otimes X_{\alpha}^{'} \otimes \cdots \otimes X_{\alpha}^{'}}_{r_2\, times}|0\rangle$.

6.2 Quantum encoding

There are infinitely many $p \times p$ matrices, and thus infinitely many single qubit gates. However, it turns out that the properties of the complete set can be understood from the properties of a much smaller set. It is possible to build up an arbitrary single qubit gate using a finite set of quantum gates. More generally, an arbitrary quantum computation on any number of qubits can be generated by a finite set of gates that is said to be universal for quantum computation. To obtain such a universal set, we first can construct some quantum gates involving multiple qubits. We already define single qubit gates in Definition 2. To obtain such a universal set, we need quantum controlled-NOT, shortly CNOT, gate which is a multiple qubits gate.

Definition 3 ([13], pp. 177–193, 484–488) The prototypical multi-qubit quantum logic gate is the controlled-NOT gate. This gate has two input qubits, known as the control qubit and the target qubit, respectively. The CNOT acts on qubits in two-dimensional quantum state space as:

$$\begin{aligned} CNOT\,|00\rangle &= |00\rangle\,,\ \ CNOT\,|01\rangle = |01\rangle\,, \\ CNOT\,|10\rangle &= |11\rangle\,,\ \ CNOT\,|11\rangle = |10\rangle\,. \end{aligned}$$

Definition 4 Let $r_1 + r_2\alpha$ be an element of R_p. Then, we define CNOT for p-dimensional quantum state space over R_p as follows:

$$CNOT_{r_1+r_2\alpha}\,|r_1 + r_2\alpha\ r_1 + r_2\alpha\rangle = |r_1 + r_2\alpha 0\rangle\,.$$

Here, $CNOT_{r_1+r_2\alpha}$ is a matrix with type $p^4 \times p^4$. Note $CNOT_{r_1+r_2\alpha}\,|r_3 + r_4\alpha\ 0\rangle = |r_3 + r_4\alpha 0\rangle$ for $r_1 + r_2\alpha \neq r_3 + r_4\alpha$.

For example, $CNOT_1\,|10\rangle = |11\rangle$, $CNOT_2\,|20\rangle = |22\rangle$, $CNOT_\alpha\,|\alpha 0\rangle = |\alpha\alpha\rangle$.

Example 7 Using these quantum gates and taking $\alpha = 2+i$, let us encode the quantum state

$$\begin{aligned} |\psi\rangle = {} & a_0\,|0\rangle + a_1\,|1\rangle + a_2\,|2\rangle + a_3\,|3\rangle + a_4\,|4\rangle + a_5\,|\alpha\rangle \\ & + a_6\,|2\alpha\rangle + a_7\,|3\alpha\rangle + a_8\,|4\alpha\rangle + a_9\,|1+\alpha\rangle + \cdots + a_{24}\,|4+4\alpha\rangle \end{aligned}$$

to

$$\begin{aligned} \left|\psi'\right\rangle = a_0 \left|\underbrace{0\cdots 0}_{26}\right\rangle + a_1\,|1\cdots 1\rangle + a_2\,|2\cdots 2\rangle + a_3\,|3\cdots 3\rangle \\ + a_4\,|4\cdots 4\rangle + a_5\,|\alpha\cdots\alpha\rangle + \cdots + a_{24}\,|4+4\alpha\cdots 4+4\alpha\rangle\,. \end{aligned}$$

A circuit performing this encoding is illustrated in Fig. 2. Circuit symbols of quantum gates are given in Fig. 1.

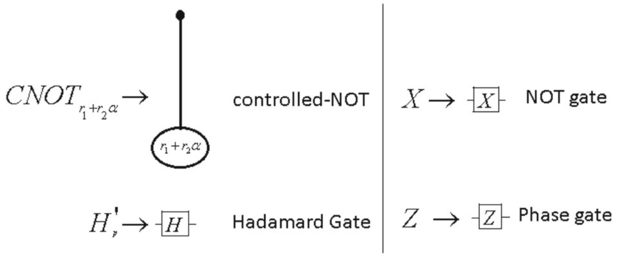

Fig. 1 Quantum gates and circuit symbols

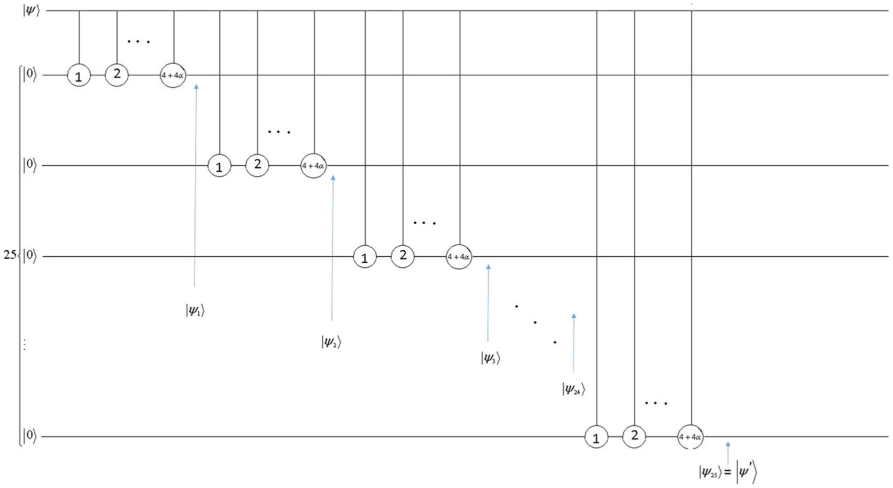

Fig. 2 Encoding circuit for the three-qubit bit flip code. The data to be encoded enters the circuit on the top line

In Fig. 2, $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, $|\psi_{24}\rangle$ are

$$|\psi_1\rangle = a_0\left|\underbrace{0\cdots0}_{26}\right\rangle + a_1\left|11\underbrace{0\cdots0}_{24}\right\rangle + a_2\left|22\underbrace{0\cdots0}_{24}\right\rangle + a_3\left|33\underbrace{0\cdots0}_{24}\right\rangle$$
$$+ a_4\left|44\underbrace{0\cdots0}_{24}\right\rangle + a_5\left|\alpha\alpha\underbrace{0\cdots0}_{24}\right\rangle + \cdots + a_{24}\left|4+4\alpha\,4+4\alpha\underbrace{0\cdots0}_{24}\right\rangle$$

$$|\psi_2\rangle = a_0\left|\underbrace{0\cdots0}_{26}\right\rangle + a_1\left|111\underbrace{0\cdots0}_{23}\right\rangle + a_2\left|222\underbrace{0\cdots0}_{23}\right\rangle + a_3\left|333\underbrace{0\cdots0}_{23}\right\rangle$$
$$+ a_4\left|444\underbrace{0\cdots0}_{23}\right\rangle + a_5\left|\alpha\alpha\alpha\underbrace{0\cdots0}_{23}\right\rangle + \cdots$$

$$+a_{24}\left|4+4\alpha 4+4\alpha\, 4+4\alpha\, \underbrace{0\cdots 0}_{23}\right\rangle,$$

$$|\psi_3\rangle = a_0\left|\underbrace{0\cdots 0}_{26}\right\rangle + a_1\left|1111\,\underbrace{0\cdots 0}_{22}\right\rangle + a_2\left|2222\,\underbrace{0\cdots 0}_{22}\right\rangle$$

$$+\,a_3\left|3333\,\underbrace{0\cdots 0}_{22}\right\rangle + a_4\left|4444\,\underbrace{0\cdots 0}_{22}\right\rangle$$

$$+\,a_5\left|\alpha\alpha\alpha\alpha\,\underbrace{0\cdots 0}_{22}\right\rangle + \cdots + a_{24}\left|4+4\alpha\, 4{+}4\,\alpha 4+4\alpha\, 4{+}4\alpha\,\underbrace{0\cdots 0}_{22}\right\rangle,$$

$$|\psi_{24}\rangle = a_0\left|\underbrace{0\cdots 0}_{26}\right\rangle + a_1\left|\underbrace{1\cdots 1}_{25}0\right\rangle + a_2\left|\underbrace{2\cdots 2}_{25}0\right\rangle + a_3\left|\underbrace{3\cdots 3}_{25}0\right\rangle + a_4\left|\underbrace{4\cdots 4}_{25}0\right\rangle$$

$$+\,a_5\left|\underbrace{\alpha\cdots\alpha}_{25}0\right\rangle + \cdots + a_{24}\left|\underbrace{4+4\alpha\cdots 4+4\alpha}_{25}0\right\rangle.$$

$|\psi_{25}\rangle = \left|\psi^{'}\right\rangle$ is given above. Using these quantum logical gates and basis vectors, one can encode codes given in Tables 1, 2 and 3 in previous section.

7 Conclusion

Since there is a transformation between quantum error correction codes over the finite field $\mathbb{F}_q$ and additive codes over $\mathbb{F}_q$ which are self-orthogonal with respect to certain inner products [10], we consider these additive codes as the Gray images of cyclic codes over R_q containing their Hermitian duals and Hermitian self-orthogonal additive cyclic codes over R_{p^2}, respectively. The structures of cyclic codes and their duals over R_q are determined, and the condition for cyclic codes to contain their duals is given. Considering the images of these cyclic codes under the Gray map φ, we obtain two classes of q-ary quantum error correcting codes. We also tabulate all nontrivial cyclic codes over R_5 of length 9 and 11 which contain their Hermitian duals and quantum codes obtained by Gray images of these codes. Note that we can tabulate all nontrivial cyclic codes over R_q of some length n. But as the length n increases, the table occupies more space in the paper. Also, for $q = p^2$, the structure of additive cyclic codes over R_q is studied and the circumstances of these codes to be self-orthogonal with respect to Hermitian inner product are given. Introducing the map δ, we obtain a class of p-ary quantum error correcting codes of length $2n$ from the additive cyclic codes over R_{p^2} of length n. We furthermore give some examples of additive cyclic codes over R_{25} of length 11 and quantum codes over $\mathbb{F}_5$ of length 22 obtained by the help of δ-images of these codes.

Acknowledgements The work was supported by TÜBİTAK (The Scientific and Technological Research Council of TURKEY) with Project Number 116F318. The author wishes to thank the associate editor and the anonymous referee whose comments have greatly improved this paper.

References

1. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**(3), 1183–1188 (2007)
2. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**, 3065–3072 (2001)
3. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**(2), 1098–1105 (1996)
4. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over $GF(4)$. IEEE Trans. Inf. Theory **44**, 1369–1387 (1998)
5. Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**(3), 1474–1484 (2015)
6. Gottesman, D.: Stabilizer codes and quantum error correction, Caltech Ph.D. Thesis, eprint: quant-ph/9705052, (1997)
7. Güzeltepe, M.: https://www.researchgate.net/publication/335105572FirstprogramMathematicamannheim, (2019)
8. Güzeltepe, M.: https://www.researchgate.net/publication/335105498SecondprogramMathematicahamming, (2019)
9. Kai, X., Zhu, S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2013)
10. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**(11), 4892–4914 (2006)
11. Knill, E., Laflamme, R.: Theory of quantum error-correcting codes. Phys. Rev. A **55**(2), 900–911 (1997)
12. Knill, E., Laflamme, R., Viola, L.: Theory of quantum error correction for general noise. Phys. Rev. Lett. **84**(11), 2525–2528 (2000)
13. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
14. Özen, M., Güzeltepe, M.: Quantum codes from codes over Gaussian integers with respect to the Mannheim metric. Quantum Inf. Comput. **12**(9–10), 813–819 (2012)
15. Rains, E.M.: Nonbinary quantum codes. IEEE Trans. Inf. Theory **45**(6), 1827–1832 (1999)
16. Shor, P.W.: Scheme for reducing decoherence in quantum memory. Phys. Rev. A **52**(4), 2493–2496 (1995)
17. Steane, A.: Multiple-particle interference and quantum error correction. Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. **452**(1954), 2551–2577 (1996)
18. Zhang, G., Chen, B., Li, L.: New optimal asymmetric quantum codes from constacyclic codes. Mod. Phys. Lett. B **28**(15), 1450126 (2014)