ORIGINAL PAPER

ON THE QUANTUM CODES OVER Y_q

ABDULLAH DERTLI[1], YASEMIN CENGELLENMIS[2]

Manuscript received: 19.03.2017; Accepted paper: 05.11.2020;
Published online: 30.12.2020.

Abstract: *In this paper, the quantum codes over F_q are constructed by using the cyclic codes over $Y_q = F_q + uF_q + vF_q + uvF_q$ with $u^2 = 1, v^2 = 1, uv = vu$, and $q = p^m, p$ is an odd prime. Moreover, the parameters of quantum codes over F_q are determined.*
Keywords: *Cyclic codes; quantum codes; Gray map.*

1. INTRODUCTION

Quantum error correcting codes are used in quantum computing to protect quantum information from errrors. The first error correcting code was discovered by Shor in [1] and independently by Steane in [2]. Although the theory quantum error correcting codes has differences from theory classical error correcting codes, Calderbank et al, gave a way to construct quantum error correcting codes from classical error correcting codes.

Many quantum error correcting codes have been constructed by using classical error correcting codes over many finite rings [3-16].

In this paper, in section 2, we give some knowledges about the ring Y_q. In section 3, a necessary and sufficient condition for cyclic codes over Y_q that contains its dual is given. The parameters of quantum error correcting codes are obtained from cyclic codes over Y_q. Some examples are given.

2. PRELIMINARIES

In [17], the commutative ring $Y_q = F_q + uF_q + vF_q + uvF_q$ with $u^2 = 1, v^2 = 1, uv = vu$ was introduced, where F_q is a finite field with q elements and $q = p^m, p$ is an odd prime. The skew cyclic codes over Y_q were studied. For $q = 3$, the commutative ring Y_3 was introduced by Mehmet Ozen et al. in [14]. In this paper the quantum codes over F_3 were constructed by using cyclic codes over Y_3.

Let

$$\lambda_1 = \left(\frac{q^2+1}{4}\right)(1+u+v+uv)$$

[1] Ondokuz Mayıs University, Mathematics Department, 55270 Atakum, Samsun, Turkey.
E-mail: abdullah.dertli@gmail.com
[2] Trakya University, Mathematics Department, 22030 Iskender, Edirne, Turkey.
E-mail: ycengellenmis@gmail.com.

$$\lambda_2 = (\frac{q^2+1}{4})(1+u) + (\frac{q^2-1}{4})(v+uv)$$

$$\lambda_3 = (\frac{q^2+1}{4})(1+v) + (\frac{q^2-1}{4})(u+uv)$$

$$\lambda_4 = (\frac{q^2+1}{4})(1+uv) + (\frac{q^2-1}{4})(u+v)$$

It is easy to show that $\lambda_i^2 = \lambda_i, \lambda_i\lambda_j = 0$ and $\sum_{k=1}^{4} \lambda_k = 1$, where $i, j = 1,2,3,4$ and $i \neq j$. This show that $Y_q = \sum_{k=1}^{4} \lambda_k F_q$. Therefore, for any $a \in Y_q$, a can be expresed uniquely as $a = \sum_{k=1}^{4} \lambda_k a_k$, where $a_k \in F_q$, for $k = 1,2,3,4$.

We define the Gray map Ψ from Y_q to F_q^4 as follows,

$$\Psi : Y_q \longrightarrow F_q^4$$

$$a + ub + vc + uvd \longmapsto \beta$$

where

$$\beta = ((\tfrac{q^2+1}{4})(a+b+c+d), (\tfrac{q^2+1}{4})(a+b) + (\tfrac{q^2-1}{4})(c+d), (\tfrac{q^2+1}{4})(a+c) + (\tfrac{q^2-1}{4})(b+d), (\tfrac{q^2+1}{4})(a+d) + (\tfrac{q^2-1}{4})(b+c)).$$

This map Ψ can be extended to Y_q^n in obvious way.

Theorem 1. *The Gray map Ψ is a distance preserving map from Y_q^n (Lee distance) to F_q^{4n} (Hamming distance) and it is also F_q-linear.*

The Hamming distance $d_H(x, y)$ between two vector x and y over F_q is the Hamming weight of the vector $x - y$.

The Lee weight $w_L(x)$ of $x = (x_0, x_1, ..., x_{n-1}) \in Y_q^n$ is defined as $w_L(x) = w_H(\Psi(x))$. The Lee distance $d_L(x, y)$ is given by $d_L(x, y) = w_L(x - y)$ for any $x, y \in Y_q^n$.

A linear code of length n over Y_q is a Y_q-submodule of Y_q^n.

Lemma 2. *Let C be a linear code of length n over Y_q with rank k and minimum Lee distance d, then $\Psi(C)$ is a $[4n, k, d]$ linear code over F_q.*

For any $x = (x_0, \dots, x_{n-1}), y = (y_0, \dots, y_{n-1})$ the inner product is defined as

$$xy = \sum_{i=0}^{n-1} x_i y_i$$

If $xy = 0$, then x and y are said to be orthogonal. Let C be a linear code of length n over Y_q, the dual of C

$$C^{\perp} = \{x \ : \forall y \in C, xy = 0\}$$

which is also a linear code over Y_q of length n. A code C is self orthogonal, if $C \subset C^{\perp}$ and self dual, if $C = C^{\perp}$.

Theorem 3. *Let C be a linear code of length n over Y_q. If C is self orthogonal, so is $\Psi(C)$.*

Proof: It is proved that as in [4].

If B_i ($i = 1,2,3,4$) are codes over F_q, we denote their direct sum by

$$B_1 \oplus B_2 \oplus B_3 \oplus B_4 = \{b_1 + ... + b_4 \ : \ b_i \in B_i, i = 1,...,4\}$$

Definition 4. *Let C be a linear code of length n over Y_q, we define*

$$C_1 = \left\{ (\frac{q^2+1}{4})(a+b+c+d) \in F_q^n \ : \ a+ub+vc+uvd \in C \right\}$$

$$C_2 = \left\{ (\frac{q^2+1}{4})(a+b) + (\frac{q^2-1}{4})(c+d) \in F_q^n \ : \ a+ub+vc+uvd \in C \right\}$$

$$C_3 = \left\{ (\frac{q^2+1}{4})(a+c) + (\frac{q^2-1}{4})(b+d) \in F_q^n \ : \ a+ub+vc+uvd \in C \right\}$$

$$C_4 = \left\{ (\frac{q^2+1}{4})(b+d) + (\frac{q^2-1}{4})(a+c) \in F_q^n \ : \ a+ub+vc+uvd \in C \right\}$$

It is note that C_i ($i = 1,...,4$) are linear codes over F_q^n. Moreover, $C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4$ and $|C| = |C_1||C_2||C_3||C_4|$.

Theorem 5. *Let $C = \sum_{i=1}^{4} \lambda_i C_i$ be a linear code of length n over Y_q. Then $C^{\perp} = \sum_{i=1}^{4} \lambda_i C_i^{\perp}$.*

Lemma 6. *If G_i are generator matrices of q-ary linear codes C_i ($i = 1,...,4$), then the generator matrix of C is*

$$G = \begin{bmatrix} \lambda_1 G_1 \\ \lambda_2 G_2 \\ \lambda_3 G_3 \\ \lambda_4 G_4 \end{bmatrix}$$

Let d_L minimum Lee weight of linear code C over Y_q. Then,

$$d_L = d_H(\Psi(C)) = \min\{d_H(C_1), d_H(C_2), d_H(C_3), d_H(C_4)\}$$

Where $d_H(C_i)$ denotes the minimum Hamming weights of codes $C_1, C_2, C_3, C_4,$ respectively.

Proposition 7. *Let $C=\sum_{i=1}^{4}\lambda_i C_i$ be a linear code of length n over Y_q, where C_i are codes over F_q of length n for $i=1,...,4$. Then C is a cyclic code over Y_q iff C_i, $i=1,...,4$ are all cyclic codes over F_q.*

Proof: Let $\left(a_0^i, a_1^i, ..., a_{n-1}^i\right)\in C_i$, where $i=1,...,4$. Assume that $m_i=\lambda_1 a_i^1+\lambda_2 a_i^2+\lambda_3 a_i^3+\lambda_4 a_i^4$ for $i=0,1,...,n-1$. Then $\left(m_0, m_1, ..., m_{n-1}\right)\in C$. Since C is a cyclic code, it follows that $\left(m_{n-1}, m_0, ..., m_{n-2}\right)\in C$. Note that

$$(m_{n-1}, m_0, ..., m_{n-2})=\lambda_1(a_{n-1}^1, a_0^1, ..., a_{n-2}^1)+...+\lambda_4(a_{n-1}^4, a_0^4, ..., a_{n-2}^4)$$

Hence $(a_{n-1}^i, a_0^i, ..., a_{n-2}^i)\in C_i$, for $i=1,...,4$. Therefore, C_1, C_2, C_3, C_4 are cyclic codes over F_q.

Conversely, suppose that C_1, C_2, C_3, C_4 are cyclic codes over F_q. Let $(m_0, m_1, ..., m_{n-1})\in C$ where $m_i=\lambda_1 a_i^1+...+\lambda_4 a_i^4$ for $i=0,...,n-1$. Then $\left(a_0^i, a_1^i, ..., a_{n-1}^i\right)\in C_i$ for $i=1,...,4$. Note that

$$\left(m_{n-1}, m_0, ..., m_{n-2}\right)=\lambda_1(a_{n-1}^1, a_0^1, ..., a_{n-2}^1)+...+\lambda_4(a_{n-1}^4, a_0^4, ..., a_{n-2}^4)\in C=\lambda_1 C_1\oplus\lambda_2 C_2\oplus\lambda_3 C_3\oplus\lambda_4 C_4.$$

So, C is a cyclic code over Y_q.

Proposition 8. *Suppose $C=\sum_{i=1}^{4}\lambda_i C_i$ is a cyclic code of length n over Y_q. Then*

$$C=\left\langle \lambda_1 f_1, \lambda_2 f_2, \lambda_3 f_3, \lambda_4 f_4\right\rangle$$

where f_1, f_2, f_3, f_4 are generator polynomials of $C_1, C_2, C_3, C_4,$ respectively.

Lemma 9. *For any cyclic code $C=\sum_{i=1}^{4}\lambda_i C_i$ of length n over Y_q, there exists a unique polynomial $f(x)$ such that $C=\langle f(x)\rangle$ and $f(x)\,|\,x^n-1$ where $f_i(x)$ are the generator polynomials of $C_i, i=1,2,3,4$ and $f(x)=\lambda_1 f_1(x)+\lambda_2 f_2(x)+\lambda_3 f_3(x)+\lambda_4 f_4(x).$*

Lemma 10. *Let $C=\sum_{i=1}^{4}\lambda_i C_i$ be a cyclic code of length n over Y_q, where C_1, C_2, C_3, C_4 are codes over F_q. Then*

$$C^{\perp}=\left\langle \lambda_1 h_1^*+\lambda_2 h_2^*+\lambda_3 h_3^*+\lambda_4 h_4^*\right\rangle$$

where for $h_i^*(x)$ are the reciprocal polynomials of $h_i(x)=\left(x^n-1\right)/f_i(x)$, that is $h_i^*(x)=x^{\deg h_i(x)}h_i\left(x^{-1}\right)$ for $i=1,2,3,4$.

Lemma 11. *(9) A cyclic code C with generator polynomial $f(x)$ contains its dual code if*

$$x^n - 1 \equiv 0 \left(\bmod ff^*\right)$$

where $f^*(x)$ is the reciprocal polynomial of $f(x)$.

3. QUANTUM CODES FROM CYCLIC CODES OVER Y_q

Lemma 12. *(13) Let C_1 and C_2 be linear codes over F_q with parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$, respectively and $C_2^{\perp} \subseteq C_1$. Furthermore, let*

$$d = \min\{w_t(v):\ v \in (C_1 \setminus C_2^{\perp}) \cup (C_2 \setminus C_1^{\perp})\} \geq \min\{d_1, d_2\}$$

Then, there exists a quantum error correcting code C with parameters $[[n, k_1 + k_2 - n, d]]_q$. In particular, if $C_1^{\perp} \subseteq C_1$, then there exists a quantum error correcting code C with parameters $[[n, 2k_1 - n, d]]$, where $d_1 = \min\{w_t(v):\ v \in C_1 \setminus C_1^{\perp}\}$.

Theorem 13. *Let C be a cyclic code of arbitrary length n over Y_q, where $f(x) = \lambda_1 f_1(x) + \lambda_2 f_2(x) + \lambda_3 f_3(x) + \lambda_4 f_4(x)$, then $C^{\perp} \subseteq C$ iff $x^n - 1 \equiv 0 \left(\bmod f_i(x) f_i^*(x)\right)$, where $f_i^*(x)$ are the reciprocal polynomials of $f_i(x)$ respectively, for $i = 1,2,3,4$.*

Proof: Let $x^n - 1 \equiv 0 \left(\bmod f_i(x) f_i^*(x)\right)$ for $i = 1,2,3,4$. By using Lemma 11 $C_i^{\perp} \subseteq C_i$ for $i = 1,2,3,4$. By using this, we get $\lambda_i C_i^{\perp} \subseteq \lambda_i C_i$ for $i = 1,2,3,4$. Hence, $\sum_{j=1}^{4} \lambda_j C_j^{\perp} \subseteq \sum_{j=1}^{4} \lambda_j C_j$. So, we have $\left\langle \sum_{j=1}^{4} \lambda_j h_j^*(x) \right\rangle \subseteq \left\langle \sum_{j=1}^{4} \lambda_j f_j(x) \right\rangle$. This implies that $C^{\perp} \subseteq C$.

Conversely, if $C^{\perp} \subseteq C$, then $\sum_{j=1}^{4} \lambda_j C_j^{\perp} \subseteq \sum_{j=1}^{4} \lambda_j C_j$. Since C_i are the q-ary codes such that $\lambda_i C_i$ is equal to C mod λ_i, $i = 1,2,3,4$, we have $C_i^{\perp} \subseteq C_i$, $i = 1,2,3,4$. So, $x^n - 1 \equiv 0 \left(\bmod f_i(x) f_i^*(x)\right)$, $i = 1,2,3,4$.

Theorem 14. *Let $C = \sum_{i=1}^{4} \lambda_i C_i$ be a cyclic code of length n over Y_q. If $C_i^{\perp} \subseteq C_i$ where $i = 1,2,3,4$, then $C^{\perp} \subseteq C$ and there exists a quantum error-correcting code with parameters $[[4n, 2k - 4n, d_L]]$, where d_L is the minimum Lee weight of the code C and k is the dimension of the code $\Psi(C)$.*

4. EXAMPLE

Let $n=5$, $x^{10}-1=(x+1)^5(x+4)^5$ *in* $F_5[x]$. *Let* $f_1(x)=f_2(x)=x+4$, $f_3(x)=f_4(x)=f_5(x)=f_6(x)=x+1$. *Thus* $C=\langle \eta_1 f_1, \eta_2 f_2, ..., \eta_6 f_6 \rangle$. $C_i, i=1,...,6$ *are* $[10,9,2]$ *codes of length* 10. *So,* $\Psi(C)$ *is* $[40,36,2]$ *linear code. By Theorem 13,* $C^{\perp} \subseteq C$ *. Using Theorem 14, we obtain a quantum code with parameters* [[40,32,2]].

Table 1. Some parameters of quantum codes.

n	***q***	C_i	$\Psi(C)$	**[[*N*,*K*,*D*]]**
3	19	[3,2,2]	[12,8,2]	[[12,4,2]]
4	9	[4,3,2]	[16,12,2]	[[16,8,2]]
5	5	[5,3,3]	[20,12,3]	[[20,4,3]]
12	3	[12,9,2]	[48,36,2]	[[48,24,2]]
20	9	[20,16,4]	[80,64,4]	[[80,48,4]]
27	3	[27,21,2]	[108,84,2]	[[108,60,2]]
30	5	[30,29,2]	[120,116,2]	[[120,112,2]]
36	5	[36,34,2]	[144,136,2]	[[144,128,2]]

CONCLUSION

In this paper, by using cyclic codes over the finite ring Y_q some parameters of quantum codes are obtained.

REFERENCES

[1] Shor, P. W., *Phys. Rev. A*, **52**, 2493, 1995.
[2] Steane, A.M., *Phys. Rev. A*, **54**, 4741, 1996.
[3] Calderbank, A.R., Rains, E.M., Shor, P.M. Sloane, N.J.A., *IEEE Trans. Inf. Theory*, **44**, 1369, 1998.
[4] Dertli, A., Cengellenmis, Y., Eren, S., *Int. J. Quantum Inf.*, **13**, 1550031, 2015.
[5] Dertli, A., Cengellenmis, Y., Eren, S., *Int. J. Algebra*, **9**, 115, 2015.
[6] Dertli, A., Cengellenmis, Y., Eren, S., *Discrete Math. Algorithms Appl.*, **8**(2), 1650036, 2016.
[7] Dertli, A., Cengellenmis, Y., Eren, S., *Int. J. Quantum Inf.*, **14**(1), 1650012, 2016.
[8] Dertli, A., Cengellenmis, Y., Eren, S., *Palestine J. Math.*, **4**, 547, 2015.
[9] Qian, J., *J. Inf. Comput. Sci.*, **10**, 1715, 2013.
[10] Qian, J., Ma, W., Gou, W., *Int. J. Quantum Inform.*, **7**, 1277, 2009.
[11] Ashraf, M., Mohammad, G., *Int. J. Quantum Inform.*, **12**,1450042, 2014.
[12] Ashraf, M., Mohammad, G., *Int. J. Inf. Coding Theory*, **2**, 137, 2015.
[13] Ashraf, M., Mohammad, G., *Quantum Inform. Proc.*, **15**, 4089, 2016.
[14] Ozen, M., Ozzaim, N.T., Ince, H., *J. Phys. Conf. Ser.*, **766**(1), 012020, 2016.
[15] Kai, X., Zhu, S., *Int. J. Quantum Inform.*, **9**, 689, 2011.
[16] Yin, X., Ma, W., *International Joint Conferences of IEEE TrustCom-11*, 2011. https://doi.org/10.1109/TrustCom.2011.122
[17] Dertli, A., Cengellenmis, Y., *J. Sci. Arts*, **2**, 215, 2017.