International Journal of Discrete Mathematics
2019; 4(1): 52-56
http://www.sciencepublishinggroup.com/j/dmath
doi: 10.11648/j.dmath.20190401.18
ISSN: 2578-9244 (Print); ISSN: 2578-9252 (Online)

New Non-binary Quantum Codes Over F_q+uF_q+vF_q+uvF_q

Leilei Gao

Department of Mathematics, School of Mathematics and Statistics, Shandong University of Technology, Zibo, China

Email address:
gaoleileixzc@163.com

To cite this article:
Leilei Gao. New Non-binary Quantum Codes Over F_q+uF_q+vF_q+uvF_q. *International Journal of Discrete Mathematics*. Vol. 4, No. 1, 2019, pp. 52-56. doi: 10.11648/j.dmath.20190401.18

Received: February 24, 2019; **Accepted**: April 10, 2019; **Published**: May 6, 2019

Abstract: Let R= F_q+uF_q+vF_q+uvF_q be a commutative ring with u^2=u, v^2=v, uv=vu, where q is a power of an odd prime. Ashraf and Mohammad constructed some new quantum codes from cyclic codes. Under this background, another Gray map from R to F_q^4 is given. This map can be naturally extended to R^n. The problem on the ring turns to the field by this isomorphic map now. Therefore, This mapping is obviously a weight-preserving and distance-preserving map. The results show that the codes after mapping are self-orthogonal codes over F_q if they are self-orthogonal codes over R. Some computational examples show that some better non-binary quantum codes can be obtained under this Gray map. We discuss the structure of linear codes. On this basis, the structure of the generating matrix of linear codes is obtained. The structure of their dual codes is also obtained. The CSS construction guarantees the existence of quantum codes. Finally, with the help of the CSS construction, we get some good quantum codes. By comparison, our quantum codes have better parameters.

Keywords: Gray Map, Cyclic Codes, New Non-binary Quantum Codes

1. Introduction

Quantum error-correcting codes have experienced tremendous growth since the discovery that there exists quantum error-correcting codes which protect quantum information as classical error-correcting codes protect classical information. In 1994, the quantum computer theory of quantum parallel computing proposed by Shor *et al.* on the basis of quantum superposition and coherence, the most essential quantum characteristics, attracted the attention of experts and scholars from home and abroad [1]. One of the important research problems of quantum error-correcting codes is to construct quantum codes with high code rate and large minimum distance. In recent years, the theory of quantum codes constructions develops rapidly. Many good quantum codes are constructed by classical error-correcting codes with self-orthogonal or dual containing properties over finite fields [2].

Recently, there are many papers on quantum codes construction from cyclic codes by classical error-correcting codes over finite rings. Qian *et al.* constructed some quantum codes over the ring F_2+uF_2 with $u^2=0$ [3]. Kai and Zhu studied quantum codes construction over F_4+uF_4 with $u^2=0$ [4]. Ashraf and Mohammad made many outstanding contributions in quantum code [5-6]. One of their contributions is that they constructed some new non-binary quantum codes over $F_q+uF_q+vF_q+uvF_q$ with $u^2=v^2=0$ [7]. On the basis of previous studies, many other scholars have made great contributions of quantum codes from cyclic codes over different rings [3, 8-10]. These results show that some good quantum codes can be obtained by classical codes over finite rings.

One should note that one of the important problems of codes over rings is to design the Gray map from rings to finite fields. The Gray map connects the codes over rings and the codes over finite fields. Therefore, designing the effective Gray map preserving self-orthogonal properties from rings to finite fields is crucial for constructing quantum codes by codes over rings. In this correspondence, we design another Gray map from $F_q+uF_q+vF_q+uvF_q$ to F_q (q is a power of an odd prime). The computational examples show that our Gray map can produce better quantum codes (see [7, 11-12]).

The rest of this paper is organized as follows. In Section 2, we give a new Gray map. Some properties of this Gray map are given. Then in Section 3, some examples under this Gray map are recomputed and get some better quantum codes. In this sense, this Gray map is more effective to produce new or good non-binary quantum codes. In Section 4, we summary the full paper.

2. Gray Map

Let F_q be a finite field with q elements, where q is a power of an odd prime. Denote a commutative ring $R=F_q+uF_q+vF_q+uvF_q$, where $u^2=u, v^2=v$ and $uv=vu$. From the Chinese Remainder Theorem, for any $r\in R$, r can be expressed uniquely as

$$r=\varepsilon_1a+\varepsilon_2b+\varepsilon_3c+\varepsilon_4d, \tag{1}$$

Where $a,b,c,d\in F_q$ and $\varepsilon_1=uv$, $\varepsilon_2=u-uv,$ $\varepsilon_3=v-uv,$ $\varepsilon_4=1-u-v+uv.$ It is easy to check that $\varepsilon_i^{\ 2}=\varepsilon_i,$ $\varepsilon_i\varepsilon_j=\ \varepsilon_j\varepsilon_i=0,$ where $i,j=1,2,3,4$ and $i\neq j.$ In fact, from the Chinese Remainder Theorem, we have $R=\varepsilon_1R\oplus\ \varepsilon_2R\oplus\varepsilon_3R\oplus\varepsilon_4R.$ Therefore,

$$\begin{aligned}\varepsilon_4R&=(1-u-v+uv)(F_q+uF_q+vF_q+uvF_q)\\&=F_q-uF_q-vF_q+uvF_q\\&=(1-u-v+uv)F_q\\&=\varepsilon_4F_q.\end{aligned}\tag{2}$$

Similarly, we have $\varepsilon_1R=\varepsilon_1F_q,$ $\varepsilon_2R=\varepsilon_2F_q,$ $\varepsilon_3R=\varepsilon_3F_q,$ which implies that

$$\begin{aligned}R&=\varepsilon_1R\oplus\varepsilon_2R\oplus\varepsilon_3R\oplus\varepsilon_4R\\&=\varepsilon_1F_q\oplus\varepsilon_2F_q\oplus\varepsilon_3F_q\oplus\varepsilon_4F_q.\end{aligned}\tag{3}$$

Obviously, this ring is a principal ideal ring but not a chain ring because of its four maximal ideals [7].

Let C be nonempty and $C\subseteq R^n.$ If C is an R -submodule of R^n, then C is called a linear code of length n over R [13]. An element of C is called a codeword. A linear code C over R is called cyclic if every $\vec{c}=(c_0,c_1,\ldots,c_{n-1})\in C$ implies that $(c_{n-1},c_0,\ldots,c_{n-2})\in C$. For any $\vec{a}=(a_0,a_1,\ldots,a_{n-1})$ and $\vec{b}=(b_0,b_1,\ldots,b_{n-1})\in R^n$, the inner product of $\vec{a}$ and $\vec{b}$ is given by

$$\vec{a}\cdot\vec{b}=a_0b_0+a_1b_1+\cdots+a_{n-1}b_{n-1}\,. \tag{4}$$

If $\vec{a}\cdot\vec{b}=0$, then $\vec{a}$ and $\vec{b}$ are said to be orthogonal. The dual code of C is defined as

$$C^{\perp}=\{\vec{a}\in R^n\mid\vec{a}\cdot\vec{b}=0,\forall\vec{b}\in C\}\,. \tag{5}$$

A code C is called self-orthogonal if $C\subseteq C^{\perp}$ and self dual if $C=C^{\perp}.$

Now define a new Gray map as follows

$$\varphi:R\to F_q^4$$

$$\varepsilon_1a+\varepsilon_2b+\varepsilon_3c+\varepsilon_4d\mapsto(a+b+c+d,a-b+c-d,a+b-c-d,a-b-c+d). \tag{6}$$

This map can be naturally extended to R^n. Define the Lee weight of any element x of R to be $w_L(x)=w_H(\varphi(x))$ and the Lee weight of any element $\vec{c}=(c_0,c_1,\ldots,c_{n-1})$ of R^n to be $w_L(\vec{c})=\sum_{i=0}^{n-1}w_Lc_i.$ For any elements $\vec{c},$ $\vec{c}'\in R,$ the Lee distance between $\vec{c}$ and $\vec{c}'$ is given by $d_L(\vec{c},\vec{c}')=w_L(\vec{c}-\vec{c}')$. Further, the minimum Lee distance of the code C is defined as $d_L(C)=w_L(C)$ the minimum Lee weight of C.

Based on the above definitions, it's tempting to conclude that φ is F_q -linear and it is also a distance-reserving isometry from (R^n,d_L) to $(F_q^{\ 4n},d_H)$, where d_L and d_H denote the Lee and Hamming distance in R^n and $F_q^{\ 4n}$, respectively. Let C be a linear code of length n over R with parameters $[n,k,d]$, where $|C|=q^k$ and $d_L(C)=d.$ Because φ is a bijective map, then we have $\varphi(C)$ is a linear code with parameters $[4n,k,d]$ over F_q, which implies that $|C|=|\varphi(C)|$ and $d_L(C)=d_H(\varphi(C)).$

Next, quantum codes can be constructed by self-orthogonal codes over F_q . It means that self-orthogonal codes over finite fields are crucial for quantum codes construction. We will give a connection between self-orthogonal codes over R and self-orthogonal codes over F_q by the Gray map φ in the following.

Theorem 1 *[7] Let C be a linear code of length n over R. Then $\varphi(C)$ is a self-orthogonal code over F_q if C is a self-orthogonal code over R.*

Proof Let C be a self-orthogonal code over R and $\alpha=\varepsilon_1\vec{a}+\varepsilon_2\vec{b}+\varepsilon_3\vec{c}+\varepsilon_4\vec{d},$ $\beta=\varepsilon_1\vec{a}_1+\varepsilon_2\vec{b}_1+\varepsilon_3\vec{c}_1+\varepsilon_4\vec{d}_1\in C,$ where $\vec{a},\vec{b},\vec{c},\vec{d},\vec{a}_1,\vec{b}_1,\vec{c}_1,\vec{d}_1\in F^n.$ Then $\alpha\cdot\beta=\varepsilon_1\vec{a}\cdot\vec{a}_1+\varepsilon_2\vec{b}\cdot\vec{b}_1+\varepsilon_3\vec{c}\cdot\vec{c}_1+\varepsilon_4\vec{d}\cdot\vec{d}_1=0.$ So we get $\vec{a}\cdot\vec{a}_1=\vec{b}\cdot\vec{b}_1=\vec{c}\cdot\vec{c}_1=\ \vec{d}\cdot\vec{d}_1=0.$ Therefore,

$$\varphi(\alpha)\cdot\varphi(\beta)=(\vec{a}+\vec{b}+\vec{c}+\vec{d},\vec{a}-\vec{b}+\vec{c}-\vec{d},\vec{a}+\vec{b}-\vec{c}-\vec{d},\vec{a}-\vec{b}-\vec{c}+\vec{d})\cdot(\vec{a}_1+\vec{b}_1+\vec{c}_1+\vec{d}_1,\vec{a}_1-$$

$$\vec{b}_1+\vec{c}_1-\vec{d}_1, \vec{a}_1+\vec{b}_1-\vec{c}_1-\vec{d}_1, \vec{a}_1-\vec{b}_1-\vec{c}_1+\vec{d}_1) = 4\vec{a}\cdot\vec{a}_1+4\vec{b}\cdot\vec{b}_1+4\vec{c}\cdot\vec{c}_1+4\vec{d}\cdot\vec{d}_1=0.$$

Hence, $\varphi(C)$ is a self-orthogonal code over F_q. □

3. Quantum Codes from Cyclic Codes

First, we introduce some basic results on linear codes and cyclic codes over R. Then some computational examples show that some better non-binary quantum codes can be obtained under the Gray map.

For a linear code C of length n over R, we define [7]

$$C_1=\{\vec{a}\in F_q^n \mid \exists \vec{b},\vec{c},\vec{d}\in F_q^n, s.t. \varepsilon_1\vec{a}+\varepsilon_2\vec{b}+\varepsilon_3\vec{c}+\varepsilon_4\vec{d}\in C\},$$

$$C_2=\{\vec{b}\in F_q^n \mid \exists \vec{a},\vec{c},\vec{d}\in F_q^n, s.t. \varepsilon_1\vec{a}+\varepsilon_2\vec{b}+\varepsilon_3\vec{c}+\varepsilon_4\vec{d}\in C\},$$

$$C_3=\{\vec{c}\in F_q^n \mid \exists \vec{a},\vec{b},\vec{d}\in F_q^n, s.t. \varepsilon_1\vec{a}+\varepsilon_2\vec{b}+\varepsilon_3\vec{c}+\varepsilon_4\vec{d}\in C\},$$

$$C_4=\{\vec{d}\in F_q^n \mid \exists \vec{a},\vec{b},\vec{c}\in F_q^n, s.t. \varepsilon_1\vec{a}+\varepsilon_2\vec{b}+\varepsilon_3\vec{c}+\varepsilon_4\vec{d}\in C\}. \tag{7}$$

Clearly, C_i is a linear code of length n over F_q^n for each $i=1,2,3,4.$ Now C can be expressed as

$$C=\varepsilon_1C_1\oplus\varepsilon_2C_2\oplus\varepsilon_3C_3\oplus\varepsilon_4C_4, \tag{8}$$

which implies that $|C|=\prod_{i=1}^{4}|C_i|$. The generator matrix of C can be expressed as

$$G=\begin{pmatrix}\varepsilon_1G_1\\ \varepsilon_2G_2\\ \varepsilon_3G_3\\ \varepsilon_4G_4\end{pmatrix}, \tag{9}$$

where G_i is the generator matrix of C_i, $i=1,2,3,4$ [7].

Let $C=\varepsilon_1C_1\oplus\varepsilon_2C_2\oplus\varepsilon_3C_3\oplus\varepsilon_4C_4$ be a linear code of length n over R, where C_i is a linear code of length n over F_q, $i=1,2,3,4.$ It's easy to prove that C is a cyclic code if and only if C_i is a cyclic code, $i=1,2,3,4.$ In fact, suppose that $(c_{i,0},c_{i,1},\ldots,c_{i,n-1})\in C_i$, $i=1,2,3,4.$ Then let $c_j=\varepsilon_1c_{1,j}+\varepsilon_2c_{2,j}+\varepsilon_3c_{3,j}+\varepsilon_4c_{4,j}$, $j=0,1,\ldots,n-1.$ Obviously, C is a cyclic code so $(c_0,c_1,\ldots,c_{n-1})$ and $(c_{n-1},c_0,\ldots,c_{n-2})\in C.$ Therefore, $(c_{n-1},c_0,\ldots,c_{n-2})=\sum_{i=1}^{4}\varepsilon_i(c_{i,n-1},c_{i,0},\ldots,c_{i,n-2}).$ According to the uniqueness presentation of decomposition of linear codes over R, there must have $(c_{i,n-1},c_{i,0},\ldots,c_{i,n-2})\in C_i$, which implies that C_i is a cyclic code. The converse is similar.

The cyclic code C above can be expressed as follows

$$C=<\sum_{i=1}^{4}\varepsilon_ig_i(x)>, \tag{10}$$

where $g_i(x)$ is the generator polynomial of $C_i, i=1,2,3,4.$ We can easily get that $|C|=q^{4n-\sum_{i=1}^{4}\deg g_i(x)}$ [7]. Denote $g(x)=\sum_{i=1}^{4}\varepsilon_ig_i(x)$ then $g(x)\mid x^n-1$. Moreover,

$$C^{\perp}=<\sum_{i=1}^{4}\varepsilon_ih_i^{*}(x)>, \tag{11}$$

where $h_i^*(x)$ is the reciprocal polynomial of $h_i(x)=\frac{x^n-1}{g_i(x)}$ for $i=1,2,3,4,$ *i.e.*, $h_i^*(x)=x^{\deg h_i(x)}h_i(x^{-1})$ (see the reference [7] and [13]). According to the definition of dual code, $|C^{\perp}|=\sum_{i=1}^{4}\deg g_i(x).$

Lemma 1 *[14] Let* C *and* $\overline{C}$ *be two linear codes over* F_q *with parameters* $[n,k,d]$ *and* $[n,\bar{k},\bar{d}]$, *respectively. If* $\overline{C}^{\perp}\subseteq C$, *then an* $[[n,k+\bar{k}-n,d']]_q$ *quantum code can be obtained, where* $d'=\min\{w_H(v)\mid v\in(C\setminus\overline{C}^{\perp})\cup(\overline{C}\setminus C^{\perp})\}\geq\min\{d,\bar{d}\}$. *In particular, if* $C^{\perp}\subseteq C$, *then an quantum code with parameters* $[[n,2k-n,\tilde{d}]]_q$ *can be obtained, where* $\tilde{d}=\min\{w_H(v)\mid v\in C\setminus C^{\perp}\}$.

Lemma 2 *[7] Let* $C=\oplus_{i=1}^{4}\varepsilon_iC_i=<\sum_{i=1}^{4}\varepsilon_ig_i(x)>$ *be a cyclic code of length* n *over* R, *where* $C_i=(g_i(x))$ *for* $i=1,2,3,4.$ *Then* $C^{\perp}\subseteq C$ *if and only if* $x^n-1\equiv0(\bmod\ g_i(x)g_i^*(x))$ *for* $i=1,2,3,4.$

By Lemmas 1 and 2, the non-binary quantum codes can be constructed as follows.

Theorem 2 *[3] Let* $C = \oplus_{i=1}^{4} \varepsilon_i C_i$ *be a cyclic code of length* n *over* R *. If* $C_i^{\perp} \subseteq C, i = 1,2,3,4,$ *then* $C^{\perp} \subseteq C$ *. Then a quantum code with parameters* $[[4n, 2k-4n, d]]_q$ *can be obtained, where* $d = \min\{w_L(v) \mid v \in C \setminus C^{\perp}\}$*.*

According to Theorem 2, some non-binary quantum codes from cyclic codes over R are constructed. It seems that an available source for non-binary quantum codes in the literature doesn't exist. So we take some quantum codes as known non-binary quantum codes [7, 11-12]. Moreover, quantum codes, constructed by our Gray map, listed in the Table 1 have the better parameters. We only write the coefficients of the generating polynomials according to the ascending power just for simplicity. For example, 21 represents $x+2$ and the polynomial $x+8$ is represented as 81.

Table 1. *New quantum codes* $[[n,k,d]]_q$.

n	<$g_1(x)$, $g_2(x)$, $g_3(x)$, $g_4(x)$>	$\phi(C)$	$[[n, k, d]]_q$	$[[n', k', d']]_q$
9	$<1,1,1,41>$	$[36,35,2]_{13}$	$[[36,34,2]]_{13}$	$[[36,30,2]]_{13}$ ref.[11]
15	$<21,81,541,6151>$	$[60,53,4]_{11}$	$[[60,46,4]]_{11}$	$[[63,39,4]]_{11}$ ref.[12]
22	$<411421,411421,134411,134411>$	$[88,68,4]_5$	$[[88,48,4]]_5$	$[[88,48,2]]_5$ ref.[7]
24	$<1,1,1,21>$	$[96,95,2]_5$	$[[96,94,2]]_5$	$[[96,90,2]]_5$ ref.[11]
28	$<4213421,4213421,4312431,4312431>$	$[112,88,4]_5$	$[[112,64,4]]_5$	$[[112,64,2]]_5$ ref.[7]
28	$<1,1,1,21>$	$[112,111,2]_5$	$[[112,110,2]]_5$	$[[112,104,2]]_5$ ref.[11]
31	$<4101,4101,4111,4111>$	$[124,112,3]_5$	$[[124,100,4]]_5$	$[[124,100,3]]_5$ ref.[7]

In Example 1, the construction process of a good quantum code compared with the one given is described in detail. The two codewords have the same length and dimensions but this code has the larger minimum distance than that one.

Example 1 Let $R = F_5 + uF_5 + vF_5 + uvF_5$ and $n = 11$. $x^{11} - 1 = (x+4)(x^5 + 4x^4 + 4x^3 + x^2 + 3x + 4) \cdot (x^5 + 2x^4 + 4x^3 + x^2 + x + 4)$ over F_5. Let $g(x) = \varepsilon_1 g_1(x) + \varepsilon_2 g_2(x) + \varepsilon_3 g_3(x) + \varepsilon_4 g_4(x),$ where $g_1(x) = g_2(x) = x^5 + 2x^4 + 4x^3 + x^2 + x + 4,$ $g_3(x) = g_4(x) = x^5 + 4x^4 + 4x^3 + x^2 + 3x + 4$. Let $C =< g(x) >$ be a cyclic code over R. Clearly, $g_i(x) g_i^*(x)$ divides $x^{11} - 1$ for each $i = 1,2,3,4.$ Hence, by Lemma 2, $C^{\perp} \subseteq C$. Further, $\varphi(C)$ is a linear code over F_5 with parameters $[44,24,7]$. For Theorem 2, there is a quantum code with parameters $[[44,4,7]]_5$. This quantum code is better than the known quantum code $[[44,4,5]]_5$ [7] because of its larger minimum distance.

4. Conclusion

In this paper, a Gray map from R^n to F_q^{4n} was constructed. The problems on rings are relatively less studied. Therefore, the problem on the ring turned to the field by this isomorphic map. Then we briefly discussed the properties of cyclic codes under this Gray map, laying the foundation for the following operations. Finally, we got some good quantum codes. By comparison, our quantum codes had better parameters. We hope that we can get better quantum codes by effective methods in the future.

References

[1] Shor, P. W.: Scheme for reducing decoherence in quantum memory, Phys. Rev. A, 52, 2493-2496 (1995).

[2] Tang, Y., Zhu, S., Kai, X., Ding, J.: New quantum codes from dual-containing cyclic codes over finite rings, Quantum Inf. Process., 15, 4489-4500 (2016).

[3] Qian, J., Ma, W., Gou, W.: Quantum codes from cyclic codes over finite ring, Int. J. Quantum Inf., 7, 1277-1283 (2009).

[4] Kai, X., Zhu, S.: Quaternary construction of quantum codes from cyclic codes over F_4+uF_4, Int. J. Quantum Inf., 9, 689-700 (2011).

[5] Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over F_3+vF_3, Int. J. Quantum Inf., 12, 1450042 (2014)

[6] Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over F_p+vF_p, Int. J. Inf. Coding Theory, 3 (2), 137-144 (2015)

[7] Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over $F_q+uF_q+vF_q+uvF_q$, Quantum Inf Process, 15, 4089-4098 (2016)

[8] Gao, J.: Quantum codes from cyclic codes over $F_q+vF_q+v^2F_q+v^3F_q$, Int. J. Quantum Inf., 13 (8), 1550063 (1-8) (2015).

[9] Ozen, M., Ozzaim, N. T., Ince, H.: Quantum codes from cyclic codes over $F_3+uF_3+vF_3+uvF_3$, International Conference on Quantum Science and Applications, Journal of Physics: Conference Series, 766, 0120202, (2016).

[10] Gao, J., Wang, Y.: Quantum codes derived from negacyclic codes, Int. J. Theor. Phys. 57, 682-686 (2018)

[11] Gao, Y. Gao, J. Fu, F-W.: Quantum codes from cyclic codes over the ring $F_q+v_1F_q+\ldots+v_rF_q$, Appl. Algebra Eng. Comm., doi: 10.1007/s00200-018-0366-y (2018).

[12] La Guardia, G. G.: Quantum codes derived from cyclic codes. Int. J. Theor. Phys., 56, 2479-2484 (2017)

[13] Ma, F., Gao, J., Fu, F-W.: Constacyclic codes over the ring $F_q+vF_q+V^2F_q$ and their applications of constructing new non-binary quantum codes, Quantum Inf. Process., 17: 122 (2018)

[14] Calderbank, A. R., Rains, E. M., Shor, P. M., Sloane, N. J. A.: Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory, 44, 1369-1387 (1998)