LCD Codes and Quantum Mysteries: Insights into Construction Techniques from Cyclic Codes over Finite Commutative Rings

Anju Sharma, Vinod Kumar, and Mamta Kansal*

Department of Mathematics, Guru Kashi University, Bathinda, Punjab, India.
*Department of Mathematics, Maharaja Ranjit Singh Punjab Technical University, Bathinda-151001 (Punjab).
e-mail: shabnam7191bwn@gmail.com, e-mail: vinod.k4bais@gmail.com,
*e-mail:mamtakansal2k8@yahoo.com

Correspondence Author: Vinod Kumar

Abstract:

Let F_q be a field of order q, whereas and are two not zero items of F_q, and q is a fraction of an unusual prime p. This article's main objective is to investigate the structural characteristics of cyclic codes over the finite ring R = $F_q[m_1]$. In $\{\left\{\frac{[m_1 m_2 - m_2 m_{1i}, m_2]}{m^2-\alpha^2}\right\}, (m^2 - \beta^2)\}$. The researcher constructs quantum-error-correcting (QEC) codes over R by decomposing the ring R into its parts, $R = D_1 \oplus D_2 \oplus D_3 \oplus D_4$, utilising orthogonal idempotent $D_1, D_2, D_3, and\ D_4$. As an example, we create a few ideal LCD codes.

Keywords: LCD code, Cyclic code, Quantum code, Gray map;

1. Introduction:

Until otherwise noted, the value of the order q is denoted by Fq (where q is an odd prime power), and its non-zero components are a and b. The finite ring R = Fq[u1, u2]/hu21- a2, u22 -b2, u1u2 -u2u1i will now be discussed. Verifying that R is a non-chain semi-local ring of order q4 is simple. Building quantum-error-correcting (QEC) coding is a great usage for cyclic codes. Classical error-correcting (CEC) codes are not the same as QEC codes. When Calderbank et al. [1] figured out how to get QEC codes using CEC coding over GF (4), it was a huge advance in 1998. Additionally, Calderbank et al. [1] presented a technique for creating QEC codes using CEC codes. Cycle coding spanning finite fields has been extensively studied in great detail (see, e.g., [2–5] and reference thereto). Gao et al. [6] created new quantum computations over Fq in 2015 using cyclic coding over Fq + vFq + v2Fq + v3Fq (in which q = pm, p is a prime that corresponds to 3j(p 1), v4 = v, and m is a positive integer). Subsequently, several tripartite quantum computer codes were built by Ozen et al. [7] using cyclic codes constructed over F3 + uF3 + vF3 + uvF3. Improved quantum and LCD coding spanning the ring Fpm + vFpm with v2 = 1, where m is a positive integer, were discovered in 2021 by Ashraf et al. [8]. The structural characteristics of cyclic codes over the FIELDS R are covered in this piece of writing. Researchers build a Grey mapping on the resulting ring R that yields stronger parameters and helps find stronger codes for quantum phenomena across R than those found in [8–13] (and their reference). Our primary goals in this study are to build quantum-error-correcting (QEC) codes over the bounded ring R and investigate the structural features of cyclic algorithms over it. Additionally, we research LCD codes.

The following are this paper's main contributions:

1. As shown in Table 1, this research presents better quantum code structures compared to those found in prior references [8–13].

2. A number of new codes for quantum systems are provided in this paper; Table 2.

3. As shown in Table 3, this research examines a few ideal LCD codes over the field R.

Table 1: Quantum coding generated over R from cycle coding.

$[[n^0, k^0, d^0]]_q$	$[[n, k, d]]_q$	h(C)	$h_4(X)$	$h_3(X)$	$h_2(X)$	$h_1(X)$	n
$[[40, 24, 2]]_5$ [9]	$[[40, 32, 2]]_5$	[40, 36, 2]	X+4	X+4	X+1	X+1	11
$[[80, 54, 3]]_5$ [11]	$[[80, 56, 3]]_5$	[80, 68, 3]	$(X+2)^2$ X+4	$(X+2)^2$ X+4	$(X+2)^2$ X+4	$(X+2)^2$ X+4	21
$[[88, 48, 2]]_5$ [9]	$[[88, 80, 2]]_5$	[88, 84, 2]	X+4	X+4	X+1	X+1	23
$[[112, 64, 2]]_5$ [9]	$[[112, 104, 2]]_5$	[112, 108, 2]	X+3	X+3	X+2	X+2	29
$[[120, 32, 3]]_5$ [12]	$[[120, 88, 3]]_5$	[120, 104, 3]	$(X+1)^2$ X^2+X+1	$(X+1)^2$ X^2+X+1	$(X+1)^2$ X^2+X+1	$(X+1)^2$ X^2+X+1	31
$[[124, 100, 4]]_5$ [8]	$[[124, 106, 4]]_5$	[124, 115, 4]	(X^3+X^2+X+4) (X^3+X^2+3X+4)	X+4	X+4	X+4	32
$[[140, 112, 2]]_5$ [9]	$[[140, 118, 3]]_5$	[140, 129, 3]	(X+4) $(X^6+X^5+X^4+X^3+X^2+X+1)$	$(X+4)^2$	X+4	X+4	36
$[[168, 96, 2]]_5$ [10]	$[[168, 112, 4]]_5$	[168, 140, 4]	(X+4) $(X^6+2X^4+3X^3+2X^2+X+1)$	(X+4) $(X^6+2X^4+3X^3+2X^2+X+1)$	(X+4) $(X^6+2X^4+3X^3+2X^2+X+1)$	(X+4) $(X^6+2X^4+3X^3+2X^2+X+1)$	43

Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

$[[96, 80, 3]]_7$ [8]	$[[96, 84, 3]]_7$	[96, 90, 3]	(X+3) (X^2+X+4)	(X+3)	(X+3)	(X+3)	25
$[[312, 282, 3]]_{13}$ [13]	$[[312, 288, 3]]_{13}$	[312, 300, 3]	$(X+3)^2$ (X+12)	$(X+3)^2$ (X+12)	$(X+3)^2$ (X+12)	$(X+3)^2$ (X+12)	79
$[[48, 32, 4]]_{17}$ [8]	$[[48, 34, 4]]_{17}$	[48, 41, 4]	(X+1) $(X^2+4X+16)$ (X^2+X+1)	(X+1)	(X+1)	1	12
	$[[76, 40, 4]]_{19}$	[76, 58, 4]	$(X+18)^{14}$	$(X+18)^2$	(X+18)	(X+18)	20

Table 2. From code with cycles over R to new quantum codes.

	[[n, k, d]]$_q$	*h*(C)	**h_4(X)**	**h_3(X)**	**h_2(X)**	**h_1(X)**	**n**
New quantum code	$[[36, 22, 3]]_3$	[36, 29, 3]	1	(X+2)	$(X+2)^2$	$(X+2)^4$	10
New quantum code	$[[100, 84, 3]]_5$	[100, 92, 3]	1	(X+4)	(X+4)	$(X+4)^6$	26
New quantum code	$[[60, 46, 3]]_5$	[60, 53, 3]	1	1	(X+4)	$(X+4)^2(X^2+X+1)$	16
New quantum code	$[[56, 44, 4]]_7$	[56, 50, 4]	1	(X+6)	(X+1)	$(X+1)(X+6)^3$	15
New quantum code	$[[44, 30, 4]]_{11}$	[44, 37, 4]	1	(X+10)	(X+10)	$(X+10)^5$	12

Table 3. LCD code graphics in grayscale with length n over R.

	***h*(C)**	**h_4(X)**	**h_3(X)**	**h_2(X)**	**h_1(X)**	**n**
Optimal	$[16, 11, 4]_3$	$(X+1)(X^2+1)$	$(X+1)$	$(X+1)$	1	5
Optimal	$[88, 84, 2]_3$	$(X+1)$	$(X+1)$	$(X+1)$	$(X+1)$	23
	$[24, 17, 4]_5$	$(X+1)(X^2+X+1)$ (X^2+4X+1)	$(X+1)$	$(X+1)$	1	7
Optimal	$[32, 27, 4]_7$	$(X+1)$ (X^2+4X+1)	$(X+1)$	$(X+1)$	1	9
Optimal	[148, 124, 5]11	$X^6+4X^5+3X^4$ $+7X^3$ $+3X^2+4X+1$	$X^6+4X^5+3X^4$ $+7X^3$ $+3X^2+4X+1$	$X^6+4X^5+3X^4$ $+7X^3$ $+3X^2+4X+1$	$X^6+4X^5+3X^4$ $+7X^3$ $+3X^2+5X+1$	38
	$[156, 100, 4]_{11}$	$(X^2+X+1)(X^{11}+X^{10}+$ $X^9+X^8+X^7+X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)$	$(X^2+X+1)(X^{11}+X^{10}+$ $X^9+X^8+X^7+X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)$	$(X^2+X+1)(X^{11}+X^{10}+$ $X^9+X^8+X^7+X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)$	$(X^2+X+1)(X^{11}+X^{10}+$ $X^9+X^8+X^7+X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)$	40
	$[44, 4, 11]_{19}$	$(X^{10}+$ $X^9+X^8+X^7+X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)$	$(X^{10}+$ $X^9+X^8+X^7+X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)$	$(X^{10}+$ $X^9+X^8+X^7+X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)$	$(X^{10}+$ $X^9+X^8+X^7+X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)$	12
	$[112, 60, 8]_{19}$	$(X+1)(X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)(X^6+$ $8X^5+3X^4+8X^3+3X^2$	$(X+1)(X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)(X^6+$ $8X^5+3X^4+8X^3+3X^2$	$(X+1)(X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)(X^6+$	$(X+1)(X^6+$ $X^5+X^4+X^3+X^2$ $+X+1)(X^6+$ $11X^5+3X^4+11X^3+3X^2$	29

		+8X+1)	+8X+1)	$11X^5+3X^4+11X^3+3X^2$ +11X+1)	+11X+1)	
	$[136, 100, 4]_{19}$	(X+1)($X^8+13X^7+15X6+16X^5+8X^4+16X^3+15X^2$ +13X+1)	(X+1)($X^8+13X^7+15X6+16X^5+8X^4+16X^3+15X^2$ +13X+1)	(X+1)($X^8+13X^7+15X6+16X^5+8X^4+16X^3+15X^2$ +13X+1)	(X+1)($X^8+13X^7+15X6+16X^5+8X^4+16X^3+15X^2$ +13X+1)	35

2. Preliminaries Result

The following subsection describes the Grey map over the ring R and deals with the investigation of certain preliminary issues. Additionally, we establish a few key findings that are necessary for the conversations that follow. A code C is linear if it is an R-submodule of Rn (where n is a positive integer). We refer to the components of C as codewords. The total amount of code words in C, denoted by jCj, is the dimension of C. We remember the following fundamental explanations:

(i) The number of locations where two vectors, y = (yn ,-------- y2, y1), and x = (xn ,-------- x2,x1,) differ is known as the Hamming is the distance, and it is represented by the symbol d(x, y).

(ii) The number of non-zero xi, represented by wt(x), is the Hamming weight of a vector x = (xn ,----x1, x2).

(iii) The dual of linear code C is C ⊥ = {x ∈ R n |x · y = 0 ∃ y ∈ C}. The Euclidean inner product of any two vectors, x = (xn ,------, x2 ,x1) and y = (yn ,----------, y2,y1), is defined as yx = yn xn 1+--------------+ y1 x1 +y0 x0 .

(iv) The code C is considered dual contained if C ⊥ ⊆ C, self-orthogonal when C = C?, and self-dual when C = C?. It is obvious that R = Fq + Fq m1 + Fq m2 + Fq m1m2 is a mathematical equation for the field, that's why Here, Fq is the finite field of order q, where $q = p^m$ for odd prime p and $m^2 = A^2$, $n^2 = B^2$, and $m^2 n^2 = n^2 m^2$. With four maximal concepts, it is a commutative non-chain semi-local field. X = α1 + α2m1 + α3m2 + α4m1m2 is a representation of a substance X of R, where ai €2 Fq and 1< i< 5. Every single component of this field may be expressed using a set of orthogonal idempotents.

$$D1=\frac{(A+m)+(B+n)}{4mn}$$

$$D2=\frac{(A+m)+(B-n)}{4mn}$$

$$D3=\frac{(A-m)+(B+n)}{4mn}$$

$$D1=\frac{(A-m)+(B-n)}{4mn}$$

It is easy to demonstrate that ∆ 2 i equals ∆i.

where 1 ≤ i, j ≤ 4, and i 6= j. Additionally, 0 = ∆i∆j, and ∆1 + ∆2 + ∆3 + ∆4 = 1. The formula that we are able to acquire is R = D1R ⊕ D2R ⊕ D3R ⊕ D4R = D1Fq ⊕ D2Fq ⊕ D3Fq ⊕ D4Fq, considering the Chinese the remains Theorem. Therefore, we can write X = A1 + A2u1 + A3m2 + A4m1m2 = D1X1 + D2X2 + D3X3 + D4X4, where Ai, Xi ∈ Fq and 1 ≤ i < 4. This allows us to represent every component X of R.

The Gray map η : R −→ F_q^{4n} is defined by η(D1X1 + D2X2 + D3X3 + D4X4) = (D1, D2, D3, D4)A

A GL4(Fq) is a constant matrix, and GL4(Fq) is the linear subgroup of all 4* 4 inverted matrix across the domain Fq such that AAT = eI44, where A T is the transposition of A and e Fq0. This defines the Grey map : R F 4 q.

Researchers are able to expand the linear Grey mapping from R^n to F_q^{4n} , where n is an even integer, component-wise. The Le weight for the component X = D1X1 + D2X2 + D3X3 + D4X4 ∈ R can be expressed as wL(X) = wH(η(X)), where wH is the Hamming is the weighted over Fq. We start our conversation with what follows Grey map (1) outcome is that.

Proposition 1. The map η : R −→ F_q^{4n} defined in (1) is an Fq-linear and distance-preserving map from (R n , dL) to (F_q^{4n}, dH), where dL = dH.

Proof. Let X, X 0 ∈ R^n such that X = D1X1 + D2X2 + D3X3 + D4X4.

and Xi , X_i' ∈ F_q^{4n} for 1 ≤ i ≤ 4. Then, we have η(X + X') = η(D1X1 + D1X_1' + D2X2 + D2X_2' + D3X3 + D3X_3' + D4X4 + D4X_4') = η(D1(X1 + X_1') + D2(X2 +X_2') + D3(D3 +X_3') + D4(D4 + X_4')) = (X1 + X_1' , X2 + X_2' , D3 + X_3' , D4 + X_4')A = (X1, X2, X3, X4)A + (X_1' , X_2' , X_3', X_4')A = η(X) + η(X') f or all X, X 0 ∈ Rn . Furthermore, for any α ∈ Fq, we have η(αX) = η(D1αX1 + D2αX2 + D3αX3 + D4αX4) = (αX1, αX2, αX3, αX4)A = α(X1, X2, X3, X4)A = αη(X) f or all X ∈ Rn .

η is therefore a Fq-linear. Regarding the latter, we are aware that dL(X, X') = wL(X – X') = wH(η(X –X')) = wH(η(X) − η(X')) = dH(η(X), η(X')).

Consequently, η is a map that preserves distance.

Define D1 ⊗ D2 ⊗ D3 ⊗ D4 = {(X1, X2, X3, X4) | Xi ∈ Di : 1 ≤ i ≤ 4} and D1 ⊕ D2 ⊕ D3 ⊕ D4 = {(X1 + X2 + X3 + X4) | Xi ∈ Di : 1 ≤ i ≤ 4}. Let C be a length n linear code over R. The reasecher define that C1 = {X1 ∈ F_q^{4n}| D1X1 + D2X2 + D3X3 + D4X4 ∈ C, where X2, X3, X4 ∈ F_q^{4n}}, C2 = {X2 ∈ F_q^{4n}| D1X1 + D2X2 + D3X3 + D4X4 ∈ C, where X1, X3, X4 ∈ F_q^{4n}}, C3 = {X3 ∈ F_q^{4n}| D1X1 + D2X2 + D3X3 + D4X4 ∈ C, where X1, X2, X4 ∈ F_q^{4n}}, and C4 = {D4 ∈ F_q^{4n} | D1X1 + D2X2 + D3X3 + D4X4 ∈ C, where X1, X2, X3 ∈ F_q^{4n}}.

Each Ci is now a linear code over Fq with length n. for 1 ≤ i ≤ 4. Therefore, any length of n linear code can be expressed as C = D1C1 ⊕ D2C2 ⊕ D3C3 ⊕ D4C4 and |C| = |C1||C2||C3||C4| over R. If a matrix's rows produce C, the matrix is referred to as a generator matrix of C. A generator matrix of C is M if Mi are the generator matrices of the linear code Ci for i = 1, 2, 3, 4, and so on. N= $\begin{pmatrix} D1N1 \\ D2N2 \\ D3N3 \\ D4N4 \end{pmatrix}$

and a η(C) generating matrix is

$$\eta\ (N)= \eta\begin{pmatrix} (D1N1) \\ D2N2 \\ D3N3 \\ D4N4 \end{pmatrix}$$

3.Conclusions

Several structural characteristics of periodic codes across the ring $R = F_q[M_1, N_2]/ \langle N^2{}_{1-\alpha 2}, N^2{}_{2-B2}, M_1N^2{}_{-N2}M_1\rangle$ are covered in this paper. Here, α and β denote non-zero members of Fq. Additionally, we produce quantum codes that are superior to those reported in [8–13]. We are able to receive LCD codes via the circle R as a programme. One can extend this research to the output of infinite circles. In order to examine new and improved quantum codes in the future, we believe our work will inspire viewers to look at these codes instead of other limit circles.

References

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

2. Grassl, M.; Beth, T. On optimal quantum codes. Int. J. Quantum Inf. 2004, 2, 55–64. [CrossRef].

3. Qian, J.; Ma, W.; Gou, W. Quantum codes from cyclic codes over finite ring. Int. J. Quantum Inf. 2009, 7, 1277–1283. [CrossRef].

4. Kai, X.; Zhu, S. Quaternary construction of quantum codes from cyclic codes over F4 + uF4. Int. J. Quantum Inf. 2011, 9, 689–700. [CrossRef].

5. Li, R.; Xu, Z.; Li, X. Binary construction of quantum codes of minimum distance three and four. IEEE Trans. Inf. Theory 2004, 50, 1331–1335. [CrossRef].

6. Gao, J. Quantum codes from cyclic codes over Fq + vFq + v2 Fq + v3 Fq. Int. J. Quantum Inf. 2015, 13, 1550063. [CrossRef].

7. Özen, M.; Özzaim, N.T.; Ince, H. Quantum codes from cyclic codes over F3 + uF3 + vF3 + uvF3. Int. Conf. Quantum Sci. Appl. J. Phys. Conf. Ser. 2016, 766, 012020-1–012020-6.

8. Ashraf, M.; Khan, N.; Mohammad, G. New Quantum and LCD Codes Over the Finite Field of Odd Characteristic. Int. J. Theor. Phys. 2021, 60, 2322–2332. [CrossRef].

9. Ashraf, M.; Mohammad, G. Quantum codes from cyclic codes over Fq + uFq + vFq + uvFq. Quantum Inf. Process. 2016, 15, 4089–4098. [CrossRef].

10. Ashraf, M.; Mohammad, G. Quantum codes over F0 p from cyclic codes over Fp[u, v]/hu2 1, v3 v, uv vui. Cryptogr. Commun. 2019, 11, 325–335. [CrossRef].

11. Bag, T.; Dinh, H.Q.; Upadhyay, A.K.; Yamaka, W. New non binary quantum codes from cyclic codes over product ring. IEEE Commun. Lett. 2019, 24, 486–490. [CrossRef]

12. Islam, H.; Prakash, O. Quantum codes from the cyclic codes over Fp[u, v, w]/hu2 1, v2 1, w2 1, uv vu, vw wv, wu uwi. J. Appl. Math. Comput. 2019, 60, 625–635. [CrossRef]

13. Dinh, H.Q.; Bag, T.; Upadhyay, A.K.; Ashraf, M.; Mohammad, G.; Chinnakum, W. Quantum codes from a class of constacyclic codes over finite commutative rings. J. Algebra Appl. 2020, 19, 2150003. [CrossRef].

14. Bag, T.; Upadhyay, A.K. Study on negacyclic codes over the ring Zp[u]/huk+1 ui. J. Appl. Math. Comput. 2019, 59, 693–700. [CrossRef].

15. Islam, H.; Prakash, O. New quantum and LCD codes over the finite field of even characteristic. Def. Sci. J. 2020, 71, 656–661. [CrossRef].

16. Massey, J.L. Linear codes with complementary duals. Discret. Math. 1992, 106, 337–342. [CrossRef].

17. Yang, X.; Massey, J.L. The condition for a cyclic code to have a complementary dual. Discret. Math. 1994, 126, 391–393. [CrossRef].

18. Islam, H.; Prakash, O. Construction of LCD and new quantum codes from cyclic codes over a finite non chain ring. Cryptogr. Commun. 2022, 14, 59–73. [CrossRef].

19. Bosma, W.; Cannon, J. Handbook of Magma Functions; University of Sydney: Sydney, Australia, 1995.

20. Aydin, N.; Liu, P.; Yoshino, B. A Database of Quantum Codes. 2021. Available online: http://quantumcodes.info/ (accessed on 7 August 2021).

21. Kumar, N., Kumar, V., & Aggarwal, A. (2022, October). Biorthogonality Collection of Finite System of Functions in Multiresolution Analysis on L 2 (K). In 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1-5). IEEE.