Bull. Aust. Math. Soc. **107** (2023), 330–341
doi:10.1017/S0004972722001344

GALOIS LCD CODES OVER $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$

ASTHA AGRAWAL✉, **GYANENDRA K. VERMA** and **R. K. SHARMA**

(Received 2 May 2022; accepted 10 October 2022; first published online 15 December 2022)

Abstract

Wu and Shi ['A note on k-Galois LCD codes over the ring $\mathbb{F}_q + u\mathbb{F}_q$', *Bull. Aust. Math. Soc.* **104**(1) (2021), 154–161] studied k-Galois LCD codes over the finite chain ring $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q$, where $u^2 = 0$ and $q = p^e$ for some prime p and positive integer e. We extend the results to the finite nonchain ring $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v$ and $uv = vu$. We define a correspondence between the l-Galois dual of linear codes over $\mathcal{R}$ and the l-Galois dual of their component codes over $\mathbb{F}_q$. Further, we construct Euclidean LCD and l-Galois LCD codes from linear codes over $\mathcal{R}$. We prove that any linear code over $\mathcal{R}$ is equivalent to a Euclidean code over $\mathbb{F}_q$ with $q > 3$ and an l-Galois LCD code over $\mathcal{R}$ with $0 < l < e$ and $p^{e-l} + 1 \mid p^e - 1$. Finally, we investigate MDS codes over $\mathcal{R}$.

2020 *Mathematics subject classification*: primary 94B05; secondary 94B99.

Keywords and phrases: linear code, Euclidean LCD code, l-Galois LCD code, Gray map, MDS code.

1. Introduction

An LCD code (shortened form for linear complementary dual code) is a linear code which intersects its dual trivially. LCD codes were defined and characterised by Massey [13] over finite fields. For a two-user binary adder channel, an optimal linear coding solution is obtained by LCD codes. LCD codes have applications in many areas including consumer electronics, data storage communication systems and cryptography. Yang and Massey [16] derived LCD cyclic codes. Carlet and Guilley [2] constructed several LCD codes and presented an implementation of binary LCD codes against fault injection and side channel attacks.

Carlet *et al.* [5] demonstrated that any linear code over $\mathbb{F}_q$ $(q > 3)$ is equivalent to a Euclidean LCD code and any linear code over $\mathbb{F}_{q^2}$ $(q > 2)$ is equivalent to a Hermitian LCD code. Carlet *et al.* [4] characterised binary LCD codes in terms of their orthogonal or symplectic basis and proved that almost all binary LCD codes are odd-like codes with odd-like duals. Fan and Zhang [7] generalised Euclidean

The first and second authors are supported by UGC, New Delhi, Govt. of India under grant DEC18-417932 and CSIR, New Delhi, Govt. of India under F. No. 09/086(1407)/2019-EMR-I, respectively.

and Hermitian inner products to the l-Galois inner product over finite fields and studied self-dual constacyclic codes for the l-Galois inner product over finite fields. Liu *et al.* [11] obtained l-Galois LCD codes over finite fields, where they characterised λ-constacyclic codes as l-Galois LCD codes. In [12], some criteria for a linear code to be an LCD code over a finite commutative ring were obtained.

A linear code C with parameters $[n, k, d]$ over a finite field is said to be a maximum distance separable (MDS) code if the minimum distance d of the code C attains the Singleton bound, that is, $d = n - k + 1$. MDS codes have very good theoretical and practical properties. Jin [8] used generalised Reed–Solomon codes to create numerous classes of LCD MDS codes. Extending this work, Chen [6] proposed an alternative method to construct new LCD MDS codes from generalised Reed–Solomon codes. Carlet *et al.* [3] discussed the existence of Euclidean LCD MDS codes over a finite field and gave several constructions of Euclidean and Hermitian LCD MDS codes. Li *et al.* [10] studied linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ for the Euclidean inner product and discussed some properties of Euclidean dual and MDS codes. Several authors investigated skew cyclic codes, constacyclic codes and quantum error correcting codes over the ring $\mathcal{R}$ [1, 9, 17]. Prakash *et al.* [14] enumerated self-dual and LCD double circulant codes over a class of finite commutative nonchain rings R_q and investigated the algebraic structure of 1-generator quasi-cyclic (QC) codes over R_q for $q = 3$. The l-Galois LCD codes over the finite chain ring $\mathbb{F}_q + u\mathbb{F}_q$ are studied in [15], showing that for any linear code over $\mathbb{F}_q + u\mathbb{F}_q$, there exist equivalent Euclidean and l-Galois LCD codes. Taking inspiration from [15], we consider l-Galois linear codes over the finite nonchain ring, $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ and characterise l-Galois LCD codes over this ring.

Section 2 contains the basic mathematical background we require. We define an inner product which is a generalisation of Euclidean and Hermitian inner products over $\mathcal{R}$. In Section 3, we construct l-Galois LCD codes over $\mathcal{R}$. We also discuss basic results on the Gray image of an l-Galois LCD code and its dual. In Section 4, we construct Euclidean and l-Galois LCD codes from linear codes over $\mathcal{R}$. Moreover, we demonstrate that a linear code over $\mathcal{R}$ is equivalent to a Euclidean and an l-Galois LCD code over $\mathcal{R}$. In Section 5, we look at MDS codes over $\mathcal{R}$ and give results connecting $C^{\perp_l}$ and C whenever one of them is an MDS code. The l-Galois LCD MDS codes over $\mathcal{R}$ seem worthy of further study.

2. Preliminaries

Throughout, q denotes a prime power, that is, $q = p^e$ for some integer $e > 0$, and $\mathbb{F}_q$ the finite field of order q. Let us consider the ring $\mathcal{R} = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q = \{a + ub + vc + uvd \mid u^2 = u, v^2 = v, uv = vu, a, b, c, d \in \mathbb{F}_q\}$. It is easy to see that $\mathcal{R}$ is a commutative principal ideal ring. Since it has four maximal ideals, it is a semi-local ring and a finite nonchain ring. Let $\gamma_1 = 1 - u - v + uv$, $\gamma_2 = uv$, $\gamma_3 = u - uv$, $\gamma_4 = v - uv$, so that $\sum_{i=1}^{4} \gamma_i = 1$, $\gamma_i^2 = \gamma_i$ and $\gamma_i\gamma_j = 0$ for $i \neq j$. By the Chinese remainder theorem, $\mathcal{R} = \gamma_1\mathcal{R} \oplus \gamma_2\mathcal{R} \oplus \gamma_3\mathcal{R} \oplus \gamma_4\mathcal{R}$ and $\gamma_i\mathcal{R} \cong \gamma_i\mathbb{F}_q$ for $i = 1, 2, 3, 4$. For any $a \in \mathcal{R}$,

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

a can be uniquely written as $a = \sum_{i=1}^{4} \gamma_i a_i$, where $a_i \in \mathbb{F}_q$ for $i = 1, 2, 3, 4$. Hence, $\mathcal{R} \cong \gamma_1\mathbb{F}_q \oplus \gamma_2\mathbb{F}_q \oplus \gamma_3\mathbb{F}_q \oplus \gamma_4\mathbb{F}_q$.

DEFINITION 2.1. A code C over $\mathcal{R}$ of length n is a nonempty subset of $\mathcal{R}^n$. The code C is said to be linear if it is an $\mathcal{R}$-submodule of $\mathcal{R}^n$.

DEFINITION 2.2. The Hamming weight $wt_H(x)$ of $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ is the number of nonzero x_i for $i \in \{1, 2, \ldots, n\}$. For $y \in \mathbb{F}_q^n$, the Hamming distance between x and y is the Hamming weight of the vector $x - y$.

DEFINITION 2.3. The Hamming distance of a code C, denoted by $d_H(C)$, is the number $d_H(C) = \min\{wt_H(x) \mid x \neq 0\}$.

DEFINITION 2.4. For $r = a_1 + a_2u + a_3v + a_4uv \in \mathcal{R}$, the Lee weight of r is $wt_L(r) = wt_H(a_1, a_1 + a_2, a_1 + a_3, a_1 + a_2 + a_3 + a_4)$. The definition of Lee weight can be extended to $\mathcal{R}^n$: for $s = (s_1, s_2, \ldots, s_n) \in \mathcal{R}^n$, the Lee weight of s is $wt_L(s) = \sum_{i=1}^{n} wt_L(s_i)$. If $t = (t_1, t_2, \ldots, t_n) \in \mathcal{R}^n$, then the Lee distance between the two vectors s and t is $d_L(s, t) = wt_L(s - t) = \sum_{i=1}^{n} wt_L(s_i - t_i)$.

DEFINITION 2.5. The Lee distance of the code C, denoted by $d_L(C)$, is the number $d_L(C) = \min\{d_L(s - t) \mid s \neq t\}$.

A function $\rho : \mathcal{R} \mapsto \mathbb{F}_q^4$ is a Gray map if it is bijective and distance preserving. From [17], the function $\rho : \mathcal{R} \to \mathbb{F}_q^4$ defined by

$$\rho(r) = \rho(a_1 + a_2u + a_3v + a_4uv) = (a_1, a_1 + a_2, a_1 + a_3, a_1 + a_2 + a_3 + a_4)$$

is a Gray map. An equivalent Gray map for $r = \sum_{i=1}^{4} \gamma_i r_i \in \mathcal{R}$, where $r_i \in \mathbb{F}_q$ for $i = 1, 2, 3, 4$, is

$$\rho(r) = \rho\Big(\sum_{i=1}^{4} \gamma_i r_i\Big) = (r_1, r_2, r_3, r_4).$$

We can easily extend this to a map from $\mathcal{R}^n$ to $\mathbb{F}_q^{4n}$. By the definition of the Gray map, ρ is linear over $\mathbb{F}_q$ and it preserves distance from $(\mathcal{R}^n, d_L)$ to $(\mathbb{F}_q^{4n}, d_H)$, where d_L is the Lee distance and d_H is the Hamming distance. The following result can be obtained directly from the definition of ρ.

PROPOSITION 2.6. *For a linear code C of length n over the ring $\mathcal{R}$ with cardinality q^k and Lee distance d, $\rho(C)$ is a $[4n, k, d]$ linear code over $\mathbb{F}_q$.*

Define a Frobenius operator $F : \mathcal{R} \to \mathcal{R}$ over $\mathcal{R}$ by

$$F(a_1 + a_2u + a_3v + a_4uv) = a_1^p + ua_2^p + va_3^p + uva_4^p.$$

Equivalently, $F(r) = \gamma_1 r_1^p + \gamma_2 r_2^p + \gamma_3 r_3^p + \gamma_4 r_4^p$ for $r = \sum_{i=1}^{4} \gamma_i r_i \in \mathcal{R}$.

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

For $s = (s_1, s_2, \ldots, s_n)$ and $t = (t_1, t_2, \ldots, t_n) \in \mathcal{R}^n$ and $0 \le l \le e-1$, define the l-Galois inner product,

$$[s,t]_l = \sum_{i=1}^{n} s_i F^l(t_i).$$

REMARK 2.7. This inner product is a generalisation of the Euclidean and Hermitian inner products for $l = 0$ and $l = e/2$ (when e is even), respectively.

From now on, we write $[s,t], [s,t]_H$ and $[s,t]_l$ for the Euclidean, Hermitian and l-Galois inner product over $\mathcal{R}$ and $\langle s,t\rangle, \langle s,t\rangle_H$ and $\langle s,t\rangle_l$ for the Euclidean, Hermitian and l-Galois inner product over $\mathbb{F}_q$, respectively. The l-Galois dual code $C^{\perp_l}$ of C over $\mathcal{R}$ is defined by

$$C^{\perp_l} = \{s \in \mathcal{R}^n \mid [t,s]_l = 0 \text{ for all } t \in C\}.$$

Clearly, $C^{\perp_l}$ is a linear code over $\mathcal{R}$. A linear code over $\mathcal{R}$ is said to be l-Galois LCD if $C \cap C^{\perp_l} = \{0\}$. It is well known that for a Frobenius ring $\mathcal{R}$ and a linear code C over the ring $\mathcal{R}$ of length n, the product of the cardinalities of C and $C^{\perp_l}$ is equal to the cardinality of $\mathcal{R}^n$, that is, $|C||C^{\perp_l}| = |\mathcal{R}^n|$.

REMARK 2.8. For $l = 0$ and $l = e/2$ (when e is even), this construction gives the Euclidean and the Hermitian dual code, respectively.

3. l-Galois linear codes over $\mathcal{R}$

In this section, we derive a necessary and sufficient condition for C to be an l-Galois LCD code over $\mathcal{R}$ with respect to its component codes. Also, we give a relationship between an l-Galois LCD code and its Gray image.

A linear code C over $\mathcal{R}$ can be decomposed into four component codes over the finite field $\mathbb{F}_q$ as follows:

$$\begin{aligned}
C_1 &= \{x \in \mathbb{F}_q^n \mid \gamma_1 x + \gamma_2 y + \gamma_3 z + \gamma_4 w \in C \text{ for some } y, z, w \in \mathbb{F}_q^n\},\\
C_2 &= \{y \in \mathbb{F}_q^n \mid \gamma_1 x + \gamma_2 y + \gamma_3 z + \gamma_4 w \in C \text{ for some } x, z, w \in \mathbb{F}_q^n\},\\
C_3 &= \{z \in \mathbb{F}_q^n \mid \gamma_1 x + \gamma_2 y + \gamma_3 z + \gamma_4 w \in C \text{ for some } x, y, w \in \mathbb{F}_q^n\},\\
C_4 &= \{w \in \mathbb{F}_q^n \mid \gamma_1 x + \gamma_2 y + \gamma_3 z + \gamma_4 w \in C \text{ for some } x, y, z \in \mathbb{F}_q^n\}.
\end{aligned}$$

The C_i are linear codes over $\mathbb{F}_q$ for $1 \le i \le 4$ and $C = \gamma_1 C_1 \oplus \gamma_2 C_2 \oplus \gamma_3 C_3 \oplus \gamma_4 C_4$. We say C_1, C_2, C_3 and C_4 are component codes of the linear code C. The cardinality of a linear code C is the product of the cardinalities of its component codes, that is,

$$|C| = |C_1||C_2||C_3||C_4|.$$

The Lee distance of a linear code C is the minimum of the Hamming distances of its component codes,

$$d_L(C) = \min_{1 \le i \le 4} \{d_H(C_i)\}.$$

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

Let $C^{p^l} = \{(F^l(c_1), F^l(c_2), \ldots, F^l(c_n)) \mid (c_1, c_2, \ldots, c_n) \in C\}$ and $F^l(G) = (F^l(g_{ij}))$ for a matrix $G = (g_{ij})$ over $\mathcal{R}$. For $1 \le i \le 4$, let G_i be the generator matrix for C_i. Then the generator matrices for C and $\rho(C)$ are

$$G = \begin{bmatrix} \gamma_1 G_1 \\ \gamma_2 G_2 \\ \gamma_3 G_3 \\ \gamma_4 G_4 \end{bmatrix} \quad \text{and} \quad \rho(G) = \begin{bmatrix} \rho(\gamma_1 G_1) \\ \rho(\gamma_2 G_2) \\ \rho(\gamma_3 G_3) \\ \rho(\gamma_4 G_4) \end{bmatrix},$$

where $\rho(\gamma_i G_i)$ is a matrix over $\mathbb{F}_q$ for $1 \le i \le 4$. Since $\gamma_i \gamma_j = 0$ for $i \ne j$ and $\gamma_i^2 = \gamma_i$ for $i = 1, 2, 3, 4$,

$$G(F^{e-l}(G))^T = \begin{bmatrix} \gamma_1 G_1 F^{e-l}(G_1)^T & 0 & 0 & 0 \\ 0 & \gamma_2 G_2 F^{e-l}(G_2)^T & 0 & 0 \\ 0 & 0 & \gamma_3 G_3 F^{e-l}(G_3)^T & 0 \\ 0 & 0 & 0 & \gamma_4 G_4 F^{e-l}(G_4)^T \end{bmatrix}.$$

We call C an $[n, k, d]$ code over $\mathcal{R}$ if C is a code of length n, $|C| = q^k$ and d is the Lee distance. If the C_i are the component codes of C, with parameters $[n, k_i, d_i]$ for $i = 1, 2, 3, 4$, then $k = \sum_{i=1}^4 k_i$ and $d = \min_{1 \le i \le 4}\{d_i\}$.

In the following lemma, we observe that the Euclidean dual of $C^{p^{(e-l)}}$ is equal to the l-Galois dual code of C.

LEMMA 3.1. *If C is an $[n, k, d]$ linear code over $\mathcal{R}$, then $C^{p^{(e-l)}}$ is an $[n, k, d]$ linear code over $\mathcal{R}$ and $C^{\perp_l} = (C^{p^{(e-l)}})^{\perp}$. Moreover, if C has generator matrix G, then $F^{e-l}(G)$ is a generator matrix of $C^{p^{(e-l)}}$.*

The next theorem gives the decomposition of the l-Galois dual code into its component codes. Consequently, we obtain a relation between l-Galois LCD codes over $\mathcal{R}$ and l-Galois LCD component codes over $\mathbb{F}_q$.

THEOREM 3.2. *For a linear code $C = \bigoplus_{i=1}^4 \gamma_i C_i$ over $\mathcal{R}$:*

(1) $C^{\perp_l} = \bigoplus_{i=1}^4 \gamma_i C_i^{\perp_l}$;
(2) *C is an l-Galois LCD code over $\mathcal{R}$ if and only if all its component codes C_i are l-Galois LCD codes over $\mathbb{F}_q$ for $1 \le i \le 4$;*
(3) *C is an l-Galois self-orthogonal linear code over $\mathcal{R}$ if and only if all its component codes C_i are l-Galois self-orthogonal codes over $\mathbb{F}_q$ and C is a self-dual code if and only if all its component codes C_i are self-dual codes over $\mathbb{F}_q$ for $1 \le i \le 4$.*

PROOF. (1) If $x = \gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3 + \gamma_4 x_4 \in C^{\perp_l}$, then $[y, x]_l = 0$ for any $y = \gamma_1 y_1 + \gamma_2 y_2 + \gamma_3 y_3 + \gamma_4 y_4 \in C$. Since $\gamma_i^2 = \gamma_i$ and $\gamma_i \gamma_j = 0$ for $i \ne j$, $[y, x]_l = \gamma_1 \langle y_1, x_1 \rangle_l + \gamma_2 \langle y_2, x_2 \rangle_l + \gamma_3 \langle y_3, x_3 \rangle_l + \gamma_4 \langle y_4, x_4 \rangle_l$. Thus, $\langle y_i, x_i \rangle_l = 0$ for all $y_i \in C_i$ and $i = 1, 2, 3, 4$, that is, $x_i \in C_i^{\perp_l}$ for $i = 1, 2, 3, 4$. Therefore, $x \in \gamma_1 C_1^{\perp_l} \oplus \gamma_2 C_2^{\perp_l} \oplus \gamma_3 C_3^{\perp_l} \oplus \gamma_4 C_4^{\perp_l}$.

Conversely, let $w = \gamma_1 w_1 + \gamma_2 w_2 + \gamma_3 w_3 + \gamma_4 w_4 \in \gamma_1 C_1^{\perp_l} \oplus \gamma_2 C_2^{\perp_l} \oplus \gamma_3 C_3^{\perp_l} \oplus \gamma_4 C_4^{\perp_l}$, where $w_i \in C_i^{\perp_l}$. For any $y = \gamma_1 y_1 + \gamma_2 y_2 + \gamma_3 y_3 + \gamma_4 y_4 \in C$, where $y_i \in C_i$, $[y, w]_l =$

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

$\gamma_1\langle y_1, w_1\rangle_l + \gamma_2\langle y_2, w_2\rangle_l + \gamma_3\langle y_3, w_3\rangle_l + \gamma_4\langle y_4, w_4\rangle_l = 0$, which implies that $w \in C^{\perp_l}$. Hence, $C^{\perp_l} = \gamma_1 C_1^{\perp_l} \oplus \gamma_2 C_2^{\perp_l} \oplus \gamma_3 C_3^{\perp_l} \oplus \gamma_4 C_4^{\perp_l}$.

(2) Suppose that C is an l-Galois LCD code over $\mathcal{R}$, that is, $C \cap C^{\perp_l} = \{0\}$. Let $x_i \in C_i \cap C_i^{\perp_l}$ for some $i = 1, 2, 3, 4$, that is, $\langle y_i, x_i\rangle_l = 0$ for all $y_i \in C_i$. Now take $x = \gamma_i x_i \in C$. Then for any $y = \gamma_1 y_1 + \gamma_2 y_2 + \gamma_3 y_3 + \gamma_4 y_4 \in C$, where $y_j \in C_j$ for $j = 1, 2, 3, 4$, $[y, x]_l = [\gamma_1 y_1 + \gamma_2 y_2 + \gamma_3 y_3 + \gamma_4 y_4, \gamma_i x_i]_l = \gamma_i\langle y_i, x_i\rangle_l = 0$, since $\gamma_i^2 = \gamma_i$ and $\gamma_i\gamma_j = 0$ for $i \neq j$. This implies that $x \in C \cap C^{\perp_l} = \{0\}$, that is, $x = 0$, consequently, $x_i = 0$. Hence, C_i is an l-Galois LCD code over $\mathbb{F}_q$.

Conversely, suppose the C_i are l-Galois LCD codes over $\mathbb{F}_q$ for $i = 1, 2, 3, 4$. Let $x = \gamma_1 x_1 + \gamma_2 x_2 + \gamma_2 x_3 + \gamma_4 x_4 \in C \cap C^{\perp_l}$. Then $x_i \in C_i \cap C_i^{\perp_l}$ and $C_i \cap C_i^{\perp_l} = \{0\}$, which implies that $x = 0$. Thus, C is an l-Galois LCD code.

The proof of part (3) follows easily from part (1), so we omit the proof. □

REMARK 3.3. Parts (1) and (3) in Theorem 3.2 have been proved for the Euclidean dual over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ in [10].

The next corollary gives a necessary and sufficient condition for an l-Galois LCD code over $\mathcal{R}$ in terms of generator matrices.

COROLLARY 3.4. *Let $C = \bigoplus_{i=1}^{4} \gamma_i C_i$ with generator matrix*

$$G = \begin{bmatrix} \gamma_1 G_1 \\ \gamma_2 G_2 \\ \gamma_3 G_3 \\ \gamma_4 G_4 \end{bmatrix},$$

where G_i is a generator matrix for C_i over $\mathbb{F}_q$. Then, C is an l-Galois LCD code over $\mathcal{R}$ if and only if the matrix $G_i(F^{e-l}(G_i))^T$ is nonsingular for $i = 1, 2, 3, 4$ over $\mathbb{F}_q$.

PROOF. By Theorem 3.2, C is an l-Galois LCD code if and only if the C_i are l-Galois LCD codes over $\mathbb{F}_q$. From [11, Theorem 2.4], C_i is an l-Galois LCD code if and only if $G_i(F^{e-l}(G_i))^T$ is nonsingular over $\mathbb{F}_q$. □

Now, by using the definition of ρ, we derive some useful properties of the Gray image of l-Galois dual codes over $\mathcal{R}$.

LEMMA 3.5. *If C is an $[n, k]$ linear code over $\mathcal{R}$, then $\rho(C^{\perp_l}) = \rho(C)^{\perp_l}$.*

PROOF. If $\rho(x) \in \rho(C^{\perp_l})$, where $x \in C^{\perp_l}$, then $[z, x]_l = 0$ for all $z \in C$. Let $z = \sum_{i=1}^{4} \gamma_i z_i$ and $x = \sum_{i=1}^{4} \gamma_i x_i$, where $z_i \in C_i$ and $x_i \in C_i^{\perp_l}$, so that $[z, x]_l = \gamma_1\langle z_1, x_1\rangle_l + \gamma_2\langle z_2, x_2\rangle_l + \gamma_3\langle z_3, x_3\rangle_l + \gamma_4\langle z_4, x_4\rangle_l = 0$. Hence, $\langle z_i, x_i\rangle_l = 0$ for $i = 1, 2, 3, 4$. Now, $\langle \rho(z), \rho(x)\rangle_l = \sum_{i=1}^{4} z_i \cdot x_i^{p^l} = \sum_{i=1}^{4}\langle z_i, x_i\rangle_l = 0$ for all $\rho(z) \in \rho(C)$. Thus, $\rho(x) \in \rho(C)^{\perp_l}$. Therefore, $\rho(C^{\perp_l}) \subseteq \rho(C)^{\perp_l}$.

Conversely, the cardinality of $\rho(C^{\perp_l})$ is equal to $C^{\perp_l}$, that is, $|\rho(C^{\perp_l})| = q^{4n}/|C|$. Moreover, $|\rho(C)^{\perp_l}| = q^{4n}/|\rho(C)| = q^{4n}/|C|$. Hence, $\rho(C^{\perp_l}) = \rho(C)^{\perp_l}$. □

LEMMA 3.6. *If C is a linear code over $\mathcal{R}$, then $\rho(C \cap C^{\perp_l}) = \rho(C) \cap \rho(C^{\perp_l})$.*

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

PROOF. If $\rho(x) \in \rho(C \cap C^{\perp_l})$ for some $x \in C \cap C^{\perp_l}$, then $\rho(x) \in \rho(C) \cap \rho(C^{\perp_l})$. Hence, $\rho(C \cap C^{\perp_l}) \subseteq \rho(C) \cap \rho(C^{\perp_l})$. Conversely, if $y \in \rho(C) \cap \rho(C^{\perp_l})$, then $y \in \rho(C)$ and $y \in \rho(C^{\perp_l})$. Since ρ is bijective, there is a unique $x \in C \cap C^{\perp_l}$ such that $\rho(x) = y$. Hence, $\rho(C) \cap \rho(C^{\perp_l}) \subseteq \rho(C \cap C^{\perp_l})$. Therefore, $\rho(C \cap C^{\perp_l}) = \rho(C) \cap \rho(C^{\perp_l})$. □

THEOREM 3.7. *A linear code C is an l-Galois LCD code over $\mathcal{R}$ if and only if $\rho(C)$ is an l-Galois LCD code over $\mathbb{F}_q$.*

PROOF. Suppose C is an l-Galois LCD code over $\mathcal{R}$, that is, $C \cap C^{\perp_l} = \{0\}$. From Lemma 3.6, $\rho(C) \cap \rho(C)^{\perp_l} = \{0\}$. Conversely, if $\rho(C)$ is an l-Galois LCD code, then

$$\{0\} = \rho(C) \cap \rho(C)^{\perp_l} = \rho(C) \cap \rho(C^{\perp_l}) = \rho(C \cap C^{\perp_l}),$$

so that $C \cap C^{\perp_l} = \{0\}$. Therefore, C is an l-Galois LCD code over $\mathcal{R}$. □

4. Construction of a Galois LCD code equivalent to a linear code

We give a construction of Euclidean and l-Galois LCD codes over $\mathcal{R}$ with the help of their component codes over $\mathbb{F}_q$. We show that for every linear code C, there exists a Euclidean LCD code and an l-Galois LCD code which are equivalent to C.

Let m and w be integers with $m \geq 1$ and $0 \leq w \leq m$ and let b be an element in $\mathbb{F}_q^m$ with Hamming weight w. The support of b is the set $S = \{i_1, i_2, \ldots, i_w\}$ of indices at which the components of b are nonzero. Denote the $m \times m$ diagonal matrix whose entries are $b_1, b_2, \ldots, b_m$ by $\mathrm{diag}_m[b]$. For an $m \times m$ square matrix P over $\mathbb{F}_q$, let P_S denote the submatrix of P obtained by deleting the $i_1, i_2, \ldots, i_w$th columns and rows of P. We write $P_S = I$ if $S = \{1, 2, \ldots, m\}$ and $P_\emptyset = P$.

LEMMA 4.1 [5]. *Let P be an $m \times m$ matrix over $\mathbb{F}_q$ and t an integer with $0 \leq t \leq m-1$. Assume that $\det(P_J) = 0$ for any $J \subseteq \{1, 2, \ldots, m\}$ with $0 \leq |J| \leq t$. Then for every element $b \in \mathbb{F}_q^m$ with support S and Hamming weight w such that $1 \leq w \leq t+1$,*

$$\det\left(P + \mathrm{diag}_m[b]\right) = \left(\prod_{i \in S} b_i\right) \det(P_S).$$

Fix $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}^n$, where $\alpha_j = \sum_{i=1}^{4} \gamma_i \alpha_{ji}$, $\alpha_{ji} \in \mathbb{F}_q$ for $j = 1, 2, \ldots, n$. Define

$$C^\alpha = \{\alpha \cdot c \mid c \in C\} = \{(\alpha_1 c_1, \alpha_2 c_2, \ldots, \alpha_n c_n) \mid (c_1, c_2, \ldots, c_n) \in C\}.$$

Clearly, C^α is a linear code over $\mathcal{R}$. Let

$$G = \begin{bmatrix} \gamma_1 G_1 \\ \gamma_2 G_2 \\ \gamma_3 G_3 \\ \gamma_4 G_4 \end{bmatrix} \quad \text{and} \quad G^\alpha = \begin{bmatrix} \gamma_1 G_1^{\alpha_1'} \\ \gamma_2 G_2^{\alpha_2'} \\ \gamma_3 G_3^{\alpha_3'} \\ \gamma_4 G_4^{\alpha_4'} \end{bmatrix}$$

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

be generator matrices for C and C^α, where G^α is obtained by multiplying the jth column of G by α_j and $G_i^{\alpha_i'}$ is the matrix obtained by multiplying the jth column of G_i by α_{ji} and $\alpha_i' = (\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}) \in \mathbb{F}_q^n$ for $i = 1, 2, 3, 4$.

REMARK 4.2. Note that, if $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}^n$ and $\alpha_j \neq 0$ for $1 \leq j \leq n$, then C and C^α are equivalent codes over $\mathcal{R}$.

The following theorem gives a construction of Euclidean LCD codes over $\mathcal{R}$ from linear codes over $\mathcal{R}$. We denote the parameters of the component codes C_i by $[n, k_i, d_i]$ for $i = 1, 2, 3, 4$.

THEOREM 4.3. *All notation is as above. Let $C = \bigoplus_{i=1}^4 \gamma_i C_i$ be an $[n, k, d]$ linear code over $\mathcal{R}$, where the component codes C_i over $\mathbb{F}_q$ have generator matrices $G_i = [I_{k_i} : M_i]$. Let $P_i = G_i G_i^T$ and $t_i \leq k_i - 1$ be nonnegative integers such that $\det((P_i)_{S_i}) = 0$ for any $S_i \subseteq \{1, 2, \ldots, k_i\}$ with $0 \leq |S_i| \leq t_i$ and assume there exist $R_i \subseteq \{1, 2, \ldots, k_i\}$ with cardinality $t_i + 1$ such that $\det((P_i)_{R_i}) \neq 0$. If $\alpha \in \mathcal{R}^n$ is such that $\alpha_{ji} \in \mathbb{F}_q \setminus \{+1, -1\}$ if $j \in R_i$ and $\alpha_{ji} \in \{+1, -1\}$ if $j \in \{1, 2, \ldots, n\} \setminus R_i$ for $i = 1, 2, 3, 4$, then C^α is a Euclidean LCD code over $\mathcal{R}$.*

PROOF. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}^n$ and $c = (c_1, c_2, \ldots, c_n) \in C$. For $\alpha_j, c_j \in \mathcal{R}$, we write $\alpha_j = \sum_{i=1}^4 \gamma_i \alpha_{ji}$, $\alpha_{ji} \in \mathbb{F}_q$, and $c_j = \sum_{i=1}^4 \gamma_i c_{ji}$, $c_{ji} \in C_i$. We note that $\alpha_j c_j = (\sum_{i=1}^4 \gamma_i \alpha_{ji})(\sum_{i=1}^4 \gamma_i c_{ji}) = \sum_{i=1}^4 \gamma_i \alpha_{ji} c_{ji}$, since $\gamma_i \gamma_m = 0$ for $i \neq m$ and $\gamma_i^2 = \gamma_i$ for $i, m = 1, 2, 3, 4$ and $j = 1, 2, \ldots, n$. Now,

$$\begin{aligned} C^\alpha &= \{(\alpha_1 c_1, \alpha_2 c_2, \ldots, \alpha_n c_n) \mid (c_1, c_2, \ldots, c_n) \in C\} \\ &= \left\{ \left(\sum_{i=1}^4 \gamma_i \alpha_{1i} c_{1i}, \sum_{i=1}^4 \gamma_i \alpha_{2i} c_{2i}, \ldots, \sum_{i=1}^4 \gamma_i \alpha_{ni} c_{ni} \right) \mid (c_1, c_2, \ldots, c_n) \in C \right\} \\ &= \left\{ \sum_{i=1}^4 \gamma_i (\alpha_{1i} c_{1i}, \alpha_{2i} c_{2i}, \alpha_{3i} c_{3i}, \ldots, \alpha_{ni} c_{ni}) \mid (c_1, c_2, \ldots, c_n) \in C \right\} = \bigoplus_{i=1}^4 \gamma_i C_i^{\alpha_i'}. \end{aligned}$$

Here, $C_i^{\alpha_i'} = \{(\alpha_{1i} c_{1i}, \alpha_{2i} c_{2i}, \alpha_{3i} c_{3i}, \ldots, \alpha_{ni} c_{ni}) \mid (c_{1i}, c_{2i}, \ldots, c_{ni}) \in C_i\}$ and $\alpha_i' = (\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni})$. Clearly, the $C_i^{\alpha_i'}$ are linear codes over $\mathbb{F}_q$ with generator matrices $G_i^{\alpha_i'}$ for $i = 1, 2, 3, 4$. Also, $\alpha = \sum_{i=1}^4 \gamma_i \alpha_i'$. From [5, Theorem 5.1], each $C_i^{\alpha_i'}$ is a Euclidean LCD code over $\mathbb{F}_q$ and by Theorem 3.2 (with $l = 0$), C^α is a Euclidean LCD code. □

Next, we use the technique described in [5] to establish the existence of α for which C^α is a Euclidean LCD code for a given linear code C over $\mathcal{R}$.

COROLLARY 4.4. *Let $\mathbb{F}_q$ $(q > 3)$ be a finite field and C be an $[n, k, d]$ linear code over $\mathcal{R}$. Then C^α is an $[n, k, d]$ Euclidean LCD code over $\mathcal{R}$ for some $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ in $\mathcal{R}^n$ with $\alpha_j \neq 0$ for $1 \leq j \leq n$.*

PROOF. Let $C = \bigoplus_{i=1}^4 \gamma_i C_i$ be a linear code over $\mathcal{R}$. If C is a Euclidean LCD code, then we can take $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}^n$ such that $\alpha_j = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$ for $1 \leq j \leq n$. Then, $C^\alpha = C$, a Euclidean LCD code over $\mathcal{R}$.

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

If C is not a Euclidean LCD code, then by Theorem 3.2, C_i is not a Euclidean LCD code for some $i = 1, 2, 3, 4$. If G_i is the generator matrix for C_i, then $\det(G_i G_i^T) = 0$. Set $P_i = G_i G_i^T$. There exists an integer $t_i \geq 0$ and $R_i \subseteq \{1, 2, \ldots, k_i\}$ with cardinality $|R_i| = t_i + 1$ such that $\det((P_i)_{R_i}) \neq 0$ and $\det((P_i)_{S_i}) = 0$ for any $S_i \subseteq \{1, 2, \ldots, k_i\}$ with $0 \leq |S_i| \leq t_i$. Also, $\mathbb{F}_q^* \setminus \{-1, 1\} \neq \emptyset$ since $q > 3$. Choose $\alpha_i' = (\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}) \in \mathbb{F}_q^n$ such that $\alpha_{ji} \in \mathbb{F}_q^* \setminus \{-1, 1\}$ if $j \in R_i$ and $\alpha_{ji} = 1$ if $j \in \{1, 2, \ldots, k_i\} \setminus R_i$. By [5, Theorem 5.1], $C_i^{\alpha_i'}$ is a Euclidean LCD code over $\mathbb{F}_q$. Take $\alpha = \sum_{m=1}^{4} \gamma_m \alpha_m' \in \mathcal{R}^n$, where $\alpha_m' = \alpha_i'$ for $m = i$ and $\alpha_m' = (1, 1, \ldots, 1)$ for $m \neq i$. Then by Theorem 4.3, $C^\alpha = \bigoplus_{m=1}^{4} \gamma_m C_m^{\alpha_m'}$ is an $[n, k, d]$ Euclidean LCD code over $\mathcal{R}$. □

Next, we construct an l-Galois LCD code from a given linear code over a finite field. Then similarly, we provide the construction over $\mathcal{R}$.

THEOREM 4.5. *Let $\mathbb{F}_q$ $(q = p^e)$ be a finite field. For $0 < l < e$ and $p^{e-l} + 1 \mid p^e - 1$, set $\beta = (p^e - 1)/(p^{e-l} + 1)$. Let $G = [I_k : M]$ be a generator matrix for a linear code C over $\mathbb{F}_q$ with parameters $[n, k, d]$ and denote the matrix $G(F^{e-l}(G))^T$ by P. Let t with $0 \leq t \leq k - 1$ be an integer such that $\det(P_I) = 0$ for any $I \subseteq \{1, 2, \ldots, k\}$ with $0 \leq |I| \leq t$, and assume there exist $J \subseteq \{1, 2, \ldots, k\}$ with cardinality $t + 1$ such that $\det(P_J) \neq 0$. Suppose $a \in \mathbb{F}_q^n$ such that $a_j \in \mathbb{F}_q \setminus (\mathbb{F}_q^*)^\beta$ for $j \in J$ and $a_j \in (\mathbb{F}_q^*)^\beta$ for $j \in \{1, 2, \ldots, n\} \setminus J$. Then, C^a is an l-Galois LCD code over $\mathbb{F}_q$.*

PROOF. A generator matrix G^a for C^a is obtained by multiplying the jth column of the matrix $G = [I_k : M = (m_{is})]$ by a_j for $1 \leq j \leq n$. The (ij)th entry of $G^a(F^{e-l}(G^a))^T$ is $a_i^{p^{e-l}+1} + \sum_{s=1}^{n-k} a_{k+s}^{p^{e-l}+1} m_{is}^{p^{e-l}+1}$ if $i = j$ and $\sum_{s=1}^{n-k} a_{k+s}^{p^{e-l}+1} m_{is} m_{js}^{p^{e-l}}$ if $i \neq j$. Since $a_{k+s} \notin J$, $a_{k+s}^{p^{e-l}+1} = 1$ for $1 \leq s \leq n - k$. The (ij)th entry of $G^a(F^{e-l}(G^a))^T$ is $a_i^{p^{e-l}+1} + \sum_{s=1}^{n-k} m_{is}^{p^{e-l}+1}$ if $i = j$ and $\sum_{s=1}^{n-k} m_{is} m_{js}^{p^{e-l}}$ if $i \neq j$. The (ij)th entry of $G(F^{e-l}(G))^T$ is $1 + \sum_{s=1}^{n-k} m_{is}^{p^{e-l}+1}$ if $i = j$ and $\sum_{s=1}^{n-k} m_{is} m_{js}^{p^{e-l}}$ if $i \neq j$. Hence, $G^a(F^{e-l}(G^a))^T = G(F^{e-l}(G))^T + \mathrm{diag}_k[b]$, where $b = (a_1^{p^{e-l}+1} - 1, a_2^{p^{e-l}+1} - 1, \ldots, a_k^{p^{e-l}+1} - 1)$. Note that the support of b is the set J. By Lemma 4.1, $\det(G^a(F^{e-l}(G^a))^T) = \det(P + \mathrm{diag}_k[b]) = (\prod_{j \in J} b_j) \det(P_J) \neq 0$. Hence, C^a is an l-Galois LCD code over $\mathbb{F}_q$. □

THEOREM 4.6. *All notation is as above. For $0 < l < e$ and $p^{e-l} + 1 \mid p^e - 1$, set $\beta = (p^e - 1)/(p^{e-l} + 1)$. Let $C = \bigoplus_{i=1}^{4} \gamma_i C_i$ be an $[n, k, d]$ linear code over $\mathcal{R}$, where the C_i are the component codes over $\mathbb{F}_q$ with generator matrices G_i. Let $P_i = G_i(F^{e-l}(G_i))^T$ and $0 \leq t_i \leq k_i - 1$ be an integer such that $\det((P_i)_{S_i}) = 0$ for any $S_i \subseteq \{1, 2, \ldots, k_i\}$ with $0 \leq |S_i| \leq t_i$ and assume there exist $R_i \subseteq \{1, 2, \ldots, k_i\}$ with cardinality $t_i + 1$ such that $\det((P_i)_{R_i}) \neq 0$. Suppose $\alpha \in \mathcal{R}^n$ such that $\alpha_{ji} \in \mathbb{F}_q \setminus (\mathbb{F}_q^*)^\beta$ for all $j \in R_i$ and $\alpha_{ji} \in (\mathbb{F}_q^*)^\beta$ for all $j \in \{1, 2, \ldots, n\} \setminus R_i$, for $i = 1, 2, 3, 4$. Then, C^α is an l-Galois LCD code over $\mathcal{R}$.*

PROOF. Since $C^\alpha = \bigoplus_{i=1}^{4} \gamma_i C_i^{\alpha_i'}$, where $\alpha_i' = (\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}) \in \mathbb{F}_q^n$ and the $C_i^{\alpha_i'}$ are linear codes over $\mathbb{F}_q$ with generator matrices $G_i^{\alpha_i'}$, by Theorem 4.5, the $C_i^{\alpha_i'}$ are l-Galois

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

LCD codes over $\mathbb{F}_q$ for $i = 1, 2, 3, 4$. Therefore, by Theorem 3.2, C^α is an l-Galois LCD code over $\mathcal{R}$. □

The following corollary shows the existence of α for which C^α is an l-Galois LCD code equivalent to the linear code C over $\mathcal{R}$.

COROLLARY 4.7. *Let $\mathbb{F}_q$ ($q = p^e$) be a finite field. For $0 < l < e$ and $p^{e-l} + 1 \mid p^e - 1$, set $\beta = (p^e - 1)/(p^{e-l} + 1)$ ($\beta > 1$). Let C be an $[n, k, d]$ linear code over the ring $\mathcal{R}$. Then, C^α is an $[n, k, d]$ l-Galois LCD code over the ring $\mathcal{R}$ for some $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}^n$ with $\alpha_j \neq 0$ for $1 \leq j \leq n$.*

PROOF. Let $C = \bigoplus_{i=1}^{4} \gamma_i C_i$ be a linear code over $\mathcal{R}$. Take $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{R}^n$, where $\alpha_j = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$ for $1 \leq j \leq n$, if C is l-Galois LCD code over $\mathcal{R}$. Then, $C^\alpha = C$, which is an l-Galois LCD code over $\mathcal{R}$.

If C is not an l-Galois LCD code, then by Theorem 3.2, C_i is not an l-Galois LCD code for some $1 \leq i \leq 4$. If G_i is the generator matrix for C_i, then $\det(G_i(F^{e-l}(G_i))^T) = 0$. Let $P_i = G_i(F^{e-l}(G_i))^T$. Then there exists an integer $t_i \geq 0$ and $R_i \subseteq \{1, 2, \ldots, k_i\}$ with cardinality $|R_i| = t_i + 1$ such that $\det((P_i)_{R_i}) \neq 0$ and $\det((P_i)_{S_i}) = 0$ for any $S_i \subseteq \{1, 2, \ldots, k_i\}$ with cardinality $0 \leq |S_i| \leq t_i$. Also, since $\beta > 1$, $\mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^\beta \neq \emptyset$. Choose $\alpha_i' = (\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}) \in \mathbb{F}_q^n$ such that $\alpha_{ji} \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^\beta$ for $j \in R_i$ and $\alpha_{ji} = 1$ for $j \in \{1, 2, \ldots, k_i\} \setminus R_i$. By Theorem 4.5, $C_i^{\alpha_i'}$ is l-Galois LCD code over $\mathbb{F}_q$. Take $\alpha = \sum_{m=1}^{4} \gamma_m \alpha_m' \in \mathcal{R}^n$, where $\alpha_m' = \alpha_i'$ for $m = i$ and $\alpha_m' = (1, 1, \ldots, 1)$ for $m \neq i$. By Theorem 4.6, C^α is an $[n, k, d]$ l-Galois LCD code over the ring $\mathcal{R}$. □

5. MDS codes over $\mathcal{R}$

For a linear code C over the ring $\mathcal{R}$ with parameters $[n, k, d]$, we have $|C| \leq |\mathcal{R}|^{n-d+1}$ and so $d \leq n - \log_{|\mathcal{R}|} |C| + 1$, the Singleton bound on the ring $\mathcal{R}$. Since $|\mathcal{R}| = q^4$ and $|C| = q^k$, where $k = \sum_{i=1}^{4} k_i$, the Singleton bound is $d \leq n - \frac{1}{4} \sum_{i=1}^{4} k_i + 1$. A code which attains the Singleton bound is called an MDS code. We have the following result for an MDS code over a finite field $\mathbb{F}_q$.

LEMMA 5.1 [11]. *If C is a linear code over $\mathbb{F}_q$, then the following are equivalent:*

(1) *C is an MDS code over $\mathbb{F}_q$;*
(2) *$C^\perp$ is an MDS code over $\mathbb{F}_q$;*
(3) *$C^{\perp_l}$ is an MDS code over $\mathbb{F}_q$.*

The following theorem shows that a linear code is an MDS code if and only if its Euclidean (l-Galois) dual is an MDS code over the ring $\mathcal{R}$.

THEOREM 5.2. *Let $C = \bigoplus_{i=1}^{4} \gamma_i C_i$ be a linear code over the ring $\mathcal{R}$, where the C_i are the component codes over the finite field $\mathbb{F}_q$.*

(1) *C is an MDS code over the ring $\mathcal{R}$ if and only if the C_i are MDS codes over $\mathbb{F}_q$ with the same parameters for each $i = 1, 2, 3, 4$.*

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

(2) *C is an MDS code over the ring $\mathcal{R}$ if and only if $C^{\perp}$ is an MDS code over $\mathcal{R}$.*
(3) *C is an MDS code over the ring $\mathcal{R}$ if and only if $C^{\perp_l}$ is an MDS code over $\mathcal{R}$.*

PROOF. (1) Suppose C is an MDS code over the ring $\mathcal{R}$ with parameters $[n, k, d]$, where $4d = 4n - \sum_{i=1}^{4} k_i + 4$. Since $d = \min_{1\le i\le 4}\{d_i\}$, where $d_i = d_H(C_i)$, it follows that $d = d_j$ for some $j = 1, 2, 3, 4$. This implies $4d_j = 4n - \sum_{i=1}^{4} k_i + 4$. Now $d_i \le n - k_i + 1$ for $i = 1, 2, 3, 4$ and so $\sum_{i=1}^{4} d_i \le 4n - \sum_{i=1}^{4} k_i + 4 = 4d_j$. Since d_j is the minimum of the d_i for $i = 1, 2, 3, 4$, we have $4d_j \le \sum_{i=1}^{4} d_i$. It follows that $4d_j = \sum_{i=1}^{4} d_i$ which is only possible when $d_1 = d_2 = d_3 = d_4$. Hence, the C_i are MDS codes over $\mathbb{F}_q$ with the same parameters.

Conversely, if the C_i are MDS codes with the same parameters, that is, $d_1 = d_2 = d_3 = d_4$ and $d_i = n - k_i + 1$, then $4d_i = 4n - \sum_{i=1}^{4} k_i + 4$ for $i = 1, 2, 3, 4$. Since $d = \min_{1\le i\le 4}\{d_i\}$, this implies $4d = 4n - \sum_{i=1}^{4} k_i + 4$. Hence, C is an MDS code.

(2) Let C be an MDS code over the ring $\mathcal{R}$. By part (1), the C_i are MDS codes over $\mathbb{F}_q$ having the same parameters for each $i = 1, 2, 3, 4$. Hence, the $C_i^{\perp}$ are MDS codes over $\mathbb{F}_q$ with the same parameters for each $i = 1, 2, 3, 4$. This implies that $C^{\perp}$ is an MDS code over the ring $\mathcal{R}$. A similar argument can be made for the converse.

(3) Let C be an MDS code over the ring $\mathcal{R}$. Then, $C^{p^{(e-l)}}$ is also an MDS code over the ring $\mathcal{R}$. By Lemma 3.1, $C^{\perp_l} = (C^{p^{(e-l)}})^{\perp}$, and hence $C^{\perp_l}$ is an MDS code over $\mathcal{R}$. Conversely, if $C^{\perp_l}$ is an MDS code over $\mathcal{R}$, it follows that $C^{p^{(e-l)}}$ is an MDS code. Hence, C is an MDS code over $\mathcal{R}$. □

REMARK 5.3. Result (1) in the above theorem over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ is proved in [10].

Acknowledgements

The third author is ConsenSys Blockchain chair professor. He thanks ConsenSys AG for that privilege. The authors thank the reviewer for valuable comments and suggestions.

References

[1] M. Ashraf and G. Mohammad, 'Quantum codes from cyclic codes over $F_q + uF_q + vF_q + \mathrm{uv}F_q$', *Quantum Inf. Process.* **15**(10) (2016), 4089–4098.
[2] C. Carlet and S. Guilley, 'Complementary dual codes for counter-measures to side-channel attacks', *Adv. Math. Commun.* **10**(1) (2016), 131–150.
[3] C. Carlet, S. Mesnager, C. Tang and Y. Qi, 'Euclidean and Hermitian LCD MDS codes', *Des. Codes Cryptogr.* **86**(11) (2018), 2605–2618.
[4] C. Carlet, S. Mesnager, C. Tang and Y. Qi, 'New characterization and parametrization of LCD codes', *IEEE Trans. Inform. Theory* **65**(1) (2019), 39–49.
[5] C. Carlet, S. Mesnager, C. Tang, Y. Qi and R. Pellikaan, 'Linear codes over F_q are equivalent to LCD codes for $q > 3$', *IEEE Trans. Inform. Theory* **64**(4, part 2) (2018), 3010–3017.
[6] B. Chen and H. Liu, 'New constructions of MDS codes with complementary duals', *IEEE Trans. Inform. Theory* **64**(8) (2018), 5776–5782.
[7] Y. Fan and L. Zhang, 'Galois self-dual constacyclic codes', *Des. Codes Cryptogr.* **84**(3) (2017), 473–492.

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press

[8] L. Jin, 'Construction of MDS codes with complementary duals', *IEEE Trans. Inform. Theory* **63**(5) (2017), 2843–2847.
[9] J. Kaboré and M. E. Charkani, 'Constacyclic codes over $F_q + uF_q + vF_q + \mathrm{uv}F_q$', Preprint, 2016, arXiv:1507.03084 [cs.IT].
[10] P. Li, X. Guo, S. Zhu and X. Kai, 'Some results on linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$', *J. Appl. Math. Comput.* **54**(1–2) (2017), 307–324.
[11] X. Liu, Y. Fan and H. Liu, 'Galois LCD codes over finite fields', *Finite Fields Appl.* **49** (2018), 227–242.
[12] Z. Liu and J. Wang, 'Linear complementary dual codes over rings', *Des. Codes Cryptogr.* **87**(12) (2019), 3077–3086.
[13] J. L. Massey, 'Linear codes with complementary duals', *Discrete Math.* **106/107** (1992), 337–342. 1992.
[14] O. Prakash, S. Yadav, H. Islam and P. Solé, 'Self-dual and LCD double circulant codes over a class of non-local rings', *Comput. Appl. Math.* **41**(6) (2022), 1–16.
[15] R. Wu and M. Shi, 'A note on k-Galois LCD codes over the ring $F_q + uF_q$', *Bull. Aust. Math. Soc.* **104**(1) (2021), 154–161.
[16] X. Yang and J. L. Massey, 'The condition for a cyclic code to have a complementary dual', *Discrete Math.* **126**(1–3) (1994), 391–393.
[17] T. Yao, M. Shi and P. Solé, 'Skew cyclic codes over $F_q + uF_q + vF_q + uvF_q$', *J. Algebra Comb. Discrete Struct. Appl.* **2**(3) (2015), 163–168.

ASTHA AGRAWAL, Department of Mathematics,
Indian Institute of Technology Delhi, New Delhi 110016, India
e-mail: asthaagrawaliitd@gmail.com

GYANENDRA K. VERMA, Department of Mathematics,
Indian Institute of Technology Delhi, New Delhi 110016, India
e-mail: gkvermaiitdmaths@gmail.com

R. K. SHARMA, Department of Mathematics,
Indian Institute of Technology Delhi, New Delhi 110016, India
e-mail: rksharmaiitd@gmail.com

https://doi.org/10.1017/S0004972722001344 Published online by Cambridge University Press