Bull. Aust. Math. Soc. **104** (2021), 154–161
doi:10.1017/S0004972720001331

A NOTE ON k-GALOIS LCD CODES OVER THE RING $\mathbb{F}_q + u\mathbb{F}_q$

RONGSHENG WU and MINJIA SHI ✉

(Received 19 August 2020; accepted 12 October 2020; first published online 14 December 2020)

Abstract

We study the k-Galois linear complementary dual (LCD) codes over the finite chain ring $R = \mathbb{F}_q + u\mathbb{F}_q$ with $u^2 = 0$, where $q = p^e$ and p is a prime number. We give a sufficient condition on the generator matrix for the existence of k-Galois LCD codes over R. Finally, we show that a linear code over R (for $k = 0, q > 3$) is equivalent to a Euclidean LCD code, and a linear code over R (for $0 < k < e$, $(p^{e-k} + 1) \mid (p^e - 1)$ and $(p^e - 1)/(p^{e-k} + 1) > 1$) is equivalent to a k-Galois LCD code.

2020 *Mathematics subject classification*: primary 94B05; secondary 94B15.

Keywords and phrases: Euclidean LCD codes, Gray map, k-Galois LCD codes, linear codes, linear complementary dual codes.

1. Introduction

Linear complementary dual (LCD) codes over finite fields are linear codes satisfying $C \cap C^{\perp} = \{\mathbf{0}\}$. These codes were first proposed by Massey [10] and shown to provide an optimum linear coding solution for a two-user adder channel in the binary case. Massey also obtained the asymptotic property for binary LCD codes. Later, a necessary and sufficient condition for a cyclic code to be an LCD code over a finite field was derived in [15]. The asymptotic property for LCD codes over a finite field was generalised by Sendrier (by using hull dimension spectra) [13]. The linear programming bound on the largest size of an LCD code of given length and minimum distance was presented in [3]. Güneri *et al.* [5] characterised LCD quasi-cyclic codes by using their concatenated structure and showed that Hermitian LCD codes were asymptotically good. Zhu and Shi [16] showed that LCD four circulant codes satisfy a modified Gilbert–Varshamov bound. Constructing LCD codes with good parameters has important applications in both theory and practice. Many good LCD codes, such as generalised Reed–Solomon codes, were constructed from classical linear codes (see

This research is supported by the National Natural Science Foundation of China (12071001, 61672036), the Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03) and the Natural Science Foundation of Anhui Provence (2008085QA04).

[2, 6, 12, 14]). Mesnager *et al.* [11] provided a construction of algebraic geometry LCD codes which could be resistant against side channel attack.

Recently, k-Galois dual codes were introduced in [4] for studying Galois constacyclic codes (a generalisation of Euclidean constacyclic and Hermitian constacyclic codes). The k-Galois LCD codes over finite fields have been studied in [8]. A necessary and sufficient condition for linear codes to be k-Galois LCD was obtained and several classes of k-Galois LCD maximum distance separable codes were exhibited. A remarkable result for LCD codes was established by Carlet *et al.* [1], showing that any linear code over $\mathbb{F}_q$ is equivalent to a Euclidean LCD code for $q \geq 4$, and any linear code over $\mathbb{F}_{q^2}$ is equivalent to a Hermitian LCD code for $q \geq 3$. Later, these results were generalised to k-Galois codes over finite fields by using Gröbner bases [8]. A natural question arises as to how to characterise k-Galois LCD codes over a finite chain ring R. Another interesting problem is to study the connection between k-Galois LCD codes over finite fields and linear codes in the context of finite chain rings.

In this paper we answer both questions positively for the chain ring $R = \mathbb{F}_q + u\mathbb{F}_q$ with $u^2 = 0$. Section 2 gathers together the notation and definitions needed in the rest of the paper. In Section 3 we obtain a sufficient condition for a code C to be a k-Galois LCD code with q even. In Section 4 we show that any linear code over R is equivalent to a Euclidean LCD code with $q > 3$, and any linear code over R is equivalent to a k-Galois LCD code with $(p^{e-k} + 1) \mid (p^e - 1)$ and $(p^e - 1)/(p^{e-k} + 1) > 1$.

2. Preliminaries

2.1. Gray map. Throughout this paper, $q = p^e$ is a positive power of a prime p and $\mathbb{F}_q$ denotes the finite field with q elements. Let $\mathbb{F}_q^n$ be the set of all q-ary vectors of length n. The ring $R = \mathbb{F}_q + u\mathbb{F}_q$, with $u^2 = 0$, is a local ring and its only maximal ideal is $(u) = \{au : a \in \mathbb{F}_q\}$. The residue field $R/(u)$ is isomorphic to $\mathbb{F}_q$. The group of units, R^*, of the ring R is $R^* = R\backslash(u)$ and it is isomorphic to the product of a cyclic group of order $q - 1$ by an elementary abelian group of order q.

The Gray map ϕ from R to $\mathbb{F}_q^2$ is defined by $\phi(a + bu) = (b, a + b)$, for $a, b \in \mathbb{F}_q$. The Lee weight is defined as $w_L(a + bu) = w_H(b) + w_H(a + b)$, where w_H denotes the Hamming weight. It is a bijective map which can be extended into a map (denoted by Φ) from R^n to $\mathbb{F}_q^{2n}$. The Lee distance of $\mathbf{x}, \mathbf{y} \in R^n$ is defined by $w_L(\mathbf{x} - \mathbf{y})$. The Gray map is a linear isometry from (R^n, d_L) to $(\mathbb{F}_q^{2n}, d_H)$, where d_L and d_H denote the Lee distance and Hamming distance in R^n and $\mathbb{F}_q^{2n}$, respectively.

A code C over R is a nonempty subset of R^n. The code is linear if it is an R-submodule of R^n. It is well known that an R-linear code C is permutation equivalent to an R-linear code with a generator matrix of the form

$$G = \begin{pmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uC \end{pmatrix}, \tag{2.1}$$

https://doi.org/10.1017/S0004972720001331 Published online by Cambridge University Press

where I_{k_1} and I_{k_2} denote the $k_1 \times k_1$ and $k_2 \times k_2$ identity matrices, respectively, and A, C, B_1 and B_2 are matrices over $\mathbb{F}_q$. If C is a linear code over R with generator matrix G defined in (2.1) and minimum Lee distance d, we say that C is of type $(n; k_1, k_2, d)$.

2.2. *k*-Galois dual codes. Let k and e be integers with $0 \le k < e$. Let F be the Frobenius operator over R defined by $F(a + ub) = a^p + ub^p$. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ be two elements of R^n. Define the k-Galois form

$$\langle \mathbf{x}, \mathbf{y} \rangle_k = x_1 F^k(y_1) + x_2 F^k(y_2) + \cdots + x_n F^k(y_n).$$

For a linear code C over R, let $C^{\perp_k}$ denote its k-Galois dual, that is,

$$C^{\perp_k} = \{\mathbf{x} \in R^n \mid \langle \mathbf{x}, \mathbf{y} \rangle_k = 0 \text{ for all } \mathbf{y} \in C\}.$$

In particular, if $e = 0$, $C^{\perp_0}$ (denoted $C^{\perp}$ for convenience) is just the Euclidean dual code of C; if e is even and $k = e/2$, $C^{\perp_k}$ (denoted $C^{\perp_H}$ for convenience) is just the Hermitian dual code of C. It is easy to check that $C^{\perp_k}$ is also a linear code over R. A code C is called k-Galois LCD if it satisfies $C \cap C^{\perp_k} = \{\mathbf{0}\}$.

For an $m \times m$ matrix $M = (m_{ij})_{m \times m}$, let M^T denote the transposed matrix of M. If the determinant $\det(M)$ is a unit in R, we say that M is nonsingular. In addition, we denote $M^{(p^k)} = (m_{ij}^{p^k})_{m \times m}$. Let $C^{(p^k)} = \{(c_1^{p^k}, c_2^{p^k}, \ldots, c_n^{p^k}) \mid (c_1, c_2, \ldots, c_n) \in C\}$.

LEMMA 2.1 [7, Proposition 2.2]. *Let C be a linear code over R. Then the k-Galois dual $C^{\perp_k}$ is equal to the Euclidean dual $(C^{(p^{e-k})})^{\perp}$ of $C^{(p^{e-k})}$.*

The following theorem gives a partial characterisation of k-Galois LCD codes, and it is analogous to the result over finite fields [8, Theorem 2.4].

THEOREM 2.2. *Let $C \neq \{\mathbf{0}\}$ be a linear code over R of type $(n; k_1, k_2, d)$ with the generator matrix G. If $G(G^{(p^{e-k})})^T$ is nonsingular, then C is a k-Galois LCD code over R.*

PROOF. For any codeword $\mathbf{c} \in C$, there exists an element $\mathbf{v} \in R^{k_1+k_2}$ such that $\mathbf{c} = \mathbf{v}G$. Since $G(G^{(p^{e-k})})^T$ is nonsingular, $\mathbf{c}(G^{(p^{e-k})})(G(G^{(p^{e-k})})^T)^{-1}G = \mathbf{v}G = \mathbf{c}$. If $\mathbf{c} \in C^{\perp_k}$, then $\mathbf{c}(G^{(p^{e-k})}) = 0$ from Lemma 2.1, which gives $\mathbf{c} = 0$. The result follows from the definition of LCD codes. □

2.3. Equivalence. Recall that a monomial matrix M over R of order n is an $n \times n$ matrix with exactly one unit element in each row and column. In other words, a monomial matrix M can be written in the form PD, where P is a permutation matrix and $D = \mathrm{diag}_n[\mathbf{w}]$, $\mathbf{w} = (w_1, w_2, \ldots, w_n) \in (R^*)^n$ and $\mathrm{diag}_n[\mathbf{w}]$ denotes the diagonal matrix whose elements on the diagonal are $w_1, w_2, \ldots, w_n$.

We are now ready to define equivalence. Let C_1 and C_2 be linear codes over R of the same length and let G_1 be a generator matrix C_1. The codes C_1 and C_2 are equivalent if there is a monomial matrix M such that G_1M is a generator matrix of C_2. In particular, if D is an identity matrix, then C_1 and C_2 are called permutation equivalent.

https://doi.org/10.1017/S0004972720001331 Published online by Cambridge University Press

PROPOSITION 2.3. *Let C be a k-Galois LCD code over R. If C_1 is permutation equivalent to C, then C_1 is also k-Galois LCD.*

3. k-Galois LCD codes over R

LEMMA 3.1. *Let C be a linear code over R* (with $p = 2$) *of type $(n; k_1, k_2, d)$. Then*

$$\Phi(C^{\perp_k}) = (\Phi(C)^{(p^{e-k})})^{\perp}.$$

PROOF. Let $\mathbf{x} = \mathbf{a} + \mathbf{b}u \in C$ and $\mathbf{y} = \mathbf{c} + \mathbf{d}u \in C^{\perp_k}$, where $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathbb{F}_q^n$. Thus, $\langle \mathbf{x}, \mathbf{y} \rangle_k = 0$ implies $\langle \mathbf{a}, \mathbf{c} \rangle_k + u(\langle \mathbf{b}, \mathbf{c} \rangle_k + \langle \mathbf{a}, \mathbf{d} \rangle_k) = 0$. Utilising the Gray map,

$$\langle \Phi(\mathbf{y}), \Phi(\mathbf{x}) \rangle_{e-k} = \langle \mathbf{d}, \mathbf{b} \rangle_{e-k} + \langle \mathbf{c}, \mathbf{a} \rangle_{e-k} + \langle \mathbf{d}, \mathbf{a} \rangle_{e-k} + \langle \mathbf{c}, \mathbf{b} \rangle_{e-k} + \langle \mathbf{d}, \mathbf{b} \rangle_{e-k} = 0.$$

Therefore, $\Phi(\mathbf{y}) \in (\Phi(C)^{(p^{e-k})})^{\perp}$ and $\Phi(C^{\perp_k}) \subseteq (\Phi(C)^{(p^{e-k})})^{\perp}$.

On the other hand, from the definition of the Gray map and the generator matrix $G^{\perp_k}$, it is easy to check that the codes $\Phi(C^{\perp_k})$ and $(\Phi(C)^{(p^{e-k})})^{\perp}$ have the same size. □

LEMMA 3.2. *Let C be a linear code over R of type $(n; k_1, k_2, d)$. Then*

$$\Phi(C \cap C^{\perp_k}) = \Phi(C) \cap \Phi(C^{\perp_k}).$$

PROOF. Let $\Phi(\mathbf{x}) \in \Phi(C \cap C^{\perp_k})$. Since the Gray map Φ is bijective, $\mathbf{x} \in C \cap C^{\perp_k}$ and so $\Phi(C \cap C^{\perp_k}) \subseteq \Phi(C) \cap \Phi(C^{\perp_k})$.

On the other hand, letting $\mathbf{y} \in \Phi(C) \cap \Phi(C^{\perp_k})$, there exists a unique $\mathbf{u} \in C \cap C^{\perp_k}$ such that $\Phi(\mathbf{u}) = \mathbf{y}$. This implies $\Phi(C) \cap \Phi(C^{\perp_k}) \subseteq \Phi(C \cap C^{\perp_k})$. □

The next theorem gives a connection between k-Galois LCD codes over R and their image codes.

THEOREM 3.3. *Let C be a linear code over R* (with $p = 2$) *of type $(n; k_1, k_2, d)$. Then C is k-Galois LCD if and only if $\Phi(C)$ is q-ary k-Galois LCD with parameters* $[2n, 2k_1 + k_2, d]$.

PROOF. If C is a k-Galois LCD code over R, then from Lemmas 3.1 and 3.2,

$$\Phi(C \cap C^{\perp_k}) = \Phi(C) \cap \Phi(C^{\perp_k}) = \Phi(C) \cap (\Phi(C)^{(p^{e-k})})^{\perp} = \{\mathbf{0}\}.$$

In other words, $\Phi(C)$ is k-Galois LCD by [8, Lemma 2.3]. If $\Phi(C)$ is k-Galois LCD over $\mathbb{F}_q$, a similar argument can be made to prove that C is k-Galois LCD over R. □

4. k-Galois LCD codes from the linear codes over R

For $I = \{i_1, i_2, \ldots, i_t\} \subseteq \{1, 2, \ldots, m\}$ and a square matrix N, define N_I to be the submatrix of N obtained by deleting the i_1th, i_2th, $\ldots, i_t$th rows and columns of N. Set $N_I = 1$ if $I = \{1, 2, \ldots, m\}$ and $N_{\emptyset} = N$ for convenience. The support S of a vector $\mathbf{x} \in R^n$ is defined as the set of indices where it is nonzero.

https://doi.org/10.1017/S0004972720001331 Published online by Cambridge University Press

LEMMA 4.1. *Let N be an $m \times m$ matrix over R. For every $\mathbf{u} = (u_1, u_2, \ldots, u_m) \in R^m$ with support S,*

$$\det(N + \mathrm{diag}_m[\mathbf{u}]) = \det(N) + \sum_{i \in S} u_i \det(N_{\{i\}}) + \sum_{\substack{i<j \\ i,j \in S}} (u_i u_j) \det(N_{\{i,j\}}) + \cdots + \Big(\prod_{i \in S} u_i\Big) \det(N_S).$$

PROOF. The proof is by induction on the size, $s = |S|$, of S. For the initial case $s = 1$, let $\mathbf{u}$ be a vector in R^m with nonzero component i_1. Then

$$\det(N + \mathrm{diag}_m[\mathbf{u}]) = \det(N) + u_{i_1} \det(N_{\{i_1\}}),$$

showing that the claim holds for $s = 1$.

By induction, we may assume that the statement holds for $s = 1, 2, \ldots, t \leq m - 1$. Firstly, denote by $\mathbf{u}$ a codeword with support $S = \{i_1, i_2, \ldots, i_{t+1}\}$. Let $\mathbf{u}'$ be the word obtained from $\mathbf{u}$ by changing $u_{i_{t+1}}$ into 0 and $\bar{\mathbf{u}}$ the word obtained by deleting the i_{t+1} component of $\mathbf{u}$. Let $S_1 = S \backslash \{i_{t+1}\}$. Therefore,

$$\begin{aligned}\det(N + \mathrm{diag}_m[\mathbf{u}]) &= \det(N + \mathrm{diag}_m(\mathbf{u}')) + u_{i_{t+1}} \det(N_{\{i_{t+1}\}} + \mathrm{diag}_{m-1}[\bar{\mathbf{u}}]) \\ &= \det(N) + \sum_{i \in S_1} u_i \det(N_{\{i\}}) + \cdots + \Big(\prod_{i \in S_1} u_i\Big) \det(N_{S_1}) \\ &\quad + u_{i_{t+1}} \Big(\det(N_{\{i_{t+1}\}}) + \sum_{i \in S_1} u_i \det(N_{\{i, i_{t+1}\}}) + \cdots \\ &\quad + \Big(\prod_{i \in S_1} u_i\Big) \det(N_{\{S_1, i_{t+1}\}}) \Big) \\ &= \det(N) + \sum_{i \in S} u_i \det(N_{\{i\}}) + \cdots + \Big(\prod_{i \in S} u_i\Big) \det(N_S),\end{aligned}$$

yielding the result. □

4.1. Case I: $k = 0$. Let C be a linear code over R with the generator matrix G of type $(n; k_1, k_2, d)$ and let $S = \{i_1, i_2, \ldots, i_s\} \subseteq \{1, 2, \ldots, k_1\}$. Consider an element $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in R^n$, where $a_i \in R \backslash \{-1 + bu, 1 + bu : b \in \mathbb{F}_q\}$ if $i \in S$, and $a_i \in \{-1, 1\}$ otherwise. Define

$$C_{\mathbf{a}} = \{(a_1 c_1, a_2 c_2, \ldots, a_n c_n) \mid (c_1, c_2, \ldots, c_n) \in C\}.$$

The generator matrix $G_{\mathbf{a}}$ of $C_{\mathbf{a}}$ is obtained from G by multiplying its jth column by a_j for $j \in \{1, 2, \ldots, n\}$. Let $N = GG^T$ and $N' = G_{\mathbf{a}} G_{\mathbf{a}}^T$. Then

$$N' = G_{\mathbf{a}} G_{\mathbf{a}}^T = N + \mathrm{diag}_{k_1+k_2}[\mathbf{u}],$$

where $\mathbf{u} = (a_1^2 - 1, a_2^2 - 1, \ldots, a_{k_1}^2 - 1, 0, \ldots, 0)$.

THEOREM 4.2. *Keep the notation as above. Let t be a nonnegative integer less than $k_1 + k_2$. Suppose that* $\det(N_I) \in (u)$ *for any $I \subseteq \{1, 2, \ldots, k_1 + k_2\}$ with $0 \leq \#I \leq t$.*

https://doi.org/10.1017/S0004972720001331 Published online by Cambridge University Press

Suppose there exists a subset S of $\{1, 2, \ldots, k_1\}$ with size $t+1$ such that $\det(N_S) \in R\backslash(u)$. Then $C_{\mathbf{a}}$ is a Euclidean LCD code of length n over R. In particular, if $a_j \notin (u)$ for $1 \leq j \leq n$, then $C_{\mathbf{a}}$ is a Euclidean LCD code over R of type $(n; k_1, k_2, d)$.

PROOF. From the discussion above and Lemma 4.1,

$$\begin{aligned}\det(N') = \det(G_{\mathbf{a}}G_{\mathbf{a}}^T) &= \det(N + \mathrm{diag}_{k_1+k_2}[\mathbf{u}]) \\ &= \det(N) + \sum_{i\in S} u_i \det(N_{\{i\}}) + \cdots + \Big(\prod_{i\in S} u_i\Big)\det(N_S) \\ &= Z + U,\end{aligned}$$

where $U = (\prod_{i\in S} u_i)\det(N_S)$ is a unit in R and $Z = \det(N') - U$ is a zero divisor in R since every component of Z is a zero divisor from the assumption of the theorem. Thus, $\det(N') \in R^*$ and $C_{\mathbf{a}}$ is a Euclidean LCD code over R from [9, Lemma 2.3] and Theorem 2.2. In particular, if $a_j \notin (u)$ for $j \in \{1, 2, \ldots, n\}$, then $C_{\mathbf{a}}$ is equivalent to the code C by the definition. □

THEOREM 4.3. *Let C be a linear code of type $(n; k_1, k_2, d)$ over R with q a prime power ($q > 3$). Then there exists a Euclidean LCD code C' which is equivalent to C over R.*

PROOF. It is sufficient to consider the case when the code C is not Euclidean LCD. Let C be a linear code over R with the generator matrix G of type $(n; k_1, k_2, d)$. Then $\det(GG^T)$ is a zero divisor in R from [9, Lemma 2.3] and Theorem 2.2.

Let $N = GG^T$. There exists a nonnegative integer t less than $k_1 + k_2$ such that $\det(N_I) \in (u)$ for any $I \subseteq \{1, 2, \ldots, k_1 + k_2\}$ with $0 \leq \#I \leq t$, and $\det(N_S) \in R\backslash(u)$ with $S \subseteq \{1, 2, \ldots, k_1 + k_2\}$ of size $t + 1$. Since $q > 3$, the set $R^*\backslash\{1 + bu, -1 + bu\} \neq \emptyset$ with $b \in \mathbb{F}_q$. Let $C' = C_{\mathbf{a}}$, choosing $a_j \in R^*\backslash\{-1 + bu, 1 + bu\}$ if $j \in S$ and $a_j \in \{-1, 1\}$ otherwise. The desired result follows from Theorem 4.2. □

COROLLARY 4.4. *Let q be a prime power with $q > 3$. A Euclidean LCD code over R of type $(n; k_1, k_2, d)$ exists if there is a linear code over R of type $(n; k_1, k_2, d)$. In particular, if $p = 2$, then a q-ary Euclidean LCD code with parameters $[2n, 2k_1 + k_2, d]$ exists if there is a linear code over R of type $(n; k_1, k_2, d)$.*

4.2. Case II: $0 < k < e$ and $(p^{e-k} + 1) \mid (p^e - 1)$. Again, let C be a linear code over R with the generator matrix G of type $(n; k_1, k_2, d)$, where $q = p^e$ is a positive power of a prime number p. Let $S = \{i_1, i_2, \ldots, i_s\} \subseteq \{1, 2, \ldots, k_1\}$. To simplify the notation we set $\alpha = (p^e - 1)/(p^{e-k} + 1)$. Consider the element $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in R^n$ with $a_i \in R\backslash\{b + du : b \in (\mathbb{F}_q^*)^\alpha, d \in \mathbb{F}_q\}$ if $i \in S$ and $a_i \in (\mathbb{F}_q^*)^\alpha$ otherwise. Define

$$C_{\mathbf{a}} = \{(a_1c_1, a_2c_2, \ldots, a_nc_n) \mid (c_1, c_2, \ldots, c_n) \in C\}$$

and define the generator matrix $G_{\mathbf{a}}$ of $C_{\mathbf{a}}$ as before. Let $\hat{N} = G(G^{(p^{e-k})})^T$ and $\hat{N}' = G_{\mathbf{a}}(G_{\mathbf{a}}^{(p^{e-k})})^T$. Then

$$\hat{N}' = G_{\mathbf{a}}(G_{\mathbf{a}}^{(p^{e-k})})^T = \hat{N} + \mathrm{diag}_{k_1+k_2}[\mathbf{u}'],$$

https://doi.org/10.1017/S0004972720001331 Published online by Cambridge University Press

where $\mathbf{u}' = (a_1^{p^{e-k}+1} - 1, a_2^{p^{e-k}+1} - 1, \dots, a_{k_1}^{p^{e-k}+1} - 1, 0, \dots, 0)$.

THEOREM 4.5. *Keep the notation as above. Let t be a nonnegative integer less than $k_1 + k_2$. Suppose that $\det(\hat{N}_I) \in (u)$ for any $I \subseteq \{1, 2, \dots, k_1 + k_2\}$ with $0 \le \#I \le t$. Suppose there exists a subset S of $\{1, 2, \dots, k_1\}$ with size $t + 1$ such that $\det(\hat{N}_S) \in R\backslash(u)$. Then $C_{\mathbf{a}}$ is a k-Galois LCD code of length n over R. In particular, if $a_j \notin (u)$ for $1 \le j \le n$, then $C_{\mathbf{a}}$ is a k-Galois LCD code over R of type $(n; k_1, k_2, d)$.*

PROOF. Again from Lemma 4.1,

$$\det(\hat{N}') = \det(G_{\mathbf{a}}(G_{\mathbf{a}}^{(p^{e-k})})^T) = \det(\hat{N} + \mathrm{diag}_{k_1+k_2}[\mathbf{u}'])$$
$$= \det(\hat{N}) + \sum_{i \in S} u_i \det(\hat{N}_{\{i\}}) + \cdots + \Big(\prod_{i \in S} u_i\Big) \det(\hat{N}_S).$$

It is easy to check that $\det(\hat{N}') \in R^*$ from the assumption of the theorem. Thus, $C_{\mathbf{a}}$ is a k-Galois LCD code over R from [9, Lemma 2.3] and Theorem 2.2. In particular, if $a_j \notin (u)$ for $j \in \{1, 2, \dots, n\}$, then $C_{\mathbf{a}}$ is equivalent to the code C by the definition. □

THEOREM 4.6. *Let C be a linear code of type $(n; k_1, k_2, d)$ over R ($\alpha > 1$). Then there exists a k-Galois LCD code C' which is equivalent to C over R.*

PROOF. It is sufficient to consider the case when the code C is not k-Galois LCD. Let C be a linear code over R with the generator matrix G of type $(n; k_1, k_2, d)$. Then $\det(G(G^{(p^{e-k})})^T)$ is a zero divisor in R from [9, Lemma 2.3] and Theorem 2.2.

Let $\hat{N} = G(G^{(p^{e-k})})^T$. There exists a nonnegative integer less than $k_1 + k_2$ such that $\det(\hat{N}_I) \in (u)$ for any $I \subseteq \{1, 2, \dots, k_1 + k_2\}$ with $0 \le \#I \le t$, and $\det(\hat{N}_S) \in R\backslash(u)$ with $S \subseteq \{1, 2, \dots, k_1 + k_2\}$ of size $t + 1$. Since $\alpha > 1$, the set

$$R^* \backslash \{b + du \mid b \in (\mathbb{F}_q^*)^\alpha, d \in \mathbb{F}_q\} \neq \emptyset.$$

Thus, let $C' = C_{\mathbf{a}}$ by choosing $a_i \in R^* \backslash \{b + du : b \in (\mathbb{F}_q^*)^\alpha, d \in \mathbb{F}_q\}$ if $i \in S$ and $a_i \in (\mathbb{F}_q^*)^\alpha$ otherwise. The desired result follows from Theorem 4.5. □

COROLLARY 4.7. *Let $\alpha > 1$. A k-Galois LCD code over R of type $(n; k_1, k_2, d)$ exists if there is a linear code over R of type $(n; k_1, k_2, d)$. In particular, if $p = 2$, then a q-ary k-Galois LCD code with parameters $[2n, 2k_1 + k_2, d]$ exists if there is a linear code over R of type $(n; k_1, k_2, d)$.*

REMARK 4.8. Suppose e is even and $k = e/2$. Then for a linear code C of type $(n; k_1, k_2, d)$ over R with $p^k > 2$, there exists a Hermitian LCD code C' which is equivalent to C over R.

In other words, Theorems 4.3 and 4.6 generalise the results of [1, Corollaries 13, 18], concerning the constructions of Euclidean and Hermitian LCD codes over $\mathbb{F}_q$, to the k-Galois LCD codes over the chain ring R. Furthermore, Theorems 4.3 and 4.6 also generalise the results of [7, Theorem 4.8] introduced in [1].

It could be interesting to explore the possible connection between k-Galois LCD codes and linear codes over different rings, such as $R = \mathbb{F}_q[u]/(u^k)$. The hull of the

https://doi.org/10.1017/S0004972720001331 Published online by Cambridge University Press

k-Galois linear codes, an extension of k-Galois LCD codes, over R or a finite chain ring is also a topic of interest.

References

[1] 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) (2018), 3010–3017.

[2] B. Chen and H. Liu, 'New construction of MDS codes with complementary duals', *IEEE Trans. Inform. Theory* **64**(8) (2018), 5776–5782.

[3] S. Dougherty, J. Kim, B. Özkaya, L. Sok and P. Solé, 'The combinatorics of LCD codes: linear programming bound and orthogonal matrices' *Int. J. Inf. Coding Theory* **4**(2–3) (2017), 116–128.

[4] Y. Fan and L. Zhang, 'Galois self-dual constacyclic codes', *Des. Codes Cryptogr.* **84**(3) (2017), 473–492.

[5] C. Güneri, B. Özkaya and P. Solé, 'Quasi-cyclic complementary dual codes', *Finite Fields Appl.* **42** (2016), 67–80.

[6] L. Jin, 'Construction of MDS codes with complementary duals', *IEEE Trans. Inform. Theory* **63**(5) (2017), 2843–2847.

[7] H. Liu and X. Pan, 'Galois hulls of linear codes over finite fields', *Des. Codes Cryptogr.* **88** (2020), 241–255.

[8] X. Liu, Y. Fan and H. Liu, 'Galois LCD codes over finite fields', *Finite Fields Appl.* **49** (2018), 227–242.

[9] X. Liu and H. Liu, 'LCD codes over finite chain rings', *Finite Fields Appl.* **34** (2015), 1–19.

[10] J. Massey, 'Linear codes with complementary dual', *Discrete Math.* **106/107** (1992), 337–342.

[11] S. Mesnager, C. Tang and Y. Qi, 'Complementary dual algebraic geometry codes', *IEEE Trans. Inform. Theory* **64**(4) (2018), 2390–2397.

[12] B. Pang, S. Zhu and Z. Sun, 'On LCD negacyclic codes over finite fields', *J. Syst. Sci. Complex.* **31**(4) (2018), 1065–1077.

[13] N. Sendrier, 'Linear codes with complementary duals meet the Gilbert–Varshamov bound', *Discrete Math.* **285**(1–3) (2004), 345–347.

[14] X. Shi, Q. Yue and S. Yang, 'New LCD MDS codes constructed from generalized Reed–Solomon codes', *J. Algebra Appl.* **18**(8) (2019), 1950150.

[15] X. Yang and J. Massey, 'The condition for a cyclic code to have a complementary dual', *Discrete Math.* **126** (1994), 391–393.

[16] H. Zhu and M. Shi, 'On linear complementary dual four circulant codes', *Bull. Aust. Math. Soc.* **98** (2018), 159–166.

RONGSHENG WU, Ministry of Education Key Laboratory of Intelligent Computing and Signal Processing, School of Mathematical Sciences, Anhui University, Hefei, Anhui 230601, P. R. China
e-mail: wrs2510@163.com

MINJIA SHI, Ministry of Education Key Laboratory of Intelligent Computing and Signal Processing, School of Mathematical Sciences, Anhui University, Hefei, Anhui 230601, P. R. China
e-mail: smjwcl.good@163.com

https://doi.org/10.1017/S0004972720001331 Published online by Cambridge University Press