Galois LCD codes over mixed alphabets

Maryam Bajalan [a], Alexandre Fotue Tabue [b], Joël Kabore [c],
Edgar Martínez-Moro [d,*,1]

[a] *Department of Mathematics, Malayer University, Hamedan, Iran*
[b] *Department of Mathematics, HTTC Bertoua, The University of Bertoua, Cameroon*
[c] *Department of Mathematics, University Joseph Ki-Zerbo, Ouagadougou, Burkina-Faso*
[d] *Institute of Mathematics, University of Valladolid, Castilla, Spain*

A R T I C L E   I N F O

A B S T R A C T

In this work we give a characterization of Galois Linear Complementary Dual codes and Galois-invariant codes over mixed alphabets of finite chain rings, which leads to the study of the Gray image of $\mathbb{F}_p\mathbb{F}_p[\theta]$-linear codes, where $p \in \{2; 3\}$ and $\theta \neq \theta^2 = 0$ that provides LCD codes over $\mathbb{F}_p$.

* Corresponding author.
E-mail addresses: mar.bajalan@gmail.com (M. Bajalan), alexfotue@gmail.com (A. Fotue Tabue), jokabore@yahoo.fr (J. Kabore), edgar.martinez@uva.es (E. Martínez-Moro).

0. Introduction

Linear codes over a mixed alphabet of finite chain rings have become a great research avenue in coding theory, see for example [1–5,7,8,14]. In [7], Borges et al. were the pioneers in studying the algebraic structure of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes as $\mathbb{Z}_4$-submodules (additive groups) of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, where α and β are two positive integers. Later, Aydogdu and Siap generalized these $\mathbb{Z}_2\mathbb{Z}_4$-additive codes to $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes in [1] and to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes in [3], where r and s are positive integers, $1 \leq r \leq s$, and p is a prime number. Note that this last condition implies that the ring $\mathbb{Z}_{p^r}$ of integers modulo p^r is the homomorphic image of the ring $\mathbb{Z}_{p^s}$ of integers modulo p^s. A general approach for codes over a mixed alphabet of finite chain rings is explored in [8] by Borges et al., which they called S_1S_2-linear codes, where S_1 and S_2 are finite chain rings such that S_1 is the homomorphic image of S_2 by a ring epimorphism.

Let $S|R$ be a Galois extension of finite chain rings of degree m and denote by σ the generator of $\text{Aut}_R(S)$, one can introduce a non-degenerate h-sesquilinear form $\langle \cdot, \cdot \rangle_h : S^n \times S^n \to S$ defined as

$$\langle \mathbf{u}, \mathbf{v} \rangle_h = \sum_{j=1}^n u_j \sigma^h(v_j),$$

where $0 \leq h < m$. For any S-linear code C in S^n (i.e. an S-submodule on S^n), one can define the h-Galois dual $C^{\perp_h}$ of C as $C^{\perp_h} = \{\mathbf{u} \in S^n \ : \ \langle \mathbf{u}, \mathbf{v} \rangle_h = 0_S \text{ for all } \mathbf{v} \in C\}$. A linear code is Galois Linear Complementary Dual (Galois LCD), if it meets one of its Galois duals trivially. An S-linear code C of length n is Galois-invariant over R, if $\sigma(C) = C$, where $\sigma(C) := \{(\sigma(c_1), \cdots, \sigma(c_n)) \ : \ (c_1, \cdots, c_n) \in C\}$.

When $h = 0$ we have the case of Euclidean LCD codes that have been widely applied in data storage, communication systems, consumer electronics, and cryptography. Carlet and Guilley in [9] showed an application of LCD codes against side-channel and fault injection attacks and presented several constructions of LCD codes. Recently, $\mathbb{Z}_2\mathbb{Z}_4$-linear and $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear ($u^3 = 0$ and $u^2 \neq 0$) complementary dual codes are studied by Benbelkacem et al. in [5] and X. Hou et al. in [14], respectively.

In [18,11], the authors studied trace codes, Galois invariance and Galois correspondence over finite commutative chain rings. In [20], R. Wu, and M. Shi, constructed a class of mixed alphabet codes with few weights from irreducible cyclic codes. Motivated by these previous works, we give a characterization of Galois LCD codes and generalize the concept of Galois-invariant codes to a mixed alphabet over finite chain rings.

The paper is organized as follows. In Section 1, we review the concept of Galois extensions of finite chain rings and some facts on linear codes over a mixed alphabet. The first main results are given in Section 2, where we give a simple characterization of Galois LCD codes and Galois-invariant codes over any mixed alphabet of finite chain rings and provide a generalized Delsarte's theorem for linear codes over this type of alphabets. Section 3 studies the Gray image of Galois LCD and Galois-invariant codes

over some mixed alphabets based on Jitman's Gray map [15]. In the work, we show several examples of these constructions and furthermore, we give an optimal binary LCD code, which is the Gray image of a $\mathbb{Z}_2\mathbb{Z}_4$-LCD code.

1. Preliminaries

All the properties and facts about finite chain rings in this section can be found in [19]. Throughout all the paper, S will denote a finite chain ring with maximal ideal $\mathtt{J}(S)$. We will denote by θ a generator of $\mathtt{J}(S)$ such that $\theta^{s-1} \neq \theta^s = 0$, where s is its nilpotency index and $\mathbb{F}_{q^m}$ will denote the residue field of S (q is a power of a prime number). $S^\times$ will denote the unit group of S and for a fixed positive integer r such that $1 \leq r < s$, we will denote by $\overline{} : S \to S/\langle\theta^r\rangle$, the surjective ring homomorphism that maps x to $\overline{x}$, where $\overline{x} = x + \langle\theta^r\rangle$ and $\pi : S \to \mathbb{F}_{q^m}$ is the canonical ring projection. We set $\overline{S} = S/\langle\theta^r\rangle$. Note that $\overline{S}$ is also a finite chain ring which has the same residue field as S. The maximal ideal $\overline{S}$ is $\mathtt{J}(\overline{S})$ generated by $\overline{\theta}$ with nilpotency index r. Moreover, the ring $\overline{S}$ is also an S-module with the law

$$
\begin{aligned}
* : S \times \overline{S} &\to \overline{S} \\
(a, x) &\mapsto \overline{a}x.
\end{aligned}
\tag{1}
$$

1.1. Galois extensions of a finite chain ring

In a finite chain ring S for any θ in $\mathtt{J}(S)\backslash\mathtt{J}(S)^2$, there exists a unique chain of ideals of S given by

$$
\{0_S\} = \mathtt{J}(S)^s \subsetneq \mathtt{J}(S)^{s-1} = \theta^{s-1}S \subsetneq \cdots \subsetneq \mathtt{J}(S) = \theta S \subsetneq S.
\tag{2}
$$

Thus for any θ in $\mathtt{J}(S)\backslash\mathtt{J}(S)^2$, and for any t in $\{0, 1, \cdots, s\}$, $\mathtt{J}(S)^t = \theta^t S = S\theta^t$. This chain of ideals allows defining the valuation ϑ of S as follows:

$$
\begin{aligned}
\vartheta : S &\to \{0, 1, \ldots, s\} \\
x &\mapsto \max\{t \in \{0, 1, \ldots, s\} \ : \ x \in \mathtt{J}(S)^t\}.
\end{aligned}
\tag{3}
$$

Note that $S^\times = S\backslash\mathtt{J}(S)$, since the ring S is local. The restriction of the canonical ring projection π given by $\pi_{\upharpoonright_{S^\times}} : S^\times \to \mathbb{F}_{q^m}\backslash\{0\}$ is a multiplicative group epimorphism and its kernel is $1_S + \mathtt{J}(S)$. Moreover, there is a unique subgroup $\Gamma(S)^*$ of $S^\times$ such that $S^\times = (\Gamma(S)^*) \cdot (1_S + \mathtt{J}(S))$ with $(\Gamma(S)^*) \cap (1_S + \mathtt{J}(S)) = \{1_S\}$ and the restriction $\pi_{\upharpoonright_{S^\times}}$ is a multiplicative group-isomorphism. The reciprocal bijection of $\pi_{\upharpoonright_{S^\times}}$ will be denoted by $\iota : \mathbb{F}_{q^m}\backslash\{0\} \to \Gamma(S)^*$. By convention $\iota(0_{\mathbb{F}_{q^m}}) = 0_S$. The *Teichmüller set* of S is given by $\Gamma(S) = \Gamma(S)^* \cup \{0_S\}$. Therefore, for any θ in $\mathtt{J}(S)\backslash S^s$ there is a unique s-tuple of surjective maps $(\gamma_0, \gamma_1, \cdots, \gamma_{s-1})$ from S into $\Gamma(S)$ such that for any x in S

$$
x = \gamma_0(x) + \gamma_1(x)\theta + \cdots + \gamma_{s-1}(x)\theta^{s-1}.
\tag{4}
$$

The right-hand side of (4) is called the θ-adic decomposition of x. The degree $\deg_\theta$ of an element $x \in S$ is defined by

$$
\begin{aligned}
\deg_\theta : S &\to \{0, 1, \ldots, s\} \cup \{-\infty\} \\
x &\mapsto \max\{t \in \{0, 1, \ldots, s-1\} \cup \{-\infty\} \ : \ \gamma_t(x) \neq 0_S\}.
\end{aligned}
\tag{5}
$$

For j in $\{0, 1, \ldots, s-1\} \cup \{-\infty\}$, it denotes $\Gamma_j(S) := \{x \in S \ : \ \deg_\theta(x) \leq j\}$ and we have

$$
\Gamma_{-\infty}(S) = \{0_S\} \subsetneq \Gamma(S) = \Gamma_0(S) \subsetneq \Gamma_1(S) \subsetneq \cdots \subsetneq \Gamma_{s-1}(S) = S.
$$

Note that for any j in $\{0; 1; \cdots; s-1\}$, we have $\theta^{s-j}\Gamma_{j-1}(S) = \theta^{s-j}S$ and if $r \leq j$ then $\overline{\Gamma_j(S)} = \Gamma_{r-1}(\overline{S}) = \overline{S}$. Thus, the map $\overline{} : \Gamma_{r-1}(S) \to \overline{S}$ is bijective, its reciprocal map will be denoted by $\iota : \overline{S} \to \Gamma_{r-1}(S)$. Therefore, the following map

$$
\begin{aligned}
\chi : \overline{S} &\to \theta^{s-j}S \\
x &\mapsto \theta^{s-r}\iota(x),
\end{aligned}
$$

is an isomorphism of S-modules.

Let S and R be two finite chain rings. We say that S is a ring-extension of R and it denotes $S \,|\, R$, if R is a subring of S and $1_R = 1_S$. The ring-extension $S \,|\, R$ is a Galois extension of degree m, if $S \cong R[X]/\langle f \rangle$ (as ring), where f is a monic basic polynomial over R of degree m. The group $\mathrm{Aut}_R(S)$ (so-called Galois extension $\overline{S} \,|\, \overline{R}$) is given by all ring-automorphisms ρ of S such that the restriction $\rho_{|R} : R \to R$ is the identity map. From [19, Theorem XV.2], $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) \cong \mathrm{Aut}_R(S)$ and $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) \cong \mathrm{Aut}_{\overline{R}}(\overline{S})$ such that for any x in S, we have $\overline{\sigma(x)} = \overline{\sigma}(\overline{x})$ and $\pi(\sigma(x)) = \mathrm{Fr}_q(\pi(x))$ with $\mathrm{Aut}_R(S) = \langle \sigma \rangle$ and $\mathrm{Aut}_{\overline{R}}(\overline{S}) = \langle \overline{\sigma} \rangle$. Thus the group $\mathrm{Aut}_{\overline{R}}(\overline{S})$ is cyclic of order m. The ring S can be regarded as a free R-module of rank m and $m = \mathrm{rank}_R(S) = |\mathrm{Aut}_R(S)|$.

1.2. Linear codes over a mixed alphabet of finite chain rings

Given the rings S and $\overline{S}$ as above, we define the set $\overline{S}S = \{(x \,\|\, y) \ : \ x \in \overline{S} \text{ and } y \in S\}$. The set $\overline{S}S$ is called *mixed alphabet of chain rings S and $\overline{S}$*. Let α and β to be positive integers, the S-scalar multiplication $*$ on $\overline{S}^\alpha \times S^\beta$ is defined as:

$$
a * (x_0, x_1, \ldots, x_{\alpha-1} \,\|\, y_0, y_1, \ldots, y_{\beta-1}) = (\overline{a}x_0, \overline{a}x_1, \ldots, \overline{a}x_{\alpha-1} \,\|\, ay_0, ay_1, \ldots, ay_{\beta-1}).
\tag{6}
$$

Note that the S-scalar multiplication $*$ provides an S-module structure for $\overline{S}^\alpha \times S^\beta$. The S-submodules of $\overline{S}^\alpha \times S^\beta$ are called $\overline{S}S$-linear codes of block-length (α, β).

The concept of independence of vectors in codes over rings defined in [10] can be easily extended to $\overline{S}S$-linear codes as follows: the non-zero elements $\mathbf{c}_1, \ldots, \mathbf{c}_\mu$ in $\overline{S}^\alpha \times S^\beta$ are

S-*independent*, if every S-linear combination $\sum_{i=1}^{\mu} a_i * \mathbf{c}_i = \mathbf{0}$ implies that $a_i * \mathbf{c}_i = \mathbf{0}$, for all $i \in \{1, \ldots, \mu\}$. Let C be an $\overline{S}S$-linear code of block-length (α, β). The codewords $\mathbf{c}_1, \ldots, \mathbf{c}_\mu$ in C form an S-*basis* for C, if they are S-independent (in the previous sense) and they generate C.

For any positive integer μ, we denote by $\mathbf{M}_{\mu \times \alpha}(\overline{S})$ and $\mathbf{M}_{\mu \times \beta}(S)$ the additive groups of $(\mu \times \alpha)$-matrices over $\overline{S}$ and $(\mu \times \beta)$-matrices over S, respectively. We will define the set

$$\mathbf{M}_\mu(\overline{S}^\alpha S^\beta) = \left\{ (\mathrm{X} \,\|\, \mathrm{Y}) \; : \; (\mathrm{X}, \mathrm{Y}) \in \mathbf{M}_{\mu \times \alpha}(\overline{S}) \times \mathbf{M}_{\mu \times \beta}(S) \right\}$$

of mixed matrices whose μ rows are in $\overline{S}^\alpha \times S^\beta$. Note that $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$ is an additive group. For any $1 \le \delta \le \mu$, the operation in (6) naturally extends to $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$ as follows

$$\mathrm{P} * (\mathrm{X} \,\|\, \mathrm{Y}) = (\overline{\mathrm{P}}\mathrm{X} \,\|\, \mathrm{PY}), \tag{7}$$

for any P in $\mathbf{M}_{\delta \times \mu}(S)$ and for any $(\mathrm{X} \,\|\, \mathrm{Y})$ in $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$. When $\delta = \mu$, the additive group $\mathbf{M}_{\mu \times \mu}(S)$ is a ring with unit group $\mathrm{GL}_\mu(S)$, so the operation $*$ provides to the set $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$ a structure of $\mathbf{M}_{\mu \times \mu}(S)$-module.

A mixed-matrix G in $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$ is called a *generator mixed-matrix* for an $\overline{S}S$-linear code C, if the rows of G form an S-basis for C. This generator mixed-matrix can be written as $(\mathrm{G}_X \,\|\, \mathrm{G}_Y)$, where $\overline{\mathrm{G}}_X$ is a $\mu \times \alpha$-matrix over $\overline{S}$ and G_Y is a $\mu \times \beta$-matrix.

It is important to note that the set of mixed generator matrices for any $\overline{S}S$-linear code C with generator mixed-matrix G in $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$ is $\{\mathrm{P} * \mathrm{G} \; : \; \mathrm{P} \in \mathrm{GL}_\mu(S)\}$. It turns out that the number of rows of a generator mixed-matrix of any $\overline{S}S$-linear code C depends only on the algebraic structure of C and it is called the *rank* of C and we denote it by $\mathrm{rk}(C)$. Due to the structure theorem of finite modules over a finite chain ring, for any $\overline{S}S$-linear code C of length (α, β), there is a unique array $(\alpha, \beta; k_0, \ldots, k_{r-1}; \ell_0, \ldots, \ell_{s-1})$ of positive integers, called the *type* of C, such that C isomorphic to the S-module $\prod_{\substack{t=0 \\ k_t \ne 0}}^{r-1} \left(\overline{S} / \langle \overline{\theta}^{r-t} \rangle \right)^{k_t} \times \prod_{\substack{t=0 \\ \ell_t \ne 0}}^{s-1} (S / \langle \theta^{s-t} \rangle)^{\ell_t}$. The following result shows that any $\overline{S}S$-linear code of length (α, β) with rank μ admits a generator mixed-matrix in $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$.

Proposition 1. *[8, Proposition 3.2.] Any $\overline{S}S$-linear code of type $(\alpha, \beta; k_0, \ldots, k_{r-1}; \ell_0, \ldots, \ell_{s-1})$ has a generator mixed-matrix that is permutation equivalent to*

$$\left(\begin{array}{c|c} \mathrm{B} & \theta^{s-r}\mathrm{T} \\ \hline \mathrm{U} & \mathrm{A} \end{array} \right), \tag{8}$$

where

$$B = \begin{pmatrix} I_{k_0} & B_{0,1} & B_{0,2} & B_{0,3} & \cdots & B_{0,r-1} & B_{0,r} \\ 0 & \overline{\theta}I_{k_1} & \overline{\theta}B_{1,2} & \overline{\theta}B_{1,3} & \cdots & \overline{\theta}B_{1,r-1} & \overline{\theta}B_{1,r} \\ 0 & 0 & \overline{\theta}^2 I_{k_2} & \overline{\theta}^2 B_{2,3} & \cdots & \overline{\theta}^2 B_{2,r-1} & \overline{\theta}^2 B_{2,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \overline{\theta}^{r-1}I_{k_{r-1}} & \overline{\theta}^{r-1}B_{r-1,r} \end{pmatrix},$$

$$T = \begin{pmatrix} 0 & T_{0,1} & T_{0,2} & T_{0,3} & \cdots & T_{0,r-1} & T_{0,r} \\ 0 & 0 & \theta T_{1,2} & \theta T_{1,3} & \cdots & \theta T_{1,r-1} & \theta T_{1,r} \\ 0 & 0 & 0 & \theta^2 T_{2,3} & \cdots & \theta^2 T_{2,r-1} & \theta^2 T_{2,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & \theta^{r-1}T_{r-1,r} \end{pmatrix},$$

$$U = \begin{pmatrix} 0 & U_{0,1} & U_{0,2} & U_{0,3} & \cdots & U_{0,r-1} & U_{0,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & U_{s-r-1,1} & U_{s-r-1,2} & U_{s-r-1,3} & \cdots & U_{s-r-1,r-1} & U_{s-r-1,r} \\ 0 & 0 & \overline{\theta}U_{s-r,2} & \overline{\theta}U_{s-r,3} & \cdots & \overline{\theta}U_{s-r,r-1} & \overline{\theta}U_{s-r,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & \overline{\theta}^{r-1}U_{s-2,r} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

and

$$A = \begin{pmatrix} I_{\ell_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,s-1} & A_{0,s} \\ 0 & \theta I_{\ell_1} & \theta A_{1,2} & \theta A_{1,3} & \cdots & \theta A_{1,s-1} & \theta A_{1,s} \\ 0 & 0 & \theta^2 I_{\ell_2} & \theta^2 A_{2,3} & \cdots & \theta^2 A_{2,s-1} & \theta^2 A_{2,s} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \theta^{s-1}I_{\ell_{s-1}} & \theta^{s-1}A_{s-1,s} \end{pmatrix}.$$

Here $B_{i,j}$ are matrices over $\overline{S}$, and $T_{i,j}$ are matrices over S for $0 \leq i < r$, and $0 < j \leq r$. Furthermore, for $0 \leq i < s-1$, $0 < j \leq r$ and $0 < t \leq s$, $U_{i,j}$ are matrices over $\overline{S}$, and $A_{j,t}$ are matrices over R. Also, I_{k_i} and I_{ℓ_j} are identity matrices of sizes k_i and ℓ_j, respectively, where $0 \leq i \leq r-1$ and $0 \leq j \leq s-1$. Of course, if $r = s$, then the matrices U and A are suppressed in (8).

We can have a generator mixed-matrix over $\overline{S}^\alpha \times S^\beta$ as $\left(\begin{array}{c|c} I_\alpha & O \\ \hline O & I_\beta \end{array} \right)$ of type $(\alpha, \beta; \alpha, 0, \ldots, 0; \beta, 0, \ldots, 0)$, whereas $\overline{S}^\alpha \times S^\beta$ is not free as an S-module. In this case, we will say that an $\overline{S}S$-linear code is *weakly-free* if $k_1 = \cdots = k_{r-1} = \ell_1 = \cdots = \ell_{s-1} = 0$. Thus, a generator mixed-matrix in the form (8) of any weakly-free $\overline{S}S$-linear code C is

$$\left(\begin{array}{c|c} B & \theta^{s-r}T \\ \hline U & A \end{array}\right), \text{ where } A = \left(\begin{array}{cc} I_k & | & A_0 \end{array}\right), B = \left(\begin{array}{cc} I_\ell & | & B_0 \end{array}\right), T = \left(\begin{array}{cc} O & | & T_0 \end{array}\right) \text{ and }$$

$U = \left(\begin{array}{cc} O & | & U_0 \end{array}\right)$, where O is the zero matrix in $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$.

Remark 1. Let C be an $\overline{S}S$-linear code with generator mixed-matrix G in the form of Equation (8) of type $(\alpha, \beta; k_0, \cdots, k_{r-1}; \ell_0, \cdots, \ell_{s-1})$. The map

$$\begin{aligned} \texttt{End}_G : \mathbf{M}(C) &\to & C \\ \mathbf{m} &\mapsto & \mathbf{m} * G \end{aligned} \tag{9}$$

is bijective, where $\mathbf{M}(C) = \prod\limits_{\substack{t=0 \\ k_t \neq 0}}^{r} (\Gamma_{r-t}(S))^{k_t} \times \prod\limits_{\substack{t=0 \\ \ell_t \neq 0}}^{s} (\Gamma_{s-t}(S))^{\ell_t}$. Moreover, $|C| = $

$q^{m\left(\sum\limits_{t=0}^{r-1}(r-t)k_t + \sum\limits_{t=0}^{s-1}(s-t)\ell_t\right)}$.

Example 1.1. Let C be a $\mathbb{Z}_4\mathbb{Z}_8$-linear code of block-length $(3; 4)$ with generator mixed-matrix

$$\left(\begin{array}{ccc|cccc} 2 & 1 & 0 & 2 & 6 & 3 & 5 \\ 0 & 2 & 0 & 1 & 2 & 4 & 0 \\ 1 & 1 & 1 & 0 & 4 & 0 & 4 \\ 2 & 1 & 2 & 4 & 2 & 6 & 0 \end{array}\right).$$

Hence, as described in Proposition 1, C is permutation equivalent to a linear code with generator mixed-matrix:

$$\left(\begin{array}{ccc|cccc} 1 & 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 0 & 6 & 6 \\ \hline 0 & 0 & 0 & 1 & 0 & 6 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 1 \end{array}\right).$$

Thus the type of C is $(3, 4; 2, 0; 2, 0, 0)$ and $|C| = 2^{10}$. Moreover, C is weakly-free.

2. Characterization of Galois-invariant and Galois LCD codes over mixed alphabets

Throughout this section, $S|R$ will be a Galois extension with degree m and σ a generator of $\texttt{Aut}_R(S)$. Let $(\mathbf{x} \| \mathbf{y}) \in \overline{S}^\alpha \times S^\beta$ and $G \in \mathbf{M}_{\mu \times \alpha}(\overline{S}) \times \mathbf{M}_{\mu \times \beta}(S)$. For any $h \in \{0, 1, \ldots, m-1\}$, the h-Galois image of $(\mathbf{x} \| \mathbf{y})$ is given by

$$\sigma^h((\mathbf{x} \| \mathbf{y})) = \left(\overline{\sigma}^h(x_0), \cdots, \overline{\sigma}^h(x_{\alpha-1}), \| \sigma^h(y_0), \cdots, \sigma^h(y_{\beta-1})\right),$$

and the h-Galois image of G is given by $\sigma^h(\mathrm{G}) = \begin{pmatrix} \sigma^h(\mathrm{G}[1:]) \\ \vdots \\ \sigma^h(\mathrm{G}[\mu:]) \end{pmatrix}$, where G$[i:]$ is the

i-th row of G. If C is an $\overline{S}S$-linear code with generator mixed-matrix G, then $\sigma^h(C) :=$ $\left\{ \sigma^h(\mathbf{c}) : \text{ for all } \mathbf{c} \in C \right\}$ is also an $\overline{S}S$-linear code with generator mixed-matrix $\sigma^h(\mathrm{G})$.

2.1. Galois duality and Galois LCD codes

The h-Galois inner-product $\langle \cdot ; \cdot \rangle_h$ on $\overline{S}^\alpha \times S^\beta$ is defined as follows:

$$\langle (\mathbf{x} \,\|\, \mathbf{y}) , (\mathbf{x}' \,\|\, \mathbf{y}') \rangle_h = \theta^{s-r} \left(\sum_{j=0}^{\alpha-1} \iota(x_j \overline{\sigma}^h(x'_j)) \right) + \sum_{j=0}^{\beta-1} y_j \sigma^h(y'_j), \tag{10}$$

where $(\mathbf{x} \,\|\, \mathbf{y})$ and $(\mathbf{x}' \,\|\, \mathbf{y}')$ are in $\overline{S}^\alpha \times S^\beta$.

Note that $\langle (\mathbf{x} \,\|\, \mathbf{y}) , (\mathbf{x}' \,\|\, \mathbf{y}') \rangle_h = \chi(\langle \mathbf{x}, \mathbf{x}' \rangle_h) + \langle \mathbf{y}, \mathbf{y}' \rangle_h$, for all $(\mathbf{x}, \mathbf{x}')$ in $\overline{S}^\alpha \times \overline{S}^\alpha$ and $(\mathbf{y}, \mathbf{y}')$ in $S^\beta \times S^\beta$. For any (μ, λ) in $(\mathbb{N} \backslash \{0\})^2$, the h-Galois mixed-matrix product is defined as follows:

$$\begin{array}{rcl} \langle \cdot, \cdot \rangle_h : \mathbf{M}_\mu(\overline{S}^\alpha S^\beta) \times \mathbf{M}_\lambda(\overline{S}^\alpha S^\beta) & \to & \mathbf{M}_{\mu \times \lambda}(S) \\ (\mathrm{X}, \mathrm{Y}) & \mapsto & \langle \mathrm{X}, \mathrm{Y} \rangle_h = (\langle \mathrm{X}[i:], \mathrm{Y}[j:] \rangle_h)_{\substack{0 \le i < \mu \\ 0 \le i < \lambda}}. \end{array} \tag{11}$$

Moreover, $\langle \mathrm{X}, \mathrm{Y} \rangle_h = \langle \mathrm{X}, \sigma^h(\mathrm{Y}) \rangle_0$ and for any $\mathbf{m} \in S^\mu$, we have $\langle \mathbf{m} * \mathrm{X}, \mathrm{Y} \rangle_h = \mathbf{m} \langle \mathrm{X}, \mathrm{Y} \rangle_h$.

If $h = 0$, it is just the usual *Euclidean inner-product* and if $m = 2h$ it is the *Hermitian inner-product*. For any $\overline{S}S$-linear code C, the h-*Galois dual code* of C, denoted by $C^{\perp_h}$, is defined as

$$C^{\perp_h} = \left\{ \mathbf{u} \in \overline{S}^\alpha \times S^\beta : (\text{ for all } \mathbf{c} \in C)(\langle \mathbf{u}, \mathbf{c} \rangle_h = 0) \right\}.$$

Clearly, $C^{\perp_h}$ is an $\overline{S}S$-linear code of block-length (α, β). Theorem 9 in [3] holds for any finite chain ring, which follows that if the type of C is $(\alpha, \beta; k_0, \ldots, k_{r-1}; \ell_0, \ldots, \ell_{s-1})$, then the type of its h-Galois dual is

$$\left(\alpha, \beta; \alpha - \sum_{t=0}^{r-1} k_t, k_{r-1}, \ldots, k_1; \beta - \sum_{t=0}^{s-1} \ell_t, \ell_{s-1}, \ldots, \ell_1 \right).$$

Therefore, $|C| \times |C^{\perp_h}| = |\overline{S}^\alpha \times S^\beta|$ and moreover, C is weakly-free if and only if $C^{\perp_h}$ is weakly-free.

Remark 2. Let C be an $\overline{S}S$-linear code. Since $\langle \mathbf{u}, \mathbf{v} \rangle_h = \langle \mathbf{u}; \sigma^h(\mathbf{v}) \rangle_0 = \sigma^h \left(\langle \mathbf{u}; \mathbf{v} \rangle_{m-h} \right)$, it follows that $C^{\perp_h} = (\sigma^h(C))^{\perp_0} = \sigma^h(C^{\perp_{m-h}})$ and $C = (C^{\perp_h})^{\perp_{m-h}} = (C^{\perp_{m-h}})^{\perp_h}$.

The h-Galois hull of C is defined to be its intersection with its h-Galois dual, and is denoted by $\mathcal{H}_h(C)$. Thus, if C is a weakly-free $\overline{S}S$-linear code with generator mixed-matrix G in $\mathbf{M}_\mu(\overline{S}^\alpha S^\beta)$ then

$$\mathcal{H}_h(C) = \left\{ \mathbf{m} * \mathrm{G} \; : \; (\exists\, \mathbf{m} \in \mathbf{M}(C))\, (\langle \mathbf{m} * \mathrm{G}, \mathrm{G} \rangle_h = \mathbf{0}) \right\}. \tag{12}$$

We say that C is *h-Galois self-orthogonal* $\mathcal{H}_h(C) = C$ and C is *h-Galois self-dual* if $C = C^{\perp_h}$. C is a linear complementary h-Galois dual code (h-Galois LCD code) if $\mathcal{H}_h(C) = \{\mathbf{0}\}$. Note that if C and C' are monomial-equivalent $\overline{S}S$-linear codes, then C is h-Galois LCD code if and only if C' is h-Galois LCD code. Moreover, since $|C| \times |C^{\perp_h}| = |\overline{S}^\alpha \times S^\beta|$, it follows that any $\overline{S}S$-linear code C of block-length is an h-Galois LCD code if and only if $C \oplus C^{\perp_h} = \overline{S}^\alpha \times S^\beta$. Of course, if C is an h-Galois LCD code, then C is weakly-free.

From now on in the paper, $\mathbf{0}_\mu := \underbrace{(0, 0, \cdots, 0)}_{\mu \text{ times}}$, for some positive integer μ. We will need the following remark in the proof of the first result of this paper.

Remark 3. We have that $\mathtt{GL}_\mu(S) = \{\mathrm{M} \in \mathbf{M}_{\mu \times \mu}(S) : \mathtt{det}(\mathrm{M}) \notin \mathtt{J}(S)\}$, since $S^\times = S \backslash \mathtt{J}(S)$. Thus $\mathrm{M} \notin \mathtt{GL}_\mu(S)$ if and only if there exists $\mathbf{m} \in S^\mu$ such that $\theta^{s-1}\mathbf{m} \neq \mathbf{0}_\mu$ and $\theta^{s-1}\mathbf{m}\mathrm{M} = \mathbf{0}_\mu$.

From Theorem 2 in [6], LCD codes over chain rings are free. Thus from [6, Corollary 2], any code over a chain ring with generator mixed-matrix G is an LCD code if and only if GG^T is invertible. In [5], it was proved that for any $\mathbb{Z}_2\mathbb{Z}_4$-linear code C with generator mixed-matrix G, if GG^T is invertible then code C is a 0-Galois LCD code, but the inverse is not true (see Corollary 3.9 and Remark 3.8). The following result gives a characterization of Galois LCD codes over the finite chain ring mixed alphabet $\overline{S}S$. Note that been weakly-free is not a restriction since, as pointed before, h-Galois LCD codes are always weakly-free.

Theorem 1. *Let C be a weakly-free $\overline{S}S$-linear code with generator mixed-matrix G as in (8),*

$$\mathrm{G} = \begin{pmatrix} \mathrm{G}^{(r)} \\ \hline \mathrm{G}^{(s)} \end{pmatrix} = \left(\begin{array}{c||c} \mathrm{B} & \theta^{s-r}\mathrm{T} \\ \hline \mathrm{U} & \mathrm{A} \end{array} \right),$$

where $\mathrm{A} = \begin{pmatrix} \mathrm{I}_k & | & \mathrm{A}_0 \end{pmatrix}$, $\mathrm{B} = \begin{pmatrix} \mathrm{I}_\ell & | & \mathrm{B}_0 \end{pmatrix}$, $\mathrm{T} = \begin{pmatrix} \mathrm{O} & | & \mathrm{T}_0 \end{pmatrix}$ *and* $\mathrm{U} = \begin{pmatrix} \mathrm{O} & | & \mathrm{U}_0 \end{pmatrix}$.
Let us denote by $C^{(r)}$ the $\overline{S}$-linear code with generator matrix B and by $C^{(s)}$ the S-linear code with generator matrix A. If $\iota\left(\mathrm{B}\overline{\sigma}^h(\mathrm{U})^T \right) + \mathrm{T}\sigma^h(\mathrm{A})^T \in \mathbf{M}_{\ell \times k}(\mathtt{J}(S))$, then the following assertions are equivalent.

1. *C is an h-Galois LCD code.*

2. $A\sigma^h(A)^T$ *and* $B\overline{\sigma}^h(B)^T$ *are invertible.*

3. *There is a matrix P in* $\mathtt{GL}_\mu(S)$ *such that* $\langle G, G\rangle_h P = \left(\begin{array}{c|c} \theta^{s-r}I_k & O \\ \hline O & I_\ell \end{array}\right)$, *with* $\mu = k+\ell$.

4. $C^{(r)}$ *and* $C^{(s)}$ *are h-Galois LCD codes.*

Proof. We have

$$\langle G, G\rangle_h = \left(\begin{array}{c|c} \langle G^{(r)}, G^{(r)}\rangle_h & \langle G^{(r)}, G^{(s)}\rangle_h \\ \hline \langle G^{(s)}, G^{(r)}\rangle_h & \langle G^{(s)}, G^{(s)}\rangle_h \end{array}\right)$$

$$= \left(\begin{array}{c|c} \theta^{s-r}\left(\iota\left(B\overline{\sigma}^h(B)^T\right) + \theta^{s-r}T\sigma^h(T)^T\right) & \theta^{s-r}\left(\iota\left(B\overline{\sigma}^h(U)^T\right) + T\sigma^h(A)^T\right) \\ \hline \theta^{s-r}\left(\iota\left(U\overline{\sigma}^h(B)^T\right) + A\sigma^h(T)^T\right) & \theta^{s-r}\iota\left(U\overline{\sigma}^h(U)^T\right) + A\sigma^h(A)^T \end{array}\right).$$

Assume that $\iota\left(B\overline{\sigma}^h(U)^T\right) + T\sigma^h(A)^T \in \mathbf{M}_{\ell\times k}(\mathtt{J}(S))$.

1. $\Rightarrow$ **2.** Assume that either $B\overline{\sigma}^h(B)^T$ or $A\sigma^h(A)^T$ is a non-invertible matrix.

-   If $A\sigma^h(A)^T$ is non-invertible in $\mathbf{M}_{\ell\times\ell}(S)$ then, from Remark 3, there exists $\mathbf{m}$ in S^ℓ such that $\theta^{s-1}\mathbf{m} \neq \mathbf{0}_\ell$ and $\theta^{s-1}\mathbf{m}A\sigma^h(A)^T = \mathbf{0}_\ell \in S^\ell$. Thus, $(\mathbf{0}_k, \theta^{s-1}\mathbf{m})\langle G, G\rangle_h = \mathbf{0}_\mu$. It follows that

    $$(\mathbf{0}_k, \theta^{s-1}\mathbf{m})\langle G, G\rangle_h = \langle(\mathbf{0}_k, \theta^{s-1}\mathbf{m}) * G, G\rangle_h = \mathbf{0}_\mu.$$

    Now $(\mathbf{0}_k, \theta^{s-1}\mathbf{m}) * G = (\mathbf{0}_k, \theta^{s-1}\mathbf{m} \neq \mathbf{0}, \theta^{s-1}m A_0)$ since $\theta^{s-1}\mathbf{m} \neq \mathbf{0}_\ell$. From (12), we have $(\mathbf{0}_k, \theta^{s-1}\mathbf{m}) * G \in \mathcal{H}_h(C)$. Hence, C is a non h-Galois LCD code.

-   If the matrix $B\overline{\sigma}^h(B)^T$ is non-invertible in $\mathbf{M}_{k\times k}(\overline{S})$ then, again from Remark 3, there exists an element $\mathbf{m}$ in $(\Gamma_r(S))^k$ such that $\overline{\theta}^{\,r-1}\overline{\mathbf{m}} \neq \mathbf{0}_k$ and $\overline{\theta}^{\,r-1}\overline{\mathbf{m}}(B\overline{\sigma}^h(B)^T) = \mathbf{0}_k \in \overline{S}^k$. Thus, $(\theta^{r-1}\mathbf{m}, \mathbf{0}_\ell)\langle G, G\rangle_h = \mathbf{0}_\mu$. Since

    $$\theta^{r-1}\mathbf{m} * (B\overline{\sigma}^h(B)^T) = \overline{\theta}^{\,r-1}\overline{\mathbf{m}}(B\overline{\sigma}^h(B)^T), \text{ and}$$
    $$T\sigma^h(A)^T + \iota\left(B\overline{\sigma}^h(U)^T\right) \in \mathbf{M}_{\ell\times k}(\mathtt{J}(S)),$$

    it follows that

    $$(\theta^{r-1}\mathbf{m}, \mathbf{0}_\ell)\langle G, G\rangle_h = \langle(\theta^{r-1}\mathbf{m}, \mathbf{0}_\ell) * G, G\rangle_h = \mathbf{0}_\mu.$$

    From Equation (12), we have

    $$\mathbf{0} \neq (\theta^{r-1}\mathbf{m}, \mathbf{0}_\ell) * G = (\overline{\theta}^{\,r-1}\overline{\mathbf{m}}, \overline{\theta}^{\,r-1}\overline{\mathbf{m}}B_0, \theta^{s-1}\mathbf{m}T) \in \mathcal{H}_h(C).$$

    Thus, C is a non h-Galois LCD code.

    Therefore, either if $B\overline{\sigma}^h(B)^T$ or $A\sigma^h(A)^T$ is non-invertible, then C is not an h-Galois LCD code.

2. ⇒ 3. Assume that the matrices $B\overline{\sigma}^h(B)^T$ and $A\sigma^h(A)^T$ are invertible. Then $\iota\left(B\overline{\sigma}^h(B)^T\right) + \theta^{s-r}T\sigma^h(T)^T$ and $\langle G^{(s)}, G^{(s)}\rangle_h$ are also invertible. There are invertible matrices P_1 and P_2 with entries in S such that $P_1\langle G^{(s)}, G^{(s)}\rangle_h = \langle G^{(s)}, G^{(s)}\rangle_h P_1 = I_\ell$ and $P_2\langle G^{(r)}, G^{(r)}\rangle_h = \langle G^{(r)}, G^{(r)}\rangle_h P_2 = \theta^{s-r}I_k$. It follows that

$$\langle G, G\rangle_h \left(\begin{array}{c|c} P_2 & O \\ \hline O & P_1 \end{array}\right) = \left(\begin{array}{c|c} \theta^{s-r}I_k & \langle G^{(r)}, G^{(s)}\rangle_h P_1 \\ \hline \langle G^{(s)}, G^{(r)}\rangle_h P_2 & I_\ell \end{array}\right).$$

Then we have that

$$\langle G, G\rangle_h \left(\begin{array}{c|c} P_2 & O \\ \hline O & P_1 \end{array}\right) \left(\begin{array}{c|c} I_k & O \\ \hline -\langle G^{(r)}, G^{(s)}\rangle_h P_2 & I_\ell \end{array}\right)$$

$$= \left(\begin{array}{c|c} \theta^{s-r}I_k - \langle G^{(r)}, G^{(s)}\rangle_h P_1 \langle G^{(s)}, G^{(r)}\rangle_h P_2 & \langle G^{(r)}, G^{(s)}\rangle_h P_1 \\ \hline O & I_\ell \end{array}\right).$$

Now, $\langle G^{(r)}, G^{(s)}\rangle_h P_1 \langle G^{(s)}, G^{(r)}\rangle_h P_2 = \theta^{2(s-r)}M_1$, where M_1 is a matrix with entries in S. It follows that

$$\theta^{s-r}I_k - \langle G^{(r)}, G^{(s)}\rangle_h P_1 \langle G^{(s)}, G^{(r)}\rangle_h P_2 = \theta^{s-r}\left(I_k + \theta^{s-r}M_1\right)$$

and $I_k + \theta^{s-r}M_1$ is invertible. Hence there is an invertible matrix P_3 with entries in S such that $P_3(I_k + \theta^{s-r}M_1) = (I_k + \theta^{s-r}M_1)P_3 = I_k$. Thus

$$\langle G, G\rangle_h \left(\begin{array}{c|c} P_2 & O \\ \hline O & P_1 \end{array}\right) \left(\begin{array}{c|c} I_k & O \\ \hline -\langle G^{(r)}, G^{(s)}\rangle_h P_2 & I_\ell \end{array}\right) \left(\begin{array}{c|c} P_3 & O \\ \hline O & I_\ell \end{array}\right)$$

$$= \left(\begin{array}{c|c} \theta^{s-r}I_k & \langle G^{(r)}, G^{(s)}\rangle_h P_1 \\ \hline O & I_\ell \end{array}\right)$$

Now, $\langle G^{(r)}, G^{(s)}\rangle_h P_1 = \theta^{s-r}M_2$, where M_2 is a matrix with entries in S. Thus

$$\langle G, G\rangle_h \left(\begin{array}{c|c} P_2 & O \\ \hline O & P_1 \end{array}\right) \left(\begin{array}{c|c} I_k & O \\ \hline -\langle G^{(r)}, G^{(s)}\rangle_h P_2 & I_\ell \end{array}\right) \left(\begin{array}{c|c} P_3 & O \\ \hline O & I_\ell \end{array}\right) \left(\begin{array}{c|c} I_k & -M_2 \\ \hline O & I_\ell \end{array}\right)$$

$$= \left(\begin{array}{c|c} \theta^{s-r}I_k & O \\ \hline O & I_\ell. \end{array}\right).$$

Now if we take

$$P = \left(\begin{array}{c|c} P_2 & O \\ \hline O & P_1 \end{array}\right) \left(\begin{array}{c|c} I_k & O \\ \hline -\langle G^{(r)}, G^{(s)}\rangle_h P_2 & I_\ell \end{array}\right) \left(\begin{array}{c|c} P_3 & O \\ \hline O & I_\ell \end{array}\right) \left(\begin{array}{c|c} I_k & -M_2 \\ \hline O & I_\ell \end{array}\right),$$

we have $\langle \mathrm{G}, \mathrm{G} \rangle_h \mathrm{P} = \left(\begin{array}{c|c} \theta^{s-r} \mathrm{I}_k & \mathrm{O} \\ \hline \mathrm{O} & \mathrm{I}_\ell \end{array} \right)$ and $\mathrm{P} \in \mathtt{GL}_\mu(S)$, with $\mu = k + \ell$.

3. $\Rightarrow$ **1.** Assume that there is a matrix P in $\mathtt{GL}_\mu(S)$ such that $\langle \mathrm{G}, \mathrm{G} \rangle_h \mathrm{P} = \left(\begin{array}{c|c} \theta^{s-r} \mathrm{I}_k & \mathrm{O} \\ \hline \mathrm{O} & \mathrm{I}_\ell \end{array} \right)$, with $\mu = k + \ell$. Let $\mathbf{c} \in \mathcal{H}_h(C)$. Since

$$\mathcal{H}_h(C) = \left\{ \mathbf{m} * \mathrm{G} \; : \; (\mathbf{m} \in (\Gamma_r(S))^k \times S^\ell)(\langle \mathbf{m} * \mathrm{G}, \mathrm{G} \rangle_h = \mathbf{0}_\mu) \right\},$$

there exists $(\mathbf{m}, \mathbf{m}')$ in $(\Gamma_r(S))^k \times S^\ell$ such that $\langle (\mathbf{m}, \mathbf{m}') * \mathrm{G}, \mathrm{G} \rangle_h = \mathbf{0}_\mu$. As $\langle (\mathbf{m}, \mathbf{m}') * \mathrm{G}, \mathrm{G} \rangle_h = (\mathbf{m}, \mathbf{m}') \langle \mathrm{G}, \mathrm{G} \rangle_h$ and $\langle \mathrm{G}, \mathrm{G} \rangle_h \mathrm{P} = \left(\begin{array}{c|c} \theta^{s-r} \mathrm{I}_k & \mathrm{O} \\ \hline \mathrm{O} & \mathrm{I}_\ell \end{array} \right)$, it deduces that $(\mathbf{m}, \mathbf{m}') \langle \mathrm{G}, \mathrm{G} \rangle_h = \mathbf{m} \left(\begin{array}{c|c} \theta^{s-r} \mathrm{I}_k & \mathrm{O} \\ \hline \mathrm{O} & \mathrm{I}_\ell \end{array} \right) = \mathbf{0}_\mu \mathrm{P}^{-1} = \mathbf{0}_\mu$. Hence $\mathbf{m} \theta^{s-r} \mathrm{I}_k = \theta^{s-r} \mathbf{m} = \mathbf{0}_k$ and $\mathbf{m}' \mathrm{I}_\ell = \mathbf{m}' = \mathbf{0}_\ell$. But $\theta^{s-r} \mathbf{m} = \mathbf{0}_k \Leftrightarrow \mathbf{m} \in \theta^r S^k$. So $\mathbf{m} \in (\theta^r S^k) \cap (\Gamma_r(S))^k = \{\mathbf{0}_k\}$. Consequently $(\mathbf{m}, \mathbf{m}') = \mathbf{0}_\mu$ and henceforth C is an h-Galois LCD code.

2. $\Leftrightarrow$ **4.** From [17, Theorem 2.4.], it follows that $\pi_r(C^{(r)})$ is an h-Galois LCD code if and only if the matrix $\pi_r(\mathrm{B}(\overline{\sigma}^h(\mathrm{B}))^T)$ is invertible, and $\pi_s(C^{(s)})$ is an h-Galois LCD code if and only if the matrix $\pi_s(\mathrm{A}(\sigma^h(\mathrm{A}))^T)$ is invertible. Note that the proof of [6, Theorem 4] can be easily adapted to the present situation, and thus $C^{(r)}$ is an h-Galois LCD code if and only if $\mathrm{B}(\overline{\sigma}^h(\mathrm{B}))^T$ is invertible, and $C^{(s)}$ is an h-Galois LCD code if and only if $\mathrm{A}(\sigma^h(\mathrm{A}))^T$ is an invertible matrix. $\quad\square$

An $\overline{S}S$-linear code C is called *separable* if $C = C_X \times C_Y$, where C_X is an $\overline{S}$-linear code and C_Y is an S-linear code. It is easy to see that C has a generator mixed-matrix in the form $\left(\begin{array}{c|c} \mathrm{B} & \mathrm{O} \\ \hline \mathrm{O} & \mathrm{A} \end{array} \right)$, where B is a generator matrix for C_X and A is a generator matrix for C_Y. From Theorem 1, we have a generalization of [6, Proposition 4.3] as follows:

Corollary 1. *A separable $\overline{S}S$-linear code C is an h-Galois LCD code if and only if both C_X and C_Y are h-Galois LCD codes.*

Corollary 2. *Let C be an $\overline{S}S$-linear code with generator mixed-matrix* G.

1. *If* $\mathrm{G} = (\mathrm{B} \,||\, \theta^{s-r}\mathrm{T})$ *and* $\mathrm{B} := (\mathrm{I}_k \,|\, \mathrm{B}_0)$, *then C is h-Galois LCD if and only if* $\mathrm{B}\overline{\sigma}^h(\mathrm{B})^T$ *is invertible.*
2. *If* $\mathrm{G} = (\mathrm{U} \,||\, \mathrm{A})$ *and* $\mathrm{A} := (\mathrm{I}_\ell \,|\, \mathrm{A}_0)$, *then C is h-Galois LCD if and only if* $\mathrm{A}\overline{\sigma}^h(\mathrm{A})^T$ *is invertible.*

Remark 4. An $\overline{S}S$-linear code C is an h-Galois LCD code if and only if $C^{\perp_h}$ is an h-Galois LCD code.

Example 2.1. Let C be the $\mathbb{Z}_2\mathbb{Z}_4$-linear code of block-length $(3,5)$ with generator mixed-matrix $\left(\begin{array}{c|c} \mathrm{B} & 2\mathrm{T} \\ \hline \mathrm{U} & \mathrm{A} \end{array}\right)$, where

$$\left(\begin{array}{c|c} \mathrm{B} & 2\mathrm{T} \\ \hline \mathrm{U} & \mathrm{A} \end{array}\right) = \left(\begin{array}{ccc||ccccc} 1 & 0 & 1 & 0 & 2 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 & 2 & 0 & 2 \\ \hline 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 \end{array}\right).$$

We have $\sigma = \mathrm{Id}_{\mathbb{Z}_4}$, $\mathrm{TA}^T + \iota(\mathrm{BU}^T) = (0,0)^T \in \{0,2\}^2$, $\det(\mathrm{AA}^T) = 3$ and $\det(\mathrm{BB}^T) = 1$. Note that applying Theorem 1 we have that C is an LCD code.

2.2. Galois-invariant codes

The extension of a finite chain ring $\overline{S}|\overline{R}$ is also Galois and its Galois group $\mathrm{Aut}_{\overline{R}}(\overline{S})$ is generated by $\overline{\sigma}$. The set $\overline{S}S$ has a ring structure under the component-wise addition and multiplication. For example, the set $\mathbb{F}_2S := \{(x \| y) : x \in \mathbb{F}_2, y \in S\}$ where $S = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$, is a ring structure under the following laws: $(x\|y) + (x'\|y') := (x+x'\|y+y')$ and $(x\|y) \cdot (x'\|y') := (xx'\|yy')$.

Therefore, the ring-extension $\overline{S}S \,|\, \overline{R}R$ is Galois and its Galois group G is $\left\{(\overline{\sigma}^i \| \sigma^i) : 0 \le i < m\right\}$. Without loss of generality, we say that σ is a generator of the Galois group of $\overline{S}S \,|\, \overline{R}R$. Let C be an $\overline{S}S$-linear code of type $(\alpha, \beta; k_0, \dots, k_{r-1}; \ell_0, \dots, \ell_{s-1})$. One can define the *subring-subcode* of C to $\overline{R}R$ as $\mathrm{Res}_R(C) = C \cap (\overline{R}^\alpha \times R^\beta)$ and the *trace code* $\mathrm{Tr}(C)$ of C over R as

$$\mathrm{Tr}(C) = \left\{ \left(\overline{\mathrm{Tr}}(c_0), \dots, \overline{\mathrm{Tr}}(c_{\alpha-1}) \,\|\, \mathrm{Tr}(c_0'), \dots, \mathrm{Tr}(c_{\beta-1}')\right) : \right.$$
$$\left. (c_0, \dots, c_{\alpha-1} \,\|\, c_0', \dots, c_{\beta-1}') \in C \right\}, \tag{13}$$

where $\mathrm{Tr} = \sum\limits_{i=0}^{m-1} \sigma^i$ and $\overline{\mathrm{Tr}} = \sum\limits_{i=0}^{m-1} \overline{\sigma}^i$. It is clear that $\mathrm{Tr}(\sigma(C)) = \mathrm{Tr}(C)$ and $\mathrm{Res}_R(C)$, $\mathrm{Tr}(C)$ are also $\overline{R}R$-linear codes. The smallest submodule of the S-module $\overline{S}^\alpha \times S^\beta$ containing C will be denoted $\mathrm{Ext}(C)$. So $\mathrm{Ext}(C)$ is the set of all S-linear combinations of codewords in C. The same arguments as in [18] can be easily adapted to the mixed alphabets to prove that $\mathrm{Res}_R(C) = \mathrm{Res}(\mathrm{Ext}(\mathrm{Res}_R(C)))$; $\mathrm{Res}_R(C) \subseteq \mathrm{Tr}(C)$ and $C \subseteq \mathrm{Ext}(\mathrm{Res}_R(C))$. Note that $\mathrm{Ext}(\mathcal{H}_0(C)) = \mathcal{H}_0(\mathrm{Ext}(C))$. The following theorem generalizes Delsarte's celebrated result that relates the restriction and the trace operators by means of the duality.

Proposition 2 *(Generalized Delsarte's theorem). Let $S|R$ be a Galois extension of a finite chain ring. Any $\overline{S}S$-linear code C satisfies*

$$\mathbf{Tr}(C^{\perp_h}) = \mathbf{Res}_R(C)^{\perp_0},$$

where $C^{\perp_h}$ is the h-Galois dual of C in $\overline{S}^\alpha \times S^\beta$ and $\mathbf{Res}(C)^{\perp_0}$ is the Euclidean dual of $\mathbf{Res}_R(C)$ in $\overline{R}^\alpha \times R^\beta$.

Proof. Let C be an $\overline{S}S$-linear code of block-length (α, β). Let $\mathbf{a} \in \mathbf{Tr}(C^{\perp_h})$. Then there exists $\mathbf{b}$ in $C^{\perp_h}$ such that $\mathbf{a} = \mathbf{Tr}(\mathbf{b})$. Therefore, for all $\mathbf{c}$ in $\mathbf{Res}_R(C)$, we have $0 = \langle \mathbf{b}, \mathbf{c} \rangle_h = \langle \mathbf{b}, \mathbf{c} \rangle_0$ and

$$\langle \mathbf{a}, \mathbf{c} \rangle_0 = \theta^{s-r} \sum_{j=0}^{\alpha-1} \iota(\overline{\mathbf{Tr}}(x_j) c_j) + \sum_{j=0}^{\beta-1} \mathbf{Tr}(y_j) c'_j = \mathbf{Tr}(\langle \mathbf{b}, \mathbf{c} \rangle_0) = \mathbf{Tr}(0) = 0.$$

Hence $\mathbf{a} \in \mathbf{Res}_R(C)^{\perp_0}$. This proves that $\mathbf{Tr}(C^{\perp_h}) \subseteq \mathbf{Res}_R(C)^{\perp_0}$.

On the other hand, since the inclusion $\mathbf{Res}_R(C)^{\perp_0} \subseteq \mathbf{Tr}(C^{\perp_h})$ is equivalent to $\mathbf{Tr}(C^{\perp_h})^{\perp_0} \subseteq \mathbf{Res}_R(C)$. Let $\mathbf{a} \in \mathbf{Tr}(C^{\perp_h})^{\perp_0}$. By definition, for all $\mathbf{b} \in C^{\perp_h}$ and for all $\lambda \in S$, we have $\lambda * \mathbf{b} \in C^{\perp_h}$ and $0 = \langle \mathbf{a}, \mathbf{Tr}(\lambda * \mathbf{b}) \rangle_0 = \mathbf{Tr}(\langle \lambda * \mathbf{b}, \mathbf{a} \rangle_{m-h}) = \mathbf{Tr}(\lambda * \langle \mathbf{a}, \mathbf{b} \rangle_{m-h}) = \mathbf{Tr}(\lambda \langle \mathbf{a}, \mathbf{b} \rangle_{m-h})$. Therefore, for all $\lambda \in S$, we have $0 = \mathbf{Tr}(\lambda \langle \mathbf{a}, \mathbf{b} \rangle_{m-h})$. Since $S|R$ is Galois, the symmetric bilinear form $\langle \cdot ; \cdot \rangle : S \times S \mapsto R$ defined by $\langle x, y \rangle = \mathbf{Tr}(xy)$ is non-degenerate, it follows that for all $\mathbf{b}$ in $C^{\perp_h}$, $\langle \mathbf{a}, \mathbf{b} \rangle_{m-h} = 0$. From Remark 2, $(C^{\perp_h})^{\perp_{m-h}} = C$ and so $\mathbf{a} \in (C^{\perp_h})^{\perp_{m-h}} = C$. Now $\mathbf{a} \in \mathbf{Tr}(C^{\perp_h})^{\perp_0} \subseteq \overline{R}^\alpha \times R^\beta$. Hence $\mathbf{a} \in \mathbf{Res}_R(C)$. $\square$

The $\overline{S}S$-linear code C is G-invariant if $\sigma(C) = C$, for some generator σ of G. From Remark 2, a relationship between Galois duality and G-invariance is the following

Corollary 3. *If C is a G-invariant code, then $C^{\perp_h} = C^{\perp_0}$.*

Since the arguments in [18, Lemma 2 and Theorem 1] also hold for any $\overline{S}S$-linear code C of block-length (α, β). Therefore, we have that

Corollary 4.

1. *If C is a G-invariant code, then $\mathbf{Res}_R(C) = \mathbf{Tr}(C)$.*
2. *If $C = \mathbf{Ext}(D)$, where $D \subseteq \overline{R}^\alpha \times R^\beta$, then C is a G-invariant code.*

Consider the map

$$
\begin{aligned}
\chi : \overline{S}^\alpha \times S^\beta &\to \theta^{s-r} S^\alpha \times S^\beta \\
(\mathbf{x} \,\|\, \mathbf{y}) &\mapsto (\theta^{s-r} \iota(\mathbf{x}) \,\|\, \mathbf{y}).
\end{aligned}
\tag{14}
$$

Note that $\theta^{s-r} \Gamma_r(S) = \theta^{s-r} S$ and χ is an isomorphism of S-modules. In Theorem 1 in [18], it was proved that if S is a Galois extension of the chain ring R, then any S-linear code is a G-invariant code if and only if it has a generator matrix over R. The following

result provides a characterization of G-invariant codes over a finite chain ring mixed alphabet.

Theorem 2. *Let $S|R$ be a Galois extension of a finite chain ring and C an $\overline{S}S$-linear code with generator mixed-matrix G. The following statements are equivalent.*

1. *C is a G-invariant code.*
2. *$\chi(C)$ is a G-invariant code.*
3. *C has a generator mixed-matrix over $\overline{R}R$.*

Proof. We have $\sigma \circ \chi = \chi \circ \sigma$.

$1. \Rightarrow 2.$) Assume that $\sigma(C) = C$. Then $\sigma(\chi(C)) = \chi(\sigma(C)) = \chi(C)$. Thus, $\chi(C)$ is a G-invariant code.

$2. \Rightarrow 3.$) Assume that the code $\chi(C)$ is G-invariant. From [18, Theorem 1], there exists a matrix (G_X, G_Y) in $\mathbf{M}_{k \times \alpha}(\Gamma_r(R)) \times \mathbf{M}_{k \times \beta}(R)$ and a matrix P in $\mathtt{GL}_\mu(S)$ such that $\chi(G) = P(\theta^{s-r} G_X \,|\, G_Y)$. It follows that $G = P * (\overline{G_X} \,\|\, G_Y)$ and thus, $(\overline{G_X} \,\|\, G_Y)$ is a generator mixed-matrix of the code C over the ring $\overline{R}R$.

$3. \Rightarrow 1.$) It is a straightforward consequence of item 2 in Corollary 4. □

The G-core of the code C, denoted by C_G, is the largest G-invariant subcode of C. It is easy to see that $C_G = \bigcap_{i=0}^{m-1} \sigma^i(C)$. Note that C is G-invariant if and only if $C = C_G$. From Corollary 4 and Theorem 2, we have the following two results that can be proven add in the same steps as the proofs in [18, Corollary 1 and Theorem 2].

Corollary 5. *Let $S|R$ be a Galois extension of finite chain rings and C an $\overline{S}S$-linear code. The following statements follow.*

1. *$C_G = \mathtt{Ext}(\mathtt{Res}_R(C))$.*
2. *If $\mathtt{Res}_R(C) = \mathtt{Tr}(C)$, then C is G-invariant.*

Corollary 6. *Let $S|R$ be a Galois extension with Galois group G and C be an $\overline{S}S$-linear code. The following assertions are satisfied.*

1. *C is a G-invariant code if and only if $C^{\perp_h}$ is a G-invariant code.*
2. *If C is a G-invariant code, then C is an h-Galois LCD code for some $0 \le h \le |G|$ if and only if $\mathtt{Res}_R(C)$ is an LCD code.*

3. Gray image of linear codes over finite chain rings

In [13], a homogeneous weight $\mathtt{wt}_{\overline{S}}$ on the finite chain ring $\overline{S}$ was defined as follows: if $r = 1$ then $\mathtt{wt}_{\overline{S}}$ is the Hamming weight $\mathtt{w}_H$, otherwise

$$\mathtt{wt}_{\overline{S}}(x) = \begin{cases} 0, & \text{if } x = 0_{\overline{S}}; \\ (q^m - 1)q^{m(r-2)}, & \text{if } \vartheta(x) \leq r - 2; \\ q^{m(r-1)}, & \text{if } \vartheta(x) = r - 1. \end{cases} \tag{15}$$

Thus, for any $(x \,\|\, y) \in \overline{S}S$, the weight of $(x \,\|\, y)$ is defined by: $\mathtt{wt}_{q^m}((x \,\|\, y)) = \mathtt{wt}_{\overline{S}}(x) + \mathtt{wt}_S(y)$, where $\mathtt{wt}_{\overline{S}}$ and $\mathtt{wt}_S$ are the homogeneous weights on $\overline{S}$ and S, respectively. This homogeneous weight $\mathtt{wt}_{q^m}$ can be extended component-wise on $\overline{S}^\alpha \times S^\beta$ as:

$$\mathtt{wt}_{q^m}(x_0, \cdots, x_{\alpha-1} \,\|\, y_0, \cdots, y_{\beta-1})$$
$$= \mathtt{wt}_{\overline{S}}(x_0) + \cdots + \mathtt{wt}_{\overline{S}}(x_{\alpha-1}) + \mathtt{wt}_S(y_0) + \cdots + \mathtt{wt}_S(y_{\beta-1}).$$

Let $\varpi_m = (1, \cdots, 1)$ and $\underline{\varepsilon}_m = (0, 1, \varepsilon, \cdots, \varepsilon^{q^m-2})$ be vectors in $(\mathbb{F}_{q^m})^{q^m}$, where ε is an element in $\mathbb{F}_{q^m}$ of order $q^m - 1$. We use the tensor product $\otimes$ (expanded from right to left) over $\mathbb{F}_{q^m}$ to defined the vector

$$c_t = \underbrace{\varpi_m \otimes \cdots \otimes \varpi_m}_{r-t-2 \text{ times}} \otimes \underline{\varepsilon}_m \otimes \underbrace{\varpi_m \otimes \cdots \otimes \varpi_m}_{t \text{ times}},$$

for $0 \leq t < r \leq s$. Consider the matrix $\mathrm{G}_{(q^m, r)}$, whose c_t is its t-th row. Of course, if $r = 2$, then $c_0 = \underline{\varepsilon}_m$ and $c_1 = \varpi_m$. Note that $\mathrm{G}_{(q^m, r)}$ is a generator matrix of the first order generalized Reed-Müller code $\mathrm{RM}_{q^m}(1, r - 1)$ over $\mathbb{F}_{q^m}$ length q^{r-1} (see for example [16] for a definition and reference on Reed-Müller and Generalized Reed-Müller codes). Then, Jitman's Gray map defined in [15] is naturally generalized to $\overline{S}^\alpha \times S^\beta$ as follows

$$\Phi_{(S,r)} : \overline{S}^\alpha \times S^\beta \to (\mathrm{RM}_{q^m}(1, r - 1))^\alpha \times (\mathrm{RM}_{q^m}(1, s - 1))^\beta \tag{16}$$
$$(\mathbf{a}, \mathbf{b}) \mapsto \left(\overline{\gamma}(\mathbf{a})\mathrm{G}_{(q^m, r)}, \gamma(\mathbf{b})\mathrm{G}_{(q^m, s)} \right),$$

where

$$\overline{\gamma} : \overline{S}^\alpha \to ((\mathbb{F}_{q^m})^\alpha)^r \qquad \gamma : S^\beta \to ((\mathbb{F}_{q^m})^\beta)^s$$
$$\mathbf{a} \mapsto (\widetilde{\overline{\gamma}_0(\mathbf{a})}, \widetilde{\overline{\gamma}_1(\mathbf{a})}, \cdots, \widetilde{\overline{\gamma}_{r-1}(\mathbf{a})}) \quad \text{and} \quad \mathbf{b} \mapsto (\widetilde{\overline{\gamma}_0(\overline{\mathbf{b}})}, \widetilde{\overline{\gamma}_1(\overline{\mathbf{b}})}, \cdots, \widetilde{\overline{\gamma}_{s-1}(\overline{\mathbf{b}})})$$

are bijective maps defined with the t-th $\overline{\theta}$-adic coordinate map $\overline{\gamma}_t : \overline{S} \to \Gamma(\overline{S})$ that is usually extended coordinate-wise to $\overline{\gamma}_t : \overline{S}^n \to \Gamma(\overline{S})^n$, where $n \in \{\alpha, \beta\}$. From [15, Proposition 3.1.], it is easy to see that the Jitman's Gray map $\Phi_{(S,r)}$ is an injective isometry from $\left(\overline{S}^\alpha \times S^\beta; d_{\mathtt{hom}} \right)$ to $\left((\mathbb{F}_{q^m})^{\alpha q^{m(r-1)} + \beta q^{m(s-1)}}; d_{\mathtt{H}} \right)$, where $d_{\mathtt{H}}$ denotes the Hamming distance on $(\mathbb{F}_{q^m})^{\alpha q^{m(r-1)} + \beta q^{m(s-1)}}$.

Let C be an $\overline{S}S$-linear code C of the block-length (α, β). Then

$$\Phi_{(S,r)}(C) \subseteq (\mathrm{RM}_{q^m}(1, r - 1))^\alpha \times (\mathrm{RM}_{q^m}(1, s - 1))^\beta \subseteq (\mathbb{F}_{q^m})^{\alpha q^{m(r-1)} + \beta q^{m(s-1)}}$$

and $\Phi_{(S,r)}(C)$ is called the Jitman's Gray image of C. Now

$$\left((\mathrm{RM}_{q^m}(1,r-1))^\alpha \times (\mathrm{RM}_{q^m}(1,s-1))^\beta\right)^{\perp_h}$$
$$= \left((\mathrm{RM}_{q^m}(1,r-1))^{\perp_h}\right)^\alpha \times \left((\mathrm{RM}_{q^m}(1,s-1))^{\perp_h}\right)^\beta,$$

and $(\mathrm{RM}_{q^m}(1,r-1))^{\perp_h} = (\widetilde{\sigma}(\mathrm{RM}_{q^m}(1,r-1)))^{\perp_0}$ and $(\mathrm{RM}_{q^m}(1,s-1))^{\perp_h} = (\widetilde{\sigma}(\mathrm{RM}_{q^m}(1,s-1)))^{\perp_0}$. One can check that $\widetilde{\sigma}(\mathrm{RM}_{q^m}(1,r-1))$ is also a first order Generalized Reed-Müller code over $\mathbb{F}_{q^m}$ of length q^{r-1}.

Note that if $S = \mathbb{F}_{q^m}[\theta]$, then $\Phi_{(S,r)}$ is a monomorphism of $\mathbb{F}_{q^m}$-linear spaces. Thus, Jitman's Gray image of any $\mathbb{F}_{q^m}[\overline{\theta}]\mathbb{F}_{q^m}[\theta]$-linear code with type $(\alpha,\beta; k_0,k_1,\ldots k_{r-1}; \ell_0,\ell_1,\ldots,\ell_{s-1})$ is a linear code of length $q^{m(r-1)}\alpha + q^{m(s-1)}\beta$ and dimension $\sum_{t=0}^{r-1}(r-t)k_t + \sum_{t=0}^{s-1}(s-t)\ell_t$.

Remark 5. In [13], a Gray map on any finite chain ring is defined, we will call it Greferath's Gray map $\Psi_{(S,r)}$. It is important to note that for Jitman's Gray map $\Phi_{(S,r)}$ and Greferath's Gray map $\Psi_{(S,r)}$ on $\overline{S}^\alpha \times S^\beta$, there exists a permutation map $\tau : (\mathbb{F}_{q^m})^{\alpha q^{m(r-1)}+\beta q^{m(s-1)}} \to (\mathbb{F}_{q^m})^{\alpha q^{m(r-1)}+\beta q^{m(s-1)}}$ such that $\Psi_{(S,r)} = \tau \circ \Phi_{(S,r)}$. Without loss of generality in the sequel of this paper, we will use Jitman's Gray map $\Phi_{(S,r)}$ on $\overline{S}^\alpha \times S^\beta$. For any $\overline{S}S$-linear code C, the subset $\Phi_{(S,r)}(C)$ of $\overline{S}^\alpha \times S^\beta$ is called the Gray image of C. Note that $\Phi_{(S,r)}(C)$ is not always linear.

Example 3.1. Consider the finite chain ring $R := \mathbb{F}_q[\theta]$ with $\theta \neq \theta^2 = 0$. Then we have that $\mathrm{G}_{(q,2)} = \begin{pmatrix} 0 & 1 & 2 & \cdots & q-1 \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$, and Jitman's Gray map $\Phi_{(R,1)}$ is given by

$$\Phi_q : (\mathbb{F}_q)^\alpha \times R^\beta \to (\mathbb{F}_q)^{\alpha+2\beta}$$
$$(\mathbf{a}||\mathbf{b}) \mapsto \left(\mathbf{a},(\gamma_0(\mathbf{b}),\gamma_1(\mathbf{b}))\mathrm{G}_{(q,2)}\right).$$

Thus $\Phi_q(\mathbf{a}||\mathbf{b}) = (\mathbf{a},\gamma_1(\mathbf{b}),\gamma_0(\mathbf{b})+\gamma_1(\mathbf{b}),\gamma_0(\mathbf{b})+2\gamma_1(\mathbf{b}),\cdots,\gamma_0(\mathbf{b})+(q-1)\gamma_1(\mathbf{b}))$.

In the following, we will establish the conditions for a Galois LCD $\overline{S}S$-linear code C so that its Gray image C is an LCD code over $\mathbb{F}_{q^m}$. Generalized Reed-Müller codes over $\mathbb{F}_{q^m}$ of the length $q^{m(r-1)}$ have the following properties (see [16]):

- for $i \leq j \leq r-1$, $\mathrm{RM}_{q^m}(i,r-1) \subseteq \mathrm{RM}_{q^m}(j,r-1)$;
- $\mathrm{RM}_{q^m}(i,r-1)^{\perp_0} = \mathrm{RM}_{q^m}(j,r-1)$, with $j = (r-1)(q^m-1)-i-1$.

If we fix $i = 1$ in the above term and assume that $(r-1)(q^m-1) \geq 3$. We have

$$\mathrm{RM}_{q^m}(i,r-1)^{\perp_0} = \mathrm{RM}_{q^m}((r-1)(q^m-1)-2,r-1).$$

Thus

$$\mathrm{RM}_{q^m}(1, r-1) \subseteq \mathrm{RM}_{q^m}(i, r-1)^{\perp_0} = \mathrm{RM}_{q^m}((r-1)(q^m-1)-2, r-1).$$

Since $0 < r \leq s$, it follows that $0 \leq (r-1)(q^m-1) \leq (s-1)(q^m-1)$ and we have the following result:

Lemma 1. *Let C be an $\overline{S}S$-linear code C of the block-length (α, β) with $0 < r \leq s$ and $h \in \{0, 1, \ldots, m-1\}$. If*

$$(r-1)(q^m-1) \geq 3$$

then $\Phi_{(S,r)}(C) \subseteq (\Phi_{(S,r)}(C))^{\perp_h}$.

As $0 < r \leq s$, it follows that $0 \leq (r-1)(q^m-1) \leq (s-1)(q^m-1) \leq 2$ if and only if $m = 1$ and $(q, s) \in \{(2; 2), (2; 3), (3; 2)\}$. In the case $q \in \{2; 3\}$ and $s = 2$, either $S = \mathbb{Z}_{q^2}$ or $S = \mathbb{F}_q[\theta]$ with $\theta \neq \theta^2 = 0$. The map

$$\varphi_q : \quad \mathbb{Z}_{q^2} \quad \rightarrow \quad \mathbb{F}_q[\theta]$$
$$b + qc \mapsto \pi(b) + \theta\pi(c)$$

is extended to $(\mathbb{F}_q)^\alpha \times (\mathbb{Z}_{q^2})^\beta$ as follows

$$\Upsilon_q : (\mathbb{F}_q)^\alpha \times (\mathbb{Z}_{q^2})^\beta \rightarrow (\mathbb{F}_q)^\alpha \times (\mathbb{F}_q[\theta])^\beta$$
$$(\mathbf{a} \| \mathbf{b} + q\mathbf{c}) \quad \mapsto (\mathbf{a} \| \pi(\mathbf{b}) + \theta\pi(\mathbf{c})).$$

Denote $\star$ the component-wise product. The following result is straightforward.

Proposition 3. *The maps $\varphi_q : \mathbb{Z}_{q^2} \to \mathbb{F}_q[\theta]$ and $\Upsilon_q : (\mathbb{F}_q)^\alpha \times (\mathbb{Z}_{q^2})^\beta \to (\mathbb{F}_q)^\alpha \times (\mathbb{F}_q[\theta])^\beta$ are bijective and for all $(\mathbf{v}, \mathbf{w})$ in $((\mathbb{F}_q)^\alpha \times (\mathbb{Z}_{q^2})^\beta)^2$ and $(x, y) \in \{0, 1, \ldots, q-1\}^2$, the following assertions are satisfied.*

1. $d_{hom}(\mathbf{v}, \mathbf{w}) = d_{hom}(\Upsilon_q(\mathbf{v}), \Upsilon_q(\mathbf{w}))$,
2. $\Upsilon_q((x + qy) * \mathbf{u}) = (\pi(x) + \theta\pi(y)) * \Upsilon_q(\mathbf{u})$,
3. $\Upsilon_q(\mathbf{u} \star \mathbf{v}) = \Upsilon_q(\mathbf{u}) \star \Upsilon_q(\mathbf{v})$,
4. $\Upsilon_q(\mathbf{v} + \mathbf{w}) = \Upsilon_q(\mathbf{v}) + \Upsilon_q(\mathbf{w}) + \Upsilon_q\left(q * \left(\mathbf{u}^{\star(q-1)} \star \mathbf{v}^{\star(q-1)}\right)\right)$, *where* $\mathbf{u}^{\star(q-1)} = \underbrace{u \star u \star \cdots \star u}_{q-1 \ times}$.

Note that for any $\mathbb{F}_q\mathbb{Z}_{q^2}$-linear code C, the subset $\Upsilon_q(C)$ of $(\mathbb{F}_q)^\alpha \times (\mathbb{F}_q[\theta])^\beta$ is $\mathbb{F}_q\mathbb{F}_q[\theta]$-linear if and only if $q * \left(\mathbf{u}^{\star(q-1)} \star \mathbf{v}^{\star(q-1)}\right) \in C$, for any $(\mathbf{u}, \mathbf{v})$ in $C \times C$.

Lemma 2. *Let $\mathbf{u} = (u \| u')$ and $\mathbf{v} = (v \| v')$ in $(\mathbb{F}_q)^\alpha \times (\mathbb{Z}_{q^2})^\beta$ such that $q * \left(\mathbf{u}^{\star(q-1)} \star \mathbf{v}^{\star(q-1)}\right) = (\mathbf{0}_\alpha \| \mathbf{0}_\beta)$. The following statements hold.*

1. $\varphi_q(\langle \mathbf{u}, \mathbf{v} \rangle) = \langle \Upsilon_q(\mathbf{u}), \Upsilon_q(\mathbf{v}) \rangle$ *and* $\langle \Phi_q(\Upsilon_q(\mathbf{u})), \Phi_q(\Upsilon_q(\mathbf{v})) \rangle_0 \in \mathbb{F}_q$.
2. *If* $q = 2$ *then* $\langle \Upsilon_2(\mathbf{u}), \Upsilon_2(\mathbf{v}) \rangle = \theta \langle \Phi_2(\Upsilon_2(\mathbf{u})), \Phi_2(\Upsilon_2(\mathbf{v})) \rangle_0$;
3. *If* $q = 3$ *then* $\langle \Phi_3(\Upsilon_3(\mathbf{u})), \Phi_3(\Upsilon_3(\mathbf{v})) \rangle_0 = \langle u; v \rangle_0$.

Proof. We set $\mathbf{u} = (u \,\|\, u'_1 + q u'_2)$ and $\mathbf{v} = (v \,\|\, v'_1 + q v'_2)$, where $(u, v) \in ((\mathbb{F}_q)^\alpha)^2$ and $(u'_1, u'_2, v'_1, v'_2) \in \{0, 1, \ldots, q-1\}^{4\beta}$. Suppose that $q * (\mathbf{u}^{\star(q-1)} \star \mathbf{v}^{\star(q-1)}) = (\mathbf{0}_\alpha \,\|\, \mathbf{0}_\beta)$. We have

$$q * \left(\mathbf{u}^{\star(q-1)} \star \mathbf{v}^{\star(q-1)} \right) = (\mathbf{0}_\alpha \,\|\, q * (u'_1 \star v'_1)^{\star(q-1)}).$$

Therefore, $q * (u'_1 \star v'_1)^{\star(q-1)} = \mathbf{0}_\beta$ implies that either $q(u'_1)^{\star(q-1)} = \mathbf{0}_\beta$ or $q(v'_1)^{\star(q-1)} = \mathbf{0}_\beta$. It follows that $\langle u'_1, v'_1 \rangle_0 = 0$. Thus

1. $\langle \Upsilon_q(\mathbf{u}), \Upsilon_q(\mathbf{v}) \rangle = \theta \left(\langle u, v \rangle_0 + \pi(\langle u'_1, v'_2 \rangle_0 + \langle u'_2, v'_1 \rangle_0) \right)$ and $\langle \mathbf{u}, \mathbf{v} \rangle = q(\iota(\langle u, v \rangle_0) + \langle u'_1, v'_2 \rangle_0 + \langle u'_2, v'_1 \rangle_0)$, since $\langle u'_1 + q u'_2, v'_1 + q v'_2 \rangle_0 = q(\langle u'_1, v'_2 \rangle_0 + \langle u'_2, v'_1 \rangle_0)$. Hence, $\varphi_q(\langle \mathbf{u}, \mathbf{v} \rangle) = \langle \Upsilon_q(\mathbf{u}), \Upsilon_q(\mathbf{v}) \rangle$.
2. If $q = 2$, then

$$\langle \Phi_2(\Upsilon_2(\mathbf{u})), \Phi_2(\Upsilon_2(\mathbf{v})) \rangle_0 = \langle u, v \rangle_0 + (\pi(u'_1), \pi(u'_2)) \mathrm{G}_{(2,2)} \mathrm{G}_{(2,2)}^T \begin{pmatrix} \pi(v'_1)^T \\ \pi(v'_2)^T \end{pmatrix}, \text{ and}$$

$$\mathrm{G}_{(2,2)} \mathrm{G}_{(2,2)}^T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus $(\pi(u'_1), \pi(u'_2)) \mathrm{G}_{(2,2)} \mathrm{G}_{(2,2)}^T \begin{pmatrix} \pi(v'_1) \\ \pi(v'_2) \end{pmatrix} = \langle \pi(u'_1), \pi(v'_2) \rangle_0 + \langle \pi(u'_2), \pi(v'_1) \rangle_0 \in \mathbb{F}_q$, since $\langle u'_1, v'_1 \rangle_0 = 0$. Hence $\langle \Upsilon_2(\mathbf{u}), \Upsilon_2(\mathbf{v}) \rangle = \theta \langle \Phi_2(\Upsilon_2(\mathbf{u})), \Phi_2(\Upsilon_2(\mathbf{v})) \rangle_0$.
3. If $q = 3$, then

$$\langle \Phi_3(\Upsilon_3(\mathbf{u})), \Phi_3(\Upsilon_3(\mathbf{v})) \rangle_0 = \langle u, v \rangle_0 + (\pi(u'_1), \pi(u'_2)) \mathrm{G}_{(3,2)} \mathrm{G}_{(3,2)}^T \begin{pmatrix} \pi(v'_1)^T \\ \pi(v'_2)^T \end{pmatrix}, \text{ and}$$

$$\mathrm{G}_{(3,2)} \mathrm{G}_{(3,2)}^T = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus $\langle \Phi_3(\Upsilon_3(\mathbf{u})), \Phi_3(\Upsilon_3(\mathbf{v})) \rangle_0 = \langle u, v \rangle_0 \in \mathbb{F}_q$, since $\langle u'_1, v'_1 \rangle_0 = 0$. Hence $\langle \Phi_3(\Upsilon_3(\mathbf{u})), \Phi_3(\Upsilon_3(\mathbf{v})) \rangle_0 = \langle u; v \rangle_0$. $\square$

Let $\mathcal{C}$ be an $\mathbb{F}_q \mathbb{Z}_{q^2}$-linear code of block-length (α, β). We will define the set $\mathcal{D}_\mathcal{C}$ as

$$\mathcal{D}_\mathcal{C} = \left\{ q * \left(\mathbf{u}^{\star(q-1)} \star \mathbf{v}^{\star(q-1)} \right) \,:\, (\mathbf{u}, \mathbf{v}) \in \mathcal{C} \times \mathcal{C}^\perp \right\}.$$

Note that $\Upsilon(\mathcal{D}_\mathcal{C}) = \mathcal{D}_{\Upsilon(\mathcal{C})}$ and $\mathcal{D}_\mathcal{C} \subseteq \{\mathbf{0}_\alpha\} \times \{0, q\}^\beta$. The following results are consequences of Lemma 2.

Corollary 7. *Let C be an $\mathbb{F}_q\mathbb{Z}_{q^2}$-linear code such that $\mathcal{D}_C = \{(\mathbf{0}_\alpha \,\|\, \mathbf{0}_\beta)\}$. The following assertions hold.*

1. $\Upsilon_q(C^\perp) = \Upsilon_q(C)^\perp$, *where* $(\Upsilon_q(C))^\perp$ *denotes the Euclidean dual of* $\Upsilon_q(C)$ *as an $\mathbb{F}_q\mathbb{F}_q[\theta]$-linear code.*
2. *If $q = 2$, then $\Phi_2(\Upsilon_2(C^\perp)) = \Phi_2(\Upsilon_2(C))^\perp$, where $\Phi_2(\Upsilon_2(C))^\perp$ denotes the Euclidean dual of $\Phi_2(\Upsilon_2(C))$ as an $\mathbb{F}_2$-linear code.*
3. *If $q = 3$, then $\Phi_3(\Upsilon_3(C^\perp)) = (C_X)^\perp$, where C_X is the punctured code obtained from C by deleting these β last coordinates.*

Theorem 3. *Let C be an $\mathbb{F}_q\mathbb{Z}_{q^2}$-linear code such that $\mathcal{D}_C = \{(\mathbf{0}_\alpha \,\|\, \mathbf{0}_\beta)\}$. The following statements hold.*

1. *C is an $\mathbb{F}_q\mathbb{Z}_{q^2}$-LCD code if and only if $\Upsilon_q(C)$ is an $\mathbb{F}_q\mathbb{F}_q[\theta]$-LCD code.*
2. *If $q = 2$, then C is a $\mathbb{Z}_2\mathbb{Z}_4$-LCD code if and only if $\Phi_2(\Upsilon_2(C))$ is a binary LCD code.*
3. *If $q = 3$, then C is a $\mathbb{Z}_3\mathbb{Z}_9$-LCD code if and only if C_X is a ternary LCD code.*

We end the paper with an example of an optimal LCD code over $\mathbb{F}_p$ ($p \in \{2; 3\}$) derived from this family of $\mathbb{F}_p R$-LCD codes (either $R = \mathbb{Z}_{p^2}$, or $R = \mathbb{F}_p[\theta]$ with $u^2 = 0$).

Example 3.2. Consider the $\mathbb{Z}_2\mathbb{Z}_4$-LCD code C given in Example 2.1. From [7, Theorem 3.], the parity-check matrix H of C is given by:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Thus

$$2 * H = \begin{pmatrix} 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}.$$

Then, we have

$$\mathcal{D}_C = \big\{ 2 * (\mathbf{u} \star \mathbf{v}) : (\mathbf{u}, \mathbf{v}) \in C \times C^\perp \big\} = \{(\mathbf{0}_3 \,\|\, \mathbf{0}_5)\}.$$

From Theorem 3, $\Upsilon_2(C)$ is an $\mathbb{F}_2\mathbb{F}_2[\theta]$-LCD code. The binary image $\Phi_2(\Upsilon_2(C))$ has parameters $[13, 4, 6]$. This is an optimal code which is obtained directly in contrast to the indirect constructions presented in [12].

4. Conclusions

The concept and basic properties of LCD and Galois-invariant codes over finite chain rings have been generalized to linear complementary dual codes over a mixed alphabet of finite chain rings. We have studied the Jitman's Gray image of an $\overline{S}S$-code and when it is an LCD code. When $q \in \{2; 3\}$, any $\mathbb{F}_q\mathbb{Z}_{q^2}$-linear code $\mathcal{C}$ such that $\mathcal{D}_\mathcal{C} = \{(\mathbf{0}_\alpha \parallel \mathbf{0}_\beta)\}$, is an LCD code if and only if the code given by its Jitman's Gray image is an LCD code. Thus we have covered the rings $\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_9, \mathbb{F}_2[X]/\langle X^2 \rangle, \mathbb{F}_2[X]/\langle X^3 \rangle, \mathbb{F}_3[X]/\langle X^2 \rangle$. The construction of binary or ternary LCD codes from Jitman's Gray image of $\mathbb{Z}_4\mathbb{Z}_8$-LCD code, $\mathbb{Z}_2\mathbb{Z}_8$-LCD code, $\mathbb{F}_2\mathbb{F}_2[u]$-LCD code, or $\mathbb{F}_2[v]\mathbb{F}_2[u]$-LCD code ($u^2 \neq u^3 = 0$ and $v \neq v^2 = 0$) remains as an open problem.

Data availability

No data was used for the research described in the article.

Acknowledgments

References

[1] I. Aydogdu, I. Siap, The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes: bounds on the minimum distance, Appl. Math. Inf. Sci. 7 (6) (2013) 2271–2278.

[2] I. Aydogdu, T. Abualrub, I. Siap, On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes, Int. J. Comput. Math. 92 (9) (2015) 1806–1814.

[3] I. Aydogdu, I. Siap, On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, Linear Multilinear Algebra 63 (10) (2015) 2089–2102.

[4] I. Aydogdu, I. Siap, R. Ten-Valls, On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes, Finite Fields Appl. 48 (Nov. 2017) 241–260.

[5] N. Benbelkacem, J. Borges, S.T. Dougherty, C. Fernández-Córdoba, On $\mathbb{Z}_2\mathbb{Z}_4$-additive complementary dual codes and related LCD codes, Finite Fields Appl. 62 (2020) 101622.

[6] S. Bhowmick, A. Fotue-Tabue, E. Martínez-Moro, R. Bandi, S. Bagchi, Do non-free LCD codes over finite commutative Frobenius rings exist?, Des. Codes Cryptogr. 88 (2020) 825–840.

[7] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifa, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality, Des. Codes Cryptogr. 54 (2010) 167–179.

[8] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, Linear and cyclic codes over direct product of finite chain rings, Math. Methods Appl. Sci. (2017) 1–11.

[9] C. Carlet, S. Guilley, Complementary dual codes for countermeasures to side-channel attacks, Adv. Math. Commun. 10 (1) (Mar. 2016) 131–150.

[10] S.T. Dougherty, H. Liu, Independence of vectors in codes over rings, Des. Codes Cryptogr. 51 (2009) 55–68.

[11] A. Fotue Tabue, E. Martínez-Moro, C. Mouaha, Galois correspondence on linear codes over finite chain rings, Discrete Math. 343 (2020) 111653.

[12] M. Grassl, Code tables: bounds on the parameters of various types of codes, online database, available at, http://www.codetables.de/. (Accessed 30 July 2022).

[13] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear $(36, 3^{12}, 15)$ ternary code, IEEE Trans. Inf. Theory 45 (Nov. 1999) 2522–2524.

[14] X. Hou, X. Meng, J. Gao, On $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic and complementary dual codes, IEEE Access 9 (May 2021) 65914–65924.

[15] J. Jitman, P. Udomkavanich, The Gray image of codes over finite chain rings, Int. J. Contemp. Math. Sci. 5 (10) (2010) 449–458.

[16] T. Kasami, S. Lin, W.W. Peterson, New generalizations of the Reed-Muller codes. Part I: primitive codes, IEEE Trans. Inf. Theory IT-14 (2) (March 1968).

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

[18] E. Martínez-Moro, A.P. Nicolás, F. Rua, On trace codes and Galois invariance over finite commutative chain rings, Finite Fields Appl. 22 (2013) 114–121.

[19] B.R. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.

[20] R. Wu, M. Shi, Some classes of mixed alphabet codes with few weights, IEEE Commun. Lett. 25 (5) (May. 2021) 1431–1434, https://doi.org/10.1109/LCOMM.2020.3038876.