Galois Correspondence on Linear Codes over Finite Chain Rings

A. Fotue Tabue[a], E. Martínez-Moro[b,*], C. Mouaha[c]

[a]*Department of mathematics, Faculty of Sciences, University of Yaoundé 1, Cameroon*
[b]*Institute of Mathematics, University of Valladolid, Spain*
[c]*Department of mathematics, Higher Teachers Training College of Yaoundé, University of Yaoundé 1, Cameroon*

Abstract

Given $S|R$ a finite Galois extension of finite chain rings and $\mathscr{B}$ an S-linear code we define two Galois operators, the closure operator and the interior operator. We proof that a linear code is Galois invariant if and only if the row standard form of its generator matrix has all entries in the fixed ring by the Galois group and show a Galois correspondence in the class of S-linear codes. As applications some improvements of upper and lower bounds for the rank of the restriction and trace code are given and some applications to S-linear cyclic codes are shown.

Keywords: Finite chain rings, Galois Correspondence, Linear codes, Cyclic codes.
AMS Subject Classification 2010: 51E22; 94B05

1. Introduction

Let R a be finite chain ring of index nilpotency s, S the *Galois extension* of R of rank m, and G the group of ring automorphisms of S fixing R. We will denote by $\mathscr{L}(S^\ell)$ (resp. $\mathscr{L}(R^\ell)$) the set of S-linear codes (resp. R-linear codes) of length ℓ. There are two classical constructions that allow us to build an element of $\mathscr{L}(R^\ell)$ from an element $\mathscr{B}$ of $\mathscr{L}(S^\ell)$. One is the *restriction code* of $\mathscr{B}$ which is defined as $\mathrm{Res}_R(\mathscr{B}) := \mathscr{B} \cap R^\ell$. The second one is based on the fact that the trace map $\mathrm{Tr}_R^S = \sum_{\sigma \in G} \sigma$ is a linear form, therefore it follows that the set

$$\mathrm{Tr}_R^S(\mathscr{B}) := \left\{ (\mathrm{Tr}_R^S(c_1), \cdots, \mathrm{Tr}_R^S(c_\ell)) | (c_1, \cdots, c_\ell) \in \mathscr{B} \right\}, \tag{1}$$

is an R-linear code. The relation between the trace code and the restriction code will be given by a generalization (see Theorem 1) of the celebrated result due to Delsarte [2]

$$\mathrm{Tr}_R^S(\mathscr{B}^{\perp_{\varphi'}}) = \mathrm{Res}_R(\mathscr{B})^{\perp_\varphi}, \tag{2}$$

where $\perp_\varphi$ and $\perp_{\varphi'}$ denote the duality operators associated to the bilinear forms $\varphi : \mathsf{R}^\ell \times \mathsf{R}^\ell \to \mathsf{R}$ and $\varphi' : \mathsf{S}^\ell \times \mathsf{S}^\ell \to \mathsf{S}$ defined in Section 2.3.

Restriction codes is a core topic in coding theory. Note that many well-known codes can be defined as a restriction code, for instance BCH codes and, more generally, alternant codes (see [10, Chap.12]). Also in [1] restriction codes and the closure operator on the set of linear codes over $\mathbb{F}_{q^m}$ of length ℓ are used intensely to determine the parameters of additive cyclic codes. More recently, the restriction code, trace code and Galois invariance over extension of finite fields were studied in [6], and their results were extended to separable Galois extensions of finite chain rings in [8]. In this paper, we will study the following operators on $\mathscr{L}(\mathsf{S}^\ell)$

$$
\begin{array}{rcl}
\widetilde{} : \mathscr{L}(\mathsf{S}^\ell) & \to & \mathscr{L}(\mathsf{S}^\ell) \\
\mathscr{B} & \mapsto & \widetilde{\mathscr{B}} := \bigvee_{\sigma \in G} \sigma(\mathscr{B}),
\end{array}
\quad \text{and} \quad
\begin{array}{rcl}
{}^\circ : \mathscr{L}(\mathsf{S}^\ell) & \to & \mathscr{L}(\mathsf{S}^\ell) \\
\mathscr{B} & \mapsto & \overset{\circ}{\mathscr{B}} := \bigcap_{\sigma \in G} \sigma(\mathscr{B})
\end{array} ,
$$

and we will give answer to the question if there is a Galois correspondence between $\mathscr{B}$ and G for each $\mathscr{B}$ in $\mathscr{L}(\mathsf{S}^\ell)$. We will make some improvements of the bounds for the rank of restriction and trace of S-linear code and also, when ℓ and q are coprime, we will answer whether a linear cyclic code over R is a restriction of a linear cyclic Galois invariant code over a extension of R or not.

The outline of the paper is as follows. In Section 2 we give some preliminaries in finite commutative chain rings and their Galois extensions. We also formulate a generator matrix in row standard form for linear codes over finite chain rings. Section 3 presents the study of the Galois operators on the lattice of linear codes. Finally in Section 4 we describe linear cyclic codes over finite chain rings as the restriction of a linear cyclic code over a Galois extension of a finite chain ring.

2. Preliminaries

2.1. Finite chain rings

A finite commutative ring with identity is called a *finite chain ring* if its ideals are linearly ordered by inclusion. It is well known that every ideal of a finite chain ring is principal and therefore its maximal ideal is unique. R will denote a finite chain ring, θ a generator of its maximal ideal $\mathfrak{m} = \mathsf{R}\theta$, $\mathbb{F}_{p^n} = \mathsf{R}/\mathfrak{m}$ its residue field, and $\pi : \mathsf{R} \to \mathbb{F}_q$ the canonical projection. As stated before the ideals of R form a chain $\mathsf{R} \supsetneq \mathsf{R}\theta \supsetneq \cdots \supsetneq \mathsf{R}\theta^{s-1} \supsetneq \mathsf{R}\theta^s = \{0\}$ where the integer s is called the *nilpotency index* of R. It is easy to see that the cardinal of $\mathsf{R}^\times$, the set of ring units, is $p^{n(s-1)}(p^n - 1)$. Thus $\mathsf{R}^\times \simeq \Gamma(\mathsf{R})^* \times (1 + \mathsf{R}\theta)$ where $\Gamma(\mathsf{R})^* = \{b \in \mathsf{R} \mid b \neq 0, b^{p^n} = b\}$ is the only subgroup of $\mathsf{R}^\times$ isomorphic to $\mathbb{F}_{p^n} \setminus \{0\}$. The set $\Gamma(\mathsf{R}) = \Gamma(\mathsf{R})^* \cup \{0\}$ is a complete set of representatives of R modulo θ and it is called the *Teichmüller set* of R. The set $\Gamma(\mathsf{R})$ is a coordinate set of R [11, Proposition 3.3], i.e. each element $a \in \mathsf{R}$ can be expressed uniquely as a θ-*adic decomposition*

$$
a = a_0 + a_1\theta + \cdots + a_{s-1}\theta^{s-1}, \tag{3}
$$

where $a_0, a_1, \cdots, a_{s-1} \in \Gamma(\mathsf{R})$. The θ-adic decomposition of elements of R allows us to defines the t-th θ-adic coordinate function as

$$
\begin{array}{rcl}
\gamma_t : \mathsf{R} & \to & \Gamma(\mathsf{R}) \\
a & \mapsto & a_t
\end{array}
\quad t = 0, 1, \cdots, s-1, \tag{4}
$$

where $a = \gamma_0(a) + \gamma_1(a)\theta + \cdots + \gamma_{s-1}(a)\theta^{s-1}$. Therefore we have a *valuation function* of R, defined by $\vartheta_\mathsf{R}(a) := \min\{t \in \{0, 1, \cdots, s\} \mid \gamma_t(a) \neq 0\}$ and a *degree function* of R, defined by $\deg_\mathsf{R}(a) := \max\{t \in \{0, 1, \cdots, s\} \mid \gamma_t(a) \neq 0\}$, for each a in R. We will assume that $\vartheta_\mathsf{R}(0) = s$ and $\deg_\mathsf{R}(0) = -\infty$.

2.2. Galois extensions

Let R and S be two finite chain rings with residue fields $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ respectively. We say that S is an *extension* of R and we denote it by S|R if $R \subseteq S$ and $1_R = 1_S$. $\text{Aut}_R(S)$ will denote the group of automorphisms of S which fix the elements of R. Note that the map $\sigma : a \mapsto \sum_{t=0}^{s-1} \gamma_t(a)^q \theta^t$ for all $a \in S$, is in $\text{Aut}_R(S)$ and throughout of this paper G will be the subgroup of $\text{Aut}_R(S)$ generated by σ. For each subring T such that $R \subseteq T \subseteq S$ and for each subgroup of G one can respectively define the *fixed group* of T in G and the *fixed ring* of H in S as

$$\text{Stab}_G(T) := \left\{ \varrho \in G \,\middle|\, \varrho(a) = a, \text{ for all } a \in T \right\}, \qquad \text{Fix}_S(H) := \left\{ a \in S \,\middle|\, \varrho(a) = a, \text{ for all } \varrho \in H \right\}.$$

Definition 2.1. The ring S is a *Galois extension* of R with Galois group G if

1. $\text{Fix}_S(G) = R$ and
2. there are elements $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}; \alpha_0^*, \alpha_1^*, \cdots, \alpha_{m-1}^*$ in S such that

$$\sum_{t=0}^{m-1} \sigma^i(\alpha_t)\sigma^j(\alpha_t^*) = \delta_{i,j},$$

for all $i, j = 0, 1, \cdots, |G| - 1$(where $\delta_{i,j} = 1_S$ if $i = j$, and 0_S otherwise).

Note that a Galois extension is separable but the converse is not true in general as it was stated in [9], for a complete discussion on this fact see [15]. If S|R is a *Galois extension* with Galois group G then Tr_R^S is a free generator of $\text{Hom}_R(S, R)$ as an S-module. The following result in [3, Chap. III, Theorem 1.1] provide us the Galois correspondence for finite chain rings.

Lemma 1. *Let $S|R$ be a Galois extension with Galois group G. If T a Galois extension of R and T is a subring of S, then the Galois group of $T|R$ is $Stab_G(T)$. Furthermore, $Stab_G(Fix_S(H)) = H$ and $Fix_S(Stab_G(T)) = T$.*

We say that the pair $(\text{Stab}_G, \text{Fix}_S)$ is a *Galois correspondence* between G and S. Note that the Galois extension S|R is a free R-module with $|G| = \text{rank}_R(S)$ (see [3, Chap. III], [9, Theorem V.4]) and $G = \text{Aut}_R(S)$ (see [9, Theorem XV.10]). From now on $\underline{\alpha} := \{\alpha_0, \alpha_1, \cdots, \alpha_{m-1}\}$ will denote a free R-basis of S and $\mathbb{M}_{\underline{\alpha}} := \left(\text{Tr}_R^S(\alpha_i \alpha_j) \right)_{\substack{0 \le i < m \\ 0 \le j < m}}$ will be the matrix associate to $\underline{\alpha}$.

Proposition 1. *Let $S|R$ be a Galois extension with Galois group G. Then the matrix $\mathbb{M}_{\underline{\alpha}}$ is invertible.*

Proof. Since $\text{rank}_R(S) = \text{rank}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = m$, by [9, Theorem V.5], $\{\pi(\alpha_0), \pi(\alpha_1), \cdots, \pi(\alpha_{m-1})\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. So In fact, $\text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \circ \pi = \pi \circ \text{Tr}_R^S$ and $\pi(S^\times) = \mathbb{F}_{q^m} \setminus \{0\}$. So by [16, Theorem 8.3] the determinant of $\mathbb{M}_{\underline{\alpha}}$ is a ring unit. □

Hence there are elements $\alpha_0^*, \alpha_1^*, \cdots, \alpha_{m-1}^*$ in S such that $\text{Tr}_R^S(\alpha_i \alpha_j^*) = \delta_{i,j}$ and $(\alpha_0^*, \alpha_1^*, \cdots, \alpha_{m-1}^*) = \mathbb{M}_{\underline{\alpha}}^{-1}(\alpha_0, \alpha_1, \cdots, \alpha_{m-1})$. Thus the set $\{\alpha_0^*, \alpha_1^*, \cdots, \alpha_{m-1}^*\}$ is a free R-basis of S called the *trace-dual basis* of $\{\alpha_0, \alpha_1, \cdots, \alpha_{m-1}\}$.

2.3. Bilinear forms

An *S-linear code* of length ℓ is a S-module of S^ℓ, and the elements of $\mathscr{B}$ are called *codewords*. From now on we will assume that all codes are of length ℓ unless stated otherwise.

Let be $\mathbf{a}$ and $\mathbf{b}$ in S^ℓ, their Euclidean inner product is defined as $(\mathbf{a}, \mathbf{b})_E = a_1 b_1 + a_2 b_2 + \cdots + a_\ell b_\ell$, and if m is even their Hermitian inner product is defined as $(\mathbf{a}, \mathbf{b})_H = (\sigma^{\frac{m}{2}}(\mathbf{a}), \mathbf{b})_E$. Note that $(-, -)_E$ is a symmetric bilinear form.

For all $\mathbf{a}$ in S^ℓ and $\mathbf{b}$ in R^ℓ, $\mathtt{Tr}_R^S((\mathbf{a}, \mathbf{b})_E) = \left(\mathtt{Tr}_R^S(\mathbf{a}), \mathbf{b} \right)_E$, and if m is even, $\mathtt{Tr}_R^S((\mathbf{a}, \mathbf{b})_H) = \mathtt{Tr}_R^S((\mathbf{a}, \mathbf{b})_E)$, since $\mathtt{Tr}_R^S\left(\sigma^{\frac{m}{2}}(\mathbf{a})\right) = \mathtt{Tr}_R^S(\mathbf{a})$. Throughout the paper $\varphi = (-, -)_E$ and if m is even $\varphi' = (-, -)_H$, otherwise $\varphi' = (-, -)_E$. It is clear that

$$\varphi(\mathbf{b}, \mathtt{Tr}_R^S(\mathbf{a})) = \varphi(\mathtt{Tr}_R^S(\mathbf{a}), \mathbf{b}) = \mathtt{Tr}_R^S(\varphi'(\mathbf{a}, \mathbf{b})), \text{ for all } \mathbf{a} \in S^\ell \text{ and } \mathbf{b} \in R^\ell. \tag{5}$$

Lemma 2. *Let $\mathscr{B}$ be an S-linear code. Then*

$$\mathscr{B}^{\perp_{\varphi'}} := \left\{ \boldsymbol{a} \in S^\ell \,|\, \varphi'(\boldsymbol{a}, \boldsymbol{c}) = 0, \text{ for all } \boldsymbol{c} \in \mathscr{B} \right\}$$

is an S-linear code of the same length as $\mathscr{B}$ and $\left(\mathscr{B}^{\perp_{\varphi'}} \right)^{\perp_{\varphi'}} = \mathscr{B}$.

Proof. Let $\mathbf{a}$ be in S^ℓ, the map $\varphi'_{\mathbf{a}} := \varphi'(\mathbf{a}, -)$ is an S-linear form. Therefore $\mathscr{B}^{\perp_{\varphi'}} = \underset{\mathbf{c} \in \mathscr{B}}{\cap} \mathtt{Ker}(\varphi'_{\mathbf{c}})$ is an S-linear code. If m is odd, $\varphi = \varphi' = (-, -)_E$, by [12, Theorem 3.10. (iii)], $\left(\mathscr{B}^\perp \right)^\perp = \mathscr{B}$. Otherwise,

$$\mathscr{B}^{\perp_H} = \left\{ \mathbf{a} \in S^\ell \,|\, (\mathbf{a}, \mathbf{c})_E = 0, \text{ for all } \mathbf{c} \in \sigma^{\frac{m}{2}}(\mathscr{B}) \right\} = (\sigma^{\frac{m}{2}}(\mathscr{B}))^\perp.$$

Thus $\left(\mathscr{B}^{\perp_H} \right)^{\perp_H} = \left(\sigma^{\frac{m}{2}}(\mathscr{B})^\perp \right)^{\perp_H} = \left(\sigma^{\frac{2m}{2}}(\mathscr{B})^\perp \right)^\perp$. Since $\sigma^{\frac{2m}{2}} = \sigma^m = \mathtt{Id}$ it follows that $\left(\mathscr{B}^{\perp_H} \right)^{\perp_H} = \left(\mathscr{B}^\perp \right)^\perp = \mathscr{B}$. $\qquad\square$

The S-linear code $\mathscr{B}^{\perp_{\varphi'}}$ is called φ'-*dual code* of the code $\mathscr{B}$ associated to the S-bilinear form φ'. The following theorem generalizes Delsarte's celebrated result [2].

Theorem 1 (Delsarte Theorem). *Let $\mathscr{B}$ be an S-linear code then $\mathtt{Tr}_R^S(\mathscr{B}^{\perp_{\varphi'}}) = \mathtt{Res}_R(\mathscr{B})^\perp$.*

Proof. Let $\mathbf{a} \in \mathtt{Tr}_R^S(\mathscr{B}^{\perp_{\varphi'}})$. Then $\mathbf{a} = \mathtt{Tr}_R^S(\mathbf{b})$ and $\mathbf{b} \in \mathscr{B}^{\perp_{\varphi'}}$. For all $\mathbf{c} \in \mathtt{Res}_R(\mathscr{B})$,

$$\begin{aligned} \varphi(\mathbf{a}, \mathbf{c}) &= \varphi(\mathtt{Tr}_R^S(\mathbf{b}), \mathbf{c}), \\ &= \mathtt{Tr}_R^S(\varphi'(\mathbf{b}, \mathbf{c})), \text{ from (5)} \\ &= \mathtt{Tr}_R^S(0), \\ &= 0. \end{aligned}$$

Thus $\mathtt{Tr}_R^S(\mathscr{B}^{\perp_{\varphi'}}) \subseteq \mathtt{Res}_R(\mathscr{B})^\perp$.

On the other hand, let $\mathbf{a} \in \left(\mathtt{Tr}_R^S(\mathscr{B}^{\perp_{\varphi'}}) \right)^\perp$, we have that for all $\mathbf{c}$ in $\mathscr{B}^{\perp_{\varphi'}}$, $\varphi(\mathbf{a}, \mathtt{Tr}_R^S(\mathbf{c})) = 0$. Thus for all λ in S $\lambda \mathbf{c} \in \mathscr{B}$ and it follows that $\varphi(\mathbf{a}, \mathtt{Tr}_R^S(\lambda \mathbf{c})) = 0$. Considering the relation (5) we have that $\mathtt{Tr}_R^S(\varphi'(\mathbf{a}, \lambda \mathbf{c})) = 0$ and since $\varphi'(\mathbf{a}, -)$ is linear we get that $\varphi'(\mathbf{a}, \lambda \mathbf{c}) = \lambda \varphi'(\mathbf{a}, \mathbf{c})$. Hence, $\mathtt{Tr}_R^S(\lambda \varphi'(\mathbf{a}, \mathbf{c})) = 0$ for all λ in S. Therefore by Lemma 2 we have $\mathtt{Res}_R(\mathscr{B}) \subseteq \mathtt{Tr}_R^S(\mathscr{B}^{\perp_{\varphi'}})$.

$\qquad\square$

2.4. Generator matrix in row standard form

Usually to each S-linear code can be associated a generator matrix in standard form that involves permuting the columns of the original generator matrix, i.e. the code generated by the new matrix is permutation equivalent to the original one (see [12, Proposition 3.2]). We will now reformulate a more detailed version of this result in order to define a unique generator matrix in row standard canonical for an S-linear code that generates the code and that will be helpful in determining whether a code is Galois invariant or not.

Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ be non-zero vectors in S^ℓ, we say that they are *S-independent* if for all $a_1, a_2, \ldots, a_k$ in S we have that $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{0}$ implies that $a_i\mathbf{v}_i = \mathbf{0}$, for all i. Let $\mathscr{B}$ be an S-linear code, the codewords $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k \in \mathscr{B}$ form an *S-basis* of $\mathscr{B}$ if they are independent and they *generate* $\mathscr{B}$ as an S module. Any S-linear code $\mathscr{B}$ admits an S-basis and any two S-basis of $\mathscr{B}$ has the same number of codewords, see [4, Theorems 4.6–4.7]. The number of codewords of an S-basis of $\mathscr{B}$ is called rank of $\mathscr{B}$ and it will be denoted as $\mathrm{rank}_S(\mathscr{B})$. We also will denote by $\mathrm{row}(A)$ the S-linear code generated by the rows of the matrix A.

The set of all $k \times \ell$ matrices over S will be denote by $S^{k \times \ell}$. A matrix $A \in S^{k \times \ell}$ is said be a *full-rank matrix* if $\mathrm{rank}(A) = k$. A matrix A with entries in S is called a *generator matrix* for the code $\mathscr{B}$ if the set of rows of A is a basis of $\mathscr{B}$, therefore it is a full-rank matrix. We will denote by $\mathrm{GL}_k(S)$ the group of invertible matrices in $S^{k \times k}$. We say that the matrices A and B in $S^{k \times \ell}$ are row-equivalent if there exists a matrix $P \in \mathrm{GL}_k(S)$ such that $B = PA$.

Definition 2.2. Let A be a matrix in $S^{k \times \ell}$ and $A[i :]$ the i-th row of A; $A[: j]$ the j-th column of A; $A[i; j]$ the (i, j)-entry of A.

1. The *valuation function* of A is the mapping $\vartheta_A : \{1, \cdots, k\} \to \{0, 1, \cdots, s\}$, defined by

$$\vartheta_A(i) := \vartheta_S(A[i :]) := \min\{\vartheta_S(A[i; j]) \mid 1 \leq j \leq \ell\}.$$

2. The *pivot* of a nonzero row $A[i :]$ of A, is the first entry among all the entries least with valuation in that row. By convention, the pivot of the zero row is its first entry.
3. The *pivot function* of A is the mapping $\rho : \{1, \cdots, k\} \to \{1, \cdots, \ell\}$, defined by

$$\rho(i) := \min\left\{j \in \{1; \cdots; \ell\} \mid \vartheta_S(A[i; j]) = \vartheta_i\right\}.$$

Note that from the definition the pivot of the row $A[i :]$ is the element $A[i, \rho(i)]$. Let ϱ be a ring automorphism of S, it is clear that the pivot function and valuation function of the matrices A and $\big(\varrho(A[i; j])\big)_{\substack{1 \leq i \leq k \\ 1 \leq j \leq \ell}}$ provide the same values.

Definition 2.3 (Matrix in row standard form [5])**.** A matrix $A \in S^{k \times \ell}$ is in row standard form if it satisfies the following conditions

1. The pivot function of A is injective and the valuation function of A is increasing,
2. for all $i \in \{1, \cdots, k\}$, there is $\vartheta_i \in \{0, 1, \cdots, s-1\}$ such that $A[i; \rho(i)] = \theta^{\vartheta_i}$ and $A[i :] \in (\theta^{\vartheta_i} S)^\ell$ and
3. for all pairs $i, t \in \{1, \cdots, k\}$ such that $t \neq i$, then
   (a) either $i > t$ and $\deg_R\big(A[t; \rho(i)]\big) < \vartheta_i$,
   (b) or $A[i; \rho(t)] = 0$.

Note that a matrix in row standard form is a nonzero matrix and that its rows are linearly independent. Moreover, if $A \in S^{k \times \ell}$ is in row standard form, then for any ring automorphism ϱ of S, the matrix $\left(\varrho(A[i;j])\right)_{\substack{1 \le i \le k \\ 1 \le j \le \ell}}$ is also in row standard form.

Let $A \in S^{k \times \ell}$ be a nonzero matrix, we say that a matrix $B \in S^{k \times \ell}$ is the *row standard form* of A if B is in row standard form and B is row-equivalent to A. A proof of the existence and unicity of the row standard form of a matrix can be found in [5]. Since the set of all generator matrices of any S-linear code $\mathscr{B}$ is a coset under row equivalence, it follows that $\mathscr{B}$ has a unique generator matrix in row standard form that will be denoted by $\text{RSF}(\mathscr{B})$. As usual we define the type of a linear code as follows.

Definition 2.4 (Type of a linear code). Let $\mathscr{B}$ be an S-linear code of length ℓ. Denoted by θ^{ϑ_i} the i-th pivot of $\text{RSF}(\mathscr{B})$. The *type* $\mathscr{B}$ is the $(s+1)$-tuples

$$(\ell; k_0, k_1, \cdots, k_{s-1})$$

where $k_t := |\{\vartheta_i \,|\, \vartheta_i = t\}|$.

Note that if $(\ell; k_0, k_1, \cdots, k_{s-1})$ is the type of an S-linear code $\mathscr{B}$ then we can be compute the S-rank of $\mathscr{B}$ and the number of codewords of $\mathscr{B}$, of the following way:

$$\text{rank}_S(\mathscr{B}) = \sum_{t=0}^{s-1} k_t, \quad \text{and} \quad |\mathscr{B}| = q^{m\left(\sum_{t=0}^{s-1} k_t(s-t)\right)}.$$

3. Galois action on $\mathscr{L}(S^\ell)$.

Let $S|R$ be a Galois extension of finite chain ring with Galois group G. The Galois group G acts on $\mathscr{L}(S^\ell)$ as follows; Let $\mathscr{B}$ in $\mathscr{L}(S^\ell)$ and σ in G

$$\sigma(\mathscr{B}) = \left\{ (\sigma(c_0), \sigma(c_1), \cdots, \sigma(c_{\ell-1})) \,\middle|\, (c_0, c_1, \cdots, c_{\ell-1}) \in \mathscr{B} \right\}. \tag{6}$$

Definition 3.1 (Galois invariance). A linear code $\mathscr{B}$ over S is called *Galois invariant* if $\sigma(\mathscr{B}) = \mathscr{B}$ for all $\sigma \in G$.

An direct consequence of this definition is the following fact. Let $\mathscr{B}$ be an S-linear code and m an even number, if $\mathscr{B}$ is a Galois invariant code then $\mathscr{B}^{\perp_{\varphi'}} = \mathscr{B}^\perp$ (note that $\mathscr{B}^{\perp_{\varphi'}} = (\sigma^{\frac{m}{2}}(\mathscr{B}))^{\perp_E}$). Therefore, we will consider only the euclidean inner product from now on.

Lemma 3. *Let $\mathscr{B}$ be an S-linear code and A a generator matrix of $\mathscr{B}$.*

1. $\sigma(\mathscr{B}^\perp) = \sigma(\mathscr{B})^\perp$*, and* $\sigma(\text{row}(A)) = \text{row}(\sigma(A))$*, for all* $\sigma \in G$*.*
2. *The following assertions are equivalent:*
   (a) $\mathscr{B}$ *is Galois invariant;*
   (b) $\mathscr{B}^\perp$ *is Galois invariant.*

The following theorem allows us to check the Galois invariance of a code by checking its generator matrix in row standard form.

Theorem 2. *Let $\mathscr{B}$ be an S-linear code and $A \in S^{k \times \ell}$ a generator matrix of $\mathscr{B}$. Then the following facts are equivalent.*

1. $\mathcal{B}$ *is Galois invariant.*
2. $RSF(\mathcal{B})$ *in* $R^{k \times \ell}$.

Proof.

$1. \Rightarrow 2.$ Let σ in G. Then the matrix $\sigma(\mathrm{RSF}(\mathcal{B}))$ is the generator matrix in row standard form of $\sigma(\mathcal{B})$, by the uniqueness of generator matrix in row standard form, it follows $\mathrm{RSF}(\mathcal{B}) = \sigma(\mathrm{RSF}(\mathcal{B}))$ for all σ in G, thus $\mathrm{RSF}(\mathcal{B}) \in \mathrm{Fix}_{\mathrm{S}}(G)^{k \times \ell}$. As $\mathrm{S}|\mathrm{R}$ is a Galois separable extension with Galois group G, it follows that $\mathrm{Fix}_{\mathrm{S}}(G) = \mathrm{R}$. Hence $\mathrm{RSF}(\mathcal{B}) \in \mathrm{R}^{k \times \ell}$.

$2. \Rightarrow 1.$ If $\mathrm{RSF}(\mathcal{B}) \in \mathrm{R}^{k \times \ell}$, Then $\sigma(\mathrm{RSF}(\mathcal{B})) = \mathrm{RSF}(\mathcal{B})$ is a generator matrix of $\mathcal{B}$ and of $\sigma(\mathcal{B})$, therefore $\mathcal{B}$ is Galois invariant (see [8, Theorem 1]).

$\square$

Corollary 1. *Let $\mathcal{B}$ be a linear code over S, $\mathcal{B}$ is Galois invariant if and only if $RSF(\mathcal{B}) = RSF(Res(\mathcal{B}))$.*

The proof follows directly from Theorem 2 above. We have also the following result.

Corollary 2. *Let $\mathcal{B}$ be a linear code over S of the type $(\ell; k_0, k_1, \cdots, k_{s-1})$. Then the following conditions are equivalent.*

1. $\mathcal{B}$ *is Galois invariant,*
2. $Res_R(\mathcal{B})$ *is of type $(\ell; k_0, k_1, \cdots, k_{s-1})$.*

For all $\mathcal{B}_1, \mathcal{B}_2 \in \mathcal{L}(\mathrm{S}^\ell)$, $\mathcal{B}_1 \vee \mathcal{B}_2 = \mathcal{B}_1 + \mathcal{B}_2$ is the smallest S-linear code containing $\mathcal{B}_1$ and $\mathcal{B}_2$. Note that $\left(\mathcal{L}(\mathrm{S}^\ell); \cap, \vee \right)$ is a lattice and for each $\mathscr{E} \subseteq \mathrm{S}^\ell$ we define $\mathrm{Ext}(\mathscr{E})$, the *extension code* of $\mathscr{E}$ to S, as the code form by all S-linear combinations of elements in $\mathscr{E}$.

Proposition 2. *The operators*

$$\mathcal{L}(S^\ell) \underset{Ext}{\overset{Tr_R^S; Res_R}{\rightleftarrows}} \mathcal{L}_\ell(R) \tag{7}$$

are lattice morphisms. Moreover,

$$Ext(\mathscr{C}^\perp) = Ext(\mathscr{C})^\perp \ and \ Tr_R^S(Ext(\mathscr{C})) = Res_R(Ext(\mathscr{C})) = \mathscr{C} \ for \ all \ \mathscr{C} \in \mathcal{L}_\ell(R).$$

Proof. Let $\mathcal{B}$ and $\mathcal{B}'$ be two S-linear codes. The trace map $\mathrm{Tr}_{\mathrm{R}}^{\mathrm{S}}$ is surjective and we have $\mathrm{Tr}_{\mathrm{R}}^{\mathrm{S}}(\mathcal{B} + \mathcal{B}') = \mathrm{Tr}_{\mathrm{R}}^{\mathrm{S}}(\mathcal{B}) + \mathrm{Tr}_{\mathrm{R}}^{\mathrm{S}}(\mathcal{B}')$ and $\mathrm{Tr}_{\mathrm{R}}^{\mathrm{S}}(\mathcal{B} \cap \mathcal{B}') = \mathrm{Tr}_{\mathrm{R}}^{\mathrm{S}}(\mathcal{B}) \cap \mathrm{Tr}_{\mathrm{R}}^{\mathrm{S}}(\mathcal{B}')$. Applying Theorem 2 we get that $\mathrm{Res}_{\mathrm{R}}$ is a lattice morphism. On the other hand, let $\mathscr{C}$ in $\mathcal{L}_\ell(\mathrm{R})$, the S-linear code $\mathrm{Ext}(\mathscr{C})$ is Galois invariant, thus $\mathrm{Tr}_{\mathrm{R}}^{\mathrm{S}}(\mathrm{Ext}(\mathscr{C})) = \mathrm{Res}_{\mathrm{R}}(\mathrm{Ext}(\mathscr{C})) = \mathscr{C}$ and $\mathrm{Ext}(\mathscr{C}^\perp) = \mathrm{Ext}(\mathscr{C})^\perp$.

$\square$

Definition 3.2 (Galois closure and Galois interior). Let $\mathcal{B}$ be a linear code over S.

1. The *Galois closure* of $\mathcal{B}$, denoted by $\widetilde{\mathcal{B}}$, is the smallest linear code over S, containing $\mathcal{B}$, which is Galois invariant,

$$\widetilde{\mathcal{B}} := \bigcap \left\{ \mathcal{T} \in \mathcal{L}(\mathrm{S}^\ell) \middle| \mathcal{T} \subseteq \mathcal{B} \text{ and } \mathcal{T} \text{ Galois invariant} \right\}.$$

2. The *Galois interior* of $\mathcal{B}$, denoted $\overset{\circ}{\mathcal{B}}$, is the greatest S-linear subcode of $\mathcal{B}$, which is Galois invariant,

$$\overset{\circ}{\mathcal{B}} := \bigvee \left\{ \mathcal{T} \in \mathscr{L}(S^{\ell}) \,\middle|\, \mathcal{T} \supseteq \mathcal{B} \text{ and } \mathcal{T} \text{ Galois invariant} \right\}.$$

A map $J_G : \mathscr{L}(S^{\ell}) \to \mathscr{L}(S^{\ell})$ is called a *Galois operator* if J_G is an morphism of lattices such that

1. $J_G(J_G(\mathcal{B})) = J_G(\mathcal{B})$ and
2. for all $\mathcal{B}$ in $\mathscr{L}(S^{\ell})$ the code $J_G(\mathcal{B})$ is Galois invariant.

The Galois closure and Galois interior are indeed Galois operators and $\widetilde{\overset{\circ}{\mathcal{B}}} = \overset{\circ}{\mathcal{B}}$, $\overset{\circ}{\widetilde{\mathcal{B}}} = \widetilde{\mathcal{B}}$. From Definition 3.2, it follows that $\mathcal{B}$ is Galois invariant if and only if $\widetilde{\mathcal{B}} = \overset{\circ}{\mathcal{B}}$.

Proposition 3. *If $\mathcal{B}$ is a linear code over S then $\left(\overset{\circ}{\mathcal{B}}{}^{\perp} \right) = \left(\widetilde{\mathcal{B}} \right)^{\perp}$.*

Proof. It is clear that $\overset{\circ}{\mathcal{B}} \subseteq \mathcal{B}$ and, by duality, $\left(\overset{\circ}{\mathcal{B}} \right)^{\perp} \subseteq \mathcal{B}^{\perp}$. Now $\overset{\circ}{\mathcal{B}}$ is Galois invariant therefore $\left(\overset{\circ}{\mathcal{B}} \right)^{\perp}$ is Galois invariant by Remark 3 and it contains $\mathcal{B}^{\perp}$. Note that $\widetilde{\mathcal{B}^{\perp}}$ is the smallest Galois invariant linear code containing $\mathcal{B}^{\perp}$ hence $\left(\widetilde{\mathcal{B}^{\perp}} \right) \subseteq \left(\overset{\circ}{\mathcal{B}} \right)^{\perp}$. Since $\mathcal{B}^{\perp} \subseteq \widetilde{\mathcal{B}^{\perp}}$, again by duality we have that $\left(\widetilde{\mathcal{B}^{\perp}} \right)^{\perp} \subseteq \mathcal{B}$. Now the code $\left(\widetilde{\mathcal{B}^{\perp}} \right)^{\perp}$ is Galois invariant and is contained in $\mathcal{B}$, since the largest code that is Galois invariant and contained in $\mathcal{B}$ is $\overset{\circ}{\mathcal{B}}$, it follows that $\left(\widetilde{\mathcal{B}^{\perp}} \right)^{\perp} \subseteq \overset{\circ}{\mathcal{B}}$, and both inclusions give the equality. $\square$

Let $\{\alpha_0, \alpha_1, \cdots, \alpha_{m-1}\}$ be a free R-basis of S and $\{\alpha_0^*, \alpha_1^*, \cdots, \alpha_{m-1}^*\}$ its trace-dual basis. We define the i-th projection as

$$\begin{array}{rccc} \mathrm{Pr}_i: & S^{\ell} & \to & R^{\ell} \\ & c & \mapsto & \mathrm{Tr}_R^S(\alpha_i^* c). \end{array} \qquad i = 0, \ldots, m-1. \tag{8}$$

Since $c_j = \sum\limits_{i=0}^{m-1} \mathrm{Tr}_R^S(\alpha_i^* c_j)\alpha_i$, for all $c_j \in S$, and $\mathcal{B}$ is linear over S, it follows that $\mathrm{Pr}_i(\mathcal{B}) = \mathrm{Tr}_R^S(\mathcal{B})$.

Lemma 4. *Let $\mathcal{B}$ be a linear code over S. Then $\mathcal{B} \subseteq Ext_S(Tr_R^S(\mathcal{B}))$ and $Res_R(\mathcal{B}) \subseteq Tr_R^S(\mathcal{B})$.*

The following lemma relates the Galois closure and Galois interior with the constructions of the trace code, the restriction code and the extension code.

Lemma 5. *Let $\mathcal{B}$ be a linear code over S. Then $\overset{\circ}{\mathcal{B}} = Ext(Res_R(\mathcal{B})) = \bigcap\limits_{\sigma \in G} \sigma(\mathcal{B})$.*

Proof. By Definition 3.2 and Lemma 4 we have $\mathrm{Ext}(\mathrm{Res}_R(\mathcal{B})) \subseteq \overset{\circ}{\mathcal{B}} \subseteq \mathcal{B}$. On the other hand, the linear code $\overset{\circ}{\mathcal{B}}$ over S is Galois invariant therefore we have $\mathrm{Ext}(\mathrm{Res}_R(\overset{\circ}{\mathcal{B}})) = \overset{\circ}{\mathcal{B}}$ (see [8, Theorem 1]). Since $\overset{\circ}{\mathcal{B}} \subseteq \mathcal{B}$ we get that $\overset{\circ}{\mathcal{B}} \subseteq \mathrm{Ext}(\mathrm{Res}_R(\mathcal{B}))$. Thus we have $\mathrm{Ext}(\mathrm{Res}_R(\mathcal{B})) = \bigcap\limits_{\sigma \in G} \sigma(\mathcal{B})$ (see [8, Corollary 1]). $\square$

Proposition 4. *If $\mathcal{B}$ be a linear code over S then $\widetilde{\mathcal{B}} = Ext(Tr_R^S(\mathcal{B})) = \bigvee_{\sigma \in G} \sigma(\mathcal{B})$.*

Proof.

$$
\begin{aligned}
\widetilde{\mathscr{B}} &= ((\widetilde{\mathscr{B}})^{\perp})^{\perp}, \text{ by [12, Theorem 3.10 (iii)]} \\
&= \left(\left(\overset{\circ}{\mathscr{B}^{\perp}}\right)\right)^{\perp}, \text{ by Proposition 3,} \\
&= \text{Ext}(\text{Res}_{\text{R}}(\left(\mathscr{B}^{\perp}\right))^{\perp}, \text{ by Lemma 5} \\
&= \text{Ext}\left(\text{Res}_{\text{R}}(\mathscr{B})^{\perp}\right)^{\perp}, \text{ by Proposition 3,} \\
&= \text{Ext}\left(\text{Tr}_{\text{R}}^{\text{S}}(\mathscr{B})^{\perp}\right)^{\perp}, \text{ by Theorem 1.}
\end{aligned}
$$

Note that $\text{Ext}\left(\text{Tr}_{\text{R}}^{\text{S}}(\mathscr{B})^{\perp}\right) = \text{Ext}\left(\text{Tr}_{\text{R}}^{\text{S}}(\mathscr{B})\right)^{\perp}$, therefore it follows that $\widetilde{\mathscr{B}} = \left(\text{Ext}\left(\text{Tr}_{\text{R}}^{\text{S}}(\mathscr{B})\right)^{\perp}\right)^{\perp}$. Again by [12, Theorem 3.10(iii)] we also have that $\widetilde{\mathscr{B}} = \text{Ext}\left(\text{Tr}_{\text{R}}^{\text{S}}(\mathscr{B})\right)$. Since $\mathscr{B} \subseteq \bigvee_{\sigma \in G} \sigma(\mathscr{B})$ is Galois invariant then we have $\widetilde{\mathscr{B}} \subseteq \bigvee_{\sigma \in G} \sigma(\mathscr{B})$. Finally $\sigma(\mathscr{B}) \subseteq \widetilde{\mathscr{B}}$ for all $\sigma \in G$, therefore $\bigvee_{\sigma \in G} \sigma(\mathscr{B}) \subseteq \widetilde{\mathscr{B}}$. □

Remark 1. Note that by Lemma 5 and Propostion 4 we get the following fact. Let $\mathscr{B}$ be an S-linear code, then $\text{Res}_{\text{R}}(\overset{\circ}{\mathscr{B}}) = \text{Res}_{\text{R}}(\mathscr{B})$ and $\text{Res}_{\text{R}}(\widetilde{\mathscr{B}}) = \text{Tr}_{\text{R}}^{\text{S}}(\mathscr{B})$. Thus (by Delsarte's Theorem) $\text{Res}_{\text{R}}(\mathscr{B}^{\perp}) = \text{Res}_{\text{R}}(\mathscr{B})^{\perp}$ if and only if $\mathscr{B}$ is Galois invariant.

Remark 2. In the case that S, R are finite fields the properties of the Galois closure and Galois interior as well as Proposition 3 and Lemma 5 were stated by Stichtenoth in [14].

Note also that we have $\widetilde{\widetilde{\mathscr{B}}} = \widetilde{\mathscr{B}}$, thus from Remark 1 it follows that

$$
\text{Res}_{\text{R}}(\widetilde{\widetilde{\mathscr{B}}}) = \text{Tr}_{\text{R}}^{\text{S}}(\widetilde{\mathscr{B}}) \text{ and } \text{Res}_{\text{R}}(\widetilde{\mathscr{B}}) = \text{Tr}_{\text{R}}^{\text{S}}(\mathscr{B}).
$$

Hence $\text{Tr}_{\text{R}}^{\text{S}}(\mathscr{B}) = \text{Tr}_{\text{R}}^{\text{S}}(\widetilde{\mathscr{B}})$ (see [8, Proposition 1]). Thus as a corollary we recover the following result.

Corollary 3 (Theorem 2, [8])**.** *The S-linear code $\mathscr{B}$ is Galois invariant if and only if $Tr_{R}^{S}(\mathscr{B}) = Res(\mathscr{B})$.*

Finally we are in condition for enunciate a Galois correspondence statement. For any $\mathscr{B}$ in $\mathscr{L}\left(\text{S}^{\ell}\right)$, we consider $\mathscr{L}(\mathscr{B})$ the lattice of S-linear subcode of $\mathscr{B}$. Let us define

$$
\begin{array}{cccc}
\text{Stab:} & \mathscr{L}(\mathscr{B}) & \to & \text{Sub}(G) \\
& \mathscr{T} & \mapsto & \text{Stab}(\mathscr{T}),
\end{array}
\quad \text{and} \quad
\begin{array}{cccc}
\text{Fix}_{\mathscr{B}}: & \text{Sub}(G) & \to & \mathscr{L}(\mathscr{B}) \\
& H & \mapsto & \underset{\sigma \in H}{\cap} \sigma(\mathscr{B}),
\end{array}
$$

where $\text{Stab}(\mathscr{T}) = \left\{\sigma \in G \,\middle|\, \sigma(\mathbf{c}) = \mathbf{c}, \text{ for all } \mathbf{c} \in \mathscr{T}\right\}$.

Let H a subgroup of G, we say that $\mathscr{B}$ is H-invariant if $\text{Fix}_{\mathscr{B}}(H) = \mathscr{B}$. Note that $\text{Fix}_{\mathscr{B}}(H)$ is an H-interior of $\mathscr{B}$. From Lemma 5 it follows that

$$
\text{Fix}_{\mathscr{B}}(H) = \text{Ext}(\text{Res}_{\text{T}}(\mathscr{B})),
$$

where $\text{T} = \text{Fix}_{\text{S}}(H)$. Moreover $\text{Fix}_{\mathscr{B}}(\text{Stab}(\mathscr{B})) = \mathscr{B}$ and $\text{Stab}(\text{Fix}_{\mathscr{B}}(H)) = H$. Therefore we have a Galois correspondence on $\mathscr{L}(\mathscr{B})$ as follows.

Theorem 3. *For each $\mathscr{B}$ in $\mathscr{L}\left(S^{\ell}\right)$, the pair $(\text{Stab}; \text{Fix}_{\mathscr{B}})$ is a Galois correspondence between $\mathscr{B}$ and G.*

4. Rank bounds

Let $\mathscr{B}$ be an S-linear code and $\{\mathbf{c}_i \mid 1 \leq i \leq k\}$ be the S-basis of $\mathscr{B}$ in row standard form, i.e. $\mathbf{c}_i := \mathrm{RSF}(\mathscr{B})[i :]$. For each $i = 1, 2, \ldots, k$, we will denote by m_i the integer such that $\sigma^{m_i}(\mathbf{c}_i) = \mathbf{c}_i$ and $\sigma^{m_i-1}(\mathbf{c}_i) \neq \mathbf{c}_i$. The set $\{m_i \mid i = 1, 2, \cdots, k\}$ is called the *level set* of $\mathscr{B}$.

Note that the set $\left\{ \mathrm{Tr}_{\mathsf{R}}^{\mathsf{S}}(\alpha_j^* \mathbf{c}_i) \mid 0 \leq j < m \text{ and } 1 \leq i \leq k \right\}$ is an R-generating set of $\mathrm{Tr}_{\mathsf{R}}^{\mathsf{S}}(\mathscr{B})$ thus taking into account Lemma 4 we have the obvious upper bounds for the rank of restriction codes and trace codes

$$\mathrm{rank}_{\mathsf{R}}(\mathrm{Res}_{\mathsf{R}}(\mathscr{B})) \leq \mathrm{rank}_{\mathsf{S}}(\mathscr{B}) \leq \mathrm{rank}_{\mathsf{R}}\left(\mathrm{Tr}_{\mathsf{R}}^{\mathsf{S}}(\mathscr{B})\right) \leq m \cdot \mathrm{rank}_{\mathsf{S}}(\mathscr{B}). \tag{9}$$

The inequality $\mathrm{rank}_{\mathsf{R}}(\mathrm{Res}_{\mathsf{R}}(\mathscr{B})) \leq \mathrm{rank}_{\mathsf{S}}(\mathscr{B})$ in (4) follows from the fact that an R-basis of $\mathrm{Res}_{\mathsf{R}}(\mathscr{B})$ is also S-independent and $\mathrm{rank}_{\mathsf{R}}(\mathscr{B}) = m \, \mathrm{rank}_{\mathsf{S}}(\mathscr{B})$. Note that it is also clear that $\mathrm{rank}_{\mathsf{S}}\left(\overset{\circ}{\mathscr{B}}\right) = \mathrm{rank}_{\mathsf{R}}(\mathrm{Res}_{\mathsf{R}}(\mathscr{B}))$ and that $\mathrm{rank}_{\mathsf{R}}\left(\mathrm{Tr}_{\mathsf{R}}^{\mathsf{S}}(\mathscr{B})\right) = \mathrm{rank}_{\mathsf{S}}\left(\widetilde{\mathscr{B}}\right)$. We can sharpen the upper bound in (4) for the rank of trace codes as follows (note that it has some resemblances with Shibuya's lower bound for codes over finite fields in [13, Theorem 1]).

Proposition 5. *Let $\mathscr{B}$ be an S-linear code, $\underline{\mathbf{B}} := \{c_i \mid 1 \leq i \leq k\}$ be the S-basis of $\mathscr{B}$ in row standard form and $\{m_i \mid i = 1, 2, \cdots, k\}$ its level set then*

$$rank_R\left(Tr_R^S(\mathscr{B})\right) = rank_S\left(\widetilde{\mathscr{B}}\right) \leq \sum_{i=1}^{k} m_i \leq m \, rank_S(\mathscr{B}) - (m-1) rank_S\left(\overset{\circ}{\mathscr{B}}\right). \tag{10}$$

Proof. Let $\mathscr{B}'$ be the S-linear code generated by $\{\sigma^j(\mathbf{c}_i) \mid 0 \leq j < m_i \text{ and } 1 \leq i \leq k\}$. It is clear that $\widetilde{\mathscr{B}} \subseteq \mathscr{B}'$ since $\mathscr{B}'$ is Galois invariant. Thus $\mathrm{rank}_{\mathsf{S}}\left(\widetilde{\mathscr{B}}\right) \leq \sum_{i=1}^{k} m_i$ and taking into account that $m_i \leq m$ we have that

$$
\begin{aligned}
\sum_{i=1}^{k} m_i &\leq |\{\mathbf{c} \in \underline{\mathbf{B}} \mid \sigma(\mathbf{c}) = \mathbf{c}\}| + \left|\left\{\sigma^j(\mathbf{c}) \mid \mathbf{c} \in \underline{\mathbf{B}}, \, 0 \leq j < m \text{ and } \sigma(\mathbf{c}) \neq \mathbf{c}\right\}\right| \\
&= \mathrm{rank}_{\mathsf{S}}\left(\overset{\circ}{\mathscr{B}}\right) + m\left(\mathrm{rank}_{\mathsf{S}}(\mathscr{B}) - \mathrm{rank}_{\mathsf{S}}\left(\overset{\circ}{\mathscr{B}}\right)\right).
\end{aligned}
$$

$\square$

We can also obtain an straight forward lower bound for the R-rank of restriction codes as follows. Let $\mathscr{B}$ be an S-linear code such that $\mathrm{Res}_{\mathsf{R}}(\mathscr{B}) \neq \{\mathbf{0}\}$, then $\mathrm{rank}_{\mathsf{R}}(\mathrm{Res}_{\mathsf{R}}(\mathscr{B})) \geq |\{i \mid \mathrm{RSF}(\mathscr{B})[i :] \in \mathsf{R}^\ell\}|$ since the rows of $\mathrm{RSF}(\mathscr{B})$ which are in R^ℓ form a matrix in row standard form, thus they are R-independent codewords in $\mathrm{Res}_{\mathsf{R}}(\mathscr{B})$.

A non-trivial lower bound can be found in the following result, note that it has some resemblances with Stichtenoth's lower bound for codes over finite fields in [14, Corollary 1] since the bound is related with the rank of $\overset{\circ}{\mathscr{B}}{}^\perp$.

Proposition 6. *Let $\mathscr{B}$ be an S-linear code of type $(\ell; k_0, k_1, \cdots, k_{s-1})$ and $\{m_i^\perp \mid i = 1, 2, \cdots, \ell - k_0\}$ the level set of $\mathscr{B}^\perp$. Then*

$$rank_R(Res_R(\mathscr{B})) \geq \ell - \sum_{i=1}^{\ell - k_0} m_i^\perp \geq m k_0 - (m-1)\left(\ell - rank_R\left(Res_R\left(\mathscr{B}^\perp\right)\right)\right). \tag{11}$$

Proof. We just use Proposition 5 and Delsarte's Theorem.

$$
\begin{aligned}
\mathrm{rank}_R(\mathrm{Res}_R(\mathscr{B})) \;&\geq\; \ell - \mathrm{rank}_R(\mathrm{Res}_R(\mathscr{B})^\perp) \\
&=\; \ell - \mathrm{rank}_S((\overset{\circ}{\mathscr{B}})^\perp),\ \text{since } \overset{\circ}{\mathscr{B}} = \mathrm{Ext}(\mathrm{Res}_R(\mathscr{B})), \\
&=\; \ell - \mathrm{rank}_S(\widetilde{\mathscr{B}^\perp}),\ \text{since } (\overset{\circ}{\mathscr{B}})^\perp = \widetilde{(\mathscr{B}^\perp)}, \\
&\geq\; \ell - \sum_{i=1}^{\ell - k_0} m_i^\perp,\ \text{by Proposition 5}, \\
&\geq\; \ell - m\,\mathrm{rank}_S\left(\mathscr{B}^\perp\right) + (m-1)\mathrm{rank}_R\left(\mathrm{Res}_R(\mathscr{B}^\perp)\right),\ \text{By Inequality 10}, \\
&=\; m\,k_0 + (m-1)\left(\ell - \mathrm{rank}_R\left(\mathrm{Res}_R(\mathscr{B}^\perp)\right)\right),\ \text{because } \mathrm{rank}_S\left(\mathscr{B}^\perp\right) = \ell - k_0, \\
&=\; m\,k_0 + (m-1)\left(\ell - \mathrm{rank}_R\left(\mathrm{Tr}_R^S(\mathscr{B})^\perp\right)\right),\ \text{Delsarte's Theorem.}
\end{aligned}
$$

$\square$

Note that the first inequality holds because if $\mathscr{C}$ is an R-code of type $(\ell; k_0, k_1, \cdots, k_{s-1})$ then $\mathscr{C}^\perp$ is of type $(\ell; \ell - \sum_{i=0}^{s-1} k_i, k_{s-1}, \cdots, k_1)$ [12, Theorem 3.10 (ii)], in other words, $\mathrm{rank}_R\left(\mathscr{C}^\perp\right) \geq \ell - \mathrm{rank}_R(\mathscr{C})$ and the equality holds if and only if $\mathscr{C}$ is a free code.

From Porposition 5 and Proposition 6 follows directly the following corollary relating the rank of the restriction code and the free ranks of the code and the trace code.

Corollary 4. *Let $\mathscr{B}$ be an R-code of type $(\ell; k_0, k_1, \cdots, k_{s-1})$ and $(\ell; k_0^{(t)}, k_1^{(t)}, \cdots, k_{s-1}^{(t)})$ be the type of $\mathrm{Tr}_R^S(\mathscr{B})$ and $(\ell; k_0^{(r)}, k_1^{(r)}, \cdots, k_{s-1}^{(r)})$ be the type of $\mathrm{Res}_R(\mathscr{B})$, then*

1. $\mathrm{rank}_R(\mathrm{Res}_R(\mathscr{B})) \geq \ell - \displaystyle\sum_{i=1}^{\ell - k_0} m_i^\perp \geq m\,k_0 - (m-1)k_0^{(t)}.$
2. $m\,k_0 - (m-1)k_0^{(r)} \leq \ell - k_0^{(t)} \leq m(\ell - k_0) - (m-1)(\ell - k_0^{(r)}).$

5. An application to Linear Cyclic Codes

In this section we will assume that $(\ell, q) = 1$ and the multiplicative order of q modulo ℓ will be denoted by $\mathrm{ord}_\ell(q) = m$. A subset $\mathscr{C}$ of R^ℓ, is *cyclic*, if for all $(c_0, \cdots, c_{\ell-2}, c_{\ell-1}) \in \mathscr{C}$ we have $(c_{\ell-1}, c_0, \cdots, c_{\ell-2}) \in \mathscr{C}$. We will denote by $\mathscr{R}_\ell$ the quotient ring of $\mathrm{R}[x]$ by the ideal generated by $x^\ell - 1$. As usual, we identify the R-modules $(\mathrm{R}^\ell, +)$ and $(\mathscr{R}_\ell, +)$ and if the polynomial $g \in \mathrm{R}[x]$ has degree less or equal to $\ell - 1$ then we identify g and its quotient class in $\mathscr{R}_\ell$. We define the map

$$
\Psi: \quad \begin{array}{ccc} \mathrm{R}^\ell & \to & \mathscr{R}_\ell \\ (c_0, c_1, \cdots, c_{\ell-1}) & \mapsto & c_0 + c_1 x + \cdots + c_{\ell-1} x^{\ell-1} + \langle x^\ell - 1 \rangle, \end{array} \tag{12}
$$

where $\langle x^\ell - 1 \rangle$ is the ideal of $\mathrm{R}[x]$ generated by $x^\ell - 1$. It is well known that Ψ is an isomorphism of R-modules and any R-linear code $\mathscr{C}$ of length ℓ is cyclic if and only if $\Psi(\mathscr{C})$ is an ideal of $\mathscr{R}_\ell$. The Galois extension S of R such that $\mathrm{rank}_R(\mathrm{S}) = m$ is the splitting ring of $x^\ell - 1 = \displaystyle\prod_{i=0}^{\ell-1}(x - \xi^i)$, where ξ is an element in $\Gamma(\mathrm{S})$ such that $\xi^i \neq 1$ for $i = 0, \ldots, \ell-1$ and $\xi^\ell = 1$. The q-cyclotomic coset modulo ℓ containing a will be denoted by

$$
Z_a = \left\{ a q^j \bmod \ell \;\middle|\; 0 \leq j < z_a \right\},
$$

where z_a is the smallest nonnegative integer such that $aq^{z_a} \equiv a \pmod{\ell}$. The set $\mathrm{Cl}_q(\ell) := \{a_1, a_2, \cdots, a_u\}$ will be the subset of $\{0, 1, \cdots, \ell-1\}$ such that for all $a \in \{0, 1, \cdots, \ell-1\}$ there is a unique index i such that $a \in Z_{a_i}$. Let $a \in \mathrm{Cl}_q(\ell)$, Λ_a will denote the Hensel's lift of the minimal polynomial of $\pi(\xi)^a$ over $\mathbb{F}_q$ to the ring R, where $\pi(\xi)$ is a primitive root of $x^\ell - 1$. Then

$$x^\ell - 1 = \prod_{a \in \mathrm{Cl}_q(\ell)} \Lambda_a,$$

is the factorization of $x^\ell - 1$ into a product of distinct basic irreducible polynomials over R. For each element $a \in \mathrm{Cl}_q(\ell)$ by $\widehat{\Lambda_a}$ we will denote the monic polynomial in $\mathscr{R}_\ell$ such that $x^\ell - 1 = \widehat{\Lambda_a}\Lambda_a$. Then there exists a pair $(u, v) \in (\mathscr{R}_\ell)^2$ such that $u\Lambda_a + v\widehat{\Lambda_a} = \mathbf{1}$. The idempotents of $\mathscr{R}_\ell$ are described in the following result.

Lemma 6 (Theorem 2.9 [17]). *The set* $\left\{ e_a := v\widehat{\Lambda_a} \,\middle|\, a \in Cl_q(\ell) \right\}$ *is the set of the mutually orthogonal non-zero idempotents of* $\mathscr{R}_\ell$ *and* $\displaystyle\sum_{a \in Cl_q(\ell)} e_a = 1$.

The last equality implies the decomposition of $\mathscr{R}_\ell$ into the direct sum of ideals of the form $\Psi(\mathscr{C}_a) := \langle e_a \rangle$ such that $\Psi(\mathscr{C}_a)\Psi(\mathscr{C}_{a'}) = \{\mathbf{0}\}$ (since $e_a e_{a'} = 0$ if $a \neq a'$), i.e.

$$\mathscr{R}_\ell := \bigoplus_{a \in \mathrm{Cl}_q(\ell)} \Psi(\mathscr{C}_a). \tag{13}$$

Let $\mathscr{C}$ be an R-linear cyclic subcode of $\mathscr{C}_a$. Since $\Psi(\mathscr{C}_a)$ is a principal ideal in $\mathscr{R}_\ell$, there exists $f \in \mathscr{R}_\ell$ such that $\Psi(\mathscr{C}) = \langle f \rangle$ and e_a divides f. If $\mathscr{C} \neq \mathscr{C}_a$, then $\omega_a \notin \Psi(\mathscr{C})$. Therefore there exits an integer $\mathsf{t} \in \{0, 1, \cdots, s-1\}$ such that $f(x) = \theta^{\mathsf{t}}\omega_a(x)$ and we have the following.

Proposition 7. *Let* $a \in Cl_q(\ell)$*, the cyclic R-subcodes of the R-linear cyclic code* $\Psi(\mathscr{C}_a) := \langle \omega_a \rangle$ *are*

$$\{0\} \subsetneq \mathscr{C}_{a,s-1} \subsetneq \cdots \subsetneq \mathscr{C}_{a,1} \subsetneq \mathscr{C}_a, \tag{14}$$

and $\mathscr{C}_{\mathsf{t}_a} := \theta^{\mathsf{t}_a}\mathscr{C}_a$ *is the only R-linear cyclic subcode of* $\mathscr{C}_a$ *such that* $\theta^{s-\mathsf{t}_a}\mathscr{C}_{\mathsf{t}_a} = \{0\}$ *and* $\theta^{s-\mathsf{t}_a-1}\mathscr{C}_{\mathsf{t}_a} \neq \{0\}$.

Corollary 5. *For each R-linear cyclic code* $\mathscr{C}$ *of length* ℓ *there exists a unique multi-index*

$$(\mathsf{t}_a)_{a \in Cl_q(\ell)} \in \{0, 1, \cdots, s\}^{Cl_q(\ell)}$$

such that $\mathscr{C} := \displaystyle\bigoplus_{a \in Cl_q(\ell)} \mathscr{C}_{\mathsf{t}_a}$.

Consider the set $\circlearrowleft_\ell (\mathrm{R})$ of all the cyclic codes over R of length ℓ and $\mathscr{A}_\ell(q, s) := \{0, 1, \cdots, s\}^{\mathrm{Cl}_q(\ell)}$ the set of all the multi-indices. Corollary 5 establishes that

$$\mathfrak{I}: \begin{array}{ccc} \mathscr{A}_\ell(q, s) & \to & \circlearrowleft_\ell (\mathrm{R}) \\ \underline{\mathbf{t}} & \mapsto & \displaystyle\bigoplus_{a \in \mathrm{Cl}_q(\ell)} \mathscr{C}_{\mathsf{t}_a}. \end{array} \tag{15}$$

is a bijection between the sets $\mathscr{A}_\ell(q, s)$ and $\circlearrowleft_\ell (\mathrm{R})$. Let $\mathbf{t}$ be the multi-index associate to a R-linear cyclic code $\mathscr{C}$, the integers $k_j = |\{a \in \mathrm{Cl}_q(\ell)|\mathsf{t}_a = j\}|$ with $0 \leq j \leq s-1$ determine the type $(\ell; k_0, k_1, \cdots, k_{s-1})$ of $\mathscr{C}$. Moreover, $\mathscr{C}_a$ is a minimal free R-linear cyclic code of R-rank z_a. In the rest of the paper we will face this question:

Let $\mathscr{C}$ be an R-linear cyclic code of length ℓ How one can construct an S-linear cyclic code $\mathscr{B}$ of length ℓ, such that $\mathscr{C} = Res_R(\mathscr{B})$ and $\mathscr{B}$ is Galois invariant?

Consider the set $A := \{a_1, a_2, \cdots, a_k\} \subseteq \{0, 1, \cdots, \ell - 1\}$ and the evaluation ev_ξ in $\underline{\xi} := (1, \xi, \xi^2, \cdots, \xi^{\ell-1})$ defined by

$$\mathrm{ev}_\xi : \quad \mathscr{P}(A) \quad \rightarrow \quad S^\ell$$
$$f \quad \mapsto \quad (f(1), f(\xi), \cdots, f(\xi^{\ell-1})).$$

The R-module $\mathscr{P}(A)$ is free and spanned by $\{x^a \mid a \in A\}$. Thus $\mathrm{ev}_\xi(\mathscr{P}(A))$ is the free S-linear code $\mathscr{B}(A)$ with generator matrix

$$W_A := \begin{pmatrix} 1 & \xi^{a_1} & \cdots & \xi^{(\ell-1)a_1} \\ \vdots & \vdots & & \vdots \\ 1 & \xi^{a_k} & \cdots & \xi^{(\ell-1)a_k} \end{pmatrix} \tag{16}$$

and the subset A of $\{0, 1, \cdots, \ell - 1\}$, is called *defining set* of $\mathscr{B}(A)$.

Let $u \in \{0, 1, \cdots, \ell\}$, the set of *multiples* of u is $uA := \{u a \bmod \ell \mid a \in A\}$, the *opposite* of A is $-A := \{\ell - 1 - a \mid a \in A\}$ and a subset A is said *q-invariant* if $A = qA$. The q-closure of A is

$$\widetilde{A} := \bigcup_{a \in A} Z_a.$$

It is clear that the q-closure of A is the smallest q-invariant subset of $\{0, 1, \cdots, \ell - 1\}$ contained A. The *complementary* of A is $\overline{A} := \{a \in \{0, 1, \cdots, \ell - 1\} \mid a \notin A\}$.

Proposition 8. *Let A be a subset of $\{0, 1, \cdots, \ell - 1\}$. Then $\mathscr{B}(A)$ is cyclic and its generator polynomial is $\prod_{a \in \overline{A}} (x - \xi^{-a})$.*

Proof. Consider the codeword $\mathbf{c}_f = \mathrm{ev}_\xi(f) = \left(f(0); \cdots ; f(\xi^{\ell-2}); f(\xi^{\ell-1}) \right)$ determined by $f(x) = \sum_{i=1}^{k} f_i x^{a_i} \in \mathscr{P}(A)$. For $g(x) = \sum_{i=1}^{k} f_i \xi^{-a_i} x^{a_i} \in \mathscr{P}(A)$ and $\left(g(0); g(\xi); \cdots ; g(\xi^{\ell-1}) \right)$ is the shift of $\mathbf{c}_f$ and therefore $\mathscr{B}(A)$ is a cyclic code. On the other hand we have $\Psi(\mathbf{c}_f) = \sum_{j=1}^{\ell-1} f(\xi^j) x^j$ and

$$\Psi(\mathbf{c}_f)(\xi^a) = \sum_{i=1}^{k} f_i \xi^{-a_i} \left(\sum_{j=1}^{\ell-1} \xi^{j(a_i+a)} \right) \ell \sum_{i=1}^{k} f_i \xi^{-a_i} \delta_{-a_i, a}, \quad a = 0, \cdots, \ell - 1.$$

Thus $a \in -\overline{A}$ if and only if $\Psi(\mathbf{c}_f)(\xi^a) = 0$ and therefore $\Psi(\mathbf{c}_f)(\xi^a) = \left(\prod_{a \in \overline{A}} (x - \xi^{-a}) \right) f(x)$. Note that $\mathscr{B}(A)$ is an S-free module of rank $|A|$ and Ψ is an S-module isomorphism, thus $\prod_{a \in \overline{A}} (x - \xi^{-a})$ is the generator polynomial of $\mathscr{B}(A)$.

$\square$

It is easy to check that $\sum_{j=0}^{\ell-1} \xi^{ij} = \ell \delta_{i,0}$, for all $i = 0, 1, \cdots, \ell - 1$, therefore the following result holds.

Lemma 7. *Let A and B be two subsets of $\{0, 1, \cdots, \ell - 1\}$. Then*

1. *$A \subseteq B$ if and only if $\mathscr{B}(A) \subseteq \mathscr{B}(B)$;*
2. *$A \cap (-B) = \emptyset$ if and only if $\mathscr{B}(A) \perp \mathscr{B}(B)$.*

Consider $2^{\{0,1,\cdots,\ell-1\}}$ the set of the subsets of $\{0, 1, \cdots, \ell - 1\}$ and $\circlearrowleft_\ell(\mathbb{S})$ the set of cyclic codes over $\mathbb{S}$ of length ℓ, from Lemma 6 we get the following.

Corollary 6. *For $\mathsf{t} = 0, 1, \cdots, s$, the map*

$$\mathscr{B}_{\mathsf{t}}: \begin{array}{ccc} 2^{\{0,1,\cdots,\ell-1\}} & \to & \circlearrowleft_\ell(\mathbb{S}) \\ A & \mapsto & \theta^{\mathsf{t}}\mathscr{B}(A), \end{array} \tag{17}$$

is a monomorphism of lattices. Moreover, $\mathscr{B}_{\mathsf{t}}(A)$ decomposes as

$$\mathscr{B}_{\mathsf{t}}(A) = \bigoplus_{a \in Cl_q(\ell)} \mathscr{B}_{\mathsf{t}}(A \cap Z_a)$$

and $\mathscr{B}_{\mathsf{t}}(A)^\perp = \theta^{s-\mathsf{t}}\mathscr{B}(-\overline{A})$ for any subset $A \subseteq \{0, 1, \cdots, \ell - 1\}$.

For $\mathsf{t} = 0, 1, \cdots, s$, we have $\mathscr{B}_{\mathsf{t}}(\emptyset) = \{\mathbf{0}\}$ and $\mathscr{B}_{\mathsf{t}}(\{0, 1, \cdots, \ell - 1\}) = (\mathbb{S}\theta^{\mathsf{t}})^\ell$, and the following properties of the code $\mathscr{B}_{\mathsf{t}}(A)$ hold.

Theorem 4. *Let $A \subseteq \{0, 1, \cdots, \ell - 1\}$, then $\mathscr{B}_{\mathsf{t}}(A)$ is Galois invariant if and only if A is q-invariant.*

Proof. Just note that $\sigma(\mathscr{B}_{\mathsf{t}}(A)) = \mathscr{B}_{\mathsf{t}}(qA)$, for all $\sigma \in G$. $\qquad\square$

The following result extends [1, Theorem 5] to finite chain rings.

Corollary 7. *Let $A \subseteq \{0, 1, \cdots, \ell - 1\}$, then $\mathscr{B}\left(\widetilde{A}\right)$ is the Galois closure of $\mathscr{B}(A)$.*

Consider the set $\mathscr{G}_\ell^\circ(\mathbb{S})$ of all the $\mathbb{S}$-linear cyclic codes of length ℓ, which are Galois invariant. Then the map

$$\mathscr{B}: \begin{array}{ccc} \mathscr{A}_\ell(q,s) & \to & \mathscr{G}_\ell^\circ(\mathbb{S}) \\ \underline{\mathbf{t}} & \mapsto & \bigoplus_{a \in Cl_q(\ell)} \mathscr{B}_{\underline{\mathbf{t}}_a}(Z_a). \end{array} \tag{18}$$

is a bijection. We consider the $\mathbb{R}$-linear cyclic code $\mathfrak{J}_{\mathsf{t}}(A)$ defined by

$$\mathfrak{J}_{\mathsf{t}}(A) := \mathrm{Tr}_{\mathbb{R}}^{\mathbb{S}}(\mathscr{B}_{s-\mathsf{t}}(A))^\perp, \tag{19}$$

where A is an q-invariant subset of $\{0, 1, \cdots, \ell - 1\}$. According to Theorem 4, $\mathscr{B}(A)$ is Galois invariant, and by Remark 1 and Theorem 3 we have $\mathfrak{J}_{\mathsf{t}}(A) = \mathrm{Res}_{\mathbb{R}}(\mathscr{B}_{\mathsf{t}}(A)^\perp)$, and by Corollary 6 it follows that $\mathfrak{J}_{\mathsf{t}}(A) = \mathrm{Res}_{\mathbb{R}}(\mathscr{B}_{s-\mathsf{t}}(-\overline{A}))$. Hence $\mathfrak{J}_{\mathsf{t}_a}(\overline{Z_a}) = \mathrm{Res}_{\mathbb{R}}\left(\mathscr{B}_{s-\mathsf{t}_a}(-\overline{Z_a})\right)$ and the bijection in Equation (15) can be rewritten as

$$\mathfrak{J}: \begin{array}{ccc} \mathscr{A}_\ell(q,s) & \to & \circlearrowleft_\ell(\mathbb{R}) \\ \underline{\mathbf{t}} & \mapsto & \bigoplus_{a \in Cl_q(\ell)} \mathrm{Res}_{\mathbb{R}}\left(\mathscr{B}_{s-\mathsf{t}_a}(-Z_a)\right). \end{array} \tag{20}$$

Consider now the $\mathbb{S}$-linear cyclic code given by

$$\mathscr{B}(\underline{\mathbf{t}})^\perp := \bigoplus_{a \in Cl_q(\ell)} \mathscr{B}_{s-\mathsf{t}_a}(-Z_a),$$

from Proposition 2, $\mathfrak{J}(\underline{\mathbf{t}}) = \mathrm{Res}_{\mathbb{R}}\left(\mathscr{B}(\underline{\mathbf{t}})^\perp\right)$ and by Theorem 4(2) $\mathscr{B}(\underline{\mathbf{t}})^\perp$ is Galois invariant. The following theorem gives an answer to the previous question.

Theorem 5. *For each $\underline{t}$ in $\mathscr{A}_\ell(q,s)$ we have that*

$$\mathfrak{J}(\underline{t}) = Res_S\left(\mathscr{B}(\underline{t})^\perp\right), \quad rank_R(\mathfrak{J}(\underline{t})) = \sum_{i=1}^{u} z_{a_i},$$

and

$$W_{\underline{t}} := \begin{pmatrix} \theta^{s-t_{a_1}} W_{a_1} \\ \theta^{s-t_{a_2}} W_{a_2} \\ \vdots \\ \theta^{s-t_{a_u}} W_{a_u} \end{pmatrix}$$

is a generator matrix of $\mathscr{B}(\underline{t})^\perp$ where W_{a_i}'s are generator matrices of $\mathscr{B}(-Z_{a_i})$'s in Equation (16).

Theorem 5 generalizes the construction of [12, Theorem 4.14] to linear cyclic codes over finite chain rings. Finally, it is important to note Theorem 2 implies that for a subset $A \subseteq \{0,1,\cdots,\ell-1\}$ the matrix in Equation (16) verifies $\mathrm{RSF}(W_A) \in \mathbb{R}^{|A|\times\ell}$ if and only if A is q-invariant.

Finally we will show a BCH-like bound for the minimum Hamming distance (d_H) of this type of codes. A subset $I \subseteq \{0,1,\cdots,\ell-1\}$ is an *interval* of length v if there exists $(u,w) \in \{0,1,\cdots,\ell-1\}^2$ such that $(w,\ell) = 1$ and

$$I = \left\{ wu\,\mathrm{mod}\,\ell; w(u+1)\mathrm{mod}\,\ell; \cdots; w(u+v-1)\mathrm{mod}\,\ell \right\}. \tag{21}$$

Theorem 6 (BCH-bound)**.** *If A is an interval of length v then $d_H(\mathfrak{J}_t(A)) \geq v+1$.*

Proof. Let $A = \left\{ wa_1\mathrm{mod}\,\ell; w(a_1+1)\mathrm{mod}\,\ell; \cdots; w(a_1+a_k-1)\mathrm{mod}\,\ell \right\}$ for some integer w such that $(w,\ell) = 1$. Then $\zeta := \xi^w$ is also a primitive root of $x^\ell - 1$. Suppose that $\mathbf{c}$ is a nonzero codeword of $\mathscr{B}_{s-t}(-\overline{A})$ with the least Hamming weight. Then $W_A\mathbf{c}^T = \mathbf{0}$. Consider $\{j\,|\,c_j \neq 0\} \subseteq \{j_1,j_2,\cdots,j_v\} := \underline{v}$. Consider $\mathbf{m} = (c_{j_1},c_{j_2},\cdots,c_{j_v})$ where $\mathbf{c} = (\cdots,0,c_{j_i},0,\cdots,0,c_{j_{i+1}},0,\cdots)$. Thus the equality $W_A\mathbf{c}^T = \mathbf{0}$ becomes $W_{\underline{v}}\mathbf{m}^T = \mathbf{0}$, where $W_{\underline{v}} := \begin{pmatrix} \zeta^{j_1 a_1} & \cdots & \xi^{j_v a_1} \\ \vdots & & \vdots \\ \zeta^{j_1(a_1+a_v-1)} & \cdots & \xi^{j_v(a_1+a_v-1)} \end{pmatrix}$. We have

$$\det(W_{\underline{v}}) = -\zeta^{v\left(\sum_{t=1}^{v} j_t\right)} \prod_{1 \leq a < b \leq v} \left(\zeta^{j_a} - \zeta^{j_b}\right)$$

is invertible since $\zeta \in \Gamma(S)^*$. Therefore $\mathbf{m} = \mathbf{0}$ which is a contradiction because $\mathbf{c} \neq \mathbf{0}$. Hence $d_H(\mathfrak{J}_t(A)) \geq d_H(\mathscr{B}_{s-t}(-\overline{A})) \geq v+1$. $\qquad\square$

References

[1] Bierbrauer J., *The Theory of Cyclic Codes and a Generalization to Additive Codes*. Des. Codes Cryptography 25(2): 189-206 (2002)

[2] Philippe Delsarte, *On subfield subcodes of modified Reed-Solomon codes*, IEEE Trans. Inform. Theory IT-21 (5) (1975)

[3] F. DeMayer and E. Ingranham, *Separable Algebras Over Commutative Rings*. Lecture Notes in Mathematics, Vol 181, Springer-Verlag, Berlin (1971).

[4] S. T. Dougherty and H. Liu, *Independence of vectors in codes over rings*. Des. Codes Cryptogr. 51:55-68 (2009).

[5] Chen Feng, Roberto W. Nóbrega, Frank R. Kschischang and Danilo Silva. *Communication Over Finite-Chain-Ring Matrix Channels* IEEE Trans. Inf. Theory, 60-10, 5899–5917

[6] Marta Giorgetti, Andrea Previtali, *Galois invariance, trace codes and subfield subcodes*, Finite Fields Appl. 16 (2) 96-99(2010).

[7] T. Honold and I. Landjev, *Linear Codes over Finite Chain rings*; Electmon. J. Combin., 7 (2000), pp. reseach Paper 11, 22pp. (electronic)

[8] Martinez-Moro E., Nicolas A.P.,Rua F.,*On trace codes and Galois invariance over finite commutative chain rings*, Finite Fields Appl. Vol. 22, pp. 114-121 (2013).

[9] McDonald B. R., *Finite Rings with Identity*, Marcel Dekker, New York (1974).

[10] McWilliams F. J. and Sloane N. J. A., *The Theory of Error-Correcting Codes,* North-Holland Mathematical Library, Vol.16, North-Holland Publishing Co., Amsterdam, (1977).

[11] Alexandr A. Nechaev, *Finite rings with applications*, in: Handbook of Algebra, vol. 5, Elsevier/North-Holland, Amsterdam, 2008, pp. 213–320.

[12] Norton G.H., Sālāgean A., *On the Structure of Linear and Cyclic Codes over a Finite Chain Ring*, AAECC Vol. 10, pp. 489-506, (2000).

[13] Shibuya T., Matsumoto R. and Sakaniwa K., *An Improved Bound for the Dimension of Subfield Subcodess*, IEICE Trans. Fundamentals, Vol. E80-A, No. 5, (1987).

[14] Stichtenoth, Henning On the dimension of subfield subcodes. IEEE Trans. Inform. Theory 36 (1990), no. 1, 90–93.

[15] E.A. Whelan , *A note on finite local rings*, Rocky Mountain J.Math. 22(2)(1992)757-759.

[16] Z.-X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific,Vol 24 (2003).

[17] Z.-X. Wan, *Cyclic codes over Galois rings*, Algebra Colloq. 6(3) (1999), pp. 291-304.