Galois Theory for Linear Codes

A. Fotue Tabue[1] and E. Martínez-Moro[2] and C. Mouaha[1]

[1] *Department of mathematics, Faculty of Sciences, University of Yaoundé 1, Cameroon,*
alexfotue@gmail.com, cmouaha@yahoo.fr
[2] *Institute of Mathematics, University of Valladolid, Spain,* Edgar.Martinez@uva.es

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

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

is an $\mathtt{R}$-linear code. The relation between the trace code and the restriction code will be given by a generalization of the celebrated result due to Delsarte [**?**]

$$\mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}(\mathscr{B}^{\perp_{\varphi'}}) = \mathtt{Res}_{\mathtt{R}}(\mathscr{B})^{\perp_\varphi}, \tag{2}$$

where $\perp_\varphi$ and $\perp_{\varphi'}$ denote the duality operators associated to the nondegenerate bilinear forms $\varphi : \mathtt{R}^\ell \times \mathtt{R}^\ell \to \mathtt{R}$ and $\varphi' : \mathtt{S}^\ell \times \mathtt{S}^\ell \to \mathtt{S}$ respectively defined as follows. Let be $\mathbf{a}$ and $\mathbf{b}$ in $\mathtt{S}^\ell$, their Euclidian inner product is defined as $(\mathbf{a},\mathbf{b})_{\mathtt{E}} = a_1b_1 + a_2b_2 + \cdots + a_\ell b_\ell$, and if m is even their Hermitian inner product is defined as $(\mathbf{a},\mathbf{b})_{\mathtt{H}} = (\sigma^{\frac{m}{2}}(\mathbf{a}),\mathbf{b})_{\mathtt{E}}$. Note that $(-,-)_{\mathtt{E}}$ is a nondegenerate symmetry bilinear form.
For all $\mathbf{a}$ in $\mathtt{S}^\ell$ and $\mathbf{b}$ in $\mathtt{R}^\ell$, $\mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}((\mathbf{a},\mathbf{b})_{\mathtt{E}}) = \left(\mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}(\mathbf{a}),\mathbf{b}\right)_{\mathtt{E}}$, and if m is even, $\mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}((\mathbf{a},\mathbf{b})_{\mathtt{H}}) = \mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}((\mathbf{a},\mathbf{b})_{\mathtt{E}})$, since $\mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}\left(\sigma^{\frac{m}{2}}(\mathbf{a})\right) = \mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}(\mathbf{a})$. Throughout the paper $\varphi = (-,-)_{\mathtt{E}}$ and if m is even $\varphi' = (-,-)_{\mathtt{H}}$, otherwise $\varphi' = (-,-)_{\mathtt{E}}$. It is clear that

$$\varphi(\mathbf{b}, \mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}(\mathbf{a})) = \varphi(\mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}(\mathbf{a}), \mathbf{b}) = \mathtt{Tr}^{\mathtt{S}}_{\mathtt{R}}(\varphi'(\mathbf{a},\mathbf{b})), \text{ for all } \mathbf{a} \in \mathtt{S}^\ell \text{ and } \mathbf{b} \in \mathtt{R}^\ell. \tag{3}$$

A finite commutative ring $\mathtt{R}$ with identity is called a *finite chain ring* if its ideals are linearly ordered by inclusion $\mathtt{R}$ form a chain $\mathtt{R} \supsetneq \mathtt{R}\theta \supsetneq \cdots \supsetneq \mathtt{R}\theta^{s-1} \supsetneq \mathtt{R}\theta^s = \{0\}$. The set $\Gamma(\mathtt{R}) = \Gamma(\mathtt{R})^* \cup \{0\}$ is a complete set of representatives of $\mathtt{R}$ modulo θ and each element a of $\mathtt{R}$ can be expressed uniquely as a *θ-adic decomposition* $a = \gamma_0(a) + \gamma_1(a)\theta + \cdots + \gamma_{s-1}(a)\theta^{s-1}$. Therefore we have a *valuation function* of $\mathtt{R}$, defined by $\vartheta_{\mathtt{R}}(a) := \mathtt{min}\{t \in \{0,1,\cdots,s\} \,|\, \gamma_t(a) \neq 0\}$ and a *degree function* of

$\mathtt{R}$, defined by $\mathtt{deg}_{\mathtt{R}}(a) := \mathtt{max}\{t \in \{0,1,\cdots,s\} \,|\, \gamma_t(a) \neq 0\}$, for each a in $\mathtt{R}$. We will assume that $\vartheta_{\mathtt{R}}(0) = s$ and $\mathtt{deg}_{\mathtt{R}}(0) = -\infty$.

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

$$\mathtt{Fix}_{\mathtt{S}}(H) := \left\{ a \in \mathtt{S} \;\middle|\; \rho(a) = a, \text{ for all } \rho \in H \right\}.$$

Definition 1 *The ring $\mathtt{S}$ is a* Galois extension *of $\mathtt{R}$ with Galois group G if*

1. *$\mathtt{Fix}_{\mathtt{S}}(G) = \mathtt{R}$ and*
2. *there are elements $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}; \alpha_0^*, \alpha_1^*, \cdots, \alpha_{m-1}^*$ in $\mathtt{S}$ 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 $\delta_{i,j} = 1_{\mathtt{S}}$ if $i = j$, and $0_{\mathtt{S}}$ otherwise).

Let A be a matrix in $\mathtt{S}^{k\times\ell}$ 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
$$\vartheta_A(i) := \vartheta_{\mathtt{S}}(A[i:]) := \mathtt{min}\{\vartheta_{\mathtt{S}}(A[i;j]) \,|\, 1 \leq j \leq \ell\}.$$
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
$$\rho(i) := \mathtt{min}\left\{ j \in \{1;\cdots;\ell\} \,|\, \vartheta_S(A[i;j]) = \vartheta_i \right\}.$$

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

Definition 2 (Matrix in row standard form [?]) *A matrix $A\in \mathtt{S}^{k\times\ell}$ 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 $A[i:]\in(\theta^{\vartheta_i}\mathtt{S})^{\ell}$ and*
3. *for all pairs $i,t\in\{1,\cdots,k\}$ such that $t\neq i$, then either $i>t$ and $\mathtt{deg}_{\mathtt{R}}(A[t;\rho(i)])<\vartheta_i$ or $A[i;\rho(t)]=0$.*

Let $A\in\mathtt{S}^{k\times\ell}$ be a nonzero matrix, we say that a matrix $B\in\mathtt{S}^{k\times\ell}$ 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 [**?**]. Since the set of all generator matrices of any $\mathtt{S}$-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 $\mathtt{RSF}(\mathscr{B})$. As usual we define the type of a linear code as follows. Let $\mathscr{B}$ be an $\mathtt{S}$-linear code of length ℓ. Denoted by θ^{ϑ_i} the i-th pivot of $\mathtt{RSF}(\mathscr{B})$. The *type* $\mathscr{B}$ is the $(s+1)$-tuples $(\ell;k_0,k_1,\cdots,k_{s-1})$ where $k_t:=|\{\vartheta_i\,|\,\vartheta_i=t\}|$. Clearly the $\mathtt{S}$-rank of $\mathscr{B}$ and the number of codewords of $\mathscr{B}$, are

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

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

$$\sigma(\mathscr{B})=\left\{(\sigma(c_0),\sigma(c_1),\cdots,\sigma(c_{\ell-1}))\,\middle|\,(c_0,c_1,\cdots,c_{\ell-1})\in\mathscr{B}\right\}. \tag{4}$$

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

Theorem 3 *Let $\mathscr{B}$ be an $\mathtt{S}$-linear code and $A\in\mathtt{S}^{k\times\ell}$ a generator matrix of $\mathscr{B}$. Then the following facts are equivalent.*

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

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

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

1. *$\mathscr{B}$ is Galois invariant,*
2. *$\mathtt{Res}_{\mathtt{R}}(\mathscr{B})$ is of type $(\ell;k_0,k_1,\cdots,k_{s-1})$.*

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

Proposition 1 *The operators*

$$\mathscr{L}(\mathtt{S}^\ell) \underset{\mathtt{Ext}}{\overset{\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}};\mathtt{Res}_{\mathtt{R}}}{\rightleftarrows}} \mathscr{L}_\ell(\mathtt{R}) \tag{5}$$

are lattice morphisms. Moreover,

$$\mathtt{Ext}(\mathscr{C}^\perp) = \mathtt{Ext}(\mathscr{C})^\perp \text{ and } \mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(\mathtt{Ext}(\mathscr{C})) = \mathtt{Res}_{\mathtt{R}}(\mathtt{Ext}(\mathscr{C})) = \mathscr{C} \text{ for all } \mathscr{C} \in \mathscr{L}_\ell(\mathtt{R}).$$

Definition 4 (Galois closure and Galois interior) *Let $\mathscr{B}$ be a linear code over $\mathtt{S}$.*

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

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

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

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

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

1. $\mathtt{J}_G(\mathtt{J}_G(\mathscr{B})) = \mathtt{J}_G(\mathscr{B})$ and

2. for all $\mathscr{B}$ in $\mathscr{L}(\mathtt{S}^\ell)$ the code $\mathtt{J}_G(\mathscr{B})$ is Galois invariant.

The Galois closure and Galois interior are indeed Galois operators and $\widetilde{\overset{\circ}{\mathscr{B}}} = \overset{\circ}{\mathscr{B}}$, $\overset{\circ}{\widetilde{\mathscr{B}}} = \widetilde{\mathscr{B}}$. From Definition 4, it follows that $\mathscr{B}$ is Galois invariant if and only if $\widetilde{\mathscr{B}} = \overset{\circ}{\mathscr{B}}$.

Proposition 2 *If $\mathscr{B}$ is a linear code over $\mathtt{S}$ then* $\left(\overset{\circ}{\mathscr{B}^{\perp}}\right) = \left(\widetilde{\mathscr{B}}\right)^{\perp}$.

Lemma 5 *Let $\mathscr{B}$ be a linear code over $\mathtt{S}$. Then* $\overset{\circ}{\mathscr{B}} = \mathtt{Ext}(\mathtt{Res}_{\mathtt{R}}(\mathscr{B})) = \bigcap_{\sigma \in G} \sigma(\mathscr{B})$.

For any $\mathscr{B}$ in $\mathscr{L}\left(\mathtt{S}^\ell\right)$, we consider $\mathscr{L}(\mathscr{B})$ the lattice of $\mathtt{S}$-linear subcode of $\mathscr{B}$. Let us define

$$\begin{array}{rccc} \mathtt{Stab}: & \mathscr{L}(\mathscr{B}) & \rightarrow & \mathtt{Sub}(G) \\ & \mathscr{T} & \mapsto & \mathtt{Stab}(\mathscr{T}), \end{array} \quad \text{and} \quad \begin{array}{rccc} \mathtt{Fix}_{\mathscr{B}}: & \mathtt{Sub}(G) & \rightarrow & \mathscr{L}(\mathscr{B}) \\ & H & \mapsto & \bigcap_{\sigma \in H} \sigma(\mathscr{B}), \end{array}$$

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

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

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

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

Theorem 6 *For each $\mathscr{B}$ in $\mathscr{L}\left(\mathtt{S}^\ell\right)$, the pair $(\mathtt{Stab}; \mathtt{Fix}_{\mathscr{B}})$ is a Galois correspondence between $\mathscr{B}$ and G.*

References

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

[2] 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).

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

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