On trace codes, duality and Galois invariance

EKU Seminar on Coding Theory

E. Martínez-Moro

imUVa Instituto de Investigación en Matemáticas

Universidad de Valladolid

Acknowledgements

Main reference: E. Martínez-Moro and A.P. Nicolás and I.F. Rua "On trace codes and Galois invariance over finite commutative chain rings". Finite Fields and Their Applications (2013), **22**(0), 114 – 121.

Outline

Instituto de Matemáticas

Introduction

Let $\mathbb{F}_{q^e}$ be the finite field of q^e elements, q a power of a prime, and let C be a linear code over $\mathbb{F}_{q^m}$ of length n, i.e., a linear subspace of $\mathbb{F}_{q^e}^n$. There are two classical constructions that allow us to build a linear code over $\mathbb{F}_q$ from C.

If C has dimension k over $\mathbb{F}_{q^e}$ and minimum distance d, then the subfield subcode (or restriction of C to $\mathbb{F}_q$) is defined as

$$\mathrm{Res}_{\mathbb{F}_q}(C) = C \cap \mathbb{F}_q^n.$$

The code $\mathrm{Res}_{\mathbb{F}_q}(C)$ is a $\mathbb{F}_q$-linear code of length n, dimension $k_s \geq ek - (e-1)n$ and minimum distance $d_s \geq d$.

Introduction

Let $\mathbb{F}_{q^e}$ be the finite field of q^e elements, q a power of a prime, and let C be a linear code over $\mathbb{F}_{q^m}$ of length n, i.e., a linear subspace of $\mathbb{F}_{q^e}^n$. There are two classical constructions that allow us to build a linear code over $\mathbb{F}_q$ from C.

If C has dimension k over $\mathbb{F}_{q^e}$ and minimum distance d, then the subfield subcode (or restriction of C to $\mathbb{F}_q$) is defined as

$$\mathrm{Res}_{\mathbb{F}_q}(C) = C \cap \mathbb{F}_q^n.$$

The code $\mathrm{Res}_{\mathbb{F}_q}(C)$ is a $\mathbb{F}_q$-linear code of length n, dimension $k_s \geq ek - (e-1)n$ and minimum distance $d_s \geq d$.

The trace code of C is given by

$$\mathrm{Tr}_{\mathbb{F}_{q^e}|\mathbb{F}_q}(C) = \left\{ \left(\mathrm{Tr}_{\mathbb{F}_{q^e}|\mathbb{F}_q}(c_1), \ldots, \mathrm{Tr}_{\mathbb{F}_{q^e}|\mathbb{F}_q}(c_n) \right) \mid (c_1, \ldots, c_n) \in C \right\}$$

where $\mathrm{Tr}_{\mathbb{F}_{q^e}|\mathbb{F}_q}$ denotes the trace function over $\mathbb{F}_q$. The dimension k_t of the trace code fulfills $k \leq ek_t$.

Chain Rings

A commutative ring R is said a chain ring if the lattice of all its ideals is a chain. This implies that R is a principal ideal ring and its chain of ideals is

$$R > \mathfrak{m} > \cdots > \mathfrak{m}^{t-1} > \mathfrak{m}^t = 0,$$

for some $t \in \mathbb{N}$, where $\mathfrak{m} = \mathfrak{N}(R)$ denotes the nilradical of R. In particular, R is a local ring and the quotient $R/\mathfrak{m}$ is a finite field $\mathbb{F}_q$. If $t > 1$, then $\mathfrak{m}^i = Rp^i$, for $i = 1, \ldots, t$, with p any element in $\mathfrak{m}^2 \setminus \mathfrak{m}$. In such a case, any element $a \in R$ can be uniquely written as $a = \sum_{i=0}^{t-1} a_i p^i$, with $a_i \in \Gamma(R) = \{b \in R \mid b^q = b\}$.

Chain Rings

The set $\Gamma(R)$ is a coordinate set of R, i.e., a complete set of representatives of R mod $\mathfrak{m} = Rp$. If $\pi : R \to R/\mathfrak{m}$ is the canonical projection, a monic polynomial $f \in R[x]$ is called basic irreducible if $\pi(f)$ is irreducible in $(R/\mathfrak{m})[x]$.

Let R and S be two finite commutative chain rings such that $R \subset S$ and $1_R = 1_S$. We say that S is an extension of R and we denote it by $S|R$. Provided that $\mathfrak{m}$ and $\mathfrak{M}$ are the maximal ideals of R and S respectively, we say that the extension $S|R$ is separable if $\mathfrak{m}S = \mathfrak{M}$. The last condition is equivalent to the condition $S \cong R[x]/(f)$, where (f) is the ideal generated by a monic basic irreducible polynomial $f \in R[x]$.

Chain Rings

The set $\Gamma(R)$ is a coordinate set of R, i.e., a complete set of representatives of R mod $\mathfrak{m} = Rp$. If $\pi : R \to R/\mathfrak{m}$ is the canonical projection, a monic polynomial $f \in R[x]$ is called basic irreducible if $\pi(f)$ is irreducible in $(R/\mathfrak{m})[x]$.

Let R and S be two finite commutative chain rings such that $R \subset S$ and $1_R = 1_S$. We say that S is an extension of R and we denote it by $S|R$. Provided that $\mathfrak{m}$ and $\mathfrak{M}$ are the maximal ideals of R and S respectively, we say that the extension $S|R$ is separable if $\mathfrak{m}S = \mathfrak{M}$. The last condition is equivalent to the condition $S \cong R[x]/(f)$, where (f) is the ideal generated by a monic basic irreducible polynomial $f \in R[x]$.

Galois Extensions of Chain Rings

let us assume that $S|R$ is a separable extension of finite commutative chain rings. The group G of all automorphims γ of S such that $\gamma|_R$ is the identity is called the Galois group of $S|R$.

It can be proven that the extension $S|R$ is Galois, that is, $S^G = R$, where $S^G = \{s \in S \mid \gamma(s) = s, \forall \gamma \in G\}$ is the fixed subring of S. Moreover, G is isomorphic to the Galois group of the extension $\mathbb{F}_{q^e}|\mathbb{F}_q$ where $\mathbb{F}_{q^e}$ is the residue field $S/\mathfrak{M}$.

Galois Extensions of Chain Rings

let us assume that $S|R$ is a separable extension of finite commutative chain rings. The group G of all automorphims γ of S such that $\gamma|_R$ is the identity is called the Galois group of $S|R$.

It can be proven that the extension $S|R$ is Galois, that is, $S^G = R$, where $S^G = \{s \in S \,|\, \gamma(s) = s, \forall\gamma \in G\}$ is the fixed subring of S. Moreover, G is isomorphic to the Galois group of the extension $\mathbb{F}_{q^e}|\mathbb{F}_q$ where $\mathbb{F}_{q^e}$ is the residue field $S/\mathfrak{M}$.

Galois Extensions of Chain Rings

Thus, G is a cyclic group and it is generated by the power map $\gamma(a) = a^q$, for a suitable primitive element $a \in S$. Furthermore, the set $B = \{\gamma^i(a) \mid i = 0, \ldots, e-1\}$ is a free $R-$basis of S, i.e., B is a normal basis of S, and we can assume w.l.o.g. that $B \subset \Gamma(S)$, the coordinate system of S. Moreover, S is also an unramified extension of R. So, the maximal ideal $\mathfrak{M}$ of S is generated by the maximal ideal of R, that is, $\mathfrak{M} = S\mathfrak{m} = Sp$. Hence, the lattice of ideals of S is

$$S > Sp > Sp^2 > Sp^3 > \cdots > Sp^t = 0.$$

Galois Extensions of Chain Rings

Thus we can write any element $s \in S$ as $s = p^l u$, where $l = 0, 1, \ldots, t$ is unique and $u \in S \setminus Sp$ is a unit of S unique modulo Sp^{t-l}. The function $\nu : S \to \{0, 1, \ldots, t\}$ defined by $\nu(p^l u) = l$ is well-defined because of the uniqueness of l. It verifies that $\nu(s) = 0$ if and only if s is a unit of S.

Galois invariant codes

Let $S|R$ be a separable extension of finite chain rings and let G be the group of R-automorphims of S. If $\gamma \in G$, then γ acts naturally over S^n coordinatewise.

A code of length n over S is any subset $C \subseteq S^n$. The code $C \subseteq S^n$ is called linear if it is a submodule of S^n, and it is called G-invariant (Galois invariant) if

$$\gamma(C) = C \text{ for all } \gamma \in G.$$

Galois invariant codes

The trace function Tr of an element $s \in S$ over R is defined as $\mathrm{Tr}(s) = \sum_{\gamma \in G} \gamma(s)$. This action can be also extended to S^n coordinatewise and a code $C \subseteq S^n$ is called trace invariant if $\mathrm{Tr}(C) = C$. Note that $\mathrm{Tr}(C)$ is a code over R.

Given a linear code C, we define the restriction of C, $\mathrm{Res}(C)$, as the set of all the elements of C which have components in R, i.e., $\mathrm{Res}(C) = C \cap R^n$ and it is also a code over R.

Galois invariant codes

The trace function Tr of an element $s \in S$ over R is defined as $\mathrm{Tr}(s) = \sum_{\gamma \in G} \gamma(s)$. This action can be also extended to S^n coordinatewise and a code $C \subseteq S^n$ is called trace invariant if $\mathrm{Tr}(C) = C$. Note that $\mathrm{Tr}(C)$ is a code over R.

Given a linear code C, we define the restriction of C, $\mathrm{Res}(C)$, as the set of all the elements of C which have components in R, i.e., $\mathrm{Res}(C) = C \cap R^n$ and it is also a code over R.

Galois invariant codes

A third construction is the following. If C is a linear code over R (i.e., a linear submodule of R^n), then we define the extension of C as the S-linear code $\mathrm{Ext}(C) = C \otimes_R S$, i.e., the set of all S-linear combinations of codewords in C.

Notice that if C, D are two codes over R and $C \subseteq D$, then $\mathrm{Ext}(C) \subseteq \mathrm{Ext}(D)$. Notice also that $\mathrm{Res}(C) = \mathrm{Res}(\mathrm{Ext}(\mathrm{Res}(C)))$ for any code C over R.

Galois invariant codes

A third construction is the following. If C is a linear code over R (i.e., a linear submodule of R^n), then we define the extension of C as the S-linear code $\mathrm{Ext}(C) = C \otimes_R S$, i.e., the set of all S-linear combinations of codewords in C.

Notice that if C, D are two codes over R and $C \subseteq D$, then $\mathrm{Ext}(C) \subseteq \mathrm{Ext}(D)$. Notice also that $\mathrm{Res}(C) = \mathrm{Res}(\mathrm{Ext}(\mathrm{Res}(C)))$ for any code C over R.

Lemma: Canonical Form

Lemma.- Let S be a finite commutative chain ring with maximal ideal Sp, and let C be a linear code. There exist elements $c_i = (0, \ldots, 0, p^{\alpha_i}, y_{ii+1}, \ldots, y_{in}) \in C$, $i = 1, \ldots, m$, with $\alpha_i \in \mathbb{N} \cup \{0\}$ and $y_{ij} \in S$, such that the code generated by $\{c_1, \ldots, c_m\}$ is (permutationally) equivalent to C.

Proof: Let $\{b_1, \ldots, b_l\}$ be any generator system of C as submodule of S^n. Let A be the $l \times n$ matrix constructed by stacking the generators words $b_i = (a_{i1}, \ldots, a_{in})$, for $i = 1, \ldots, l$.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{ln} \end{bmatrix}$$

Instituto de Matemáticas

Lemma: Canonical Form

Lemma.- Let S be a finite commutative chain ring with maximal ideal Sp, and let C be a linear code. There exist elements $c_i = (0, \ldots, 0, p^{\alpha_i}, y_{ii+1}, \ldots, y_{in}) \in C$, $i = 1, \ldots, m$, with $\alpha_i \in \mathbb{N} \cup \{0\}$ and $y_{ij} \in S$, such that the code generated by $\{c_1, \ldots, c_m\}$ is (permutationally) equivalent to C.

Proof: Let $\{b_1, \ldots, b_l\}$ be any generator system of C as submodule of S^n. Let A be the $l \times n$ matrix constructed by stacking the generators words $b_i = (a_{i1}, \ldots, a_{in})$, for $i = 1, \ldots, l$.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{ln} \end{bmatrix}$$

Lemma: Canonical Form

Since S is a principal ideal ring, it is possible to transform A by a sequence of elementary transformations into a matrix of the form

$$B = \begin{bmatrix} p^{\nu_1} & y_{12} & \cdots & y_{1k} & y_{1k+1} & \cdots & y_{1n} \\ 0 & p^{\nu_2} & \cdots & y_{2k} & y_{2k+1} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & p^{\nu_m} & y_{mm+1} & \cdots & y_{mn} \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

where $\nu_1 \leq \nu_2 \leq \cdots \leq \nu_m < t$, $\nu_i \leq \nu(y_{ij})$, for all $i = 1, \ldots, m$ and $j = i + 1, \ldots, n$, and $\nu_i > \nu(y_{ki})$, for all $i = 1 = 1, \ldots, m$ and $k < i$ (unless $y_{ki} = 0$).

Lemma: Canonical Form

Notice that only row operations and column permutations are needed in such a transformation, so the first m rows of B generate a code C' permutationally equivalent to C. □

Instituto de Matemáticas

Main Theorem

Theorem.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G. A S-linear code C is G-invariant if and only if $C = \mathrm{Ext}\left(\mathrm{Res}\left(C\right)\right)$ or, equivalently, if and only if the S-submodule C admits a generator system in R^n.

Corollary

Let C be a linear S-code. If G is the Galois group of $S|R$, the code $C_G = \bigcap_{\gamma \in G} \gamma(C)$ is the largest G-invariant subcode of C. This code is called the G-core of C. As a consequence of the main theorem we obtain the relationship between the G-core of C and the extension-restriction code.

Corollary.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G, and let C be a linear $S-$code. If $C_G = \bigcap_{\gamma \in G} \gamma(C)$, then $C_G = \mathrm{Ext}(\mathrm{Res}(C)) = \mathrm{Ext}(\mathrm{Res}(C_G))$.

Corollary

Let C be a linear S-code. If G is the Galois group of $S|R$, the code $C_G = \bigcap_{\gamma \in G} \gamma(C)$ is the largest G-invariant subcode of C. This code is called the G-core of C. As a consequence of the main theorem we obtain the relationship between the G-core of C and the extension-restriction code.

Corollary.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G, and let C be a linear $S-$code. If $C_G = \bigcap_{\gamma \in G} \gamma(C)$, then $C_G = \mathrm{Ext}(\mathrm{Res}(C)) = \mathrm{Ext}(\mathrm{Res}(C_G))$.

Corollary

Proof.- Let $D = \text{Ext}(\text{Res}(C))$. This is a G-invariant subcode of C by the previous Theorem, and so $D = D_G$. On the other hand, $D \subseteq C$, thus $D = D_G \subseteq C_G$, which is G-invariant. Using again the main theorem, $C_G = \text{Ext}(\text{Res}(C_G)) \subseteq \text{Ext}(\text{Res}(C)) = D$. This concludes the proof. $\square$

Invariance

Lemma.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G. For any S-linear code C

$$\mathrm{Res}(C) \subseteq \mathrm{Tr}(C).$$

Moreover, if C is G-invariant, then

$$\mathrm{Res}(C) = \mathrm{Tr}(C).$$

Lemma.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G. Then, for any $v \in S^n$, $v \in \mathrm{Ext}\left(\mathrm{Tr}\left(Sv\right)\right)$.

Invariance

Lemma.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G. For any S-linear code C

$$\mathrm{Res}(C) \subseteq \mathrm{Tr}(C).$$

Moreover, if C is G-invariant, then

$$\mathrm{Res}(C) = \mathrm{Tr}(C).$$

Lemma.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G. Then, for any $v \in S^n$, $v \in \mathrm{Ext}\left(\mathrm{Tr}\left(Sv\right)\right)$.

Invariance Theorem

Theorem.- For any separable extension $S|R$ of finite commutative chain rings, and for any S-linear code C,

$$\operatorname{Res}(C) = \operatorname{Tr}(C)$$

if and only if C is invariant under the Galois group of $S|R$.

Galois closure

The Galois closure $\bar{C}$ of an arbitrary code C over S is the smallest Galois closed code over S containing C. It may be obtained from C by taking the span of all images of some set of generators of C under the Galois automorphisms.

Galois closure

Proposition.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G. If C is a $S-$linear code, and $\bar{C}$ is its Galois closure, then $\mathrm{Tr}(C) = \mathrm{Tr}(\bar{C})$.

Proof: Since $C \subseteq \bar{C}$ we have $\mathrm{Tr}(C) \subseteq \mathrm{Tr}(\bar{C})$. On the other hand, let $c \in \bar{C}$, then $c = \sum_j \lambda_j \sigma_j(c_j)$ where $\lambda_j \in S, c_j \in C$ and $\sigma_j \in G$. Now, because $\mathrm{Tr}(x) = \mathrm{Tr}(\sigma(x))$ for all $x \in S^n$, we have that

$$\mathrm{Tr}(c) = \mathrm{Tr}\left(\sum_j \lambda_j \sigma_j(c_j)\right) = \sum_j \mathrm{Tr}\left(\lambda_j \sigma_j(c_j)\right)$$

$$= \sum_j \mathrm{Tr}\left(\sigma_j^{-1}(\lambda_j) c_j\right) = \mathrm{Tr}\left(\sum_j \sigma_j^{-1}(\lambda_j) c_j\right) \in \mathrm{Tr}(C) \quad \square$$

Galois closure

Proposition.- Let $S|R$ be a separable extension of finite commutative chain rings with Galois group G. If C is a $S-$linear code, and $\bar{C}$ is its Galois closure, then $\mathrm{Tr}(C) = \mathrm{Tr}(\bar{C})$.

Proof: Since $C \subseteq \bar{C}$ we have $\mathrm{Tr}(C) \subseteq \mathrm{Tr}(\bar{C})$. On the other hand, let $c \in \bar{C}$, then $c = \sum_j \lambda_j \sigma_j(c_j)$ where $\lambda_j \in S, c_j \in C$ and $\sigma_j \in G$. Now, because $\mathrm{Tr}(x) = \mathrm{Tr}(\sigma(x))$ for all $x \in S^n$, we have that

$$\mathrm{Tr}(c) = \mathrm{Tr}\left(\sum_j \lambda_j \sigma_j(c_j)\right) = \sum_j \mathrm{Tr}\left(\lambda_j \sigma_j(c_j)\right)$$

$$= \sum_j \mathrm{Tr}\left(\sigma_j^{-1}(\lambda_j) c_j\right) = \mathrm{Tr}\left(\sum_j \sigma_j^{-1}(\lambda_j) c_j\right) \in \mathrm{Tr}(C) \quad \square$$

Galois closure

Theorem [Delsarte].-
Let $S|R$ be a separable extension of finite commutative chain rings. If C is a $S-$linear code, then $\mathrm{Res}(C)^{\perp} = \mathrm{Tr}(C^{\perp})$, where $C^{\perp}$ is the orthogonal complement to C with respect to the usual scalar product, and $\mathrm{Res}(C)^{\perp}$ is the orthogonal complement of $\mathrm{Res}(C)$ in R^n.

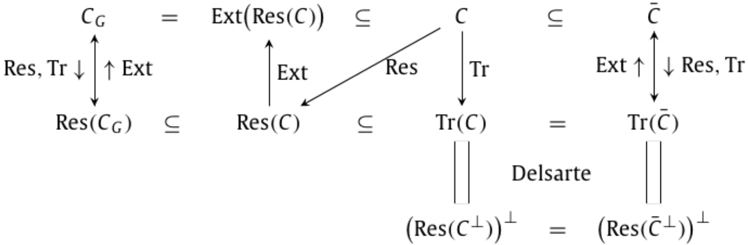
Proof:
Since $S|R$ is Galois, the bilinear form $B : S \times S \to R$ defined by $B(x, y) = \mathrm{Tr}(xy)$ is non degenerate. The proof follows the lines of the classical Delsarte's theorem □

Galois closure

Theorem [Delsarte].-
Let $S|R$ be a separable extension of finite commutative chain rings. If C is a $S-$linear code, then $\mathrm{Res}(C)^{\perp} = \mathrm{Tr}(C^{\perp})$, where $C^{\perp}$ is the orthogonal complement to C with respect to the usual scalar product, and $\mathrm{Res}(C)^{\perp}$ is the orthogonal complement of $\mathrm{Res}(C)$ in R^n.

Proof:
Since $S|R$ is Galois, the bilinear form $B : S \times S \to R$ defined by $B(x, y) = \mathrm{Tr}(xy)$ is non degenerate. The proof follows the lines of the classical Delsarte's theorem $\square$

The picture


$C_G = \mathrm{Ext}(\mathrm{Res}(C)) \subseteq C \subseteq \bar{C}$
Res, Tr ↓
↑ Ext
Ext
Res
Tr
Ext ↑
↓ Res, Tr
$\mathrm{Res}(C_G) \subseteq \mathrm{Res}(C) \subseteq \mathrm{Tr}(C) = \mathrm{Tr}(\bar{C})$
Delsarte
$(\mathrm{Res}(C^\perp))^\perp = (\mathrm{Res}(\bar{C}^\perp))^\perp$