Galois invariance, trace codes and subfield subcodes

Marta Giorgetti*, Andrea Previtali

Dipartimento di Fisica e Matematica, Università dell’Insubria, Via Valleggio, 11, Como–22100, Italy

**A R T I C L E  I N F O**

Article history:
Received 26 February 2009
Revised 21 September 2009
Available online 2 February 2010
Communicated by W. Cary Huffman

Keywords:
Trace codes
Subfield subcodes
Galois invariant

**A B S T R A C T**

Given a Galois extension we relate subfield subcodes with trace codes showing that a code is invariant under the Galois group if and only if its restriction coincides with the trace code.
© 2010 Elsevier Inc. All rights reserved.

1. Introduction

Given a field extension \( E/K \) and a linear code \( C \) over \( E \) there are at least two constructions starting from \( C \) and leading to linear codes over \( K \). One simply considers all elements of \( C \) having components in \( K \). This is called the restriction of \( C \) to \( K \) and will be denoted with \( \text{Res}(C) \). It is also known as the subfield subcode of \( C \). The second construction exploits the field trace \( \text{Tr} \) from \( E \) to \( K \). Namely, we first extend \( \text{Tr} \) from \( E \) to \( E^n \), setting \( \text{Tr}(c) = (\text{Tr}(c_1), \ldots, \text{Tr}(c_n)) \), then define \( \text{Tr}(C) = \{\text{Tr}(c) : c \in C\} \). This is a linear code defined over \( K \) and we call it the trace code associated to \( C \). In [3] Delsarte has shown that these codes are related: the dual of the restriction of \( C \) is the trace of the dual code of \( C \) (see Theorem 3).

We now restrict our attention to Galois extensions \( E/K \). This is of course always the case when dealing with codes defined over finite fields. Let \( \Gamma \) be the Galois group of \( E \) over \( K \), \( \Gamma = \text{Gal}(E/K) \), then we say a linear code \( C \) over \( E \) is \( \Gamma \)-invariant if \( C^\gamma = C \) for all \( \gamma \in \Gamma \), where \( \gamma \) is extended in the obvious way from \( E \) to \( E^n \), \( n \) being the length of \( C \). Given a linear code \( D \) over \( K \), we may extend

---

* Corresponding author.
E-mail addresses: marta.giorgetti@uninsubria.it (M. Giorgetti), andrea.previtali@uninsubria.it (A. Previtali).

1071-5797/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2010.01.002
scalars and obtain a linear code $C$ over $E$, $C = E \otimes_K D$. This code will be called the **extension** of $D$ to $E$ and denoted $\text{Ext}(D)$. If $E/K$ is Galois, then $C = \text{Ext}(D)$ is a $\Gamma^*$-invariant code.

By using elementary linear algebra, we prove that extension and restriction realize a one-to-one correspondence between $K$-linear codes and $\Gamma^*$-invariant $E$-linear codes.

One direction of this correspondence (if the code is Galois invariant then its subfield subcode equals its trace code), can already be found in [5, Lemma 1], [1, Theorem 4] and [2, Theorem 12.7]. Exploiting this result we prove that

\[
\text{Res}(C) \subseteq \text{Tr}(C)
\]

always holds. One might wonder whether the inverse inclusion also holds. This is generally false, but we show that the key to equality is related to $\Gamma^*$-invariance. Namely, we show that restriction and trace lead to the same code if and only if the original code is $\Gamma^*$-invariant.

2. Trace and Galois invariant codes

Given a Galois extension $E/K$ with Galois group $\Gamma$, we prove that extension and restriction realize a one-to-one correspondence between $K$-linear codes and $\Gamma^*$-invariant $E$-linear codes.

**Theorem 1.** Let $E/K$ be a Galois extension with group $\Gamma$ and $C$ an $E$-subspace of $E^n$. Then $C$ is $\Gamma^*$-invariant if and only if $C = \text{Ext}(\text{Res}(C))$ or, equivalently, if and only if $C$ admits a basis in $K^n$.

**Proof.** Let $D$ be a $K$-linear code, $D = \bigoplus_j K u_j$, then $\text{Ext}(D) = \bigoplus_j E u_j$ with $u_j \in K^n$. Set $C = \text{Ext}(D)$, then $C^\gamma = \bigoplus_j E u_j^\gamma = C$, since $u_j^\gamma = u_j$ for any $\gamma \in \Gamma$. Thus any extended code is $\Gamma^*$-invariant.

Conversely, assume $C$ is a $\Gamma^*$-invariant $E$-linear code and let $u_1, \ldots, u_k$ be a Gauss–Jordan reduced normalized basis, that is, the left-most non-zero entry of any $u_j$ is 1 and the components in the same positions for the other basis elements are zero. Since a permutation of the coordinates does not affect $\Gamma^*$-invariance, we may assume that $u_i = e_i + a_i$, where $e_i$ is the $i$-th standard vector and $\text{Supp}(a_i) \subseteq \{k+1, \ldots, n\}$. Now $u_i^\gamma = e_i + a_i^\gamma = \sum_j \lambda_j u_j$, for some $\lambda_j \in E$. This forces $\lambda_j = \delta_{ij}$ and $a_i^\gamma = a_i$. Thus $a_i$ and $u_i \in K^n$. \hfill $\square$

Given an $E$-linear code $C$, we define the $\Gamma^*$-core of $C$ as $C_\Gamma = \bigcap_{\gamma \in \Gamma} C^\gamma$, that is, the largest $\Gamma^*$-invariant subcode of $C$.

**Corollary 2.** $C_\Gamma = \text{Ext}(\text{Res}(C))$.

**Proof.** Set $T = \text{Ext}(\text{Res}(C))$. Since $T$ is an extension–restriction code, thanks to Theorem 1, it is $\Gamma^*$-invariant, $T = T_\Gamma$. Moreover, $T \subseteq C$, thus $T \subseteq C_\Gamma$. Since $C_\Gamma$ is $\Gamma^*$-invariant, $C_\Gamma = \text{Ext}(\text{Res}(C_\Gamma)) \subseteq \text{Ext}(\text{Res}(C)) = T$. \hfill $\square$

A celebrated result of Delsarte [3] states that restriction and trace codes are related via dualization, namely:

**Theorem 3 (Delsarte).** Given a Galois extension $E/K$ and an $E$-linear code $C$, then we have

\[
\text{Res}(C)^\perp = \text{Tr}(C^\perp),
\]

where $C^\perp$ is the orthogonal complement to $C$ with respect to the usual scalar product.

We would like to unravel relations between $\text{Res}(C)$ and $\text{Tr}(C)$. We show they need not coincide.
Example 4. Let $K = \mathbb{F}_p(x)$, $E = K(\alpha)$, where $\alpha^p = x$. Then $E/K$ is an inseparable extension and $\text{Tr}(C) = 0$ for any $E$-linear code. On the other hand, $\text{Res}(C)$ need not be zero, e.g. $\text{Res}(E^n) = K^n$.

Example 5. Let $E/K$ be a quadratic extension with char $K \neq 2$. Then $E = K[\alpha], \alpha^2 = a \in K$ and $C = E\nu, \nu = (1, \alpha)$. Then $\text{Tr}(\nu) = (2, 0)$ and $\text{Tr}(\alpha \nu) = (0, 2a)$. Thus $\text{Tr}(C) = K^2$ while $\text{Res}(C) = 0$.

Notice that in this example $\text{Res}(C) \leq \text{Tr}(C)$. We prove this is the case if $E/K$ is separable.

Lemma 6. For any separable extension $E/K$ and any $E$-linear code $C$

$$\text{Res}(C) \leq \text{Tr}(C).$$

Proof. For $\nu \in K^n$, $\lambda \in E$,

$$\text{Tr}(\lambda \nu) = \text{Tr}(\lambda) \nu.$$

Since $E/K$ is separable, there exists $\alpha \in E$ such that $\text{Tr}(\alpha) = 1$ (see [4, Corollary 8.17]). Let $\nu \in \text{Res}(C) = C \cap K^n$, then $\nu = \text{Tr}(\alpha \nu) \in \text{Tr}(C)$. $\square$

We prove that if $C$ is a $\Gamma$-invariant code then $\text{Res}(C) = \text{Tr}(C)$.

Lemma 7. Let $E/K$ be a Galois extension with group $\Gamma$. If $C$ is an $E$-linear $\Gamma$-invariant code, then

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

Proof. It is enough to prove that $\text{Res}(C) \geq \text{Tr}(C)$. Since $C$ is $\Gamma$-invariant $\text{Tr}(c) = \sum_{\gamma \in \Gamma} c^\gamma \in C$. Trivially, $\text{Tr}(c) \in K^n$, then $\text{Tr}(c) \in \text{Res}(C)$. $\square$

We now prove that $\Gamma$-invariance is also a necessary condition. We first state an independent result.

Lemma 8. For any $\nu \in E^n, v \in \text{Ext}(\text{Tr}(Ev))$.

Proof. Since $E/K$ is Galois, it is separable hence $B(\nu, w) := \text{Tr}(\nu w)$ defines a non-degenerate bilinear $K$-form on $E$ considered as a $K$-vector space. Let $\lambda_1, \ldots, \lambda_m$ denote a $K$-basis for $E$. Then there exists a $K$-basis $\mu_1, \ldots, \mu_m$ of $E$ which is trace-dual to $\lambda_1, \ldots, \lambda_m$, that is,

$$\text{Tr}(\mu_k \lambda_j) = \delta_{kj}.$$

Let $\nu = (a_1, \ldots, a_n), a_i = \sum_j a_{ij} \lambda_j$. Then

$$\sum_k \lambda_k \text{Tr}(\mu_k a_i) = \sum_k a_{ik} \lambda_k = a_i.$$

Thus $\nu = \sum_k \lambda_k \text{Tr}(\mu_k \nu) \in \text{Ext}(\text{Tr}(E\nu))$. $\square$

Theorem 9. For any Galois extension $E/K$ and any $E$-linear code $C$

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

if and only if $C$ is invariant under $\Gamma$, the Galois group of $E/K$. 

Proof. It is enough to show that $\text{Res}(C) = \text{Tr}(C)$ forces $C$ to be $\Gamma$-invariant. Assume $C$ is a counterexample of minimum dimension and set $D = \bigcap_{\gamma \in \Gamma} C^\gamma$, then we claim $\dim(C/D) = 1$. In fact, let $C > V > D$ with $\dim(V/D) = 1$. Then

$$\text{Res}(C) = \text{Res}(V) = \text{Res}(D) = \text{Tr}(D) \leq \text{Tr}(V) \leq \text{Tr}(C) = \text{Res}(C).$$

Hence equality holds throughout, $V$ is a counterexample, too, and, by minimality, $C = V$.

Therefore $C = D \oplus E_v$. Now $\text{Tr}(D) = \text{Tr}(C) = \text{Tr}(D) + \text{Tr}(E_v)$, so $\text{Tr}(E_v) \leq \text{Tr}(D)$. By Lemma 8, $v \in \text{Ext}(\text{Tr}(E_v)) \leq \text{Ext}(\text{Tr}(D)) = D$ against $D \neq C$. □

References