Finite Fields and Their Applications 16 (2010) 96–99

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

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

ARTICLE INFO

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

ABSTRACT

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.

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 $\mathrm{Res}(C)$. It is also known as the subfield subcode of C. The second construction exploits the field trace Tr from E to K. Namely, we first extend Tr from E to E^n setting

$$\mathrm{Tr}\big((c_1,\dots,c_n)\big) = \big(\mathrm{Tr}(c_1),\dots,\mathrm{Tr}(c_n)\big),$$

then define $\mathrm{Tr}(C) = \{\mathrm{Tr}(c)\colon\ c \in C\}$. 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 Γ be the Galois group of E over K, $\Gamma = Gal(E/K)$, then we say a linear code C over E is Γ-invariant if $C^{\gamma} = C$ for all $\gamma \in \Gamma$, where γ 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
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 $\mathrm{Ext}(D)$. If E/K is Galois, then $C = \mathrm{Ext}(D)$ is a Γ-invariant code.

By using elementary linear algebra, we prove that extension and restriction realize a one-to-one correspondence between K-linear codes and Γ-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

$$\mathrm{Res}(C) \leqslant \mathrm{Tr}(C)$$

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 Γ-invariance. Namely, we show that restriction and trace lead to the same code if and only if the original code is Γ-invariant.

2. Trace and Galois invariant codes

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

Theorem 1. *Let E/K be a Galois extension with group Γ and C an E-subspace of E^n. Then C is Γ-invariant if and only if $C = \mathrm{Ext}(\mathrm{Res}(C))$ 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 $\mathrm{Ext}(D) = \bigoplus_j E u_j$ with $u_j \in K^n$. Set $C = \mathrm{Ext}(D)$, 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 Γ-invariant.

Conversely, assume C is a Γ-invariant E-linear code and let $u_1, \dots, u_k$ 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 Γ-invariance, we may assume that $u_i = e_i + a_i$, where e_i is the i-th standard vector and $\mathrm{Supp}(a_i) \subseteq \{k+1, \dots, n\}$. 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 $u_i \in K^n$. $\square$

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

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

Proof. Set $T = \mathrm{Ext}(\mathrm{Res}(C))$. Since T is an extension–restriction code, thanks to Theorem 1, it is Γ-invariant, $T = T_\Gamma$. Moreover, $T \leqslant C$, thus $T \leqslant C_\Gamma$. Since C_Γ is Γ-invariant, $C_\Gamma = \mathrm{Ext}(\mathrm{Res}(C_\Gamma)) \leqslant \mathrm{Ext}(\mathrm{Res}(C)) = T$. $\square$

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*

$$\mathrm{Res}(C)^\perp = \mathrm{Tr}\big(C^\perp\big),$$

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

We would like to unravel relations between $\mathrm{Res}(C)$ and $\mathrm{Tr}(C)$. 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 $\mathrm{Tr}(C) = 0$ for any E-linear code. On the other hand, $\mathrm{Res}(C)$ need not be zero, e.g. $\mathrm{Res}(E^n) = K^n$.

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

Notice that in this example $\mathrm{Res}(C) \leqslant \mathrm{Tr}(C)$. 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*

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

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

$$\mathrm{Tr}(\lambda v) = \mathrm{Tr}(\lambda) v.$$

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

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

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

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

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

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

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

Proof. Since E/K is Galois, it is separable hence $B(v, w) := \mathrm{Tr}(vw)$ 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,

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

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

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

Thus $v = \sum_k \lambda_k \mathrm{Tr}(\mu_k v) \in \mathrm{Ext}(\mathrm{Tr}(Ev))$. $\square$

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

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

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

Proof. It is enough to show that $\mathrm{Res}(C) = \mathrm{Tr}(C)$ forces C to be Γ-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

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

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

Therefore $C = D \oplus Ev$. Now $\mathrm{Tr}(D) = \mathrm{Tr}(C) = \mathrm{Tr}(D) + \mathrm{Tr}(Ev)$, so $\mathrm{Tr}(Ev) \leqslant \mathrm{Tr}(D)$. By Lemma 8, $v \in \mathrm{Ext}(\mathrm{Tr}(Ev)) \leqslant \mathrm{Ext}(\mathrm{Tr}(D)) = D$ against $D \neq C$. $\square$

References

[1] J. Bierbrauer, The theory of cyclic codes and a generalization to additive codes, Des. Codes Cryptogr. 25 (2002) 189–206.
[2] J. Bierbrauer, Introduction to Coding Theory, Chapman and Hall, CRC Press, 2004.
[3] P. Delsarte, On subfield subcodes of modified Reed–Solomon codes, IEEE Trans. Inform. Theory IT-21 (5) (1975) 575–576.
[4] P. Morandi, Field and Galois Theory, Grad. Texts in Math., vol. 167, Springer-Verlag, New York, 1996.
[5] H. Stichtenoth, On the dimension of subfield subcodes, IEEE Trans. Inform. Theory 36 (1) (1990) 90–93.