On the action of the symmetric group on error-correcting codes

Lahcene Ladjelat

Abstract. In this paper we consider some of the consequences of the action of the symmetric group of degree n on the set of all block codes of length n over a finite field. After that we study how to compute a permutation between two equivalent codes, with respect to this action, using a non-fully discriminant signature under some conditions.

M.S.C. 2010: 94B05, 94B10, 94B12, 94B15.
Key words: Error block code; signature; the weight enumerator of a code; permutation group.

1 Introduction

This work deals with the action of the symmetric group of degree n on the set of all codes of length n over a finite field. This action defines an equivalence relation between two codes of length n, which is used to classify codes in equivalence classes. This equivalence relation takes linear code onto linear code and preserves length, cardinality, dimension, minimum distance and other parameters. The core of this work is concerned with establishing that under certain conditions the permutation between two codes can be computed. Here is a short guide to the contents of this paper. The second and third sections give a concise introduction of the Theory of error correcting codes and some consequences of the action of the symmetric group on the set of codes. The results quoted in this section are well-known and they are re-obtained by using properties of equivalence relations and bijections. In section 4 we recall the notion of signature due to N. Sendrier [5, 6] and establish that under certain conditions, when the signature is not fully discriminant, the permutation between two codes can be computed.

2 Generalities and notations

Let $\mathbb{F}_q$ be the finite field of q elements and n be a positive integer. We consider the n-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$ (The direct product $\mathbb{F}_q^n$ of n copies of $\mathbb{F}_q$). The elements of $\mathbb{F}_q^n$ will be called *words* or *vectors*. The Hamming distance $d(x, y)$

Applied Sciences, Vol.18, 2016, pp. 60-65.

between two words $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ...y_n)$ is the number of positions in which they differ. The weight of a word x is defined to be $d(x, (0, 0, ..., 0))$. A code C of length n over $\mathbb{F}_q$ is a nonempty subset of $\mathbb{F}_q^n$. Elements of a code are called *codewords*. C is called a linear code if it is a vector subspace of $\mathbb{F}_q^n$. The minimum distance of a code C is the number $d(C) = \min\{d(x, y) : x, y \in C \text{ and } x \neq y\}$. The weight enumerator of a code C is the polynomial $W_C(X) = \sum_{i=0}^{i=n} A_i X^i$, where A_i is the number of codewords of weight i.

3 The action of the symmetric group S_n

Let S_n be the symmetric group of degree n, that is the set of all permutations of the set $\{1, 2, 3, ..., n\}$ equipped with the operation of composition, and let $\mathcal{C}(n, q)$ denote the set of all codes of length n over $\mathbb{F}_q$. The group S_n acts on the set $\mathcal{C}(n, q)$ via the mapping

$$S_n \times \mathcal{C}(n, q) \to \mathcal{C}(n, q), \ (\sigma, C) \mapsto \sigma(C),$$

where $\sigma(C) = \left\{\sigma(x) = (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) \,|x = (x_1, x_2, ..., x_n) \in C\right\}$

Under these considerations, if $C \in \mathcal{C}(n, q)$, the orbit of C under S_n, denoted by $\mathcal{O}(C)$, is the set $\mathcal{O}(C) = \{\sigma(C) \,|\sigma \in S_n\}$.

Definition 3.1. Two codes C and D of the same length n are said to be equivalent if they belong to the same orbit. i.e. if there exists a permutation $\sigma \in S_n$ such that $\sigma(C) = D$.

Definition 3.2. The permutation group of a code C of length n, denoted by $Perm(C)$, is the subgroup of all the elements $\sigma \in S_n$ such that $\sigma(C) = C$.

Proposition 3.1. *Let C be a code of length n over $\mathbb{F}_q$. The number of equivalent codes to C is $\dfrac{n!}{|Perm(C)|}$.*

Proof. Denote by $S_n/Perm(C)$ the set of all left cosets of S_n with respect to $Perm(C)$. Let us consider the mapping

$f : \mathcal{O}(C) \longrightarrow S_n/Perm(C)$ defined by $\sigma(C) \mapsto \sigma Perm(C)$

f is one-to-one and onto, therefore the sets $\mathcal{O}(C)$ and $S_n/Perm(C)$ have the same cardinality $|\mathcal{O}(C)| = |S_n/Perm(C)| = \dfrac{n!}{|Perm(C)|}$. □

If the codes C and D are equivalents, what is the number of permutations $\sigma \in S_n$ such that $\sigma(C) = D$? The next Proposition gives the answer of this question.

Proposition 3.2. *Let C be a code of length n. The number of permutations in S_n that produce the same equivalent code to C is $|Perm(C)|$.*

Proof. On S_n let us define the equivalence relation : $\sigma \sim \pi$ if and only if $\sigma(C) = \pi(C)$

This means that the two permutations define the same equivalent code to C. Denote by $[\sigma]$ the equivalence class of σ modulo the relation $\sim$. Consider the mapping

$g : Perm(C) \longrightarrow [\sigma]$ defined by $\pi \longmapsto \sigma\pi^{-1}$. It is clear that g is one-to-one. It remains to show that it is also onto.

Let $\tau \in [\sigma]$, we have $\tau(C) = \sigma(C)$, which means that $\tau^{-1}\sigma(C) = C$, so $\tau^{-1}\sigma \in Perm(C)$. Finally $g(\tau^{-1}\sigma) = \sigma(\tau^{-1}\sigma)^{-1} = \sigma\sigma^{-1}\tau = \sigma$. As g is bijective we have $|[\sigma]| = |Perm(C)|$ which completes the proof. □

4 Determination of the equivalence of two codes

In this section we recall the notion of signature due to N. Sendrier and we study a case when the signature is not fully discriminant.

Let C be a code of length n and $J \subset \{1, 2, 3, ..., n\}$, then the code C *punctured* in J is the code C_J which consists of all elements $(x_1, x_2, ..., x_n) \in C$, where the coordinates x_i indexed by J are replaced by zeros. If $J = \{i\}$ we will write C_i instead of $C_{\{i\}}$. we can easily see that if $\sigma \in S_n$, then $\sigma(C_J) = \sigma(C)_{\sigma(J)}$.

As in section 3, let $\mathcal{C}(n, q)$ denote the set of all codes of length n over $\mathbb{F}_q$ and let $\mathcal{C}(q) = \bigcup_{n \geq 1} \mathcal{C}(n, q)$ to be the set of all codes over $\mathbb{F}_q$.

Definition 4.1. Let E be a nonempty set. An invariant over E is a mapping

$$\nu : \mathcal{C}(q) \longrightarrow E$$

such that for all $\sigma \in S_n$ and all $C \in \mathcal{C}(q)$ we have $\nu(\sigma(C)) = \nu(C)$.

For instance the length, the cardinality or the minimum distance are invariants over the integers. The weight enumerator is an invariant over the polynomials with integer coefficients.

Definition 4.2. Let E to be a nonempty set. A signature over E is a mapping

$$S : \mathcal{C}(q) \times \{1, 2, 3, ..., n\} \longrightarrow E$$

such that for all $\sigma \in S_n$ and all $(C, i) \in \mathcal{C}(q) \times \{1, 2, 3, ..., n\}$, the following equality holds $S(C, i) = S(\sigma(C), \sigma(i))$.

For instance, if ν is an invariant then $(C, i) \longrightarrow \nu(C_i)$ is a signature.

A signature S is said to be *fully discriminant for* C if for all i and j distinct in $\{1, 2, ..., 3\}$,we have $S(C, i) \neq S(C, j)$.

The question we address here is to compute the permutation $\sigma \in S_n$ which maps a given code C to an equivalent code $D = \sigma(C)$.

If $D = \sigma(C)$ and if S is fully discriminant for C, then σ will be unique and, for all $i \in \{1, 2, ..., n\}$, there exits a unique element $j \in \{1, 2, ..., n\}$ such that $S(C, i) = S(D, j)$, and we have $\sigma(i) = j$. We can thus obtain the permutation σ. In the remainder of this section we will restrict our attention to determine the permutation σ, where the signature is not fully discriminant in a particular case.

From now on, let C and D be two equivalent codes of length n such that $\sigma(C) = D$ for a permutation $\sigma \in S_n$. Let S to be a signature defined by

$$S(C, i) = \nu(C_i), \tag{4.1}$$

where ν is an invariant.

Suppose also that S satisfies the following condition:

There exist exactly s elements $i_1, i_2, ..., i_s \in \{1, 2, ..., n\}$, $2 \leq s \leq n-2$ such that:

$$\begin{cases} S(C, i_1) = S(C, i_2) = ... = S(C, i_s), \text{ and} \\ S(C, i) \neq S(C, j) \text{ if } i \neq j \text{ both in } \{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}. \end{cases} \tag{4.2}$$

Proposition 4.1. *If the condition* (4.2) *holds for a signature S, then the set $\{i_1, i_2, ..., i_s\}$ is stable under the action of $Perm(C)$ the permutation group of C.*

Proof. For a permutation $\sigma \in Perm(C)$ and an element $i_k \in \{i_1, i_2, ..., i_s\}$, we have $S(\sigma(C), \sigma(i_k)) = S(C, i_k)$ because S is a signature, and we have $S(\sigma(C), \sigma(i_k)) = S(C, \sigma(i_k))$ because $\sigma \in Perm(C)$, from the two equations above, we see that $S(C, \sigma(i_k)) = S(C, i_k)$. Because of the condition (4.2), we conclude that $\sigma(i_k) \in \{i_1, i_2, ..., i_s\}$ which means that the set $\{i_1, i_2, ..., i_s\}$ is stable under the action of $Perm(C)$. □

Proposition 4.2. *If $D = \sigma(C)$ and the condition* (4.2) *holds for the triple $(S, C, \{i_1, i_2, ..., i_s\})$, then it also holds for the triple $(S, D, \{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\})$.*

Proof. If $\sigma(i_k)$ and $\sigma(i_l)$ are distinct, then

$$\begin{aligned} S(D, \sigma(i_k)) &= S(\sigma(C), \sigma(i_k)) && \text{by definition of } D \\ &= S(C, i_k) && S \text{ is a signature} \\ &= S(C, i_l) && \text{from condition (4.2)} \\ &= S(\sigma(C), \sigma(i_l)) && \text{since } S \text{ is a signature} \\ &= S(D, \sigma(i_l)) && \text{by the definition of } D. \end{aligned}$$

If i and j are distinct in$\{1, 2, ..., n\} \setminus \{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$, then there exist a and b distinct in $\{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}$ such that $\sigma(a) = i$ and $\sigma(b) = j$. By (4.2), we have $S(D, i) = S(\sigma(C), \sigma(a)) = S(C, a) \neq S(C, b) = S(\sigma(C), \sigma(b)) = S(D, j)$. □

Under the considerations of Proposition 4.2, we give below how to compute the permutation σ, i.e. to compute $\sigma(e)$ for all $e \in \{1, 2, ..., n\}$.

Because $D = \sigma(C)$ we have

$$\{S(C, e) : e \in \{1, 2, ..., n\}\} = \{S(D, t) : t \in \{1, 2, ..., n\}\} \tag{4.3}$$

Let i be an element in $\{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}$. from the equality (4.3) we can find an element $j \in \{1, 2, ..., n\} \setminus \{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$ such that $S(\sigma(C), \sigma(i)) = S(C, i) = S(D, j)$. Therefore $\sigma(i) = j$.

Now fix i in $\{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_s\}$ with $\sigma(i) = j$ as above. In order to compute $\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)$ we define the mapping

$$\Phi_C : \{i_1, i_2, ..., i_s\} \longrightarrow E \text{ by } \Phi_C(\alpha) = \nu(C_{\{i,\alpha\}}),$$

where ν is the invariant over E defined by the condition (4.1) and $C_{\{i,\alpha\}}$ is the code C punctured in the positions i and α.

Proposition 4.3. *Under the conditions of Proposition 4.2, if the mapping Φ_C is injective, then the images $\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)$ are completely determined.*

Proof. First we can see that is easy to show that the mapping Φ_D, defined for D and $j = \sigma(i)$ in the same way as Φ_C, is also injective if Φ_C it is. Because $D = \sigma(C)$ we have the equality

$$\Phi_C\{i_1, i_2, ..., i_s\} = \Phi_D\{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\},$$

so for an arbitrary element $\alpha \in \{i_1, i_2, ..., i_s\}$, there exists some element β in $\{\sigma(i_1), \sigma(i_2), ..., \sigma(i_s)\}$ such that $\Phi_C(\alpha) = \Phi_D(\beta)$, and because

$$\Phi_C(\alpha) = \nu(C_{\{i,\alpha\}}) = \nu(\sigma(C)_{\sigma(\{i,\alpha\})}) = \nu(D_{\{j,\sigma(\alpha)\}}) = \Phi_D(\sigma(\alpha))$$

we have $\Phi_D(\sigma(\alpha)) = \Phi_D(\beta)$.And therefore we obtain $\sigma(\alpha) = \beta$. □

Example 4.3. We consider, over $\mathbb{F}_2$, the codes

$$C = \{10010, 10100, 10001, 01010, 00001\} \quad \text{and} \quad D = \{01001, 00101, 10001, 01010, 10000\}$$

and as invariant we will take the weight enumerator polynomial. We get for C,

$$\begin{cases} C_1 = \{00010, 00100, 00001, 01010\} \\ C_2 = \{10010, 10100, 10001, 00010, 00001\} \\ C_3 = \{10010, 10000, 10001, 01010, 00001\} \\ C_4 = \{10000, 10100, 10001, 01000, 00001\} \\ C_5 = \{10010, 10100, 10000, 01010, 00000\} \end{cases}, \text{ and } \begin{cases} S(C,1) = W_{C_1}(X) = 3X + X^2 \\ S(C,2) = W_{C_2}(X) = 2X + 3X^2 \\ S(C,3) = W_{C_3}(X) = 2X + 3X^2 \\ S(C,4) = W_{C_4}(X) = 3X + 2X^2 \\ S(C,5) = W_{C_5}(X) = 1 + X + 3X^2. \end{cases}$$

For this example, we have $s = 2$, and $\{i_1, i_2\} = \{2, 3\}$. Now for D we get in the same way,

$$\begin{cases} D_1 = \{01001, 00101, 00001, 01010, 00000\} \\ D_2 = \{00001, 00101, 10001, 00010, 10000\} \\ D_3 = \{01001, 00001, 10001, 01010, 10000\} \\ D_4 = \{01001, 00101, 10001, 01000, 10000\} \\ D_5 = \{01000, 00100, 10000, 01010\} \end{cases}, \text{ and } \begin{cases} S(D,1) = W_{D_1}(X) = 1 + X + 3X^2 \\ S(D,2) = W_{D_2}(X) = 3X + 2X^2 \\ S(D,3) = W_{D_3}(X) = 2X + 3X^2 \\ S(D,4) = W_{D_4}(X) = 2X + 3X^2 \\ S(D,5) = W_{D_5}(X) = 3X + X^2, \end{cases}$$

so we have $\sigma\{i_1, i_2\} = \sigma\{2, 3\} = \{3, 4\}$. The system of equalities

$$\begin{cases} S(C,1) = S(D,5) \\ S(C,4) = S(D,2) \\ S(C,5) = S(D,1) \end{cases}$$

gives $\sigma(1) = 5$, $\sigma(4) = 2$ and $\sigma(5) = 1$. If we choose $i = 5$ (then $j = 1$), we shall obtain

$$\begin{cases} \Phi_C(2) = W_{C_{\{5,2\}}} = 1 + 2X + 2X^2 \\ \Phi_C(3) = W_{C_{\{5,3\}}} = 1 + X + 2X^2 \\ \Phi_D(3) = W_{D_{\{1,3\}}} = 1 + X + 2X^2 \\ \Phi_D(4) = W_{D_{\{1,4\}}} = 1 + 2X + 2X^2. \end{cases}$$

The mappings Φ_C and Φ_D are injective, and therefore we get $\sigma(2) = 4$ and $\sigma(3) = 3$. Thus the permutation is $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$.

5 Conclusions

The purpose of this paper was to study some of the consequences of the action of the symmetric group of degree n on the set of all block codes of length n over a finite field, and how to compute a permutation between two equivalent codes, with respect to this action, using a non-fully discriminant signature under some conditions.

References

[1] A. Bouvier, D. Richard, *Groupes: observation, théorie, pratique* (2-nd. ed.), Hermann 1979.

[2] L.J. Goldstein, *Abstract Algebra: a first course*, Prentice Hall Inc., Englewood Cliffs, New Jersy 1973.

[3] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland 1977.

[4] E. Petrank, R.M. Roth, *Is code equivalence easy to decide?* IEEE transactions on Information Theory, 43,5(1997), 1602-1604.

[5] N. Sendrier, *The Support Splitting Algorithm*, Research Report 3637, INRIA-Rocquencourt, March 1999.

[6] N. Sendrier, *Un algorithme pour trouver la permutation entre deux codes binaires équivalents*, Mémoire d'habilitation à diriger des recherches, INRIA-Rocquencourt, March 2002.

Author's address:

Lahcene Ladjelat
University of M'Sila 28000, Department of Mathematics,
P.O.Box 166, Ichbilia 28105 M'Sila, Algeria.
E-mail: ladjelat_lahcene@yahoo.fr