

# Automorphism group of a code

---

## 10.1 AUTOMORPHISM GROUP OF A BINARY CODE

Let  $\mathcal{C}$  be a binary code of length  $n$ . If  $\sigma$  is a permutation of the set  $S = \{1, 2, \dots, n\}$ , then  $\mathcal{C}' = \{\sigma(c) | c \in \mathcal{C}\}$  is a code equivalent to  $\mathcal{C}$ . If, however,  $\mathcal{C}' = \mathcal{C}$  then  $\sigma$  is called an **automorphism** of the code  $\mathcal{C}$ . Let  $\text{Aut}(\mathcal{C})$  denote the set of all automorphisms of  $\mathcal{C}$ . Observe that if  $\sigma, \tau$  are in  $\text{Aut}(\mathcal{C})$ , then so is  $\sigma\tau$ . The set  $S_n$  of all permutations of  $S$  being a finite group, it follows that  $\text{Aut}(\mathcal{C})$  is a subgroup of  $S_n$ .

### Definition 10.1

The subgroup  $\text{Aut}(\mathcal{C})$  of  $S_n$  is called the **automorphism group** of the code  $\mathcal{C}$ .

### Remark 10.1

To every permutation  $\sigma$  of  $S$  corresponds a permutation matrix  $\mathbf{P}$  of order  $n$  such that  $\sigma(\mathbf{c}) = \mathbf{cP}$  for  $\mathbf{c}$ , the vector associated with  $c \in \mathcal{C}$  and conversely. Writing  $(\mathbf{c})\sigma$  for  $\sigma(\mathbf{c})$ , we find that the map  $\sigma \rightarrow \mathbf{P}$  gives an isomorphism between the symmetric group  $S_n$  of degree  $n$  and the group of all permutation matrices of order  $n$ . We may thus have (up to isomorphism)

$$\text{Aut}(\mathcal{C}) = \{\mathbf{P} | \mathbf{P} \text{ is a permutation matrix of order } n \text{ with } \mathbf{cP} \in \mathcal{C} \forall c \in \mathcal{C}\}$$

It is, in general, not easy to determine the automorphism group of a code. We consider some examples.

**Examples 10.1****Case (i)**

Consider first the repetition code

$$\mathcal{C} = \{00 \cdots 0 \quad 11 \cdots 1\}$$

of length  $n$ . Every transposition  $(1 \ i) \in \text{Aut}(\mathcal{C})$  and, so,

$$\text{Aut}(\mathcal{C}) = S_n$$

**Case (ii)**

Let  $\mathcal{C}$  be the  $(n, n+1)$  parity check code. Then  $\mathcal{C}$  is obtained from the set of all words of length  $n$  by adding an overall parity check.  $\mathcal{C}$  is then a linear code of dimension  $n$  with a basis consisting of the  $n$  elements  $c_1 c_2 \cdots c_{n+1}$  of weight 2 with  $c_{n+1} = 1$ . The transpositions

$$(1 \ 2), (1 \ 3), \dots, (1 \ n)$$

leave the basis elements of  $\mathcal{C}$  unchanged and are, therefore, in  $\text{Aut}(\mathcal{C})$ . Let

$$c = c_1 c_2 \cdots c_n c_{n+1} \in \mathcal{C}$$

Then

$$c_{n+1} = \sum_{i=1}^n c_i$$

Applying the transposition  $\sigma = (1, n+1)$  to  $\mathbf{c}$ , gives

$$\sigma(\mathbf{c}) = (c_{n+1} \ c_2 \ \cdots \ c_n c_1)$$

and

$$c_{n+1} = \sum_{i=1}^n c_i$$

shows that

$$c_i = \sum_{i=2}^{n+1} c_i$$

Thus  $\sigma(\mathbf{c}) \in \mathcal{C}$ . Therefore

$$(1, n+1) \in \text{Aut}(\mathcal{C})$$

As the transpositions

$$(12), \dots, (1 \ n+1)$$

generate the symmetric group  $S_{n+1}$  of degree  $n+1$ , we have

$$\text{Aut}(\mathcal{C}) = S_{n+1}$$

**Case (iii)**

Let  $\mathcal{C}$  be the code of length 4 generated by 1011, 1001. Then

$$\mathcal{C} = \{0000, 1011, 1001, 0010\}$$

Clearly

$$(1\ 4) \in \text{Aut}(\mathcal{C})$$

but none of  $(1\ 2), (1\ 3), (2\ 3), (2\ 4), (3\ 4)$  is in  $\text{Aut}(\mathcal{C})$ . But then none of

$$(1\ 2\ 4) = (1\ 4)(1\ 2)$$

$$(1\ 3\ 4) = (1\ 4)(1\ 3)$$

$(1\ 4)(2\ 3)$  is in  $\text{Aut}(\mathcal{C})$ . It is also clear that  $(1\ 2\ 3), (2\ 3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4)$  do not belong to  $\text{Aut}(\mathcal{C})$ . A simple observation of the elements of  $\mathcal{C}$  shows that none of the cycles of length 4 is in  $\text{Aut}(\mathcal{C})$ . Hence

$$\text{Aut}(\mathcal{C}) = \{1, (1\ 4)\}$$

**Case (iv)**

Let

$$\mathcal{C} = \{0000, 1011, 1001, 0010, 1100, 0111, 0101, 1110\}$$

Clearly

$$(1\ 2), (1\ 4), (2\ 4) \in \text{Aut}(\mathcal{C})$$

but

$$(1\ 3), (2\ 3), (3\ 4) \notin \text{Aut}(\mathcal{C})$$

Then

$$(1\ 2\ 3) = (1\ 3)(1\ 2)$$

$$(1\ 3\ 4) = (1\ 4)(1\ 3)$$

$$(2\ 3\ 4) = (2\ 4)(2\ 3)$$

$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$  cannot be in  $\text{Aut}(\mathcal{C})$ .

Since any cycle of length 4 is a product of the three transpositions  $(1\ 2), (1\ 3), (1\ 4)$  in some order two of which are in  $\text{Aut}(\mathcal{C})$  but one is not, it follows that none of these four cycles is in  $\text{Aut}(\mathcal{C})$ . Hence

$$\text{Aut}(\mathcal{C}) = \{1, (1\ 2), (1\ 4), (2\ 4), (1\ 2\ 4), (1\ 4\ 2)\}$$

**Case (v)**

Let  $\mathcal{C}$  be a linear code and  $\mathcal{C}_1$  be a code obtained from  $\mathcal{C}$  by adding an overall parity check. Any element of  $\mathcal{C}_1$  is of the form

$$c' = (c, c_{n+1})$$

where  $c \in \mathcal{C}$  and

$$c_{n+1} = \sum_{i=1}^n c_i$$

If

$$\sigma \in \text{Aut}(\mathcal{C}) \quad \text{as } c_{n+1} = \sum c_i = \sum c_{\sigma(i)}$$

then

$$(\sigma(c), c_{n+1}) \in \mathcal{C}_1$$

Thus  $\sigma \in \text{Aut}(\mathcal{C}_1)$  and, so,  $\text{Aut}(\mathcal{C}) \leq \text{Aut}(\mathcal{C}_1)$ .

### Remark 10.2

Let  $\mathcal{C}$  be a linear code of length  $n$ ,  $\{c^1, c^2, \dots, c^k\}$  a set of linearly independent elements and  $\sigma$  a permutation of the set  $\{1, 2, \dots, n\}$ . Then the elements

$$\sigma(c^1), \sigma(c^2), \dots, \sigma(c^k)$$

are again linearly independent. Thus if  $\mathcal{C}$  is a linear code of dimension  $k$  then

$$\sigma(\mathcal{C}) = \{\sigma(c) | c \in \mathcal{C}\}$$

is again a linear code of dimension  $k$ . In particular, if  $\sigma \in \text{Aut}(\mathcal{C})$ , then  $\sigma(\mathcal{C}) = \mathcal{C}$ .

### Proposition 10.1

If  $\mathcal{C}$  is a linear code, then

$$\text{Aut}(\mathcal{C}) = \text{Aut}(\mathcal{C}^\perp)$$

### Proof

Let  $\sigma \in \text{Aut}(\mathcal{C})$ . For  $c' \in \mathcal{C}^\perp$ ,  $\mathbf{c}(\mathbf{c}')^t = 0 \forall c$  in  $\mathcal{C}$  (here  $\mathbf{a}^t$  denotes the transpose of the row vector  $\mathbf{a}$  and  $\mathbf{c}$  is the vector formed from the elements of the code word  $c$ ) which then implies that

$$\sigma(\mathbf{c})\sigma(\mathbf{c}')^t = 0 \forall c \in \mathcal{C}$$

As  $\sigma(\mathcal{C}) = \mathcal{C}$ , it follows that  $\mathbf{c}\sigma(\mathbf{c}')^t = 0 \forall c \in \mathcal{C}$ . Thus  $\sigma(c') \in \mathcal{C}^\perp$  and, so,  $\sigma \in \text{Aut}(\mathcal{C}^\perp)$ . Hence

$$\text{Aut}(\mathcal{C}) \leq \text{Aut}(\mathcal{C}^\perp)$$

This then implies that ( $\mathcal{C}^\perp$  being a linear code)

$$\text{Aut}(\mathcal{C}^\perp) \leq \text{Aut}((\mathcal{C}^\perp)^\perp) = \text{Aut}(\mathcal{C}) \quad \blacksquare$$

The above result is not true for non-linear codes.

### Examples 10.2

#### Case (i)

Let

$$\mathcal{C} = \{000, 100, 010, 001, 110, 111\}$$

It is clear that

$$\text{Aut}(\mathcal{C}) = \{1, (1 \ 2)\}$$

Also  $\mathcal{C}^\perp = \{000\}$  and  $\text{Aut}(\mathcal{C}^\perp) = S_3$  – the symmetric group of degree 3.

**Case (ii)**

Let

$$\mathcal{C} = \{000, 110, 111, 101, 010\}$$

Clearly  $\text{Aut}(\mathcal{C}) = 1$ . Now,  $\mathcal{C}^\perp = \{000\}$  and so  $\text{Aut}(\mathcal{C}^\perp) = S_3$  – the symmetric group of degree 3.

Incidentally, we have also given an example of a code the automorphism group of which is trivial.

**Case (iii)**

The code

$$\mathcal{C} = \{000, 100, 010, 001, 110\}$$

is a non-linear code and  $(1 \ 2) \in \text{Aut}(\mathcal{C})$  while  $(1 \ 3), (2 \ 3)$  are not in  $\text{Aut}(\mathcal{C})$ . Therefore

$$\text{Aut}(\mathcal{C}) = \{1, (1 \ 2)\}$$

is a group of order 2.

**Proposition 10.2**

Let  $\mathcal{C}$  be a linear code and  $\mathcal{C}_1$  be obtained from  $\mathcal{C}$  by adding the all one vector  $\mathbf{1}$ . Then

$$\text{Aut}(\mathcal{C}) \leq \text{Aut}(\mathcal{C}_1)$$

while equality holds if  $\mathcal{C}$  is of odd length and the code words have only even weights.

**Proof**

We need to consider only the case when  $\mathbf{1} \notin \mathcal{C}$ . Then

$$\mathcal{C}_1 = \mathcal{C} \cup \{\mathbf{c} + \mathbf{1} \mid \mathbf{c} \in \mathcal{C}\}$$

As

$$\sigma(\mathbf{c} + \mathbf{1}) = \sigma(\mathbf{c}) + \mathbf{1} \in \mathcal{C}_1 \quad \forall \sigma \in \text{Aut}(\mathcal{C})$$

we have  $\text{Aut}(\mathcal{C}) \leq \text{Aut}(\mathcal{C}_1)$ .

Now suppose that  $\mathcal{C}$  is of odd length and its words have only even weights. Then every word of the form  $\mathbf{c} + \mathbf{1}$ ,  $\mathbf{c} \in \mathcal{C}$ , has odd weight. For any  $\sigma \in \text{Aut}(\mathcal{C}_1)$  and  $\mathbf{c} \in \mathcal{C}$ ,  $\sigma(\mathbf{c})$  is in  $\mathcal{C}_1$  having even weight and, so,  $\sigma(\mathbf{c}) \in \mathcal{C}$ . Thus  $\text{Aut}(\mathcal{C}_1) \leq \text{Aut}(\mathcal{C})$ .

**The automorphism group of a cyclic code**

The automorphism group of a cyclic code contains all cycles of length  $n$  (i.e. cyclic permutations of the set  $\{1, 2, \dots, n\}$ ) and their powers.

Now  $n$  being odd, there exist integers  $r$  and  $s$  such that

$$1 \equiv 2r + ns$$

Then, with  $I = \langle X^n - 1 \rangle$  the ideal of  $\mathbb{B}[X]$  generated by  $X^n - 1$

$$\begin{aligned} X + I &= X^{2r} \cdot X^{ns} + I \\ &= X^{2r} + I \end{aligned}$$

as  $X^{ns} - 1 \in I$ . If  $r < 0$ , let  $t$  be the least positive integer such that

$$2r + 2nt > 0$$

Then

$$X^{2r} + I = X^{2(r+nt)} + I$$

Thus

$$\sigma_2: \{1 + I, X + I, \dots, X^{n-1} + I\} \rightarrow \{1 + I, X + I, \dots, X^{n-1} + I\}$$

given by

$$\sigma_2(X + I) = X^2 + I$$

is an onto map and hence a permutation. For any polynomial  $a(X) \in \mathbb{B}[X]$  of degree at most  $n - 1$

$$\sigma_2(a(X) + I) = a(X^2) + I = (a(X) + I)^2$$

so that whenever  $a(X) + I$  is in a cyclic code  $\mathcal{C}$  of length  $n$  (i.e. an ideal of  $\mathbb{B}[X]/I$ ), then so is  $\sigma_2(a(X) + I)$ . Therefore,  $\sigma_2$  is in  $\text{Aut}(\mathcal{C})$ . Clearly, the order of the permutation  $\sigma_2$  is the number of elements in the cyclotomic coset  $C_1$  modulo  $n$  relative to 2 determined by 1.

**Examples 10.3****Case (i)**

Let  $\mathcal{C} = \langle X + 1 + I \rangle$ , where  $I = \langle X^3 - 1 \rangle$ , be the cyclic code of length 3 generated by  $1 + X$ . Here the cyclotomic coset  $C_1 = \{1, 2\}$  and  $\sigma_2$  is a transposition. Therefore,

$$\text{Aut}(\mathcal{C}) \geq \{1, \sigma_2, (1 \ 2 \ 3), (1 \ 3 \ 2)\}$$

and so it is  $S_3$ —the symmetric group of degree 3.

Alternatively, observe that

$$\mathcal{C} = \{000, 110, 011, 101\}$$

and it is clear that the transpositions  $(1\ 2), (1\ 3)$  which generate  $S_3$  are in  $\text{Aut}(\mathcal{C})$  and, therefore,  $\text{Aut}(\mathcal{C}) = S_3$ .

**Case (ii)**

The cyclic code of length 5 generated by  $1 + X$  is

$$\begin{aligned}\mathcal{C} &= \{(a_0, a_0 + a_1, a_1 + a_2, a_2 + a_3, a_3) \mid a_i \in \mathbb{B}\} \\ &= \{00000, 11000, 01100, 00110, 00011, 10100, 11110, \\ &\quad 11011, 01111, 01010, 00101, 10010, 10111, 11101, \\ &\quad 01001, 10001\}\end{aligned}$$

The permutation  $\sigma_2$  maps

$$1 \rightarrow 1, X \rightarrow X^2, X^2 \rightarrow X^4, X^3 \rightarrow X, X^4 \rightarrow X^3$$

and so

$$\sigma_2 = (2\ 3\ 5\ 4)$$

which is a cycle of length 4.

However, a simple observation shows that

$$(1\ 2), (1\ 3), (1\ 4), (1\ 5) \in \text{Aut}(\mathcal{C})$$

and, therefore,  $\text{Aut}(\mathcal{C}) = S_5$ .

**Exercise 10.1**

Determine the automorphism group of the  $(4, 7)$  binary Hamming code.

## 10.2 AUTOMORPHISM GROUP OF A NON-BINARY CODE

**Definition 10.2**

A **monomial matrix** over a field  $F$  is a square matrix with exactly one non-zero entry in every row and in every column.

For example

$$\begin{pmatrix} 0 & 2 & 0 \\ 3 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is a monomial matrix of order 3 while

$$\begin{pmatrix} 0 & 2 & 0 \\ 3 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

is not a monomial matrix.