

# A NEW CLASS OF ISODUAL CYCLIC CODES OF RATE 1/2 OVER $\mathbb{F}_p$

CHERIF MIHOUBI, PATRICK SOLÉ

**ABSTRACT.** A new class of isodual cyclic codes of parameters  $[n, k]_p$ , is found for  $n$  singly even, not a multiple of  $p$ .

**Mathematics Subject Classification (2010):** 94B15, 94B05, 94B60, 12E20.

**Keywords:** cyclic codes, generator polynomial, isodual codes.

*Article history:*

Received 28 February 2016

Received in revised form 14 April 2016

Accepted 16 April 2016

## 1. INTRODUCTION

In the present work, we consider cyclic codes over  $\mathbb{F}_p$  of rate 1/2, where  $p$  is a prime number. An important subclass of these is that of isodual codes, i.e. codes equivalent to their duals. We propose, in the cases:  $n = 2m$ , with  $m$  odd, a construction of isodual cyclic codes.

Recently a new results on the optimization of the minimum distance of cyclic codes of rate 1/2 over  $\mathbb{F}_3$  and the characterization of generating polynomial of an isodual cyclic code over  $\mathbb{F}_3$  and  $\mathbb{F}_5$  are presented in [6] and [7]. Generally the characterization of the generating polynomial of an isodual cyclic code is left as a challenging open problem.

## 2. ISODUAL CYCLIC CODES OF RATE 1/2 OVER $\mathbb{F}_p$

Some familiarity with coding theory is in [5], [8]. Let  $\mathbb{F}_p$  denote the Galois field of  $p$  elements. Recall that the rate of a linear code of length  $n$  and dimension  $k$  is  $k/n$ . Two linear codes are said to be equivalent if one can be obtained from the other by permutation of coordinates. A linear code is said to be isodual if and only if it is equivalent to its dual. Recall that a cyclic code of length  $n$  over  $\mathbb{F}_p$  can be regarded as an ideal in the principal ideal ring  $F_p[X]/(X^n - 1)$ . If  $g(X)$  denote the generator polynomial of a cyclic code  $C$ , then the generator of the dual code, denoted by  $h(X)$  is, up to sign, the reciprocal of its complement

$$h(X) = \frac{X^n - 1}{g(X)},$$

where the reciprocal polynomial  $f^*(X)$  of a polynomial  $f(X)$ , of degree  $n$  over  $F_p$ , is defined by

$$f^*(X) = X^n f\left(\frac{1}{X}\right).$$

The parameters of a  $p$ -ary code are denoted by  $[n, k]_p$  and are length and dimension. The algorithm to compute the minimum distance of a cyclic codes is in [9] and some optimal linear codes of rate  $1/2$  over  $\mathbb{F}_5$  and  $\mathbb{F}_7$  are described in [3]. In [2] the online table of self-dual codes over  $\mathbb{F}_7$  is maintained.

### 3. SPECIAL CLASS OF ISODUAL CYCLIC CODES OF PARAMETERS $[n, \frac{n}{2}]_p$

For  $m$  a positive integer consider the cyclotomic polynomial

$$\Phi_m(X) := \prod_{\substack{1 \leq k \leq m \\ (k, m)=1}} (X - e^{2\pi i k/m}).$$

Thus the first five cyclotomic polynomials are

$$\Phi_1(X) = X - 1, \Phi_2(X) = X + 1, \Phi_3(X) = X^2 + X + 1, \Phi_4(X) = X^2 + 1,$$

$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1.$$

If  $p$  is a prime, then

$$(3.1) \quad \Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1,$$

and, if  $m$  is an odd number, then

$$(3.2) \quad \Phi_{2m}(X) = \Phi_m(-X).$$

Hence,

$$(3.3) \quad X^m - 1 = \prod_{d/m} \Phi_d(X).$$

Since  $\Phi_m(X) \in \mathbb{Z}[X]$  (see, for example, N. Jacobson [4] or K. Conrad [1]), for a fixed prime  $p$ , they can reduce them modulo  $p$ . It is known the following result:

**Theorem 3.1.** ([1], [4]) *Let  $p$  be a fixed prime. Then  $\Phi_m(X)$  is irreducible in  $\mathbb{F}_p[X]$  if and only if  $m$  is not a multiple of  $p$ , and  $p \pmod{m}$  is a generator of the multiplicative group of  $\mathbb{Z}_m$ .*

If  $p$  is a fixed prime we begin our study of cyclic codes of parameters  $[n, \frac{n}{2}]$ ,  $n$  singly even, and not a multiple of  $p$ . the following theorem is the main result of the paper.

**Theorem 3.2.** *If  $p, m$  be two distinct odd primes such that  $p \pmod{m}$  is a generator of the multiplicative group of  $\mathbb{Z}_m$  and  $n = 2m$ , then a cyclic code of parameters  $[n, \frac{n}{2}]$  is isodual.*

*Proof.* Let  $C$  be a cyclic code of parameters  $[n, \frac{n}{2}]$  having the generator polynomial denoted by  $g(X)$ . Since by (3.1)-(3.3),

$$X^n - 1 = \Phi_1(X)\Phi_2(X)\Phi_m(X)\Phi_{2m}(X)$$

$$= (X - 1)(X + 1)(X^{m-1} + X^{m-2} + \dots + X + 1)(X^{m-1} - X^{m-2} + \dots - X + 1),$$

and, by Theorem 3.1,  $\Phi_m(X)$  and  $\Phi_m(-X)$  are irreducible in  $\mathbb{F}_p[X]$ , it follows that there are only 4 choice for  $g(X)$  of degree  $\frac{n}{2}$ :

$$\begin{aligned} g(X) &= (X - 1)\Phi_m(X), \\ g(X) &= (X - 1)\Phi_{2m}(X), \\ g(X) &= (X + 1)\Phi_m(X), \\ g(X) &= (X + 1)\Phi_{2m}(X), \end{aligned}$$

where

$$\Phi_m(X) = X^{m-1} + X^{m-2} + \dots + X + 1,$$

and we have always

$$\Phi_m^*(X) = \Phi_m(X).$$

We compute the generator of the dual code. First we have respectively

$$\begin{aligned} (X^n - 1)/g(X) &= (X + 1)\Phi_{2m}(X), \\ (X^n - 1)/g(X) &= (X + 1)\Phi_m(X), \\ (X^n - 1)/g(X) &= (X - 1)\Phi_{2m}(X), \\ (X^n - 1)/g(X) &= (X - 1)\Phi_m(X). \end{aligned}$$

Taking reciprocal of both sides, we obtain

$$\left( \frac{X^n - 1}{g(X)} \right)^* = \pm g(-X).$$

Since the map  $g(X) \mapsto \pm g(-X)$  is an isometry, we see that the cyclic code of generator  $g(X)$  and its dual are equivalent codes.  $\square$

**Example 3.3.** If  $p = 3$ , for  $n = 34, 38, 58, 62$ , the cyclic codes of parameters  $[n, \frac{n}{2}]$  are isodual (see [7], Proposition 3).

**Example 3.4.** If  $p = 5$ , for  $n = 22, 38$ , the cyclic codes of rate  $\frac{1}{2}$  are isodual (see [6], Proposition 2.1 and 2.3)

**Example 3.5.** If  $p = 7$ , then the following table gives several examples of isodual cyclic codes.

$m$	$p \pmod{m}$	order of $p \pmod{m}$	$n$	type of code
11	7	10	22	isodual
13	7	12	26	isodual
17	7	16	34	isodual
19	7	18	38	isodual
23	7	22	46	isodual
29	7	28	58	isodual
31	7	30	62	isodual
37	7	36	74	isodual
41	7	40	82	isodual
43	7	42	86	isodual

**Remark 3.6.** Using the algorithm in [9], it can be shown that the largest minimum distance of the all codes of parameters  $[n, \frac{n}{2}]_7$  is equal to 4.

#### 4. CONCLUSION

In this work, following the lead of [6] and [7] we have studied isodual cyclic codes over the field  $\mathbb{F}_p$  and have provided a simple construction valid for all lengths  $n$  of the form twice an odd number  $m$ . The value of the minimum distance of these codes has been determined for such  $n$  not a multiple of  $p$ . It is possible that other constructions or other lengths yield larger minimum distances.

**Acknowledgement.** The authors would like to thank the referee for his suggestions which improve the original manuscript.

#### REFERENCES

- [1] K. Conrad, *Cyclotomic extension*, <http://www.math.uconn.edu/kconrad/math5211s13/handouts/cyclotomic.pdf>.
- [2] P. Gaborit, *Table of Self-Dual Codes over GF(7)*, [tables; online], [http://www.unilim.fr/pages\\_perso/philippe.gaborit/SD/GF7.htm](http://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF7.htm).
- [3] T. A. Gulliver, P. R. J. Ostergard and N. Senkevitch, Optimal linear rate 1/2 codes over  $\mathbb{F}_5$  and  $\mathbb{F}_7$ , *Discrete Math.* **265** (2003), 59-70.
- [4] N. Jacobson, *Lectures in abstract algebra*, vol. III, D. Van Nostrand Company, Inc. Princeton, 1964.
- [5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
- [6] C. Mihoubi, Isodual Cyclic Codes of rate  $\frac{1}{2}$  over  $GF(5)$ , *Int. J. Open Problems Comp. Math.* **4** (2011), 33-39.
- [7] C. Mihoubi and P. Solé, Optimal and Isodual Ternary Cyclic Codes of rate  $\frac{1}{2}$ , *Bull. Math. Sci.*, **2** (2012), 343-357.
- [8] E. M. Rains and N. J. A. Sloane, *Self-dual codes, Handbook of Coding Theory*, in V. S. Pless and W. C. Huffman (eds), Elsevier, Amsterdam, 1998.
- [9] J. F. Voloch, Computing the minimal distance of cyclic codes, *Comp. and Appl. Math.*, **24** (2005), 393-398.

DÉPARTEMENT DE MATHÉMATIQUES, UNIVERSITÉ MED BOUDIAF DE M'SILA, BP 581 HODNA  
M'SILA 28000, ALGÉRIE

*E-mail address:* `cherif.mihoubi@yahoo.fr`

TÉLÉCOM PARISTECH, DÉPT COMELEC, 46 RUE BARRAULT 75013 PARIS, FRANCE

*E-mail address:* `sole@telecom-paristech.fr`