Int. J. Open Problems Compt. Math., Vol. 4, No. 4, December 2011
ISSN 1998-6262; Copyright ©ICSRS Publication, 2011
www.i-csrs.org

Isodual Cyclic Codes of rate 1/2 over GF(5)

Cherif Mihoubi

Département de Mathématiques,
(a) Université Hadj Lakhdar Batna 5000, Algérie.
(b) Université de M'sila 28000, M'sila Algérie.
e-mail: cherif.mihoubi@yahoo.fr

Abstract

A new classes of isodual cyclic codes of parameters $[n, k]_5$***, are found for*** n ***singly even, not a multiple of*** 5***.***

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

1 Introduction

In the present work, we consider cyclic codes over F_5 of rate 1/2. An important subclass of these is that of isodual codes, i.e. codes equivalent to their duals. We propose, in the case $n = 2m$ with m odd, three constructions of isodual cyclic codes over F_5. The characterization of the generating polynomial of an isodual cyclic code is left as a challenging open problem.

2 Cyclic codes of rate $1/2$ over $\mathbf{F}_5$

Some familiarity with coding theory is in [6,7]. Let F_5 denote the Galois field of five 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** iff it is equivalent to its dual. Recall that a cyclic code of length n over F_5 can be regarded as an ideal in the principal ideal ring $F_5[x]/(x^n - 1)$. 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_5, is defined by

$$f^*(x) = x^n f(\frac{1}{x})$$

The parameters of a $5-$ary code are denoted by $[n, k]_5$ and are length and dimension. In recent last years, good linear codes over $GF(5)$ were constructed. In [3] a new minimum distance bounds for linear codes over $GF(5)$ are discovered. Crassl and White presents 55 new codes in [1]. The classification of all optimal linear codes $[n, n/2]$ over $GF(5)$ and $GF(7)$ is presented in [5] respectively to the length 12 and 8. Crassl maintains an electronic table(online) on upper and lower bounds of the minimum distance of linear codes in [2]. P. Gaborit, presents a table of self-dual codes over $GF(5)$, [tables; online] in [4]. The algorithm to compute the minimum distance of a cyclic codes is in [8].

2.1 Cyclic Codes of parameters $[22, 11]_5$

We begin our study of cyclic codes of parameters $[n, \frac{n}{2}]$, n even, and not a multiple of 5. The following decomposition into irreducible factors

$$\begin{aligned} x^{22} - 1 \;\; &= \;\; (1+x)(4+x)(1+3x+4x^2+4x^3+x^4+x^5)(4+x+x^2+4x^3+2x^4 \\ &\quad +x^5)(1+x+4x^2+4x^3+3x^4+x^5)(4+3x+x^2+4x^3+4x^4+x^5) \end{aligned}$$

over F_5 comprizes 4 polynomials of degree 5 and two linear polynomials. Thus there are $\binom{2}{4} \times \binom{1}{2} = 12$ possible generators polynomials of degree 11. All polynomials and the corresponding generated codes that are isodual are recorded in the following table.

Table 1

n°	g(x)	$\left[\begin{smallmatrix} u^*(x)= \\ v^*(x)= \end{smallmatrix}\right.$	$[\frac{x^{22}-1}{g(x)}]^* =$
1	423233112341	$\left[\begin{smallmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{smallmatrix}\right.$	$[-g(-x)]^*$
2	100000000001	$\left[\begin{smallmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{smallmatrix}\right.$	$g(-x)$
3	441111442211	$\left[\begin{smallmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{smallmatrix}\right.$	$-g(-x)$
4	443311444411	$\left[\begin{smallmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{smallmatrix}\right.$	$-g(-x)$
5	122222222221	$\left[\begin{smallmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{smallmatrix}\right.$	$g(-x)$
6	412344223231	$\left[\begin{smallmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{smallmatrix}\right.$	$[-g(-x)]^*$
7	113314322221	$\left[\begin{smallmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{smallmatrix}\right.$	$[-g(-x)]^*$
8	423232323231	$\left[\begin{smallmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{smallmatrix}\right.$	$-g(-x)$

n°	g(x)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{22}-1}{g(x)}]^* =$
9	144141143241	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$g(-x)$
10	142341141441	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$g(-x)$
11	400000000001	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$-g(-x)$
12	122223413311	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$

We summarize our first result by:

Proposition 2.1 *All cyclic codes of parameters* $[22, 11]_5$ *are isodual.*

2.2 Cyclic Codes of parameters $[26, 13]_5$

We have $\binom{2}{1} \times \binom{6}{3} = 40$ possible choices for the generating polynomial of the cyclic codes $C[26, 13]_5$.

$$\begin{aligned} x^{26} - 1 &= (1+x)(4+x)(1+x+4x^2+x^3+x^4)(1+2x+2x^3+x^4)(1+2x+x^2+2x^3 \\ &\quad +x^4)(1+3x+3x^3+x^4)(1+3x+x^2+3x^3+x^4)(1+4x+4x^2+4x^3+x^4) \end{aligned}$$

All polynomials and the corresponding generated codes that are either isodual or not are recorded in the following table.

Table 2

n°	g(x)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{26}-1}{g(x)}]^* =$
1	11314011041311	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
2	41202223330341	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$
3	12121433412121	/	*not isod*
4	40133423122401	/	*not isod*
5	12210100101221	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
6	40010423104001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$
7	13433300333431	/	*not isod*
8	44014123414011	/	*not isod*
9	12222222222221	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
10	40000000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$
11	12312144121321	/	*not isod*
12	40431023042101	/	*not isod*
13	13040011004031	/	*not isod*
14	44422314233111	/	*not isod*
15	13240244204231	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$

n°	g(x)	$\left[\begin{smallmatrix} u^*(x)= \\ v^*(x)= \end{smallmatrix}\right.$	$[\frac{x^{26}-1}{g(x)}]^* =$
16	44213032024311	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$-g(-x)$
17	14011133111041	/	*not isod*
18	43132300232421	/	*not isod*
19	14123344332141	/	*not isod*
20	43040041001021	/	*not isod*
21	13410111101431	/	*not isod*
22	44033141422011	/	*not isod*
23	13014222241031	/	*not isod*
24	44402000030111	/	*not isod*
25	14312022021341	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$g(-x)$
26	43340214301221	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$-g(-x)$
27	14032111123041	/	*not isod*
28	43110141404421	/	*not isod*
29	10432433423401	/	*not isod*
30	42424423113131	/	*not isod*
31	10000000000001	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$g(-x)$
32	42323232323231	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$-g(-x)$
33	14103000030141	/	*not isod*
34	43011232344021	/	*not isod*
35	10010433401001	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$g(-x)$
36	42310100404231	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$-g(-x)$
37	10134033043101	/	*not isod*
38	42213114424331	/	*not isod*
39	11303233230311	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$g(-x)$
40	41211041044341	$\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$	$-g(-x)$

Remark: 40% of the cyclic codes $[26, 13]_5$ are isodual.

Proposition 2.2 *If* $\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$ *then the cyclic codes of parameters* $C[26, 13]_5$ *are isodual.*

2.3 Cyclic Codes of parameters $[38, 19]_5$

For cyclic codes of parameters $[38, 19]_5$, the factorization of $x^{38} - 1$ yields $12 = 2 \times \binom{2}{4}$ possible generators polynomials of degree $19 = 1 + 2 \times 9$.

$$x^{38} - 1 \quad = \quad (1 + x)(4 + x)(4 + 4x + 2x^2 + 4x^3 + 2x^4 + 2x^5 + 2x^6 +$$

$$3x^7 + x^9)(1 + 4x + 3x^2 + 4x^3 + 3x^4 + 2x^5 + 3x^6 + 3x^7$$
$$+x^9)(4 + 2x^2 + 3x^3 + 3x^4 + 3x^5 + x^6 + 3x^7 + x^8 + x^9)$$
$$(1 + 3x^2 + 3x^3 + 2x^4 + 3x^5 + 4x^6 + 3x^7 + 4x^8 + x^9)$$

In table 3, we note eatch generator polynomial of the cyclic code $[38, 19]_5$ and the reciprocal of its complement.

Table 3

n°	g(x)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$[\frac{x^{38}-1}{g(x)}]^* =$
1	4400223333331133111 1	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$-g(-x)$
2	12222222222222222221	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$g(-x)$
3	43321324124303204001	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$[-g(-x)]^*$
4	40010320213413243221	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$
5	10000000000000000001	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$g(-x)$
6	44442244222222330011	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$-g(-x)$
7	14003223232341234141	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$g(-x)$
8	40000000000000000001	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$-g(-x)$
9	10010330312443342231	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$[-g(-x)]^*$
10	13224334421303301001	$\begin{bmatrix} u^*(x)=-v(x) \\ v^*(x)=-u(x) \end{bmatrix}$	$[-g(-x)]^*$
11	42323232323232323231	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$-g(-x)$
12	14143214323232230041	$\begin{bmatrix} u^*(x)=v^*(-x) \\ v^*(x)=u^*(-x) \end{bmatrix}$	$g(-x)$

Proposition 2.3 *All cyclic codes of parameters* $[38, 19]_5$ *are isodual.*

2.4 Cyclic Codes of parameters $[42, 21]_5$

The factorization of $x^{42} - 1$ into irreducible factors yields 80 possible generators polynomials of degree 21 of the cyclic codes of parameters $[42, 21]_5$.

$$\begin{aligned} x^{42} - 1 \quad = \quad & (1 + x)(4 + x)(1 + x + x^2)(1 + 4x + x^2)(1 + 2x^2 + 2x^3 + 2x^4 \\ & +x^6)(1 + 2x^2 + 3x^3 + 2x^4 + x^6)(1 + x + x^2 + x^3 + x^4 + x^5 \\ & +x^6)(1 + x + 3x^2 + 4x^3 + 3x^4 + x^5 + x^6)(1 + 4x + x^2 + 4x^3 \\ & +x^4 + 4x^5 + x^6)(1 + 4x + 3x^2 + x^3 + 3x^4 + 4x^5 + x^6) \end{aligned}$$

We give some polynomials and the corresponding generated code with the possibility that are isodual or not in the table 4. For the isodual codes $[42, 21]_5$ we have always: $u^*(x) = u(x)$, $v^*(x) = v(x)$.

Table 4

n°	g(x)	$[\frac{x^{42}-1}{g(x)}]^* =$
1	1343441034004301443431	*not isodual*
2	1101434141441414341011	*not isodual*
3	4101131111144444244041	*not isodual*
4	4313144024001301142421	*not isodual*
5	1434433001441003344341	$g(-x)$
6	4233122324411323342231	$-g(-x)$
7	1223423334114333243221	$g(-x)$
8	4424132001144003241311	$-g(-x)$
9	1301323321441233231031	*not isodual*
10	1112441241001421442111	*not isodual*
11	4142144211004431143141	*not isodual*
12	4301222331144223334021	*not isodual*

Proposition 2.4 *If* $\left[\begin{smallmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{smallmatrix}\right.$ *then the cyclic codes of parameters* $C[42,21]_5$ *are isodual.*

3 Isodual Cyclic Codes

We give three constructions of isodual cyclic codes. We suppose that $n = 2m$ with m odd and not a multiple of 5. In that case the factorization

$$x^m - 1 = (x-1)u(x)v(x)$$

yields, by changing x into $-x$ the factorization

$$x^m + 1 = (x+1)u(-x)v(-x).$$

We choose

$$g(x) = (x-1)u(x)v(-x).$$

We consider the following three cases

1. $u^*(x) = u(x)$, $v^*(x) = v(x)$
2. $u^*(x) = \epsilon v(x)$, $v^*(x) = \eta u(x)$
3. $u^*(x) = v^*(-x)$, $v(x)^* = u^*(-x)$

with ϵ, $\eta = \pm 1$.

Proposition 3.1 *Keep the above notation. In the three cases the cyclic code of generator $g(x)$ is isodual.*

Proof. In each case we compute the generator of the dual code. First

$$(x^n - 1)/g(x) = (x + 1)u(-x)v(x).$$

Taking reciprocals of both sides, we obtain in the three cases: $\pm g(-x)$ or $[-g(-x)]^*$. The result follows.

4 Open Problem

The characterization of the generating polynomial of an isodual cyclic code over GF(5) is now known. Is it possible to extend these result to other finite fields ?

ACKNOWLEDGEMENTS. The author is very grateful to P. Solé (Enst Paris) for his help and his precious directives.

References

[1] M. Crassl, G. White, *New codes from chains of quasi-cyclic codes*, Proc. ISIT2005, Adelaide, Australia, pp. 2095-2099, 2005.

[2] M. Crassl, *Bounds on the minimum distance of linear codes* , [Electronic table; online], http://www.codetables.de.

[3] R. Daskalov, P. Hristov, E. Metodieva, New minimum distance bounds for linear codes over GF(5), *Discrete. Mathematics*, vol. 275(2004), pp.97-110.

[4] P. Gaborit, Table of Self-Dual Codes over GF(5), [tables; online], http://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF5.htm.

[5] T. A. Gulliver, P. R. J. Ostergard and N. Senkevitch, Optimal linear rate 1/2 codes over F_5 and F_7. *Discrete Mathematics*, vol 265(2003), pp. 59-70.

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

[7] E. M. Rains and N. J. A. Sloane, *Self-dual codes, Handbook of Coding Theory*, (V. S. Pless and W. C. Huffman, eds.), Elsevier, Amsterdam, 1998.

[8] J. F. Voloch, Computing the minimal distance of cyclic codes, *Comp and Applied Mathematics*, vol 24(2005), pp. 393-398.