

Optimal and isodual ternary cyclic codes of rate $1/2$

Cherif Mihoubi · Patrick Solé

Received: 12 January 2012 / Revised: 9 May 2012 / Accepted: 4 July 2012 / Published online: 26 July 2012
© The Author(s) 2012. This article is published with open access at SpringerLink.com

Abstract This work is twofold. First, the largest minimum distance of a ternary cyclic codes of parameters $[n, \frac{n}{2}]$, is determined for n even, not a multiple of 3, by using the Chen algorithm, for $n = 26, 34, 38, 46, 50, 58, 62, 68, 70, 74$. Next, seven new classes of isodual ternary cyclic codes are introduced for n singly even, not a multiple of 3.

Keywords Cyclic codes · Minimum distance · Isodual codes

Mathematics Subject Classification (2000) 94B15 · 94B05 · 94B065

1 Introduction

An important class of ternary codes of rate $1/2$ is that of self-dual codes [5], because of its connections with invariant theory, combinatorial designs, and modular forms.

Communicated by S.K. Jain.

C. Mihoubi (✉)
Département de Mathématiques, Université Hadj Lakhdar, 5000 Batna, Algeria
e-mail: cherif.mihoubi@yahoo.fr

C. Mihoubi
Université de M'sila, Bp 581, Hodna, 28000 M'sila, Algeria

P. Solé
Telecom ParisTech, 46 rue Barrault, 75634 Paris Cedex 13, France

P. Solé
Mathematics Department, King Abdulaziz University, Jeddah, Saudi Arabia
e-mail: sole@telecom-paristech.fr

This class is a subclass of formally self dual codes in [2]. In the present work, we consider cyclic ternary codes of rate $1/2$. An important subclass of these is that of cyclic *isodual codes*, i.e. cyclic codes equivalent to their duals. Isodual codes are in particular formally self dual.

Following [2] we consider the largest minimum distance $d_F(n)$ of a fsd ternary code of length n . We introduce $d_I(n)$ the largest minimum distance of an isodual code of length n . Clearly $d_I(n) \leq d_F(n)$. Another function of interest is the largest minimum distance $d_C(n)$ of a cyclic code of length n and rate $1/2$.

Our contribution is twofold. First, we establish by electronic calculation, using an algorithm due to Chen, the value of $d_C(n)$ for n even ≤ 74 . Second, inspired by this numerical data, we propose, in the case $n = 2m$ with m odd, *seven constructions* of ternary isodual cyclic codes. They hold when n is singly even, that is at lengths where self dual ternary codes do not exist. The characterization of the generating polynomial of an isodual cyclic code is left as a challenging open problem.

The material is organized as follows. The next section reviews the necessary notation and definitions. Section 3 derives the seven constructions of isodual cyclic codes and gives a table of values of $d_I(n)$ and $d_C(n)$ for small values of n . Section 4 contains the numerical data on cyclic codes of rate $1/2$ over \mathbb{F}_3 , arranged in subsections by values of the length.

2 Notation and definitions

We assume that the reader has gained some familiarity with coding theory [1,4]. Let $\mathbb{F}_3 = \{0, 1, 2\}$ denote the Galois field of three elements. Recall that the *rate* of a linear code of length n and dimension k is k/n . Two ternary linear codes are said to be *equivalent* if one can be obtained from the other by permutation of coordinate places and negation of some coordinate entries. A linear code is said to be *isodual* iff it is equivalent to its dual. Recall that a cyclic code of length n over \mathbb{F}_q can be regarded as an ideal in the principal ideal ring $\mathbb{F}_q[x]/(x^n - 1)$. 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 \mathbb{F}_3 , is defined by

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

The elements of a code C are called codewords, and the weight $wt(x)$ of a codeword x is the number of positions where x is nonzero. The Hamming distance $d(x, y)$ between two codewords x and y is $d(x, y) = wt(x - y)$. The minimum distance of a code C is:

$$d(C) = \min\{d(x, y) / x, y \in C, x \neq y\}.$$

If C is linear then $d(C)$ equals the minimum weight of a nonzero codeword. The three parameters of a q -ary code are denoted by $[n, k, d]_q$ and are length, dimension, minimum distance. The so-called *fundamental problem of coding theory* is

- Find $d_q(n, k)$, the largest value of d for which a code of parameters $[n, k, d]_q$ exists.

A code that attains this value is called an optimal code. With the notation of the introduction we have, by definition,

$$d_C(n) \leq d_3(n, n/2),$$

and

$$d_I(n) \leq d_F(n) \leq d_3(n, n/2).$$

3 Isodual cyclic codes

3.1 Constructions

We give seven constructions of isodual ternary cyclic codes and illustrate them by examples in the next section. We suppose that $n = 2m$ with m odd and not a multiple of 3. 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 seven cases

- (1) $u^*(x) = u(x), v^*(x) = v(x)$
- (2) $u^*(x) = \epsilon v(x), v^*(x) = \eta u(x)$
- (3) $u^*(x) = -v^*(x)$
- (4) $u^*(x) = u(x), v^*(x) = v(-x)^*$
- (5) $u^*(x) = u(-x)^*, v^*(x) = v(x)$
- (6) $u^*(x) = u(x), v^*(x) = \eta v(-x)$
- (7) $u^*(x) = \epsilon u(-x), v^*(x) = v(x)$

with $\epsilon, \eta = \pm 1$.

Proposition 1 *Keep the above notation In the seven cases above 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 first five cases $\pm g(-x)$, and in the last two cases $[-g(-x)]^*$. The result follows. □

3.2 Table of values of $d_I(n)$ and $d_C(n)$

In this table we note the different values of $d_I(n)$ and $d_C(n)$ respectively for isodual and cyclic codes of parameters $[n, \frac{n}{2}]_3$ according to the length of the code.

n	26	34	38	46	50	58	62	68	70	74
$d_I(n)$	6	4	4	9	4	4	4		14	14
$d_C(n)$	8	4	4	13	4	4	4	8	14	14

Remark For $n = 34, 38, 50, 58, 62, 70, 74$ the minimum distance of the best isodual code of parameters $[n, \frac{n}{2}]_3$ is the same as that of the best cyclic code of rate one-half.

4 Optimal cyclic codes of rate 1/2 over \mathbb{F}_3

4.1 Cyclic codes of parameters $[26, 13]_3$

We begin our study of the minimum distance of ternary cyclic codes of parameters $[n, \frac{n}{2}]$, n even, and not a multiple of 3. For linear codes the upper and lower bounds from [3] on $d_3(n, n/2)$ coincide for $2 \leq n \leq 24$. For $n \geq 26$ (see [3]) the upper bounds are not always met. The table of bounds on $d_3(n, n/2)$ for $26 \leq n \leq 74$ is given below.

n	26	28	32	34	38	40	44	46	50
d_3	8-9	9-10	10-11	11-12	11-13	12-14	13-15	14-15	14-17

n	52	56	58	62	64	68	70	74
d_3	15-18	16-18	17-19	17-20	18-21	16-22	17-23	18-24

The algorithm of Chen as described in [6] allows us to derive the minimum distances of all ternary cyclic codes of length 26 and dimension 13. The following decomposition into irreducible factors

$$x^{26} - 1 = (1+x)(2+x)(1+2x+x^3)(2+2x+x^3)(2+x^2+x^3)(2+x+x^2+x^3)(1+2x+x^2+x^3)(1+2x^2+x^3)(1+x+2x^2+x^3)(2+2x+2x^2+x^3)$$

Table 1 Length 26

$g(x)$	codeword(a)	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{26}-1}{g(x)} \right]^* =$	wt(a)
10000000000001	10000000000001000000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$g(-x)$	2
22121212121211	21000000000002100000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$-g(-x)$	4
11220102101001	10100000100001010000010000	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=-v(-x) \end{bmatrix}$	$[-g(-x)]^*$	6
20120100020121	12001010000002100202000000			8
12112100012111	21000100000000200000000211			7
22000102100211	22200000000102202020000000			8
10020222110211	12010000000002102000000000	$\begin{bmatrix} u^*(x)=-u(-x) \\ v^*(x)=v(x) \end{bmatrix}$	$[-g(-x)]^*$	6
12011200010121	10100000100001010000010000	$\begin{bmatrix} u^*(x)=u(-x)^* \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	6
20000000000001	10000000000002000000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$-g(-x)$	2
12222222222221	11000000000002200000000000	$\begin{bmatrix} u^*(x)=v(x) \\ v^*(x)=u(x) \end{bmatrix}$	$g(-x)$	4
10111211001201	22000000100001100000020000	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	6
21120102202001	10100000100002020000020000	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=-v(-x) \end{bmatrix}$	$[-g(-x)]^*$	6
12121021020221	10200001000002000012000200			7

over \mathbb{F}_3 comprises 8 polynomials of degree 3 and two linear polynomials. Thus there are $\binom{8}{4} \binom{2}{1} = 140$ possible generators polynomials of degree $3 \times 4 + 1 = 13$. Some of these polynomials along with a minimum weight codeword a and its weight are recorded in Table 1.

Remark There are 54 codes with the optimal minimum distance 8 among the 140 cyclic codes of parameters $[26, 13]_3$.

We summarize our first experimental result by

Proposition 2 We have $d_C(26) = 8$. Note that $d_3(26, 13) \in \{8, 9\}$, by [3].

4.2 Cyclic codes of parameters $[n, \frac{n}{2}]_3$ where $n = 34, 38, 50, 58, 62$

– In the cases $n = 34, 38, 58, 62$, for the all cyclic codes of parameters $[n, \frac{n}{2}]_3$, we have

$$x^n - 1 = (1 + x)(1 + x + x^2 + \dots + x^{\frac{n}{2}-2} + x^{\frac{n}{2}-1}) \\ (2 + x)(1 + 2x + x^2 + \dots + 2x^{\frac{n}{2}-2} + x^{\frac{n}{2}-1}).$$

Thus there are four choices for the generator polynomial of each code.

For the cyclic codes of parameters $[50, 25]_3$, we have 8 possible choices for the generator polynomial $g(x)$ of degree 25.

$$x^{50} - 1 = (1 + x)(2 + x)(1 + x + x^2 + x^3 + x^4)(1 + 2x + x^2 + 2x^3 + x^4) \\ (1 + x^5 + x^{10} + x^{15} + x^{20})(1 + 2x^5 + x^{10} + 2x^{15} + x^{20}).$$

But in all cases, the maximal minimum distance d_C of such codes is equal to 4, and we have always:

$$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix} \text{ with } \left[\frac{x^n - 1}{g(x)} \right]^* = \pm g(-x).$$

Proposition 3 For $n = 34, 38, 50, 58, 62$ the cyclic codes of parameters $[n, n/2]_3$ are isodual.

4.3 Cyclic codes of parameters $[46, 23]_3$

For cyclic codes of parameters $[46, 23]$, the factorization of $x^{46} - 1$ yields $12 = 2 \times \binom{4}{2}$ possible generator polynomials of degree $23 = 1 + 2 \times 11$.

$$x^{46} - 1 = (1 + x)(2 + x)(1 + 2x + x^2 + x^3 + 2x^4 + x^6 + x^8 + x^{11}) \\ (2 + 2x + 2x^2 + x^3 + x^4 + 2x^6 + 2x^8 + x^{11}) \\ (2 + x^3 + x^5 + 2x^7 + 2x^8 + x^9 + x^{10} + x^{11}) \\ (1 + x^3 + x^5 + 2x^7 + x^8 + x^9 + 2x^{10} + x^{11}).$$

The analogue of Table 1 is Table 2 below.
For the isodual cyclic codes $[46, 23]_3$ we have:

$$\begin{bmatrix} u^*=\epsilon v \\ v^*=\eta u \end{bmatrix}; \quad \epsilon, \quad \eta = \pm 1$$

or

$$u^*(x) = -v^*(x)$$

with

$$\left[\frac{x^{46} - 1}{g(x)} \right]^* = \pm g(-x).$$

The optimum distance of such a cyclic codes is

Proposition 4 We have $d_C(46) = 13$. Note that $d_3(46, 23) \in \{14, 15\}$.

Table 2 Length 46

$g(x)$	codeword(a)	$\begin{bmatrix} u^*(x) = \\ v^*(x) = \end{bmatrix}$	$\begin{bmatrix} x^{46}-1 \\ g(x) \end{bmatrix}^*$	$wf(a)$
222222111100220020000011	1020201000000000000000000000000020002000002010000000020	$u^*(x) = -v^*(x)$	$-g(-x)$	9
200202112120101200201221	21110000011000000000000000000200010002200000202200			13
100000000000000000000001	100000000000000000000000010000000000000000000000000000	$\begin{bmatrix} u^*(x) = u(x) \\ v^*(x) = u(x) \end{bmatrix}$	$g(-x)$	2
12222222222222222222221	11000000000000000000000002200000000000000000000000000	$\begin{bmatrix} u^*(x) = -v(x) \\ v^*(x) = -u(x) \end{bmatrix}$	$g(-x)$	4
211201001202012122101001	2212100100000000000000000200200000021000000100021			13
22000011001100222211111	101020001000000000000000000020001000000000020101000	$u^*(x) = -v^*(x)$	$-g(-x)$	9
121212212100120012000021	102020100000000000000000000000002000200000201000000020	$u^*(x) = -v^*(x)$	$g(-x)$	9
112201002202011112202001	122220010000000000000000020010000002200000200000200011			13
22121212121212121211	21000000000000000000000002100000000000000000000000000	$u^*(x) = -v^*(x)$	$-g(-x)$	4
2000000000000000000000001	1000000000000000000000000000020000000000000000000000000	$\begin{bmatrix} u^*(x) = -v(x) \\ v^*(x) = -u(x) \end{bmatrix}$	$-g(-x)$	2
10020221110202200102211	221200000210000000000000000002000100002100000202100			13
120000210021001212212121	1010200010000000000000000000020001000000000020101000	$u^*(x) = -v^*(x)$	$g(-x)$	9

Table 3 Length 68

$g(x)$	codeword(a)	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} = \begin{bmatrix} x^{68}-1 \\ g(x) \end{bmatrix}^* = \text{wt}(a)$
201011221001001021002021120020020121	220...0110...0220...0110...0	8
20201020102010201020102010201020101	2010....00...02010....00....0	4
22201002001122020022010020011220201	210...0210...0210...0210...0	8
21201001001221010021020020021120201	220...0110...0220...0110...0	8
2000000000000000000000000000000001	100.....020.....0	2
20101122001002011001011220010020111	210...0210...0210...0210...0	8
10102121002012120021201012202101021	20....010....020....010.....0	4
11020220211010222001111020022220101	10....010...010.....010.....0	4
12010120221010212002121020012120101	20.....010...020...010...0	4
102020202020202020202020202020201	1010.....02020.....0	4
10102222002011110022201011202202011	10...010...010.....010...0	4
1000000000000000000000000000000001	10.....010.....0	2

4.4 Cyclic codes of parameters $[68, 34]_3$

Likewise the factorization of $x^{68} - 1$ yields 12 possibilities for the generator polynomial of the code.

$$\begin{aligned}
 x^{68} - 1 = & (1 + x)(2 + x)(1 + x^2)(1 + 2x + 2x^4 + 2x^5 + 2x^6 + 2x^{10} \\
 & + x^{11} + 2x^{12} + x^{15} + x^{16})(1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \\
 & + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16}) \\
 & (1 + x + 2x^4 + x^5 + 2x^6 + 2x^{10} + 2x^{11} + 2x^{12} + 2x^{15} + x^{16}) \\
 & (1 + 2x + x^2 + 2x^3 + x^4 + 2x^5 + x^6 + 2x^7 + x^8 + 2x^9 + x^{10} \\
 & + 2x^{11} + x^{12} + 2x^{13} + x^{14} + 2x^{15} + x^{16}).
 \end{aligned}$$

The analogue of Table 1 is Table 3.

If we take all $g(x)$ that divide $x^{68} - 1$, as indicated in Table 4, we have always:

$$\left[\frac{x^{68} - 1}{g(x)} \right]^* \neq \pm g(-x)$$

and

$$\left[\frac{x^{68} - 1}{g(x)} \right]^* \neq [-g(-x)]^*.$$

This shows that the isodual cyclic codes of parameters $[68, 34]_3$ are not isodual by the constructions of the preceding section.

Proposition 5 We have $d_C(68) = 8$. Note that $d_3(68, 34) \geq 16$.

Table 4 Length 70

$g(x)$	codeword(a)	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} =$	$\begin{bmatrix} x^{70}-1 \\ g(x) \end{bmatrix}^* =$	$w(a)$
1021110100000202120121022202110001101	11110..20..20..10..2220..10..10..20..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	12
12222011101000202100122220020210211	1110..20..10..10..2220..10..20..20..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	12
1222222222222222222222222222222221	110.....0220.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	4
112010110022210102201012220011010211	220..010.....010..0220..010..010..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	8
11201202002221001220200010111022221	1110..20..20..010..2220..10..010..20..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	12
10110001120220121021202000010111201	1110..20..10..10..2220..10..20..020..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	12
111121210121201201002012100212120011	10..10..10..10..10..10..10..10..10..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	10
1000010202020121122011110222222221	10..10..10..10..10..10..10..10..10..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	10
100000200000200000020000020000001	10.....01..020..020.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	4
122220111102222011110222201111022221	2000010.....02000010.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	4
12222222201111022112102022020100001	10..10..10..10..10..10..10..10..10..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	10
11002121001210200102102121012112111	10..10..10..10..10..10..10..10..10..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	10
1111200212021010122010121121020011	2020..10..10..10..010..20..1020..20..10..20..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	12
10000000200000100220101200210122221	1010..1010..10..10..11010..101010..10..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	14
1000020000200002000020000200000001	1000010.....02000020.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	4
1222222011111022222011111102222221	20..010.....020.....010..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	4
122221012002101022001000002000000001	101010..10110..10..010..010..1010..1010..0100	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	14
110020121121010221010101202120021111	101020..020..01010..02010..01020002020..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	12
121222102222201210101212210112220021	210...020...020...010...0210...020...010...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	10

Table 4 continued

$g(x)$	codeword(a)	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} =$	$\begin{bmatrix} x^{70}-1 \\ g(x) \end{bmatrix}^* =$	$w(a)$
1121212011000020020012000210002000001	210..020..020..010..0210...020..020..10..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=u(-x) \end{bmatrix}$	$[-g(-x)]^*$	10
112120110022202101101202220011021211	120..010...010...0210...020...020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	8
100000000000000000000000000000000001	10.....010.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$	2

4.5 Cyclic codes of parameters [70, 35]₃

The factorization of $x^{70} - 1$ yields 48 possibilities for the generator polynomial $g(x)$ of degree 35 of the code.

$$\begin{aligned}
 x^{70} - 1 = & (1 + x)(2 + x)(1 + x + x^2 + x^3 + x^4)(1 + 2x + x^2 + 2x^3 + x^4) \\
 & (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)(1 + 2x + x^2 + 2x^3 + x^4 + 2x^5 + x^6) \\
 & (1 + 2x + 2x^2 + x^3 + 2x^4 + x^5 + x^7 + 2x^8 + x^{10} + x^{12}) \\
 & (1 + x + 2x^2 + 2x^3 + 2x^4 + 2x^5 + 2x^7 + 2x^8 + x^{10} + x^{12}) \\
 & (1 + x^2 + 2x^4 + 2x^5 + 2x^7 + 2x^8 + 2x^9 + 2x^{10} + x^{11} + x^{12}) \\
 & (1 + x^2 + 2x^4 + x^5 + x^7 + 2x^8 + x^9 + 2x^{10} + 2x^{11} + x^{12}).
 \end{aligned}$$

For this codes we have 3 cases:

$$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix} \text{ or } \begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix} \text{ with } \left[\frac{x^{70} - 1}{g(x)} \right]^* = \pm g(-x)$$

or

$$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix} \text{ with } \left[\frac{x^{70} - 1}{g(x)} \right]^* = [-g(-x)]^*.$$

We summarize the parameters of the cyclic codes [70, 35]₃ in Tables 4 and 5 below.

Remark The cyclic codes of parameters [70, 35]₃ are all isodual.

Proposition 6 *The optimal minimum distance of the cyclic codes of parameters [70, 35]₃ is $d_C(70) = 14$.*

4.6 Cyclic codes of parameters [74, 37]₃

The determination of the minimum distance for these codes required in some cases up to 12 hours of CPU time on a PC. The factorisation of $x^{74} - 1$ yields 12 possible choices for a generator polynomial of degree 37.

$$\begin{aligned}
 x^{74} - 1 = & (1 + x)(2 + x)(1 + 2x^2 + 2x^4 + x^5 + 2x^7 + 2x^{11} + x^{13} + 2x^{14} + 2x^{16} \\
 & + x^{18})(1 + 2x^2 + 2x^4 + 2x^5 + x^7 + x^{11} + 2x^{13} + 2x^{14} + 2x^{16} + x^{18}) \\
 & (1 + x + 2x^2 + 2x^3 + x^4 + 2x^5 + 2x^6 + 2x^8 + 2x^9 + 2x^{10} + 2x^{12} \\
 & + 2x^{13} + x^{14} + 2x^{15} + 2x^{16} + x^{17} + x^{18})(1 + 2x + 2x^2 + x^3 + x^4 \\
 & + x^5 + 2x^6 + 2x^8 + x^9 + 2x^{10} + 2x^{12} + x^{13} + x^{14} + x^{15} + 2x^{16} \\
 & + 2x^{17} + x^{18}).
 \end{aligned}$$

The analogue of Table 1 is Table 6.

Proposition 7 *We have $d_C(74) = 14$.*

Table 5 Length 70 continued

$g(x)$	codeword(a)	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} =$	$\begin{bmatrix} x^{70}-1 \\ g(x) \end{bmatrix}^*$	$w(a)$
1000020001200021002002000001102121211	210...020..010..010...0210...020..010...010...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	10
120022211012221210121022222201222121	210...020..010...010...0210...020..010..010...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$g(-x)$	10
222212201212102220202222110122120011	110...010..020..010...0220...020..010...020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$-g(-x)$	10
200002000110001100100200002102222221	220...010..020..010...0110...020..010...020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	10
2000000000000000000000000000000001	10.....020.....020.....020.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$	2
21111102100001002002200022000100001	110...010...020..010...0220...020..010..020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	10
220012112022111101011102121201121111	220...010..020..010...0110...020..010...020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$-g(-x)$	10
2121100222020202221020222111020021	2020..10..10..10..20..1020..020..10..20..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$-g(-x)$	12
221211011002220201200200000100000001	101010..10120..010..10...10..1010..1010..10..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	14
221212102121210212121021212102121211	10.....010..0200.....020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$	4
200002000010000200001000020000100001	20.....010..020.....010...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$	4
20000000200000100120101100220221211	1010..1010..10..10...21010..101010..010..0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	14
21001022211101021101010110022121	101020..20..1010..2010..1020..2020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$-g(-x)$	12
21211122202220110200201110022220021	10...20..10..020..10..20..10..20...10..20...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$-g(-x)$	10
22121210212120211102021010200001	10..20..10..20..10..20...10..20..10..020...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	10
221210212102121021210212102121021211	1000010.....2000020.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$	4
20000020000010000002000000000000001	20.....10.....20.....10.....0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$	4
200001020210102221102121210212121211	10..20..10..020..10..20..10...20..10..20...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x) \end{bmatrix}$	$[-g(-x)]^*$	10
21001111002220100102201111011222121	10..20..10..20..10..20..10..20...10..20...0	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(-x)^* \end{bmatrix}$	$-g(-x)$	10

Table 5 continued

$g(x)$	codeword(a)	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} =$	$\left[\frac{x^{70}-1}{g(x)} \right]^* =$	$w(a)$
211110210012101101202202120021022221	220...010.....010...0220...010.....010...0	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} = \begin{bmatrix} u(x) \\ v(x) \end{bmatrix}$	$-g(-x)$	8
201121010000020222011102101120002101	2120...10..20..10...2120...10..20...10...0	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} = \begin{bmatrix} u(x) \\ v(x) \end{bmatrix}$	$-g(-x)$	12
211022020012122001120200010121021211	2120...10..20...10...2120...10..20...10...0	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} = \begin{bmatrix} u(x) \\ v(-x) \end{bmatrix}$	$[-g(-x)]^*$	12
211020210012110102102022120021010221	120...10.....10..0210.....20.....020...0	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} = \begin{bmatrix} u(x) \\ v(x) \end{bmatrix}$	$-g(-x)$	8
22121212121212121212121212121211	210.....210.....0	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} = \begin{bmatrix} u(x) \\ v(x) \end{bmatrix}$	$-g(-x)$	4
221210212020001012200112120010110221	2120...10..20...10...2120...10..20...10...0	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} = \begin{bmatrix} u(x) \\ v(-x) \end{bmatrix}$	$[-g(-x)]^*$	12
202100012202102220111010000020212201	2120...10...20...10...2120...10...20...10...0	$\begin{bmatrix} u^*(x) \\ v^*(x) \end{bmatrix} = \begin{bmatrix} u(x) \\ v(-x) \end{bmatrix}$	$-g(-x)$	12

Table 6 Length 74

$g(x)$	codeword(a)	$\begin{matrix} u^*(x) = \\ v^*(x) = \end{matrix}$	$\left[\frac{x^{74}-1}{g(x)} \right]^* =$	wt(a)
11112222112222002222220022221122221111	10102000200010..010...010...01010...020...020	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$g(-x)$	11
12222100020220200222220202202000122221	210..020..02001020..010..010..02010020..0200012	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$g(-x)$	14
100000000000000000000000000000000001	10.....010.....0	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$g(-x)$	2
1222222222222222222222222222222222221	110.....0220.....0	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$g(-x)$	4
1000010001200210011100120021000100001	110020020...0200200110020...0110...110...0200	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$g(-x)$	14
11002200222200110000001100222200220011	2010100020...010...02000101020..010...010...0	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$		11
21211212211212001212120012122112122121	10102000200010...010...010...01010...020...020	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$		11
20000100011002200121200110022000200001	120020010...0200100120020...0210...0210...0100	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$-g(-x)$	14
221212121212121212121212121212121211	210.....0210.....0	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$-g(-x)$	4
200000000000000000000000000000000001	10.....020.....0	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$-g(-x)$	2
22121100020210100212100202101000221211	1100020..02002010..010..020..02010010..0100022	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$-g(-x)$	14
21001200121200210000002100121200120021	2010100020.....010...02000101020...010...010...0	$\begin{matrix} u^* = u \\ v^* = v \end{matrix}$	$-g(-x)$	11

Acknowledgments The authors thanks the referees for helpful suggestions that greatly improved the presentation of the material. They are very grateful to H. Aissaoui (Telecom ParisTech) for the optimization of the research algorithm of the minimum distance of a cyclic codes $C [26, 13]_3$.

Open Access This article is distributed under the terms of the Creative Commons Attribution License which permits any use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

References

1. Cary Huffman, W., Pless, V.: *Fundamentals of Error Correcting Codes*. Cambridge University Press, Cambridge (2003)
2. Dougherty, S.T., Gulliver, T.A., Harada, M.: Optimal ternary formally self-dual codes. *Discrete Math.* **196**, 117–135 (1999)
3. Grassl, M.: Bounds on the minimum distance of linear codes (Electronic table; online). <http://www.codetables.de/win/math/dw/voorlincood.html>
4. MacWilliams, F.J., Sloane, N.J.A.: *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam (1977)
5. Rains, E.M., Sloane, N.J.A.: Self-dual codes. In: Pless, V.S., Huffman, W.C. (eds.) *Handbook of Coding Theory*. Elsevier, Amsterdam (1998)
6. Voloch, J.F.: Computing the minimal distance of cyclic codes. *Comp. Appl. Math.* **24**, 393–398 (2005)