Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Finite Fields and Their Applications 10 (2004) 530–539

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Some families of $\mathbb{Z}_4$-cyclic codes

Gerardo Vega[a] and Jacques Wolfmann[b,*]

[a] *Dirección General de Servicios de Cómputo Académico, Universidad Nacional Autónoma de México, 04510 México D.F., Mexico*

[b] *GRIM, Université Toulon-Var, 83957 La Garde Cedex, France*

Received 17 April 2003; revised 27 September 2003

Communicated by N.J.A. Sloane

Abstract

We introduce and solve several problems on $\mathbb{Z}_4$-cyclic codes. We study the link between $\mathbb{Z}_4$-linear cyclic codes and $\mathbb{Z}_4$-cyclic codes (not necessarily linear) obtained by using two binary linear cyclic codes. We use these results to present a family of $\mathbb{Z}_4$-self-dual linear cyclic codes.
© 2003 Elsevier Inc. All rights reserved.

Keywords: Codes; Cyclic codes over $\mathbb{Z}_4$; $\mathbb{Z}_4$-self-dual linear cyclic codes

1. Introduction

After the publication of [4], which solved the old problem of the formal duality of Kerdock and Preparata codes by using $\mathbb{Z}_4$-cyclic codes and the Gray map, $\mathbb{Z}_4$-cyclic codes have been extensively studied. The Nechaev–Gray map (introduced in [11]) also plays an important role. The action of these two transforms on $\mathbb{Z}_4$-cyclic codes (linear or not) was considered in [11,12]. This approach gives rise to constructions of new interesting binary codes that may be obtained from $\mathbb{Z}_4$-linear cyclic codes [1,2]. Furthermore, $\mathbb{Z}_4$-cyclic codes which are self-dual codes were used to study and construct important lattices and $\mathbb{F}_2$-self-dual codes (see [10]).

In this work, we introduce and solve several problems on $\mathbb{Z}_4$-cyclic codes (not necessarily linear) and we use these results to present a family of $\mathbb{Z}_4$-self-dual linear cyclic codes. In particular, we improve a result of [6] and we generalize results of [10].

[*] Corresponding author. Fax: +33-4-94-14-2633.
E-mail address: wolfmann@univ-tln.fr (J. Wolfmann).

1071-5797/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2003.11.003

1.1. Notation and definitions

$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$ is the ring of integer modulo 4 and $\mathbb{F}_2$ is the finite field of order 2.

Let $\mathbb{A}$ be a commutative ring and let m be a positive integer, $m \geqslant 1$.

A linear code of length m over $\mathbb{A}$ is a submodule of $\mathbb{A}^m$. A cyclic code of length m over $\mathbb{A}$ is a shift invariant subset of $\mathbb{A}^m$ (which is not necessarily a linear code).

Under the usual identification of vectors with polynomials, linear cyclic codes of length m over $\mathbb{A}$ are identified as ideals in the quotient ring $\mathscr{A} = \mathbb{A}[x]/(x^m - 1)$. The elements of this ring are the polynomials over $\mathbb{A}$ with degree at most $m - 1$ with addition and multiplication computed modulo $x^m - 1$.

This quotient ring will be denoted by $\mathscr{A}_2(m)$ if $\mathbb{A} = \mathbb{F}_2$ and by $\mathscr{A}_4(m)$ if $\mathbb{A} = \mathbb{Z}_4$.

We denote by $\langle g(x) \rangle_i^m$ the principal ideal generated by $g(x) \in \mathscr{A}_i(m)$ for $i = 2, 4$.

In terms of sets, we are considering $A_2(n)$ as a subset of $A_4(n)$. However, we have to distinguish between the addition over $\mathbb{Z}_4$ denoted by "$+$" and the binary addition denoted by "$\oplus$". When necessary, we will specify if products are computed over $\mathbb{Z}_4$ or over $\mathbb{F}_2$.

If $\mathbb{A} = \mathbb{Z}_4$, then the binary reduction of $u(x) \in \mathscr{A}_4(m)$ is denoted by $\tilde{u}(x)$. If $\tilde{f}(x)$ is a divisor of $x^n - 1$ in $\mathbb{F}_2[x]$, n odd, then there exists a unique monic divisor $f(x)$ of $x^n - 1$ in $\mathbb{Z}_4[x]$ such that the binary reduction of $f(x)$ is $\tilde{f}(x)$. The polynomial $f(x)$ is called the Hensel lift of $\tilde{f}(x)$ (see [4]). One way of finding this polynomial is by Graeffe's method: $f(x^2) = \varepsilon \tilde{f}(x)\tilde{f}(-x)$ calculated in $\mathbb{Z}_4[x]$, with $\varepsilon \in \{-1, +1\}$.

Recall that the componentwise product of two polynomials $\tilde{f}(x) = \sum_{i=0}^{n-1} f_i x^i$ and $\tilde{g}(x) = \sum_{i=0}^{n-1} g_i x^i$ in $A_2(n)$ denoted by $\tilde{f}(x) * \tilde{g}(x)$ is defined to be $\tilde{f}(x) * \tilde{g}(x) = \sum_{i=0}^{n-1} f_i g_i x^i$

Let $\tilde{u}(x)$ be a divisor of $x^n - 1$ in $\mathbb{F}_2[x]$ with n odd and let β be a primitive nth root of unity over $\mathbb{F}_2$. Define $(\tilde{u} \circledast \tilde{u})(x)$ as the divisor of $x^n - 1$ in $\mathbb{F}_2[x]$ whose roots are the $\beta^i \beta^j$ such that β^i and β^j are roots of $\tilde{u}(x)$.

Observe that if R and $R^{\circledast}$ are the sets of roots of $\tilde{u}(x)$ and $(\tilde{u} \circledast \tilde{u})(x)$, respectively, then $R \subseteq R^{\circledast}$ and $\tilde{u}(x)$ divides $(\tilde{u} \circledast \tilde{u})(x)$.

1.2. Nechaev–Gray map

Since in this work we will describe cyclic codes only by their polynomial representations, we only introduce polynomial versions of the Nechaev permutation and the Gray and Nechaev–Gray maps. See [11,12] for more details on the original definitions.

The Gray map Φ is the function from $\mathscr{A}_4(n)$ into $\mathscr{A}_2(2n)$ defined by

$$\Phi(u(x)) = \tilde{q}(x) \oplus x^n(\tilde{q}(x) \oplus \tilde{r}(x)),$$

where $u(x) = \tilde{r}(x) + 2\tilde{q}(x)$ with $\tilde{r}(x)$ and $\tilde{q}(x)$ in $\mathscr{A}_2(n)$ and where $\oplus$ is the binary addition.

Let n be odd. The Nechaev permutation is the permutation π of $\mathscr{A}_2(2n)$ defined as

$$\pi(\tilde{m}(x)) = \sum_{i=0}^{2n-1} m_{\tau(i)}x^i,$$

where τ is the permutation on $\{0, 1, ..., 2n-1\}$ given by
$\tau = (1, n+1)(3, n+3)\cdots(n-2, 2n-2)$.

The Nechaev–Gray map Ψ is defined by $\Psi = \pi\Phi$ where π is the Nechaev permutation.

It was proved in [11] that $\Psi(u(x)) = \Phi(u(-x))$.

1.3. Two types of $\mathbb{Z}_4$-cyclic codes

As mentioned before, we identify every cyclic code with its polynomial representation and in this work "cyclic code" means shift-invariant code and not necessarily "linear code". Let $(\tilde{a}(x), \tilde{b}(x))$ be an ordered pair of binary polynomials whose product is a factor of $x^n - 1$ in $\mathbb{F}_2[x]$ with n odd. We also consider $\tilde{c}(x)$ such that $x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x)$. Let $a(x)$, $b(x)$ and $c(x)$ be the Hensel lifts of $\tilde{a}(x), \tilde{b}(x)$ and $\tilde{c}(x)$, respectively. We consider two types of $\mathbb{Z}_4$-cyclic codes:

(A) $\langle a(x)b(x) + 2a(x)\rangle_4^n$;

(B) $\langle \tilde{a}(x)\tilde{b}(x)\rangle_2^n + 2\langle \tilde{a}(x)\rangle_2^n$.

The reasons to be interested in these two types of codes are explained now by means of known facts and open problems.

Many examples show that type (B) codes are not always $\mathbb{Z}_4$-linear. When they are $\mathbb{Z}_4$-linear and also self-dual codes, they have been used in the study of lattices (see for example [10]). Hence, it is interesting to know when type (B) codes are $\mathbb{Z}_4$-linear and when they are self-dual codes.

The following well known and easy to prove result gives a first answer [4]:

Fact 1. *Let $\tilde{C}_1$ and $\tilde{C}_2$ be two linear codes of odd length n over $\mathbb{F}_2$. Then $C = \tilde{C}_1 + 2\tilde{C}_2$ is a $\mathbb{Z}_4$-linear code if and only if*

$$\tilde{C}_1 * \tilde{C}_1 \subseteq \tilde{C}_2. \tag{1}$$

Remarks. (1) If in addition $\tilde{C}_1$ and $\tilde{C}_2$ are two binary linear cyclic codes then (1) implies $\tilde{C}_1 \subseteq \tilde{C}_2$ which means that $\tilde{C}_1 = \langle \tilde{a}(x)\tilde{b}(x)\rangle_2^n$ and $\tilde{C}_2 = \langle \tilde{a}(x)\rangle_2^n$ where $\tilde{a}(x)\tilde{b}(x)$ divides $x^n - 1$ in $\mathbb{F}_2[x]$. In other words, C is a type (B) code.

(2) Unfortunately, condition (1) is not trivial to check and therefore a more practical criterion is needed.

The next result shows the importance of type (A) codes. It comes from [3] and is detailed in [11] (see also [5,8]).

Fact 2. *Every $\mathbb{Z}_4$-linear cyclic code C of odd length n is of type* (A) *and the cardinality of C is $4^{\deg c(x)}2^{\deg b(x)}$.*

Type (A) codes whose Nechaev–Gray images are linear cyclic binary codes are characterized in [12] as follows:

Fact 3. *Let n be odd.*

If C is a type (A) *code, defined as previously by means of $a(x), b(x), c(x)$ and if $\tilde{e}(x)$ is such that $x^n - 1 = (\tilde{c} \circledast \tilde{c})(x)\tilde{e}(x)$ in $\mathbb{F}_2[x]$, then*:

(I) *The following properties are equivalent*:
 (1) $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n * \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n \subseteq \langle \tilde{a}(x) \rangle_2^n$.
 (2) *$\Psi(C)$ is a binary linear cyclic code.*
 (3) *$\tilde{a}(x)$ divides $\tilde{e}(x)$ in $\mathbb{F}_2[x]$.*

(II) *If one of these conditions is satisfied then $\Psi(C) = \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}$.*

Several open problems about types (A) and (B) codes remain.

The main goal of this work is to solve the following ones:

P_1: When are type (B) codes $\mathbb{Z}_4$-linear?

(find a better condition than (1))

P_2: When does $\langle a(x)b(x) + 2a(x) \rangle_4^n = \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2\langle \tilde{a}(x) \rangle_2^n$?

P_3: What are the Nechaev–Gray images of type (B) codes?

2. Results

2.1. Binary linear cyclic codes of length 2n, n odd

The next theorem will show how a binary linear cyclic code of length $2n$ (n odd) can be obtained from two binary linear cyclic codes of length n by means of the Nechaev–Gray map.

We first need a useful lemma.

Lemma 4. *Let $f(x)$ be in $\mathscr{A}_4(n)$ with n odd such that $f(x) = \tilde{r}(x) + 2\tilde{q}(x)$ with $\tilde{r}(x)$ and $\tilde{q}(x)$ in $\mathscr{A}_2(n)$. If Ψ is the Nechaev–Gray map then,*

$$\Psi(f(x)) = (x^n + 1)\tilde{q}(x) \oplus x\frac{d}{dx}[(x^n + 1)\tilde{r}(x)].$$

Proof. let $O(\tilde{r})(x) = \sum_{i \text{ odd}} \tilde{r}_i x^i$ be the odd part of $\tilde{r}(x)$.

Calculating over $\mathbb{F}_2$ and since n is odd, obviously $O(\tilde{r})(x) = x\frac{d}{dx}(\tilde{r}(x))$.

On the other hand, $f(-x) = \tilde{r}(x) + 2(\tilde{q}(x) \oplus O(\tilde{r})(x))$.

From $\Psi(f(x)) = \Phi(f(-x))$, we find

$$\begin{aligned}\Psi(f(x)) &= \tilde{q}(x) \oplus x\frac{d}{dx}(\tilde{r}(x)) \oplus x^n\left[\tilde{q}(x) \oplus \tilde{r}(x) \oplus x\frac{d}{dx}(\tilde{r}(x))\right]\\ &= (x^n+1)\tilde{q}(x) \oplus (x^n+1)x\frac{d}{dx}(\tilde{r}(x)) \oplus x^n\tilde{r}(x).\end{aligned}$$

We obtain the expected result by calculating $\frac{d}{dx}[(x^n+1)\tilde{r}(x)]$. □

We now prove that the Nechaev–Gray images of the type (B) codes of odd length n are the binary linear cyclic codes of length $2n$.

Theorem 5. *Let C be a type* (B) *code of odd length n. If Ψ is the Nechaev–Gray map, then the binary code $\Psi(C)$ is a linear cyclic code of length $2n$.*

More precisely, if $C = \langle \tilde{a}(x)\tilde{b}(x)\rangle_2^n + 2\langle \tilde{a}(x)\rangle_2^n$, then,

$$\Psi(C) = \langle \tilde{a}(x)^2\tilde{b}(x)\rangle_2^{2n}.$$

Proof. If $\mathscr{C}_1 = \langle \tilde{a}(x)\rangle_2^n$ and $\mathscr{C}_2 = \langle \tilde{a}(x)\tilde{b}(x)\rangle_2^n$, it is easy to prove that $\mathscr{C}_1 + 2\mathscr{C}_2$ is a direct sum. The cardinality of C is $|C| = |\mathscr{C}_1||\mathscr{C}_2| = 4^{\deg \tilde{c}(x)}2^{\deg \tilde{b}(x)}$ which also is the cardinality of $\langle \tilde{a}(x)^2\tilde{b}(x)\rangle_2^{2n}$. Because Ψ is a bijective map, we deduce that $|\Psi(C)| = |\langle \tilde{a}(x)^2\tilde{b}(x)\rangle_2^{2n}|$. Thus, we just need to prove that $\Psi(C) \subseteq \langle \tilde{a}(x)^2\tilde{b}(x)\rangle_2^{2n}$.

A typical word of C can be written as $f(x) = \tilde{\lambda}(x)\tilde{a}(x)\tilde{b}(x) + 2\tilde{\mu}(x)\tilde{a}(x)$ with $\tilde{\lambda}(x)$ and $\tilde{\mu}(x)$ in $\mathscr{A}_2(n)$ and where the products are calculated in $\mathscr{A}_2(n)$. Let $\tilde{c}(x)$ be such that $x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x)$ in $\mathbb{F}_2[x]$. Since $\frac{d}{dx}[\tilde{a}(x)^2\tilde{b}(x)^2] = 0$, then by applying Lemma 4 with $\tilde{r}(x) = \tilde{\lambda}(x)\tilde{a}(x)\tilde{b}(x)$ and $\tilde{q}(x) = \tilde{\mu}(x)\tilde{a}(x)$ we find:

$$\Psi(f(x)) = \tilde{\mu}(x)\tilde{a}(x)^2\tilde{b}(x)\tilde{c}(x) \oplus x\tilde{a}(x)^2\tilde{b}(x)^2\frac{d}{dx}[\tilde{\lambda}(x)\tilde{c}(x)]$$

and this means that $\Psi(f(x))$ belongs to $\langle \tilde{a}(x)^2\tilde{b}(x)\rangle_2^{2n}$. □

Corollary 6. *The set of binary linear cyclic codes of length $2n$, n odd, is the set of Nechaev–Gray images of the type* (B) *codes of length n.*

Proof. We just have to remark that any divisor of $x^{2n} - 1$ in $\mathbb{F}_2[x]$ with n odd, can be written as $\tilde{a}(x)^2\tilde{b}(x)$ where $\tilde{a}(x)\tilde{b}(x)$ divides $x^n - 1$ (possibly $\tilde{a}(x)$ or $\tilde{b}(x)$ or both equal to 1). □

Recall that if $\tilde{U}$ and $\tilde{V}$ are two binary linear codes of length n then the $|u \mid u+v|$ image of $(\tilde{U}, \tilde{V})$ is $\{(u, u \oplus v) | u \in U, v \in V\}$ which is a binary linear code of length $2n$.

We now prove that any binary linear cyclic code of length $2n$, n odd, is a $|u \mid u+v|$ image.

As before, if $\tilde{m}(x) \in \mathscr{A}_2(n)$ then $O(\tilde{m}(x))$ denotes the odd part of $\tilde{m}(x)$.

Remark that if $\tilde{E}$ is a linear binary code then $O(\tilde{E})$ also is a linear binary code.

Corollary 7. *With the notation above, define*

$$\tilde{C}_1 = \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n, \quad \tilde{C}_2 = \langle \tilde{a}(x) \rangle_2^n \quad \textit{and} \quad \tilde{D} = \tilde{C}_2 \oplus O(\tilde{C}_1).$$

Then,

$$\langle \tilde{a}(x)^2 \tilde{b}(x) \rangle_2^{2n} \textit{ is the } |u \,|\, u+v| \textit{ image of } (\tilde{D}, \tilde{C}_1).$$

Proof. Remember that if $f(x) = \tilde{r}(x) + 2\tilde{q}(x)$ then $\Psi(f(x)) = \Phi(f(-x))$ and $f(-x) = \tilde{r}(x) + 2(\tilde{q}(x) \oplus O(\tilde{r})(x))$. With $\tilde{d}(x) = \tilde{q}(x) \oplus O(\tilde{r})(x)$, we deduce from the definition of Φ that $\Psi(f(x)) = \tilde{d}(x) \oplus x^n(\tilde{d}(x) \oplus \tilde{r}(x)$.

Now if $\tilde{r}(x) \in \tilde{C}_1$ and $\tilde{q}(x) \in \tilde{C}_2$ then the right side of the above equality is the polynomial representation of the $|u \,|\, u+v|$ image of a member of $(\tilde{D}, \tilde{C}_1)$. The final result is obtained by using Theorem 5. □

Remark. Comparison with [6].

In [6] it is shown that $\langle \tilde{a}(x)^2 \tilde{b}(x) \rangle_2^{2n}$ is equivalent to the $|u \,|\, u+v|$ image of $(\tilde{C}_2, \tilde{C}_1)$. Actually, with the notation above it can be seen from the definitions that this equivalence is obtained by using the Nechaev permutation π because $\Psi = \pi\Phi$ and $\Phi(f(x)) = \tilde{q}(x) \oplus x^n(\tilde{q}(x) \oplus \tilde{r}(x))$.

The improvement here is, on the one hand that $\langle \tilde{a}(x)^2 \tilde{b}(x) \rangle_2^{2n}$ is exactly the $|u \,|\, u+v|$ image (and not only equivalent to) and on the other hand, is the Nechaev–Gray image of $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2\langle \tilde{a}(x) \rangle_2^n$. This last point will be useful in the sequel.

2.2. $\mathbb{Z}_4$-linearity of type (B) codes

As was already said, in general type (B) codes are not linear. The following result characterizes their linearity and solves P_1 and P_2.

Theorem 8. *Let n be odd and let* $\tilde{a}(x)$, $\tilde{b}(x), \tilde{c}(x)$ be in $\mathbb{F}_2[x]$ *such that* $x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x)$.

The Hensel lifts of $\tilde{a}(x)$, $\tilde{b}(x), \tilde{c}(x)$ *are* $a(x)$, $b(x)$, $c(x)$.

Let $\tilde{e}(x)$ *be such that* $x^n - 1 = (\tilde{c} \circledast \tilde{c})(x)\tilde{e}(x)$ *in* $\mathbb{F}_2[x]$.

The conditions below are equivalent:

(1) $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2\langle \tilde{a}(x) \rangle_2^n$ *is a linear code.*

(2) $\tilde{a}(x)$ *divides* $\tilde{e}(x)$ *in* $\mathbb{F}_2[x]$.

(3) $\langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n + 2\langle \tilde{a}(x) \rangle_2^n = \langle a(x)(b(x)+2) \rangle_4^n$.

Proof. Notations: $\tilde{C}_1 = \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n$, $\tilde{C}_2 = \langle \tilde{a}(x) \rangle_2^n$ and $C = \tilde{C}_1 + 2\tilde{C}_2$.

If C is a $\mathbb{Z}_4$-linear code then Fact 1 gives $\tilde{C}_1 * \tilde{C}_1 \subseteq \tilde{C}_2$ and this implies (2), according to Fact 3.

Again from Fact 3, if (2) is true then $\Psi(\langle a(x)(b(x)+2) \rangle_4^n) = \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}$.

Applying Theorem 5 we also have : $\Psi(C) = \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}$. Since Ψ is a bijective map, it follows that $\langle a(x)(b(x)+2) \rangle_4^n = C$ and (3) is satisfied. Obviously, (3) implies (1). □

Remarks. (a) If one of the conditions of the Theorem is true then (Fact 3),

$$\Psi(\langle a(x)b(x) + 2a(x) \rangle_4^n) = \langle \tilde{a}(x)^2\tilde{b}(x) \rangle_2^{2n}.$$

(b) In order to solve P_1, condition (2) above is better than condition (1) of Fact 1, which is not easy to check.

3. A family of $\mathbb{Z}_4$-self-dual linear cyclic codes

We now characterize codes of the form $C = \tilde{C}_1 + 2\tilde{C}_2$, where $\tilde{C}_1$ and $\tilde{C}_2$ are binary linear cyclic codes, such that C is a $\mathbb{Z}_4$-self-dual linear code. It will be necessary, first, to set some preliminaries.

Definition 9. Let $\tilde{C}$ be a binary code and let s be any integer, $s \geqslant 1$. The code $\tilde{C}$ is said to be s-divisible if for every word c of $\tilde{C}$, the weight of c is divisible by s.

The following lemma is the binary version of Mc Eliece's Theorem (see for instance [9, Theorem 3.20, p. 1015]).

Lemma 10. *Let $\tilde{C}$ be a binary linear cyclic code of odd length n with generator $\tilde{g}(x)$ and check polynomial $\tilde{h}(x)$ (that is $x^n - 1 = \tilde{g}(x)\tilde{h}(x)$ in $\mathbb{F}_2[x]$). Let R be the set of roots of $\tilde{h}(x)$ in the splitting field of $x^n - 1$ over $\mathbb{F}_2[x]$. If t is the smallest integer such that $\beta_1\beta_2\cdots\beta_t = 1$ where $\beta_1, \beta_2, \dots, \beta_t$ are in R, then $\tilde{C}$ is 2^{t-1}-divisible and is not 2^t-divisible.*

As a consequence of the previous lemma we have the next corollary.

Corollary 11. *With the above notations, let $\tilde{h}^*(x)$ be the reciprocal polynomial of $\tilde{h}(x)$. The code $\tilde{C}$ is 2^s-divisible with $s \geqslant 3$ if and only if $((\tilde{h} \circledast \tilde{h})(x), \tilde{h}^*(x)) = 1$.*

Proof. Let $R^{\circledast}$ be the set of roots of $(\tilde{h} \circledast \tilde{h})(x)$ and let R^* be the set of roots of $\tilde{h}^*(x)$. Recall that $\beta \in R$ if and only if $\beta^{-1} \in R^*$. If $\tilde{C}$ is 2^s-divisible with $s \geqslant 3$, then the smallest

t such that $\beta_1\beta_2\cdots\beta_t = 1$ is at least 4, because if $t \leqslant 3$ then by the lemma, $\tilde{C}$ will be at most 2^2-divisible. Consequently, $\tilde{C}$ is 2^s-divisible with $s \geqslant 3$ if and only if the smallest t such that $\beta_1\beta_2\cdots\beta_t = 1$ is at least 4 or equivalently, if and only if there do not exist $\beta_i, \beta_j, \beta_k \in R$ such that $\beta_k^{-1} \in R^*$ and : $\beta_i\beta_j = \beta_k^{-1}$ or $\beta_i = \beta_k^{-1}$ or $\beta_i = 1 \in R^*$. Clearly this last condition happens if and only if $R^{\circledast} \cap R^* = \phi$, in other words if and only if $((h \circledast h)(x), \tilde{h}^*(x)) = 1$. □

We are now in position to state the expected characterization.

Theorem 12. *Let $\tilde{C}_1$ and $\tilde{C}_2$ be two binary linear cyclic codes of odd length n. Then the code $C = \tilde{C}_1 + 2\tilde{C}_2$ is a $\mathbb{Z}_4$-self-dual linear code if and only if*

$$\tilde{C}_2 = \tilde{C}_1^{\perp} \quad \textit{and} \quad \tilde{C}_1 \textit{ is } 8\textit{-divisible.}$$

Proof. If C is a $\mathbb{Z}_4$-linear code, then according to Remark (1) which follows from Fact 1, C is a type (B) code. There exist binary polynomials $\tilde{a}(x)$, $\tilde{b}(x)$, $\tilde{c}(x)$, with $a(x)$, $b(x)$, $c(x)$ as their corresponding Hensel lifts, such that

$$x^n - 1 = \tilde{a}(x)\tilde{b}(x)\tilde{c}(x) \quad \text{in } \mathbb{F}_2[x], \tilde{C}_1 = \langle \tilde{a}(x)\tilde{b}(x) \rangle_2^n, \tilde{C}_2 = \langle \tilde{a}(x) \rangle_2^n.$$

Furthermore, since C is linear Theorem 8 implies $C = \langle a(x)b(x) + 2a(x) \rangle_4^n$.

Now, if C is a self-dual $\mathbb{Z}_4$-code then $c^*(x) = a(x)$ (see for example [8]). Thus $\tilde{c}^*(x) = \tilde{a}(x)$ and therefore $\tilde{C}_2 = \tilde{C}_1^{\perp}$. On the other hand, if $c^*(x) = a(x)$ then by condition (2) in Theorem 8 we know that $c^*(x)$ divides $\tilde{e}(x)$ which proves that $((c \circledast c)(x), c^*(x)) = 1$. By Corollary 11 we conclude that $\tilde{C}_1$ is 8-divisible.

Conversely, define two binary polynomials $\tilde{g}(x)$ and $\tilde{h}(x)$ such that $x^n - 1 = \tilde{g}(x)\tilde{h}(x)$ in $\mathbb{F}_2[x]$, $\tilde{C}_1 = \langle \tilde{g}(x) \rangle_2^n$, $\tilde{C}_2 = \tilde{C}_1^{\perp} = \langle \tilde{h}^*(x) \rangle_2^n$ and assume that $\tilde{C}_1$ is 8-divisible.

From Corollary 11 we know that $(h \circledast h)(x)$ and $\tilde{h}^*(x)$ have no common roots. Therefore, if $x^n - 1 = (h \circledast h)(x)\tilde{e}(x)$ then $\tilde{h}^*(x)$ divides both $\tilde{e}(x)$ and $\tilde{g}(x)$. Now applying Theorem 8 with $\tilde{a}(x) = \tilde{h}^*(x)$, $\tilde{c}(x) = \tilde{h}(x)$ and $\tilde{b}(x)$ defined by $\tilde{g}(x) = \tilde{h}^*(x)\tilde{b}(x)$, it follows that C satisfies condition (2) of this theorem and thus C is a $\mathbb{Z}_4$-linear code and is also equal to $\langle a(x)b(x) + 2a(x) \rangle_4^n$. Its dual code is $\langle c^*(x)b^*(x) + 2c^*(x) \rangle_4^n$. Since $\tilde{c}^*(x) = \tilde{a}(x)$, and consequently $\tilde{b}^*(x) = \tilde{b}(x)$, we have $c^*(x) = a(x)$ and $b^*(x) = b(x)$ and this means that $C^{\perp} = C$. □

Corollary 13. *Let $\tilde{C}_1$ and $\tilde{C}_2$ be two linear cyclic binary codes of odd length n and minimum distances d_1 and d_2, respectively.*

If $C = \tilde{C}_1 + 2\tilde{C}_2$ is a $\mathbb{Z}_4$-self-dual linear code of odd length n then its Nechaev–Gray image $\Psi(C)$ is a $\mathbb{F}_2$-self-dual linear cyclic code of length 2n and minimum distance $min(d_1, 2d_2)$.

Proof. The proof of Theorem 12 shows that $\Psi(C) = \langle \tilde{a}(x)^2 \tilde{b}(x) \rangle_2^{2n}$ with $\tilde{a}(x) = \tilde{c}^*(x)$ and $\tilde{b}(x) = \tilde{b}^*(x)$. Since $x^{2n} - 1 = \tilde{a}(x)^2 \tilde{b}(x)^2 \tilde{c}(x)^2$, the generator of $\Psi(C)^\perp$ is $\tilde{c}^*(x)^2 \tilde{b}^*(x)$ which also is the generator of $\Psi(C)$. Hence $\Psi(C) = \Psi(C)^\perp$.

On the other hand, by the remark after Corollary 7, the code $\Psi(C)$ is equivalent to the $|u \,|\, u+v|$ image of $(\tilde{C}_2, \tilde{C}_1)$. It is well known (see [7], p. 76) that the minimum distance of such an image is $\min(d_1, 2d_2)$. □

Remark. Theorem 12 and Corollary 13 present a generalization of results of [10] where examples of $\tilde{C}_1 + 2\tilde{C}_2$ which are $\mathbb{Z}_4$-self-dual linear code are introduced. Proposition 4.2 in [10] only gives the "if" part of Theorem 12 in the special case of irreducible cyclic codes.

Corollary 14. *If $\tilde{C}$ is the dual code of the 2-correcting BCH binary code of length $2^m - 1$ with $m \geqslant 5$ if m is odd and $m \geqslant 8$ if m is even, then $\tilde{C} + 2\tilde{C}^\perp$ is a $\mathbb{Z}_4$-self-dual linear code.*

Proof. As we can see in [7, p. 451, 452], the code $\tilde{C}$ is 8-divisible. □

Remark. In Chapter 15 of [7] we can find other examples of 8-divisible codes.

4. Conclusions

In this paper, it was shown that all binary linear cyclic codes of length $2n$ with n odd, are Nechaev–Gray images of $\mathbb{Z}_4$-cyclic codes constructed by using binary linear cyclic codes of length n. They have been typically divided into two classes since we can distinguish which are Nechaev–Gray map images of linear cyclic codes over $\mathbb{Z}_4$, from those which are only Nechaev–Gray map images of nonlinear cyclic codes over $\mathbb{Z}_4$. This gives another classification of all linear cyclic codes of length n over $\mathbb{Z}_4$,depending on whether the Nechaev–Gray images of these codes are linear or not.

In the final part of this work we have presented a new method for constructing $\mathbb{Z}_4$-self-dual linear cyclic codes by means of 8-divisible binary linear cyclic codes.

An open problem now is to consider what happens when n is an even number. Only few partial results are known regarding the study of $\mathbb{Z}_4$-linear cyclic codes in this case (see [13]). Another question is if the methods and results of this paper could be extended to codes over $\mathbb{Z}_{p^t}$ with p prime by using generalized Gray maps (for example see [14–17]).

Acknowledgments

The authors thank the Universidad Autónoma Metropolitana, unidad Iztapalapa, where part of this work was done.

References

[1] N. Aydin, D.K. Ray-Chaudhuri, Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes, IEEE Trans. Inform. Theory 48 (2002) 2065–2069.

[2] S. Bouyuklieva, Some results of type IV codes over $\mathbb{Z}_4$ and some new binary codes, IEEE Trans. Inform. Theory 48 (2002) 768–773.

[3] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, Designs, Codes Cryptogr. 6 (1) (1995) 21–35.

[4] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.

[5] P. Kanwar, S.R. López-Permouth, Cyclic codes over the integers modulo p^m, Finite Fields their Appl. 3 (1997) 334–352.

[6] J.H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (1991) 343–345.

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

[8] V.S. Pless, Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 42 (1996) 1594–1600.

[9] V.S. Pless, W.C. Huffman, Handbook of Coding Theory, Elsevier, Amsterdam, 1998.

[10] V.S. Pless, P. Solé, Z. Qian, Cyclic self-dual $\mathbb{Z}_4$-codes, Finite Fields their Appl. 3 (1997) 48–69.

[11] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (1999) 2527–2532.

[12] J. Wolfmann, Binary images of cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 47 (2001) 1773–1779.

Cyclic codes of even length over $\mathbb{Z}_4$

[13] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, Proceedings of the International Workshop on Coding and Cryptography, WCC 2001, Paris, France, 2001, pp. 83–92.

Codes over $\mathbb{Z}_{p^t}$ and Generalized Gray map

[14] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, IEEE Trans. Inform. Theory 44 (1998) 1543–1547.

[15] M. Greferath, E. Schidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, IEEE Trans. Inform. Theory 45 (1999) 2522–2524.

[16] S. Ling, J.T. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, IEEE Trans. Inform. Theory 48 (2002) 2592–2605.

[17] H. Tapia-Recillas, G. Vega, Some constacyclic codes over $\mathbb{Z}_{2^k}$ and binary quasi-cyclic codes, Discrete Appl. Math. 128 (2003) 305–316.