There is exactly one $\mathbb{Z}_2\mathbb{Z}_4$-cyclic 1-perfect code

Joaquim Borges and Cristina Fernández-Córdoba

Abstract

Let $C$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of length $n > 3$. We prove that if the binary Gray image of $C$, $C = \Phi(C)$, is a 1-perfect nonlinear code, then $C$ cannot be a $\mathbb{Z}_2\mathbb{Z}_4$-cyclic code except for one case of length $n = 15$. Moreover, we give a parity check matrix for this cyclic code. Adding an even parity check coordinate to a $\mathbb{Z}_2\mathbb{Z}_4$-additive 1-perfect code gives an extended 1-perfect code. We also prove that any such code cannot be $\mathbb{Z}_2\mathbb{Z}_4$-cyclic.

Index Terms

Perfect codes, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, simplex codes.

I. INTRODUCTION

A $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C$ is the binary Gray image of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $C \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, and if $\beta = 0$, then $C$ is a binary linear code. If $\alpha = 0$, then $C$ is called $\mathbb{Z}_4$-linear. In 1997, a first family of $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect codes was presented in [11] in the more general context of translation-invariant propelinear codes. Lately, in 1999, all $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect codes were fully classified in [6]. Specifically, for every appropriate values of $\alpha$ and $\beta$, there exists exactly one $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect code $C$. Note that when $\beta = 0$, then $C$ is a Hamming code. In subsequent papers ( [5] and [9]), $\mathbb{Z}_2\mathbb{Z}_4$-linear extended 1-perfect codes were also classified. But it was not until 2010, when an exhaustive description of general $\mathbb{Z}_2\mathbb{Z}_4$-linear codes appeared [3]. More recently, in 2014, $\mathbb{Z}_2\mathbb{Z}_4$-cyclic codes have been defined in [1], and also studied in [4].

After all these papers, a natural question is to ask for the existence or nonexistence of $\mathbb{Z}_2\mathbb{Z}_4$-cyclic 1-perfect codes, of course, excluding the linear (Hamming) case when $\beta = 0$. In this paper, we show that such codes do not exist with only one exception. This unique $\mathbb{Z}_2\mathbb{Z}_4$-cyclic 1-perfect code has binary length 15, with $\alpha = 3$ and $\beta = 6$. We also give a parity check matrix for such code. If we add an even parity check coordinate to a $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect code, then we obtain a $\mathbb{Z}_2\mathbb{Z}_4$-linear extended 1-perfect code. We show that none of these codes can be $\mathbb{Z}_2\mathbb{Z}_4$-cyclic.

Manuscript received Month day, year; revised Month day, year.

J. Borges is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: joaquim.borges@uab.cat)

C. Fernández-Córdoba is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: cristina.fernandez@uab.cat).

This work has been partially supported by the Spanish MICINN grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.
The paper is organized as follows. In the next section, we give basic definitions and properties. Moreover, we give the type of all $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect codes, computing some parameters that were not specified in [6]. In Section III, we give the main results of this paper. First, we prove that in a $\mathbb{Z}_2\mathbb{Z}_4$-cyclic 1-perfect code, $\beta$ must be a multiple of $\alpha$. This, immediately excludes a lot of cases. For the remaining ones, using a key property of simplex codes, we prove that $\alpha$ cannot be greater than 3. Therefore, finally, we have only one possible case when $\alpha = 3$ and $\beta = 6$. In Example 3.2 we give a parity check matrix for this code in a cyclic form. In Section IV we prove that a $\mathbb{Z}_2\mathbb{Z}_4$-linear extended 1-perfect code, with $\alpha > 0$, cannot be $\mathbb{Z}_2\mathbb{Z}_4$-cyclic.

II. Preliminaries

Denote by $\mathbb{Z}_2$ and $\mathbb{Z}_4$ the rings of integers modulo 2 and modulo 4, respectively. A binary code of length $n$ is any non-empty subset $C$ of $\mathbb{Z}_2^n$. If that subset is a vector space then we say that it is a linear code. Any non-empty subset $C$ of $\mathbb{Z}_4^n$ is a quaternary code of length $n$, and an additive subgroup of $\mathbb{Z}_4^n$ is called a quaternary linear code. The elements of a code are usually called codewords.

Given two binary vectors $u, v \in \mathbb{Z}_2^n$, the (Hamming) distance between $x$ and $y$, denoted $d(u, v)$, is the number of coordinates in which they differ. The (Hamming) weight of any vector $z \in \mathbb{Z}_2^n$, $w(z)$, is the number of nonzero coordinates of $z$. The Lee weights of any vector $z \in \mathbb{Z}_2^n$, $w_L(z)$, is the rational sum of the Lee weights of its components. If $a, b \in \mathbb{Z}_4^n$, then the Lee distance between $a$ and $b$ is $d_L(a, b) = w_L(a - b)$. For a vector $u \in \mathbb{Z}_2^n \times \mathbb{Z}_4^\beta$ we write $u = (u | u')$ where $u \in \mathbb{Z}_2^n$ and $u' \in \mathbb{Z}_4^\beta$. The weight of $u$ is $w(u) = w(u) + w_L(u')$. If $u, v \in \mathbb{Z}_2^n \times \mathbb{Z}_4^\beta$, the distance between $u = (u | u')$ and $v = (v | v')$ is defined as $d(u, v) = d(u, v) + d_L(u', v')$. The classical Gray map $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ is defined by

$$\phi(0) = (0, 0), \quad \phi(1) = (0, 1), \quad \phi(2) = (1, 1), \quad \phi(3) = (1, 0).$$

If $a = (a_1, \ldots, a_m) \in \mathbb{Z}_4^m$, then the Gray map of $a$ is the coordinatewise extended map $\phi(a) = (\phi(a_1), \ldots, \phi(a_m))$.

We naturally extend the Gray map for vectors $u = (u | u') \in \mathbb{Z}_2^n \times \mathbb{Z}_4^\beta$ so that $\Phi(u) = (u | \phi(u'))$. Clearly, the Gray map transforms Lee distances and weights to Hamming distances and weights. Hence, if $u, v \in \mathbb{Z}_2^n \times \mathbb{Z}_4^\beta$, we have that $d(u, v) = d(\Phi(u), \Phi(v))$.

A binary code $C$ of length $n$ is called 1-perfect if any vector not in $C$ is at distance one from exactly one codeword in $C$. Such codes have minimum distance 3 between any pair of codewords, and the cardinality is $|C| = 2^n/(n + 1)$.

It is well known that $n = 2^t - 1$, for some $t \geq 2$ and hence $|C| = 2^{2^t-t-1}$. For any $t$, there is exactly one linear 1-perfect code, up to coordinate permutation, which is called the Hamming code. An extended 1-perfect code $C'$ is obtained by adding an even parity check coordinate to a 1-perfect code $C$. In this case, $C'$ has minimum distance 4, length $n + 1 = 2^t$, and size $|C'| = 2^{2^t-t-1}$.

The dual of a binary Hamming code is a constant weight code called simplex. The dual of an extended Hamming code is a linear Hadamard code. In this paper, we make use of two important properties [8], [10]:

(a) A binary Hamming code is cyclic, that is, its coordinates can be arranged such that the cyclic shift of any codeword is again a codeword. Therefore, simplex codes are also cyclic.
(b) An extended Hamming code of length greater than 4 is not cyclic. Hence, a linear Hadamard code of length greater than 4 is not cyclic.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $C$ is an additive subgroup of $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$. Such codes are extensively studied in \cite{3}. Since $C$ is a subgroup of $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, it is also isomorphic to a group $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$. Therefore, $C$ is of type $2^{\gamma+\delta}$ as a group, it has $|C| = 2^{\gamma+\delta}$ codewords, and the number of codewords of order less than two in $C$ is $2^{\gamma+\delta}$.

Let $X$ (respectively $Y$) be the set of $\mathbb{Z}_2$ (respectively $\mathbb{Z}_4$) coordinate positions, so $|X| = \alpha$ and $|Y| = \beta$. Unless otherwise stated, the set $X$ corresponds to the first $\alpha$ coordinates and $Y$ corresponds to the last $\beta$ coordinates. Call $C_X$ (respectively $C_Y$) the punctured code of $C$ by deleting the coordinates outside $X$ (respectively $Y$), and removing repeated codewords, if necessary. Let $C_b$ be the subcode of $C$ which contains all order two codewords and the zero codeword. Let $\kappa$ be the dimension of $(C_b)_X$, which is a binary linear code.

According to \cite{3}, and considering all these parameters, we say that $C$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. The binary Gray image of $C$ is $C = \Phi(C) = \{\Phi(x) \mid x \in C\}$. In this case, $C$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and its length is $n = \alpha + 2\beta$.

The standard inner product in $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, defined in \cite{3}, can be written as

$$\mathbf{u} \cdot \mathbf{v} = 2 \left( \sum_{i=1}^{\alpha} u_i v_i \right) + \sum_{j=1}^{\beta} u_j' v_j' \in \mathbb{Z}_4,$$

where the computations are made taking the zeros and ones in the $\alpha$ binary coordinates as quaternary zeros and ones, respectively. The dual code of $C$, is defined in the standard way by

$$C^\perp = \{ \mathbf{v} \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \mid \mathbf{u} \cdot \mathbf{v} = 0, \text{ for all } \mathbf{u} \in C \}.$$

The types of dual codes are related in \cite{3}.

**Proposition 2.1 (\cite{3}):** If $C$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then its dual code $C^\perp$ is of type $(\alpha, \beta; \alpha + \gamma - 2\kappa, \beta - \gamma - \delta + \kappa; \alpha - \kappa)$. 

Let $C$ be a $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect code. Then, the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\Phi^{-1}(C)$ is also called 1-perfect code. Such codes are completely characterized.

**Proposition 2.2 (\cite{6}):**

(i) Let $n = 2^t - 1$, where $t \geq 4$. Then, for every $r$ such that $2 \leq r \leq t \leq 2r$, there is exactly one $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect code of length $n$, up to coordinate permutation, with parameters $\alpha = 2^r - 1$ and $\beta = 2^{t-1} - 2^{r-1}$.

(ii) There are no other $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect codes.

Here, we strengthen a little this result by computing the type of these codes. Since $r$ and $t$ completely determine a $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect code, we denote such code by $C_{r,t}$. The corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive code is $C_{r,t} = \Phi^{-1}(C_{r,t})$.

**Proposition 2.3:** Let $C_{r,t}$ be of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and let $(C_{r,t})^\perp$ be the dual code of type $(\bar{\alpha}, \bar{\beta}; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$. Then,
(i) The parameters of $C_{r,t}$ are:
\[
\alpha = 2^r - 1; \quad \beta = 2^{t-1} - 2^{r-1}; \\
\gamma = 2^r - 1 - 2r + t; \\
\delta = 2^{t-1} - 2^{r-1} + r - t; \\
\kappa = \gamma.
\]

(ii) The parameters of $(C_{r,t})^\perp$ are:
\[
\bar{\alpha} = \alpha; \quad \bar{\beta} = \beta; \\
\bar{\gamma} = 2r - t; \quad \bar{\delta} = t - r; \\
\bar{\kappa} = \bar{\gamma}.
\]

Proof: The parameters $\alpha$, $\beta$, $\bar{\alpha}$ and $\bar{\beta}$ follow directly from Proposition 2.1.

On the one hand, the binary linear code $C_0 = \langle \{x \mid 0, \ldots, 0 \in C_{r,t}\} \rangle_X$ is clearly 1-perfect, i.e. a Hamming code. Hence, $C_0$ has dimension $2^r - r - 1$. This means that the zero codeword in $(C_{r,t})^\perp$ (and any other one) is repeated $2^{2^r-r-1}$ times in $C_{r,t}$. On the other hand, consider a vector of the form
\[
u = (u \mid u') = (0, \ldots, 0 \mid 0, \ldots, 0, 2, 0, \ldots, 0) \in \mathbb{Z}_2^2 \times \mathbb{Z}_4^4,
\]
where $\alpha = 2^r - 1$ and $\beta = 2^{t-1} - 2^{r-1}$. Since the minimum distance in $C_{r,t}$ is 3, the minimum weight is also 3 because $C_{r,t}$ is distance invariant [11]. Hence $\nu$ must be at distance one from a weight 3 codeword $x = (x \mid x')$, where $w(x) = 1$ and $x' = u'$. Indeed, if $w(x) = 0$ and $w(x') = 3$, then $2x$ would have weight 2. Therefore, $(C_{r,t})^\perp$ has $2^\beta$ distinct codewords of order two (including here the zero codeword). We conclude that $C_{r,t}$ has $2^\beta \cdot 2^{2^r-r-1}$ order two codewords (again, including the zero codeword). Thus, the dimension of $(C_{r,t})^\perp$ is
\[
\gamma + \delta = \beta + 2^r - r - 1 = 2^{t-1} + 2^{r-1} - r - 1.
\]

The size of $C_{r,t}$ is $2^{2^r-t-1}$. Therefore,
\[
\gamma + 2\delta = 2^t - t - 1.
\]

Combining Equations [1] and [2] we obtain the values of $\gamma$ and $\delta$.

As can be seen in [6], the quotient group $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta / C_{r,t}$ is isomorphic to $\mathbb{Z}_2^{2^r-t} \times \mathbb{Z}_4^{t-1}$. In other words, $C_{r,t}^\perp$ has parameters $\bar{\gamma} = 2r - t$ and $\bar{\delta} = t - r$. Now, the values of $\kappa$ and $\bar{\kappa}$ are easily obtained by applying Proposition 2.1.

Let $v = (v_1, \ldots, v_m)$ be an element in $\mathbb{Z}_2^m$ or $\mathbb{Z}_4^m$. We denote by $\sigma(v)$ the right cyclic shift of $v$, i.e. $\sigma(v) = (v_m, v_1, \ldots, v_{m-1})$. We recursively define $\sigma^j(v) = \sigma(\sigma^{j-1}(v))$, for $j = 2, 3, \ldots$. For vectors $\nu = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ we extend the definition of $\sigma$ as the double right cyclic shift of $\nu$, that is, $\sigma(\nu) = (\sigma(u) \mid \sigma(u'))$.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $C \subseteq \mathbb{Z}_2^2 \times \mathbb{Z}_4^4$ is a $\mathbb{Z}_2\mathbb{Z}_4$-cyclic code if for each codeword $x \in C$, we have that $\sigma(x) \in C$. Such codes were first defined in [1] and also studied in [4]. As can be seen in [1], the dual of a $\mathbb{Z}_2\mathbb{Z}_4$-cyclic code is also $\mathbb{Z}_2\mathbb{Z}_4$-cyclic.
III. THERE IS NO NONTRIVIAL $\mathbb{Z}_2\mathbb{Z}_4$-CYCLIC PERFECT CODES WITH ONE EXCEPTION

We say that a code is nontrivial if it has more than two codewords and its minimum distance is $d > 1$. Apart from 1-perfect codes, there is only another nontrivial binary perfect code. It is the linear binary Golay code of length 23. But this code has not any $\mathbb{Z}_2\mathbb{Z}_4$-linear structure apart from the binary linear one [12]. Therefore, any binary nonlinear and nontrivial $\mathbb{Z}_2\mathbb{Z}_4$-linear perfect code is a 1-perfect code.

In this section, we prove that for any $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect code, which is not a Hamming code, its corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive code cannot be $\mathbb{Z}_2\mathbb{Z}_4$-cyclic with exactly one exception.

**Proposition 3.1:** If $C_{r,t}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-cyclic 1-perfect code, then $t = r$ or $t = 2r$.

**Proof:** By the argument in the proof of Proposition 2.3, we may assume that $C_{r,t}$ contains a codeword of the form $x = (x \mid 2, 0, \ldots, 0)$ with $w(x) = 1$. Now, consider the codeword $z = \sigma^\beta(x)$. If $z \neq x$ then $z + x$ would have weight 2. Consequently, $z$ must be equal to $x$ implying that $\beta$ is a multiple of $\alpha$, that is, $2^t - 1 \leq 2^r - 1$ is a multiple of $2^r - 1$. Thus,

$$\frac{2^{t-1}(2^t - 1)}{2^r - 1} \in \mathbb{N} \implies \frac{(2^t - 1)}{2^r - 1} \in \mathbb{N}.$$ 

Therefore $r$ divides $t - r$ implying that $r$ divides $t$. Since $r \leq t \leq 2r$, the only possibilities are $t = r$ or $t = 2r$. 

If $t = r$, then $C_{r,t} = \Phi(C_{r,t})$ is linear, i.e. a Hamming code. In effect, it is well known that its coordinates can be arranged such that it is a binary cyclic code. We are interested in those codes whose binary Gray image is not linear, that is, when $t = 2r$. For this case, $t = 2r$, we have that $C_{r,2r}$ is of type

$$(2^r - 1, 2^{r-1}(2^r - 1); 2^r - 1, 2^{r-1}(2^r - 1) - r; 2^r - 1),$$

and applying Proposition 2.3 we obtain that its dual code $C_{r,2r}^\perp$ is of type

$$(2^r - 1, 2^{r-1}(2^r - 1); 0, 0).$$

**Example 3.2:** For $r = 2$ we have that the type of $C_{2,4}$ is $(3, 6; 3, 4; 3)$. By Proposition 2.3 its dual code $C_{2,4}^\perp$ is of type $(3, 6; 0, 2; 0)$. Consider the matrix

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

The matrix $H$ generates a code of type $(3, 6; 0, 2; 0)$. Any column is not a multiple of another one. Hence the code $C_*$ with parity check matrix $H$ has minimum distance at least 3, type $(3, 6; 3, 4; 3)$ and size $2^{11}$. Therefore, $C_*$ is the $\mathbb{Z}_2\mathbb{Z}_4$-additive 1-perfect code $C_{2,4}$ and $H$ generates $C_{2,4}^\perp$. Note that the second row of $H$ is the shift of the first one. Also, the first row minus the second one gives the shift of the second row. Since the shift of any row of $H$ is a codeword, we have that the shift of any codeword is again a codeword. Consequently, $C_{2,4}^\perp$ is a $\mathbb{Z}_2\mathbb{Z}_4$-cyclic code and so is $C_{2,4}$.

From now on, we denote by $D^{(r)}$ the code $C_{r,2r}^\perp$ of binary length $n = \alpha + 2\beta = 2^{2r} - 1$. Hence, $D^{(r)}_b$ is the set of codewords of order 2 and the zero codeword. Recall that the dual of a binary Hamming code is called simplex.
Of course, the coordinates of a simplex code can be arranged such that the code is cyclic. We denote by $S_r$ a cyclic simplex code of length $2^r - 1$.

**Lemma 3.3:** The code $D^{(r)}$ is a constant weight code, where all nonzero codewords have weight $2^{2r-1}$.

**Proof:** The weight distributions of dual codes are related by the MacWilliams identity [7], [11], as well as for binary linear codes. It is well known that any 1-perfect code has the same weight distribution as the Hamming code of the same length. Therefore, $D^{(r)}$ must have the same weight distribution as the simplex code of length $n = 2^{2r} - 1$. Hence, the weight of any nonzero codeword is $(n + 1)/2 = 2^{2r-1}$. ■

**Proposition 3.4:** If $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$-cyclic, then $(D^{(r)})_X = S_r$. Moreover, a codeword $z \in D^{(r)}$ has the zero vector in the $\mathbb{Z}_2$ part, $z = (0, \ldots , 0 | z'_1, \ldots , z'_b)$, if and only if $z \in D^{(r)}_0$.

**Proof:** A generator matrix for $D^{(r)}$ would have the form

$$G = \left( \begin{array}{c|c} G_1 & G_2 \end{array} \right),$$

where $G_1$ is a $r \times 2^r - 1$ generator matrix for $(D^{(r)})_X$. Since the minimum weight of $C_{r,2r}$ is 3, $G_1$ has neither repeated columns, nor the zero column. Therefore $G_1$ has as columns all the nonzero binary vectors of length $r$ and $(D^{(r)})_X = S_r$. The size of $D^{(r)}$ is $|D^{(r)}| = 2^{2r}$ and the number of codewords of order less than or equal to 2 is $|D^{(r)}_0| = 2^r$. Hence, $D^{(r)}$ can be viewed as a set of $2^r$ cosets of $D^{(r)}_0$. We conclude that each codeword in $(D^{(r)})_X$ appears $2^r$ times in $D^{(r)}$. So, the zero codeword in $(D^{(r)})_X$ appears in $D^{(r)}$ exactly in the codewords of $D^{(r)}_0$. ■

**Proposition 3.5:** Suppose that $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$-cyclic. If we change the coordinates ‘2’ by ‘1’ in $(D^{(r)}_b)_Y$ we obtain $2^{r-1}$ copies of $S_r$.

**Proof:** Clearly, when we change the twos by ones in $(D^{(r)}_b)_Y$, we obtain a binary linear cyclic code $D$ with constant weight and dimension $r$. By [2], $D$ must be a simplex code or a replication of a simplex code. Since the dimension is $r$, we conclude that $D$ is a replication of a simplex code of length $2^r - 1$. Moreover, since $(D^{(r)}_b)_Y$ is cyclic, $D$ is a replication of $S_r$. ■

Therefore, if $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$-cyclic, any order 4 codeword is of the form:

$$z = (x_1, \ldots , x_\alpha \mid y^{(1)}, \ldots , y^{(2^{r-1})}),$$

where $y^{(i)} = (y_1^{(i)}, \ldots , y_\alpha^{(i)})$, for all $i = 1, \ldots , 2^{r-1}$. The set of coordinate positions of $y^{(i)}$ will be called the $i$th block. Taking into account that $2z \in D^{(r)}_b$ and by Proposition 3.5 we see that $z$ has $2^{r-1}$ odd coordinates (i.e. coordinates from $\{1,3\}$) in any block at the same positions. In other words, $y^{(i)} \equiv y^{(j)} \pmod{2}$, for all $i, j = 1, \ldots , 2^{r-1}$.

**Corollary 3.6:** Let $z = (x_1, \ldots , x_\alpha \mid y^{(1)}, \ldots , y^{(2^{r-1})}) \in D^{(r)}$ be an order 4 codeword and assume that $D^{(r)}$ is...
\[ Z_2Z_4 \text{-cyclic. Then, } (y^{(1)}, \ldots, y^{(2r-1)}) \text{ has:} \]

\[
\begin{align*}
2^{2r-2} & \quad \text{odd coordinates} \\
2^{r-2}(2^{r-1} - 1) & \quad \text{twos, and} \\
2^{r-2}(2^{r-1} - 1) & \quad \text{zeroes.}
\end{align*}
\]

**Proof:** The result follows from Lemma 3.3, Proposition 3.4 and Proposition 3.5.

For any binary vector \( x = (x_1, \ldots, x_m) \), the support of \( x \) is the set of nonzero positions, \( \text{supp}(x) = \{ i \mid x_i \neq 0 \} \). Note that \( w(x) = |\text{supp}(x)| \). We define \( \overline{\text{supp}}(x) = \{1, \ldots, m\} \setminus \text{supp}(x) \) as the complementary support of \( x \).

**Lemma 3.7:** Let \( S_r \) be a cyclic simplex code of length \( 2^r - 1 \), with \( r > 2 \). For any pair of codewords \( x, y \in S_r \) we have that \( |\text{supp}(x) \cap \text{supp}(y)| \) is even. In other words, \( x \) cannot have an odd number of nonzero positions in \( \overline{\text{supp}}(y) \).

**Proof:** The distance between \( x \) and \( y \) must be \( 2^{r-1} \). Therefore,

\[
d(x, y) = |\text{supp}(x)| + |\text{supp}(y)| - 2|\text{supp}(x) \cap \text{supp}(y)| = 2^{r-1}.
\]

But the weight of any codeword is \( 2^{r-1} \). Thus,

\[
2^{r-1} + 2^{r-1} - 2|\text{supp}(x) \cap \text{supp}(y)| = 2^{r-1},
\]

implying that \( |\text{supp}(x) \cap \text{supp}(y)| = 2^{r-2} \), which is even for \( r > 2 \). Hence, \( |\text{supp}(x) \cap \overline{\text{supp}}(y)| \) is also even for \( r > 2 \).

**Proposition 3.8:** Suppose that \( D^{(r)} \) is \( Z_2Z_4 \)-cyclic and \( r > 2 \). Let \( z = (x_1, \ldots, x_\alpha \mid y^{(1)}, \ldots, y^{(2^{r-1})}) \in D^{(r)} \) be an order 4 codeword. For any distinct \( i, j \), define

\[ N_{i,j} = \{ \ell \mid 1 \leq \ell \leq \alpha, \ y^{(i)}_\ell, y^{(j)}_\ell \in \{0, 2\}, \ y^{(i)}_\ell \neq y^{(j)}_\ell \}, \]

i.e. \( N_{i,j} \) is the set of coordinate positions where \( y^{(i)} \) has a ‘2’ and \( y^{(j)} \) has ‘0’ or vice versa. Then, \( |N_{i,j}| \) is even.

**Proof:** Suppose to the contrary that \( |N_{i,j}| \) is odd. Assume that \( i < j \) and consider the codeword \( v = \sigma^{\alpha(j-1)}(z) \).

Clearly, \( u = v + z \) has the zero vector in the \( Z_2 \) part. Thus, by Proposition 3.4, \( u \) is an order two codeword. Now, comparing with the codeword \( 2v \) (or \( 2z \)), we can see that \( u \) has an odd number of twos in \( \overline{\text{supp}}(2v) \) in the \( j \)th block, contradicting Lemma 3.7.

As a consequence, we obtain that in any order 4 codeword, the number of twos in any block has the same parity.

**Corollary 3.9:** Suppose that \( D^{(r)} \) is \( Z_2Z_4 \)-cyclic and \( r > 2 \). Let \( (x_1, \ldots, x_\alpha \mid y^{(1)}, \ldots, y^{(2^{r-1})}) \in D^{(r)} \) be an order 4 codeword. Put \( \eta_\ell(y) = \{|\ell| 1 \leq \ell \leq \alpha, \ y^{(k)}_\ell = 2\} \). Then, \( \eta_1(y), \ldots, \eta_{2^{r-1}}(y) \) all have the same parity.

**Proof:** Straightforward from Proposition 3.8.

**Lemma 3.10:** Suppose that \( D^{(r)} \) is \( Z_2Z_4 \)-cyclic and \( r > 2 \). As before, let \( z = (x_1, \ldots, x_\alpha \mid y^{(1)}, \ldots, y^{(2^{r-1})}) \in D^{(r)} \) be an order 4 codeword. Then, there exist different \( k, k' \in \{1, \ldots, 2^{r-1}\} \) such that \( \eta_k(y) \neq \eta_{k'}(y) \). Moreover,
if for some \( \ell \in \{1, \ldots, \alpha\} \) we have \( y^{(k)}_\ell = 0 \) and \( y^{(k')}_\ell = 2 \), then

\[
\{ i : 1 \leq i \leq 2^{r-1}, \quad y^{(i)}_\ell = 0 \} = \{ j : 1 \leq j \leq 2^{r-1}, \quad y^{(j)}_\ell = 2 \} = 2^{r-2}.
\]

**Proof:** The total number of twos in \( z \) is \( 2^{r-2}(2^{r-1} - 1) \) (see Corollary 3.6). But this number is not divisible by \( 2^{r-1} \) and hence not all the blocks have the same number of twos. This proves that \( \eta_k(y) \neq \eta_k'(y) \) for some \( k, k' \in \{1, \ldots, 2^{r-1}\} \).

Let \( k \) and \( k' = k + 1 \) be such that \( \eta_k(y) \neq \eta_{k'}(y) \). Without loss of generality, we assume that \( k' = 2^{r-1} \) and \( k = 2^{r-1} - 1 \). After some shifts of \( z \), we can get the situation that \( y^{(k)}_\alpha \neq y^{(k')}_\alpha \), where \( y^{(k)}_\alpha, y^{(k')}_\alpha \in \{0, 2\} \).

That is, the last coordinates of the last two blocks are in \( \alpha \), \( y^{(2^{r-1})} \). Hence, by Corollary 3.9, \( \eta_{2^{r-1}}(y) \) must change its parity as well, implying that \( y^{(2^{r-1}-2)}_\alpha \neq y^{(2^{r-1}-1)}_\alpha \) and \( y^{(2^{r-1}-2)}_\alpha, y^{(2^{r-1}-1)}_\alpha \in \{0, 2\} \). With the same argument, \( y^{(2^{r-1}-3)}_\alpha \neq y^{(2^{r-1}-2)}_\alpha \), \( y^{(2^{r-1}-3)}_\alpha, y^{(2^{r-1}-2)}_\alpha \in \{0, 2\} \), and so on. Therefore, in this last coordinate, half of the blocks have a ‘0’ and half of the blocks have a ‘2’. \hfill \square

Now, we are ready to prove the nonexistence of a \( \mathbb{Z}_2\mathbb{Z}_4 \)-cyclic code \( D(r) \) for \( r > 2 \).

**Theorem 3.11:** There is no \( \mathbb{Z}_2\mathbb{Z}_4 \)-cyclic 1-perfect code \( C \) such that \( C = \Phi(C) \) is nonlinear except for the case when \( C = C^* \) is the code of Example 3.2 of type \( (3, 6; 3, 4; 3) \), which is a \( \mathbb{Z}_2\mathbb{Z}_4 \)-cyclic code.

**Proof:** Assume that \( C \) is a \( \mathbb{Z}_2\mathbb{Z}_4 \)-cyclic 1-perfect code such that \( C = \Phi(C) \) is nonlinear. By Proposition 3.1, \( C \) must be a code \( C_{7,2r} \). If \( r = 2 \), then we have seen the \( \mathbb{Z}_2\mathbb{Z}_4 \)-cyclic code \( C^* = C_{2,4} \) in Example 3.2. Suppose now that \( r > 2 \).

Let \( z = (x_1, \ldots, x_\alpha | y^{(1)}, \ldots, y^{(2^{r-1})}) \in C^1 \) be an order 4 codeword. Define

\[
\lambda = \left\{ \ell : 1 \leq \ell \leq \alpha, \quad y^{(\ell)}_\ell = 2, \quad \forall i = 1, \ldots, 2^{r-1} \right\}, \quad \text{and}
\mu = \left\{ \ell : 1 \leq \ell \leq \alpha, \quad \text{such that } \exists k, k' \text{ with } y^{(k)}_\ell \neq y^{(k')}_\ell; \right\}
\]

\[
\{ y^{(k)}_\ell \neq y^{(k')}_\ell \in \{0, 2\} \}.
\]

Then, by Lemma 3.10 the number of twos in \( z \) is \( 2^{r-1}\lambda + 2^{r-2}\mu \). We have seen in Corollary 3.6 that this must equal \( 2^{r-2}(2^{r-1} - 1) \). Thus, we obtain

\[
2\lambda + \mu = 2^{r-1} - 1,
\]

implying that \( \mu \) is an odd number. But this is a contradiction with Proposition 3.8. \hfill \square

**IV. The Nonexistence of Nontrivial \( \mathbb{Z}_2\mathbb{Z}_4 \)-Cyclic Extended Perfect Codes**

Given a \( \mathbb{Z}_2\mathbb{Z}_4 \)-additive 1-perfect code \( C_{r,t} \) (\( 2 \leq r \leq t \leq 2r \)), we denote by \( C'_{r,t} \) the extended code obtained by adding an even parity check coordinate (of course, at the \( \mathbb{Z}_2 \) part). Then, \( C'_{r,t} \) is a \( \mathbb{Z}_2\mathbb{Z}_4 \)-additive extended 1-perfect code. Recall that \( C_{r,t} \) is of type

\[
(2^t - 1, 2^{t-1} - 2^{r-1}; 2^r - 1 - 2r + t, 2^{t-1} - 2^{r-1} + r - t; 2^r - 1 - 2r + t).
\]
Since \(|C'_{r,t}| = |C_{r,t}|, |(C'_{r,t})_b| = |(C_{r,t})_b|, \) and \(|((C'_{r,t})_b)_x| = |((C_{r,t})_b)_x|\), we have that \(C'_{r,t}\) is of type 
\[
(2^r, 2^{t-1} - 2^{t-1}; 2^r - 1 - 2r + t, 2^{t-1} - 2^{t-1} + r - t; 2^r - 1 - 2r + t).
\]

In this section, we prove that \(C'_{r,t}\) is not \(\mathbb{Z}_2\mathbb{Z}_4\)-cyclic for \(t > 2\). For this, we begin examining the case \(r = 2\). In such case, we have \(t \in \{2, 3, 4\}\). The case \(t = r = 2\) corresponds to a binary linear cyclic code of length 4 and two codewords. Such code is the trivial repetition code of length 4. Hence, we consider the cases \(t = 3\) and \(t = 4\).

**Lemma 4.1:** The codes \(C'_{2,3}\) and \(C'_{2,4}\) are not \(\mathbb{Z}_2\mathbb{Z}_4\)-cyclic.

**Proof:** First, we consider the code \(C'_{2,3}\). The type of \(C'_{2,3}\) is \((4, 2; 2, 1; 2)\). Hence, \(C'_{2,3}\) contains 8 codewords of order 4. Let \(x = (x_1', x_2')\) be one such codeword. Since any codeword in \(C'_{2,3}\) has weight 4 or 8, it follows that \(x_1'\) and \(x_2'\) must be both odd coordinates (otherwise 2x would have weight 2). Also, we have that \(w(x) = 2\). If we consider the codeword \(x + \sigma(x)\), we can see that \(x + \sigma(x)\) must have weight 4, implying that \(x = (1, 0, 1, 0)\) (or \(x = (0, 1, 0, 1)\)). Now, take a codeword \(y = (y_1', y_2')\) such that \(y_1' = x_1'\) and \(y_2' \neq x_2'\) (a simple counting argument shows that exactly half of the codewords have equal the last two coordinates). We have that \(d(x, y) \in \{0, 4\}\) and hence \(d(x, y) \in \{2, 6\}\), a contradiction.

The code \(C'_{2,4}\) is an extension of the code \(C^*\) in Example 3.2. Consider the dual code \(D = (C'_{2,3})^\perp\). If \(H\) is a generator matrix for \(C'_{2,4}\), then a generator matrix for \(D\) can be obtained adding, first, a zero column to \(H\) and, second, the row \(f = (1, \ldots, 1 | 2, \ldots, 2)\). Hence, \(D\) is of type \((4, 6; 1, 2; 1)\) and any nonzero codeword \(z \neq f\) has weight 8. Let \(x\) be an order 4 codeword. Clearly, \(x\) must have 4 odd coordinates in the quaternary part (otherwise, 2x would not have weight 8). This implies that \(z = x + \sigma^4(x)\) is an order 4 vector. If \(D\) is cyclic, then \(z = (z | z') \in D\). Note that \(z\) has zeros in all the binary positions, i.e. \(z = (0, \ldots, 0)\). Thus, \(z'\) has 4 odd coordinates and two coordinates, say \(z'_1\) and \(z'_2\), equal to ‘2’. But note that \(z'_1\) or \(z'_2\) (or both) is obtained as the addition of two odd coordinates. Therefore, \(x - \sigma^4(x)\) has weight less than 8, getting a contradiction.

Now, we establish the main result of this section.

**Theorem 4.2:** If \(C' = C'_{r,t}\) is a \(\mathbb{Z}_2\mathbb{Z}_4\)-additive extended 1-perfect code with \(t \geq 3\), then \(C'\) is not \(\mathbb{Z}_2\mathbb{Z}_4\)-cyclic.

**Proof:** Consider the subcode \(C'_0 = \{(x | 0, \ldots, 0)\}\). If \(C'\) is \(\mathbb{Z}_2\mathbb{Z}_4\)-cyclic, then clearly \((C'_0)_x\) is a binary linear cyclic code. For every vector \(v = (v | 0, \ldots, 0)\) of odd weight, we have that \(v\) must be at distance 1 from one codeword in \(C'\). Since no codeword \(z\) can have only an odd coordinate in the \(\mathbb{Z}_4\) part (otherwise 2z would have weight 2), it follows that \(v\) is at distance 1 from a codeword in \((C'_0)_x\). Therefore \(C'_0\) must be an extended Hamming code. But such code cannot be cyclic unless it has length 4 [8]. The result then follows by Lemma 4.1.

**References**

[1] T. Abualrub, I. Siap and H. Aydin, “\(\mathbb{Z}_2\mathbb{Z}_4\)-additive cyclic codes,” IEEE Trans. Inform. Theory, vol. 60, pp. 1508-1514, 2014.

[2] A. Bonisoli, “Every equidistant linear code is a sequence of dual Hamming codes,” Ars Combin., vol. 18, pp. 181-186, 1984.

[3] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, “\(\mathbb{Z}_2\mathbb{Z}_4\)-linear codes: generator matrices and duality,” Designs, Codes and Cryptography, vol. 54, pp. 167-179, 2010.

[4] J. Borges, C. Fernández-Córdoba and R. Ten-Valls, “\(\mathbb{Z}_2\mathbb{Z}_4\)-additive cyclic codes, generator polynomials and dual codes,” arXiv: 1406.4425, 2015.
[5] J. Borges, K.T. Phelps and J. Rifà, “The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 2028-2034, 2003.

[6] J. Borges and J. Rifà, “A characterization of 1-perfect additive codes,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 1688-1697, 1999.

[7] P. Delsarte and V. Levenshtein, “Association schemes and coding theory,” *IEEE Trans. Inform. Theory*, 44, pp. 2477-2504 (1998).

[8] J. Justensen and S. Forchhammer, *Two-dimensional Information Theory and coding*, Cambridge Univ. Press., 2010.

[9] D.S. Krotov, “$\mathbb{Z}_4$-linear perfect codes”, *Diskret. Anal. Issled. Oper.*, Ser. 1. 7(4), pp. 78–90, 2000. In Russian.

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

[11] J. Pujol and J. Rifà, “Translation-invariant propelinear codes,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 590-598, 1997.

[12] J. Rifà, “On a categorial isomorphism between a class of completely regular codes and a class of distance regular graphs. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-8*, vol. 508 LNCS, pp. 164-179, 1990.