Noname manuscript No.
(will be inserted by the editor)

Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

José Joaquín Bernal · Joaquim Borges · Cristina Fernández-Córdoba · Mercè Villanueva

Received: date / Accepted: date

Abstract An alternative permutation decoding method is described which can be used for any binary systematic encoding scheme, regardless whether the code is linear or not. Thus, the method can be applied to some important codes such as $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, which are binary and, in general, nonlinear codes in the usual sense. For this, it is proved that these codes allow a systematic encoding scheme. As particular examples, this permutation decoding method is applied to some Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

Keywords Permutation decoding, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, Hadamard codes

Mathematics Subject Classification (2000) 94B60 · 94B25

1 Introduction

We denote by $\mathbb{F}^n$ the set of all binary vectors of length n and by $\mathrm{wt}(v)$ the *(Hamming) weight* of any vector $v \in \mathbb{F}^n$, that is, the number of its nonzero coordinates. The *(Hamming) distance* between two vectors $u, v \in \mathbb{F}^n$ is defined as $d(u, v) = \mathrm{wt}(u + v)$. Given a binary code of length n, $C \subseteq \mathbb{F}^n$, we denote by d_C its *minimum distance*, that is, the minimum distance between any pair of different codewords in C. We say that C is a *t-error-correcting* code, where $t = \lfloor (d_C - 1)/2 \rfloor$.

For a vector $v \in \mathbb{F}^n$ and a set $I \subseteq \{1, \ldots, n\}$, $|I| = k$, we define $v_I \in \mathbb{F}^k$ as the vector v restricted to the I coordinates. For example, if $I = \{1, \ldots, k\}$

This work was partially supported by the Spanish MICINN under Grants TIN2010-17358 and TIN2013-40524-P, and by the Catalan AGAUR under Grant 2009SGR1224. The authors are in alphabetical order.

José Joaquín Bernal is with the Dept. of Mathematics, Universidad de Murcia, Spain. E-mail: josejoaquin.bernal@um.es · Joaquim Borges, Cristina Fernández-Córdoba and Mercè Villanueva are with the Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, Spain. E-mail: {jborges, cfernandez, mvillanueva}@deic.uab.cat

and $v = (v_1, \ldots, v_n)$, then $v_I = (v_1, \ldots, v_k)$. If C is a binary code of length n, then $C_I = \{v_I : v \in C\}$.

If C has size $|C| = 2^k$, then C is a *systematic* code if there is a set $I \subseteq \{1, \ldots, n\}$ of k coordinate positions such that $|C_I| = 2^k$. In other words, C_I is $\mathbb{F}^k$. Such a set I is also referred to as a set of *systematic coordinates* or an *information set*. Given a systematic code of size $|C| = 2^k$ with information set I, a *systematic encoding for* I is a one-to-one map $f : \mathbb{F}^k \to \mathbb{F}^n$, such that for any information vector $a \in \mathbb{F}^k$, the corresponding codeword $f(a)$ satisfies that $f(a)_I = a$.

Let us consider the group of permutations on n symbols, $\mathcal{S}_n$, acting on $\mathbb{F}^n$ by permuting the coordinates of each vector. That is, for every $v = (v_1, \ldots, v_n) \in \mathbb{F}^n$ and $\pi \in \mathcal{S}_n$, $\pi(v_1, \ldots, v_n) = (v_{\pi^{-1}(1)}, \ldots, v_{\pi^{-1}(n)})$. Then, for any binary code C, we denote by $\mathrm{PAut}(C)$ its *permutation automorphism group*, i.e., $\mathrm{PAut}(C) = \{\pi \in \mathcal{S}_n : \pi(C) = C\}$. Moreover, a binary code C' is said to be *permutation equivalent* to C if there exists $\pi \in \mathcal{S}_n$ such that $\pi(C) = C'$.

Not every binary code of size 2^k is systematic, but every binary linear code is systematic. Indeed, if $C \subseteq \mathbb{F}^n$ is a binary linear code of dimension k, it is permutation equivalent to a code with generator and parity check matrices:

$$G = \left(Id_k \; A \right) \quad \text{and} \quad H = \left(A^T \; Id_{n-k} \right), \tag{1}$$

where Id_r denotes the $r \times r$ identity matrix, A is a $k \times (n-k)$ matrix, and A^T is the transpose of A. In general, for any information set I, we say that a generator (resp. parity check) matrix is in *standard form* if the columns in the positions inside (resp. outside of) I are the columns of Id_k. Then the map $f : \mathbb{F}^k \to \mathbb{F}^n$ given by

$$f(v) = v\, G, \tag{2}$$

for any $v \in \mathbb{F}^k$, is clearly a systematic encoding.

Permutation decoding was introduced in [12] and [9]. A description of the standard method for linear codes can be found in [10, p.513]. Given a t-error-correcting linear code $C \subseteq \mathbb{F}^n$ with fixed information set I, we consider $y = x + e$ the received vector, where $x \in C$ and e is the error vector. We assume that y has less than $t+1$ errors, that is, $\mathrm{wt}(e) \leq t$. The idea of permutation decoding is to use the elements of $\mathrm{PAut}(C)$ in order to move the nonzero coordinates of e out of I. So, on the one hand the method is based on the existence of some special subsets $S \subseteq \mathrm{PAut}(C)$, called PD-sets, verifying that for any vector $e \in \mathbb{F}^n$ with $\mathrm{wt}(e) \leq t$, there is an element $\pi \in S$ such that $\mathrm{wt}(\pi(e)_I) = 0$. On the other hand, the main tool of this decoding algorithm is the following theorem which gives us a necessary and sufficient condition for a received vector $y \in \mathbb{F}^n$ having its systematic coordinates correct.

Theorem 1 ([10]) *Let C be a t-error-correcting linear code with information set I and parity check matrix H in standard form. Let $y = x + e$, where $x \in C$ and e verifies that $\mathrm{wt}(e) \leq t$. Then*

$$\mathrm{wt}(Hy^T) = \mathrm{wt}(He^T) \leq t \iff \mathrm{wt}(e_I) = 0. \tag{3}$$

Let $C \subseteq \mathbb{F}^n$ be a t-error-correcting linear code with information set I and parity check matrix H in standard form. Assume that we have found a PD-set for the information set I, $S \subseteq \mathrm{PAut}(C)$, and denote by $y = x + e$ the received vector, where $x \in C$ and e is the error vector. Then, the permutation decoding algorithm works as follows:

1. If $\mathrm{wt}(Hy^T) \leq t$, then the systematic coordinates of y are correct and we can recover x from (2).
2. Else, we search $\pi \in S$ such that $\mathrm{wt}(H\pi(y)^T) \leq t$. If there is no such π, we conclude that more than t errors have occurred.
3. If we have successfully found π, we take x' the unique codeword such that $x'_I = \pi(y)_I$. Then, the decoded vector is $\pi^{-1}(x')$.

In this paper, we show that $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are systematic. Moreover, we give a systematic encoding method for these codes. However, for $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, Theorem 1 holds just in some obvious cases, not in general. Nevertheless, we give an alternative method for permutation decoding which does not need (3). Such method does not use the syndrome Hy^T to check whether the systematic coordinates are correct or not. Therefore, the method can be used for $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, of course, assuming that we know an appropriate PD-set.

The paper is organized as follows. In Section 2, we show that any $\mathbb{Z}_2\mathbb{Z}_4$-linear code is systematic. Moreover, we give an information set and a systematic encoding for that information set. In Section 3, we see under which conditions the standard permutation decoding method works for $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. We also present the alternative permutation decoding method. Such method does not use the syndrome of a received vector in order to check whether the systematic coordinates are correct or not. We show this new method applied to some examples of Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. These codes are, in general, nonlinear codes in the binary sense, but they have high error-correcting capability.

2 Systematic encoding for $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

For every pair n_1, n_2 of nonnegative integers, define the component-wise Gray map $\Phi : \mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2} \longrightarrow \mathbb{F}^{n_1+2n_2}$ as

$$\Phi(x, y) = (x, \phi(y_1), \ldots, \phi(y_{n_2})) \\ \forall x \in \mathbb{Z}_2^{n_1},\ \forall y = (y_1, \ldots, y_{n_2}) \in \mathbb{Z}_4^{n_2};$$

where $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ is the usual Gray map, that is,

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

The parameters n_1, n_2 of the Gray map Φ will be treated dependently on the context.

The *Lee weights* over the elements in $\mathbb{Z}_4$ are defined as $\omega t_L(0) = 0, \omega t_L(1) = \omega t_L(3) = 1, \omega t_L(2) = 2$. Then, the *Lee weight* of a vector $u = (u_1, \ldots, u_{n_1+n_2}) \in \mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2}$ is defined as $\omega t_L(u) = \mathrm{wt}(u_1, \ldots, u_{n_1}) + \sum_{i=1}^{n_2} \omega t_L(u_{n_1+i})$. Finally, the *Lee distance* between two vectors $u, v \in \mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2}$ is defined as $d_L(u, v) = \omega t_L(u - v)$. Note that the Gray map is an isometry which transforms Lee distances into Hamming distances.

Let C be a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $n = \alpha + 2\beta$ and size $|C| = 2^k = 2^{\gamma+2\delta}$ [2]. As usual, denote by $\mathcal{C}$ the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive code, i.e. $\mathcal{C} = \Phi^{-1}(C)$. If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, it is permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with generator matrix of size $(\kappa + (\gamma - \kappa) + \delta) \times (\kappa + (\alpha - \kappa) + (\beta - \gamma - \delta + \kappa) + (\gamma - \kappa) + \delta)$ as follows [2]:

$$\mathcal{G} = \left(\begin{array}{cc|ccc} Id_\kappa & T_b & 2T_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 2T_1 & 2Id_{\gamma-\kappa} & \mathbf{0} \\ \hline \mathbf{0} & S_b & S_q & R & Id_\delta \end{array}\right), \tag{4}$$

where T_b, S_b are matrices over $\mathbb{Z}_2$; T_1, T_2, R are matrices over $\mathbb{Z}_4$ with all their entries in $\{0, 1\} \subset \mathbb{Z}_4$; and S_q is a matrix over $\mathbb{Z}_4$. We say that $(\alpha, \beta; \gamma, \delta; \kappa)$ is the type of $\mathcal{C}$, and $\mathcal{G}$ is a matrix in standard form for the $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$. Note that when $\alpha = 0$, the $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are linear codes over $\mathbb{Z}_4$, and when $\beta = 0$, they are binary linear codes.

Given two vectors $u, v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, the inner product is defined as in [2]:

$$\langle u, v \rangle = 2(\sum_{i=1}^{\alpha} u_i v_i) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \ \in \ \mathbb{Z}_4,$$

where the computations are made taking the zeros and ones in the α binary coordinates as quaternary zeros and ones, respectively. The additive dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is then defined in the standard way:

$$\mathcal{C}^\perp = \{y \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \ : \ \langle x, y \rangle = 0 \text{ for all } x \in \mathcal{C}\}.$$

It is also shown in [2] that if $\mathcal{C}$ has a generator matrix in standard form (4), then $\mathcal{C}^\perp$ can be generated by the matrix:

$$\mathcal{H} = \left(\begin{array}{cc|ccc} T_b^t & Id_{\alpha-\kappa} & \mathbf{0} & \mathbf{0} & 2S_b^t \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 2Id_{\gamma-\kappa} & 2R^t \\ \hline T_2^t & \mathbf{0} & Id_{\beta+\kappa-\gamma-\delta} & T_1^t & -\left(S_q + RT_1\right)^t \end{array}\right), \tag{5}$$

which also represents a parity check matrix for $\mathcal{C}$. Moreover, $\mathcal{C}^\perp$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$, where

$$\begin{aligned} \bar{\gamma} &= \alpha + \gamma - 2\kappa, \\ \bar{\delta} &= \beta - \gamma - \delta + \kappa, \\ \bar{\kappa} &= \alpha - \kappa. \end{aligned} \tag{6}$$

There are some cases where the systematic encoding of C is clear. The first case is when C is linear. Then, we can apply simply the standard systematic

encoding for linear codes by considering the generator matrix G of C as in (1). It is clear that C is linear, for example, when $\beta = 0$ and also when $\delta = 0$. In general, if $\mathcal{G}$ is a generator matrix of $\mathcal{C} = \Phi^{-1}(C)$ as in (4), where $\{u_i\}_{i=1}^{\gamma}$ and $\{v_j\}_{j=1}^{\delta}$ are the row vectors of order two and order four in $\mathcal{G}$, respectively, then C is a binary linear code if and only if $2v_j * v_k \in \mathcal{C}$, for all j, k satisfying $1 \leq j < k \leq \delta$, where $*$ is the component-wise product [5].

The second case is when $\gamma = \kappa$. If we consider a code $\mathcal{C}$ with $\gamma = \kappa$, then it is permutation equivalent to a code with generator and the parity check matrices

$$\mathcal{G} = \left(\begin{array}{cc|cc} Id_\kappa & T_b & 2T_2 & \mathbf{0} \\ \mathbf{0} & S_b & S_q & Id_\delta \end{array}\right), \mathcal{H} = \left(\begin{array}{cc|cc} T_b^t & Id_{\alpha-\kappa} & \mathbf{0} & 2S_b^t \\ T_2^t & \mathbf{0} & Id_{\beta+\kappa-\gamma-\delta} & -S_q^t \end{array}\right). \tag{7}$$

It is clear that for any information vector $(u, v) \in \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$, we have that $(u, v)\mathcal{G} = (u, z, v)$ for some $z \in \mathbb{Z}_2^{\alpha-\gamma} \times \mathbb{Z}_4^{\beta-\delta}$ and, therefore, the set $I = \{1, \ldots, \kappa, \alpha + \beta - \delta + 1, \ldots, \alpha + \beta\}$ is a set of systematic coordinates. Hence, we have the following systematic encoding:

$$f(a) = \Phi(\Phi^{-1}(a)\mathcal{G}), \quad \forall a \in \mathbb{F}^k. \tag{8}$$

Even though in those cases a systematic encoding is clear, we can not use the same method to $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in general. Therefore, we are going to define a method that use the $\mathbb{Z}_2\mathbb{Z}_4$-linearity of the code and can be used for all values of $\alpha, \beta, \gamma, \delta$ and κ.

Let us consider a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with a generator matrix in standard form (4) and $C = \Phi(\mathcal{C})$. For each quaternary coordinate position $\alpha + i$, with $i \in \{1, \ldots, \beta\}$, we denote by $\varphi_1(\alpha + i)$ and $\varphi_2(\alpha + i)$ the corresponding pair of binary coordinate positions in $\{1, \ldots, \alpha + 2\beta\}$, that is, $\varphi_1(\alpha + i) = \alpha + 2i - 1$ and $\varphi_2(\alpha + i) = \alpha + 2i$. We define the following sets of coordinate positions in $\{1, \ldots, \alpha + 2\beta\}$:

$J_1 = \{1, \ldots, \kappa\}$, $|J_1| = \kappa$.
$J_2 = \{j_1, \ldots, j_{\gamma-\kappa}\}$, where $j_i = \varphi_1(\alpha + \beta + \kappa - \gamma - \delta + i)$, $|J_2| = \gamma - \kappa$.
$J_3 = \{\varphi_1(\alpha+\beta-\delta+1), \varphi_2(\alpha+\beta-\delta+1), \ldots, \varphi_1(\alpha+\beta), \varphi_2(\alpha+\beta)\}$, $|J_3| = 2\delta$.

Note that J_1, J_2, J_3 are related with the column indices of Id_κ, $Id_{\gamma-\kappa}$, Id_δ in (4), respectively. We are going to show that $J = J_1 \cup J_2 \cup J_3$ is a set of systematic coordinates for the $\mathbb{Z}_2\mathbb{Z}_4$-linear code C. We shall refer to J as the *standard information set* or *standard set of systematic coordinates*.

Given an information vector $a = (a_1, \ldots, a_{\gamma+2\delta}) \in \mathbb{F}^{\gamma+2\delta}$, we consider the representation $a = (b, c, d)$, where $b = (a_1, \ldots, a_\kappa)$, $c = (c_1, \ldots, c_{\gamma-\kappa}) = (a_{\kappa+1}, \ldots, a_\gamma)$ and $d = (a_{\gamma+1}, \ldots, a_{\gamma+2\delta})$. Note that $\Phi^{-1}(a) = (b, c, d') \in \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$, where $d' = \Phi^{-1}(d)$.

For a quaternary vector $x = (x_1, \ldots, x_\ell)$ of arbitrary length ℓ, define $\Phi_1(x) = (\phi_1(x_1), \ldots, \phi_1(x_\ell))$, where ϕ_1 is the first component of the Gray map, i.e., $\phi_1(0) = \phi_1(1) = 0$ and $\phi_1(2) = \phi_1(3) = 1$. Then, we define the bijection $\sigma : \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta} \longrightarrow \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$ as

$$\sigma(\Phi^{-1}(a)) = \sigma(b, c, d') = (b, c + \Phi_1(d'R), d'). \tag{9}$$

We remark that σ is not a group automorphism of $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. For example, assume that R is a 1×1 matrix (hence $\gamma - \kappa = \delta = 1$) with its entry equal to 1. Then, we easily obtain that $\sigma(1,\ldots,1,1,1) = (1,\ldots,1,1,1)$, but $\sigma\left(-(1,\ldots,1,1,1)\right) = \sigma(1,\ldots,1,1,3) = (1,\ldots,1,0,3)$ which is not the inverse element of $(1,\ldots,1,1,1)$. Note also that $c + \Phi_1(d'R) = \Phi_1(2c + d'R) = \left(\Phi(\Phi^{-1}(a)\mathcal{G})\right)_{J_2}$.

Now, we have

$$\begin{aligned}\left(\Phi(\sigma(\Phi^{-1}(a))\mathcal{G})\right)_J &= (b, \Phi_1(2c + 2\Phi_1(d'R) + d'R), d)\\ &= (b, c + \Phi_1(d'R) + \Phi_1(d'R), d) = (b, c, d).\end{aligned}$$

It follows that the codeword $\sigma(\Phi^{-1}(a))\mathcal{G}$ verifies that

$$\left(\Phi(\sigma(\Phi^{-1}(a))\mathcal{G})\right)_J = (b, c, d) = a.$$

Since $|J| = \kappa + \gamma - \kappa + 2\delta = \gamma + 2\delta$, we conclude that J is a set of systematic coordinates. Therefore, we have proved the following theorem.

Theorem 2 *If C is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then C is a systematic code. Moreover, if we assume that the generator matrix of $\mathcal{C} = \Phi^{-1}(C)$ is in standard form (4), then $J = J_1 \cup J_2 \cup J_3$ is a set of systematic coordinates for C.*

Note that in the case $\gamma = \kappa$, we have $a = (b, d)$, hence σ is the identity map. Therefore, as a result, for $\gamma = \kappa$ we obtain the same systematic encoding function given in (8).

Corollary 1 *Let C be a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length n, size $|C| = 2^k$ and such that $\mathcal{C} = \Phi^{-1}(C)$ has generator matrix in standard form (4). Then, the function $f : \mathbb{F}^k \longrightarrow \mathbb{F}^n$ defined as*

$$f(a) = \Phi\left(\sigma\left(\Phi^{-1}(a)\right)\mathcal{G}\right), \quad \forall a \in \mathbb{F}^k \tag{10}$$

is a systematic encoding for C and the information set J.

The following example shows that the set of systematic coordinates is not unique, in general.

Example 1 Consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ generated by

$$\mathcal{G} = \left(\begin{array}{cc|ccc} 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 \\ \hline 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

Let $C = \Phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear code in $\mathbb{F}^8$. A set of systematic coordinates is $\{2, 4, 6, 8\}$. However, the standard set of systematic coordinates would be $\{1, 5, 7, 8\}$.

Note that this encoding method requires, in some cases, two products by the generator matrix. However, this is not a meaningful change of complexity order.

3 An alternative permutation decoding algorithm

In this section, we are going to see that the standard permutation decoding algorithm can be applied to $\mathbb{Z}_2\mathbb{Z}_4$-linear codes just in a few cases. This is because, even if we find a PD-set, Theorem 1 can not be used in general. We shall present an alternative permutation decoding algorithm where Theorem 3 replaces Theorem 1.

Let C be a t-error correcting $\mathbb{Z}_2\mathbb{Z}_4$-linear code with information set J. Let $\mathcal{C} = \Phi^{-1}(C)$ be the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. On the one hand, we have seen that if C is linear, then the usual systematic encoding can be applied considering the matrices as in (1), so Theorem 1 works. On the other hand, if $\gamma = \kappa$, then we have seen that we can assume that $\mathcal{C}$ has a parity check matrix $\mathcal{H}$ containing the identity matrix as in (7). Then, denote the received vector $y = x + e \in \mathbb{F}^{\alpha+2\beta}$, where $c \in C$ and e is the error vector. It is easy to see that we may adapt Theorem 1 to this context, that is, we have that, under the condition $\mathrm{wt}(e) \leq t$,

$$\omega t_L(\mathcal{H}\Phi^{-1}(y)^T) = \omega t_L(\mathcal{H}\Phi^{-1}(e)^T) \leq t \iff \mathrm{wt}(e_J) = 0. \tag{11}$$

where, recall that $\omega t_L()$ represents the Lee weight. We say that C satisfies (11) if for all error vector e such that $\mathrm{wt}(e) \leq t$ we have that e satisfies (11). The following result shows that in the nonlinear case, (11) holds if and only if $\gamma = \kappa$.

Proposition 1 *Let $\mathcal{C}$ be a t-error-correcting $\mathbb{Z}_2\mathbb{Z}_4$-additive code of length n, type $(\alpha, \beta; \gamma, \delta; \kappa)$ and parity check matrix $\mathcal{H}$, such that $C = \Phi(\mathcal{C})$ is a binary nonlinear code. Then, C satisfies (11) if and only if $\gamma = \kappa$.*

Proof: The case $\gamma = \kappa$ has been discussed above, so assume $\gamma > \kappa$.

Denote by e_i the binary vector of length n which has weight one and its nonzero coordinate is at position i $(1 \leq i \leq n)$. Define the three binary coordinate sets:

$L_1 = \{\kappa + 1, \cdots, \alpha\}$,
$L_2 = \{\varphi_1(\alpha+1), \varphi_2(\alpha+1), \ldots, \varphi_1(\alpha+\beta+\kappa-\gamma-\delta), \varphi_2(\alpha+\beta+\kappa-\gamma-\delta)\}$,
$L_3 = \{j_1, \ldots, j_{\gamma-\kappa}\}$, where $j_i = \varphi_2(\alpha+\beta+\kappa-\gamma-\delta+i)$.

We have that $L = L_1 \cup L_2 \cup L_3 = \{1, \ldots, n\} \setminus J$, where J is the standard information set. First, note that, by the definition of $\mathcal{H}$ as in (5), it is easy to check that for $k_1, \ldots, k_r \in L_3$ we have that $\omega t_L(\mathcal{H}\Phi^{-1}(e_{k_1} + \cdots + e_{k_r})^T) \geq 2r$. Second, $\omega t_L(\mathcal{H}\Phi^{-1}(e)^T) = \omega t_L(\mathcal{H}\Phi^{-1}(\varepsilon_1)^T) + \omega t_L(\mathcal{H}\Phi^{-1}(\varepsilon_2)^T)$, where $\varepsilon_1 = (\varepsilon_1^1, \ldots, \varepsilon_1^n) \in \mathbb{F}^n$ is given by $(\varepsilon_1)_{L_1} = e_{L_1}$, $\varepsilon_1^i = 0$ if $i \notin L_1$, and $\varepsilon_2 = (\varepsilon_2^1, \ldots, \varepsilon_2^n) \in \mathbb{F}^n$ is given by $(\varepsilon_2)_{L\setminus L_1} = e_{L\setminus L_1}$, $\varepsilon_2^i = 0$ if $i \in L_1$. By using these properties, we will see that there exists an error vector of weight at most t not satisfying (11).

Consider an error vector $e \in \mathbb{F}^n$ such that $\mathrm{wt}(e) = t$, $\mathrm{wt}(e_J) = 0$ and $\mathrm{wt}(e_{L_3}) \neq 0$. If $\mathrm{wt}(e_{L_2}) = 0$, we obtain $\omega t_L(\mathcal{H}\Phi^{-1}(e)^T) = \omega t_L(\mathcal{H}\Phi^{-1}(\varepsilon_1)) + \omega t_L(\mathcal{H}\Phi^{-1}(\varepsilon_2)) \geq \mathrm{wt}(\varepsilon_1) + 2\mathrm{wt}(\varepsilon_2) > \mathrm{wt}(e) = t$ and e does not satisfy (11).

Now assume $\mathrm{wt}(e_{L_2}) \neq 0$. If $\omega t_L(\mathcal{H}\Phi^{-1}(e)^T) > t$, then we have finished. If $\omega t_L(\mathcal{H}\Phi^{-1}(e)^T) \leq t$, since $\mathrm{wt}(e_{L_3}) \neq 0$ and for all $j \in L_3$ $\omega t_L(\mathcal{H}\Phi^{-1}(e_j)^T) \geq 2$, we have that there exists $i \in L_2$ such that $\mathrm{wt}(e+e_i) = t-1$ and $\omega t_L(\mathcal{H}\Phi^{-1}(e+e_i)^T) > t$. In both cases, we have that C does not satisfy (11). □

Theorem 3 *Let C be a binary systematic t-error-correcting code of length n. Let I be a set of systematic coordinates and let f be a systematic encoding for I. Suppose that $y = x + e$ is a received vector, where $x \in C$ and $\mathrm{wt}(e) \leq t$. Then, the systematic coordinates of y are correct, i.e. $y_I = x_I$, if and only if $\mathrm{wt}(y + f(y_I)) \leq t$.*

Proof: If $\mathrm{wt}(y + f(y_I)) \leq t$, then $f(y_I)$ is the closest codeword to y, that is, $f(y_I) = x$. Hence the systematic coordinates are the same $y_I = x_I$.

If $x_I = y_I$, then $\mathrm{wt}(y + f(y_I)) = \mathrm{wt}(y + x) = \mathrm{wt}(e) \leq t$. □

Now, let us consider a $\mathbb{Z}_2\mathbb{Z}_4$-linear code $\mathcal{C}$ with information set I. Assume that $S \subseteq \mathrm{PAut}(C)$ is a PD-set for I and y is a received vector. As an alternative method with respect to the algorithm described in Section 1 we can use the following decoding process:

1. If $\mathrm{wt}(y + f(y_I)) \leq t$, then $x = f(y_I)$ is the decoded vector and y_I is the information vector.
2. Else, we search $\pi \in S$ such that $\mathrm{wt}(\pi(y) + f(\pi(y)_I)) \leq t$. If there is no such π, we conclude that more than t errors have occurred.
3. If we have successfully found π, then the decoded vector is

$$x = \pi^{-1}(f(\pi(y)_I)).$$

Note that $\mathrm{wt}(\pi(y) + f(\pi(y)_I)) \leq t$ implies that $f(\pi(y)_I)$ is the closest codeword to $\pi(y)$. Therefore, the closest codeword to y is $\pi^{-1}(f(\pi(y)_I))$.

Finally, we show through the next two examples, how to apply a permutation decoding for $\mathbb{Z}_2\mathbb{Z}_4$-linear codes using the previous methods. Both examples correspond to Hadamard $\mathbb{Z}_4$-linear codes ($\mathbb{Z}_2\mathbb{Z}_4$-linear codes with $\alpha = 0$). Note that, using a code in standard form, it is easy to see that the binary α coordinates are always systematic, so they do not affect to the permutation decoding methods applied.

A binary Hadamard code is a binary code of length n, $2n$ codewords and minimum distance $n/2$, which can be constructed from a Hadamard matrix [1,10]. They have a high error correcting capability $t = \lfloor (n-2)/4 \rfloor$. However, linear Hadamard codes are not suitable for a syndrome decoding since the number of syndromes is also very high. Recently, for these codes, a partial permutation decoding, that is a permutation decoding up to $s < t$ errors, was presented in [6]. Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes have been completely classified [3,7] and they include the linear case. The examples below are in fact linear, but we do not use their linearity to apply the permutation decoding algorithms.

Example 2 Consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ with generator and parity check matrices:

$$\mathcal{G} = \left(\begin{array}{c} 3\ 2\ 1\ 0 \\ \hline 2\ 3\ 0\ 1 \end{array}\right), \qquad \mathcal{H} = \left(\begin{array}{c} 1\ 0\ 1\ 2 \\ \hline 0\ 1\ 2\ 1 \end{array}\right).$$

The corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ is a 1-error-correcting code of type $(0, 4; 0, 2; 0)$ (i.e., C is a $\mathbb{Z}_4$-linear code). In fact, C is a Hadamard $\mathbb{Z}_4$-linear code [7]. Let $\vartheta = (1, 3, 5, 7)(2, 4, 6, 8)$. It is straightforward to check that $\vartheta \in \mathrm{PAut}(C)$ (note that $\mathcal{C}$ is a quaternary cyclic code) [11]. Moreover, $S = \{id, \vartheta, \vartheta^2\}$ is a PD-set for the standard information set $I = \{5, 6, 7, 8\}$. Since $\gamma = \kappa$, we can use the systematic encoding f defined in (8).

For example, let $a = (0, 1, 0, 1) \in \mathbb{F}^4$ be an information vector. Then, the corresponding codeword is

$$x = f(a) = \Phi\left(\Phi^{-1}(a)\mathcal{G}\right) = \Phi\left((1, 1)\mathcal{G}\right) = \Phi(1, 1, 1, 1) = (0, 1, 0, 1, 0, 1, 0, 1).$$

Suppose now that the received vector is $y = x+e$, where $e = (0, 0, 0, 0, 0, 0, 0, 1)$. The syndrome of y is

$$\Phi\left(\mathcal{H}\Phi^{-1}(y)^T\right) = \Phi\left(\mathcal{H}(1, 1, 1, 0)^T\right) = \Phi((2, 3)^T) = (1, 1, 1, 0)^T,$$

which has weight $3 > t = 1$. However, considering the vector $z = \vartheta(y) = (0, 0, 0, 1, 0, 1, 0, 1)$, we have that the syndrome is

$$\Phi\left(\mathcal{H}\Phi^{-1}(z)^T\right) = \Phi((3, 0)^T) = (1, 0, 0, 0)^T,$$

which has weight $1 \leq t = 1$. Therefore, the systematic coordinates of z have no errors. Hence, we decode y as

$$\begin{aligned} \vartheta^{-1}\left(\Phi(\Phi^{-1}(z_I)\mathcal{G})\right) &= \vartheta^{-1}\left(\Phi((1, 1)\mathcal{G})\right) = \vartheta^{-1}(\Phi(1, 1, 1, 1)) \\ &= (0, 1, 0, 1, 0, 1, 0, 1) = x, \end{aligned}$$

and the information vector is $x_I = (0, 1, 0, 1)$.

Example 3 Consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ with generator matrix:

$$\mathcal{G} = \left(\begin{array}{c} 2\ 2\ 2\ 0\ 0\ 2\ 0\ 0 \\ \hline 3\ 2\ 1\ 2\ 3\ 0\ 1\ 0 \\ 2\ 3\ 0\ 3\ 2\ 1\ 0\ 1 \end{array}\right).$$

The corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ is a 3-error-correcting code of type $(0, 8; 1, 2; 0)$ (i.e., C is a $\mathbb{Z}_4$-linear code). In fact, C is also a Hadamard $\mathbb{Z}_4$-linear code [7]. We know that $\langle \vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4 \rangle \subseteq \mathrm{PAut}(C)$ [11], where

$$\begin{aligned} \vartheta_1 =& (1, 5)(2, 6)(3, 11)(4, 12)(9, 13)(10, 14)(7, 15)(8, 16), \\ \vartheta_2 =& (1, 3, 5, 11)(2, 4, 6, 12)(9, 7, 13, 15)(10, 8, 14, 16), \\ \vartheta_3 =& (9, 13)(10, 14)(7, 15)(8, 16), \\ \vartheta_4 =& (1, 9)(2, 10)(5, 13)(6, 14). \end{aligned} \tag{12}$$

Moreover, it is easy to check using the MAGMA software package [4] that we can take the elements in the subgroup $S = \langle \vartheta_1, \vartheta_2, \vartheta_4 \rangle$ as a PD-set for the information set $I = \{11, 13, 14, 15, 16\}$. In this case, we can not use the standard permutation decoding, since $\gamma \neq \kappa$. However, we can still perform a permutation decoding using the alternative method presented in this section.

For example, let $a = (1, 1, 1, 1, 1) \in \mathbb{F}^5$ be an information vector. Using the systematic encoding given by (10), the corresponding codeword is

$$\begin{aligned} x = f(a) &= \Phi\left(\sigma(\Phi^{-1}(a))\mathcal{G}\right) = \Phi\left((1+1, 2, 2)\mathcal{G}\right) \\ &= \Phi(2, 2, 2, 2, 2, 2, 2, 2) = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1). \end{aligned}$$

Suppose now that the received vector is $y = x + e$, where

$$e = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1).$$

By considering the standard information set, the information coordinates of y are $y_I = (1, 0, 1, 0, 0)$ and

$$f(y_I) = \Phi(\sigma(\Phi^{-1}(y_I))\mathcal{G}) = (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0),$$

so $\mathrm{wt}(y + f(y_I)) = 5 > t = 3$. However, considering the vector $z = \vartheta_1(y) = (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$, we have that $z_I = (1, 1, 1, 1, 1)$ and

$$f(z_I) = \Phi(\sigma(\Phi^{-1}(z_I))\mathcal{G}) = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1),$$

so $\mathrm{wt}(z + f(z_I)) = 3 \leq t = 3$. Therefore, the systematic coordinates of z have no errors. Hence, we decode y as $\vartheta_1^{-1}(f(z_I)) = x$ and the information vector is $x_I = (1, 1, 1, 1, 1)$.

Acknowledgements

The authors thank Prof. J. Rifà for valuable discussions in an earlier version of this paper. They also thank the anonymous referees for their valuable comments, which enabled them to improve the quality of the paper.

References

1. E.F. Assmus and J.D. Key, *Designs and their codes*, Cambridge University Press, Great Britain, 1992.
2. 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.
3. 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. on Information Theory*, vol. 49(8), pp. 2028-2034, 2003.
4. J.J. Cannon and W. Bosma (Eds.) *Handbook of* MAGMA *Functions*, Edition 2.13, 4350 pages, 2006.
5. C. Fernández-Córdoba, J. Pujol and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel," *Designs Codes and Cryptography*, vol. 56, pp. 43-59, 2010.

6. W. Fish, J. D. Key and E. Mwambene, "Partial permutation decoding for simplex codes," *Advances in Mathematics of Comunications*, vol. 6, no. 4, pp. 505-516, 2012.
7. D.S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," *Electron. Notes in Discr. Math.*, vol. 6, pp. 107-112, 2001.
8. D.S. Krotov, "On the automorphism groups of the additive 1-perfect binary codes," Proceedings of the 3rd International Castle Meeting on Coding Theory and Applications, Cardona, Spain, pp. 171-176, 2011.
9. F.J. MacWilliams, "Permutation decoding of systematic codes," *Bell Syst. Tech. J.*, vol. 43, pp. 485-505, 1964.
10. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.
11. J. Pernas, J. Pujol and M. Villanueva, "Characterization of the automorphism group of quaternary linear Hadamard codes," *Designs, Codes and Cryptography* (2012), DOI 10.1007/s10623-012-9678-2.
12. E. Prange. "The use of information sets in decoding cyclic codes," *IEEE Trans. Info. Theory*, vol. 8, no. 5, pp. S5-S9, 1962.