Des. Codes Cryptogr. (2011) 61:31–40
DOI 10.1007/s10623-010-9437-1

Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$

M. Bilal · J. Borges · S. T. Dougherty · C. Fernández-Córdoba

Received: 3 June 2010 / Revised: 16 September 2010 / Accepted: 16 September 2010 /
Published online: 5 October 2010

Abstract Known upper bounds on the minimum distance of codes over rings are applied to the case of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, that is subgroups of $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$. Two kinds of maximum distance separable codes are studied. We determine all possible parameters of these codes and characterize the codes in certain cases. The main results are also valid when $\alpha = 0$, namely for quaternary linear codes.

Keywords Additive codes · Minimum distance bounds · Maximum distance separable codes

Mathematics Subject Classification (2000) 94B60 · 94B25

1 Introduction

We denote by $\mathbb{Z}_2$ and $\mathbb{Z}_4$ the ring of integers modulo 2 and modulo 4, respectively. A *binary linear code* is a subspace of $\mathbb{Z}_2^n$. A *quaternary linear code* is a subgroup of $\mathbb{Z}_4^n$.

Communicated by W. H. Haemers.

M. Bilal (✉) · J. Borges · C. Fernández-Córdoba
Department of Information and Communications Engineering,
Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain
e-mail: mbilal@deic.uab.cat

J. Borges
e-mail: jborges@deic.uab.cat

C. Fernández-Córdoba
e-mail: cfernandez@deic.uab.cat

S. T. Dougherty
Department of Mathematics, University of Scranton, Scranton, PA 18510, USA
e-mail: doughertys1@scranton.edu

In [3], Delsarte defines additive codes as subgroups of the underlying abelian group in a translation association scheme. For the binary Hamming scheme, the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$ [4]. Thus, the subgroups $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in a binary Hamming scheme.

As in [1] and [2], we define an extension of the usual Gray map. We define $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n$, where $n = \alpha + 2\beta$, given by $\Phi(x, y) = (x, \phi(y_1), \ldots, \phi(y_\beta))$ for any $x \in \mathbb{Z}_2^\alpha$ and any $y = (y_1, \ldots, y_\beta) \in \mathbb{Z}_4^\beta$, 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 map Φ is an isometry which transforms Lee distances in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ to Hamming distances in $\mathbb{Z}_2^{\alpha+2\beta}$.

Denote by $wt_H(v_1)$ the Hamming weight of $v_1 \in \mathbb{Z}_2^\alpha$ and by $wt_L(v_2)$ the Lee weight of $v_2 \in \mathbb{Z}_4^\beta$. For a vector $\mathbf{v} = (v_1, v_2) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, define the weight of $\mathbf{v}$, denoted by $wt(\mathbf{v})$, as $wt_H(v_1) + wt_L(v_2)$, or equivalently, the Hamming weight of $\Phi(\mathbf{v})$. Denote by $d(\mathcal{C})$ the minimum distance between codewords in $\mathcal{C}$. Let $\mathbf{0}, \mathbf{1}, \mathbf{2}$ be the all-zero vector, the all-one vector and the all-two vector, respectively. The length of these vectors will be clear from the context.

Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is also isomorphic to an abelian structure $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and the number of order two codewords in $\mathcal{C}$ 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 α coordinates and Y corresponds to the last β coordinates. Call $\mathcal{C}_X$ (respectively $\mathcal{C}_Y$) the punctured code of $\mathcal{C}$ by deleting the coordinates outside X (respectively Y). Let $\mathcal{C}_b$ be the subcode of $\mathcal{C}$ which contains all order two codewords and let κ be the dimension of $(\mathcal{C}_b)_X$, which is a binary linear code. For the case $\alpha = 0$, we will write $\kappa = 0$. Considering all these parameters, we will say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Throughout this paper, we shall always assume that $\beta > 0$ and we shall specify when α is strictly positive.

Definition 1 Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, which is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. We say that the binary image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*linear code* of binary length $n = \alpha + 2\beta$ and type $(\alpha, \beta; \gamma, \delta; \kappa)$, where γ, δ and κ are defined as above.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. Every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma} \lambda_i \mathbf{u}_i + \sum_{j=1}^{\delta} \mu_j \mathbf{v}_j,$$

where $\lambda_i \in \mathbb{Z}_2$ for $1 \leq i \leq \gamma$, $\mu_j \in \mathbb{Z}_4$ for $1 \leq j \leq \delta$ and $\mathbf{u}_i, \mathbf{v}_j$ are vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ of order two and four, respectively. The vectors $\mathbf{u}_i, \mathbf{v}_j$ give us a generator matrix $\mathcal{G}$ of size $(\gamma + \delta) \times (\alpha + \beta)$ for the code $\mathcal{C}$.

$\mathcal{G}$ can be written as

$$\mathcal{G} = \left(\begin{array}{c|c} B_1 & 2B_3 \\ \hline B_2 & Q \end{array} \right),$$

where B_1, B_2, B_3 are matrices over $\mathbb{Z}_2$ of size $\gamma \times \alpha$, $\delta \times \alpha$ and $\gamma \times \beta$, respectively; and Q is a matrix over $\mathbb{Z}_4$ of size $\delta \times \beta$ with quaternary row vectors of order four.

It is shown in [2] that the generator matrix for a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ can be written in the following standard form:

$$\mathcal{G}_S = \left(\begin{array}{cc|ccc} I_\kappa & T' & 2T_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 2T_1 & 2I_{\gamma-\kappa} & \mathbf{0} \\ \hline \mathbf{0} & S' & S & R & I_\delta \end{array}\right),$$

where T', T_1, T_2, R, S' are matrices over $\mathbb{Z}_2$ and S is a matrix over $\mathbb{Z}_4$.

In [2], the following inner product is defined for any two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$:

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

The *additive dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined in the standard way

$$\mathcal{C}^\perp = \left\{ \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \langle \mathbf{u}, \mathbf{v} \rangle = 0 \quad \text{for all } \mathbf{u} \in \mathcal{C} \right\}.$$

If $C = \phi(\mathcal{C})$, the binary code $\Phi(\mathcal{C}^\perp)$ is denoted by $C_\perp$ and called the $\mathbb{Z}_2\mathbb{Z}_4$-dual code of C. Moreover, in [2] it was proved that the additive dual code $\mathcal{C}^\perp$, which is also a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, is of type $(\alpha, \beta; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$, where

$$\begin{aligned} \bar{\gamma} &= \alpha + \gamma - 2\kappa, \\ \bar{\delta} &= \beta - \gamma - \delta + \kappa, \\ \bar{\kappa} &= \alpha - \kappa. \end{aligned} \tag{1}$$

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Define the usual Hamming weight enumerator of $\mathcal{C}$ to be

$$W_{\mathcal{C}}(x, y) = \sum_{\mathbf{c} \in \mathcal{C}} x^{n-wt(\mathbf{c})} y^{wt(\mathbf{c})},$$

where $n = \alpha + 2\beta$. We know from [1,2,4,8] that this weight enumerator satisfies the MacWilliams identities, i.e.

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + y, x - y).$$

It follows that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and $\mathcal{C}^\perp$ its additive dual code, then $|\mathcal{C}||\mathcal{C}^\perp| = 2^n$, where $n = \alpha + 2\beta$.

The paper is organized as follows. In Sect. 2 we state two upper bounds for the minimum distance of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. Such bounds are simply particular cases of known bounds for codes over rings. In Sect. 3 we define the corresponding two kinds of maximum distance separable (MDS) codes, i.e. codes with minimum distance achieving any of those bounds. We investigate the existence of such MDS codes giving the possible parameters. Moreover, we completely determine the minimum distance of such codes. In Sect. 4, we give examples of all different types of MDS codes. Finally, in Sect. 5 we summarize the results and give some conclusions.

2 Bounds on the minimum distance

The usual Singleton bound [9] for a code $\mathcal{C}$ of length n over an alphabet of size q is given by

$$d(\mathcal{C}) \leq n - \log_q |\mathcal{C}| + 1.$$

This is a combinatorial bound and does not rely on the algebraic structure of the code. It is well known [7] that for the binary case, $q = 2$, the only codes achieving this bound are the repetition codes (with $d(C) = n$), codes with minimum distance 2 and size 2^{n-1} or the trivial code containing all 2^n vectors. We remark that sometimes the singleton codes, i.e. codes with just one codeword, are also considered in this class, but it depends on the definition of minimum distance for such codes.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and let C be its binary Gray image, $C = \Phi(\mathcal{C})$. Since $d(\mathcal{C}) = d(C)$, we immediately obtain

$$d(\mathcal{C}) \leq \alpha + 2\beta - \gamma - 2\delta + 1. \tag{2}$$

This version of the Singleton bound was previously stated for quaternary linear codes ($\alpha = 0$) in [5].

From [5] we know that if $\mathcal{C}$ is a code of length n over a ring R with minimum distance $d(\mathcal{C})$ then

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \leqslant n - rank(\mathcal{C}), \tag{3}$$

where $rank(\mathcal{C})$ is the minimal cardinality of a generating system for $\mathcal{C}$.

Let $\mathcal{X}$ be the map from $\mathbb{Z}_2$ to $\mathbb{Z}_4$ which is the normal inclusion from the additive structure in $\mathbb{Z}_2$ to $\mathbb{Z}_4$, that is $\mathcal{X}(0) = 0$, $\mathcal{X}(1) = 2$ and its extension $(\mathcal{X}, Id) : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \to \mathbb{Z}_4^{\alpha+\beta}$, denoted also by $\mathcal{X}$.

Theorem 1 *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then*

$$\frac{d(\mathcal{C}) - 1}{2} \leqslant \frac{\alpha}{2} + \beta - \frac{\gamma}{2} - \delta; \tag{4}$$

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \leqslant \alpha + \beta - \gamma - \delta. \tag{5}$$

Proof Bound (4) is the same as Bound (2). Clearly $d(\mathcal{C}) \leqslant d(\mathcal{X}(\mathcal{C}))$, hence Bound (5) follows from Bound (3). □

Lemma 1 *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then Bound (4) is strictly stronger than Bound (5) if and only if*

(i) $d(\mathcal{C})$ *is even and* $\alpha \geqslant \gamma$*;*
(ii) $d(\mathcal{C})$ *is odd and* $\alpha > \gamma$*.*

Proof If $d(\mathcal{C})$ is even then Bound (4) is stronger that Bound (5) if and only if

$$\alpha + 2\beta - \gamma - 2\delta + 1 < 2(\alpha + \beta - \gamma - \delta + 1),$$

this reduces to $\gamma - 1 < \alpha$, or similarly, $\alpha \geq \gamma$.

If $d(\mathcal{C})$ is odd then Bound (4) is stronger that Bound (5) if and only if

$$\alpha + 2\beta - \gamma - 2\delta + 1 < 2(\alpha + \beta - \gamma - \delta) + 1,$$

which implies $\gamma < \alpha$. □

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. If $\mathcal{C} = \mathcal{C}_X \times \mathcal{C}_Y$, then $\mathcal{C}$ is called *separable*.

Theorem 2 *If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code which is separable, then the minimum distance is given by*

$$d(\mathcal{C}) = \min\{d(\mathcal{C}_X), d(\mathcal{C}_Y)\}.$$

Proof The code $\mathcal{C}$ is distance invariant [8] i.e. $d(\mathcal{C}) = wt(\mathcal{C})$, where $wt(\mathcal{C}) = \min\{wt(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}, \mathbf{v} \neq \mathbf{0}\}$ is the minimum weight of $\mathcal{C}$.

If $(a, b) \in \mathcal{C}$ then, for a separable code, $(a, \mathbf{0}) \in \mathcal{C}$ and $(\mathbf{0}, b) \in \mathcal{C}$ or similarly $a \in \mathcal{C}_X$, $b \in \mathcal{C}_Y$, and we know that

$$\begin{aligned} d(\mathcal{C}) = wt(\mathcal{C}) &= \min\{wt(a, b) | (a, b) \in \mathcal{C}\} \\ &= \min\{wt(a, \mathbf{0}), wt(\mathbf{0}, b) \mid a \in \mathcal{C}_X, \ b \in \mathcal{C}_Y\} \\ &= \min\{d(\mathcal{C}_X), d(\mathcal{C}_Y)\}. \end{aligned}$$

□

Corollary 1 *If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ which is separable, then*

$$d(\mathcal{C}) \leq \min\left\{\alpha - \kappa + 1, \overline{d}\right\}, \tag{6}$$

where $\overline{d}$ is the maximum value satisfying both Bound (4) and Bound (5).

3 Maximum distance separable codes

We say that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is maximum distance separable (MDS) if $d(\mathcal{C})$ meets the bound given in (4) or (5). In the first case, we say that $\mathcal{C}$ is MDS with respect to the Singleton bound, briefly MDSS. In the second case, $\mathcal{C}$ is MDS with respect to the rank bound, briefly MDSR. Let $\mathcal{C}^i$ be the punctured code of $\mathcal{C}$ by deleting the ith coordinate position.

Lemma 2 *If $\mathcal{C}$ is an MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with $d(\mathcal{C}) > 1$ and $\alpha > 0$ then, if $i \in X$, the minimum distance of $\mathcal{C}^i$ is*

$$d(\mathcal{C}^i) = d(\mathcal{C}) - 1.$$

Proof Let $i \in X$, then $\mathcal{C}^i$ is of type $(\alpha - 1, \beta; \gamma, \delta; \kappa^*)$, where $\kappa - 1 \leqslant \kappa^* \leqslant \kappa$.

We know that $d(\mathcal{C}) - 1 \leqslant d\left(\mathcal{C}^i\right) \leqslant d(\mathcal{C})$. If $d\left(\mathcal{C}^i\right) = d(\mathcal{C})$, then by Theorem 1 we have a contradiction, hence $d\left(\mathcal{C}^i\right) = d(\mathcal{C}) - 1$. □

Proposition 1 *If $\mathcal{C}$ is an MDSR $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, $\alpha > 0$, then $d(\mathcal{C})$ is odd and $\alpha = 1$.*

Proof Assume $d(\mathcal{C})$ is even. Let $i \in X$, $d\left(\mathcal{C}^i\right)$ is odd by Lemma 2. By Theorem 1, we have

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor = \alpha + \beta - \gamma - \delta,$$

and

$$\left\lfloor \frac{d\left(\mathcal{C}^i\right) - 1}{2} \right\rfloor \leqslant \alpha - 1 + \beta - \gamma - \delta.$$

But since $d\left(\mathcal{C}^i\right)$ is odd, this implies that

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor = \left\lfloor \frac{d\left(\mathcal{C}^i\right) - 1}{2} \right\rfloor,$$

which is a contradiction.

If $\alpha > 1, i \in X$ then $d\left(\mathcal{C}^i\right)$ is even where

$$\left\lfloor \frac{d\left(\mathcal{C}\right)-1}{2} \right\rfloor = \left\lfloor \frac{d\left(\mathcal{C}^i\right)-1}{2} \right\rfloor = \alpha - 1 + \beta - \gamma - \delta. \tag{7}$$

Then $\mathcal{C}^i$ is an MDSR code with $\alpha - 1 > 0$ and $d\left(\mathcal{C}^i\right)$ is even, which is a contradiction. □

Now, we characterize all MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. By the *even code* we mean the set of all even weight vectors. By the *repetition code* we mean the code such that its binary Gray image is the binary repetition code with the all-zero and the all-one codewords.

Theorem 3 *Let $\mathcal{C}$ be an MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ such that $1 < |\mathcal{C}| < 2^{\alpha+2\beta}$. Then $\mathcal{C}$ is either*

(i) the repetition code of type $(\alpha, \beta; 1, 0; \kappa)$ and minimum distance $d(\mathcal{C}) = \alpha + 2\beta$, where $\kappa = 1$ if $\alpha > 0$ and $\kappa = 0$ otherwise; or
(ii) the even code with minimum distance $d(\mathcal{C}) = 2$ and type $(\alpha, \beta; \alpha-1, \beta; \alpha-1)$ if $\alpha > 0$, or type $(0, \beta; 1, \beta-1; 0)$ otherwise.

Proof If $\mathcal{C}$ is an MDSS code, so is $C = \Phi(\mathcal{C})$. Therefore C is the binary repetition code or the binary even code (C cannot be the odd code since C contains the all-zero vector). The parameters of $\mathcal{C}$ are clear in both cases. Note also, that cases (i) and (ii) correspond to additive dual codes, so the parameters are related by the equations in (1). □

Since the codes described in (i) and (ii) of Theorem 3 are additive dual codes, it is still true that the dual of an MDSS code is again MDSS, which is a well known property for linear codes over finite fields [7].

We can also give a strong condition for a $\mathbb{Z}_2\mathbb{Z}_4$-additive code to be MDSR.

Theorem 4 *Let $\mathcal{C}$ be an MDSR $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ such that $1 < |\mathcal{C}| < 2^{\alpha+2\beta}$. Then, either*

(i) $\mathcal{C}$ is the repetition code as in (i) of Theorem 3 with $\alpha \leq 1$; or
(ii) $\mathcal{C}$ is of type $(\alpha, \beta; \gamma, \alpha+\beta-\gamma-1; \alpha)$, where $\alpha \leq 1$ and $d(\mathcal{C}) = 4-\alpha \in \{3, 4\}$; or
(iii) $\mathcal{C}$ is of type $(\alpha, \beta; \gamma, \alpha+\beta-\gamma; \alpha)$, where $\alpha \leq 1$ and $d(\mathcal{C}) \leq 2-\alpha \in \{1, 2\}$.

Proof Recall that $\mathcal{C}_b$ is the subcode of $\mathcal{C}$ which contains all order 2 codewords. Let D be the binary linear code which is as $\mathcal{C}_b$ but replacing coordinates 2 with 1. The code D has length $\alpha + \beta$ and dimension $\gamma + \delta$. Obviously, $2d(D) \geq d(\mathcal{C}_b) \geq d(\mathcal{C})$. Since $\mathcal{C}$ is MDSR, we obtain

$$2d(D) \geq 2(\alpha + \beta - \gamma - \delta) + 1,$$

and then

$$d(D) \geq \alpha + \beta - \gamma - \delta + 1,$$

implying that D is a binary MDSS code. Thus D is the binary repetition code, the binary even code or the trivial code containing all vectors.

In the first case, we have that the dimension of D is $\gamma + \delta = 1$ and the minimum distance of $\mathcal{C}$ is

$$d(\mathcal{C}) = 2\alpha + 2\beta - 1 \quad \text{if } d(\mathcal{C}) \text{ is odd},$$
$$d(\mathcal{C}) = 2\alpha + 2\beta \quad \text{if } d(\mathcal{C}) \text{ is even}.$$

If $\alpha = 0$, then $d(\mathcal{C}) = 2\beta - 1$ is not possible because $\mathcal{C}$ contains the all-two vector. Hence $d(\mathcal{C})$ must be even and $d(\mathcal{C}) = 2\beta$ implying that $\mathcal{C}$ is the quaternary code formed by the all-zero and the all-two vectors. If $\alpha > 0$, then by Proposition 1, $d(\mathcal{C})$ is odd and $\alpha = 1$. Therefore $d(\mathcal{C}) = 1 + 2\beta$ and $\mathcal{C} = \{(0, \mathbf{0}), (1, \mathbf{2})\}$.

In the second case, when D is the binary even code, we have that the dimension of D is $\gamma + \delta = \alpha + \beta - 1$. Therefore $d(\mathcal{C}) = 3$ if $d(\mathcal{C})$ is odd, and $d(\mathcal{C}) = 4$ if $d(\mathcal{C})$ is even. If $\alpha > 0$, then $\alpha = 1$ and $d(\mathcal{C})$ is odd, by Proposition 1. If $\alpha = 0$, then we claim that $d(\mathcal{C}) = 4$. Indeed, if $x \in \mathcal{C}$ would have weight 3, then $2x$ would have weight 6 and D would contain a codeword of weight 3, which is not possible.

Finally, if D contains all possible vectors, then its dimension is $\gamma + \delta = \alpha + \beta$. In this case,

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor = 0,$$

and then $d(\mathcal{C}) \leq 2$. By Proposition 1, $\alpha \leq 1$ and if $\alpha = 1$, then $d(\mathcal{C}) = 1$.

This completes the proof. □

Note that it is not true that the additive dual code of an MDSR code is again MDSR. See the examples in the next section.

The *rank* of a binary code C is the dimension of the linear span of C. If C is linear, then the rank is simply the dimension of C. For MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes we can state which are the possible values for the rank of the binary images.

Corollary 2 *If $\mathcal{C}$ is an MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive code, then $C = \Phi(\mathcal{C})$ is a linear code or it has rank equal to* $\log_2 |C| + 1$. *In this last case, $\mathcal{C}$ is an MDSR code with minimum distance* 3 *or* 4.

Proof Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$.

If $\mathcal{C}$ is an MDSS code (cases (i) or (ii) in Theorem 3 or case (i) in Theorem 4), then $C = \Phi(\mathcal{C})$ is clearly a binary linear code. For cases (ii) and (iii) in Theorem 4, we apply the result given in [6] which states that the rank of C must be in the range

$$\gamma + 2\delta, \ldots, \min\left\{\beta + \delta + \kappa, \gamma + 2\delta + \frac{\delta(\delta - 1)}{2}\right\}.$$

For case (ii) in Theorem 4, since $\delta = \alpha + \beta - \gamma - 1$ and $\kappa = \alpha$, we have that

$$\gamma + 2\delta = 2\alpha + 2\beta - \gamma - 2;$$
$$\beta + \delta + \kappa = 2\alpha + 2\beta - \gamma - 1 = \gamma + 2\delta + 1.$$

Therefore, if $\delta \leq 1$, then the rank of C is $\gamma + 2\delta$ and C is linear. If $\delta > 1$, then C is linear or it has rank $\gamma + 2\delta + 1$.

For case (iii) in Theorem 4, we have

$$\gamma + 2\delta = 2\alpha + 2\beta - \gamma;$$
$$\beta + \delta + \kappa = \alpha + 2\beta - \gamma + \kappa.$$

But $\alpha = \kappa$, thus $\gamma + 2\delta = \beta + \delta + \kappa$ and C is linear. □

4 Examples

Examples 1 and 2 satisfy Bound (4). Example 1 is an MDS code with $\gamma = 0$. Example 2 is an MDS code with $\alpha > 1$.

Example 1 Consider a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}_2$ of length 2 with generator matrix

$$\mathcal{G}_2 = (1 \mid 1).$$

The code is of type $(1, 1; 0, 1; 0)$ and $d(\mathcal{C}_2) = 2$. Applying Bound (4) we get that $\mathcal{C}_2$ is an MDSS code. In fact, it is the even code with $\alpha = \beta = 1$. Its additive dual code $\mathcal{C}_2^{\perp}$ is the repetition code $\{(0, 0), (1, 2)\}$, which is MDSS and MDSR. However, note that $\mathcal{C}_2$ is not an MDSR code.

Example 2 Consider a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}_3$ generated by the following generator matrix

$$\mathcal{G}_3 = \left(\begin{array}{cc|c} 0 & 1 & 1 \\ 1 & 1 & 0 \end{array}\right).$$

The code $\mathcal{C}_3$ is of type $(2, 1; 1, 1; 1)$ with minimum weight $d(\mathcal{C}_3) = 2$. This is again an MDSS code, which is the even code for $\alpha = 2$ and $\beta = 1$. The code $\mathcal{C}_3$ is not an MDSR code, but $\mathcal{C}_3^{\perp} = \{(0, 0, 0), (1, 1, 2)\}$ is again MDSS and MDSR.

The next example satisfies Bound (5).

Example 3 Consider a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}_4$ generated by the following generator matrix

$$\mathcal{G}_4 = \left(\begin{array}{c|ccc} 1 & 2 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 1 & 0 & 0 & 2 \end{array}\right).$$

The code $\mathcal{C}_4$ is of type $(1, 3; 3, 0; 1)$ with minimum weight $d(\mathcal{C}_4) = 3$. Thus, $\mathcal{C}_4$ is an MDSR code (but not MDSS).

Codes in Examples 4 and 5 are separable codes where $d(\mathcal{C})$ is $d(\mathcal{C}_Y)$ and $d(\mathcal{C}_X)$ respectively.

Example 4 Let C_8 be the binary linear code of length 8 with $d(C_8) = 4$ and generator matrix

$$G_8 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix},$$

and let $\mathcal{C}_1$ be the quaternary linear code length 1 and minimum weight $d(\mathcal{C}_1) = 2$ with generator matrix

$$\mathcal{G}_1 = (2).$$

The $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}_9 = \mathcal{C}_8 \times \mathcal{C}_1$ has length 9 and has parameters $(8, 1; 5, 0; 4)$. Applying Bound (6) we get

$$d(\mathcal{C}_9) \leqslant \min\{5, 2\} = 2.$$

Example 5 Let C_2 be the binary linear code of length 2 with $d(C_2) = 2$ and generator matrix

$$G_2 = \begin{pmatrix} 1 & 1 \end{pmatrix},$$

and let $\mathcal{C}_4$ be the quaternary linear code with length 4 and minimum weight $d(\mathcal{C}_4) = 4$ generated by

$$\mathcal{G}_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

The $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}_6 = C_2 \times \mathcal{C}_4$ has length 6 and has parameters (2, 4; 3, 1; 1). Applying Bound (6) we get

$$d(\mathcal{C}_6) \leqslant \min\{2, 4\} = 2.$$

The next example gives a general construction for MDS codes meeting Bound (5) starting from binary MDS codes.

Example 6 Let C be a binary $[n, k, d]$ MDS code. Applying χ to all but one coordinate gives a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ with $\alpha = 1$, $\beta = n - 1$, $\gamma = k$, $\delta = 0$ and $d(\mathcal{C}) = 2d - 1$. Then $d = n - k + 1 = \alpha + \beta - \gamma + 1$ so that $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor = \left\lfloor d - \frac{1}{2} \right\rfloor = d - 1 = \alpha + \beta - (\gamma + \delta)$ and meets Bound (5). Of course, this construction works for the even binary code and the repetition binary code which are the possible binary linear MDS codes with more than one codeword.

Finally the next example shows an MDSR $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}_8$. From Examples 1 to 5, all of them have binary linear image but our next example has a binary non-linear image.

Example 7 Let $\mathcal{C}_8$ be an MDSR $\mathbb{Z}_2\mathbb{Z}_4$-additive code given by following generator matrix.

$$\mathcal{G}_8 = \left(\begin{array}{c|ccccccc} 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right).$$

The code $\mathcal{C}_8$ is of type $(1, 7; 5, 2; 1)$ with $d(\mathcal{C}_8) = 3$, it also meets Bound (5). Since $2(0 \,|\, 1110010) * (0 \,|\, 1001101) \notin \mathcal{C}_8$, where $*$ denotes the component-wise product, then from [6] the rank is 10 and therefore; $\mathcal{C}_8$ has a binary non-linear image.

5 Conclusions

As a summary, we enumerate the possible maximum distance separable $\mathbb{Z}_2\mathbb{Z}_4$-additive codes of type $(\alpha, \beta; \gamma, \delta; \kappa)$, with $\beta > 0$ and $\gamma + 2\delta < \alpha + 2\beta$:

1. Repetition codes with two codewords of type $(\alpha, \beta; 1, 0; 1)$, $\alpha > 0$; or $(0, \beta; 1, 0; 0)$ in the quaternary linear case. These are MDSS codes which are also MDSR if and only if $\alpha \leq 1$. Their minimum distance is $\alpha + 2\beta$.

2. Even codes of type $(\alpha, \beta; \alpha - 1, \beta; \alpha - 1)$, $\alpha > 0$, which are MDSS codes but not MDSR; or $(0, \beta; 1, \beta - 1; 0)$ in the quaternary linear case, which are MDSS and MDSR codes. In any case, these codes have minimum distance 2.
3. Codes of type $(1, \beta; \gamma, \beta - \gamma; 1)$ with minimum distance 3. These are MDSR codes but not MDSS, except for $\beta = \gamma = 1$, which is a repetition code. Note that, for $\beta > 1$ and $\gamma = 1$, it is not possible to have minimum distance 3; otherwise the binary Gray image would be an MDSS code that does not exist.
4. Quaternary linear codes of type $(0, \beta; \gamma, \beta - \gamma - 1; 0)$ with minimum distance 4. Again, these are MDSR codes but not MDSS, except for $\gamma = 1$ and $\beta = 2$, which is a repetition code. For $\beta \neq 2$ and $\gamma = 1$, it is not possible to have minimum distance 4; otherwise the binary Gray image would be an MDSS code that does not exist.
5. Codes of type $(\alpha, \beta; \gamma, \alpha + \beta - \gamma; \alpha)$, where $\alpha \leq 1$ and minimum distance $d(\mathcal{C}) \leq 2 - \alpha$. These are MDSR codes but not MDSS, except for the case $(0, \beta; 1, \beta - 1; 0)$ which is already included in 2.

In the first two cases, the binary Gray images are linear codes. In Cases 3 and 4, let C be the binary Gray image of such a code, then C is linear or its linear span has size $2|C|$. In Case 5, the binary Gray images are linear codes.

As a conclusion we have that all MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are zero or one error-correcting codes with the exception of the trivial repetition codes containing two codewords.

Acknowledgments This work has been supported by the Spanish MICINN grants MTM2009-08435 and PCI2006-A7-0616 and the Catalan AGAUR grant 2009 SGR1224.

References

1. Borges J., Fernández C., Pujol J., Rifà J., Villanueva M.: On $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and duality. VJMDA, pp. 171–177, Ciencias, 23. Secr. Publ. Intercamb. Ed., Valladolid (2006).
2. Borges J., Fernández-Córdoba C., Pujol J., Rifà J., Villanueva M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. Des. Codes Cryptogr. **54**(2), 167–179 (2010).
3. Delsarte P.: An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl. **10**, vi + 97 (1973).
4. Delsarte P., Levenshtein V.: Association schemes and coding theory. IEEE Trans. Inform. Theory **44**(6), 2477–2504 (1998).
5. Dougherty S.T., Shiromoto K.: Maximum distance codes over rings of order 4. IEEE Trans. Inform. Theory **47**, 400–404 (2001).
6. Fernández-Córdoba C., Pujol J., Villanueva M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel. Des. Codes Cryptogr. **56**(1), 43–59 (2010).
7. MacWilliams F.J., Sloane N.J.A.: The Theory of Error Correcting Codes. North-Holland Publishing Co., Amsterdam (1977).
8. Pujol J., Rifà J.: Translation invariant propelinear codes. IEEE Trans. Inform. Theory **43**, 590–598 (1997).
9. Singleton R.C.: Maximum distance q-ary codes. IEEE Trans. Inform. Theory **10**, 116–118 (1964).