Universitat Autònoma de Barcelona

Departament d'Enginyeria de la Informació i de les Comunicacions

Codes over Rings: Maximum Distance Separability and Self-Duality

Submitted to Universitat Autònoma de Barcelona
in partial fulfillment of the requirements for the
degree of Doctor of Philosophy in Computer Science

by Muhammad Bilal

Supervised by Dr. Joaquim Borges i Ayats and Dr. Cristina Fernández-Córdoba

Bellaterra, October 5, 2012

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Bellaterra, October 5, 2012

Dr. Joaquim Borges i Ayats (Adviser)

Dr. Cristina Fernández-Córdoba (Adviser)

To my family

Abstract

Bounds on the size of a code are an important part of coding theory. One of the fundamental problems in coding theory is to find a code with largest possible distance d. Researchers have found different upper and lower bounds on the size of linear and nonlinear codes; e.g., Plotkin, Johnson, Singleton, Elias, Linear Programming, Griesmer, Gilbert and Varshamov bounds. In this dissertation we have studied the Singleton bound, which is an upper bound on the minimum distance of a code, and have defined maximum distance separable (MDS) $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. Two different forms of these bounds are presented in this work where we have characterized all maximum distance separable $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with respect to the Singleton bound (MDSS codes) and strong conditions are given for maximum distance separable $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with respect to the rank bound (MDSR codes).

Generation of new codes has always been an interesting topic, where one can study the properties of these newly generated codes and establish new results. Self-dual codes are an important class of codes. There are numerous constructions of self-dual codes from combinatorial objects. In this work we have given two methods for generating self-dual codes from 3-class association schemes, namely pure construction and bordered construction. Binary self-dual codes are generated by using these two methods from non-symmetric 3-class association schemes and self-dual codes from rectangular association schemes are generated over $\mathbb{Z}_k$.

Borges, Dougherty and Fernández-Córdoba in 2011 presented a method to generate new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes from existing $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes by extending their length. In this work we have verified whether properties like separability, antipodality and code Type are retained or not, when using this method.

Acknowledgments

The work done during my stay at Universitat Autònoma de Barcelona has been made possible by the help and positive critique of a many people who guided me through this journey and made it possible for me to complete my thesis.

I would like to start by thanking Josep Rifà for giving me an opportunity to work at the Combinatorics, Coding and Security Group (CCSG) research group. I thank all the group members for welcoming me and helping me adjust in the new environment.

I would like to express my deepest appreciation to my supervisors Quim and Cristina for their support and guidance throughout my dissertation. They have been very patient with me and at times have ignored my mistakes. Their positive attitude towards things has helped me a lot during this research period and without their mentorship and help, I could not have completed my dissertation.

I would also like to thank the people at the departament d'Enginyeria de la Informació i de les Comunicacions for welcoming me from the first day and making me feel comfortable working here. I thanks my fellow students, seniors and juniors, for all their help and support.

I thank Steven Dougherty for all his ideas and I wish to acknowledge his helpful comments on our research work.

In the end I thank my parents, who are back home in Pakistan but their prayers have always been with me. I thank my parents-in-law for their prayers. My wonderful wife, Sundus, for her help and support during our study period, be it at Sweden or here in Spain. She has been with me through thick and thin and has been a inspiration for me. My beautiful son Ayaan, whose addition to our small family is the most wonderful thing that happened to me and has been a motivation for me to do more in life. I thank you all once again.

Preface

This thesis is written to show the work that has been done during my stay at the Departament of Information and Communication Engineering at Universitat Autònoma de Barcelona. The thesis is presented in the form of a compendium of publications.

The thesis starts with an introduction to how the communication technologies have been developed through the history and how an article written by Claude Shannon brought revolution in the field of communications and started the field of information theory and coding theory. An introduction to binary, quaternary and $\mathbb{Z}_2\mathbb{Z}_4$-additive codes is given. The second chapter comprises of basics of binary, quaternary and $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. We define minimum distance, minimum weight, inner product, generator matrix, parity check matrix, dual codes and self-dual codes. The third chapter consists of the theory related to the contributions and a short description for each contribution. We start by talking about bounds on the minimum distance of codes, in particular the Singleton bound, which we apply to $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. After this, we give contributions related to this topic. Next, association schemes are defined and we discuss how we have constructed self-dual codes from the adjacency matrices of 3-class association schemes. We give descriptions for the contributions related to these constructions. Finally, extension of $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes is discussed in the light of the work done in [BDFC12] and we check if certain properties of these new codes are retained or not. We also list the related contributions for it. In the fourth chapter, one can read the summary of all the work done during my Ph.D., and also we give ideas about possible future research topics. I hope you have a good read.

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

Contents

Chapter 1

Introduction

Every day, we come in contact with and use various modern communication systems and media, the most common being mobile phones, television, Internet, etc. Using these media we instantly come in contact with people in different cities, countries and continents. We are instantly informed about different events that occur around the world through Internet and television. Email and social media have made it possible to instantly send messages to your friends and family across the globe. We can not imagine a world without these means of communications and yet most of these important communication systems were made during the last century. If we go back in the history, we can take a look at the most important developments in the last 2 centuries.

One of the earliest invention of significance importance was the electric battery in 1799 made by Alessandro Volta. This made it possible for Samuel Morse to develop electric telegraph, which was the first electronic method of communication. Telephony came into being by the invention of telephone in 1870 by Alexander Graham Bell and the first telephony company, Bell Telephone Company, was established in 1877. The development of wireless communication started from the work of Oersted, Faraday, Gauss, Maxwell and Hertz during the nineteenth century. There has been significant growth in communication services during the last 65 years. The invention of transistor in 1947 by Walter Brattain, John Bardeen and William Shockley; the integrated circuit in 1958 by Jack Kilby and Robert Noyce; and the laser by Townes and Schawlow in 1958, have made it possible to develop small-size, low-power, low-weight and high-speed electronic circuits that are used in construction of satellite communication systems, wideband microwave radio systems and lightwave communication systems using fiver optic cables.

In 1948, Claude Shannon published the landmark paper “A mathematical theory of communication" [Sha48] that signified the beginning of both information theory and coding theory. Given a communication channel which may corrupt information sent over it, Shannon identified a number called *channel capacity* and prove that some reliable communication is possible at a rate that is below the channel capacity. The results given by Shannon guarantee that data can be encoded in such a way before transmission that the altered data can be decoded with a specified degree of accuracy. Some examples where we use these results are storage devices, compact discs and communication done over mobile phones. Please refer to [PS01] to read further about the history of communication systems.

The communication channels contain a source that sends information over a channel to a receiver. For example, in a compact disc, the information is in the form of text, audio or video. The information is placed on the disc which acts as a channel and we, the users, are the receivers. The channel can be noisy, meaning that information sent over it may contain errors when received at the other end. Suppose that binary data is being sent over a channel. Ideally when we sent 0 we would like to receive 0 but due to noise in the channel sometime we will receive 1 instead. Noise in a compact disc can be caused by fingerprints or scratches on the disc. The fundamental problem in coding theory is to determine what message was sent on the basis of what is received.

In a simple communication channel, we have a source with a message $\mathbf{x}$, containing k information bits which is to be sent to the receiver. The message passes through the channel to the receiver. Any noise may distort the message and it will not be recoverable at the receiver side. To counter this problem we add redundancy to the message. The source passes the message $\mathbf{x}$, containing k bits of information, to the encoder, see 1.1. The encoder sends n bits to the channel, meaning it adds $n-k$ bits of redundancy to the message. The amount of redundancy added by the encoder is measured by the ratio n/k. The reciprocal of this ratio, namely k/n is called *code rate*. The channel adds noise $\mathbf{e}$ to the message and a distorted message $\mathbf{y}$ is received. The received message is sent to the decoder where errors are removed, redundancy is stripped off and an estimate message $\hat{\mathbf{x}}$ is obtained. Shannon's Theorem guarantees that our hopes will be fulfilled a certain percentage of the time. Refer to [HP03] to read further about communication channels and coding theory.

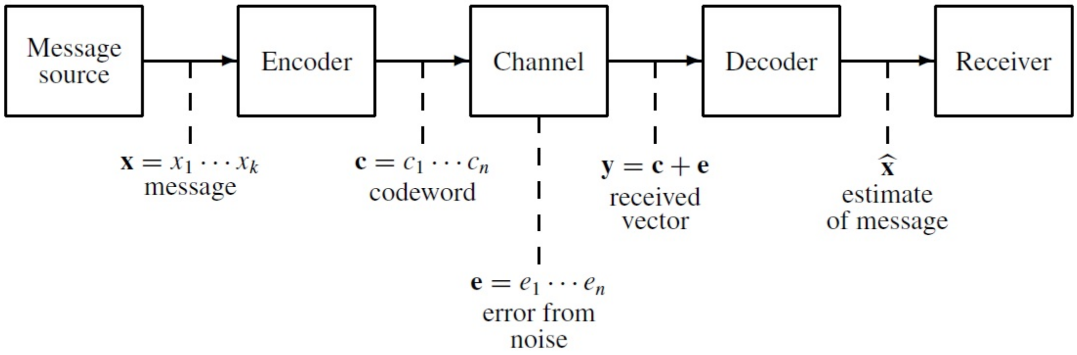
Message source
Encoder
Channel
Decoder
Receiver
$\mathbf{x} = x_1 \cdots x_k$ message
$\mathbf{c} = c_1 \cdots c_n$ codeword
$\mathbf{y} = \mathbf{c} + \mathbf{e}$ received vector
$\widehat{\mathbf{x}}$ estimate of message
$\mathbf{e} = e_1 \cdots e_n$ error from noise

Figure 1.1: Communication Channel

Binary codes are the most commonly used codes in communications. Thus, codes are subsets of $\mathbb{Z}_2^n$, which is a space of binary words of length n. Linear codes are the most commonly used and studied codes because of their algebraic structure and because they are easier to encode and decode than non-linear codes. For any linear code there is a generator matrix which is used to generate codewords.

The study of codes over the ring $\mathbb{Z}_4$ attracted great interest through the work of Calderbank, Hammons, Kumar, Sloane, and Solé in the early 1990's which resulted in the publication of a paper [HKC$^+$94] showing how several well-known families of nonlinear binary codes were related to linear codes over $\mathbb{Z}_4$. A binary code with an algebraic structure over $\mathbb{Z}_4$ is called $\mathbb{Z}_4$-linear code and the codes which are defined as additive subgroups of $\mathbb{Z}_4$ are called *quaternary linear codes*. In [HKC$^+$94], it was proved that the well-known Kerdock and Preparata-like codes are $\mathbb{Z}_4$-linear codes and, moreover, they are $\mathbb{Z}_4$-dual codes.

Additive codes were first defined by Delsarte in 1973 in terms of association schemes [Del73], [DL98]. In general, an additive code, in a translation association scheme, is defined as a subgroup of the underlying abelian group. On the other hand, translation invariant propelinear codes were first defined by Pujol and Rifà in 1997 in [PR97] where it is proved that all these binary codes are group-isomorphic to subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \times \mathbb{Q}_8^\sigma$, being $\mathbb{Q}_8$ the non-abelian quaternion group on eight elements. In the special case when the association scheme is the binary Hamming scheme, that is, when the underlying abelian group is of order 2^n, the additive codes coincide with the abelian translation invariant propelinear codes. Hence, as it is pointed out in [DL98], the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ with $\alpha + 2\beta = n$, $(\alpha, \beta \geq 0)$. Therefore, the subgroups $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in the binary Hamming scheme.

Chapter 2

Coding Theory

This is an introductory chapter where we give basic definitions for binary codes, codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. We define the minimum distance, minimum weight, generator matrix, parity-check matrix, dual codes and self-dual codes over all the rings mentioned above.

2.1 Binary Codes

Let $\mathbb{Z}_2$ be the ring of integers modulo two. Let $\mathbb{Z}_2^n$ be the set of all binary words of length n. A subset C of $\mathbb{Z}_2^n$ is called a *binary code* of length n and an element $v \in C$ is called a *codeword*. When C is a linear subspace of $\mathbb{Z}_2^n$, C is a *linear code*, and the sum of two codewords is also a codeword; i.e., $v + w \in C$ for all $v, w \in C$. If C is a linear code, we say that C is an (n, k) code, where n is the *length* and k represents the *dimension* of the linear subspace C in $\mathbb{Z}_2^n$. The number of codewords present are $|C| = 2^k$.

The *Hamming weight* of a vector $v \in \mathbb{Z}_2^n$ is the number of nonzero coordinates of v and is denoted by $w_H(v)$. For example, the Hamming weight of the vector $v = (0, 1, 1, 0, 0, 1, 1)$ $\in \mathbb{Z}_2^7$ is 4. The *Hamming distance* between two vectors $v, w \in C$ is the number of coordinates in which v and w differ from one another and it is denoted by $d_H(v, w)$. The *minimum Hamming distance* of a code C is denoted by $d_H(C)$ and is given as:

$$d_H(C) = \min \{d_H(v, w) : v, w \in C, v \neq w\}.$$

The *minimum Hamming weight* of a code C is defined as

$$w_H(C) = \min\{w_H(v) : v \in C,\ v \neq \mathbf{0}\},$$

where **0** denotes the all-zero vector.

Let C be a binary code of length n with A_i being the number of codewords of Hamming weight *i*. Then $\{A_1, A_2, \ldots, A_n\}$ is called the *weight distribution* of C. The Hamming weight enumerator for a binary code C is defined as

$$W_C(X_0, X_1) = \sum_{i=1}^{n} A_i {X_0}^{n-i} {X_1}^{i}.$$

W_C is a homogeneous polynomial of degree *n* in X_0 and X_1.

A code C is *distance invariant* if the Hamming weight distribution of $c + C$ is the same for all $c \in C$. Note that all linear codes must be distance invariant simply because $c + C = C$, for all $c \in C$.

Let C be an (n, k) binary linear code. It is possible to find k linearly independent codewords in C such that every codeword v in C is a linear combination of these k codewords; that is, there exists a set of linearly independent codewords $\{g_0, g_1, \ldots, g_{k-1}\}$ such that

$$v = u_0 g_0 + u_1 g_1 + \ldots + u_{k-1} g_{k-1},$$

where $u_i \in \{0, 1\}$, for $0 \leqslant i < k$. We can arrange these k linearly independent codewords as the rows of a $k \times n$ matrix

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix},$$

where G is called the *generator matrix* for C. The *parity check matrix* H of a code C is a

$(n-k) \times n$ matrix whose rows generate the orthogonal code of C; i.e.,

$$v \cdot H^T = 0, \text{ if and only if } v \in C.$$

For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for C. The remaining $r = n - k$ coordinates are termed a redundancy set and r is called the *redundancy of C*. If the first k coordinates form an information set, the code has a unique generator matrix of the form

$$G_S = [I_k P],$$

where I_k is the $k \times k$ identity matrix and P is the redundancy matrix of size $k \times r$. Such a generator matrix is in *standard form*. For a code C with generator matrix G_S, the parity check matrix is given as:

$$H_S = \left[P^T I_{n-k}\right].$$

Two codes C_1 and C_2 are said to be *permutation-equivalent*, if one can be obtained from the other by permuting the coordinates. The *inner product* of two vectors $v, w \in \mathbb{Z}_2^n$ is defined as:

$$(v, w) = \sum_{i=1}^{n} v_i w_i.$$

Let C be a binary linear code of length *n* and dimension *k*, we define the dual of C, $C^\perp$, as the orthogonal space of C given as

$$C^\perp = \{v \in \mathbb{Z}_2^n : (v, w) = 0, \ \forall\, w \in C\}.$$

The dual of a binary linear code is again a binary linear code. The dual code $C^\perp$ for the code C with dimension k has dimension $n - k$. The parity check matrix H of a code C is the generator matrix for $C^\perp$. The code C is said to be *self-dual* if it is equal to its dual; i.e., $C = C^\perp$ and *self-orthogonal* if it is contained in its dual; i.e., $C \subseteq C^\perp$.

If we know the weight distribution of a linear binary code then the distribution of its dual can be computed by the MacWilliams identities [MS83].

According to MacWilliams identities, two equivalent formulations of the result for binary dual codes are:

$$W_{C^{\perp}}(X_0, X_1) = \frac{1}{|C|} W_C(X_0 + X_1, X_0 - X_1). \tag{2.1}$$

$$\sum_{u \in C^{\perp}} X_0^{n-wt(u)} X_1^{wt(u)} = \frac{1}{|C|} \sum_{u \in C} (X_0 + X_1)^{n-wt(u)} (X_0 - X_1)^{wt(u)}. \tag{2.2}$$

A binary self-dual code C with all weights divisible by 4 is of Type II; otherwise, the code C is of Type I. A Type I code may or may not be of Type II, but all Type II codes are also of Type I. A self-dual code is said to be *strictly* Type I if it is of Type I and not of Type II.

Example 1 *The code $C_1 = \{00, 11\}$ is a (2,1) code with weight enumerator polynomial $x^2 + y^2$ and it is a strictly Type I code.*

2.2 Codes over $\mathbb{Z}_4$

Let $\mathbb{Z}_4$ be the ring of integers mod 4 and let $\mathbb{Z}_4^n$ be the set of all n-tuples over $\mathbb{Z}_4$; i.e.,

$$\mathbb{Z}_4^n = \{ (x_1, x_2, ...x_n) | \, x_i \in \mathbb{Z}_4 \;\; for \; i = 1, 2, \dots, n \}.$$

Any non-empty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is called a *quaternary code* or a code over $\mathbb{Z}_4$ and n is the length of the code. Any n-tuple in a quaternary code $\mathcal{C}$ is called a *codeword* of $\mathcal{C}$. Any additive subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear* code.

Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be *equivalent*, if one can be obtained from the other by permuting the coordinates and, if needed, changing the sign of certain coordinates. Quaternary codes that differ only by a permutation of coordinates are said to be *permutation-equivalent*. The *automorphism group $Aut(\mathcal{C})$* of a quaternary code $\mathcal{C}$ is the group generated by all permutations and sign-changes of the coordinates that preserves the set of codewords of $\mathcal{C}$.

Let $\mathcal{C}$ be a quaternary linear code of length n. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is 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

$|C| = 2^{\gamma+2\delta}$ codewords and $2^{\gamma+\delta}$ of these codewords have order two including the all-zero codeword.

Let $\mathcal{C}$ be a quaternary linear code of length n. A $k \times n$ matrix G over $\mathbb{Z}_4$ is called a *generator matrix* for $\mathcal{C}$ if the rows of G generate $\mathcal{C}$ and there is no proper subset of the rows of G that generates $\mathcal{C}$.

Proposition 1 *[HKC*$^+$*94] Any quaternary linear code $\mathcal{C}$ containing some nonzero codewords is permutation-equivalent to a quaternary linear code with a generator matrix of the form*

$$\begin{bmatrix} I_\delta & A & B \\ 0 & 2I_\gamma & 2C \end{bmatrix}, \tag{2.3}$$

where A and C are matrices over $\mathbb{Z}_4$ with all its entries in $\{0,1\} \subset \mathbb{Z}_4$ and B is a matrix over $\mathbb{Z}_4$. $\mathcal{C}$ is of type $4^\delta 2^\gamma$ and contains $2^{2\delta+\gamma}$ codewords.

Example 2 *Let $\mathcal{K}_4$ denote a quaternary linear code with generator matrix*

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix}.$$

$\mathcal{K}_4$ is of type $4^1 2^2$. If we compare this generator matrix to Equation (2.3) we can clearly see that

$$I_\delta = [1]\,,\; A = \begin{bmatrix} 1 & 1 \end{bmatrix},$$
$$B = [1]\,,\; I_\gamma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\; C = [1]\,.$$

The inner product of any two vectors $v, w \in \mathbb{Z}_4^n$ is defined as

$$(v,w) = \sum_{i=1}^{n} v_i w_i.$$

Let $\mathcal{C}$ be a quaternary linear code of length n, we define the dual code of $\mathcal{C}$, $\mathcal{C}^\perp$, as the orthogonal space of $\mathcal{C}$ given as

$$C^{\perp} = \{v \in \mathbb{Z}_4^n : (v, w) = 0, \ \forall\, w \in C\},$$

The dual code $\mathcal{C}^{\perp}$ of a quaternary linear code $\mathcal{C}$ with generator matrix given by Equation (2.3) has the following generator matrix

$$\begin{bmatrix} -B^t - C^tA^t & C^t & I_{n-\delta-\gamma} \\ 2A^t & 2I_\gamma & 0 \end{bmatrix},$$

where n is the length of $\mathcal{C}$. $\mathcal{C}^{\perp}$ is an abelian group of type $4^{n-\delta-\gamma}2^{\gamma}$ and it contains $2^{2n-2\delta-\gamma}$ codewords.

The Lee weights of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$, respectively. Hence, for a vector $v = (v_1, \ldots, v_n) \in \mathbb{Z}_4^n$ the Lee weight is given as $w_L(v) = \sum_{i=1}^{n} w_L(v_i)$. The Lee weight function defines a distance function called *Lee distance* defined as

$$d_L(u, v) = w_L(u - v),$$

where u and v are vectors over in $\mathbb{Z}_4^n$. The *minimum Lee distance* for a code $\mathcal{C}$ is the minimum value of $d_L(u, v)$ for $u, v \in \mathcal{C}$ such that $u \neq v$. We denote it by $d_L(\mathcal{C})$. The *minimum Lee weight* of a code $\mathcal{C}$ is defined as

$$w_L(\mathcal{C}) = \min\{w_L(v) : v \in \mathcal{C}, \ v \neq \mathbf{0}\},$$

where **0** denotes the all-zero vector.

The Gray map, ϕ, provides a one-to-one correspondence between a $\mathbb{Z}_4$ and $\mathbb{Z}_2^2$:

$$\begin{aligned} &\mathbb{Z}_4 \xrightarrow{\phi} \mathbb{Z}_2^2 \\ &0 \longrightarrow 00 \\ &1 \longrightarrow 01 \quad . \\ &2 \longrightarrow 11 \\ &3 \longrightarrow 10 \end{aligned}$$

If $\mathcal{C}$ is a quaternary code, then $C = \phi(\mathcal{C})$ is the binary image of $\mathcal{C}$ under ϕ, where $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$ is the component-wise extended function. A binary code C is said to be $\mathbb{Z}_4$-*linear* if its coordinates can be arranged in a way that it is an image under the Gray map of a quaternary linear code.

Perhaps the most important property of the Gray map is that it preserves the weights of vectors during transformation from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$; i.e.,

$$w_L(u) = w(\phi(u)), \forall u \in \mathbb{Z}_4^n.$$

In general, the $\mathbb{Z}_4$-linear code $C = \phi(\mathcal{C})$ is not linear, so it may not have a dual. The $\mathbb{Z}_4$-dual of $\phi(\mathcal{C})$ is $C_\perp = \phi(\mathcal{C}^\perp)$

$$\begin{tikzcd} \mathcal{C} \arrow[r, "\phi"] \arrow[d, "\perp"] & C = \phi(\mathcal{C}) \\ \mathcal{C}^\perp \arrow[r, "\phi"] & C_\perp = \phi(\mathcal{C}^\perp). \end{tikzcd}$$

Although the two codes $C = \phi(\mathcal{C})$ and $C_\perp = \phi(\mathcal{C}^\perp)$ may not be dual, they are called *formally dual* which means that the weight enumerators of the binary codes are related under *MacWilliams identities*, see Equations (2.1), (2.2).

2.3 $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

If $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, then $\mathcal{C}$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code*. We will take an extension of the usual Gray map denoted by Φ: $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n$, where $n = \alpha + 2\beta$, given by

$$\Phi\left(v, w\right) = \left(v, \phi\left(w_1\right), \ldots,\ \phi\left(w_\beta\right)\right),\ \forall\, v \in \mathbb{Z}_2^\alpha,\ \forall\ \left(w_1, \ldots, w_\beta\right) \in \mathbb{Z}_4^\beta;$$

where ϕ: $\mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$ is the usual Gray map defined earlier.

The binary image of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code under the extended Gray map is called a

$\mathbb{Z}_2\mathbb{Z}_4$-*linear code* and has length $n = \alpha + 2\beta$. Since a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is also isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. So $\mathcal{C}$ is of type $2^\gamma 4^\delta$, the number of codewords in $\mathcal{C}$ is $|\mathcal{C}| = 2^{\gamma+2\delta}$ and the number of order two codewords of $\mathcal{C}$ is $2^{\gamma+\delta}$. This Gray map is an isometry which transforms Lee distances defined in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ to Hamming distances defined in $\mathbb{Z}_2^{\alpha+2\beta}$.

Let $v_1 \in \mathbb{Z}_2^n$ and $v_2 \in \mathbb{Z}_4^\beta$. Denote by $w_H(v_1)$ the Hamming weight of v_1 and $w_L(v_2)$ the Lee weight of v_2. For a vector $v = (v_1, v_2) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, define the weight of v, denoted by $w(v)$ as $w_H(v_1) + w_L(v_2)$ or, equivalently, the Hamming weight of $\Phi(v)$. Denote by $d\left(\mathcal{C}\right)$ the minimum distance between codewords in $\mathcal{C}$, where the distance between two vectors $v, w \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is given as

$$d\left(u, v\right) = w\left(u - v\right).$$

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 $\alpha = 0$, κ is 0.

Taking into account all the parameters mentioned above we say $\mathcal{C}$ is of type $(\alpha,\ \beta;\ \gamma,\ \delta;\ \kappa)$. Two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes of the same type are said to be *monomially-equivalent*, if one can be obtained from the other by permutation of the coordinates and, if needed, also by changing the signs of certain $\mathbb{Z}_4$ coordinates. If two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomially-equivalent, then after Gray map the $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are permutation-equivalent as binary codes. The inverse may not be true.

The $\mathbb{Z}_2\mathbb{Z}_4$-additive codes of type $(\alpha,\ \beta;\ \gamma,\ \delta;\ \kappa)$ are a generalization of binary linear codes and quaternary linear codes. If $\beta = 0$, a $\mathbb{Z}_2\mathbb{Z}_4$-additive code is a binary linear code and if $\alpha = 0$, a $\mathbb{Z}_2\mathbb{Z}_4$-additive code is a quaternary linear code.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. Although $\mathcal{C}$ is not a free module, every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma} \lambda_i u_i + \sum_{j=\gamma+1}^{\gamma+\delta} \mu_j v_j,$$

where $\lambda_i \in \mathbb{Z}_2$, $\mu_j \in \mathbb{Z}_4$ and $u_i,\ v_j \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ for $1 \leqslant i \leqslant \gamma$ and $\gamma+1 \leqslant j \leqslant \gamma+\delta$. These $\gamma+\delta$ vectors give us a generator matrix $\mathcal{G}$ of size $(\gamma+\delta)\times(\alpha+\beta)$ for a code $\mathcal{C}$. $\mathcal{G}$ is given as

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

where B_1, B_2 are matrices over $\mathbb{Z}_2$ of size $\gamma\times\alpha$ and $\delta\times\alpha$, respectively; B_3 is a matrix over $\mathbb{Z}_4$ of size $\gamma\times\beta$ with all entries in $\{0,1\}\subset\mathbb{Z}_4$ and Q is a matrix over $\mathbb{Z}_4$ of size $\delta\times\beta$ with quaternary row vectors of order four.

Theorem 2 *[BFCP$^+$10] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha,\ \beta;\ \gamma,\ \delta;\ \kappa)$. Then, $\mathcal{C}$ is permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with canonical generator matrix of the form*

$$\mathcal{G}_S = \left[\begin{array}{cc|ccc} I_k & T_b & 2T_2 & 0 & 0 \\ 0 & 0 & 2T_1 & 2I_{\gamma-\kappa} & 0 \\ \hline 0 & S_b & S_q & R & I_\delta \end{array}\right],$$

where T_b, S_b are matrices over $\mathbb{Z}_2$; T_1, T_2, R are matrices over $\mathbb{Z}_4$ with all entries in $\{0,1\}\subset\mathbb{Z}_4$ and S_q is a matrix over $\mathbb{Z}_4$.

We define the inner product of vectors $u, v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ as

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

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha,\ \beta;\ \gamma,\ \delta;\ \kappa)$. The additive dual code of $\mathcal{C}$ denoted by $\mathcal{C}^\perp$ is defined as

$$\mathcal{C}^\perp = \left\{ v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \,|(u,v) = 0,\, \forall\, u \in \mathcal{C} \right\}.$$

The additive dual code $\mathcal{C}^\perp$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. The weight enumerator polynomial of $C = \Phi(\mathcal{C})$ is related to the weight enumerator polynomial of $\Phi(\mathcal{C}^\perp)$ by MacWilliams identities, see Equations (2.1), (2.2).

Theorem 3 *[BFCP$^+$10] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha,\ \beta;\ \gamma,\ \delta;\ \kappa)$. The* *additive dual code $\mathcal{C}^\perp$ is of type $(\alpha, \beta; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$, where*

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

Theorem 4 *[BFCP+10] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha,\ \beta;\ \gamma,\ \delta;\ \kappa)$ with generator matrix $\mathcal{G}_S$, then the dual code $\mathcal{C}^\perp$ has generator matrix of the form*

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

where T_b, T_2 are matrices over $\mathbb{Z}_2$; T_1, R, S_b are matrices over $\mathbb{Z}_4$ with all entries in $\{0, 1\} \subset \mathbb{Z}_4$ and S_q is a matrix over $\mathbb{Z}_4$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, we say that $\mathcal{C}$ is an additive self-orthogonal code if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and $\mathcal{C}$ is an additive self-dual code if $\mathcal{C} = \mathcal{C}^\perp$.

Lemma 5 *[BDFC12] If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code, then $\mathcal{C}$ is of type $(2\kappa, \beta; \beta + \kappa - 2\delta, \delta; \kappa)$, $|C| = 2^{\kappa+\beta}$ and $|C_b| = 2^{\kappa+\beta-\delta}$.*

Lemma 6 *[BDFC12] If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code, then the subcode $(C_b)_X$ is a binary self-dual code.*

Denote by $\mathbf{1}$ and $\mathbf{2}$ the all one and all two vectors. A binary code C is *antipodal* if for any codeword $z \in C$, $z + \mathbf{1} \in C$, otherwise it is *non-antipodal*. If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, we say that $\mathcal{C}$ is antipodal if $\Phi(\mathcal{C})$ is antipodal. Clearly, a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is antipodal if and only if $(\mathbf{1}^\alpha, \mathbf{2}^\beta) \in \mathcal{C}$, where α and β indicate the length of the all-one and all-two vectors, respectively.

Example 3 *Consider a code $\mathcal{C}_1$ with generator matrix*

$$\mathcal{G} = \left[\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 0 & 2 \\ \hline \end{array}\right].$$

The code $\mathcal{C}_1$ is of type $(2,1;2,0;1)$ and has the following codewords

$$\mathcal{C}_1 = \{(00\,|\,0),(00\,|\,2),(11\,|\,0),(11\,|\,2)\}.$$

We can easily see that this code is antipodal as $(11\,|\,2) \in \mathcal{C}$.

Proposition 7 *[BDFC12] Let $\mathcal{C}$ be an additive self-dual code of type $(2\kappa, \beta; \beta+\kappa-2\delta, \delta; \kappa)$. The following statements are equivalent*

- *$\mathcal{C}_X$ is binary self-orthogonal.*
- *$\mathcal{C}_X$ is binary self-dual.*
- *$|\mathcal{C}_X| = 2^{\kappa}$.*
- *$\mathcal{C}_Y$ is a quaternary self-orthogonal code.*
- *$\mathcal{C}_Y$ is a quaternary self-dual code.*
- *$|\mathcal{C}_Y| = 2^{\beta}$.*
- *$\mathcal{C} = \mathcal{C}_X \oplus \mathcal{C}_Y$.*

Proposition 8 *[BDFC12] If $\mathcal{C}_X$ is a binary self-dual code of length $\alpha = 2\kappa$ and $\mathcal{C}_Y$ is a quaternary self-dual code of type $(0,\beta;\gamma,\delta;\kappa)$ then $\mathcal{C} = \mathcal{C}_X \oplus \mathcal{C}_Y$ is an additive self-dual code of type $(2\kappa,\beta;\beta+\kappa-2\delta,\delta;\kappa)$.*

Definition 9 *A $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}$ with even and odd weights is of Type 0. A $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}$ with all weights divisible by 2 is of Type I and a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}$ with all weights divisible by 4 is of Type II. A Type I code may or may not be of Type II, but all Type II codes are also of Type I.*

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. If $\mathcal{C} = \mathcal{C}_X \oplus \mathcal{C}_Y$, then $\mathcal{C}$ is called *separable*. If $\mathcal{C}$ is a separable $\mathbb{Z}_2\mathbb{Z}_4$-additive code, then the generator matrix of $\mathcal{C}$ in standard form is

$$\mathcal{G}_S = \left[\begin{array}{cc|ccc} I_k & T' & 0 & 0 & 0 \\ 0 & 0 & 2T_1 & 2I_{\gamma-\kappa} & 0 \\ 0 & 0 & S_q & R & I_\delta \end{array}\right].$$

Theorem 10 *[BDFC12] If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of Type I or Type II, then $\mathcal{C}$ is antipodal.*

Theorem 11 *[BDFC12] If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of Type 0, then $\mathcal{C}$ is non-separable and non-antipodal.*

Chapter 3

Contributions

This chapter contains the basic theory on bounds on the size of codes, definition of the Singleton bound, association schemes, self-dual codes from 3-class association schemes and extensions of $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes along with the contributions. We start with the bounds on the size of codes and define the Singleton bound. We define an MDS code. Then we state the contributions related to this topic and give a short description for them. Next we give a little history of association schemes and define them. We define intersection numbers, symmetric association schemes, non-symmetric association schemes and adjacency matrices. A short description of the work done on the generation of self-dual codes from 2-class association schemes in [DKS07] is given, which motivated us to generate self-dual code from 3-class association schemes. Contributions related to this topic are stated along with a short summary for each of them. The last section is about extension of $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes. We study the work done in [BDFC12] and see if the properties like Type, separability and antipodality are preserved when one extends the length of a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code. The contribution related to this topic is also given.

3.1 Optimal $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

3.1.1 Bounds on the size of codes

In this section we will describe codes that have as many codewords as possible for a given length and minimum distance. The minimum distance d of a codeword, Hamming or Lee, is a simple measure of the goodness of a code. One of the fundamental problems in coding theory is to produce a code with largest possible d. Alternatively, determine the maximum number of codewords, $A(n,d)$, for a given n and d. A (n,M,d) code $\mathcal{C}$ is a code with length n, distance d and M codewords. A code of length n and minimum distance at least d will be called *optimal* if it has $A\left(n,d\right)$ codewords. There can be other ways to define optimal codes; e.g., one can find the largest d for a given n and M, such that there exists a code with M codewords, length n and minimum distance d, or find the smallest n for a given d and M, such that there exists a code with M codewords, length n and minimum distance d.

3.1.2 Singleton Bound

The Singleton bound, which was introduced by Richard Collom Singleton in 1964 [Sin64], is an upper bound on the minimum distance of a code. We start by defining the bound for binary codes.

Theorem 12 (Singleton Bound [Sin64]) *Let C be a binary (possibly nonlinear) code of length n with minimum Hamming distance $d_H(C)$, then*

$$d_H(C) \leqslant n - \log_2 |C| + 1. \tag{3.1}$$

The Singleton bound is a rather weak bound in general, codes that meet this bound are known as *MDS* or *maximum distance separable* codes. MDS contains a very important class of codes known as Reed-Solomon codes, useful in many applications. This is a combinatorial bound and does not rely on the algebraic structure of the code. It is well known [MS83] that for the binary case, the only codes achieving this bound are the repetition codes, 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.

In the case of quaternary codes, we consider the rank bound. From [DS01], we know that if $\mathcal{C}$ is a code of length n over $\mathbb{Z}_4$ with minimum Lee distance $d_L(\mathcal{C})$ then

$$\left\lfloor \frac{d_L(\mathcal{C})-1}{2} \right\rfloor \leqslant n - rank(\mathcal{C}), \tag{3.2}$$

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

3.1.3 Contributions

The Singleton bound described above along with the MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were studied and presented in the form of the following two articles.

(i) M. Bilal, J. Borges, S. Dougherty, C. Fernández-Córdoba, *Optimal codes over* $\mathbb{Z}_2 \times \mathbb{Z}_4$. In libro de actas VII Jornadas de Matemática Discreta y Algorítmica, Castro Urdiales (Spain), pp. 131-139, (2010).

(ii) M. Bilal, J. Borges, S. Dougherty, C. Fernández-Córdoba, *Maximum Distance Separable codes over* $\mathbb{Z}_4$ *and* $\mathbb{Z}_2 \times \mathbb{Z}_4$. Designs, codes and cryptography, vol.61, n.1, pp. 31-40, (2011).

In contribution (i), we have given two forms of the Singleton bound for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. The first bound is an extension of the Singleton bound for binary codes, Equation 3.1, described in [Sin64]. We achieved this by applying the Singleton bound to $C = \Phi(\mathcal{C})$. The second bound is an extension of the results in [DS01], given by Equation 3.2. We also defined MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

In contribution (ii), we extended the work done in contribution (i). A $\mathbb{Z}_2\mathbb{Z}_4$-additive code attaining the bound obtained from Equation 3.1 is defined as an MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive code with respect to the Singleton bound, briefly MDSS. In the second case; i.e., the bound obtained from Equation 3.2, $\mathcal{C}$ is an MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive code with respect to the rank bound, briefly MDSR, if $\mathcal{C}$ attains this bound. The main results are also valid when $\alpha = 0$, namely quaternary linear codes. We completely characterized MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and strong conditions are given for MDSR $\mathbb{Z}_2\mathbb{Z}_4$-additive 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.

3.2 Self-dual codes from 3-class association schemes

3.2.1 Association schemes

Incomplete-block design for experiments were first developed by Yates at Rothamsted Experimental Station. He produced a remarkable collection of designs for individual experiments. These designs posed questions for the statisticians: (i) what is the best way of choosing subsets of the treatments to allocate to the blocks, given the recourse constraints? (ii) how should one analyze the data from the experiments?

Designs with partial balance help statisticians answer these two questions. The designs were introduced by Bose and Nair in [BN39]. The fundamental concept here was association scheme, which was defined in its own right by Bose and Shimamoto in [BS52]. Many experiments have more than one system of blocks, which can have complicated inter-relationships. The general structure is an orthogonal block structure and although they were introduced separately of partially balanced incomplete-block designs, they also are association schemes. Thus association schemes play an important part in the design of experiments. Association schemes also come into play in permutation groups, quite independently of any statistical applications. Much of the modern literature about association schemes is in the language of abstract algebra.

The subject became an object of algebraic interest with the publication of [BM59] and the introduction of the Bose-Mesner algebra. The most important contribution to the theory was the thesis of P. Delsarte [Del73] who recognized and fully used the connections with coding theory and design theory.

Association schemes are about the relations between pair of elements of a set. Let X be a finite set, $|X| = v$. Let R_i be a subset of $X \times X$, $\forall i \in \mathcal{I} = \{0, \ldots, d\}, d > 0$. We define $\Re = \{R_i\}_{i \in \mathcal{I}}$. We say that $(X, \Re)$ is a *d-class association scheme* if the following properties are satisfied:

(i) $R_0 = \{(x,x) : x \in X\}$ is the identity relation.

(ii) For every $x, y \in X$, $(x,y) \in R_i$ for exactly one i.

(iii) $\forall\, i \in \mathcal{I},\ \exists\, i' \in \mathcal{I}$ such that $R_i^T = R_{i'}$, where $R_i^T = \{(x,y) : (y,x) \in R_i\}$.

(iv) If $(x,y) \in R_k$, the number of $z \in X$ such that $(x,z) \in R_i$ and $(z,y) \in R_j$ is a constant p_{ij}^k.

The values p_{ij}^k are called *intersection numbers*. The elements $x, y \in X$ are called i^{th} *associates* if $(x,y) \in R_i$. If $i = i'$ for all i then the association scheme is said to be *symmetric*, otherwise it is *non-symmetric*. The association scheme $(X, \Re)$ is *commutative* if $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \mathcal{I}$. Note that a symmetric association scheme is always commutative but the converse is not true.

The adjacency matrix A_i for the relation R_i for $i \in \mathcal{I}$, is the $v \times v$ matrix with rows and columns labeled by the points of X and defined by

$$(A_i)_{x,y} = \begin{cases} 1, & if\ (x,y) \in R_i, \\ 0, & \quad otherwise. \end{cases}$$

The conditions (i)-(iv) in the definition of $(X, \Re)$ are equivalent to:

(i) A_0 = I (the identity matrix).

(ii) $\sum_{i \in \mathcal{I}} A_i = J$ (the all-ones matrix).

(iii) $\forall\, i \in \mathcal{I}, \exists\, i' \in \mathcal{I}$, such that $A_i = A_{i'}^T$.

(iv) $\forall\, i, j \in \mathcal{I}, \quad A_i A_j = \sum\limits_{k \in \mathcal{I}} p_{ij}^k A_k$.

If the association scheme is symmetric, then $A_i = A_i^T$, for all $i \in \mathcal{I}$. If the association scheme is commutative, then $A_i A_j = A_j A_i$, for all $i, j \in \mathcal{I}$. The adjacency matrices generate a $(n+1)$-dimensional algebra $\mathbf{A}$ of symmetric matrices. This algebra is called the Bose-Mesner algebra.

Higman [Hig75] proved that a d-class association scheme with $d \leq 4$ is always commutative, meaning that $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \mathcal{I}$.

3.2.2 Self-dual codes from 3-class association schemes

2-class association schemes consist of either strongly regular graphs (SRG) or doubly regular tournaments (DRT). Self-dual codes from the adjacency matrices of 2-class association schemes were presented in [DKS07]. The purpose of the work done in [DKS07] was to unify the earlier known constructions of double circulant codes, thus generalizing Quadratic Double Circulant Codes [Gab02] and to construct codes with high minimum distance. Examples were given for codes over $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$ and $\mathbb{Z}_4$.

3.2.3 Contributions

Following the work done in [DKS07] with 2-class association schemes, we have presented two methods to generate self-dual codes from 3-class association schemes. In this regards we have done two publications which are the following.

(i) M. Bilal, J. Borges, S. Dougherty, C. Fernández-Córdoba, *Binary self-dual codes from 3-class association schemes*, 3rd International Castle Meeting on Coding Theory and Applications, Cardona (Spain), Servei de publicacions UAB, pp. 59-64, (2011).

(ii) M. Bilal, J. Borges, C. Fernández-Córdoba, *Self-dual codes over $\mathbb{Z}_k$ from rectangular association schemes*, In libro de actas VII Jornadas de Matemática Discreta y Algorítmica, Almería (Spain), pp. 103-110, (2012).

In contribution (i), we have generated binary self-dual codes from the adjacency matrices of 3-class association schemes. Two methods for construction of self-dual codes are used, namely pure construction and bordered construction. We have given conditions for both symmetric and non-symmetric association schemes.

In contribution (ii), we used 3-class rectangular association schemes to generate self-dual codes over several rings. We used pure and bordered constructions to obtain these codes over $\mathbb{Z}_k$. All values of k are determined so that we can obtain such self-dual codes from the adjacency matrices.

3.3 Extensions of $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes

3.3.1 $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes. Type and separability

$\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes were defined in Chapter 2 along with properties like code Type, separability and antipodality. In [BDFC12], all three Types of self-dual $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are defined and the possible values of α, β such that there exist a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are given.

The $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes are extended by increasing the length of the codewords. The standard techniques of invariant theory were used to achieve the results. The paper summarizes all the results in the form a table where all the possible minimum values of (α, β) are given for all separable or non-separable codes of each Type. The paper also gives weight enumerators for each of the three Types of codes.

3.3.2 Contributions

Following [BDFC12], given a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code, one can easily extend this code and generate an extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code with greater length. In the following communication, we have studied these constructions and checked if properties like separability, antipodality and code Type are retained or not.

(*) M. Bilal, J. Borges, S. Dougherty, C. Fernández-Córdoba, *Extensions of Z2Z4-additive self-dual codes preserving their properties*, IEEE 2012 International Symposium on Information Theory, MIT Cambridge, Conference publication, pp. 3101-3105, (2012).

In the above contribution we used the technique given in [BDFC12]; i.e., extending the length of code, to obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code with greater length. We extended Type 0, I and II codes using this technique. We have concluded that, given a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual of type $(\alpha, \beta; \gamma, \delta; \kappa)$, one can extend the length of the code and obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(\alpha + \alpha', \beta + \beta'; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$ while preserving the Type, separability or non-separability, and antipodality or non-antipodality.

Chapter 4

Conclusion

This chapter starts with the summary of the work done for this dissertation. We summarize all topics and provide the main results from our research. The chapter ends with some ideas about future work.

4.1 Summary and main results

Researchers have been working in coding theory ever since Claude Shannon published the landmark paper [Sha48]. Through the years there have been many developments in this field. Apart from the codes that are produced by the researchers for communications systems, there has been quite a lot of work done in classifying codes and learning their mathematical aspects. This thesis, which is more about the classification of codes, is presented in the form of a compendium of publications, which were presented at different conferences and in a journal during my PhD. studies.

By now the reader knows that the thesis is mainly comprised of two parts: bounds on the minimum distance of a code and self-dual codes.

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

In the first part of our research we studied bounds on the minimum distance of a code. We studied the Singleton bound and MDS codes and applied the bound to $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

We have done publications on this topic in which we presented two forms of Singleton bound for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. The codes that meet these bounds are called MDSS and MDSR codes. We presented our results along with examples for each of these bounds. The main results are also valid when $\alpha = 0$, namely for quaternary linear codes. For details see [BBDFC10] and [BBDFC11b]. The main results from these contributions are as follows:

Theorem 13 *If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with parameters $(\alpha, \beta, \gamma, \delta, \kappa)$, then*

$$\frac{d(\mathcal{C}) - 1}{2} \leqslant \frac{\alpha}{2} + \beta - \frac{\gamma}{2} - \delta, \tag{4.1}$$

$$\left\lfloor \frac{d\,(\mathcal{C}) - 1}{2} \right\rfloor \leqslant \alpha + \beta - \gamma - \delta. \tag{4.2}$$

This theorem gives us two bounds for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. We say that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is MDS if $d\,(\mathcal{C})$ meets the bound given in (4.1) or (4.2). 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.

The following theorem characterizes all MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. By the *even code* we mean the set of all even weight vectors and 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 14 *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.

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

Theorem 15 *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 14 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* $d(\mathcal{C}) \leq 2-\alpha \in \{1,2\}$.

4.1.2 Self-dual codes

The second part is about self-dual codes, their generation from association schemes and extensions of $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes while preserving their properties.

Self-dual codes from 2-class association schemes were first given in [DKS07]. In our work we use 3-class association schemes to generate self-dual codes. We use two methods of generating self-dual codes from 3-class association schemes, the pure and the bordered construction. Starting from the parameters of a 3-class association scheme we state which linear combinations of the adjacency matrices give a generator matrix of a self-dual code, using pure and bordered constructions.

In [BBDFC11a] we use the two constructions to generate binary self-dual codes from symmetric and non-symmetric 3-class association schemes. Using the non-symmetric 3-class association schemes, we give the conditions and parameters and use them to generate binary self-dual codes from pure and bordered constructions. For the case of binary self-dual codes from symmetric 3-class association schemes, the number of equations and parameters become quite a lot, so for the sake of simplicity we use the rectangular association scheme, which is a symmetric association scheme. We give the conditions and parameters such that the generated binary code is self-dual, using pure and bordered constructions.

In [BBFC12] we use 3-class rectangular association schemes to construct self-dual codes over several rings. We use the pure and bordered construction to get self-dual codes over $\mathbb{Z}_k$. We completely determine the values of k along with the parameters and necessary conditions which we use to obtain self-dual codes from the adjacency matrices of 3-class rectangular association schemes using pure and bordered constructions.

In [BDFC12], a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code was extended to generate an extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code with greater length. These extended codes were studied and we investigated if properties like the Type and separability are retained in the extended code or not when using this extension method. We found that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, we extend the length of the code $\mathcal{C}$ and obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}$ of type $(\alpha + \alpha', \beta + \beta'; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$ preserving the Type, separability or non-separability, and antipodality or non-antipodality. For further details please read [BBDFC12]

4.2 Future Work

Here we would like to give some research ideas for the future work that come up as a result of the research work done during this Ph.D.

First, in this work we have studied the Singleton bound for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. As a future work one can apply other bounds like Plotkin bound, Johnson bound, Linear Programming bound, etc. over $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and present new results.

Second, we have generated self-dual codes from 3-class association schemes using two constructions, namely pure and bordered construction and we have given results for binary self-dual codes from non-symmetric association schemes and self-dual codes over $\mathbb{Z}_k$ from rectangular association schemes. It would be interesting to generate self-dual codes from other association schemes like Johnson schemes, Hamming schemes, etc., and over other rings and fields.

Third, it would be interesting to see whether properties like Type and separability or antipodality of a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code are preserved or not if we use other known constructions; e.g., neighbor construction or building-up construction of self-dual codes.

Bibliography

[BBDFC10] M. Bilal, J. Borges, S. Dougherty, and C. Fernández-Córdoba. Optimal codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$. *In libro de actas VII Jornadas de Matemática Discreta y Algorítmica, Castro Urdiales (Spain)*, pages 131–139, 2010.

[BBDFC11a] M. Bilal, J. Borges, S. Dougherty, and C. Fernández-Córdoba. Binary self-dual codes from 3-class association schemes. *3rd International Castle Meeting on Coding Theory and Applications, Cardona (Spain), Servei de publicacions UAB*, pages 59–64, 2011.

[BBDFC11b] M. Bilal, J. Borges, S. Dougherty, and C. Fernández-Córdoba. Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$. *Designs, Codes and Cryptography*, 61(1):31–40, 2011.

[BBDFC12] M. Bilal, J. Borges, S. Dougherty, and C. Fernández-Córdoba. Extensions of $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes preserving their properties. *IEEE International Symposium on Information Theory, MIT Cambridge, Conference publication*, pages 3101–3105, 2012.

[BBFC12] M. Bilal, J. Borges, and C. Fernández-Córdoba. Self-dual codes over $\mathbb{Z}_k$ from rectangular association schemes. *In libro de actas VIII Jornadas de Matemática Discreta y Algorítmica, Almería (Spain)*, pages 103–110, 2012.

[BDFC12] J. Borges, S. T. Dougherty, and C. Fernández-Córdoba. Characterization and constructions of self-dual codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$. *Advances in Mathematics of Communications*, 6(3):287–303, 2012.

[BFCP$^+$06] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva. On $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and duality. *V Jornadas de Matemática Discreta y Algorítmica, Soria (Spain)*, pages 171–177, 2006.

[BFCP$^+$10] 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*, 54(2):167–179, 2010.

[BM59] R. C. Bose and D. M. Mesner. On linear associative algebras corresponding to association schemes of partially balanced designs. *Institute of Mathematical Statistics*, 30(1):21–38, 1959.

[BN39] R.C. Bose and K. R. Nair. Partially balanced incomplete block designs. *Sankhya*, 4:337–372, 1939.

[BS52] R.C. Bose and T. Shimamoto. Classification and analysis of partially balanced incomplete block designs with two associate classes. *J. Amer. Statist. Assoc.*, 47:151–184, 1952.

[DC05] J. Degraer and K. Coolsaet. Classification of three-class association schemes using backtracking with dynamic variable ordering. *Discrete mathematics*, 300:71–81, 2005.

[Del73] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Rep.*, 10, 1973.

[DKS07] S. T. Dougherty, J. L. Kim, and P. Solé. Double circulant codes from two class association schemes. *Advances in Mathematics of Communications*, 1(1):45–64, 2007.

[DL98] P. Delsarte and V. Levenshtein. Association schemes and coding theory. *IEEE Transactions on Information Theory*, 44(6):2477–2504, 1998.

[DS01] S. T. Dougherty and Keisuke Shiromoto. Maximum distance codes over rings of order 4. *IEEE Transaction of Information Theory*, 47(1):400–404, 2001.

[Gab02] P. Gaborit. Quadratic double circulant codes over fields. *Journal of Combinatorial Theory Series A*, 97(1):85–107, 2002.

[Hig75] D. G. Higman. Coherent configurations. *Geom.Dedicata*, 4:1–32, 1975.

[HKC$^+$94] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, 1994.

[HP03] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[Jørag] L. K. Jørgensen. Non-symmetric 3-class association schemes. *Research Report Series*, R-2005-13, Aalborg Universitetsforlag.

[MS83] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1983.

[PR97] J. Pujol and J. Rifà. Translation invariant propelinear codes. *IEEE Transactions on Information Theory*, 43(2):590–598, 1997.

[PS01] J. G. Proakis and M. Salehi. *Communication Systems Engineering (2nd Edition)*. Prentice Hall, 2001.

[RS98] E. M. Rains and N. J. A. Sloane. Self-dual codes. *Information Science Research, AT&T Labs Research*, 1998.

[Sha48] C. Shannon. A mathematical theory of communication. *Bell System Tech.*, (J. 27):379–423 and 623–656, 1948.

[Shi00] K. Shiromoto. Singleton bounds for codes over finite rings. *Journal of Algebraic Combinatorics*, 12:95–99, 2000.

[Sin64] R. C. Singleton. Maximum distance q-nary codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964.

Appendices

Appendix A

Optimal codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$

Optimal codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$ *

M. Bilal[1], J. Borges[1], S.T. Dougherty[2], and C. Fernández-Córdoba[1]

[1] Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra (Spain).
{mbilal,jborges,cfernandez}@deic.uab.cat
[2] Dept. of Mathematics, University of Scranton, Scranton, PA 18510 (USA).
doughertys1@scranton.edu

Abstract. We study additive codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$ with largest minimum distance. We find two kinds of maximum distance separable codes and we state which are the possible parameters, i.e. the type of the code, for such codes.

Key words: Additive codes, minimum distance bounds, maximum distance separable codes.

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 $\mathbb{Z}_4^n$.

In [4] 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 $\alpha + 2\beta = n$ [3]. 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 $\Phi(x, y) = (x, \phi(y_1), \dots, \phi(y_\beta))$ for any $x \in \mathbb{Z}_2^\alpha$ and any $y = (y_1, \dots, y_\beta) \in \mathbb{Z}_4^\beta$, 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 $wt_L(v_2)$ 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

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

weight of $\Phi(\mathbf{v})$. Denote by $d(\mathcal{C})$ the minimum distance between codewords in $\mathcal{C}$. Let $\mathbf{0}$ be the all-zero vector (binary or quaternary).

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 $(\alpha, \beta; \gamma, \delta; \kappa)$.

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

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

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 $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$:

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

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

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

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

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

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 [1,2,3,6] 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 $n = \alpha + 2\beta$.

2 Bounds on the minimum distance

The usual Singleton bound [7] for codes over an alphabet of size q is given by

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

This bound is a combinatorial bound and does not rely on the algebraic structure of the code. In [5], the following Singleton bound for the Lee weight of a quaternary linear code is given. For a code $\mathcal{C}$ of type $2^\gamma 4^\delta$ we have

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \leq n - \delta - \frac{\gamma}{2}.$$

Theorem 1. *If $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with parameters $(\alpha, \beta, \gamma, \delta, \kappa)$, then*

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

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

Proof. Bound (1) can be obtained by simply applying the Singleton bound given in [7] to $C = \Phi(\mathcal{C})$.

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 $\mathcal{X}$.

We know that

$$d(\mathcal{C}) \leqslant d(\mathcal{X}(\mathcal{C})).$$

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

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

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

Hence the theorem follows.

Lemma 1. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then Bound (1) is strictly stronger than Bound (2) 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 (1) is stronger that Bound (2) if and only if

$$\begin{aligned} \alpha + 2\beta - \gamma - 2\delta + 1 &< 2(\alpha + \beta - \gamma - \delta + 1), \\ \alpha + 2\beta - \gamma - 2\delta + 1 &< 2\alpha + 2\beta - 2\gamma - 2\delta + 2, \\ \alpha - \gamma + 1 &< 2\alpha - 2\gamma + 2, \\ \gamma - 1 &< \alpha, \\ i.e.\ \alpha &\geqslant \gamma. \end{aligned}$$

If $d(\mathcal{C})$ is odd then Bound (1) is stronger that Bound (2) if and only if

$$\begin{aligned} \alpha + 2\beta - \gamma - 2\delta + 1 &< 2(\alpha + \beta - \gamma - \delta) + 1, \\ \alpha + 2\beta - \gamma - 2\delta + 1 &< 2\alpha + 2\beta - 2\gamma - 2\delta + 1, \\ \alpha - \gamma &< 2\alpha - 2\gamma, \\ \gamma &< \alpha. \end{aligned}$$

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*

$$d(\mathcal{C}) = \min\{d(\mathcal{C}_X), d(\mathcal{C}_Y)\}. \tag{3}$$

Proof. The code $\mathcal{C}$ is distance invariant [6] i.e. $d(\mathcal{C}) = wt(\mathcal{C})$, where $wt(\mathcal{C}) = \min\{wt(v) | v \in \mathcal{C}, v \neq \mathbf{0}\}$ 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

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

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*

$$d(\mathcal{C}) \leq \min\left\{\alpha - \kappa + 1, \overline{d}\right\}, \tag{4}$$

where $\overline{d}$ is the maximum value satisfying both Bound (1) and Bound (2).

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 (1) or (2). Let $\mathcal{C}^i$ be the punctured code of $\mathcal{C}$ be deleting the i^{th} 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*

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

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 MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, $\alpha >\ 0$, such that $d(\mathcal{C})$ meets Bound (2), 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

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

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

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

Then $\mathcal{C}^i$ is an MDS code meeting Bound (2) with $\alpha - 1 > 0$ and $d\left(\mathcal{C}^i\right)$ is even, which is a contradiction.

Lemma 3. *If $\mathcal{C}$ is an MDS $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with $\alpha > 1$ such that $d\left(\mathcal{C}\right)$ meets Bound (1), then the punctured code $\mathcal{C}^i$, $i \in X$, is again an MDS code meeting Bound (1).*

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

Since $\mathcal{C}$ is an MDS code then

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

After puncturing we get

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

hence $\mathcal{C}^i$ is again an MDS code.

Proposition 2. *If $\mathcal{C}$ is an MDS code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ satisfying Bound (1), then $\gamma \leqslant 1$.*

Proof. From Lemma 1 we know that $\alpha \geqslant \gamma$. From Lemma 3 by puncturing binary coordinates, we can get a code of type $(1, \beta; \gamma, \delta; \kappa^*)$ and hence $\gamma \leqslant 1$.

The next proposition gives a general construction for MDS codes meeting Bound (2) starting from binary MDS codes.

Proposition 3. *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 $\mathcal{C}$ of type $(1, n-1; k, 0; 1)$ which satisfies Bound (2).*

Proof. The type of the code $\mathcal{C}$ is obtained directly from construction.

After applying χ, the $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ has $d\left(\mathcal{C}\right) = 2d - 1$. Then $d = n - k + 1 = \alpha + \beta - \gamma + 1$. So $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor = d - 1 = \alpha + \beta - (\gamma + \delta)$ which meets Bound (2).

In particular, this construction works for the even binary code and the ambient space $\mathbb{Z}_2^n$ which are the possible binary linear MDS codes with more than one codeword.

3.1 Examples

Examples 1 and 2 satisfies Bound (1). 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 (1) we get

$$\begin{aligned} \frac{2-1}{2} &\leqslant \frac{1}{2} + 1 - \frac{0}{2} - 1, \\ \frac{1}{2} &\leqslant \frac{1}{2}. \end{aligned}$$

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 $d(\mathcal{C}_3) = 2$. When we apply Bound (1) we obtain the following results.

$$\begin{aligned} \frac{d(C)-1}{2} &\leqslant \frac{\alpha}{2} + \beta - \frac{\gamma}{2} - \delta, \\ \frac{2-1}{2} &\leqslant \frac{1}{2} + 1 - \frac{1}{2} - 1, \\ 0.5 &\leqslant 0.5. \end{aligned}$$

The next example satisfies Bound (2).

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

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

The code $\mathcal{C}_4$ is of type $(1, 3; 3, 0; 1)$ with minimum weight $d(\mathcal{C}_4) = 3$. When we apply Bound (2) we obtain the following results.

$$\begin{aligned} \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor &\leqslant \alpha + \beta - 3 - 0, \\ \left\lfloor \frac{3-1}{2} \right\rfloor &\leqslant 4 - 3, \\ 1 &\leqslant 1. \end{aligned}$$

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

Example 4. Let C_8 be a 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 $\mathcal{C}_1$ a quaternary linear code length 1 and minimum weight $d(\mathcal{C}_1) = 2$ has 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 (4) we get

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

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

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

and $\mathcal{C}_4$ a quaternary linear code length with length 4 and minimum weight $d(\mathcal{C}_4) = 4$ has generator matrix

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

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

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

References

[1] J. Borges, C. Fernández, J. Pujol, J. Rifà and M. Villanueva. On $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and duality. *V Jornades de Matemàtica Discreta i Algorísmica*, Soria (Spain), Jul. 11-14, pp. 171-177, 2006.

[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(2), pp. 167-179, 2010.

[3] P. Delsarte and V. Levenshtein. Association Schemes and Coding Theory. *IEEE Trans. Inform. Theory*, vol. 44(6), pp. 2477-2504, 1998.

[4] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep.Suppl.*, vol. 10, 1973.

[5] S.T. Dougherty and K. Shiromoto. Maximum distance codes over rings of order 4". *IEEE Transactions of Information Theory*, Vol. 47,pp. 400-404, 2001.

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

[7] R. C. Singleton. Maximum distance q-ary codes. *IEEE Transactions of Information Theory*, Vol. 10, pp. 116 -118, 1964.

Appendix B

Maximum Distance Separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$

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 $1 \le i \le \gamma$, $\mu_j \in \mathbb{Z}_4$ for $1 \le j \le \delta$ 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 $d\left(\mathcal{C}\right)$ then

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

where $rank\left(\mathcal{C}\right)$ 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 $(\mathcal{X}, Id) : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \rightarrow \mathbb{Z}_4^{\alpha+\beta}$, 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*

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

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

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

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

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

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

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

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

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*

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

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

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

□

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

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

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 $d\left(\mathcal{C}_2\right) = 2$. 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 $d\left(\mathcal{C}_3\right) = 2$. 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 $d\left(\mathcal{C}_4\right) = 3$. Thus, $\mathcal{C}_4$ is an MDSR code (but not MDSS).

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

Example 4 Let C_8 be the binary linear code of length 8 with $d\left(C_8\right) = 4$ 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 $d\left(\mathcal{C}_1\right) = 2$ with generator matrix

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

The $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}_9 = C_8 \times \mathcal{C}_1$ has length 9 and has parameters $(8, 1; 5, 0; 4)$. Applying Bound (6) we get

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

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 $\mathcal{C}_6 = \mathcal{C}_2 \times \mathcal{C}_4$ 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).

Appendix C

Binary self–dual codes from 3-class association schemes

Binary Self-Dual Codes from 3-Class Association Schemes*

Muhammad Bilal[1], **Joaquim Borges**[1], **Steven T. Dougherty**[2], **and Cristina Fernández-Córdoba**[1]

mbilal@deic.uab.cat, joaquim.borges@uab.cat, doughertys1@scranton.edu, cristina.fernandez@uab.cat

[1] Universitat Autònoma de Barcelona, Spain
[2] University of Scranton, USA

Abstract. Three class association schemes are used to construct binary self-dual codes over $\mathbb{F}_2$. We use the pure and bordered construction to get self-dual codes starting from the adjacency matrices of symmetric and non-symmetric 3-class association schemes.

Keywords: Self-dual codes, association schemes, 3-class association schemes.

1 Introduction

Self-dual codes are an important class of codes both over fields and rings. There are numerous constructions of self-dual codes from combinatorial objects. In [1], self-dual codes were constructed from two class association schemes. In this paper, we extend that work by constructing self-dual codes from three class association schemes. We begin with some definitions from coding theory and then give some definitions from the theory of association schemes.

Let C be a binary code. We define the *dual* code $C^\perp$ as $C^\perp = \{w \mid w \cdot v = 0,\ \forall\, v \in C\}$. The code is said to be *self-dual* if it is equal to its dual and *self-orthogonal* if it is contained in its dual. A self-dual code is *Type II* if the Euclidean weight of each of its elements is a multiple of 4. We refer the reader to [3] for a complete description of self-dual codes.
Let X be a finite set, $|X| = v$. Let R_i be a subset of $X \times X$, $\forall i \in \mathcal{I} = \{0, \ldots, d\}, d > 0$. We define $\Re = \{R_i\}_{i \in \mathcal{I}}$. We say that $(X, \Re)$ is a *d-class association scheme* if the following properties are satisfied:

(i) $R_0 = \{(x, x) : x \in X\}$ is the identity relation.
(ii) For every $x, y \in X$, $(x, y) \in R_i$ for exactly one i.
(iii) $\forall\, i \in \mathcal{I},\ \exists\, i' \in \mathcal{I}$ such that $R_i^t = R_{i'}$, where $R_i^t = \{(x, y) : (y, x) \in R_i\}$.
(iv) If $(x, y) \in R_k$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant p_{ij}^k.

* This work has been supported by the Spanish MICINN grant MTM2009-08435 and the Catalan AGAUR grant 2009 SGR1224.

The values p_{ij}^k are called *intersection numbers*. The elements $x, y \in X$ are called i^{th} *associates* if $(x, y) \in R_i$. If $i = i'$ for all i then the association scheme is said to be *symmetric*, otherwise it is *non-symmetric*. The association scheme $(X, \Re)$ is *commutative* if $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \mathcal{I}$. Note that a symmetric association scheme is always commutative but the converse is not true. Higman [2] proved that a d-class association scheme with $d \leq 4$ is always commutative, meaning that $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \mathcal{I}$.

The adjacency matrix A_i for the relation R_i for $i \in \mathcal{I}$, is the $v \times v$ matrix with rows and columns labeled by the points of X and defined by

$$(A_i)_{x,y} = \begin{cases} 1, if\ (x, y) \in R_i, \\ 0, \quad otherwise. \end{cases}$$

The conditions (i)-(iv) in the definition of $(X, \Re)$ are equivalent to:

(i) A_0 = I (the identity matrix).
(ii) $\sum_{i \in \mathcal{I}} A_i = J$ (the all-ones matrix).
(iii) $\forall\, i \in \mathcal{I}, \exists\, i' \in \mathcal{I}$, such that $A_i = A_{i'}^t$.
(iv) $\forall\, i, j \in \mathcal{I}, \quad A_i A_j = \sum\limits_{k \in \mathcal{I}} p_{ij}^k A_k$.

If the association scheme is symmetric, then $A_i = A_i^t$, for all $i \in \mathcal{I}$. If the association scheme is commutative, then $A_i A_j = A_j A_i$, for all $i, j \in \mathcal{I}$. The adjacency matrices generate a $(n + 1)$-dimensional algebra A of symmetric matrices. This algebra is called the Bose-Mesner algebra.

2 3-class association schemes and self dual codes

Let $(X, \Re)$ be a 3-class association scheme. The adjacency matrix for R_0 is I and the adjacency matrices of R_1, R_2 and R_3 are A_1, A_2 and $J - I - A_1 - A_2$, respectively.

Lemma 1. *If $(X, \Re)$ is a 3-class association scheme then the following equations hold:*

(i) $A_1 J = J A_1 = p_{11}^0 J$*,* $A_2 J = J A_2 = p_{22}^0 J$*.*
(ii) $A_1 A_2 = A_2 A_1 = p_{12}^0 I + p_{12}^1 A_1 + p_{12}^2 A_2 + p_{12}^3 (J - I - A_1 - A_2)$*.*

Note that the number of ones per row (or column) in A_1 is p_{11}^0, A_2 is p_{22}^0 and A_3 is p_{33}^0.

Over $\mathbb{F}_2$, we describe the following construction which we shall use in our construction of self-dual codes. For arbitrary values of $r, s, t, u \in \mathbb{F}_2$ let

$$\begin{aligned} Q_R(r, s, t, u) &= rA_0 + sA_1 + tA_2 + uA_3 \\ &= rI + sA_1 + tA_2 + u(J + I + A_1 + A_2) \\ &= (r + u) I + (s + u) A_1 + (t + u) A_2 + uJ. \end{aligned} \tag{1}$$

We write Q for $Q_R(r, s, t, u)$. We will define two different methods of constructing self-dual codes, the pure and bordered construction. The *pure* construction is

$$\mathcal{P}_R(r, s, t, u) = (I \mid Q). \tag{2}$$

The *bordered* construction is

$$\mathcal{B}_R(r,s,t,u) = \left(\begin{array}{c|c|c|c} 1 & 0\dots 0 & a & b\dots b \\ \hline 0 & & c & \\ \vdots & I & \vdots & Q \\ 0 & & c & \end{array}\right). \tag{3}$$

We define the code $P_R(r,s,t,u)$ to be the row span over $\mathbb{F}_2$ of $\mathcal{P}_R(r,s,t,u)$ and let $B_R(r,s,t,u)$ be the row span over $\mathbb{F}_2$ of $\mathcal{B}_R(r,s,t,u)$. Both codes are free and have the size of a self-dual code with the code $P_R(r,s,t,u)$ having length $2v$ and the code $B_R(r,s,t,u)$ having length $2v+2$. Thus to construct a self-dual code we need only make them self-orthogonal. We write $\mathcal{P}$ and $\mathcal{B}$ for $\mathcal{P}_R\,(r,s,t,u)$ and $\mathcal{B}_R\,(r,s,t,u)$, respectively and also P and B for $P_R\,(r,s,t,u)$and $B_R\,(r,s,t,u)$, respectively.

3 Self-dual codes from non-symmetric three class association schemes

Let $(X,\Re)$ be a 3-class association scheme. If it is non-symmetric then we can order the relations such that $R_2 = R_1^t$ and R_3 is a symmetric relation. The association scheme is uniquely determined by R_1. If we denote the adjacency matrix for R_1 by A then the adjacency matrices of R_0, R_2 and R_3 are I, A^t and $J-I-A-A^t$, respectively.

Lemma 2. *If $(X,\Re)$ is a non-symmetric 3-class association scheme then the following equations hold:*

$$\begin{aligned} &AJ = JA = \kappa J, \\ &AA^t = A^tA = \kappa I + \lambda\,(A + A^t) + \mu\,(J - I - A - A^t)\,, \\ &A^2 = \alpha A + \beta A^t + \gamma\,(J - I - A - A^t)\,, \end{aligned} \tag{4}$$

where $\kappa = p_{12}^0 = p_{21}^0$, $\lambda = p_{12}^1 = p_{21}^1$, $\mu = p_{12}^3 = p_{21}^3$, $\alpha = p_{11}^1$, $\beta = p_{11}^2$ and $\gamma = p_{11}^3$. Moreover, $\alpha = \lambda$ and κ is the number of ones at each row and at each column of A.

Related to $(X,\Re)$ we have the parameters v, κ, λ, μ, α, β and γ as in Equation (4). For the code P to be self-orthogonal we need

$$(I \mid Q)(I \mid Q)^T = \mathbf{0}.$$

Namely we need $QQ^T = I$.

For the pure construction to give a Type II code we need the inner product of any row with itself to be $0 \pmod 4$, that is we need

$$1 + r + s\kappa + t\kappa + u(v+1) \equiv 0 \pmod 4.$$

For B to be self-dual we need the following:

$$1 + a + vb = 0 \tag{5}$$

$$ac + b\,[r + s\kappa + t\kappa + u(v+1)] = 0 \tag{6}$$

$$I + cJ + QQ^T = \mathbf{0}. \tag{7}$$

The first equation is the inner-product of the top row with itself. The second is the inner-product of the top row with any other row, and the third ensures that the other rows are orthogonal to each other. Computing QQ^t for the non-symmetric three class association scheme we obtain:

$$\begin{aligned} QQ^T &= [r+u+(s+t)(\kappa+\mu)]\, I \\ &\quad + [(s+t)(r+u+\lambda+\mu)+(s+u)(t+u)(\lambda+\beta)]\,(A+A^T) \\ &\quad + [(s+t)\mu+uv]\, J. \end{aligned}$$

Theorem 3. *Let C be the binary linear code generated by $\mathcal{P}$ with parameters v, κ, λ, μ, α, β and γ. The code C is self-dual if and only if one of the following holds:*

(i) $s \neq t$; $\kappa \neq \lambda = r+u+\mu$; $\mu = uv$.
(ii) $s = t$; $r = u$; $s = u$ *or* $\lambda = \beta$; $uv = 0$.

Corollary 4. *Let C be the binary linear code generated by $\mathcal{P}$. The code C is Type II if and only if one of the following holds:*

(i) $Q = wI + D$, $\mu = \lambda + w = 0$, $\lambda \neq \kappa$ *and* $a + \kappa \equiv 3 \pmod 4$*; or*
(ii) $Q = wI + D + J$, $\mu = \lambda + w = v$, $\lambda \neq \kappa$ *and* $1 + v \equiv \kappa + w \pmod 4$*; or*
(iii) $Q = I + A + A^T$*;* $\lambda = \beta$ *and* κ *is odd; or*
(iv) $Q = I + A + A^T + J$*;* $\lambda = \beta$ *and* v *is even; or*
(v) $Q = I + J$ *and* $v \equiv 0 \pmod 4$.

Where $w \in \{0,1\}$, D stands for A or A^T.

For $b = 0$ we will always have a code, generated by $\mathcal{B}$, with minimum weight 2 which does not lead to any interesting results, hence we confine ourselves to codes generated by $\mathcal{B}$ for $b = 1$.

Theorem 5. *Let C be the binary linear code generated by $\mathcal{B}$ with parameters v, κ, λ, μ, α, β, γ, a, c and $b = 1$. The code C is self-dual if and only if $a = 0$, $c = v = 1$ and one of the following holds:*

(i) $s \neq t$; $r = \kappa \neq \lambda$, $\mu \neq u$.
(ii) $s = t$; $r = 0$, $u = 1$, $(t+u)(\lambda+\beta) = 0$.

Corollary 6. *Let C be a binary self-dual code generated by $\mathcal{B}$, with $b = 1$. The code C is Type II if and only if one of the following conditions holds:*

(i) $Q = D$*, with* $a = 0$, $v \equiv 3$, $\kappa \equiv 2$, $\mu \equiv 1$, $c = 1$ *and* $\lambda \equiv 1$*; or*
(ii) $Q = I + D + J$*, with* $a = 0$, $v \equiv 3$, $\kappa \equiv 0$, $\mu \equiv 0$, $c = 1$ *and* $\lambda \equiv 1.$*; or*
(iii) $Q = I + D$*, with* $a = 0$, $v \equiv 3$, $\kappa \equiv 1$, $\mu \equiv 1$, $c = 1$ *and* $\lambda \equiv 0$*; or*
(iv) $Q = D + J$*, with* $a = 0$, $v \equiv 3$, $\kappa \equiv 3$, $\mu \equiv 0$, $c = 1$ *and* $\lambda \equiv 0$.
(v) $Q = I + A + A^t + J$ *with* $a = 0$, $v \equiv 1$, κ *is even,* $c = 1$ *and* $\lambda + \beta \equiv 0$.
(vi) $Q = I + J$ *with* $a = 0$, $v \equiv 1$ *and* $c = 1$.

Where D stands for A or A^T and the congruences are modulo 4.

4 Self-dual codes from symmetric three class association schemes

For symmetric three class association schemes, the number of equations and parameters increase, so for the sake of simplicity we focus on a particular example. Consider the rectangular scheme $n \times m$ $(n, m \geq 2)$ which is defined as follows. Consider two sets A and B with $|A| = n \geq 2$ and $|B| = m \geq 2$. Let $X = A \times B$ and define the binary relations over X:

$$\begin{aligned} R_0 &= \left\{ ((x,y),(x,y)) \in X^2 \right\}; \\ R_1 &= \left\{ ((x,y),(x,y')) \in X^2 \middle| \, y \neq y' \right\}; \\ R_2 &= \left\{ ((x,y),(x',y)) \in X^2 \middle| \, x \neq x' \right\}; \\ R_3 &= \left\{ ((x,y),(x',y')) \in X^2 \middle| \, x \neq x' \, and \, y \neq y' \right\}. \end{aligned}$$

$(X, \Re)$ is a symmetric 3-class association scheme with parameters:

$$\begin{aligned} & v = nm; p_{11}^0 = m-1; p_{22}^0 = n-1; p_{33}^0 = (m-1)(n-1); \\ & p_{11}^1 = m-2; p_{23}^1 = p_{32}^1 = n-1; p_{33}^1 = (n-1)(m-2); \\ & p_{13}^2 = p_{31}^2 = m-1; p_{22}^2 = n-2; p_{33}^2 = (n-2)(m-1); \\ & p_{12}^3 = p_{21}^3 = 1; p_{31}^3 = p_{13}^3 = m-2; p_{23}^2 = p_{32}^2 = n-2 = p_{33}^3 = (n-2)(m-2); \\ & \text{and } p_{ij}^k = 0, \text{ for all other cases.} \end{aligned}$$

Lemma 7. *If $(X, \Re)$ is a $n \times m$ symmetric rectangular association scheme, then the following equations hold:*

(i) $A_1 J = J A_1 = (m-1) J$, $A_2 J = J A_2 = (n-1) J$, $J^2 = n^2 m^2 J$;
(ii) $A_1^2 = (m-1) I + (m-2) A_1$; $A_2^2 = (n-1) I + (n-2) A_2$;
(iii) $A_1 A_2 = A_2 A_1 = A_3 = J - I - A_1 - A_2$.

For the code P to be self-orthogonal we need $QQ^T = I$ as previously. For B to be self-dual we need the following:

$$1 + a + nmb = 0 \tag{8}$$

$$ac + b\left[r + s(m+1) + t(n+1) + u(m+1)(n+1)\right] = 0 \tag{9}$$

$$I + cJ + QQ^T = \mathbf{0}. \tag{10}$$

The first equation is the inner-product of the top row with itself. The second is the inner-product of the top row with any other row, and the third ensures that the other rows are orthogonal to each other. Computing QQ^t for the rectangular association scheme we obtain:

$$\begin{aligned} QQ^T &= Q^2 \\ &= \left[(r+u) + (s+u)(m+1) + (t+u)(n+1)\right] I \\ &+ \left[(s+u) m\right] A_1 + \left[(t+u) n\right] A_2 + unmJ. \end{aligned}$$

Theorem 8. *Let C be a binary linear code generated by $\mathcal{P}$. The code C is self-dual if $r + s + t + u = 1$ and*

(i) If m is even and n is odd then C is self-dual whenever $r \neq s$.
(ii) If n is even and m is odd then C is self-dual whenever $r \neq t$.

(iii) If m and n are odd then C is self-dual whenever $r = 1$, $s = t = u = 0$.

Where all operations are over $\mathbb{F}_2$

Again we only consider cases where $b = 1$ in $\mathcal{B}$.

Theorem 9. *Let C be a binary linear code generated by $\mathcal{B}$, with $b = 1$. The code C is self-dual if and only if*

$$Q = I + J, a = 0, c = 1$$

with m and n odd. Moreover the code C is Type II if and only if $nm \equiv 3 \pmod{4}$.

References

1. S. T. Dougherty, J. L. Kim, and P. Solé. Double Circulant Codes from Two Class Association Schemes. *Advances in Mathematics of Communications*, vol. 1, no. 1, pp. 45-64, (2007).
2. D. G. Higman. Coherent Configurations. *Geom.Dedicata*, vol. 4, pp. 1-32, (1975).
3. E. Rains and N. J. A. Sloane. Self-dual codes in the Handbook of Coding Theory, V. S. Pless and W. C. Huffman. *eds., Elsevier, Amsterdam*, pp. 177-294, (1998).

Appendix D

Self-dual codes over $\mathbb{Z}_k$ from rectangular association schemes

Self-dual codes over $\mathbb{Z}_k$ from rectangular association schemes [⋆]

M. Bilal[1], J. Borges[1], and C. Fernández-Córdoba[1]

Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra (Spain).
mbilal,jborges,cfernandez@deic.uab.cat

Abstract. 3-class association schemes are used to construct self-dual codes over several rings. We have used the pure and bordered construction to get self-dual codes over $\mathbb{Z}_k$. We completely determine the values of k so that we can obtain such self-dual codes from the adjacency matrices of 3-class rectangular association schemes.

Key words: Association schemes, symmetric association schemes, rectangular association schemes, self-dual codes.

1 Introduction

Self-dual codes are an important class of codes over both fields and rings. There are various constructions available to generate self-dual codes from combinatorial objects. In [1], self-dual codes were constructed from 2-class association schemes. In [4], binary self-dual codes were constructed from non-symmetric 3-class association schemes and from rectangular association schemes in the case of symmetric 3-class association schemes. In this paper, we construct self-dual codes from 3-class rectangular association schemes over $\mathbb{Z}_k$. We begin with some definitions from coding theory and then give some definitions from the theory of association schemes.

Let R denote a finite commutative ring with identity. A *code* of length n over R is a subset of R^n and the code is said to be linear if it is an $R-$submodule of R^n.

We define the *dual* code $C^\perp$ of a code C with respect to the usual inner product, that is $C^\perp = \{w \mid w\cdot v = 0,\ \forall\ v \in C\}$. The code is said to be *self-dual* if it is equal to its dual and *self-orthogonal* if it is contained in its dual. We refer the reader to [2] for a complete description of self-dual codes.

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

Let X be a finite set, $|X| = v$. Let R_i be a subset of $X \times X$, $\forall i \in \mathcal{I} = \{0, \ldots, d\}$, $d > 0$. We define $\Re = \{R_i\}_{i \in \mathcal{I}}$. We say that $(X, \Re)$ is a *d-class association scheme* if the following properties are satisfied:

(i) $R_0 = \{(x, x) : x \in X\}$ is the identity relation.
(ii) For every $x, y \in X$, $(x, y) \in R_i$ for exactly one i.
(iii) $\forall\, i \in \mathcal{I}$, $\exists\, i' \in \mathcal{I}$ such that $R_i^T = R_{i'}$, where $R_i^T = \{(x, y) : (y, x) \in R_i\}$.
(iv) If $(x, y) \in R_k$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant p_{ij}^k.

The values p_{ij}^k are called *intersection numbers*. The elements $x, y \in X$ are called i^{th} *associates* if $(x, y) \in R_i$. If $i = i'$ for all i then the association scheme is said to be *symmetric*, otherwise it is *non-symmetric*. The association scheme $(X, \Re)$ is *commutative* if $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \mathcal{I}$. Note that a symmetric association scheme is always commutative but the converse is not true.

The adjacency matrix A_i for the relation R_i for $i \in \mathcal{I}$, is the $v \times v$ matrix with rows and columns labeled by the points of X and defined by

$$(A_i)_{x,y} = \begin{cases} 1, \, if \;\; (x, y) \in R_i, \\ 0, \quad otherwise. \end{cases}$$

The conditions (i)-(iv) in the definition of $(X, \Re)$ are equivalent to:

(i) $A_0 = I$ (the identity matrix).
(ii) $\sum_{i \in \mathcal{I}} A_i = J$ (the all-ones matrix).
(iii) $\forall\, i \in \mathcal{I}, \exists\, i' \in \mathcal{I}$, such that $A_i = A_{i'}^T$.
(iv) $\forall\, i, j \in \mathcal{I}, \quad A_i A_j = \sum\limits_{k \in \mathcal{I}} p_{ij}^k A_k$.

If the association scheme is symmetric, then $A_i = A_i^T$, for all $i \in \mathcal{I}$. If the association scheme is commutative, then $A_i A_j = A_j A_i$, for all $i, j \in \mathcal{I}$. The adjacency matrices generate a $(n + 1)$-dimensional algebra $\mathbf{A}$ of symmetric matrices. This algebra is called the Bose-Mesner algebra.

Higman [3] proved that a d-class association scheme with $d \leq 4$ is always commutative.

2 Self-dual codes from 3-class association schemes

Let $(X, \Re)$ be a 3-class association scheme. The adjacency matrix for R_0 is I and the adjacency matrices for R_1, R_2 and R_3 are A_1, A_2 and $J - I - A_1 - A_2$, respectively.

Lemma 1. *If $(X, \Re)$ is a 3-class association scheme then the following equations hold.*

$$A_1 J = J A_1 = p_{11}^0 J, A_2 J = J A_2 = p_{22}^0 J;$$
$$A_1 A_2 = A_2 A_1 = p_{12}^0 I + p_{12}^1 A_1 + p_{12}^2 A_2 + p_{12}^3 \left(J - I - A_1 - A_2\right).$$

Note that the number of ones per row (or column) in A_1 is p^0_{11}, A_2 is p^0_{22} and A_3 is p^0_{33}.

Let A_0, A_1, A_2, A_3 be the adjacency matrices of $(X, \Re)$. Given a ring R of characteristic m, we describe the following construction which we shall use in our construction of self-dual codes. For arbitrary values of $r, s, t, u \in R$ let

$$\begin{aligned} Q_R\left(r,s,t,u\right) &= rA_0 + sA_1 + tA_2 + uA_3 \\ &= rI + sA_1 + tA_2 + u\left(J - I - A_1 - A_2\right) \\ &= \left(r-u\right)I + \left(s-u\right)A_1 + \left(t-u\right)A_2 + uJ. \end{aligned} \tag{1}$$

We write Q for $Q_R\left(r,s,t,u\right)$. We define two different methods of constructing self-dual codes, the pure and bordered construction. In both cases, the generator matrices are defined by using the matrix Q. In the *pure* construction, the generator matrix is

$$\mathcal{P}_R(r,s,t,u) = (I \mid Q). \tag{2}$$

In the *bordered* construction the generator matrix is

$$\mathcal{B}_R(r,s,t,u) = \left(\begin{array}{c|c|c|c} 1 & 0\ldots0 & a & b\ldots b \\ \hline 0 & & c & \\ \vdots & I & \vdots & Q \\ 0 & & c & \end{array}\right). \tag{3}$$

Codes generated by $\mathcal{P}_R(r,s,t,u)$ and $\mathcal{B}_R(r,s,t,u)$ are free and have length $2v$ and $2v+2$, respectively. Thus, to construct a self-dual code we need only make it self-orthogonal.

For the code generated by $\mathcal{P}_R(r,s,t,u)$ to be self-orthogonal we need

$$(I \mid Q)(I \mid Q)^T = \mathbf{0}.$$

Namely, we need $QQ^T = -I$.

For the code generated by $\mathcal{B}_R(r,s,t,u)$ to be self-dual we need the following:

$$1 + a^2 + vb^2 = 0; \tag{4}$$

$$ac + b(r + s\kappa + t\kappa + u(v - 2\kappa - 1)) = 0; \tag{5}$$

$$I + c^2J + QQ^T = \mathbf{0}. \tag{6}$$

The first equation is the inner product of the top row with itself. The second is the inner product of the top row with any other row, and the third ensures that the other rows are orthogonal to each other.

We write $\mathcal{P}$ and $\mathcal{B}$ for $\mathcal{P}_R\left(r,s,t,u\right)$ and $\mathcal{B}_R\left(r,s,t,u\right)$ respectively.

In [4], a generation of binary self-dual codes from non-symmetric 3-class association schemes was studied along with the binary self-dual codes from 3-class rectangular association scheme. In this paper, we study the generation of self-dual codes from 3-class rectangular association schemes over $\mathbb{Z}_k$.

3 Self-dual codes from rectangular association schemes

Let $(X, \Re)$ be a 3-class association scheme. The case of binary non-symmetric 3-class association schemes was studiend in [4]. If the 3-class association scheme is symmetric, then the number of conditions and equations increase when generating self-dual codes from 3-class association schemes over $\mathbb{Z}_k$, for $k \geq 2$. Therefore, we limit ourselves to the rectangular association scheme $n \times m$ $(n, m \geq 2)$ which is defined as follows.

Consider two sets A and B with $|A| = n \geq 2$ and $|B| = m \geq 2$. Let $X = A \times B$ and define the binary relations over X:

$$\begin{aligned} R_0 &= \left\{((x,y),(x,y)) \in X^2\right\}; \\ R_1 &= \left\{ \left((x,y),(x,y')\right) \in X^2 \middle| \, y \neq y'\right\}; \\ R_2 &= \left\{ \left((x,y),(x',y)\right) \in X^2 \middle| \, x \neq x'\right\}; \\ R_3 &= \left\{ \left((x,y),(x',y')\right) \in X^2 \middle| \, x \neq x' \, and \; y \neq y'\right\}. \end{aligned}$$

$(X, \Re)$ is a symmetric 3-class association scheme with parameters:

$v = nm, p_{11}^0 = m-1; p_{22}^0 = n-1; p_{33}^0 = (m-1)(n-1);$
$p_{11}^1 = m-2; p_{23}^1 = p_{32}^1 = n-1; p_{33}^1 = (n-1)(m-2);$
$p_{13}^2 = p_{31}^2 = m-1; p_{22}^2 = n-2; p_{33}^2 = (n-2)(m-1);$
$p_{12}^3 = p_{21}^3 = 1; p_{31}^3 = p_{13}^3 = m-2; p_{23}^2 = p_{32}^2 = n-2 = p_{33}^3 = (n-2)(m-2);$
and $p_{ij}^k = 0,$ for all other cases.

Lemma 2. *If $(X, \Re)$ is a $n \times m$ rectangular association scheme, then the following equations hold:*

$$\begin{aligned} &A_1 J = J A_1 = (m-1) J, A_2 J = J A_2 = (n-1) J, J^2 = n^2 m^2; \\ &A_1^2 = (m-1) I + (m-2) A_1, A_2^2 = (n-1) I + (n-2) A_2; \\ &A_1 A_2 = A_2 A_1 = A_3 = J - I - A_1 - A_2. \end{aligned}$$

Proof. The proof follows by applying Lemma 1 to a rectangular association scheme. □

Using Lemma 2 and Equation (1) we obtain:

$$\begin{aligned} QQ^T = Q^2 \\ &= \Big[(r-u)^2 + (s-u)^2 (m-1) + (t-u)^2 (n-1) - 2(s-u)(t-u)\Big] I \\ &+ \Big[2(r-u)(s-u) + (s-u)^2 (m-2) - 2(s-u)(t-u)\Big] A_1 \\ &+ \Big[2(r-u)(t-u) + (t-u)^2 (n-2) - 2(s-u)(t-u)\Big] A_2 \\ &+ [u\left[2(r-u) + 2(s-u)(m-1) + 2(t-u)(n-1) + un^2m^2\right] \\ &+ 2(s-u)(t-u)]J. \end{aligned} \tag{7}$$

Let $\rho = r - u$, $\sigma = s - u$ and $\tau = t - u$. We can write Equation (7) as

$$\begin{aligned} Q^2 = {} & \left[\rho^2 + \sigma^2 (m-1) + \tau^2 (n-1) - 2\sigma\tau\right] I \\ & + \left[2\rho\sigma + \sigma^2 (m-2) - 2\sigma\tau\right] A_1 \\ & + \left[2\rho\tau + \tau^2 (n-2) - 2\sigma\tau\right] A_1 \\ & + \left[u\left[2\rho + 2\sigma (m-1) + 2\tau (n-1) + un^2m^2\right] + 2\sigma\tau\right] J. \end{aligned} \tag{8}$$

For the code generated by $\mathcal{P}$ to be self-orthogonal we need

$$\begin{aligned} \rho^2 + \sigma^2 (m-1) + \tau^2 (n-1) - 2\sigma\tau &= -1, \\ 2\rho\sigma + \sigma^2 (m-2) - 2\sigma\tau &= 0, \\ 2\rho\tau + \tau^2 (n-2) - 2\sigma\tau &= 0, \\ u\left[2\rho + 2\sigma (m-1) + 2\tau (n-1) + un^2m^2\right] + 2\sigma\tau &= 0. \end{aligned} \tag{9}$$

and, for a code generated by $\mathcal{B}$ to be self-orthogonal, along with Equations (4) and (5), we need

$$\begin{aligned} \rho^2 + \sigma^2 (m-1) + \tau^2 (n-1) - 2\sigma\tau &= -1; \\ 2\rho\sigma + \sigma^2 (m-2) - 2\sigma\tau &= 0; \\ 2\rho\tau + \tau^2 (n-2) - 2\sigma\tau &= 0; \\ u\left[2\rho + 2\sigma (m-1) + 2\tau (n-1) + un^2m^2\right] + 2\sigma\tau &= -c^2. \end{aligned} \tag{10}$$

Theorem 1. *Let C be a code generated from a $n \times m$ rectangular association scheme over $\mathbb{Z}_k$ by using the pure or the bordered construction. Let $k = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factor decomposition of k. If C is a self-dual code, then*

$$\alpha_0 \leq 1 \quad \textit{and} \quad p_i \equiv 1 \pmod 4 \;\; \forall i = 1, \ldots, r. \tag{11}$$

Moreover, if (11) is satisfied, then there exist values of n and m such that C is a self-dual code.

Proof. Assume that C is a self-dual code. Thus, Equations (9) or (10) are satisfied over $\mathbb{Z}_k$. Note that the first three equations are the same in both cases. From these three equations, it is easy to obtain $(\rho - \sigma - \tau)^2 \equiv -1 \pmod k$. Hence, -1 is a quadratic residue modulo k and, using classical results of number theory, it follows (11).

If (11) is satisfied, then we can take the following values:

$$\begin{aligned} m &\equiv \ 1 && \pmod{k}; \\ n &\equiv \ 2 && \pmod{k}; \\ \rho^2 &\equiv -1 && \pmod{k}; \\ \tau &\equiv \ 0 && \pmod{k}; \\ \sigma &\equiv 2\rho && \pmod{k}. \end{aligned}$$

With these values, the first three equations in (9) or (10) are satisfied. The fourth equation becomes:

$$2u(\rho + 2u) \equiv 0 \pmod{k}, \ \text{ or } \ 2u(\rho + 2u) \equiv -c^2 \pmod{k};$$

respectively in (9) or (10). Clearly, the equation has solutions in both cases. It is also straightforward to find solutions for the Equations (4) and (5), as we can see in the following example. □

Example 1. Consider the 3-class rectangular association scheme with $n = 2$ and $m = 6$. The parameters are:

$$\begin{array}{l} p^0_{11} = 5; p^0_{22} = 1; p^0_{33} = 5; \\ p^1_{11} = 4; p^1_{23} = p^1_{32} = 1; p^1_{33} = 4; \\ p^2_{13} = p^2_{31} = 5; p^2_{22} = 0; p^2_{33} = 0; \\ p^3_{12} = p^3_{21} = 1; p^3_{31} = p^3_{13} = 4; p^2_{23} = p^2_{32} = 0 = p^3_{33} = 0; \\ \text{and } p^k_{ij} = 0 \text{ for all other cases.} \end{array}$$

The adjacency matrices are:

$$A_0 = I, \ A_1 = \begin{bmatrix} 0&1&1&1&1&1&0&0&0&0&0&0 \\ 1&0&1&1&1&1&0&0&0&0&0&0 \\ 1&1&0&1&1&1&0&0&0&0&0&0 \\ 1&1&1&0&1&1&0&0&0&0&0&0 \\ 1&1&1&1&0&1&0&0&0&0&0&0 \\ 1&1&1&1&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&1&1&1&1 \\ 0&0&0&0&0&0&1&0&1&1&1&1 \\ 0&0&0&0&0&0&1&1&0&1&1&1 \\ 0&0&0&0&0&0&1&1&1&0&1&1 \\ 0&0&0&0&0&0&1&1&1&1&0&1 \\ 0&0&0&0&0&0&1&1&1&1&1&0 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0&0&0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0&0&0&0&0 \end{bmatrix}, \; A_3 = \begin{bmatrix} 0&0&0&0&0&0&0&1&1&1&1&1\\ 0&0&0&0&0&0&1&0&1&1&1&1\\ 0&0&0&0&0&0&1&1&0&1&1&1\\ 0&0&0&0&0&0&1&1&1&0&1&1\\ 0&0&0&0&0&0&1&1&1&1&0&1\\ 0&0&0&0&0&0&1&1&1&1&1&0\\ 0&1&1&1&1&1&0&0&0&0&0&0\\ 1&0&1&1&1&1&0&0&0&0&0&0\\ 1&1&0&1&1&1&0&0&0&0&0&0\\ 1&1&1&0&1&1&0&0&0&0&0&0\\ 1&1&1&1&0&1&0&0&0&0&0&0\\ 1&1&1&1&1&0&0&0&0&0&0&0 \end{bmatrix}.$$

The code C generated by $\mathcal{P}$, with $Q = 2I + 4A_1$, is a self-dual code over $\mathbb{Z}_5$.

We can generate two self-dual codes over $\mathbb{Z}_5$ with $\mathcal{B}$, using $Q = 2I + 4A_1$ with $a \equiv 2 \pmod 5$ or $a \equiv 3 \pmod 5$ along with $b \equiv c \equiv 0 \pmod 5$.

Note that $\rho^2 \equiv -1 \pmod k$, $\tau \equiv 0 \pmod k$ and $\sigma \equiv 2\rho \pmod k$ in this example.

References

[1] S. T. Dougherty, J. L. Kim, and P. Solé. Double Circulant Codes from Two Class Association Schemes. *AMC*, vol 1, Number 1.

[2] E. Rains and N. J. A. Sloane. Self-dual codes *in the Handbook of Coding Theory, V.S. Pless and W.C. Huffman. Elsevier*, Amsterdam, 177-294, 1998.

[3] D. G. Higman. Coherent Configurations *Geom.Dedicata*, Vol. 4, pp.1-32, 1975.

[4] M. Bilal, J. Borges, S. T. Dougherty, C. Fernández. Binary Self-dual codes from 3-class association schemes. *III International Castle Meeting on Coding Theory and Applications*, UAB vol. 5 , pp: 59 - 64.UAB- (September 2011). ISBN: 978-84-490-2688-1.

Appendix E

Extensions of $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes preserving their properties

Extensions of $\mathbb{Z}_2\mathbb{Z}_4$-Additive Self-Dual Codes Preserving Their Properties

M. Bilal
Dept. of Information and
Communications Engineering
Universitat Autònoma de Barcelona
08193-Bellaterra (Spain)
mbilal@deic.uab.cat

S.T. Dougherty
Dept. of Mathematics
University of Scranton
Scranton, PA 18510 (USA)
doughertys1@scranton.edu

C. Fernández-Córdoba
Dept. of Information and
Communications Engineering
Universitat Autònoma de Barcelona
08193-Bellaterra (Spain)
cfernandez@deic.uab.cat

J. Borges
Dept. of Information and
Communications Engineering
Universitat Autònoma de Barcelona
08193-Bellaterra (Spain)
jborges@deic.uab.cat

***Abstract*—Following [5], given a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code, one can easily extend this code and generate an extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code with greater length. In this communication we study these constructions and check if properties like separability and code Type are retained or not.**

***Keywords*-Self-dual codes, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, separability.**

I. 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 $\mathbb{Z}_4^n$.

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 $\alpha + 2\beta = n$ [2]. 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 which were first defined in [6] and then later deeply studied in [1].

As in [4] and [1], 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 $\Phi(\mathbf{x}, \mathbf{y}) = (\mathbf{x}, \phi(y_1), \ldots, \phi(y_\beta))$ for any $\mathbf{x} \in \mathbb{Z}_2^\alpha$ and any $\mathbf{y} = (y_1, \ldots, y_\beta) \in \mathbb{Z}_4^\beta$, where $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ is the usual Gray map, that is, $\phi(0) = (0,0),\ \phi(1) = (0,1),\ \phi(2) = (1,1),\ \phi(3) = (1,0)$.

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 $(\alpha, \beta; \gamma, \delta; \kappa)$.

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.

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 [1]:

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

where T', T_1, T_2, R, S' are matrices over $\mathbb{Z}_2$ and S is a matrix over $\mathbb{Z}_4$. Let $\mathbf{0}$ be the all-zero vector or matrix. The dimension of these vectors or matrices will be clear from the context.

The *Hamming weight* of a vector $\mathbf{v}_X \in \mathbb{Z}_2^\alpha$ is the number of its nonzero coordinates and it is denoted by $wt_H(\mathbf{v}_X)$. The *Hamming distance* between two vectors $\mathbf{v}_X, \mathbf{u}_X \in \mathbb{Z}_2^\alpha$ is the number of coordinates in which $\mathbf{v}_X$ and $\mathbf{u}_X$ differ from one another, and it is denoted by $d_H(\mathbf{v}_X, \mathbf{u}_X)$. The *Lee weights* of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$ respectively. The Lee weight of a vector $\mathbf{v}_Y = (v_1, \ldots, v_\beta) \in \mathbb{Z}_4^\beta$ is then $w_L(\mathbf{v}_Y) = \sum_i w_L(v_i)$. The *Lee Distance* between $\mathbf{v}_Y, \mathbf{u}_Y \in \mathbb{Z}_4^\beta$ is $d_L(\mathbf{v}_Y, \mathbf{u}_Y) = wt_L(\mathbf{v}_Y - \mathbf{u}_Y)$. For a vector $\mathbf{v} = (\mathbf{v}_X, \mathbf{v}_Y) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, define the weight of $\mathbf{v}$, denoted by $wt(\mathbf{v})$, as $wt_H(\mathbf{v}_X) + wt_L(\mathbf{v}_Y)$ and for $\mathbf{v}, \mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ define the distance as $d(\mathbf{v}, \mathbf{u}) = wt(\mathbf{v} - \mathbf{u})$.

The map Φ is an isometry which transforms distances in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ to Hamming distances in $\mathbb{Z}_2^{\alpha+2\beta}$.

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

In [1], the following inner product is defined for any two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$:

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

The $\mathbb{Z}_2\mathbb{Z}_4$-*additive dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined in the standard way

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

If $C = C^\perp$, then we say that C is a *self-dual* code. If $C \subseteq C^\perp$, meaning all vectors are orthogonal to each other, then we say that C is *self-orthogonal*. 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. $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes were studied in [5].

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*. If $\mathcal{C}$ is a separable $\mathbb{Z}_2\mathbb{Z}_4$-additive code, then the generator matrix of $\mathcal{C}$ in standard form is

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

Definition 2: A binary code C is *antipodal* if for any codeword $c \in C$, we have $c + \mathbf{1} \in C$. If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code then we say that $\mathcal{C}$ is *antipodal* if $\Phi(\mathcal{C})$ is antipodal, where $\Phi(\mathcal{C})$ is the binary image of $\mathcal{C}$.

Definition 3: If a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code has odd weights, then it is said to be of *Type 0*. If the code has only even weights then we say that the code is of *Type I* and if the code has only doubly even weights then it is a *Type II* code.

In [5] it is proven that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code then the following statements hold:

(i) $\mathcal{C}$ is antipodal if and only if $\mathcal{C}$ is Type I or Type II.
(ii) If $\mathcal{C}$ is separable then $\mathcal{C}$ is antipodal.

Therefore a Type 0 code is non-antipodal and non-separable. A Type I or Type II code is antipodal and separable or non-separable.

Theorem 1: [5] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with α, $\beta > 0$.

(i) If $\mathcal{C}$ is Type 0, then $\alpha \geq 2$, $\beta \geq 2$.
(ii) If $\mathcal{C}$ is Type I and separable, then $\alpha \geq 2$, $\beta \geq 1$.
(iii) If $\mathcal{C}$ is Type I and non-separable, then $\alpha \geq 4$, $\beta \geq 4$.
(iv) If $\mathcal{C}$ is Type II, then $\alpha \geq 8$, $\beta \geq 4$.

The following table combines all the results given above for Type 0, I and II codes.

II. Construction Technique: Extending The Length

The construction technique that is described below is from [5]. In [5] examples are given for all the minimum values of α and β that are given in Table I. In this paper we shall extend $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes retaining the original properties like the type of the code and separability.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and let $\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ with $\mathbf{v} \notin \mathcal{C}$. We define $\mathcal{C}_\mathbf{v} = \{\mathbf{u} \in \mathcal{C} | [\mathbf{u}, \mathbf{v}] = 0\}$. It is immediate that $\mathcal{C}_\mathbf{v}$ is a subgroup of $\mathcal{C}$ and that the index $[\mathcal{C} : \mathcal{C}_\mathbf{v}]$ is either 2 or 4. In either case we have $[\mathcal{C} : \mathcal{C}_\mathbf{v}] = [\mathcal{C}_\mathbf{v}^\perp : \mathcal{C}]$ and $\mathcal{C}_\mathbf{v}^\perp = \langle \mathcal{C}, \mathbf{v} \rangle$. Let $\mathbf{w}$ be a vector such that $\mathcal{C} = \langle \mathcal{C}_\mathbf{v}, \mathbf{w} \rangle$. We can then write $\mathcal{C}_\mathbf{v}^\perp = \langle \mathcal{C}, \mathbf{v}, \mathbf{w} \rangle$. We shall form a code $\bar{C}$ by extending the code $C = \mathcal{C}_\mathbf{v}^\perp$ in the following manner.

	Type 0	Type I	Type II
separable/ non-separable	non-separable	separable/ non-separable	separable/ non-separable
antipodality	non-antipodal	antipodal	antipodal
separable $\alpha, \beta; a, b \geqslant 0$	- -	$\alpha = 2 + 2a$ $\beta = 1 + b$	$\alpha = 8 + 8a$ $\beta = 4 + 4b$
non-separable $\alpha, \beta; a, b \geqslant 0$	$\alpha = 2 + 2a$ $\beta = 2 + b$	$\alpha = 4 + 2a$ $\beta = 4 + b$	$\alpha = 8 + 8a$ $\beta = 4 + 4b$

TABLE I
Possible values of α and β

For $\mathbf{u} = (\mathbf{u}_X, \mathbf{u}_Y) \in \mathcal{C}_\mathbf{v}^\perp$ we let $\bar{\mathbf{u}} = (\mathbf{u}'_X, \mathbf{u}_X, \mathbf{u}_Y, \mathbf{u}'_Y)$ where $\mathbf{u}'_X$ is an extension of the binary part and $\mathbf{u}'_Y$ is an extension of the quaternary part. Then let $\bar{C} = \left\langle \bar{\mathbf{u}} | \, \mathbf{u} \in \mathcal{C}_\mathbf{v}^\perp \right\rangle$.

We shall choose $\mathbf{u}'_X$ and $\mathbf{u}'_Y$ such that $\bar{C}$ is a self-orthogonal code. We denote by α' the length of $\mathbf{u}'_X$ and by β' the length of $\mathbf{u}'_Y$. If $\bar{C}$ is not self-dual we may need to add more vectors to the code. In all cases we let $\mathbf{u}'_X$ and $\mathbf{u}'_Y$ be $\mathbf{0}$ if $\mathbf{u} \in \mathcal{C}_\mathbf{v}$ and we denote by $\bar{\mathcal{C}_\mathbf{v}}$ the extension of $\mathcal{C}_\mathbf{v}$. Since $\mathcal{C} = \langle \mathcal{C}_\mathbf{v}, \mathbf{w} \rangle$, we denote $\bar{\mathcal{C}} = \langle \bar{\mathcal{C}_\mathbf{v}}, \bar{\mathbf{w}} \rangle$.

Theorem 2: [5] If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and $\mathbf{v} \notin \mathcal{C}$. Let $\mathbf{w}$, $\mathcal{C}_\mathbf{v}$ be as before and $C = \mathcal{C}_\mathbf{v}^\perp = \langle \mathcal{C}, \mathbf{v}, \mathbf{w} \rangle$. There exists a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $D = \langle \bar{C}, V \rangle$ of type $(\alpha + \alpha', \beta + \beta'; \gamma', \delta'; \kappa')$, for some set of vectors V with the following conditions :

(i) $\alpha' \neq 0$ and $\beta' = 0$ only if $[\mathbf{v}, \mathbf{w}] = 2$ and $[\mathbf{v}, \mathbf{v}] \in \{0, 2\}$.
(ii) $\alpha' = 0$ and $\beta' \neq 0$ only if $[\mathbf{v}, \mathbf{w}] = 2$ or $[\mathbf{v}, \mathbf{w}] \in \{1, 3\}$ and $[\mathbf{v}, \mathbf{v}] \in \{1, 3\}$.
(iii) $\alpha' \neq 0$ and $\beta' \neq 0$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code and $\mathbf{v} \notin \mathcal{C}$. We define $o_\mathcal{C}(\mathbf{v}) = |\langle \mathcal{C}, \mathbf{v} \rangle| / |\mathcal{C}|$. Note that $o_\mathcal{C}(\mathbf{v})$ is not the order of $\mathbf{v}$. In fact, $o_\mathcal{C}(\mathbf{v}) \in \{2, 4\}$ and $o_\mathcal{C}(\mathbf{v}) = 2$ if and only if $2\mathbf{v} \in \mathcal{C}$. Similarly, for a set of vectors V such that $V \cap \mathcal{C} = \emptyset$, we define $o_\mathcal{C}(V) = |\langle \mathcal{C}, V \rangle| / |\mathcal{C}|$. Note that, by definition, if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code, $\mathbf{v} \notin \mathcal{C}$ and $\mathbf{w} \in \mathcal{C}$ such that $\mathcal{C} = \langle \mathcal{C}_\mathbf{v}, \mathbf{w} \rangle$, then

$$o_{\mathcal{C}_\mathbf{v}}(\mathbf{w}) = [\mathcal{C} : \mathcal{C}_\mathbf{v}], \tag{1}$$

and, by definition of $\mathcal{C}_\mathbf{v}^\perp$,

$$o_\mathcal{C}(\mathbf{v}) = [\mathcal{C}_\mathbf{v}^\perp : \mathcal{C}] = [\mathcal{C} : \mathcal{C}_\mathbf{v}]. \tag{2}$$

Lemma 1: [5] Let $\mathcal{C} \subset \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ be an additive self-dual code, $\mathbf{v}$ and $\mathbf{w}$ as above and $C = \mathcal{C}_\mathbf{v}^\perp = \langle \mathcal{C}_\mathbf{v}, \mathbf{w}, \mathbf{v} \rangle$. Then $\bar{C}$ is a self-orthogonal code and we can construct a set V of self-orthogonal vectors so that $\langle \bar{C}, V \rangle$ is self-dual if and only if

$$o_{\bar{C}}(V) = \frac{\sqrt{2^{\alpha' + 2\beta'}}}{o_{\bar{\mathcal{C}}}(\bar{\mathbf{v}}) \big(o_{\bar{\mathcal{C}_\mathbf{v}}}(\bar{\mathbf{w}}) / o_{\mathcal{C}_\mathbf{v}}(\mathbf{w}) \big)}. \tag{3}$$

If $o_{\bar{C}}(V) = 1$, then $V = \emptyset$ and $\bar{C}$ is self-dual.

A. Examples of Codes for minimum values of α and β

The following generator matrices generate $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes for the minimum values of α and β taken from Table I.

The code $\mathcal{C}_1$ generated by the matrix $\mathcal{G}_1$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(2, 2; 1, 1; 1)$. The code has vectors with odd weight, hence it is a Type 0 code, and therefore it is non-separable.

$$\mathcal{G}_1 = \left(\begin{array}{cc|cc} 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 \end{array}\right).$$

The code $\mathcal{C}_2$ generated by the matrix $\mathcal{G}_2$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(2, 1; 2, 0; 1)$. The code $\mathcal{C}_2$ is a separable Type I code.

$$\mathcal{G}_2 = \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 0 & 2 \end{array}\right).$$

The code $\mathcal{C}_3$ generated by the matrix $\mathcal{G}_3$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(4, 4; 4, 1; 2)$. The code $\mathcal{C}_3$ is a non-separable Type I code.

$$\mathcal{G}_3 = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

Let C_H be the extended binary Hamming code of length 8 with generator matrix

$$G_H = \left(\begin{array}{cccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right).$$

The code C_H is a binary self-dual code. Let $\mathcal{D}$ be the quaternary linear code generated by

$$\mathcal{G}_D = \left(\begin{array}{cccc} 2 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 \end{array}\right).$$

The code $\mathcal{D}$ is a quaternary self-dual code. Since both codes C_H and $\mathcal{D}$ have doubly even weights we can generate a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}_4 = C \times \mathcal{D}$ which will be a Type II separable code. The code $\mathcal{C}_4$ is of type $(8, 4; 6, 1; 4)$ and it is generated by

$$\mathcal{G}_4 = \left(\begin{array}{cc} G_H & \mathbf{0} \\ \mathbf{0} & \mathcal{G}_D \end{array}\right).$$

Finally, the code $\mathcal{C}_5$ generated by the matrix $\mathcal{G}_5$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(8, 4; 6, 1; 4)$. The code $\mathcal{C}_5$ is a non-separable Type II code.

$$\mathcal{G}_5 = \left(\begin{array}{cccccccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

B. Extending a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual Type 0 code

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of Type 0. By Table I, the possible values of α and β are $\alpha = 2 + 2a$ and $\beta = 2 + b$, $a, b \geq 0$. We shall extend the binary coordinate first. Let $\mathbf{v} \notin \mathcal{C}$ be such that $[\mathbf{v}, \mathbf{v}] = 2$ and we select $\mathbf{w} \in \mathcal{C} \backslash \mathcal{C}_{\mathbf{v}}$ such that $[\mathbf{v}, \mathbf{w}] = 2$. Define $\mathbf{v}'_X = (0, 1)$ and $\mathbf{w}'_X = (1, 1)$. By Lemma 1, $o_{\bar{\mathcal{C}}}(V) = 1$ and hence $V = \emptyset$. By using the technique described before, we can extend the code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{\mathcal{C}}$ which is of type $(\alpha + 2, \beta; \gamma', \delta'; \kappa')$. The new code generated is of Type 0 and therefore non-separable.

Example 1: Take the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_1$ generated by $\mathcal{G}_1$. We can extend the binary coordinates by selecting $\mathbf{v} = (0, 1 \mid 0, 0)$ and $\mathbf{w} = (0, 1 \mid 3, 3)$ along with the $\mathbf{v}'_X$ and $\mathbf{w}'_X$ given above. The extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{\mathcal{C}}_1$ with generator matrix $\bar{\mathcal{G}}_1$ has type $(4, 2; 2, 1; 2)$. It is non-separable and is of Type 0.

$$\bar{\mathcal{G}}_1 = \left(\begin{array}{cccc|cc} 0 & 0 & 1 & 0 & 1 & 3 \\ 1 & 1 & 0 & 1 & 3 & 3 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{array}\right).$$

Next we extend the quaternary coordinates. Let $\mathbf{v} \notin \mathcal{C}$ be such that $[\mathbf{v}, \mathbf{v}] = 2$ and we select $\mathbf{w} \in \mathcal{C} \backslash \mathcal{C}_{\mathbf{v}}$ such that $[\mathbf{v}, \mathbf{w}] = 2$. Define $\mathbf{v}'_Y = (1, 1)$ and $\mathbf{w}'_Y = (2, 0)$. By Lemma 1, $o_{\bar{\mathcal{C}}}(V) = 1$ and hence $V = \emptyset$. By using the technique described before, we can extend the code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{\mathcal{C}}$ which is of type $(\alpha, \beta + 2; \gamma', \delta'; \kappa')$. The new code generated is of Type 0 and therefore non-separable and non-antipodal.

Example 2: Take the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_1$ generated by $\mathcal{G}_1$. We can extend the quaternary coordinates by selecting $\mathbf{v} = (0, 1 \mid 0, 0)$ and $\mathbf{w} = (0, 1 \mid 3, 3)$ along with the $\mathbf{v}'_Y$ and $\mathbf{w}'_Y$ given above. The extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{\mathcal{C}}_1$ with generator matrix $\bar{\mathcal{G}}_1$ has type $(2, 4; 1, 2; 1)$. It is non-separable and is of Type 0.

$$\bar{\mathcal{G}}_1 = \left(\begin{array}{cc|cccc} 1 & 0 & 1 & 3 & 0 & 0 \\ 0 & 1 & 3 & 3 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right).$$

C. Extending a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual Type I code

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of Type I. By Table I, the possible values of α and β for separable codes are $\alpha = 2 + 2a$ and $\beta = 1 + b$, $a, b \geq 0$, and for non-separable codes are $\alpha = 4 + 2a$ and $\beta = 4 + b$, $a, b \geq 0$.

We start by extending the binary coordinates first. Let $\mathbf{v} \notin \mathcal{C}$ such that $[\mathbf{v}, \mathbf{v}] = 2$ and we select $\mathbf{w} \in \mathcal{C} \backslash \mathcal{C}_{\mathbf{v}}$ such that $[\mathbf{v}, \mathbf{w}] = 2$. Define $\mathbf{v}'_X = (0, 1)$ and $\mathbf{w}'_X = (1, 1)$. By Lemma 1, $o_{\bar{\mathcal{C}}}(V) = 1$ and hence $V = \emptyset$. By using the technique described earlier we can extend the code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}$ which is of type $(\alpha + 2, \beta; \gamma', \delta'; \kappa')$.

Example 3: Take the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_2$ generated by $\mathcal{G}_2$. We can extend the binary coordinates by selecting $\mathbf{v} = (1, 0 \mid 2)$ and $\mathbf{w} = (1, 1 \mid 0)$ along with the $\mathbf{v}'_X$ and $\mathbf{w}'_X$ given above. The extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}_2$, with generator matrix $\bar{\mathcal{G}}_2$, obtained by extending the binary coordinates of $\mathcal{C}_2$ has type $(4, 1; 3, 0; 2)$. It is separable and is of Type I.

$$\bar{\mathcal{G}}_2 = \left(\begin{array}{cccc|c} 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 0 \end{array} \right).$$

Take the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_3$ generated by $\mathcal{G}_3$. We can extend the binary coordinates by selecting $\mathbf{v} = (0, 1, 0, 0, \mid 1, 1, 1, 1)$ and $\mathbf{w} = (1, 0, 1, 0 \mid 2, 0, 0, 0)$ along with the $\mathbf{v}'_X$ and $\mathbf{w}'_X$ given above. The extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}_3$, with generator matrix $\bar{\mathcal{G}}_3$, obtained by extending the binary coordinates of $\mathcal{C}_3$ has type $(6, 4; 5, 1; 3)$. It is non-separable and is of Type I

$$\bar{\mathcal{G}}_3 = \left(\begin{array}{cccccc|cccc} 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right).$$

Now we extend the quaternary part. Let $\mathbf{v} \notin \mathcal{C}$ such that $[\mathbf{v}, \mathbf{v}] = 2$ and we select $\mathbf{w} \in \mathcal{C} \backslash \mathcal{C}_{\mathbf{v}}$ such that $[\mathbf{v}, \mathbf{w}] = 2$. Define $\mathbf{v}'_Y = (1, 1)$ and $\mathbf{w}'_Y = (2, 0)$. By Lemma 1, $o_{\bar{\mathcal{C}}}(V) = 1$ and hence $V = \emptyset$. By using the technique described earlier we can extend the code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}$ which is of type $(\alpha, \beta + 2; \gamma', \delta'; \kappa')$.

Example 4: Take the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_2$ generated by $\mathcal{G}_2$. We can extend the quaternary coordinates by selecting $\mathbf{v} = (1, 0 \mid 2)$ and $\mathbf{w} = (1, 1 \mid 0)$ along with the $\mathbf{v}'_Y$ and $\mathbf{w}'_Y$ given above. When we extend the quaternary coordinates of $\mathcal{C}_2$ we get a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}_2$ matrix $\bar{\mathcal{G}}_2$ of type $(2, 3; 2, 1; 1)$. It is separable and is of Type I.

$$\bar{\mathcal{G}}_2 = \left(\begin{array}{cc|ccc} 0 & 0 & 2 & 0 & 0 \\ 1 & 0 & 2 & 1 & 1 \\ 1 & 1 & 0 & 2 & 0 \end{array} \right).$$

Take the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes $\mathcal{C}_3$ generated by $\mathcal{G}_3$. We can extend the quaternary coordinates by selecting $\mathbf{v} = (0, 1, 0, 0, \mid 1, 1, 1, 1)$ and $\mathbf{w} = (1, 0, 1, 0 \mid 2, 0, 0, 0)$ along with the $\mathbf{v}'_Y$ and $\mathbf{w}'_Y$ given above.When we extend the quaternary coordinates of $\mathcal{C}_3$, we get a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}_3$ with generator matrix $\bar{\mathcal{G}}_3$ of type $(4, 6; 4, 2; 2)$. It is non-separable and is of Type I.

$$\bar{\mathcal{G}}_3 = \left(\begin{array}{cccc|cccccc} 0 & 1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \right).$$

Hence the extended code generated by a Type I code $\mathcal{C}$ using the method described above, both extending the binary or the quaternary coordinates, will generate a Type I separable code if $\mathcal{C}$ is separable and non-separable if $\mathcal{C}$ is non-separable.

D. Extending a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual Type II code

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual Type II code. By Table I, the possible values of α and β are $\alpha = 8 + 8a$ and $\beta = 4 + 4b$, $a, b \geq 0$.

We start by extending the binary part first. Let $\mathbf{v} \notin \mathcal{C}$ such that $[\mathbf{v}, \mathbf{v}] = 2$ and we select $\mathbf{w} \in \mathcal{C} \backslash \mathcal{C}_{\mathbf{v}}$ such that $[\mathbf{v}, \mathbf{w}] = 2$. Define $\mathbf{v}'_X = (1, 0, 0, 0, 0, 0, 1, 1)$ and $\mathbf{w}'_X = (0, 1, 1, 1, 0, 0, 0, 1)$. By Lemma 1, $o_{\bar{\mathcal{C}}}(V) = 3$ and hence $V = (1, 0, 0, 0, 1, 1, 1, 0), (0, 0, 0, 1, 1, 0, 1, 1), (1, 0, 1, 1, 0, 0, 1, 0)$. By using the technique described earlier we can extend the code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}$ which is of type $(\alpha + 8, \beta; \gamma', \delta'; \kappa')$.

Example 5: We consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_4$ generated by $\mathcal{G}_4$. We can extend the binary coordinates by selecting $\mathbf{v} = (0, 0, 0, 0, 1, 0, 0, 0 \mid \mathbf{0})$ and $\mathbf{w} = (0, 1, 0, 0, 1, 0, 1, 1 \mid \mathbf{0})$ along with the $\mathbf{v}'_X$, $\mathbf{w}'_X$ and V given above. The extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}_4$ with generator matrix $\bar{\mathcal{G}}_4$ has type $(16, 4; 10, 1; 8)$. It is separable and is of Type II.

$$\bar{\mathcal{G}}_4 = \begin{pmatrix} \bar{\mathcal{G}}_H & \mathbf{0} \\ \mathbf{0} & \mathcal{G}_D \end{pmatrix},$$

where $\bar{\mathcal{G}}_H$ is

$$\bar{\mathcal{G}}_H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_5$ generated by $\mathcal{G}_5$. We can extend the binary coordinates by selecting $\mathbf{v} = (0, 0, 0, 0, 0, 0, 0, 0 \mid 0, 0, 0, 1)$ and $\mathbf{w} = (0, 0, 0, 1, 1, 0, 1, 1 \mid 1, 1, 1, 1)$ along with the $\mathbf{v}'_X$, $\mathbf{w}'_X$ and V given above. The extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}_5$ with generator matrix $\bar{\mathcal{G}}_5$ has type $(16, 4; 10, 1; 8)$. It is non-separable and is of Type II.

$$\bar{\mathcal{G}}_5 = \left(\begin{array}{c|c} \mathcal{G}_B & \mathcal{G}_Q \end{array} \right),$$

where

$$\mathcal{G}_B = \begin{pmatrix} 0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&0\\ 0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1\\ 0&1&1&1&0&0&0&1&1&1&0&1&1&0&0&0\\ 1&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0\\ 1&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&0&1&1&0&0&0&0&0&0&0&0\\ 1&0&1&1&0&0&1&0&0&0&0&0&0&0&0&0 \end{pmatrix},$$

and

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

Now we will extend the quaternary part of a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual non-separable code. Again let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of Type II. Let $\mathbf{v} \notin \mathcal{C}$ such that $[\mathbf{v},\mathbf{v}] = 1$ and we select $\mathbf{w} \in \mathcal{C}\backslash\mathcal{C}_{\mathbf{v}}$ such that $[\mathbf{v},\mathbf{w}] = 1$. Define $\mathbf{v}'_Y = (1,1,1,0)$ and $\mathbf{w}'_Y = (1,1,1,1)$. By Lemma 1, $o_{\bar{C}}(V) = 2$, hence we select $V = \{(\mathbf{0},0,2,2,0),(\mathbf{0},2,2,0,0)\}$. If $\mathcal{C}$ is of type $(\alpha,\beta;\gamma,\delta;\kappa)$ then by extending the code $\mathcal{C}$ we get a new code $\bar{C}$ which is of type $(\alpha,\beta+4;\gamma',\delta';\kappa')$.

Example 6: We consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_4$ generated by $\mathcal{G}_4$. We can extend the quaternary coordinates by selecting $\mathbf{v} = (0,2,1,0)$ and $\mathbf{w} = (3,1,3,1)$ along with the $\mathbf{v}'_Y$, $\mathbf{w}'_Y$ and V given above. The extended $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}_4$ with generator matrix $\bar{\mathcal{G}}_4$ has type $(16,4;10,1;8)$. It is separable and is of Type II.

$$\mathcal{G}_4 = \begin{pmatrix} G_H & \mathbf{0} \\ \mathbf{0} & \bar{\mathcal{G}}_D \end{pmatrix},$$

where $\bar{\mathcal{G}}_D$ is

$$\bar{\mathcal{G}}_D = \begin{pmatrix} 0&2&0&2&0&0&0&0\\ 2&2&0&0&0&0&0&0\\ 0&2&1&0&1&1&1&0\\ 3&1&3&1&1&1&1&1\\ 0&0&0&0&0&2&2&0\\ 0&0&0&0&2&2&0&0 \end{pmatrix}.$$

We consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\mathcal{C}_5$ generated by $\mathcal{G}_5$. We can extend the quaternary coordinates by selecting $\mathbf{v} = (0,0,0,0,0,0,0,0 \mid 0,0,0,1)$ and $\mathbf{w} = (0,0,0,1,1,0,1,1 \mid 1,1,1,1)$ along with the $\mathbf{v}'_Y$, $\mathbf{w}'_Y$ and V given above. When we extend the quaternary coordinates of $\mathcal{C}_5$ we get a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}_5$ matrix $\bar{\mathcal{G}}_5$ of type $(8,8;8,2;4)$. It is non-separable and is of Type II.

$$\bar{\mathcal{G}}_5 = \left(\begin{array}{c|c} \mathcal{G}_B & \mathcal{G}_Q \end{array} \right),$$

where

$$\mathcal{G}_B = \begin{pmatrix} 1&0&0&1&0&1&1&0\\ 0&1&0&0&1&1&1&0\\ 0&0&1&0&0&1&1&1\\ 0&0&0&0&0&1&1&0\\ 0&0&0&0&0&1&1&0\\ 0&0&0&0&0&1&1&0\\ 0&0&0&1&1&0&1&1\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix},$$

and

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

Hence, the extended code generated by a Type II code $\mathcal{C}$, using the method described above and both extending the binary or the quaternary coordinates, will generate a Type II separable code if $\mathcal{C}$ is separable and non-separable if $\mathcal{C}$ is non-separable.

III. Conclusion

In this communication, we studied the code extension technique described in [5] for $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes. The following theorem summarizes our results.

Theorem 3: If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code of type $(\alpha,\beta;\gamma,\delta;\kappa)$ then given the proper choices of $\mathbf{v}'_X$, $\mathbf{w}'_X$, $\mathbf{v}'_Y$, $\mathbf{w}'_Y$ and V, one can extend the length of the code $\mathcal{C}$ and obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual code $\bar{C}$ of type $(\alpha+\alpha',\beta+\beta';\bar{\gamma},\bar{\delta};\bar{\kappa})$ preserving both the Type and separability or non-separability.

References

[1] 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(2), pp. 167-179, 2010.

[2] P. Delsarte and V. Levenshtein. *Association Schemes and Coding Theory*, IEEE Trans. Inform. Theory, vol. 44(6), pp. 2477-2504, 1998.

[3] P. Delsarte. *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep.Suppl., vol. 10, 1973.

[4] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva. *On $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and duality*, V Jornades de Matemàtica Discreta i Algorísmica, Soria (Spain), Jul. 11-14, pp. 171-177, (2006).

[5] J. Borges, S. T. Dougherty, C. Fernández-Córdoba. *Self-dual Codes Over $\mathbb{Z}_2 \times \mathbb{Z}_4$. Clasification and Constructions*, Submitted to Advances in Mathematics of Communications. (2011). Preprint: arxiv:0910.3084.

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

Muhammad Bilal

Bellaterra, October 5, 2012