$\mathbb{Z}_2\mathbb{Z}_4$-Additive Codes: duality and invariants

Mercè Villanueva

Combinatorial and Coding Group (CCG):
J. Borges; C. Fernández; J. Pujol; J. Rifà; M. Villanueva

Department of Information and Communications Engineering
Universitat Autònoma de Barcelona

The Claude Shannon Workshop on Coding and Cryptography
Cork, 17-18 May, 2010

Outline

1. Introduction
   - Quaternary linear codes
2. $\mathbb{Z}_2\mathbb{Z}_4$-additive codes
   - Definitions
   - Generator matrices
   - Dual codes. Parity-check matrices
   - Gray map. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes
3. Rank and kernel of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes
   - Definitions
   - Rank of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes
   - Kernel of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes
4. Families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

1 Introduction
- Quaternary linear codes

2 $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

3 Rank and kernel of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

4 Families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

Quaternary linear codes

Let $\mathcal{C} \subseteq \mathbb{Z}_4^n$ be a quaternary code.
If $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, then $\mathcal{C}$ is a quaternary linear code.

Example 1.

The quaternary code $\mathcal{C}_0 = \{\mathbf{121}, 323, 103, 301, 000, 202, 220, \mathbf{022}\}$ is a quaternary linear code.

- Generator matrices.
- Dual codes. Parity-check matrices.
- Gray map. $\mathbb{Z}_4$-linear codes.

Two quaternary codes $\mathcal{C}_1$ and $\mathcal{C}_2$ both of length n are monomially equivalent if one can be obtained from the other by permutating the coordinates and (if necessary) changing the signs of certain coordinates.

They are permutation equivalent if they differ only by a permutation of coordinates.

Generator matrices

A quaternary linear code $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$.

Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$.

Its order is a power of two and its type is of the form $4^\delta 2^\gamma$.

- The number of codewords is $|\mathcal{C}| = 2^\gamma 4^\delta$.
- The number of order two codewords is $2^{\gamma+\delta}$.

Moreover, we can define a generator matrix of the code containing γ codewords of order 2 and δ codewords of order 4.

Example 2.

Let $\mathcal{C}_0$ be the quaternary linear code of length 3 and type $2^1 4^1$:

$$\begin{array}{ll} \mathbf{121} & 000 \\ 323 & 202 \\ 103 & 220 \\ 301 & \mathbf{022} \end{array} \qquad \mathcal{G}_0 = \left(\begin{array}{ccc} 0 & 2 & 2 \\ \hline 1 & 2 & 1 \end{array}\right).$$

- The number of codewords is $2^1 4^1 = 8$.
- The number of codewords of order 2 is $2^2 = 4$.

Example 3.

Let $\mathcal{C}_1$ be the quaternary linear code of length 4 and type $2^0 4^2$:

2110	2330	0220
1101	3303	2202
3211	1233	2022
1321	3123	0000
0312	0132	
1013	3031	

$$\mathcal{G}_1 = \begin{pmatrix} \overline{2} & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

- The number of codewords is $2^0 4^2 = 16$.
- The number of codewords of order 2 is $2^2 = 4$.

Proposition 1.

Any quaternary linear code $\mathcal{C}$ of length n and type $4^\delta 2^\gamma$ is permutation equivalent to a quaternary linear code with generator matrix of the form

$$\mathcal{G}_S = \left(\begin{array}{ccc} 2T & 2I_\gamma & \mathbf{0} \\ \hline S & R & I_\delta \end{array}\right), \tag{1}$$

where R, T are matrices over $\mathbb{Z}_2$ of size $\delta \times \gamma$ and $\gamma \times (n-\gamma-\delta)$, respectively; and S is a matrix over $\mathbb{Z}_4$ of size $\delta \times (n-\gamma-\delta)$.

Examples 4.

$$\mathcal{G}_2 = \left(\begin{array}{cccc} 2 & 2 & \mathbf{2} & 0 \\ \hline 0 & 3 & 1 & \mathbf{1} \end{array}\right) \qquad \mathcal{G}_3 = \left(\begin{array}{cccccccc} 2 & 2 & 0 & \mathbf{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{2} & 0 & 0 & 0 \\ \hline 2 & 0 & 2 & 1 & 1 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \mathbf{1} \end{array}\right)$$

Dual codes. Parity-check matrices

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

$$u \cdot v = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n \in \mathbb{Z}_4.$$

Let $\mathcal{C}$ be a quaternary linear code. The quaternary dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined in the standard way:

$$\mathcal{C}^\perp = \{v \in \mathbb{Z}_4^n \mid u \cdot v = 0 \text{ for all } u \in \mathcal{C}\}.$$

It is easy to see that $\mathcal{C}^\perp$ is a subgroup of $\mathbb{Z}_4^n$, so $\mathcal{C}^\perp$ is also a quaternary linear code.

Proposition 2.

The quaternary dual code $\mathcal{C}^{\perp}$ of the quaternary linear code $\mathcal{C}$ of length n with generator matrix $\mathcal{G}_S$ as (1) has generator matrix

$$\mathcal{H}_S = \left(\begin{array}{c|ccc} \mathbf{0} & 2I_\gamma & 2R^t \\ \hline I_{n-\gamma-\delta} & T^t & -(S+RT)^t \end{array}\right), \tag{2}$$

where R, T are matrices over $\mathbb{Z}_2$ of size $\delta \times \gamma$ and $\gamma \times (n-\gamma-\delta)$, respectively; and S is a matrix over $\mathbb{Z}_4$ of size $\delta \times (n-\gamma-\delta)$.

Proposition 3.

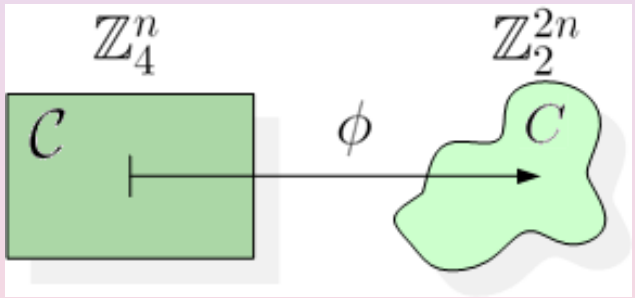
If $\mathcal{C}$ is a quaternary linear code of length n and type $4^\delta 2^\gamma$, then the quaternary dual code $\mathcal{C}^{\perp}$ is of length n and type $4^{n-\gamma-\delta}2^\gamma$.

Gray map. $\mathbb{Z}_4$-linear codes

The usual Gray map $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ is defined as

$$\varphi(0) = 00, \quad \varphi(1) = 01, \quad \varphi(2) = 11, \quad \varphi(3) = 10.$$

and the (exended) Gray map $\phi(x_1, \ldots, x_n) \to (\varphi(x_1), \ldots \varphi(x_n))$



Quaternary linear codes can be viewed as binary codes under the usual Gray map. If $\mathcal{C}$ is a quaternary linear code, then the corresponding binary code $C = \phi(\mathcal{C})$ is said to be a $\mathbb{Z}_4$-linear code.

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

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\phi} & C = \phi(\mathcal{C}) \\ {\scriptstyle dual}\downarrow & & \\ \mathcal{C}^\perp & \xrightarrow{\phi} & C_\perp = \phi(\mathcal{C}^\perp) \end{array}$$

Since 1994 these codes have became significant [HKCSS94]. It was proved that

- the Kerdock and Preparata-like code are $\mathbb{Z}_4$-linear codes,
- the $\mathbb{Z}_4$-dual code of the Kerdock code is the Preparata-like code.

1 Introduction

2 $\mathbb{Z}_2\mathbb{Z}_4$-additive codes
- Definitions
- Generator matrices
- Dual codes. Parity-check matrices
- Gray map. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

3 Rank and kernel of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

4 Families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

Definitions

If $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, then $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code.

Two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomially equivalent if one can be obtained from the other by permutating the coordinates and (if necessary) changing the signs of certain $\mathbb{Z}_4$ coordinates.

They are permutation equivalent if they differ only by a permutation of coordinates.

Example 5.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code generated by

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

$$\mathcal{C} = \left\{ \begin{array}{c} (00 \mid 0000), (11 \mid 2211), (00 \mid 0022), (11 \mid 2233) \\ (10 \mid 2020), (01 \mid 0231), (10 \mid 2002), (01 \mid 0213) \end{array} \right\}$$

The code $\mathcal{C}$ can be seen as the quaternary linear code generated by

$$\left(\begin{array}{cccccc} 2 & 0 & 2 & 0 & 2 & 0 \\ 2 & 2 & 2 & 2 & 1 & 1 \end{array}\right).$$

$$\left\{ \begin{array}{c} (000000), (222211), (000022), (222233) \\ (202020), (020231), (202002), (020213) \end{array} \right\}$$

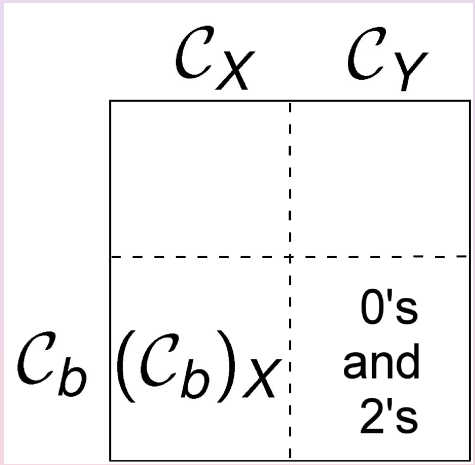
A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, so it is also isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore:

- the order of $\mathcal{C}$ is $|\mathcal{C}| = 2^\gamma 4^\delta$
- 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 out of 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 $\kappa = 0$.



Then, we will say that $\mathcal{C}$ is of type $(\alpha, \beta; \gamma, \delta; \kappa)$.

Example 6.

Let $\mathcal{C}_1$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code generated by

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

- The order of $\mathcal{C}_1$ is $4^1 2^1$, so $\gamma = 1$ and $\delta = 1$.
- We know that $X = \{1, 2\}$ and $Y = \{3, 4, 5, 6\}$, so $\alpha = 2$ and $\beta = 4$.
- The subcode $\mathcal{C}_b$ (all order two codewords) is generated by $(10 \mid 2020)$ and $(00 \mid 0022)$. The binary code $(\mathcal{C}_b)_X$ is generated by (10), so $\kappa = 1$.
- Then, we say that $\mathcal{C}_1$ is of type $(2, 4; 1, 1; 1)$.

Generator matrices

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 as a linear combination of $\{u_i\}_{i=1}^{\gamma}$ of order two and $\{v_j\}_{j=0}^{\delta}$ of order four.

Moreover, the vectors u_i, v_j give us a generator matrix $\mathcal{G}$ of $\mathcal{C}$ of the form

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

where B_1, B_2, B_3 are matrices over $\mathbb{Z}_2$, and Q is a matrix over $\mathbb{Z}_4$.

Theorem 4.

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

$$\mathcal{G}_S = \left(\begin{array}{ccccc} I_\kappa & T_b & 2T_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 2T_1 & 2I_{\gamma-\kappa} & \mathbf{0} \\ \hline \mathbf{0} & S_b & S_q & R & I_\delta \end{array}\right), \tag{3}$$

where T_b, T_1, T_2, R, S_b are matrices over $\mathbb{Z}_2$ and S_q is a matrix over $\mathbb{Z}_4$.

Lemma 5.

There exists a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ if and only if

$$\begin{gathered} \alpha, \beta, \gamma, \delta, \kappa \geq 0, \quad \alpha + \beta > 0, \\ 0 < \delta + \gamma \leq \beta + \kappa \quad \text{and} \quad \kappa \leq \min(\alpha, \gamma). \end{gathered} \tag{4}$$

Examples 7.

$$\mathcal{G}_2 = \left(\begin{array}{c|ccc} \mathbf{1} & 2 & 0 & 0 \\ \hline 0 & 1 & \mathbf{1} & 0 \\ 0 & 3 & 0 & \mathbf{1} \end{array}\right) \qquad \mathcal{G}_3 = \left(\begin{array}{cc|cccc} \mathbf{1} & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & \mathbf{2} & 0 & 0 \\ 0 & 0 & 2 & 0 & \mathbf{2} & 0 \\ \hline 0 & 1 & 3 & 1 & 1 & \mathbf{1} \end{array}\right)$$

The code generated by $\mathcal{G}_2$ is of type $(1, 3; 1, 2; 1)$. The code generated by $\mathcal{G}_3$ is of type $(2, 4; 3, 1; 1)$.

Dual codes. Parity-check matrices

The inner product for any two vectors $u, v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is defined as:

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

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

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

It is easy to see that $\mathcal{C}^\perp$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, so $\mathcal{C}^\perp$ is also a $\mathbb{Z}_2\mathbb{Z}_4$-additive code.

One could think on $\mathbb{Z}_2\mathbb{Z}_4$-additive codes only as quaternary linear codes, changing ones by twos in the coordinates over $\mathbb{Z}_2$.

However, they are not equivalent to the quaternary linear codes, since the inner product defined in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ gives us that the dual code of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code is not equivalent to the dual code of the corresponding quaternary linear code.

Example 8.

Taking $\alpha = \beta = 1$ and the vectors $v = (1 \mid 3)$ and $w = (1 \mid 2)$, it is easy to check that $v \cdot w = 0$, so v and w are orthogonal.

Taking $\beta = 2$ and changing the ones by twos in the coordinates over $\mathbb{Z}_2$ of these vectors, we get $\bar{v} = (23)$ and $\bar{w} = (22)$, which are not orthogonal in the quaternary sense.

Example 9 (cont.).

- Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code generated by

$$\left(\begin{array}{c|c} 1 & 3 \end{array}\right).$$

Then, $\mathcal{C} = \{(0 \mid 0), (1 \mid 3), (0 \mid 2), (1 \mid 1)\}$ and $\mathcal{C}^{\perp} = \{(0 \mid 0), (1 \mid 2)\}$.
Note that $\mathcal{C}$ is of type $(1, 1; 0, 1; 0)$ and $\mathcal{C}^{\perp}$ is of type $(1, 1; 1, 0; 1)$.

- The corresponding quaternary linear code $\mathcal{D}$ is generated by

$$\left(\begin{array}{c|cc} 2 & 3 \end{array}\right).$$

Then, $\mathcal{D} = \{(00), (23), (02), (21)\}$ and $\mathcal{D}^{\perp} = \{(00), (32), (20), (12)\}$.
Note that $\mathcal{D}$ is of type $(0, 2; 0, 1; 0)$ and $\mathcal{D}^{\perp}$ is of type $(0, 2; 0, 1; 0)$.

Theorem 6.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with canonical generator matrix (3). Then, the generator matrix of $\mathcal{C}^\perp$ is

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

where T_b, T_1, T_2, R, S_b are matrices over $\mathbb{Z}_2$ and S_q is a matrix over $\mathbb{Z}_4$.

Theorem 7.

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 then of type $(\alpha, \beta; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$, where $\bar{\gamma} = \alpha + \gamma - 2\kappa$, $\bar{\delta} = \beta - \gamma - \delta + \kappa$ and $\bar{\kappa} = \alpha - \kappa$.

Example 10.

Let $\mathcal{C}_1$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(2,4;2,1;1)$ with generator matrix $\mathcal{G}_1$. The additive dual code $\mathcal{C}_1^\perp$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with generator matrix $\mathcal{H}_1$.

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

- $\mathcal{H}_1$ is a generator matrix of $\mathcal{C}_1^\perp$ and a parity-check matrix of $\mathcal{C}_1$.
- The code $\mathcal{C}_1$ is of type $(2,4;2,1;1)$ and $\mathcal{C}_1^\perp$ is of type $(2,4;2,2;1)$.
- The code $\mathcal{C}_1$ has $2^2 4 = 2^4$ codewords and $\mathcal{C}_1^\perp$ has $2^2 4^2 = 2^6$ codewords, so $|\mathcal{C}_1| \cdot |\mathcal{C}_1^\perp| = 2^2 4^4 = 2^{10}$.

Gray map. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

The Gray map is $\Phi : \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \to \mathbb{Z}_2^{\alpha+2\beta}$:

$$\Phi(x_1, \ldots, x_\alpha, x_{\alpha+1}, \ldots, x_{\alpha+\beta}) \to (x_1, \ldots, x_\alpha, \varphi(x_{\alpha+1}), \ldots \varphi(x_{\alpha+\beta})).$$

As for quaternary linear codes, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes can be view as binary codes under the Gray map.

If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, then the corresponding binary code $C = \Phi(\mathcal{C})$ is said to be a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $n = \alpha + 2\beta$ and type $(\alpha, \beta; \gamma, \delta; \kappa)$, where γ, δ and κ are defined as above.

Again, in general the $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ it is not linear, so it need not have a dual. However, the corresponding binary code $C_\perp = \Phi(\mathcal{C}^\perp)$ is called $\mathbb{Z}_2\mathbb{Z}_4$-dual code of C.

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\Phi} & C = \Phi(\mathcal{C}) \\ {\scriptstyle dual}\downarrow & & \\ \mathcal{C}^\perp & \xrightarrow{\Phi} & C_\perp = \Phi(\mathcal{C}^\perp) \end{array}$$

MAGMA. Computational Algebra System

`http://magma.maths.usyd.edu.au/magma/`
`http://www.scg.uab.cat`

Some functions for $\mathbb{Z}_2\mathbb{Z}_4$-**additive codes**:

- `Z2Z4AdditiveCode(L : Alpha:=0, OverZ2:=false) List -> Rec`
- `Z2Z4Type(C) : Rec -> [ RngIntElt ]`
- `Z2Z4GeneratorMatrix(C) : Rec -> ModMatRngElt`
- `Z2Z4ParityCheckMatrix(C) : Rec -> ModMatRngElt`
- `Z2Z4MinRowsGeneratorMatrix(C) : Rec -> ModMatRngElt`
- `Z2Z4MinRowsParityCheckMatrix(C) : Rec -> ModMatRngElt`
- `Z2Z4StandardForm(C) : Rec -> Rec, Map, ModMatRngElt, GrpPermElt`
- `Z2Z4Dual(C) : Rec -> Rec`
- `Z2Z4DualType(C) : Rec -> [ RngIntElt ]`
- `IsZ2Z4SelfOrthogonal(C) : Rec -> BoolElt`
- `IsZ2Z4SelfDual(C) : Rec -> BoolElt`
- `Z2Z4GrayMap(C) : Rec -> Map`
- `Z2Z4GrayMapImage(C) : Rec -> [ ModTupRngElt ]`
- `HasZ2Z4LinearGrayMapImage(C) : Rec -> BoolElt, Code, Map`

1 Introduction

2 $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

3 Rank and kernel of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes
- Definitions
- Rank of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes
- Kernel of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

4 Families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

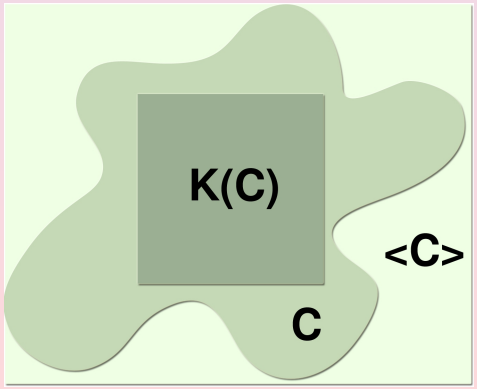
Definitions

Two structural properties of non-linear binary codes are the rank and the kernel. Let C be a binary code, such that $\mathbf{0} \in C$.

- The rank of a binary code C, r, is simply the dimension of the linear span of C, that is $r = dim(\langle C \rangle)$.
- The kernel of a binary code C is

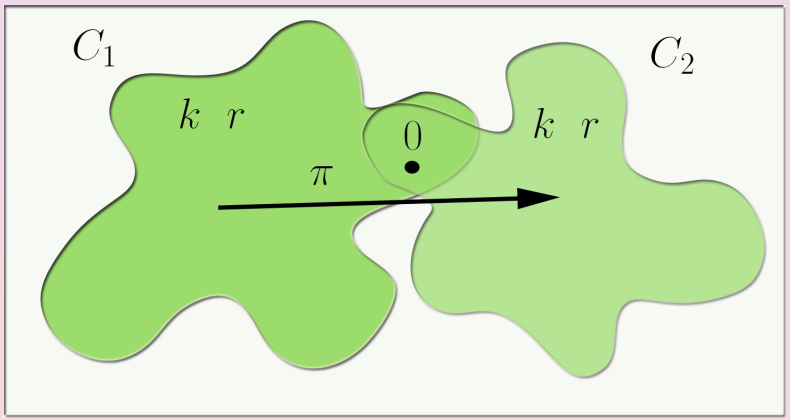
$$K(C) = \{x \in C \mid C = C + x\}.$$

Since $K(C)$ is a linear subspace of C, $k = dim(K(C))$.



Two binary codes C_1 and C_2 are isomorphic if there exists a coordinate permutation $\pi \in S_n$ such that $C_2 = \{\pi(c) \mid c \in C_1\}$.

Two binary codes C_1 and C_2 are equivalent if there exists a vector $a \in \mathbb{Z}_2^n$ and a coordinate permutation $\pi \in S_n$ such that $C_2 = \{a + \pi(c) \mid c \in C_1\}$.



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

Let $\mathcal{G}$ be a generator matrix of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$. Let $\{u_i\}_{i=1}^{\gamma}$ be the rows of order two and $\{v_j\}_{j=0}^{\delta}$ the rows of order four in $\mathcal{G}$. Then $\langle C \rangle = \langle \phi(\mathcal{C}) \rangle$ is generated by

$$\{\phi(u_1), \cdots, \phi(u_\gamma),$$
$$\phi(v_1), \cdots, \phi(v_\delta), \phi(2v_1), \cdots, \phi(2v_\delta),$$

$$\phi(2v_1 * v_2), \cdots, \phi(2v_{\delta-1} * v_\delta)\},$$

where $u * v$ denote the component-wise product, $u, v \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$.

Example 11.

Consider the code $\mathcal{C}_2$ with generator matrix:

$$\mathcal{G}_2 = \left(\begin{array}{c} u_1 \\ u_2 \\ \hline v_1 \\ v_2 \\ v_3 \end{array}\right) = \left(\begin{array}{cccccccc} 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ \hline 1 & 0 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\begin{aligned} 2v_1 * v_2 &= 00000000 = \mathbf{0} \\ 2v_1 * v_3 &= 20002000 = u_2 \\ 2v_2 * v_3 &= 00200000 \end{aligned}$$

Then $\langle \phi(\mathcal{C}_2) \rangle$ is generated by:

$$\begin{gathered} \phi(u_1), \phi(u_2) \\ \phi(v_1), \phi(v_2), \phi(v_3), \phi(2v_1), \phi(2v_2), \phi(2v_3) \\ \phi(2v_2 * v_3) \end{gathered}$$

and $rank(\phi(\mathcal{C}_2))$ is $\gamma + 2\delta + 1 = 9$.

Theorem 8.

Let $\alpha, \beta, \gamma, \delta, \kappa$ be integer numbers satisfying (4). Then, there exists a $\mathbb{Z}_2\mathbb{Z}_4$-linear code C of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and rank r, if and only if

$$r \in \{\gamma + 2\delta, \ldots, \min\left(\beta + \delta + \kappa,\ \gamma + 2\delta + \binom{\delta}{2}\right)\}.$$

Examples 12.

- Type $(\alpha, 5; 2, 3; 1)$, $r \in \{8, \ldots, \min(9, 11)\} = \{8, 9\}$.
- Type $(\alpha, 8; 2, 3; 1)$, $r \in \{8 \ldots, \min(12, 11)\} = \{8, 9, 10, 11\}$.

Kernel dimension of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

Let $\mathcal{G}$ be a generator matrix of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ and let $C = \Phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear code. Then,

$$K(C) = \{x \in C \mid C = C + x\}$$

$$K(C) = \{\phi(u) \mid u \in \mathcal{C} \text{ and } 2u * v \in \mathcal{C}, \forall v \in \mathcal{G}\}.$$

Note that all codewords of order two in $\mathcal{C}$ belong to $K(C)$ and $K(C)$ is a $\mathbb{Z}_2\mathbb{Z}_4$-linear subcode of C.

Example 13.

Consider the code $\mathcal{C}_2$ with generator matrix:

$$\mathcal{G}_2 = \begin{pmatrix} u_1 \\ u_2 \\ \hline v_1 \\ v_2 \\ v_3 \end{pmatrix} = \left(\begin{array}{cccccccc} 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ \hline 1 & 0 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\begin{aligned} 2v_1 * v_2 &= 00000000 = \mathbf{0} \\ 2v_1 * v_3 &= 20002000 = u_2 \\ 2v_2 * v_3 &= 00200000 \end{aligned}$$

Then $K(\phi(\mathcal{C}_2))$ is generated by:

$$\begin{gathered} \phi(u_1), \phi(u_2) \\ \phi(2v_1), \phi(2v_2), \phi(2v_3) \\ \phi(v_1) \end{gathered}$$

and $dim(K(\phi(\mathcal{C}_3))) = 6$.

Theorem 9.

Let $\alpha, \beta, \gamma, \delta, \kappa$ be integer numbers satisfying (4). Then, there exists a $\mathbb{Z}_2\mathbb{Z}_4$-linear code C of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and dimension of the kernel k, if and only if

$$k \in \begin{cases} \{\gamma+\delta, \ldots, \gamma+2\delta-2, \gamma+2\delta\} & \text{if} \quad s \geq 2 \\ \{\gamma+2(\delta-\lceil\frac{\delta-1}{2}\rceil), \ldots, \gamma+2(\delta-1), \gamma+2\delta\} & \text{if} \quad s=1 \\ \{\gamma+2\delta\} & \text{if} \quad s=0, \end{cases}$$

where $s = \beta - (\gamma - \kappa) - \delta$.

Examples 14.

- Type $(\alpha, 7; 2, 5; 1)$, $s = 1$ $\quad k \in \{-, 8, -, 10, -, 12\}$.
- Type $(\alpha, 8; 2, 5; 1)$, $s = 2 \geq 2$ $\quad k \in \{7, 8, 9, 10, -, 12\}$.

1 Introduction

2 $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

3 Rank and kernel of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

4 Families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

Results on binary 1-perfect codes

A binary 1-perfect code C of length n is a subset of $\mathbb{Z}_2^n$, such that for some integer $r \geq 0$ every $x \in \mathbb{Z}_2^n$ is within distance r from exactly one codeword of C.

- Borges-Rifà 98. Characterization of 1-perfect $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.
- Borges-Phelps-Rifà 02,03. Computation of rank and dimension of the kernel for all (extended) 1-perfect $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.
- Rifà-Solov'eva-Villanueva 08. Intersection problem for 1-perfect $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

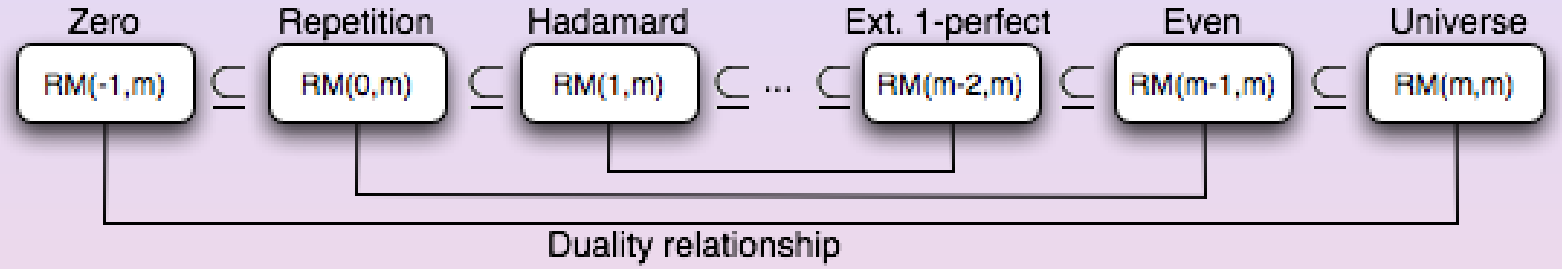
Results on binary Hadamard codes

A binary Hadamard code of length $n = 2^m$ is a binary code with $2n$ codewords and minimum Hamming distance $n/2$.

- Phelps-Rifà-Villanueva 06. Rank and kernel for Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.
- Rifà-Solov'eva-Villanueva 09. Intersection problem for Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

Results on Reed-Muller codes

A binary Reed-Muller family of codes is



- Borges-Fernández-Phelps 08. Rank and kernel for nonlinear Reed-Muller codes (ZRM and QRM codes).
- Pujol-Rifà-Solov'eva 09. Construction of quaternary linear Reed-Muller codes having the same parameters as the binary linear Reed-Muller codes.
- Pujol-Rifà-Ronquillo 09. Construction of additive Reed-Muller codes.
- Pernas-Pujol-Villanueva 10. Classification of some families of quaternary Reed-Muller codes such that, after the Gray map, they have the same parameters as the binary linear Reed-Muller codes.

Bibliography


J. Borges, C. Fernández, 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, 2010.


C. Fernández, J. Pujol, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel," *Designs, Codes and Cryptography*, vol. 56(1), pp. 43, 2010.


J. Borges, C. Fernández, J. Pujol, J. Rifà and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-additive codes. A MAGMA package" Autonomous University of Barcelona (UAB), 2007. `http://www.scg.uab.cat`


J. Borges, K.T. Phelps and J. Rifà, "The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes", *IEEE Trans. on Information Theory*, vol. 49(8), pp. 2028-2034, 2003.


J. Borges, K.T. Phelps, J. Rifà and V.A. Zinoviev, "On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes", *IEEE Trans. on Information Theory*, vol. 49(11), pp. 2834-2843, 2003.


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 Trans. on Information Theory*, vol. 40, pp. 301-319, 1994.


K.T. Phelps, J. Rifà and M. Villanueva, "On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: Rank and Kernel", *IEEE Trans. on Information Theory*, vol. 52(1), pp. 316-319, 2006.