On the Kernel of $\mathbb{Z}_{2^s}$-Linear Codes

Carlos Vela Cabello

joint work with Prof. C. Fernández-Córdoba and Prof. M. Villanueva

Department of Information and Communications Engineering
Universitat Autònoma de Barcelona, Spain.
{cristina.fernandez,carlos.vela,merce.villanueva}@uab.cat

5^{th} International Castle Meeting on Coding Theory and Applications
Vihula Manor, Estonia
August 28-31, 2017.

Universitat Autònoma de Barcelona

Outline

Binary Hadamard codes

A binary code C of length n is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code C of length n is a Hadamard code if,

- C has $2n$ codewords and
- C has minimum distance $n/2$.

The minimum distance d, of a code C, is $\min\{d_H(u,v) : u, v \in C, u \neq v\}$. The Hamming distance d_H between $u, v \in \mathbb{Z}_2^n$, $d_H(u,v)$ is the number of coordinates in which u and v differ.
Linear binary Hadamard codes are also know as **First Order Reed-Müller codes**

Binary Hadamard codes

A binary code C of length n is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code C of length n is a Hadamard code if,

- C has $2n$ codewords and
- C has minimum distance $n/2$.

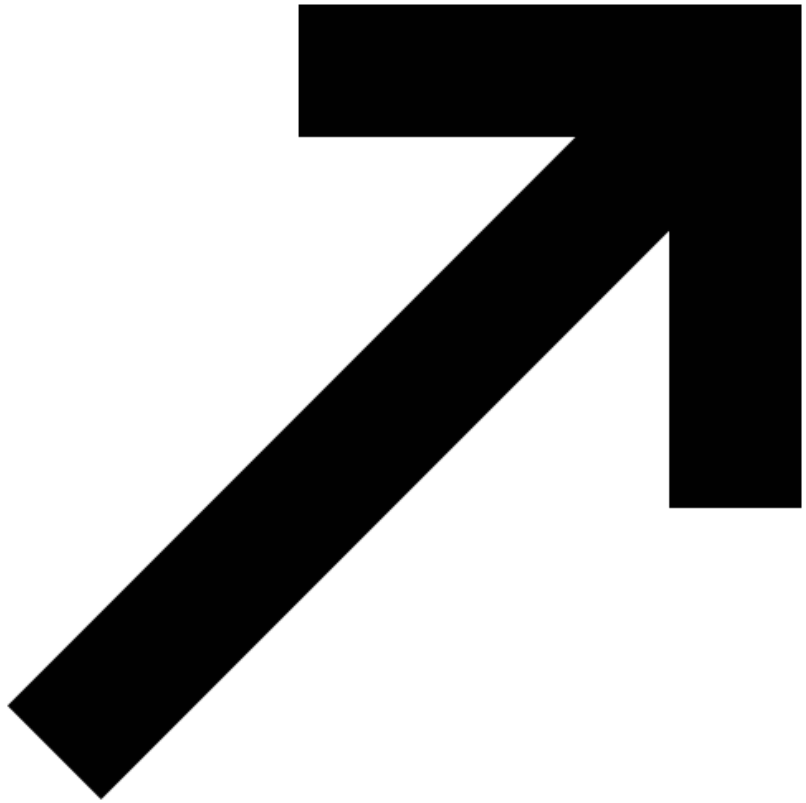
The minimum distance d, of a code C, is $\min\{d_H(u,v) : u, v \in C, u \neq v\}$. The Hamming distance d_H between $u, v \in \mathbb{Z}_2^n$, $d_H(u,v)$ is the number of coordinates in which u and v differ.
Linear binary Hadamard codes are also know as **First Order Reed-Müller codes**

Binary code

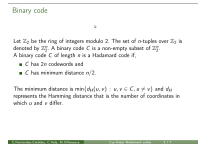
Let $\mathbb{Z}_2$ be the ring of integers modulo 2. The set of n-tuples over $\mathbb{Z}_2$ is denoted by $\mathbb{Z}_2^n$. A binary code C is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code C of length n is a Hadamard code if,

- C has $2n$ codewords and
- C has minimum distance $n/2$.

The minimum distance is $\min\{d_H(u,v) : u, v \in C, u \neq v\}$ and d_H represents the Hamming distance that is the number of coordinates in which u and v differ.



$\mathbb{Z}_{2^s}$-Additive code


Binary code

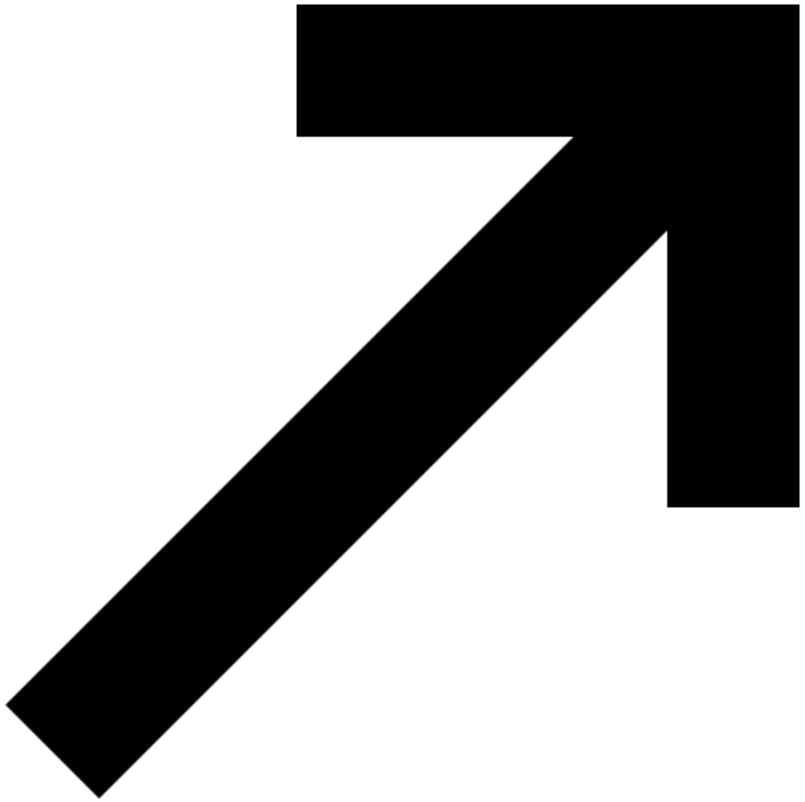
Let $\mathbb{Z}_2$ be the ring of integers modulo 2. The set of n-tuples over $\mathbb{Z}_2$ is denoted by $\mathbb{Z}_2^n$. A binary code C is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code C of length n is a Hadamard code if,

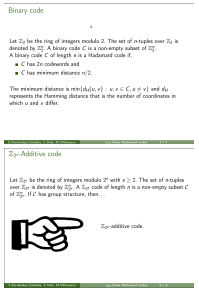
- C has $2n$ codewords and
- C has minimum distance $n/2$.

The minimum distance is $\min\{d_H(u,v) : u,v \in C, u \neq v\}$ and d_H represents the Hamming distance that is the number of coordinates in which u and v differ.

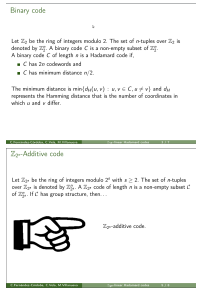
Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 2$. The set of vectors of length n over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. A code over $\mathbb{Z}_{2^s}$ of length n is a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_{2^s}^n$. If $\mathcal{C}$ has group structure, then...

$\mathbb{Z}_{2^s}$-additive code.




Binary code
Let $\mathbb{Z}_2$ be the ring of integers modulo 2. The set of n-tuples over $\mathbb{Z}_2$ is denoted by $\mathbb{Z}_2^n$. A binary code C is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code C of length n is a Hadamard code if:
C has $2n$ codewords and
C has minimum distance $n/2$.
The minimum distance is $\min\{d_H(u,v) : u, v \in C, u \neq v\}$ and d_H represents the Hamming distance that is the number of coordinates in which u and v differ.
$\mathbb{Z}_{2^s}$-Additive code
Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 2$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. A $\mathbb{Z}_{2^s}$-code of length n is a non-empty subset C of $\mathbb{Z}_{2^s}^n$. If C has group structure, then ...
$\mathbb{Z}_{2^s}$-additive code.

$\mathbb{Z}_{2^s}$-Additive codes



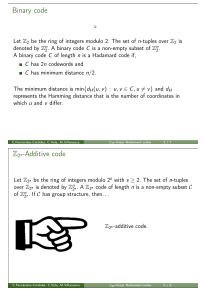
Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2^s}^n$, it is isomorphic to an abelian structure $\mathbb{Z}_{2^s}^{t_1} \times \mathbb{Z}_{2^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_4^{t_{s-1}} \times \mathbb{Z}_2^{t_s}$, and we say that $\mathcal{C}$ is of type $(n; t_1, \ldots, t_s)$.
The standard form of its generator matrix is

- t_1 generators of order 2^s,
- t_2 generators of order 2^{s-1},

$$\vdots$$

- t_s generators of order 2.

Gray map



The classical Gray map is $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$

$$\begin{aligned} \phi(0) &= (0,0) \\ \phi(1) &= (0,1) \\ \phi(2) &= (1,1) \\ \phi(3) &= (1,0) \end{aligned}$$

ISOMETRY

Let $u \in \mathbb{Z}_{2^s}$. The generalized Gray map image of u is (Carlet, 1998),

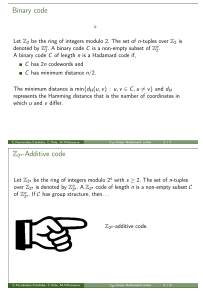
$$\phi(u) = (u_s, \ldots, u_s) + (u_1, \ldots, u_{s-1})Y,$$

where:

- $[u_1, u_2, \ldots, u_s]_2$ is the binary expansion of u
- Y is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$.
- but...

~~ISOMETRY~~

Gray map



The classical Gray map is $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$

$$\begin{aligned} \phi(0) &= (0,0) \\ \phi(1) &= (0,1) \\ \phi(2) &= (1,1) \\ \phi(3) &= (1,0) \end{aligned}$$

ISOMETRY

Let $u \in \mathbb{Z}_{2^s}$. The generalized Gray map image of u is (Carlet, 1998),

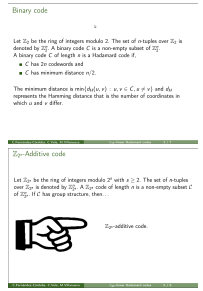
$$\phi(u) = (u_s, \ldots, u_s) + (u_1, \ldots, u_{s-1})Y,$$

where:

- $[u_1, u_2, \ldots, u_s]_2$ is the binary expansion of u
- Y is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$.
- but...

~~ISOMETRY~~

Gray map



The classical Gray map is $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$

$$\begin{aligned} \phi(0) &= (0,0) \\ \phi(1) &= (0,1) \\ \phi(2) &= (1,1) \\ \phi(3) &= (1,0) \end{aligned}$$

ISOMETRY

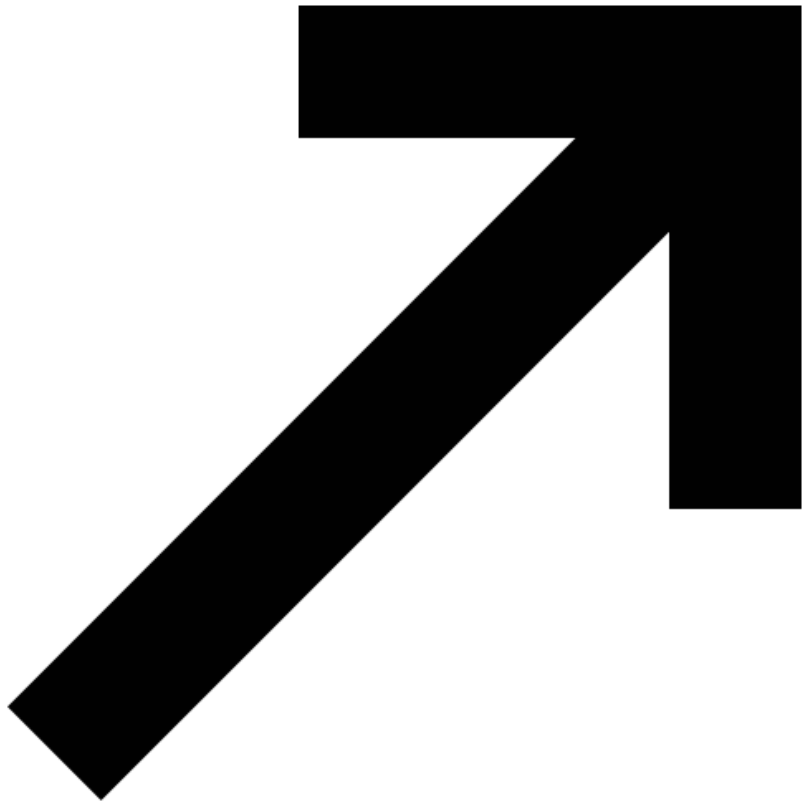
Let $u \in \mathbb{Z}_{2^s}$. The generalized Gray map image of u is (Carlet, 1998),

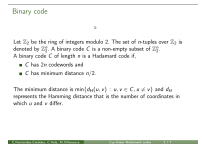
$$\phi(u) = (u_s, \ldots, u_s) + (u_1, \ldots, u_{s-1})Y,$$

where:

- $[u_1, u_2, \ldots, u_s]_2$ is the binary expansion of u
- Y is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$.
- but...

~~ISOMETRY~~

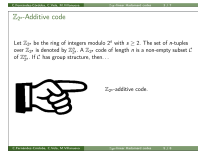



Binary code

Let $\mathbb{Z}_2$ be the ring of integers modulo 2. The set of n-tuples over $\mathbb{Z}_2$ is denoted by $\mathbb{Z}_2^n$. A binary code C is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code C of length n is a Hadamard code if...

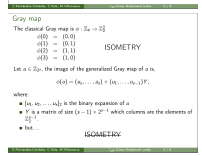
- C has $2n$ codewords and
- C has minimum distance $n/2$.

The minimum distance is $\min\{d_H(u,v) : u,v \in C, u \neq v\}$ and d_H represents the Hamming distance that is the number of coordinates in which u and v differ.


$\mathbb{Z}_{2^s}$-Additive code

Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 2$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. A $\mathbb{Z}_{2^s}$- code of length n is a non-empty subset C of $\mathbb{Z}_{2^s}^n$. If C has group structure, then...

$\mathbb{Z}_{2^s}$-additive code.


Gray map

The classical Gray map is $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$

$$\begin{array}{rcl} \phi(0) & = & (0,0) \\ \phi(1) & = & (0,1) \\ \phi(2) & = & (1,1) \\ \phi(3) & = & (1,0) \end{array}$$

ISOMETRY

Let $a \in \mathbb{Z}_{2^s}$, the image of the generalized Gray map of a is,

$$\phi(a) = (a_1, \ldots, a_l) = (a_1, \ldots, a_{l-1})V,$$

where

- $(a_1, a_2, \ldots, a_l)_2$ is the binary expansion of a
- V is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$.
- but...

ISOMETRY

Binary code

Let $\mathbb{Z}_2$ be the ring of integers modulo 2. The set of n-tuples over $\mathbb{Z}_2$ is denoted by $\mathbb{Z}_2^n$. A binary code C is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code C of length n is a Hadamard code if,

- C has $2n$ codewords and
- C has minimum distance $n/2$.

The minimum distance is $\min\{d_H(u,v) : u, v \in C, u \neq v\}$ and d_H represents the Hamming distance that is the number of coordinates in which u and v differ.

$\mathbb{Z}_{2^s}$-Additive code

Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 2$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. A $\mathbb{Z}_{2^s}$ code of length n is a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_{2^s}^n$. If $\mathcal{C}$ has group structure, then...

$\mathbb{Z}_{2^s}$-additive code.

Gray map

The classical Gray map is $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$

$$\begin{array}{rcl} \phi(0) & = & (0,0) \\ \phi(1) & = & (0,1) \\ \phi(2) & = & (1,1) \\ \phi(3) & = & (1,0) \end{array}$$

ISOMETRY

Let $a \in \mathbb{Z}_{2^s}$, the image of the generalized Gray map of a is,

$$\phi(a) = (a_{s-1}, \ldots, a_1) + (a_1, \ldots, a_{s-1})V,$$

where

- $(a_1, a_2 \ldots, a_s)_2$ is the binary expansion of a.
- V is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$.
- but...

ISOMETRY

$\mathbb{Z}_{2^s}$-Additive code

Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 2$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. A $\mathbb{Z}_{2^s}$ code of length n is a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_{2^s}^n$. If $\mathcal{C}$ has group structure, then...

$\mathbb{Z}_{2^s}$-additive code.

Gray map

The classical Gray map is $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$

$$\begin{array}{rcl} \phi(0) & = & (0,0) \\ \phi(1) & = & (0,1) \\ \phi(2) & = & (1,1) \\ \phi(3) & = & (1,0) \end{array}$$

ISOMETRY

Let $u \in \mathbb{Z}_{2^s}$, the image of the generalized Gray map of u is,

$$\phi(u) = (u_s, \ldots, u_s) + (u_1, \ldots, u_{s-1})Y,$$

where:

- $[u_1, u_2, \ldots, u_s]_2$ is the binary expansion of u
- Y is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$.
- but...

~~ISOMETRY~~

$\mathbb{Z}_{2^s}$-Additive code

Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 2$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. A $\mathbb{Z}_{2^s}$ code of length n is a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_{2^s}^n$. If $\mathcal{C}$ has group structure, then...

$\mathbb{Z}_{2^s}$-additive code.

Binary code

Let $\mathbb{Z}_2$ be the ring of integers modulo 2. The set of n-tuples over $\mathbb{Z}_2$ is denoted by $\mathbb{Z}_2^n$. A binary code $\mathcal{C}$ is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code $\mathcal{C}$ of length n is a Hadamard code if,

- $\mathcal{C}$ has $2n$ codewords and
- $\mathcal{C}$ has minimum distance $n/2$.

The minimum distance is $\min\{d_H(u,v) : u, v \in \mathcal{C}, u \neq v\}$ and d_H represents the Hamming distance that is the number of coordinates in which u and v differ.

Gray map

The classical Gray map is $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$

$$\begin{array}{rcl} \phi(0) & = & (0,0) \\ \phi(1) & = & (0,1) \\ \phi(2) & = & (1,1) \\ \phi(3) & = & (1,0) \end{array}$$

ISOMETRY

Let $u \in \mathbb{Z}_{2^s}$, the image of the generalized Gray map of u is,

$$\phi(u) = (u_s, \ldots, u_s) + (u_1, \ldots, u_{s-1})Y,$$

where:

- $[u_1, u_2, \ldots, u_s]_2$ is the binary expansion of u
- Y is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$.
- but...

~~ISOMETRY~~

$\mathbb{Z}_{2^s}$-Additive code

Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 2$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. A $\mathbb{Z}_{2^s}$ code of length n is a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_{2^s}^n$. If $\mathcal{C}$ has group structure, then...

$\mathbb{Z}_{2^s}$-additive code.

Binary code

Let $\mathbb{Z}_2$ be the ring of integers modulo 2. The set of n-tuples over $\mathbb{Z}_2$ is denoted by $\mathbb{Z}_2^n$. A binary code C is a non-empty subset of $\mathbb{Z}_2^n$.
A binary code C of length n is a Hadamard code if,

- C has $2n$ codewords and
- C has minimum distance $n/2$.

The minimum distance is $\min\{d_H(u,v) : u, v \in C, u \neq v\}$ and d_H represents the Hamming distance that is the number of coordinates in which u and v differ.

We construct $\mathbb{Z}_{2^s}$-Linear Hadamard codes!

Construction of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

How are their generator matrices?

Let $T_i = \{j \cdot 2^{s-i} : j \in \{0, 1, \ldots, 2^i - 1\}\}$, for all $i \in \{1, \ldots, s\}$. Note that $T_s = \{0, \ldots, 2^s - 1\}$.

Let t_1, $t_2, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$. Consider the matrix $A^{t_1,\ldots,t_s}$ whose columns are of the form z^T with

$$z \in \{1\} \times T_s^{t_1-1} \times T_{s-1}^{t_2} \times \cdots \times T_1^{t_s}.$$

We can also construct these matrices, recursively, in the following way.

Construction of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

How are their generator matrices?

Let $T_i = \{j \cdot 2^{s-i} : j \in \{0, 1, \ldots, 2^i - 1\}\}$, for all $i \in \{1, \ldots, s\}$. Note that $T_s = \{0, \ldots, 2^s - 1\}$.

Let t_1, $t_2, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$. Consider the matrix $A^{t_1,\ldots,t_s}$ whose columns are of the form z^T with

$$z \in \{1\} \times T_s^{t_1-1} \times T_{s-1}^{t_2} \times \cdots \times T_1^{t_s}.$$

We can also construct these matrices, recursively, in the following way.

Construction of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

How are their generator matrices?

Let $T_i = \{j \cdot 2^{s-i} : j \in \{0, 1, \ldots, 2^i - 1\}\}$, for all $i \in \{1, \ldots, s\}$. Note that $T_s = \{0, \ldots, 2^s - 1\}$.

Let t_1, t_2,...,t_s be nonnegative integers with $t_1 \geq 1$. Consider the matrix $A^{t_1,\ldots,t_s}$ whose columns are of the form z^T with

$$z \in \{1\} \times T_s^{t_1-1} \times T_{s-1}^{t_2} \times \cdots \times T_1^{t_s}.$$

We can also construct these matrices, recursively, in the following way.

Construction of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

How are their generator matrices?

Let $T_i = \{j \cdot 2^{s-i} : j \in \{0, 1, \ldots, 2^i - 1\}\}$, for all $i \in \{1, \ldots, s\}$. Note that $T_s = \{0, \ldots, 2^s - 1\}$.

Let t_1, t_2,. . . ,t_s be nonnegative integers with $t_1 \geq 1$. Consider the matrix $A^{t_1,\ldots,t_s}$ whose columns are of the form z^T with

$$z \in \{1\} \times T_s^{t_1-1} \times T_{s-1}^{t_2} \times \cdots \times T_1^{t_s}.$$

We can also construct these matrices, recursively, in the following way.

Construction of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

A little algorithm:

- Start with the matrix $A^{1,0,\ldots,0} = (1)$.
- Given a matrix $A^{t_1,\ldots,t_s}$ we construct:

$$A^{t_1',\ldots,t_s'} = \begin{pmatrix} A^{t_1,\ldots,t_s} & A^{t_1,\ldots,t_s} & \ldots & A^{t_1,\ldots,t_s} \\ 0 \cdot \mathbf{2}^{i-1} & 1 \cdot \mathbf{2}^{i-1} & \ldots & (2^{s-i+1}-1) \cdot \mathbf{2}^{i-1} \end{pmatrix}$$

where $i \in \{1, \ldots, s\}$, $t_j' = t_j$ for $j \neq i$ and $t_i' = t_i + 1$.

Theorem

Let $t_1, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$. The $\mathbb{Z}_{2^s}$-linear code $\Phi(\mathcal{H}^{t_1,\ldots,t_s}) = H^{t_1,\ldots,t_s}$ of type $(n; t_1, t_2, \ldots, t_s)$ is a binary Hadamard code of length 2^t, with $t = (\sum_{i=1}^{s}(s-i+1) \cdot t_i) - 1$.

Construction of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

A little algorithm:

- Start with the matrix $A^{1,0,\ldots,0} = (1)$.
- Given a matrix $A^{t_1,\ldots,t_s}$ we construct:

$$A^{t_1',\ldots,t_s'} = \begin{pmatrix} A^{t_1,\ldots,t_s} & A^{t_1,\ldots,t_s} & \ldots & A^{t_1,\ldots,t_s} \\ 0 \cdot 2^{i-1} & 1 \cdot 2^{i-1} & \ldots & (2^{s-i+1}-1) \cdot 2^{i-1} \end{pmatrix}$$

where $i \in \{1,\ldots,s\}$, $t_j' = t_j$ for $j \neq i$ and $t_i' = t_i + 1$.

Theorem

Let $t_1,\ldots,t_s$ be nonnegative integers with $t_1 \geq 1$. The $\mathbb{Z}_{2^s}$-linear code $\Phi(\mathcal{H}^{t_1,\ldots,t_s}) = H^{t_1,\ldots,t_s}$ of type $(n; t_1, t_2, \ldots, t_s)$ is a binary Hadamard code of length 2^t, with $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$.

Construction of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

A little algorithm:

- Start with the matrix $A^{1,0,\ldots,0} = (1)$.
- Given a matrix $A^{t_1,\ldots,t_s}$ we construct:

$$A^{t_1',\ldots,t_s'} = \begin{pmatrix} A^{t_1,\ldots,t_s} & A^{t_1,\ldots,t_s} & \ldots & A^{t_1,\ldots,t_s} \\ 0 \cdot \mathbf{2}^{i-1} & 1 \cdot \mathbf{2}^{i-1} & \ldots & (2^{s-i+1}-1) \cdot \mathbf{2}^{i-1} \end{pmatrix}$$

where $i \in \{1,\ldots,s\}$, $t_j' = t_j$ for $j \neq i$ and $t_i' = t_i + 1$.

Theorem

Let $t_1,\ldots,t_s$ be nonnegative integers with $t_1 \geq 1$. The $\mathbb{Z}_{2^s}$-linear code $\Phi(\mathcal{H}^{t_1,\ldots,t_s}) = H^{t_1,\ldots,t_s}$ of type $(n; t_1, t_2, \ldots, t_s)$ is a binary Hadamard code of length 2^t, with $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$.

Construction of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

A little algorithm:

- Start with the matrix $A^{1,0,\ldots,0} = (1)$.
- Given a matrix $A^{t_1,\ldots,t_s}$ we construct:

$$A^{t_1',\ldots,t_s'} = \begin{pmatrix} A^{t_1,\ldots,t_s} & A^{t_1,\ldots,t_s} & \ldots & A^{t_1,\ldots,t_s} \\ 0 \cdot \mathbf{2}^{i-1} & 1 \cdot \mathbf{2}^{i-1} & \ldots & (2^{s-i+1}-1) \cdot \mathbf{2}^{i-1} \end{pmatrix}$$

where $i \in \{1,\ldots,s\}$, $t_j' = t_j$ for $j \neq i$ and $t_i' = t_i + 1$.

Theorem

Let $t_1,\ldots,t_s$ be nonnegative integers with $t_1 \geq 1$. The $\mathbb{Z}_{2^s}$-linear code $\Phi(\mathcal{H}^{t_1,\ldots,t_s}) = H^{t_1,\ldots,t_s}$ of type $(n; t_1, t_2, \ldots, t_s)$ is a binary Hadamard code of length 2^t, with $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$.

Example of Construction ($s = 3$)

$$A^{1,0,0} = (1)$$

$$A^{1,0,1} = \begin{pmatrix} 1\ 1 \\ 0\ 4 \end{pmatrix}, \quad A^{1,1,0} = \begin{pmatrix} 11\ 11 \\ 02\ 46 \end{pmatrix}, \quad A^{2,0,0} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67 \end{pmatrix},$$

$$A^{1,1,1} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 02\ 46\ 02\ 46 \\ 00\ 00\ 44\ 44 \end{pmatrix}, \quad A^{2,0,1} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 44\ 44\ 44\ 44 \end{pmatrix},$$

$$A^{2,1,0} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 22\ 22\ 22\ 22\ 44\ 44\ 44\ 44\ 66\ 66\ 66\ 66 \end{pmatrix}.$$

Example of Construction ($s = 3$)

$$A^{1,0,0} = (1)$$

$$A^{1,0,1} = \begin{pmatrix} 1\ 1 \\ 0\ 4 \end{pmatrix}, \quad A^{1,1,0} = \begin{pmatrix} 11\ 11 \\ 02\ 46 \end{pmatrix}, \quad A^{2,0,0} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67 \end{pmatrix},$$

$$A^{1,1,1} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 02\ 46\ 02\ 46 \\ 00\ 00\ 44\ 44 \end{pmatrix}, \quad A^{2,0,1} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 44\ 44\ 44\ 44 \end{pmatrix},$$

$$A^{2,1,0} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 22\ 22\ 22\ 22\ 44\ 44\ 44\ 44\ 66\ 66\ 66\ 66 \end{pmatrix}.$$

Example of Construction ($s = 3$)

$$A^{1,0,0} = (1)$$

$$A^{1,0,1} = \begin{pmatrix} 1\ 1 \\ 0\ 4 \end{pmatrix}, \quad A^{1,1,0} = \begin{pmatrix} 11\ 11 \\ 02\ 46 \end{pmatrix}, \quad A^{2,0,0} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67 \end{pmatrix},$$

$$A^{1,1,1} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 02\ 46\ 02\ 46 \\ 00\ 00\ 44\ 44 \end{pmatrix}, \quad A^{2,0,1} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 44\ 44\ 44\ 44 \end{pmatrix},$$

$$A^{2,1,0} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 22\ 22\ 22\ 22\ 44\ 44\ 44\ 44\ 66\ 66\ 66\ 66 \end{pmatrix}.$$

Example of Construction ($s = 3$)

$$A^{1,0,0} = (1)$$

$$A^{1,0,1} = \begin{pmatrix} 1\ 1 \\ 0\ 4 \end{pmatrix}, \quad A^{1,1,0} = \begin{pmatrix} 11\ 11 \\ 02\ 46 \end{pmatrix}, \quad A^{2,0,0} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67 \end{pmatrix},$$

$$A^{1,1,1} = \begin{pmatrix} 11\ 11\ 11\ 11 \\ 02\ 46\ 02\ 46 \\ 00\ 00\ 44\ 44 \end{pmatrix}, \quad A^{2,0,1} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 44\ 44\ 44\ 44 \end{pmatrix},$$

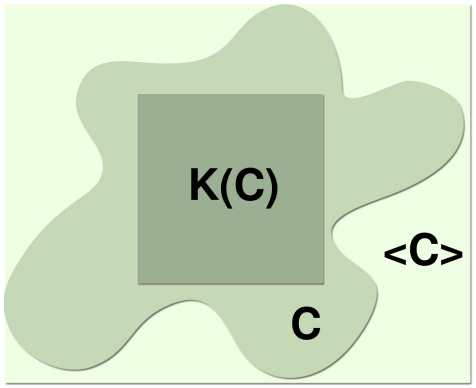
$$A^{2,1,0} = \begin{pmatrix} 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11\ 11 \\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67\ 01\ 23\ 45\ 67 \\ 00\ 00\ 00\ 00\ 22\ 22\ 22\ 22\ 44\ 44\ 44\ 44\ 66\ 66\ 66\ 66 \end{pmatrix}.$$

Rank & Kernel

To classify the constructed codes we will use two structural properties of binary codes which are the rank and the dimension of the kernel.

The rank of a binary code C is the dimension of the linear span, $\langle C \rangle$, of C.

The kernel of a binary code C is define as $K(C) = \{x \in \mathbb{Z}_2^n : x + C = C\}$. If the all-zero vector belongs to C, then $K(C)$ is a linear subcode of C.

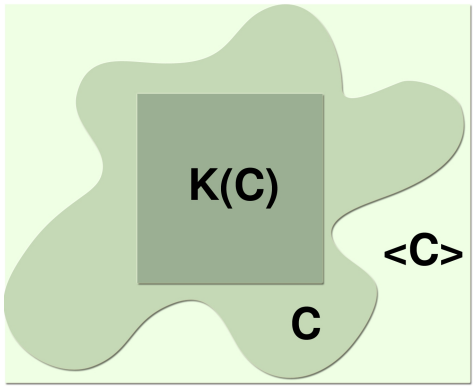


Rank & Kernel

To classify the constructed codes we will use two structural properties of binary codes which are the rank and the dimension of the kernel.

The rank of a binary code C is the dimension of the linear span, $\langle C \rangle$, of C.

The kernel of a binary code C is define as $K(C) = \{x \in \mathbb{Z}_2^n : x + C = C\}$. If the all-zero vector belongs to C, then $K(C)$ is a linear subcode of C.

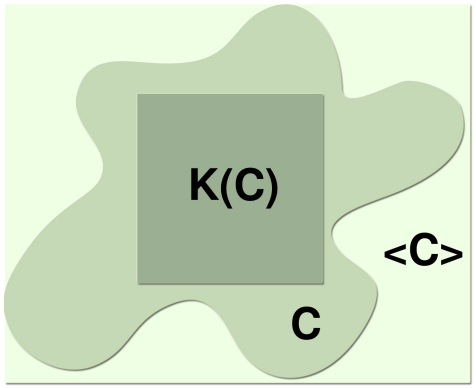


Rank & Kernel

To classify the constructed codes we will use two structural properties of binary codes which are the rank and the dimension of the kernel.

The rank of a binary code C is the dimension of the linear span, $\langle C \rangle$, of C.

The kernel of a binary code C is define as $K(C) = \{x \in \mathbb{Z}_2^n : x + C = C\}$. If the all-zero vector belongs to C, then $K(C)$ is a linear subcode of C.



The case $s = 2$

A construction of $\mathbb{Z}_4$-Linear Hadamard codes is given in:

Krotov, D. S., $\mathbb{Z}_4$-linear Hadamard and extended perfect codes, WCC2001, International Workshop on Coding and Cryptography, ser. Electron. Notes Discrete Math., **6** (2001), 107–112.

An a classification by using the rank and the dimension of the kernel is given in:

Phelps, K. T., 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. Inf. Theory, **52** (2006), no. 1, 316–319.

Kernel of $\mathbb{Z}_{2^s}$-Linear Hadamard codes

We define $\sigma \in \{1, \ldots, s\}$ as the integer such that $\mathrm{ord}(\mathbf{w}_2) = 2^{s+1-\sigma}$.

Theorem

Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{2^s}$-additive Hadamard code of type $(n; t_1, \ldots, t_s)$ such that $\Phi(\mathcal{H})$ is nonlinear. Let $\mathcal{H}_b$ be the subcode of $\mathcal{H}$ which contains all codewords of order two. Let $P = \{\mathbf{2}^p\}_{p=0}^{\sigma-2}$ if $\sigma \geq 2$, and $P = \emptyset$ if $\sigma = 1$. Then,

$$\left\langle \Phi(\mathcal{H}_b), \Phi(P), \Phi(\sum_{i=0}^{s-2} \mathbf{2}^i) \right\rangle = K(\Phi(\mathcal{H})),$$

and $ker(\Phi(\mathcal{H})) = \sigma + \sum_{i=1}^{s} t_i$.

Example of Kernel

Let $\mathcal{H}^{3,0}$ be a $\mathbb{Z}_4$-additive code. In this case $\sigma = 1$

$$A^{3,0} = \begin{pmatrix} 11 & 11 & 11 & 11 & 11 & 11 & 11 & 11 \\ 01 & 23 & 01 & 23 & 01 & 23 & 01 & 23 \\ 00 & 00 & 11 & 11 & 22 & 22 & 33 & 33 \end{pmatrix}.$$

$$\mathcal{H}_b^{3,0} = \begin{matrix} \{(2222222222222222), \\ (0202020202020202), \\ (0000222200002222)\} \end{matrix}$$

$$P = \{(1111111111111111)\}$$

Example of Kernel

Let $\mathcal{H}^{3,0}$ be a $\mathbb{Z}_4$-additive code. In this case $\sigma = 1$

$$A^{3,0} = \begin{pmatrix} 11 & 11 & 11 & 11 & 11 & 11 & 11 & 11 \\ 01 & 23 & 01 & 23 & 01 & 23 & 01 & 23 \\ 00 & 00 & 11 & 11 & 22 & 22 & 33 & 33 \end{pmatrix}.$$

$$\mathcal{H}_b^{3,0} = \begin{matrix} \{(2222222222222222), \\ (0202020202020202), \\ (0000222200002222)\} \end{matrix}$$

$$P = \{(1111111111111111)\}$$

Example of Kernel

Let $\mathcal{H}^{3,0}$ be a $\mathbb{Z}_4$-additive code. In this case $\sigma = 1$

$$A^{3,0} = \begin{pmatrix} 11 & 11 & 11 & 11 & 11 & 11 & 11 & 11 \\ 01 & 23 & 01 & 23 & 01 & 23 & 01 & 23 \\ 00 & 00 & 11 & 11 & 22 & 22 & 33 & 33 \end{pmatrix}.$$

$$\mathcal{H}_b^{3,0} = \begin{array}{c} \{(2222222222222222), \\ (0202020202020202), \\ (0000222200002222)\} \end{array}$$

$$P = \{(1111111111111111)\}$$

	$t=8$		$t=9$	
	type	(r,k)	type	(r,k)
$\mathbb{Z}_4$	$(2^7;1,7)$	**(9,9)**	$(2^8;1,8)$	**(10,10)**
	$(2^7;2,5)$	**(9,9)**	$(2^8;2,6)$	**(10,10)**
	$(2^7;3,3)$	(10,7)	$(2^8;3,4)$	(11,8)
	$(2^7;4,1)$	(12,6)	$(2^8;4,2)$	(13,7)
			$(2^8;5,0)$	(16,6)
$\mathbb{Z}_8$	$(2^6;1,0,6)$	**(9,9)**	$(2^7;1,0,7)$	**(10,10)**
	$(2^6;1,1,4)$	**(9,9)**	$(2^7;1,1,5)$	**(10,10)**
	$(2^6;1,2,2)$	(10,7)	$(2^7;1,2,3)$	(11,8)
	$(2^6;1,3,0)$	(12,6)	$(2^7;1,3,1)$	(13,7)
	$(2^6;2,0,3)$	(11,6)	$(2^7;2,0,4)$	(12,7)
	$(2^6;2,1,1)$	(13,5)	$(2^7;2,1,2)$	(14,6)
	$(2^6;3,0,0)$	(17,4)	$(2^7;2,2,0)$	(17,5)
			$(2^7;3,0,1)$	(18,5)

Type, rank and kernel of all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

	$t=8$		$t=9$	
	type	(r,k)	type	(r,k)
$\mathbb{Z}_4$	$(2^7;1,7)$	**(9,9)**	$(2^8;1,8)$	**(10,10)**
	$(2^7;2,5)$	**(9,9)**	$(2^8;2,6)$	**(10,10)**
	$(2^7;3,3)$	(10,7)	$(2^8;3,4)$	(11,8)
	$(2^7;4,1)$	(12,6)	$(2^8;4,2)$	(13,7)
			$(2^8;5,0)$	(16,6)
$\mathbb{Z}_8$	$(2^6;1,0,6)$	**(9,9)**	$(2^7;1,0,7)$	**(10,10)**
	$(2^6;1,1,4)$	**(9,9)**	$(2^7;1,1,5)$	**(10,10)**
	$(2^6;1,2,2)$	(10,7)	$(2^7;1,2,3)$	(11,8)
	$(2^6;1,3,0)$	(12,6)	$(2^7;1,3,1)$	(13,7)
	$(2^6;2,0,3)$	(11,6)	$(2^7;2,0,4)$	(12,7)
	$(2^6;2,1,1)$	(13,5)	$(2^7;2,1,2)$	(14,6)
	$(2^6;3,0,0)$	(17,4)	$(2^7;2,2,0)$	(17,5)
			$(2^7;3,0,1)$	(18,5)

Type, rank and kernel of all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

t	3	4	5	6	7	8	9	10	11
$\mathbb{Z}_4$	1	1	2	2	3	3	4	4	5
$\mathbb{Z}_8$	1	1	2	3	4	6	7	9	11
$\mathbb{Z}_{16}$	1	1	1	2	4	5	8	10	14

Number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

Thank you for your attention

Tänan teid tähelepanu eest