

# Minimum weight bases for some classes of linear codes

F. I. Solov'eva

Presented at conference  
WOMEN IN MATHEMATICS  
Sobolev Institute of Mathematics  
MAY 12, 2021  
Novosibirsk, Russia

F. I. Solov'eva with Sobolev Institute of Mathematics and Novosibirsk State University

## Main definitions

The Galois field of the characteristic  $p$  is denoted by  $GF(p^m)$ .

We denote a *primitive element* of the Galois field  $GF(p^m)$  by  $\alpha$ .

The vector space of all vectors over  $\mathbb{F} = GF(p)$  of length  $n = p^m$  we denote by  $\mathbb{F}^n$ .

## Main definitions

The Galois field of the characteristic  $p$  is denoted by  $GF(p^m)$ .

We denote a *primitive element* of the Galois field  $GF(p^m)$  by  $\alpha$ .

The vector space of all vectors over  $\mathbb{F} = GF(p)$  of length  $n = p^m$  we denote by  $\mathbb{F}^n$ .

## Main definitions

The Galois field of the characteristic  $p$  is denoted by  $GF(p^m)$ .

We denote a *primitive element* of the Galois field  $GF(p^m)$  by  $\alpha$ .

The vector space of all vectors over  $\mathbb{F} = GF(p)$  of length  $n = p^m$  we denote by  $\mathbb{F}^n$ .

# Main definitions

Any subset of  $\mathbb{F}^n$  is called a *code* of length  $n$ .

A code is called *linear* if it is linear subspace of  $\mathbb{F}^n$ .

A code is called *cyclic* if it is linear and cyclic shift of every its codeword belongs to the code.

# Main definitions

Any subset of  $\mathbb{F}^n$  is called a *code* of length  $n$ .

A code is called *linear* if it is linear subspace of  $\mathbb{F}^n$ .

A code is called *cyclic* if it is linear and cyclic shift of every its codeword belongs to the code.

# Main definitions

Any subset of  $\mathbb{F}^n$  is called a *code* of length  $n$ .

A code is called *linear* if it is linear subspace of  $\mathbb{F}^n$ .

A code is called *cyclic* if it is linear and cyclic shift of every its codeword belongs to the code.

# Main definitions

A basis of a linear code is called a *minimum weight basis* if it consists of codewords of minimum nonzero weight.



# Motivations

The study of an explicit minimum weight basis property for linear codes is motivated in coding theory by the classical problem of a short representation of linear (cyclic) codes and is related to the question of reconstructing codes from their minimum distance graphs or their designs.

It is important in cryptography.

# Motivations

The study of an explicit minimum weight basis property for linear codes is motivated in coding theory by the classical problem of a short representation of linear (cyclic) codes and is related to the question of reconstructing codes from their minimum distance graphs or their designs.

It is important in cryptography.

# Motivations

The study of explicit minimum weight basis property for linear codes is also important in testing theory for fast isomorphism testing of strongly regular graphs.

[T. Kaufman and M. Sudan, “Algebraic property testing: the role of invariance,” Proceedings of 40th ACM Symposium on Theory of Computing STOC, pp. 403–412, 2008.]

[ T. Kaufman and S. Litsyn, “Almost orthogonal linear codes are locally testable,” Proceedings of 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 317–326, 2005.]

# Survey

Glagolev, 1971, proved that each binary linear code  $C$  can be transformed into a binary linear code  $D$  with the same parameters and a minimum weight basis.

In 1992 Simonis proved an analogous result over  $GF(q)$  for any  $q$ .

Note that here  $D$  is not necessary equivalent to  $C$ .

[See Glagolev lemma in the paper of Ya. M. Kurlyandchik, "On logarithmical asymptotic of maximal cyclic spread  $r > 2$  length," *Discretnyj Analiz*, vol. 19, pp. 48–55, 1971 (in Russian)]

[J. Simonis, "On generator matrices of codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 2, pp. 516–516, 1992.]

# Survey

Glagolev, 1971, proved that each binary linear code  $C$  can be transformed into a binary linear code  $D$  with the same parameters and a minimum weight basis.

In 1992 Simonis proved an analogous result over  $GF(q)$  for any  $q$ .

Note that here  $D$  is not necessary equivalent to  $C$ .

[See Glagolev lemma in the paper of Ya. M. Kurlyandchik, “On logarithmical asymptotic of maximal cyclic spread  $r > 2$  length,” *Discretnyj Analiz*, vol. 19, pp. 48–55, 1971 (in Russian)]

[J. Simonis, “On generator matrices of codes,” *IEEE Trans. Inform. Theory*, vol. 38, no. 2, pp. 516–516, 1992.]

# Survey

The Glagolev's result for Hamming codes immediately implies the existence of minimum weight codewords bases.

Reed-Solomon, the binary Reed-Muller codes, the linear Greisner codes have minimum weight bases (see MacWilliams and Sloane book).

[F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland Publishing Company, 1977.]

# Survey

The Glagolev's result for Hamming codes immediately implies the existence of minimum weight codewords bases.

Reed-Solomon, the binary Reed-Muller codes, the linear Greisner codes have minimum weight bases (see MacWilliams and Sloane book).

[F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland Publishing Company, 1977.]

# Survey

For the class of binary narrow-sense BCH codes of length  $2^m - 1$  it is known that codes with designed distance  $2^{m-2} + 1$  do not possess a minimum weight basis, while codes with designed distance 7 of small length do, see the work of Augot, Charpin and Sendrier.

[D. Augot, P. Charpin and N. Sendrier, “Studying the locator polynomials of minimum weight codewords of BCH codes,” IEEE Trans. Inform. Theory, vol. 30, no. 3, pp. 960–973, 1992.]



# Survey

In 2011 Grigorescu and Kaufman presented an asymptotical result on existence of a single orbit affine generator of minimum weight for extended primitive double-error correcting BCH  $\overline{C}_{1,3}$  codes of length  $n = 2^m$  for  $m \geq 20$ .

[E. Grigorescu and T. Kaufman, “Explicit Low-Weight Bases for BCH Codes,” IEEE Trans. Inform. Theory, vol. 58, no. 2, pp. 78–81, 2011.]

An element of  $GF(p^m)$  is called *a zero* of a cyclic code if it is a zero of its generator polynomial.

The code  $C_{1,\dots,\delta-1}$  with zeroes  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$  is called the *narrow-sense BCH code with the designed distance  $\delta$*  and its minimum distance is at least  $\delta$  by BCH bound.

An element of  $GF(p^m)$  is called *a zero* of a cyclic code if it is a zero of its generator polynomial.

The code  $C_{1,\dots,\delta-1}$  with zeroes  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$  is called the *narrow-sense BCH code with the designed distance  $\delta$*  and its minimum distance is at least  $\delta$  by BCH bound.

For a vector  $c = (c_0, \dots, c_{p^m-2})$  of length  $p^m - 1$  we denote its extension by  $\bar{c}$ , i.e.

$$\bar{c} = (c_0, \dots, c_{p^m-2}, -\sum_{i=0}^{p^m-2} c_i).$$

The *extended code*  $\bar{C}$  of  $C$  is  $\{\bar{c} : c \in C\}$ . The last position of the extended code is indexed by the zero of  $GF(p^m)$ , thus the code positions are indexed by the elements of  $GF(p^m)$ .

For a vector  $c = (c_0, \dots, c_{p^m-2})$  of length  $p^m - 1$  we denote its extension by  $\bar{c}$ , i.e.

$$\bar{c} = (c_0, \dots, c_{p^m-2}, -\sum_{i=0}^{p^m-2} c_i).$$

The *extended code*  $\bar{C}$  of  $C$  is  $\{\bar{c} : c \in C\}$ . The last position of the extended code is indexed by the zero of  $GF(p^m)$ , thus the code positions are indexed by the elements of  $GF(p^m)$ .

# Affine invariance

*The affine group* of  $GF(p^m)$  is the group of the mappings represented by pairs  $(\gamma, \sigma)$ ,  $\gamma, \sigma \in GF(p^m)$ ,  $\gamma \neq 0$  that send  $\beta$  to  $\beta\gamma + \sigma$ ,  $\beta \in GF(p^m)$ .

The affine group of  $GF(p^m)$  naturally acts on the coordinate positions of  $F^{p^m}$  and a code  $C$  of length  $p^m$  is called *affine-invariant* if the affine group preserves the set of its codewords.

The extended BCH codes are affine-invariant.

## Affine invariance

*The affine group* of  $GF(p^m)$  is the group of the mappings represented by pairs  $(\gamma, \sigma)$ ,  $\gamma, \sigma \in GF(p^m)$ ,  $\gamma \neq 0$  that send  $\beta$  to  $\beta\gamma + \sigma$ ,  $\beta \in GF(p^m)$ .

The affine group of  $GF(p^m)$  naturally acts on the coordinate positions of  $F^{p^m}$  and a code  $C$  of length  $p^m$  is called *affine-invariant* if the affine group preserves the set of its codewords.

The extended BCH codes are affine-invariant.

## Affine invariance

*The affine group* of  $GF(p^m)$  is the group of the mappings represented by pairs  $(\gamma, \sigma)$ ,  $\gamma, \sigma \in GF(p^m)$ ,  $\gamma \neq 0$  that send  $\beta$  to  $\beta\gamma + \sigma$ ,  $\beta \in GF(p^m)$ .

The affine group of  $GF(p^m)$  naturally acts on the coordinate positions of  $F^{p^m}$  and a code  $C$  of length  $p^m$  is called *affine-invariant* if the affine group preserves the set of its codewords.

The extended BCH codes are affine-invariant.



# Single orbit affine generator

A codeword of an affine-invariant code  $C$  whose affine transformations span  $C$  is called a *single orbit affine generator*.

## Main results

### Theorem 1. Mogilnykh and S.

The minimum weight bases of the following classes of binary codes could be chosen from affine orbits of certain explicitly represented minimum weight codewords:

extended primitive double-error correcting BCH code of length  $n = 2^m$  for  $4 \leq m \leq 19$  (for  $m \geq 20$  it was proven by Grigorescu et al.),

extended cyclic code  $\overline{C_{1,5}}$  of length  $n = 2^m$ ,  $m \geq 5$  and

extended cyclic codes  $\overline{C_{1,2^i+1}}$  of lengths  $n = 2^m$ ,  $(i, m) = 1$  for  $3 \leq i \leq \frac{m-5}{4} - o(m)$ .

[I. Yu. Mogilnykh and F. I. Solov'eva, "On explicit minimum weight bases for extended cyclic codes related to Gold functions," Des. Codes Cryptogr., vol. 86, no. 11, pp. 2619–2627, 2018.]

## Main results

### Theorem 1. Mogilnykh and S.

The minimum weight bases of the following classes of binary codes could be chosen from affine orbits of certain explicitly represented minimum weight codewords:

extended primitive double-error correcting BCH code of length  $n = 2^m$  for  $4 \leq m \leq 19$  (for  $m \geq 20$  it was proven by Grigorescu et al.),

extended cyclic code  $\overline{C_{1,5}}$  of length  $n = 2^m$ ,  $m \geq 5$  and

extended cyclic codes  $\overline{C_{1,2^i+1}}$  of lengths  $n = 2^m$ ,  $(i, m) = 1$  for  $3 \leq i \leq \frac{m-5}{4} - o(m)$ .

[I. Yu. Mogilnykh and F. I. Solov'eva, "On explicit minimum weight bases for extended cyclic codes related to Gold functions," Des. Codes Cryptogr., vol. 86, no. 11, pp. 2619–2627, 2018.]

## Main results


### Theorem 1. Mogilnykh and S.

The minimum weight bases of the following classes of binary codes could be chosen from affine orbits of certain explicitly represented minimum weight codewords:

extended primitive double-error correcting BCH code of length  $n = 2^m$  for  $4 \leq m \leq 19$  (for  $m \geq 20$  it was proven by Grigorescu et al.),

extended cyclic code  $\overline{C_{1,5}}$  of length  $n = 2^m$ ,  $m \geq 5$  and

extended cyclic codes  $\overline{C_{1,2^i+1}}$  of lengths  $n = 2^m$ ,  $(i, m) = 1$  for  $3 \leq i \leq \frac{m-5}{4} - o(m)$ .

[I. Yu. Mogilnykh and F. I. Solov'eva, "On explicit minimum weight bases for extended cyclic codes related to Gold functions," Des. Codes Cryptogr., vol. 86, no. 11, pp. 2619–2627, 2018.] 

## Main results


### Theorem 1. Mogilnykh and S.

The minimum weight bases of the following classes of binary codes could be chosen from affine orbits of certain explicitly represented minimum weight codewords:

extended primitive double-error correcting BCH code of length  $n = 2^m$  for  $4 \leq m \leq 19$  (for  $m \geq 20$  it was proven by Grigorescu et al.),

extended cyclic code  $\overline{C_{1,5}}$  of length  $n = 2^m$ ,  $m \geq 5$  and

extended cyclic codes  $\overline{C_{1,2^i+1}}$  of lengths  $n = 2^m$ ,  $(i, m) = 1$  for  $3 \leq i \leq \frac{m-5}{4} - o(m)$ .

[I. Yu. Mogilnykh and F. I. Solov'eva, "On explicit minimum weight bases for extended cyclic codes related to Gold functions," Des. Codes Cryptogr., vol. 86, no. 11, pp. 2619–2627, 2018.] 

# Main results

## Theorem 2. Mogilnykh and S.

For any prime  $p$ ,  $p \neq 2, 3$  the codes  $C_{1,2}$  and  $\overline{C_{1,2}}$  over  $GF(p)$  are not spanned by their codewords of the minimum nonzero weight.

# Lemma

Lemma. Mogilnykh and S.

Let  $\alpha$  be a primitive element of  $GF(p^m)$ ,  $p, m \geq 3$ ,

$$c(x) = 2 + x^i + x^j - 2x^k,$$

where  $i, j, k$  are such that

$$\alpha^i = \alpha + 2^{-1}\alpha^2, \alpha^j = -\alpha + 2^{-1}\alpha^2, \alpha^k = 1 + 2^{-1}\alpha^2.$$

Then  $c(x)$  belongs to  $C_{1,2}$ .

## Main results

### Theorem 3. Mogilnykh and S.

For any prime  $p \neq 2$  and for any  $m \geq 3$  there is a primitive element  $\alpha$  of  $GF(p^m)$  such that the extended codeword  $\bar{c}$ , where

$$c(x) = 2 + x^i + x^j - 2x^k,$$

and  $i, j, k$  fulfill Lemma is a single orbit affine generator of the code  $\overline{C}_{1,2}$  of length  $n = p^m$ .



## More definitions

Let  $\mathbb{Z}_4$  be the ring of integers modulo four and  $\mathbb{Z}_4^N$  be the set of all quaternary words of length  $N$ .

The Lee weight of elements in  $\mathbb{Z}_4$  is

$w_L(0) = 0, w_L(1) = w_L(3) = 1$  and  $w_L(2) = 2$ .

The Lee weight  $w_L(x)$  of a word in  $\mathbb{Z}_4^N$  is the addition of the Lee weights of all its coordinates.

The Lee distance  $d_L(x, y)$  between two words  $x, y \in \mathbb{Z}_4^N$  is defined as  $d_L(x, y) = w_L(x - y)$ .

A nonempty subset  $\mathcal{C}$  of  $\mathbb{Z}_4^N$  is a quaternary code and a subgroup of  $\mathbb{Z}_4^N$  is called a *quaternary linear code*.

## More definitions

Let  $\mathbb{Z}_4$  be the ring of integers modulo four and  $\mathbb{Z}_4^N$  be the set of all quaternary words of length  $N$ .

The Lee weight of elements in  $\mathbb{Z}_4$  is

$w_L(0) = 0, w_L(1) = w_L(3) = 1$  and  $w_L(2) = 2$ .

The Lee weight  $w_L(x)$  of a word in  $\mathbb{Z}_4^N$  is the addition of the Lee weights of all its coordinates.

The Lee distance  $d_L(x, y)$  between two words  $x, y \in \mathbb{Z}_4^N$  is defined as  $d_L(x, y) = w_L(x - y)$ .

A nonempty subset  $\mathcal{C}$  of  $\mathbb{Z}_4^N$  is a quaternary code and a subgroup of  $\mathbb{Z}_4^N$  is called a *quaternary linear code*.

## More definitions

Let  $\mathbb{Z}_4$  be the ring of integers modulo four and  $\mathbb{Z}_4^N$  be the set of all quaternary words of length  $N$ .

The Lee weight of elements in  $\mathbb{Z}_4$  is

$w_L(0) = 0, w_L(1) = w_L(3) = 1$  and  $w_L(2) = 2$ .

The Lee weight  $w_L(x)$  of a word in  $\mathbb{Z}_4^N$  is the addition of the Lee weights of all its coordinates.

The Lee distance  $d_L(x, y)$  between two words  $x, y \in \mathbb{Z}_4^N$  is defined as  $d_L(x, y) = w_L(x - y)$ .

A nonempty subset  $\mathcal{C}$  of  $\mathbb{Z}_4^N$  is a quaternary code and a subgroup of  $\mathbb{Z}_4^N$  is called a *quaternary linear code*.

## More definitions

Let  $\mathbb{Z}_4$  be the ring of integers modulo four and  $\mathbb{Z}_4^N$  be the set of all quaternary words of length  $N$ .

The Lee weight of elements in  $\mathbb{Z}_4$  is

$w_L(0) = 0, w_L(1) = w_L(3) = 1$  and  $w_L(2) = 2$ .

The Lee weight  $w_L(x)$  of a word in  $\mathbb{Z}_4^N$  is the addition of the Lee weights of all its coordinates.

The Lee distance  $d_L(x, y)$  between two words  $x, y \in \mathbb{Z}_4^N$  is defined as  $d_L(x, y) = w_L(x - y)$ .

A nonempty subset  $\mathcal{C}$  of  $\mathbb{Z}_4^N$  is a quaternary code and a subgroup of  $\mathbb{Z}_4^N$  is called a *quaternary linear code*.

## More definitions

Let  $\mathbb{Z}_4$  be the ring of integers modulo four and  $\mathbb{Z}_4^N$  be the set of all quaternary words of length  $N$ .

The Lee weight of elements in  $\mathbb{Z}_4$  is

$w_L(0) = 0, w_L(1) = w_L(3) = 1$  and  $w_L(2) = 2$ .

The Lee weight  $w_L(x)$  of a word in  $\mathbb{Z}_4^N$  is the addition of the Lee weights of all its coordinates.

The Lee distance  $d_L(x, y)$  between two words  $x, y \in \mathbb{Z}_4^N$  is defined as  $d_L(x, y) = w_L(x - y)$ .

A nonempty subset  $\mathcal{C}$  of  $\mathbb{Z}_4^N$  is a quaternary code and a subgroup of  $\mathbb{Z}_4^N$  is called a *quaternary linear code*.

## More definitions

Let  $\phi : \mathbb{Z}_4^N \longrightarrow \mathbb{Z}_2^{2N}$  be given by  
 $\phi(v_1, \dots, v_N) = (\varphi(v_1), \dots, \varphi(v_N))$ , where  $\varphi$  is the *usual Gray map*:  
 $\varphi(0) = (0, 0), \varphi(1) = (0, 1), \varphi(2) = (1, 1), \varphi(3) = (1, 0)$ .

The image  $\phi(\mathcal{C})$  of the code  $\mathcal{C}$  under the Gray map  $\phi$  is called a  *$\mathbb{Z}_4$ -linear code*.

## More definitions

Let  $\phi : \mathbb{Z}_4^N \longrightarrow \mathbb{Z}_2^{2N}$  be given by  
 $\phi(v_1, \dots, v_N) = (\varphi(v_1), \dots, \varphi(v_N))$ , where  $\varphi$  is the *usual Gray map*:  
 $\varphi(0) = (0, 0), \varphi(1) = (0, 1), \varphi(2) = (1, 1), \varphi(3) = (1, 0)$ .

The image  $\phi(\mathcal{C})$  of the code  $\mathcal{C}$  under the Gray map  $\phi$  is called a  *$\mathbb{Z}_4$ -linear code*.

## More definitions

A quaternary linear code being a subgroup of  $\mathbb{Z}_4^N$  is isomorphic to an *abelian structure* of type  $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ .

Therefore  $|\mathcal{C}| = 2^\gamma 4^\delta$ .

Such code  $\mathcal{C}$  is called *quaternary linear of type*  $(N; \gamma, \delta)$ .  
Its binary image  $C = \phi(\mathcal{C})$  under the Gray map is called a  *$\mathbb{Z}_4$ -linear code of type*  $(N; \gamma, \delta)$ .

*Parameters* of a code  $\mathcal{C}$  in  $\mathbb{Z}_4^N$ : length  $N$ , size  $|\mathcal{C}|$ , code distance with respect to the Lee metric.



## More definitions

A quaternary linear code being a subgroup of  $\mathbb{Z}_4^N$  is isomorphic to an *abelian structure* of type  $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ .

Therefore  $|\mathcal{C}| = 2^\gamma 4^\delta$ .

Such code  $\mathcal{C}$  is called *quaternary linear of type*  $(N; \gamma, \delta)$ .  
Its binary image  $C = \phi(\mathcal{C})$  under the Gray map is called a  *$\mathbb{Z}_4$ -linear code of type*  $(N; \gamma, \delta)$ .

*Parameters* of a code  $\mathcal{C}$  in  $\mathbb{Z}_4^N$ : length  $N$ , size  $|\mathcal{C}|$ , code distance with respect to the Lee metric.

## More definitions

A quaternary linear code being a subgroup of  $\mathbb{Z}_4^N$  is isomorphic to an *abelian structure* of type  $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ .

Therefore  $|\mathcal{C}| = 2^\gamma 4^\delta$ .

Such code  $\mathcal{C}$  is called *quaternary linear of type  $(N; \gamma, \delta)$* .

Its binary image  $C = \phi(\mathcal{C})$  under the Gray map is called a  *$\mathbb{Z}_4$ -linear code of type  $(N; \gamma, \delta)$* .

*Parameters* of a code  $C$  in  $\mathbb{Z}_4^N$ : length  $N$ , size  $|C|$ , code distance with respect to the Lee metric.

## More definitions

A quaternary linear code being a subgroup of  $\mathbb{Z}_4^N$  is isomorphic to an *abelian structure* of type  $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ .

Therefore  $|\mathcal{C}| = 2^\gamma 4^\delta$ .

Such code  $\mathcal{C}$  is called *quaternary linear of type  $(N; \gamma, \delta)$* .  
Its binary image  $C = \phi(\mathcal{C})$  under the Gray map is called a  *$\mathbb{Z}_4$ -linear code of type  $(N; \gamma, \delta)$* .

*Parameters* of a code  $C$  in  $\mathbb{Z}_4^N$ : length  $N$ , size  $|C|$ , code distance with respect to the Lee metric.

## More definitions

A quaternary linear code being a subgroup of  $\mathbb{Z}_4^N$  is isomorphic to an *abelian structure* of type  $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ .

Therefore  $|\mathcal{C}| = 2^\gamma 4^\delta$ .

Such code  $\mathcal{C}$  is called *quaternary linear of type  $(N; \gamma, \delta)$* .  
Its binary image  $C = \phi(\mathcal{C})$  under the Gray map is called a  *$\mathbb{Z}_4$ -linear code of type  $(N; \gamma, \delta)$* .

*Parameters* of a code  $C$  in  $\mathbb{Z}_4^N$ : length  $N$ , size  $|\mathcal{C}|$ , code distance with respect to the Lee metric.

The classical *binary linear Reed – Muller code of order  $r$* ,  $0 \leq r \leq m$ , for any  $m \geq 1$  is defined as the set of all vectors of length  $2^m$  corresponding to the boolean functions of  $m$  variables of degree not more than  $r$ .

Pujol, Rifa and S. introduced two constructions of  $\lfloor \frac{m+1}{2} \rfloor$  nonequivalent families of quaternary linear Reed–Muller codes for each value of  $m$  and  $0 \leq r \leq m$ .

For fixed  $m$  and  $r$  the families were distinguished by their abelian structures.

This fact was emphasized by using subindexes  $s$  from the set  $\{0, \dots, \lfloor \frac{m-1}{2} \rfloor\}$ , so for fixed  $m$ ,  $r$  and  $s$  we have the code  $\mathcal{RM}_s(r, m)$ .

[See J. Pujol, J. Rifà and F. I. Solov'eva, Construction of Z4-Linear Reed–Muller Codes, *IEEE Transactions of Information Theory*, **55**(1) (2009), 99–104.]

It was proved that under the Gray map the corresponding  $\mathbb{Z}_4$ -linear codes have similar properties (length, dimension, minimum distance, inclusion and duality relationship) as the classical binary linear Reed–Muller ( $RM$ ) codes but these codes are not linear.

# Main results

## Theorem 4.

For any  $r$  and  $m \geq 2$ ,  $0 \leq r < m$  and for any  $s$ ,  $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$  the quaternary linear code  $\mathcal{RM}_s(r, m)$  has a minimum weight basis.

## Corollary.

The minimum weight graphs of the quaternary Reed-Muller codes are connected.



# Main results

## Theorem 4.

For any  $r$  and  $m \geq 2$ ,  $0 \leq r < m$  and for any  $s$ ,  $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$  the quaternary linear code  $\mathcal{RM}_s(r, m)$  has a minimum weight basis.

## Corollary.

The minimum weight graphs of the quaternary Reed-Muller codes are connected.

*THANK YOU FOR YOUR ATTENTION*