Reed – Muller like codes and their intersections

F. I. Solov'eva

Sobolev Institute of Mathematics, RUSSIA

Presented at International Conference
Combinatorial Designs and Codes
CDC 2021 (online)
Satellite event of the 8th European Congress of Mathematics
11 - 16 July, 2021, CROATIA, Rijeka

Main definitions

The Galois field of the characteristic 2 is denoted by $GF(2^m)$.
We denote a *primitive element* of the Galois field $GF(2^m)$ by α.
The vector space of all vectors over $\mathbb{F} = GF(2)$ of length $n = 2^m$ we denote by $\mathbb{F}^n$.

Main definitions

The Galois field of the characteristic 2 is denoted by $GF(2^m)$.
We denote a *primitive element* of the Galois field $GF(2^m)$ by α.
The vector space of all vectors over $\mathbb{F} = GF(2)$ of length $n = 2^m$ we denote by $\mathbb{F}^n$.

Main definitions

The Galois field of the characteristic 2 is denoted by $GF(2^m)$.
We denote a *primitive element* of the Galois field $GF(2^m)$ by α.
The vector space of all vectors over $\mathbb{F} = GF(2)$ of length $n = 2^m$ we denote by $\mathbb{F}^n$.

Main definitions

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

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

Main definitions

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

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

The classical *binary 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.

The Reed – Muller code is linear
has the following parameters:
the length n of the code is 2^m,
the size 2^k, $k = \sum_{i=0}^{r} \binom{m}{i}$
the *code distance* (the minimum value of the Hamming distance between any two different codewords from the code) is 2^{m-r}.

The code is called *self-complementary* if for any codeword x the code contains the vector $x + \mathbf{1}^n$, where $\mathbf{1}^n$ is the all-ones vector of length n.

The Reed – Muller code is self-complementary.

A binary self-complementary code with the parameters of the classical Reed – Muller code is called a *Reed – Muller like code*.

The code is called *self-complementary* if for any codeword x the code contains the vector $x + \mathbf{1}^n$, where $\mathbf{1}^n$ is the all-ones vector of length n.

The Reed – Muller code is self-complementary.

A binary self-complementary code with the parameters of the classical Reed – Muller code is called a *Reed – Muller like code*.

The code is called *self-complementary* if for any codeword x the code contains the vector $x + \mathbf{1}^n$, where $\mathbf{1}^n$ is the all-ones vector of length n.

The Reed – Muller code is self-complementary.

A binary self-complementary code with the parameters of the classical Reed – Muller code is called a *Reed – Muller like code*.

Reed – Muller like code is not necessarily linear.

The class of the codes contains rich families of Reed – Muller like codes obtained in

[A. K. Pulatov, Lower bound on a complexity of the circuit implementation for one class of codes. Diskretn. Analiz, Novosibirsk. V. 25 (1974) 56–61 (in Russian).]

[C. L. Liu, B. G. Ong, G. R. Ruth, A construction scheme for linear and non-linear codes. Discrete Math. V. 4 (1973) 171–184.]

[F. I. Solov'eva, On binary non-group codes, Metody Diskretn. Anal. V. (1981) 65–76 (in Russian).]

Reed – Muller like code is not necessarily linear.

The class of the codes contains rich families of Reed – Muller like codes obtained in

[A. K. Pulatov, Lower bound on a complexity of the circuit implementation for one class of codes. Diskretn. Analiz, Novosibirsk. V. 25 (1974) 56–61 (in Russian).]

[C. L. Liu, B. G. Ong, G. R. Ruth, A construction scheme for linear and non-linear codes. Discrete Math. V. 4 (1973) 171–184.]

[F. I. Solov'eva, On binary non-group codes, Metody Diskretn. Anal. V. (1981) 65–76 (in Russian).]

Reed – Muller like code is not necessarily linear.

The class of the codes contains rich families of Reed – Muller like codes obtained in

[A. K. Pulatov, Lower bound on a complexity of the circuit implementation for one class of codes. Diskretn. Analiz, Novosibirsk. V. 25 (1974) 56–61 (in Russian).]

[C. L. Liu, B. G. Ong, G. R. Ruth, A construction scheme for linear and non-linear codes. Discrete Math. V. 4 (1973) 171–184.]

[F. I. Solov'eva, On binary non-group codes, Metody Diskretn. Anal. V. (1981) 65–76 (in Russian).]

The class of the Reed – Muller like codes contains families of not only perfect and Hadamard codes but also known Z_4-linear Reed – Muller codes:

[F. I. Solov'eva, On Z4-linear codes with parameters of Reed–Muller codes, *Problems of Information Transmission*, **43**(1) (2007), 26–32.]

[J. Pujol, J. Rifà and F. I. Solov'eva, "Construction of Z4-Linear Reed–Muller Codes", IEEE Transactions of Information Theory, vol. 55, no. 1, pp. 99–104, 2009.]

The class of the Reed – Muller like codes contains families of not only perfect and Hadamard codes but also known Z_4-linear Reed – Muller codes:

[F. I. Solov'eva, On Z4-linear codes with parameters of Reed–Muller codes, *Problems of Information Transmission*, **43**(1) (2007), 26–32.]

[J. Pujol, J. Rifà and F. I. Solov'eva, "Construction of Z4-Linear Reed–Muller Codes", IEEE Transactions of Information Theory, vol. 55, no. 1, pp. 99–104, 2009.]

The class of the Reed – Muller like codes contains families of linear codes spanned by the blocks of some polarity designs.

[M. Harada, E. Novak and V. D. Tonchev, "The weight distribution of the self-dual [128; 64] polarity design code", Advances in Mathematics of Communications, vol. 10, no. 3, 2016, 643-648.]

[D. Clark, V. D. Tonchev, "A new class of majority-logic decodable codes derived from polarity designs", Advances in Mathematics of Communications, vol. 7, no. 2, pp. 175–186, 2013.]

The class of the Reed – Muller like codes contains families of linear codes spanned by the blocks of some polarity designs.

[M. Harada, E. Novak and V. D. Tonchev, "The weight distribution of the self-dual [128; 64] polarity design code", Advances in Mathematics of Communications, vol. 10, no. 3, 2016, 643-648.]

[D. Clark, V. D. Tonchev, "A new class of majority-logic decodable codes derived from polarity designs", Advances in Mathematics of Communications, vol. 7, no. 2, pp. 175–186, 2013.]

In 1994 Etzion and Vardy proposed the following problem: what is the size of the intersection of any two binary perfect codes?

[T. Etzion, A. Vardy, "Perfect binary codes: Constructions, properties and enumeration", IEEE Trans. Inform. Theory, vol. 40, no. 3, pp. 754–763, 1994.]

In 1994 Etzion and Vardy proposed the following problem: what is the size of the intersection of any two binary perfect codes?

[T. Etzion, A. Vardy, "Perfect binary codes: Constructions, properties and enumeration", IEEE Trans. Inform. Theory, vol. 40, no. 3, pp. 754–763, 1994.]

Survey

A deep contribution for an investigation of the intersection number problem was done for perfect codes and Hadamard codes, see the survey

[F. I. Solov'eva, "Survey on perfect codes", Mathematical Problems of Cybernetics, vol. 18, pp. 5–34, 2013 (in Russian).]

Survey

A deep contribution for an investigation of the intersection number problem was done for perfect codes and Hadamard codes, see the survey

[F. I. Solov'eva, "Survey on perfect codes", Mathematical Problems of Cybernetics, vol. 18, pp. 5–34, 2013 (in Russian).]

Survey

In 1997 the intersection problem for all q-ary linear codes, $q \geq 2$ was solved by Bar-Yahalom and Etzion including the intersection problem for binary Reed – Muller codes.

For some permutation π of order 2^m the Reed – Muller code $RM_{r,m}$ of order r satisfies $|RM_{r,m} \cap \pi(RM_{r,m})| \geq 2$, where 2 (the minimum one!) is attainable only for $r \leq [(m-1)/2]$.

[S. E. Bar-Yahalom, T. Etzion, "Intersection of isomorphic linear codes", Journal of Combin. Theory, Series A, vol. 80, pp. 247–256, 1997.]

Survey

In 1997 the intersection problem for all q-ary linear codes, $q \geq 2$ was solved by Bar-Yahalom and Etzion including the intersection problem for binary Reed – Muller codes.

For some permutation π of order 2^m the Reed – Muller code $RM_{r,m}$ of order r satisfies $|RM_{r,m} \cap \pi(RM_{r,m})| \geq 2$, where 2 (the minimum one!) is attainable only for $r \leq [(m-1)/2]$.

[S. E. Bar-Yahalom, T. Etzion, "Intersection of isomorphic linear codes", Journal of Combin. Theory, Series A, vol. 80, pp. 247–256, 1997.]

Survey

In 1997 the intersection problem for all q-ary linear codes, $q \geq 2$ was solved by Bar-Yahalom and Etzion including the intersection problem for binary Reed – Muller codes.

For some permutation π of order 2^m the Reed – Muller code $RM_{r,m}$ of order r satisfies $|RM_{r,m} \cap \pi(RM_{r,m})| \geq 2$, where 2 (the minimum one!) is attainable only for $r \leq [(m-1)/2]$.

[S. E. Bar-Yahalom, T. Etzion, "Intersection of isomorphic linear codes", Journal of Combin. Theory, Series A, vol. 80, pp. 247–256, 1997.]

Survey

In 1998 it was shown by Etzion and Vardy that for each $m \geq 3$ there exist two binary perfect nonlinear codes of length $2^m - 1$ with the intersection of size 2.

[T. Etzion, A. Vardy, "On perfect codes and tilings: problems and solutions", SIAM J. Disc. Math., vol. 11, no. 3, pp. 205–223, 1998.]

Survey

In 1998 it was shown by Etzion and Vardy that for each $m \geq 3$ there exist two binary perfect nonlinear codes of length $2^m - 1$ with the intersection of size 2.

[T. Etzion, A. Vardy, "On perfect codes and tilings: problems and solutions", SIAM J. Disc. Math., vol. 11, no. 3, pp. 205–223, 1998.]

Survey

It was proved that for any two integers k_1 and k_2 satisfying $1 \leq k_s \leq 2^{(n+1)/2-\log(n+1)}$, $s = 1, 2$, there exist perfect codes C_1 and C_2, both of length $n = 2^m - 1$, $m \geq 4$, with $|C_1 \cap C_2| = 2k_1 k_2$.

It was established that for any even number k such that $0 \leq k \leq 2^{n+1-2\log(n+1)}$ there exist binary perfect codes C_1 and C_2 of length $n = 2^m - 1$, $m \geq 4$ satisfying $|C_1 \cap C_2| = k$.

[S. V. Avgustinovich, O. Heden, F. I. Solov'eva, "On intersections of perfect binary codes", Bayreuther Mathematische Schriften, vol. 71, pp. 8–13, 2005.]

[S. V. Avgustinovich, O. Heden, F. I. Solov'eva, "On intersection problem for perfect binary codes", Des., Codes and Cryptogr., vol. 39, pp. 317–322, 2006.]

Survey

It was proved that for any two integers k_1 and k_2 satisfying $1 \le k_s \le 2^{(n+1)/2-\log(n+1)}$, $s = 1, 2$, there exist perfect codes C_1 and C_2, both of length $n = 2^m - 1$, $m \ge 4$, with $|C_1 \cap C_2| = 2k_1k_2$.

It was established that for any even number k such that $0 \le k \le 2^{n+1-2\log(n+1)}$ there exist binary perfect codes C_1 and C_2 of length $n = 2^m - 1$, $m \ge 4$ satisfying $|C_1 \cap C_2| = k$.

[S. V. Avgustinovich, O. Heden, F. I. Solov'eva, "On intersections of perfect binary codes", Bayreuther Mathematische Schriften, vol. 71, pp. 8–13, 2005.]

[S. V. Avgustinovich, O. Heden, F. I. Solov'eva, "On intersection problem for perfect binary codes", Des., Codes and Cryptogr., vol. 39, pp. 317–322, 2006.]

Survey

It was proved that for any two integers k_1 and k_2 satisfying $1 \leq k_s \leq 2^{(n+1)/2-\log(n+1)}$, $s = 1, 2$, there exist perfect codes C_1 and C_2, both of length $n = 2^m - 1$, $m \geq 4$, with $|C_1 \cap C_2| = 2k_1k_2$.

It was established that for any even number k such that $0 \leq k \leq 2^{n+1-2\log(n+1)}$ there exist binary perfect codes C_1 and C_2 of length $n = 2^m - 1$, $m \geq 4$ satisfying $|C_1 \cap C_2| = k$.

[S. V. Avgustinovich, O. Heden, F. I. Solov'eva, "On intersections of perfect binary codes", Bayreuther Mathematische Schriften, vol. 71, pp. 8–13, 2005.]

[S. V. Avgustinovich, O. Heden, F. I. Solov'eva, "On intersection problem for perfect binary codes", Des., Codes and Cryptogr., vol. 39, pp. 317–322, 2006.]

Main results

We investigate the following question: what is the size of the intersection of two Reed – Muller like codes?

Denote the Reed – Muller like code of order r having length 2^m by $LRM_{r,m}$ and its punctured code by $LRM^*_{r,m}$. Let λ be any function from $LRM^*_{r-1,m-1}$ to $\{0,1\}$.

Pulatov switching construction 1974

The set

$$\{(x+y, x, |x| + \lambda(y)) : x \in LRM^*_{r,m-1},\ y \in LRM^*_{r-1,m-1}\}.$$

is a punctured Reed – Muller like code of order r of length 2^m.

Main results

We investigate the following question: what is the size of the intersection of two Reed – Muller like codes?

Denote the Reed – Muller like code of order r having length 2^m by $LRM_{r,m}$ and its punctured code by $LRM^*_{r,m}$. Let λ be any function from $LRM^*_{r-1,m-1}$ to $\{0,1\}$.

Pulatov switching construction 1974

The set

$$\{(x+y, x, |x| + \lambda(y)) : x \in LRM^*_{r,m-1},\ y \in LRM^*_{r-1,m-1}\}.$$

is a punctured Reed – Muller like code of order r of length 2^m.

Main results

We investigate the following question: what is the size of the intersection of two Reed – Muller like codes?

Denote the Reed – Muller like code of order r having length 2^m by $LRM_{r,m}$ and its punctured code by $LRM^*_{r,m}$. Let λ be any function from $LRM^*_{r-1,m-1}$ to $\{0,1\}$.

Pulatov switching construction 1974

The set

$$\{(x+y, x, |x|+\lambda(y)) : x \in LRM^*_{r,m-1},\ y \in LRM^*_{r-1,m-1}\}.$$

is a punctured Reed – Muller like code of order r of length 2^m.

Main results

Further we use two special extended Reed – Muller like codes given by the Pulatov construction 1974.

Main results

Let y be a fixed vector from $LRM_{r-1,m-1}$ and $R^y = \{(x+y, x) | x \in RM_{r,m-1}\}$. Let λ be any function from $RM_{r-1,m-1}$ to $\{0,1\}$; $\pi(x_1, \ldots, x_{n/2}) = (x_{n/2}, x_1, \ldots, x_{n/2-1})$.

The codes D_λ and $D'_{\lambda'}$:

For a fixed integer i, $1 \le i \le 2^{m-1}$ we define the Reed – Muller like code $D_\lambda = D_0 \cup D_1$, where

$$D_0 = \bigcup_{y \in RM_{r-1,m-1},\, \lambda(y)=0} R^y,$$

$$D_1 = \bigcup_{y \in RM_{r-1,m-1},\, \lambda(y)=1} (R^y + (e_i, e_i)),$$

$$D'_{\lambda'} = \pi(D_{\lambda'}) = \{(u, \pi(v)) \mid (u,v) \in D_{\lambda'}\}.$$

Main results

Let y be a fixed vector from $LRM_{r-1,m-1}$ and $R^y = \{(x+y, x) | x \in RM_{r,m-1}\}$. Let λ be any function from $RM_{r-1,m-1}$ to $\{0,1\}$; $\pi(x_1, \ldots, x_{n/2}) = (x_{n/2}, x_1, \ldots, x_{n/2-1})$.

The codes D_λ and $D'_{\lambda'}$:

For a fixed integer i, $1 \le i \le 2^{m-1}$ we define the Reed – Muller like code $D_\lambda = D_0 \cup D_1$, where

$$D_0 = \bigcup_{y \in RM_{r-1,m-1},\, \lambda(y)=0} R^y,$$

$$D_1 = \bigcup_{y \in RM_{r-1,m-1},\, \lambda(y)=1} (R^y + (e_i, e_i)),$$

$$D'_{\lambda'} = \pi(D_{\lambda'}) = \{(u, \pi(v)) \mid (u, v) \in D_{\lambda'}\}.$$

Main results

Let y be a fixed vector from $LRM_{r-1,m-1}$ and $R^y = \{(x+y,x) | x \in RM_{r,m-1}\}$. Let λ be any function from $RM_{r-1,m-1}$ to $\{0,1\}$; $\pi(x_1,\ldots,x_{n/2}) = (x_{n/2}, x_1, \ldots, x_{n/2-1})$.

The codes D_λ and $D'_{\lambda'}$:

For a fixed integer i, $1 \le i \le 2^{m-1}$ we define the Reed – Muller like code $D_\lambda = D_0 \cup D_1$, where

$$D_0 = \bigcup_{y \in RM_{r-1,m-1},\, \lambda(y)=0} R^y,$$

$$D_1 = \bigcup_{y \in RM_{r-1,m-1},\, \lambda(y)=1} (R^y + (e_i, e_i)),$$

$$D'_{\lambda'} = \pi(D_{\lambda'}) = \{(u, \pi(v)) \mid (u,v) \in D_{\lambda'}\}.$$

Main results

Theorem 1.

For any $m \geq 4$ and r, $1 \leq r \leq m-2$, and numbers k_1, k_2 such that $1 \leq k_s \leq |RM_{r-1,m-1}|$, $s \in \{1,2\}$ there are two Reed – Muller like codes of order r of length 2^m with the intersection of size $2k_1k_2$.

Main results

$D_\lambda = D_\lambda(RM_{r-1,m-1})$ and $D'_{\lambda'} = D'_{\lambda'}(\nu(RM_{r-1,m-1}))$, where ν is a transposition of the first two coordinate positions of $RM_{r-1,m-1}$:

Theorem 2.

For any $m \geq 4$ and r, $1 \leq r \leq m-2$, and any number k such that

$$0 \leq k \leq |RM_{r-1,m-1}|^2$$

there are two Reed – Muller like codes of order r of length 2^m with the intersection of size k.

Main results

$D_\lambda = D_\lambda(RM_{r-1,m-1})$ and $D'_{\lambda'} = D'_{\lambda'}(\nu(RM_{r-1,m-1}))$, where ν is a transposition of the first two coordinate positions of $RM_{r-1,m-1}$:

Theorem 2.

For any $m \geq 4$ and r, $1 \leq r \leq m-2$, and any number k such that

$$0 \leq k \leq |RM_{r-1,m-1}|^2$$

there are two Reed – Muller like codes of order r of length 2^m with the intersection of size k.

Conclusion

We proved that

1. There exist two $LRM_{r,m}$ codes of order r having lengths at least 16 with the intersection number equaled $2k_1k_2$, where $1 \leq k_s \leq |RM_{r-1,m-1}|$, $s \in \{1,2\}$.

2. There exist two $LRM_{r,m}$ codes of order r having lengths at least 16 with the intersection number equaled k, where $0 \leq k \leq |RM_{r-1,m-1}|^2$.

3. The sets of numbers given in Theorems 1 and 2 do not intersect each other.

4. The minimum intersection number equaled 2 is also attainable for Reed – Muller like codes.

Conclusion

We proved that

1. There exist two $LRM_{r,m}$ codes of order r having lengths at least 16 with the intersection number equaled $2k_1k_2$, where $1 \leq k_s \leq |RM_{r-1,m-1}|$, $s \in \{1, 2\}$.

2. There exist two $LRM_{r,m}$ codes of order r having lengths at least 16 with the intersection number equaled k, where $0 \leq k \leq |RM_{r-1,m-1}|^2$.

3. The sets of numbers given in Theorems 1 and 2 do not intersect each other.

4. The minimum intersection number equaled 2 is also attainable for Reed – Muller like codes.

Conclusion

We proved that

1. There exist two $LRM_{r,m}$ codes of order r having lengths at least 16 with the intersection number equaled $2k_1k_2$, where $1 \leq k_s \leq |RM_{r-1,m-1}|$, $s \in \{1,2\}$.

2. There exist two $LRM_{r,m}$ codes of order r having lengths at least 16 with the intersection number equaled k, where $0 \leq k \leq |RM_{r-1,m-1}|^2$.

3. The sets of numbers given in Theorems 1 and 2 do not intersect each other.

4. The minimum intersection number equaled 2 is also attainable for Reed – Muller like codes.

Conclusion

We proved that

1. There exist two $LRM_{r,m}$ codes of order r having lengths at least 16 with the intersection number equaled $2k_1k_2$, where $1 \leq k_s \leq |RM_{r-1,m-1}|$, $s \in \{1,2\}$.

2. There exist two $LRM_{r,m}$ codes of order r having lengths at least 16 with the intersection number equaled k, where $0 \leq k \leq |RM_{r-1,m-1}|^2$.

3. The sets of numbers given in Theorems 1 and 2 do not intersect each other.

4. The minimum intersection number equaled 2 is also attainable for Reed – Muller like codes.

Conclusion

5. The results above are valid for punctured Reed – Muller like codes of order r with length $2^m - 1$.

6. We used the Reed – Muller like codes presented by Pulatov in 1974.

7. We generalize the results of Bar Yashalom at al.1997, Etzion 1998, Avgustinovich at al. 2005 and 2006.

Conclusion

5. The results above are valid for punctured Reed – Muller like codes of order r with length $2^m - 1$.

6. We used the Reed – Muller like codes presented by Pulatov in 1974.

7. We generalize the results of Bar Yashalom at al.1997, Etzion 1998, Avgustinovich at al. 2005 and 2006.

Conclusion

5. The results above are valid for punctured Reed – Muller like codes of order r with length $2^m - 1$.

6. We used the Reed – Muller like codes presented by Pulatov in 1974.

7. We generalize the results of Bar Yashalom at al.1997, Etzion 1998, Avgustinovich at al. 2005 and 2006.

THANK YOU FOR YOUR ATTENTION