Single orbit affine generators for extended BCH codes with designed distance three

I. Yu. Mogilnykh, F. I. Solov'eva

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

Presented at Seventeenth International Workshop on Algebraic and Combinatorial Coding Theory
ACCT 2020
October 11-17, 2020, BULGARIA

The aim of the our work is finding a basis of the extended BCH code $\overline{C_{1,2}}$ over $GF(p)$ of length $p^m - 1$ of the smallest possible weight codewords.

We show that for any prime p, $p \neq 2, 3$ and any m, $m \geq 3$ the narrow-sense BCH codes over $GF(p)$ of length $p^m - 1$ with designed distance three are not spanned by theirs minimum nonzero weight codewords.

We prove that the extensions of these codes with code distance 4 are spanned by their codewords of weight 5.

The bases could be chosen in the affine orbits of explicit codewords (*affine generator property*).

The aim of the our work is finding a basis of the extended BCH code $\overline{C_{1,2}}$ over $GF(p)$ of length $p^m - 1$ of the smallest possible weight codewords.

We show that for any prime p, $p \neq 2, 3$ and any m, $m \geq 3$ the narrow-sense BCH codes over $GF(p)$ of length $p^m - 1$ with designed distance three are not spanned by theirs minimum nonzero weight codewords.

We prove that the extensions of these codes with code distance 4 are spanned by their codewords of weight 5.

The bases could be chosen in the affine orbits of explicit codewords (*affine generator property*).

The aim of the our work is finding a basis of the extended BCH code $\overline{C_{1,2}}$ over $GF(p)$ of length $p^m - 1$ of the smallest possible weight codewords.

We show that for any prime p, $p \neq 2, 3$ and any m, $m \geq 3$ the narrow-sense BCH codes over $GF(p)$ of length $p^m - 1$ with designed distance three are not spanned by theirs minimum nonzero weight codewords.

We prove that the extensions of these codes with code distance 4 are spanned by their codewords of weight 5.

The bases could be chosen in the affine orbits of explicit codewords (*affine generator property*).

The aim of the our work is finding a basis of the extended BCH code $\overline{C_{1,2}}$ over $GF(p)$ of length $p^m - 1$ of the smallest possible weight codewords.

We show that for any prime p, $p \neq 2, 3$ and any m, $m \geq 3$ the narrow-sense BCH codes over $GF(p)$ of length $p^m - 1$ with designed distance three are not spanned by theirs minimum nonzero weight codewords.

We prove that the extensions of these codes with code distance 4 are spanned by their codewords of weight 5.

The bases could be chosen in the affine orbits of explicit codewords (*affine generator property*).

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

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.

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 and the binary Reed-Muller 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 and the binary Reed-Muller 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.]

Survey

Mogilnykh and S. showed that the minimum weight bases of the following classes 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.]

Survey

Mogilnykh and S. showed that the minimum weight bases of the following classes 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.]

Survey

Mogilnykh and S. showed that the minimum weight bases of the following classes 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.]

Survey

Mogilnykh and S. showed that the minimum weight bases of the following classes 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.]

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

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

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

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

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* δ and its minimum distance is at least δ by BCH bound.

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

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* δ and its minimum distance is at least δ by BCH bound.

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

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* δ and its minimum distance is at least δ by BCH bound.

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

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

The *extended code* $\overline{C}$ of C is $\{\overline{c} : c \in C\}$. 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 $c = (c_0, \ldots, c_{p^m-2})$ of length $p^m - 1$ we denote its extension by $\overline{c}$, i.e.

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

The *extended code* $\overline{C}$ of C is $\{\overline{c} : c \in C\}$. 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 (γ, σ), γ, $\sigma \in GF(p^m)$, $\gamma \neq 0$ that send β 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 (γ, σ), γ, $\sigma \in GF(p^m)$, $\gamma \neq 0$ that send β 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 (γ, σ), γ, $\sigma \in GF(p^m)$, $\gamma \neq 0$ that send β 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.

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

Main results

As an example let us show an explicit codeword of weight 3 in the binary cyclic code $C_{1,2}$: $\quad c(x) = 1 + x + x^i$,
where $\alpha^i = \alpha + 1$. Its extension is a single orbit affine generator for $\overline{C_{1,2}}$ (see E. Grigorescu and T. Kaufman, 2011).

Lemma. Mogilnykh and S.

Let α 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

As an example let us show an explicit codeword of weight 3 in the binary cyclic code $C_{1,2}$: $c(x) = 1 + x + x^i$,
where $\alpha^i = \alpha + 1$. Its extension is a single orbit affine generator for $\overline{C_{1,2}}$ (see E. Grigorescu and T. Kaufman, 2011).

Lemma. Mogilnykh and S.

Let α 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 2. Mogilnykh and S.

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

Conclusion

1. We showed that for any prime p, $p \neq 2, 3$ and any m, $m \geq 3$ the narrow-sense BCH codes over $GF(p)$ of length $p^m - 1$ with designed distance three and their extensions are not spanned by theirs minimum nonzero weight codewords.

2. We proved that the extensions of these codes are spanned by their codewords of weight 5.

3. The basis of the BCH code $\overline{C_{1,2}}$ could be chosen in the affine orbits of explicit codewords of weight 5.

4. For $p = 3$ the single orbit affine generator has minimum weight since the minimum distance of $\overline{C_{1,2}}$ is 5.

Conclusion

1. We showed that for any prime p, $p \neq 2, 3$ and any m, $m \geq 3$ the narrow-sense BCH codes over $GF(p)$ of length $p^m - 1$ with designed distance three and their extensions are not spanned by theirs minimum nonzero weight codewords.

2. We proved that the extensions of these codes are spanned by their codewords of weight 5.

3. The basis of the BCH code $\overline{C_{1,2}}$ could be chosen in the affine orbits of explicit codewords of weight 5.

4. For $p = 3$ the single orbit affine generator has minimum weight since the minimum distance of $\overline{C_{1,2}}$ is 5.

Conclusion

1. We showed that for any prime p, $p \neq 2, 3$ and any m, $m \geq 3$ the narrow-sense BCH codes over $GF(p)$ of length $p^m - 1$ with designed distance three and their extensions are not spanned by theirs minimum nonzero weight codewords.

2. We proved that the extensions of these codes are spanned by their codewords of weight 5.

3. The basis of the BCH code $\overline{C_{1,2}}$ could be chosen in the affine orbits of explicit codewords of weight 5.

4. For $p = 3$ the single orbit affine generator has minimum weight since the minimum distance of $\overline{C_{1,2}}$ is 5.

Conclusion

1. We showed that for any prime p, $p \neq 2, 3$ and any m, $m \geq 3$ the narrow-sense BCH codes over $GF(p)$ of length $p^m - 1$ with designed distance three and their extensions are not spanned by theirs minimum nonzero weight codewords.

2. We proved that the extensions of these codes are spanned by their codewords of weight 5.

3. The basis of the BCH code $\overline{C_{1,2}}$ could be chosen in the affine orbits of explicit codewords of weight 5.

4. For $p = 3$ the single orbit affine generator has minimum weight since the minimum distance of $\overline{C_{1,2}}$ is 5.

THANK YOU FOR YOUR ATTENTION