Constructions of linear codes with one-dimensional hull

Chengju Li
East China Normal University

July 3, 2018
The 5th Sino-Korea International Conference on Coding Theory and Its Related Topics

Abstract

The objective of this talk is to present some sufficient and necessary conditions that linear codes and cyclic codes have one-dimensional hull. Based on these characterizations, some constructions of linear codes with one-dimensional hull were given by employing quadratic number fields, partial difference sets, and difference sets. We also construct cyclic codes with one-dimensional hull. Some optimal codes with one-dimensional hull are obtained.

Introduction

Linear codes

- Definition: An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathrm{GF}(q)$ is a k-dimensional subspace of $\mathrm{GF}(q)^n$ with minimum Hamming distance d.
- Proposition: The minimum distance of any linear code is equal to its minimum nonzero weight.
- The (Euclidean) dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined by

$$\mathcal{C}^\perp = \{\mathbf{b} \in \mathrm{GF}(q)^n : \mathbf{b}\mathbf{c}^T = 0 \ \forall \ \mathbf{c} \in \mathcal{C}\},$$

where $\mathbf{b}\mathbf{c}^T$ denotes the standard inner product of the two vectors $\mathbf{b}$ and $\mathbf{c}$.

Hull

- The hull of the linear code $\mathcal{C}$ is defined to be

$$\mathrm{Hull}(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^{\perp}.$$

  It is clear that $\mathrm{Hull}(\mathcal{C})$ is also a linear code over $\mathrm{GF}(q)$. Suppose that the dimension of $\mathrm{Hull}(\mathcal{C})$ is ℓ.
- When $\ell = 0$, i.e., $\mathrm{Hull}(\mathcal{C}) = \{0\}$, the code $\mathcal{C}$ is called an LCD code.
- When $\ell = k$, i.e., $\mathcal{C} \cap \mathcal{C}^{\perp} = \mathcal{C}$, $\mathcal{C}$ is said to be self-orthogonal, where k is the dimension of $\mathcal{C}$.
- When $\ell = \frac{n}{2}$ for even n, then $\mathcal{C}$ is called a self-dual code.

History

The hull was originally introduced in 1990 by Assmus and Key to classify finite projective planes.

E. F. Assmus and J. D. Key, "Affine and projective planes," Discrete Math., vol. 83, pp. 161–187, 1990.

The hull plays an important role in determining the complexity of algorithms for checking permutation equivalence of two linear codes and computing the automorphism group of a linear code, which are very effective in general when the dimension of the hull is small.

- J. Leon, "Computing automorphism groups of error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 3, pp. 496–511, 1982.
- J. Leon, "Permutation group algorithms based on partition, I: theory and algorithms," *J. Symbolic Comput.*, vol. 12, pp. 533–583, 1991.
- N. Sendrier and G. Skersys, "On the computation of the automorphism group of a linear code," in: Proceedings of IEEE ISIT'2001, Washington, DC, p. 13, 2001.
- N. Sendrier, "Finding the permutation between equivalent codes: the support splitting algorithm," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1193–1203, 2000.

Sendrier proved that the expected dimension of the hull of a random $[n, k]$ code is a constant when n and k go to infinity.

N. Sendrier, "On the dimension of the hull," *SIAM J. Discrete Math.*, vol. 10, no. 2, pp. 282–293, 1997.

Skersys investigated the average dimension of the hulls of cyclic codes.

G. Skersys, "The average dimension of the hull of cyclic codes," *Discrete Appl. Math.*, vol. 128, no. 1, pp. 275–292, 2003.

The enumerations of cyclic codes and negacyclic codes of length n over $\mathrm{GF}(q)$ having hulls of a given dimension are established.

E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, "Hulls of cyclic and negacyclic codes over finite fields," *Finite Fields Appl.*, vol. 33, pp. 232–257, 2015.

Motivation

Due to the aforementioned algorithms, it is desired to the construct linear codes with small hull. It is clear that the linear codes with the smallest hull are LCD codes and with the second smallest hull are those with one-dimensional hull.

Mathematical tools

- Character sums.
- Quadratic number fields and prime ideal factorizations.
- difference set ...

Linear codes with one-dimensional hull

A proposition

The following proposition gives a characterization of linear codes with ℓ-dimensional hull via their generator matrices in the standard form.

Proposition

Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathrm{GF}(q)$ with generator matrix $G = [I_k, P]$. For an integer with $0 \leq \ell \leq k$, the code $\mathcal{C}$ has ℓ-dimensional hull if and only if rank$(I_k + PP^T) = k - \ell$.

Remark

Employing Proposition above, we easily see that $\mathcal{C}$ is an LCD code if and only if $\text{rank}(I_k + PP^T) = k$, and C is self-orthogonal if and only if $\text{rank}(I_k + PP^T) = 0$.

We also have the following theorem, which provides an idea to construct the linear codes with one-dimensional hull by the generator matrix.

Theorem

Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathrm{GF}(q)$ with generator matrix $G = [I_k, P]$. Then the code $\mathcal{C}$ has one-dimensional hull if the matrix PP^T has an eigenvalue -1 with multiplicity 1.

A key step

Let $\mathcal{G} = \{x_i : 1 \leq i \leq v\}$ be a finite abelian group of order v. Define a $v \times v$ matrix P by

$$P_{ij} = \rho(x_j - x_i), \tag{2.1}$$

where $\rho : \mathcal{G} \to \mathbb{C}$ is a function. Let $\phi : \mathcal{G} \to \mathbb{C}^*$ be a character, i.e., a homomorphism from $\mathcal{G}$ into the multiplicative group of nonzero complex numbers.

Then we have
(2.2)

$$P\begin{bmatrix}\phi(x_1)\\ \phi(x_2)\\ \vdots\\ \phi(x_v)\end{bmatrix}=\begin{bmatrix}\sum_{i=1}^{v}\rho(x_i-x_1)\phi(x_i)\\ \sum_{i=1}^{v}\rho(x_i-x_2)\phi(x_i)\\ \vdots\\ \sum_{i=1}^{v}\rho(x_i-x_v)\phi(x_i)\end{bmatrix}=\sum_{x\in\mathcal{G}}\rho(x)\phi(x)\begin{bmatrix}\phi(x_1)\\ \phi(x_2)\\ \vdots\\ \phi(x_v)\end{bmatrix},$$

which means that $\left[\phi(x_1),\phi(x_2),\ldots,\phi(x_v)\right]^T$ is an eigenvector of P with eigenvalue $\sum_{x\in\mathcal{G}}\rho(x)\phi(x)$.

It is well known that $\mathcal{G}$ has v characters, each of which gives an eigenvector. By the orthogonality relations for characters, these eigenvectors are linearly independent. Therefore, $\{\sum_{x\in\mathcal{G}} \rho(x)\phi(x) : \phi \in \widehat{\mathcal{G}}\}$ is the set of all eigenvalues of the matrix P.

Notation

- Let $K = \mathbb{Q}(\sqrt{r})$ be a quadratic number field and $\mathbb{O}_K$ the ring of algebraic integers.
- Let p be a prime such that -1 is a square element in the finite field $\mathbb{O}_K/\mathcal{P}$, where $\mathcal{P}$ is a prime ideal over p.
- Let $\bar{\beta} \in \mathbb{O}_K/\mathcal{P}$ satisfying that $\bar{\beta}^2 = -1$ and let $\beta \in \mathbb{O}_K$ be a preimage of $\bar{\beta}$ by the natural homomorphism $\mathbb{O}_K \to \mathbb{O}_K/\mathcal{P}$, i.e., $\beta \mapsto \bar{\beta} = \beta + \mathcal{P}$.

- Suppose that $\mathcal{G} = \mathrm{GF}(r^m)$, where r is a prime and m is an integer. Let α be a fixed primitive element of $\mathrm{GF}(r^m)$.
- Define ρ by

$$\rho(x) = \begin{cases} \eta(x), & \text{if } x \in \mathrm{GF}(r^m)^*, \\ \beta, & \text{if } x = 0, \end{cases}$$

where η is the quadratic multiplicative character of $\mathrm{GF}(r^m)^*$.

- By Equation (2.1), we get a $r^m \times r^m$ matrix P over $\mathbb{O}_K$ with entries $\beta, \pm 1$.
- The eigenvalues of the matrix P are

$$\beta + G(\eta, \phi), \ \phi \in \widehat{\mathrm{GF}(r^m)},$$

where $G(\eta, \phi)$ is the quadratic Gauss sum.

- Note that

$$\eta(-1) = \begin{cases} 1, & \text{if } r^m \equiv 1 \pmod 4; \\ -1, & \text{if } r^m \equiv 3 \pmod 4. \end{cases}$$

Then

$$P^T = \begin{cases} P, & \text{if } r^m \equiv 1 \pmod 4; \\ 2\beta I - P, & \text{if } r^m \equiv 3 \pmod 4, \end{cases}$$

where I is the identity matrix of order r^m.

- We then get

$$PP^T = \begin{cases} P^2, & \text{if } r^m \equiv 1 \pmod 4; \\ 2\beta P - P^2, & \text{if } r^m \equiv 3 \pmod 4. \end{cases}$$

- The eigenvalues of PP^T are given by (2.3)

$$\begin{cases} \{\Big(\beta + G(\eta, \phi)\Big)^2 : \phi \in \widehat{\mathrm{GF}(r^m)}\}, \\ \text{if } r^m \equiv 1 \pmod 4; \\ \{2\beta\Big(\beta + G(\eta, \phi)\Big) - \Big(\beta + G(\eta, \phi)\Big)^2 : \phi \in \widehat{\mathrm{GF}(r^m)}\}, \\ \text{if } r^m \equiv 3 \pmod 4. \end{cases}$$

- Note that $P = (P_{ij}) \in M_{r^m}(\mathbb{O}_K)$, which is the ring of all square matrices of order r^m over $\mathbb{O}_K$. Define

$$\bar{P} = (\bar{P}_{ij}),\ \bar{P}_{ij} = P_{ij} + \mathcal{P} \in \mathbb{O}_K/\mathcal{P},$$

  where $\mathcal{P}$ is a prime ideal in $\mathbb{O}_K$.
- Denote $\mathrm{GF}(q) = \mathbb{O}_K/\mathcal{P}$. Then $\bar{P} \in M_{r^m}(\mathrm{GF}(q))$. We claim that $\bar{\lambda}$ is an eigenvalue of $\bar{P}$ if λ be an eigenvalue of P. In fact, λ is a root of the polynomial

$$f(x) = \det(xI - P) = x^{r^m} + a_{r^m-1}x^{r^m-1} + \cdots + a_1 x + a_0,$$

  it is easy to check that $\bar{f}(\bar{\lambda}) = 0$, where $\bar{f}(x) = x^{r^m} + \bar{a}_{r^m-1}x^{r^m-1} + \cdots + \bar{a}_1 x + \bar{a}_0$.

Let $\mathcal{C}$ be the linear code over $\mathrm{GF}(q)$ with generator matrix $G = [I_{r^m}, \bar{P}]$. When $p = 2$, we can let $\beta = 1$ and thus $\bar{P}$ is a matrix with all entries 1, i.e., $\bar{P} \in M_{r^m}(\mathrm{GF}(2))$. It is easy to compute that the eigenvalues of $\bar{P}\bar{P}^T$ are -1 with multiplicity 1 and 0 with multiplicity $r^m - 1$.

Theorem

Let $K = \mathbb{Q}(\sqrt{r})$ and $p = 2$. Then $\mathcal{C}$ is a $[2r^m, r^m]$ binary linear code with one-dimensional hull.

Below we assume that p is an odd prime and divide into two cases according to the values of quadratic Gauss sums.

Case 1: $r \equiv 1 \pmod 4$

- $\mathbb{O}_K = \{a + b\frac{-1+\sqrt{r}}{2} : a, b \in \mathbb{Z}\}$ and $\delta_K = r$.
- The value distribution of eigenvalues of PP^T is given as follows:

$$\begin{cases} -1, & \text{occurs once;} \\ -1 \pm 2\beta\sqrt{r^m} + r^m, & \text{occurs } \frac{r^m-1}{2} \text{ times.} \end{cases}$$

A theorem

Theorem

Let $K = \mathbb{Q}(\sqrt{r})$ *and* p *an odd prime, where* $r \equiv 1 \pmod 4$ *and* $p \nmid (r^m + 4)$.

1. *If* $p \equiv 1 \pmod 4$ *and* $p \neq r$, *then* $\mathcal{C}$ *is a* $[2r^m, r^m]$ p*-ary linear code with one-dimensional hull.*
2. *If* $\left(\frac{r}{p}\right) = -1$ *and* $p \equiv 3 \pmod 4$, *then* $\mathcal{C}$ *is a* $[2r^m, r^m]$ p^2*-ary linear code with one-dimensional hull.*

Proof: When $\left(\frac{r}{p}\right) = 1$, we have $x^2 \equiv r \pmod{p}$ is solvable in $\mathbb{Z}$. It then is deduced that $p\mathbb{O}_K = \mathcal{P}_1\mathcal{P}_2$. Moreover, $\mathcal{P}_1 = (p, a + \sqrt{r})$, $\mathcal{P}_2 = (p, a - \sqrt{r})$, where $a \in \mathbb{Z}$ and $a^2 \equiv r \pmod{p}$. Without of loss generality, we assume that $\mathcal{P} = \mathcal{P}_1$. Then

$$\mathbb{O}_K/\mathcal{P} \cong \mathrm{GF}(p).$$

It is deduced that $\mathcal{C}$ is a p-ary code if $\left(\frac{r}{p}\right) = 1$.

When $\left(\frac{r}{p}\right) = -1$, $x^2 \equiv r \pmod{p}$ is not solvable in $\mathbb{Z}$. Then $p\mathbb{O}_K = \mathcal{P}$ and $\mathbb{O}_K/\mathcal{P} = \mathrm{GF}(p^2)$. Thus $\mathcal{C}$ is a p^2-ary code if $\left(\frac{r}{p}\right) = -1$. In particular, for $p \equiv 1 \pmod{4}$, -1 is a square element in $\mathrm{GF}(p)$, so $\bar{P} \in M_{r^m}(\mathrm{GF}(p))$ and $\mathcal{C}$ is a p-ary code.

Note that $p \nmid (r^m + 4)$. Then

$$(r^m + 2\beta\sqrt{r^m})(r^m - 2\beta\sqrt{r^m}) = r^m(r^m + 4) \notin p\mathbb{Z}.$$

We claim that $r^m(r^m + 4) \notin \mathcal{P}$. Otherwise, $r^m(r^m + 4) \in \mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, this leads to a contradiction. Recall that $\mathcal{P}$ is a prime ideal. Therefore, both $r^m + 2\beta\sqrt{r^m}$ and $r^m - 2\beta\sqrt{r^m}$ don't belong to $\mathcal{P}$, which means

$$-1 \pm 2\beta\sqrt{r^m} + r^m \not\equiv -1 \pmod{\mathcal{P}}.$$

It then follows that the matrix $\bar{P}\bar{P}^T$ has an eigenvalue -1 with multiplicity 1. Collecting all discussions above, the desired result then follows.

Case 2: $r \equiv 3 \pmod 4$

- $\mathbb{O}_K = \{a + b\sqrt{r} : a, b \in \mathbb{Z}\}$ and $\delta_K = 4r$.
- Let $\mathcal{P}$ be a prime ideal in $\mathbb{O}_K$ over p. Then we have $\mathbb{O}_K/\mathcal{P} \cong \mathrm{GF}(p)$ if $\left(\frac{r}{p}\right) = 1$, and $\mathbb{O}_K/\mathcal{P} \cong \mathrm{GF}(p^2)$ if $\left(\frac{r}{p}\right) = -1$.

When m is even, we have $r^m \equiv 1 \pmod 4$. Then the eigenvalues of PP^T are given as follows:

$$\begin{cases} -1, & \text{occurs once;} \\ -1 \pm 2\beta\sqrt{r^m} + r^m, & \text{occurs } \frac{r^m-1}{2} \text{ times.} \end{cases}$$

Theorem

Let $K = \mathbb{Q}(\sqrt{r})$ and m an even integer, where $r \equiv 3 \pmod 4$. Suppose that p is an odd prime such that $p \nmid (r^m + 4)$. Then we have the following.

1. *If $p \equiv 1 \pmod 4$, then $\mathcal{C}$ is a $[2r^m, r^m]$ p-ary linear code with one-dimensional hull.*
2. *If $\left(\frac{r}{p}\right) = -1$ and $p \equiv 3 \pmod 4$, then $\mathcal{C}$ is a $[2r^m, r^m]$ p^2-ary linear code with one-dimensional hull.*

When m is odd, we have $r^m \equiv 3 \pmod 4$. Then the eigenvalues of PP^T are given as follows:

$$\begin{cases} -1, & \text{occurs once;} \\ -1 + r^m, & \text{occurs } r^m - 1 \text{ times.} \end{cases}$$

Theorem

Let $K = \mathbb{Q}(\sqrt{r})$ and m an odd integer, where $r \equiv 3 \pmod 4$. Let p be an odd prime. Then we have the following.

1. *If $p \equiv 1 \pmod 4$, then $\mathcal{C}$ is a $[2r^m, r^m]$ p-ary linear code with one-dimensional hull.*
2. *If $\left(\frac{r}{p}\right) = -1$ and $p \equiv 3 \pmod 4$, then $\mathcal{C}$ is a $[2r^m, r^m]$ p^2-ary linear code with one-dimensional hull.*

Linear codes with one-dimensional hull from partial difference sets

Let $\mathcal{G}$ be a finite abelian group of order v and D a subset of $\mathcal{G}$ with k elements. The set D is called a (v, k, λ, μ) *partial difference set* in $\mathcal{G}$ if the expressions $d_1 - d_2$, for $d_1, d_2 \in D$ with $d_1 \neq d_2$, represent nonidentity elements in D exactly λ times and represent nonidentity elements not in D exactly μ times.

Lemma

Let D be a (v, k, λ, μ) $(\lambda \neq \mu)$ partial difference set in the abelian group $\mathcal{G}$ and ϕ a nontrivial character of $\mathcal{G}$. Then

$$\phi(D) := \sum_{d \in D} \phi(d) = \frac{\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}{2}$$

if D does not contain the identity of $\mathcal{G}$.

Define a function from $\mathcal{G}$ to $\mathbb{C}$ by

$$\rho(x) = \begin{cases} 1, & x \in D; \\ 0, & x \in \mathcal{G} \setminus D. \end{cases}$$

Then a $v \times v$ matrix $P = (P_{ij})$ associated with D follows from $P_{ij} = \rho(x_j - x_i)$, where $x_i, x_j \in \mathcal{G}$. It is known that $D = -D$ when $\lambda \neq \mu$. Thus P is a symmetric matrix in this case, i.e., $P = P^T$. Denote $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$. Let $K = \mathbb{Q}(\sqrt{\Delta})$ and let $\mathcal{P}$ be any prime ideal over p in $\mathbb{O}_K$, where p is a prime.

Theorem

Suppose that p is a prime. Let $\mathcal{C}$ be the linear code over $\mathrm{GF}(p)$ with generator matrix $G = [I_k, P]$, where P is the matrix associated with a (v, k, λ, μ) partial difference set D. Then $\mathcal{C}$ has one-dimensional hull if

$$k^2 \equiv -1 \pmod{p} \text{ and } \phi(D)^2 \not\equiv -1 \pmod{\mathcal{P}}$$

for all nontrivial characters ϕ of $\mathcal{G}$.

Theorem

Let D be a $(r^m, \frac{r^m-1}{2}, \frac{r^m-5}{4}, \frac{r^m-1}{4})$ Paley type partial difference set and $\mathcal{C}$ the linear code defined as above. Then $\mathcal{C}$ is a p-ary $[2r^m, r^m]$ linear code with one dimensional hull if p satisfies that

$$p \mid \frac{r^{2m} - 2r^m + 5}{4} \text{ and } p \nmid \frac{r^{2m} + 6r^m + 25}{16}.$$

Linear codes with one-dimensional hull from difference sets

Let $\mathcal{G}$ be a finite abelian group of order v and D a subset of $\mathcal{G}$ with k elements. The set D is called a (v, k, λ) *difference set* in $\mathcal{G}$ if the expressions $d_1 - d_2$, for $d_1, d_2 \in D$ with $d_1 \neq d_2$, represent every nonidentity element in $\mathcal{G}$ exactly λ times.

Define a function from $\mathcal{G}$ to $\mathbb{C}$ by

$$\rho(x) = \begin{cases} 1, & x \in D; \\ 0, & x \in \mathcal{G} \setminus D. \end{cases}$$

Then a $v \times v$ matrix $P = (P_{ij})$ associated with D follows from $P_{ij} = \rho(x_j - x_i)$, where $x_i, x_j \in \mathcal{G}$. It is known that a difference set leads to a 2-design by employing its development.

Lemma

Let P be the matrix associated with a (v, k, λ) difference set D as above. Then

$$PP^T = (k - \lambda)I_v + \lambda J,$$

where J is the $v \times v$ matrix with all entries 1.

Theorem

Suppose that p is a prime. Let $\mathcal{C}$ be the linear code over $\mathrm{GF}(p)$ with generator matrix $G = [I_k, P]$, where P is the matrix associated with a (v, k, λ) difference set D. Then $\mathcal{C}$ has one-dimensional hull if

$$k + \lambda(v-1) \equiv -1 \pmod{p} \text{ and } k - \lambda \not\equiv -1 \pmod{p}.$$

Theorem

Let D be a $(r^m, \frac{r^m-1}{2}, \frac{r^m-3}{4})$ Paley type difference set and $\mathcal{C}$ the linear code defined as above. Then $\mathcal{C}$ is a p-ary $[2r^m, r^m]$ linear code with one-dimensional hull if p satisfies that

$$p \mid \frac{r^{2m} - 2r^m + 5}{4} \text{ and } p \nmid \frac{r^m + 5}{4}.$$

Cyclic codes with one-dimensional hull

Cyclic codes

- An $[n, k]$ linear code $\mathcal{C}$ is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$.
- By identifying any vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{GF}(q)^n$ with

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathrm{GF}(q)[x]/(x^n - 1),$$

a code $\mathcal{C}$ of length n over $\mathrm{GF}(q)$ corresponds to a subset of $\mathrm{GF}(q)[x]/(x^n - 1)$. Then $\mathcal{C}$ is a cyclic code if and only if the corresponding subset is an ideal of $\mathrm{GF}(q)[x]/(x^n - 1)$.

- Note that every ideal of $\mathrm{GF}(q)[x]/(x^n-1)$ is principal. Then there is a monic polynomial $g(x)$ of the smallest degree such that $\mathcal{C}=\langle g(x)\rangle$ and $g(x) \mid (x^n-1)$. In addition, $g(x)$ is unique and called the *generator polynomial*, and $h(x)=(x^n-1)/g(x)$ is referred to as the *check polynomial* of $\mathcal{C}$.
- Denote $m=\mathrm{ord}_n(q)$. Let α be a generator of $\mathrm{GF}(q^m)^*$ and put $\beta=\alpha^{\frac{q^m-1}{n}}$. Then β is a primitive n-th root of unity. The set $S=\{0\le i\le n-1 : g(\beta^i)=0\}$ is referred to as the *defining set* of $\mathcal{C}$.

Write $A \setminus B := \{x \in A : x \notin B\}$ and $e := \gcd(n, q-1)$.

Theorem

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$ and let S be its defining set. Then the code $\mathcal{C}$ has one-dimensional hull if and only if there is a unique integer i with $0 \leq i \leq e-1$ such that $S \setminus (-S) = \{\frac{in}{e}\}$, where $-S = \{n - i : i \in S\}$.

Remark

We have

$$S \setminus (-S) = \{\frac{in}{e}\} \Rightarrow e \geq 3 \text{ and } i \neq \frac{e}{2} \text{ if } e \text{ is even.}$$

Corollary

There is no binary and ternary cyclic codes with one-dimensional hull.

The generator polynomials are used to show the sufficient and necessary conditions for cyclic codes having one-dimensional hulls.

Theorem

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$ with the generator polynomial $g(x)$. Suppose that $e = gcd(n, q-1) \geq 3$. Then the code $\mathcal{C}$ has one-dimensional hull if and only if there is a unique integer i with $1 \leq i \leq e-1$ ($i \neq \frac{e}{2}$ if e is even) such that $\frac{g(x)}{m_{\frac{in}{e}}(x)}$ is self-reciprocal, or equivalently, $g(x)m_{\frac{(e-i)n}{e}}(x)$ is self-reciprocal.

Theorem

Every cyclic code $\mathcal{C}$ with one-dimensional hull contains an LCD code and is also contained in another LCD code, i.e., there exist two LCD codes $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\mathcal{C}_1 \subset \mathcal{C} \subset \mathcal{C}_2$.

Proof.

Suppose that $\mathcal{C}$ has generator polynomial $g(x)$. Then there is a unique integer i with $1 \leq i \leq e-1$ ($i \neq \frac{e}{2}$ if e is even) such that both $\frac{g(x)}{m_{\frac{in}{e}}(x)}$ and $g(x)m_{\frac{(e-i)n}{e}}(x)$ are self-reciprocal. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two cyclic codes with generator polynomials $g(x)m_{\frac{(e-i)n}{e}}(x)$ and $\frac{g(x)}{m_{\frac{in}{e}}(x)}$, respectively. It is clear that $\mathcal{C}_1$ and $\mathcal{C}_2$ are LCD codes. The desired result is then obtained. □

[1] E. F. Assmus and J. D. Key, "Affine and projective planes," Discrete Math., vol. 83, pp. 161–187, 1990.

[2] D. Ghinelli, J. D. Key, T. P. McDonough, "Hulls of codes from incidence matrices of connected regular graphs," *Des. Codes and Cryptogr.*, vol. 70, pp. 35–54, 2014.

[3] S. L. Ma, "A survey of partial difference sets," *Des. Codes and Cryptogr.*, vol. 4, pp. 221-261, 1994.

[4] E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, "Hulls of cyclic and negacyclic codes over finite fields," *Finite Fields Appl.*, vol. 33, pp. 232–257, 2015.

[5] G. Skersys, "The average dimension of the hull of cyclic codes," *Discrete Appl. Math.*, vol. 128, no. 1, pp. 275–292, 2003.

Thanks very much for your attention!