Construction of MDS codes with complementary dual

Lingfei Jin

Fudan University

@IMS Workshop, Singapore

2016.9.28

Outline

- Background
- Results on generalized Reed-Solomon codes
- Dual codes of GRS codes
- Our construction

Background

- Linear codes with complementary dual(LCD codes) were introduced by Massey in 1992. The author showed there exists asymptotically good LCD codes.
- In 2004, Sendrier showed that LCD codes meet the asymptotic Gilbert-Varshamov bound.
- Tzeng and Hartmann proved that the minimum distance of a class of reversible cyclic codes is greater than the BCH bound .

Background

- Linear codes with complementary dual(LCD codes) were introduced by Massey in 1992. The author showed there exists asymptotically good LCD codes.
- In 2004, Sendrier showed that LCD codes meet the asymptotic Gilbert-Varshamov bound.
- Tzeng and Hartmann proved that the minimum distance of a class of reversible cyclic codes is greater than the BCH bound .

Known results on LCD

- In 1994, Yang and Massey gave a necessary and sufficient condition under which a cyclic code to have a complementary dual;
- In 2009, Esmaeili and Yari analysed LCD codes that are quasi-cyclic;
- In 2016, Dougherty et al developed a linear programming bound on the largest size of an LCD code of given length and minimum distance.

Known results on LCD

- In 1994, Yang and Massey gave a necessary and sufficient condition under which a cyclic code to have a complementary dual;
- In 2009, Esmaeili and Yari analysed LCD codes that are quasi-cyclic;
- In 2016, Dougherty et al developed a linear programming bound on the largest size of an LCD code of given length and minimum distance.

Motivation

LCD codes have application against Side-Channel Attack(SCA).

SCA: attack based on information gained from the physical implementation of a cryptosystem, such as timing information, power consumption, electromagnetic leaks or even sound which can be exploited to break the system.

SCA includes:

- Timing attack–attacks based on measuring how much time various computations take to perform.
- Power-monitoring attack–attacks that make use of varying power consumption by the hardware during computation.
- Electromagnetic attack–attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information.

LCD for countermeasure to SCA

SCA rely on the relationship between information leaked through a side channel and the secret data, there are two main countermeasures:

(1) eliminate or reduce the release of such information

(2) eliminate the relationship between the leaked information and the secret data.

A typical technique for (2) is known as masking. The actual operation is carried on a randomized version of the (masked)data.

LCD for countermeasure to SCA

SCA rely on the relationship between information leaked through a side channel and the secret data, there are two main countermeasures:

(1) eliminate or reduce the release of such information

(2) eliminate the relationship between the leaked information and the secret data.

A typical technique for (2) is known as masking. The actual operation is carried on a randomized version of the (masked)data.

LCD for countermeasure to SCA

SCA rely on the relationship between information leaked through a side channel and the secret data, there are two main countermeasures:

(1) eliminate or reduce the release of such information

(2) eliminate the relationship between the leaked information and the secret data.

A typical technique for (2) is known as masking. The actual operation is carried on a randomized version of the (masked)data.

Motivation

- LCD codes can be used in the method called Orthogonal Direct Sum Masking.
- Having C be LCD of greatest possible minimum distance simultaneously improves the resistance against SCA (FIA).

Other applications: data storage, communication systems.

- **Purpose:** Study of linear codes that are both MDS and LCD. These codes are called LCD MDS codes.
- LCD MDS codes are of both theoretical and practical importance.

SECTION 2: Some results on GRS codes

- $\mathbb{F}_q$: finite field of q elements.
- $[n, k]_q$ **linear code:** a k-dimensional subspace of $\mathbb{F}_q^n$.
- **Minimum distace** d : can correct at most $\lfloor \frac{d-1}{2} \rfloor$ errors.
- Define $C^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n : \quad \mathbf{x} \cdot \mathbf{c} = 0, \forall \mathbf{c} \in C\}$
- If $C \subseteq C^{\perp}$, then it is called self-orthogonal. It is called self-dual when the equality holds.
- LCD code: $C \cap C^{\perp} = \{\mathbf{0}\}$.

- $\mathbb{F}_q$: finite field of q elements.
- $[n,k]_q$ **linear code:** a k-dimensional subspace of $\mathbb{F}_q^n$.
- **Minimum distace** d : can correct at most $\lfloor \frac{d-1}{2} \rfloor$ errors.
- Define $C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n : \quad \mathbf{x} \cdot \mathbf{c} = 0, \forall \mathbf{c} \in C\}$
- If $C \subseteq C^\perp$, then it is called self-orthogonal. It is called self-dual when the equality holds.
- LCD code:$C \cap C^\perp = \{\mathbf{0}\}$.

MDS codes

- **Singleton Bound:** $d \leq n - k + 1$.
- If the equality holds, then it is called an MDS code.

- MDS conjecture: $n \leq q + 1$ expect when q is even and $k = 3$ or $k = q - 1$ in which case $n \leq q + 2$

- MDS codes with certain properties have been well studied for many applications (self-dual, self-orthogonal).

MDS codes

- **Singleton Bound:** $d \leq n - k + 1$.
- If the equality holds, then it is called an MDS code.
- MDS conjecture: $n \leq q + 1$ expect when q is even and $k = 3$ or $k = q - 1$ in which case $n \leq q + 2$
- MDS codes with certain properties have been well studied for many applications (self-dual, self-orthogonal).

Backgrounds on GRS codes

- Generalized Reed-Solomon code GRS($\mathbf{a}, (k-1)\infty, \mathbf{v}$):

$$\{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) : \ f(x) \in \mathbb{F}_q[x], \ \deg(f(x)) \le k-1\}. \qquad (1)$$

where $\mathbf{v} = (v_1, v_2, \dots, v_n)$ and $\mathbf{a} = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\alpha_i, i = 1, \cdots, n$ are n distinct elements in $\mathbb{F}_q$.

- It is an $[n, k]_q$ MDS code.

Another definition

For a polynomial $P(x) \in \mathbb{F}_q[x]$ with $\gcd(P(x), \prod_{i=1}^{n}(x-\alpha_i)) = 1$, define the code

$$\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v}) := \left\{ \left(\frac{v_1 f(\alpha_1)}{P(\alpha_1)}, \ldots, \frac{v_n f(\alpha_n)}{P(\alpha_n)} \right) : \ f \in \mathbb{F}_q[x];\ \deg(f) < \deg(P) \right\}. \tag{2}$$

- If $\deg(P) = k (0 \le k \le n)$, then

$$\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v}) = \mathrm{GRS}(\mathbf{a}, (k-1)\infty, \mathbf{u})$$

where $\mathbf{u} = (u_1, \ldots, u_n)$ with $u_i = \frac{v_i}{P(\alpha_i)}$.

Another definition

For a polynomial $P(x) \in \mathbb{F}_q[x]$ with $\gcd(P(x), \prod_{i=1}^{n}(x-\alpha_i)) = 1$, define the code

$$\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v}) := \left\{ \left(\frac{v_1 f(\alpha_1)}{P(\alpha_1)}, \ldots, \frac{v_n f(\alpha_n)}{P(\alpha_n)} \right) : \ f \in \mathbb{F}_q[x];\ \deg(f) < \deg(P) \right\}. \tag{2}$$

- If $\deg(P) = k (0 \le k \le n)$, then

$$\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v}) = \mathrm{GRS}(\mathbf{a}, (k-1)\infty, \mathbf{u})$$

where $\mathbf{u} = (u_1, \ldots, u_n)$ with $u_i = \frac{v_i}{P(\alpha_i)}$.

Now we are going to show that two GRS codes are disjoint under following condition.

Lemma

Let $P(x), Q(x)$ be two polynomials satisfying

(i) $\gcd(P, Q) = 1$;

(ii) $\gcd(P(x)Q(x), \prod_{i=1}^{n}(x - \alpha_i)) = 1$;

(iii) $\deg(P) + \deg(Q) \leq n$,

Then $\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v}) \cap \mathrm{GRS}(\mathbf{a}, Q(x), \mathbf{v}) = \{\mathbf{0}\}$.

SECTION 3: Duals of GRS codes

The dual $\mathrm{GRS}(\mathbf{a},(k-1)\infty,\mathbf{v})^{\perp}=\mathrm{GRS}(\mathbf{a},(n-k-1)\infty,\mathbf{u})$, where $\mathbf{u}$ is a nonzero (with all elements nonzero) solution of the system

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \cdots & v_n\alpha_n^2 \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ v_1\alpha_1^{n-2} & v_2\alpha_2^{n-2} & \cdots & v_n\alpha_n^{n-2} \end{pmatrix} \mathbf{x}^T=\mathbf{0}. \tag{3}$$

- $u_i=v_i^{-1}\prod_{1\le j\le n, j\ne i}(\alpha_i-\alpha_j)^{-1}$.

The dual $\mathrm{GRS}(\mathbf{a}, (k-1)\infty, \mathbf{v})^{\perp} = \mathrm{GRS}(\mathbf{a}, (n-k-1)\infty, \mathbf{u})$, where $\mathbf{u}$ is a nonzero (with all elements nonzero) solution of the system

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \cdots & v_n\alpha_n^2 \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ v_1\alpha_1^{n-2} & v_2\alpha_2^{n-2} & \cdots & v_n\alpha_n^{n-2} \end{pmatrix} \mathbf{x}^T = \mathbf{0}. \qquad (3)$$

- $u_i = v_i^{-1} \prod_{1 \le j \le n, j \ne i} (\alpha_i - \alpha_j)^{-1}$.

Lemma

For $0 \le k \le n$, $\mathrm{GRS}(\mathbf{a}, (k-1)\infty, \mathbf{1})^{\perp} = \mathrm{GRS}(\mathbf{a}, (n-k-1)\infty, \mathbf{u})$*, where* $\mathbf{1}$ *stands for the all-one vector and* $\mathbf{u} = (u_1, \ldots, u_n)$ *with* $u_j = \frac{1}{\prod_{1 \le i \le n, i \ne j}(\alpha_j - \alpha_i)}$ *for* $j = 1, 2, \ldots, n$.

Recall that

$$\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v}) = \left\{ \left(\frac{v_1}{P(\alpha_1)} c_1, \ldots, \frac{v_n}{P(\alpha_n)} c_n \right) : (c_1, \ldots, c_n) \in \mathrm{GRS}(\mathbf{a}, (k-1)\infty, \mathbf{1}) \right\}.$$

Corollary

Let $k = \deg(P)$ *with* $0 \le k \le n$. *Then* $\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v})^{\perp} = \mathrm{GRS}(\mathbf{a}, (n-k-1)\infty, \mathbf{u})$, *where* $\mathbf{u} = (u_1, \ldots, u_n)$ *with* $u_j = \frac{P(\alpha_j)}{v_j} \times \frac{1}{\prod_{1 \le i \le n, i \ne j} (\alpha_j - \alpha_i)}$ *for* $j = 1, 2, \ldots, n$.

SECTION 4: Our Construction

Now we give some sufficient condition under which the codes $\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v})$ are LCD MDS codes. i.e.,

$$\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v}) \cap \mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v})^{\perp} = \{\mathbf{0}\}$$

It is shown that under certain conditions

$$\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v}) \cap \mathrm{GRS}(\mathbf{a}, Q(x), \mathbf{v}) = \{\mathbf{0}\}$$

We know that

$$\mathrm{GRS}(\mathbf{a}, Q(x), \mathbf{v}) = \mathrm{GRS}(\mathbf{a}, (n-k-1)\infty, \mathbf{w})$$

with $\mathbf{w} = (w_1, \ldots, w_n)$ and $w_i = \frac{v_i}{Q(\alpha_i)}$ for all $i = 1, 2, \ldots, n$.

$$\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v})^{\perp} = \mathrm{GRS}(\mathbf{a}, (n-k-1)\infty, \mathbf{u})$$

with $\mathbf{u} = (u_1, \ldots, u_n)$ and $u_j = \frac{P(\alpha_j)}{v_j} \times \frac{1}{\prod_{1 \le i \le n, i \neq j}(\alpha_j - \alpha_i)}$ for all $j = 1, 2, \ldots, n$.

Theorem

Let $\{\alpha_1, \ldots, \alpha_n\}$ *be* n *distinct elements. Let* $P(x), Q(x)$ *be two polynomials satisfying:*

(i) $\gcd(P, Q) = 1$ *and* $\gcd(PQ, \prod_{i=1}^{n}(x - \alpha_i)) = 1$;

(ii) $\deg(P) + \deg(Q) = n$;

(iii) $\frac{P(\alpha_j)Q(\alpha_j)}{\prod_{1 \le i \le n, i \ne j}(\alpha_j - \alpha_i)} = v_j^2$, *for every* $1 \le j \le n$.

Then $\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v})$ *is an* $[n, k]_q$*-LCD MDS code, where* $k = \deg(P)$*. Furthermore,* $\mathrm{GRS}(\mathbf{a}, Q(x), \mathbf{v})$ *is the dual code of* $\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v})$*.*

- The above idea also works for GRS codes of length $q + 1$ by adding a point at infinity.

Theorem

Let $\{\alpha_1, \ldots, \alpha_n\}$ be n distinct elements. Let $P(x), Q(x)$ be two polynomials satisfying:

(i) $\gcd(P, Q) = 1$ *and* $\gcd(PQ, \prod_{i=1}^{n}(x - \alpha_i)) = 1$;

(ii) $\deg(P) + \deg(Q) = n$;

(iii) $\frac{P(\alpha_j)Q(\alpha_j)}{\prod_{1 \le i \le n, i \ne j}(\alpha_j - \alpha_i)} = v_j^2$, *for every* $1 \le j \le n$.

Then $\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v})$ *is an* $[n, k]_q$*-LCD MDS code, where* $k = \deg(P)$. *Furthermore,* $\mathrm{GRS}(\mathbf{a}, Q(x), \mathbf{v})$ *is the dual code of* $\mathrm{GRS}(\mathbf{a}, P(x), \mathbf{v})$.

- The above idea also works for GRS codes of length $q + 1$ by adding a point at infinity.

For even q

If q is even then every element of $\mathbb{F}_q$ is a square.

Theorem

If q is even and $n \le q$, then for any k with $0 \le k \le n$ there exists a q-ary $[n, k]$ LCD MDS code.

For odd q

Next we consider the case where q is odd.

Theorem

If q is an odd square and $n \leq \sqrt{q}$, then for any k with $0 \leq k \leq n$, there exists a q-ary $[n, k]$ LCD MDS code.

For sufficiently large q

- For any given $2n$ and prime power q, if $q \geq 4^{2n} \times 2n^2$, then there exists a subset $S = \{\alpha_1, \alpha_2, \ldots, \ldots, \alpha_{2n}\}$ of $\mathbb{F}_q$ such that $\alpha_j - \alpha_i$ are nonzero square elements for all $1 \leq i < j \leq m$.
- $q \equiv 1 \bmod 4$, -1 is a square. Then $\alpha_i - \alpha_j$ are nonzero square elements

Put $P(x) = \prod_{i=1}^{k}(x - \alpha_{n+i})$,$Q(x) = \prod_{i=1}^{n-k}(x - \alpha_{n+k+i})$. Then $P(\alpha_j)Q(\alpha_j)$ is a square in $\mathbb{F}_q$ for every $1 \leq j \leq n$.

Theorem

If n and q satisfy that q is odd, $q \equiv 1 \bmod 4$, and $q \geq 4^{2n} \times (2n)^2$, then for any $0 \leq k \leq n$ there exists a q-ary $[n, k]$ LCD MDS.

For sufficiently large q

- For any given $2n$ and prime power q, if $q \geq 4^{2n} \times 2n^2$, then there exists a subset $S = \{\alpha_1, \alpha_2, \ldots, \ldots, \alpha_{2n}\}$ of $\mathbb{F}_q$ such that $\alpha_j - \alpha_i$ are nonzero square elements for all $1 \leq i < j \leq m$.
- $q \equiv 1 \bmod 4$, -1 is a square. Then $\alpha_i - \alpha_j$ are nonzero square elements

Put $P(x) = \prod_{i=1}^{k}(x - \alpha_{n+i})$,$Q(x) = \prod_{i=1}^{n-k}(x - \alpha_{n+k+i})$. Then $P(\alpha_j)Q(\alpha_j)$ is a square in $\mathbb{F}_q$ for every $1 \leq j \leq n$.

Theorem

If n and q satisfy that q is odd, $q \equiv 1 \bmod 4$, and $q \geq 4^{2n} \times (2n)^2$, then for any $0 \leq k \leq n$ there exists a q-ary $[n, k]$ LCD MDS.

Main Result

Theorem (Main Result)

Let q be a prime power and let $k \geq 0$ and $n \geq 1$ be two integers. Then there exists a q-ary $[n, k]$ LCD MDS code whenever one of the following conditions is satisfied.

(i) *q is even, $n \leq q + 1$ and $0 \leq k \leq n$;*

(ii) *q is an odd square, $n \leq \sqrt{q} + 1$ and $0 \leq k \leq n$;*

(iii) *q is odd, $n = q + 1$ and even k with $4 \leq k \leq n - 4$;*

(iv) *q is odd, $q \equiv 1 \bmod 4$, and $q \geq 4^{2n} \times (2n)^2$, $0 \leq k \leq n$.*

Thank you !