Construction of Galois LCD MDS Codes

HABIBUL ISLAM

(Joint work with **Anna-Lena Horlemann**)

School of Computer Science
University of St Gallen

RICCOTA2023, 3-7 July, Rijeka

Outline

Basic definitions and results

- **Generalized Reed-Solomon Code:** Let $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_{q^m}^n$ where $\alpha_i \neq \alpha_j$ for all i, j, and $\boldsymbol{v} = (v_1, \cdots, v_n) \in \mathbb{F}_{q^m}^n$, where $v_i \neq 0$. For $1 \leq k \leq n$, GRS code of length n associated to $\boldsymbol{\alpha}, \boldsymbol{v}$ is defined by

$$GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) := \left\{ (v_1 f(\alpha_1), \cdots, v_n f(\alpha_n)) : \deg f(x) \leq k-1 \right\}$$

$\boldsymbol{\alpha} :=$ code locator, $\boldsymbol{v} :=$ column multiplier

Basic definitions and results

- **Generalized Reed-Solomon Code:** Let $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_{q^m}^n$ where $\alpha_i \neq \alpha_j$ for all i, j, and $\boldsymbol{v} = (v_1, \cdots, v_n) \in \mathbb{F}_{q^m}^n$, where $v_i \neq 0$. For $1 \leq k \leq n$, GRS code of length n associated to $\boldsymbol{\alpha}, \boldsymbol{v}$ is defined by

$$GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) := \left\{(v_1 f(\alpha_1), \cdots, v_n f(\alpha_n)) : \deg f(x) \leq k-1\right\}$$

  $\boldsymbol{\alpha}$:= code locator, $\boldsymbol{v}$:= column multiplier

- **Extended GRS Code:** Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{q^m}) = \mathbb{F}_{q^m}$, and $\boldsymbol{v} = (v_1, \ldots, v_{q^m})$, $v_i \neq 0$. The extended GRS code of lenght $q^m + 1$ based on $\boldsymbol{\alpha}, \boldsymbol{v}$ is defined by

$$GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}, \infty) := \left\{(v_1 f(\alpha_1), \cdots, v_{q^m} f(\alpha_{q^m}), f_{k-1}) : \deg f(x) \leq k-1\right\}$$

  where f_{k-1} is the coefficient of x^{k-1} in $f(x)$.

Basic definitions and results

- **Galois inner product:*** Let $0 \leq e \leq n-1$ and $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$, $\boldsymbol{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_{q^m}^n$, the *e-Galois inner product* is defined by

$$\boldsymbol{x} \cdot_e \boldsymbol{y} := \sum_{i=0}^{n-1} x_i y_i^{q^e}. \tag{1}$$

  It is the Euclidean for $e = 0$, and Hermitian inner product for $e = \frac{n}{2}$.

*Y. Fan and L. Zhang, Galois self-dual constacyclic codes, Des. Codes Cryptogr., vol. 84, no. 3, pp. 473–492, 2017.

Basic definitions and results

- **Galois Dual:**
  $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp_e} := \{\boldsymbol{x} \in \mathbb{F}_{q^m}^n : \boldsymbol{x} \cdot_e \boldsymbol{y} = 0 \text{ for all } \boldsymbol{y} \in GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})\}$
- **Galois LCD:** if $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) \cap GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp_e} = \{0\}$.
- Galois LCD codes are used to construct entanglement-assisted quantum error-correcting codes[†].

[†]X. Liu, H. Liu and L. Yu. New EAQEC codes constructed from Galois LCD codes. Quantum Inf Process, 20, 2020 https://doi.org/10.1007/s11128-019-2515-z.

Basic definitions and results

Question

How we can construct new Galois LCD MDS codes?

[‡]C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. *IEEE Trans. Inf. Theory*, **64**: 3010–3017, 2018

[§]C. Carlet, S. Mesnager, C. Tang and Y. Qi. On σ-LCD codes. *IEEE Trans. Inf. Theory*, **65**: 1694–1704, 2019.

Basic definitions and results

Question

How we can construct new Galois LCD MDS codes?

- The problem has been solved completely for **Euclidean** and **Hermitian** product [‡]
- A linear code $[n, k]$ is equivalent to a σ-LCD code. But σ can never be the Galois product, except in the trivial Euclidean case [§]

[‡] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. *IEEE Trans. Inf. Theory*, **64**: 3010–3017, 2018

[§] C. Carlet, S. Mesnager, C. Tang and Y. Qi. On σ-LCD codes. *IEEE Trans. Inf. Theory*, **65**: 1694–1704, 2019.

Basic definitions and results

Question

How we can construct new Galois LCD MDS codes?

- The problem has been solved completely for **Euclidean** and **Hermitian** product [‡]
- A linear code $[n, k]$ is equivalent to a σ-LCD code. But σ can never be the Galois product, except in the trivial Euclidean case [§]
- Still open for **Galois** product.

We do: Find suitable $\boldsymbol{\alpha}, \boldsymbol{v}$ and construct $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$

[‡] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. *IEEE Trans. Inf. Theory*, **64**: 3010–3017, 2018

[§] C. Carlet, S. Mesnager, C. Tang and Y. Qi. On σ-LCD codes. *IEEE Trans. Inf. Theory*, **65**: 1694–1704, 2019.

Construction

Lemma 1

[a] Let $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ be a GRS code of length n over $\mathbb{F}_{q^m}$. Then $\boldsymbol{c} = (v_1 f(\alpha_1), \cdots, v_n f(\alpha_n)) \in GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) \cap GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp_e}$ if and only if there exists a polynomial $g(x) \in \mathbb{F}_{q^m}[x]$ with $\deg g(x) \leq n-k-1$ such that

$$\left(v_1^{q^e+1} f^{q^e}(\alpha_1), \cdots, v_n^{q^e+1} f^{q^e}(\alpha_n)\right) = \left(u_1^{-1} g(\alpha_1), \cdots, u_n^{-1} g(\alpha_n)\right) \quad (2)$$

where $u_i = \prod_{1 \leq j \neq i \leq n} (\alpha_i - \alpha_j)$ for all i.

---

[a] M. Cao, MDS Codes With Galois Hulls of Arbitrary Dimensions and the Related Entanglement-Assisted Quantum Error Correction, IEEE Trans. Inf. Theory, vol. 67, no. 12, pp. 7964-7984, Dec. 2021.

Construction

Lemma 2

Let $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}, \infty)$ be an extended GRS code of length $q^m + 1$ over $\mathbb{F}_{q^m}$. Then
$\boldsymbol{c} = \left(v_1 f(\alpha_1), \cdots, v_{q^m} f(\alpha_{q^m}), f_{k-1}\right) \in GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}, \infty) \cap GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}, \infty)^{\perp_e}$
if and only if there exists a polynomial $g(x) \in \mathbb{F}_{q^m}[x]$ with
$\deg g(x) \leq q^m - k$ such that

$$\left(v_1^{q^e+1} f^{q^e}(\alpha_1), \cdots, v_{q^m}^{q^e+1} f^{q^e}(\alpha_{q^m}), f_{k-1}^{q^e}\right) = \left(g(\alpha_1), \cdots, g(\alpha_{q^m}), g_{q^m-k}\right). \quad (3)$$

Construction: Class 1

Theorem 1

Let $G = \{\alpha_1, \ldots, \alpha_n\}$ be an additive subgroup of $\mathbb{F}_{q^m}$, where $n = q^t$, $1 \leq t \leq m$. Let $\boldsymbol{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$. Then there exists an e-Galois LCD $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ code of length n and dimension k where $k \leq 1 + \lfloor \frac{q^t-2}{q^e+1} \rfloor$.

Construction: Class 1

Theorem 1

Let $G = \{\alpha_1, \ldots, \alpha_n\}$ be an additive subgroup of $\mathbb{F}_{q^m}$, where $n = q^t$, $1 \leq t \leq m$. Let $\boldsymbol{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$. Then there exists an e-Galois LCD $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ code of length n and dimension k where $k \leq 1 + \lfloor \frac{q^t-2}{q^e+1} \rfloor$.

- **Value of $\boldsymbol{v}$:** We have $k < n$. Let

$$v_i = \begin{cases} 1 & \text{if } 1 \leq i \leq n-k \\ \delta & \text{if } n-k+1 \leq i \leq n \end{cases}$$

where $\delta \in \mathbb{F}_{q^m}^*$ such that $o(\delta) \nmid (q^e + 1)$.

Let $\boldsymbol{v} = (v_1, \ldots, v_{n-k}, v_{n-k+1}, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$.

- $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ is e-Galois LCD.

Construction: Class 2

Theorem 2

Let q be odd prime. There exists an e-Galois LCD $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ code of length n and dimension $q^m - n$ where $q^m \geq n \geq \lceil \frac{q^{m+e}+1-q^e}{q^e+1} \rceil$.

Construction: Class 2

Theorem 2

Let q be odd prime. There exists an e-Galois LCD $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ code of length n and dimension $q^m - n$ where $q^m \geq n \geq \lceil \frac{q^{m+e}+1-q^e}{q^e+1} \rceil$.

- **Values of $\boldsymbol{\alpha}$, $\boldsymbol{v}$:**

  Let $\mathbb{F}_{q^m} = \{\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_{q^m}\}$.

  Let $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where $\alpha_i \neq \alpha_j$ for all $i \neq j$ and $\boldsymbol{v} = (v_1, \ldots, v_n)$, where $o(v_i) = 2$ for all i.

- $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ is e-Galois LCD.

Construction: Class 3

Theorem 3

There exists an e-Galois LCD $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}, \infty)$ code of length $q^m + 1$ and dimension k, where $1 \leq k \leq \lfloor \frac{q^m+q^e}{q^e+1} \rfloor$.

Construction: Class 3

Theorem 3

There exists an e-Galois LCD $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}, \infty)$ code of length $q^m + 1$ and dimension k, where $1 \leq k \leq \lfloor \frac{q^m+q^e}{q^e+1} \rfloor$.

- **Values of $\boldsymbol{\alpha}, \boldsymbol{v}$:** Let $\mathbb{F}_{q^m} = \{\alpha_1, \alpha_2, \ldots, \alpha_{q^m}\} = \boldsymbol{\alpha}$.
- When $q^e(k-1) < q^m - k$

  Let

$$v_i = \begin{cases} 1 & \text{if } 1 \leq i \leq q^m - k + 1 \\ \delta & \text{if } q^m - k + 2 \leq i \leq q^m \end{cases}$$

  where $o(\delta) \nmid (q^e + 1)$. Let $\boldsymbol{v} = (v_1, \ldots, v_{q^m})$
- $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ is e-Galois LCD.

Construction: Class 3

- When $q^e(k-1) = q^m - k$

  Let

$$v_i = \begin{cases} 1 & \text{if } 1 \leq i \leq q^m - k \\ \delta & \text{if } q^m - k + 1 \leq i \leq q^m \end{cases}$$

  where $o(\delta) \nmid (q^e + 1)$. Let $\boldsymbol{v} = (v_1, \ldots, v_{q^m})$

- $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ is e-Galois LCD.

Conclusion

We obtained three classes of Galois LCD MDS codes over $\mathbb{F}_{q^m}$ of parameters

1. $[q^t, k, d]$ where $1 \leq t \leq m$ and $k \leq 1 + \lfloor \frac{q^t-2}{q^e+1} \rfloor$.
2. $[n, q^m - n, d]$ where $\lceil \frac{q^{m+e}+1-q^e}{q^e+1} \rceil \leq n \leq q^m$.
3. $[q^m + 1, k, d]$ where $1 \leq k \leq \lfloor \frac{q^m+q^e}{q^e+1} \rfloor$.

Conclusion

We obtained three classes of Galois LCD MDS codes over $\mathbb{F}_{q^m}$ of parameters

1. $[q^t, k, d]$ where $1 \leq t \leq m$ and $k \leq 1 + \lfloor \frac{q^t-2}{q^e+1} \rfloor$.
2. $[n, q^m - n, d]$ where $\lceil \frac{q^{m+e}+1-q^e}{q^e+1} \rceil \leq n \leq q^m$.
3. $[q^m + 1, k, d]$ where $1 \leq k \leq \lfloor \frac{q^m+q^e}{q^e+1} \rfloor$.

Find different $\boldsymbol{\alpha}$, and $\boldsymbol{v}$ to define Galois LCD GRS codes $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$.

Conclusion

We obtained three classes of Galois LCD MDS codes over $\mathbb{F}_{q^m}$ of parameters

1. $[q^t, k, d]$ where $1 \leq t \leq m$ and $k \leq 1 + \lfloor \frac{q^t-2}{q^e+1} \rfloor$.
2. $[n, q^m - n, d]$ where $\lceil \frac{q^{m+e}+1-q^e}{q^e+1} \rceil \leq n \leq q^m$.
3. $[q^m + 1, k, d]$ where $1 \leq k \leq \lfloor \frac{q^m+q^e}{q^e+1} \rfloor$.

Find different $\boldsymbol{\alpha}$, and $\boldsymbol{v}$ to define Galois LCD GRS codes $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$.

THANK YOU FOR YOUR ATTENTION !