New Constructions of Self-dual MDS Codes

Jinquan Luo

Joint work with **Khawla Labad** and **Hongwei Liu**

School of Mathematics and Statistics
Central China Normal University

The 5th Sino-Korea International Conference
on Coding Theory and Its Related Topics

Outline

- Background
- Generalized Reed-Solomn codes
- Extended generalized Reed-Solomn codes
- Constructions based on multiplicative structure of $\mathbb{F}_q^*$
- Constructions based on hybird structure of $\mathbb{F}_q^*$

Background

- $\mathbb{F}_q$: finite field with q elements.

- A linear $[n, k, d]$ code over a finite field $\mathbb{F}_q$ of length n, dimension k and minimum distance d is called MDS (maximum distance separable) if it attains the Singleton bound: $d = n - k + 1$.

- The dual of the linear code C (under Euclidean inner product) is

$$C^{\perp} = \left\{(v_1, \cdots, v_n) \in \mathbb{F}_q^n : c_1 v_1 + \cdots + c_n v_n = 0 \text{ for any } (c_1, \cdots, c_n) \in C\right\}.$$

- C is called self-dual if $C = C^{\perp}$.

Background

- In general, it is hard to determine the minimal distance of self-dual code.

- Linea code C is MDS self-dual if it is both MDS and self-dual.

- Parameters of MDS self-dual code are completely characterized by its length: $[n, \frac{n}{2}, \frac{n}{2}+1]$.

Known results on MDS self-dual codes of length n:
(η is the quadratic multiplicative character on $\mathbb{F}_q$)

q	length n (even)	Reference
$q = 2^m$	$n \leq q + 1$	[4]
q odd	$(n-1)\|(q-1), \eta(1-n) = 1$	[8]
q odd	$(n-2)\|(q-1), \eta(2-n) = 1$	[8]
$q = r^s \equiv 3 \pmod 4$	$n = p^m + 1, p \equiv 3 (\mathrm{mod}\, 4)$ odd m	[5]
$q = r^s, r \equiv 1 (\mathrm{mod}\, 4), s$ odd	$n = p^m + 1$, odd $m, p \equiv 1 (\mathrm{mod}\, 4)$	[5]
$q = r^s, s \geq 2$	$n = lr, 2l\|(r-1)$	[8]
$q = r^s, s \geq 2$	$n = lr, (l-1)\|(r-1), \eta(1-l) = 1$	[8]
$q = r^s, s \geq 2$	$n = lr + 1, l\|(r-1)$ and $\eta(l) = 1$	[8]

Known results on MDS self-dual codes of length n:

$q = r^s, s \geq 2$	$n = lr + 1, (l-1)\|(r-1), \eta(-1) = 1$	[8]
$q = r^2$	$n \leq r$	[6]
$q = r^2$	$n = 2tr$ for any $t \leq (r-1)/2$	[6], [8]
$q = r^2$,	$n = tr + 1$, odd t and $1 \leq t \leq r$	[8]
$q \equiv 1 \pmod 4$	$n\|(q-1), n < q-1$	[8]
$q \equiv 1 \pmod 4$	$4^n \cdot n^2 \leq q$	[6]
$q = p^k$	$n = p^r + 1, r\|k$	[8]
$q = p^k$	$n = 2p^e, 1 \leq e < k, \eta(-1) = 1$	[8]

There are also other schemes to produce MDS self-dual codes. In [7], Kim and Lee developed a building-up technique to produce MDS self-dual code of large length from short length.

References

[1] T. Aaron Gulliver, J.L. Kim, and Y. Lee, New MDS and near- MDS self-dual codes, *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4354–4360, Sept. 2008.

[2] K. Betsumiya, S. Georgiou, T. A. Gulliver, M. Harada, and C. Koukouvinos, On self-dual codes over some prime fields, *Discrete Math.*, vol. 262, nos. 1-3, pp. 37–58, 2003.

[3] S. Georgiou and C. Koukouvinos, MDS self-dual codes over large prime fields, *Finite Fields Their Appl.*, vol. 8, no. 4, pp. 455–470, Oct. 2002.

[4] M. Grassl and T. Aaron Gulliver, On self-dual MDS codes, *Proceedings of ISIT*, 2008, pp. 1954–1957.

[5] K. Guenda, New MDS self-dual codes over finite fields,*Designs Codes Cryptogr.*, vol. 62, no. 1, pp. 31–42, Jan. 2012.

[6] L. Jin and C. Xing, New MDS self-dual codes from generalized Reed- Solomon codes, *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1434–1438, Mar. 2017.

[7] J. L. Kim and Y. Lee, Euclidean and Hermitian self-dual MDS codes over large finite fields, *J. Combinat. Theory, Series A*, vol. 105, no. 1, pp. 79–95, Jan. 2004.

[8] H. Yan, A note on the construction of MDS self-dual codes, *Cryptogr. Commun.*, Published online, March 2018, see https://doi.org/10.1007/s12095-018-0288-3

Generalized Reed-Solomn codes

Generalized Reed-Solomn (GRS) code is a standard model of MDS codes.

- Let n be a positive integer with $1 < n \leq q$.
- Choose $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$ to be an n-tuple of distinct elements of $\mathbb{F}_q$.
- Choose $\mathbf{v} = (v_1, \ldots, v_n)$ with $v_i \in \mathbb{F}_q^*$.
- For $1 \leq k \leq q$, generalized Reed-Solomon or $\mathbf{GRS}$ code

$$\mathbf{GRS}_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) : f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k-1\}.$$

Generalized Reed-Solomn codes

- The code $\mathbf{GRS}_k(\mathbf{a}, \mathbf{v})$ has a generator matrix

$$\mathbf{G}_k(\mathbf{a}, \mathbf{v}) = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \dots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & v_n\alpha_n^{k-1} \end{pmatrix}.$$

- $\mathbf{GRS}_k(\mathbf{a}, \mathbf{v})$ is a q-ary $[n, k, n-k+1]$ (MDS) code and its dual is also MDS.

Generalized Reed-Solomn codes

- $L_{\mathbf{a}}(\alpha_i) = \prod_{1 \le j \le n, j \ne i} (\alpha_i - \alpha_j)$.
- The dual of $\mathbf{GRS}$ code is explicitly determined.

$$\mathbf{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp} = \mathbf{GRS}_{n-k}(\mathbf{a}, \mathbf{uv^{-1}})$$

where $\mathbf{uv^{-1}} = (u_1 v_1^{-1}, \ldots, u_n v_n^{-1})$ with $u_i = L_{\mathbf{a}}(\alpha_i)^{-1}$ for $1 \le i \le n$.

Generalized Reed-Solomn codes

Lemma 1. *(*J.Lin and C.Xing[1]*) For n even and $k = \frac{n}{2}$, if there exist $\lambda \in \mathbb{F}_q^*$ such that*

$$\lambda L_{\mathbf{a}}(\alpha_i) = w_i^2$$

for some $w_i \in \mathbb{F}_q^*$ for all $1 \leq i \leq n$, then the code $\mathbf{GRS}_k(\mathbf{a}, \mathbf{v})$ is MDS self-dual, where $v_i = w_i^{-1}$ for all $1 \leq i \leq n$.

[1] L.Jin and C.Xing, New MDS self-dual codes from generalized Reed- Solomon codes, *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1434–1438, Mar. 2017.

Extended generalized Reed-Solomn codes

- Choose $\mathbf{a} = (\alpha_1, \ldots, \alpha_{n-1})$ to be an $(n-1)$-tuple of distinct elements of $\mathbb{F}_q$.

- Choose $\mathbf{v} = (v_1, \ldots, v_{n-1})$ with $v_i \in \mathbb{F}_q^*$.

- Extended $\mathbf{GRS}$ code of length n and dimension k:

$$\mathbf{GRS}_k(\mathbf{a}, \mathbf{v}, \infty) = \{(v_1 f(\alpha_1), \ldots, v_{n-1} f(\alpha_{n-1}), f_{k-1}) :$$

$$f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k-1\},$$

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

- the code $\mathbf{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$ has a generator matrix

$$\mathbf{G}_k(\mathbf{a}, \mathbf{v}, \infty) = \begin{pmatrix} v_1 & v_2 & \cdots & v_{n-1} & 0 \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_{n-1}\alpha_{n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_{n-1}\alpha_{n-1}^{k-1} & 1 \end{pmatrix}.$$

- $\mathbf{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$ is a q-ary $[n, k, n-k+1]$ (MDS) code and its dual is also MDS.

Extended generalized Reed-Solomn codes

- The dual of $\mathbf{GRS}$ code is explicitly determined. Precisely,

$$\mathbf{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)^{\perp} = \mathbf{GRS}_{n-k}(\mathbf{a}, \mathbf{uv^{-1}}, \infty)$$

where $\mathbf{uv^{-1}} = (u_1 v_1^{-1}, \ldots, u_n v_n^{-1})$ with $u_i = -L_{\mathbf{a}}(\alpha_i)^{-1}$ for $1 \leq i \leq n$.

Extended generalized Reed-Solomn codes

Lemma 2. *(*H.Yan[2]*) Let n be even and $k = \frac{n}{2}$. If*

$$-L_{\mathbf{a}}(\alpha_i) = w_i^2$$

for some $w_i \in \mathbb{F}_q^*$ for all $1 \leq i \leq n-1$, then the code $\mathbf{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$ is MDS self-dual code, where $v_i = w_i^{-1}$ for all $1 \leq i \leq n-1$.

[2]H. Yan, A note on the construction of MDS self-dual codes, *Cryptogr. Commun.*, Published online, March 2018, see https://doi.org/10.1007/s12095-018-0288-3

Constructions based on multiplicative structure of $\mathbb{F}_q^*$

Theorem 1. *Let $q = r^2$ where r is odd prime power.*

- $n = tm$;
- $1 \leq t \leq \frac{r-1}{\gcd(r-1,m)}$;
- $m \mid (q-1)$.

Assume both $\frac{q-1}{m}$ and n are even. Then there exists a q-ary $[n, \frac{n}{2}]$ MDS self-dual code over $\mathbb{F}_q$.

Remark: Theorem 3.4 (i) in L.Jin and C. Xing[3] is a special case of the preceding result with $m = 1$.

[3] L.Jin and C.Xing, New MDS self-dual codes from generalized Reed- Solomon codes, *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1434–1438, Mar. 2017.

Proof: Let α be a primitive m-th root of unity.

- Group isomorphism and monomorphism

$$\mathbb{F}_r^* \Big/ (\mathbb{F}_r^* \cap \langle\alpha\rangle) \simeq (\mathbb{F}_r^* \cdot \langle\alpha\rangle) \Big/ \langle\alpha\rangle \leq \mathbb{F}_q^* \Big/ \langle\alpha\rangle$$

- Choose $\beta_i \in \mathbb{F}_r^*$ $(0 \leq i \leq t-1)$ to be cost representatives of $(\mathbb{F}_r^* \times \langle\alpha\rangle) \Big/ \langle\alpha\rangle$.

- Choose vector

$$\mathbf{a} = (\alpha\beta_0, \ldots, \alpha^m\beta_0, \alpha\beta_1, \ldots, \alpha^m\beta_1, \ldots, \alpha\beta_{t-1}, \ldots, \alpha^m\beta_{t-1}).$$

Constructions based on multiplicative structure of $\mathbb{F}_q^*$

- For any $1 \leq i \leq m$ and for any $0 \leq z \leq t-1$, we have

$$L_{\mathbf{a}}(\beta_z \alpha^i) = {\beta_z}^{m-1} \cdot m \cdot \alpha^{-i} \cdot \prod_{l=0, l \neq z}^{t-1} ({\beta_z}^m - {\beta_l}^m).$$

- Note that $\beta_z^{m-1}, \prod_{l=0,l\neq z}^{t-1} ({\beta_z}^m - {\beta_l}^m), m \in \mathbb{F}_r^* \subset \mathbb{F}_q^{*2}$ since $\mathbb{F}_{r^2} = \mathbb{F}_q$.

- α is also a square since $\frac{q-1}{m}$ is even.

Then there exists a q-ary $[n, \frac{n}{2}]$ MDS self-dual code over $\mathbb{F}_q$.

Constructions based on multiplicative structure of $\mathbb{F}_q^*$

Theorem 2. *Let $q = r^2$ where r is odd prime power.*

- $n = tm + 1$ *is even;*
- $1 \leq t \leq \frac{r-1}{\gcd(r-1,m)}$*;*
- $m \mid (q-1)$.

Then there exists a q-ary $[n, \frac{n}{2}]$ MDS self-dual code over $\mathbb{F}_q$.

Constructions based on multiplicative structure of $\mathbb{F}_q^*$

Proof. By considering extended GRS codes $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$, the proof is similar as that of Theorem 1.

- $L_{\mathbf{a}}(\beta_z \alpha^i) = {\beta_z}^{m-1} \cdot m \cdot \alpha^{-i} \cdot \prod_{l=0, l\neq z}^{t-1} ({\beta_z}^m - {\beta_l}^m)$.
- $-L_{\mathbf{a}}(\beta_z \alpha^i) \in \mathbb{F}_q^{*2}$.

There exists a q-ary $[n, \frac{n}{2}]$ MDS self-dual code over $\mathbb{F}_q$.

□

Constructions based on multiplicative structure of $\mathbb{F}_q^*$

Theorem 3. *Let $q = r^2$ where r is odd prime power.*

- *$n = tm + 2$ is even;*
- *$1 \leq t \leq \frac{r-1}{\gcd(r-1,m)}$;*
- *$m \mid (q-1)$.*

Then there exists a q-ary $[n, \frac{n}{2}]$ MDS self-dual code over $\mathbb{F}_q$.

Constructions based on multiplicative structure of $\mathbb{F}_q^*$

Proof. • The elements α and β_i are chosen in the same way as in Theorem 1.

• Define the generalized Reed-Solomn code $\mathbf{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$ with

$$\mathbf{a} = (0, \alpha\beta_0, \ldots, \alpha^m\beta_0, \alpha\beta_1, \ldots, \alpha^m\beta_1, \ldots, \alpha\beta_{t-1}, \ldots, \alpha^m\beta_{t-1}).$$

• $L_{\mathbf{a}}(\beta_z\alpha^i) = {\beta_z}^m \cdot m \cdot \prod_{l=0, l\neq z}^{t-1} ({\beta_z}^m - {\beta_l}^m)$ and $L_{\mathbf{a}}(0) = \pm \left(\prod_{l=0}^{t-1} \beta_l\right)^m$.

• Both $-L_{\mathbf{a}}(\beta_z\alpha^i)$ and $-L_{\mathbf{a}}(0)$ are in $\mathbb{F}_q^{*2}$.

There exists a q-ary MDS self-dual code of length $n = mt + 2$. □

Constructions based on hybird structure of $\mathbb{F}_q^*$

Theorem 4. *Let $q = p^m$ with p odd prime.*

- $2t \mid (p-1)$;
- $e < m$;
- $n = 2tp^e$.

If $\frac{q-1}{2t}$ is even, then there exists self-dual MDS code with length $2tp^e$.

Remark: For $t = 1$, this result is exactly Theorem 4 (ii) in Yan [4].

[4] H. Yan, A note on the construction of MDS self-dual codes, *Cryptogr. Commun.*, Published online, March 2018, see https://doi.org/10.1007/s12095-018-0288-3

Proof:

- Let V be an e-dimensional $\mathbb{F}_p$-vector subspace in $\mathbb{F}_q$ satisfying $V \cap \mathbb{F}_p = 0$.

- Denote by $\omega \in \mathbb{F}_p$ a primitive element of order $2t$.

- Choose $\mathbf{a} = \bigcup_{j=0}^{2t-1} \left(\omega^j + V\right)$.

- For any $b \in \omega^i + V$,
$$L_{\mathbf{a}}(b) = \omega^{-i} \left(\prod_{0 \neq v \in V} v \right) \cdot \left(\prod_{v \in V} \prod_{h=1}^{2t-1} \left(1 + v - \omega^h\right) \right).$$

- Denote by $c = \left(\prod_{0 \neq v \in V} v \right) \cdot \left(\prod_{v \in V} \prod_{h=1}^{2t-1} \left(1 + v - \omega^h\right) \right)$. Then $L_{\mathbf{a}}(b) = \omega^{-i} c$.

Since $\omega \in \mathbb{F}_q^{*2}$. As a consequence, $\eta\left(L_{\mathbf{a}}(b)\right) = \eta(c)$ which is independent of the choice of b. Therefore there exists self-dual MDS code with length $|\mathbf{a}| = 2tp^e$.

Conclusion

- In this talk, we present four construcitons of MDS self-dual codes based on multiplicative (and additive) structure of finite fields.

- For many fixed q, the codes in our constructions have length n which is determined by two factors. In this sense, it may produce more MDS self-dual codes than before.

  For example, for $q = 151^2$, there are (approximately?) 243 differnt n for which MDS self-dual code of lengths n are constructed in all the previous works.

  In our constructions, there are 713 different lengths n.

Thanks for your attention