New MDS Self-Dual Codes From Two Disjoint Subsets

Yuting Cao
Hefei University of Technology
Shixin Zhu (zhushixin@hfut.edu.cn)
Hefei University of Technology

Research Article

Keywords: MDS self-dual codes, Generalized Reed-Solomon codes

Posted Date: May 17th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1631791/v1

Additional Declarations: No competing interests reported.

New MDS Self-Dual Codes From Two Disjoint Subsets *

Yuting Cao · Shixin Zhu

Abstract In recent years, some new classes of MDS self-dual codes were construed. The method is to obtain new structure by generalized GRS codes. In this paper, our idea is to construct MDS self-dual codes of length n where is composed with two subgroups of F_q. In particular, these two subgroups do not intersect. Several classes of new q-ary MDS self-dual codes under specific conditions are given by considering the interval of s, t.
Keywords MDS self-dual codes · Generalized Reed-Solomon codes

1 Introduction

MDS codes are a special class of codes that satisfies the Singleton constraint and have a strong error correction capability. Especially when the code length is not too long, its performance is very close to the theoretical value. In addition, it has a good algebraic structure and is easy to construct. Since MDS codes can reach the singleton bound, they are easier to be encoded and decoded. Therefore, they have been applied to communication systems. On the other hand, scholars found various applications of self-dual codes in cryptography [10] and combinatorics [13]. Therefore, it is natural to consider the intersection of these two types of codes, i.e., MDS self-dual codes. In the past 20 years, many construction methods for MDS self-dual codes and complementary MDS self-dual codes have been given, and these construction methods can be broadly classified into the following three categories according to the tools used. (1) code-based constructions using known classical codes, i.e., stable codes, algebraic geometric codes, classical self-dual linear or symmetric codes and generalized RS codes, etc.; (2) combinatorics-based constructions; (3) algebraic-based constructions. In this paper, based on the generalized Reed-Solomon codes, we combine the knowledge of coding theory, finite fields and recent algebra to give MDS self-dual codes with new parameters under specific conditions. These constructions add new lengths of codes. Since the parameters of self-dual codes are completely determined by the code length n, construct more MDS self-dual codes of different code lengths over different finite fields or finite rings is an interest problem.

Let F_q be the finite field with q elements where q is a prime power. A linear code C over F_q, represented as $[n, k, d]_q$, is a F_q linear subspace of F_q^n having dimension k and minimum distance d. We call C a maximum distance separable (MDS) code when the parameters can attain the Singleton bound, i.e., $d = n - k + 1$. For a linear code C, we will use $C^{\perp}$ to denote the dual of C in the Euclidean inner product. A linear code C is called self-dual if $C = C^{\perp}$.

*
Shixin Zhu
zhushixin@hfut.edu.cn

Yuting Cao
caoyuting9797@163.com

School of Mathematics, Hefei University of Technology, Hefei 230601, Anhui, China

1.1 The well-known results

MDS self-dual codes constructed based on orthogonal designs [1, 2] are usually given by the construction of generating matrices over small fields to obtain MDS self-dual codes over large finite fields. Guenda used cyclic codes and negative cyclic codes to construct MDS self-dual codes in [4]. Jin and Xing first proposed a systematic approach to constructing MDS self-dual codes with GRS codes in [19]. In recent years, GRS codes are one with the most popular means of building MDS self-dual codes. In [7], MDS self-dual codes over finite fields of even characteristic with any possible parameters have been discovered. Yan [3] and Grassl et al. [14] used generalized RS codes and extended generalized RS codes to build new MDS self-dual codes, and the method was extended to GRS codes with general length. Fang et al. [8] and Lebed et al. [9] used F_q^* and its two disjoint multiplicative subgroups to build a family of new MDS self-dual codes. In [8], Zhang and Feng proposed a number of new constructions of MDS Euclidean self-dual codes via cyclotomy. In [18], Sok showed some explicit compositions of MDS Euclidean self-dual codes via rational function fields.

1.2 Our results

In our work, we obtain a few new results regarding MDS self-dual codes over finite fields via GRS codes. Some of the consequences of this paper generalize the results in [5, 9, 19].

2 Preliminaries

In this section, we will recall the basic knowledge about generalized Reed-Solomon (GRS) codes. Relevant computational formulas are also cited.

Let F_q be the finite filed where q is a prime power. For n nonzero elements v_i of F_q and n distinct elements a_i of F_q, the GRS codes associated with v_i and a_i are defined as follows:

$$GRS_k(\vec{a}, \vec{v}) = \{(v_1 f(a_1), \ldots, v_n f(a_n)) : f(x) \in F_q[x] \ and \ \deg(f(x)) \leq k-1\}.$$

It is well known that $GRS_k(\vec{a}, \vec{v})$ is a q-ary $[n, k, n-k+1]$ MDS code.

Let $\eta(x)$ be the quadratic character of F_q^*. Let QR_q be the set of all squares in F_q^*. When x is a square in F_q^*, then $\eta(x) = 1$. When x is a non-square in F_q^*, then $\eta(x) = -1$. I.e.,

$$\eta(x) = \begin{cases} 1, x \in QR_q \\ -1, x \notin QR_q \end{cases}.$$

For any subset $A \subseteq F_q$, we denote the polynomial $f_A(x)$ over F_q as

$$f_A(x) = \prod_{a \in A} (x-a).$$

For any element $a \in A$, we denote

$$\delta_A(a) = \prod_{a' \in A, a' \neq a} (a - a').$$

Table 1 The known results of MDS self-dual codes

q	n even	Reference
q even	$n \leq q$	[14]
q odd	$n = q + 1$	[14]
q odd	$(n-1) \mid (q-1), \eta(1-n) = 1$	[3]
q odd	$(n-2) \mid (q-1), \eta(2-n) = 1$	[3]
$q \equiv 3 (\mathrm{mod}\ 4)$	$n \equiv 0 (\mathrm{mod}\ 4), (n-1) \mid (q-1)$	[9]
$q \equiv 1 (\mathrm{mod}\ 4)$	$(n-1) \mid (q-1)$	[9]
$q \equiv 1 (\mathrm{mod}\ 4)$	$n = 2p^l, l \leq m$	[7]
$q \equiv 1 (\mathrm{mod}\ 4)$	$n = p^l + 1, l \leq m$	[7]
$q = r^2$	$n \leq r$	[15]
$q = r^2, q \equiv 3 (\mathrm{mod}\ 4)$	$n = 2tr$, for any $t \leq \frac{r-1}{2}$	[15]
$q = r^2$	$n = tr$, even t, $1 \leq t \leq r$	[3]
$q = r^2$	$n = tr + 1$, odd t, $1 \leq t \leq r$	[3]
$q = r^2$	$n = tm$, $1 \leq t \leq \frac{r-1}{\gcd(r-1,m)}$, even $\frac{q-1}{m}$	[11]
$q = r^2$	$n = tm + 1$, even tm and $1 \leq t \leq \frac{r-1}{\gcd(r-1,m)}, m \mid q-1,$	[11]
$q = r^2$	$n = tm + 2$, odd tm and $1 \leq t \leq \frac{r-1}{\gcd(r-1,m)}, m \mid q-1,$	[11]
$q = r^s, q \equiv 3 (\mathrm{mod}\ 4)$	$n - 1 = p^m \mid q-1, p \equiv 3 (\mathrm{mod}\ 4)$, odd m	[4]
$q = r^s, r \equiv 1 (\mathrm{mod}\ 4)$, odd s	$n - 1 = p^m \mid q-1, p \equiv 1 (\mathrm{mod}\ 4)$, odd m	[4]
$q = r^s$, odd r, $s \geq 2$	$n = lr + 1$, odd l, $l \mid r-1$, $\eta(l) = 1$	[3]
$q = r^s$, odd r, $s \geq 2$	$n = lr + 1$, odd l, $l-1 \mid r-1$, $\eta(l-1) = -1$	[3]
$q = r^s$, odd r, $s \geq 2$	$n = lr$, even l, $2l \mid r-1$	[3]
$q = r^s$, odd r, $s \geq 2$	$n = lr$, even l, $l-1 \mid r-1$, $\eta(1-l) = 1$	[3]
$q = p^k$, odd prime p	$n = p^r + 1$, $r \mid k$	[3]
$q = p^k$, odd prime p	$n = 2p^e$, $1 \leq e$	[3]
$q = p^m$, odd prime p	$n = 2tp^e$, $2t \mid p-1$, $e < m$, even $q-1 \mid 2t$	[11]
$q = p^m$, even m, odd prime p	$n = 2tr^l$, $r = p^s$, $s \mid \frac{m}{2}$, $0 \leq t \leq \frac{m}{s}$, $1 \leq t \leq \frac{r-1}{2}$	[7]
$q = p^m$, even m, odd prime p	$n = (2t+1)r^l + 1, r = p^s, s \mid \frac{m}{2}$ and $0 \leq t \leq \frac{m}{s}, 1 \leq t \leq \frac{r-1}{2}$ or, $l = \frac{m}{s}, t = 0$	[7]
$q = p^m \equiv 1 (\mathrm{mod}\ 4)$	$n = p^l + 1$, $0 \leq l \leq m$	[7]
$q = r^2, r \equiv 1 (\mathrm{mod}\ 4)$	$n = s(r-1) + t(r+1), 1 \leq s \leq \frac{r+1}{2}$ and $1 \leq t \leq \frac{r-1}{2}$, even s	[9]
$q = r^2, r \equiv 3 (\mathrm{mod}\ 4)$	$n = s(r-1) + t(r+1), 1 \leq s \leq \frac{r+1}{2}$ and $1 \leq t \leq \frac{r-1}{2}$, odd s	[9]
$q = r^2, r \equiv 1 (\mathrm{mod}\ 4)$	$n = s\frac{q-1}{a} + t\frac{q-1}{b}, a \equiv 2 (\mathrm{mod}\ 4)$, even s and $1 \leq s \leq \frac{a}{\gcd(a,b)}, 1 \leq t \leq \frac{b}{\gcd(a,b)}$	[19]
$q = r^2, r \equiv 3 (\mathrm{mod}\ 4)$	$n = s\frac{q-1}{a} + t\frac{q-1}{b}, b \equiv 2 (\mathrm{mod}\ 4)$, odd $\frac{(r+1)b}{2a}s^2$ and $1 \leq s \leq \frac{a}{\gcd(a,b)}, 1 \leq t \leq \frac{b}{\gcd(a,b)}$	[19]

Table 2 Our new MDS self-dual codes

q	n even	Reference
$q=r^2, r\equiv 1(\text{mod}4)$	$n=s\frac{r+1}{b_1}+t\frac{r-1}{b_2}, b_2, \frac{r+1}{b_1}$ odd, $b_1\equiv 2(\text{mod } 4)$ and $1\leq s\leq \frac{r-1}{b_2}, 1\leq t\leq \frac{r+1}{b_1}$, s even, t odd	Theorem 3.1
$q=r^2, r\equiv 3(\text{mod } 4)$	$n=s\frac{r+1}{b_1}+t\frac{r-1}{b_2}, b_1, \frac{r-1}{b_2}$ odd, $b_2\equiv 2(\text{mod } 4)$ and $1\leq s\leq \frac{r-1}{b_2}, 1\leq t\leq \frac{r+1}{b_1}, t\equiv 0(\text{mod } 4)$	Theorem 3.5
$q=r^2, r\equiv 3(\text{mod } 4)$	$n=s\frac{q-1}{b_1}+t(r-1), b_2, \frac{r+1}{b_1}$ odd, $b_1\equiv 0(\text{mod } 4)$ and $1\leq s\leq \frac{b_1}{2}, 1\leq t\leq \frac{r+1}{b_1}$, s odd, t even	Theorem 3.8

Lemma 2.1. *[17] Let $A=\{a_1,a_2,\ldots,a_n\}$ be a subset of F_q, where n is an even integer. If $\eta\left(\delta_A(a)\right)$ are the same for all $a\in A$, then there exists a q-ary MDS self-dual code of length n.*

Lemma 2.2. *[8] (1) Let A be a subset of F_q, then for any $a\in A$,*

$$\delta_A(a)=f_A'(a),$$

where $f_A'(a)$ is the derivative of $f_A(a)$.

(2) Let A_1 and A_2 be disjoint subsets of F_q, $A=A_1\cup A_2$, then for $a\in A$,

$$\delta_A(a)=\begin{cases}\delta_{A_1}(a)f_{A_2}(a), a\in A_1\\ \delta_{A_2}(a)f_{A_1}(a), a\in A_2\end{cases}.$$

Lemma 2.3. *[8] Let $g\in GF(q)$ be a primitive n-th root of unity. Let n and q be integers satisfying $n\mid q-1$. We have*

(1) $\prod_{1\leq i\leq n}^{i\neq j}\left(g^i-g^j\right)=g^{i(n-1)}n=g^{-i}n$,

(2) $x^n-\gamma^n=\prod_{1\leq i\leq n}\left(x-\gamma g^i\right)$, for any $\gamma\in F_q$.

3 Construction of MDS self-dual codes

In this section, for $q=r^2$, we construct a concatenation using two disjoint multiplicative subgroups A and B of F_q^*, in order to get the new length of q-ary MDS self-dual codes. Let a be an integer with $a\mid q-1$. We mark it as $a=b_1b_2$, where $b_1=\gcd(a,r+1)$, $b_2=\frac{a}{\gcd(a,r+1)}$, then $b_2\mid(r-1)\frac{r+1}{b_1}$. It follows that $\gcd\left(b_2,\frac{r+1}{b_1}\right)=\gcd\left(\frac{a}{b_1},\frac{r+1}{b_1}\right)=1$, hence $b_1|(r+1)$ and $b_2|(r-1)$.

Theorem 3.1. *Let $q=r^2$ with r an odd prime power and $r\equiv 1(\text{mod } 4)$. Assume b_2 and $\frac{r+1}{b_1}$ are odd with $b_1\equiv 2(\text{mod } 4)$, then $a\equiv 2(\text{mod } 4)$. Let $n=s\frac{r+1}{b_1}+t\frac{r-1}{b_2}$ where $1\leq s\leq\frac{r-1}{b_2}$ and $1\leq t\leq\frac{r+1}{b_1}$. There exists a q-ary MDS self-dual code of length n, if s is even and t is odd.*

Proof. Let $n = s\frac{r+1}{b_1} + t\frac{r-1}{b_2}$ with b_1, b_2, r satisfying above condition. Let A and B be subgroups of F_q^*. Assume θ is a primitive element of F_q^* Assume $A = \langle\alpha\rangle, B = \langle\beta\rangle$ are subgroups of F_q^*, where $\alpha = \theta^{b_1(r-1)}$ and $\beta = \theta^{b_2(r+1)} \in QR_q$. Let $\lambda = \theta^{\frac{a}{2}} \notin QR_q$. Then, define

$$D = \left(\bigcup_{i=0}^{s-1} \beta^i A\right) \bigcup \left(\bigcup_{j=0}^{t-1} \lambda^{2j+1} B\right).$$

Since $b_1(r-1), b_2(r+1)$ are even and $a \equiv 2 \pmod 4$, then $\alpha = \theta^{b_1(r-1)}$, $\beta = \theta^{b_2(r+1)}$ are entries of QR_q and $\lambda = \theta^{\frac{a}{2}} \notin QR_q$. We have $\beta^i A \cap \lambda^{2j+1} B = \varnothing$, for any $0 \le i \le s-1, 0 \le j \le t-1$. So we get the union D of two disjoint subsets.

Firstly, we are ready to prove that $\beta^0, \ldots, \beta^{s-1}$ are the representatives of s distinct cosets of the subgroup A in F_q^*. If not, there exist $0 \le i_1 < i_2 \le s-1$ such that $\beta^{i_1} A = \beta^{i_2} A$, for the subgroup A. Hence, there exists $1 \le h \le \frac{r+1}{b_1}$ such that $\beta^{i_1 - i_2} = \alpha^h$, i.e.,

$$\theta^{b_2(r+1)(i_1-i_2) - b_1(r-1)h} = 1 \Rightarrow q-1 \mid b_2(r+1)(i_1 - i_2) - b_1(r-1)h.$$

Since $b_1(r-1)h < q-1$,

$$b_1(r-1) \Big| b_2(r+1)(i_1 - i_2) \Rightarrow \frac{(r-1)}{b_2} \Big| \frac{(r+1)}{b_1}(i_1 - i_2).$$

Since $i_1 - i_2 \le s - 1 < \frac{(r-1)}{b_2}$, there is a contradiction here.

Then, we can also prove that $\lambda^1, \lambda^3, \ldots, \lambda^{2t-1}$ are the representatives of t distinct cosets of the subgroup B in F_q^*. Otherwise, there exist $0 \le j_1 < j_2 \le t-1$ such that $\lambda^{2j_1+1} B = \lambda^{2j_2+1} B$, for the subgroup B. Hence, there exists $1 \le m \le \frac{r-1}{b_2}$ such that $\lambda^{2(j_1 - j_2)} = \beta^m$, i.e.,

$$\theta^{a(j_1-j_2) - b_2(r+1)m} = 1 \Rightarrow q-1 \mid a(j_1 - j_2) - b_2(r+1)m.$$

Since $b_2(r+1)m \le q-1$,

$$b_2(r+1) \Big| a(j_1 - j_2) \Rightarrow \frac{(r+1)}{b_1} \Big| (j_1 - j_2).$$

Since $j_1 - j_2 \le t - 1 < \frac{(r+1)}{b_1}$, there is a contradiction here. Note that $\frac{r-1}{b_2}$ and s are even, it follows that $|D| = n = s\frac{r+1}{b_1} + t\frac{r-1}{b_2}$ is even.

Next, we calculate $\delta_D\left(\lambda^{2i+1}\beta^j\right)$. By Lemma 2.2, for $0 \le i \le t-1$ and $1 \le j \le \frac{r-1}{b_2}$,

$$\begin{aligned}
\delta_D\left(\lambda^{2i+1}\beta^j\right) &= \delta_{\lambda^{2i+1}B}\left(\lambda^{2i+1}\beta^j\right) f_{\beta^h A}\left(\lambda^{2i+1}\beta^j\right) \\
&= \prod_{v=1, v\ne j}^{\frac{r-1}{b_2}} \left(\lambda^{2i+1}\beta^j - \lambda^{2i+1}\beta^v\right) \cdot \prod_{l=0, l\ne i}^{t-1} \prod_{v=1}^{\frac{r-1}{b_2}} \left(\lambda^{2i+1}\beta^j - \lambda^{2l+1}\beta^v\right) \\
&\cdot \prod_{h=0}^{s-1} \prod_{u=1}^{\frac{r+1}{b_1}} \left(\lambda^{2i+1}\beta^j - \beta^h \alpha^u\right) \\
&= \frac{r-1}{b_2} \cdot \lambda^{(2i+1)\left(\frac{r-1}{b_2} - 1\right)} \cdot \beta^{-j} \cdot \prod_{l=0, l\ne i}^{t-1} \left(\lambda^{(2i+1)\frac{r-1}{b_2}} - \lambda^{(2l+1)\frac{r-1}{b_2}}\right) \\
&\cdot \prod_{h=0}^{s-1} \left(\left(\lambda^{2i+1}\beta^j\right)^{\frac{r+1}{b_1}} - \beta^{h\frac{r+1}{b_1}}\right).
\end{aligned}$$

Since $\beta \in QR_q$ and $\frac{r-1}{b_2}$ is even, we have $\lambda^{(2i+1)\frac{r-1}{b_2}} \cdot \beta^{-j} \cdot \frac{r-1}{b_2} \in QR_q$.

So we should consider

$$\prod_{l=0,l\neq i}^{t-1} \left(\lambda^{(2i+1)\frac{r-1}{b_2}} - \lambda^{(2l+1)\frac{r-1}{b_2}}\right) \text{ and } \prod_{h=0}^{s-1} \left(\left(\lambda^{2i+1}\beta^j\right)^{\frac{r+1}{b_1}} - \beta^{\frac{r+1}{b_1}}\right).$$

Let $w = \prod_{l=0,l\neq i}^{t-1} \left(\lambda^{(2i+1)\frac{r-1}{b_2}} - \lambda^{(2l+1)\frac{r-1}{b_2}}\right)$, then

$$\left(\lambda^{(2i+1)\frac{r-1}{b_2}}\right)^{r+1} = \left(\theta^{\frac{(2i+1)b_1}{2}}\right)^{q-1} = 1, \text{ i.e., } \left(\lambda^{(2i+1)\frac{r-1}{b_2}}\right)^{r} = \lambda^{-(2i+1)\frac{r-1}{b_2}}.$$

Therefor,

$$w^r = \prod_{l=0,l\neq i}^{t-1} \left(\theta^{-\frac{(2i+1)b_1(r-1)}{2}} - \theta^{-\frac{(2l+1)b_1(r-1)}{2}}\right),$$
$$w^{r-1} = \theta^{\frac{q-1}{2}(t-1)-\frac{b_1(r-1)}{2}\left(2(i+1)(t-1)+t(t-1)-2i\right)}.$$

Thus,

$$w = \theta^{\frac{r+1}{2}(t-1)-\frac{b_1}{2}\left(2(t-1)(i+1)+t(t-1)-2i\right)+k(r+1)},$$

for some integer k. If t is odd and $b_1 \equiv 2 (\bmod\ 4)$, we have $w \in QR_q$.

For $\prod_{h=0}^{s-1} \left(\left(\lambda^{(2i+1)}\beta^j\right)^{\frac{r+1}{b_1}} - \beta^{h\frac{r+1}{b_1}}\right)$, we have

$$\prod_{h=0}^{s-1} \left(\left(\theta^{\frac{(2i+1)a}{2b_1}+\frac{jb_2(r+1)}{b_1}}\right)^{r+1} - \left(\theta^{\frac{hb_2(r+1)}{b_1}}\right)^{r+1}\right) \in F_r^* \subset QR_q.$$

By the above results, we have

$$\eta\left(\delta_D\left(\beta^i\alpha^j\right)\right) = \eta\left(\lambda^{-(2i+1)}\right) = -1.$$

Then we calculate $\delta_D\left(\beta^i\alpha^j\right)$ for $0 \le i \le s-1$ and $1 \le j \le \frac{r+1}{b_1}$. By Lemma 2.2,

$$\begin{aligned}
\delta_D\left(\beta^i\alpha^j\right) &= \delta_{\beta^i A}\left(\beta^i\alpha^j\right) f_{\lambda^{2h+1}B}\left(\beta^i\alpha^j\right) \\
&= \prod_{v=1,v\neq j}^{\frac{r+1}{b_1}} \left(\beta^i\alpha^j - \beta^i\alpha^v\right) \cdot \prod_{l=0,l\neq i}^{s-1} \prod_{v=1}^{\frac{r+1}{b_1}} \left(\beta^i\alpha^j - \beta^l\alpha^v\right) \cdot \prod_{u=1}^{\frac{r-1}{b_2}} \prod_{h=0}^{t-1} \left(\beta^i\alpha^j - \lambda^{2h+1}\beta^u\right) \\
&= \beta^{i\left(\frac{r+1}{b_1}-1\right)} \cdot \frac{r+1}{b_1} \cdot \alpha^{-j} \cdot \prod_{l=0,l\neq i}^{s-1} \left(\beta^{i\frac{r+1}{b_1}} - \beta^{l\frac{r+1}{b_1}}\right) \cdot \prod_{h=0}^{t-1} \left(\alpha^{j\frac{r-1}{b_2}} - \lambda^{(2h+1)\frac{r-1}{b_2}}\right).
\end{aligned}$$

It is easy to find that $\beta^{i\left(\frac{r+1}{b_1}-1\right)} \cdot \alpha^{-j} \in QR_q$, then we let $w' = \prod_{h=0}^{t-1} \left(\alpha^{j\frac{r-1}{b_2}} - \lambda^{(2h+1)\frac{r-1}{b_2}}\right)$. Note that

$$\left(\alpha^{j\frac{r-1}{b_2}}\right)^{r+1} = \left(\theta^{\frac{b_1(r-1)j}{b_2}}\right)^{q-1} = 1, \text{ i.e., } \left(\alpha^{j\frac{r-1}{b_2}}\right)^{r} = \alpha^{-j\frac{r-1}{b_2}},$$

$$\left(\lambda^{(2h+1)\frac{r-1}{b_2}}\right)^{r+1} = \left(\theta^{\frac{a(2h+1)}{2b_2}}\right)^{q-1} = 1, \text{ i.e., } \left(\lambda^{(2h+1)\frac{r-1}{b_2}}\right)^{r} = \lambda^{-(2h+1)\frac{r-1}{b_2}}.$$

We have

$$w'^r = \prod_{h=0}^{t-1}\left(\alpha^{-j\frac{r-1}{b_2}} - \lambda^{-(2h+1)\frac{r-1}{b_2}}\right),$$

$$w'^{r-1} = \theta^{\frac{q-1}{2}t - \frac{(r-1)}{b_2}\left(b_1 t(r-1)j + a\frac{t(t-1)}{2} + \frac{at}{2}\right)}.$$

Thus,

$$w' = \theta^{\frac{t(r+1)}{2} - \frac{b_1 tj(r-1)}{b_2} - \frac{b_1 t^2}{2} + k(r+1)},$$

for some integer k. If $b_1 \equiv 2(\mathrm{mod}\ 4)$, we have $w' \in QR_q$.

Similarly, for $\prod_{l=0,l\neq i}^{s-1}\left(\beta^{i\frac{r+1}{b_1}} - \beta^{l\frac{r+1}{b_1}}\right)$, we have

$$\prod_{l=0,l\neq i}^{s-1}\left(\beta^{i\frac{r+1}{b_1}} - \beta^{l\frac{r+1}{b_1}}\right) = \prod_{l=0,l\neq i}^{s-1}\left(\left(\theta^{\frac{ib_2(r+1)}{b_1}}\right)^{r+1} - \left(\theta^{\frac{lb_2(r+1)}{b_1}}\right)^{r+1}\right) \in F_r^* \subset QR_q.$$

By the above results, we can obtain

$$\eta\left(\delta_D\left(\lambda^{2i+1}\beta^j\right)\right) = \eta(\frac{r+1}{b_1}) = -1.$$

By Lemma 2.1, there exists a q-ary MDS self-dual code of length n. □

Remark 3.2. *When $r \equiv 1(\mathrm{mod}\ 4)$. The lengths of the MDS self-dual codes we construct are not in [9] when t is odd. Compared with the Theorem 1 in [19], we obtain new MDS self-dual codes of different lengths, by extending the range of s, t from $1 \le s \le \frac{r+1}{2v}, 1 \le t \le \frac{r-1}{2u}$ to $1 \le s \le \frac{r-1}{b_2}, 1 \le t \le \frac{r+1}{b_1}$. Specifically, when s is even, we obtain a new class of MDS self-dual codes of length n which are not present in [[19], Theorem 1].*

Example 3.3. *Let $r = 25, q = 25^2, b_1 = 26$ and $b_2 = 3$. If $s = 2, t = 1$, by Theorem 3.1, there exists a MDS self-dual code of length $n = 10$. At this point, the length we obtain is not in Table 1.*

Example 3.4. *Let $r = 25, q = 25^2$, $b_1 = 2$ and $b_2 = 1$. If $s = 18, t = 13$, by Theorem 3.1, there exists a MDS self-dual code of length $n = 546$. At this point, the length we obtain is not in Table 1. It is worth noting that when $r = 25$, we can obtain 120 new MDS self-dual codes.*

Theorem 3.5. *Let $q = r^2$ with r an odd prime power and $r \equiv 3(\mathrm{mod}\ 4)$. Assume b_1 and $\frac{r-1}{b_2}$ are odd with $b_2 \equiv 2(\mathrm{mod}\ 4)$, then $a \equiv 2(\mathrm{mod}\ 4)$. Let $n = s\frac{r+1}{b_1} + t\frac{r-1}{b_2}$, where $1 \le s \le \frac{r-1}{b_2}$ and $1 \le t \le \frac{r+1}{b_1}$. There exists a q-ary MDS self-dual code of length n, if $t \equiv 0(\mathrm{mod}\ 4)$.*

Proof. By the above construction, we have $r+1 \equiv 0(\mathrm{mod}\ 4), r-1 \equiv 2(\mathrm{mod}\ 4)$. For $1 \le s \le \frac{r-1}{b_2}$ and $1 \le t \le \frac{r+1}{b_1}$, let $n = s\frac{r+1}{b_1} + t\frac{r-1}{b_2}$. Assume $A = \langle\alpha\rangle, B = \langle\beta\rangle$ are subgroups of F_q^*, where $\alpha = \theta^{b_1(r-1)}$ and $\beta = \theta^{b_2(r+1)} \in QR_q$. Let $\zeta = \theta^{\frac{a}{2}} \notin QR_q$. Define

$$F = \left(\bigcup_{i=0}^{s-1}\zeta^{2i+1}A\right)\bigcup\left(\bigcup_{j=0}^{t-1}\alpha^j B\right).$$

It is easy to find that $\zeta^{2i+1}A \cap \alpha^j B = \varnothing$ if $a \equiv 2(\mathrm{mod}\ 4)$.

Firstly, we could prove that $\zeta^1, \zeta^3, \ldots, \zeta^{2s-1}$ are the representatives of s distinct cosets of the subgroup A in F_q^*, if $1 \le s \le \frac{r-1}{b_2}$. Similarly, we can also prove that $\alpha^0, \ldots, \alpha^{t-1}$ are the representatives of t distinct cosets of the subgroup B in F_q^*, if $1 \le t \le \frac{r+1}{b_1}$. It follows that n is even when b_1 is odd and t is even.

Next, we are ready to calculate $\delta_F\left(\alpha^i\beta^j\right)$ for $0 \le i \le t-1, 1 \le j \le \frac{r-1}{b_2}$. By Lemma 2.2,

$$\begin{aligned}\delta_F\left(\alpha^i\beta^j\right) &= \delta_{\alpha^i B}\left(\alpha^i\beta^j\right) f_{\zeta^{2h+1}A}\left(\alpha^i\beta^j\right)\\ &= \alpha^{i\left(\frac{r-1}{b_2}-1\right)} \cdot \frac{r-1}{b_2} \cdot \beta^{-j} \cdot \prod_{l=0,l\neq i}^{t-1}\left(\alpha^{\frac{(r-1)i}{b_2}} - \alpha^{\frac{(r-1)l}{b_2}}\right)\\ &\cdot \prod_{h=0}^{s-1}\left(\beta^{\frac{(r+1)j}{b_1}} - \zeta^{\frac{(r+1)(2h+1)}{b_1}}\right).\end{aligned}$$

Since $\beta, \alpha \in QR_q$, we have $\alpha^{i\left(\frac{r-1}{b_2}-1\right)} \cdot \beta^{-j} \in QR_q$.

Suppose that $p = \prod_{l=0,l\neq i}^{t-1}\left(\alpha^{\frac{(r-1)i}{b_2}} - \alpha^{\frac{(r-1)l}{b_2}}\right)$, we have

$$p = \theta^{\frac{(r+1)(t-1)}{2} - \frac{b_1(r-1)}{b_2}\left(i(t-2)+\frac{t(t-1)}{2}\right)+k(r+1)},$$

for some integer k. Since b_1, $\frac{r-1}{b_2}$ are odd and $t \equiv 0 \pmod 4$, $p \in QR_q$.

Since $p' = \prod_{h=0}^{s-1}\left(\beta^{j\frac{r+1}{b_1}} - \zeta^{(2h+1)\frac{r+1}{b_1}}\right) = \prod_{h=0}^{s-1}\left((\theta^{\frac{jb_2(r+1)}{b_1}})^{r+1} - (\theta^{\frac{b_2(2h+1)}{2}})^{r+1}\right) \in F_r^*$, then $p\prime \in QR_q$. By the above results, we have

$$\eta\left(\delta_F\left(\alpha^i\beta^j\right)\right) = \eta(\frac{r-1}{b_2}) = -1.$$

Then, we calculate $\delta_F\left(\zeta^{2i+1}\alpha^j\right)$ for $0 \le i \le s-1$ and $1 \le j \le \frac{r+1}{b_1}$. By Lemma 2.2,

$$\begin{aligned}\delta_F\left(\zeta^{2i+1}\alpha^j\right) &= \delta_{\zeta^{2i+1}A}\left(\zeta^{2i+1}\alpha^j\right) f_{\alpha^h B}\left(\zeta^{2i+1}\alpha^j\right)\\ &= \zeta^{(2i+1)\left(\frac{r+1}{b_1}-1\right)} \cdot \frac{r+1}{b_1} \cdot \alpha^{-j} \prod_{l=0,l\neq i}^{s-1}\left(\zeta^{\frac{(2i+1)(r+1)}{b_1}} - \zeta^{\frac{(2l+1)(r+1)}{b_1}}\right)\\ &\cdot \prod_{h=0}^{t-1}\left(\left(\zeta^{2i+1}\alpha^j\right)^{\frac{r-1}{b_2}} - \alpha^{h\frac{r-1}{b_2}}\right).\end{aligned}$$

Since $\beta, \alpha \in QR_q$, we have $\zeta^{(2i+1)\frac{r+1}{b_1}} \cdot \frac{r+1}{b_1} \cdot \alpha^{-j} \in QR_q$.

Since $g = \prod_{l=0,l\neq i}^{s-1}\left(\zeta^{\frac{(2i+1)(r+1)}{b_1}} - \zeta^{\frac{(2l+1)(r+1)}{b_1}}\right) = \prod_{l=0,l\neq i}^{s-1}\left((\theta^{\frac{(2i+1)b_2}{2}})^{r+1} - (\theta^{\frac{(2l+1)b_2}{2}})^{r+1}\right) \in F_r^*$, then $g \in QR_q$.

Suppose that $g' = \prod_{h=0}^{t-1}\left(\left(\zeta^{2i+1}\alpha^j\right)^{\frac{r-1}{b_2}} - \alpha^{h\frac{r-1}{b_2}}\right)$. When $t \equiv 0 \pmod 4$, we have

$$g' = \theta^{\frac{(r+1)t}{2} - \frac{tb_1(2i+1)}{2} - jtb_1\frac{(r-1)}{b_2} - b_1\frac{t(t-1)(r-1)}{2b_2} + k(r+1)} \in F_r^* \subset QR_q,$$

for some integer k. By the above results, we have

$$\eta\left(\delta_F\left(\zeta^{2i+1}\alpha^j\right)\right) = \eta\left(\zeta^{-(2i+1)}\right) = -1.$$

By Lemma 2.1, there exists a q-ary MDS self-dual code of length n. □

Remark 3.6. *When $r \equiv 3 \pmod{4}$. The MDS self-dual codes we construct is confirmed not to exist in [9]. Specifically, when $\frac{(r+1)b}{2a}s^2$ is odd, we obtain a new class of MDS self-dual codes of length n which are not present in [[19], Theorem 2].*

Example 3.7. *Let $r = 19, q = 19^2, b_1 = 5$ and $b_2 = 2$. If $s = 9, t = 4$, by Theorem 3.5, there exists a MDS self-dual code of length $n = 72$. At this point, the length of our construction is not in Table 1. It is worth noting that when $r = 19$, we can obtain 61 new MDS self-dual codes.*

Theorem 3.8. *Let $q = r^2$ with r an odd prime power and $r \equiv 3 \pmod{4}$. Assume $\frac{r+1}{b_1}$,b_2 are odd, then $b_1 \equiv 0 \pmod{4}$. Let $n = s\frac{q-1}{b_1} + t(r-1)$ where $1 \leq s \leq \frac{b_1}{2}$ and $1 \leq t \leq \frac{r+1}{b_1}$. There exists a q-ary MDS self-dual code of length n, if t is even and s is odd.*

Proof. By the above construction, for $1 \leq s \leq \frac{b_1}{2}$ and $1 \leq t \leq \frac{r+1}{b_1}$, let $n = s\frac{q-1}{b_1} + t(r-1)$. Assume $A = \langle \alpha \rangle, B = \langle \beta \rangle$ are subgroups of F_q^*, where $\alpha = \theta^{b_1}$ and $\beta = \theta^{r+1} \in QR_q$. Let $\gamma = \theta^{b_2} \notin QR_q$. Define

$$T = \left(\bigcup_{i=0}^{s-1} \gamma^{2i+1} A \right) \bigcup \left(\bigcup_{j=0}^{t-1} \alpha^j B \right).$$

It is easy to find that $\gamma^{2i+1} A \cap \alpha^j B = \varnothing$. Since $\frac{q-1}{b_1}$ and $r-1$ are even, it follows that $n = s\frac{q-1}{b_1} + t(r-1)$ is even, i.e., $|T|$ is even.

Firstly, we can prove that $\gamma^1, \ldots, \gamma^{2s-1}$ are the representatives of s distinct cosets of the subgroup A in F_q^* if $1 \leq s \leq \frac{b_1}{2}$. Similarly, we can also prove that $\alpha^0, \alpha^2, \ldots, \alpha^{t-1}$ are the representatives of t distinct cosets of the subgroup B in F_q^*, if $1 \leq t \leq \frac{(r+1)}{b_1}$.

Next, we are ready to calculate $\delta_T\left(\gamma^{2i+1}\alpha^j\right)$ for $0 \leq i \leq s-1$ and $1 \leq j \leq \frac{q-1}{b_1}$. By Lemma 2.2,

$$\begin{aligned}
\delta_T\left(\gamma^{2i+1}\alpha^j\right) &= \delta_{\gamma^{2i+1}A}\left(\gamma^{2i+1}\alpha^j\right) f_{\alpha^h B}\left(\gamma^{2i+1}\alpha^j\right) \\
&= \gamma^{(2i+1)(\frac{q-1}{b_1}-1)} \cdot \frac{q-1}{b_1} \cdot \alpha^{-j} \cdot \prod_{l=0, l\neq i}^{s-1} \left(\gamma^{\frac{(q-1)(2i+1)}{b_1}} - \gamma^{\frac{(q-1)(2l+1)}{b_1}}\right) \\
&\cdot \prod_{h=0}^{t-1} \left(\left(\gamma^{2i+1}\alpha^j\right)^{r-1} - \alpha^{h(r-1)}\right).
\end{aligned}$$

Since $\frac{q-1}{b_1}, \alpha \in QR_q$, we have $\gamma^{(2i+1)\frac{q-1}{b_1}} \cdot \frac{q-1}{b_1} \cdot \alpha^{-j} \in QR_q$.

Suppose that $v = \prod_{l=0, l\neq i}^{s-1} \left(\gamma^{(2i+1)\frac{(q-1)}{b_1}} - \gamma^{(2l+1)\frac{(q-1)}{b_1}}\right)$, we have

$$v = \theta^{\frac{(r+1)(s-1)}{2} - \frac{2b_2(r+1)}{b_1}\left((i+1)(s-1) + \frac{s(s-1)}{2} - i\right) + k(r+1)} \in F_r^* \subset QR_q,$$

for some integer k.

Suppose that $v' = \prod_{h=0}^{t-1} \left(\left(\gamma^{2i+1}\alpha^j\right)^{r-1} - \alpha^{h(r-1)}\right)$, when t is even, we have

$$v' = \theta^{\frac{(r+1)t}{2} - tb_2(2i+1) - b_1 tj - b_1\frac{t(t-1)}{2} + k(r+1)} \in F_r^* \subset QR_q,$$

for some integer k. By the above results, we have

$$\eta\left(\delta_T\left(\gamma^{2i+1}\alpha^j\right)\right) = \eta\left(\gamma^{-(2i+1)}\right) = -1.$$

Then we calculate $\delta_T\left(\alpha^i\beta^j\right)$ for $0 \le i \le t-1$ and $1 \le j \le r-1$. By Lemma 2.2,

$$\begin{aligned}\delta_T\left(\alpha^i\beta^j\right) &= \delta_{\alpha^i B}\left(\alpha^i\beta^j\right) f_{\gamma^{2h+1}A}\left(\alpha^i\beta^j\right)\\ &= \alpha^{i(r-2)}\cdot(r-1)\cdot\beta^{-j}\cdot\prod_{l=0,l\neq i}^{t-1}\left(\alpha^{i(r-1)}-\alpha^{l(r-1)}\right)\cdot\prod_{h=0}^{s-1}\left(\beta^{j\frac{q-1}{b_1}}-\gamma^{(2h+1)\frac{q-1}{b_1}}\right).\end{aligned}$$

Since $\beta,\alpha \in QR_q$, we have $\alpha^{i(r-2)}\cdot(r-1)\cdot\beta^{-j} \in QR_q$.

Suppose that $g=\prod_{l=0,l\neq i}^{t-1}\left(\alpha^{i(r-1)}-\alpha^{l(r-1)}\right)$. When b_1 is even, we have

$$g=\theta^{\frac{(r+1)(t-1)}{2}-b_1\left(i(t-2)+\frac{t(t-1)}{2}\right)+k(r+1)} \in F_r^* \subset QR_q,$$

for some integer k. Suppose that $g'=\prod_{h=0}^{s-1}\left(\beta^{j\frac{q-1}{b_1}}-\gamma^{(2h+1)\frac{q-1}{b_1}}\right)$. When s, b_2 and $\frac{r+1}{b_1}$ are odd, we have

$$g'=\theta^{\frac{s(r+1)}{2}-\frac{r+1}{b_1}((r+1)js+s^2b_2)+k(r+1)},$$

for some integer k. Thus,

$$\eta\left(g'\right)=-1.$$

By the above results,

$$\eta\left(\delta_T\left(\alpha^i\beta^j\right)\right)=-1.$$

By Lemma 2.1, there exists a q-ary MDS self-dual code of length n. □

Remark 3.9. *When $r \equiv 3(\mathrm{mod}\ 4)$. The length of the MDS self-dual codes is the form of $k_1(r+1)+k_2(r-1)$ in [9]. By calculating, we obtain a new class of q-ary MDS self-dual codes of length $n=k(r-1)$, where k is odd. Compared with [19], $n=s\frac{q-1}{b}+t\frac{q-1}{a}$, the condition of construction in [[19], Theorem 2] is not met when $a=r+1\equiv 0(\mathrm{mod}\ 4)$ and $b\equiv 0(\mathrm{mod}\ 4)$.*

Example 3.10. *Let $r=19, q=19^2, b_1=4$. If $s=1, t=4$, by Theorem 3.8, there exists a MDS self-dual code of length $n=162$. At this point, the length we obtain is not in Table 1. It is worth noting that when $r=19$, we can obtain 2 new MDS self-dual codes of length $n=\{126,162\}$.*

4 Conclusion

In this paper, we extend the construction methods of [5,9,19]. On the basis of two different multiplicative subgroups of F_q^* and generalized RS codes we obtain some new MDS self dual codes over finite fields of odd characteristics. The crucial aspect of our construction is the selection of appropriate mutually disjoint subgroups and specific parameters such that their corresponding GRS codes are Euclidean MDS self-dual codes. We continue the previous approach and prove that further extensions to obtain codes of additional lengths are possible. The direction of future studies remains to find more new Euclidean self-dual codes.

5 Declarations

Ethical Approval and Consent to participate They have no known competing financial interests or personal relationships that might influence the work reported herein. All authors gave their informed consent.

Availability of supporting data All results are the property of the author and no permission is required.

Consent for publication All authors have seen and approved the final version of the submitted manuscript. They guarantee that this article is the authors' original work and has not been previously published or considered for publication elsewhere.

Competing interests The authors have no competing interests to declare in relation to the content of this article.

Funding This study is supported by the National Natural Science Foundation of China under Grant Nos.U21A20428, 12171134, 61972126 and 61802102.

Authors' contributions C.Y.T. and Z.S.X. conceived of the presented idea. C.Y.T. developed the theory and performed the computations. Z.S.X. supervised the findings of this work. All authors provided critical feedback and helped shape the research, analysis and manuscript.

Acknowledgements The author is grateful to the editor and anonymous referees for careful reading and for many useful suggestions. This study is supported by the National Natural Science Foundation of China under Grant Nos.U21A20428, 12171134, 61972126 and 61802102.

Authors' information Yuting Cao, caoyuting9797@163.com, School of Mathematics, Hefei University of Technology, Hefei 230601, Anhui, China. Shixin Zhu, zhushixin@hfut.edu.cn, School of Mathematics, Hefei University of Technology, Hefei 230601, Anhui, China.

References

[1] Georgiou S., Koukouvinos C.: MDS self-dual codes over large prime fields. Finite Fields Appl. **8**(4), 455–470 (2002).

[2] Harada M., Kharaghani H.: Orthogonal designs and MDS self-dual codes. Austral. J. Comb. **35**, 57–67 (2006).

[3] Yan H.: A note on the constructions of MDS self-dual codes. Cryptogr. Commun. **11**(2), 259–268 (2019).

[4] Guenda K.: New MDS self-dual codes over finite fields. Des. Codes Cryptogr. **62**(1), 31–42 (2012).

[5] Massey J.: Some applications of coding theory in cryptography. In: Proc. 4th IMA Conf. Cryptogr. Coding, 33–47 (1995).

[6] Zhang A., Feng K.: On the constructions of MDS self-dual codes via cyclotomy. Finite Fields and Their Applications **77**, 101947 (2022).

[7] Fang W., Fu F.: New constructions of MDS Euclidean self-dual codes from GRS codes and extended GRS codes. IEEE Trans. Inf. Theory **65**(9), 5574–5579 (2019).

[8] Zhang A., Feng K.: A unified approach to construct MDS self-dual codes via Reed-Solomon codes. IEEE Trans. Inf. Theory **66**(6), 3650–3656 (2020).

[9] Fang X., Liu M., Luo J.: New MDS Euclidean self-orthogonal codes. IEEE Trans. Inf. Theory **67**(1),130–137 (2021).

[10] Dougherty S., S. Mesnager S., P. Solé P.: Secret-sharing schemes based on self-dual codes. in Proc. IEEE Inf. Theory Workshop, 338–342 (2008).

[11] Lebed K., Liu H., Luo J.: Construction of MDS self-dual codes over finite fields. Finite Fields Appl. **59**, 199–207 (2019).

[12] Fang X., Lebed K., Liu H., Luo J.: New MDS Euclidean self-dual codes over finite fields of odd characteristic. Des. Codes Cryptogr. **88**, 1127–1138 (2020).

[13] MacWilliams F., Sloane N.: The Theory of Error-Corrcting Codes. North Holland, Amsterdam (1977).

[14] Grass M., Gulliver T.: On self-duls MDS codes. Proc. ISIT 1954–1957 (2008).

[15] Jin L., Xing C.: New MDS self-dual codes from generalized Reed-Solomon codes. IEEE Trans. Inf. Theory **63**(3), 1434–1438 (2017).

[16] Tong H., Wang X.,: New MDS Euclidean and Hermitian self-dual codes over finite fields, Adv. in Pure Math. **77**, 325-333 (2017).

[17] Fang W., Shu T., Fang F.: Construction of MDS Euclidean self-dual codes via two subsets. IEEE Trans. Inf. Theory **67**(8), 5005-5015 (2021).

[18] Sok L.: Explicit constructions of MDS self-dual codes. IEEE Trans. Inf. Theory **66**(6), 3603-3615 (2019).

[19] Huang Z., Fang W., Fu F.: New constructions of MDS self-dual and self-orthogonal codes via GRS codes. arXiv preprint arXiv:2103.11665 (2021).

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- NewMDSSelfDualCodesFromTwoDisjointSubsets.zip