*entropy*

MDPI

*Article*

# New Construction of Maximum Distance Separable (MDS) Self-Dual Codes over Finite Fields

**Aixian Zhang * and Zhe Ji**

Department of Mathematical Sciences, Xi'an University of Technology, Xi'an 710054, China; 2170920001@stu.xaut.edu.cn

* Correspondence: zhangax@xaut.edu.cn; Tel.: +86-029-8966-7695

Received: 24 December 2018; Accepted: 17 January 2019; Published: 22 January 2019

check for updates

**Abstract:** Maximum distance separable (MDS) self-dual codes have useful properties due to their optimality with respect to the Singleton bound and its self-duality. MDS self-dual codes are completely determined by the length $n$, so the problem of constructing $q$-ary MDS self-dual codes with various lengths is a very interesting topic. Recently X. Fang et al. using a method given in previous research, where several classes of new MDS self-dual codes were constructed through (extended) generalized Reed-Solomon codes, in this paper, based on the method given in we achieve several classes of MDS self-dual codes.

**Keywords:** MDS code; self-dual code; generalized reed-solomon code; extended generalized reed-solomon code

## 1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q$ elements. A $q$-ary $[n, k, d]$ linear code $\mathcal{C}$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$ with minimum (Hamming) distance $d$. If the parameters $[n, k, d]$ satisfy $k + d = n + 1$, the code is called an MDS (maximum distance separable) code. A self-dual code is a linear code satisfying $\mathcal{C} = \mathcal{C}^\perp$. A linear complementary-dual code is a linear code satisfying $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$.

The study of MDS self-dual codes has attracted a great deal of attention in recent years due to its theoretical and practical importance. The center of the study of MDS codes includes the existence of MDS codes [1], classification of MDS codes [2], balanced MDS codes [3], non-Reed-Solomon MDS codes [4], complementary-dual MDS codes [5,6], and lowest density MDS codes [7].

As the parameters of an MDS self-dual code are completely determined by the code's length $n$, the main interest here is to determine the existence and give the construction of $q$-ary MDS self-dual codes for various lengths. The problem is completely solved for the case where $q$ is even [8]. Many MDS self-dual codes over finite fields of odd characteristics were constructed [9–14].

In [11], Jin and Xing constructed several classes of MDS self-dual code from generalized Reed-Solomon code. Yan generalized Jin and Xing's method and constructed several classes of MDS self-dual codes via generalized Reed-Solomon codes and extended generalized Reed-Solomon codes [14]. In [12], Ladad, Liu and Luo produced more classes of MDS self-dual codes based on [11] and [14]. In [9], based on the [11,12,14] more new parameter MDS self-dual codes were presented. Based on the method raised in [9], we present some classes of MDS self-dual codes.

## 2. Preliminaries

In this section we introduce some basic notations of generalized Reed-Solomon codes and extended generalized Reed-Solomon codes. For more details, the reader is referred to [15].

Throughout this paper, $q$ is a prime power, $\mathbb{F}_q$ is the finite fields with $q$ elements and let $n$ be a positive integer with $1 < n \leq q$. For any $x \in \mathbb{F}_{q^2}$, we denote by $\overline{x}$ the conjugation of $x$. Given an

$[n,k,d]$ linear code $\mathcal{C}$, its Euclidean dual code (resp. Hermitian dual code) is denoted by $\mathcal{C}^{\perp}$ (resp. $\mathcal{C}^{\perp_H}$). The codes $\mathcal{C}^{\perp}$ and $\mathcal{C}^{\perp_H}$ are defined by

$$\mathcal{C}^{\perp}=\{x=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q^n:\sum_{i=1}^{n}x_iy_i=0,\forall y=(y_1,y_2,\ldots,y_n)\in\mathcal{C}\},$$

$$\mathcal{C}^{\perp_H}=\{x=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_{q^2}^n:\sum_{i=1}^{n}x_i\overline{y_i}=0,\forall y=(y_1,y_2,\ldots,y_n)\in\mathcal{C}\},$$

respectively. In this paper, we only consider the Euclidean inner product.

Let $\vec{a}=(\alpha_1,\alpha_2,\ldots,\alpha_n)$, where $\alpha_1,\alpha_2,\ldots,\alpha_n$ are $n$ distinct elements of $\mathbb{F}_q$. Fix $n$ nonzero elements $v_1,v_2,\ldots,v_n$ of $\mathbb{F}_q$ ($v_i$ are not necessarily distinct), put $\vec{v}=(v_1,v_2,\ldots,v_n)$. For $1\le k\le n$, the $k$-dimensional generalized Reed-Solomon code (GRS for short) of length $n$ associated with $\vec{a}$ and $\vec{v}$ is defined to be

$$\mathbf{GRS}_k(\vec{a},\vec{v})=\{(v_1f(\alpha_1),v_2f(\alpha_2),\ldots,v_nf(\alpha_n)):f(x)\in\mathbb{F}_q[x],\deg(f(x))\le k-1\}. \tag{1}$$

It is well known that the code $\mathbf{GRS}_k(\vec{a},\vec{v})$ is a $q$-ary $[n,k,n-k+1]$ MDS code and the dual of a GRS code is again a GRS MDS code; indeed

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

for some $\vec{v}'=(v_1',v_2',\ldots,v_n')$ with $v_i'\neq 0$ for all $1\le i\le n$ (e.g., see [15]).

Furthermore, the extended generalized Reed-Solomon code $\mathbf{GRS}_k(\vec{a},\vec{v},\infty)$ given by

$$\mathbf{GRS}_k(\vec{a},\vec{v},\infty)=\{(v_1f(\alpha_1),v_2f(\alpha_2),\ldots,v_nf(\alpha_n),f_{k-1}):f(x)\in\mathbb{F}_q[x],\deg(f(x))\le k-1\}, \tag{2}$$

where $f_{k-1}$ stands for the coefficient of $x^{k-1}$ in $f(x)$. It is also well known that $\mathbf{GRS}_k(\vec{a},\vec{v},\infty)$ is a $q$-ary $[n+1,k,n-k+2]$ MDS code and the dual code is also a GRS MDS code (e.g., see [15]).

Put $\vec{a}=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ and denote by $\mathcal{A}_{\vec{a}}$ the matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1\\ \alpha_1 & \alpha_2 & \ldots & \alpha_n\\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_1^{n-2} & \alpha_2^{n-2} & \ldots & \alpha_n^{n-2}\end{pmatrix}$$

**Lemma 1** ([11]). *The solution space of the equation system $\mathcal{A}_{\vec{a}}X^T=\mathbf{0}$ has dimension 1 and $\{\vec{u}=(u_1,u_2,\ldots,u_n)\}$ is a basis of this solution space, where $u_i=\prod_{1\le j\le n,j\neq i}(\alpha_i-\alpha_j)^{-1}$. Furthermore, for any two polynomials $f(x),g(x)\in\mathbb{F}_q[x]$ with $\deg(f)\le k-1$ and $\deg(g)\le n-k-1$, one has $\sum_{i=1}^{n}f(\alpha_i)(u_ig(\alpha_i))=0$.*

We define

$$L_{\vec{a}}(\alpha_i)=\prod_{1\le j\le n,j\neq i}(\alpha_i-\alpha_j).$$

The conclusion of the following lemma is straightforward. For completeness, we provide its proof.

**Lemma 2** ([11]). *Let $n$ be an even number, if there exists $\lambda\in\mathbb{F}_q^*$ such that $\lambda L_{\vec{a}}(\alpha_i)$ is square element for all $i=1,2,\ldots,n$, then the code $\mathbf{GRS}_{n/2}(\vec{a},\vec{v})$ defined in (1) is MDS self-dual code of length $n$.*

**Proof.** Let $f(x), g(x) \in \mathbb{F}_q[x]$ with $\deg(f) \leq \frac{n}{2} - 1$ and $\deg(g) \leq \frac{n}{2} - 1$. By Lemma 1, we have $\sum_{i=1}^{n} f(\alpha_i)(u_i g(\alpha_i)) = 0$, where $u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$ for $i = 1, 2, \ldots, n$. Hence,

$$0 = \lambda \sum_{i=1}^{n} f(\alpha_i)(u_i g(\alpha_i)) = \sum_{i=1}^{n} f(\alpha_i)(\lambda u_i g(\alpha_i)) = \sum_{i=1}^{n} (v_i f(\alpha_i)) \quad (v_i g(\alpha_i))(\text{since } \lambda u_i = v_i^2).$$

This implies that $\mathbf{GRS}_{n/2}^{\perp}(\vec{a}, \vec{v}) = \mathbf{GRS}_{n/2}(\vec{a}, \vec{v})$. □

H. Yan [14] observed the following two results.

**Lemma 3** ([14]). *Let $n$ be an even integer and $k = \frac{n}{2}$. If $-L_{\vec{a}}(\alpha_i)$ is square element for all $i = 1, 2, \ldots, n-1$, then the code $\mathbf{GRS}_k(\vec{a}, \vec{v}, \infty)$ defined in (2) is MDS self-dual code of length $n$.*

**Lemma 4** ([14]). *Let $m \mid q-1$ be a positive integer and let $\alpha \in \mathbb{F}_q$ be a primitive $m$-th root of unity. Then for any $1 \leq i \leq m$, we have*

$$\prod_{1 \leq j \leq m, j \neq i} (\alpha^i - \alpha^j) = m\alpha^{-i}.$$

## 3. Main Result

Let $q = r^2$, where $r$ is odd prime power, $\mathbb{F}_q$ be the finite fields with $q$ elements. Suppose $m \mid q-1$, $\alpha$ is a primitive $m$-th root of unity and $\mathbf{H} =< \beta >$ is the cyclic group generated by $\beta$.

**Theorem 1.** *Let $q = r^2$, where $r$ is an odd prime power, $r \equiv 1 (\mathrm{mod} 4)$. Suppose that $m \mid (q-1)$ and $\frac{q-1}{m}$ is even, $m \equiv 0 (\mathrm{mod} 4)$. If $1 \leq t \leq \frac{2(r+1)}{gcd(2(r+1), m)}$. Then there exists an $[n = tm, \frac{n}{2}]$-MDS self-dual code.*

**Proof.** Let $\alpha$ be a primitive $m$-th root of unity and $\mathbf{H} =< \beta >$ is the cyclic group of order $2(r+1)$. By the theorem of group homomorphism,

$$(\mathbf{H} \times \langle \alpha \rangle)/\langle \alpha \rangle \cong \mathbf{H}/(\mathbf{H} \cap \langle \alpha \rangle).$$

Let $i_1, i_2, \ldots, i_t$ be $t$ distinct elements, such that $0 \leq i_1 < i_2 < \cdots < i_t < 2(r+1)$. Denote $I = \{i_1, i_2, \ldots, i_t\}$, $A = i_1 + i_2 + \cdots + i_t$ and $\mathbf{B} = \{\beta^{i_1}, \beta^{i_2}, \ldots, \beta^{i_t}\}$ be a set of coset representatives of $(\mathbf{H} \times \langle \alpha \rangle)/\langle \alpha \rangle$. Let

$$\vec{a} = (\alpha\beta^{i_1}, \ldots, \alpha^m \beta^{i_1}, \alpha\beta^{i_2}, \ldots, \alpha^m \beta^{i_2}, \ldots, \alpha\beta^{i_t}, \ldots, \alpha^m \beta^{i_t}).$$

Then the entries of $\vec{a}$ are distinct in $\mathbb{F}_q^*$.

It is known that $x^m - y^m = \prod_{j=1}^{m} (x - \alpha^j y)$. By the statement of Lemma 3, we get

$$\begin{aligned} L_{\vec{a}}(\beta^z \alpha^k) &= \prod_{1 \leq j \leq m, j \neq k} (\beta^z \alpha^k - \beta^z \alpha^j) \prod_{l \in I, l \neq z} \prod_{j=1}^{m} (\beta^z \alpha^k - \beta^l \alpha^j) \\ &= \beta^{z(m-1)} \prod_{1 \leq j \leq m, j \neq k} (\alpha^k - \alpha^j) \prod_{l \in I, l \neq z} [(\beta^z \alpha^k)^m - \beta^{lm}] \\ &= \beta^{z(m-1)} m\alpha^{-k} \prod_{l \in I, l \neq z} (\beta^{zm} - \beta^{lm}). \end{aligned}$$

Let $v = \prod_{l \in I, l \neq z} (\beta^{zm} - \beta^{lm})$, then

$$\begin{aligned} v^r &= \prod_{l\in I, l\neq z} (\beta^{zmr} - \beta^{lmr}) \quad (\text{since } \beta^{2(r+1)} = 1, \beta^r = -\beta^{-1}) \\ &= \prod_{l\in I, l\neq z} [(-\beta^{-1})^{zm} - (-\beta^{-1})^{lm}] \\ &= \prod_{l\in I, l\neq z} [(\beta^{-1})^{zm} - (\beta^{-1})^{lm}] \\ &= \prod_{l\in I, l\neq z} (\beta^{-1})^{zm+lm} (\beta^{lm} - \beta^{zm}) \\ &= (-1)^{t-1} \beta^{-(A+(t-2)z)m} v \end{aligned}$$

So $v^{r-1} = (-1)^{t-1}\beta^{-(A+(t-2)z)m}$.

Let $g$ be a generator of $\mathbb{F}_q^*$, then $\alpha = g^{\frac{q-1}{m}}, \beta = g^{\frac{r-1}{2}}, -1 = g^{\frac{r^2-1}{2}}, v = g^{\frac{r+1}{2}(t-1)-(A+(t-2)z)\frac{m}{2}+i(r+1)}$. Note that $\beta, m$ and $\alpha$ are square elements of $\mathbb{F}_q^*$, we take $\lambda = g^{\frac{r+1}{2}(t-1)}$, then $\lambda L_{\vec{a}}(\beta^z\alpha^k)$ is a square element of $\mathbb{F}_q^*$.

This implies there exists a $q$-ary $[n, \frac{n}{2}]$ MDS self-dual code. □

**Example 1.** *Let $r = 173, q = 173^2, r \equiv 1(\mathrm{mod} 4), m = 4 \times 43, \frac{q-1}{m} = 174$ is even. For $1 \leq t \leq \frac{2(r+1)}{gcd(2(r+1),m)} = 87$, we choose $t = 81$. By Theorem 1, there exists the MDS self-dual code with length $n = mt = 13{,}932$.*

**Theorem 2.** *Let $q = r^2$, where $r$ is an odd prime power. Suppose that $m$ is odd, $m \mid (q-1)$ and $\frac{q-1}{m}$ is even. If $1 \leq t \leq min\{\frac{r+1}{gcd(2(r+1),m)}, \frac{r+1}{2}\}$ and $t$ is odd, then there exists a $q$-ary $[n = tm+1, \frac{n}{2}]$ MDS self-dual code over $\mathbb{F}_q$.*

**Proof.** Let $\alpha$ and $\beta$ be the same as in Theorem 1, we choose $t$ distinct even number $i_1, i_2, \ldots, i_t$, $0 \leq i_1 < i_2 < \cdots < i_t < 2(r+1)$. Denote $I = \{i_1, i_2, \cdots, i_t\}, A = i_1 + i_2 + \ldots + i_t$. Suppose all $i_j \equiv 2(\mathrm{mod} 4), j = 1, 2, \cdots, t$. The proof is as similar as in Theorem 1. We get

$$L_{\vec{a}}(\beta^z\alpha^k) = \beta^{z(m-1)} m \alpha^{-k} \prod_{l\in I, l\neq z} (\beta^{zm} - \beta^{lm}).$$

Let $v = \prod_{l\in I, l\neq z} (\beta^{zm} - \beta^{lm})$, then we get

$$v^{r-1} = (-1)^{t-1}\beta^{-(A+(t-2)z)m}, v = g^{\frac{r+1}{2}(t-1) - \frac{(A+(t-2)z)m}{2} + i(r+1)},$$

since $\frac{A+(t-2)z}{2}$ is even, it implies that $v$ is a square element of $\mathbb{F}_q^*$. So $-L_{\vec{a}}(\beta^z\alpha^k)$ is square element of $\mathbb{F}_q^*$. By Lemma 3, there exists a $q$-ary $[n, \frac{n}{2}]$ MDS self-dual code. □

**Example 2.** *Let $r = 67, q = 67^2, m = 11, \frac{q-1}{m} = 408$ is even. Since $2(r+1) = 136 = 4 \times 34$, for $1 \leq t \leq \frac{r+1}{gcd(2(r+1),m)} = 68$, we choose $t = 27$. By Theorem 2, there exists the MDS self-dual code with length $n = mt + 1 = 298$.*

**Theorem 3.** *Let $q = r^2$, where $r$ is an odd prime power, $r \equiv 1(\mathrm{mod} 4)$. Suppose that $m$ is odd, $m \mid (q-1)$ and $\frac{q-1}{m}$ is even. If $1 \leq t \leq min\{\frac{r+1}{gcd(2(r+1),m)}, \frac{r+1}{2}\}$ and $t$ is odd, then there exists a $q$-ary $[n = tm+1, \frac{n}{2}]$ MDS self-dual code over $\mathbb{F}_q$.*

**Proof.** Let $\alpha$ and $\beta$ be the same as in Theorem 1, we choose $t$ distinct even number $i_1, i_2, \ldots, i_t$, $0 \le i_1 < i_2 < \cdots < i_t < 2(r+1)$. Denote $I = \{i_1, i_2, \cdots, i_t\}, A = i_1 + i_2 + \ldots + i_t$, and $i_j \equiv 2(\mathrm{mod}4), j = 1, 2, \cdots, t$. We define the generalized Reed -Solomon code $\mathbf{GRS}_k(\vec{a}, \vec{v})$ with

$$\vec{a} = (0, \alpha\beta^{i_1}, \ldots, \alpha^m\beta^{i_1}, \alpha\beta^{i_2}, \ldots, \alpha^m\beta^{i_2}, \ldots, \alpha\beta^{i_t}, \ldots, \alpha^m\beta^{i_t}).$$

For any $z \in I$ and $1 \le k \le m$, we get

$$\begin{aligned} L_{\vec{a}}(\beta^z\alpha^k) &= \beta^z\alpha^k \prod_{1\le j\le m, j\ne k}(\beta^z\alpha^k - \beta^z\alpha^j) \prod_{l\in I, l\ne z}\prod_{j=1}^{m}(\beta^z\alpha^k - \beta^l\alpha^j) \\ &= \beta^{zm} m \prod_{l\in I, l\ne z}(\beta^{zm} - \beta^{lm}) \end{aligned}$$

and

$$L_{\vec{a}}(0) = \prod_{l\in I}\prod_{j=1}^{m}(0 - \beta^l\alpha^j) = (-1)^{mt}\alpha^{\frac{m(m+1)}{2}}(\prod_{l\in I}\beta^l)^m.$$

Since $r \equiv 1(\mathrm{mod}4)$, $\frac{q-1}{m}$ is even, so $\alpha, \beta, m, -1$ are square elements of $\mathbb{F}_q^*$, we only need to consider $v = \prod_{l\in I, l\ne z}(\beta^{zm} - \beta^{lm})$. As the calculation in the proof of Theorem 1, $v = g^{\frac{r+1}{2}(t-1) - \frac{(A+(t-2)z)m}{2} + i(r+1)}$. Since all $i_j \equiv 2(\mathrm{mod}4)$ and $t$ is odd, so $\frac{(A+(t-2)z)m}{2}$ is even. $L_{\vec{a}}(\beta^z\alpha^k)$, $L_{\vec{a}}(0)$ are square elements of $\mathbb{F}_q^*$. By Lemma 2, there exists a $q$-ary $[n, \frac{n}{2}]$ MDS self-dual code. □

**Example 3.** *Let* $r = 101, r \equiv 1(\mathrm{mod}4), q = 101^2, m = 75, \frac{q-1}{m} = 136$ *is even. Since* $2(r+1) = 204 = 4 \times 51$, *for* $1 \le t \le \frac{r+1}{gcd(2(r+1), m)} = 34$, *we choose* $t = 33$. *By Theorem 2, there exists the MDS self-dual code with length* $n = mt + 1 = 2476$.

**Theorem 4.** *Let* $q = r^2$, *where r is an odd prime power. Suppose that* $m \mid (q-1)$, $\frac{q-1}{m}$ *is even. If* $1 \le t \le \frac{2(r+1)}{gcd(2(r+1), m)}$ *and tm is even, then there exists a q-ary* $[n = tm + 2, \frac{n}{2}]$ *MDS self-dual code over* $\mathbb{F}_q$.

**Proof.** Let $\alpha$ and $\beta$ be the same as in Theorem 1. We define the extended generalized Reed -Solomon code $\mathbf{GRS}_k(\vec{a}, \vec{v}, \infty)$ with

$$\vec{a} = (0, \alpha\beta^{i_1}, \cdots, \alpha^m\beta^{i_1}, \alpha\beta^{i_2}, \cdots, \alpha^m\beta^{i_2}, \cdots, \alpha\beta^{i_t}, \cdots, \alpha^m\beta^{i_t}).$$

For any $z \in I$ and $1 \le k \le m$, we get

$$\begin{aligned} L_{\vec{a}}(\beta^z\alpha^k) &= \beta^z\alpha^k \prod_{1\le j\le m, j\ne k}(\beta^z\alpha^k - \beta^z\alpha^j) \prod_{l\in I, l\ne z}\prod_{j=1}^{m}(\beta^z\alpha^k - \beta^l\alpha^j) \\ &= \beta^{zm} m \prod_{l\in I, l\ne z}(\beta^{zm} - \beta^{lm}) \end{aligned}$$

and

$$L_{\vec{a}}(0) = \prod_{l\in I}\prod_{j=1}^{m}(0 - \beta^l\alpha^j) = (-1)^{mt}\alpha^{\frac{m(m+1)}{2}}(\prod_{l\in I}\beta^l)^m.$$

**Case 1**: If $m$ is even, $t$ is odd.

$\beta^{zm}, m$ and $L_{\vec{a}}(0)$ are square elements of $\mathbb{F}_q^*$. Let $v = \prod_{l\in I, l\ne z}(\beta^{zm} - \beta^{lm})$, as the calculation in Theorem 1, $v = g^{\frac{r+1}{2}(t-1) - \frac{(A+(t-2)z)m}{2} + i(r+1)}$. So we only need to consider the parity of $\frac{(A+(t-2)z)m}{2}$.

- $i_1, i_2, \ldots, i_t$ are even number, so $A + (t-2)z \equiv 0(\mathrm{mod}2)$, $v$ is a square element of $\mathbb{F}_q^*$.
- $i_1, i_2, \ldots, i_t$ are odd number, so $A + (t-2)z \equiv 0(\mathrm{mod}2)$, $v$ is a square element of $\mathbb{F}_q^*$.

**Case 2**: If $m$ and $t$ are even, $r \equiv 3(\bmod 4)$, we assume $A$ is an even integer. It follows that $\frac{r+1}{2}(t-1) - \frac{(A+(t-2)z)m}{2}$ is an even integer.

**Case 3**: If $m$ is odd, $t$ is even.

- $t \equiv 0(\bmod 4)$
  (1) If $r \equiv 1(\bmod 4)$, all $i_1, i_2, \ldots, i_t$ are odd, and $A \equiv 0(\bmod 4)$, then then $(r+1)(t-1) - (A+(t-2)z)m \equiv 0(\bmod 4), v$ is a square element of $\mathbb{F}_q^*$.
  (2) If $r \equiv 3(\bmod 4)$, all $i_1, i_2, \ldots, i_t$ are even, and $A \equiv 2(\bmod 4)$, then $(r+1)(t-1) - (A+(t-2)z)m \equiv 0(\bmod 4), v$ is a square element of $\mathbb{F}_q^*$.
- $t \equiv 2(\bmod 4)$.
  (1) If $r \equiv 1(\bmod 4), A \equiv 2(\bmod 4)$, then $(r+1)(t-1) - (A+(t-2)z)m \equiv 0(\bmod 4), v$ is square of $\mathbb{F}_q^*$.
  (2) If $r \equiv 3(\bmod 4), A \equiv 0(\bmod 4)$, then $(r+1)(t-1) - (A+(t-2)z)m \equiv 0(\bmod 4), v$ is square of $\mathbb{F}_q^*$.

□

We can extend the Theorem 1 to a more general case.

**Theorem 5.** *Let $q = r^2$, where $r$ is an odd prime power. Suppose that $m \mid (q-1)$, $\frac{q-1}{m}$ is even, $s \mid m, s \mid r-1$ and $\frac{r-1}{s}$ is even. If $1 \le t \le \frac{s(r+1)}{gcd(s(r+1),m)}$, then there exists a $q$-ary $[n = tm, \frac{n}{2}]$ MDS self-dual code over $\mathbb{F}_q$.*

**Proof.** Let $\alpha$ be a primitive $m$-th root of unity and $\mathbf{H} =< \beta >$ is the cyclic group of order $s(r+1)$. By the theorem of group homomorphism,

$$(\mathbf{H} \times \langle\alpha\rangle)/\langle\alpha\rangle \cong \mathbf{H}/(\mathbf{H} \cap \langle\alpha\rangle),$$

Let $i_1, i_2, \ldots, i_t$ be $t$ distinct elements, such that $0 \le i_1 < i_2 < \cdots < i_t < 2(r+1)$. Denote $I = \{i_1, i_2, \ldots, i_t\}, A = i_1 + i_2 + \ldots + i_t$ and $\mathbf{B} = \{\beta^{i_1}, \beta^{i_2}, \ldots, \beta^{i_t}\}$ be a set of coset representatives of $\mathbf{H} \times \langle\alpha\rangle$. Let

$$\vec{a} = (\alpha\beta^{i_1}, \cdots, \alpha^m\beta^{i_1}, \alpha\beta^{i_2}, \cdots, \alpha^m\beta^{i_2}, \cdots, \alpha\beta^{i_t}, \cdots, \alpha^m\beta^{i_t}).$$

Similar with Theorem 1, we get

$$\begin{aligned} L_{\vec{a}}(\beta^z\alpha^k) &= \prod_{1\le j\le m, j\ne k}(\beta^z\alpha^k - \beta^z\alpha^j)\prod_{l\in I, l\ne z}\prod_{j=1}^{m}(\beta^z\alpha^k - \beta^l\alpha^j) \\ &= \beta^{z(m-1)} \cdot m \cdot \alpha^{-k}\prod_{l\in I, l\ne z}(\beta^{zm} - \beta^{lm}.) \end{aligned}$$

Since $\beta^{s(r+1)} = 1$, then $\beta^{r+1} = \xi_s$, where $\xi_s$ is $s$-th primitive root of unity. So $\beta^r = \xi_s\beta^{-1}$. Let $v = \prod_{l\in I, l\ne z}(\beta^{zm} - \beta^{lm})$. Since $s \mid m$, then

$$\begin{aligned} v^r &= \prod_{l\in I, l\ne z}((\beta^{-1})^{zm} - (\beta^{-1})^{lm}) \\ &= \prod_{l\in I, l\ne z}\beta^{-(l+z)m}(\beta^{lm} - \beta^{zm}) \\ &= (-1)^{t-1}\beta^{-(A+(t-2)z)m}v. \end{aligned}$$

So $v^{r-1} = (-1)^{t-1}\beta^{-(A+(t-2)z)m}$.

Let $g$ be a generator of $\mathbb{F}_q^*$. It follows that $\beta = g^{\frac{r-1}{s}}$ and $-1 = g^{\frac{r^2-1}{2}}$. So

$$v = g^{\frac{(r+1)}{2}(t-1)-[A+(t-2)z]\frac{m}{s}}.$$

**Case 1**: If $m$ odd and $t$ even, we can take $\lambda = g^{\frac{(r+1)}{2}(t-1)-A\cdot\frac{m}{s}}$. Hence, we have $\lambda L_{\vec{a}}(\beta^z\alpha^k)$ is square element of $\mathbb{F}_q^*$.

**Case 2**: If $m$ even and $2 \mid \frac{m}{s}$, we can take $\lambda = g^{\frac{(r+1)}{2}(t-1)}$. Hence, we have $\lambda L_{\vec{a}}(\beta^z\alpha^k)$ is square element of $\mathbb{F}_q^*$.

So there exists a $q$-ary MDS self-dual code with length $n$. □

## 4. Conclusions

In this paper, based on the method from [9], we construct several classes of MDS self-dual code over finite fields with odd characteristics via the generalized Reed-Solomon code and extend the generalized Reed-Solomon code.

**Author Contributions:** Original ideas, writing, original draft preparation, A.Z.; review, Z.J.; funding acquisition, A.Z.

**Funding:** This research was funded by the National Natural Science Foundation of China under Grants 11401468.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Dau, S.H.; Song, W.; Yuen, C. On the existence of MDS codes over small fields with constrained generator matrices. In Proceedings of the 2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, 29 June–4 July 2014; pp. 1787–1791.
2. Pedersen, J.P.; Dahl, C. Classification of pseudo-cyclic MDS codes. *IEEE Trans. Inf. Theory* **1991**, *37*, 365–370. [CrossRef]
3. Dau, S.H.; Song, W.; Dong, Z.; Yuen, C. Balanced sparsest generator matrices for MDS codes. In Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013; pp. 1889–1893.
4. Roth, R.M.; Lempel, A. A construction of non-Reed-Solomon type MDS codes. *IEEE Trans. Inf. Theory* **1989**, *35*, 655–657. [CrossRef]
5. Chen, B.; Liu, H. New constructions of MDS codes with complementary dual. *IEEE Trans. Inf. Theory* **2018**, *64*, 5776–5782. [CrossRef]
6. Carlet, C.; Mesnager, S.; Tang, C.; Qi, Y. Euclidean and hermitian LCD MDS codes. *Des. Codes Cryptogr.* **2018**, *86*, 2605–2618. [CrossRef]
7. Blaum, M.; Roth, R.M. On lowest density MDS codes. *IEEE Trans. Inf. Theory* **1999**, *45*, 46–59. [CrossRef]
8. Grassl, M.; Gulliver, T.A. On self-dual MDS codes. In Proceedings of the 2008 IEEE International Symposium on Information Theory, Toronto, ON, Canada, 6–11 July 2008; pp. 1954–1957.
9. Fang, X.; Labad, K.; Liu, H.; Luo, J. New parameters on MDS self-dual codes over finite fields. *arXiv* **2018**, arXiv:1811.02802vl.
10. Guenda, K. New MDS self-dual codes over finite fields. *Des. Codes Cryptogr.* **2012**, *62*, 31–42. [CrossRef]
11. Jin, L.; Xing, C. New MDS self-dual codes from generalized Reed-Solomon codes. *IEEE Trans. Inf. Theory* **2017**, *63*, 1434–1438. [CrossRef]
12. Labad, K.; Liu, H.; Luo, J. Construction of MDS self-dual codes over finite fields. *arXiv* **2018**, arXiv:1807.10625vl.
13. Kim, J.L.; Lee, Y. Euclidean and Hermitian self-dual MDS codes over large finite fields. *J. Comb. Theory Ser. A* **2006**, *105*, 79–95. [CrossRef]

14. Yan, H. A Note on the Construction of MDS Self-Dual Codes. *Cryptogr. Commun.* **2018**. [CrossRef]
15. MacWilliams, F.J.; Sloane, N.J.A. *The Theory of Error-Correcting Codes*; Elsevier: Amsterdam, The Netherland, 1977.