Quantum Information Processing (2020) 19:16
https://doi.org/10.1007/s11128-019-2506-0

New quantum MDS codes over finite fields

Xiaolei Fang[1] · Jinquan Luo[1]

Received: 17 June 2019 / Accepted: 13 November 2019 / Published online: 26 November 2019

Abstract
In this paper, we present three new classes of q-ary quantum MDS codes utilizing generalized Reed–Solomon codes satisfying Hermitian self-orthogonal property. Among our constructions, the minimum distance of some q-ary quantum MDS codes can be bigger than $\frac{q}{2}+1$. Comparing to previous known constructions, the lengths of codes in our constructions are more flexible.

Keywords Quantum MDS code · Generalized Reed–Solomon code · Hermitian construction · Hermitian self-orthogonal

1 Introduction

Quantum error-correcting codes play an important role in quantum information transmission and quantum computation. Due to the establishment of the connections between quantum codes and classical codes (see [2,4,23]), great progress has been made in the study of quantum error-correcting codes. One of these connections shows that quantum codes can be constructed from classical linear error-correcting codes satisfying symplectic, Euclidean or Hermitian self-orthogonal properties (see [1,13,24]).

Let q be a prime power. We use $[[n, k, d]]_q$ to denote a q-ary quantum code of length n, dimension q^k and minimum distance d. Similar to the classical counterparts, quantum codes have to satisfy the quantum Singleton bound: $k \leq n-2d+2$. The quantum code attaching this bound is called quantum maximum distance separable(MDS) code.

In the past few decades, quantum MDS codes have been extensively studied. The construction of q-ary quantum MDS codes with length $n \leq q+1$ has been investigated

✉ Jinquan Luo
luojinquan@mail.ccnu.edu.cn

Xiaolei Fang
fangxiaolei@mails.ccnu.edu.cn

[1] School of Mathematics and Statistics and Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Wuhan 430079, China

from classical Euclidean orthogonal codes (see [7,20]). On the other hand, some quantum MDS codes with length $n \geq q+1$ have been investigated, most of which have minimum distances less than $\frac{q}{2}+1$ (see [11]). So it is a challenging and valuable task to construct quantum MDS codes with minimal distances larger than $\frac{q}{2}+1$. Recently, researchers have constructed some of such quantum MDS codes utilizing constacyclic codes, negacyclic codes and generalized Reed–Solomon codes (see [3,5,6,8–12,14–17,21,22,25–28]). However, q-ary quantum MDS codes with minimal distances bigger than $\frac{q}{2}+1$ are far from complete.

There are dozens of papers on the construction of $[[n, n-2d, d+1]]_q$ quantum MDS codes with relatively large minimum distances. Most of the known $[[n, n-2d, d+1]]_q$ quantum MDS codes with minimum distances larger than $\frac{q}{2}+1$ have lengths $n \equiv 0, 1 \pmod{q+1}$ (see [3,5,7,9,11,14,15,21,22,28]) or $n \equiv 0, 1 \pmod{q-1}$ (see [5,7,9–12,14,21,22,25,28]), except for the following cases.

(i). $n = q^2 - l$ and $d \leq q - l - 1$ for $0 \leq l \leq q-2$ (see [17]).
(ii). $n = mq - l$ and $d \leq m - l$ for $0 \leq l < m$ and $1 < m < q$ (see [17] and also [6] for $l = 0$).
(iii). $n = t(q+1)+2$ and $1 \leq d \leq t+1$ for $1 \leq t \leq q-1$ and $(p, t, d) \neq (2, q-1, q)$ (see [6] and also [17] for $t = q-1$).

In this paper, we construct several new classes of quantum MDS codes whose minimum distances can be larger than $\frac{q}{2}+1$ via generalized Reed–Solomon codes and Hermitian construction. Their lengths are different from the above three cases and also in most cases are not of the form $n \equiv 0, 1 \pmod{q \pm 1}$. More precisely, the parameters of $[[n, n-2d, d+1]]_q$ quantum MDS codes are as follows:

(i). $n = 1 + lh + mr - \frac{q^2-1}{st} \cdot hr$ and $1 \leq d \leq \min\{\frac{s+h}{2} \cdot \frac{q+1}{s} - 1, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$, for odd $s \mid q+1$, even $t \mid q-1$, $t \geq 2$, $l = \frac{q^2-1}{s}$, $m = \frac{q^2-1}{t}$, odd $h \leq s-1$, $r \leq t$ and $q - 1 > \frac{q^2-1}{st} \cdot hr$ (see Theorem 3);
(ii). $n = lh + mr - \frac{q^2-1}{st} \cdot hr$ and $1 \leq d \leq \min\{\lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 2, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$, for odd $s \mid q+1$, even $t \mid q-1$, $t \geq 2$, $l = \frac{q^2-1}{s}$, $m = \frac{q^2-1}{t}$, $h \leq s-1$, $r \leq t$ and $q - 1 > \frac{q^2-1}{st} \cdot hr$ (see Theorem 4);
(iii). $n = lh + mr$ and $1 \leq d \leq \min\{\lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 2, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$, for even $s \mid q+1$, even $t \mid q-1$, $t \geq 2$, $l = \frac{q^2-1}{s}$, $m = \frac{q^2-1}{t}$, $h \leq \frac{s}{2}$ and $r \leq \frac{t}{2}$ (see Theorem 5).

This paper is organized as follows. In Sect. 2, we will introduce some basic knowledge and useful results on Hermitian self-orthogonality and generalized Reed–Solomon codes, which will be utilized in the proof of main results. In Sects. 3, 4 and 5, we will present our main results on the constructions of quantum MDS codes. In Sect. 6, we will make a conclusion.

2 Preliminaries

In this section, we introduce some basic notations and useful results on Hermitian self-orthogonality and generalized Reed–Solomon codes (or GRS codes for short).

Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements and $\mathbb{F}_{q^2}^* = \mathbb{F}_{q^2}\backslash\{0\}$, where q is a prime power. Obviously, $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^2}$ with q elements and denoted by $\mathbb{F}_q^* = \mathbb{F}_q\backslash\{0\}$. For any two vectors $\overrightarrow{x} = (x_1, \ldots, x_n)$ and $\overrightarrow{y} = (y_1, \ldots, y_n) \in \mathbb{F}_{q^2}$, the Euclidean and Hermitian inner products are defined as

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = \sum_{i=1}^{n} x_i y_i$$

and

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle_H = \sum_{i=1}^{n} x_i y_i^q,$$

respectively.

For a linear code C of length n over $\mathbb{F}_{q^2}$, the Euclidean dual code of C is defined as

$$C^{\perp} := \{\overrightarrow{x} \in \mathbb{F}_{q^2}^n : \langle \overrightarrow{x}, \overrightarrow{y} \rangle = 0, \text{ for all } \overrightarrow{y} \in C\},$$

and the Hermitian dual code of C is defined as

$$C^{\perp_H} := \{\overrightarrow{x} \in \mathbb{F}_{q^2}^n : \langle \overrightarrow{x}, \overrightarrow{y} \rangle_H = 0, \text{ for all } \overrightarrow{y} \in C\}.$$

If $C \subseteq C^{\perp_H}$, the code C is called Hermitian self-orthogonal.

Ashikhmin and Knill [2] proposed the Hermitian construction of quantum codes, which is a very important technique for constructing quantum codes from classical codes.

Theorem 1 [2, Corollary 1] *A q-ary quantum $[[n, n-2d, d+1]]_q$ MDS code exists provided that an $[n, d, n-d+1]_{q^2}$ MDS Hermitian self-orthogonal code exists.*

Choose two vectors $\overrightarrow{v} = (v_1, v_2, \ldots, v_n)$ and $\overrightarrow{a} = (a_1, a_2, \ldots, a_n)$, where $v_i \in \mathbb{F}_{q^2}^*$ (v_i may not be distinct) and a_i are distinct elements in $\mathbb{F}_{q^2}$. For an integer d with $1 \le d \le n$, the GRS code of length n associated with $\overrightarrow{v}$ and $\overrightarrow{a}$ is defined as follows:

$$\mathbf{GRS}_d(\overrightarrow{a}, \overrightarrow{v}) = \{(v_1 f(a_1), \ldots, v_n f(a_n)) : f(x) \in \mathbb{F}_{q^2}[x], \deg(f(x)) \le d-1\}. \tag{1}$$

A generator matrix of the code $\mathbf{GRS}_d(\overrightarrow{a}, \overrightarrow{v})$ is

$$G_d(\overrightarrow{a}, \overrightarrow{v}) = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1a_1 & v_2a_2 & \cdots & v_na_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1a_1^{d-1} & v_2a_2^{d-1} & \cdots & v_na_n^{d-1} \end{pmatrix}. \tag{2}$$

It is well known that the code $\mathbf{GRS}_d(\overrightarrow{a}, \overrightarrow{v})$ is a q-ary $[n, d, n-d+1]$ MDS code [18, Chapter 11]. The following theorem will be useful, and it has been shown in [19,28].

Theorem 2 [19,28] *The two vectors* $\overrightarrow{a} = (a_1, \ldots, a_n)$ *and* $\overrightarrow{v} = (v_1, \ldots, v_n)$ *are defined above. Then,* $\mathbf{GRS}_d(\overrightarrow{a}, \overrightarrow{v})$ *is Hermitian self-orthogonal if and only if* $\langle \overrightarrow{a}^{qi+j}, \overrightarrow{v}^{q+1}\rangle = 0$, *for all* $0 \le i, j \le d-1$.

If there are no specific statements, the following notations are fixed throughout this paper.

- Let $s \mid q+1$ and $t \mid q-1$ with t even.
- Let $l = \frac{q^2-1}{s}$ and $m = \frac{q^2-1}{t}$.
- Let g be a primitive element of $\mathbb{F}_{q^2}$, $\delta = g^s$ and $\theta = g^t$.

Lemma 2.1 *Suppose* $\gcd(s,t) = 1$. *For any* $\alpha, \beta \in \mathbb{Z}_{q^2-1}$, *the number of* (i, j) *of the equation* $\alpha + si \equiv \beta + tj \pmod{q^2-1}$ *satisfying* $0 \le i < \frac{q^2-1}{s}$ *and* $0 \le j < \frac{q^2-1}{t}$ *is* $\frac{q^2-1}{st}$.

Proof Let $\beta - \alpha = \gamma$. From $\alpha + si \equiv \beta + tj \pmod{q^2-1}$, we have $si - tj \equiv \gamma \pmod{q^2-1}$. When $0 \le i < \frac{q^2-1}{s}$ and $0 \le j < \frac{q^2-1}{t}$, $si - tj \bmod q^2-1$ runs $\frac{q^2-1}{st}$ times through every element of $\mathbb{Z}_{q^2-1}$.

Indeed, for any $\gamma \in \mathbb{Z}_{q^2-1}$, we have $si - tj \equiv \gamma \pmod{q^2-1} \Leftrightarrow s \mid tj + \gamma \Leftrightarrow tj \equiv -\gamma \pmod{s}$. Since $\gcd(s,t) = 1$, then $j \bmod s$ is unique. So when $0 \le j < \frac{q^2-1}{t}$, the number of j satisfying the equation is $\frac{q^2-1}{st}$. The values of γ and i will be determined after fixing j. So the number of (i, j) of the equation $\alpha + si \equiv \beta + tj \pmod{q^2-1}$ is $\frac{q^2-1}{st}$ satisfying $0 \le i < \frac{q^2-1}{s}$ and $0 \le j < \frac{q^2-1}{t}$ is $\frac{q^2-1}{st}$. □

The following two lemmas have been shown in [5,9]. In order to make the paper self-completeness, we will give proofs.

Lemma 2.2 [5, Lemmas 5 and 11] *Assume that* $h \le s-1$.

(i). *For any* $0 \le i, j \le \lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 3$, $l \mid (qi + j + q + 1)$ *if and only if* $qi + j + q + 1 = \mu \cdot l$, *with* $\lceil \frac{s-h}{2} \rceil + 1 \le \mu \le \lfloor \frac{s+h}{2} \rfloor - 1$.

(ii). *For any* $0 \le i, j \le \lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 2$ *with* $(i, j) \ne (0, 0)$, $l \mid (qi + j)$ *if and only if* $qi + j = \mu \cdot l$, *with* $\lceil \frac{s-h}{2} \rceil + 1 \le \mu \le \lfloor \frac{s+h}{2} \rfloor - 1$.

Proof (i). When $s \equiv h \pmod 2$, it implies $\lfloor \frac{s+h}{2} \rfloor = \frac{s+h}{2}$ and $\lceil \frac{s-h}{2} \rceil = \frac{s-h}{2}$. Since $0 \le i, j \le \frac{s+h}{2} \cdot \frac{q+1}{s} - 3 < q - 2$, $0 < qi + j + q + 1 < q^2 - 1$, that is $0 < \mu < s$. From $qi + j + q + 1 = q\left(\frac{\mu\cdot(q+1)}{s} - 1\right) + \left(q - \frac{\mu\cdot(q+1)}{s}\right)$, it follows that

$$i = \frac{\mu \cdot (q+1)}{s} - 2, \quad j = q - \frac{\mu \cdot (q+1)}{s} - 1.$$

By $i < \frac{s+h}{2} \cdot \frac{q+1}{s} - 2$ and $j < \frac{s+h}{2} \cdot \frac{q+1}{s} - 2$, it implies $\frac{s-h}{2} < \mu < \frac{s+h}{2}$. So $l \mid (qi + j)$ if and only if $qi + j = \mu \cdot l$, with $\frac{s-h}{2} + 1 \le \mu \le \frac{s+h}{2} - 1$.
When $s \not\equiv h \pmod 2$, it implies $\lfloor \frac{s+h}{2} \rfloor = \frac{s+h-1}{2}$ and $\lceil \frac{s-h}{2} \rceil = \frac{s-h+1}{2}$. Then, the proof can be completed by proceeding as the situation that $s \equiv h \pmod 2$.

(ii). In a similar way, we can complete the proof. So we omit the details.

□

Lemma 2.3 [9, Lemma 3.1] *The identity* $\sum_{\nu=0}^{m-1} \theta^{\nu\left(qi+j+\frac{q+1}{2}\right)} = 0$ *holds for all* $0 \le i, j \le \frac{q+1}{2} + \frac{q-1}{t} - 2$*, with even* $t \ge 2$.

Proof It is easy to check that the identity holds if and only if $m \nmid qi + j + \frac{q+1}{2}$. On the contrary, assume that $m \mid qi + j + \frac{q+1}{2}$. Let

$$qi + j + \frac{q+1}{2} = \mu \cdot m = q \cdot \frac{\mu(q-1)}{t} + \frac{\mu(q-1)}{t} \tag{3}$$

with $\mu \in \mathbb{Z}$. By $t \ge 2$, we have $qi + j + \frac{q+1}{2} < q^2 - 1$, which implies $0 < \mu < t$.

- If $j + \frac{q+1}{2} \le q - 1$, comparing remainder and quotient of module q on both sides of (3), we can deduce $i = j + \frac{q+1}{2} = \mu \cdot \frac{q-1}{t}$. Since t is even, $\frac{q-1}{t} \mid \frac{q-1}{2}$. From $\frac{q-1}{t} \mid j+1+\frac{q-1}{2}$, we can deduce that $\frac{q-1}{t} \mid j+1$. Since $j+1 \ge 1$, $j+1 \ge \frac{q-1}{t}$. So $i = j + \frac{q+1}{2} \ge \frac{q+1}{2} + \frac{q-1}{t} - 1$, which is a contradiction.
- When $j + \frac{q+1}{2} \ge q$, it takes $qi + j + \frac{q+1}{2} = q(i+1) + \left(j - \frac{q-1}{2}\right) = q \cdot \frac{\mu(q-1)}{t} + \frac{\mu(q-1)}{t}$. In a similar way, $j - \frac{q-1}{2} = i + 1 = \mu \cdot \frac{q-1}{t}$ which implies $\frac{q-1}{t} \mid i + 1$. Since $i + 1 \ge 1$, $i + 1 \ge \frac{q-1}{t}$. Therefore, $j = i + 1 + \frac{q-1}{2} \ge \frac{q+1}{2} + \frac{q-1}{t} - 1$, which is a contradiction.

As a result, $m \nmid qi + j + \frac{q+1}{2}$ which yields $\sum_{\nu=0}^{m-1} \theta^{\nu(qi+j+\frac{q+1}{2})} = 0$ for all $0 \le i, j \le \frac{q+1}{2} + \frac{q-1}{t} - 2$. □

3 Quantum MDS codes of length $n = 1 + lh + mr - \frac{q^2-1}{st} \cdot hr$

In this section, we assume that **s is odd**, $\mathbf{h \le s - 1}$ with **h odd** and $\mathbf{r \le t}$. Quantum MDS codes of length $n = 1 + lh + mr - \frac{q^2-1}{st} \cdot hr$ will be constructed. The construction is based on [5,9]. Firstly, we choose elements in $\mathbb{F}_{q^2}^*/\langle\delta\rangle$ as the first part of coordinates in the vector $\overrightarrow{a}$. Secondly, we choose elements from cosets of $\mathbb{F}_{q^2}^*/\langle\theta\rangle$ as the second part of coordinates in $\overrightarrow{a}$. Finally, we consider the duplicating elements between these two parts. We construct the vector $\overrightarrow{v}$ in a similar way. Then, we can construct quantum MDS codes of length $n = 1 + lh + mr - \frac{q^2-1}{st} \cdot hr$, whose minimum distances can be bigger than $\frac{q}{2} + 1$.

The next lemma has been shown in [5]. We give a new proof by Cramer's rule, which is shorter than [5].

Lemma 3.1 [5, Lemma 7] *For* $\frac{s-h}{2} + 1 \leq \mu \leq \frac{s+h}{2} - 1$, *there exists a solution in* $(\mathbb{F}_q^*)^h$ *of the following system of equations*

$$\begin{cases} u_0 + u_1 + \cdots + u_{h-1} = 1 \\ \sum_{k=0}^{h-1} g^{k\mu l} u_k = 0 \end{cases} \tag{4}$$

Proof Denote $\xi = g^l$ and $c = \frac{s-h}{2} + 1$. For any $0 \leq \nu \neq \nu' \leq h-2 < s-2$, the elements $\xi^{c+\nu}, \xi^{c+\nu'}$ and 1 are distinct. The system of Eq. (4) can be expressed in the matrix form

$$A\overrightarrow{u}^T = (1, 0, \ldots, 0)^T, \tag{5}$$

where

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \xi^c & \cdots & \xi^{(h-1)c} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{c+h-2} & \cdots & \xi^{(h-1)(c+h-2)} \end{pmatrix}_{h\times h}$$

and

$$\overrightarrow{u} = (u_0, u_1, \ldots, u_{h-1}).$$

We will show that $u_k \in \mathbb{F}_q^*$ for any $0 \leq k \leq h-1$.

It is obvious that $\det(A) \neq 0$. By Cramer's rule,

$$u_k = \frac{(-1)^k \cdot \det(D_k)}{\det(A)},$$

where

$$D_k = \begin{pmatrix} 1 & \xi^c & \cdots & \xi^{(k-1)c} & \xi^{(k+1)c} & \cdots & \xi^{(h-1)c} \\ 1 & \xi^{c+1} & \cdots & \xi^{(k-1)(c+1)} & \xi^{(k+1)(c+1)} & \cdots & \xi^{(h-1)(c+1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{c+h-2} & \cdots & \xi^{(k-1)(c+h-2)} & \xi^{(k+1)(c+h-2)} & \cdots & \xi^{(h-1)(c+h-2)} \end{pmatrix} \tag{6}$$

is an $(h-1)\times(h-1)$ matrix obtained from A by deleting the first row and the $(k+1)$th column with $0 \le k \le h-1$. It is easy to see $\det(D_k)$ is equal to nonzero constant times of a Vandermonde determinant. So $\det(D_k) \neq 0$, which implies $u_k \neq 0$.

It remains to show $u_k \in \mathbb{F}_q$, for any $0 \le k \le h-1$. Since $s \mid q+1$ and $\xi^s = 1$,

$$\xi^{k(c+\nu)q} = \xi^{-k\left(\frac{s-h}{2}+1+\nu\right)} = \xi^{k\left(\frac{s+h}{2}-1-\nu\right)} = \xi^{k(c+h-2-\nu)},$$

for any $0 \le k \le h-1$ and $0 \le \nu \le h-2$. So $(\det(A))^q = (-1)^{\frac{h-1}{2}} \cdot \det(A)$ and $\det(D_k)^q = (-1)^{\frac{h-1}{2}} \cdot \det(D_k)$. It follows that $u_k^q = \frac{(-1)^{qk}\cdot\det(D_k)^q}{(\det(A))^q} = \frac{(-1)^k\cdot\det(D_k)}{\det(A)} = u_k$, which implies $u_k \in \mathbb{F}_q^*$ with $0 \le k \le h-1$. This completes the proof. $\square$

Now, we let $\overrightarrow{u} = (u_0, u_1, \ldots, u_{h-1})$ satisfy the system of Eq. (4). Choose

$$\overrightarrow{a}_1 = (0, 1, \delta, \ldots, \delta^{l-1}, g, g\delta, \ldots, g\delta^{l-1}, \ldots, g^{h-1}, g^{h-1}\delta, \ldots, g^{h-1}\delta^{l-1})$$

and

$$\overrightarrow{v}_1 = (e, \underbrace{v_0, \ldots, v_0}_{l \text{ times}}, \ldots, \underbrace{v_{h-1}, \ldots, v_{h-1}}_{l \text{ times}}),$$

where $v_k^{q+1} = u_k$ $(0 \le k \le h-1)$ and $e^{q+1} = -l$. Then, we have the following lemma, which has been shown in [5]. We give proof in order to make the paper self-completeness.

Lemma 3.2 [5, Theorem 3] *The identity*

$$\langle \overrightarrow{a}_1^{\,qi+j}, \overrightarrow{v}_1^{\,q+1} \rangle = 0$$

holds for all $0 \le i, j \le \frac{s+h}{2} \cdot \frac{q+1}{s} - 2$.

Proof When $(i, j) = (0, 0)$,

$$\langle \overrightarrow{a}_1^{\,0}, \overrightarrow{v}_1^{\,q+1} \rangle = e^{q+1} + l(v_0^{q+1} + \cdots + v_{h-1}^{q+1}) = -l + l(u_0 + \cdots + u_{h-1}) = 0.$$

When $(i, j) \neq (0, 0)$, since δ is of order l,

$$\langle \overrightarrow{a}_1^{\,qi+j}, \overrightarrow{v}_1^{\,q+1} \rangle = \sum_{k=0}^{h-1} g^{k(qi+j)} v_k^{q+1} \sum_{\nu=0}^{l-1} \delta^{\nu(qi+j)} = \begin{cases} 0, & l \nmid qi+j, \\ l \cdot \sum\limits_{k=0}^{h-1} g^{k(qi+j)} v_k^{q+1}, & l \mid qi+j. \end{cases}$$

We consider the case $l \mid qi+j$. According to Lemma 2.2 (ii) and Lemma 3.1,

$$\langle \overrightarrow{a}_1^{\,qi+j}, \overrightarrow{v}_1^{\,q+1} \rangle = \langle \overrightarrow{a}_1^{\,\mu l}, \overrightarrow{v}_1^{\,q+1} \rangle = l \cdot \sum_{k=0}^{h-1} g^{k\mu l} v_k^{q+1} = l \cdot \sum_{k=0}^{h-1} g^{k\mu l} u_k = 0.$$

Therefore, the result holds. □

For the second part of $\overrightarrow{a}$ and $\overrightarrow{v}$, we choose

$$\overrightarrow{a}_2 = (1, \theta, \ldots, \theta^{m-1}, g, g\theta, \ldots, g\theta^{m-1}, \ldots, g^{r-1}, g^{r-1}\theta, \ldots, g^{r-1}\theta^{m-1})$$

and

$$\overrightarrow{v}_2 = (1, g^{\frac{t}{2}}, \ldots, g^{(m-1)\cdot\frac{t}{2}}, 1, g^{\frac{t}{2}}, \ldots, g^{(m-1)\cdot\frac{t}{2}}, \ldots, 1, g^{\frac{t}{2}}, \ldots, g^{(m-1)\cdot\frac{t}{2}}).$$

Then, the following lemma can be obtained.

Lemma 3.3 *The identity*

$$\langle \overrightarrow{a}_2^{qi+j}, \overrightarrow{v}_2^{q+1} \rangle = 0$$

holds for all $0 \le i, j \le \frac{q+1}{2} + \frac{q-1}{t} - 2$.

Proof By Lemma 2.3, we can calculate directly

$$\begin{aligned} \langle \overrightarrow{a}_2^{qi+j}, \overrightarrow{v}_2^{q+1} \rangle &= \sum_{k=0}^{r-1} \sum_{\nu=0}^{m-1} (g^k \theta^\nu)^{qi+j} \cdot \theta^{\nu \cdot \frac{q+1}{2}} \\ &= \sum_{k=0}^{r-1} g^{k(qi+j)} \sum_{\nu=0}^{m-1} \theta^{\nu(qi+j+\frac{q+1}{2})} \\ &= 0. \end{aligned} \tag{7}$$

□

Now, we give our first construction.

Theorem 3 *Let* $n = 1 + lh + mr - \frac{q^2-1}{st} \cdot hr$, *where odd* $s \mid q+1$, *even* $t \mid q-1$, $t \ge 2$, $l = \frac{q^2-1}{s}$, $m = \frac{q^2-1}{t}$, *odd* $h \le s-1$ *and* $r \le t$. *If* $q - 1 > \frac{q^2-1}{st} \cdot hr$, *then for any* $1 \le d \le \min\{\frac{s+h}{2} \cdot \frac{q+1}{s} - 1, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$, *there exists an* $[[n, n-2d, d+1]]_q$ *quantum MDS code.*

Proof Denote

$$A = \{g^\alpha \delta^i | 0 \le \alpha \le h-1, \quad 0 \le i \le l-1\}$$

and

$$B = \{g^\beta \theta^j | 0 \le \beta \le r-1, \quad 0 \le j \le m-1\}.$$

From Lemma 2.1, we know $|A \cap B| = \frac{q^2-1}{st} \cdot hr$. Let $A_1 = A - B$ and $B_1 = B - A$. Define

$$f_1 : A \cup \{0\} \to \mathbb{F}_q^*, \quad f_1(g^\alpha \delta^i) = v_\alpha^{q+1} \quad \text{and} \quad f_1(0) = -l,$$
$$f_2 : B \to \mathbb{F}_q^*, \quad f_2(g^\beta \theta^j) = \theta^{j \cdot \frac{q+1}{2}}.$$

Let

$$\overrightarrow{a} = (0, \overrightarrow{a}_{A_1}, \overrightarrow{a}_{B_1}, \overrightarrow{a}_{A\cap B}),$$

where $\overrightarrow{a}_S = (a_1, \dots, a_k)$ for $S = \{a_1, \dots, a_k\}$ and

$$\overrightarrow{v}^{q+1} = (-l, f_1(\overrightarrow{a}_{A_1}), \lambda f_2(\overrightarrow{a}_{B_1}), f_1(\overrightarrow{a}_{A\cap B}) + \lambda f_2(\overrightarrow{a}_{A\cap B})),$$

where $\lambda \in \mathbb{F}_q^*$ and $f_j(\overrightarrow{a}_S) = (f_j(a_1), \dots, f_j(a_k))$ with $S = \{a_1, \dots, a_k\}$ and $j = 1, 2$.

Indeed, since $q - 1 > \frac{q^2-1}{st} \cdot hr = |A \cap B|$, there exists $\lambda \in \mathbb{F}_q^*$ such that all coordinates of $f_1(\overrightarrow{a}_{A\cap B}) + \lambda f_2(\overrightarrow{a}_{A\cap B})$ are nonzero.

According to Lemmas 3.2 and 3.3, it takes

$$\langle \overrightarrow{a}^{qi+j}, \overrightarrow{v}^{q+1} \rangle = \langle \overrightarrow{a}_1^{qi+j}, \overrightarrow{v}_1^{q+1} \rangle + \lambda \langle \overrightarrow{a}_2^{qi+j}, \overrightarrow{v}_2^{q+1} \rangle = 0,$$

for any $0 \le i, j \le d-1$. As a consequence, by Theorem 2, $\mathbf{GRS}_d(\overrightarrow{a}, \overrightarrow{v})$ is Hermitian self-orthogonal. Therefore, by Theorem 1, there exists an $[[n, n-2d, d+1]]_q$ quantum MDS code, where $n = 1 + lh + mr - \frac{q^2-1}{st} \cdot hr$ and $1 \le d \le \min\{\frac{s+h}{2} \cdot \frac{q+1}{s} - 1, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$. □

Remark 3.1 We try to choose s, h, t such that $\frac{s+h}{2} \cdot \frac{q+1}{s} - 1 \approx \frac{q+1}{2} + \frac{q-1}{t} - 1$. For large q, we take $s \approx \frac{1}{2}\sqrt{2(q+1)} \cdot h$ and $t \approx \sqrt{2(q+1)}$. Then, it follows that

$$\frac{s+h}{2} \cdot \frac{q+1}{s} - 1 \approx \frac{q}{2} + \sqrt{\frac{q}{2}} \quad \text{and} \quad \frac{q+1}{2} + \frac{q-1}{t} - 1 \approx \frac{q}{2} + \sqrt{\frac{q}{2}}.$$

This indicates that the minimum distance of the quantum MDS code in Theorem 3 can reach $\frac{q}{2} + \sqrt{\frac{q}{2}}$ approximately.

Example 3.1 Let $q = 641$. Choose $s = 107$, $t = 32$, $h = 5$ and $r = 1$. In this case, one has $\frac{s+h}{2s} \cdot (q+1) - 1 = 341$ and $\frac{q+1}{2} + \frac{q-1}{t} - 1 = 340 \approx \frac{q}{2} + \sqrt{\frac{q}{2}} = 338.4$. The length is $n = 1 + lh + mr - \frac{q^2-1}{st} \cdot hr = 16{,}081$. There exists $[[16081, 15401, 341]]_{641}$ quantum MDS code, which has not been covered in any previous work.

4 Quantum MDS codes of length $n = lh + mr - \frac{q^2-1}{st} \cdot hr$

In this section, we assume **s is odd**, $\mathbf{h \leq s-1}$ and $\mathbf{r \leq t}$. Now, we consider the first part of coordinates in vectors $\overrightarrow{a}$ and $\overrightarrow{v}$. Firstly, we give two useful lemmas that are Lemmas 4.1 and 4.2, which generalize Lemma 13 and Theorem 5 in [5], respectively.

Lemma 4.1 *There exists a solution in* $(\mathbb{F}_q^*)^h$ *of the following system of equations*

$$\sum_{k=0}^{h-1} g^{k(\mu l-q-1)} u_k = 0 \tag{8}$$

for $\lceil \frac{s-h}{2} \rceil + 1 \leq \mu \leq \lfloor \frac{s+h}{2} \rfloor - 1$.

Proof Let $\xi = g^l$, $\eta = g^{-q-1} \in \mathbb{F}_q^*$ and $c = \lceil \frac{s-h}{2} \rceil + 1$. It is clear that $\xi^{c+\nu} \neq \xi^{c+\nu'}$ for any $0 \leq \nu \neq \nu' \leq h-2 < s-2$. We discuss two cases.

Case 1 h is odd. In this case, $\lceil \frac{s-h}{2} \rceil = \frac{s-h}{2}$ and $\lfloor \frac{s+h}{2} \rfloor = \frac{s+h}{2}$. The system of equations (8) can be expressed in the matrix form

$$A\overrightarrow{u}^T = (0, 0, \ldots, 0)^T, \tag{9}$$

where

$$A = \begin{pmatrix} 1 & \xi^c\eta & \xi^{2c}\eta^2 & \cdots & \xi^{(h-1)c}\eta^{h-1} \\ 1 & \xi^{c+1}\eta & \xi^{2(c+1)}\eta^2 & \cdots & \xi^{(h-1)(c+1)}\eta^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{c+h-2}\eta & \xi^{2(c+h-2)}\eta^2 & \cdots & \xi^{(h-1)(c+h-2)}\eta^{h-1} \end{pmatrix}$$

is an $(h-1) \times h$ matrix over $\mathbb{F}_{q^2}$ and

$$\overrightarrow{u} = (u_0, u_1, \ldots, u_{h-1}).$$

It is obvious that $\mathrm{rank}(A) = h-1$. We will show that $u_k \in \mathbb{F}_q^*$ for any $0 \leq k \leq h-1$.

Let

$$A' = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi^c\eta & \xi^{2c}\eta^2 & \cdots & \xi^{(h-1)c}\eta^{h-1} \\ 1 & \xi^{c+1}\eta & \xi^{2(c+1)}\eta^2 & \cdots & \xi^{(h-1)(c+1)}\eta^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{c+h-2}\eta & \xi^{2(c+h-2)}\eta^2 & \cdots & \xi^{(h-1)(c+h-2)}\eta^{h-1} \end{pmatrix}.$$

We consider the equations

$$A'\overrightarrow{u}^T = (1, 0, 0, \ldots, 0)^T. \tag{10}$$

It is easy to check that A' is row equivalent to $A'^{(q)}$ and $\det(A') \neq 0$. Similarly as the proof of Lemma 3.1, we obtain that (10) has a solution $\overrightarrow{u} = (u_0, u_1, \ldots, u_{h-1}) \in (\mathbb{F}_q^*)^h$. Since the solution of (10) is also the solution of (9), the result has been proved.

Case 2 h is even. In this case, $\lceil \frac{s-h}{2} \rceil = \frac{s-h+1}{2}$ and $\lfloor \frac{s+h}{2} \rfloor = \frac{s+h-1}{2}$. The system of equations (8) can be expressed in the matrix form

$$A \overrightarrow{u}^T = (0, 0, \dots, 0)^T, \tag{11}$$

where

$$A = \begin{pmatrix} 1 & \xi^c \eta & \xi^{2c} \eta^2 & \cdots & \xi^{(h-1)c} \eta^{h-1} \\ 1 & \xi^{c+1} \eta & \xi^{2(c+1)} \eta^2 & \cdots & \xi^{(h-1)(c+1)} \eta^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{c+h-3} \eta & \xi^{2(c+h-3)} \eta^2 & \cdots & \xi^{(h-1)(c+h-3)} \eta^{h-1} \end{pmatrix}$$

is an $(h-2) \times h$ matrix over $\mathbb{F}_{q^2}$. By $s \mid q+1$ and $\xi^s = 1$, it takes

$$\left(\xi^{k(c+\nu)} \eta^k\right)^q = \xi^{-k\left(\frac{s-h+1}{2}+1+\nu\right)} \eta^k = \xi^{k\left(\frac{s+h-1}{2}-1-\nu\right)} \eta^k = \xi^{k(c+h-3-\nu)} \eta^k,$$

for any $0 \le k \le h-1$ and $0 \le \nu \le h-3$. Therefore, A and $A^{(q)}$ are row equivalent. By deleting the first (resp. the last) column of A, we obtain an $(h-2) \times (h-1)$ matrix denoted by A_0 (resp. A_{h-1}). Then, A_0 (resp. A_{h-1}) is row equivalent to $A_0^{(q)}$ (resp. $A_{h-1}^{(q)}$). Obviously, $\mathrm{rank}(A_0) = \mathrm{rank}(A_{h-1}) = h-2$. Similarly as the proof of Case 1, we can deduce that the following equations

$$A_0 \overrightarrow{x}^T = (0, \dots, 0)^T, \quad A_{h-1} \overrightarrow{y}^T = (0, \dots, 0)^T$$

have two solutions $\overrightarrow{x} = (x_1, x_2, \dots, x_{h-1})$, $\overrightarrow{y} = (y_0, y_1, \dots, y_{h-2}) \in (\mathbb{F}_q^*)^{h-1}$. From $h < q+1$, there exists $\lambda \in \mathbb{F}_q^* \setminus \{\frac{x_1}{y_1}, \dots, \frac{x_{h-2}}{y_{h-2}}\}$ such that $\overrightarrow{u} = (0, \overrightarrow{x}) - \lambda(\overrightarrow{y}, 0) \in (\mathbb{F}_q^*)^h$. Then, it implies

$$A \overrightarrow{u}^T = \begin{pmatrix} 0 \\ A_0 \overrightarrow{x}^T \end{pmatrix} - \lambda \begin{pmatrix} A_{h-1} \overrightarrow{y}^T \\ 0 \end{pmatrix} = (0, 0, \dots, 0)^T.$$

Therefore, the result has been proved. □

We choose

$$\overrightarrow{a}_1 = (1, \delta, \dots, \delta^{l-1}, g, g\delta, \dots, g\delta^{l-1}, \dots, g^{h-1}, g^{h-1}\delta, \dots, g^{h-1}\delta^{l-1})$$

and

$$\overrightarrow{v}_1 = (v_0, v_0\delta, \dots, v_0\delta^{l-1}, v_1, v_1\delta, \dots, v_1\delta^{l-1}, \dots, v_{h-1}, v_{h-1}\delta, \dots, v_{h-1}\delta^{l-1}),$$

where $v_k^{q+1} = u_k$ $(0 \le k \le h-1)$ and $\overrightarrow{u} = (u_0, u_1, \dots, u_{h-1})$ satisfies (8).

Lemma 4.2 *The identity*

$$\langle \overrightarrow{a}_1^{qi+j}, \overrightarrow{v}_1^{q+1} \rangle = 0$$

holds for all $0 \le i, j \le \lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 3$.

Proof Similarly as Lemma 3.2, we only need to consider the case $l \mid qi + j + q + 1$. From Lemmas 2.2 (i) and 4.1, we deduce that

$$\langle \overrightarrow{a}_1^{qi+j}, \overrightarrow{v}_1^{q+1} \rangle = \langle \overrightarrow{a}_1^{\mu l - q - 1}, \overrightarrow{v}_1^{q+1} \rangle = l \cdot \sum_{k=0}^{h-1} g^{k(\mu l - q - 1)} v_k^{q+1} = 0.$$

Therefore, for all $0 \le i, j \le \lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 3$,

$$\langle \overrightarrow{a}_1^{qi+j}, \overrightarrow{v}_1^{q+1} \rangle = 0.$$

□

The vectors $\overrightarrow{a}_2$ and $\overrightarrow{v}_2$ are the same as in Sect. 3.

Theorem 4 *Let* $n = lh + mr - \frac{q^2-1}{st} \cdot hr$, *where odd* $s \mid q+1$, *even* $t \mid q-1$, $t \ge 2$, $l = \frac{q^2-1}{s}$, $m = \frac{q^2-1}{t}$, $h \le s-1$ *and* $r \le t$. *Assume that* $q - 1 > \frac{q^2-1}{st} \cdot hr$, *then for any* $1 \le d \le \min\{\lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 2, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$, *there exists an* $[[n, n-2d, d+1]]_q$ *quantum MDS code.*

Proof Similarly as Theorem 3, we also let $A = \{g^\alpha \delta^i | 0 \le \alpha \le h-1, 0 \le i \le l-1\}$, $B = \{g^\beta \theta^j | 0 \le \beta \le r-1, 0 \le j \le m-1\}$, $A_1 = A - B$ and $B_1 = B - A$. Define

$$f_1 : A \to \mathbb{F}_q^*, \ \ f_1(g^\alpha \delta^i) = (v_\alpha \delta^i)^{q+1},$$
$$f_2 : B \to \mathbb{F}_q^*, \ \ f_2(g^\beta \theta^j) = \theta^{j \cdot \frac{q+1}{2}}.$$

Let

$$\overrightarrow{a} = (\overrightarrow{a}_{A_1}, \overrightarrow{a}_{B_1}, \overrightarrow{a}_{A \cap B}),$$

where $\overrightarrow{a}_S = (a_1, \ldots, a_k)$ for $S = \{a_1, \ldots, a_k\}$ and

$$\overrightarrow{v}^{q+1} = (f_1(\overrightarrow{a}_{A_1}), \lambda f_2(\overrightarrow{a}_{B_1}), f_1(\overrightarrow{a}_{A \cap B}) + \lambda f_2(\overrightarrow{a}_{A \cap B})),$$

where $\lambda \in \mathbb{F}_q^*$ is chosen such that all the coordinates of $f_1(\overrightarrow{a}_{A \cap B}) + \lambda f_2(\overrightarrow{a}_{A \cap B})$ are nonzero and $f_j(\overrightarrow{a}_S) = (f_j(a_1), \ldots, f_j(a_k))$ with $S = \{a_1, \ldots, a_k\}$ for $j = 1, 2$.

According to Lemmas 3.3 and 4.2, similarly as the proof of Theorem 3, $\mathbf{GRS}_d(\overrightarrow{a}, \overrightarrow{v})$ is Hermitian self-orthogonal. As a consequence, by Theorem 1, there exists $[[n, n-2d, d+1]]_q$ quantum MDS code, where $n = lh + mr - \frac{q^2-1}{st} \cdot hr$ with odd h and $1 \le d \le \min\{\lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 2, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$. □

Remark 4.1 Similarly as Remark 3.1, the minimum distance can reach $\frac{q}{2} + \sqrt{\frac{q}{2}}$ approximately.

5 Quantum MDS codes of length $n = lh + mr$

In this section, **s is even**, $\mathbf{h} \leq \frac{\mathbf{s}}{\mathbf{2}}$ and $\mathbf{r} \leq \frac{\mathbf{t}}{\mathbf{2}}$ and quantum MDS codes with length $n = lh + mr$ will be constructed. Similarly as the previous constructions, we also divide the vectors $\overrightarrow{a}$ and $\overrightarrow{v}$ into two parts. However, in this case, coordinates of these two parts in the vector $\overrightarrow{a}$ have no duplication. Therefore, the quantum MDS codes in this section have larger minimum distances than the codes in previous sections.

The proof of the next result is similar to that of Lemma 4.1, and we omit the details.

Lemma 5.1 *The following system of equations*

$$\sum_{k=0}^{h-1} g^{(2k+1)(\mu l - q - 1)} u_k = 0 \tag{12}$$

has a solution denoted by $\overrightarrow{u} = (u_0, u_1, \ldots, u_{h-1}) \in (\mathbb{F}_q^*)^h$ *for all* $\lceil \frac{s-h}{2} \rceil + 1 \leq \mu \leq \lfloor \frac{s+h}{2} \rfloor - 1$.

Here, we choose

$$\overrightarrow{a}_1 = (g, g\delta, \ldots, g\delta^{l-1}, g^3, g^3\delta, \ldots, g^3\delta^{l-1}, \ldots, g^{2h-1}, g^{2h-1}\delta, \ldots, g^{2h-1}\delta^{l-1})$$

and

$$\overrightarrow{v}_1 = (v_0, v_0\delta, \ldots, v_0\delta^{l-1}, v_1, v_1\delta, \ldots, v_1\delta^{l-1}, \ldots, v_{h-1}, v_{h-1}\delta, \ldots, v_{h-1}\delta^{l-1}),$$

where $v_k^{q+1} = u_k$ $(0 \leq k \leq h-1)$ and $\overrightarrow{u} = (u_0, u_1, \ldots, u_{h-1})$ is a solution of (12).

Lemma 5.2 *The identity*

$$\langle \overrightarrow{a}_1^{qi+j}, \overrightarrow{v}_1^{q+1} \rangle = 0$$

holds for all $0 \leq i, j \leq \lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 3$.

Proof The result follows from Lemmas 2.2 (i) and 5.1. □

Now, we construct the second part of coordinates in $\overrightarrow{a}$ and $\overrightarrow{v}$. We choose

$$\overrightarrow{a}_2 = (1, \theta, \ldots, \theta^{m-1}, g^2, g^2\theta, \ldots, g^2\theta^{m-1}, \ldots, g^{2r-2}, g^{2r-2}\theta, \ldots, g^{2r-2}\theta^{m-1})$$

and

$$\overrightarrow{v}_2 = (1, g^{\frac{t}{2}}, \ldots, g^{(m-1)\cdot\frac{t}{2}}, 1, g^{\frac{t}{2}}, \ldots, g^{(m-1)\cdot\frac{t}{2}}, \ldots, 1, g^{\frac{t}{2}}, \ldots, g^{(m-1)\cdot\frac{t}{2}}).$$

Then, we have the following lemma.

Lemma 5.3 *The identity*

$$\langle \overrightarrow{a}_2^{qi+j}, \overrightarrow{v}_2^{q+1} \rangle = 0$$

holds for all $0 \leq i, j \leq \frac{q+1}{2} + \frac{q-1}{t} - 2$.

Proof By Lemma 2.3,

$$\begin{aligned} \langle \overrightarrow{a}_2^{qi+j}, \overrightarrow{v}_2^{q+1} \rangle &= \sum_{k=0}^{r-1} \sum_{\nu=0}^{m-1} (g^{2k}\theta^{\nu})^{qi+j} \cdot \theta^{\nu \cdot \frac{q+1}{2}} \\ &= \sum_{k=0}^{r-1} g^{2k(qi+j)} \sum_{\nu=0}^{m-1} \theta^{\nu(qi+j+\frac{q+1}{2})} \\ &= 0. \end{aligned} \tag{13}$$

□

Since both s and t are even, it is clear that all coordinates of $\overrightarrow{a}_1$ are nonsquares and all coordinates of $\overrightarrow{a}_2$ are squares. Thus, there exists no duplication between these two parts. Choose $\overrightarrow{a} = (\overrightarrow{a}_1, \overrightarrow{a}_2)$ and $\overrightarrow{v} = (\overrightarrow{v}_1, \overrightarrow{v}_2)$.

Theorem 5 *Let* $n = lh + mr$, *where even* $s \mid q+1$, *even* $t \mid q-1$, $t \geq 2$, $l = \frac{q^2-1}{s}$, $m = \frac{q^2-1}{t}$, $h \leq \frac{s}{2}$ *and* $r \leq \frac{t}{2}$. *Then for any* $1 \leq d \leq \min\{\lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 2, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$, *there exists an* $[[n, n-2d, d+1]]_q$ *quantum MDS code.*

Proof The vectors $\overrightarrow{a}$ and $\overrightarrow{v}$ are defined as above. According to Lemmas 5.2 and 5.3, it takes

$$\langle \overrightarrow{a}^{qi+j}, \overrightarrow{v}^{q+1} \rangle = \langle \overrightarrow{a}_1^{qi+j}, \overrightarrow{v}_1^{q+1} \rangle + \langle \overrightarrow{a}_2^{qi+j}, \overrightarrow{v}_2^{q+1} \rangle = 0,$$

for any $0 \leq i, j \leq d-1$. Therefore, by Theorem 2, the code $\mathbf{GRS}_d(\overrightarrow{a}, \overrightarrow{v})$ is Hermitian self-orthogonal. By Theorem 1, there exists an $[[n, n-2d, d+1]]_q$ quantum MDS code, where $n = lh + mr$ and $1 \leq d \leq \min\{\lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 2, \frac{q+1}{2} + \frac{q-1}{t} - 1\}$. □

Remark 5.1 When h approaches to $\frac{s}{2}$ and $t = 4$, both $\lfloor \frac{s+h}{2} \rfloor \cdot \frac{q+1}{s} - 2$ and $\frac{q+1}{2} + \frac{q-1}{t} - 1$ approach to $\frac{3}{4}q$. So the minimum distance of the quantum MDS code can approach to $\frac{3}{4}q$.

Example 5.1 When $q \equiv 9 \pmod{20}$, applying Theorem 5 with $(s, h, t, r) = (10, 4, 4, 1)$, there exist q-ary quantum MDS codes with parameters

$$\left[\left[\frac{13}{20}(q^2-1), \frac{13q^2 - 28q + 79}{20}, \frac{7q - 13}{10}\right]\right]_q$$

Table 1 Some of new $[[n, n-2d, d+1]]_{37}$ quantum MDS codes

n	$n-2d$	$d+1$
588	544	23
624	580	23
660	614	24
696	650	24
702	658	23
732	684	25
738	694	23
768	720	25
774	728	24
804	756	25
810	764	24
816	772	23
840	792	25
846	798	25
852	808	23
882	834	25
918	868	26
954	904	26

whose minimal distance is approximately $0.7q$ when q is large. In general, the length satisfies $\frac{13}{20}(q^2-1) \not\equiv 0, 1 \pmod{q \pm 1}$. Therefore, this class of quantum MDS codes are new.

Example 5.2 When $q \equiv 29 \pmod{60}$, applying Theorem 5 with $(s, h, t, r) = (30, 14, 4, 1)$, there exist quantum MDS codes with parameters

$$\left[\left[\frac{43}{60}(q^2-1), \frac{43q^2-88q+229}{60}, \frac{11q-19}{15}\right]\right]_q$$

whose minimal distance is approximately $11q/15 \approx 0.733q$ when q is large. Also, the length satisfies $\frac{43}{60}(q^2-1) \not\equiv 0, 1 \pmod{q \pm 1}$ and these quantum MDS codes are new.

6 Conclusion

Applying Hermitian construction and GRS codes, we construct several new classes of quantum MDS codes over $\mathbb{F}_{q^2}$ through Hermitian self-orthogonal GRS codes. Some of these quantum MDS codes can have minimum distance bigger than $\frac{q}{2}+1$. Since the lengths are chosen up to two variables h and r, this makes their lengths more flexible than previous constructions. Using our results, we can produce many new quantum

MDS codes with new lengths which have not appeared in previous works. We give an example.

Example 6.1 Choose $q = 37$. Utilizing the results in this paper, there are 438 new $[[n, n-2d, d+1]]_{37}$ quantum MDS codes with minimum distance $d+1 \geq \frac{q}{2}+1$, which were not reported in previous papers. We list some of new $[[n, n-2d, d+1]]_{37}$ quantum MDS codes in Table 1.

For a fixed q, it is expected to have $[[n, n-2d, d+1]]_q$ quantum MDS codes for any length of $q+1 < n \leq q^2+1$ and minimum distance $\frac{q}{2}+1 \leq d+1 \leq \min\{\frac{n}{2}, q+1\}$. But summing up all the results, such quantum MDS codes are still very sparse. It is expected that more quantum MDS codes with large minimal distance will be explored.

Acknowledgements This research is supported by National Natural Science Foundation of China under Grant Nos. 11471008 and 11871025 and the self-determined research funds of CCNU from the colleges' basic research and operation of MOE (Grant No. CCNU18TS028).

References

1. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**(3), 1183–1188 (2007)
2. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**(7), 3065–3072 (2001)
3. Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**(3), 1474–1484 (2015)
4. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory **44**(4), 1369–1387 (1998)
5. Fang, W., Fu, F.: Some new constructions of quantum MDS codes (2018). arXiv:1804.08213
6. Fang, W., Fu, F.: Two new classes of quantum MDS codes. Finite Fields Appl. **53**, 85–98 (2018)
7. Grassl, M., Beth, T., Röttler, M.: On optimal quantum codes. Int. J. Quantum Inf. **2**(1), 757–775 (2004)
8. Guardia, G.G.L.: New quantum MDS codes. IEEE Trans. Inf. Theory **57**(8), 5551–5554 (2011)
9. He, X., Xu, L., Chen, H.: New q-ary quantum MDS codes with distances bigger than $\frac{q}{2}$. Quantum Inf. Process. **15**(7), 2745–2758 (2016)
10. Jin, L., Kan, H., Wen, J.: Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes. Des. Codes Cryptogr. **84**(3), 463–471 (2017)
11. Jin, L., Ling, S., Luo, J., Xing, C.: Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. IEEE Trans. Inf. Theory **56**(9), 4735–4740 (2010)
12. Jin, L., Xing, C.: A construction of new quantum MDS codes. IEEE Trans. Inf. Theory **60**(5), 2921–2925 (2014)
13. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**(11), 4892–4914 (2006)
14. Kai, X., Zhu, S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2012)
15. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**(4), 2080–2086 (2014)
16. Li, R., Xu, Z.: Construction of $[[n, n-4, 3]]_q$ quantum MDS codes for odd prime power q. Phys. Rev. A **82**(5), 052316-1–052316-4 (2010)
17. Li, Z., Xing, L., Wang, X.: Quantum generalized Reed–Solomon codes: unified framework for quantum MDS codes. Phys. Rev. A **77**(1), 012308-1–012308-4 (2008)
18. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North Holland, Amsterdam (1977)
19. Rain, E.M.: Nonbinary quantum codes. IEEE Trans. Inf. Theory **45**(6), 1827–1832 (1999)
20. Röttler, M., Grassl, M., Beth, T.: On quantum MDS codes. In: Proceedings of the International Symposium on Information Theory, Chicago, USA, p. 356 (2004)

21. Shi, X., Yue, Q., Chang, Y.: Some quantum MDS codes with large minimum distance from generalized Reed–Solomon codes. Cryptogr. Commun. **10**(6), 1165–1182 (2018)
22. Shi, X., Yue, Q., Zhu, X.: Construction of some new quantum MDS codes. Finite Fields Appl. **46**, 347–362 (2017)
23. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), R2493–R2496 (1995)
24. Steane, A.M.: Enlargement of Calderbank–Shor–Steane quantum codes. IEEE Trans. Inf. Theory **45**(7), 2492–2495 (1999)
25. Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**(3), 881–889 (2015)
26. Yan, H.: A note on the construction of MDS self-dual codes. Cryptogr. Commun. **11**(2), 259–268 (2019)
27. Zhang, G., Chen, B.: New quantum MDS codes. Int. J. Quantum Inf. **12**(4), 1450019-1–1450019-10 (2014)
28. Zhang, T., Ge, G.: Quantum MDS codes with large minimum distance. Des. Codes Cryptogr. **83**(3), 503–517 (2017)