Des. Codes Cryptogr. (2017) 83:503–517
DOI 10.1007/s10623-016-0245-0

Quantum MDS codes with large minimum distance

Tao Zhang[1,2] · **Gennian Ge**[1,3]

Received: 24 November 2015 / Revised: 11 March 2016 / Accepted: 21 June 2016 /
Published online: 5 July 2016

Abstract Quantum MDS codes are an important family of quantum codes. In this paper, using generalized Reed–Solomon codes and Hermitian construction, we construct seven classes of quantum MDS codes. All of them provide large minimum distance and most of them are new in the sense that the parameters of quantum codes are different from all the previously known ones.

Keywords Quantum MDS code · Generalized Reed–Solomon code · Hermitian construction

Mathematics Subject Classification 81P70

1 Introduction

Quantum error-correcting codes play an important role in quantum computations and quantum communications. In [4,5], Calderbank et al. found that we can construct quantum codes from classical self-orthogonal codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ with respect to certain inner product. This was then generalized to the nonbinary case in [2,20]. Thereafter, many quantum codes have been constructed by classical linear codes with Euclidean or Hermitian self-orthogonality [1,6,21].

Let q be a prime power, an $[[n, k, d]]_q$ quantum code is a q^k-dimensional subspace of $\mathbb{C}^{q^n}$ with minimum distance d, which can detect up to $d-1$ quantum errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$ quantum errors. As in classical coding theory, one of the central tasks in quantum

Communicated by D. Jungnickel.

✉ Gennian Ge
gnge@zju.edu.cn

[1] School of Mathematical Sciences, Capital Normal University, Beijing 100048, China

[2] School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, Zhejiang, China

[3] Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China

coding theory is to construct quantum codes with good parameters. The following theorem gives a bound on the achievable minimum distance of a quantum code.

Theorem 1.1 ([15,16] Quantum Singleton Bound) *Quantum codes with parameters* $[[n, k, d]]_q$ *satisfy*

$$2d \leq n - k + 2.$$

A quantum code achieving this bound is called a quantum maximum-distance-separable (MDS) code. Just as in the classical linear codes, quantum MDS codes form an important family of quantum codes. Constructing quantum MDS codes has become a central topic for quantum codes in recent years. There are many methods to construct quantum codes, and the following theorem is one of the most frequently used construction methods since we can obtain quantum MDS codes with length larger than $q + 1$.

Theorem 1.2 ([2] Hermitian Construction) *If* C *is an* $[n, k, d]_{q^2}$*-linear code such that* $C^{\perp H} \subseteq C$*, then there exists an* $[[n, 2k - n, \geq d]]_q$*-quantum code.*

For the quantum MDS codes, we have the following corollary.

Corollary 1.3 *There is an* $[[n, n - 2k, k + 1]]_q$ *quantum MDS code whenever there exists a classical Hermitian self-orthogonal* $[n, k, n - k + 1]_{q^2}$*-MDS code.*

There have been many papers on the construction of quantum MDS codes (see [3,7–14,17–19,23,24] and the references therein). However, it is not an easy task to construct quantum MDS codes with length $n > q + 1$ and minimum distance $d > \frac{q}{2}$. In this paper, we construct some new quantum MDS codes with minimum distance $d > \frac{q}{2}$ through classical Hermitian self-orthogonal generalized Reed–Solomon codes.

This paper is organized as follows. In Sect. 2 we recall the basics about linear codes and some properties of generalized Reed–Solomon codes. In Sects. 3, 4, 5 and 6, we give seven new classes of quantum MDS codes from generalized Reed–Solomon codes. Section 7 concludes the paper.

2 Preliminaries

Throughout this paper, let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^*$ be the multiplicative group of nonzero elements of $\mathbb{F}_q$, where q is a prime power. A linear $[n, k]_q$ code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The weight $\mathrm{wt}(x)$ of a codeword $x \in C$ is the number of nonzero components of x. The distance of two codewords $x, y \in C$ is $d(x, y) = \mathrm{wt}(x - y)$. The minimum distance d of C is the minimum distance between any two distinct codewords of C. An $[n, k, d]_q$ code is an $[n, k]_q$ code with the minimum distance d.

Given two vectors $x = (x_0, x_1, \ldots, x_{n-1}),\ y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_q^n$, there are two inner products we are interested in. One is the Euclidean inner product which is defined as $\langle x, y\rangle_E = \sum_{i=0}^{n-1} x_i y_i$. When $q = l^2$, where l is a prime power, then we can also consider the Hermitian inner product which is defined by $\langle x, y\rangle_H = \sum_{i=0}^{n-1} x_i y_i^l$. The Euclidean dual code of C is defined as

$$C^{\perp E} = \{x \in \mathbb{F}_q^n |\ \langle x, y\rangle_E = 0 \text{ for all } y \in C\}.$$

Similarly the Hermitian dual code of C is defined as

$$C^{\perp H} = \{x \in \mathbb{F}_q^n |\ \langle x, y\rangle_H = 0 \text{ for all } y \in C\}.$$

A linear code C is called Euclidean (Hermitian) self-orthogonal if $C \subseteq C^{\perp E}$ ($C \subseteq C^{\perp H}$, respectively).

For a vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^2}^n$, let $x^i = (x_1^i, \ldots, x_n^i)$. For a subset S of $\mathbb{F}_{q^2}^n$, we define S^q to be the set $\{x^q \mid x \in S\}$. Then it is easy to see that for a linear code C over $\mathbb{F}_{q^2}$, we have $C^{\perp H} = (C^q)^{\perp E}$. Therefore, C is Hermitian self-orthogonal if and only if $C \subseteq (C^q)^{\perp E}$, i.e., $C^q \subseteq C^{\perp E}$.

Now we recall the basics of generalized Reed–Solomon codes. Choose n distinct elements $a_1, \ldots, a_n$ of $\mathbb{F}_q$ and n nonzero elements $v_1, \ldots, v_n$ of $\mathbb{F}_q$. For $1 \le k \le n$, we define the code

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) := \{(v_1 f(a_1), \ldots, v_n f(a_n)) \mid f(x) \in \mathbb{F}_q[x] \text{ and } \deg(f(x)) < k\},$$

where $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$. The code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ is called a generalized Reed–Solomon code over $\mathbb{F}_q$. It is well known that a generalized Reed–Solomon code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ is an MDS code with parameters $[n, k, n-k+1]_q$. The following lemma presents a criterion to determine whether or not a generalized Reed–Solomon code is Hermian self-orthogonal.

Lemma 2.1 *Let* $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{q^2}^n$ *and* $\mathbf{v} = (v_1, \ldots, v_n) \in (\mathbb{F}_{q^2}^*)^n$, *then* $GRS_k(\mathbf{a}, \mathbf{v}) \subseteq GRS_k(\mathbf{a}, \mathbf{v})^{\perp H}$ *if and only if* $\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1} \rangle_E = 0$ *for all* $0 \le j, l \le k-1$.

Proof Note that $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp H}$ if and only if $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^q \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp E}$. It is obvious that $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^q$ has a basis $\{(v_1^q a_1^{iq}, \ldots, v_n^q a_n^{iq}) | 0 \le i \le k-1\}$, and $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ has a basis $\{(v_1 a_1^i, \ldots, v_n a_n^i) | 0 \le i \le k-1\}$. So $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^q \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp E}$ if and only if $\sum_{i=1}^n v_i^{q+1} a_i^{qj+l} = 0$ for all $0 \le j, l \le k-1$. □

Note that Lemma 2.1 is just a special case of the so-called puncture code that has been introduced by Rains [20], but Lemma 2.1 is enough for our constructions.

3 q-ary quantum MDS codes, where $q = 2am + 1$

In this section, we consider q-ary quantum MDS codes, where $q = 2am + 1$. We need the following lemma for our construction.

Lemma 3.1 *Let* q *be an odd prime power with the form* $2am + 1$, ω *be a fixed primitive element of* $\mathbb{F}_{q^2}$ *and* $n = \frac{q^2-1}{2a}$. *Suppose* $\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{2na+t}) \in \mathbb{F}_{q^2}^n$ *and* $\mathbf{u} = (1, \omega^a, \ldots, \omega^{(n-1)a}) \in \mathbb{F}_{q^2}^n$. *Then we have* $\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \rangle_E = 0$ *for any* $0 \le j, l \le (a+1)m - 1$.

Proof For any $0 \le j, l \le (a+1)m - 1$, we have

$$\begin{aligned} &\left\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \right\rangle_E \\ &= \sum_{i=0}^{n-1} \omega^{[2a(i+1)+t](qj+l)} \omega^{ia(q+1)} \\ &= \omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{2ai\left(qj+l+\frac{q+1}{2}\right)}. \end{aligned}$$

We claim that $2a(qj+l+\frac{q+1}{2}) \not\equiv 0 \pmod{q^2-1}$. Otherwise $qj+l = r\frac{q+1}{2}$, we get $m(q+1)|\frac{r+1}{2}(q+1)$. Then there exists an integer r_1 such that $r = 2mr_1 - 1$. Hence $qj+l = (2mr_1-1)\frac{q+1}{2} = mr_1q + (r_1-a)m - 1 = (mr_1-1)q + (a+r_1)m$, contradicting to the fact that $0 \le j, l \le (a+1)m-1$. Then we get

$$\begin{aligned}&\left\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1}\right\rangle_E \\ &= \omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{2ai\left(qj+l+\frac{q+1}{2}\right)} \\ &= 0.\end{aligned}$$

□

Now, we have the following theorem.

Theorem 3.2 *Let q be an odd prime power with the form $2am+1$. Then for each $1 \le b \le 2a$, there exists a $[[bm(q+1), bm(q+1)-2d+2, d]]_q$-quantum MDS code, where $2 \le d \le (a+1)m+1$.*

Proof Let $\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{2na+t}) \in \mathbb{F}_{q^2}^n$ and $\mathbf{u} = (1, \omega^a, \ldots, \omega^{(n-1)a}) \in \mathbb{F}_{q^2}^n$, where $n = m(q+1) = \frac{q^2-1}{2a}$. Take $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_b)$ and $\mathbf{v} = (\underbrace{\mathbf{u}, \mathbf{u}, \ldots, \mathbf{u}}_{b \text{ times}})$.

Note that if $\omega^{2ai_1+j_1} = \omega^{2ai_2+j_2}$, where $1 \le i_1, i_2 \le n$ and $1 \le j_1, j_2 \le b$, then $i_1 = i_2$ and $j_1 = j_2$. Hence the elements of the vector $\mathbf{a}$ are mutually distinct.

Then for $0 \le j, l \le (a+1)m-1$, by Lemma 3.1, we have

$$\begin{aligned}&\left\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1}\right\rangle_E \\ &= \sum_{i=1}^{b} \left\langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1}\right\rangle_E \\ &= 0.\end{aligned}$$

Hence $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$ for $1 \le k \le (a+1)m$. Then by Corollary 1.3, the conclusion follows. □

In particular, taking $b = 1$, we obtain the following corollary which is one of the main results in [7,24].

Corollary 3.3 *Let q be an odd prime power with the form $2am+1$. Then there exists an $[[m(q+1), m(q+1)-2d+2, d]]_q$-quantum MDS code, where $2 \le d \le (a+1)m+1$.*

The elements of $\mathbf{a}_t$ in Lemma 3.1 form a coset of a subgroup of $\mathbb{F}_{q^2}^*$. The following lemma is similar to Lemma 3.1, which takes the vector obtained by deleting $q+1$ elements from $\mathbf{a}_t$.

Lemma 3.4 *Let q be an odd prime power with the form $2am+1$, ω be a fixed primitive element of $\mathbb{F}_{q^2}$ and $n = \frac{q^2-1}{2a} - q - 1$. Let $\mathbf{b}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{q-1-2a+t}, \omega^{q-1+2a+t}, \ldots, \omega^{2q-2-2a+t}, \ldots, \omega^{q^2-q-2a+t}, \cdots, \omega^{q^2-1-2a+t}) \in \mathbb{F}_{q^2}^n$. Then there exists $\mathbf{w} \in (\mathbb{F}_{q^2}^*)^n$ such that $\langle \mathbf{b}_t^{qj+l}, \mathbf{w}^{q+1}\rangle_E = 0$ for any $0 \le j, l \le (a+1)m-2$.*

Proof Let A be an $(m-2)\times(m-1)$ matrix with $A_{ij}=\omega^{aj(q+1)(2i-1)}\in\mathbb{F}_q$ for $1\le i\le m-2$ and $1\le j\le m-1$. Then there exists $\mathbf{c}\in\mathbb{F}_q^{m-1}$ such that $A\cdot\mathbf{c}^t=0$. Note that by deleting the j'-th column from matrix A, the remaining matrix is a Vandermonde matrix multiplied by $\prod_{j\neq j'}\omega^{aj(q+1)}$, hence all coordinates of $\mathbf{c}$ are nonzero. So we can represent $\mathbf{c}$ as $\mathbf{c}=(\omega^{a_1(q+1)},\ldots,\omega^{a_{m-1}(q+1)})$.

Now let $\mathbf{w}_i=(\omega^{a_1+i\frac{q-1}{2}},\ldots,\omega^{a_{m-1}+i\frac{q-1}{2}})$ and $\mathbf{w}=(\mathbf{w}_0,\mathbf{w}_1,\ldots,\mathbf{w}_q)$. Then for $0\le j,l\le(a+1)m-2$, we have

$$\begin{aligned}&\left\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\right\rangle_E\\&=\sum_{i=1}^{m-1}\omega^{a_i(q+1)}\sum_{s=0}^{\frac{q-1}{2}}\omega^{[2s(q-1)+t+2ai](qj+l)}-\sum_{i=1}^{m-1}\omega^{a_i(q+1)}\sum_{s=0}^{\frac{q-1}{2}}\omega^{[2s(q-1)+q-1+t+2ai](qj+l)}\\&=\omega^{t(qj+l)}\left(1-\omega^{(q-1)(qj+l)}\right)\sum_{i=1}^{m-1}\omega^{a_i(q+1)+2ai(qj+l)}\sum_{s=0}^{\frac{q-1}{2}}\omega^{2s(q-1)(qj+l)}.\end{aligned}$$

Note that

$$\sum_{s=0}^{\frac{q-1}{2}}\omega^{2s(q-1)(qj+l)}=\begin{cases}0; & \text{if } \frac{q+1}{2}\nmid(qj+l),\\ \frac{q+1}{2}; & \text{if } \frac{q+1}{2}\mid(qj+l).\end{cases}$$

Now assume $qj+l=r\frac{q+1}{2}$. If r is even, then $\omega^{(q-1)(qj+l)}=1$, and hence $\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=0$.

If r is odd, then we claim that $r\not\equiv 2m-1\pmod{2m}$. Otherwise, let $r=2mx+2m-1$, then $qj+l=(2mx+2m-1)\frac{q+1}{2}=[(x+1)m-1]q+(a+x+1)m$, contradicting to the fact that $0\le j,l\le(a+1)m-2$. Therefore $2a(qj+l)\pmod{q^2-1}\in\{ar(q+1)|1\le r\le 2m-3,\ r \text{ is odd}\}$. We have

$$\begin{aligned}&\left\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\right\rangle_E\\&=\frac{q+1}{2}\omega^{t(qj+l)}\left(1-\omega^{(q-1)(qj+l)}\right)\sum_{i=1}^{m-1}\omega^{a_i(q+1)+2ai(qj+l)}\\&=0,\end{aligned}$$

where the last equality follows from the definition of vector $\mathbf{c}$. □

From Lemmas 3.1 and 3.4, we have the following theorem.

Theorem 3.5 *Let q be an odd prime power with the form $2am+1$. Then for integers b,c such that $b,c\ge 0$, $1\le b+c\le 2a$ and $b\ge 1$ or $m\ge 2$, there exists a $[[(bm+c(m-1))(q+1),(bm+c(m-1))(q+1)-2d+2,d]]_q$-quantum MDS code, where $2\le d\le(a+1)m$.*

Proof Let $\mathbf{a}_t=(\omega^{2a+t},\omega^{4a+t},\ldots,\omega^{2n_1a+t})\in\mathbb{F}_{q^2}^{n_1}$, $\mathbf{u}=(1,\omega^a,\ldots,\omega^{(n_1-1)a})\in\mathbb{F}_{q^2}^{n_1}$, $\mathbf{b}_t=(\omega^{2a+t},\omega^{4a+t},\ldots,\omega^{q-1-2a+t},\omega^{q-1+2a+t},\ldots,\omega^{2q-2-2a+t},\ldots,\omega^{q^2-q+2a+t},\ldots,\omega^{q^2-1-2a+t})\in\mathbb{F}_{q^2}^{n_2}$, and $\mathbf{w}$ be the vector defined in Lemma 3.4 with length n_2, where $n_1=m(q+1)=\frac{q^2-1}{2a}$ and $n_2=(m-1)(q+1)=\frac{q^2-1}{2a}-q-1$. Take $\mathbf{a}=(\mathbf{a}_1,\mathbf{a}_2,\ldots,\mathbf{a}_b,\mathbf{b}_{b+1},\mathbf{b}_{b+2},\ldots,\mathbf{b}_{b+c})$ and $\mathbf{v}=(\underbrace{\mathbf{u},\mathbf{u},\ldots,\mathbf{u}}_{b\text{ times}},\underbrace{\mathbf{w},\mathbf{w},\ldots,\mathbf{w}}_{c\text{ times}})$.

Note that if $\omega^{2ai_1+j_1} = \omega^{2ai_2+j_2}$, where $1 \le i_1, i_2 \le n$ and $1 \le j_1, j_2 \le b$, then $i_1 = i_2$ and $j_1 = j_2$. Hence the elements of the vector $\mathbf{a}$ are mutually distinct.

Then for $0 \le j, l \le (a+1)m - 2$, by Lemmas 3.1 and 3.4, we have

$$\begin{aligned}&\left\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1} \right\rangle_E \\ &= \sum_{i=1}^{b} \left\langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1} \right\rangle_E + \sum_{i=b+1}^{b+c} \left\langle \mathbf{b}_i^{qj+l}, \mathbf{w}^{q+1} \right\rangle_E \\ &= 0.\end{aligned}$$

Hence $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$ for $1 \le k \le (a+1)m - 1$. Then by Corollary 1.3, the conclusion follows. □

4 q-ary quantum MDS codes, where $q = 2am - 1$

In this section, we consider q-ary quantum MDS codes, where $q = 2am - 1$. We first prove the following lemma.

Lemma 4.1 *Let q be an odd prime power with the form $2am - 1$, ω be a fixed primitive element of $\mathbb{F}_{q^2}$ and $n = \frac{q^2-1}{2a}$. Suppose $\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{2na+t}) \in \mathbb{F}_{q^2}^n$ and $\mathbf{u} = (1, \omega^{2a-1}, \omega^{2(2a-1)}, \ldots, \omega^{(n-1)(2a-1)}) \in \mathbb{F}_{q^2}^n$. Then we have $\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \rangle_E = 0$ for $0 \le j, l \le (a+1)m - 3$.*

Proof For any $0 \le j, l \le (a+1)m - 3$, we have

$$\begin{aligned}&\left\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \right\rangle_E \\ &= \sum_{i=0}^{n-1} \omega^{(2a-1)i(q+1)} \omega^{[t+2a(i+1)](qj+l)} \\ &= \omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{i[(q+1)(2a-1)+2a(qj+l)]}.\end{aligned}$$

We claim that $(q+1)(2a-1) + 2a(qj+l) \not\equiv 0 \pmod{q^2-1}$. Otherwise, $\frac{q+1}{2a} | (qj+l)$, then let $qj + l = r\frac{q+1}{2a}$. We get $(q^2-1) | (q+1)(r+2a-1)$, then $(q-1) | (r+2a-1)$. There exists an integer r_1 such that $r = r_1(q-1) - 2a + 1$. Then we have $qj + l = rm = [r_1(q-1) - 2a + 1]m = (r_1 m - 2)q + (2a + 1 - r_1)m - 2$, this contradicts to the fact that $0 \le j, l \le (a+1)m - 3$. We have

$$\begin{aligned}&\left\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \right\rangle_E \\ &= \omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{i[(q+1)(2a-1)+2a(qj+l)]} \\ &= \omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{2ai\left[\frac{(q+1)(2a-1)}{2a} + (qj+l)\right]} \\ &= 0.\end{aligned}$$

□

Now, we have the following theorem.

Theorem 4.2 *Let q be an odd prime power with the form $2am-1$. Then for each $1 \le b \le 2a$, there exists a $[[bm(q-1), bm(q-1)-2d+2, d]]_q$-quantum MDS code, where $2 \le d \le (a+1)m-1$.*

Proof Let $\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{2na+t}) \in \mathbb{F}_{q^2}^n$ and $\mathbf{u} = (1, \omega^{2a-1}, \omega^{2(2a-1)}, \ldots, \omega^{(n-1)(2a-1)}) \in \mathbb{F}_{q^2}^n$, where $n = m(q-1) = \frac{q^2-1}{2a}$. Take $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_b)$ and $\mathbf{v} = (\underbrace{\mathbf{u}, \mathbf{u}, \ldots, \mathbf{u}}_{b \text{ times}})$.

Note that if $\omega^{2ai_1+j_1} = \omega^{2ai_2+j_2}$, where $1 \le i_1, i_2 \le n$ and $1 \le j_1, j_2 \le b$, then $i_1 = i_2$ and $j_1 = j_2$. Hence the elements of the vector $\mathbf{a}$ are mutually distinct.

Then for $0 \le j, l \le (a+1)m-3$, from Lemma 4.1, we have

$$\begin{aligned} &\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1} \rangle_E \\ &= \sum_{i=1}^{b} \langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1} \rangle_E \\ &= 0. \end{aligned}$$

Hence $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$ for $1 \le k \le (a+1)m-2$. Then by Corollary 1.3, the conclusion follows. □

In particular, taking $b = 1$ or letting a be an odd integer and $b = 2$, we obtain the following two corollaries which are the main results in [22].

Corollary 4.3 *Let q be an odd prime power with the form $2am-1$. Then there exists an $[[m(q-1), m(q-1)-2d+2, d]]_q$-quantum MDS code, where $2 \le d \le (a+1)m-1$.*

Corollary 4.4 *Let q be an odd prime power with the form $2am-1$, where a is an odd integer. Then there exists a $[[2m(q-1), 2m(q-1)-2d+2, d]]_q$-quantum MDS code, where $2 \le d \le (a+1)m-1$.*

In order to construct more quantum MDS codes, we need the following lemma [11].

Lemma 4.5 [11] *Let A be an $(n-1) \times n$ matrix of rank $n-1$ over $\mathbb{F}_{q^2}$. Then the equation $Ax = 0$ has a nonzero solution in $\mathbb{F}_q$ if and only if $A^{(q)}$ and A are row equivalent, where $A^{(q)}$ is obtained from A by raising every entry to its q-th power.*

Then we have the following lemma.

Lemma 4.6 *Let q be an odd prime power with the form $2am-1$ and $n = \frac{q^2-1}{2a} - q + 1$. Suppose $\mathbf{b}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{q+1-2a+t}, \omega^{q+1+2a+t}, \ldots, \omega^{2q+2-2a+t}, \ldots, \omega^{q^2-q-2+2a+t}, \ldots, \omega^{q^2-1-2a+t}) \in \mathbb{F}_{q^2}^n$. Then there exists $\mathbf{w} \in (\mathbb{F}_{q^2}^*)^n$ such that $\langle \mathbf{b}_t^{qj+l}, \mathbf{w}^{q+1} \rangle_E = 0$ for $0 \le j, l \le (a+1)m-4$.*

Proof Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$. We also let A be an $(m-2) \times (m-1)$ matrix with $A_{ij} = \omega^{2aj(m-3+(q-1)(i-1))}$ for $1 \le i \le m-2$, $1 \le j \le m-1$.

Since $(m-3+(q-1)(i-1))q \equiv (m-3+(q-1)(m-i-2)) \pmod{q^2-1}$ for $1 \le i \le m-2$, then $A^{(q)}$ and A are row equivalent. By Lemma 4.5, there exists $\mathbf{c} \in \mathbb{F}_q^{m-1}$

such that $A \cdot \mathbf{c}^t = 0$. Note that by deleting any one column of matrix A, the remaining matrix is a Vandermonde matrix, hence all coordinates of $\mathbf{c}$ are nonzero. So we can represent $\mathbf{c}$ as $\mathbf{c} = (\omega^{a_1(q+1)}, \ldots, \omega^{a_{m-1}(q+1)})$.

Now let $\mathbf{w} = (\omega^{a_1}, \ldots, \omega^{a_{m-1}}, \omega^{a_1-(m-3)}, \ldots, \omega^{a_{m-1}-(m-3)}, \ldots, \omega^{a_1-(m-3)(q-2)}, \ldots, \omega^{a_{m-1}-(m-3)(q-2)}) \in (\mathbb{F}_{q^2}^*)^n$. Then for $0 \le j, l \le (a+1)m-4$, we have

$$\begin{aligned}&\left\langle \mathbf{b}_t^{qj+l}, \mathbf{w}^{q+1} \right\rangle_E \\ &\quad = \sum_{i=1}^{m-1} \omega^{a_i(q+1)+2ai(qj+l)} \sum_{s=0}^{q-2} \omega^{(q+1)(qj+l-m+3)s}.\end{aligned}$$

Note that

$$\sum_{s=0}^{q-2} \omega^{(q+1)(qj+l-m+3)s} = \begin{cases} 0; & \text{if } (q-1) \nmid (qj+l-m+3), \\ q-1; & \text{if } (q-1) | (qj+l-m+3). \end{cases}$$

Assume $qj+l-m+3 = t(q-1)$, we claim that $t \not\equiv m-2, m-1 \pmod m$. Otherwise, if $t \equiv m-2 \pmod m$, let $t = rm+m-2$, then $0 \le r \le a$. If $r \le a-1$, then $qj+l = t(q-1)+m-3 = (mr+m-3)q+(q-mr-1) = (mr+m-3)q+(2a-r)m-2$ and $(2a-r)m-2 > (a+1)m-4$ which is a contradiction. If $r = a$, then $qj+l = t(q-1)+m-3 = (am+m-3)q+(am-2)$ and $am+m-3 > (a+1)m-4$, which is also a contradiction. Similarly, $t \not\equiv m-1 \pmod m$. Hence $qj+l \pmod{\frac{q^2-1}{2a}} \in \{t(q-1)+m-3 | 0 \le t \le m-3\}$. Thus

$$\begin{aligned}&\left\langle \mathbf{b}_t^{qj+l}, \mathbf{w}^{q+1} \right\rangle_E \\ &\quad = (q-1) \sum_{i=1}^{m-1} \omega^{a_i(q+1)+2ai(qj+l)} \\ &\quad = 0,\end{aligned}$$

where the last equation is from the definition of $\mathbf{c}$. □

Now, we can prove the following theorem.

Theorem 4.7 *Let q be an odd prime power with the form $2am-1$. Then for integers b, c such that $b, c \ge 0$, $1 \le b+c \le 2a$ and $b \ge 1$ or $m \ge 2$, there exists a $[[(bm+c(m-1))(q-1), (bm+c(m-1))(q-1)-2d+2, d]]_q$-quantum MDS code, where $2 \le d \le (a+1)m-2$.*

Proof Let $\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{2n_1a+t}) \in \mathbb{F}_{q^2}^{n_1}$, $\mathbf{u} = (1, \omega^{2a-1}, \omega^{2(2a-1)}, \ldots, \omega^{(n_1-1)(2a-1)}) \in \mathbb{F}_{q^2}^{n_1}$, $\mathbf{b}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{q+1-2a+t}, \omega^{q+1+2a+t}, \ldots, \omega^{2q+2-2a+t}, \ldots, \omega^{q^2-q-2+2a+t}, \ldots, \omega^{q^2-1-2a+t}) \in \mathbb{F}_{q^2}^{n_2}$ and $\mathbf{w}$ be the vector defined in Lemma 4.6 with length n_2, where $n_1 = \frac{q^2-1}{2a}$ and $n_2 = \frac{q^2-1}{2a} - q + 1$. Take $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_b, \mathbf{b}_{b+1}, \mathbf{b}_{b+2}, \ldots, \mathbf{b}_{b+c})$ and $\mathbf{v} = (\underbrace{\mathbf{u}, \mathbf{u}, \ldots, \mathbf{u}}_{b \text{ times}}, \underbrace{\mathbf{w}, \mathbf{w}, \ldots, \mathbf{w}}_{c \text{ times}})$.

Note that if $\omega^{2ai_1+j_1} = \omega^{2ai_2+j_2}$, where $1 \le i_1, i_2 \le n$ and $1 \le j_1, j_2 \le b$, then $i_1 = i_2$ and $j_1 = j_2$. Hence the elements of the vector $\mathbf{a}$ are mutually distinct.

Then for $0 \le j, l \le (a+1)m-4$, from Lemmas 4.1 and 4.6, we have

$$\begin{aligned}&\left\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1}\right\rangle_E\\ &= \sum_{i=1}^{b}\left\langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1}\right\rangle_E + \sum_{i=b+1}^{b+c}\left\langle \mathbf{b}_i^{qj+l}, \mathbf{w}^{q+1}\right\rangle_E\\ &= 0.\end{aligned}$$

Hence $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$ for $1 \le k \le (a+1)m-3$. Then by Corollary 1.3, the conclusion follows. □

The following lemma is a similar result as Lemma 4.6.

Lemma 4.8 *Let q be an odd prime power with the form $2am-1$, where a is an odd integer and $n = \frac{q^2-1}{a} - q + 1$. Suppose $\mathbf{b}_t = (\omega^{a+t}, \omega^{2a+t}, \ldots, \omega^{q-a+1+t}, \omega^{q+a+1+t}, \ldots, \omega^{2q+2-a+t}, \ldots, \omega^{q^2-q-2+a+t}, \cdots, \omega^{q^2-1-a+t}) \in \mathbb{F}_{q^2}^n$. Then there exists $\mathbf{w} \in (\mathbb{F}_{\mathbf{q^2}}^*)^{\mathbf{n}}$ such that $\langle \mathbf{b}_t^{qj+l}, \mathbf{w}^{q+1}\rangle_E = 0$ for $0 \le j, l \le (a+1)m-3$.*

Proof Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$. We also let A be an $(2m-2)\times(2m-1)$ matrix with $A_{ij} = \omega^{a(i(q-1)-1)j}$ for $1 \le i \le 2m-2$, $1 \le j \le 2m-1$.

Since $a(i(q-1)-1)q \equiv a((2m-1-i)(q-1)-1) \pmod{q^2-1}$ for $1 \le i \le 2m-1$, then $A^{(q)}$ and A are row equivalent. By Lemma 4.5, there exists $\mathbf{c} \in \mathbb{F}_q^{2m-1}$ such that $A \cdot \mathbf{c}^t = 0$. Since by deleting any one column of matrix A, the remaining matrix is a Vandermonde matrix, then all coordinates of $\mathbf{c}$ are nonzero. Hence we can represent $\mathbf{c}$ as $\mathbf{c} = (\omega^{a_1(q+1)}, \ldots, \omega^{a_{2m-1}(q+1)})$.

Now let $\mathbf{v} = (\omega^{a_1}, \ldots, \omega^{a_{2m-1}}, \omega^{a_1+1}, \ldots, \omega^{a_{2m-1}+1}, \cdots, \omega^{a_1+q-2}, \ldots, \omega^{a_{2m-1}+q-2}) \in (\mathbb{F}_{q^2}^*)^n$. Then for $0 \le j, l \le (a+1)m-4$, we have

$$\begin{aligned}&\left\langle \mathbf{b}_t^{qj+l}, \mathbf{w}^{q+1}\right\rangle_E\\ &= \sum_{i=1}^{2m-1} \omega^{a_i(q+1)+ia(qj+l)} \sum_{s=0}^{q-2} \omega^{(q+1)(qj+l+1)s}.\end{aligned}$$

Note that

$$\sum_{s=0}^{q-2} \omega^{(q+1)(qj+l+1)s} = \begin{cases} 0; & \text{if } (q-1) \nmid (qj+l+1),\\ q-1; & \text{if } (q-1) \mid (qj+l+1).\end{cases}$$

Assume $qj+l+1 = t(q-1)$, then $t \not\equiv 0, 2m-1 \pmod{2m}$. Otherwise, if $t \equiv 0 \pmod{2m}$, let $t = 2rm$. Then $qj+l = t(q-1)-1 = (2rm-1)q + (2a-2r)m - 2$ and $\min\{2rm-1, (2a-2r)m-2\} > (a+1)m-3$, which is a contradiction. Similarly, $t \not\equiv 2m-1 \pmod{2m}$. Thus

$$\begin{aligned}&\sum_{i=1}^{n} v_i^{q+1} a_i^{qj+l}\\ &= (q-1)\sum_{i=1}^{m-1} \omega^{a_i(q+1)+ia(qj+l)}\\ &= 0,\end{aligned}$$

where the last equation is from the definition of $\mathbf{c}$. □

Then we can immediately get the quantum codes in the following theorem.

Theorem 4.9 *Let q be an odd prime power with the form $2am-1$, where a is an odd integer. Then for integers c_1, c_2, c_3 such that $c_1, c_2, c_3 \geq 0$, $0 \leq c_1 + c_2 \leq a$, $0 \leq c_1 + c_3 \leq a$ and $c_1 + c_2 + c_3 \geq 1$, there exists a $[[(c_1(2m-1) + (c_2 + c_3)m)(q-1), (c_1(2m-1) + (c_2 + c_3)m)(q-1) - 2d + 2, d]]_q$-quantum MDS code, where $2 \leq d \leq (a+1)m - 1$.*

Proof Let $\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \ldots, \omega^{2n_1a+t}) \in \mathbb{F}_{q^2}^{n_1}$, $\mathbf{u} = (1, \omega^{2a-1}, \omega^{2(2a-1)}, \ldots, \omega^{(n_1-1)(2a-1)}) \in \mathbb{F}_{q^2}^{n_1}$, $\mathbf{b}_t = (\omega^{a+t}, \omega^{2a+t}, \ldots, \omega^{q-a+1+t}, \omega^{q+a+1+t}, \ldots, \omega^{2q+2-a+t}, \ldots, \omega^{q^2-q-2+a+t}, \ldots, \omega^{q^2-1-a+t}) \in \mathbb{F}_{q^2}^{n_2}$ and $\mathbf{w}$ be the vector defined in Lemma 4.8 with length n_2, where $n_1 = m(q-1) = \frac{q^2-1}{2a}$ and $n_2 = (m-1)(q-1) = \frac{q^2-1}{a} - q + 1$. Take $\mathbf{a} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{c_1}, \mathbf{a}_{c_1+1}, \mathbf{a}_{c_1+2}, \ldots, \mathbf{a}_{c_1+c_2}, \mathbf{a}_{c_1+a+1}, \mathbf{a}_{c_1+a+2}, \ldots, \mathbf{a}_{c_1+a+c_3})$ and $\mathbf{v} = (\underbrace{\mathbf{w}, \mathbf{w}, \ldots, \mathbf{w}}_{c_1 \text{ times}}, \underbrace{\mathbf{u}, \mathbf{u}, \ldots, \mathbf{u}}_{c_2+c_3 \text{ times}})$.

Note that if $\omega^{2ai_1+j_1} = \omega^{2ai_2+j_2}$, where $1 \leq i_1, i_2 \leq n$ and $1 \leq j_1, j_2 \leq b$, then $i_1 = i_2$ and $j_1 = j_2$. Hence the elements of the vector $\mathbf{a}$ are mutually distinct.

Then for $0 \leq j, l \leq (a+1)m - 3$, from Lemmas 4.1 and 4.8, we have

$$\begin{aligned}
&\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1} \rangle_E \\
&= \sum_{i=1}^{c_1} \langle \mathbf{b}_i^{qj+l}, \mathbf{w}^{q+1} \rangle_E + \sum_{i=c_1+1}^{c_1+c_2} \langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1} \rangle_E + \sum_{i=c_1+a+1}^{c_1+a+c_3} \langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1} \rangle_E \\
&= 0.
\end{aligned}$$

Hence $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$ for $1 \leq k \leq (a+1)m - 2$. Then by Corollary 1.3, the conclusion follows. □

5 q-ary quantum MDS codes, where $q = 2am - 1$ and $\gcd(a, m) = 1$

In this section, we consider q-ary quantum MDS codes, where $q = 2am-1$ and $\gcd(a, m) = 1$. As a preparation, we have the following lemma.

Lemma 5.1 *Let q be an odd prime power with the form $q = 2am - 1$, where $\gcd(a, m) = 1$. Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$, $f \in \{0, 1\}$, and s, t be integers such that $0 \leq s \leq m$, $0 \leq t \leq a-1$ and $s + t \geq 1$. Suppose $\mathbf{b}_{i,f} = (\omega^{2a+i(q+1)+f}, \omega^{4a+i(q+1)+f}, \ldots, \omega^{2as+i(q+1)+f})$, $\mathbf{c}_{i,f} = (\omega^{2m+i(q+1)+f}, \omega^{4m+i(q+1)+f}, \ldots, \omega^{2mt+i(q+1)+f})$ and $\mathbf{a}_f = (\mathbf{b}_{0,f}, \mathbf{c}_{0,f}, \mathbf{b}_{1,f}, \mathbf{c}_{1,f}, \ldots, \mathbf{b}_{q-2,f}, \mathbf{c}_{q-2,f})$. Then there exists $\mathbf{v} \in (\mathbb{F}_{q^2}^*)^{(s+t)(q-1)}$ such that $\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \rangle_E = 0$ for $0 \leq j, l \leq am + s + t - 3$.*

Proof Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$. We also let A be an $(s+t-1) \times (s+t)$ matrix with $A_{ij} = \omega^{2aj(s+t-2+(q-1)(i-1))}$ for $1 \leq i \leq s+t-1$, $1 \leq j \leq s$ and $A_{ij} = \omega^{2mj(s+t-2+(q-1)(i-1))}$ for $1 \leq i \leq s+t-1$, $s+1 \leq j \leq s+t$.

Since $(s+t-2+(q-1)(i-1))q \equiv (s+t-2+(q-1)(s+t-1-i)) \pmod{q^2-1}$ for $1 \leq i \leq s+t-1$, then $A^{(q)}$ and A are row equivalent. By Lemma 4.5, there exists $\mathbf{c} \in \mathbb{F}_q^{s+t}$ such that $A \cdot \mathbf{c}^t = 0$. Note that by deleting the j'-th column from matrix A, the remaining matrix is a Vandermonde matrix multiplied by $\prod_{j_1 \neq j'} \omega^{2aj_1(s+t-2)} \prod_{j_2 \neq j'} \omega^{2mj_2(s+t-2)}$, hence all coordinates of $\mathbf{c}$ are nonzero. So we can represent $\mathbf{c}$ as $\mathbf{c} = (\omega^{e_1(q+1)}, \ldots, \omega^{e_{s+t}(q+1)})$.

Now let $\mathbf{u}_i = (\omega^{e_1+i}, \ldots, \omega^{e_{s+t}+i})$ and $\mathbf{v} = (\mathbf{u}_0, \mathbf{u}_{-(s+t-2)}, \ldots, \mathbf{u}_{-(s+t-2)(q-2)})$, then for any $0 \le j, l \le am + s + t - 3$, we have

$$\begin{aligned}
&\left\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \right\rangle_E \\
&= \sum_{i=1}^{s} \sum_{k=0}^{q-2} \omega^{(2ai+k(q+1)+f)(qj+l)} \omega^{(e_i-(s+t-2)k)(q+1)} \\
&\quad + \sum_{i=1}^{t} \sum_{k=0}^{q-2} \omega^{(2mi+k(q+1)+f)(qj+l)} \omega^{(e_{s+i}-(s+t-2)k)(q+1)} \\
&= \omega^{f(qj+l)} \left(\sum_{i=1}^{s} \omega^{2ai(qj+l)+e_i(q+1)} + \sum_{i=1}^{t} \omega^{2mi(qj+l)+e_{s+i}(q+1)} \right) \sum_{k=0}^{q-2} \omega^{k(q+1)(qj+l-s-t+2)}.
\end{aligned}$$

Note that

$$\sum_{k=0}^{q-2} \omega^{k(q+1)(qj+l-s-t+2)} = \begin{cases} 0; & \text{if } (q-1) \nmid (qj+l-s-t+2), \\ q-1; & \text{if } (q-1) | (qj+l-s-t+2). \end{cases}$$

If $qj+l-s-t+2 = r(q-1)$, we claim that $0 \le r \le s+t-2$ or $am \le r \le am+s+t-2$. Otherwise, if $r > s+t-2$, then $qj+l = r(q-1)+s+t-2 = (r-1)q+q+s+t-r-2 = (r-1)q+2am+s+t-r-3$. Since $0 \le j, l \le am+s+t-3$, we have $am \le r \le am+s+t-2$. Note that $\omega^{2ai(am(q-1))} = \omega^{2mi(am(q-1))} = 1$, we have

$$\begin{aligned}
&\left\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \right\rangle_E \\
&= \omega^{f(qj+l)}(q-1) \left(\sum_{i=1}^{s} \omega^{2ai(r(q-1)+s+t-2)+e_i(q+1)} + \sum_{i=1}^{t} \omega^{2mi(r(q-1)+s+t-2)+e_{s+i}(q+1)} \right) \\
&= 0,
\end{aligned}$$

where the last equation is from the definition of $\mathbf{c}$. □

Then we have the following theorem.

Theorem 5.2 *Let q be an odd prime power with the form $q = 2am-1$, where $gcd(a, m) = 1$. Then for integer c such that $1 \le c \le 2(a+m-1)$, there exists a $[[c(q-1), c(q-1) - 2d + 2, d]]_q$-quantum MDS code, where $2 \le d \le am + c_1 - 1$,*

$$c_1 = \begin{cases} c; & \text{if } 1 \le c \le a+m-1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a+m \le c \le 2(a+m-1). \end{cases}$$

Proof If $1 \le c \le a+m-1$, let $c = s+t$ such that $0 \le s \le m$, $0 \le t \le a-1$. Let $\mathbf{b}_i = (\omega^{2a+i(q+1)}, \omega^{4a+i(q+1)}, \ldots, \omega^{2as+i(q+1)})$, $\mathbf{c}_i = (\omega^{2m+i(q+1)}, \omega^{4m+i(q+1)}, \ldots, \omega^{2mt+i(q+1)})$. Take $\mathbf{a} = (\mathbf{b}_0, \mathbf{c}_0, \mathbf{b}_1, \mathbf{c}_1, \cdots, \mathbf{b}_{q-2}, \mathbf{c}_{q-2})$.

If $a+m \le c \le 2(a+m-1)$, $c_1 = \lfloor \frac{c}{2} \rfloor$, let $c_1 = s_1 + t_1$ and $c - c_1 = s_2 + t_2$ such that $0 \le s_1, s_2 \le m$, $0 \le t_1, t_2 \le a-1$. Let $\mathbf{b}_{i,0} = (\omega^{2a+i(q+1)}, \omega^{4a+i(q+1)}, \ldots, \omega^{2as_1+i(q+1)})$, $\mathbf{c}_{i,0} = (\omega^{2m+i(q+1)}, \omega^{4m+i(q+1)}, \ldots, \omega^{2mt_1+i(q+1)})$, $\mathbf{b}_{i,1} = (\omega^{2a+i(q+1)+1}, \omega^{4a+i(q+1)+1}, \ldots, \omega^{2as_2+i(q+1)+1})$ and $\mathbf{c}_{i,1} = (\omega^{2m+i(q+1)+1}, \omega^{4m+i(q+1)+1}, \ldots, \omega^{2mt_2+i(q+1)+1})$. Take $\mathbf{a} = (\mathbf{b}_{0,0}, \mathbf{c}_{0,0}, \mathbf{b}_{1,0}, \mathbf{c}_{1,0}, \cdots, \mathbf{b}_{q-2,0}, \mathbf{c}_{q-2,0}, \mathbf{b}_{0,1}, \mathbf{c}_{0,1}, \mathbf{b}_{1,1}, \mathbf{c}_{1,1}, \cdots, \mathbf{b}_{q-2,1}, \mathbf{c}_{q-2,1})$.

If $\omega^{2ai_1+j_1(q+1)} = \omega^{2mi_2+j_2(q+1)}$, where $1 \le i_1 \le m$, $1 \le i_2 \le a-1$ and $0 \le j_1, j_2 \le q-2$. Then $\omega^{2ai_1-2mi_2+(j_1-j_2)(q+1)} = 1$, therefore $(q+1)|(2ai_1-2mi_2)$, that is $(2am)|(2ai_1-2mi_2)$. And then $a|mi_2$, which contradicts to the fact $\gcd(a,m)=1$. Hence the elements of vector $\mathbf{a}$ are mutually distinct.

Then by Corollary 1.3 and Lemma 5.1, the conclusion follows. □

6 q-ary quantum MDS codes, where $q = 2am+1$ and $\gcd(a,m)=1$

In this section, we consider q-ary quantum MDS codes, where $q = 2am+1$ and $\gcd(a,m)=1$.

Lemma 6.1 *Let q be an odd prime power with the form $q = 2am+1$, where $gcd(a,m)=1$. Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$, $f \in \{0,1\}$, and s,t be integers such that $0 \le s \le m$, $0 \le t \le a-1$ and $s+t \ge 1$. Suppose $\mathbf{b}_{i,f} = (\omega^{2a+i(q-1)+f}, \omega^{4a+i(q-1)+f}, \ldots, \omega^{2as+i(q-1)+f})$, $\mathbf{c}_{i,f} = (\omega^{2m+i(q-1)+f}, \omega^{4m+i(q-1)+f}, \ldots, \omega^{2mt+i(q-1)+f})$ and $\mathbf{a}_f = (\mathbf{b}_{0,f}, \mathbf{c}_{0,f}, \mathbf{b}_{1,f}, \mathbf{c}_{1,f}, \ldots, \mathbf{b}_{q,f}, \mathbf{c}_{q,f})$. Then there exists $\mathbf{v} \in (\mathbb{F}_{q^2}^*)^{(s+t)(q+1)}$ such that $\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \rangle_E = 0$ for $0 \le j,l \le am+s+t-1$.*

Proof Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$. We also let A be an $(s+t-1)\times(s+t)$ matrix with $A_{ij} = \omega^{2aj((q+1)i-\frac{q+1}{2})} \in \mathbb{F}_q$ for $1 \le i \le s+t-1$, $1 \le j \le s$ and $A_{ij} = \omega^{2mj((q+1)i-\frac{q+1}{2})} \in \mathbb{F}_q$ for $1 \le i \le s+t-1$, $s+1 \le j \le s+t$. Then there exists $\mathbf{c} \in \mathbb{F}_q^{s+t}$ such that $A \cdot \mathbf{c}^t = 0$. Note that by deleting the j'-th column from matrix A, the remaining matrix is a Vandermonde matrix multiplied by $\prod_{j_1 \ne j'} \omega^{aj_1(q+1)} \prod_{j_2 \ne j'} \omega^{mj_2(q+1)}$, hence all coordinates of $\mathbf{c}$ are nonzero. So we can represent $\mathbf{c}$ as $\mathbf{c} = (\omega^{e_1(q+1)}, \ldots, \omega^{e_{s+t}(q+1)})$.

Now let $\mathbf{u}_i = (\omega^{e_1+i\frac{q-1}{2}}, \ldots, \omega^{e_{s+t}+i\frac{q-1}{2}})$ and $\mathbf{v} = (\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_q)$, then for any $0 \le j,l \le am+s+t-1$, we have

$$\begin{aligned}
&\left\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \right\rangle_E \\
&= \sum_{i=1}^{s}\sum_{k=0}^{q} \omega^{(2ai+k(q-1)+f)(qj+l)} \omega^{\left(e_i+k\frac{q-1}{2}\right)(q+1)} \\
&\quad + \sum_{i=1}^{t}\sum_{k=0}^{q} \omega^{(2mi+k(q-1)+f)(qj+l)} \omega^{\left(e_{s+i}+k\frac{q-1}{2}\right)(q+1)} \\
&= \omega^{f(qj+l)} \left(\sum_{i=1}^{s} \omega^{2ai(qj+l)+e_i(q+1)} + \sum_{i=1}^{t} \omega^{2mi(qj+l)+e_{s+i}(q+1)} \right) \sum_{k=0}^{q} \omega^{k(q-1)\left(qj+l+\frac{q+1}{2}\right)}.
\end{aligned}$$

Note that

$$\sum_{k=0}^{q} \omega^{k(q-1)\left(qj+l+\frac{q+1}{2}\right)} = \begin{cases} 0; & \text{if } (q+1) \nmid \left(qj+l+\frac{q+1}{2}\right), \\ q+1; & \text{if } (q+1) \mid \left(qj+l+\frac{q+1}{2}\right). \end{cases}$$

If $qj+l+\frac{q+1}{2} = r(q+1)$, we claim that $1 \le r \le s+t-1$ or $am+1 \le r \le am+s+t-1$. If $r < am+1$, then $qj+l = r(q+1)-\frac{q+1}{2} = (r-1)q+r+am$. Since $0 \le j,l \le am+s+t-1$, we have $1 \le r \le s+t-1$. If $r \ge am+1$, then $qj+l = r(q+1)-\frac{q+1}{2} = rq+r-am-1$,

hence $am+1 \le r \le am+s+t-1$. Note that $\omega^{2ai(am(q-1))} = \omega^{2mi(am(q-1))} = 1$, we have

$$\begin{aligned}&\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \rangle_E \\ &= \omega^{f(qj+l)}(q+1)\left(\sum_{i=1}^{s} \omega^{2ai\left(r(q+1)-\frac{q+1}{2}\right)+e_i(q+1)} + \sum_{i=1}^{t} \omega^{2mi\left(r(q+1)-\frac{q+1}{2}\right)+e_{s+i}(q+1)}\right) \\ &= 0,\end{aligned}$$

where the last equation is from the definition of $\mathbf{c}$. □

Combining Lemmas 2.1, 6.1 and Hermitian construction, we have the following theorem.

Theorem 6.2 *Let q be an odd prime power with the form $q = 2am+1$, where $gcd(a, m) = 1$. Then for integer c such that $1 \le c \le 2(a+m-1)$, there exists a $[[c(q+1), c(q+1) - 2d + 2, d]]_q$-quantum MDS code, where $2 \le d \le am + c_1 + 1$,*

$$c_1 = \begin{cases} c; & \text{if } 1 \le c \le a+m-1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a+m \le c \le 2(a+m-1). \end{cases}$$

7 Conclusion

Quantum MDS codes are an important family of quantum codes. In this paper, using generalized Reed–Solomon codes and Hermitian construction, we construct many new quantum MDS codes with large minimum distances. In Table 1, we list the quantum MDS codes constructed in this paper. In the following remarks, using our results in this paper, we can produce quantum codes which include some of the previously known results and some new quantum MDS codes.

Remark 7.1 (1) Consider the quantum MDS codes having type $[[a(q+1), a(q+1) - 2d + 2, d]]_q$ with large minimum distance. In [7,14,24], the authors constructed a class of quantum MDS codes with $a = \frac{q-1}{\lambda}$ and minimum distance $2 \le d \le \frac{q+1}{2} + \frac{q-1}{\lambda}$, where λ is an even divisor of $q-1$. In our construction, Class 1 not only works for $a = \frac{q-1}{\lambda}$, where λ is an even divisor of $q-1$ ($take\ b = 1$), but also works for $a = \frac{q-1}{\lambda}$, where λ is an odd divisor of $q-1$ (take $b = 2$ and choose m such that $\frac{q-1}{2m}$ is odd). Moreover, a can be an integer not a divisor of $q-1$ ($take\ b \nmid (q-1)$).

(2) Class 2 gives us more choices of a for the quantum MDS codes having type $[[a(q+1), a(q+1) - 2d + 2, d]]_q$ with large minimum distance.

(3) Consider the quantum MDS codes having type $[[a(q-1), a(q-1) - 2d + 2, d]]_q$ with large minimum distance. In [14,22], the authors constructed a class of quantum MDS codes with $a|(q+1)$. In Class 3 of our construction, the integer a not only can be a divisor of $q+1$, but also can be an integer not a divisor of $q+1$.

(4) Classes 4 and 5 give us more choices of a for the quantum MDS codes having type $[[a(q-1), a(q-1) - 2d + 2, d]]_q$ with large minimum distance.

(5) Class 6 (Class 7) is a class of $[[c(q-1), c(q-1) - 2d + 2, d]]_q$-quantum MDS code ($[[c(q+1), c(q+1) - 2d + 2, d]]_q$-quantum MDS code, respectively) with large minimum distance for any $1 \le c \le 2(a+m-1)$, where $q = 2am-1$ ($q = 2am+1$, respectively), $\gcd(a, m) = 1$. Although, for some choices of c, the quantum codes may be contained in Classes 3, 4 and 5 (Classes 1 and 2, respectively), there still some new quantum MDS codes.

Table 1 Quantum MDS codes

Class	Length	Distance
1	$n = bm(q+1)$, $m \mid \frac{q-1}{2}$, $bm \le q-1$	$2 \le d \le \frac{q+1}{2} + m$
2	$n = (bm + c(m-1))(q+1)$, $m \mid \frac{q-1}{2}$, $b, c \ge 0$, $(b+c)m \le q-1$ and $b \ge 1$ or $m \ge 2$	$2 \le d \le \frac{q-1}{2} + m$
3	$n = bm(q-1)$, $m \mid \frac{q+1}{2}$, $bm \le q+1$	$2 \le d \le \frac{q-1}{2} + m$
4	$n = (bm + c(m-1))(q-1)$, $m \mid \frac{q+1}{2}$, $b, c \ge 0$, $(b+c)m \le q+1$ and $b \ge 1$ or $m \ge 2$	$2 \le d \le \frac{q-3}{2} + m$
5	$n = (c_1(2m-1) + (c_2+c_3)m)(q-1)$, $m \mid \frac{q+1}{2}$, $c_1, c_2, c_3 \ge 0$, $0 \le c_1 + c_2 \le \frac{q+1}{2m}$, $0 \le c_1 + c_3 \le \frac{q+1}{2m}$ and $c_1 + c_2 + c_3 \ge 1$	$2 \le d \le \frac{q-1}{2} + m$
6	$n = c(q-1)$, $q = 2am - 1$, $\gcd(a, m) = 1$, $1 \le c \le 2(a+m-1)$	$2 \le d \le \frac{q-1}{2} + c_1$, $c_1 = \begin{cases} c; & \text{if } 1 \le c \le a+m-1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a+m \le c \le 2(a+m-1). \end{cases}$
7	$n = c(q+1)$, $q = 2am + 1$, $\gcd(a, m) = 1$, $1 \le c \le 2(a+m-1)$	$2 \le d \le \frac{q+1}{2} + c_1$, $c_1 = \begin{cases} c; & \text{if } 1 \le c \le a+m-1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a+m \le c \le 2(a+m-1). \end{cases}$

Acknowledgements The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper. Research supported by the National Natural Science Foundation of China under Grant Nos. 11431003 and 61571310.

References

1. Aly S.A., Klappenecker A., Sarvepalli P.K.: On quantum and classical BCH codes. IEEE Trans. Inform. Theory **53**(3), 1183–1188 (2007).
2. Ashikhmin A., Knill E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inform. Theory **47**(7), 3065–3072 (2001).
3. Bierbrauer J., Edel Y.: Quantum twisted codes. J. Combin. Des. **8**(3), 174–188 (2000).
4. Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A.: Quantum error correction and orthogonal geometry. Phys. Rev. Lett. **78**(3), 405–408 (1997).
5. Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory **44**(4), 1369–1387 (1998).
6. Chen H., Ling S., Xing C.: Quantum codes from concatenated algebraic–geometric codes. IEEE Trans. Inform. Theory **51**(8), 2915–2920 (2005).
7. Chen B., Ling S., Zhang G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inform. Theory **61**(3), 1474–1484 (2015).
8. Feng K.: Quantum codes $[[6, 2, 3]]_p$ and $[[7, 3, 3]]_p (p \ge 3)$ exist. IEEE Trans. Inform. Theory **48**(8), 2384–2391 (2002).

9. Grassl M., Rotteler M.: Quantum MDS codes over small fields. In: *Proceedings of the International Symposium on Information Theory*, pp. 1104–1108 (2015).
10. Grassl M., Beth T., Roetteler M.: On optimal quantum codes. Int. J. Quantum Inf. **2**(01), 55–64 (2004).
11. Jin L., Xing C.: A construction of new quantum MDS codes. IEEE Trans. Inform. Theory **60**(5), 2921–2925 (2014).
12. Jin L., Ling S., Luo J., Xing C.: Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. IEEE Trans. Inform. Theory **56**(9), 4735–4740 (2010).
13. Kai X., Zhu S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inform. Theory **59**(2), 1193–1197 (2013).
14. Kai X., Zhu S., Li P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inform. Theory **60**(4), 2080–2086 (2014).
15. Ketkar A., Klappenecker A., Kumar S., Sarvepalli P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inform. Theory **52**(11), 4892–4914 (2006).
16. Knill E., Laflamme R.: Theory of quantum error-correcting codes. Phys. Rev. A (3) **55**(2), 900–911 (1997).
17. La Guardia G.G.: New quantum MDS codes. IEEE Trans. Inform. Theory **57**(8), 5551–5554 (2011).
18. Laflamme R., Miquel C., Paz J.P., Zurek W.H.: Perfect quantum error correcting code. Phys. Rev. Lett. **77**(1), 198 (1996).
19. Li Z., Xing L., Wang X.: Quantum generalized Reed–Solomon codes: unified framework for quantum maximum-distance-separable codes. Phys. Rev. A, **77**(1), 012308 (2008).
20. Rains E.M.: Nonbinary quantum codes. IEEE Trans. Inform. Theory **45**(6), 1827–1832 (1999).
21. Steane A.M.: Enlargement of Calderbank–Shor–Steane quantum codes. IEEE Trans. Inform. Theory **45**(7), 2492–2495 (1999).
22. Wang L., Zhu S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**(3), 881–889 (2015).
23. Zhang G., Chen B.: New quantum MDS codes. Int. J. Quantum Inf. **12**(4), 1450019 (2014).
24. Zhang T., Ge G.: Some new classes of quantum MDS codes from constacyclic codes. IEEE Trans. Inform. Theory **61**(9), 5224–5228 (2015).