




New Entanglement-Assisted Quantum MDS Codes Derived From Generalized Reed-Solomon Codes

Guanmin Guo¹ · Ruihu Li¹ 

Received: 15 November 2019 / Accepted: 29 January 2020 / Published online: 13 February 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract

Entanglement-assisted quantum error-correcting codes (abbreviate to EAQECCs) expand the usual paradigm of quantum error correction by allowing two parties to make use of pre-shared entanglement. It is well-known that we can construct an EAQECC from arbitrary classical linear code. In this paper, we construct several classes of entanglement-assisted quantum MDS (EAQMDS) codes by utilizing generalized Reed-Solomon (GRS) codes. The main contribution of the paper is extend the code length of EAQMDS in the literature (Guo et al. 2019). Consequently, the results show that almost all of these EAQMDS codes are new in the sense that the parameters of these codes are not covered by the previously known ones.

Keywords Entanglement-assisted quantum error-correcting codes · Generalized Reed-Solomon codes · MDS codes · Rank

Mathematics Subject Classification (2010) 81P45 · 81P70 · 94B05

1 Introduction

Quantum error correcting codes (QECCs) can safeguard quantum information from unwanted noise. As pioneer discovery in the area of quantum error correction theory, entanglement-assisted stabilizer formalism was developed to construct QECCs with the help of pre-shared entanglement between the sender and the receiver. It was proposed by Brun et al. in [1], and includes the standard stabilizer formalism as a special case. It has been proven that the construction of quantum codes can be derived from arbitrary classical linear

This work is supported by the National Natural Science Foundation of China under Grant Nos.11801564 and 11471011.

✉ Ruihu Li
llzsy2015@163.com

Guanmin Guo
gmguo_xjtukgd@yeah.net

¹ Department of Basic Sciences, Air Force Engineering University, Xi'an, Shaanxi 710051, People's Republic of China

error-correcting codes without certain dual-containing properties, which greatly simplifies their construction and leads to a more general framework for construction of quantum codes. Currently, many researchers focused on studying the construction of EAQECCs and many new and good-performing codes have been found (see [4–24]).

Let q be a prime power. An $[[n, k, d; c]]_q$ EAQECC that encodes k information qubits in n channel qubits with the help of c pairs of maximally-entangled ebits can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, where d is the minimum distance of the code. If $c = 0$, then it is called a standard $[[n, k, d]]_q$ quantum code.

Similar to the quantum Singleton bound of standard quantum codes, we have the following more general EA-quantum Singleton bound.

Lemma 1 (EA-quantum Singleton bound [1–3]) *An EAQECC $[[n, k, d; c]]_q$ satisfies $n + c - k \geq 2(d - 1)$ if $d \leq \frac{n+2}{2}$, where $0 \leq c \leq n - 1$. Particularly, if $c = 0$, then $n - k \geq 2(d - 1)$. An $[[n, k, d; c]]_q$ EAQECC achieving $n + c - k = 2(d - 1)$ is called an EAQMDS code, an EAQMDS code with $c = 0$ is a standard QMDS code.*

Just like QMDS codes, EAQMDS codes is also of significantly theoretical interest, since EAQMDS codes can achieve the entanglement-assisted quantum Singleton bound. The search for best-performing codes has been an ongoing endeavor. In the past few years, a large number of EAQMDS codes also have been constructed by employing GRS codes and constacyclic MDS codes in [8–11, 13–24]. Up to now, GRS and extended GRS codes are the most important classes of MDS codes, and many new results on EAQMDS codes have been published based on them. In [8], Fan et al. proposed several constructions of q -ary EAQMDS codes based on classical constacyclic codes and Reed-Solomon(for short RS) codes. Since Guenda et al. [11] established a link between the number of maximally shared qubits required to construct an EAQECC and the hull of the classical code, construction of EAQMDS codes based on the dimension of the Euclidean and Hermitian hull of GRS codes has been a hot issue. In [20], Luo and Cao studied the hull of GRS and extended GRS codes over finite fields with respect to the Euclidean inner product and constructed several new infinite families of EAQMDS codes. In [23], Fang and Fu et al. completely determined all possible parameters for q -ary EAQMDS codes of length $n \leq q$ and also obtained several new classes of q -ary EAQMDS codes of length $n > q$ via GRS and extended GRS codes. Meanwhile, Li and Zhu et al. [9] constructed two classes of EAQMDS codes by using GRS codes. Enlightened by the work of [9] and [24], we construct several classes of q -ary EAQMDS codes with flexible parameters.

The remainder of this paper is organized as follows. In Section 2, we present the fundamentals which are needed in the rest of the paper. In Section 3, several classes of EAQMDS codes are derived from GRS codes. In Section 4, we conclude the paper.

2 Preliminaries

Firstly, we recall some definitions and basic theory of GRS codes and EAQECCs.

Let q be a prime power and \mathbb{F}_{q^2} be the finite field with q^2 elements. Let $\mathbb{F}_{q^2}^*$ denote the multiplicative group of nonzero elements of \mathbb{F}_{q^2} . For any $\alpha \in \mathbb{F}_{q^2}^*$, the conjugation of α is denoted by $\bar{\alpha} = \alpha^q$. Let $\mathbb{F}_{q^2}^n$ be the \mathbb{F}_{q^2} vector space of n -tuples. A linear code \mathcal{C} of length n is an \mathbb{F}_{q^2} subspace of $\mathbb{F}_{q^2}^n$. A linear code of length n over \mathbb{F}_{q^2} is called an $[[n, k, d]]_{q^2}$ code if its dimension is k and minimum Hamming distance is d .

Let $\mathbf{x} = \{x_1, x_2, \dots, x_n\}$, $\mathbf{y} = \{y_1, y_2, \dots, y_n\} \in \mathbb{F}_{q^2}^n$, the Euclidean and Hermitian dual code of \mathcal{C} are defined as

$$\mathcal{C}^\perp = \left\{ \mathbf{x} \mid \mathbf{x} \in \mathbb{F}_{q^2}^n, \langle \mathbf{x}, \mathbf{y} \rangle_E = x_1y_1 + x_2y_2 + \dots + x_ny_n = 0, \text{ for all } \mathbf{y} \in \mathcal{C} \right\}.$$

and

$$\mathcal{C}^{\perp H} = \left\{ \mathbf{x} \mid \mathbf{x} \in \mathbb{F}_{q^2}^n, \langle \mathbf{x}, \mathbf{y} \rangle_H = x_1\overline{y_1} + x_2\overline{y_2} + \dots + x_n\overline{y_n} = 0, \text{ for all } \mathbf{y} \in \mathcal{C} \right\}.$$

If $\mathcal{C}^\perp \subseteq \mathcal{C}$ ($\mathcal{C}^{\perp H} \subseteq \mathcal{C}$), then \mathcal{C} is called a (Hermitian) dual-containing code and \mathcal{C}^\perp ($\mathcal{C}^{\perp H}$) is called a self-orthogonal code.

The GRS codes are defined as follows.

For a positive integer k , let

$$\mathbb{F}_{q^2}[x]_k = \{f(x) \in \mathbb{F}_{q^2}[x] \mid \deg(f(x)) \leq k - 1\}$$

be an \mathbb{F}_{q^2} -linear space of dimension k . Let $\mathbf{a} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ with $\alpha_1, \alpha_2, \dots, \alpha_n$ distinct elements, $\mathbf{v} = (v_1, v_2, \dots, v_n) \in (\mathbb{F}_{q^2}^*)^n$, and $k \leq n$ ($\leq q^2$). Therefore, we have the generalized Reed-Solomon code

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n)) \mid \text{for all } f(x) \in \mathbb{F}_{q^2}[x]_k\}.$$

It is known that the GRS code is an $[n, k, n - k + 1]$ linear MDS code over \mathbb{F}_{q^2} . A generator matrix of $GRS_k(\mathbf{a}, \mathbf{v})$ is presented by

$$G = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \dots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & v_n\alpha_n^{k-1} \end{pmatrix}.$$

In [5], Wilde and Brun proved that EAQECCs can be constructed using classical linear codes with respect to the Hermitian case as follows.

Theorem 1 [5] *If \mathcal{C} is an $[n, k, d]_{q^2}$ classical code over \mathbb{F}_{q^2} with parity check matrix H , then there exists an EAQECC with parameters $[[n, 2k - n + c, d; c]]_q$, where $c = \text{rank}(HH^\dagger)$ is the number of maximally entangled states required and H^\dagger is the conjugate transpose of H over \mathbb{F}_{q^2} .*

3 New EAQMDS Codes

We devote this section to derive several classes of entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes over \mathbb{F}_{q^2} . As we all know, the dual of a GRS code is also a GRS code. Hence we just need to consider k -dimensional codes of length n with $1 \leq k \leq \lfloor n/2 \rfloor$. We also always assume that ω is a primitive element of \mathbb{F}_{q^2} , that is $\mathbb{F}_{q^2}^* = \langle \omega \rangle$. Then we present our contributions in the following.

3.1 Length $n = 1 + \frac{q-1}{h}(q+1)$, q is Even

In this subsection, we always assume that $q = hm + 1$, $h \geq 1$ is an integer, $n = 1 + \frac{q^2-1}{h}$. Set $\alpha_1 = \omega^{q+1}$, $\alpha_2 = \omega^{q-1}$, then $\text{ord}(\alpha_1) = q - 1$, $\text{ord}(\alpha_2) = q + 1$. Moreover, let $\theta = \alpha_1^h$,

then $\text{ord}(\theta) = \frac{q-1}{h}$. Thus $\text{gcd}(\text{ord}(\theta), \text{ord}(\alpha_2))=1$. Hence, $\langle \theta \rangle, \alpha_2 \langle \theta \rangle, \dots, \alpha_2^q \langle \theta \rangle$ are distinct cosets in the multiplicative group $\mathbb{F}_{q^2}^*$. Assume

$$\begin{aligned} \mathbf{a}_s &= \left(0, \alpha_2^0(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{h}-1}), \alpha_2^1(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{h}-1}), \right. \\ &\quad \left. \dots, \alpha_2^q(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{h}-1}) \right) \in \mathbb{F}_{q^2}^n, \\ \mathbf{u} &= \left(1, \omega^{-ch}, \dots, \omega^{-c(\frac{q-1}{h}-1)h} \right), \\ \mathbf{v} &= \left(1, \underbrace{\mathbf{u}, \mathbf{u}, \dots, \mathbf{u}}_{(q+1) \text{ times}} \right) \in (\mathbb{F}_{q^2}^*)^n. \end{aligned}$$

For any $0 \leq i, j \leq n - 1$, we have

$$\begin{aligned} \left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E &= \omega^{s(qi+j)} \sum_{t=0}^{\frac{q-1}{h}-1} \theta^{t(qi+j)} \omega^{-ch(q+1)t} \sum_{v=0}^q \alpha_2^{v(qi+j)} \\ &= \omega^{s(qi+j)} \sum_{t=0}^{\frac{q-1}{h}-1} \theta^{t(qi+j-c)} \sum_{v=0}^q \alpha_2^{v(qi+j)}. \end{aligned}$$

Thus

$$\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E = \begin{cases} 0, & \frac{q-1}{h} \nmid qi + j - c, \\ \omega^{s(qi+j)n}, & \frac{q-1}{h} \mid qi + j - c, q + 1 \mid qi + j. \end{cases}$$

Then $\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if

$$\begin{cases} qi + j \equiv c, & \text{mod } \frac{q-1}{h}, \\ qi + j \equiv 0, & \text{mod } q + 1. \end{cases}$$

According to [24], the system has a solution

$$qi + j \equiv \frac{1}{2} \left(\frac{q-1}{h} + 1 \right) (q + 1)c \pmod{n}.$$

Hence, $\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if $\frac{q^2-1}{h} \mid qi + j - \frac{1}{2} \left(\frac{q-1}{h} + 1 \right) (q + 1)c$.

We firstly present the following result.

Lemma 2 [24] *Suppose the notations \mathbf{a}_s, \mathbf{v} be given as above. Let $q = hm + 1$ be a prime power and $h \geq 1$ be an integer. Assume c is some integer such that $1 \leq c \leq h + 1$.*

- (1) *If c is some integer such that $c = l\frac{q-1}{h}, l = 1, 2, \dots$. Suppose $(c - 1)\frac{q-1}{h} + 1 \leq k \leq c\frac{q-1}{h}$, then for any $0 \leq i, j \leq k - 1$, $\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if $(i, j) = (\frac{1}{2}(\frac{q-1}{h} + 1)c + r\frac{q-1}{h}, \frac{1}{2}(\frac{q-1}{h} + 1)c + r\frac{q-1}{h}), r \in [-\frac{1}{2}(\frac{q-1}{h} + 1)l, c - [\frac{1}{2}(\frac{q-1}{h} + 1)l + 1]]$.*
- (2) *If c is some integer such that $1 + l\frac{q-1}{h} \leq c < (l + 1)\frac{q-1}{h}, l = 0, 1, \dots$. Suppose $\frac{1}{2}(\frac{q-1}{h} + 1)c + \lceil \frac{c-l-2}{2} \rceil \frac{q-1}{h} + 1 \leq k \leq \frac{1}{2}(\frac{q-1}{h} + 1)c + \lceil \frac{c-l}{2} \rceil \frac{q-1}{h}$, then for any $0 \leq i, j \leq k - 1$, $\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if $(i, j) = (\frac{1}{2}(\frac{q-1}{h} + 1)c + r\frac{q-1}{h}, \frac{1}{2}(\frac{q-1}{h} + 1)c + r\frac{q-1}{h}), r \in [-\lceil \frac{c+l-1}{2} \rceil, \lceil \frac{c-l-2}{2} \rceil]$.*

Next we will obtain below result in the light of the previous lemma.

With the same manner in Theorem 2, there exists the linear code $GRS_{n-k}(\mathbf{a}, \mathbf{w}_r)$ has parameters $[n, n - k, k + 1]_{q^2}$ and parity check matrix $H = G$.

Apparently, $\text{rank}(GG^\dagger) = \text{rank}(G_s G_s^\dagger) = c$. It follows from Theorem 1 that the result holds.

This completes the proof. □

Firstly, we compare parameters of new EAQMDS codes with corresponding QMDS codes in Theorem 2 [25] for q even by Table 1.

Particularly, when $c = 1$, if $h = q - 1$, then we have $k = c = 1$; if $h < q - 1$, then we obtain $\frac{1}{2}(\frac{q-1}{h} + 1) + 1 \leq k \leq \frac{1}{2}(\frac{q-1}{h} + 1) + \frac{q-1}{h}$.

3.2 Length $n = 1 + \frac{q-1}{h} \cdot \frac{q+1}{2}, q \equiv 1 \pmod{4}$

In this subsection, we always assume that $q = hm + 1, h \geq 1$ is an integer, $n = 1 + \frac{q^2-1}{2h}$. Set $\alpha_1 = \omega^{q+1}, \alpha_2 = \omega^{2(q-1)}$, then $\text{ord}(\alpha_1) = q - 1, \text{ord}(\alpha_2) = \frac{q+1}{2}$. Moreover, let $\theta = \alpha_1^h$, then $\text{ord}(\theta) = \frac{q-1}{h}$. Thus $\text{gcd}(\text{ord}(\theta), \text{ord}(\alpha_2))=1$. Hence, $\langle \theta \rangle, \alpha_2 \langle \theta \rangle, \dots, \alpha_2^{\frac{q+1}{2}-1} \langle \theta \rangle$ are distinct cosets in the multiplicative group $\mathbb{F}_{q^2}^*$. Assume

$$\begin{aligned} \mathbf{a}_s &= \left(0, \alpha_2^0(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{h}-1}), \alpha_2^1(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{h}-1}), \right. \\ &\quad \left. \dots, \alpha_2^{\frac{q+1}{2}-1}(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{h}-1}) \right) \in \mathbb{F}_{q^2}^n, \\ \mathbf{u} &= \left(1, \omega^{-ch}, \dots, \omega^{-c(\frac{q-1}{h}-1)h} \right), \\ \mathbf{v} &= \underbrace{(1, \mathbf{u}, \mathbf{u}, \dots, \mathbf{u})}_{\frac{q+1}{2} \text{ times}} \in (\mathbb{F}_{q^2}^*)^n. \end{aligned}$$

Firstly, we present the following result.

For any $0 \leq i, j \leq n - 1$, we have

$$\begin{aligned} \left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E &= \omega^{s(qi+j)} \sum_{t=0}^{\frac{q-1}{h}-1} \theta^{t(qi+j)} \omega^{-ch(q+1)t} \sum_{v=0}^{\frac{q+1}{2}-1} \alpha_2^{v(qi+j)} \\ &= \omega^{s(qi+j)} \sum_{t=0}^{\frac{q-1}{h}-1} \theta^{t(qi+j-c)} \sum_{v=0}^{\frac{q+1}{2}-1} \alpha_2^{v(qi+j)}. \end{aligned}$$

Thus

$$\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E = \begin{cases} 0, & \frac{q-1}{h} \nmid qi + j - c, \\ \omega^{s(qi+j)n}, & \frac{q-1}{h} \mid qi + j - c, \frac{q+1}{2} \mid qi + j. \end{cases}$$

Then $\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if

$$\begin{cases} qi + j \equiv c, & \text{mod } \frac{q-1}{h}, \\ qi + j \equiv 0, & \text{mod } \frac{q+1}{2}. \end{cases}$$

According to [24], the system has a solution

$$qi + j \equiv \frac{q + 1}{2}c \pmod{n}.$$

Table 1 Some EAQMDS codes of length $n = 1 + r \frac{q-1}{h}, 1 \leq r \leq h$

Type	Paras.	k	Ref.
QMDS	$[[n, n - 2k, k + 1]]_q$	$1 \leq k \leq r \frac{q-1}{h}$	[25]
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$ $(1 \leq c \leq h + 1)$	$c = l \frac{q-1}{h}, l = 1, 2, \dots$ $(c - 1) \frac{q-1}{h} + 1 \leq k \leq c \frac{q-1}{h}$	NEW
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$ $(1 \leq c \leq h + 1)$	$1 + l \frac{q-1}{h} \leq c < (l + 1) \frac{q-1}{h}, l = 0, 1, \dots$ $\frac{1}{2} \left(\frac{q-1}{h} + 1 \right) c + \left\lceil \frac{c-l-2}{2} \right\rceil \frac{q-1}{h} + 1 \leq k \leq \frac{1}{2} \left(\frac{q-1}{h} + 1 \right) c + \left\lceil \frac{c-l}{2} \right\rceil \frac{q-1}{h}$	NEW

Next, we discuss the following two cases:

3.2.1 $\frac{q-1}{h}$ is Even

Lemma 3 [24] *Let $q = hm + 1$ be a prime power with $h \geq 1$ an integer, where m is even. Set $n = \frac{q^2-1}{2h}$. Assume c is some even integer such that $2 \leq c \leq 2h$.*

- (1) *If c is some even integer such that $c = l\frac{q-1}{h}, l = 1, 2, \dots$. Suppose $(c - 1)\frac{q-1}{2h} + 1 \leq k \leq c\frac{q-1}{2h}$, then for any $0 \leq i, j \leq k - 1, \left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if $(i, j) = (r\frac{q-1}{2h} + \frac{c}{2}, r\frac{q-1}{2h} + \frac{c}{2}), r \in [-l, c - (l + 1)]$.*
- (2) *If c is some even integer such that $2 + l\frac{q-1}{h} \leq c < (l + 1)\frac{q-1}{h}, l = 0, 1, \dots$. Suppose $(c - l - 1)\frac{q-1}{2h} + \frac{c}{2} + 1 \leq k \leq (c - l)\frac{q-1}{2h} + \frac{c}{2}$, then for any $0 \leq i, j \leq k - 1, \left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if $(i, j) = (r\frac{q-1}{2h} + \frac{c}{2}, r\frac{q-1}{2h} + \frac{c}{2}), r \in [-l, c - (l + 1)]$.*

Theorem 4 *Let $q = hm + 1$ be a prime power with $h \geq 1$ an integer, where m is even. Set $n = 1 + \frac{q^2-1}{2h}$. Assume c is some even integer such that $2 \leq c \leq 2h$, then*

- (1) *For any $c = l\frac{q-1}{h}, l = 1, 2, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $(c - 1)\frac{q-1}{2h} + 1 \leq k \leq c\frac{q-1}{2h}$.*
- (2) *For any $2 + l\frac{q-1}{h} \leq c < (l + 1)\frac{q-1}{h}, l = 0, 1, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $(c - l - 1)\frac{q-1}{2h} + \frac{c}{2} + 1 \leq k \leq (c - l)\frac{q-1}{2h} + \frac{c}{2}$.*

We can also obtain a more general result.

Theorem 5 *Let $q = hm + 1$ be a prime power with $h \geq 1$ an integer, where m is even. Set $n = 1 + r\frac{q^2-1}{2h}, 1 \leq r \leq 2h$. Assume c is some even integer such that $2 \leq c \leq 2h$, then*

- (1) *For any $c = l\frac{q-1}{h}, l = 1, 2, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $(c - 1)\frac{q-1}{2h} + 1 \leq k \leq c\frac{q-1}{2h}$.*
- (2) *For any $2 + l\frac{q-1}{h} \leq c < (l + 1)\frac{q-1}{h}, l = 0, 1, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $(c - l - 1)\frac{q-1}{2h} + \frac{c}{2} + 1 \leq k \leq (c - l)\frac{q-1}{2h} + \frac{c}{2}$.*

3.2.2 $\frac{q-1}{h}$ is Odd

Lemma 4 [24] *Let $q = hm + 1$ be a prime power with $h \geq 1$ an even integer, where m is odd. Set $n = 1 + \frac{q^2-1}{2h}$. Assume c is some integer such that $1 \leq c \leq \frac{h}{2}$.*

- (1) *If c is some integer such that $c = l\frac{q-1}{h}, l = 1, 2, \dots$. Suppose $(c - 1)\frac{q-1}{h} + 1 \leq k \leq c\frac{q-1}{h}$, then for any $0 \leq i, j \leq k - 1, \left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if $(i, j) = (\frac{1}{2}(\frac{q-1}{h} + 1)c + r\frac{q-1}{h}, \frac{1}{2}(\frac{q-1}{h} + 1)c + r\frac{q-1}{h}), r \in [-\frac{1}{2}(\frac{q-1}{h} + 1)l, c - [\frac{1}{2}(\frac{q-1}{h} + 1)l + 1]]$.*

- (2) If c is some integer such that $1 + l\frac{q-1}{h} \leq c < (l + 1)\frac{q-1}{h}, l = 0, 1, \dots$. Suppose $\frac{1}{2}(\frac{q-1}{h} + 1)c + \lceil \frac{c-l-2}{2} \rceil \frac{q-1}{h} + 1 \leq k \leq \frac{1}{2}(\frac{q-1}{h} + 1)c + \lceil \frac{c-l}{2} \rceil \frac{q-1}{h}$, then for any $0 \leq i, j \leq k - 1, \langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \rangle_E \neq 0$ if and only if $(i, j) = (\frac{1}{2}(\frac{q-1}{h} + 1)c + r\frac{q-1}{h}, \frac{1}{2}(\frac{q-1}{h} + 1)c + r\frac{q-1}{h}), r \in [-\lceil \frac{c+l-1}{2} \rceil, \lceil \frac{c-l-2}{2} \rceil]$.

Next we will obtain the following result in the light of the previous lemma.

Theorem 6 Let $q = hm + 1$ be a prime power with $h \geq 1$ an even integer, where m is odd. Set $n = 1 + \frac{q^2-1}{2h}$. Assume c is some integer such that $1 \leq c \leq \frac{h}{2}$, then

- (1) For any $c = l\frac{q-1}{h}, l = 1, 2, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $(c - 1)\frac{q-1}{h} + 1 \leq k \leq c\frac{q-1}{h}$.
- (2) For any $1 + l\frac{q-1}{h} \leq c < (l + 1)\frac{q-1}{h}, l = 0, 1, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $\frac{1}{2}(\frac{q-1}{h} + 1)c + \lceil \frac{c-l-2}{2} \rceil \frac{q-1}{h} + 1 \leq k \leq \frac{1}{2}(\frac{q-1}{h} + 1)c + \lceil \frac{c-l}{2} \rceil \frac{q-1}{h}$.

Theorem 7 Let $q = hm + 1$ be a prime power with $h \geq 1$ an even integer, where m is odd. Set $n = 1 + r\frac{q^2-1}{2h}, 1 \leq r \leq 2h$. Assume c is some integer such that $1 \leq c \leq \frac{h}{2}$, then

- (1) For any $c = l\frac{q-1}{h}, l = 1, 2, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $(c - 1)\frac{q-1}{h} + 1 \leq k \leq c\frac{q-1}{h}$.
- (2) For any $1 + l\frac{q-1}{h} \leq c < (l + 1)\frac{q-1}{h}, l = 0, 1, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $\frac{1}{2}(\frac{q-1}{h} + 1)c + \lceil \frac{c-l-2}{2} \rceil \frac{q-1}{h} + 1 \leq k \leq \frac{1}{2}(\frac{q-1}{h} + 1)c + \lceil \frac{c-l}{2} \rceil \frac{q-1}{h}$.

We compare parameters of new EAQMDS codes with corresponding QMDS codes in Theorem 2 [25] for $q \equiv 1 \pmod{4}$ by Table 2.

3.3 Length $n = 1 + \frac{q-1}{2h}(q + 1), q \equiv 3 \pmod{4}$

In this subsection, we always assume that $q = 2hm + 1, h \geq 1$ is an integer, $n = 1 + \frac{q^2-1}{2h}$. Set $\alpha_1 = \omega^{2(q+1)}, \alpha_2 = \omega^{q-1}$, then $\text{ord}(\alpha_1) = \frac{q-1}{2}, \text{ord}(\alpha_2) = q+1$. Moreover, let $\theta = \alpha_1^h$, then $\text{ord}(\theta) = \frac{q-1}{2}$. Thus $\text{gcd}(\text{ord}(\theta), \text{ord}(\alpha_2))=1$. Hence, $\langle \theta \rangle, \alpha_2 \langle \theta \rangle, \dots, \alpha_2^q \langle \theta \rangle$ are distinct cosets in the multiplicative group \mathbb{F}_q^* . Assume

$$\begin{aligned} \mathbf{a}_s &= \left(0, \alpha_2^0(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{2h}-1}), \alpha_2^1(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{2h}-1}), \right. \\ &\quad \left. \dots, \alpha_2^q(w^s, w^s\theta, \dots, w^s\theta^{\frac{q-1}{2h}-1}) \right) \in \mathbb{F}_{q^2}^n, \\ \mathbf{u} &= \left(1, \omega^{-2ch}, \dots, \omega^{-2c(\frac{q-1}{2h}-1)h} \right), \\ \mathbf{v} &= \left(1, \underbrace{\mathbf{u}, \mathbf{u}, \dots, \mathbf{u}}_{(q+1) \text{ times}} \right) \in (\mathbb{F}_{q^2}^*)^n. \end{aligned}$$

We firstly give the following result.

Table 2 Some EAQMDS codes of length $n = 1 + r \frac{q-1}{2h}, 1 \leq r \leq 2h$

Type	Paras.	k	Ref.
QMDS	$[[n, n - 2k, k + 1]]_q$	$1 \leq k \leq r \frac{q-1}{2h}$	[25]
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$	$c = l \frac{q-1}{h}, l = 1, 2, \dots$	NEW
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$	$(c - 1) \frac{q-1}{2h} + 1 \leq k \leq c \frac{q-1}{2h}$ $2 + l \frac{q-1}{h} \leq c < (l + 1) \frac{q-1}{h}, l = 0, 1, \dots$	NEW
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$	$(c - l - 1) \frac{q-1}{2h} + \frac{c}{2} + 1 \leq k \leq (c - l) \frac{q-1}{2h} + \frac{c}{2}$	NEW
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$	$c = l \frac{q-1}{h}, l = 1, 2, \dots$	NEW
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$	$(c - 1) \frac{q-1}{h} + 1 \leq k \leq c \frac{q-1}{h}$	NEW
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$	$1 + l \frac{q-1}{h} \leq c < (l + 1) \frac{q-1}{h}, l = 0, 1, \dots$	NEW
		$\frac{1}{2} \left(\frac{q-1}{h} + 1 \right) c + \left\lfloor \frac{c-l-2}{2} \right\rfloor \frac{q-1}{h} + 1 \leq k \leq \frac{1}{2} \left(\frac{q-1}{h} + 1 \right) c + \left\lceil \frac{c-l}{2} \right\rceil \frac{q-1}{h}$	

For any $0 \leq i, j \leq n - 1$, we have

$$\begin{aligned} \left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E &= \omega^{s(qi+j)} \sum_{t=0}^{\frac{q-1}{2h}-1} \theta^{t(qi+j)} \omega^{-2ch(q+1)t} \sum_{v=0}^q \alpha_2^{v(qi+j)} \\ &= \omega^{s(qi+j)} \sum_{t=0}^{\frac{q-1}{2h}-1} \theta^{t(qi+j-c)} \sum_{v=0}^q \alpha_2^{v(qi+j)}. \end{aligned}$$

Thus

$$\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E = \begin{cases} 0, & \frac{q-1}{2h} \nmid qi + j - c, \\ \omega^{s(qi+j)} n, & \frac{q-1}{2h} \mid qi + j - c, q + 1 \mid qi + j. \end{cases}$$

Then $\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if

$$\begin{cases} qi + j \equiv c, & \text{mod } \frac{q-1}{2h}, \\ qi + j \equiv 0, & \text{mod } q + 1. \end{cases}$$

According to [24], the system has a solution

$$qi + j \equiv \frac{1}{2} \left(\frac{q-1}{2h} + 1 \right) (q+1)c \pmod{n}.$$

According to previous discussions, we can obtain the result as follows.

Lemma 5 [24] *Let $q = 2hm + 1$ be a prime power with $h \geq 1$ an integer. Set $n = 1 + \frac{q^2-1}{2h}$. Assume c is some integer such that $1 \leq c \leq 2h + 1$.*

- (1) *If c is some integer such that $c = l \frac{q-1}{2h}, l = 1, 2, \dots$. Suppose $(c - 1) \frac{q-1}{2h} + 1 \leq k \leq c \frac{q-1}{2h}$, then for any $0 \leq i, j \leq k - 1$, $\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if $(i, j) = (\frac{1}{2}(\frac{q-1}{2h} + 1)c + r \frac{q-1}{2h}, \frac{1}{2}(\frac{q-1}{2h} + 1)c + r \frac{q-1}{2h}), r \in [-\frac{1}{2}(\frac{q-1}{2h} + 1)l, c - [\frac{1}{2}(\frac{q-1}{2h} + 1)l + 1]]$.*
- (2) *If c is some integer such that $1 + l \frac{q-1}{2h} \leq c < (l + 1) \frac{q-1}{2h}, l = 0, 1, \dots$. Suppose $\frac{1}{2}(\frac{q-1}{2h} + 1)c + \lceil \frac{c-l-2}{2} \rceil \frac{q-1}{2h} + 1 \leq k \leq \frac{1}{2}(\frac{q-1}{2h} + 1)c + \lceil \frac{c-l}{2} \rceil \frac{q-1}{2h}$, then for any $0 \leq i, j \leq k - 1$, $\left\langle \mathbf{a}_s^{qi+j}, \mathbf{v}^{q+1} \right\rangle_E \neq 0$ if and only if $(i, j) = (\frac{1}{2}(\frac{q-1}{2h} + 1)c + r \frac{q-1}{2h}, \frac{1}{2}(\frac{q-1}{2h} + 1)c + r \frac{q-1}{2h}), r \in [-\lceil \frac{c+l-1}{2} \rceil, \lceil \frac{c-l-2}{2} \rceil]$.*

Theorem 8 *Let $q = 2hm + 1$ be a prime power with $h \geq 1$ an integer. Set $n = 1 + \frac{q^2-1}{2h}$. Assume c is some integer such that $1 \leq c \leq 2h + 1$, then*

- (1) *For any $c = l \frac{q-1}{2h}, l = 1, 2, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $(c - 1) \frac{q-1}{2h} + 1 \leq k \leq c \frac{q-1}{2h}$.*
- (2) *For any $1 + l \frac{q-1}{2h} \leq c < (l + 1) \frac{q-1}{2h}, l = 0, 1, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $\frac{1}{2}(\frac{q-1}{2h} + 1)c + \lceil \frac{c-l-2}{2} \rceil \frac{q-1}{2h} + 1 \leq k \leq \frac{1}{2}(\frac{q-1}{2h} + 1)c + \lceil \frac{c-l}{2} \rceil \frac{q-1}{2h}$.*

We can similarly yield a more general result as follows.

Table 3 Some EAQMDS codes of length $n = 1 + r \frac{q-1}{2h}$, $1 \leq r \leq 2h$

Type	Paras.	k	Ref.
QMDS	$[[n, n - 2k, k + 1]]_q$	$1 \leq k \leq r \frac{q-1}{2h}$	[25]
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$ $(1 \leq c \leq 2h + 1)$	$c = l \frac{q-1}{2h}$, $l = 1, 2, \dots$ $(c - 1) \frac{q-1}{2h} + 1 \leq k \leq c \frac{q-1}{2h}$	NEW
EAQMDS	$[[n, n - 2k + c, k + 1; c]]_q$ $(1 \leq c \leq 2h + 1)$	$1 + l \frac{q-1}{2h} \leq c < (l + 1) \frac{q-1}{2h}$, $l = 0, 1, \dots$ $\frac{1}{2} (\frac{q-1}{2h} + 1)c + \left\lceil \frac{c-l-2}{2} \right\rceil \frac{q-1}{2h} + 1 \leq k \leq \frac{1}{2} (\frac{q-1}{2h} + 1)c + \left\lceil \frac{c-l}{2} \right\rceil \frac{q-1}{2h}$	NEW

Theorem 9 Let $q = 2hm + 1$ be a prime power with $h \geq 1$ an integer. Set $n = 1 + r \frac{q^2-1}{2h}$, $1 \leq r \leq 2h$. Assume c is some integer such that $1 \leq c \leq 2h + 1$, then

- (1) For any $c = l \frac{q-1}{2h}$, $l = 1, 2, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $(c - 1) \frac{q-1}{2h} + 1 \leq k \leq c \frac{q-1}{2h}$.
- (2) For any $1 + l \frac{q-1}{2h} \leq c < (l + 1) \frac{q-1}{2h}$, $l = 0, 1, \dots$, there exist EAQMDS codes with parameters $[[n, n - 2k + c, k + 1; c]]_q$, where $\frac{1}{2}(\frac{q-1}{2h} + 1)c + \lceil \frac{c-l-2}{2} \rceil \frac{q-1}{2h} + 1 \leq k \leq \frac{1}{2}(\frac{q-1}{2h} + 1)c + \lceil \frac{c-l}{2} \rceil \frac{q-1}{2h}$.

Now, we compare parameters of new EAQMDS codes with corresponding QMDS codes in Theorem 2 [25] for $q \equiv 3 \pmod{4}$ by Table 3.

4 Conclusion and Discussion

We have known that GRS and extended GRS codes have become one of the best resources for constructing optimal quantum codes and entanglement-assisted quantum codes. In this paper we have employed GRS codes to construct several classes of entanglement-assisted quantum MDS codes which have best parameters. In addition to the existing results, these quantum codes are new. The further investigation is to construct q -ary EAQMDS codes that minimum distance as large as possible with respect to the code length.

Acknowledgments This work is supported by the National Natural Science Foundation of China under Grant Nos. 11801564 and 11471011.

References

1. Brun, T.A., Devetak, I., Hsieh, M.-H.: Correcting quantum errors with entanglement. *Science* **314**, 436–439 (2006)
2. Grassl, M.: Entanglement-assisted quantum communication beating the quantum Singleton bound. Talk at AQIS, Taiwan, China (2016)
3. Lai, C., Ashikhmin, A.: Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators. *IEEE Trans. Inf. Theory* **64**(1), 622–639 (2018)
4. Hsieh, M.-H., Devetak, I., Brun, T.A.: General entanglement-assisted quantum error-correcting codes. *Phys. Rev. A* **76**, 062313 (2007)
5. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. *Phys. Rev. A* **77**, 064302 (2008)
6. Lai, C.Y., Brun, T.A.: Entanglement increases the error-correcting ability of quantum error-correcting codes. *Phys. Rev. A* **88**, 012320 (2013)
7. Lai, C.Y., Brun, T.A., Wilde, M.M.: Duality in entanglement-assisted quantum error correction. *IEEE Trans. Inf. Theory* **59**, 4020–4024 (2013)
8. Fan, J., Chen, H., Xu, J.: Construction of q -ary entanglement-assisted quantum MDS codes with minimum distance greater than $q + 1$. *Quantum Inf. Comput.* **16**, 0423–0434 (2016)
9. Li, L., Zhu, S., Liu, L., Kai, X.: Entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes. *Quantum Inf. Process.* **18**, 153 (2019)
10. Li, R., Guo, L., Xu, Z.: Entanglement-assisted quantum codes achieving the quantum Singleton bound but violating the quantum Hamming bound. *Quantum Inf. Comput.* **14**, 1107–1116 (2014)
11. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. *Des. Codes Cryptogr.* **86**, 121–136 (2018)
12. Guo, L., Li, R.: Linear Plotkin bound for entanglement-assisted quantum codes. *Phys. Rev. A* **87**, 032309 (2013)

13. Lv, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. *Quantum Inf. Process.* **17**, 69 (2018)
14. Qian, J., Zhang, L.: Entanglement-assisted quantum codes from arbitrary binary linear codes. *Des. Codes Cryptogr.* **77**, 193–202 (2015)
15. Lv, L., Ma, W., Li, R., Ma, Y., Liu, Y., Cao, H.: Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance. *Finite Fields Appl.* **53**, 309–325 (2018)
16. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. *Quantum Inf Process.* **16**, 303 (2017)
17. Liu, Y., Li, R., Lv, L., Ma, Y.: Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. *Quantum Inf. Process.* **17**, 210 (2018)
18. Qian, J., Zhang, L.: Constructions of new entanglement-assisted quantum MDS and almost MDS codes. *Quantum Inf. Process.* **18**, 71 (2019)
19. Li, R., Guo, G., Song, H., Liu, Y.: New constructions of entanglement-assisted quantum MDS codes from negacyclic codes. *Int. J. Quantum Inf.* **17**(3), 1950022 (2019)
20. Luo, G., Cao, X.: MDS codes with hulls of arbitrary dimensions and their quantum error correction. *IEEE Trans. Inf. Theory* **65**(5), 2944–2952 (2019)
21. Luo, G., Cao, X.: Two new families of entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes. *Quantum Inf. Process.* **18**, 89 (2019)
22. Sari, M., Kolotoğlu, M.: An application of constacyclic codes to entanglement-assisted quantum MDS codes. *E. Comp. Appl. Math.* **38**, 75 (2019)
23. Fang, W., Fu, F., Li, L., Zhu, S.: Euclidean and hermitian hulls of MDS codes and their applications to EAQECCs. [arXiv:1812.09019](https://arxiv.org/abs/1812.09019) (2019)
24. Guo, G., Li, R., Liu, Y., Wang, J.: Some construction of entanglement-assisted quantum MDS codes. (submitted) (2019)
25. Fang, W., Fu, F.: Some new constructions of quantum MDS codes. *IEEE Transactions on Information Theory*, <https://doi.org/10.1109/TIT.2019.2939114> (2019)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.