Quantum Information and Computation, Vol. 14, No. 13&14 (2014) 1107–1116

ENTANGLEMENT-ASSISTED QUANTUM CODES ACHIEVING THE QUANTUM SINGLETON BOUND BUT VIOLATING THE QUANTUM HAMMING BOUND

RUIHU LI [a] LUOBIN GUO
School of Science, Air Force Engineering University, Xi'an, Shaanxi 710051, P. R. China

ZONGBEN XU
Institute for Information and System Sciences, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China

Received February 16, 2013
Revised December 30, 2013

We give an infinite family of degenerate entanglement-assisted quantum error-correcting codes (EAQECCs) which violate the EA-quantum Hamming bound for non-degenerate EAQECCs and achieve the EA-quantum Singleton bound, thereby proving that the EA-quantum Hamming bound does not asymptotically hold for degenerate EAQECCs. Unlike the previously known quantum error-correcting codes that violate the quantum Hamming bound by exploiting maximally entangled pairs of qubits, our codes do not require local unitary operations on the entangled auxiliary qubits during encoding. The degenerate EAQECCs we present are constructed from classical error-correcting codes with poor minimum distances, which implies that, unlike the majority of known EAQECCs with large minimum distances, our EAQECCs take more advantage of degeneracy and rely less on the error correction capabilities of classical codes.

Keywords: Entanglement-assisted quantum error-correcting code (EAQECC), EA-quantum Singleton bound, EA-quantum Hamming bound, maximal-distance-separable (MDS) code.
Communicated by: R Jozsa & R Laflamme

1 Introduction

Quantum error-correcting codes (QECCs) play a vital role in reliable quantum information transmission as well as fault-tolerant quantum computation [1, 2, 3, 4, 5]. The most widely studied class of quantum codes are stabilizer (or additive) quantum codes, which are specified by Abelian groups of tensor products of Pauli operators. The majority of QECCs studied so far are stabilizer codes, binary [1, 2, 6, 7, 8, 9, 10, 11, 12] or non-binary [13, 14, 15, 16].

A q-ary stabilizer code can be constructed from classical codes over finite fields $\mathbf{F}_q$ or $\mathbf{F}_{q^2}$ with certain self-orthogonal properties, where q is a prime power and $\mathbf{F}_q$ is the finite field with q elements [9, 15]. Unfortunately, the need for a self-orthogonal parity check matrix presents a substantial obstacle to importing the classical theory in quantum codes entirely, especially in the context of modern codes such as low-density parity check (LDPC) codes [17]. Brun, Devetak and Hsieh devised the entanglement-assisted (EA) stabilizer formalism in [17],

[a] liruihu2008@aliyun.com.

including the standard stabilizer formalism [6, 7, 9, 15] as a special case. They showed that if shared entanglement between the encoder and decoder is available, classical linear quaternary (and binary) codes that are not self-orthogonal can be transformed into EAQECCs. This EA stabilizer formalism generalized the idea of Bowen's [18]. Following [17], there are a lot of papers making further study of EAQECCs [19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34], and [26] showing that entanglement can increase the error-correcting ability of quantum error-correcting codes.

An $[[n, k, d_{ea}; c]]$ EAQECC encodes k information qubits into n physical qubits with the help of c maximally entangled pairs of qubits, called ebits. In the entanglement-assisted protocol given by Brun, Devetak, and Hsieh [17], the sender and receiver pre-share c pairs of maximally entangled qubits. The sender possesses arbitrary k-qubit information and her half of the c maximally entangled pairs. The k-qubit information is encoded with $n-k-c$ ancilla qubits and the c entangled qubits. The sender sends the resulting n qubits to the receiver through a noisy channel. The receiver then performs measurements on these n qubits together with his half of the c pre-shared pairs to diagnose errors. With an $[[n, k, d_{ea}; c]]$ EAQECC, up to $\lfloor \frac{d_{ea}-1}{2} \rfloor$ errors on the noisy n qubits can be corrected.

As in classical coding theory, there are many bounds on QECCs and EAQECCs, such as the quantum Singleton bound [8, 9, 11] and the quantum Hamming bound for nondegenerate (or pure) QECCs [6], the EA-quantum Singleton bound and the EA-quantum Hamming bound for nondegenerate EAQECCs [17, 18]. For definitions of degenerate and nondegenerate EAQECCs, see Section 2.

Lemma 1.1 (EA-quantum Singleton bound [17]) If $\mathcal{Q}^{ea} = [[n, k, d_{ea}; c]]$, then $n + c - k \geq 2(d_{ea} - 1)$. An EAQECC achieving this bound is called a *maximal-distance-separable* (MDS) EAQECC.

Lemma 1.2 (EA-quantum Hamming bound [18]) If $[[n, k, d_{ea}; c]]$ is a nondegenerate EAQECC, $t = \lfloor \frac{d_{ea}-1}{2} \rfloor$, then $2^{n+c-k} \geq \sum_{i=0}^{t} 3^i \binom{n}{i}$.

All standard QECCs satisfy the quantum Singleton bound and all EAQECCs satisfy the EA-Singleton bound [8, 26]. It is not known whether a degenerate stabilizer code can violate the quantum Hamming bound without pre-shared entanglement (see [7, 11, 35, 36]), although there is an impure subsystem code that beats the Hamming bound [37]. The degenerate (or impure) quantum codes are a particularly interesting class of quantum codes because they can pack more quantum information. A striking feature of degenerate quantum codes is that they can be used to correct more errors than they can uniquely identify, not all correctable errors need to be distinguished or even detected by active error correction strategies [3, 38]. It is known that well-designed degenerated codes may outperform all non-degenerate ones over correlated noise channels and very noisy channels [38, 39, 40, 41, 42] and have important applications in purifying quantum states [42]. Degenerate codes were also used in proving the security of quantum communication protocols [43].

In [15], Ketkar *et al.* showed that all standard QECCs achieving the quantum Singleton bound must be nondegenerate and obey the quantum Hamming bound. In [26], Lai *et al.* discussed the construction of optimal EAQECCs. An $[[n, k, d_{ea}; c]]$ EAQECC is *optimal* in

the sense that d_{ea} is the highest achievable minimum distance for given parameters n, k and c. They showed that there are degenerate EAQECCs achieving the EA-Singleton bound. It is natural to ask whether there exists a degenerate EAQECC that violates the EA-quantum Hamming bound. In this paper, we will show that there are degenerate EAQECCs achieving the EA-Singleton bound but beating the EA-quantum Hamming bound.

Remark Note that Dong et al. [29] constructed quantum error-correcting codes of length n, dimension 1, and minimum distance n that exploit 1 qubit that does not suffer from errors. If we let an ebit play the role of the error-free qubit, these codes may be considered to violate the EA-quantum Hamming bound. However, as noted in [29], because this approach requires a protocol that involves some local unitary operations on the ebit during encoding, one-way classical communication is necessary in addition to the ebit for encoding and decoding. Because QECCs that take advantage of ebits are called EAQECCs most typically when their protocols do not require additional resources other than ebits (see, for example, Section IV of [33] and the noiseless case in [34], where their QECCs that can also be seen as EAQECCs only require maximally entangled pairs when used as EAQECCs), we follow this practice in the relevant literature in this regard and do not rely on any additional resource such as a classical channel for encoding and decoding except ebits. In fact, all quantum error-correcting codes we construct in this paper employ exactly the same protocol as the original entanglement-assisted one given by Brun, Devetak, and Hsieh [17] and hence are EAQECCs in the strict sense.

This paper is organized as follows. In Section 2, basic concepts on the EA-stabilizer formalism and additive codes over the quaternary field $\mathbf{F}_4$ are reviewed. In Section 3, explicit constructions of MDS EAQECCs are presented and MDS EAQECCs violating the EA-quantum Hamming bound are proved. Finally, in Section 4, discussions and remarks are drawn.

2 The EA-stabilizer formalism and additive codes

In this section, we review some basic knowledge on symplectic spaces, the EA formalism and additive codes for the propose of this paper. For more details, we refer the reader to [9], [17], [19] and [25].

Let $\mathbf{F}_2$ be the binary field and $\mathbf{F}_2^{2n}$ the $2n$-dimensional binary row vector space over $\mathbf{F}_2$, whose elements are denoted as $(a \mid b) = (a_1, a_2, \ldots, a_n \mid b_1, b_2, \ldots, b_n)$. Define the weight $wt_s((a \mid b))$ of $(a \mid b)$ to be the number of coordinates i such that at least one of a_i and b_i is 1, and the distance $d_s((a \mid b), (a^{'} \mid b^{'}))$ between $(a \mid b)$ and $(a^{'} \mid b^{'})$ to be $wt_s((a - a^{'} \mid b - b^{'}))$.

Let

$$K_{2n} = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}.$$

The symplectic inner product of $(a \mid b)$ and $(a^{'} \mid b^{'})$ with respect to K_{2n} is defined to be

$$((a \mid b), (a^{'} \mid b^{'}))_s = (a \mid b) K_{2n} (a^{'} \mid b^{'})^T = a(b^{'})^T + b(a^{'})^T.$$

The vector space $\mathbf{F}_2^{2n}$ equipped with this symplectic inner product is called a $2n$-dimensional symplectic space. If S is a linear subspace of $\mathbf{F}_2^{2n}$, then the symplectic dual $S^{\perp s}$ of S is the subspace

$$S^{\perp s}= \{(x \mid y) \in \mathbf{F}_2^{2n} \mid ((a \mid b),(x \mid y))_s = 0 \text{ for all } (a \mid b) \in S\}.$$

From [44] we know that $dim S^{\perp s} = 2n - dim S$ for any subspace S of $\mathbf{F}_2^{2n}$. A subspace S of $\mathbf{F}_2^{2n}$ is called *totally isotropic* if $S \subseteq S^{\perp s}$ and *totally non-isotropic* if $S \cap S^{\perp s} = \{0\}$ [44]. A totally isotropic subspace and a totally non-isotropic subspace are called an isotropic subspace and a non-isotropic subspace in [17], respectively.

Let $\mathcal{G}_n$ be the n-fold Pauli group, whose elements are written as $g = i^{\lambda} X(a)Z(b)$ where $\lambda \in Z_4$ and $(a \mid b) \in \mathbf{F}_2^{2n}$. The center of $\mathcal{G}_n$ is $Z(\mathcal{G}_n)= \{\pm I, \pm iI\}$, and the quotient group $\bar{\mathcal{G}}_n = \mathcal{G}_n / Z(\mathcal{G}_n)$ is isometrically isomorphism to the symplectic space $\mathbf{F}_2^{2n}$ under the map $\tau(i^{\lambda} X(a)Z(b)) = (a \mid b)$ [9]. If $\mathcal{A}$ is a subgroup of $\mathcal{G}_n$, then $\tau(\mathcal{A})$ is a subspace of $\mathbf{F}_2^{2n}$. For a subgroup $\mathcal{A}$, denote its centralizer as $\mathcal{Z}(\mathcal{A})$ [19] which is denoted as $\mathcal{N}(\mathcal{A})$ in [17] and [26], then $\tau(\mathcal{Z}(\mathcal{A})) = \tau(\mathcal{A})^{\perp s}$, where $\tau(\mathcal{A})^{\perp s}$ is the symplectic dual space of $\tau(\mathcal{A})$. If $\tau(\mathcal{A})$ is a totally isotropic subspace of $\mathbf{F}_2^{2n}$, $\mathcal{A}$ is called an isotropic subgroup of $\mathcal{G}_n$. If $\tau(\mathcal{A})$ is a totally non-isotropic subspace of $\mathbf{F}_2^{2n}$, $\mathcal{A}$ is called a symplectic subgroup of $\mathcal{G}_n$ in [17] and an entanglement subgroup in [19], respectively.

Let $\mathbf{F}_4 = \{0, 1, \omega, \varpi\}$ be the field of four elements, where $\varpi = 1 + \omega = \omega^2$, $\omega^3 = 1$, and the conjugation is defined by $\overline{x} = x^2$. Let $\mathbf{F}_4^n$ be the n-dimensional row vector space over $\mathbf{F}_4$. For $u = (u_1, u_2, ..., u_n)$ and $v = (v_1, v_2, ..., v_n) \in \mathbf{F}_4^n$, their trace inner product is defined as $(u,v)_T = Tr(u\overline{v}^T) = \sum_1^n (u_j \overline{v_j} + \overline{u_j} v_j) = \sum_1^n (u_j v_j^2 + u_j^2 v_j)$, and their Hermitian inner product is defined as $(u,v)_h = \sum_1^n u_j \overline{v_j} = \sum_1^n u_j v_j^2$. Following the terminology of [9], we define an $(n, 2^m)$ *additive code* $\mathcal{C}$ of length n over $\mathbf{F}_4$ to be a subgroup of size 2^m of $\mathbf{F}_4^n$. The *trace dual* $\mathcal{C}^{\perp T}$ of an $(n, 2^m)$ additive code $\mathcal{C}$ is the $(n, 2^{2n-m})$ additive code $\mathcal{C}^{\perp T} = \{u \in \mathbf{F}_4^n \mid (u,v)_T = 0 \text{ for all } v \in \mathcal{C}\}$. If $\mathcal{C}$ is an $[n,k]_4$ linear code, its Hermitian dual is defined as $\mathcal{C}^{\perp h} = \{u \in \mathbf{F}_4^n \mid (u,v)_h = 0 \text{ for all } v \in \mathcal{C}\}$, and $\mathcal{C}^{\perp h}$ is an $[n, n-k]_4$ linear code. An $[n,k]_4$ linear code $\mathcal{C}$ is an $(n, 2^{2k})$ additive code, and $\mathcal{C}^{\perp T} = \mathcal{C}^{\perp h}$ is an $(n, 2^{2(n-k)})$ additive code.

Now, we can give the EA formalism of [17] as follows.

Theorem 2.0 ([17, 19]) Let $\mathcal{S}$ be a subgroup of $\mathcal{G}_n$ of size 2^m, $\mathcal{S}_I$ be an isotropic subgroup of size 2^l and $\mathcal{S}_E$ an entanglement subgroup of size 2^{2c}. If $\mathcal{S} = \mathcal{S}_I \times \mathcal{S}_E$, then $\mathcal{S}$ can be extended into an Abelian subgroup $\tilde{\mathcal{S}}$ of $\mathcal{G}_{n+c}$ with c maximally entangled pairs. $\tilde{\mathcal{S}}$ stabilizes an EAQECC $\mathcal{Q}^{ea} = [[n, k, d_{ea}; c]]$, where $k = n+c-m = n-c-l$, $d_{ea} = \min \{wt(g) \mid g \in \mathcal{Z}(\mathcal{S}) \backslash \mathcal{S}_I\}$, and $\mathcal{Z}(\mathcal{S})$ is the centralizer of $\mathcal{S}$. $\mathcal{S}$ is called the *EA stabilizer* of $\mathcal{Q}^{ea}$.

Let the EA stabilizer of $\mathcal{Q}^{ea} = [[n, k, d_{ea}; c]]$ be $\mathcal{S}$. If all non-identity elements in $\mathcal{S}_I$ have weight greater than d_{ea}, then $\mathcal{Q}^{ea}$ is called a *nondegenerate* EAQECC, otherwise a *degenerate* one [26, 45]. It is very hard to construct EAQECCs using the framework of Theorem 2.0. In [25, 45], using relationship among $\mathcal{G}_n$, $\mathbf{F}_2^{2n}$ and $\mathbf{F}_4^n$, we reformulated Theorem 2.0 as the following equivalent Theorem 2.1. We give a condensed proof here, for more details please see [25].

Theorem 2.1 ([25, 45]) If there exists an $(n, 2^m)$ additive code $\mathcal{C}$ such that $R(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp T}$ forms an $(n, 2^l)$ additive code, then there exists an EAQECC $\mathcal{Q}^{ea} = [[n, k, d_{ea}; c]]$, where $k = n - c - l$, $2c = m - l$ and $d_{ea} = \min \{wt_s(\alpha) \mid \alpha \in C^{\perp T} \setminus R(\mathcal{C})\}$. $\mathcal{C}$ is called the *additive*

EA stabilizer of $\mathcal{Q}^{ea}$.

Proof. From [9], we know that there is a map ϕ from $\mathbf{F}_2^{2n}$ to $\mathbf{F}_4^n$ as: $\phi((a \mid b))= \omega a+\varpi b \in \mathbf{F}_4^n$ for $\alpha = (a \mid b) \in \mathbf{F}_2^{2n}$, and $wt_s(\alpha) = wt(\phi(\alpha))$ and $(\alpha, \beta)_s = (\phi(\alpha), \phi(\beta))_T$ for $\beta \in \mathbf{F}_2^{2n}$. Define $\sigma = \phi \circ \tau$, then σ is an isometrically isomorphism from $\overline{\mathcal{G}}_n$ onto $\mathbf{F}_4^n$.

Let $\mathcal{C}_E$ be a complement subgroup of $R(\mathcal{C})$ in $\mathcal{C}$, i.e., $\mathcal{C} = R(\mathcal{C})+ \mathcal{C}_E$ and $R(\mathcal{C})\cap\mathcal{C}_E= \{0\}$. Let $\mathcal{S} = \sigma^{-1}(\mathcal{C})$. It is not difficult to check that $\sigma^{-1}(R(\mathcal{C})) = \mathcal{S}_I$, $\sigma^{-1}(\mathcal{C}_E) = \mathcal{S}_E$ and $\mathcal{S} = \mathcal{S}_I \times \mathcal{S}_E$. From the parameters of $\mathcal{C}$ and $R(\mathcal{C})$, one can derive the sizes of $\mathcal{S}$ and $\mathcal{S}_I$ are 2^m and 2^l, respectively. Thus the theorem follows according to Theorem 2.0 $\square$.

Since each $[n, s]_4$ linear code over $\mathbf{F}_4$ is an $(n, 2^{2s})$ additive code, we have

Corollary 2.2 If there exists an $[n, s]_4$ linear code $\mathcal{C}$ such that $R(\mathcal{C}) = \mathcal{C}\cap\mathcal{C}^{\perp h}$ forms an $[n, r]_4$ linear code, then there exists an EAQECC $\mathcal{Q}^{ea}= [[n, k, d_{ea}; c]]$, where $k = n+c-2s = n-s-r$, $c = s - r$ and $d_{ea} = \min \{wt(\alpha) \mid \alpha \in C^{\perp h} \setminus R(\mathcal{C})\}$. And $\mathcal{C}^{\perp h}$ stabilizes an EAQECC $\mathcal{Q}^{ea\perp} = [[n, s - r, d_{ea}^{\perp h}; n - s - r]]$, $d_{ea}^{\perp h} = \min \{wt(\alpha) \mid \alpha \in C \setminus R(\mathcal{C})\}$.

Notation The EAQECCs $\mathcal{Q}^{ea}$ and $\mathcal{Q}^{ea\perp}$ in Corollary 2.2 are called linear EAQECCs in [45], and $\mathcal{Q}^{ea\perp}$ is called dual EAQECC of $\mathcal{Q}^{ea}$ in [27, 47].

3 Construction of MDS EAQECCs

In this section, we will construct an $[[n, 1, d_{ea}; c]]$ EAQECC for each $n \geq 6$. This EAQECC achieves the EA-Singleton bound.

The first $[[3, 1, 3; 2]]$ EAQECC proposed by Bowen in [18] and the $[[4, 1, 3; 1]]$ in [17] are MDS EAQECCs, and these two codes are nondegenerate and based on the $[[5, 1, 3]]$ quantum MDS code. Lai and Brun constructed degenerate MDS EAQECCs $[[7, 1, 5; 2]]$, $[[9, 1, 7; 4]]$ and $[[n, 1, n; n - 1]]$ for odd n in [26, 27]. Now we will use quaternary linear codes to construct an infinite class of MDS EAQECCs. Some of these EAQECCs violate the EA-quantum Hamming bound. Our construction is based on Corollary 2.2 and the following lemma.

Lemma 3.1 If there exists an $[n, n - s]_4$ linear code $\mathcal{C}$ such that $R(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp h}$ forms an $[n, s-1]_4$ linear code, then there exists an EAQECC $\mathcal{Q}^{ea}= [[n, 1, d_{ea}; n-2s+1]]$, where where $d_{ea} = \min \{wt(\alpha) \mid \alpha \in \mathcal{C}^{\perp h} \setminus R(\mathcal{C})\}$.

Proof. Since $\mathcal{C}$ is an $(n, 2^{2(n-s)})$ additive code and $R(\mathcal{C})$ is an $(n, 2^{2(s-1)})$ additive code, according to Theorem 2.1, $\mathcal{C}$ stabilizes an EAQECC $[[n, k, d_{ea}; c]$ with $2c = 2(n-s)-2(s-1)$, $k = n + c - 2(n - s) = 1$ and $d_{ea} = min\{wt(\alpha) \mid \alpha \in \mathcal{C}^{\perp h} \setminus R(\mathcal{C})\}$. Hence the lemma holds $\square$.

In the following of this section, we let $\mathbf{0_n} = (0, 0, ..., 0)$ and $\mathbf{1_n} = (1, 1, ..., 1)$. For $k \geq 1$ and $s \geq 0$, let $M_{k\times s}$ be the following $k \times s$ matrix

$$M_{k\times s} = \begin{pmatrix} \mathbf{0_s} \\ \vdots \\ \mathbf{0_s} \\ \mathbf{1_s} \end{pmatrix}.$$

Theorem 3.2 Let $n \geq 6$ be an integer, $n_1 = \lfloor \frac{n}{4} \rfloor$ for even n and $n_1 = \lfloor \frac{n-3}{4} \rfloor$ for odd n.

(1) If $n = 4n_1 + n_2$, $n_2 = 0$ or 2, $1 \leq i \leq n_1$, then there is an $[[n, 1, n-2i+1; n-4i+1]]$ EAQECC.
(2) If $n = 4n_1 + n_2 + 3$, $n_2 = 0$ or 2, $1 \leq i \leq n_1$, then there is an $[[n, 1, n-2i; n-4i-1]]$ EAQECC.

Proof. Let $f = (\omega, \varpi)$ and $g = (0, 1)$.
(1) For even $n = 4n_1 + n_2 \geq 6$, let $1 \leq i \leq n_1$ and $2t = n - 4i$. Construct a $2i \times n$ matrix $H_{2i\times n} = \begin{pmatrix} A_{2i\times 4i} & M_{2i\times 2t} \end{pmatrix}$ with

$$A_{2i\times 4i} = \begin{pmatrix} \mathbf{1_2} & \mathbf{1_2} & \mathbf{0_2} & \mathbf{0_2} & \cdots & \mathbf{0_2} & \mathbf{0_2} \\ \mathbf{0_2} & \mathbf{1_2} & \mathbf{1_2} & \mathbf{0_2} & \cdots & \mathbf{0_2} & \mathbf{0_2} \\ & & & \vdots & & & \\ \mathbf{0_2} & \mathbf{0_2} & \mathbf{0_2} & \mathbf{0_2} & \cdots & \mathbf{1_2} & \mathbf{1_2} \\ f & f & f & f & \cdots & f & g \end{pmatrix}.$$

Let the code generated by $H_{2i\times n}$ be $\mathcal{C}^{\perp h}$. Then $\mathcal{C}^{\perp h}$ is an $[n, 2i]_4$ code, $\mathcal{C}$ is an $[n, n-2i]_4$ code and $R(\mathcal{C})$ has dimension $2i - 1$.

Denote the j-th row of $A_{2i\times 4i}$ as β_j, $1 \leq j \leq 2i$, then each $\alpha \in \mathcal{C}^{\perp h} \setminus R(\mathcal{C})$ is of the form $\gamma(\beta, \mathbf{1_{2t}})$, where $\beta = \beta_{2i} + x_1\beta_1 + \cdots + x_{2i-1}\beta_{2i-1}$, $x_j \in \mathbf{F}_4$ for $1 \leq j \leq 2i$, $\gamma \in \mathbf{F}_4$ and $\gamma \neq 0$. Since the $(2l-1)$-th and $2l$-th entries of β_{2i} are different and the $(2l-1)$-th and $2l$-th entries of β_j are equal for $1 \leq l \leq 2i$ and $1 \leq j \leq 2i-1$, the $(2l-1)$-th and $2l$-th entries of β are different and $wt(\beta) \geq 2i$. From $(\beta, \beta)_h = 1$, one can derive that $wt(\beta)$ is odd, which implies $wt(\beta) \geq 2i+1$ and $wt((\beta, \mathbf{1_{2t}})) \geq n - 2i + 1$. Thus, we have shown that $d_{ea} = min\{wt(\alpha) \in \mathcal{C}^{\perp h} \setminus R(\mathcal{C})\} \geq n - 2i + 1$. According to Lemma 3.1, we can obtain an $[[n, 1, n-2i+1; n-4i+1]]$ MDS EAQECC.

(2) For $n = 7, 9$, we construct a $3 \times n$ matrix $H_{3\times n} = \begin{pmatrix} A_{3\times 5} & M_{3\times(n-5)} \end{pmatrix}$ with

$$A_{3\times 5} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & \omega & \varpi & 1 \\ 0 & \omega & 1 & \varpi & 0 \end{pmatrix}.$$

Suppose $H_{3\times n}$ generates the code $\mathcal{C}^{\perp h}$. Then $\mathcal{C}^{\perp h}$ is an $[n, 3]_4$ code, $\mathcal{C}$ is an $[n, n-3]_4$ code and $R(\mathcal{C})$ has dimension $r = 2$. It is easy to check that $d_{ea} = n - 2$, hence there is an $[[n, 1, n-2; n-5]]$ MDS EAQECC.

For $n = 4n_1 + n_2 + 3 \geq 11$, $n_2 = 0$ or $n_2 = 2$, then $n_1 \geq 2$. Let $1 \leq i \leq n_1$ and $2t + 1 = n - 4i - 2$. We construct $H_{(2i+1)\times n} = \begin{pmatrix} A_{(2i+1)\times(4i+2)} & M_{(2i+1)\times(2t+1)} \end{pmatrix}$ with

$$A_{(2i+1)\times(4i+2)} = \begin{pmatrix} \mathbf{1_2} & \mathbf{1_2} & \mathbf{0_2} & \cdots & \mathbf{0_2} & \mathbf{0_2} \\ \mathbf{0_2} & \mathbf{1_2} & \mathbf{1_2} & \cdots & \mathbf{0_2} & \mathbf{0_2} \\ & & & \vdots & & \\ \mathbf{0_2} & \mathbf{0_2} & \mathbf{0_2} & \cdots & \mathbf{1_2} & \mathbf{1_2} \\ f & f & f & \cdots & f & f \end{pmatrix}.$$

Suppose $H_{(2i+1)\times n}$ generates the code $\mathcal{C}^{\perp h}$. Then $\mathcal{C}^{\perp h}$ is an $[n, 2i+1]_4$ code, $\mathcal{C}$ is an $[n, n-(2i+1)]_4$ code and $R(\mathcal{C})$ has dimension $2i$. Similar to the discussion of case (1), it is easy to check that $d_{ea} = n - 2i$, and there is an $[[n, 1, n-2i; n-4i-1]]$ MDS EAQECC.

Summarizing the above discussions, the theorem holds □.

To the best of our knowledge, there is no known degenerate standard QECC that violates the quantum Hamming bound [35, 36]. However, many of the EAQECCs constructed in Theorem 3.2 violate the EA-quantum Hamming bound.

Theorem 3.3 There exist infinitely many degenerate MDS EAQECCs violating the EA-quantum Hamming bound.

Proof. Let $m \geq 2$, we now show the $[[4m, 1, 2m+1; 1]] = [[n, 1, d_{ea}; 1]]$ EAQECCs given in Theorem 3.2 violating the EA-quantum Hamming bound.

Denote $f(t) = \binom{4t}{t}$. It is easy to check $f(3) > (\frac{16}{3})^3$ and $f(t+1)/f(t) > \frac{16}{3}$ for $t \geq 3$, which imply $f(t) > (\frac{16}{3})^t$ and $3^t f(t) > 16^t = 2^{4t}$. Thus, for $m \geq 3$, one can deduce

$$\sum_{i=0}^{m} 3^i \binom{n}{i} > 3^m \binom{4m}{m} > 2^{4m} = 2^{n+c-k}.$$

From $1 + 3\binom{8}{1} + 3^2\binom{8}{2} > 2^8$ and the previous discussion for $m \geq 3$, we have proved that all the EAQECCs $[[4m, 1, 2m+1; 1]]$ (for $m \geq 2$) given in Theorem 3.2 violate the EA-quantum Hamming bound. This proves Theorem 3.3 □.

Similarly, one can check the EAQECCs of parameters $[[4m+3, 1, 2m+3; 2]]$ for $m \geq 2$, $[[4m+2, 1, 2m+3; 3]]$ for $m \geq 3$ and $[[4m+1, 1, 2m+3; 4]]$ for $m \geq 3$, given in Theorem 3.2, also violate the EA-quantum Hamming bound. These results show the EA-quantum Hamming bound does not hold asymptotically for degenerate EAQECCs, whereas the quantum Hamming bound for standard QECCs holds asymptotically [11].

4 Discussion and conclusion

We have shown that there exist infinitely many degenerate EAQECCs violating the EA-quantum Hamming bound, and this fact implies the EA-quantum Hamming bound does not hold asymptotically for degenerate EAQECCs. This is the first illustration of degenerate EAQECCs pack more efficiently than their nondegenerate counterparts. The EAQECCs we constructed also illustrate the following noteworthy facts.

(1) Entanglement can greatly increase the minimum distance of quantum codes (for further evidences, please see [26]). The $[[4m, 1, 2m+1; 1]] = [[n, 1, d_{ea}; 1]]$ code, consuming one ebit, has minimum distance $d_{ea} = 2m+1$ and can correct $m = \lfloor \frac{n}{4} \rfloor$ errors. On the other hand, a binary QECC of length $n+1$ can correct no more than $\lfloor \frac{n+2}{6} \rfloor \leq \frac{2m+1}{3}$ errors and has minimum distance $d \leq \frac{4m+2}{3} + 1$ [12]. Generally, for $c \geq 1$, our $[[n, 1, d_{ea}; c]]$ EAQECC has minimum distance $d_{ea} = \frac{n+c+1}{2}$, while a binary QECC of length $n+c$ is of minimum distance $d_{n+c} \leq \frac{n+c+1}{3} + 1$, hence $d_{ea} - d_{n+c} \geq \frac{n+c+1}{6} - 1$.

(2) Our results imply that some optimal EAQECCs can be constructed from "poor" classical codes; the current idea (given in [17]) of constructing good EAQECCs from good classical codes may be an illusion in some case. The reasons are as follows: The classical codes $\mathcal{C}$ and $\mathcal{C}^{\perp h}$ we used for constructing MDS EAQECCs are "poor" codes whose distance can not exceed 4, and are not MDS classical codes. For MDS standard quantum codes, the underlying classical codes are required to be MDS codes [15]. Recently, in [45], it is proved that: For given $k \geq 2$, there are infinite families of n and c, such that an optimal $[[n, k, d_{ea}; c]]$ EAQEC

code must be degenerate. Ref.[45] also showed that a degenerate $[[49, 2, 38; 45]]$ EAQECC exists and is optimal, this EAQECC is constructed from classical codes $\mathcal{C}$ with $\mathcal{C} = [49, 46, 2]_4$ and $\mathcal{C}^{\perp h} = [49, 3, 4]_4$. But a nondegenerate $[[49, 2, d; 45]]$ EAQECC must have $d \leq 37$, and a $[[49, 2, d; 45]]$ EAQEC code constructed from an optimal quaternary linear code, by the method of [17], must have $d \leq 36$. All these evidences show that EAQECCs have some properties different from that of classical codes and standard QECCs.

(3) Our results also show that entanglement seems to allow codes saturating the EA-quantum Singleton bound for a much broader set of parameters. It is known that there are only two nontrivial binary QECCs (codes with distance $d \geq 3$), $[[5, 1, 3]]$ and $[[6, 0, 4]]$ achieving the quantum Singleton bound, and finite nontrivial binary and quaternary classical codes achieving the Singleton bound [9, 15]. Whereas for EAQECCs, for each $n \geq 3$, there is at least one $[[n, k, d_{ea}; c]]$ EAQECC achieving the EA-quantum Singleton bound. Enlarging the parameter space of MDS EAQECCs maybe playing a role in quantum information processing. This problem deserves further study.

Acknowledgments

We are indebted to the anonymous reviewers for constructive comments and suggestions on our manuscript, which improve the manuscript significantly. This work is supported by National Natural Science Foundations of China under Grant No.11071255 and 61075054.

References

1. P. W. Shor (1995), *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev.A, **52**, pp. R2493-2496.
2. A. M. Steane (1996), *Error correcting codes in quantum theory*, Phys. Rev. Lett., **77**, pp. 793-797.
3. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters (1996), *Mixed state entanglement and quantum error correction,* Phys. Rev. A, **54**, pp. 3824-3851.
4. M. A. Nielsen and I. L. Chuang (2000), *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, England.
5. F. Gaintan (2008), *Quantum Error Correction and Fault Tolerant Quantum Computation*. CRC Press, Taylor & Francis Group.
6. D. Gottesman (1996), *Class of quantum error-correcting codes saturating the quantum Hamming bound,* Phys. Rev. A, **54**, pp. 1862-1868.
7. D. Gottesman (1997), *Stabilizer codes and quantum error correction*, Ph.D. Thesis, California Institute of Technology. quant-ph/9707027.
8. E. Knill and R. Laflamme (1997), *A theory of quantum error correcting codes*, Phys. Rev. A, **55**, pp. 900-911.
9. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane (1998), *Quantum error-correction via codes over GF(4)*, IEEE. Trans. Inf. Theory, **44**, pp. 1369-1387.
10. A. M. Steane (1999), *Enlargement of Calderbank-Shor-Steane quantum codes,* IEEE Trans. Inf. Theory, **45**, pp. 2492-2495.
11. A. Ashikhmin and S. Litsn (1999), *Upper bounds on the size of quantum codes,* IEEE Trans.Inf. Theory, **45**, pp. 1206-1215.
12. E. M. Rains (1999), *Quantum shadow enumerators,* IEEE. Trans. Inf. Theory, **45**, pp. 2361-2366.
13. E. M. Rains (1999), *Nonbinary quantum code*, IEEE. Trans. Inf. Theory, **45**, pp. 1827-1832.
14. A. Ashikhim and E. Knill (2001), *Nonbinary quantum stabilizer codes*, IEEE. Trans. Inf. Theory, **47**, pp. 3065-3072.
15. A. Ketkar, A. Klappenecker and S. Kumar (2006), *Nonbinary stablizer codes over finite fields*, IEEE. Trans. Inf. Theory, **52**, pp. 4892-4914.

16. M. Hamada (2008), *Concatenated quantum codes constructible in polynomial time: efficient decoding and error correction*, IEEE. Trans. Inf. Theory, **54**, pp. 5689-5704.
17. T. Brun, I. Devetak, and M. H. Hsieh (2006), *Correcting quantum errors with entanglement,* Science **314**, pp. 436-439.
18. G. Bowen (2002), *Entanglement required in achieving entanglement-assisted channel capacities,* Phys. Rev. A, **66**, 052313.
19. M. H. Hsieh, I. Devetak, and T. Brun (2007), *General entanglement-assisted quantum error-correcting codes,* Phys. Rev. A, **76**, 062313.
20. M. H. Hsieh (2008), *Entanglement-assisted quantum coding theory,* arXiv:0807.2080v2.
21. M. H. Hsieh, T. A. Brun and I. Devetak (2009), *Entanglement-assisted quantum quasicyclic low-density parity-check codes,* Phys. Rev. A, **79**, 032340.
22. Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, and V. D. Tonchev (2010), *Entanglement-assisted quantum low-density parity-check codes,* Phys. Rev. A, **82**, 042338.
23. M. M. Wilde (2008), *Quantum coding with entanglement,* arXiv:0806.4212.
24. M. M. Wilde and T. A. Brun (2008), *Optimal entanglement formulas for entanglement-assisted quantum coding,* Phys. Rev. A, **77**, 064302.
25. R. Li (2010), *Introduction to entanglement-assisted quantum coding theory,* preprint.
26. C. Y. Lai and T. A. Brun (2013), *Entanglement increases the error-correcting ability of quantum error-correcting codes,* Phys. Rev. A, **88**, 012320. See also arXiv:1008.2598v1.
27. C. Y. Lai, T. A. Brun and M. M. Wilde (2011), *Dualities and Identities for Entanglement-Assisted Quantum Codes,* arXiv:1010.5506v2.
28. M. H. Hsieh, W. T. Yen, and L. Y. Hsu (2011), *High performance entanglement-assisted quantum LDPC codes need little entanglement,* IEEE Trans. Inf. Theory, **57**, pp. 1761-1769.
29. Y. Dong, X. Deng, M. Jiang, Q. Chen, S. Yu (2009), *Entanglement-enhanced quantum error-correcting codes,* Phys. Rev. A., **79**, 042342.
30. D. Cao and Y. Song (2013), *Novel class of entanglement-assisted quantum codes with minimal ebits,* J. Commun. Netw., **15**, pp. 217-221.
31. Y. Fujiwara, V. D. Tonchev (2013), *A characterization of entanglement-assisted quantum low-density parity-check codes,* IEEE Trans. Inf. Theory, **59**, pp. 3347-3353.
32. J. Shin, J. Heo, T. A. Brun (2013), *General quantum error-correcting code with entanglement based on code-word stabilized quantum code,* arXiv:1311.1533.
33. B. Shaw, M. M. Wilde, O. Oreshkov, I. Kremsky and D. A. Lidar (2008), *Encoding one logical qubit into six physical qubits,* Phys. Rev. A, **78**, 012337.
34. Y. Fujiwara (2013), *Quantum error correction via less noisy qubits,* Phys. Rev. Lett., **110**,170501.
35. Z. Li and L. Xing (2010), *On a problem concerning the quantum Hamming bound for impure quantum codes,* IEEE. Trans. Inf. Theory, **56**, pp. 4731-4734.
36. P. Sarvepalli and A. Klappenecker (2010), *Degenerate quantum codes and the quantum Hamming bound,* Phys. Rev. A, **81**, 032318.
37. A. Klappenecker and P. Sarvepalli (2007), *On subsystem codes beating the quantum Hamming or Singleton bound,* Proc. R. Soc. A, **463**, pp. 2887-2905.
38. P. W. Shor and J. A. Smolin (1996), *Quantum error-correcting codes need not completely reveal the error syndrome,* arXiv: 9604006v2.
39. N. J. Cerf (2000), *Pauli cloning of a quantum bit,* Phys. Rev. Lett., **84**, pp. 4497-4500.
40. D. P. DiVincenzo, P. W. Shor and J. A. Smolin (1996), *Quantum-channel capacity of very noisy channels,* Phys. Rev. A, **57**, pp. 830-839.
41. G. Smith and J. A. Smolin (2007), *Degenerate quantum codes for Pauli channels,* Phys. Rev. Lett., **98**, 030501.
42. K. H. Ho and H. F. Chau (2008), *Purifying Greenberger-Horne-Zeilinger states using degenerate quantum codes,* Phys. Rev. A, **78**, 042329.
43. P. W. Shor and J. Preskill (2000), *Simple proof of security of the BB84 quantum key distribution protocol,* Phys. Rev. Lett., **85**, pp. 441-444.
44. Z. Wan (1993), *Geometry of Classical Groups over Finite Fields.* Chart Well Bratt, Lund, Sweden.

45. L. Guo and R. Li (2013), *Linear Plotkin bound for entanglement-assisted quantum codes,* Phys. Rev. A, **87**, 032309.
46. W. C. Huffman (2005), *On the classification and enumeration of self-dual codes,* Finite Fields Appl., **11**, pp. 451-490.
47. C. Y. Lai, T. A. Brun, and M. M. Wilde (2013), *Duality in Entanglement-assisted quantum error correction*, IEEE Trans Inf. Theory, **49**, pp. 4020-4024.