PNAS RESEARCH ARTICLE | ENGINEERING

Entanglement-assisted concatenated quantum codes

Jihao Fan[a], Jun Li[b,1], Yongbin Zhou[a], Min-Hsiu Hsieh[c], and H. Vincent Poor[d,1]

Contributed by H. Vincent Poor; received February 7, 2022; accepted April 19, 2022; reviewed by Todd Brun and Robert Malaney

Entanglement-assisted concatenated quantum codes (EACQCs), constructed by concatenating two quantum codes, are proposed. These EACQCs show significant advantages over standard concatenated quantum codes (CQCs). First, we prove that, unlike standard CQCs, EACQCs can beat the nondegenerate Hamming bound for entanglement-assisted quantum error-correction codes (EAQECCs). Second, we construct families of EACQCs with parameters better than the best-known standard quantum error-correction codes (QECCs) and EAQECCs. Moreover, these EACQCs require very few Einstein–Podolsky–Rosen (EPR) pairs to begin with. Finally, it is shown that EACQCs make entanglement-assisted quantum communication possible, even if the ebits are noisy. Furthermore, EACQCs can outperform CQCs in entanglement fidelity over depolarizing channels if the ebits are less noisy than the qubits. We show that the error-probability threshold of EACQCs is larger than that of CQCs when the error rate of ebits is sufficiently lower than that of qubits. Specifically, we derive a high threshold of 47% when the error probability of the preshared entanglement is 1% to that of qubits.

entanglement-assisted quantum error-correction code | error-correction code | concatenated quantum code | quantum Hamming bound | entanglement fidelity

Significance

Code concatenation that uses two or more short component codes is a significant method for designing powerful codes. Concatenated classical codes are not only asymptotically good in theory, but also have been widely used in practice. However, construction of concatenated quantum codes (CQCs) suffers severe orthogonality constraints. We introduce entanglement to concatenated codes and propose entanglement-assisted CQCs (EACQCs). The enhanced performance of EACQCs under noisy ebit conditions demonstrates considerable advantages in both quantum communication and quantum computation. Among them, we show that EACQCs can beat the best-known quantum codes, either standard or entanglement-assisted. Moreover, we derive a high threshold of 47% when the error probability of ebits is 1% to that of qubits.

Quantum error-correction codes (QECCs) are necessary to realize quantum communications and to make fault-tolerant quantum computers (1, 2). The stabilizer formalism provides a useful way to construct QECCs from classical codes, but certain orthogonality constraints are required (3). The entanglement-assisted (EA) QECC (EAQECC) (4–6) generalizes the stabilizer code. By presharing some entangled states between the sender (Alice) and the receiver (Bob), EAQECCs can be constructed from any classical linear codes without the orthogonality constraints. Therefore, the construction could be greatly simplified. As an important physical resource, entanglement can boost the classical information capacity of quantum channels (7–12). Recently, it has been shown that EAQECCs can violate the nondegenerate quantum Hamming bound (13) or the quantum Singleton bound (14).

Compared to standard QECCs, EAQECCs must establish some amount of entanglement before transmission. This preshared entanglement is the price to be paid for enhanced communication capability. In a sense, we need to consider the net transmission of EAQECCs—i.e., the number of qubits transmitted minus that of ebits preshared. Further, it is difficult to preserve too many noiseless ebits in EAQECCs at present. Thus, we have to use as few ebits as possible to conduct the communication—e.g., one or two ebits are preferable (15–18). In addition, EAQECCs with positive net transmission and little entanglement can lead to catalytic quantum codes (4, 6), which are applicable to fault-tolerant quantum computation (FTQC). In ref. 4, a table of best-known EAQECCs of length up to 10 was established through computer search or algebraic methods. Several EAQECCs in ref. 4 have larger minimum distances than the best-known standard QECCs of the same length and net transmission. However, for larger code lengths, the efficient construction of EAQECCs with better parameters than standard QECCs is still unknown.

In classical coding theory, concatenated codes (CCs), originally proposed by Forney in the 1960s (19), provide a useful way of constructing long codes from short ones. CCs can achieve very large coding gains with reasonable encoding and decoding complexity (20). Moreover, CCs can have large minimum distances since the distances of the component codes are multiplied. As a result, CCs have been widely used in many digital communication systems—e.g., the NASA standard for the Voyager program (21) and the compact disc (20). Similarly, in QECCs, the concatenated quantum codes (CQCs), introduced by Knill and Laflamme in 1996 (22), are also effective for constructing good quantum codes. In particular, it has been shown that CQCs are of great importance in realizing FTQC (23–25).

Moreover, there exists a specific phenomenon in QECCs, called "error degeneracy," which distinguishes quantum codes from classical ones in essence. It is widely believed that degenerate codes can correct more quantum errors than nondegenerate ones. Indeed,

Author contributions: J.F., J.L., Y.Z., M.-H.H., and H.V.P. designed research; J.F., J.L., M.-H.H., and H.V.P. performed research; J.F. and M.H.H. contributed new reagents/analytic tools; J.F. and M.-H.H. analyzed data; and J.F., J.L., Y.Z., M.-H.H., and H.V.P. wrote the paper.

Reviewers: T.B., University of Southern California Viterbi School of Engineering; and R.M., University of New South Wales.

The authors declare no competing interest.

[1]To whom correspondence may be addressed. Email: jun.li@njust.edu.cn or poor@princeton.edu.

This article contains supporting information online at https://www.pnas.org/lookup/suppl/doi:10.1073/pnas.2202235119/-/DCSupplemental.

Published June 10, 2022.

there are some open problems concerning whether degenerate codes can violate the nondegenerate quantum Hamming bound (26) or can improve the quantum-channel capacity (27, 28). Many CQCs have been shown to be degenerate, even if the component codes are nondegenerate—e.g., Shor's $[[9,1,3]]$ code and the $[[25,1,9]]$ CQC (23, 29). If we introduce extra entanglement to CQCs, it is possible to improve the error-degeneracy performance of CQCs.

In this article, we generalize the idea of concatenation to EAQECCs and propose EACQCs. We show that EACQCs can beat the nondegenerate quantum Hamming bound, while standard CQCs cannot. Several families of degenerate EACQCs that can surpass the nondegenerate Hamming bound for EAQECCs are constructed. The same conclusion could be reached for asymmetric error models, in which the phase-flip errors (Z errors) happen more frequently than the bit-flip errors (X errors) (30, 31). Furthermore, we derive a number of EACQCs with better parameters than the best-known QECCs and EAQECCs. In particular, we see that many EACQCs have positive net transmission, and each of them consumes only one or two ebits. Thus, they give rise to catalytic EACQCs with little entanglement and better parameters than the best-known QECCs. Further, we show that the EACQC scheme makes EA quantum communication possible, even if the ebits are noisy. We compute the entanglement fidelity (EF) of the [[15,1,9;10]] EACQC by using Bowen's [[3,1,3;2]] EAQECC (32) or the [[3,1,3;2]] EA repetition code (4, 6) as the inner code. The outer code is the standard [[5,1,3]] stabilizer code. We show that the [[15,1,9;10]] EACQC performs much better than the [[25,1,9]] CQC over depolarizing channels if the ebits suffer a lower error rate than the qubits. Moreover, we compute the error-probability threshold of EACQCs, and we show that EACQCs have much higher thresholds than CQCs when the error rate of ebits is sufficiently lower than that of qubits.

EA Stabilizer Formalism

Let $q=2^m$ ($m\geq 1$ is an integer) and denote by $GF(q)$ the extension field of the binary field $GF(2)$. Let $\mathbb{C}$ be the field of complex numbers, and let $V_n=(\mathbb{C}^q)^{\otimes n}=\mathbb{C}^{q^n}$ be the q^n-dimensional Hilbert space, where n is a positive integer. Define two error operators on $\mathbb{C}^q$ by $X(a)|x\rangle=|a+x\rangle$ and $Z(b)|x\rangle=(-1)^{tr(bx)}|x\rangle$, where $a,b,x\in GF(q)$, and "tr" denotes the trace operator from $GF(q)$ to $GF(2)$. For a vector $\mathbf{u}=(u_1,\cdots,u_n)\in GF(q)^n$, denote by $X(\mathbf{u})=X(u_1)\otimes\cdots\otimes X(u_n)$ and $Z(\mathbf{u})=Z(u_1)\otimes\cdots\otimes Z(u_n)$. Let $\Xi_n=\{X(\mathbf{a})Z(\mathbf{b})|\mathbf{a},\mathbf{b}\in GF(q)^n\}$ and let $\mathcal{G}_n=\{(-1)^uX(\mathbf{a})Z(\mathbf{b})|\mathbf{a},\mathbf{b}\in GF(q)^n,u\in GF(2)\}$ be the group generated by Ξ_n. For the operator $e=(-1)^uX(\mathbf{a})Z(\mathbf{b})\in\mathcal{G}_n$, the weight of e is defined by $\mathrm{wt}_Q(e)=|\{1\leq i\leq n:(a_i,b_i)\neq(0,0)\}|$. The definition of quantum stabilizer codes is given below.

Definition 1: A stabilizer code Q is a q^k -dimensional ($k\geq 0$) subspace of V_n such that $Q=\bigcap_{e\in T}\{|\phi\rangle\in V_n:e|\phi\rangle=|\phi\rangle\}$, where T is a subgroup of $\mathcal{G}_n$. $Q=[[n,k,d]]_q$ has minimum distance d if it can detect all errors $e\in\mathcal{G}_n$ of weight $\mathrm{wt}_Q(e)$ up to $d-1$. Further, Q is called nondegenerate if every stabilizer in T has weight larger than or equal to d; otherwise, it is called degenerate.

A CQC is derived from an inner code and an outer code. In general, the component codes of CQCs can be chosen as stabilizer codes or nonstabilizer codes. In this article, it suffices to consider only the case of stabilizer codes. Let the inner and outer codes be $Q_I=[[n_1,k_1,d_1]]$ and $Q_O=[[n_2,k_2,d_2]]_{2^{k_1}}$, respectively. Then, we can derive a CQC (33) with parameters $Q_C=[[n_1n_2,k_1k_2,d_C\geq d_1d_2]]$.

An EAQECC with parameters $Q_e=[[n,k,d;c]]_q$ can encode k qudits into n qudits by consuming c pairs of maximally entangled states between Alice and Bob. It should be noted that EAQECCs can be constructed from arbitrary classical linear codes directly. The Calderbank–Shor–Steane framework (3, 34) provides a useful way to construct both QECCs and EAQECCs from classical linear codes.

Lemma 1 (4)**.** *Let $C_1=[n,k_1,d_1]_q$ and $C_2=[n,k_2,d_2]_q$ be two linear codes over $GF(q)$. Denote the parity-check matrices of C_1 and C_2 by H_1 and H_2, respectively. There exists an EAQECC with parameters $Q_e=[[n,k_1+k_2-n+c,d_e\geq\min\{d_1,d_2\};c]]_q$, where $c=rank(H_1H_2^T)$, and H_2^T is the transpose of H_2.*

EAQECCs can also be constructed by using the Hermitian construction (3, 4, 35) as follows.

Lemma 2 (4)**.** *Let $C=[n,k,d]_{q^2}$ be a linear code over $GF(q^2)$. Denote the parity-check matrix of C by H. There exists an EAQECC with parameters $Q_e=[[n,2k-n+c,d_e\geq d;c]]_q$, where $c=rank(HH^\dagger)$, and $H^\dagger$ is the conjugate transpose of H over $GF(q^2)$.*

Results

We organize the main results of our study in the following order. First, we present the construction of EACQCs from two component quantum codes. Second, we construct several families of EACQCs violating the nondegenerate Hamming bound for EAQECCs. Third, we derive a number of EACQCs with better parameters than the best-known QECCs and EAQECCs. Finally, we show that EACQCs can correct errors in the ebits. It is shown that EACQCs can outperform CQCs in EF and have higher error-probability thresholds than CQCs.

EACQCs. We generalize CQCs to EACQCs by concatenating two quantum codes, which can be chosen as either standard QECCs or EAQECCs. In this article, sometimes we represent an $[[n,k,d]]_q$ QECC as an $[[n,k,d;0]]_q$ EAQECC so that we can unify the representation of QECCs and EAQECCs. Let the inner code be $Q_I=[[n_1,k_1,d_1;c_1]]$, which requires c_1 ebits. Denote by $k_1^*\equiv k_1-c_1$ the net transmission of Q_I. Let the outer code be $Q_O=[[n_2,k_2,d_2;c_2]]_{2^{k_1}}$, which can either be binary or nonbinary depending on k_1. Q_O uses c_2 edits, or, equivalently, c_2k_1 ebits. Denote by $k_2^*\equiv k_2-c_2$ the net transmission of Q_O. Notice that, for classical linear codes and quantum codes over the binary field $GF(2)$, we usually neglect the index in the code parameters if there is no ambiguity.

We prove the following result about EACQCs.

Theorem 1. *Let $Q_I=[[n_1,k_1,d_1;c_1]]$ be the inner code, and let $Q_O=[[n_2,k_2,d_2;c_2]]_{2^{k_1}}$ be the outer code. There exists an EACQC $\mathcal{Q}_e$ with parameters*

$$\mathcal{Q}_e=[[n_1n_2,k_1k_2,d_e\geq d_1d_2;c_e]], \qquad [1]$$

where $c_e=c_1n_2+c_2k_1$ is the number of ebits. The net transmission is $k_e^*=k_1k_2-c_e$.

Proof: Based on the idea of code concatenation, we simply concatenate the inner code Q_I with the outer code Q_O to derive the EACQC (19, 22, 33). First, we encode the information state $|\mu\rangle$ by using the outer code Q_O, i.e.,

$$\begin{aligned}|\mu\rangle&\mapsto|\psi\rangle_O\\&=(U_O\otimes\widehat{I}_{B_O})|\mu\rangle\otimes|0\rangle^{\otimes(n_2-k_2-c_2)k_1}\otimes|\Psi_+\rangle_{AB}^{\otimes c_2k_1},\end{aligned} \qquad [2]$$

where there are c_2k_1 Einstein–Podolsky–Rosen (EPR) pairs, $|\Psi_+\rangle_{AB}^{\otimes c_2k_1}$, preshared between Alice and Bob during the outer encoding, and $\widehat{I}_{B_O}$ is the identity operator on Bob's halves of ebits during the outer encoding. The outer encoding operation U_O is applied to the qubits on Alice's side.

Suppose that we can represent $|\psi\rangle_O$ by

$$|\psi\rangle_O = \sum_{\nu_1,\cdots,\nu_{n_2}=0}^{2^{k_1}} \ell_{\nu_1\cdots\nu_{n_2}} |\nu_1\cdots\nu_{n_2}\rangle, \quad [3]$$

where $\ell_{\nu_1\cdots\nu_{n_2}} (0 \le \nu_1, \cdots, \nu_{n_2} \le 2^{k_1})$ should satisfy the normalization condition. We separate each basis state $|\nu_1\cdots\nu_{n_2}\rangle$ in $|\psi\rangle_O$ into n_2 subblocks, i.e., $|\nu_1\cdots\nu_{n_2}\rangle = |\nu_1\rangle\cdots|\nu_{n_2}\rangle$ for $0 \le \nu_1, \cdots, \nu_{n_2} \le 2^{k_1}$. For each subblock $|\nu_i\rangle (1 \le i \le n_2)$, we do the inner encoding as follows:

$$|\nu_i\rangle \mapsto |\psi_i\rangle_I = (U_I \otimes \widehat{I}_{B_I})|\nu_i\rangle \otimes |0\rangle^{\otimes n_1-k_1-c_1} \otimes |\Phi_+\rangle_{AB}^{\otimes c_1}, \quad [4]$$

where $|\Phi_+\rangle_{AB}^{\otimes c_1}$ are c_1 EPR pairs preshared between Alice and Bob during each inner encoding. The encoding operation $U_I \otimes \widehat{I}_{B_I}$ is applied to the qubits in Alice's side, while Bob's halves of ebits do not need to be encoded during each inner encoding. It is easy to see that the number of ebits used during the whole inner encoding is c_1n_2. The encoding process of EACQCs is given in Fig. 1.

The numbers of ebits used during the outer and the inner encoding are equal to c_2k_1 and c_1n_2, respectively. Therefore, the total number of ebits is equal to $c_e = c_1n_2 + c_2k_1$. It is easy to see that the dimension of the EACQC $\mathscr{Q}_e$ is equal to $2^{k_1k_2}$. Similar to the principle of code concatenation in refs. 19, 22, and 33, the minimum distance of $\mathscr{Q}_e$ is at least d_1d_2. Therefore, we can obtain an EAQECC with parameters $\mathscr{Q}_e = [[n_1n_2, k_1k_2, d_e \ge d_1d_2; c_e]]$. □

It is easy to see that if the inner and outer codes are both standard QECCs, then the EACQC is a standard CQC. Moreover, we can use different inner codes in EACQCs. Let $Q_{I_i} = [[n_{I_i}, k_{I_i}, d_{I_i}; c_{I_i}]]$ $(1 \le i \le n_2)$ be n_2 inner codes. For simplicity, we let $k_1 \equiv k_{I_1} = \ldots = k_{I_{n_2}}$, and let $d_1 \equiv d_{I_1} = \ldots = d_{I_{n_2}}$. Let the outer code be $Q_O = [[n_2, k_2, d_2; c_2]]_{2^{k_1}}$. Then, we can derive an EACQC with parameters

$$\mathscr{Q}'_e = [[\sum_{i=1}^{n_2} n_{I_i}, k_1k_2, d'_e \ge d_1d_2; c'_e]], \quad [5]$$

where $c'_e = \sum_{i=1}^{n_2} c_{I_i} + c_2k_1$. The net transmission is $k_1k_2 - c'_e$.

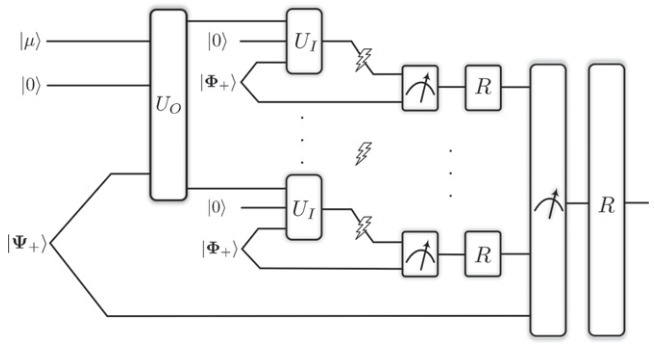

Fig. 1. The encoding circuit of EACQCs. The information state $|\mu\rangle$ is first encoded with the outer encoder U_O by presharing c_2k_1 EPR pairs $|\Psi_+\rangle = |\Psi_+\rangle_{AB}^{\otimes c_2k_1}$ between Alice and Bob. For the output of U_O, each subblock is encoded with the inner encoder U_I by presharing c_1 EPR pairs $|\Phi_+\rangle = |\Phi_+\rangle_{AB}^{\otimes c_1}$ between Alice and Bob.

EACQCs Beating the Nondegenerate Quantum Hamming Bound. First, let us review the nondegenerate Hamming bound for EAQECCs (36).

Lemma 3 (36). *For a binary nondegenerate $Q_e = [[n, k, d; c]]$ EAQECC, it must satisfy*

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} 3^i \binom{n}{i} \le 2^{n+c-k}. \quad [6]$$

Taking the limit as $n \to \infty$, this yields the asymptotic bound on the rate k/n:

$$\frac{k}{n} \le 1 + \frac{c}{n} - \frac{\delta}{2}\log_2 3 - H_2\left(\frac{\delta}{2}\right), \quad [7]$$

where $\delta = d/n$, and $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function.

To the best of our knowledge, no degenerate CQCs have been discovered that violate the nondegenerate quantum Hamming bound (36). However, the situation is quite different in the EA case. We can easily construct several families of degenerate EACQCs that violate the Hamming bound in Lemma 3. We summarize these EACQCs as follows.

Theorem 2. *There exist the following four families of EACQCs with parameters*

① $\mathscr{Q}_{e_1} = [[5n_2, 1, d_{e_1} \ge 3n_2; n_2 - 1]]$, *where* $n_2 \ge 3$ *is odd.*
② $\widetilde{\mathscr{Q}}_{e_1} = [[5n_2, 1, \widetilde{d}_{e_1} \ge 3n_2 - 3; n_2 - 1]]$, *where* $n_2 \ge 10$ *is even.*
③ $\mathscr{Q}_{e_2} = [[4n_2, 1, d_{e_2} \ge 3n_2; 2n_2 - 1]]$, *where* $n_2 \ge 11$ *is odd.*
④ $\widetilde{\mathscr{Q}}_{e_2} = [[4n_2, 1, \widetilde{d}_{e_2} \ge 3n_2 - 3; 2n_2 - 1]]$, *where* $n_2 \ge 32$ *is even.*

EACQCs in ① − ④ can beat the nondegenerate quantum Hamming bound for EAQECCs.

Proof: The proof is given in *SI Appendix*, section 1. □

We give an explicit example to illustrate the construction of EACQCs. Let $Q_I = [[5, 1, 3; 0]]$ be the inner code, and let $Q_O = [[3, 1, 3; 2]]$ be the outer code in ref. 4. Then, we can derive an EACQC with parameters $\mathscr{Q}_e = [[15, 1, 9; 2]]$ by Theorem 1. This code can beat the nondegenerate Hamming bound for EAQECCs in Eq. **6**. Notice that $Q_I = [[5, 1, 3; 0]]$ and $Q_O = [[3, 1, 3; 2]$ are both nondegenerate codes (3, 4), while $\mathscr{Q}_e = [[15, 1, 9; 2]]$ is degenerate. Also notice that Q_I and Q_O cannot beat the nondegenerate Hamming bound in Eq. **6**, but their EACQC $\mathscr{Q}_e = [[15, 1, 9; 2]]$ can do so. If we encode one of the qubits of the outer encoding by using the $[[4, 1, 3; 1]]$ EAQECC, then we derive a $[[14, 1, 9; 3]]$ EACQC. This code can also beat the nondegenerate Hamming bound for EAQECCs.

For asymmetric channel models, we present a construction of EACQCs that can beat the nondegenerate Hamming bound for asymmetric EAQECCs. Let d_X and d_Z be two positive integers. From ref. 37, an asymmetric EAQECC $Q_A = [[n, k, d_Z/d_X; c]]_q$ can detect any X error of weight up to $d_X - 1$ and any Z error of weight up to $d_Z - 1$ simultaneously. The number of edits is c. One can further obtain nondegenerate Hamming bounds for asymmetric EAQECCs (36, 37).

Lemma 4 (37). *A binary nondegenerate asymmetric EAQECC* $[[n, k, d_Z/d_X; c]]$ *must satisfy*

$$\sum_{i=0}^{\lfloor \frac{d_X-1}{2} \rfloor} \binom{n}{i} \sum_{j=0}^{\lfloor \frac{d_Z-1}{2} \rfloor} \binom{n}{j} \leq 2^{n+c-k}. \quad [8]$$

Let $Q_I = [[n_1, 1, n_1/1; 0]]$ be a binary asymmetric EAQECC derived from the $[n_1, 1, n_1]$ repetition code, where $n_1 \geq 2$ is an integer. We use Q_I as the inner code. Let $Q_O = [[n_2, 1, d_2/d_2; n_2 - 1]]$ be the outer code, where $d_2 = n_2 - 1$ for even $n_2 \geq 2$, or $d_2 = n_2$ for odd $n_2 \geq 3$. We concatenate Q_I with Q_O according to Fig. 1. Then, we have the following result about asymmetric EACQCs.

Corollary 1. *There exists a family of asymmetric EACQCs with parameters*

$$\mathcal{Q}_A = [[n_1 n_2, 1, n_1 d_2/d_2; n_2 - 1]], \quad [9]$$

where $n_1 \geq 2$ *is an integer,* $d_2 = n_2 - 1$ *for even* $n_2 \geq 2$, *or* $d_2 = n_2$ *for odd* $n_2 \geq 3$.

For any integer $n_1 \geq 2$ and any odd $n_2 \geq 3$, $\mathcal{Q}_A$ in Corollary 1 can beat the nondegenerate Hamming bound for asymmetric EAQECCs in Lemma 4. For any integer $n_1 \geq 2$ and any even $n_2 \geq 8$, $\mathcal{Q}_A$ can also beat the nondegenerate Hamming bound. Let $n_1 = 2$ and $n_2 = 3$. We can derive an asymmetric EACQC with parameters $\mathcal{Q}_A = [[6, 1, 6/3; 2]]$.

EACQCs Beating Existing QECCs and EAQECCs. Similar to classical coding theory, constructing quantum codes with parameters better than the best-known results is a central topic in quantum coding theory. It is even more attractive since degenerate quantum codes have significant potential to outperform any nondegenerate quantum code. Indeed, a number of the best-known QECCs in ref. 29 have been shown to be degenerate.

As argued in ref. 4, we say that an EAQECC $[[n, k_1, d; c]]$ is better than a QECC $[[n, k, d]]$ if the net transmission $(k_1 - c)$ is larger than k. Ref. 29 collects a list of classical linear codes and QECCs with the best parameters currently known. According to the construction of EAQECCs in Lemma 2, the quaternary codes in ref. 29 correspond to the best-known nondegenerate EAQECCs. In general, it is not difficult to construct nondegenerate EAQECCs with positive net transmissions better than the best-known QECCs based on ref. 29. However, how to construct degenerate EAQECCs with positive net transmissions that can beat the best-known nondegenerate EAQECCs is largely unknown. This addresses the important question of whether degeneracy can improve on the coding limit in EAQECCs.

We give two explicit constructions to show that EACQCs can beat the best-known QECCs and EAQECCs. According to refs. 38 and 39, there exists a cyclic maximum-distance-separable (MDS) code with parameters $[17, 9, 9]_{16}$. From Lemma 2, we can derive an EA quantum MDS (EAQMDS) code with parameters $[[17, 5, 9; 4]]_4$. Let $Q_I = [[4, 2, 2]]$ be the inner code, and let $Q_O = [[17, 5, 9; 4]]_4$ be the outer code. Then, we can derive an EACQC with parameters $\mathcal{Q}_e = [[68, 10, 18; 8]]$. Compared with the best-known $Q = [[68, 2, 16]]$ QECC in ref. 29, the EACQC $\mathcal{Q}_e$ has a larger minimum distance, while maintaining the same length and net transmission. $\mathcal{Q}_e$ also has a larger minimum distance than the best-known nondegenerate $[[68, 10, 16; 8]]$ EAQECC from ref. 29 of the same length and net transmission.

Let $Q_O = [[65, 17, 33; 16]]_8$ be an EAQMDS code constructed from a cyclic MDS code [65,33,33] in ref. 38, and let $Q_I = [[8, 3, 3; 0]]$. Then, we can derive an EACQC with parameters $\mathcal{Q}_e = [[520, 51, 99; 48]]$ by using $Q_O = [[65, 17, 33; 16]]_8$ and $Q_I = [[8, 3, 3; 0]]$ as the outer and inner codes, respectively. This EACQC is better than the asymptotic Gilbert–Varshamov bound for EAQECCs in ref. 36. In *SI Appendix*, Table S1 and S2, we list more constructions of EACQCs with parameters better than the best-known QECCs and EAQECCs.

In practice, we prefer to use as few ebits as possible to do the EA communication since storing a large number of noiseless ebits is quite difficult. Let $Q_I = [[5, 1, 3; 0]]$ be the inner code, and let $Q_O = [[3, 2, 2; 1]]$ be the outer code; then, we can derive a [[15,2,6;1]] EACQC. This code has larger minimum distance than the best-known standard [[15,1,5]] QECC in ref. 29. By using the MAGMA software (40), we know that there exists a nondegenerate [[15, 8,6;7]] EAQECC. This code has the same minimum distance and net transmission as the $[[15, 2, 6; 1]]$ EACQC. However, the EACQC consumes only one ebit and, thus, is more practical. In *SI Appendix*, Table S3, we list a number of EACQCs with parameters better than the best-known QECCs and EAQECCs, and each EACQC consumes only one ebit.

In ref. 41, several families of q-ary EAQMDS codes with distances larger than $q + 1$ and consuming very few edits were constructed. We use EAQMDS codes in ref. 41 as the outer codes to construct EACQCs that consume very few ebits. We give an example to illustrate the construction. Let $Q_I = [[4, 2, 2; 0]]$ be the inner code, and let a $Q_O = [[17, 4, 8; 1]]_4$ EAQMDS code in ref. 41 be the outer code. Then, we can derive an EACQC with parameters $\mathcal{Q}_e = [[68, 8, 16; 2]]$. This code has a larger minimum distance than the best-known [[68,6,14]] QECC in ref. 29 of the same length and net transmission. It also has a larger minimum distance than the best-known nondegenerate $[[68, 19, 15; 13]]$ EAQECC in ref. 29 of the same length and net transmission. In *SI Appendix*, Table S4, we list a number of EACQCs with better parameters than the best-known QECCs and EAQECCs in ref. 29, and each code consumes only a few ebits.

Thresholds of EACQCs with Noisy Ebits. In this section, we evaluate the performance of EACQCs with noisy ebits. We compute the EF and the error-probability threshold of EACQCs and compare them to standard CQCs. For a quantum channel, the use of a QECC should improve the EF when the error probability is below a specific value, which we call the "threshold." In practical applications, QECCs with sufficiently high thresholds are needed. We will show that EACQCs can outperform CQCs in EF if the ebits are less noisy than the qubits. Further, we will show that the threshold of EACQCs is much higher than that of CQCs when the error probability of ebits is sufficiently lower than that of qubits.

During the process of EA quantum communication, the preshared ebits of Bob need to be stored faultlessly, and EAQECCs can only correct errors on the transmitted qubits. However, noise in Bob's ebits may be inevitable in practical applications (6, 42), and maintaining a large number of noiseless ebits is extremely difficult. In this section, we use EACQCs to correct errors in ebits. In the EACQC scheme, suppose that we use an EAQECC Q_I as the inner code and use a standard stabilizer code Q_O as the outer code. We show that the outer code Q_O cannot only correct errors on the physical qubits, but also can correct errors on the ebits. We construct two EACQCs and show that they can outperform CQCs in EF when the error probability of ebits is lower than that of qubits. We construct a $\mathcal{Q}_B = [[15, 1, 9; 10]]^B$ EACQC by using the $[[5, 1, 3]]$ stabilizer code as the outer code and Bowen's $[[3, 1, 3; 2]]$ EAQECC (32) as the inner code.

Alternately, we can use the $[[5,1,3]]$ stabilizer code as the outer code and the $[[3,1,3;2]]$ EA repetition code as the inner code to construct another $\mathcal{Q}_R=[[15,1,9;10]]^R$ EACQC with the same parameters. Recall that the standard $Q_C=[[25,1,9]]$ CQC is the concatenation of the $[[5,1,3]]$ stabilizer code with itself. It is known that Bowen's $[[3,1,3;2]]$ EAQECC is equivalent to the $[[5,1,3]]$ stabilizer code, and they have the same stabilizers. Thus, the $\mathcal{Q}_B=[[15,1,9;10]]^B$ EACQC is equivalent to the $Q_C=[[25,1,9]]$ CQC. Then, the $\mathcal{Q}_B=[[15,1,9;10]]^B$ EACQC has the same error-correction ability as the $Q_C=[[25,1,9]]$ CQC. Nevertheless, we show that EACQCs can outperform CQCs in EF if the error probability of ebits is lower than that of qubits.

The detailed EF computation of the two EACQCs and the CQC was put in *SI Appendix*, section 3. The EFs of the two EACQCs and the CQC are plotted in Fig. 2. We compare the EF of EACQCs with that of the $[[25,1,9]]$ CQC. If $p_a=p_b$, the EF of the $\mathcal{Q}_B=[[15,1,9;10]]^B$ EACQC is equal to that of the $[[25,1,9]]$ CQC. When $p_b=0.5p_a$, the EF of the $\mathcal{Q}_B=[[15,1,9;10]]^B$ and the $\mathcal{Q}_R=[[15,1,9;10]]^R$ EACQCs can outperform that of the [[25,1,9]] CQC (Fig. 2*B*). As p_b becomes even lower—e.g., $p_b=0.1p_a, 0.01p_a$—the EF of $\mathcal{Q}_B=[[15,1,9;10]]^B$ and $\mathcal{Q}_R=[[15,1,9;10]]^R$ performs much better than that of the $[[25,1,9]]$ CQC (Fig. 2 *C* and *D*). Moreover, $\mathcal{Q}_B=[[15,1,9;10]]^B$ performs better than $\mathcal{Q}_R=[[15,1,9;10]]^R$ when $p_b=p_a$ (Fig. 2*A*). While $p_b=0.1p_a, 0.01p_a$, $\mathcal{Q}_R=[[15,1,9;10]]^R$ performs much better than $\mathcal{Q}_B=[[15,1,9;10]]^B$ and the [[25,1,9]] CQC (Fig. 2 *C* and *D*).

We compare the error-probability threshold of the two EACQCs with that of the CQC. For the [[5,1,3]] stabilizer code and the $[[25,1,9]]$ CQC, the thresholds are $p>0.09$ and $p>0.18$, respectively. Thus, the CQC scheme can improve the error-probability threshold. For the EACQCs, when $p_b=0.5p_a$, the thresholds of $\mathcal{Q}_B=[[15,1,9;10]]^B$ and $\mathcal{Q}_R=[[15,1,9;10]]^R$ are $p>0.25$ and $p>0.14$, respectively. While p_b becomes sufficiently lower—e.g., $p_b=0.01p_a$—the thresholds of $\mathcal{Q}_B=[[15,1,9;10]]^B$ and $\mathcal{Q}_R=[[15,1,9;10]]^R$ are $p>0.41$ and $p>0.47$, respectively. Therefore, the EACQC scheme can greatly improve the error-probability threshold when the error probability of ebits is much lower than that of qubits.

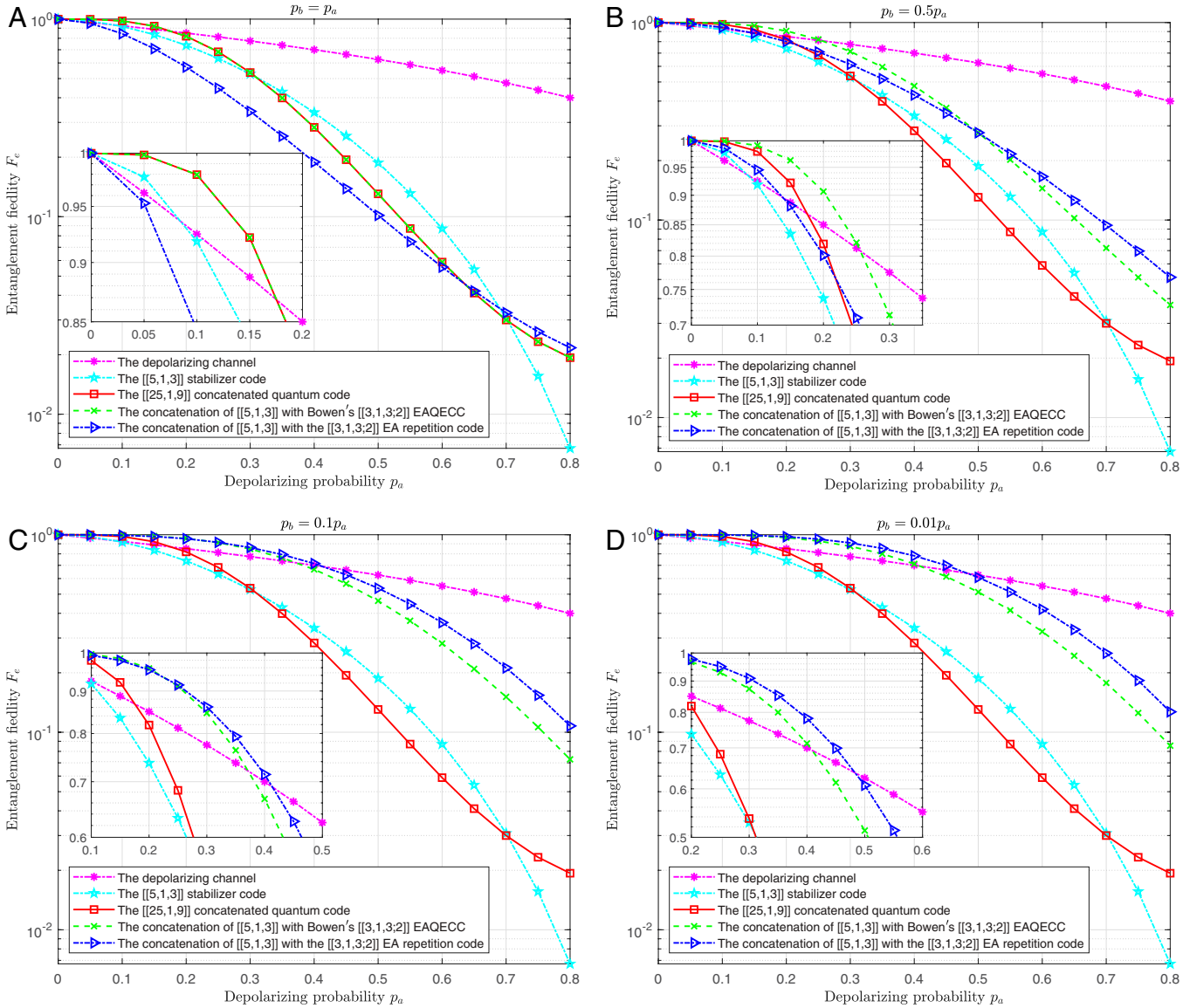

Fig. 2. The EF of EACQCs and CQCs for $p_b=p_a$ (*A*), $p_b=0.5p_a$ (*B*), $p_b=0.1p_a$ (*C*), and $p_b=0.01p_a$ (*D*).

Discussion

In this article, we have proposed the construction of EACQCs by concatenating an inner code with an outer code. We not only have generalized the idea of concatenation to EAQECCs, but also have shown that EACQCs can outperform many existent results. We have further shown that EACQCs can beat the nondegenerate Hamming bound for EAQECCs, while standard CQCs cannot do so. We have derived many EACQCs with larger minimum distances than the best-known QECCs and EAQECCs in ref. 29 of the same length and net transmission. In addition, we have constructed several catalytic EACQCs with little entanglement and better parameters than the best-known QECCs and EAQECCs. We have also constructed a family of asymmetric EACQCs that can beat the nondegenerate Hamming bound for asymmetric EAQECCs. Finally, we have computed the EF of two EACQCs and compared them with the $[[25, 1, 9]]$ CQC. We have shown that EACQCs can outperform CQCs in EF when the ebits are less noisy than qubits. In particular, we have shown that EACQCs have much higher error thresholds than CQCs when the error probability of ebits is sufficiently lower than that of qubits. These properties of EACQCs make them very competitive with standard CQCs for both quantum communication and FTQC.

Data Availability. There are no data underlying this article.

ACKNOWLEDGMENTS. J.F. and M.-H.H. thank Markus Grassl for helpful discussions. This study was supported by National Natural Science Foundation of China Grant 61802175 and NSF Grant CCF-1908308.

Author affiliations: [a]School of Cyber Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China; [b]School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China; [c]Quantum Computing Research Center, Hon Hai Research Institute, Taipei City 114, Taiwan; and [d]Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544

1. I. H. Deutsch, Harnessing the power of the second quantum revolution. *PRX Quantum* **1**, 020101 (2020).
2. J. Preskill, Quantum computing in the NISQ era and beyond. *Quantum* **2**, 79 (2018).
3. A. Calderbank, E. Rains, P. Shor, N. Sloane, Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory* **44**, 1369–1387 (1998).
4. T. Brun, I. Devetak, M. H. Hsieh, Correcting quantum errors with entanglement. *Science* **314**, 436–439 (2006).
5. M. H. Hsieh, I. Devetak, T. Brun, General entanglement-assisted quantum error-correcting codes. *Phys. Rev. A* **76**, 062313 (2007).
6. T. A. Brun, I. Devetak, M. H. Hsieh, Catalytic quantum error correction. *IEEE Trans. Inf. Theory* **60**, 3073–3089 (2014).
7. C. H. Bennett, P. W. Shor, J. A. Smolin, A. V. Thapliyal, Entanglement-assisted classical capacity of noisy quantum channels. *Phys. Rev. Lett.* **83**, 3081–3084 (1999).
8. S. Hao *et al.*, Entanglement-assisted communication surpassing the ultimate classical capacity. *Phys. Rev. Lett.* **126**, 250501 (2021).
9. A. S. Holevo, On entanglement-assisted classical capacity. *J. Math. Phys.* **43**, 4326–4333 (2002).
10. M. H. Hsieh, I. Devetak, A. Winter, Entanglement-assisted capacity of quantum multiple-access channels. *IEEE Trans. Inf. Theory* **54**, 3078–3090 (2008).
11. M. H. Hsieh, M. M. Wilde, Trading classical communication, quantum communication, and entanglement in quantum Shannon theory. *IEEE Trans. Inf. Theory* **56**, 4705–4730 (2010).
12. M. H. Hsieh, M. M. Wilde, Entanglement-assisted communication of classical and quantum information. *IEEE Trans. Inf. Theory* **56**, 4682–4704 (2010).
13. R. Li, L. Guo, Z. Xu, Entanglement-assisted quantum codes achieving the quantum singleton bound but violating the quantum Hamming bound. *Quantum Inf. Comput.* **14**, 1107–1116 (2014).
14. M. Grassl, Entanglement-assisted quantum communication beating the quantum singleton bound. *Phys. Rev. A (Coll. Park)* **103**, L020601 (2021).
15. M. H. Hsieh, W. T. Yen, L. Y. Hsu, High performance entanglement-assisted quantum LDPC codes need little entanglement. *IEEE Trans. Inf. Theory* **57**, 1761–1769 (2011).
16. M. H. Hsieh, T. A. Brun, I. Devetak, Entanglement-assisted quantum quasicyclic low-density parity-check codes. *Phys. Rev. A* **79**, 032340 (2009).
17. Y. Fujiwara, V. D. Tonchev, A characterization of entanglement-assisted quantum low-density parity-check codes. *IEEE Trans. Inf. Theory* **59**, 3347–3353 (2013).
18. M. M. Wilde, M. H. Hsieh, Z. Babar, Entanglement-assisted quantum Turbo codes. *IEEE Trans. Inf. Theory* **60**, 1203–1222 (2013).
19. G. D. Forney Jr., "Concatenated Codes," PhD thesis, Massachusetts Institute of Technology, Cambridge, MA (1965).
20. S. Lin, D. J. Costello, *Error Control Coding: Fundamentals and Applications* (Prentice-Hall, Inc., Upper Saddle River, NJ, ed. 2, 2004).
21. D. J. Costello, G. D. Forney, Channel coding: The road to channel capacity. *Proc. IEEE Inst. Electr. Electron. Eng.* **95**, 1150–1177 (2007).
22. E. Knill, R. Laflamme, Concatenated quantum codes. *arXiv* [Preprint] (1996). https://arxiv.org/abs/quant-ph/9608012. Accessed 20 January 2022.
23. D. Gottesman, "Stabilizer Codes and Quantum Error Correction," PhD thesis, California Institute of Technology, Pasadena, CA (1997).
24. D. Aharonov, M. Ben-Or, "Fault-tolerant quantum computation with constant error" in *STOC'97: Proceedings of the 29th Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1997), pp. 176–188.
25. E. T. Campbell, B. M. Terhal, C. Vuillot, Roads towards fault-tolerant universal quantum computation. *Nature* **549**, 172–179 (2017).
26. P. Sarvepalli, A. Klappenecker, Degenerate quantum codes and the quantum hamming bound. *Phys. Rev. A* **81**, 032318 (2010).
27. D. P. DiVincenzo, P. W. Shor, J. A. Smolin, Quantum-channel capacity of very noisy channels. *Phys. Rev. A* **57**, 830 (1998).
28. J. M. Renes, D. Sutter, F. Dupuis, R. Renner, Efficient quantum polar codes requiring no preshared entanglement. *IEEE Trans. Inf. Theory* **61**, 6395–6414 (2015).
29. M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*. www.codetables.de (2007). Accessed 20 January 2022.
30. P. K. Sarvepalli, A. Klappenecker, M. Rötteler, Asymmetric quantum codes: Constructions, bounds and performance. *Proc. Roy. Soc. A.* **465**, 1645–1672 (2009).
31. J. Fan, J. Li, J. Wang, Z. Wei, M. H. Hsieh, Asymmetric quantum concatenated and tensor product codes with large z-distances. *IEEE Trans. Commun.* **69**, 3971–3983 (2021).
32. G. Bowen, Entanglement required in achieving entanglement-assisted channel capacities. *Phys. Rev. A* **66**, 052313 (2002).
33. M. Grassl, P. Shor, G. Smith, J. Smolin, B. Zeng, Generalized concatenated quantum codes. *Phys. Rev. A* **79**, 50306 (2009).
34. A. M. Steane, Error correcting codes in quantum theory. *Phys. Rev. Lett.* **77**, 793–797 (1996).
35. M. M. Wilde, T. A. Brun, Optimal entanglement formulas for entanglement-assisted quantum coding. *Phys. Rev. A* **77**, 64302 (2008).
36. C. Y. Lai, A. Ashikhmin, Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators. *IEEE Trans. Inf. Theory* **64**, 622–639 (2017).
37. C. Galindo, F. Hernando, R. Matsumoto, D. Ruano, Asymmetric entanglement-assisted quantum error-correcting codes and BCH codes. *IEEE Access* **8**, 18571–18579 (2020).
38. F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1981).
39. G. Seroussi, R. Roth, On MDS extensions of generalized Reed-Solomon codes. *IEEE Trans. Inf. Theory* **32**, 349–354 (1986).
40. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. *J. Symbolic Comp.* **24**, 235–265 (1997).
41. J. Fan, H. Chen, J. Xu, Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q + 1$. *Quantum Inf. Comput.* **16**, 423–434 (2016).
42. C. Y. Lai, T. A. Brun, Entanglement-assisted quantum error-correcting codes with imperfect ebits. *Phys. Rev. A* **86**, 032319 (2012).